**Lab 7 Report: Creating a pfSense Firewall Event Dashboard in Kibana**

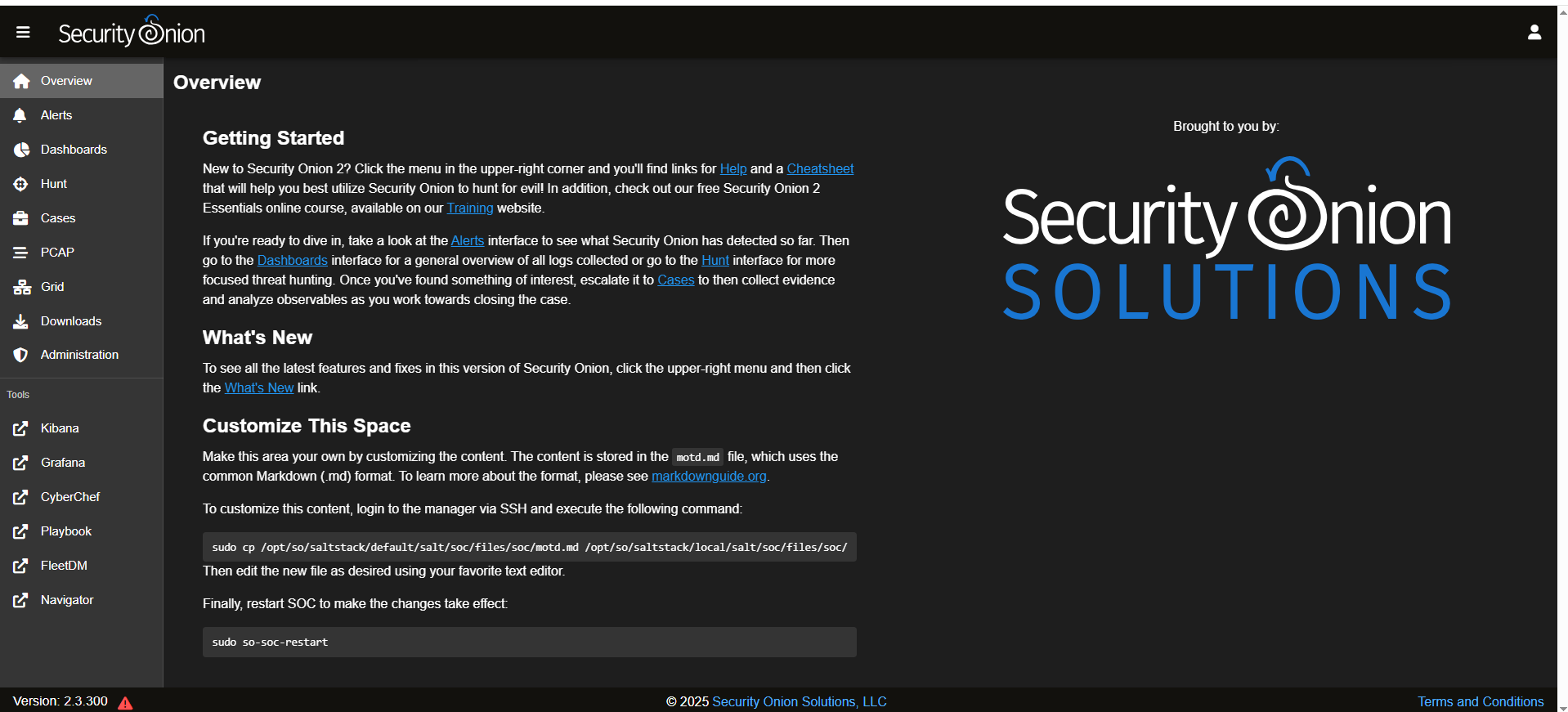
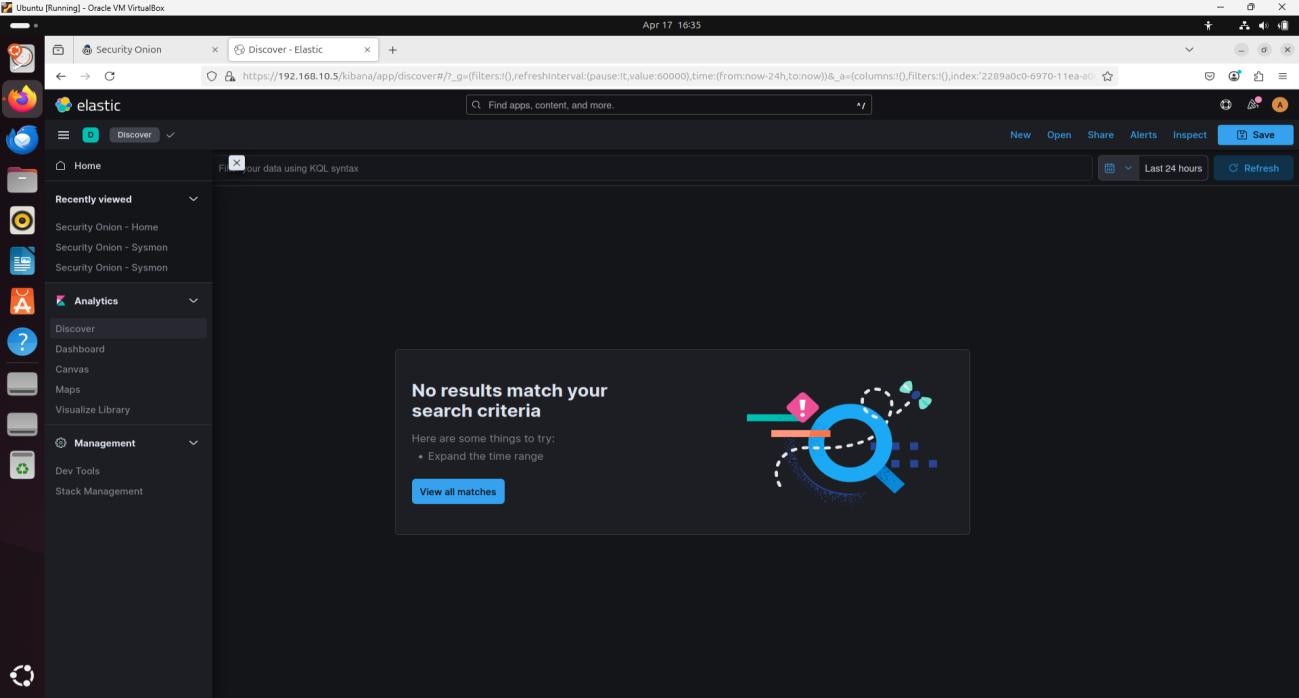
**Lab Title:** Creating a pfSense Firewall Event Dashboard in Kibana

In this lab, I created a custom Kibana dashboard to visualize pfSense firewall logs in Security Onion. The lab focused on filtering event data, creating visualizations, and arranging widgets to provide an interactive, informative dashboard.

#### 1. ****Accessed Kibana****

Logged in to Security Onion.

Opened Kibana from the left-side panel.



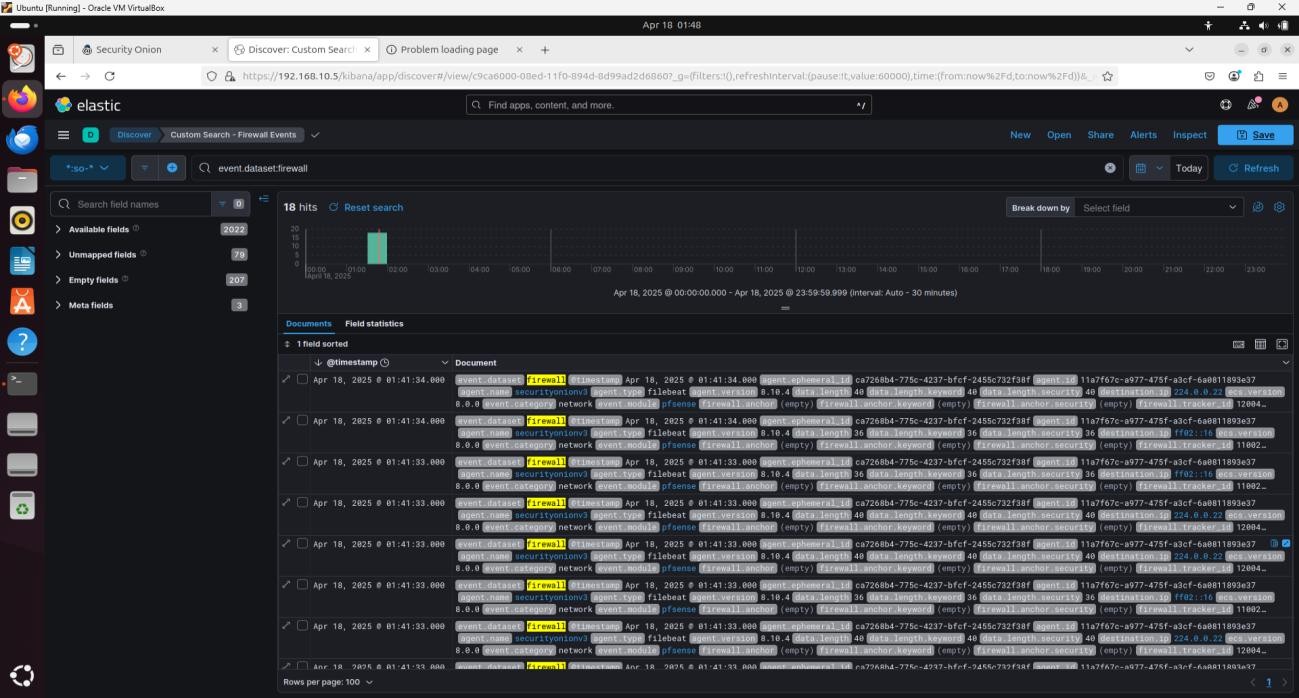
2. **Created a Custom Search Filter**

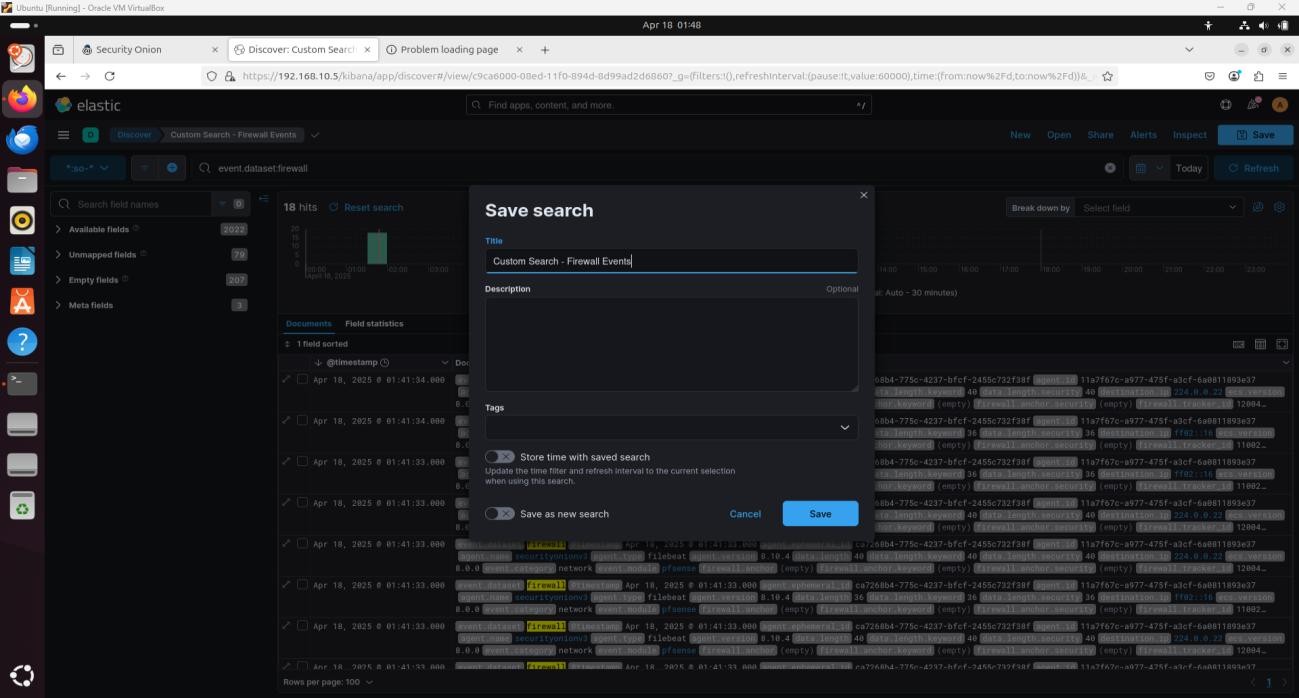
Navigated to the **Discover** page using the three-line menu icon in Kibana.

Entered the following search string:

event.dataset:firewall

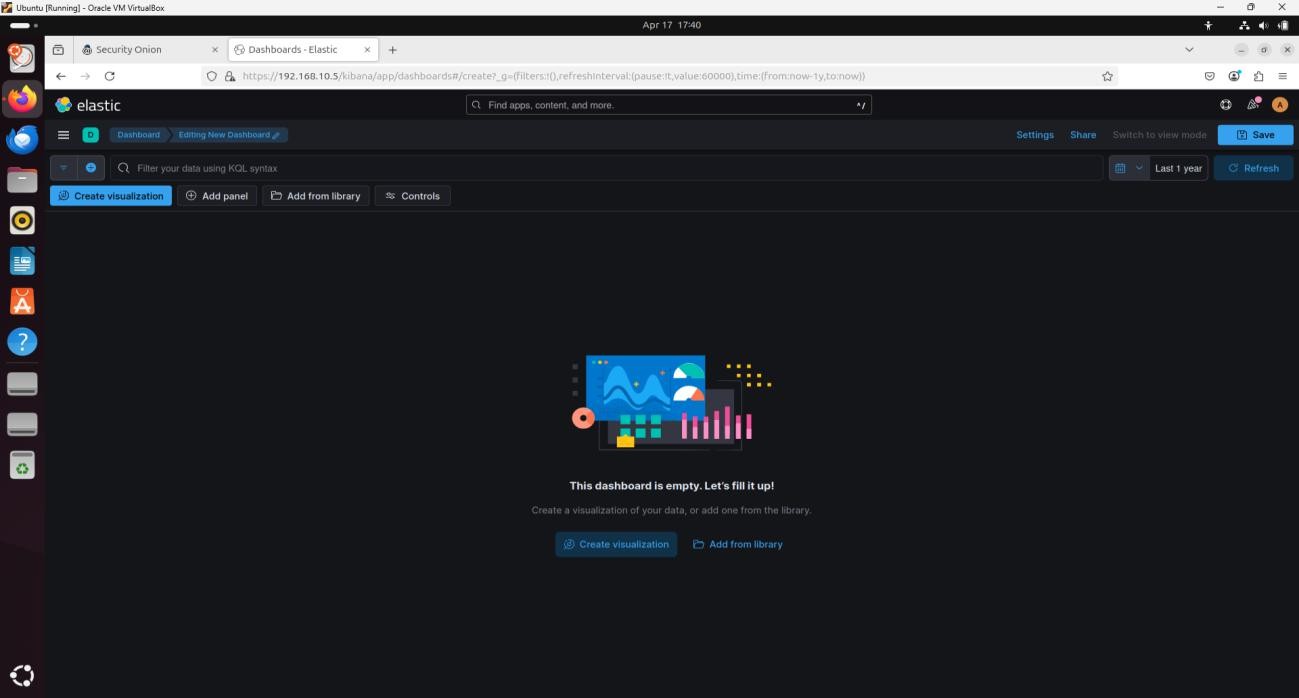
Clicked **Save** in the top-right corner and named it: **Custom Search – Firewall Events**



****

3. **Created a New Dashboard**

Clicked **Create dashboard** to open a blank dashboard.



4. **Added Visualization Panels**

##### a) ****Pie Chart****

Clicked **Create panel**

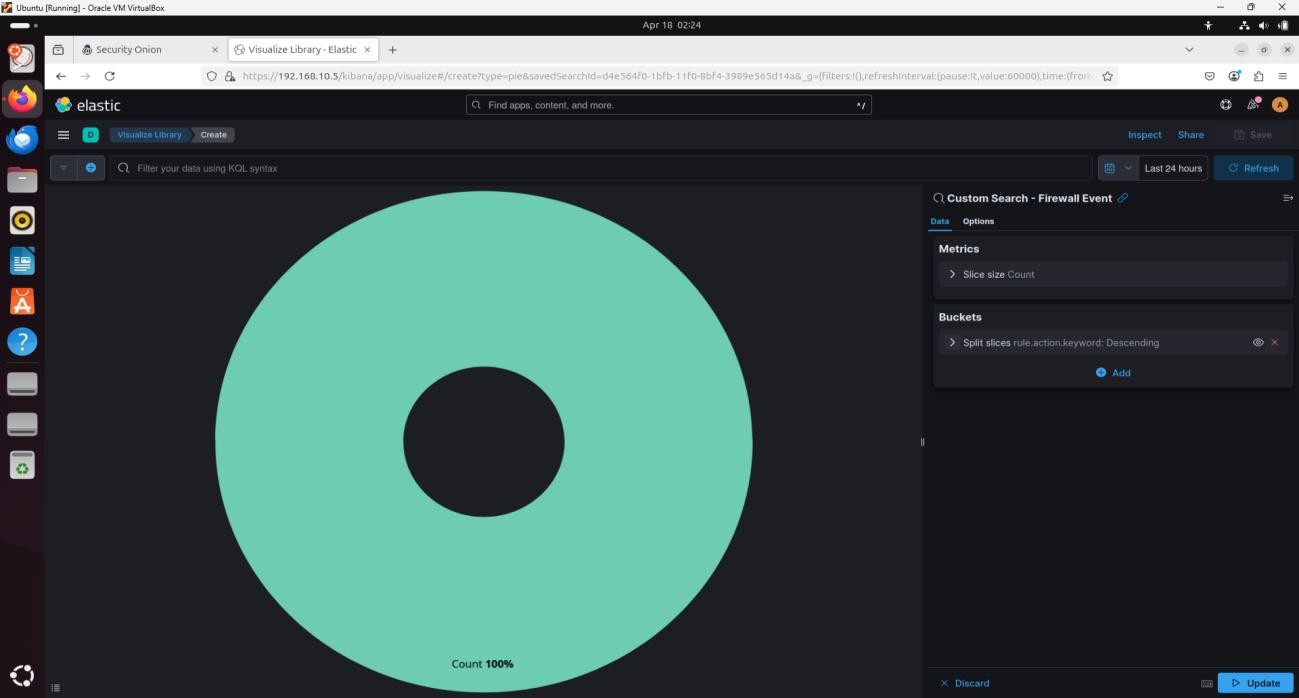
Selected **Pie chart**

Chose data source: **Custom Search – Firewall Events**

Set Field = rule.action.keyword, Size = 50

Styled as Pie (not Donut)

Saved as: **Firewall – Rule Action Summary**



##### 

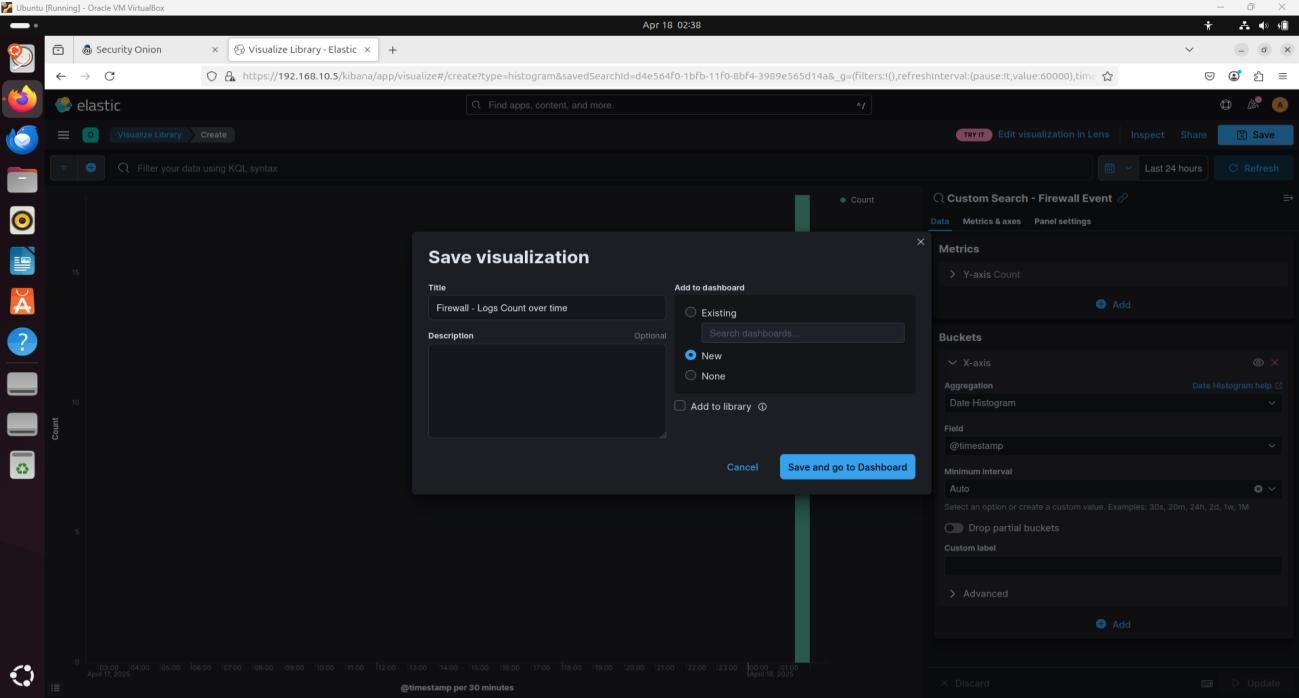
##### b) ****Vertical Bar Chart****

Type: Vertical bar

Data source: **Custom Search – Firewall Events**

Bucket: Data histogram with @timestamp

Saved as: **Firewall – Logs Count over time**

****

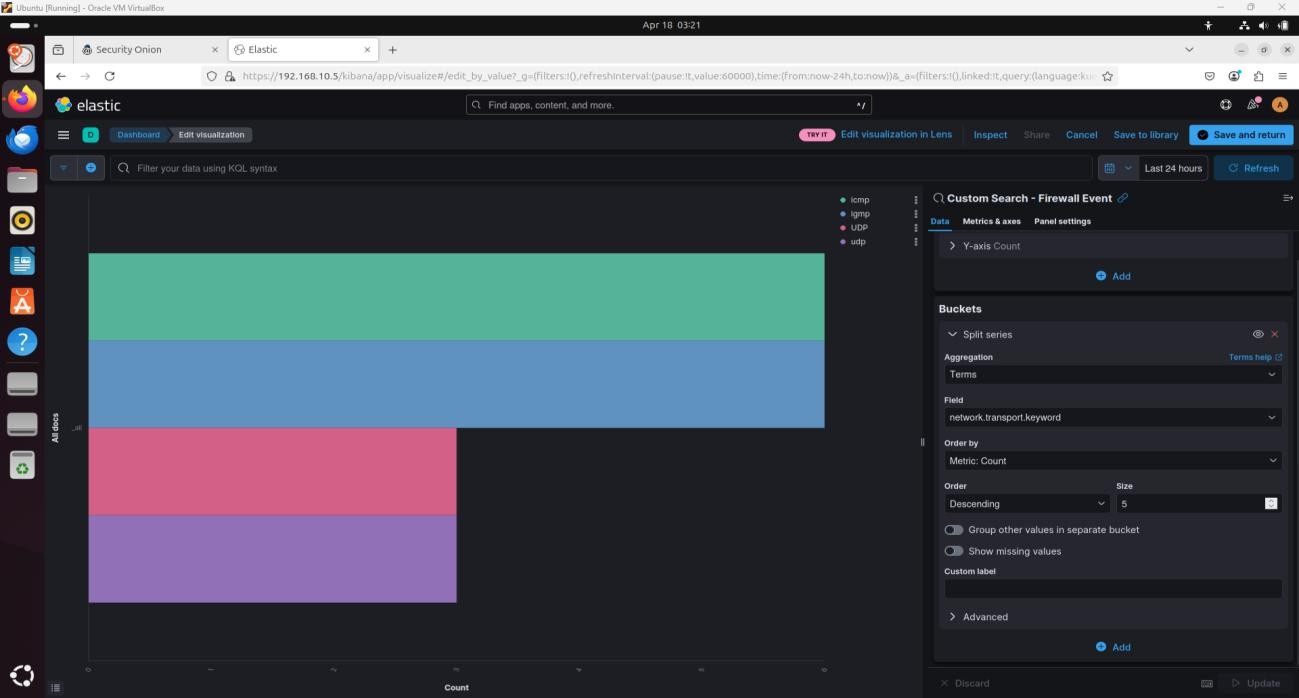
##### c) ****Horizontal Bar Chart****

Data source: **Custom Search – Firewall Events**

Bucket: Split series

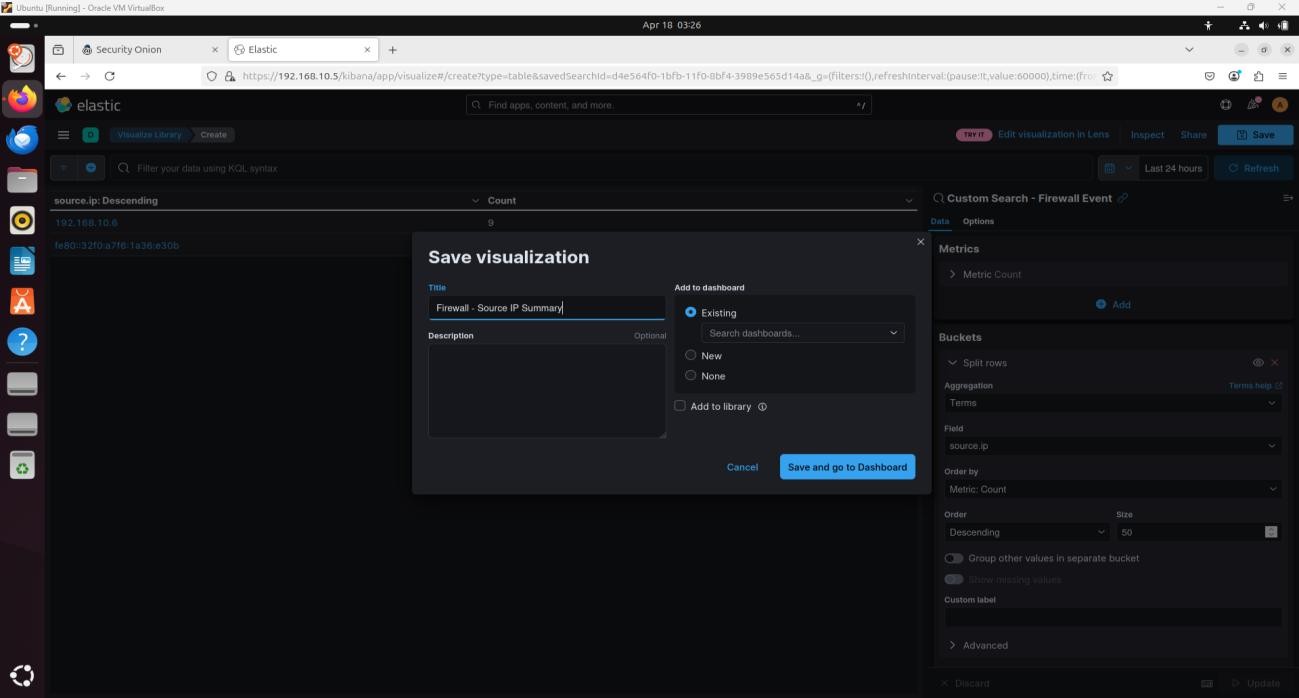
Aggregation: Terms

Field: network.transport.keyword

Saved as: **Firewall – Network Protocol Summary**

##### d) ****Data Table: Source IP Summary****

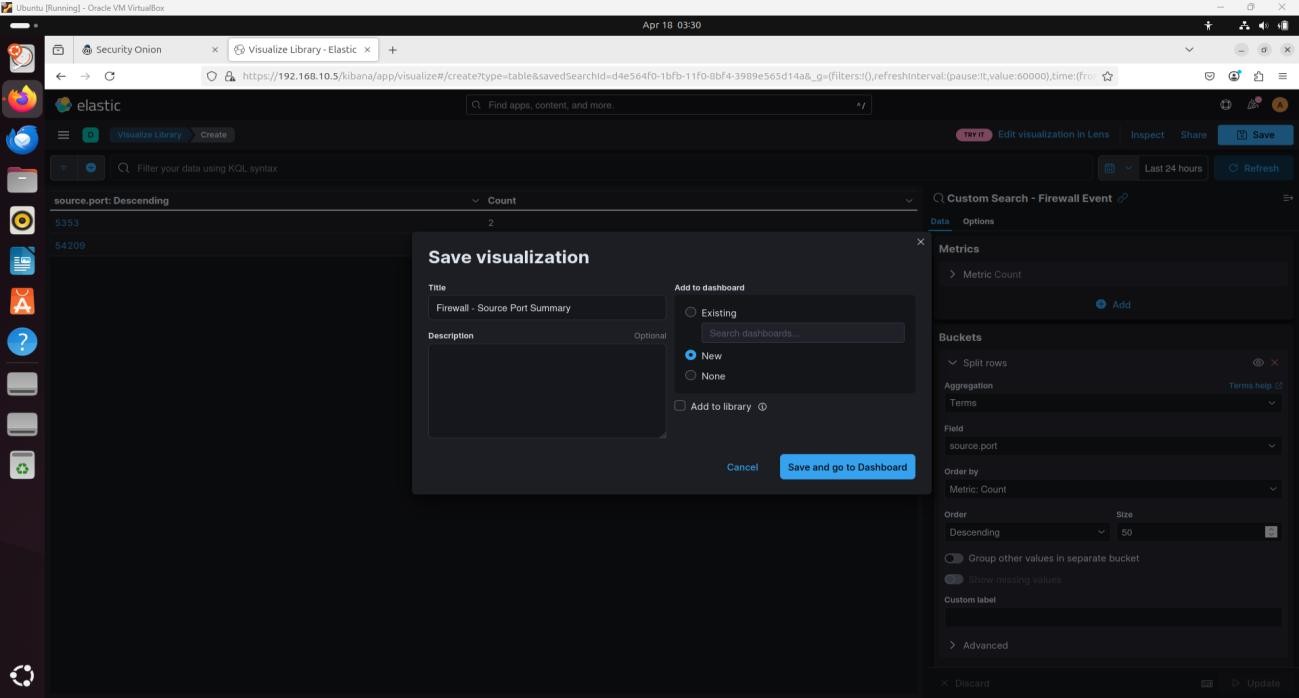
Split rows by source.ip, Size = 50

Saved as: **Firewall – Source IP Summary**

##### e) ****Data Table: Source Port Summary****

Split rows by source.port, Size = 50

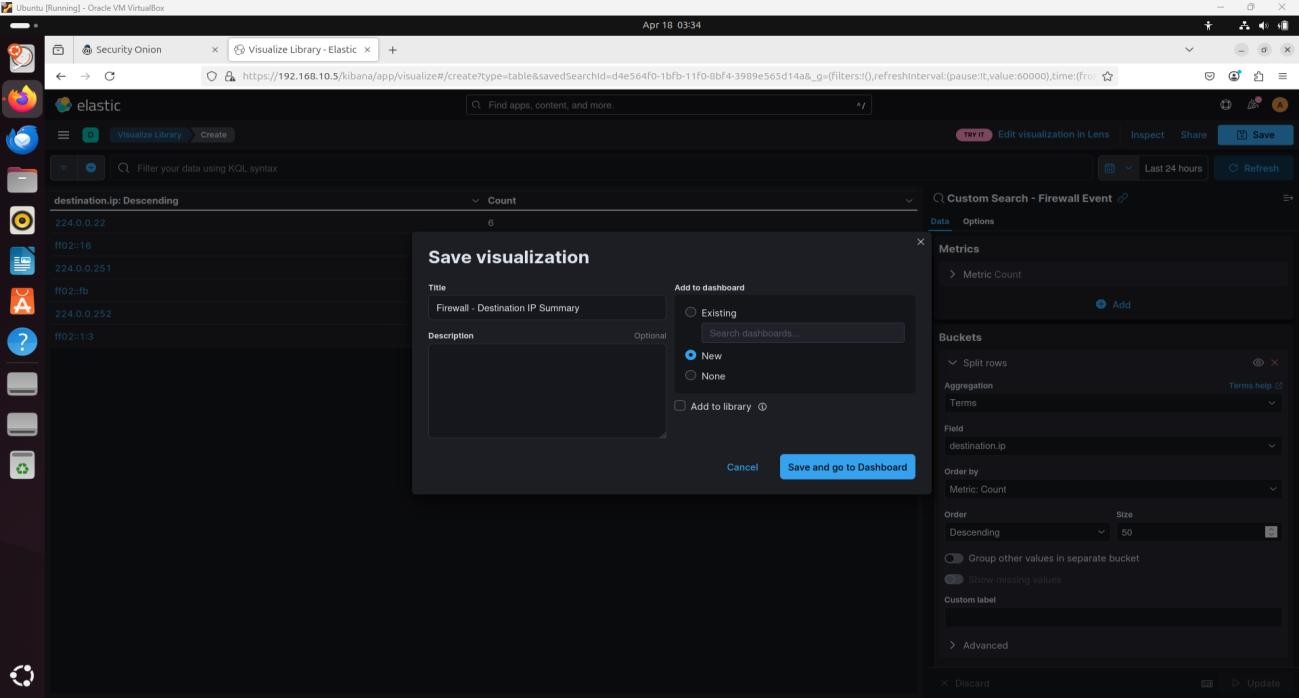
Saved as: **Firewall – Source Port Summary**

****

##### f) ****Data Table: Destination IP Summary****

Split rows by destination.ip, Size = 50

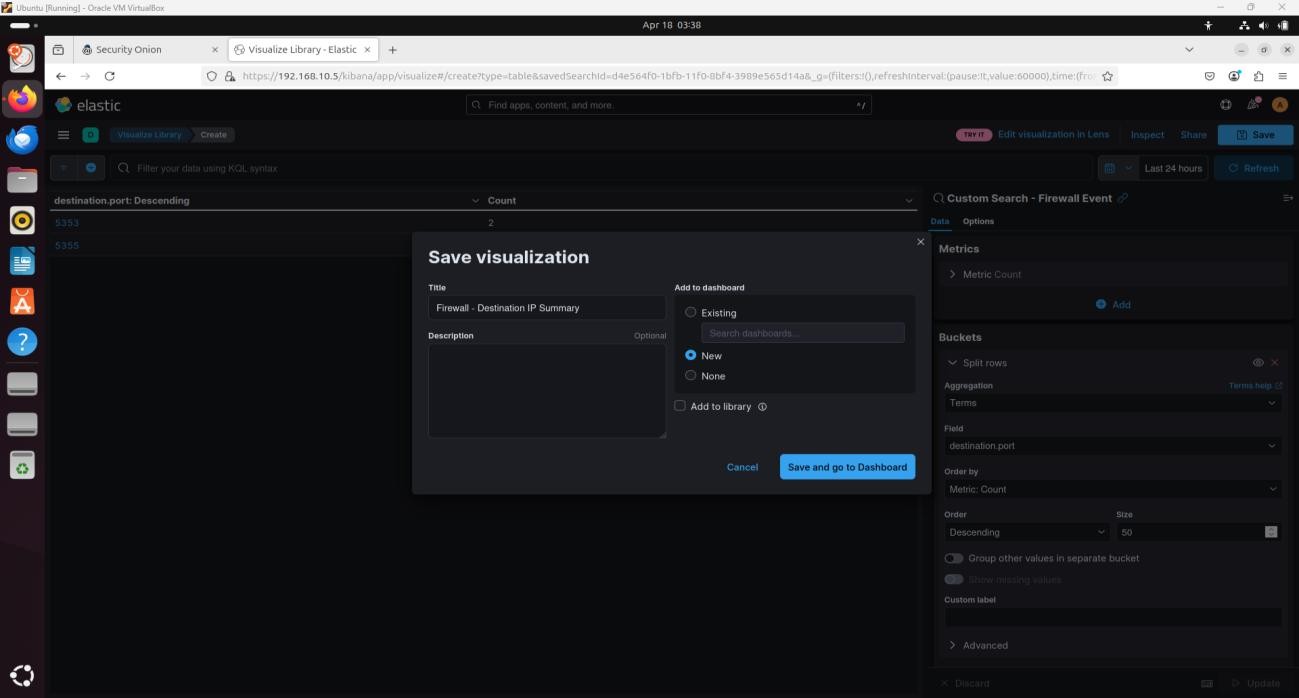
Saved as: **Firewall – Destination IP Summary**



##### g) ****Data Table: Destination Port Summary****

Split rows by destination.port, Size = 50

Saved as: **Firewall – Destination Port Summary**

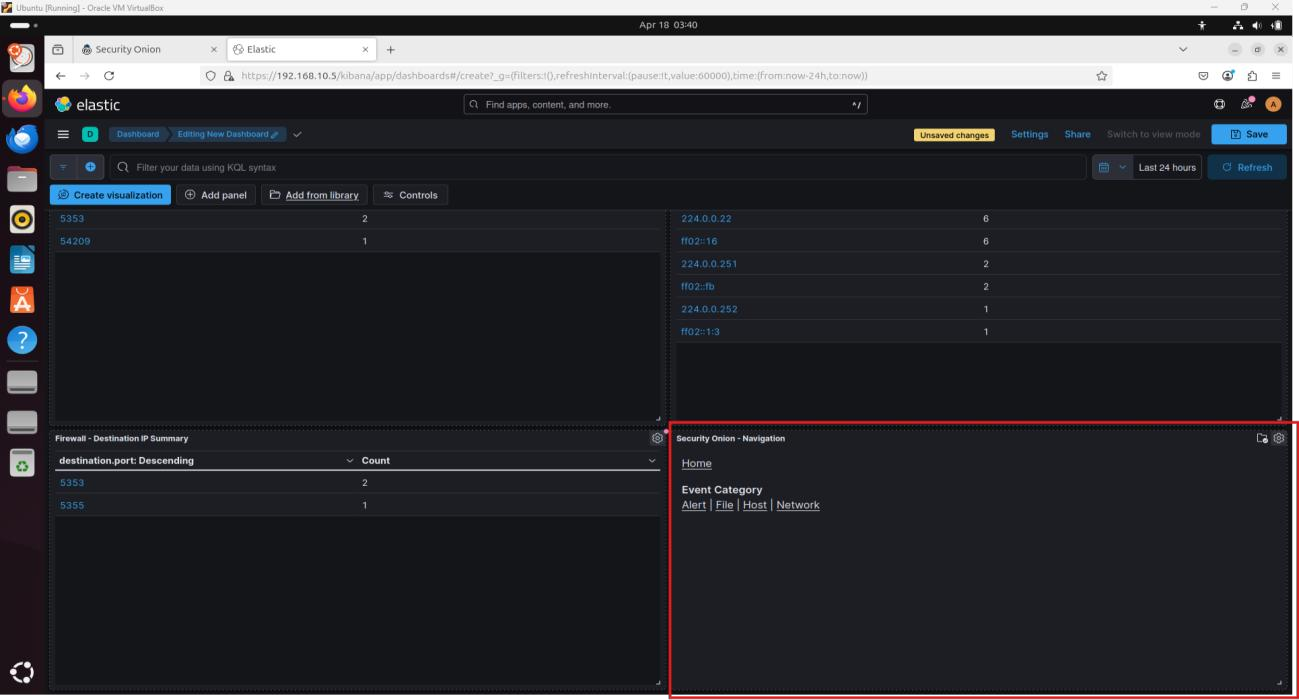


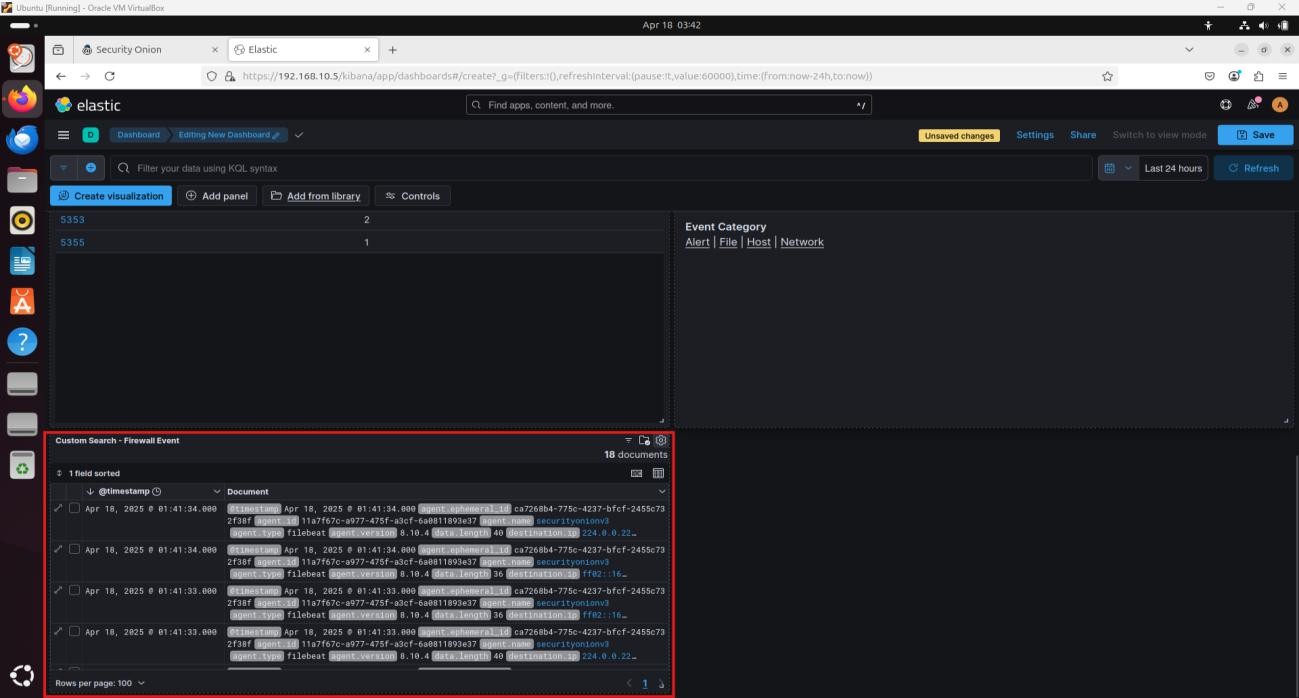
5. **Added Panels from Library**

Clicked **Add from library**

Added: **Security Onion Navigation panel**

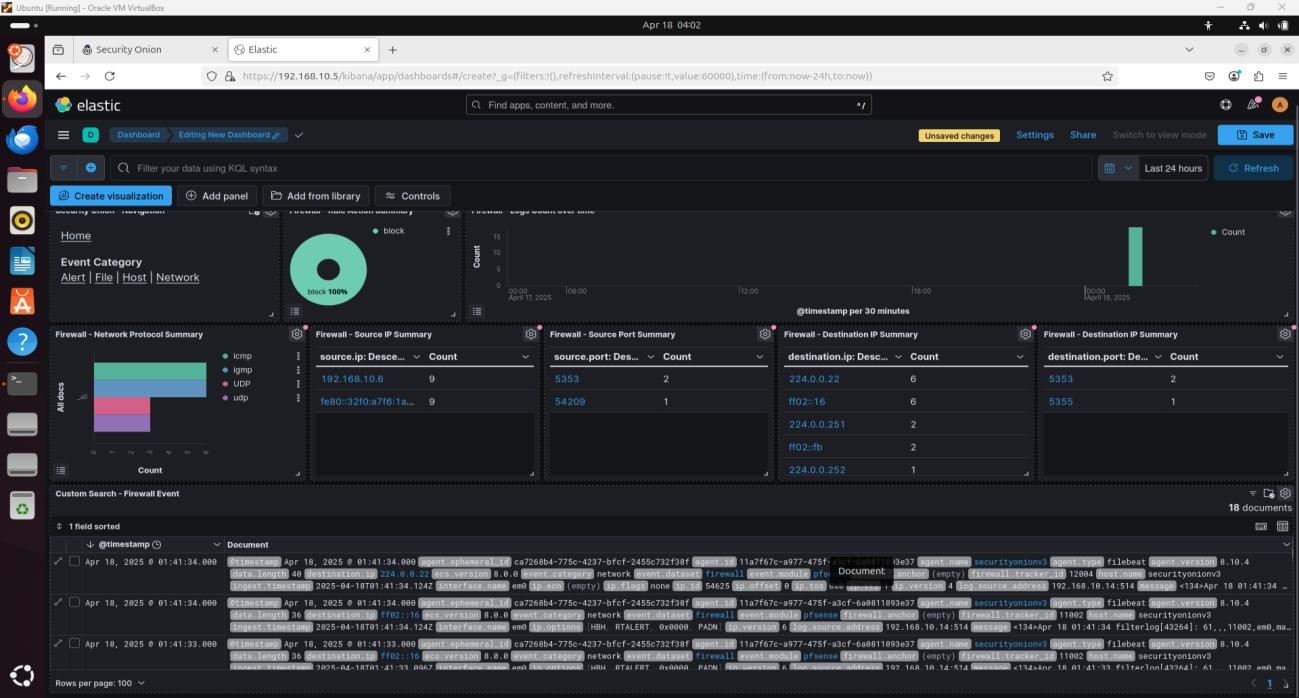
Added: **Custom Search – Firewall Events panel** (for raw event logs)





6. **Final Dashboard Edits and Save**

Resized, shuffled, and organized all widgets for readability.

Clicked **Save**, and named it: **Custom Dashboards – Firewall**

**Conclusion**

This lab guided me through setting up a detailed Kibana dashboard for pfSense firewall events. I created custom visualizations to summarize firewall rule actions, protocol use, IP sources/destinations, and ports. I also integrated existing panels for easy navigation and raw log review. This dashboard will help in quick filtering, analysis, and correlation of firewall events within the ELK stack environment.