

Introducing the Sumo Logic Security App vol.1

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

酒井剛

May 26, 2022

sumo logic

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.

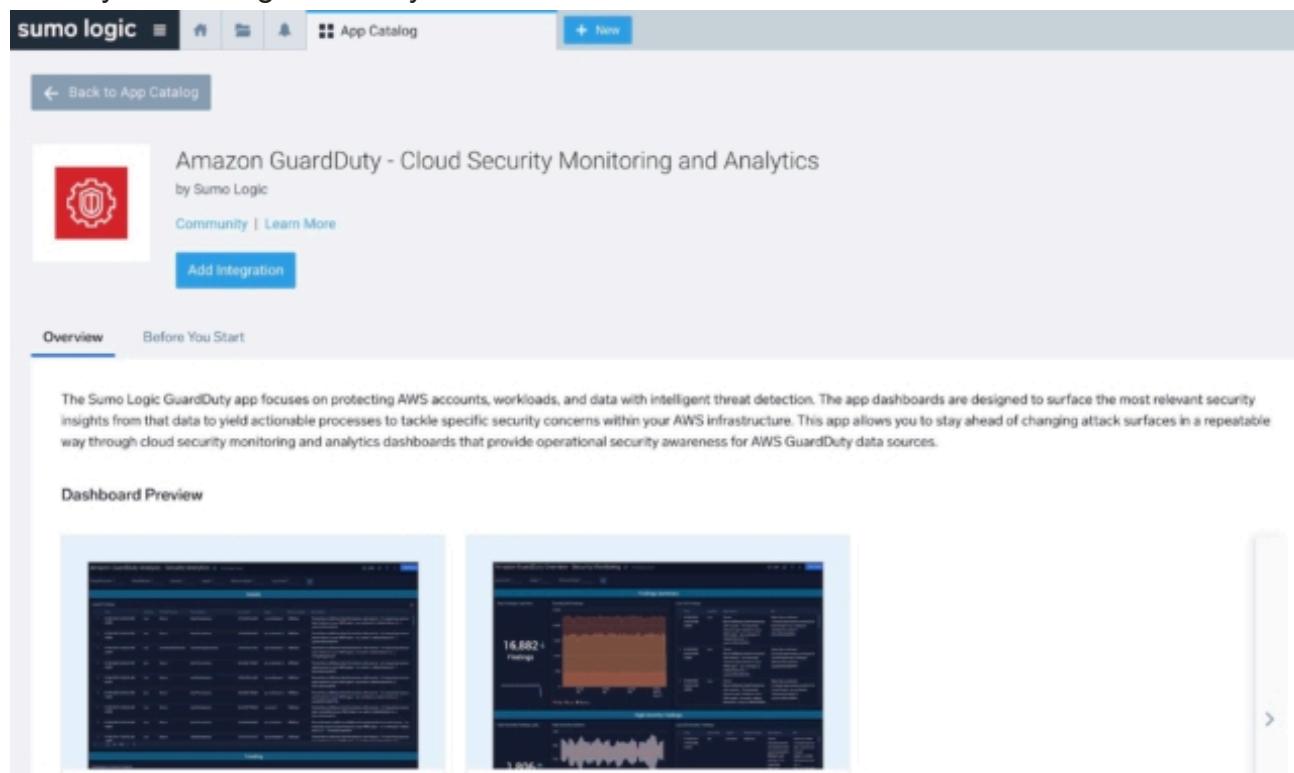
Available Plans

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.

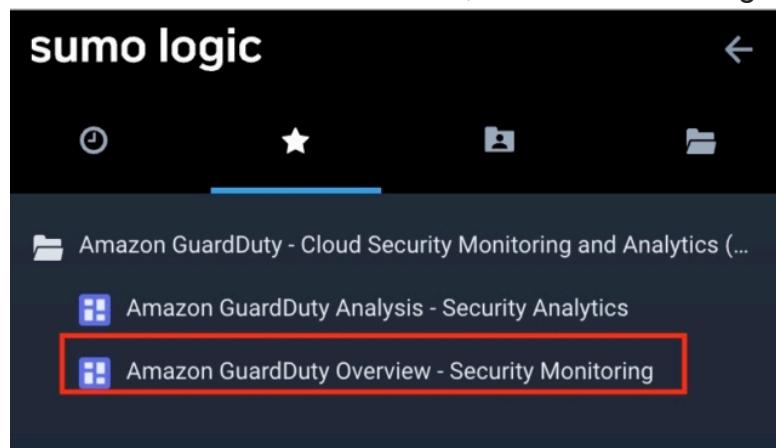


The screenshot shows the Sumo Logic App Catalog interface. At the top, there's a navigation bar with 'sumo logic' and various icons. Below it, a search bar contains 'App Catalog'. A blue button labeled '+ New' is visible. The main content area displays the 'Amazon GuardDuty - Cloud Security Monitoring and Analytics' app by Sumo Logic. It features a red icon with a gear and a red border. Below the icon, the app name and developer are listed. A 'Community' link and a 'Learn More' link are also present. A prominent blue 'Add Integration' button is at the bottom. Below this, two tabs are shown: 'Overview' (which is selected) and 'Before You Start'. A detailed description of the app's purpose follows. Under 'Dashboard Preview', two screenshots of the dashboard are shown, each displaying various monitoring metrics and data tables. A vertical scroll bar is on the right side of the preview area.

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.

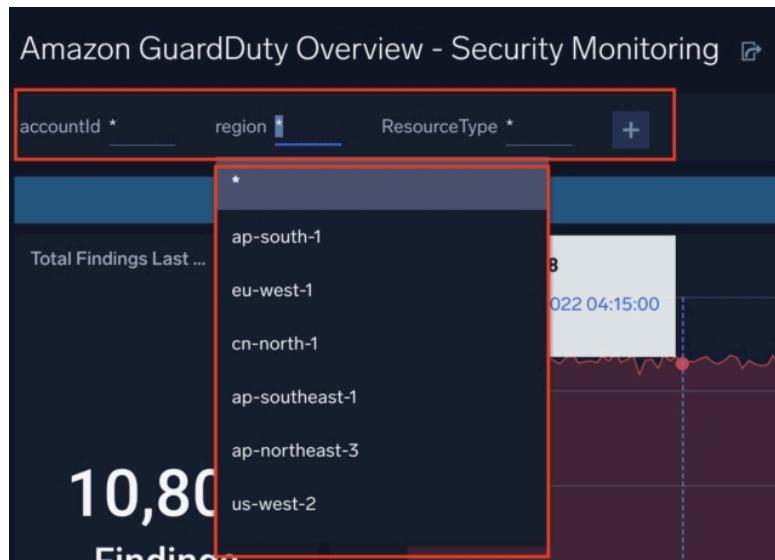
*Note: For data and environment, we used Sumo Logic's training environment.



The screenshot shows the Sumo Logic dashboard interface. At the top, there's a header with 'sumo logic' and a back arrow icon. Below the header, there are four navigation icons: a circle, a star, a user profile, and a folder. The main content area displays a list of dashboards. The first item is 'Amazon GuardDuty - Cloud Security Monitoring and Analytics (...)' with a folder icon. The second item is 'Amazon GuardDuty Analysis - Security Analytics' with a blue square icon. The third item is 'Amazon GuardDuty Overview - Security Monitoring' with a blue square icon. This last item is highlighted with a red rectangular box. A vertical scroll bar is on the right side of the content area.

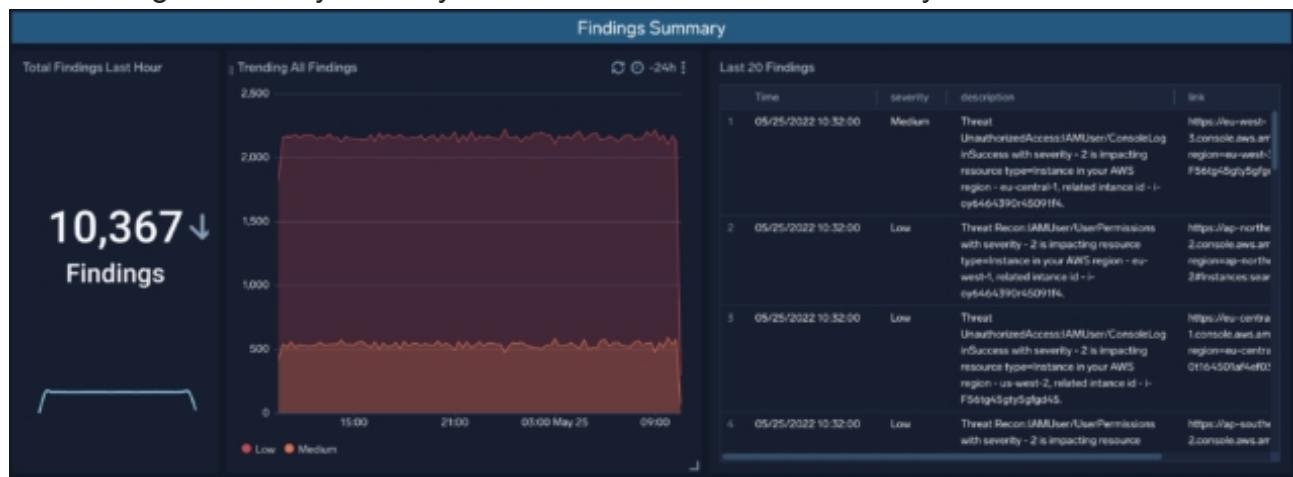
Amazon GuardDuty Overview - Security Monitoring

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



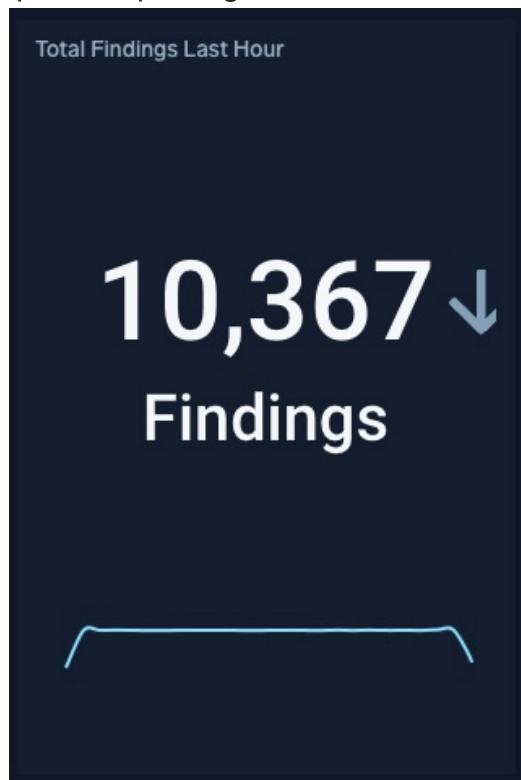
Findings Summary

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

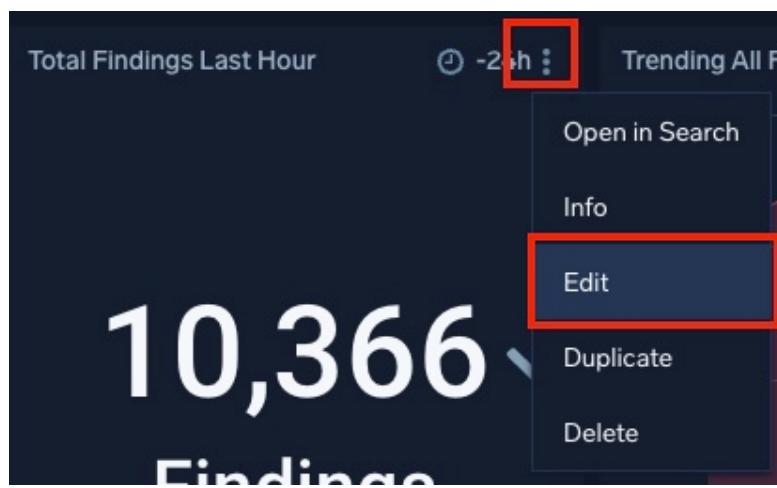


Total Findings Last Hour

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.



Amazon GuardDuty Overview - Se... Total Findings Last Hour

```

sourceCategory=Lambda/GuardDuty_HB severity
|> sum "severity"
|> join Field=@_raw "accountID", "region", "partition", "id", "arn", "type", "service.serviceName", "service.detectorID", "service.action", "title", "description" redrop
|> parse Field=@type "/*/*" as threatPurpose, ResourceType, ThreatName
|> join Field=@_raw "resource.instancesDetails.instanceArn" as instanceArn, "groupID" as groupID, "/*/*" as severityLevel, "/*/*" as severityType
|> join Field=@_raw "resource.instancesDetails.instancesDetails" as instancesDetails
|> join Field=@_raw "resource.instancesDetails.instancesDetails.accountID" as accountID, "severity" as severity, "/*/*" as severityLevel, "/*/*" as severityType
|> where accountID accountID != "000000000000"
|> where ResourceType matches ~"(ResourceType)"
|> timeline
|> sort @_timestamp

```

Relative Recent Custom

Last 15 Minutes
Last 60 Minutes
Last 3 Hours
Last 6 Hours
Last 24 Hours
Today
Yesterday
Last 3 Days
Last 7 Days
This Week

05/24/2022 11:00:16 AM - 05/25/2022 11:00:16 AM [05/25/2022]

Panel Settings

Time Series Category Single Value Metrics

10,266

(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.

Last 20 Findings				
	Time	severity	description	link
1	05/26/2022 16:59:00	Low	These findings are AuthPolicies violations. It is missing resource from resource provided region or user's region doesn't support the authPolicy.	View Details Details Region AWS Lambda AWS Lambda
2	05/26/2022 16:59:00	Low	These findings are AuthPolicies violations. It is missing resource from resource provided region or user's region doesn't support the authPolicy.	View Details Details Region AWS Lambda AWS Lambda
3	05/26/2022 16:59:00	Low	These findings are AuthPolicies violations. It is missing resource from resource provided region or user's region doesn't support the authPolicy.	View Details Details Region AWS Lambda AWS Lambda
4	05/26/2022 16:59:00	Medium	These findings are AuthPolicies violations. It is missing resource from resource provided region or user's region doesn't support the authPolicy.	View Details Details Region AWS Lambda AWS Lambda

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.

High Severity Findings		
High Severity Findings Last Hour	High Severity Outliers	Last 20 Severity Findings
<h3>No data</h3> <p>Findings</p>	<p>No Data to Display</p> <p>There is no data for your filter. You can try modifying the query or updating the time range.</p>	<p>No Data to Display</p> <p>There is no data for your filter. You can try modifying the query or updating the time range.</p>

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.



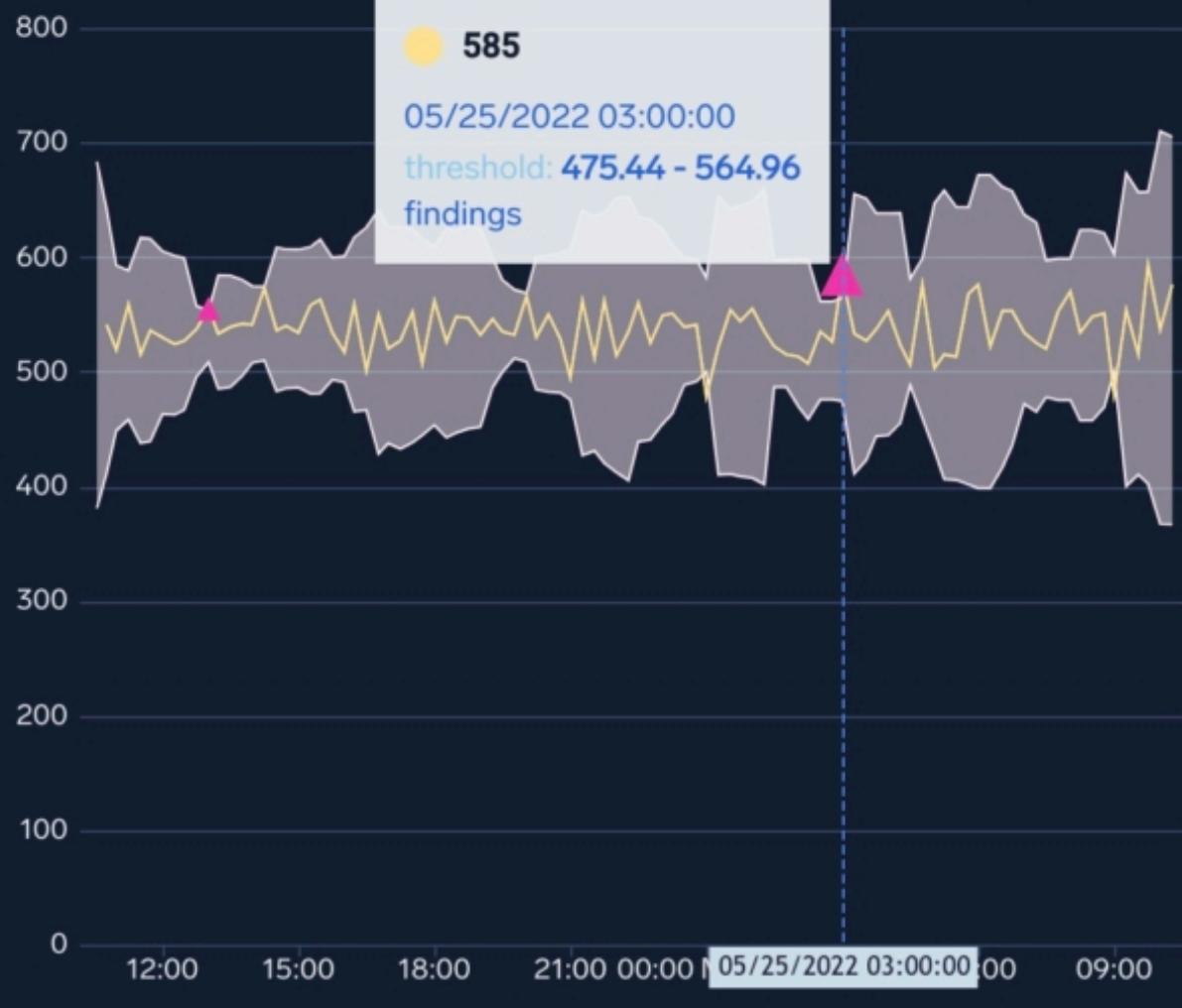
Medium Severity Outliers

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 ::



Last 20 Severity Findings

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

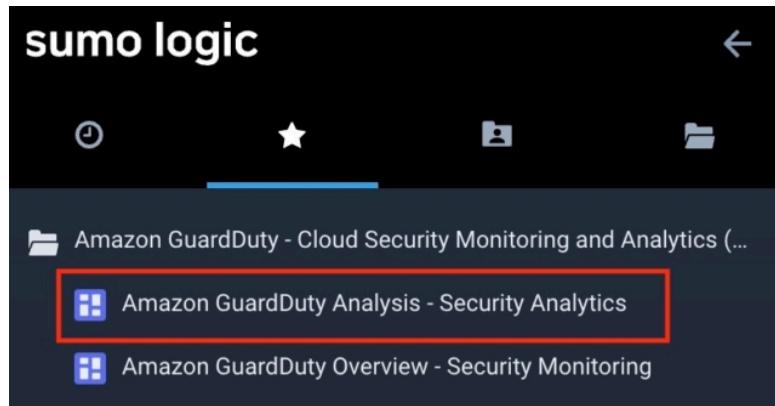
Last 20 Medium Severity Findings					
	Time	accountid	region	ResourceType	description
1	05/25/2022 10:32:00	[REDACTED]	eu-west-3	IAMUser	Threat Unauthorized inSuccess resource type=Insta region - eu oy646439
2	05/25/2022 10:31:00	[REDACTED]	ap-northeast-3	IAMUser	Threat Rec with severity type=Insta north-1, rel oy646439
3	05/25/2022 10:31:00	[REDACTED]	cn-northwest-1	IAMUser	Threat Rec with severity type=Insta southeast-0t164501a
4	05/25/2022 10:31:00	[REDACTED]	us-west-2	IAMUser	Threat Rec with severity type=Insta

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.

The screenshot shows the 'Amazon GuardDuty Analysis - Security Analytics' dashboard. At the top, there are six input fields for filtering: ThreatPurpose (set to 'CryptoCurrency'), ThreatName (*), severity (*), region (*), ResourceType (*), and accountId (*). Below these filters is a table titled 'Details' with five rows of threat data. The columns are: ThreatPurpose, ThreatName, accountId, and region. The data is as follows:

ThreatPurpose	ThreatName	accountId	region
CryptoCurrency			
PenTest			
ResourceConsumption	UnauthorizedAccess	ConsoleLoginSuccess	eu-central-1
Behavior			
Recon	UserPermissions		cn-north-1

Details

Latest Findings

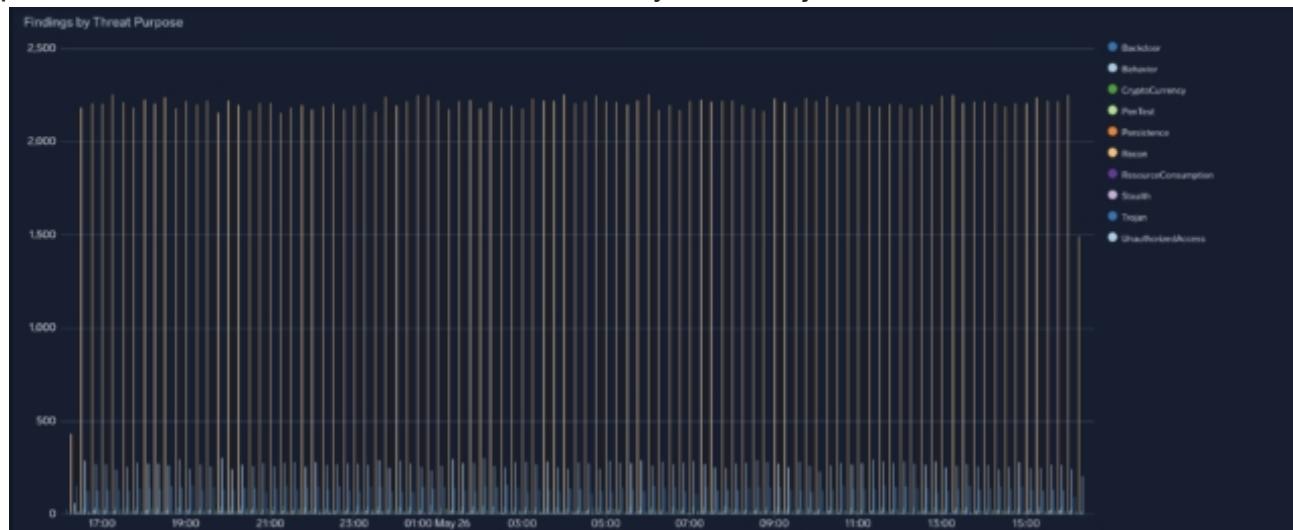
A detailed table of detections will be displayed, starting with the most recent. You can use the filters we used earlier to see the detections you want to focus on.

Latest Findings								
	Time	severity	ThreatPurpose	ThreatName	accountid	region	ResourceType	description
1	05/26/2022 16:25:00	Low	Recon	UserPermissions	11111111111111111111	ap-southeast-1	IAMUser	These findings indicate potential compromise or unauthorized access to AWS Lambda functions or AWS Lambda resources. These findings are from the UserPermissions threat objective.
2	05/26/2022 16:25:00	Low	Recon	UserPermissions	11111111111111111111	ap-southeast-2	IAMUser	These findings indicate potential compromise or unauthorized access to AWS Lambda functions or AWS Lambda resources. These findings are from the UserPermissions threat objective.
3	05/26/2022 16:25:00	Low	Recon	UserPermissions	11111111111111111111	ap-northeast-2	IAMUser	These findings indicate potential compromise or unauthorized access to AWS Lambda functions or AWS Lambda resources. These findings are from the UserPermissions threat objective.
4	05/26/2022 16:25:00	Low	Recon	UserPermissions	11111111111111111111	us-east-1	IAMUser	These findings indicate potential compromise or unauthorized access to AWS Lambda functions or AWS Lambda resources. These findings are from the UserPermissions threat objective.
5	05/26/2022 16:25:00	Low	Recon	UserPermissions	11111111111111111111	cn-north-1	IAMUser	These findings indicate potential compromise or unauthorized access to AWS Lambda functions or AWS Lambda resources. These findings are from the UserPermissions threat objective.
6	05/26/2022 16:25:00	Low	UnauthorizedAccess	ConsoleLoginSuccess	11111111111111111111	ap-northeast-3	IAMUser	These findings indicate potential unauthorized access to AWS Lambda functions or AWS Lambda resources. These findings are from the UnauthorizedAccess threat objective.

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.