citreno

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.

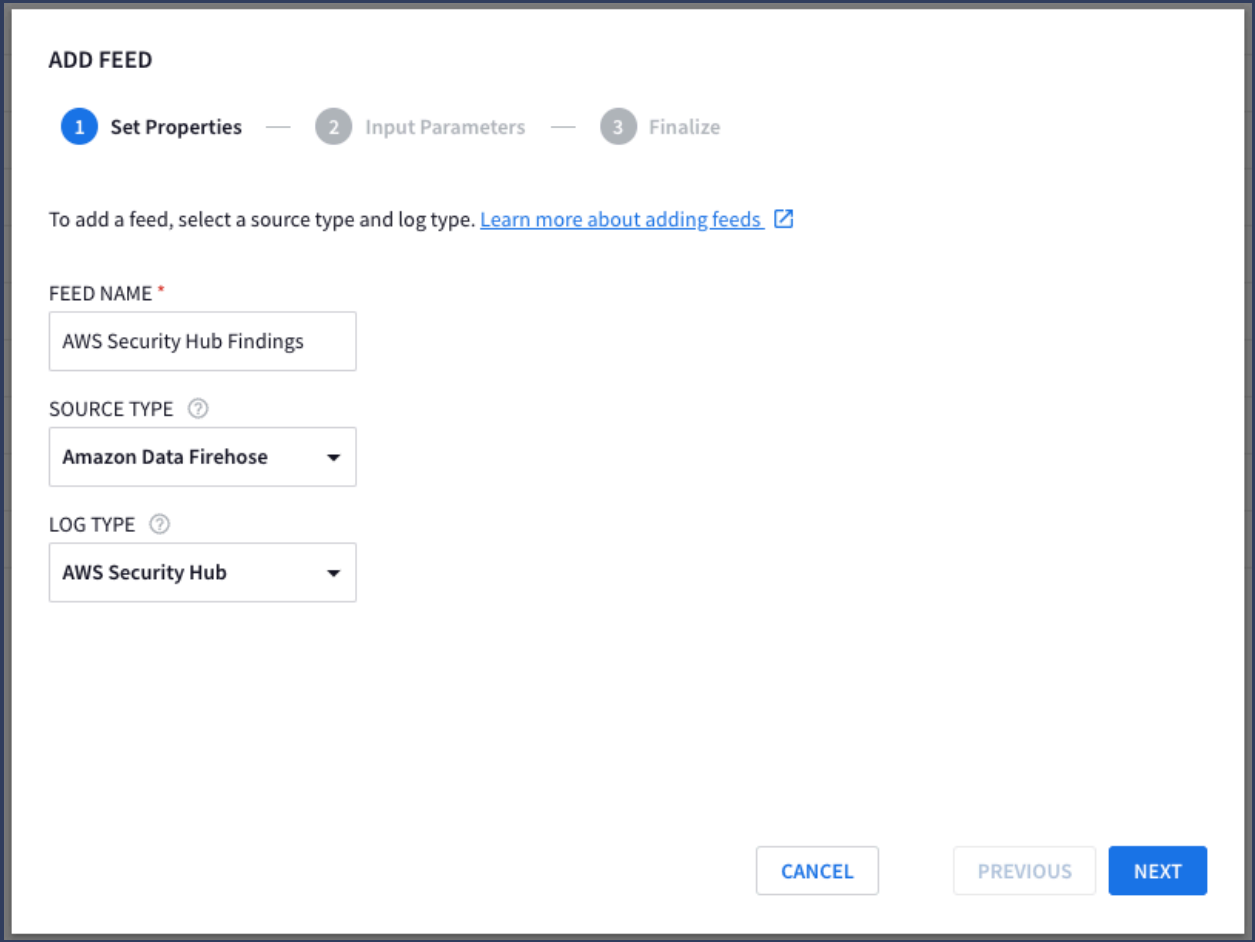
This guide is applicable to the following Chronicle log types:

- ☐ AWS_SECURITY_HUB

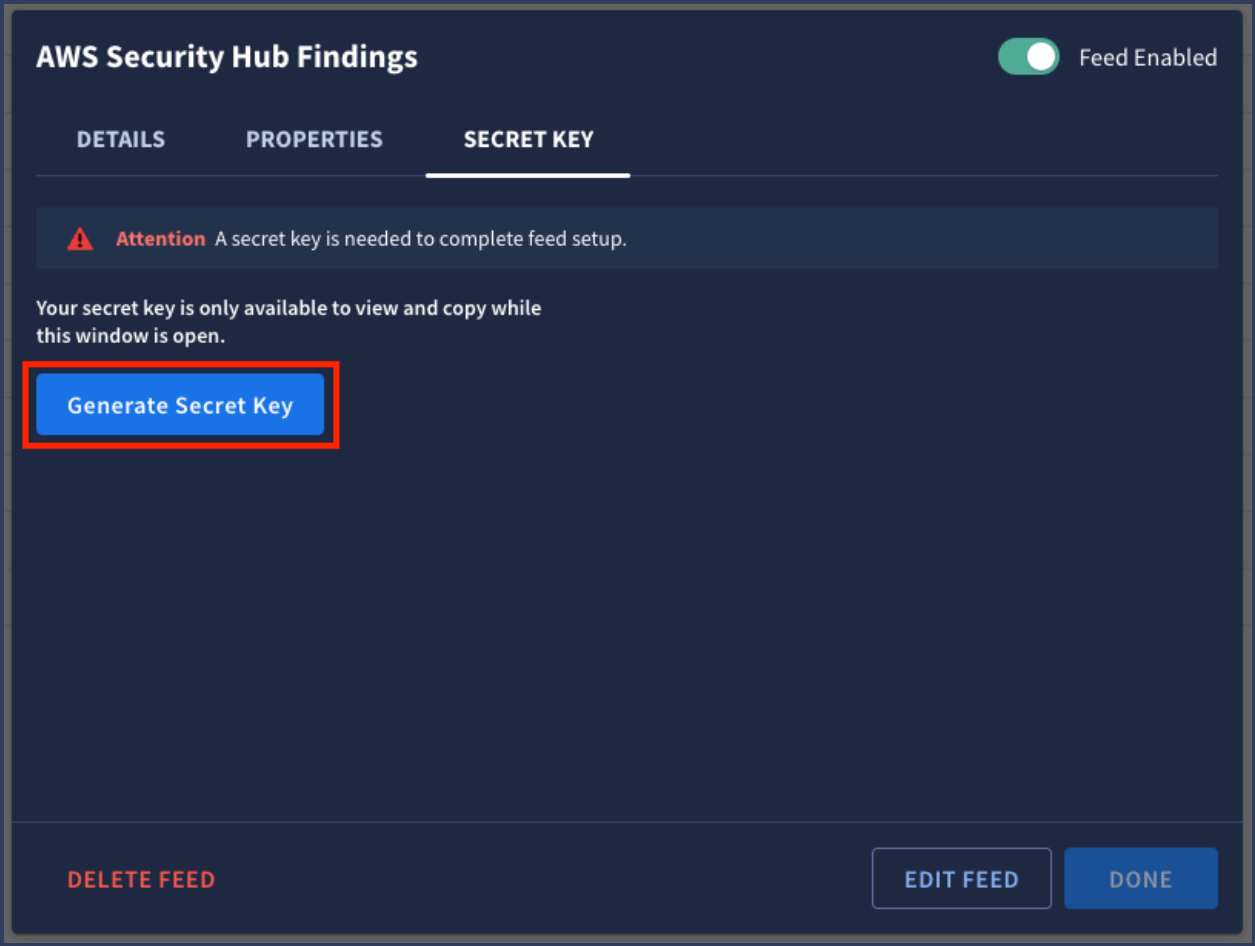
Method 1 - AWS Data Firehose

Part 1 - Google SecOps Admin

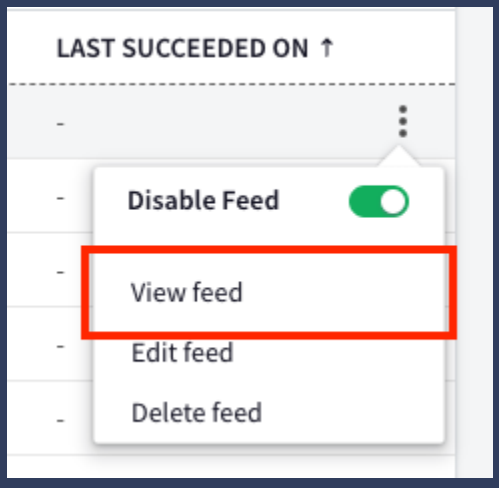
1. Navigate to SIEM Settings and select Feeds.
2. Select Add New to configure a new feed.
3. Type an appropriate name, select Amazon Data Firehose, and select the AWS Security Hub log type.



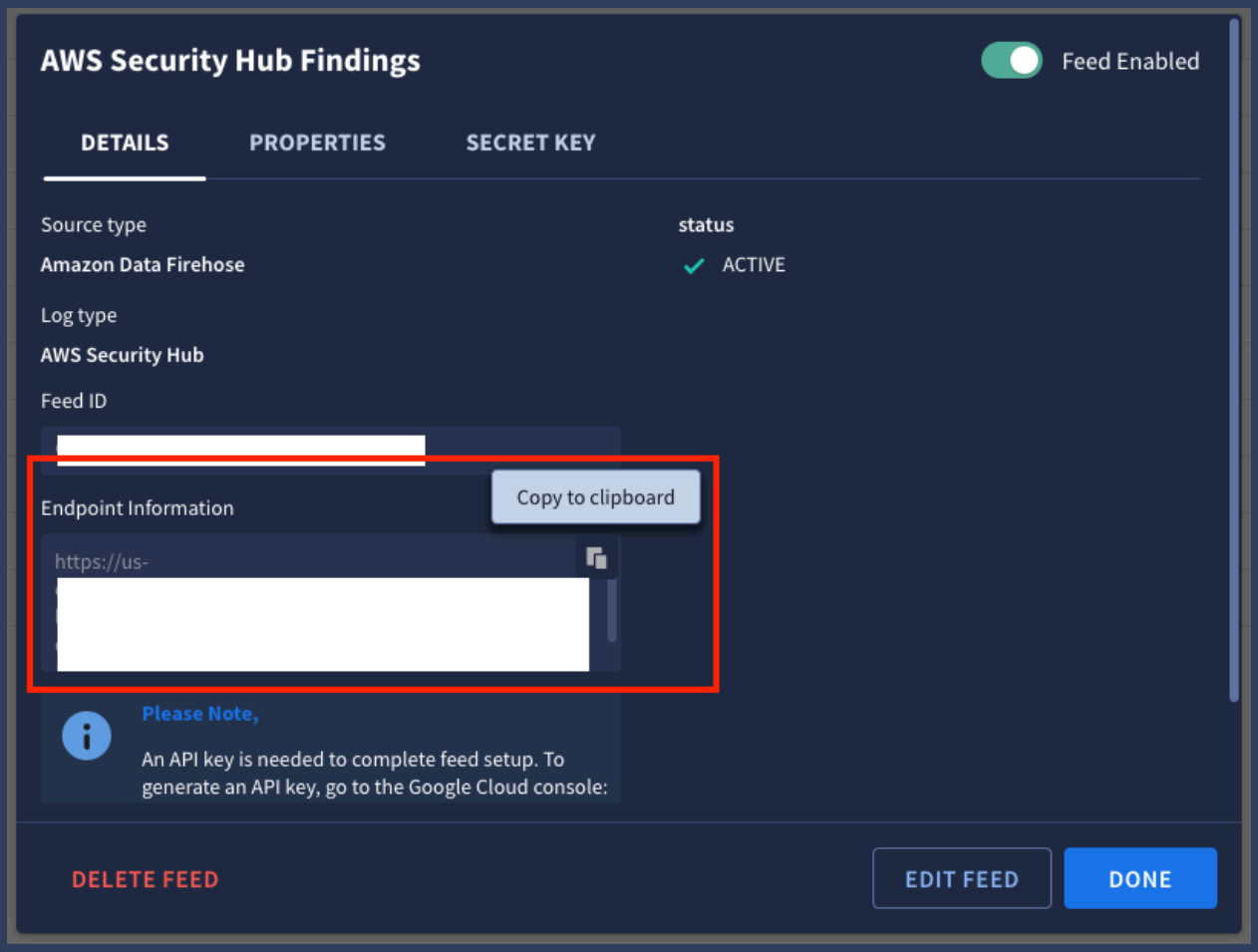
4. Select Next.
5. No split delimiter is required. Add any appropriate ingestion labels while here.
6. Select Next and then select Submit.
7. Select Generate Secret Key to generate the Secret Key which will be used as the Firehose Access Key by the AWS Admin.



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.

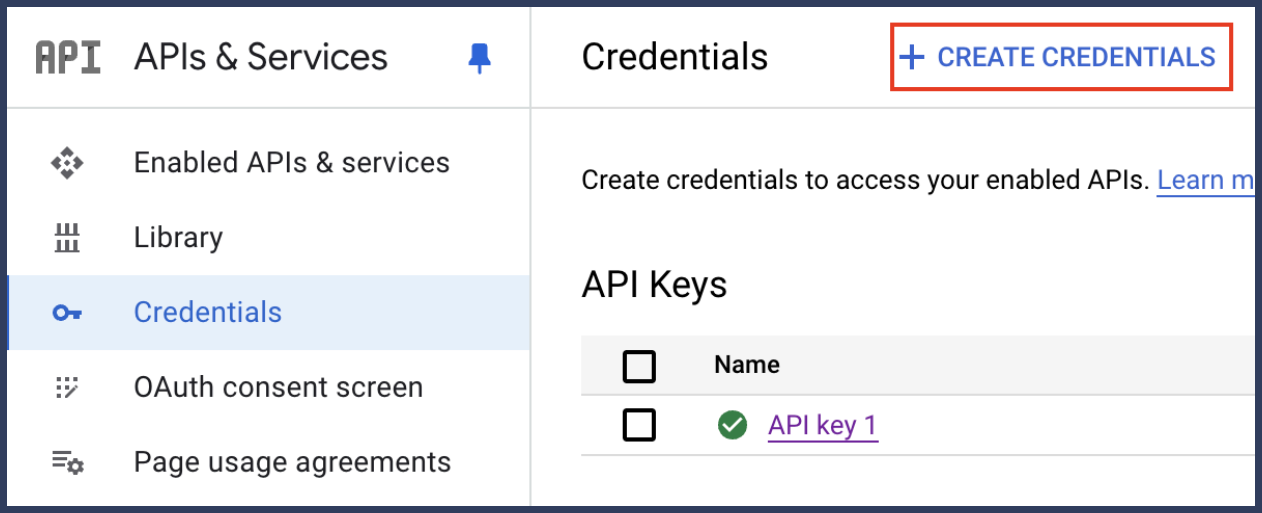


11. Copy and save the Endpoint Information. This must be provided to the AWS Admin.



Part 2 - GCP Admin

1. Navigate to 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.

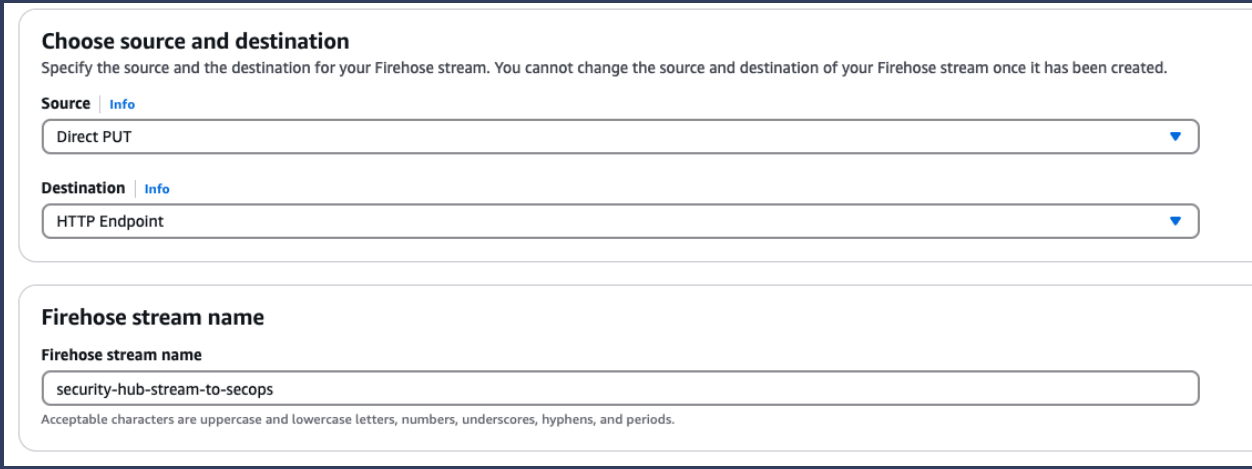


5. Copy and save the API key. This must be provided to the AWS Admin.
6. Select the API key that was just created and then select Restrict key.
7. Search for the Chronicle API, selecting Ok, and then Save.

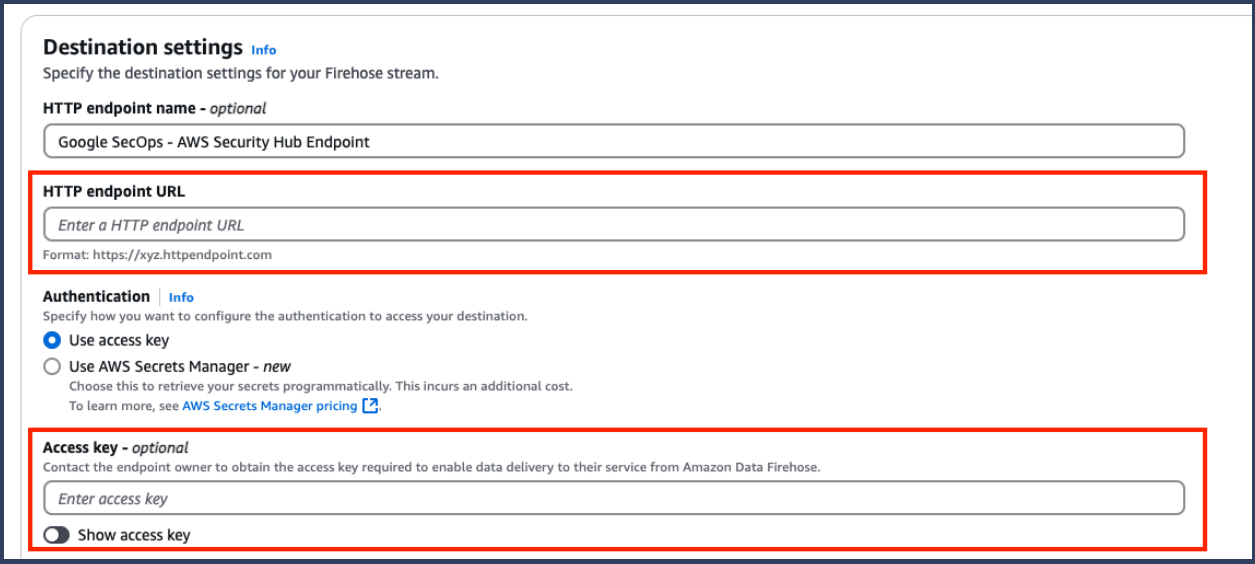
Part 3 - AWS Admin

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.

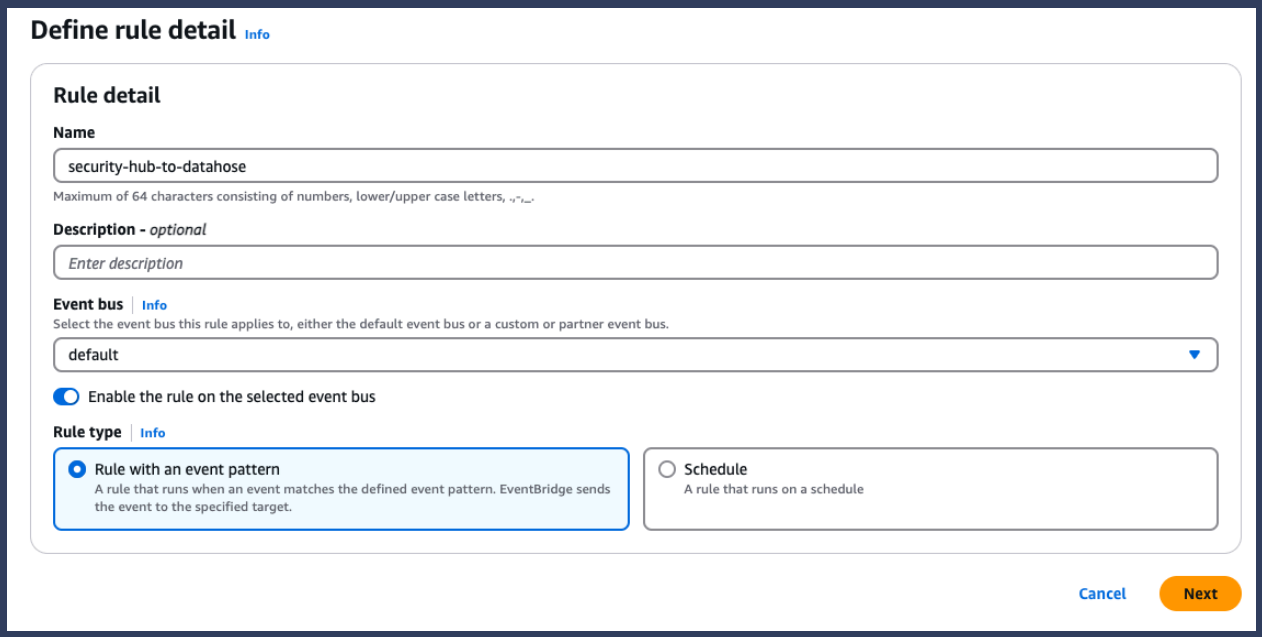
1. Navigate to console.aws.amazon.com.
2. Navigate to Amazon Data Firehose.
3. Select Create Firehose stream.
4. Select Direct PUT as Source.
5. Select HTTP Endpoint as Destination.
6. Choose a descriptive name for the stream.



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.



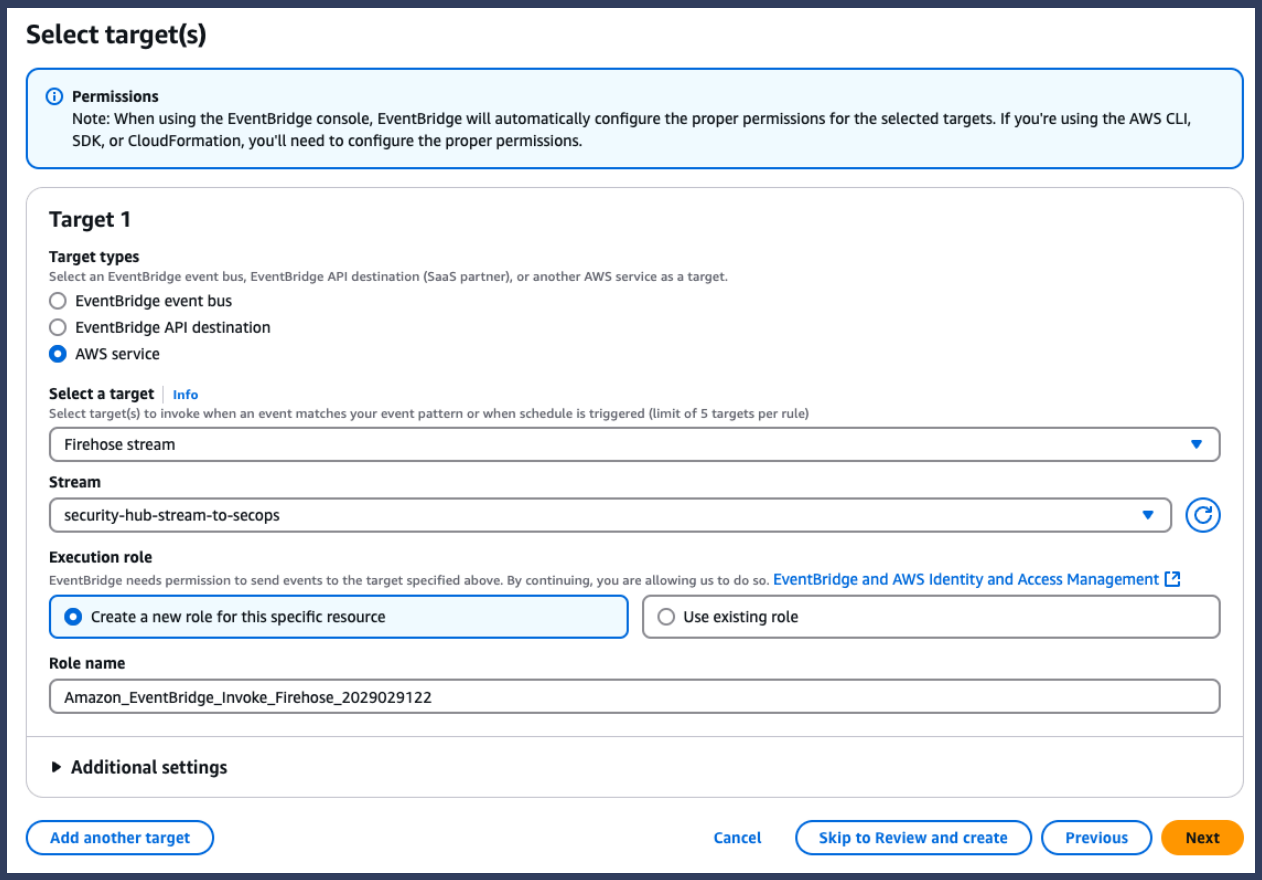
9. Configure Backup settings (if required) for failed firehose data.
    1. Select Failed data only.
    2. Select Create to create an S3 bucket.
    3. Select Browse and select the newly created S3 bucket.
    4. Optionally, create a secondary feed in Google SecOps that reads directly from the failed 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



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.



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.