Introducing the Sumo Logic Security App vol.1

dev.classmethod.jp/articles/sumo-logic_security-app-vol-1

酒井剛

May 26, 2022

Dear security operators and administrators, log analysis is important, isn't it?

Sumo Logic's built-in apps allow you to effortlessly gain security insights from ingested logs. Sumo Logic offers over 180 apps, covering not only security but also observability. In this article, we'll take a thorough look at the dashboards provided by the "Amazon GuardDuty - Cloud Security Monitoring and Analytics" app, part of the Cloud Security Monitoring and Analytics series, which specializes in security.

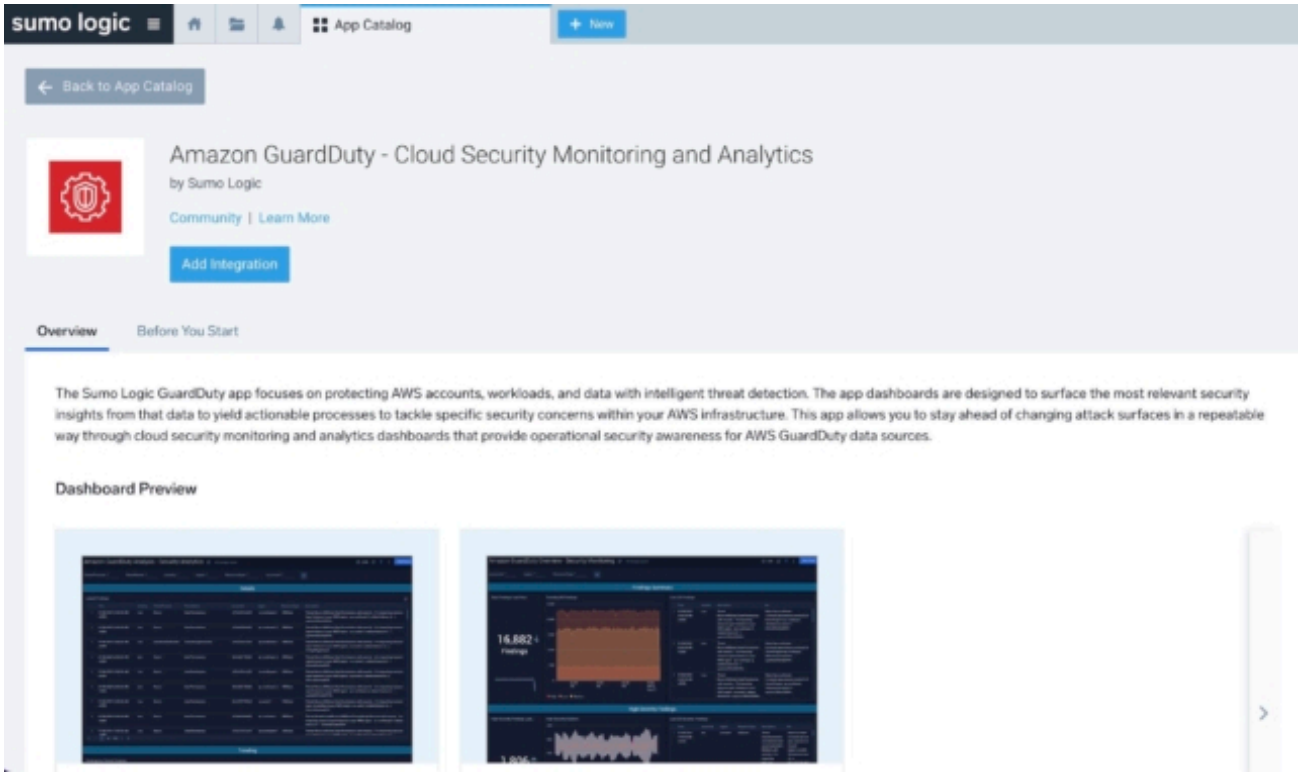
Available Plans

First of all, this app is available for all Sumo Logic plans.

Free	Trial	Essential	Enterprise Operation	Enterprise Security	Enterprise Suite
✔	✔	✔	✔	✔	✔

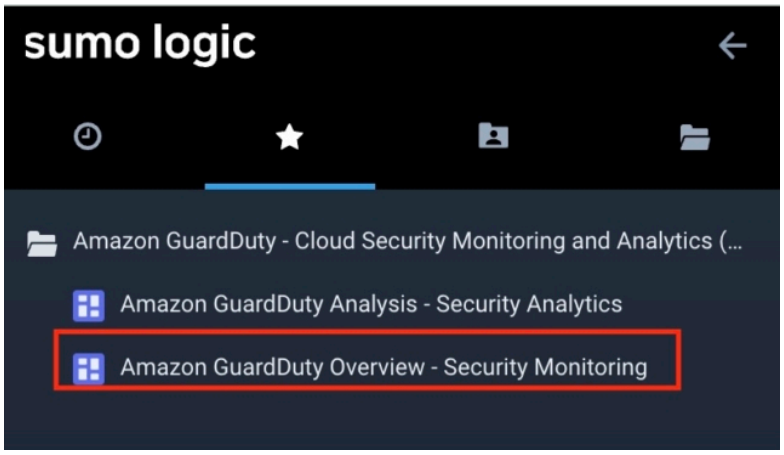
Settings before installing the app

From the Sumo Logic console, select App Catalog and install Amazon GuardDuty - Cloud Security Monitoring and Analytics.



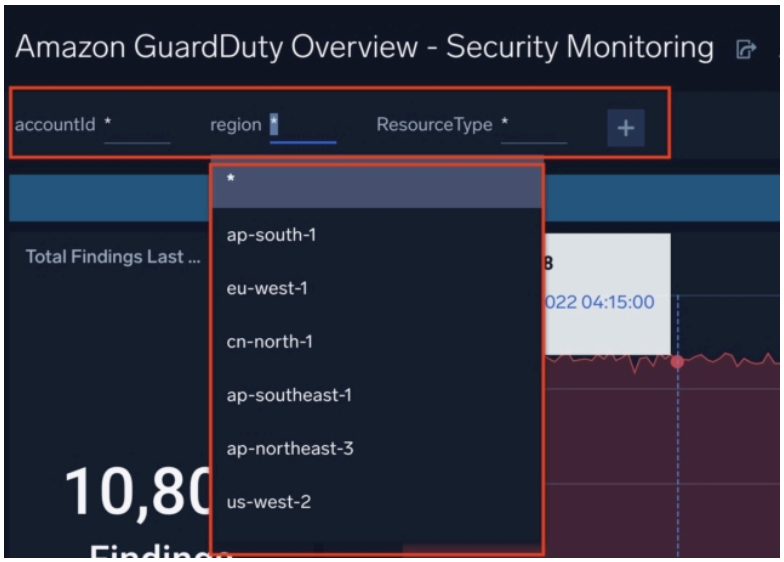
For information on log collection settings and app installation settings, please refer to the official documentation here.

Once you install the app, two dashboards will appear. Let's take a look at each dashboard. First, let's look at the Amazon GuardDuty Overview - Security Monitoring dashboard.
*Note: For data and environment, we used Sumo Logic's training environment.



Amazon GuardDuty Overview - Security Monitoring

First, here you can filter by account ID, region, or resource type across each panel in the entire dashboard.

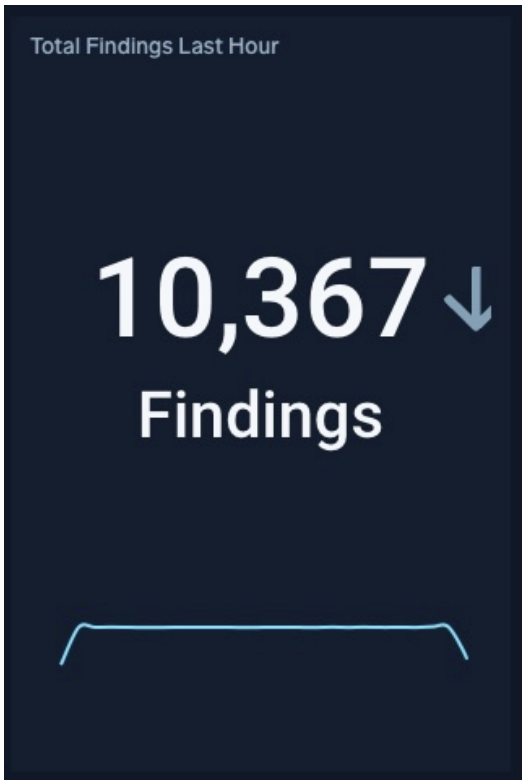


Findings Summary

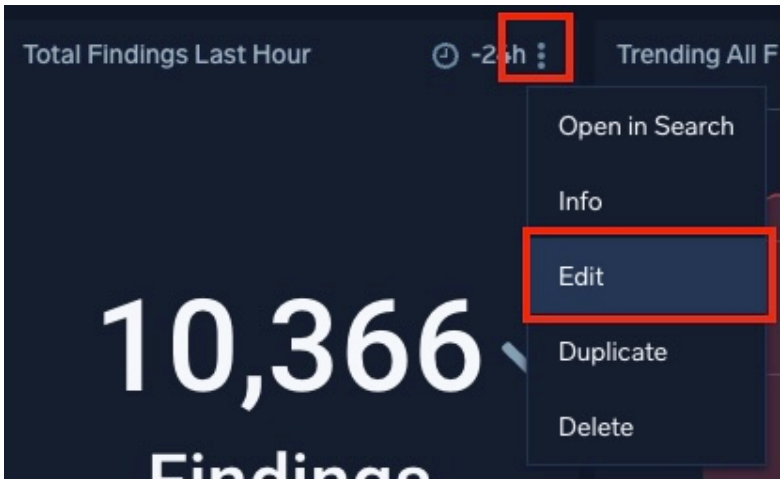
The Findings Summary allows you to check the overall GuardDuty detection status.

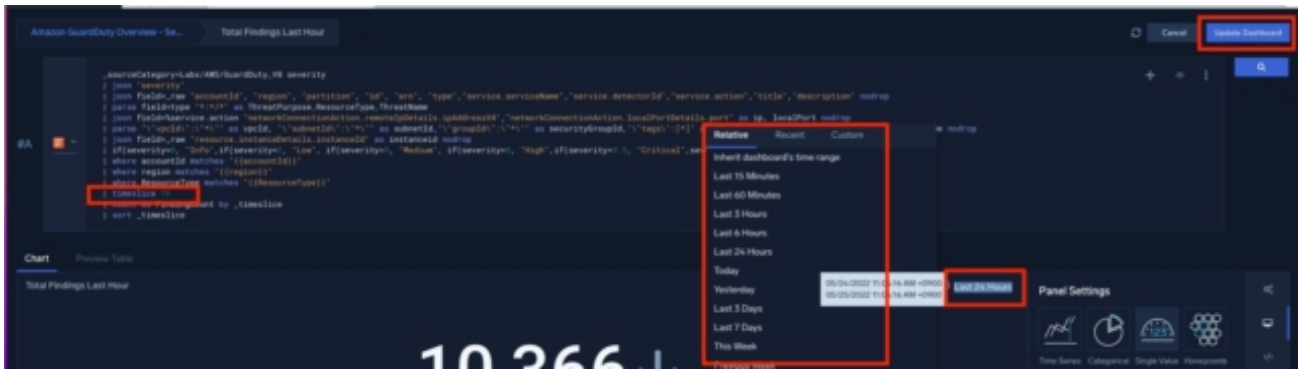
Total Findings Last Hour

This is the number of GuardDuty findings for the past hour. The graph below shows a sparkline plotting the number of findings per hour over a 24-hour period.



Also, like all panels in the dashboard, you can edit the query content and search time by selecting Edit from the three dots in the top right corner of the panel, and have the changes reflected in the dashboard.





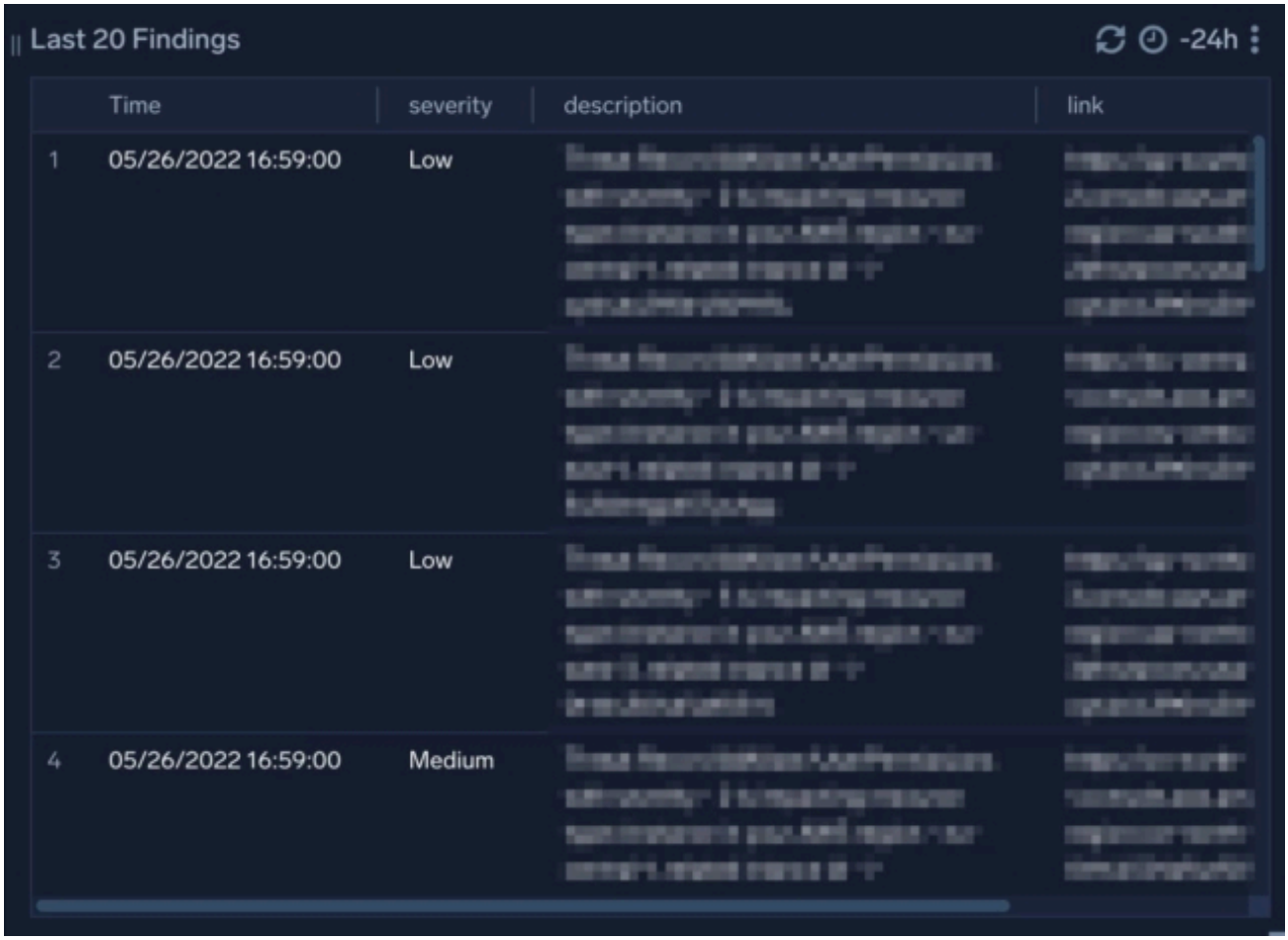
(You can edit the number of hourly Findings in the query statement to every three hours (from "1h" to "3h"), or change the search target (from "Last 24 Hours" to "Last 3 Days"), and then update the dashboard.)

Trending All Findings

This area chart shows the number of GuardDuty findings by severity within the last 24 hours.

Last 20 Findings

Displays a table summarizing the last 20 GuardDuty detections.



High Severity Findings

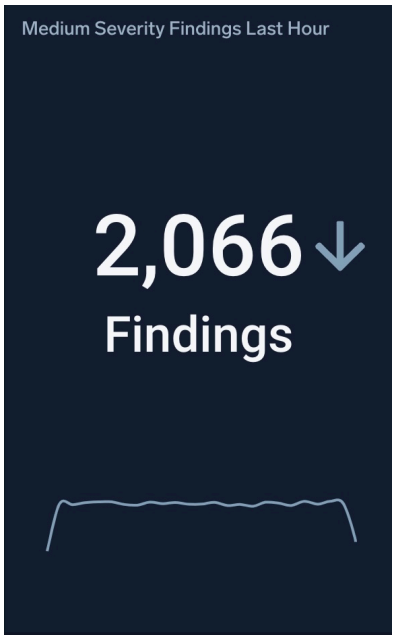
This is a panel about GuardDuty's High Severity Findings. Since there was no data in the demo environment, I will explain it in the next section, Medium Severity Findings.

Medium Severity Findings

This is a panel about GuardDuty Medium detections.

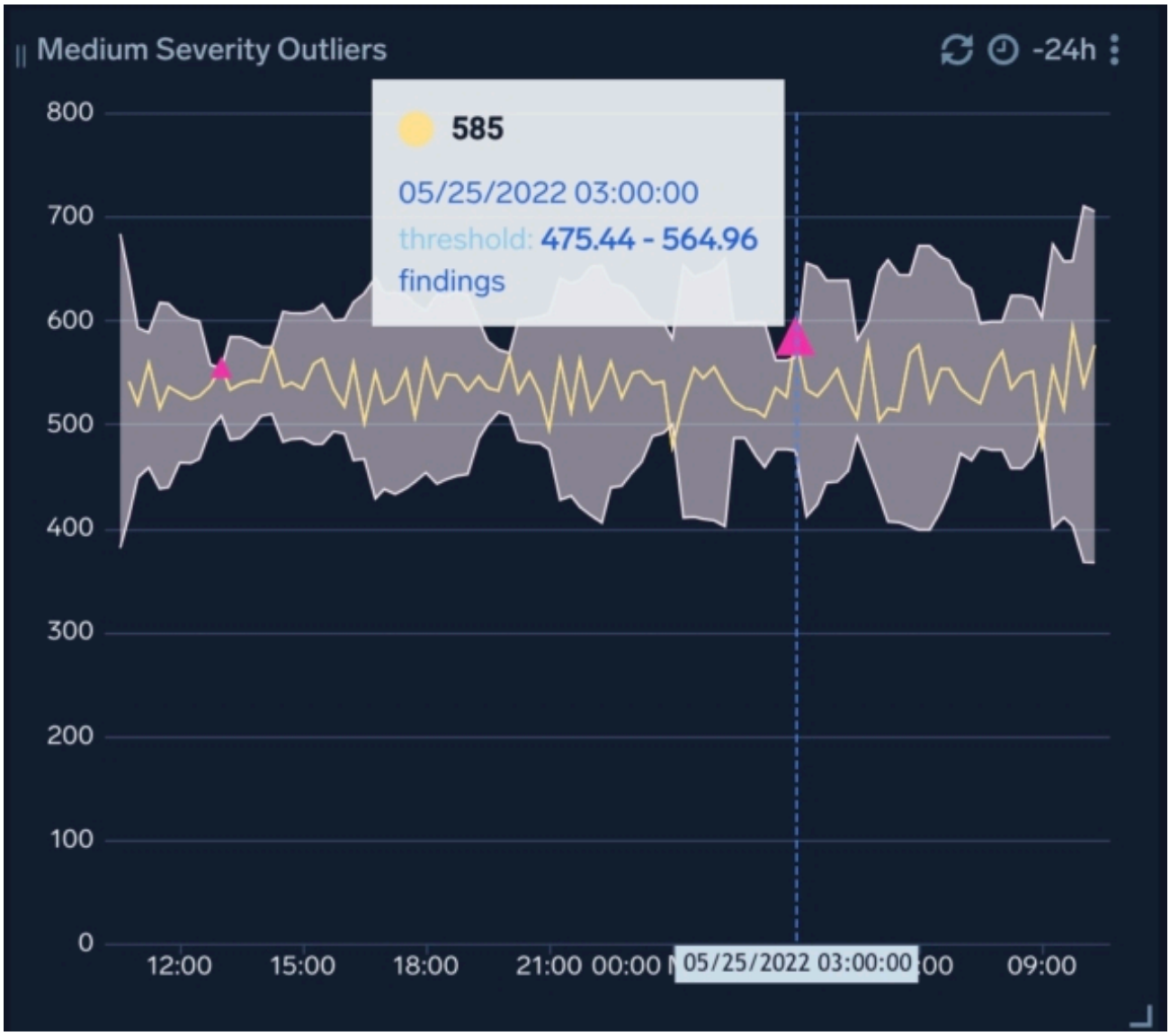
Medium Severity Findings Last Hour

This is the number of Medium Severity Findings in GuardDuty for the past hour. The graph below shows a sparkline plotting the number of Medium Severity Findings per hour over a 24-hour period.



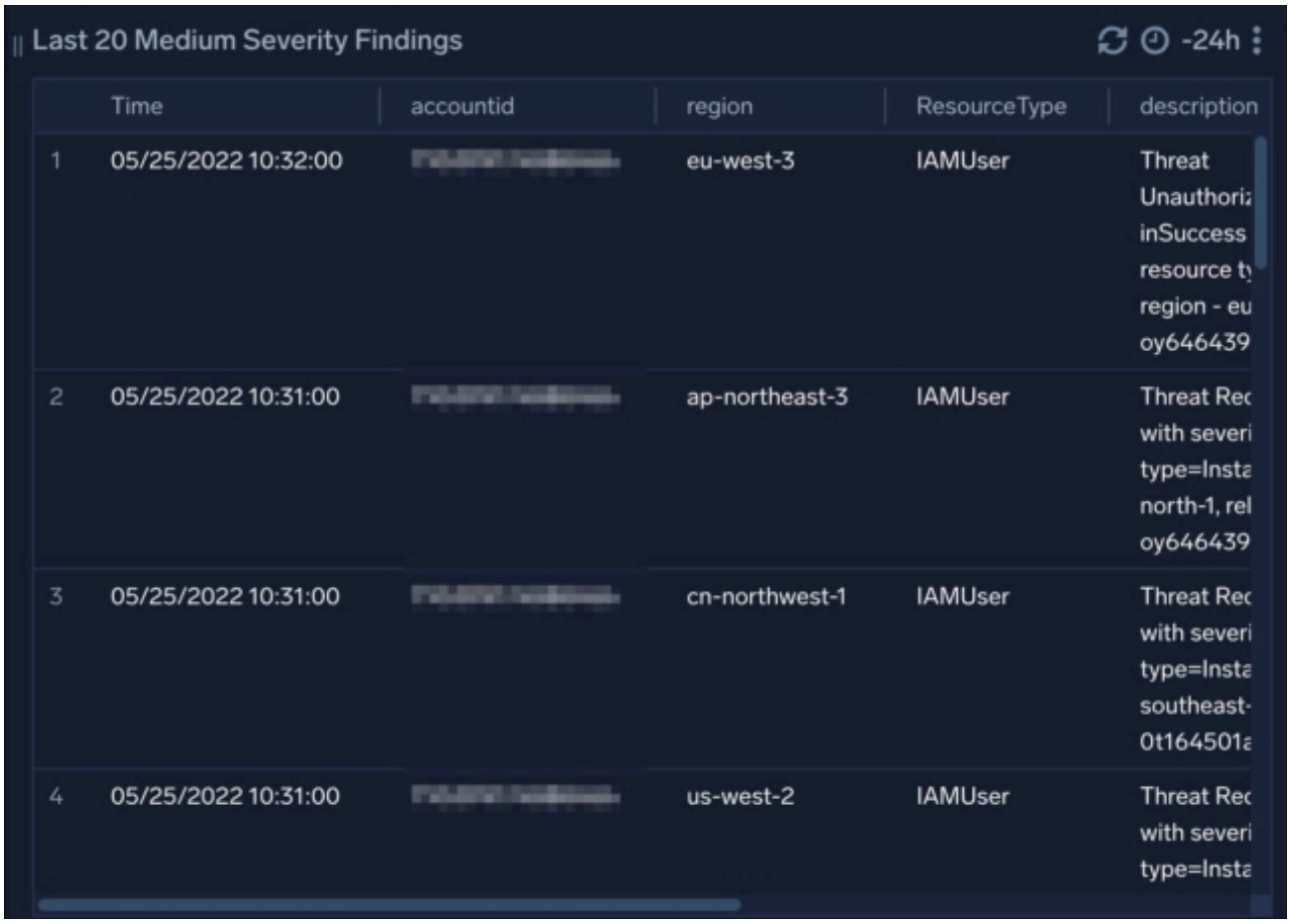
Medium Severity Outliers

A threshold is calculated from past fluctuations in Medium Severity Findings, and if there is a sudden spike (exceeding the threshold), a triangle is displayed.
You can use this threshold to issue an alert when the threshold is exceeded.


Medium Severity Outliers
-24h
585
05/25/2022 03:00:00
threshold: 475.44 - 564.96
findings
800
700
600
500
400
300
200
100
0
12:00
15:00
18:00
21:00
00:00
05/25/2022 03:00:00
09:00

Last 20 Severity Findings

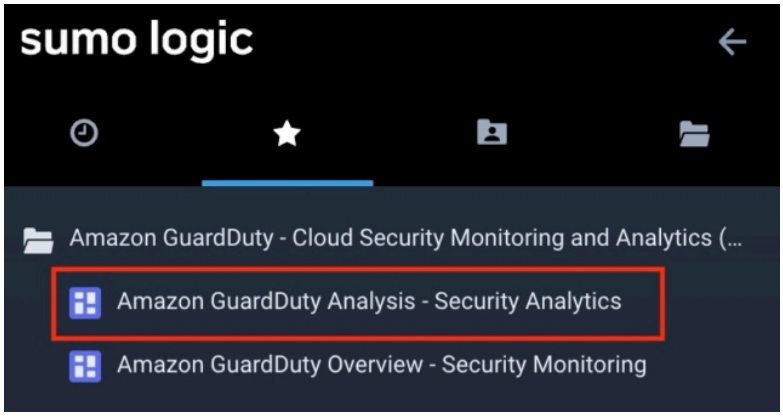
Displays a table summarizing the last 20 Medium Severity GuardDuty detections.



Low Severity Findings

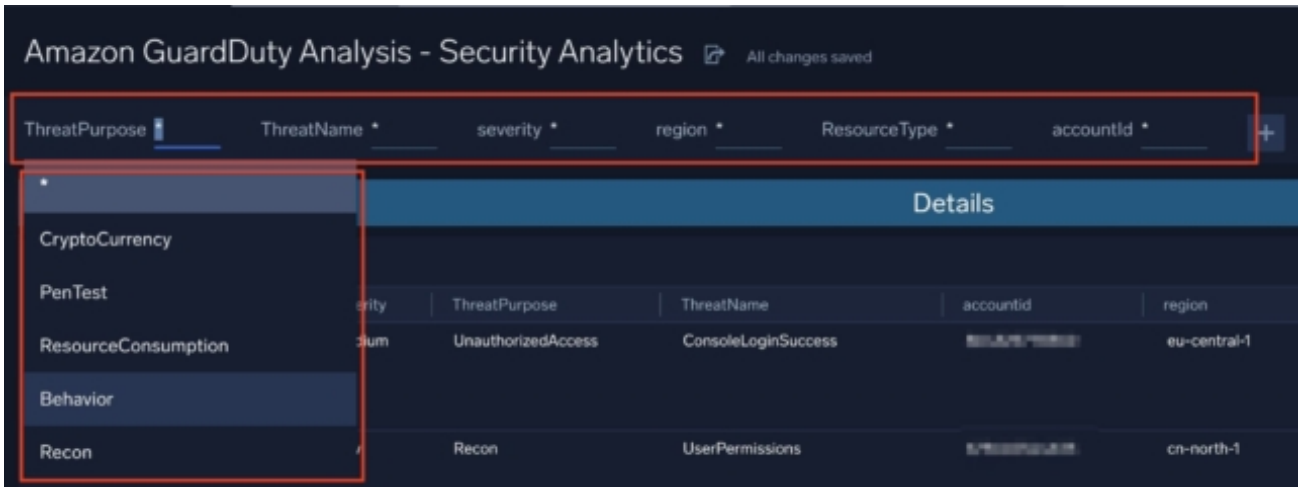
This is a panel for GuardDuty's Low detection. Each panel is the same as the Medium one.

Next, go back to the folder and look at another dashboard, "Amazon GuardDuty Analysis - Security Analytics."



Amazon GuardDuty Analysis - Security Analytics

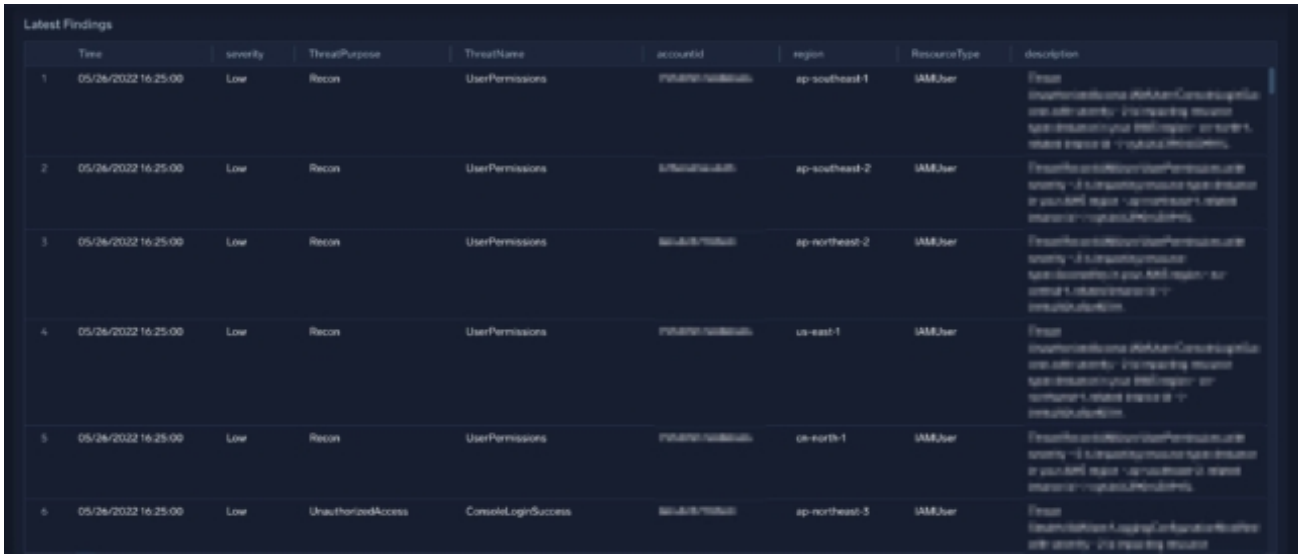
Here too, you can filter the overall information by ThreatPurpose, ThreatName, severity, region, ResourceType, and accountId.



Details

Latest Findings

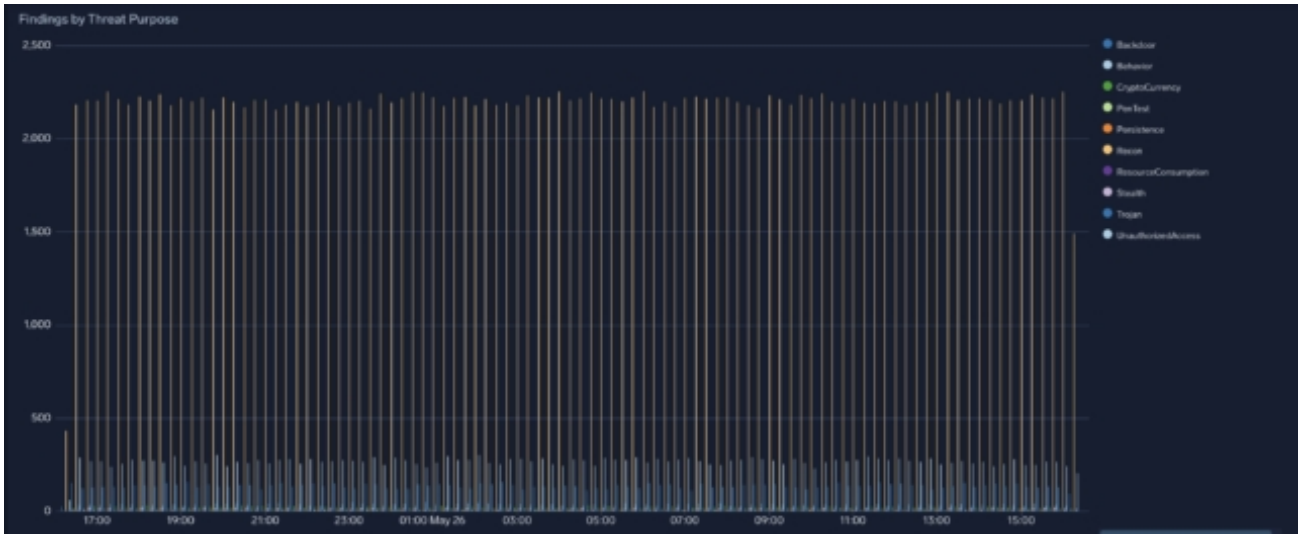
A detailed table of detections will be displayed, starting with the most recent. You can use the filters we used earlier to see the detections you want to focus on.



Trending

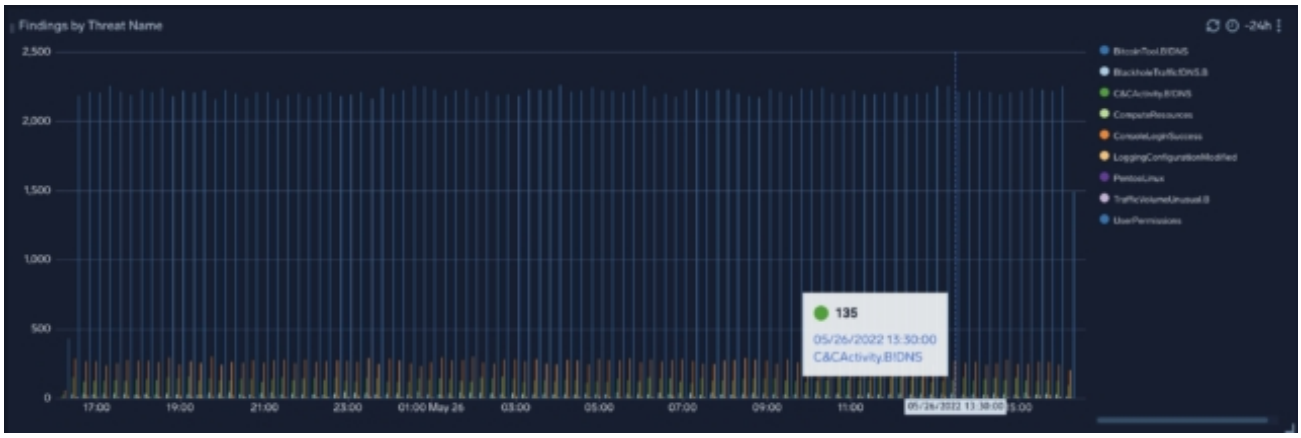
Findings by Threat Purpose

A bar graph displays the number of Findings detected by GuardDuty over a 15-minute period within the last 24 hours, broken down by threat objective.



Findings by Threat Name

Displays a bar chart showing the number of malware family names or threat names associated with threats in Findings detected by GuardDuty over a 15-minute period within the last 24 hours.



summary

This time, we introduced the dashboard provided by the "Amazon GuardDuty - Cloud Security Monitoring and Analytics" app, part of the security-focused Cloud Security Monitoring and Analytics series. It's also very easy to **create your own dashboard by cutting and pasting only the panels you need from other apps**
. We hope you'll use this article as a reference and take advantage of security insights using Sumo Logic.