Lab: Data Visualization (Sumo Logic)
Introduction

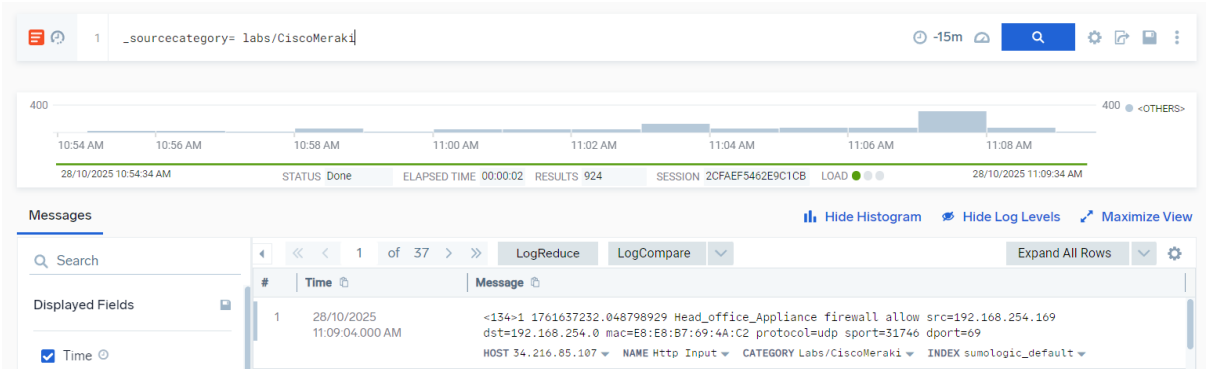
In this lab, I explored the concept of **Data Visualization** in Sumo Logic and learned how dashboards can be used as a powerful forensic and monitoring tool. Dashboards allow analysts to view critical log and metric data together in a single, unified interface. By visualizing trends, patterns, and anomalies, dashboards make it easier to quickly interpret system activity, identify security issues, and support faster decision-making.

This lab also introduced the dashboard template capabilities that simplify data scoping and make chart creation more intuitive. Through hands-on tasks, I learned how to create dashboards, add different types of panels, and modify panel content to suit specific monitoring requirements.

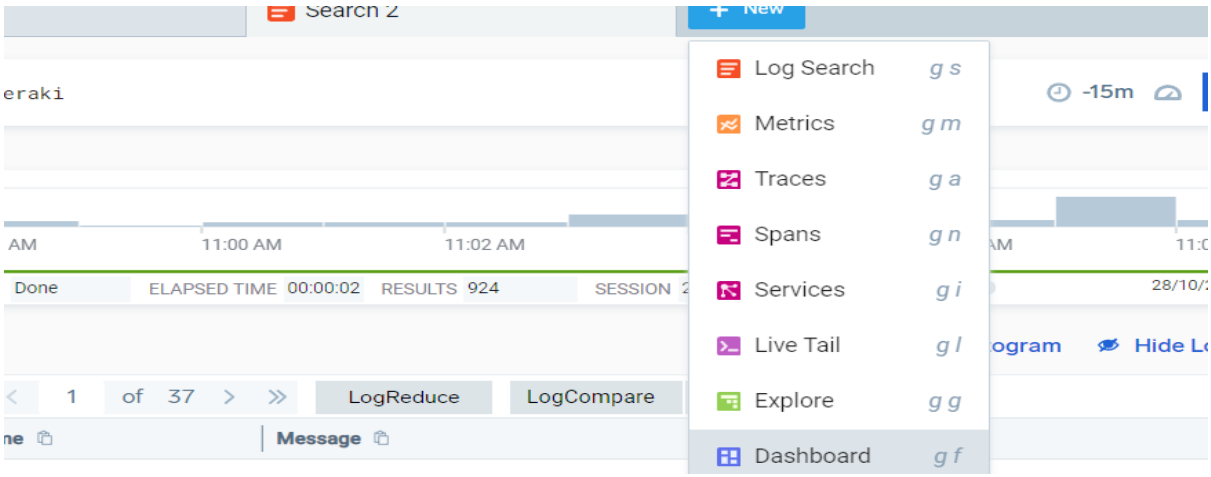
What I Did in This Lab

In this lab, I had created a new dashboard in Sumo Logic and added different panels to it. I had customized each panel by editing the search queries and selecting the appropriate visualization. I had also adjusted the dashboard layout and updated the panel settings. By the end of the lab, I had built a complete dashboard that clearly displayed important log and metric data.

First, I had clicked on **New** and then selected **Log Search**. After that, I had chosen the **source category** and selected **Cisco Meraki logs** to begin building my panel.



When I had clicked on **New**, a dropdown menu had appeared, and from the bottom of that list, I had selected **Dashboard**.



When the new window opened, I entered the following query:

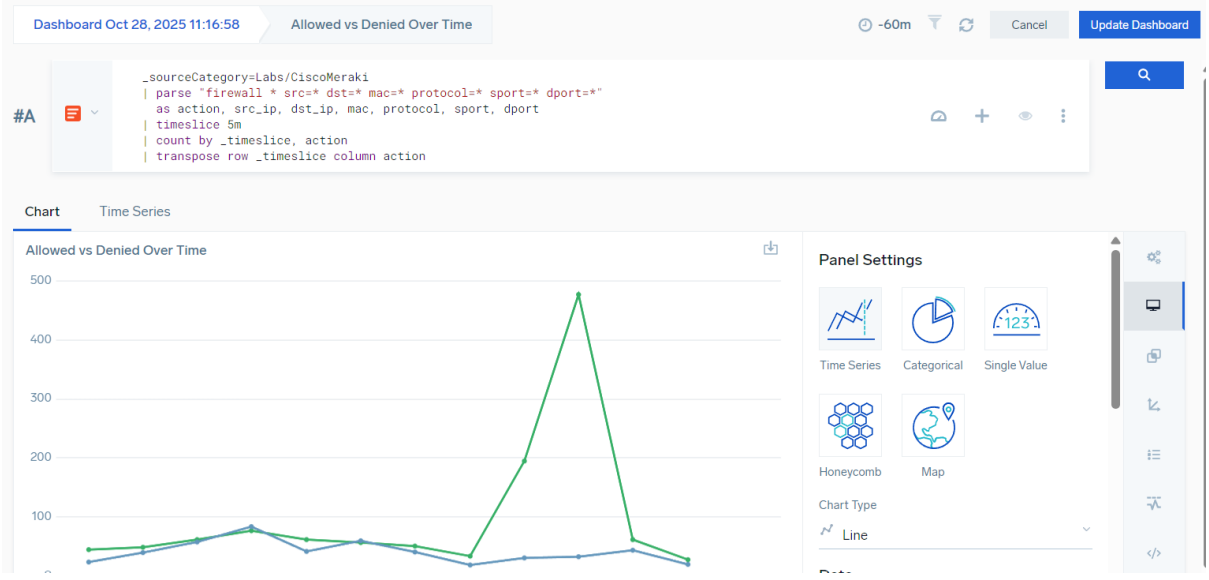
```
_sourceCategory=Labs/CiscoMeraki
| parse "firewall * src=* dst=* mac=* protocol=* sport=* dport=*"
  as action, src_ip, dst_ip, mac, protocol, sport, dport
| timeslice 5m
| count by _timeslice, action
| transpose row _timeslice column action
```

I used this query to show the traffic trend for **“allow”** versus **“deny”** actions.
It helped me see how many requests were allowed or denied within each selected time frame.

- First, the query filtered only the Cisco Meraki logs.
- Then it parsed the log line to extract important fields such as action, source IP, destination IP, ports, and protocol.
- Next, I grouped the data into 5-minute time slices.
- After that, I counted how many allow and deny events occurred in each time slice.
- Finally, I transposed the results so I could clearly compare “allow” vs “deny” traffic on a time-series graph in the dashboard.

After creating the dashboard, I clicked **Add to Dashboard** in the upper-right corner to save the panel. Later, when I selected the same dashboard and made changes, the button changed to **Update Dashboard**, allowing me to save the new edits.

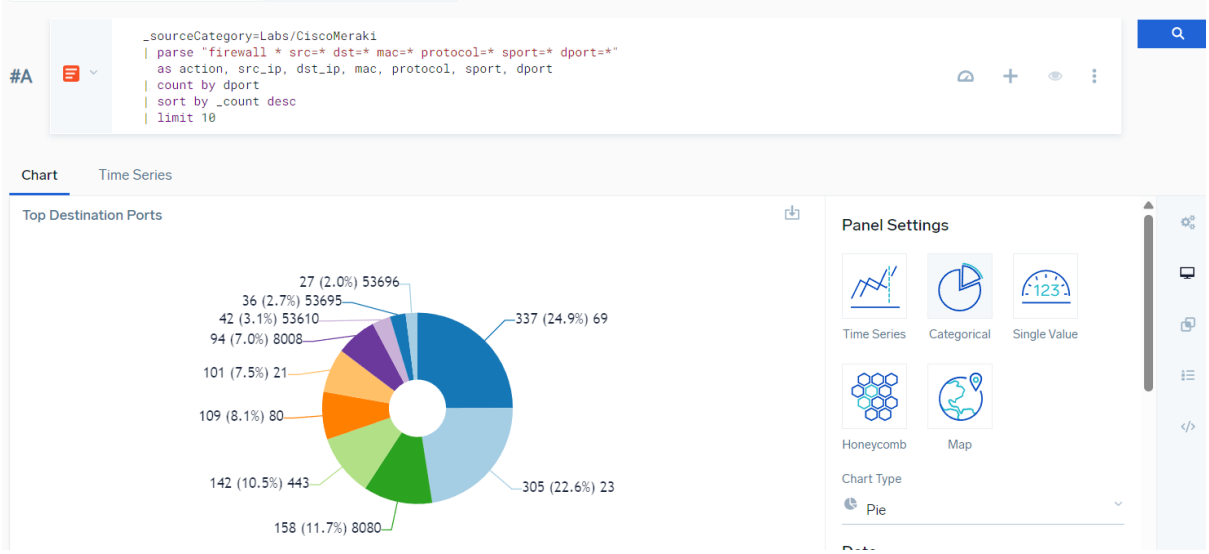
All the dashboards I created appeared in the **Personal Library**, where I could easily access and manage them.



Next, I used the same method by clicking **New → Dashboard**, and in the new panel I entered the following query to create a visualization for destination ports:

```
_sourceCategory=Labs/CiscoMeraki
| parse "firewall * src=* dst=* mac=* protocol=* sport=* dport=*"
  as action, src_ip, dst_ip, mac, protocol, sport, dport
| count by dport
| sort by _count desc
| limit 10
```

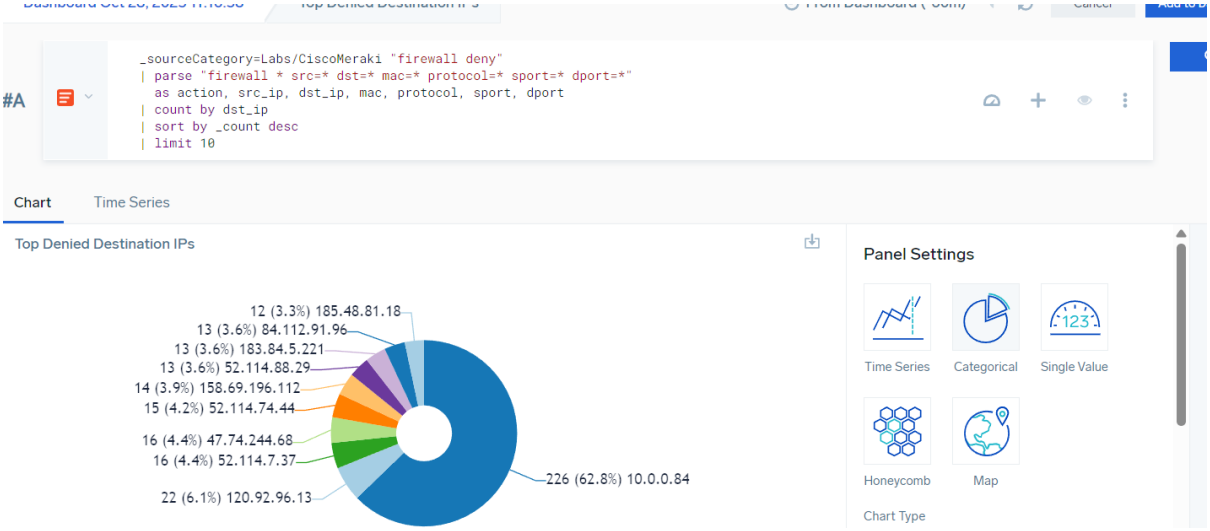
This panel showed me the **top destination ports**, helping me identify which ports were most frequently targeted or used. It was useful for spotting potential scanning activity or abused services.



Next, I created a panel for **Top Denied Destination IPs** using the **Categorical** panel type. I entered the following query:

```
_sourceCategory=Labs/CiscoMeraki "firewall deny"
| parse "firewall * src=* dst=* mac=* protocol=* sport=* dport=*"
  as action, src_ip, dst_ip, mac, protocol, sport, dport
| count by dst_ip
| sort by _count desc
| limit 10
```

This panel highlighted the **destination IPs that had the most denied traffic in last 60 minutes**, helping me identify potentially malicious hosts or unauthorized access attempts.

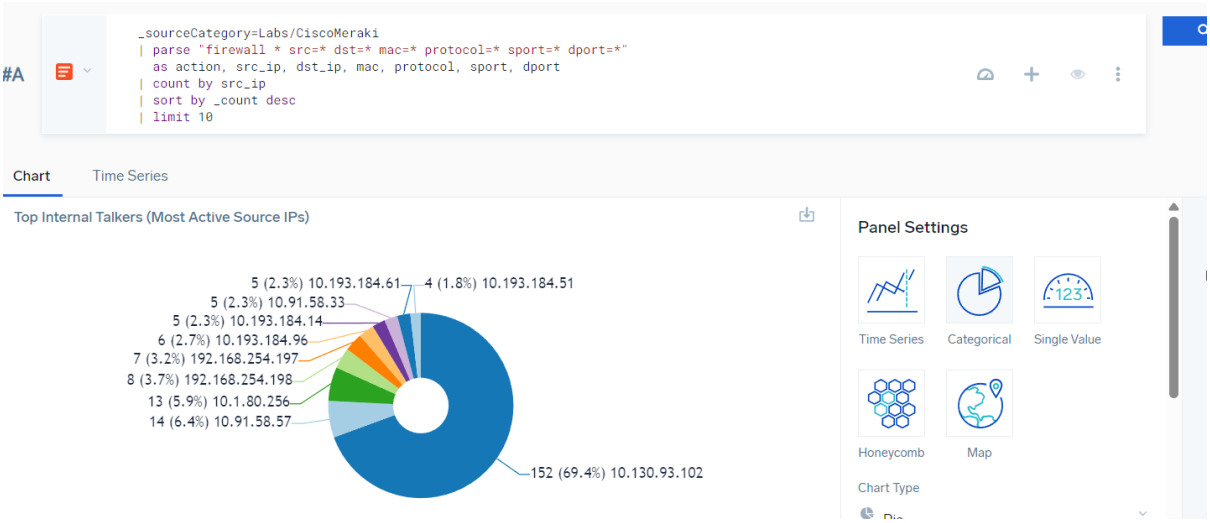


Next, I created a panel for **Top Internal Talkers (Most Active Source IPs)** using the **Categorical** panel type. I entered the following query:

```
_sourceCategory=Labs/CiscoMeraki
| parse "firewall * src=* dst=* mac=* protocol=* sport=* dport=*"
  as action, src_ip, dst_ip, mac, protocol, sport, dport
| count by src_ip
| sort by _count desc
```

```
| limit 10
```

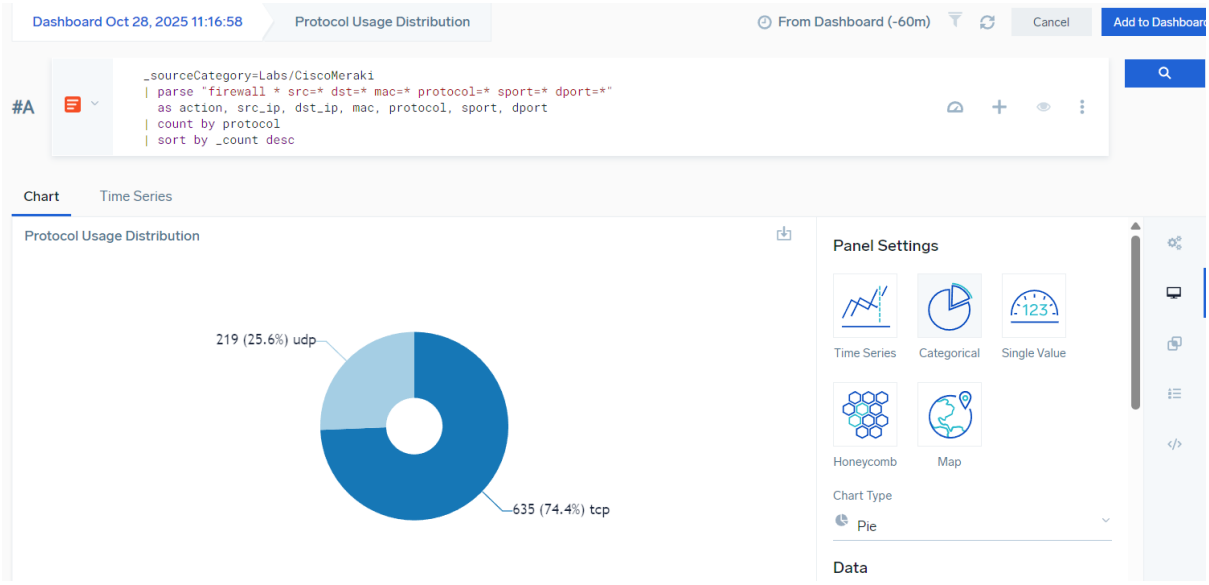
I set the time frame to the **last 60 minutes**. This panel allowed me to identify **internal hosts with the heaviest network activity**, which could indicate compromised systems or unusually high usage.



Next, I created a **Categorical (Pie Chart)** panel to analyze **traffic by protocol**. I entered the following query:

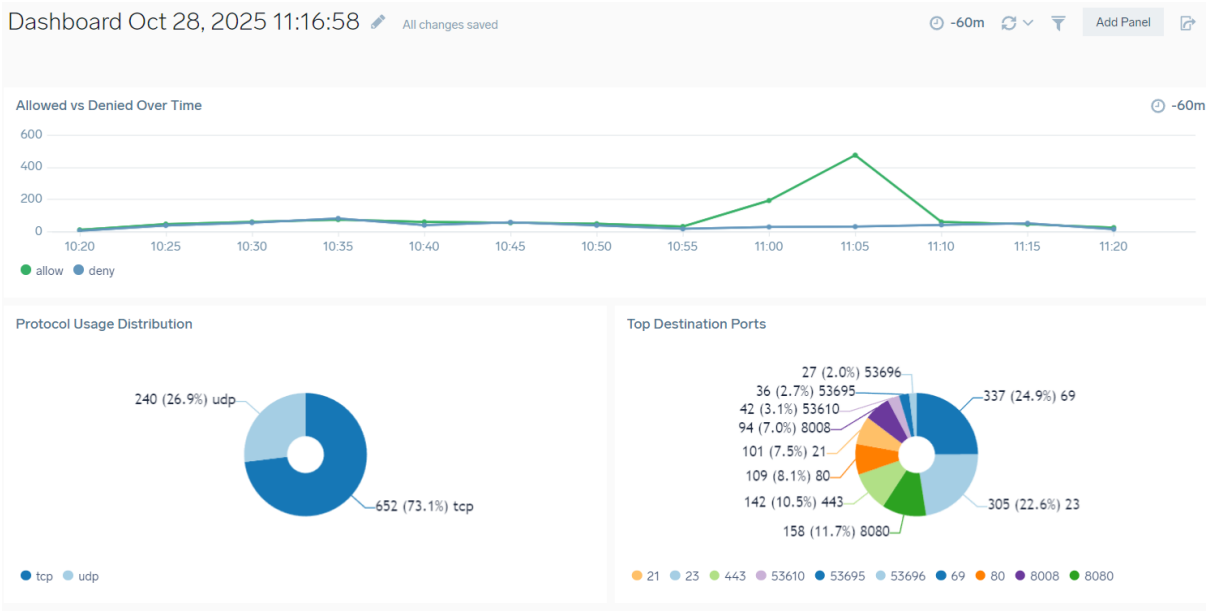
```
_sourceCategory=Labs/CiscoMeraki
| parse "firewall * src=* dst=* mac=* protocol=* sport=* dport=*"
  as action, src_ip, dst_ip, mac, protocol, sport, dport
| count by protocol
| sort by _count desc
```

This panel showed the **breakdown of traffic by protocol** (TCP, UDP, etc.), which was useful for detecting anomalies, such as a sudden spike in UDP traffic.

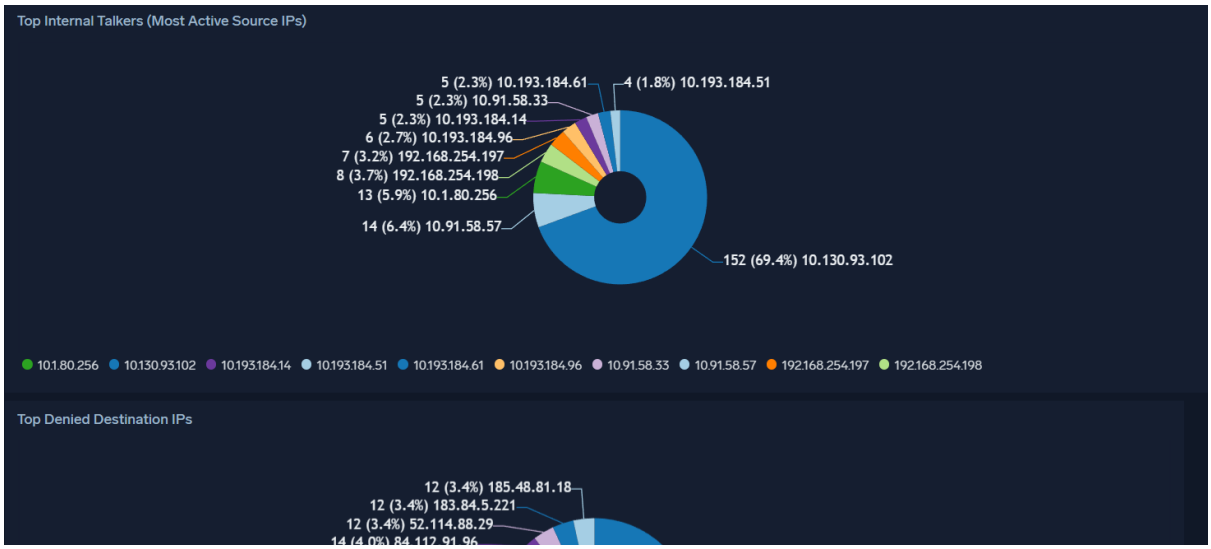


As I progressed, I kept **adding each panel** to the dashboard, so that all the visualizations were available in a single view. This included panels for **traffic trends (allow vs deny)**, **top destination ports**, **top denied destination IPs**, **top internal talkers**, and **protocol breakdown**.

The **final dashboard** provided a comprehensive view of network activity, allowing me to monitor traffic patterns, identify potential threats, and analyze anomalies all in one place.



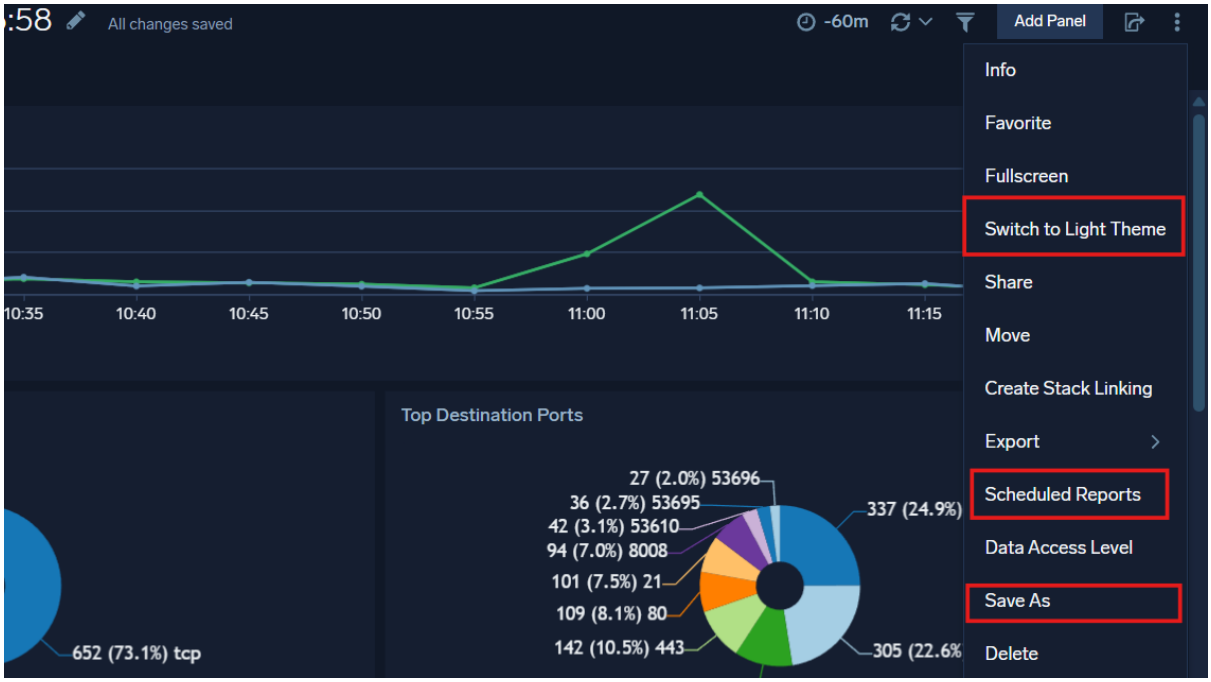
I had also switched the dashboard to **dark mode**, which made the visualizations easier to read and provided a clearer view of all the panels.



When I clicked the **three dots** in the upper-right corner, I could **switch back to white mode**.

I could also **schedule the dashboard reports** to be sent to my email.

Additionally, I could **save the dashboard to my personal library** for easy access later.



Conclusion

In this lab, I had learned how to **create and customize dashboards** in Sumo Logic to visualize network and firewall log data. I had built multiple panels showing traffic trends, top ports, denied destinations, active internal hosts, and protocol breakdowns. This lab was important because it taught me how to **quickly analyze network activity, identify anomalies, and monitor security events** in a visual and intuitive way. By the end, I had gained hands-on experience in using dashboards as a **powerful tool for network monitoring and threat detection**.