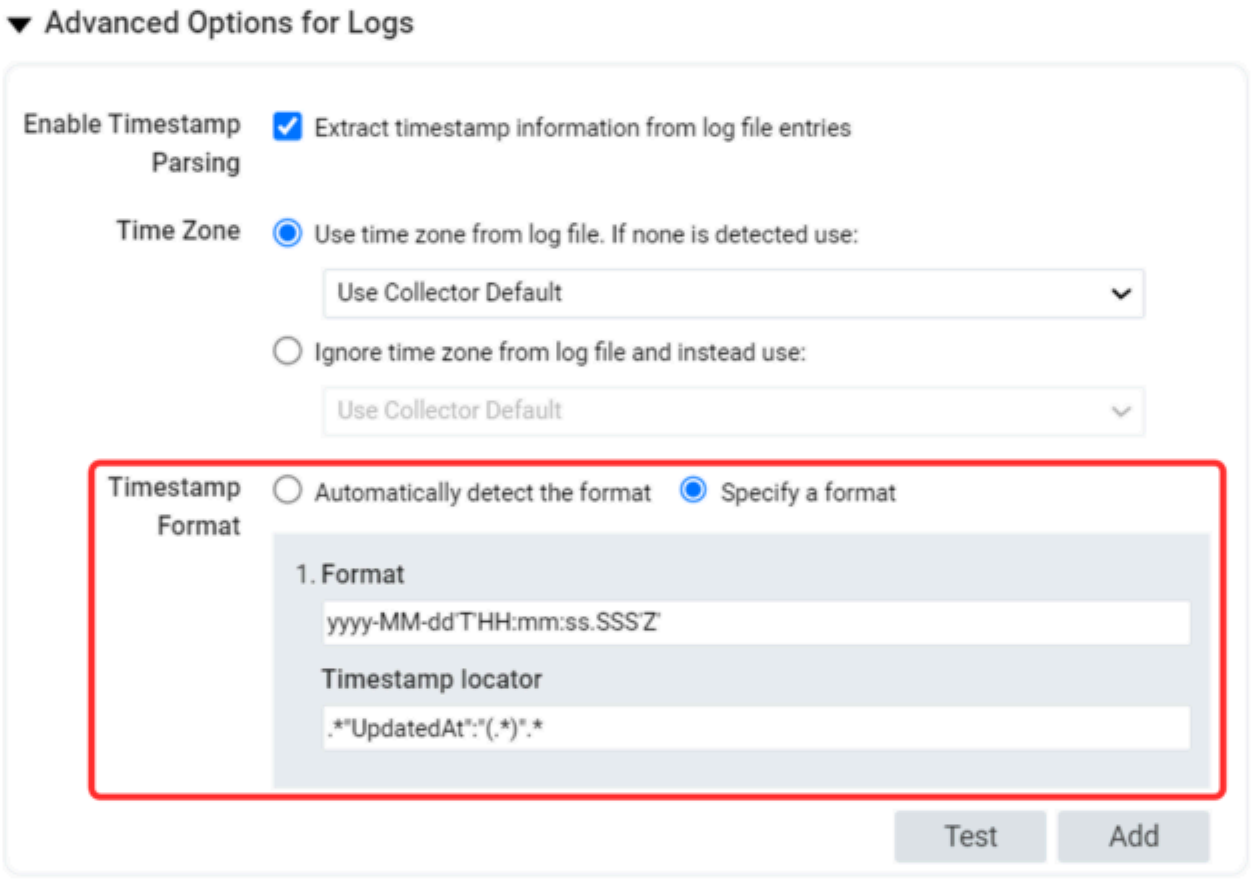
How to Send AWS Security Hub Logs to Sumo Logic

dev.classmethod.jp/articles/aws-security-hub-sumo-logic-20230711-sakumashogo

佐久間昇吾

July 11, 2023



▼ Advanced Options for Logs

Enable Timestamp Parsing ☑ Extract timestamp information from log file entries

Time Zone ● Use time zone from log file. If none is detected use:

Use Collector Default

○ Ignore time zone from log file and instead use:

Use Collector Default

Timestamp Format ○ Automatically detect the format ● Specify a format

1. Format

yyyy-MM-dd'T'HH:mm:ss.SSS'Z'

Timestamp locator

.*"UpdatedAt":"(.*)".*

First

I looked at how to send AWS Security Hub logs to Sumo Logic and visualize them using the App Catalog. The setup is the same for both single-account and multi-account integrated AWS Security Hub, so I hope this helps.

For more information about multi-account AWS Security Hub, please refer to [Update] Security Hub now integrates with AWS Organizations! Now you can easily set up and manage your organization's security check environment | Developers IO .

We will proceed under the assumption that AWS Security Hub is ready and that an S3 bucket for storing logs has already been created.

Steps to integrate AWS Security Hub logs with Sumo Logic

I tried this with reference to this document: Collecting Findings for the AWS Security Hub App | Sumo Logic .

First, create the following items on the Sumo Logic side:

STEP 1 - Sumo Logic Configuration

- **Hosted Collector**
  Reference URL: https://help.sumologic.com/docs/send-data/hosted-collectors/configure-hosted-collector/

- **S3 Source**
  Reference URL: https://help.sumologic.com/docs/send-data/hosted-collectors/amazon-aws/aws-s3-source/#create-an-amazons3-source

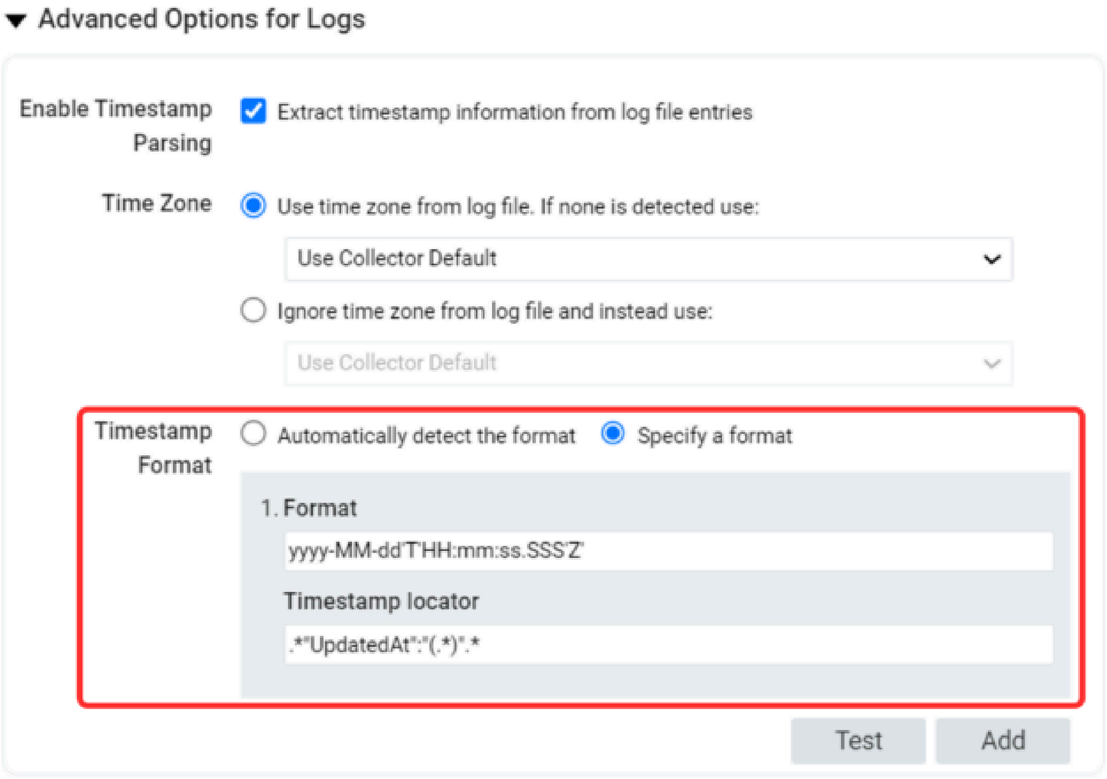
  * Set **the Advanced Options for Logs item as follows:**

  - Format

    ```
    yyyy-MM-dd'T'HH:mm:ss.SSS'Z'
    ```

  - Timestamp locator

    ```
    .*"UpdatedAt": "(.*)".*
    ```



▼ Advanced Options for Logs

Enable Timestamp Parsing ☑ Extract timestamp information from log file entries

Time Zone ● Use time zone from log file. If none is detected use: Use Collector Default

○ Ignore time zone from log file and instead use: Use Collector Default

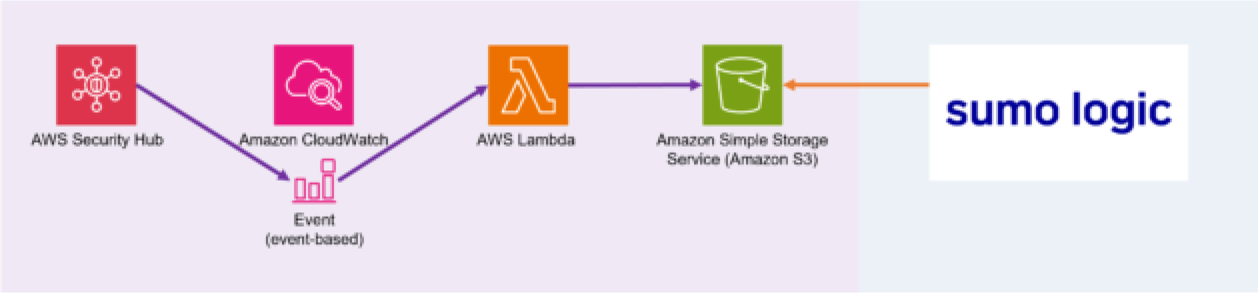
Timestamp Format ○ Automatically detect the format ● Specify a format

1. Format: yyyy-MM-dd'T'HH:mm:ss.SSS'Z'

Timestamp locator: .*"UpdatedAt":"(.*)".*

STEP 2 - Deploying resources for data collection on AWS

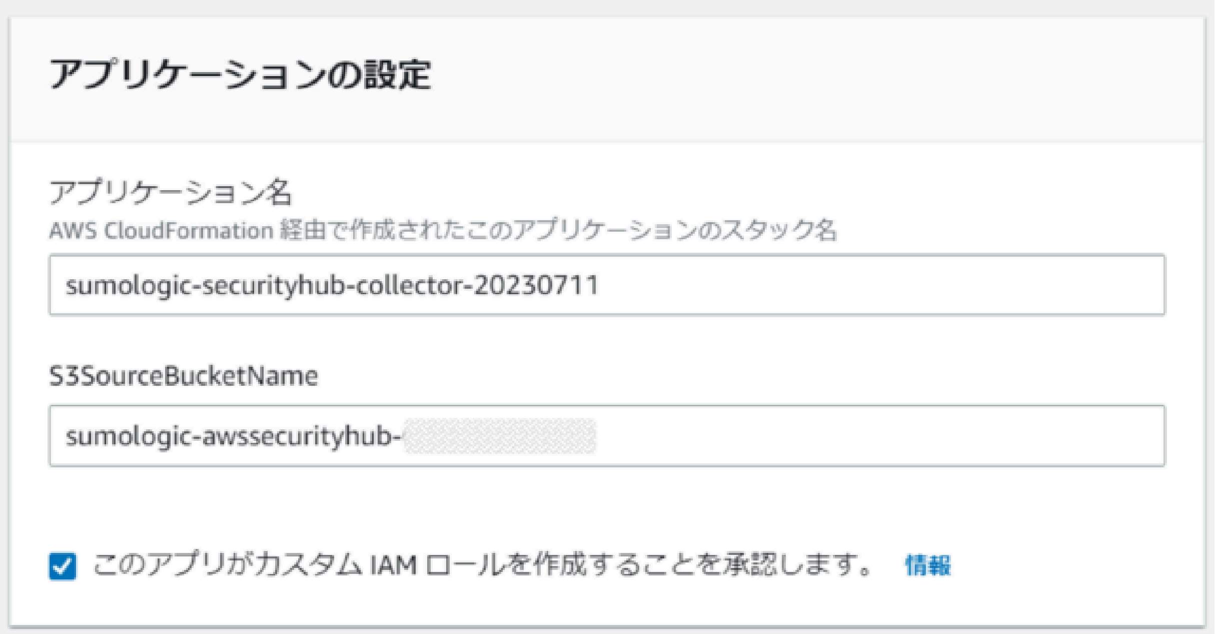
Next, we use the AWS SAM template provided by Sumo Logic to deploy a pipeline for sending data.



This procedure should be performed in the account from which you want to collect data. If you have a multi-account integration, perform this procedure in the parent AWS account.

- **Deploying the AWS SAM template**
  Go to AWS Serverless Application Repository - Sumologic-securityhub-collector | AWS and choose Deploy.

  Enter the stack name for the deployed application and the name of the S3 bucket that stores the AWS Security Hub logs. Also, check the box to agree to create a custom IAM role, and then choose Deploy.



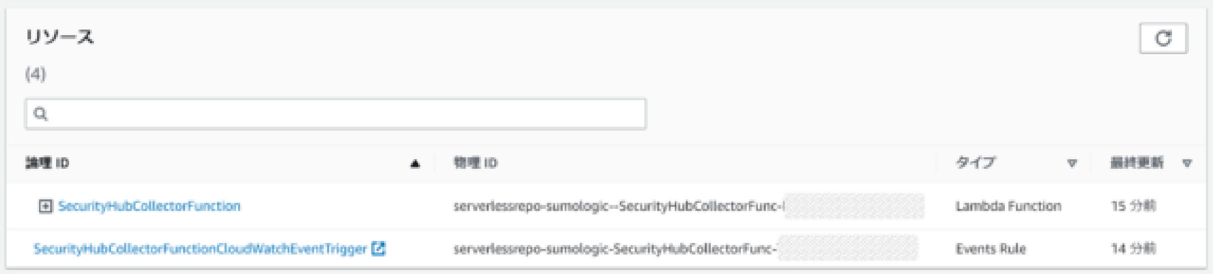
アプリケーションの設定

アプリケーション名
AWS CloudFormation 経由で作成されたこのアプリケーションのスタック名
sumologic-securityhub-collector-20230711

S3SourceBucketName
sumologic-awssecurityhub-[redacted]

☑ このアプリがカスタム IAM ロールを作成することを承認します。 情報

After a short while, you will be redirected to the Lambda console screen to confirm that the resources have been launched.



リソース

(4)

論理 ID	物理 ID	タイプ	最終更新
SecurityHubCollectorFunction	serverlessrepo-sumologic--SecurityHubCollectorFunc-[redacted]	Lambda Function	15 分前
SecurityHubCollectorFunctionCloudWatchEventTrigger	serverlessrepo-sumologic-SecurityHubCollectorFunc-[redacted]	Events Rule	14 分前

This completes the steps to integrate AWS Security Hub logs with Sumo Logic.

If no data is coming in, it's often a permissions issue. Try checking your Sumo Logic → AWS resource permissions .

In terms of the procedure, in STEP 1, creating an S3 Source, you set up permissions for Sumo Logic to collect data from your AWS S3 bucket.

Introducing the App Catalog

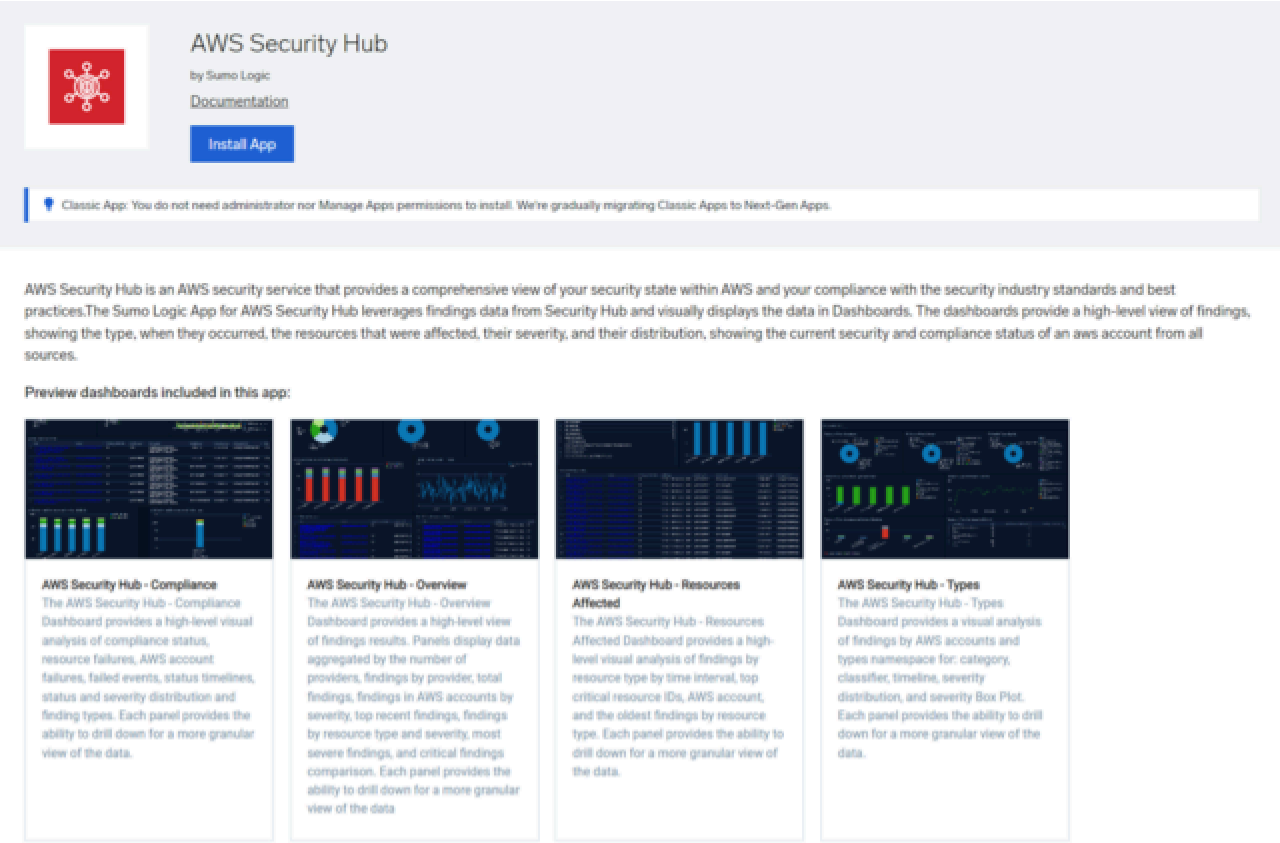
Once you have connected your data to Sumo Logic, try visualizing it in the App Catalog.

Source: Installing the AWS Security Hub App | Sumo Logic

Deploying the AWS Security Hub App

On the App Catalog screen, enter "AWS Security Hub" in the search bar to display the app, then select it.

Then select Install App.



AWS Security Hub

by Sumo Logic

Documentation

Classic App: You do not need administrator nor Manage Apps permissions to install. We're gradually migrating Classic Apps to Next-Gen Apps.

AWS Security Hub is an AWS security service that provides a comprehensive view of your security state within AWS and your compliance with the security industry standards and best practices.The Sumo Logic App for AWS Security Hub leverages findings data from Security Hub and visually displays the data in Dashboards. The dashboards provide a high-level view of findings, showing the type, when they occurred, the resources that were affected, their severity, and their distribution, showing the current security and compliance status of an aws account from all sources.

Preview dashboards included in this app:

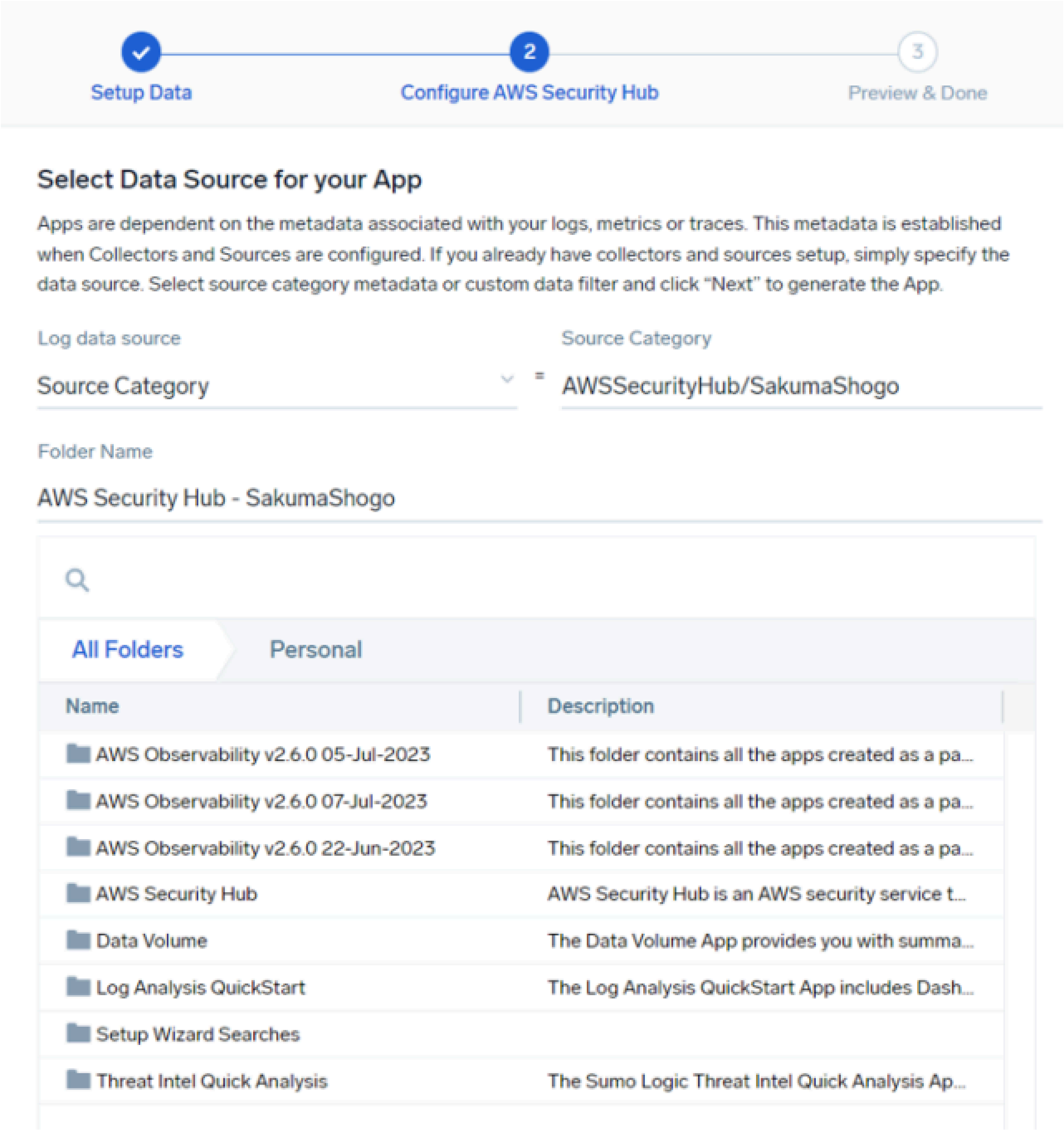
AWS Security Hub - Compliance
The AWS Security Hub - Compliance Dashboard provides a high-level visual analysis of compliance status, resource failures, AWS account failures, failed events, status timelines, status and severity distribution and finding types. Each panel provides the ability to drill down for a more granular view of the data.

AWS Security Hub - Overview
The AWS Security Hub - Overview Dashboard provides a high-level view of findings results. Panels display data aggregated by the number of providers, findings by provider, total findings, findings in AWS accounts by severity, top recent findings, findings by resource type and severity, most severe findings, and critical findings comparison. Each panel provides the ability to drill down for a more granular view of the data

AWS Security Hub - Resources Affected
The AWS Security Hub - Resources Affected Dashboard provides a high-level visual analysis of findings by resource type by time interval, top critical resource IDs, AWS account, and the oldest findings by resource type. Each panel provides the ability to drill down for a more granular view of the data.

AWS Security Hub - Types
The AWS Security Hub - Types Dashboard provides a visual analysis of findings by AWS accounts and types namespace for: category, classifier, timeline, severity distribution, and severity Box Plot. Each panel provides the ability to drill down for a more granular view of the data.

All that's left to do is set the Source Category for the S3 Source, the dashboard name, and the save location, and then select Next.



Select Data Source for your App

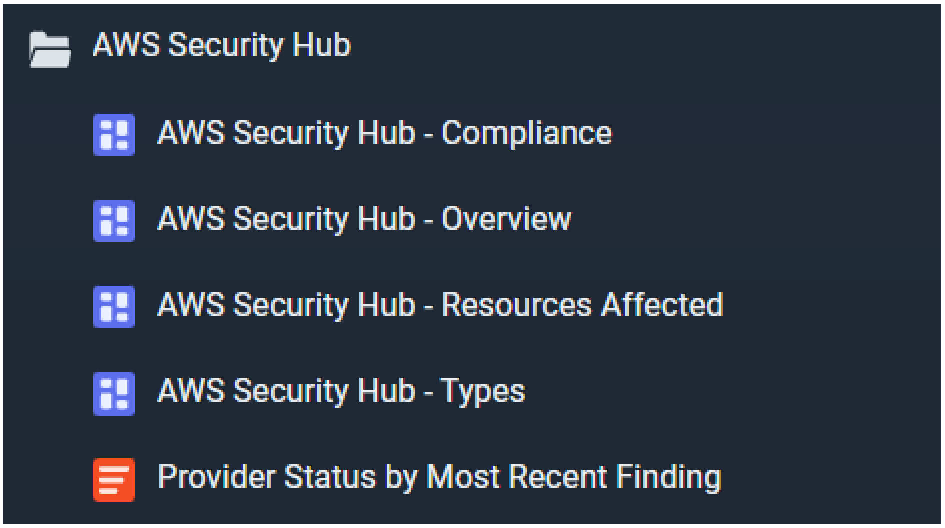
Apps are dependent on the metadata associated with your logs, metrics or traces. This metadata is established when Collectors and Sources are configured. If you already have collectors and sources setup, simply specify the data source. Select source category metadata or custom data filter and click "Next" to generate the App.

Log data source: Source Category = Source Category: AWSSecurityHub/SakumaShogo

Folder Name: AWS Security Hub - SakumaShogo

Name	Description
AWS Observability v2.6.0 05-Jul-2023	This folder contains all the apps created as a pa...
AWS Observability v2.6.0 07-Jul-2023	This folder contains all the apps created as a pa...
AWS Observability v2.6.0 22-Jun-2023	This folder contains all the apps created as a pa...
AWS Security Hub	AWS Security Hub is an AWS security service t...
Data Volume	The Data Volume App provides you with summa...
Log Analysis QuickStart	The Log Analysis QuickStart App includes Dash...
Setup Wizard Searches	
Threat Intel Quick Analysis	The Sumo Logic Threat Intel Quick Analysis Ap...

After a while, the app will be created. Check the destination folder and select the dashboard.



AWS Security Hub

AWS Security Hub - Compliance

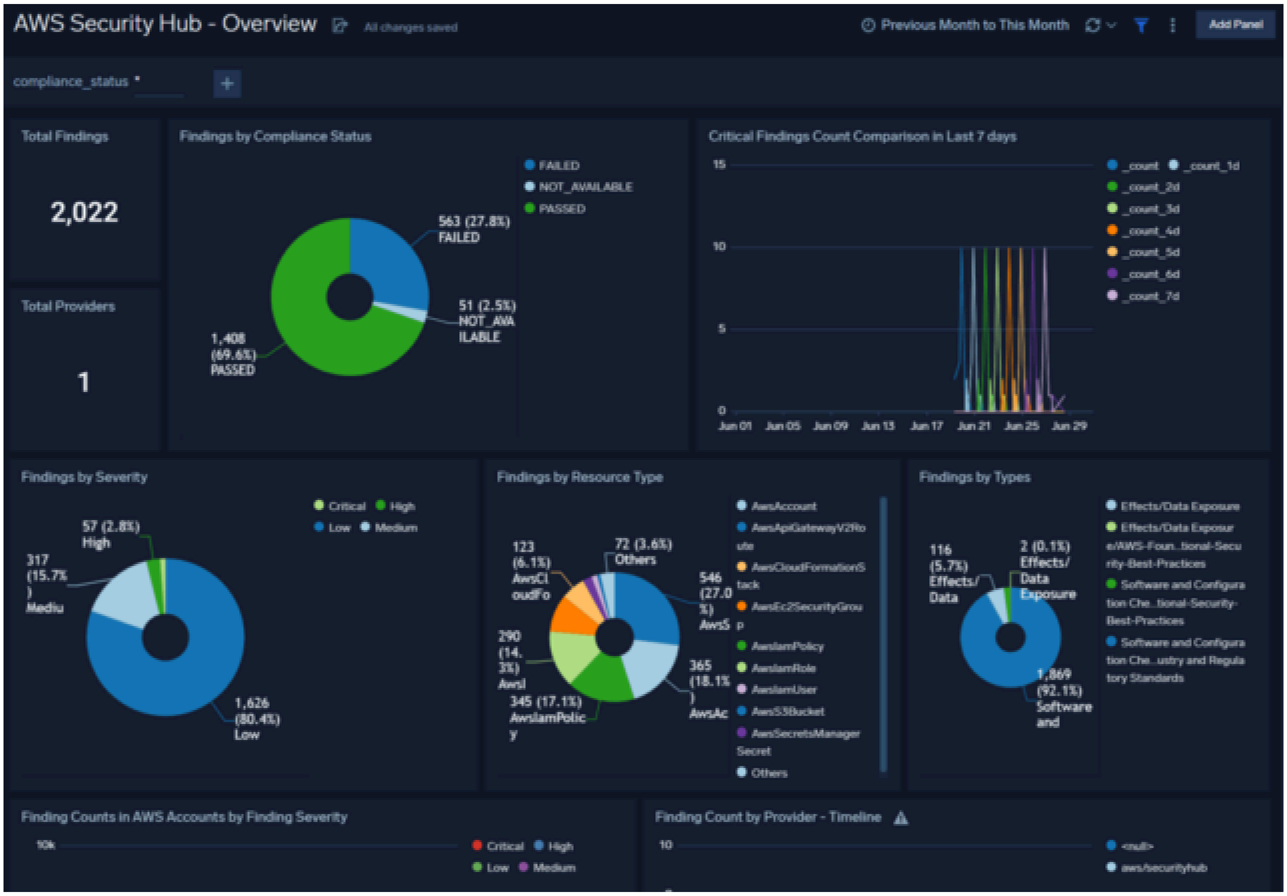
AWS Security Hub - Overview

AWS Security Hub - Resources Affected

AWS Security Hub - Types

Provider Status by Most Recent Finding

I opened the Overview dashboard, which shows how easy it is to visualize data.

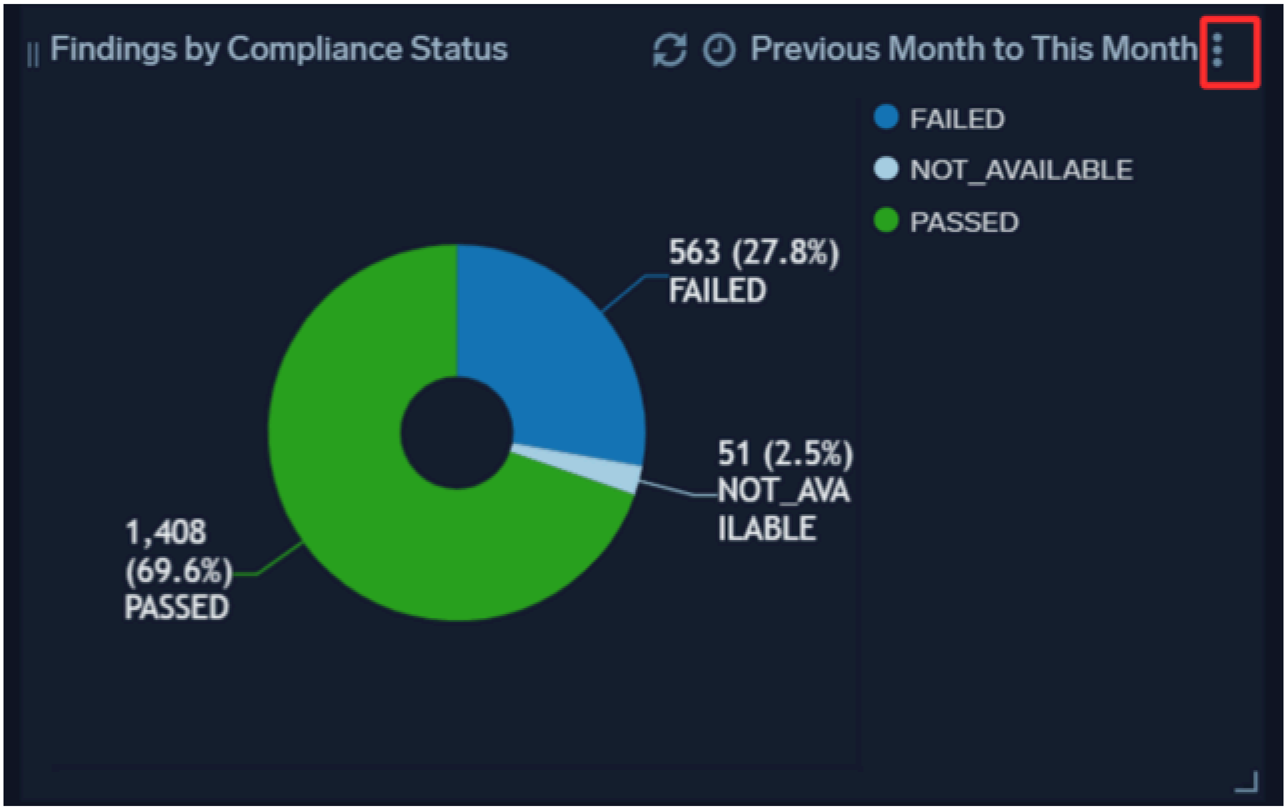


That's all for now.

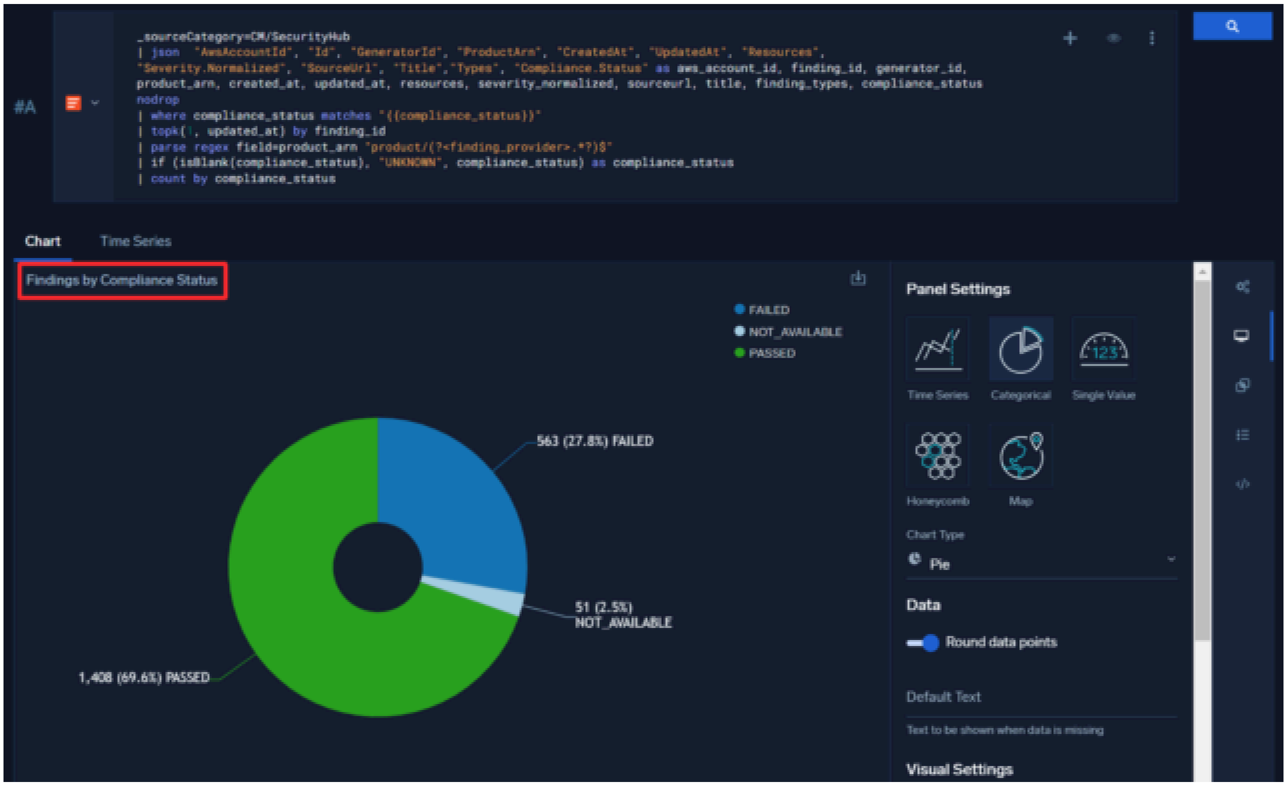
Rename a dashboard panel

As you can see from the image above, the names of each item are displayed in English. You can also change the panel name at this time.

When you place the cursor over the panel, three dots will appear in the upper right corner. Select this and click Edit.



You can change the panel name by selecting the area framed in red on the screen below. Japanese is also available. After changing the name, select Update Dashboard in the upper right corner and the panel name will be in Japanese.



```
_sourceCategory=CM/SecurityHub
| json  "AwsAccountId", "Id", "GeneratorId", "ProductArn", "CreatedAt", "UpdatedAt", "Resources",
"Severity.Normalized", "SourceUrl", "Title","Types", "Compliance.Status" as aws_account_id, finding_id, generator_id,
product_arn, created_at, updated_at, resources, severity_normalized, sourceurl, title, finding_types, compliance_status
nodrop
| where compliance_status matches "{{compliance_status}}"
| topk(1, updated_at) by finding_id
| parse regex field=product_arn "product/(?<finding_provider>.*?)$"
| if (isBlank(compliance_status), "UNKNOWN", compliance_status) as compliance_status
| count by compliance_status
```

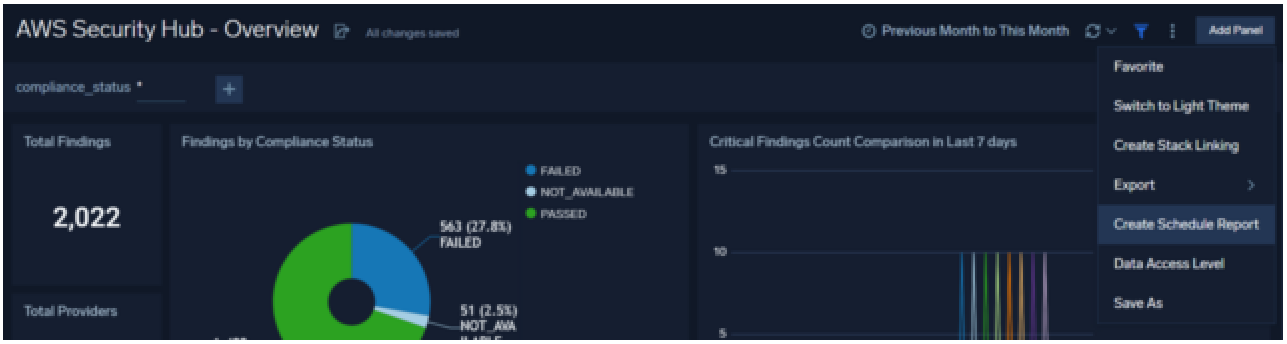
That's it. You can also check the dashboard settings at Dashboard (New) | Sumo Logic .

Regular Dashboard Reporting

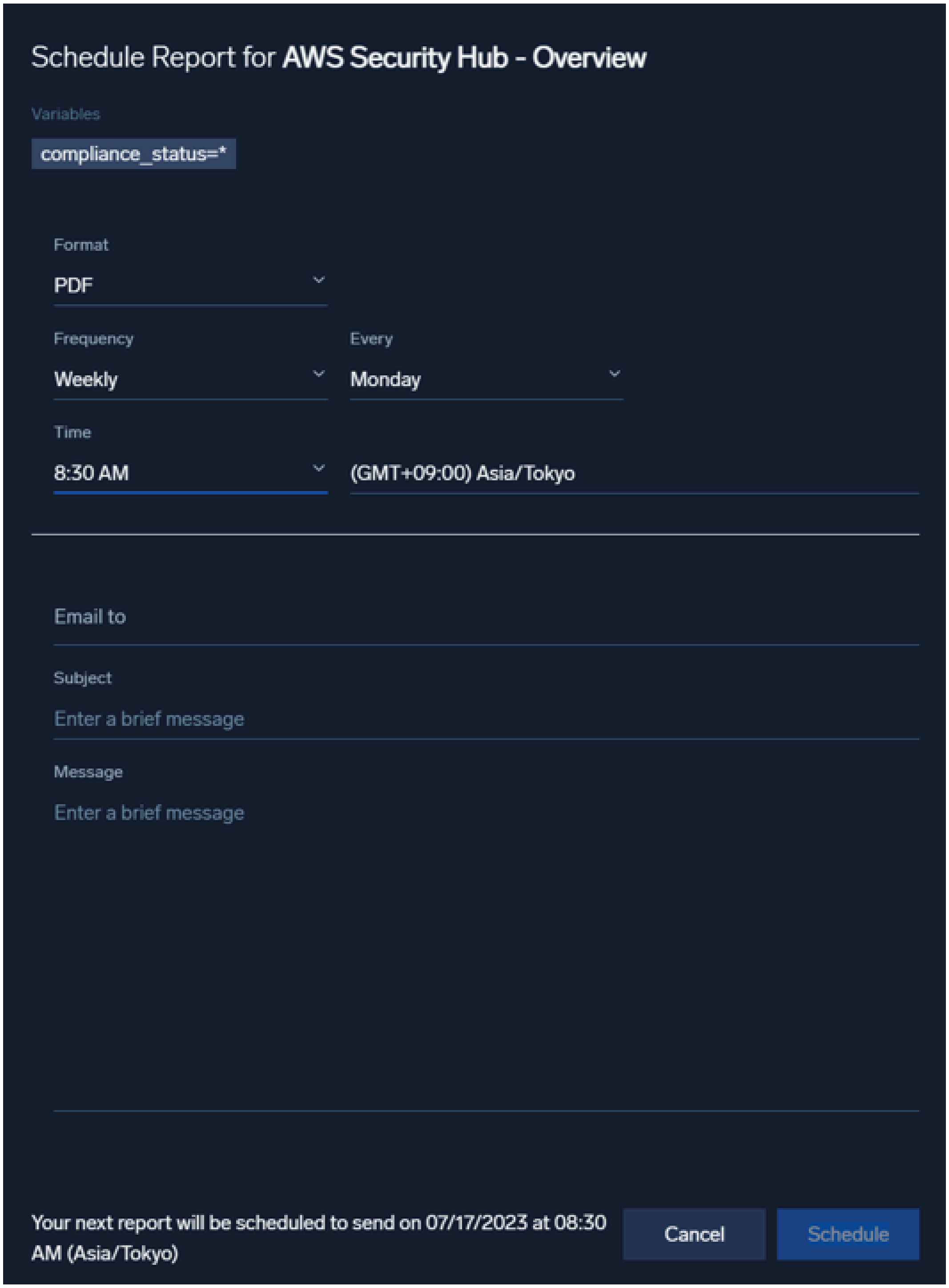
Next, we'd like to introduce Scheduled Report | Sumo Logic , a scheduled reporting feature that was updated this year .

This feature will periodically notify you of the dashboard display contents on a daily/weekly/monthly basis via email address, etc. This is expected to eliminate the need for periodic exports and the issuance of shared URLs, which were previously required. The output format is PNG or PDF.

Let's take a look at the settings screen. Select the three dots in the top right corner of the dashboard > Create Schedule Report.



The following screen will then pop up. All you have to do is select the format and frequency, enter your email address, and click Schedule.



Schedule Report for **AWS Security Hub - Overview**

Variables

compliance_status=*

Format: PDF

Frequency: Weekly

Every: Monday

Time: 8:30 AM

(GMT+09:00) Asia/Tokyo

Email to

Subject: Enter a brief message

Message: Enter a brief message

Your next report will be scheduled to send on 07/17/2023 at 08:30 AM (Asia/Tokyo)

For images, I set it to import at 8:30 on Mondays, assuming a weekly MTG.

summary

What did you think? You probably have various requirements for filtering the AWS Security Hub console, displaying specific items, etc. Even with Sumo Logic, depending on the content, you may need to edit or create new queries. However, as long as you have logs, you can easily narrow down and display items, apply filters, and customize graphs by AWS Account ID, which can improve usability in many ways.

In this article, we have introduced integration with AWS Security Hub, but we would like to continue sharing more information in the future, such as other log integration methods, how to write queries, the App Catalog, and more.

I hope this article will be of some help to someone.