# Introducing the Sumo Logic Security App vol.2

dev.classmethod.jp/articles/sumo-logic_security-app-vol-2

酒井剛

June 1, 2022

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

**Continuing from last time, I would like to take a closer look at the dashboard of the Sumo Logic security app , "Amazon VPC Flow - Cloud Security Monitoring and Analytics,"** which can quickly gain security insights from AWS VPC logs .

Vol.1 (GuardDuty episode) available here

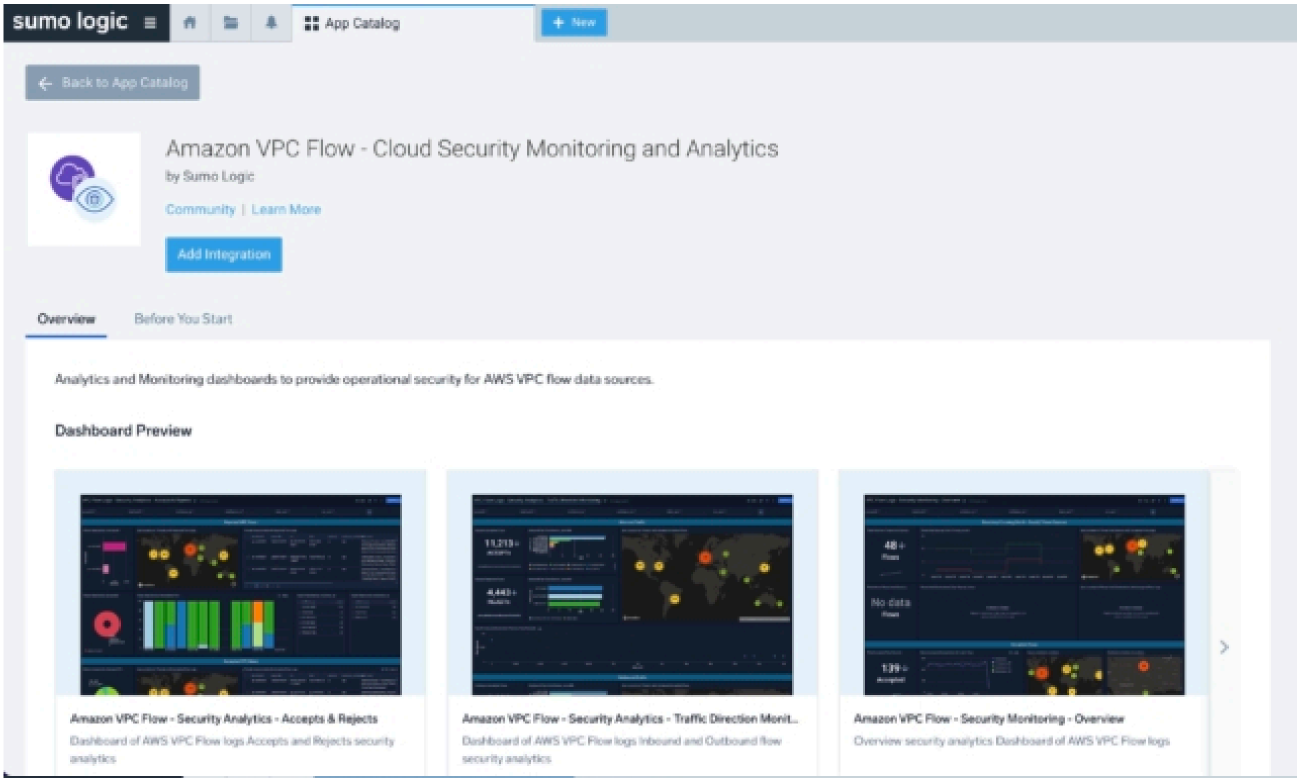
## Available Plans

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 VPC Flow - Cloud Security Monitoring and Analytics.



Amazon VPC Flow - Cloud Security Monitoring and Analytics

by Sumo Logic

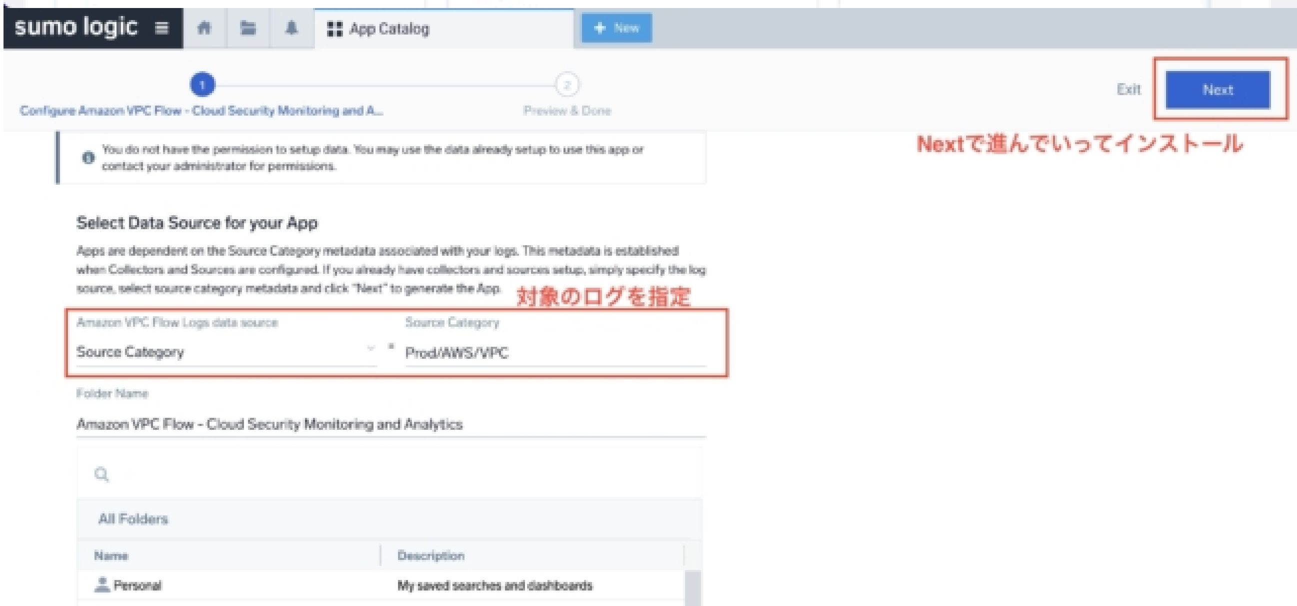
Analytics and Monitoring dashboards to provide operational security for AWS VPC flow data sources.

Dashboard Preview

Amazon VPC Flow - Security Analytics - Accepts & Rejects
Dashboard of AWS VPC Flow logs Accepts and Rejects security analytics

Amazon VPC Flow - Security Analytics - Traffic Direction Monit...
Dashboard of AWS VPC Flow logs Inbound and Outbound flow security analytics

Amazon VPC Flow - Security Monitoring - Overview
Overview security analytics Dashboard of AWS VPC Flow logs


sumo logic
App Catalog
+ New
1
Configure Amazon VPC Flow - Cloud Security Monitoring and A...
2
Preview & Done
Exit
Next
Nextで進んでいってインストール

You do not have the permission to setup data. You may use the data already setup to use this app or contact your administrator for permissions.

Select Data Source for your App

Apps are dependent on the Source Category metadata associated with your logs. This metadata is established when Collectors and Sources are configured. If you already have collectors and sources setup, simply specify the log source, select source category metadata and click "Next" to generate the App.

Amazon VPC Flow Logs data source: Source Category

Source Category: Prod/AWS/VPC

Folder Name: Amazon VPC Flow - Cloud Security Monitoring and Analytics

All Folders

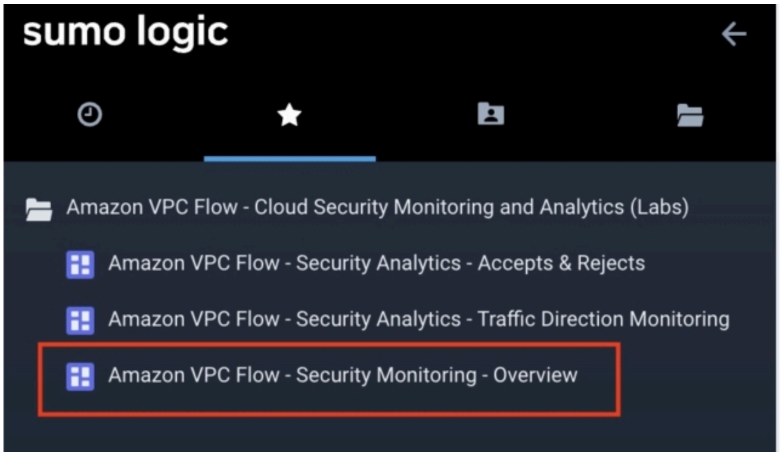
| Name | Description |
|---|---|
| Personal | My saved searches and dashboards |

*Before installing the app, you must enable VPC flow logs on the AWS side and configure the settings to import VPC flow logs into Sumo Logic. When enabling VPC flow logs on the AWS side, there are two ways to integrate logs: to S3 or to CloudWatch Logs. Logs can also be imported from AWS to Sumo from either S3 or CloudWatch Logs.

Please refer to this blog for information on the differences in VPC flow log integration destinations on the AWS side.

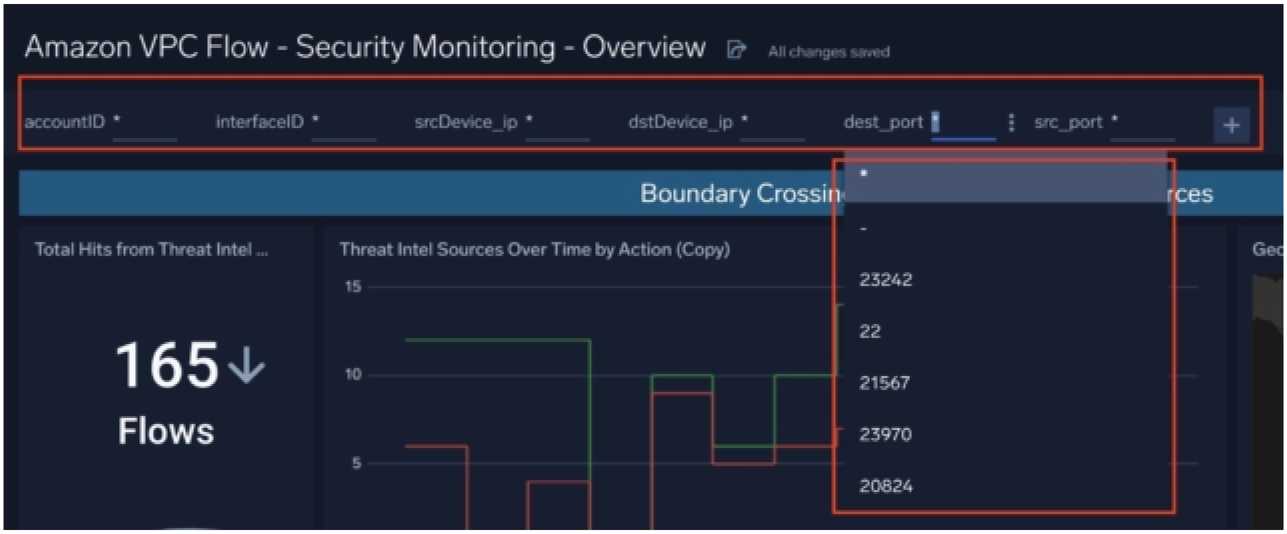
Learn how to configure Sumo Logic to retrieve from S3 here and how
to configure Sumo Logic to retrieve from CloudWatch Logs here .

Once you install the app, three dashboards will be displayed. Let's take a look at each dashboard. First, let's look at the Amazon VPC Flow - Security Monitoring - Overview dashboard.
*Note: For data and environment, we are using the Sumo Logic training environment.


sumo logic
Amazon VPC Flow - Cloud Security Monitoring and Analytics (Labs)
Amazon VPC Flow - Security Analytics - Accepts & Rejects
Amazon VPC Flow - Security Analytics - Traffic Direction Monitoring
Amazon VPC Flow - Security Monitoring - Overview

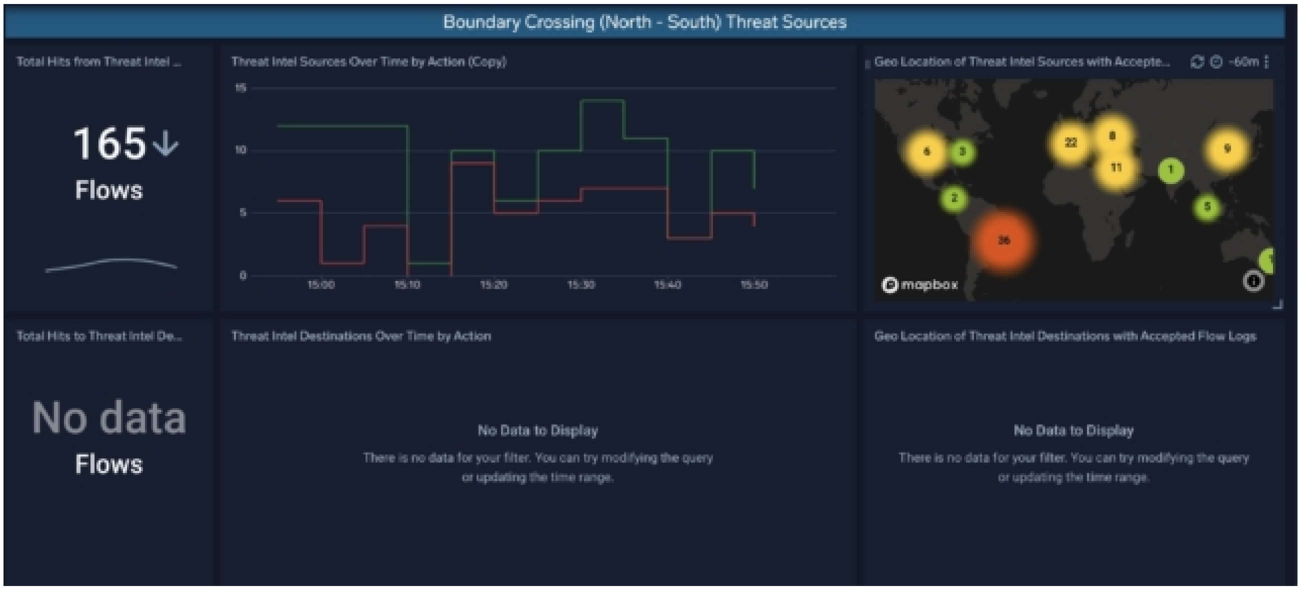
## Amazon VPC Flow - Security Monitoring - Overview

First, here you can filter the entire dashboard by Account ID, Interface ID, Source IP, Destination IP, Destination Port, and Source Port.



## Boundary Crossing (North - South) Threat Sources

Boundary Crossing (North - South) Threat Sources shows whether any logs of outbound or inbound communication between the Internet and AWS were caught by CrowdStrike's Threat Intelligence.


Boundary Crossing (North - South) Threat Sources
Total Hits from Threat Intel ...
165↓
Flows
Threat Intel Sources Over Time by Action (Copy)
15
10
5
0
15:00
15:10
15:20
15:30
15:40
15:50
Geo Location of Threat Intel Sources with Accepte...
-60m
6
3
22
8
11
1
9
2
5
36
mapbox
Total Hits to Threat Intel De...
No data
Flows
Threat Intel Destinations Over Time by Action
Geo Location of Threat Intel Destinations with Accepted Flow Logs

No Data to Display

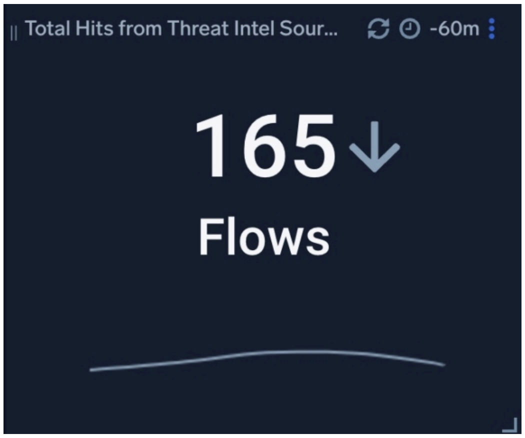
There is no data for your filter. You can try modifying the query or updating the time range.

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

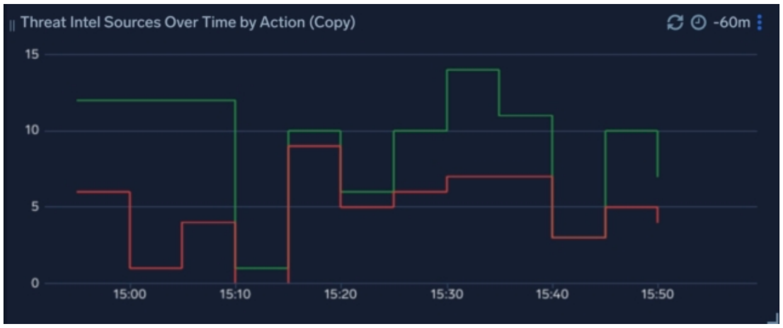
### Total Hits from Threat Intel Source

Displays the number of inbound communications for the last 15 minutes where the source IP in the communication log matches a threat IP in CrowdStrike's Threat Intelligence (the graph below shows a sparkline of the number of inbound communications that matched a threat IP every 15 minutes over a 1-hour period).



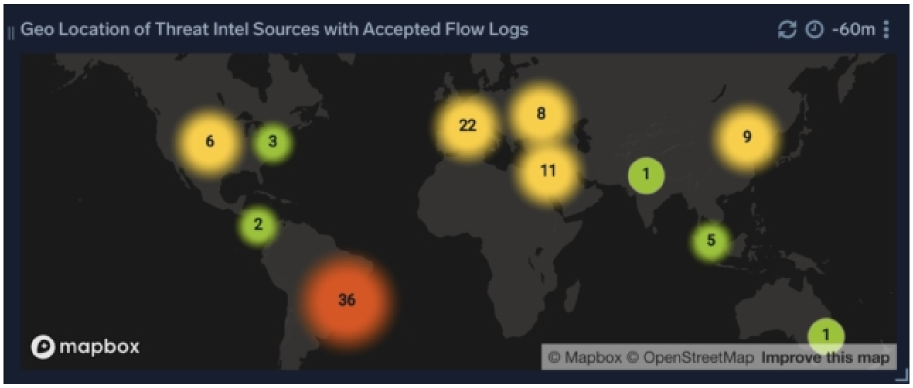
### Threat Intel Sources Over Time by Action

Displays the number of allowed and denied communication flows over a five-minute period where the source IP address in the communication log for the past hour matches a threat IP address in CrowdStrike Intelligence, as a step line chart.



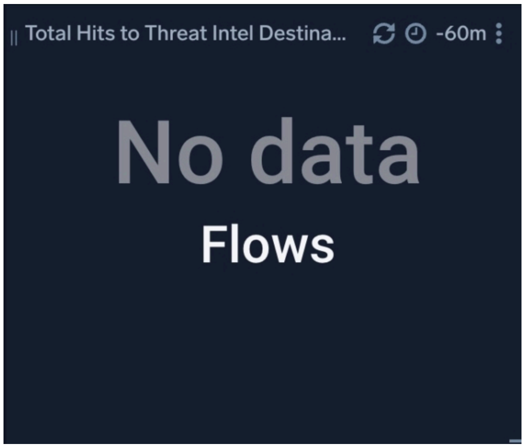
### Geo Location of Threat Intel Sources with Accepted Flow Logs

Geo-location displays allowed inbound traffic where the source IP in the communication log for the past hour matches a threat IP in CrowdStrike Intelligence.


Geo Location of Threat Intel Sources with Accepted Flow Logs
-60m
6
3
22
8
9
11
1
2
5
36
1
mapbox
© Mapbox © OpenStreetMap Improve this map

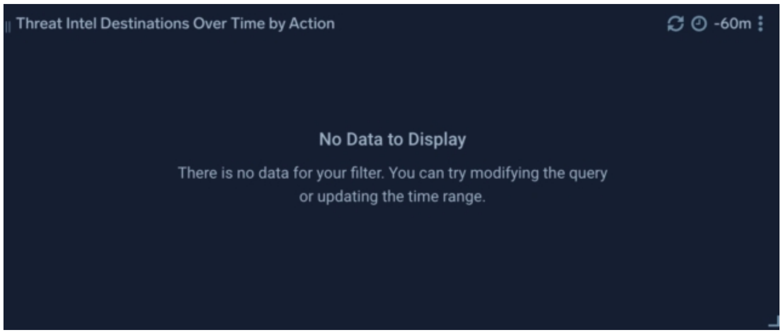
### Total Hits to Threat Intel Destinations

Displays the number of outbound communications for the last 15 minutes where the destination IP in the communications log matches a threat IP in CrowdStrike's Threat Intelligence (the graph below is a sparkline showing the number of outbound communications with a threat IP match every 15 minutes over a one-hour period). The charts for the next three panels related to destination IPs are empty because there were no matches in the demo data.



### Threat Intel Destinations Over Time by Action

Displays the number of allowed and denied traffic flows over a 5-minute interval where the destination IP address in the traffic log for the past hour matches a threat IP address in CrowdStrike Intelligence, as a step line chart.



Threat Intel Destinations Over Time by Action

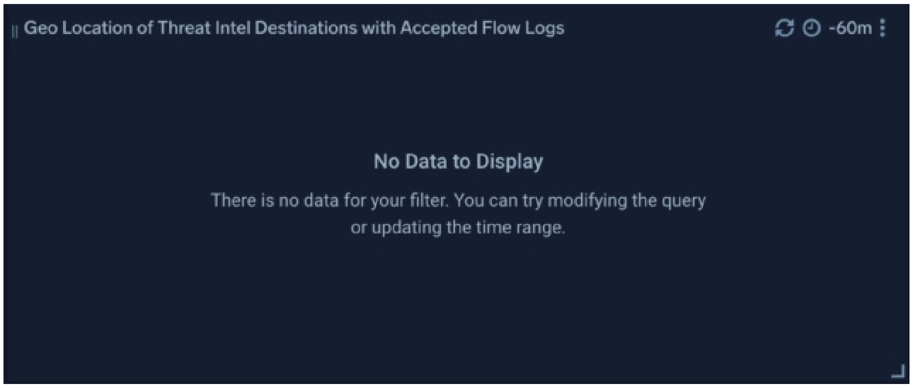
-60m

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

### Geo Location of Threat Intel Destinations with Accepted Flow Logs

Geo-location displays authorized outbound communications where the destination IP in the communication log matches a threat IP in CrowdStrike Intelligence within the last hour.



Geo Location of Threat Intel Destinations with Accepted Flow Logs

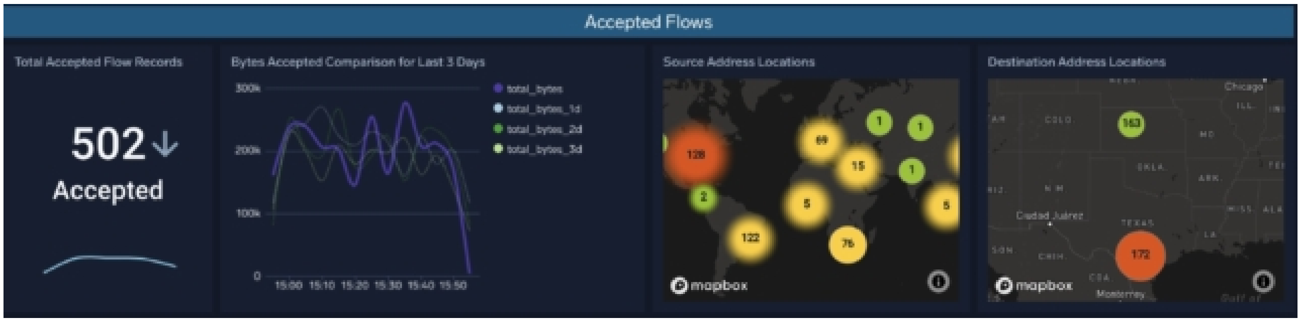
-60m

No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

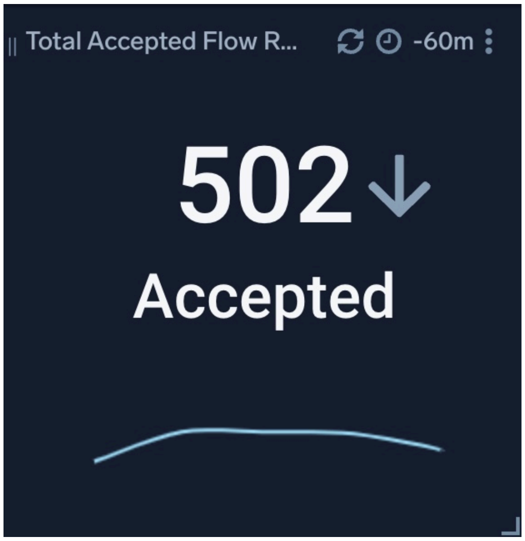
## Accepted Flows

Accepted Flows shows the accepted communications in the VPC flow logs.



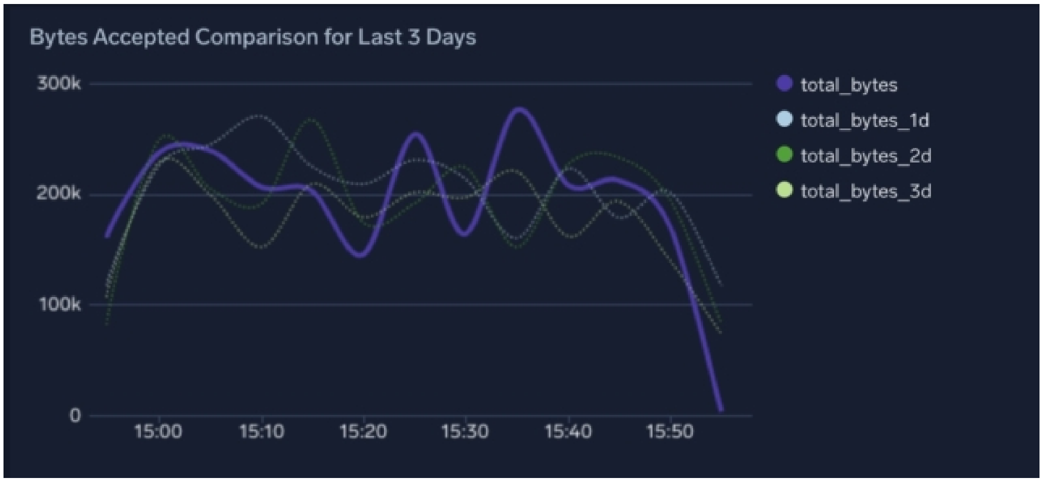
### Total Accepted Flow Records

Displays the number of permitted communication flows for the last 15 minutes (the graph below shows a sparkline of the number of permitted communication flows every 15 minutes over a 1-hour period)



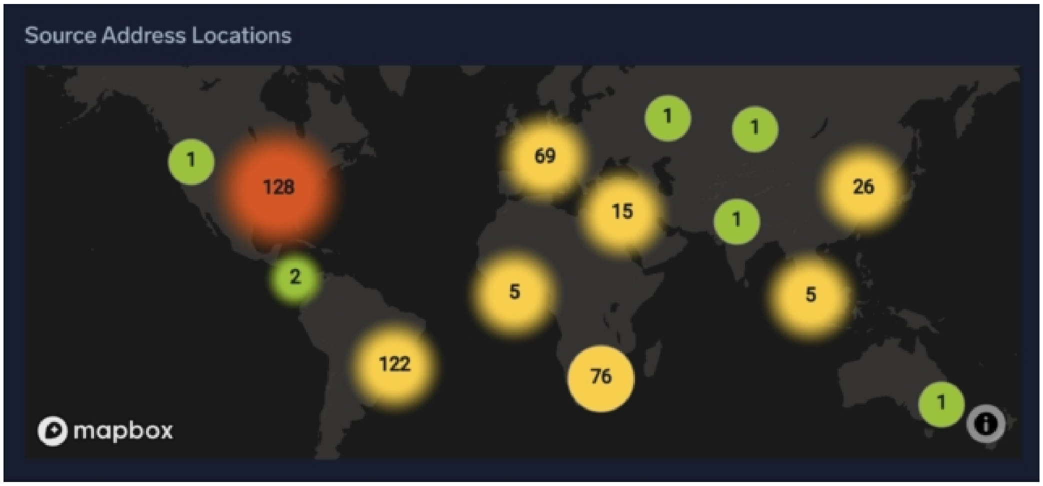
### Bytes Accepted Comparison for Last 3 Days

Displays the amount of traffic allowed every 5 minutes within the last hour and the amount of traffic for each time period over the last 3 days in a line chart.



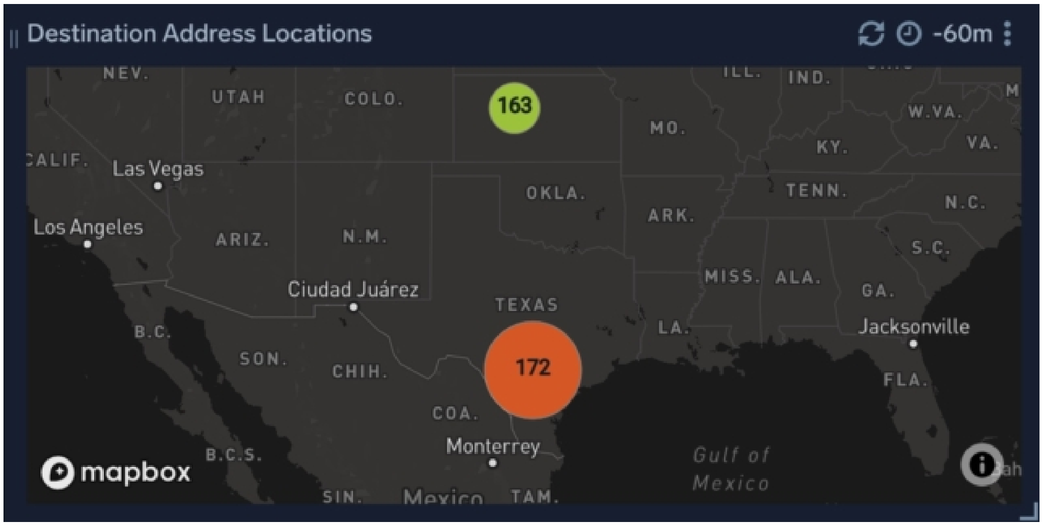
### Source Address Locations

View allowed inbound traffic for the last hour with Geo Location



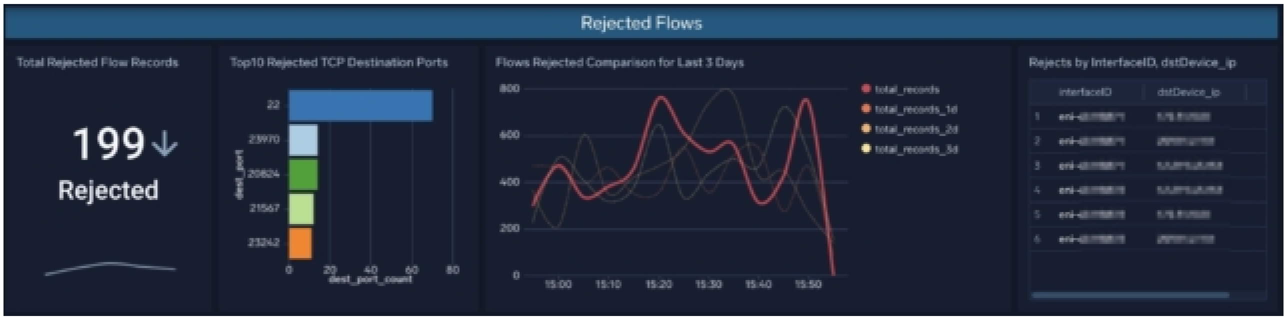
### Destination Address Locations

View all allowed outbound communications within the last hour by geolocation



## Rejected Flows

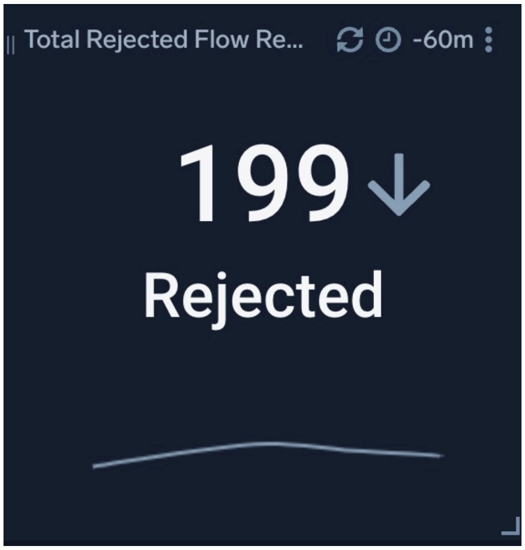
Rejected Flows shows rejected communications in the VPC flow logs.



| | interfaceID | dstDevice_ip |
|---|---|---|
| 1 | eni-[redacted] | [redacted] |
| 2 | eni-[redacted] | [redacted] |
| 3 | eni-[redacted] | [redacted] |
| 4 | eni-[redacted] | [redacted] |
| 5 | eni-[redacted] | [redacted] |
| 6 | eni-[redacted] | [redacted] |

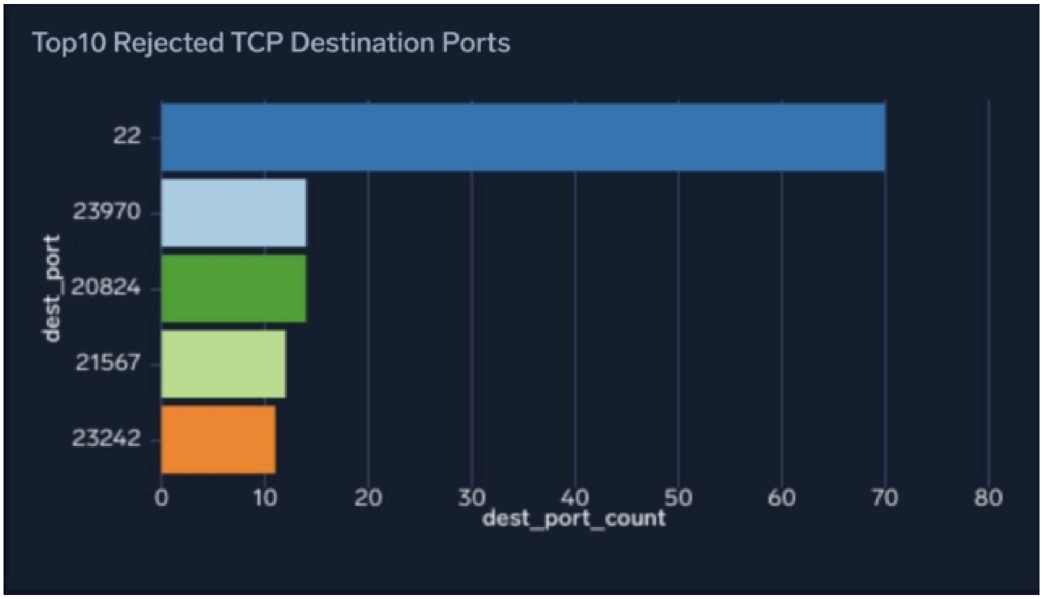
### Total Rejected Flow Records

Displays the number of rejected communication flows for the last 15 minutes (the graph below shows a sparkline of the number of rejected communication flows every 15 minutes over a 1-hour period)



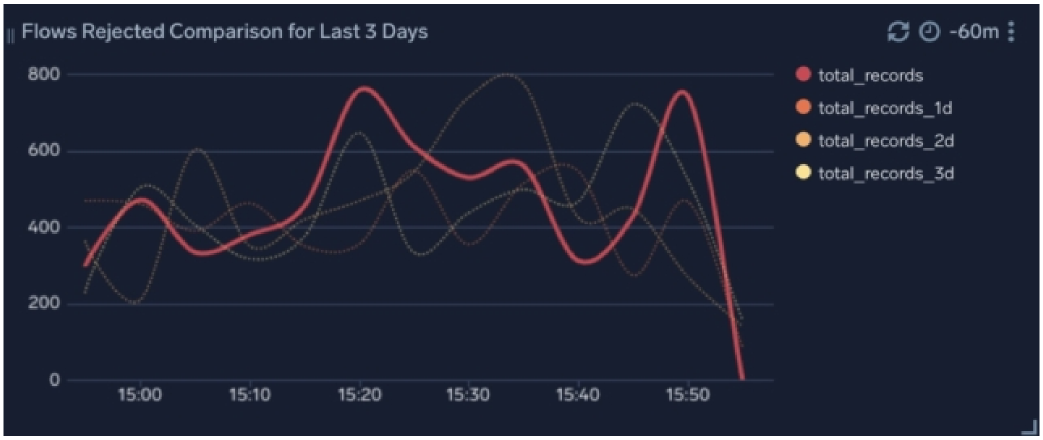
### Top 10 Rejected TCP Destination Ports

Displays the number of rejected TCP outbound communications by destination port over the past hour, sorted by frequency from most to least.



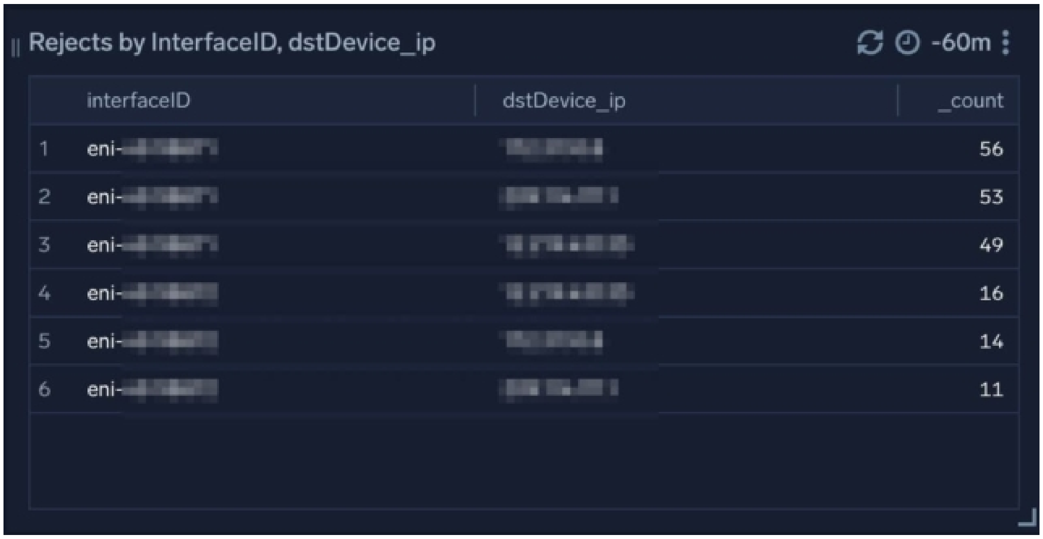
### Flows Rejected Comparison for Last 3 Days

Displays the number of rejected packets every 5 minutes for the past hour and the number of packets for each time period for the past 3 days in a line chart.



### Rejects by InterfaceID, dstDevice_ip

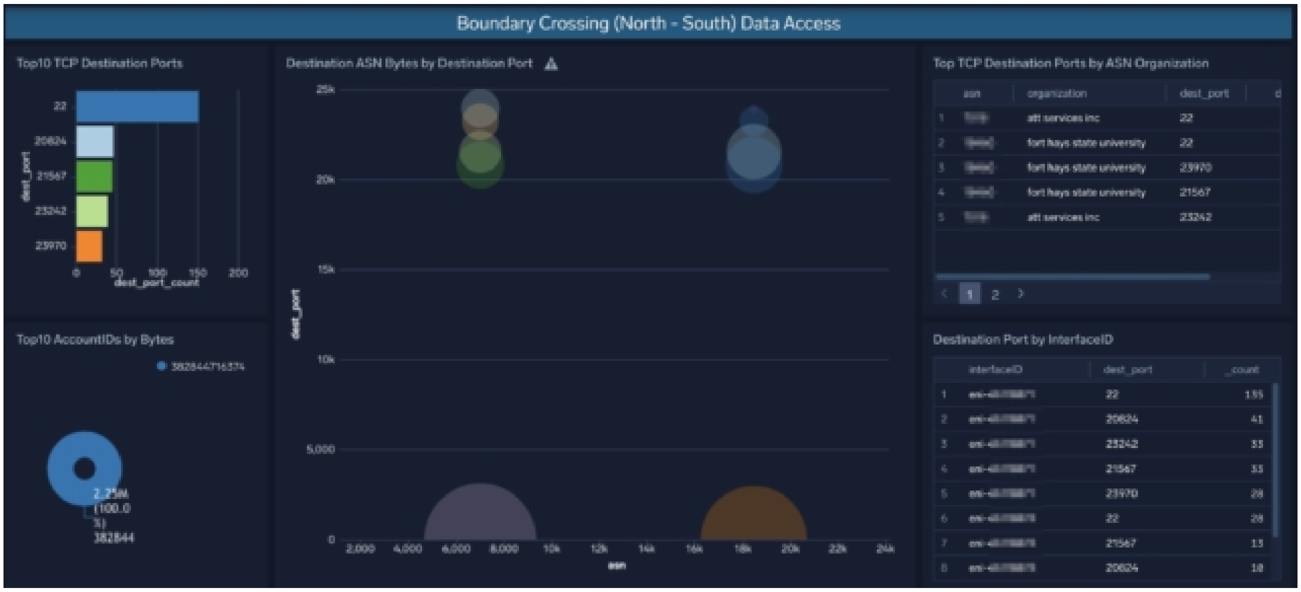
Displays a table of the number of rejected communication flows for each interface ID and destination IP address within the last hour



| | interfaceID | dstDevice_ip | _count |
|---|---|---|---|
| 1 | eni-[redacted] | [redacted] | 56 |
| 2 | eni-[redacted] | [redacted] | 53 |
| 3 | eni-[redacted] | [redacted] | 49 |
| 4 | eni-[redacted] | [redacted] | 16 |
| 5 | eni-[redacted] | [redacted] | 14 |
| 6 | eni-[redacted] | [redacted] | 11 |

## Boundary Crossing (North - South) Data Access

Boundary Crossing (North - South) Data Access displays TCP communication between the Internet and AWS and aggregated results by destination port.


Boundary Crossing (North - South) Data Access
Top10 TCP Destination Ports
22
20624
21567
23242
23970
dest_port
0
50
100
150
200
dest_port_count
Top10 AccountIDs by Bytes
382844716374
2.75M
(100.0
%)
382844
Destination ASN Bytes by Destination Port
25k
20k
15k
10k
5,000
0
dest_port
2,000
4,000
6,000
8,000
10k
12k
14k
16k
18k
20k
22k
24k
asn
Top TCP Destination Ports by ASN Organization
1
2
Destination Port by InterfaceID

Top TCP Destination Ports by ASN Organization

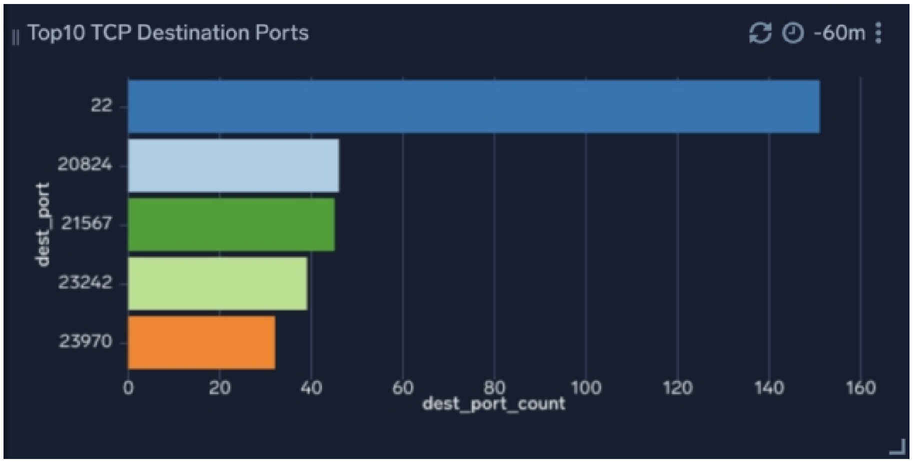
| | asn | organization | dest_port | d |
|---|---|---|---|---|
| 1 | [redacted] | att services inc | 22 | |
| 2 | [redacted] | fort hays state university | 22 | |
| 3 | [redacted] | fort hays state university | 23970 | |
| 4 | [redacted] | fort hays state university | 21567 | |
| 5 | [redacted] | att services inc | 23242 | |

Destination Port by InterfaceID

| | interfaceID | dest_port | _count |
|---|---|---|---|
| 1 | eni-[redacted] | 22 | 135 |
| 2 | eni-[redacted] | 20624 | 41 |
| 3 | eni-[redacted] | 23242 | 33 |
| 4 | eni-[redacted] | 21567 | 33 |
| 5 | eni-[redacted] | 23970 | 28 |
| 6 | eni-[redacted] | 22 | 28 |
| 7 | eni-[redacted] | 21567 | 13 |
| 8 | eni-[redacted] | 20624 | 10 |

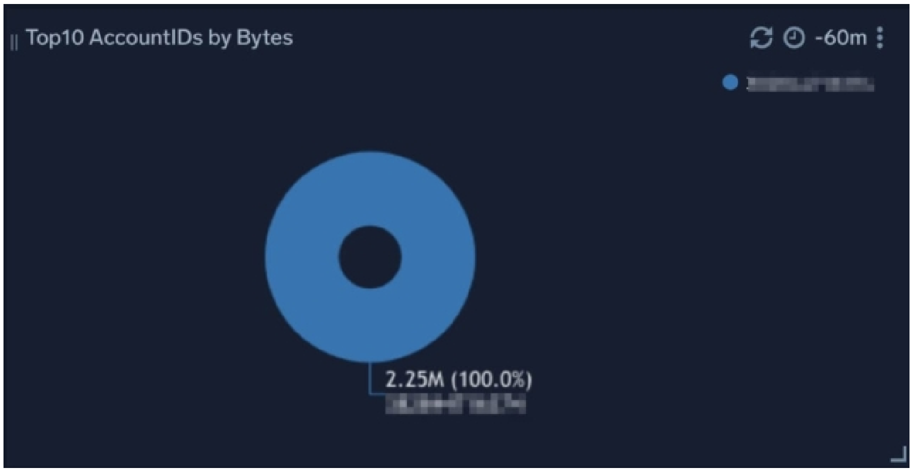
### Top 10 TCP Destination Ports

Displays the number of allowed TCP outbound communications by destination port for the past hour in a bar chart.



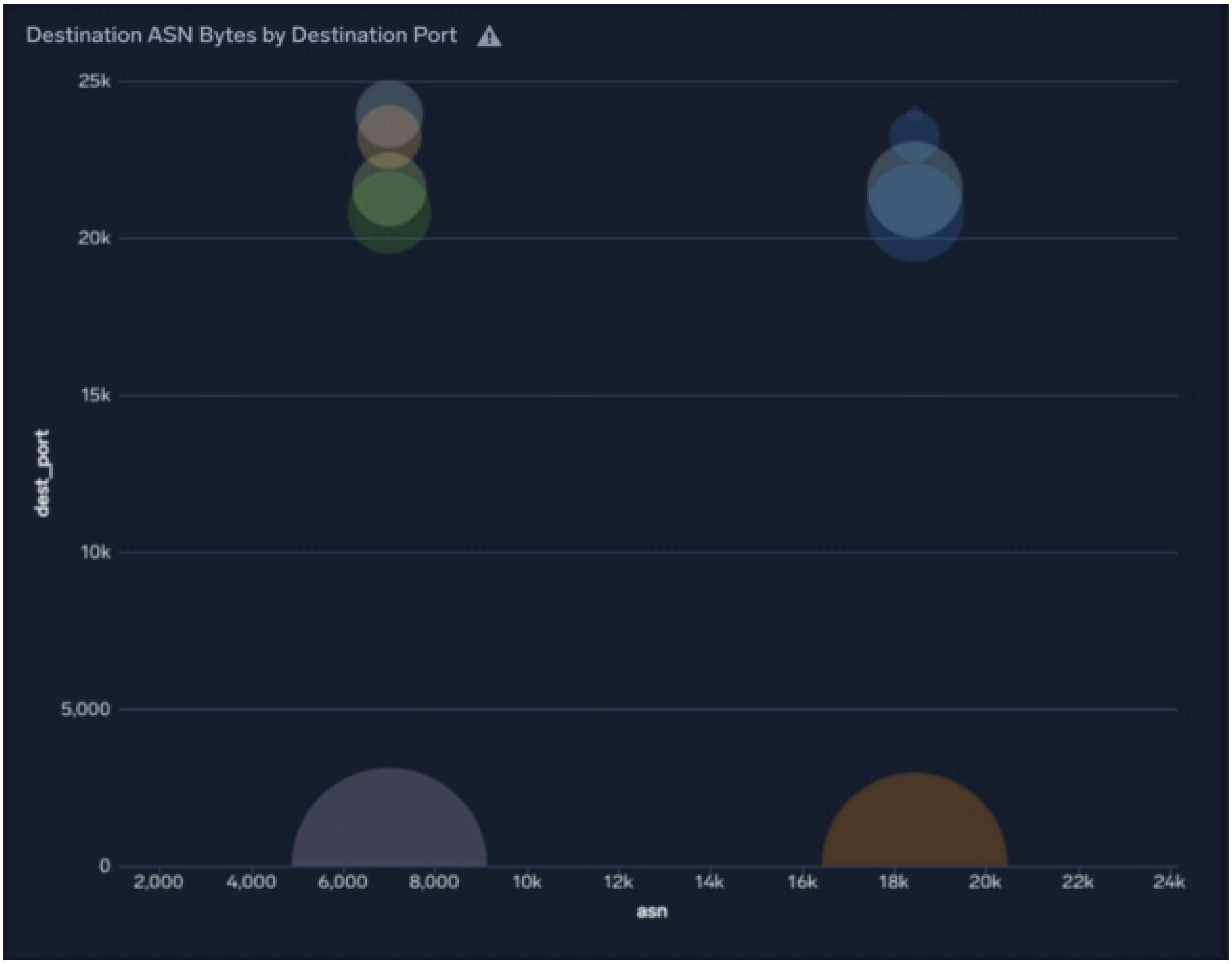
### Top 10 Account IDs by Bytes

Displays the amount of TCP inbound/outbound traffic allowed within the last hour by account ID in a donut chart.



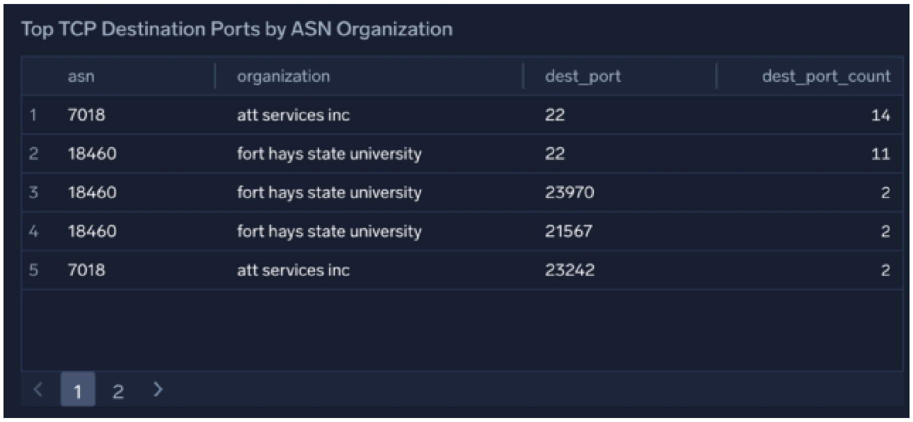
### Destination ASN Bytes by Destination Port

Displays the AS number to which the destination IP belongs and the traffic volume for each destination port for permitted outbound communications within the past hour in a bubble chart.



## Top TCP Destination Ports by ASN Organization

Displays the AS number to which the destination IP of the TCP outbound communication allowed within the last hour belongs, along with the number of ISP vendors and destination ports in descending order.

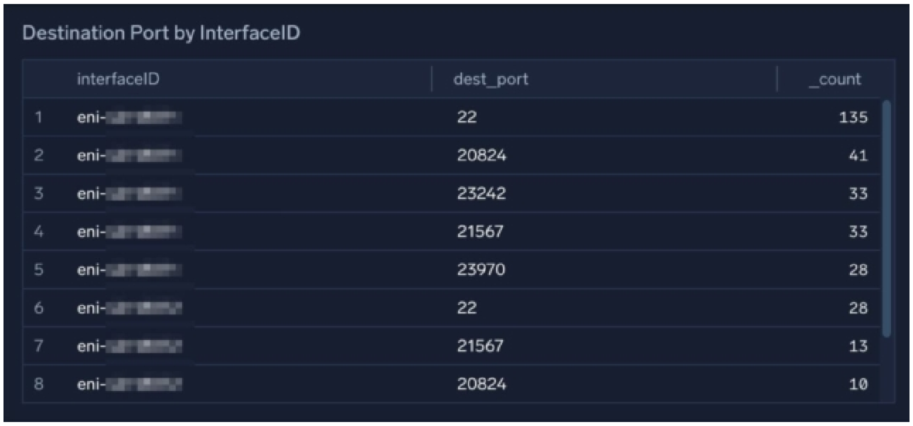


Top TCP Destination Ports by ASN Organization

| | asn | organization | dest_port | dest_port_count |
|---|---|---|---|---|
| 1 | 7018 | att services inc | 22 | 14 |
| 2 | 18460 | fort hays state university | 22 | 11 |
| 3 | 18460 | fort hays state university | 23970 | 2 |
| 4 | 18460 | fort hays state university | 21567 | 2 |
| 5 | 7018 | att services inc | 23242 | 2 |

### Destination Port by InterfaceID

Displays the number of permitted outbound communications for the last hour by interface ID and destination port in a table sorted from most to least.

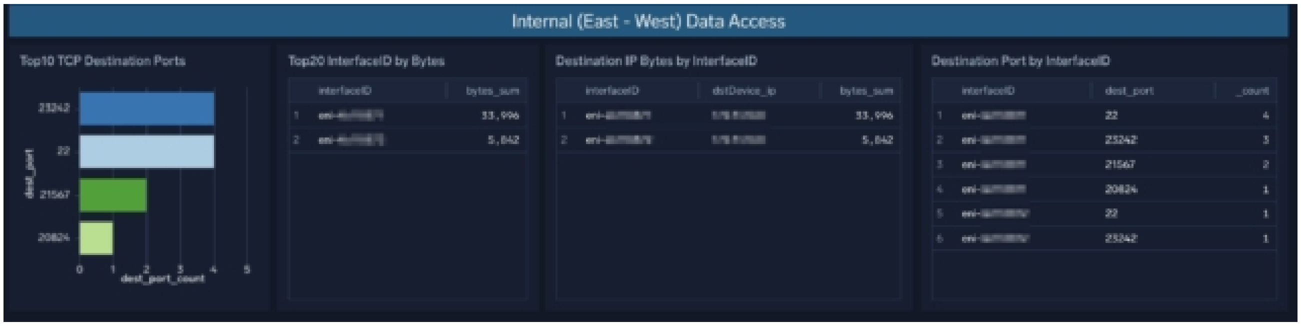


Destination Port by InterfaceID

|   | interfaceID | dest_port | _count |
|---|---|---|---|
| 1 | eni-[redacted] | 22 | 135 |
| 2 | eni-[redacted] | 20824 | 41 |
| 3 | eni-[redacted] | 23242 | 33 |
| 4 | eni-[redacted] | 21567 | 33 |
| 5 | eni-[redacted] | 23970 | 28 |
| 6 | eni-[redacted] | 22 | 28 |
| 7 | eni-[redacted] | 21567 | 13 |
| 8 | eni-[redacted] | 20824 | 10 |

## Internal (East - West) Data Access

It displays the aggregated results of internal communications between AWS and AWS.



Internal (East - West) Data Access

Top10 TCP Destination Ports

Top20 InterfaceID by Bytes

|   | interfaceID | bytes_sum |
|---|---|---|
| 1 | eni-[redacted] | 33,996 |
| 2 | eni-[redacted] | 5,842 |

Destination IP Bytes by InterfaceID

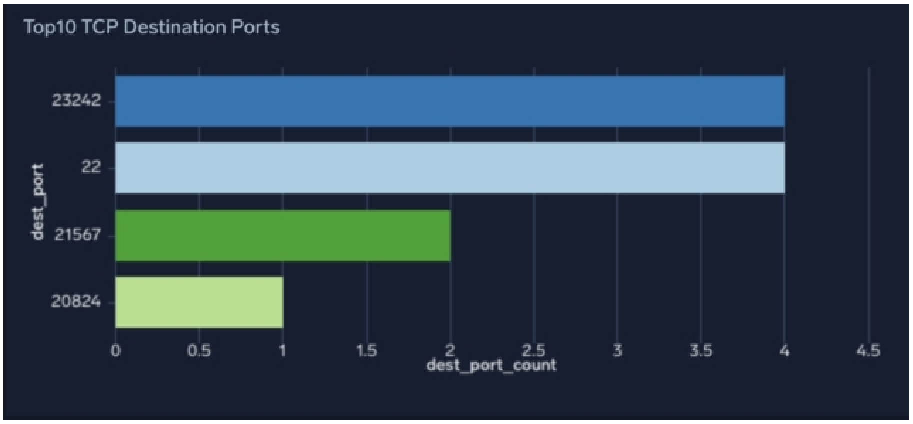
|   | interfaceID | dstDevice_ip | bytes_sum |
|---|---|---|---|
| 1 | eni-[redacted] | [redacted] | 33,996 |
| 2 | eni-[redacted] | [redacted] | 5,842 |

Destination Port by InterfaceID

|   | interfaceID | dest_port | _count |
|---|---|---|---|
| 1 | eni-[redacted] | 22 | 4 |
| 2 | eni-[redacted] | 23242 | 3 |
| 3 | eni-[redacted] | 21567 | 2 |
| 4 | eni-[redacted] | 20824 | 1 |
| 5 | eni-[redacted] | 22 | 1 |
| 6 | eni-[redacted] | 23242 | 1 |

### Top 10 TCP Destination Ports

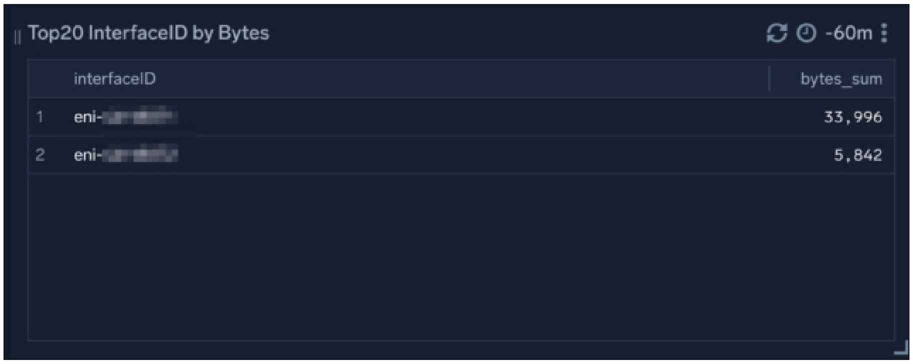
Displays the number of allowed TCP internal communications by destination port for the past hour in a bar chart.



Top10 TCP Destination Ports

### Top 20 InterfaceID by Bytes

A table showing the amount of internal communication allowed within the last hour by interface ID, sorted by traffic volume.



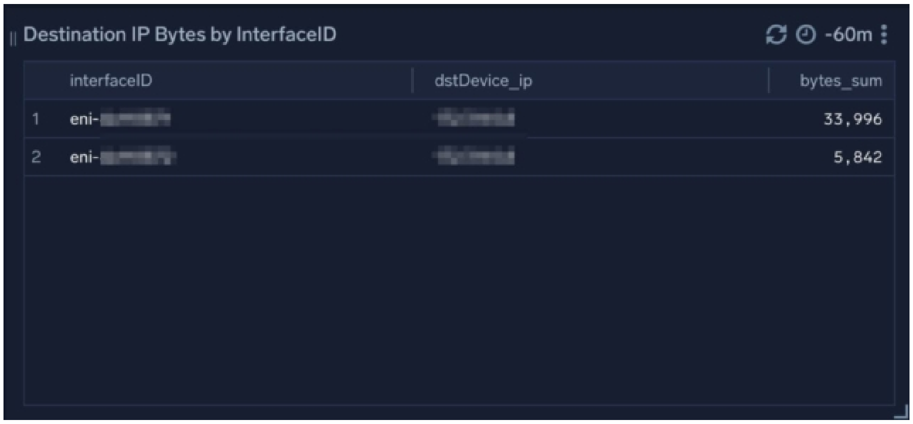
Top20 InterfaceID by Bytes

-60m

| | interfaceID | bytes_sum |
|---|---|---|
| 1 | eni-[redacted] | 33,996 |
| 2 | eni-[redacted] | 5,842 |

### Destination IP Bytes by InterfaceID

Displays a table of allowed internal communications within the last hour, sorted by interface ID and destination IP address, sorted by traffic volume.



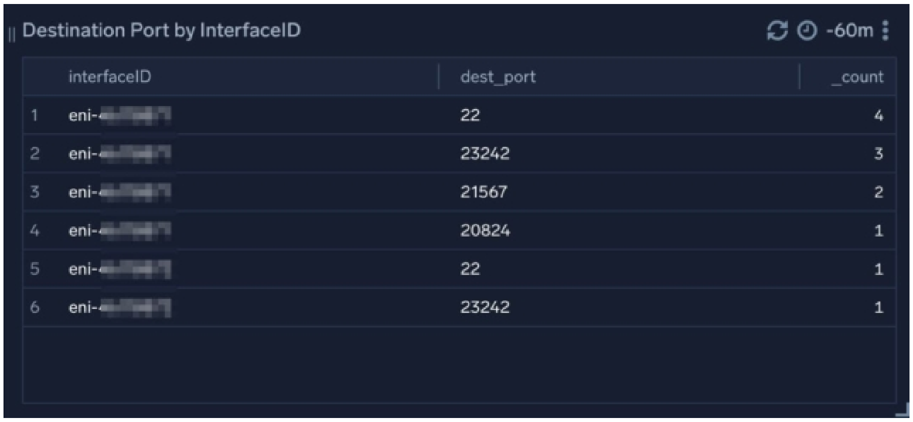
Destination IP Bytes by InterfaceID

-60m

| | interfaceID | dstDevice_ip | bytes_sum |
|---|---|---|---|
| 1 | eni-[redacted] | [redacted] | 33,996 |
| 2 | eni-[redacted] | [redacted] | 5,842 |

### Destination Port by InterfaceID

Displays the number of permitted internal communications by interface ID and destination port for the past hour in a table sorted from most to least.

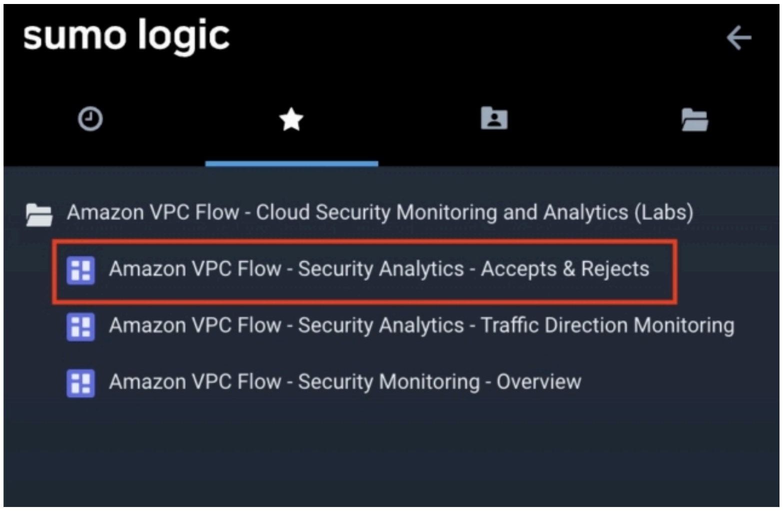


Destination Port by InterfaceID

-60m

| | interfaceID | dest_port | _count |
|---|---|---|---|
| 1 | eni-[redacted] | 22 | 4 |
| 2 | eni-[redacted] | 23242 | 3 |
| 3 | eni-[redacted] | 21567 | 2 |
| 4 | eni-[redacted] | 20824 | 1 |
| 5 | eni-[redacted] | 22 | 1 |
| 6 | eni-[redacted] | 23242 | 1 |

Next, go back to the folder and look at the next dashboard: Amazon VPC Flow - Security Analytics - Accepts & Rejects.



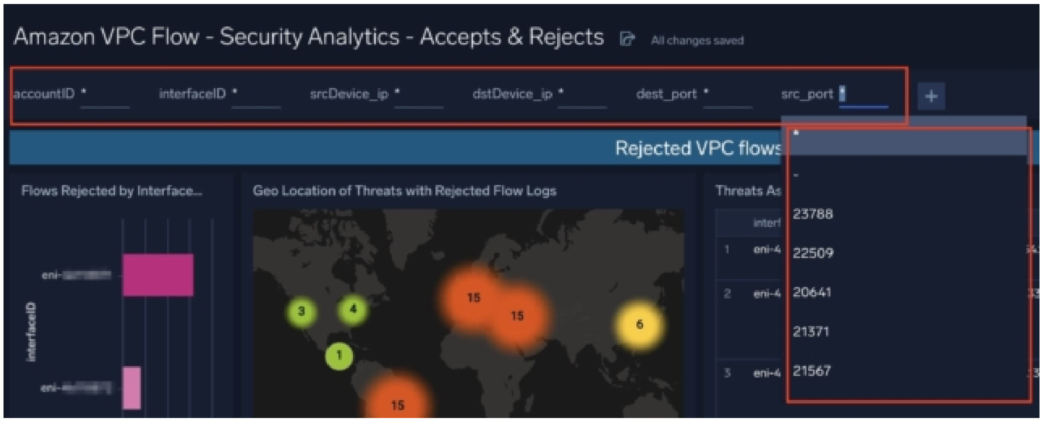
sumo logic

Amazon VPC Flow - Cloud Security Monitoring and Analytics (Labs)

- Amazon VPC Flow - Security Analytics - Accepts & Rejects
- Amazon VPC Flow - Security Analytics - Traffic Direction Monitoring
- Amazon VPC Flow - Security Monitoring - Overview

## Amazon VPC Flow - Security Analytics - Accepts & Rejects

Here too, you can filter the entire dashboard by account ID, interface ID, source IP, destination IP, destination port, and source port.



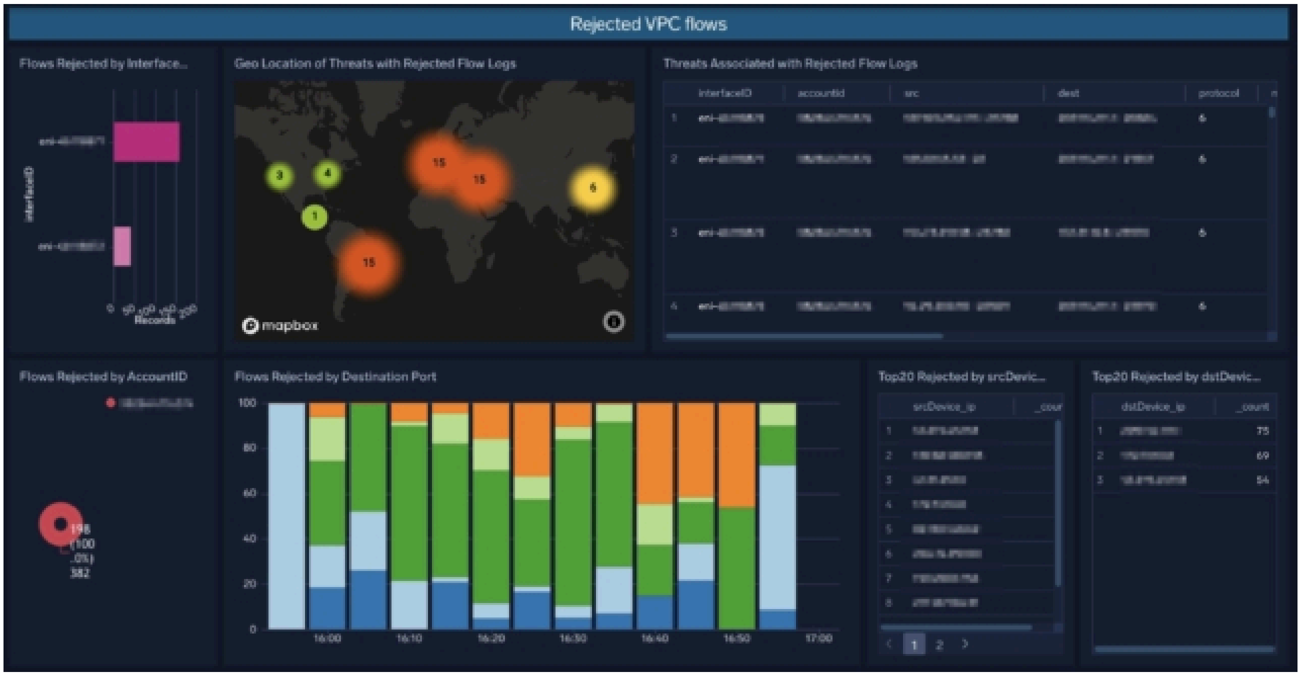
Amazon VPC Flow - Security Analytics - Accepts & Rejects All changes saved

accountID * interfaceID * srcDevice_ip * dstDevice_ip * dest_port * src_port

*
-
23788
22509
20641
21371
21567

## Rejected VPC flows

It gives you insight into rejected communications.



Threats Associated with Rejected Flow Logs

| | interfaceID | accountid | src | dest | protocol |
|---|---|---|---|---|---|
| 1 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 |
| 2 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 |
| 3 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 |
| 4 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 |

Top20 Rejected by srcDevic...

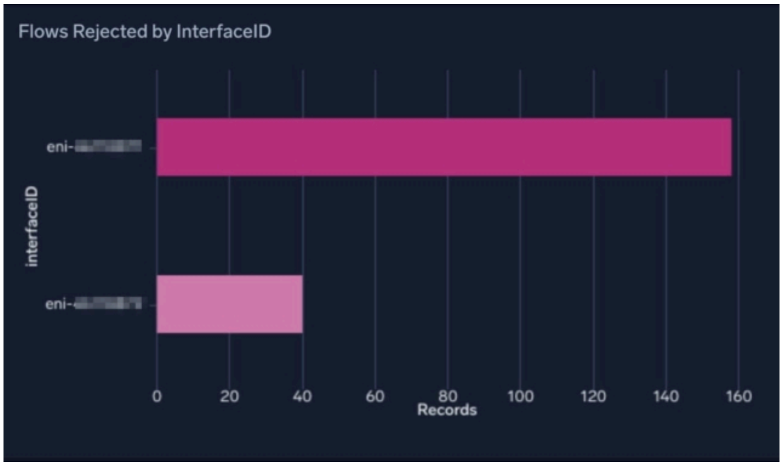
| | srcDevice_ip | _cour |
|---|---|---|
| 1 | [redacted] | |
| 2 | [redacted] | |
| 3 | [redacted] | |
| 4 | [redacted] | |
| 5 | [redacted] | |
| 6 | [redacted] | |
| 7 | [redacted] | |
| 8 | [redacted] | |

Top20 Rejected by dstDevic...

| | dstDevice_ip | _count |
|---|---|---|
| 1 | [redacted] | 75 |
| 2 | [redacted] | 69 |
| 3 | [redacted] | 54 |

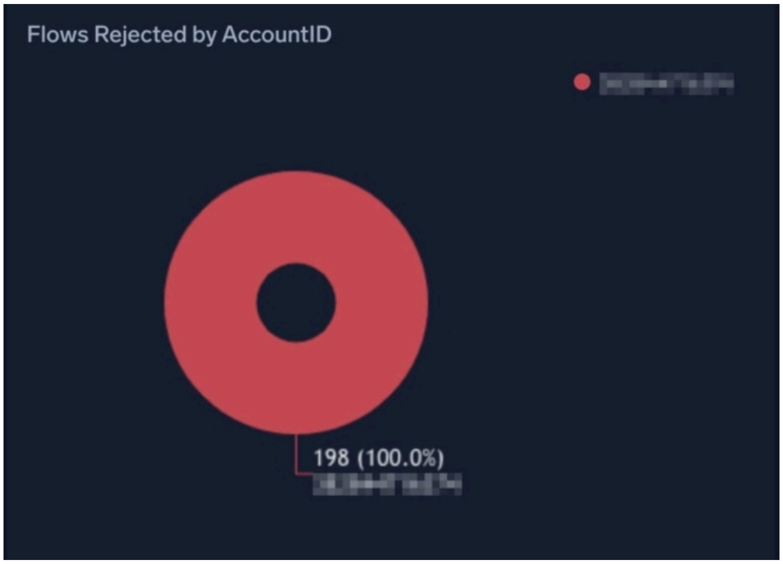
### Flows Rejected by InterfaceID

Displays the number of denied communication flows for each interface ID within the last hour in a bar chart.



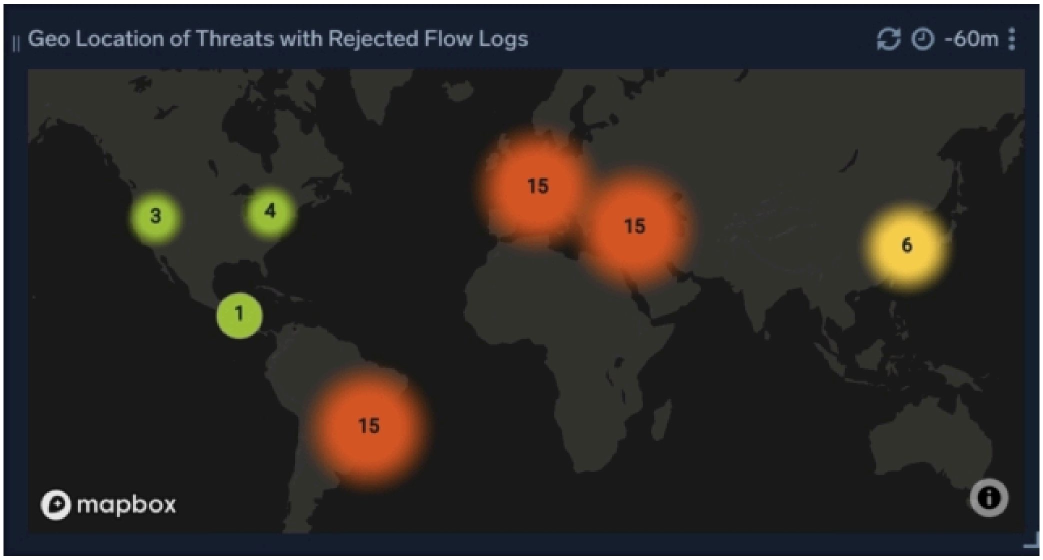
### Flows Rejected by AccountID

Displays the number of rejected communication flows for each account ID within the last hour in a donut chart.



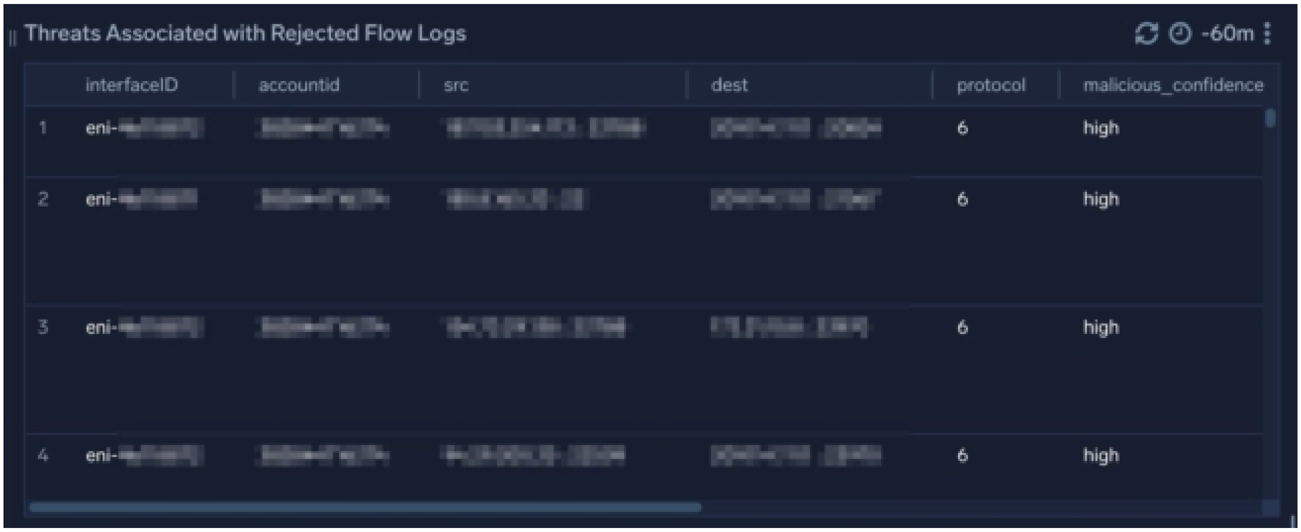
### Geo Location of Threats with Rejected Flow Logs

Geo-located view of denied inbound traffic where the source IP matches a threat IP in CrowdStrike Intelligence within the last hour



### Threats Associated with Rejected Flow Logs

Displays a table showing the number of denied communication flows within the last hour where the source IP matches a threat IP with a severity of High in CrowdStrike Intelligence.

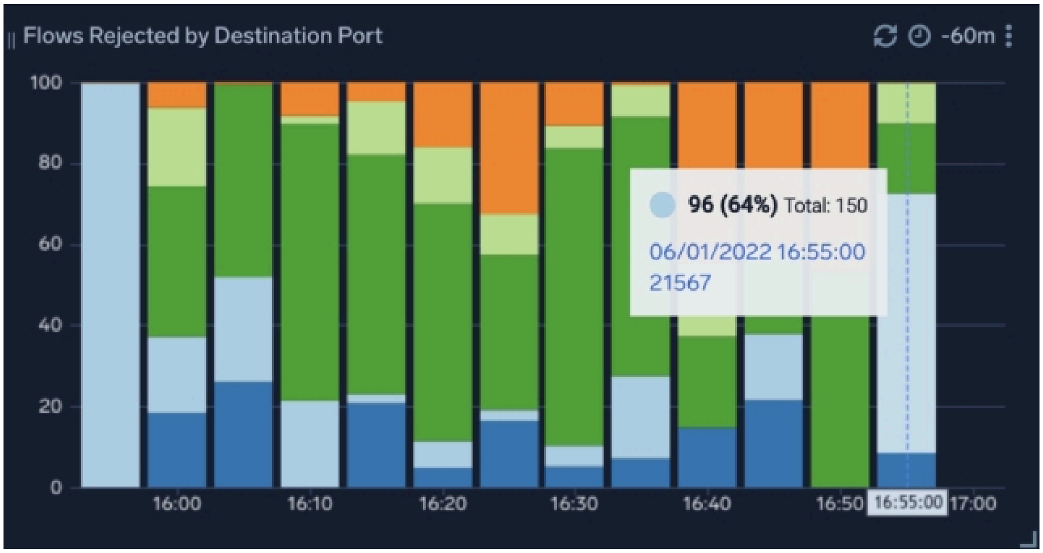


Threats Associated with Rejected Flow Logs

|   | interfaceID | accountid | src | dest | protocol | malicious_confidence |
|---|---|---|---|---|---|---|
| 1 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 | high |
| 2 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 | high |
| 3 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 | high |
| 4 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 | high |

### Flows Rejected by Destination Port

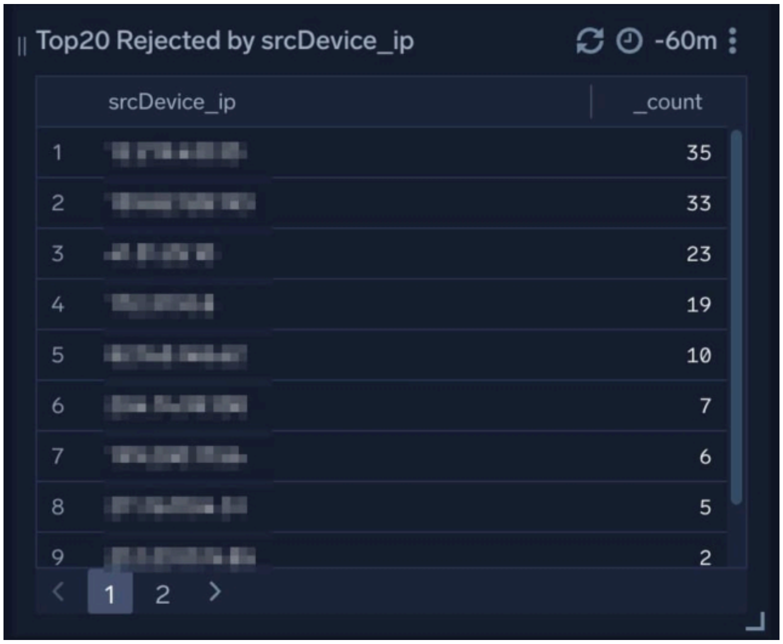
Displays the number of rejected packets by destination port for every 5 minutes within the last hour in a bar graph chart.



Flows Rejected by Destination Port

### Top20 Rejected by srcDevice_ip

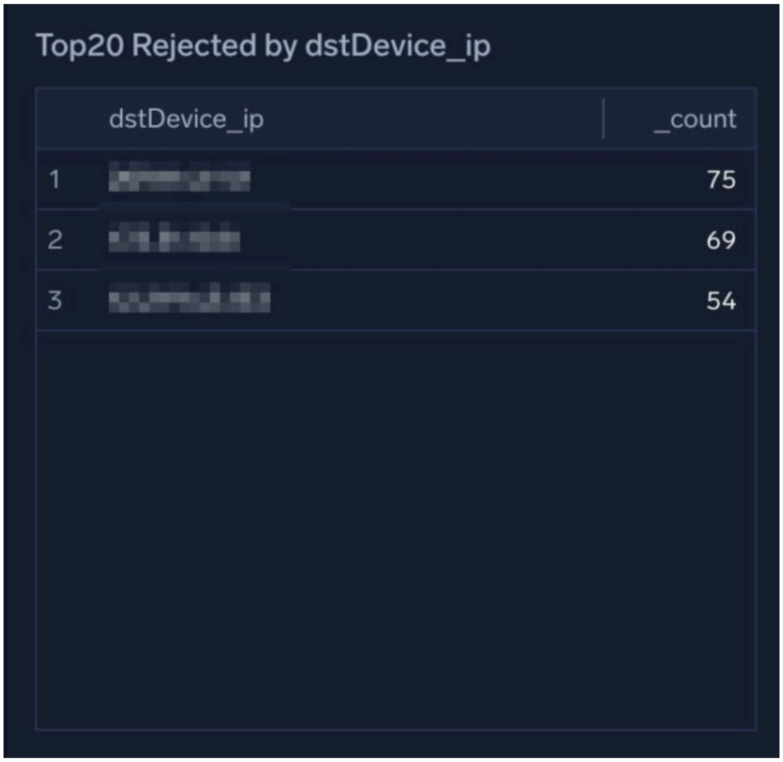
Displays a table of the top 20 source IPs for rejected communication flows within the last hour



| | srcDevice_ip | _count |
|---|---|---|
| 1 | [redacted] | 35 |
| 2 | [redacted] | 33 |
| 3 | [redacted] | 23 |
| 4 | [redacted] | 19 |
| 5 | [redacted] | 10 |
| 6 | [redacted] | 7 |
| 7 | [redacted] | 6 |
| 8 | [redacted] | 5 |
| 9 | [redacted] | 2 |

### Top20 Rejected by dstDevice_ip

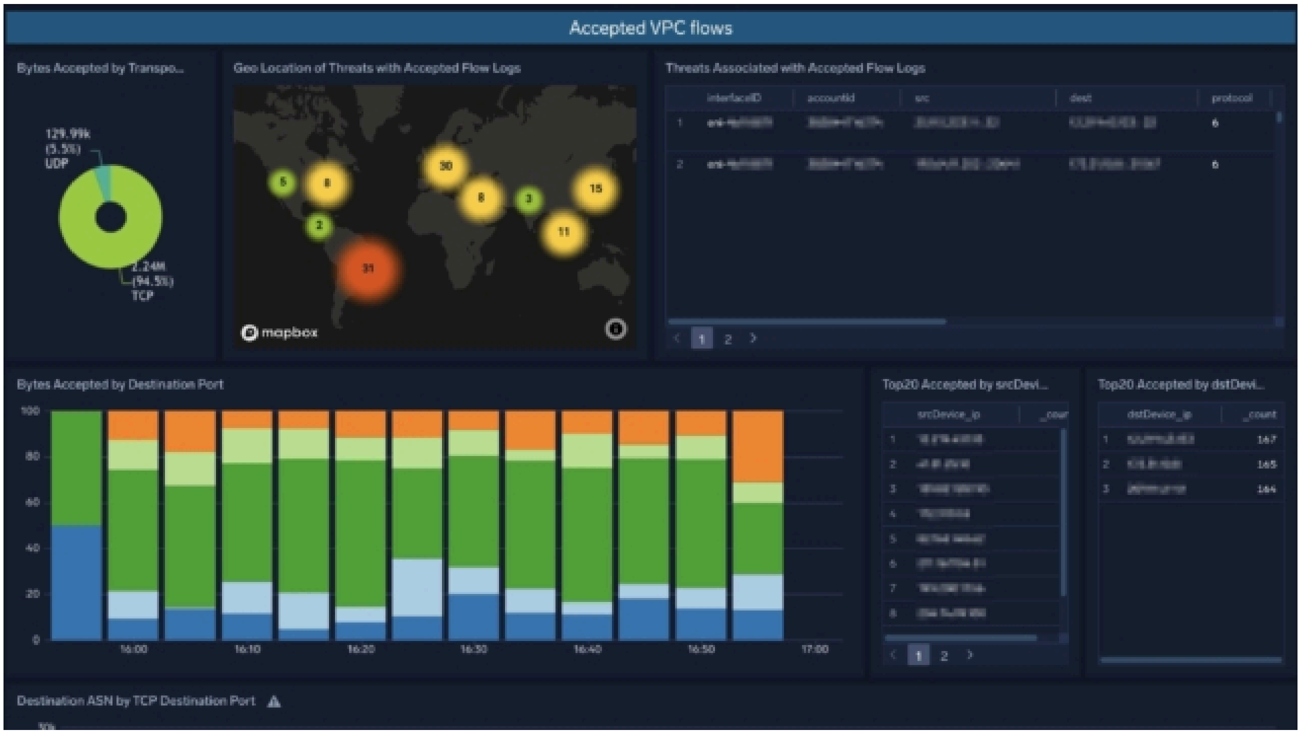
Displays a table of the top 20 destination IPs for rejected communication flows within the last hour



| | dstDevice_ip | _count |
|---|---|---|
| 1 | [redacted] | 75 |
| 2 | [redacted] | 69 |
| 3 | [redacted] | 54 |

## Accepted VPC flows

It gives you insight into allowed communications.



Accepted VPC flows

Bytes Accepted by Transpo...

Geo Location of Threats with Accepted Flow Logs

Threats Associated with Accepted Flow Logs

| | interfaceID | accountId | src | dest | protocol |
|---|---|---|---|---|---|
| 1 | [redacted] | [redacted] | [redacted] | [redacted] | 6 |
| 2 | [redacted] | [redacted] | [redacted] | [redacted] | 6 |

< 1 2 >

Bytes Accepted by Destination Port

Top20 Accepted by srcDevi...

| | srcDevice_ip | _cour |
|---|---|---|
| 1 | [redacted] | |
| 2 | [redacted] | |
| 3 | [redacted] | |
| 4 | [redacted] | |
| 5 | [redacted] | |
| 6 | [redacted] | |
| 7 | [redacted] | |
| 8 | [redacted] | |

< 1 2 >

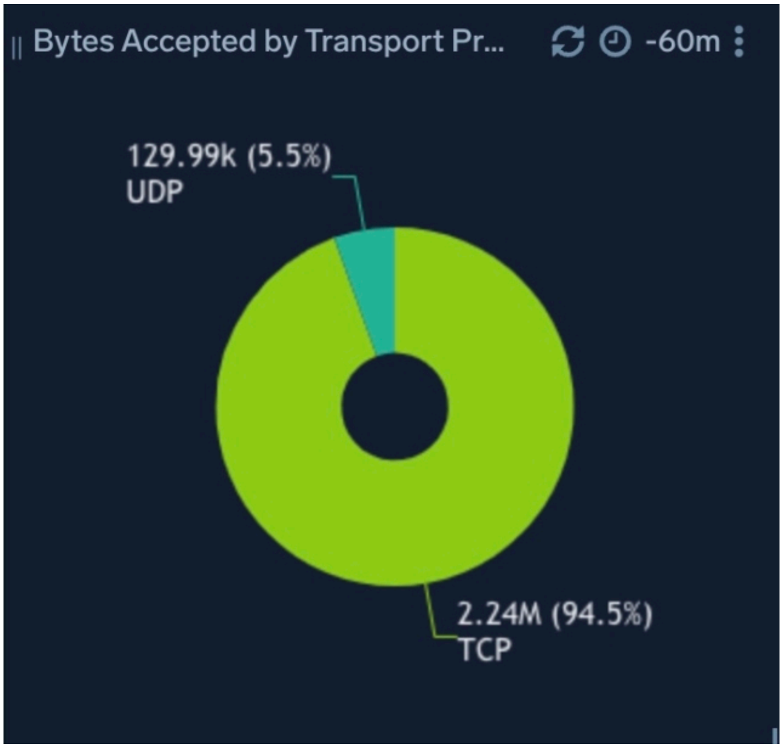
Top20 Accepted by dstDevi...

| | dstDevice_ip | _count |
|---|---|---|
| 1 | [redacted] | 167 |
| 2 | [redacted] | 165 |
| 3 | [redacted] | 164 |

Destination ASN by TCP Destination Port

### Bytes Accepted by Transport Protocol

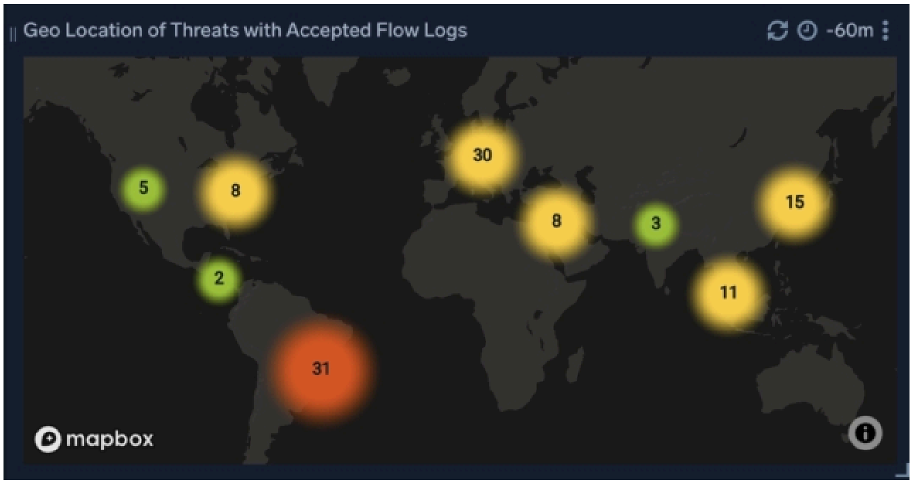
Displays the amount of traffic by protocol for permitted communication flows within the last hour in a donut chart.



Bytes Accepted by Transport Pr...

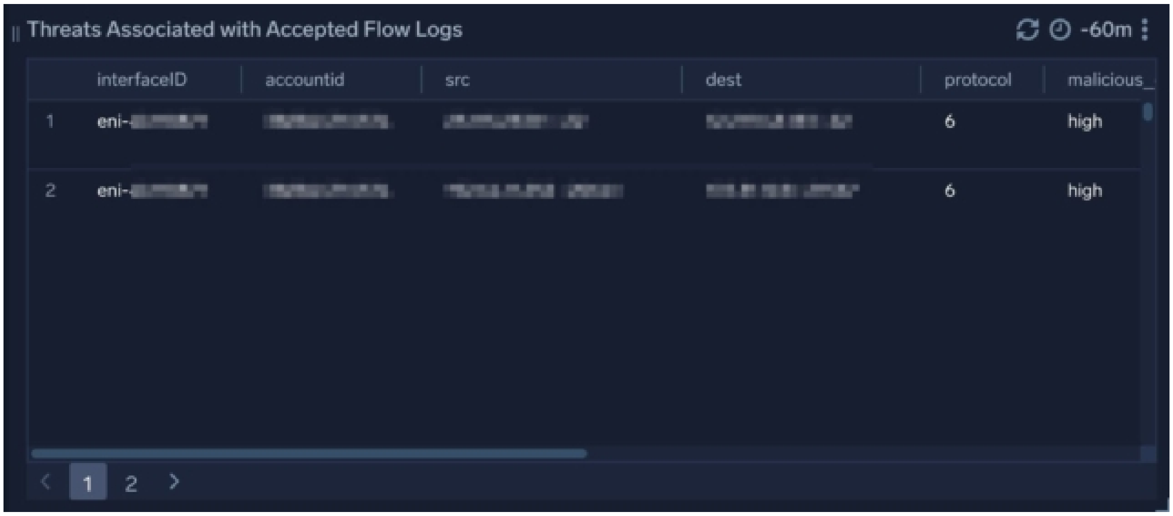
## Geo Location of Threats with Accepted Flow Logs

Geo-location of allowed inbound traffic where the source IP matches a threat IP in CrowdStrike Intelligence within the last hour



## Threats Associated with Accepted Flow Logs

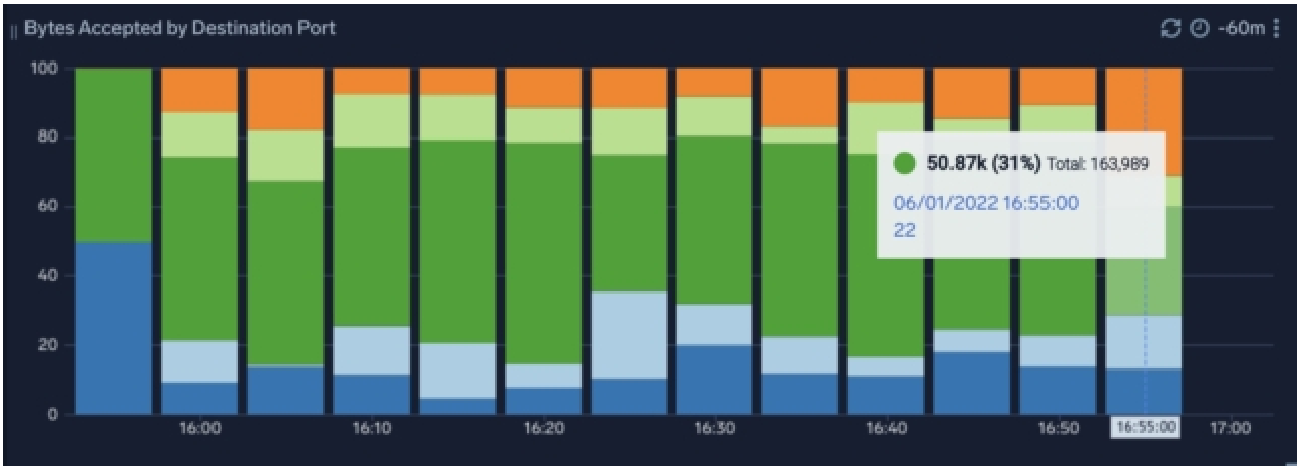
Displays communication flows (access sources) with a high severity that match authorized CrowdStrike Intelligence threat IPs within the past hour in a table format.



|  | interfaceID | accountid | src | dest | protocol | malicious_ |
|---|---|---|---|---|---|---|
| 1 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 | high |
| 2 | eni-[redacted] | [redacted] | [redacted] | [redacted] | 6 | high |

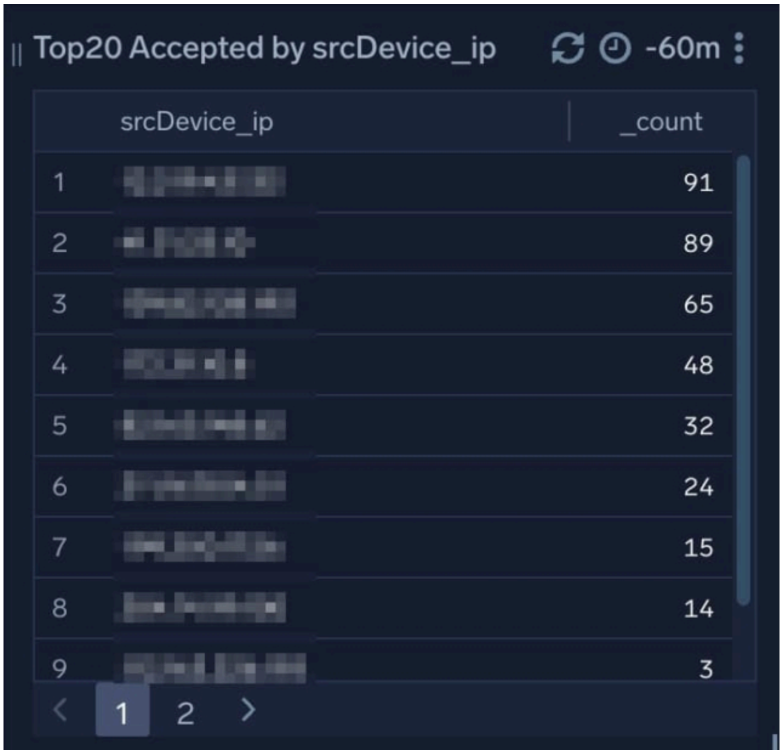
### Bytes Accepted by Destination Port

Displays the permitted traffic volume for each destination port for every 5 minutes within the past hour in a 100% stacked bar graph.



### Top20 Accepted by srcDevice_ip

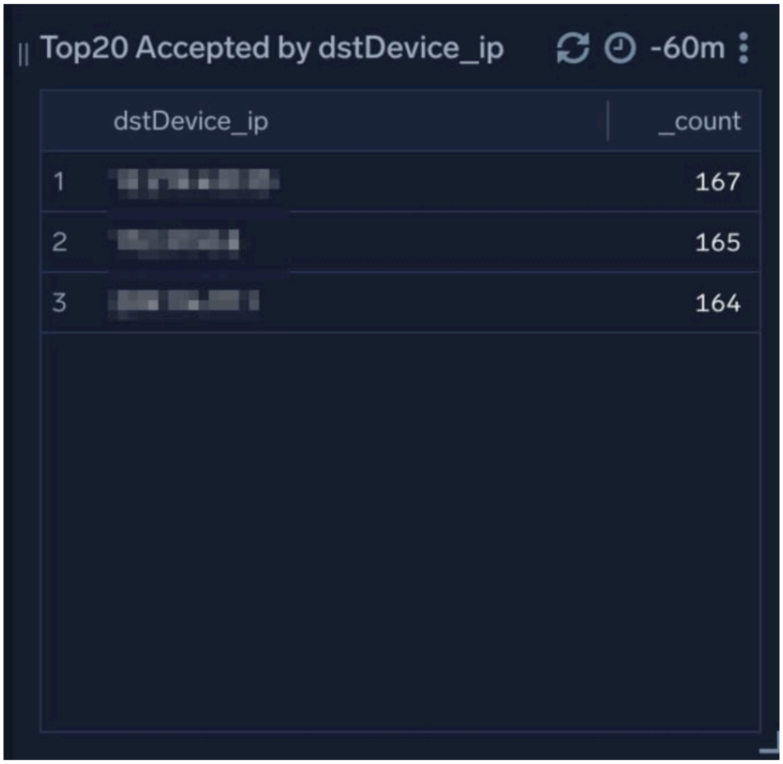
Displays a table of the top 20 source IPs for permitted communication flows within the last hour



| | srcDevice_ip | _count |
|---|---|---|
| 1 | [redacted] | 91 |
| 2 | [redacted] | 89 |
| 3 | [redacted] | 65 |
| 4 | [redacted] | 48 |
| 5 | [redacted] | 32 |
| 6 | [redacted] | 24 |
| 7 | [redacted] | 15 |
| 8 | [redacted] | 14 |
| 9 | [redacted] | 3 |

### Top20 Rejected by dstDevice_ip

Displays a table of the top 20 destination IPs for permitted communication flows within the last hour

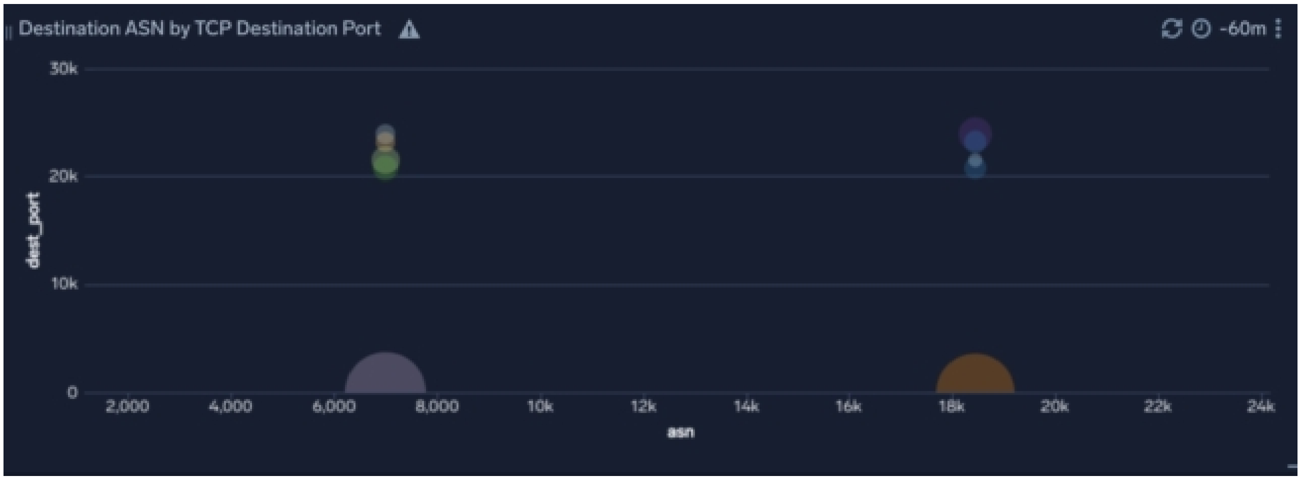


Top20 Accepted by dstDevice_ip

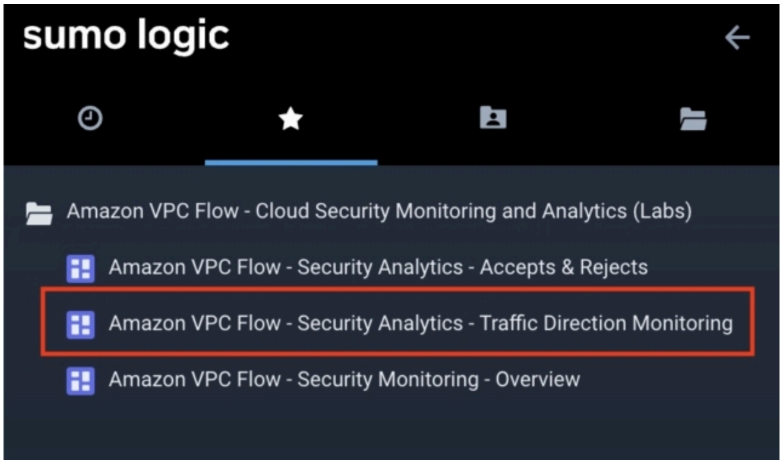
| | dstDevice_ip | _count |
|---|---|---|
| 1 | [redacted] | 167 |
| 2 | [redacted] | 165 |
| 3 | [redacted] | 164 |

### Destination ASN by TCP Destination Port

Displays the number of permitted TCP outbound communications within the past hour by AS number and destination port.



Next, go back to the folder and look at the next dashboard: Amazon VPC Flow - Security Analytics - Traffic Direction Monitoring.



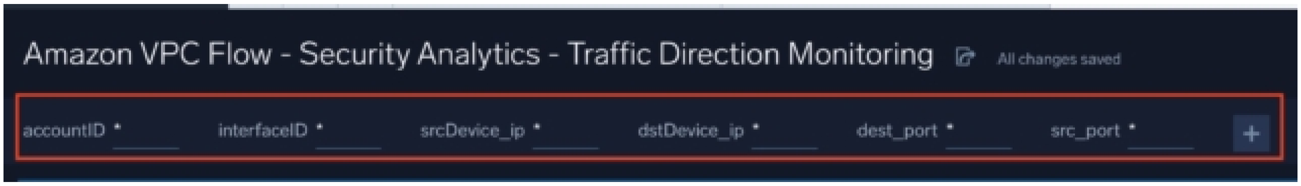
sumo logic

Amazon VPC Flow - Cloud Security Monitoring and Analytics (Labs)

- Amazon VPC Flow - Security Analytics - Accepts & Rejects
- Amazon VPC Flow - Security Analytics - Traffic Direction Monitoring
- Amazon VPC Flow - Security Monitoring - Overview

## Amazon VPC Flow - Security Analytics - Traffic Direction Monitoring

Here too, you can filter the entire dashboard by account ID, interface ID, source IP, destination IP, destination port, and source port.

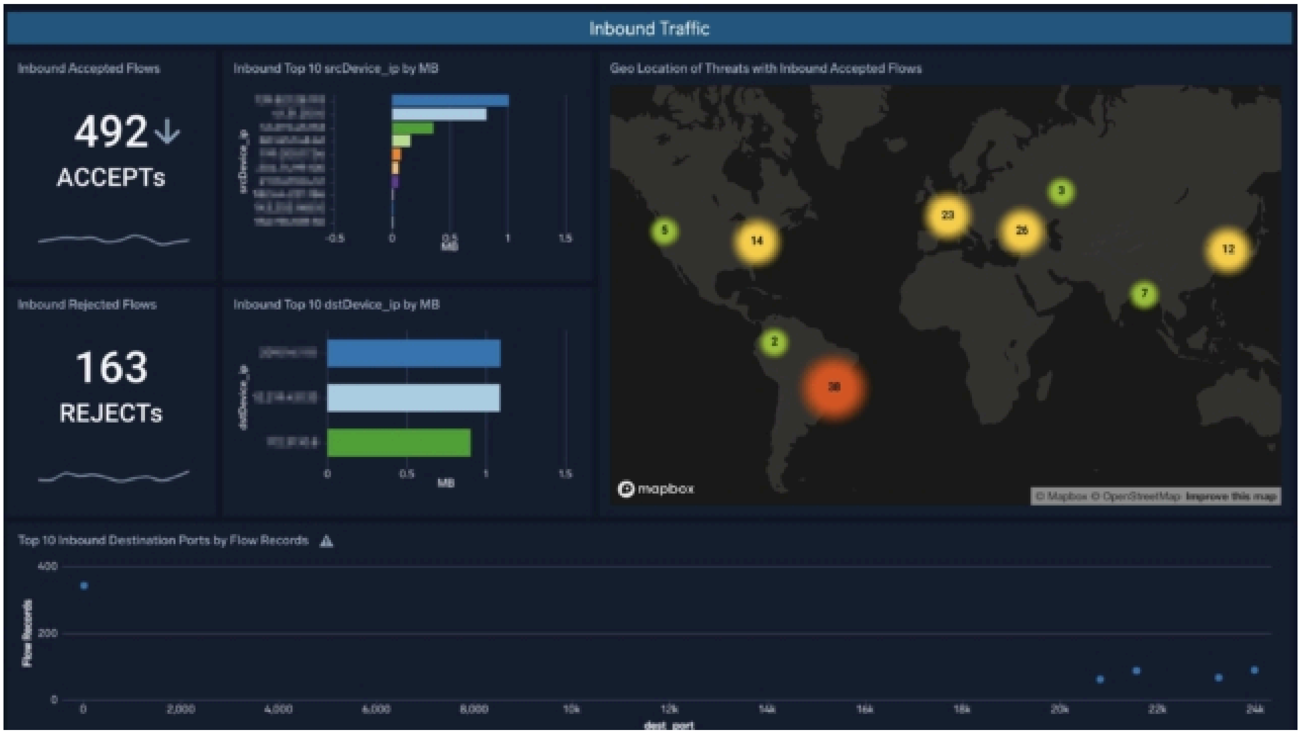


Amazon VPC Flow - Security Analytics - Traffic Direction Monitoring All changes saved

accountID * interfaceID * srcDevice_ip * dstDevice_ip * dest_port * src_port * +

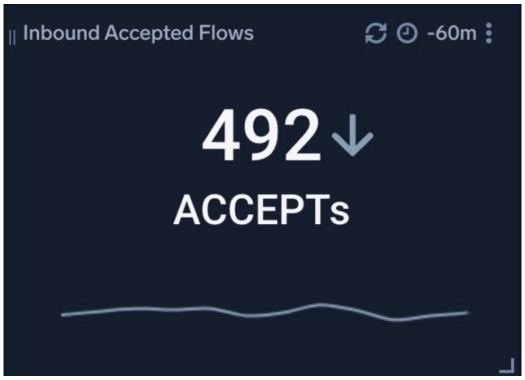
### Inbound Traffic

This is a dashboard for inbound communication between the Internet and AWS.



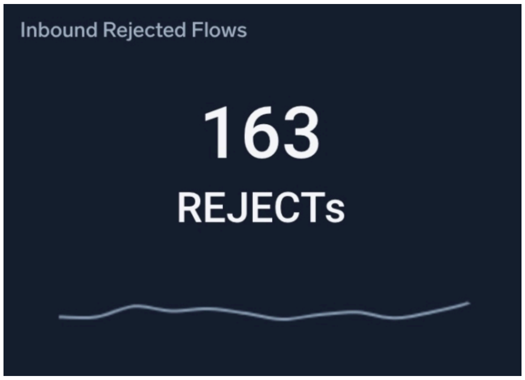
### Inbound Accepted Flows

Displays the number of inbound communications allowed over the last 5 minutes (the graph below shows a sparkline of the number of inbound communications allowed over 5-minute intervals over a 1-hour period)



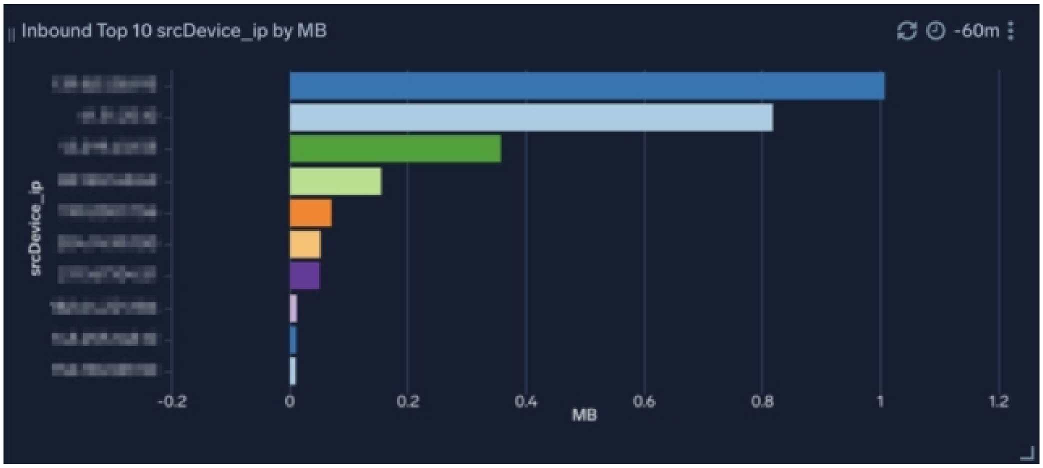
### Inbound Rejected Flows

Shows the number of rejected inbound communications over the last 5 minutes (the graph below shows a sparkline of rejected inbound communications over 5-minute intervals over a 1-hour period)



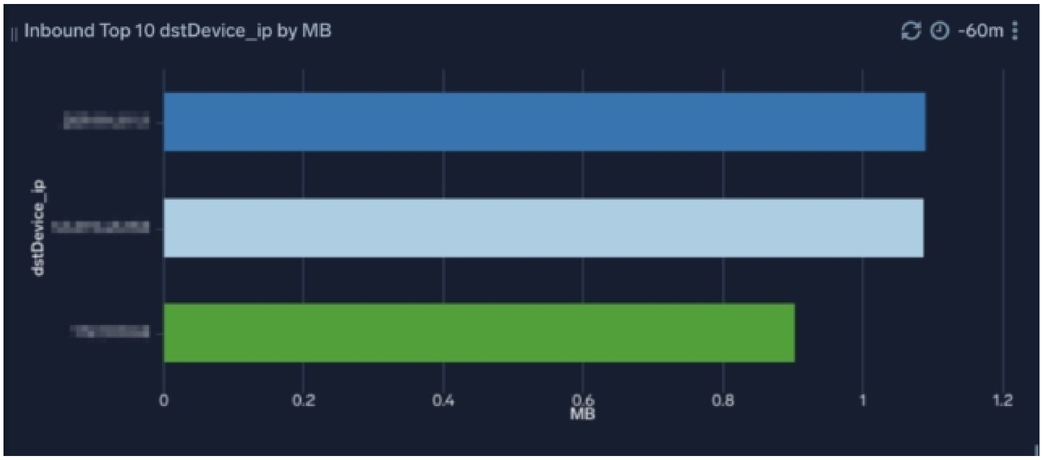
### Inbound Top 10 srcDevice_ip by MB

Displays the top 10 traffic volumes for inbound traffic by source IP address for the past hour in a bar chart.



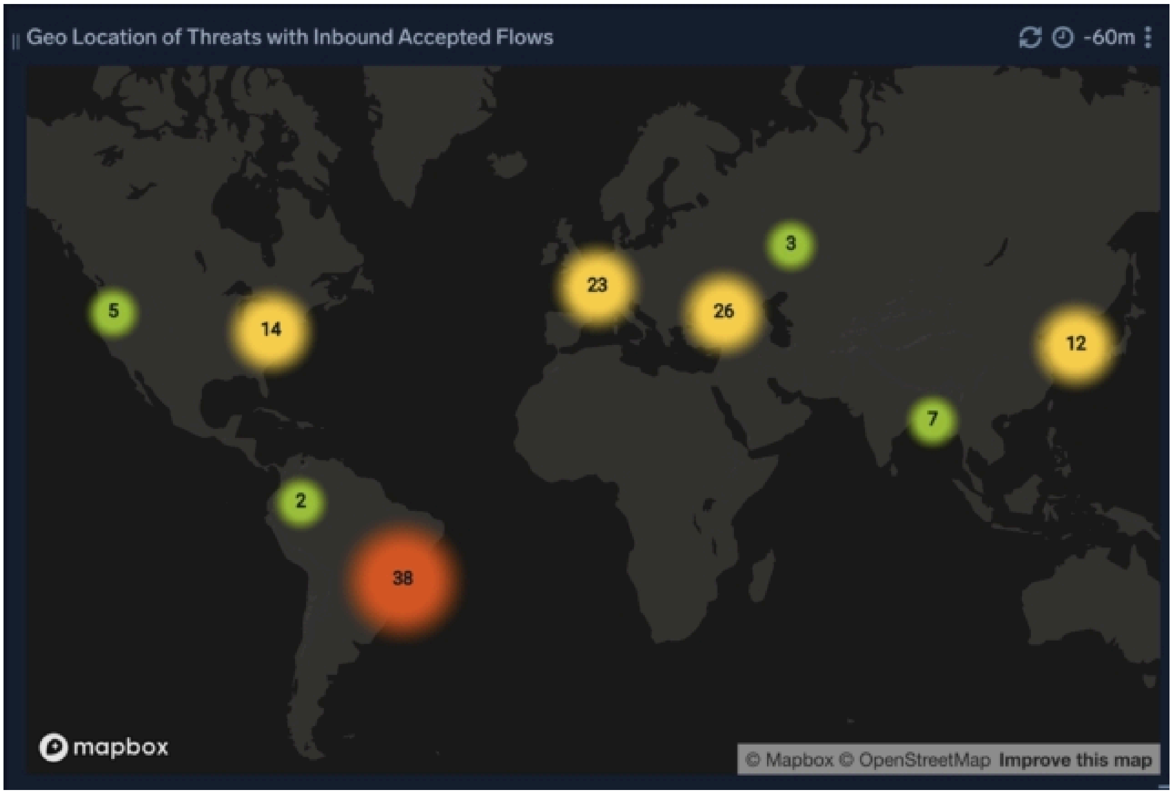
## Inbound Top 10 dstDevice_ip by MB

Displays the top 10 traffic volumes for inbound traffic by destination IP address for the past hour in a bar chart.



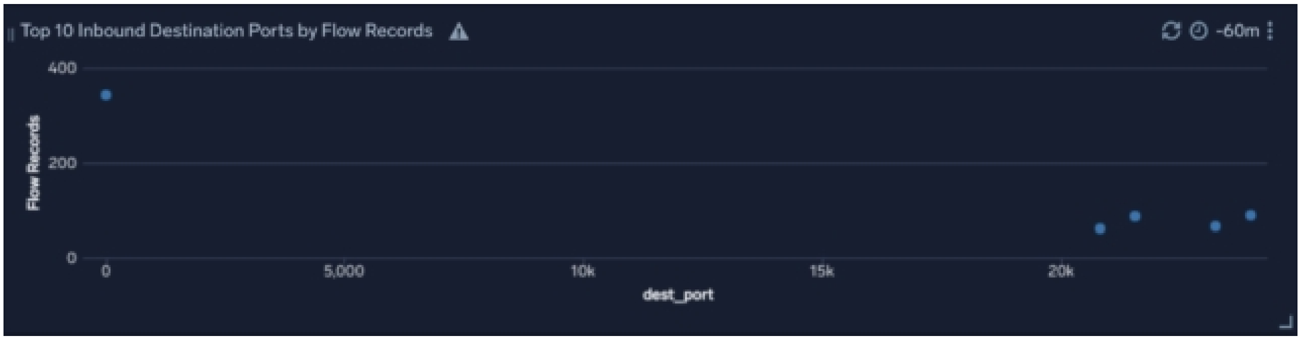
## Geo Location of Threats with Inbound Accepted Flows

Geo-location of allowed inbound communications over the last hour where the source IP matches CrowdStrike threat intelligence


Geo Location of Threats with Inbound Accepted Flows
-60m
3
23
26
5
14
12
7
2
38
mapbox
© Mapbox © OpenStreetMap Improve this map

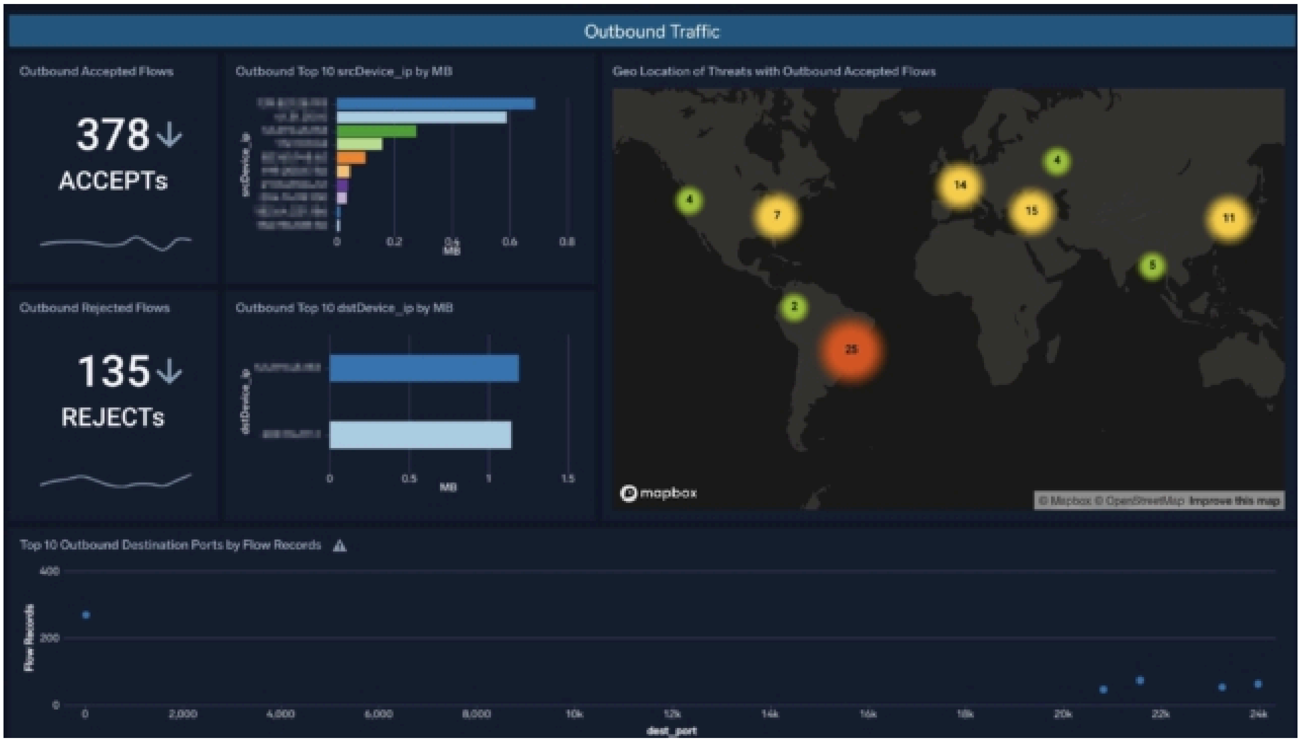
### Top 10 Inbound Destination Ports by Flow Records

Displays a scatter plot of the top 10 inbound communications by destination port for the last hour



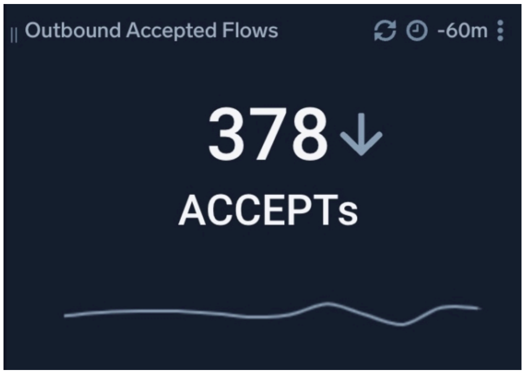
## Outbound Traffic

This is a dashboard for outbound communication between the Internet and AWS.



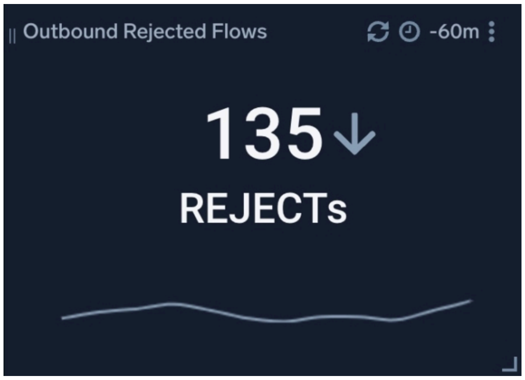
### Outbound Accepted Flows

Displays the number of outbound communications allowed over the last 5 minutes (the graph below shows a sparkline of the number of outbound communications allowed over a 5-minute interval over a 1-hour period)



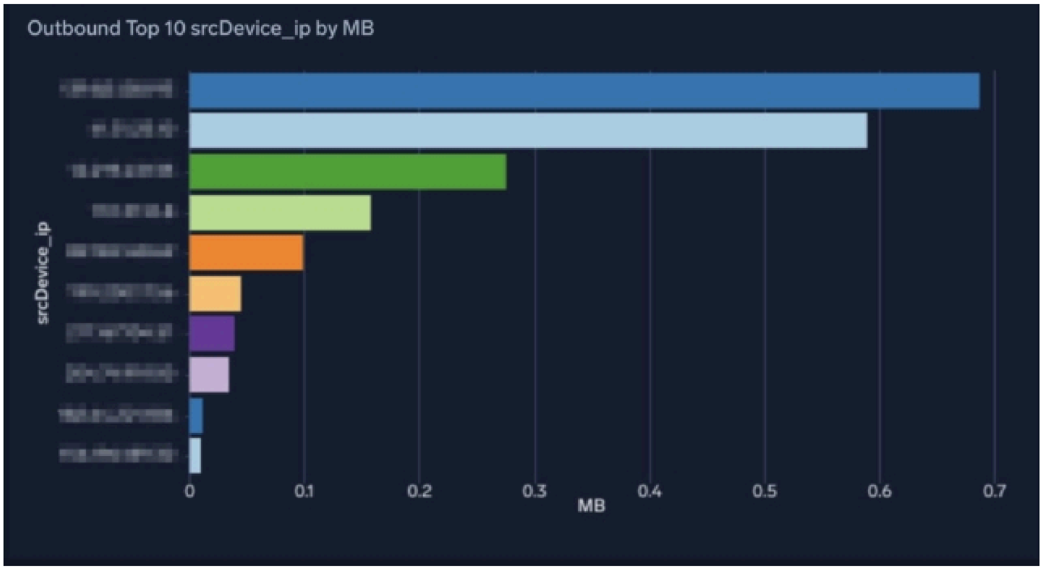
### Outbound Rejected Flows

Shows the number of rejected outbound communications over the last 5 minutes (the graph below shows a sparkline of rejected outbound communications over 5-minute intervals over a 1-hour period)



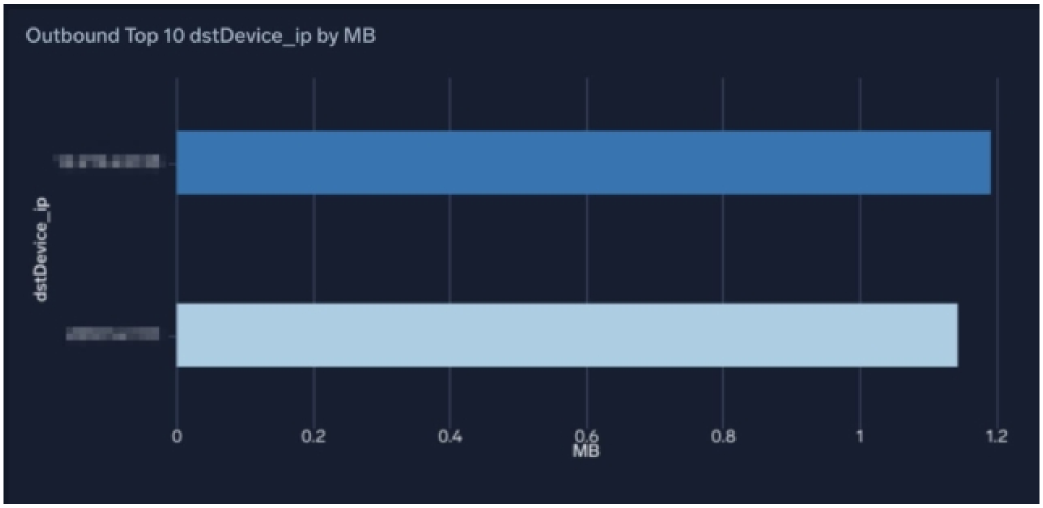
### Outbound Top 10 srcDevice_ip by MB

Displays the top 10 outbound traffic volumes by source IP for the past hour in a bar chart.



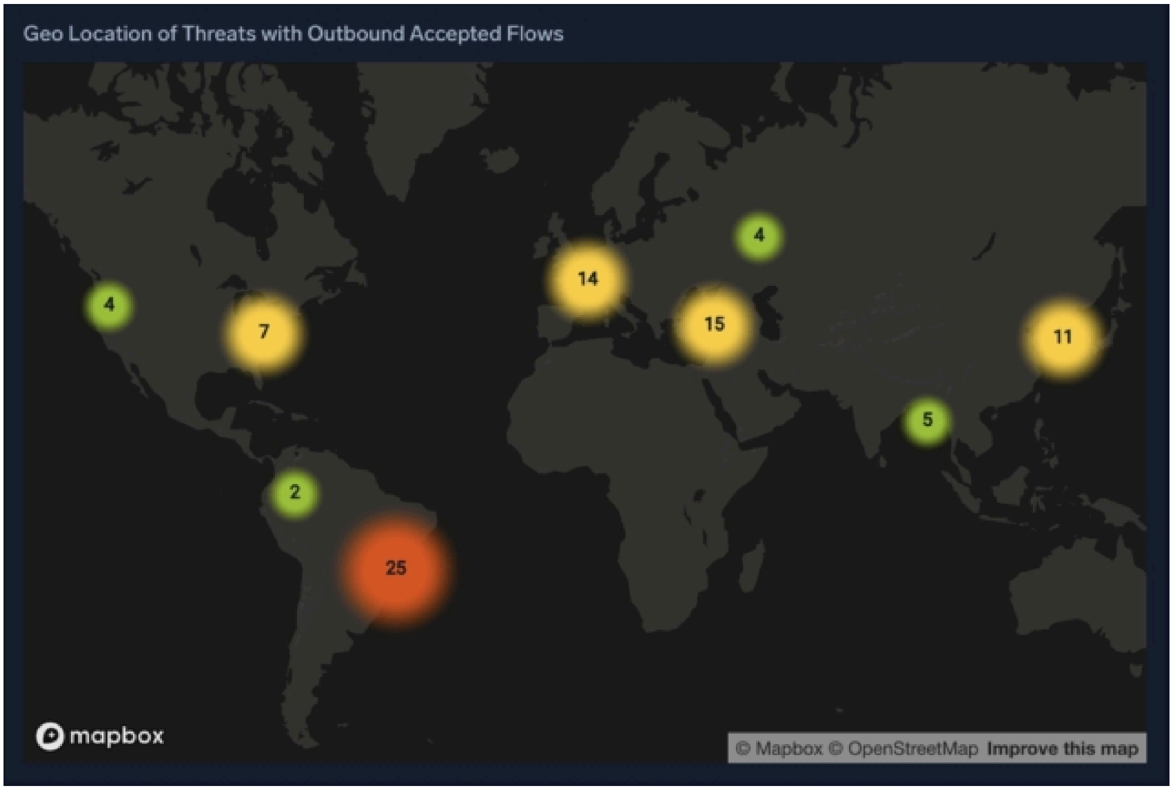
### Outbound Top 10 dstDevice_ip by MB

Displays the top 10 outbound traffic volumes by destination IP address for the past hour in a bar chart.



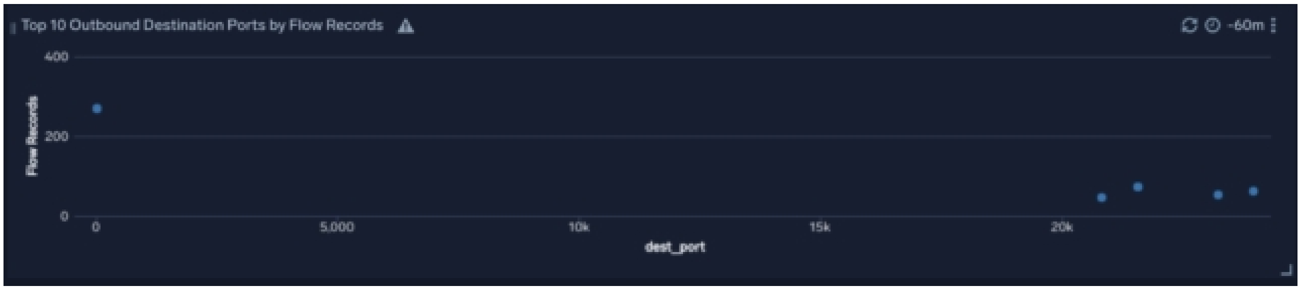
### Geo Location of Threats with Outbound Accepted Flows

Geo-location of allowed outbound communications with source IPs matching CrowdStrike threat intelligence within the last hour


Geo Location of Threats with Outbound Accepted Flows
4
4
14
7
15
11
5
2
25
mapbox
© Mapbox © OpenStreetMap Improve this map

### Top 10 Outbound Destination Ports by Flow Records

Displays a scatter plot of the top 10 outbound communications by destination port for the last hour



## summary

This time, we introduced the dashboard provided by the "Amazon VPC Flow - Cloud Security Monitoring and Analytics" App, part of the security-focused Cloud Security Monitoring and Analytics series. Checking this together with GuardDuty detection information will likely help expedite investigations into indicators of attack and root causes. We hope you will use this article as a reference and take advantage of security insights using Sumo Logic.