

# Citreno Integration Guide

## Ingesting AWS Security Hub Findings

AWS Security Hub Findings in the form of JSON logs can be ingested into Google SecOps SIEM using either Amazon Data Firehose, Amazon S3, or an Amazon S3 with SQS queuing. Findings can also be ingested directly into SOAR using the built-in integration (see details [here](#)), however, we recommend ingestion into SIEM as a baseline.

This document currently provides instructions to ingest using [Amazon Data Firehose](#). Using this method achieves the least amount of latency between time of Security Hub Finding to time of SIEM ingestion.

This guide is applicable to the following Chronicle log types:

- AWS\_SECURITY\_HUB

# Method 1 - AWS Data Firehose

## Part 1 - Google SecOps Admin

1. Navigate to **SIEM Settings** and select **Feeds**.
2. Select **Add New** to configure a new feed.
3. Type an appropriate name, select **Amazon Data Firehose**, and select the **AWS Security Hub** log type.

### ADD FEED

1 Set Properties — 2 Input Parameters — 3 Finalize

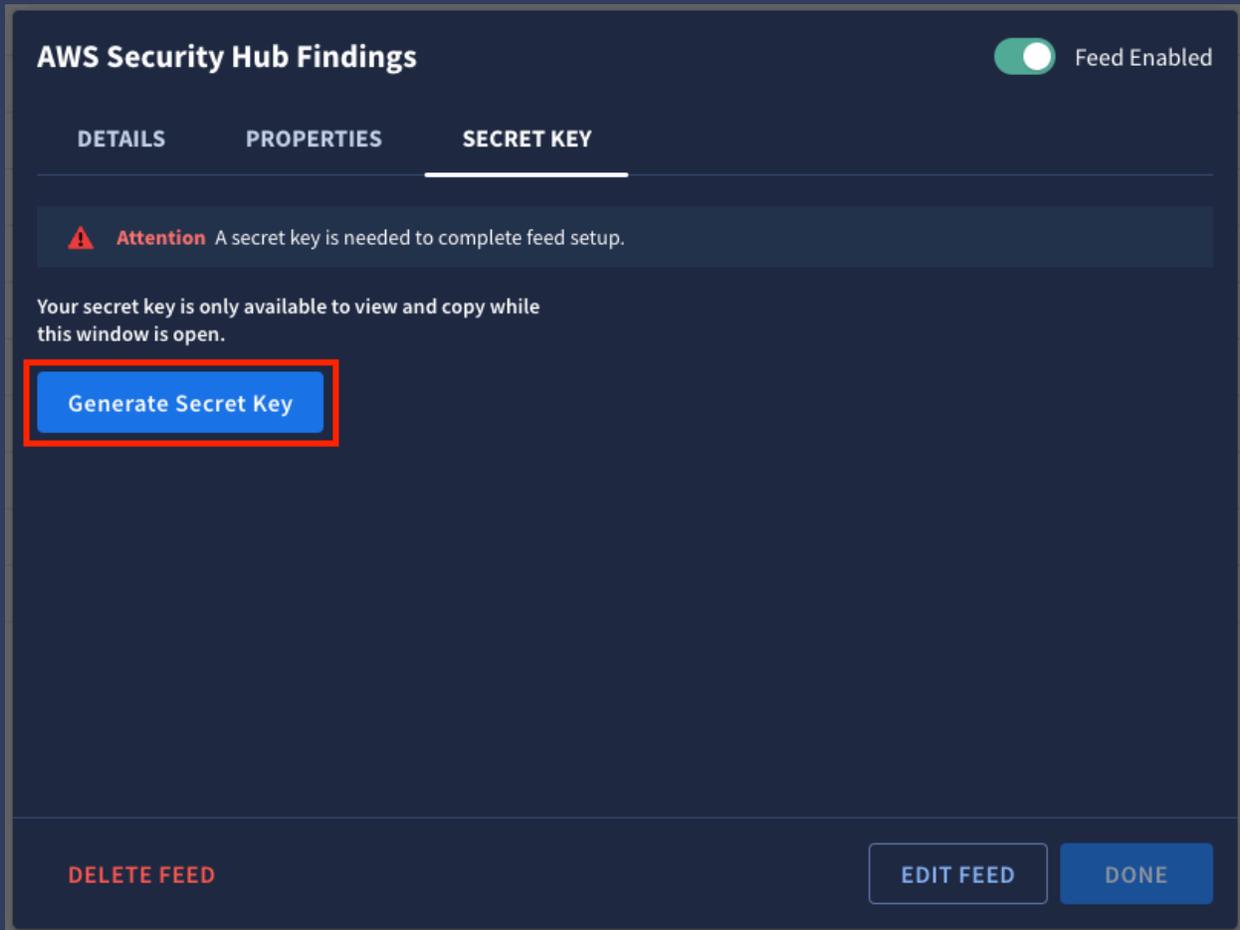
To add a feed, select a source type and log type. [Learn more about adding feeds.](#)

FEED NAME \*

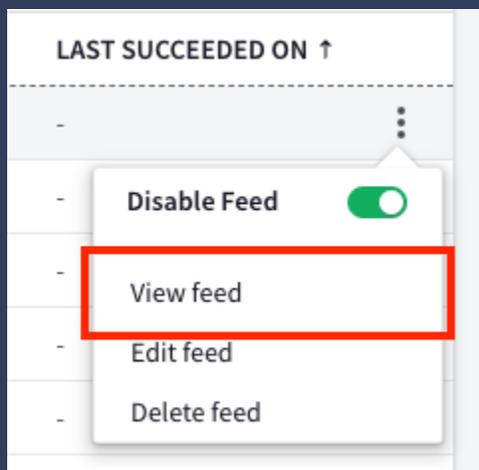
SOURCE TYPE ?

LOG TYPE ?

4. Select **Next**.
5. No split delimiter is required. Add any appropriate **ingestion labels** while here.
6. Select **Next** and then select **Submit**.
7. Select **Generate Secret Key** to generate the **Secret Key** which will be used as the **Firehose Access Key** by the AWS Admin.



8. Copy and save the **Secret Key** for future use. This must be provided to the AWS Admin.
9. Select **Done**.
10. Select **View feed** from the newly created feed's settings dropdown.



11. Copy and save the **Endpoint Information**. This must be provided to the AWS Admin.

The screenshot displays the 'AWS Security Hub Findings' interface. At the top right, there is a toggle switch labeled 'Feed Enabled' which is turned on. Below the title, there are three tabs: 'DETAILS' (selected), 'PROPERTIES', and 'SECRET KEY'. The 'DETAILS' tab shows the following information:

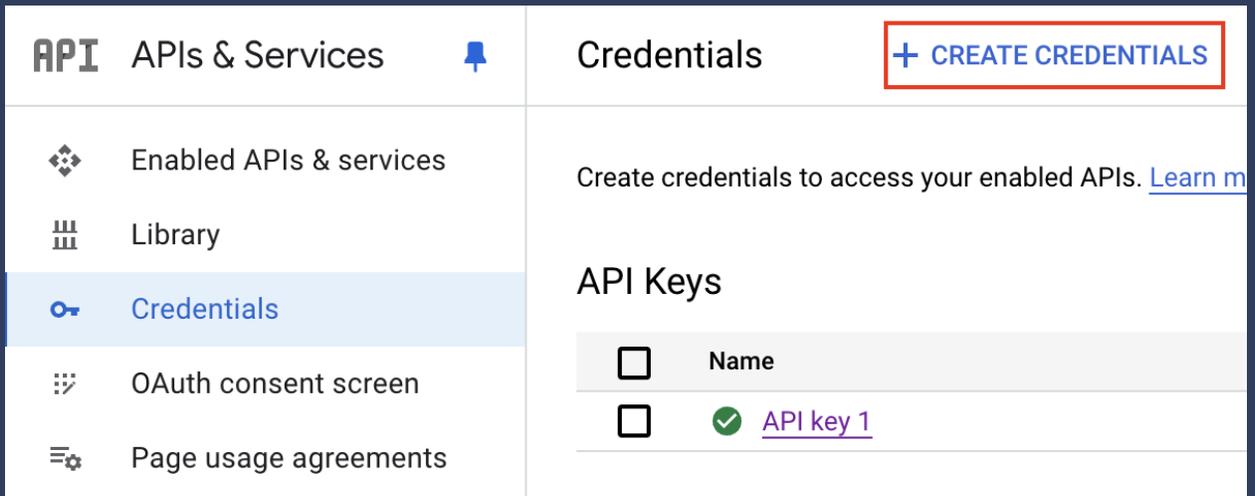
- Source type: Amazon Data Firehose
- status: ACTIVE (with a green checkmark)
- Log type: AWS Security Hub
- Feed ID: [Redacted]

The 'Endpoint Information' section is highlighted with a red box. It contains a text area with the URL 'https://us-' followed by a redacted path. A 'Copy to clipboard' button is located to the right of the text area.

Below the endpoint information, there is a 'Please Note' section with an information icon. The text reads: 'An API key is needed to complete feed setup. To generate an API key, go to the Google Cloud console:'. At the bottom of the interface, there are three buttons: 'DELETE FEED' (in red), 'EDIT FEED', and 'DONE' (in blue).

## Part 2 - GCP Admin

1. Navigate to [console.cloud.google.com](https://console.cloud.google.com)
2. Ensure the Google SecOps Project is selected.
3. Navigate to **APIs & Services** and then **Credentials**.
4. Select **+ Create Credentials**, choosing **API Key**.



The screenshot displays the Google Cloud Platform Admin console interface. On the left, the 'APIs & Services' menu is open, with 'Credentials' selected. The main content area shows the 'Credentials' page, which includes a '+ CREATE CREDENTIALS' button (highlighted with a red box) and a section for 'API Keys'. The 'API Keys' section contains a table with one entry: 'API key 1', which is marked with a green checkmark.

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	API key 1

5. Copy and save the API key. This must be provided to the AWS Admin.
6. Select the API key that was just created and then select **Restrict key**.
7. Search for the **Chronicle API**, selecting **Ok**, and then **Save**.

## Part 3 - AWS Admin

In the following steps, we configure an AWS EventBridge rule to listen for Security Hub Findings and send them to an AWS Data Firehose configured with the Google SecOps endpoint.

1. Navigate to [console.aws.amazon.com](https://console.aws.amazon.com).
2. Navigate to [Amazon Data Firehose](#).
3. Select [Create Firehose stream](#).
4. Select [Direct PUT](#) as Source.
5. Select [HTTP Endpoint](#) as Destination.
6. Choose a descriptive name for the stream.

### Choose source and destination

Specify the source and the destination for your Firehose stream. You cannot change the source and destination of your Firehose stream once it has been created.

**Source** | [Info](#)

Direct PUT

**Destination** | [Info](#)

HTTP Endpoint

---

### Firehose stream name

Firehose stream name

security-hub-stream-to-secops

Acceptable characters are uppercase and lowercase letters, numbers, underscores, hyphens, and periods.

7. Provide the [HTTP endpoint URL](#).
  1. This will be the [Endpoint Information](#) from Google SecOps combined with the [API Key](#) from GCP using a `?key=` parameter in-between.
  2. The format should resemble `[ENDPOINT]?key=[API_KEY]`. See Google documentation [here](#) for more information.
8. Set the [Access key](#) to the [Secret key](#) generated from the Google SecOps Feeds UI.

**Destination settings** [Info](#)  
Specify the destination settings for your Firehose stream.

**HTTP endpoint name - optional**  
Google SecOps - AWS Security Hub Endpoint

**HTTP endpoint URL**  
Enter a HTTP endpoint URL  
Format: https://xyz.httpendpoint.com

**Authentication** [Info](#)  
Specify how you want to configure the authentication to access your destination.

Use access key  
 Use AWS Secrets Manager - *new*  
Choose this to retrieve your secrets programmatically. This incurs an additional cost.  
To learn more, see [AWS Secrets Manager pricing](#).

**Access key - optional**  
Contact the endpoint owner to obtain the access key required to enable data delivery to their service from Amazon Data Firehose.  
Enter access key  
 Show access key

9. Configure **Backup settings** (if required) for failed firehose data.
  1. Select **Failed data only**.
  2. Select **Create** to create an S3 bucket.
  3. Select **Browse** and select the newly created S3 bucket.
  4. Optionally, create a secondary feed in Google SecOps that reads directly from the failed bucket. Documentation to ingest from an S3 Bucket can be found [here](#). This is not difficult, but will require collaboration between a Google SecOps Admin and an AWS Admin.
10. Select **Create Firehose stream**. The Firehose stream is now created.
11. Next, navigate to **Amazon EventBridge**.
12. Select **Rules** and then **Create rule**.
13. Choose a name and select **Next**

**Define rule detail** [Info](#)

**Rule detail**

**Name**

Maximum of 64 characters consisting of numbers, lower/upper case letters, -, \*, \_

**Description - optional**

**Event bus** [Info](#)

Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.

Enable the rule on the selected event bus

**Rule type** [Info](#)

**Rule with an event pattern**

A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.

**Schedule**

A rule that runs on a schedule

[Cancel](#) [Next](#)

14. Scroll to the bottom and select **Custom pattern (JSON editor)**.

15. Specify the **Event pattern** as the following:

```

{
  "source": ["aws.securityhub"],
  "detail-type": ["Security Hub Findings - Custom Action", "Security Hub Findings - Imported"]
}
```

16. Select **Next**.

17. Select **AWS service** as the target type and **Firehose stream** as the target.

18. Select the **Stream** that was previously created.

### Select target(s)

**Permissions**  
 Note: When using the EventBridge console, EventBridge will automatically configure the proper permissions for the selected targets. If you're using the AWS CLI, SDK, or CloudFormation, you'll need to configure the proper permissions.

#### Target 1

**Target types**  
 Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

EventBridge event bus  
 EventBridge API destination  
 AWS service

**Select a target** [Info](#)  
 Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

Firehose stream

**Stream**  
 security-hub-stream-to-secops

**Execution role**  
 EventBridge needs permission to send events to the target specified above. By continuing, you are allowing us to do so. [EventBridge and AWS Identity and Access Management](#)

Create a new role for this specific resource
  Use existing role

**Role name**  
 Amazon\_EventBridge\_Invoke\_Firehose\_2029029122

▶ **Additional settings**

Add another target
Cancel
Skip to Review and create
Previous
Next

19. Select **Next**, **Next** again, and then **Create Rule**.

20. AWS Security Hub Findings should now ingest into Google SecOps SIEM. Please note that in the Google SecOps Feeds UI, Amazon Data Firehose feeds will not display “last succeeded on” information.