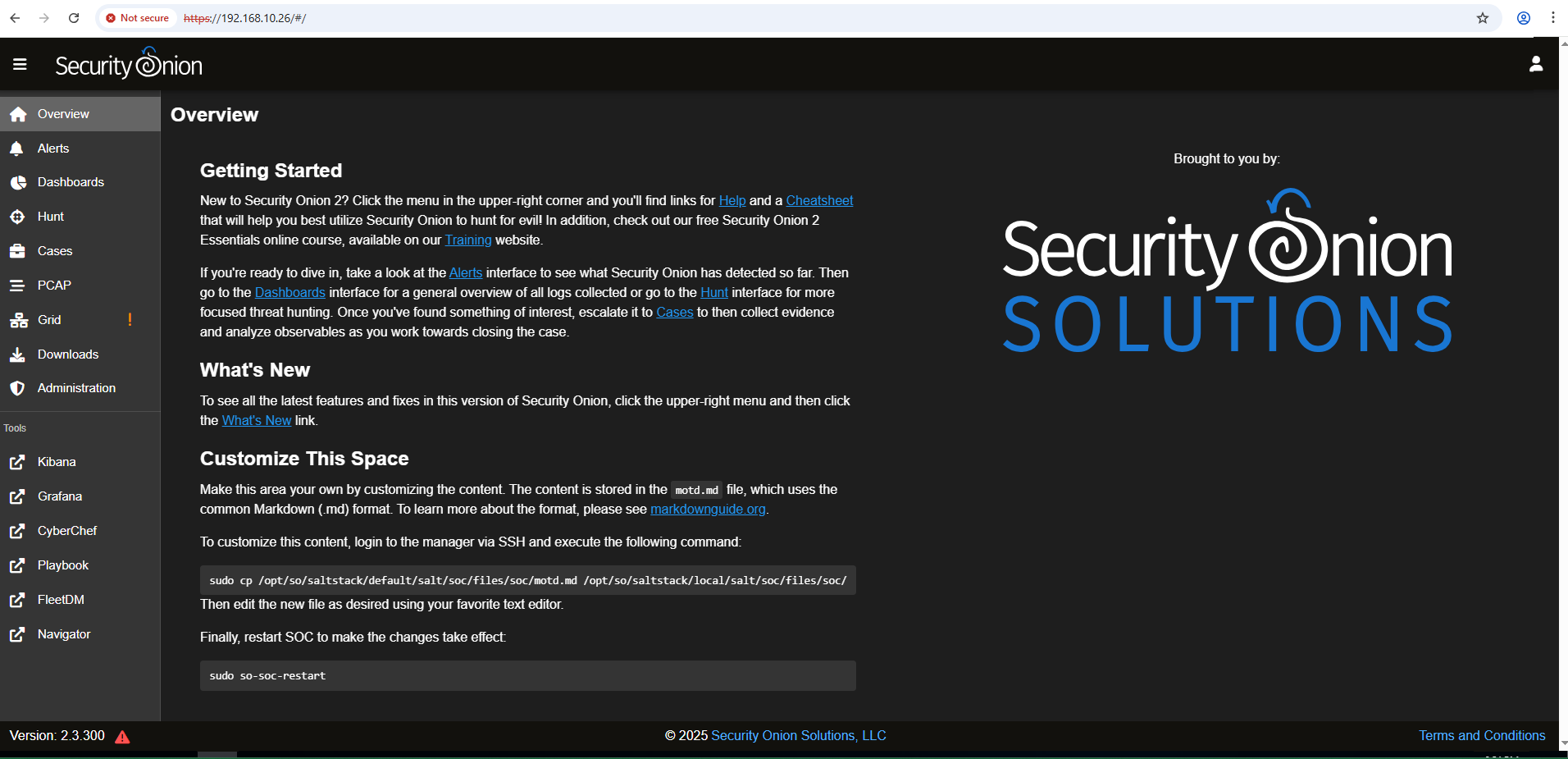
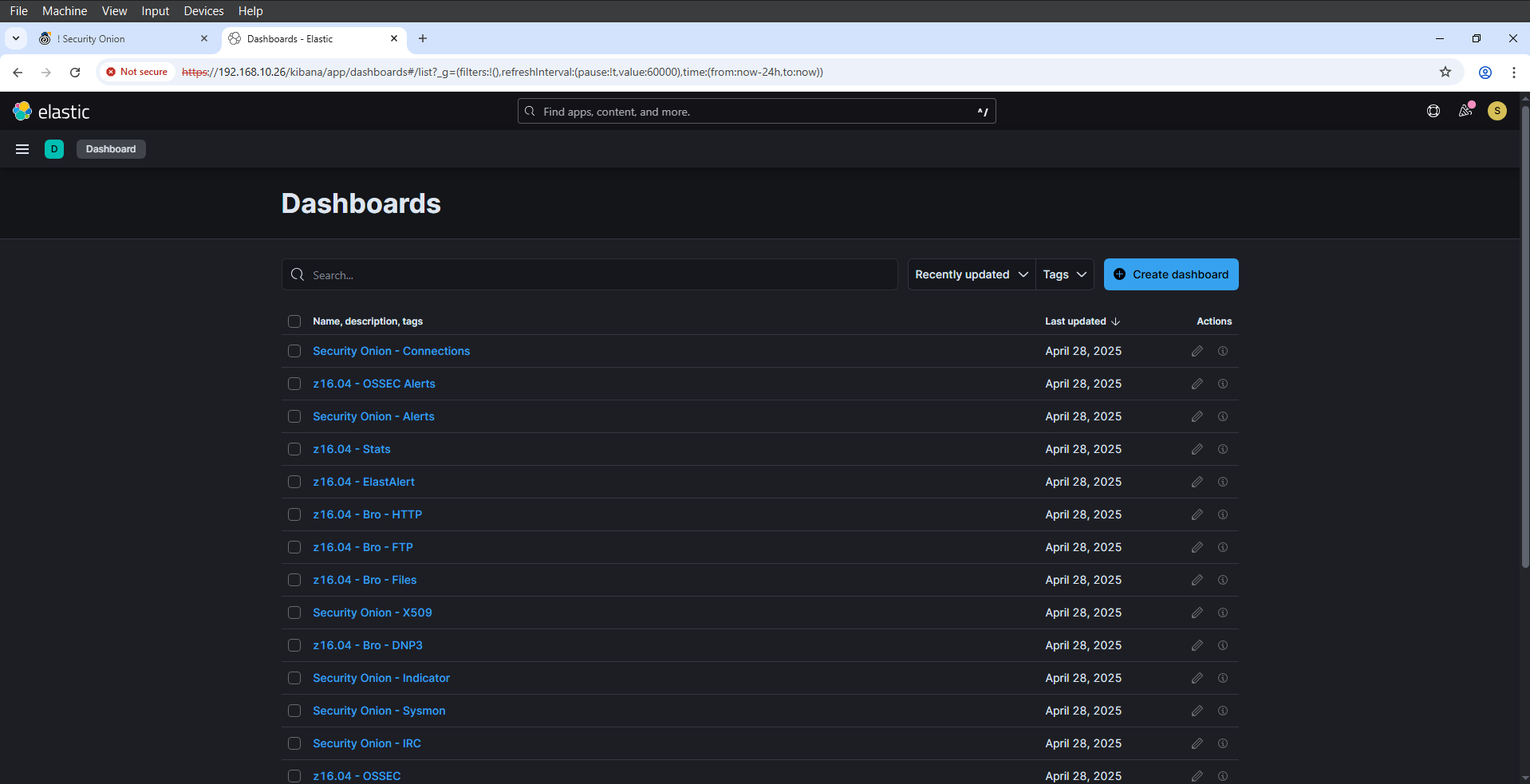
**Creating a Breach Detection Dashboard in Kibana**

During this lab, I created a breach detection dashboard using Kibana in Security Onion. The goal was to visualize and analyze the large volume of logs collected from various systems and devices. Even in a simple lab setup, we were pulling in close to one million events per day. My objective was to extract meaningful insights from this data to detect potential security incidents. I logged in to the Kibana portal through Security Onion, navigated to the dashboard section, and created a new dashboard titled "Breach Detection Portal."

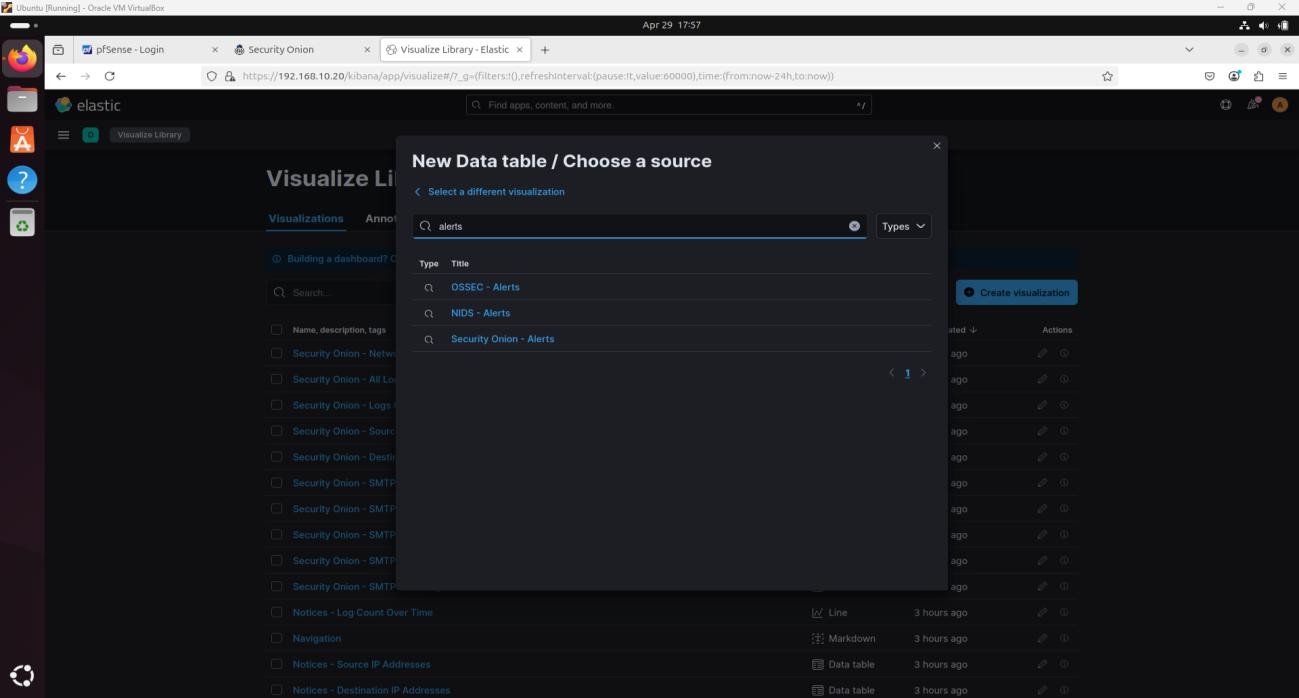


**NIDS Alerts**

I clicked on "Create new object" in the dashboard editor.



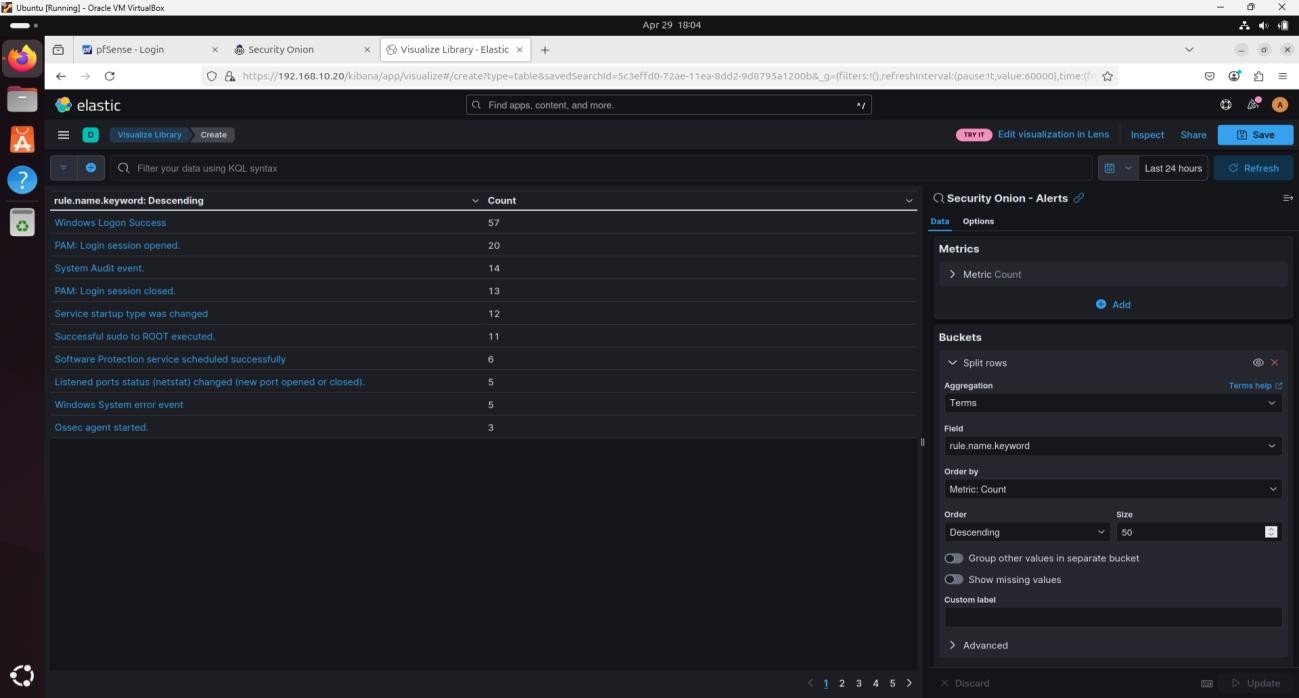
I selected "Data Table" as the visualization type.



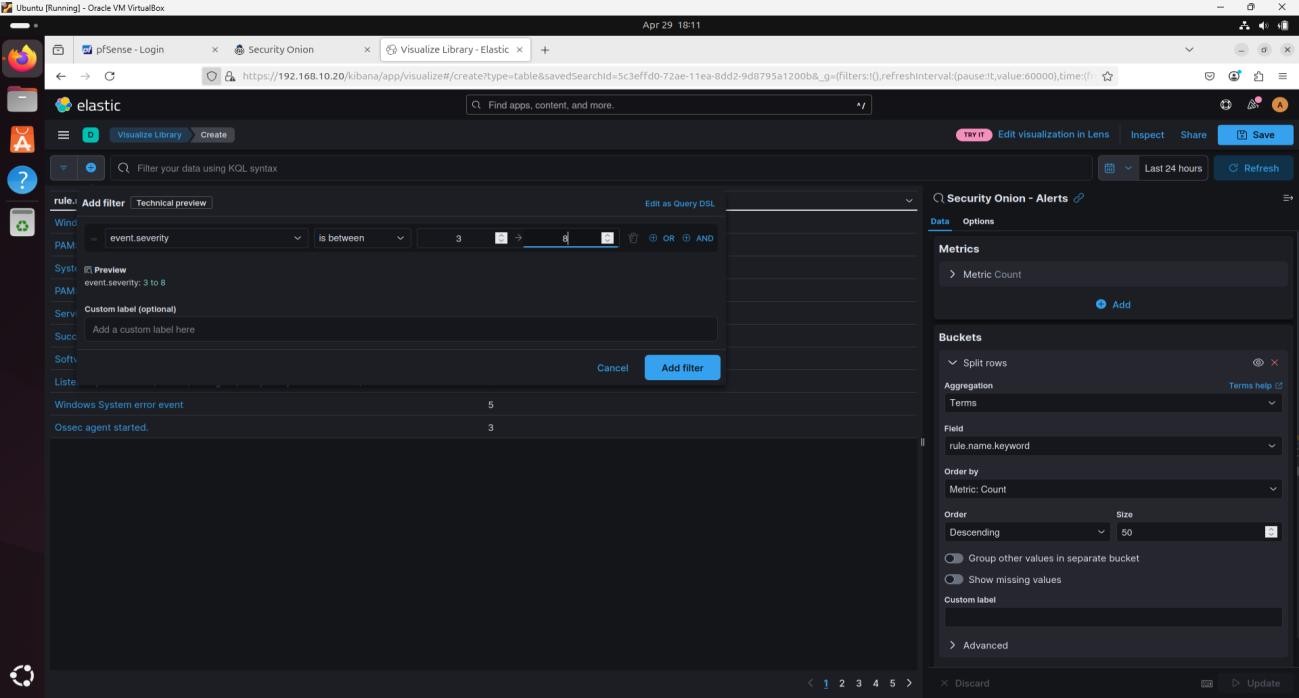
I chose "Security Onion – Alerts" as the data source.

I added a Split Rows bucket with Aggregation set to "Terms" and Field set to "rule.name.keyword."

I set the Size to 50.



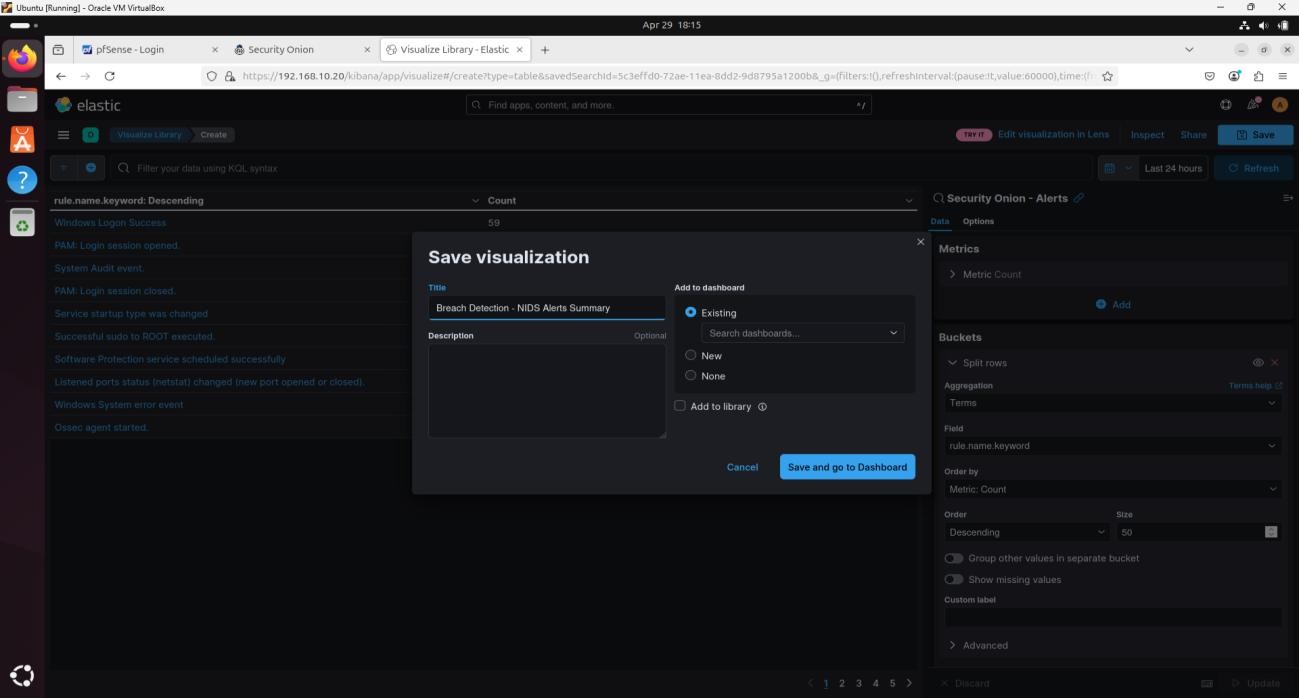
I applied a filter for "event.severity" with values between 3 and 8.

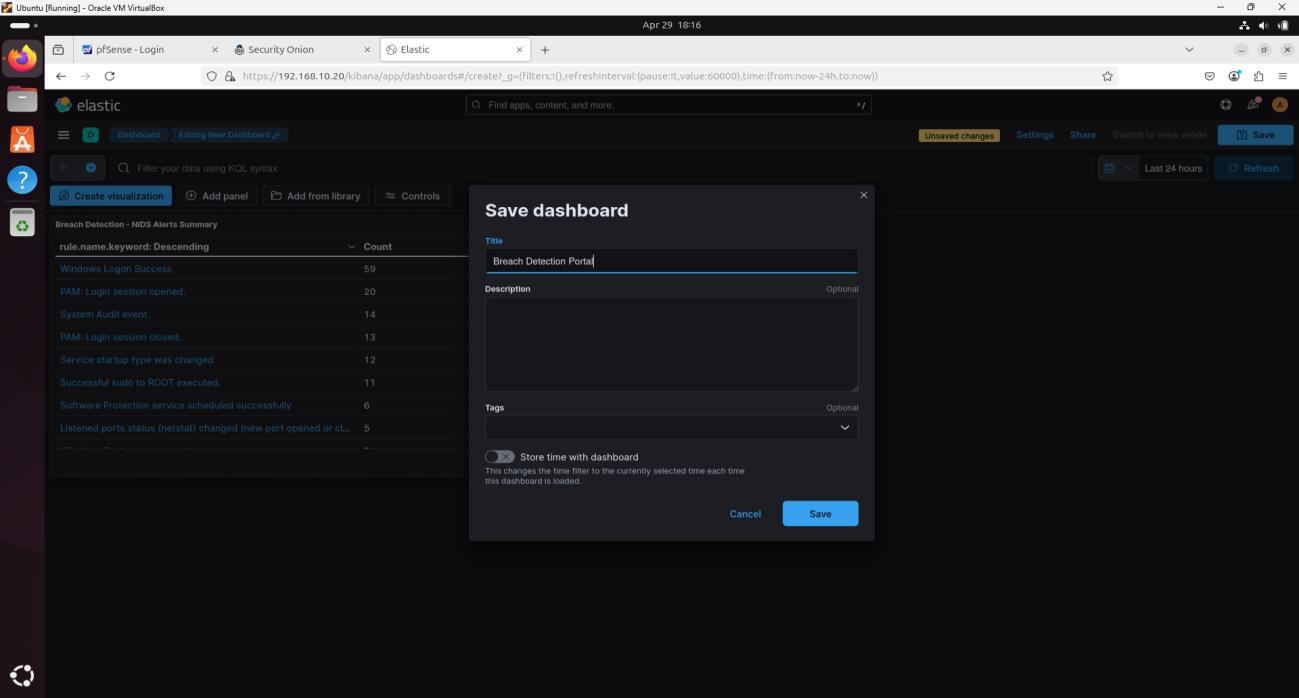


I filtered out noisy alerts by using the minus (-) icon.

I saved the visualization as "Breach Detection – NIDS Alerts Summary."

I adjusted the visualization size and layout.

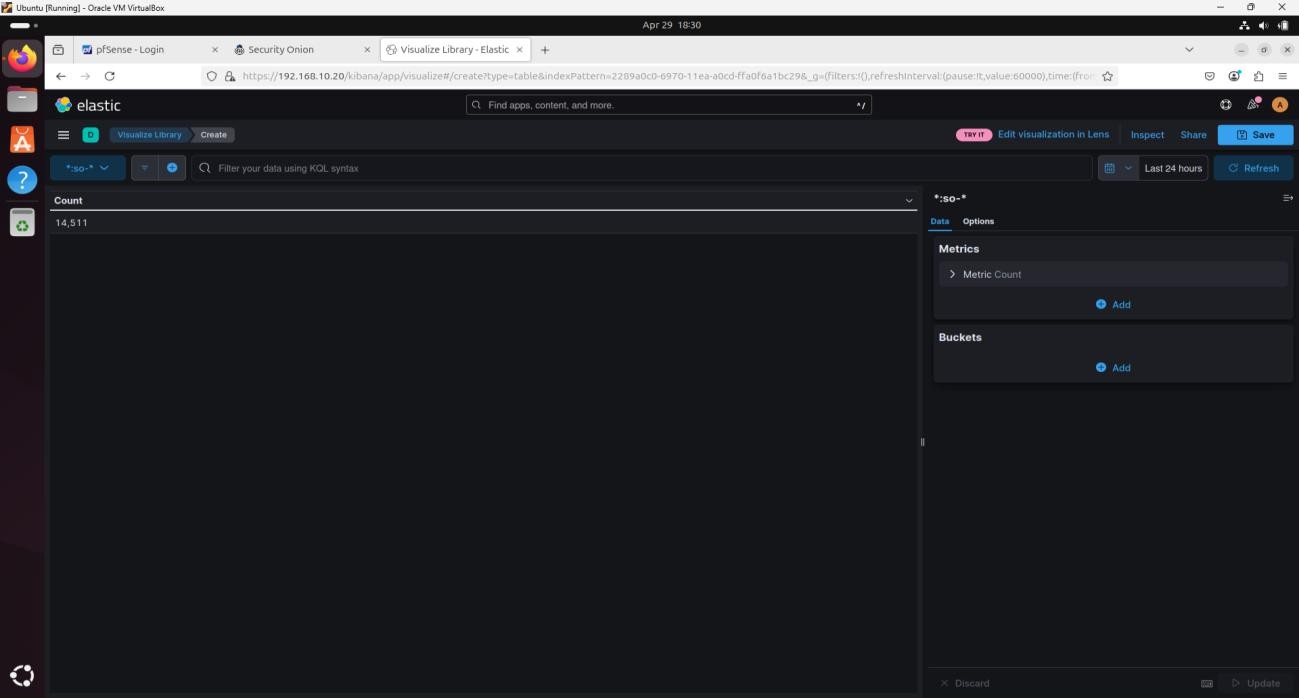
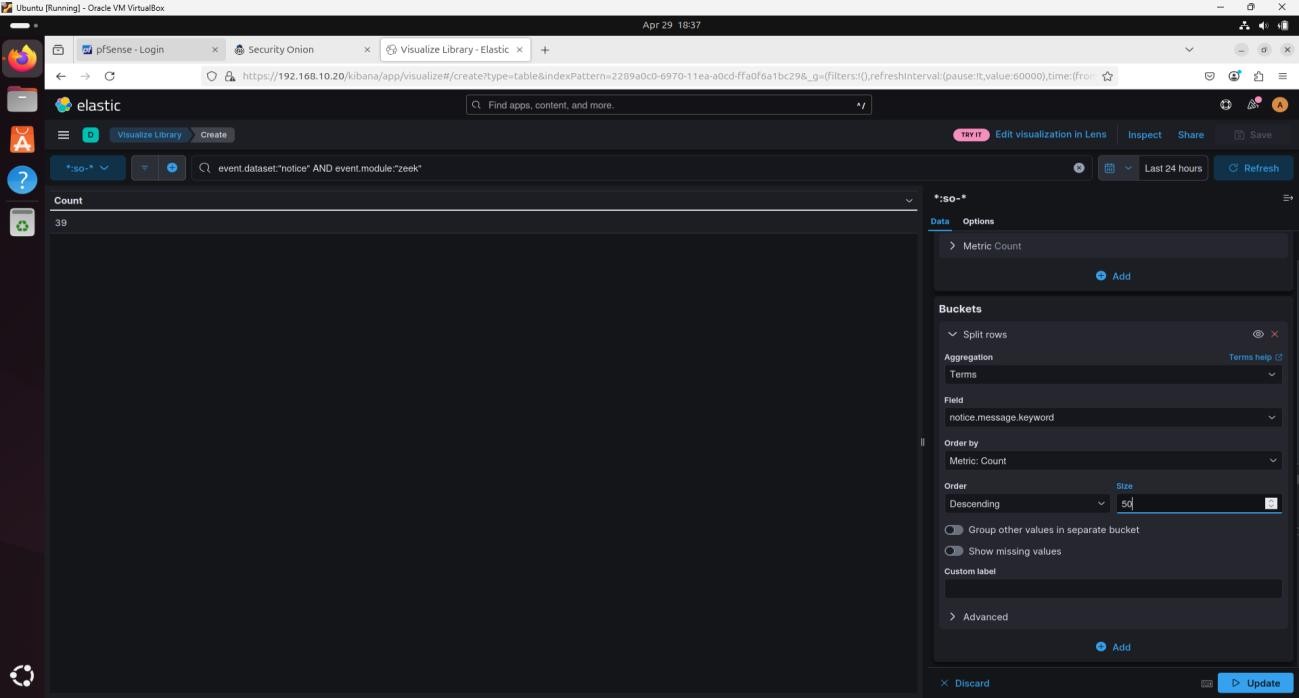




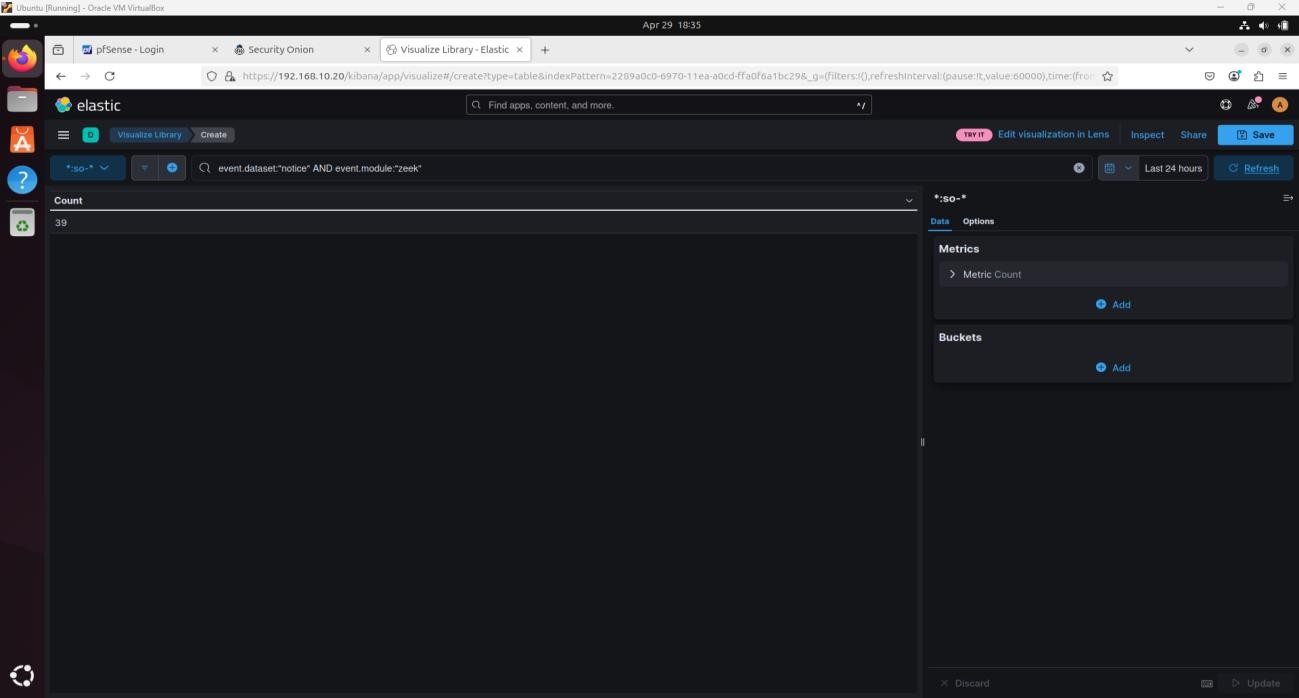
**Zeek Notices**

I edited the dashboard and added a new Data Table widget.

I used the :so- data source.

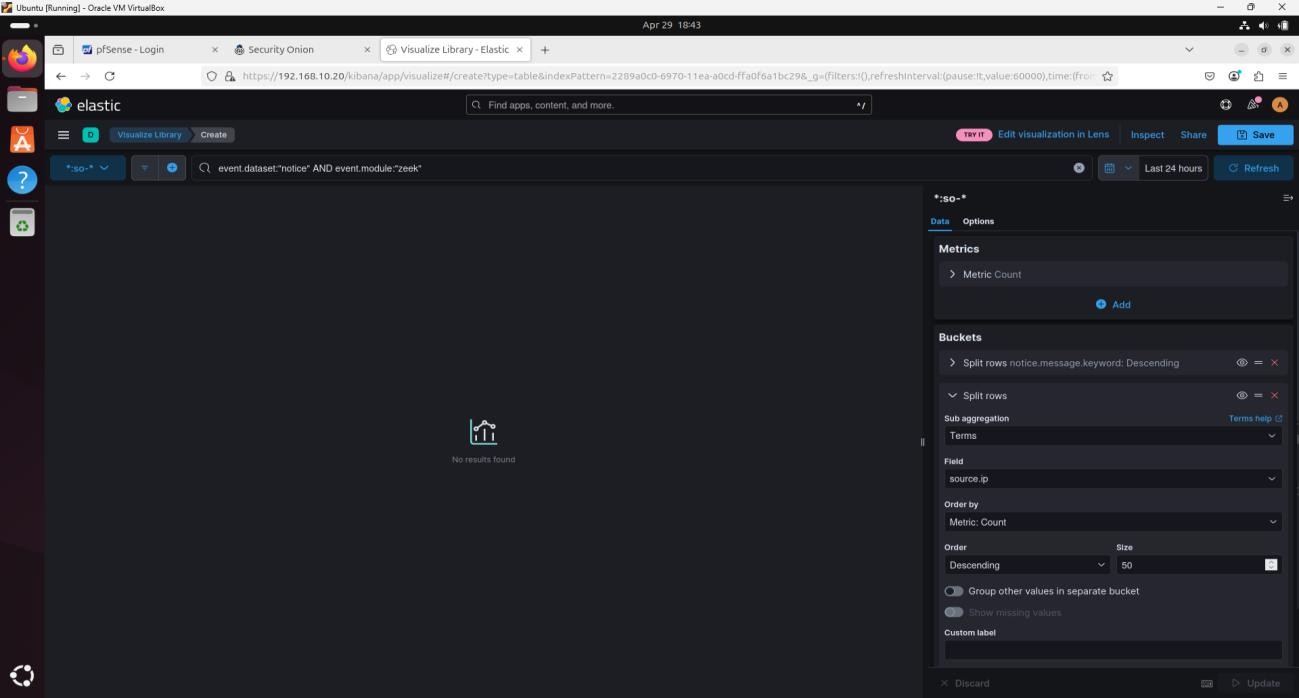


I applied the filter: event.dataset:notice AND event.module:zeek.



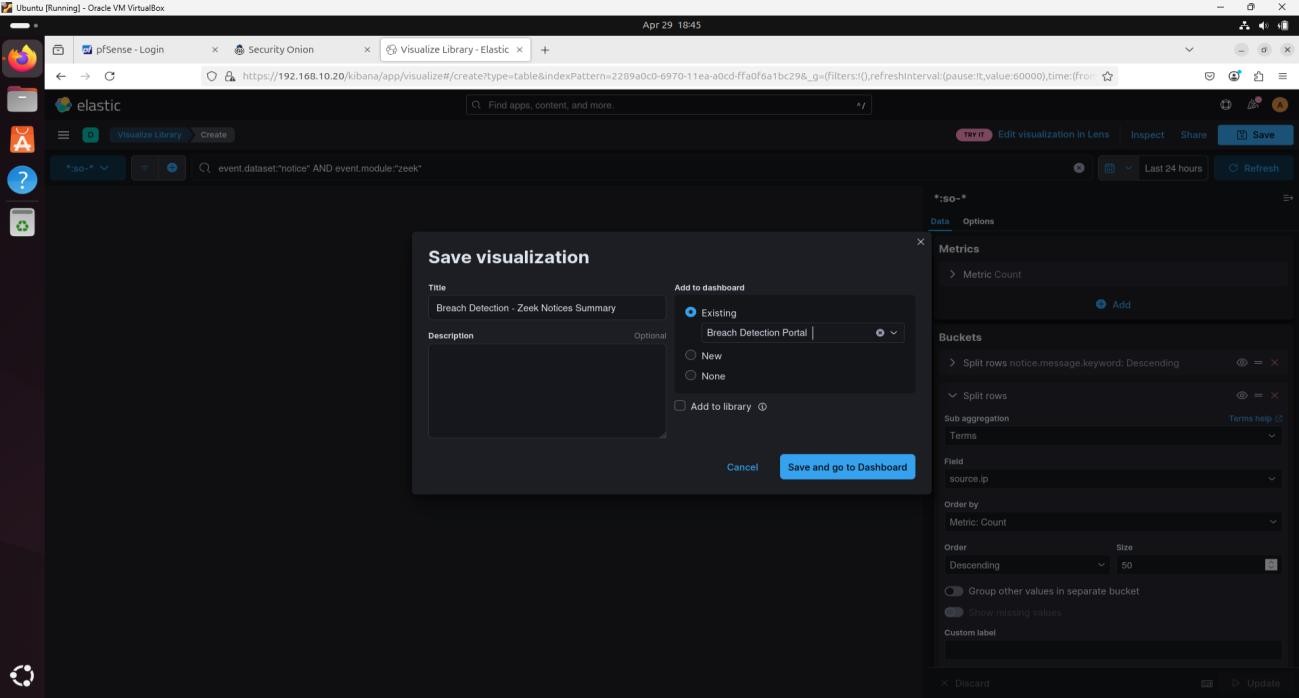
I added a Split Rows bucket with Field: notice.message.keyword, and Size: 50.

I added a second Split Rows bucket with Field: source.ip, and Size: 50.



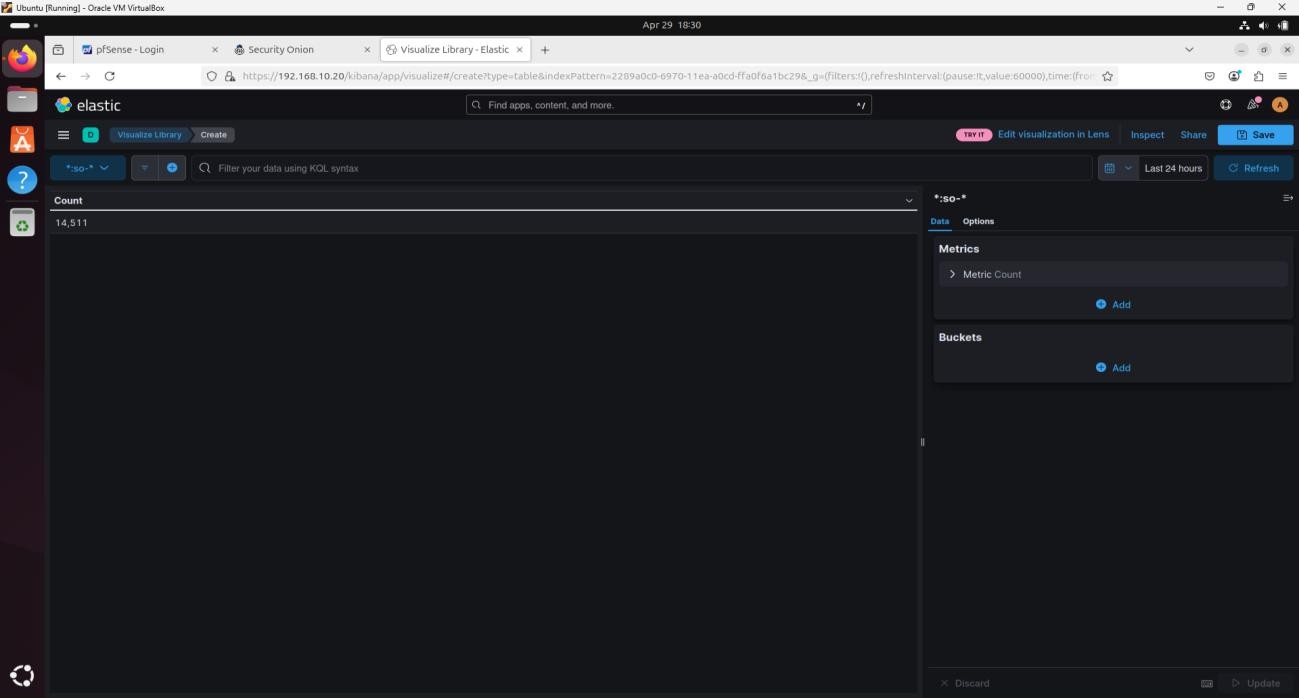
I filtered out certificate validation alerts using the filter tool.

I saved the visualization as "Breach Detection – Zeek Notices Summary."

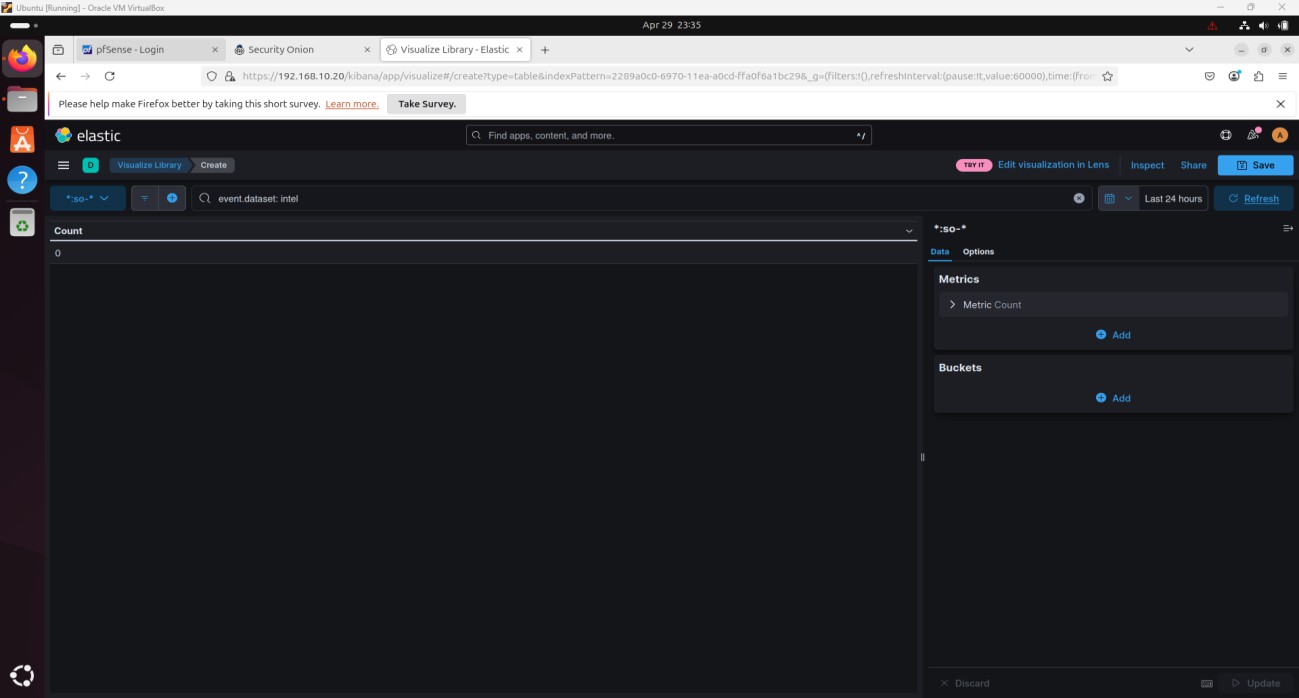


**Zeek Intel Logs**

I added a new Data Table visualization.

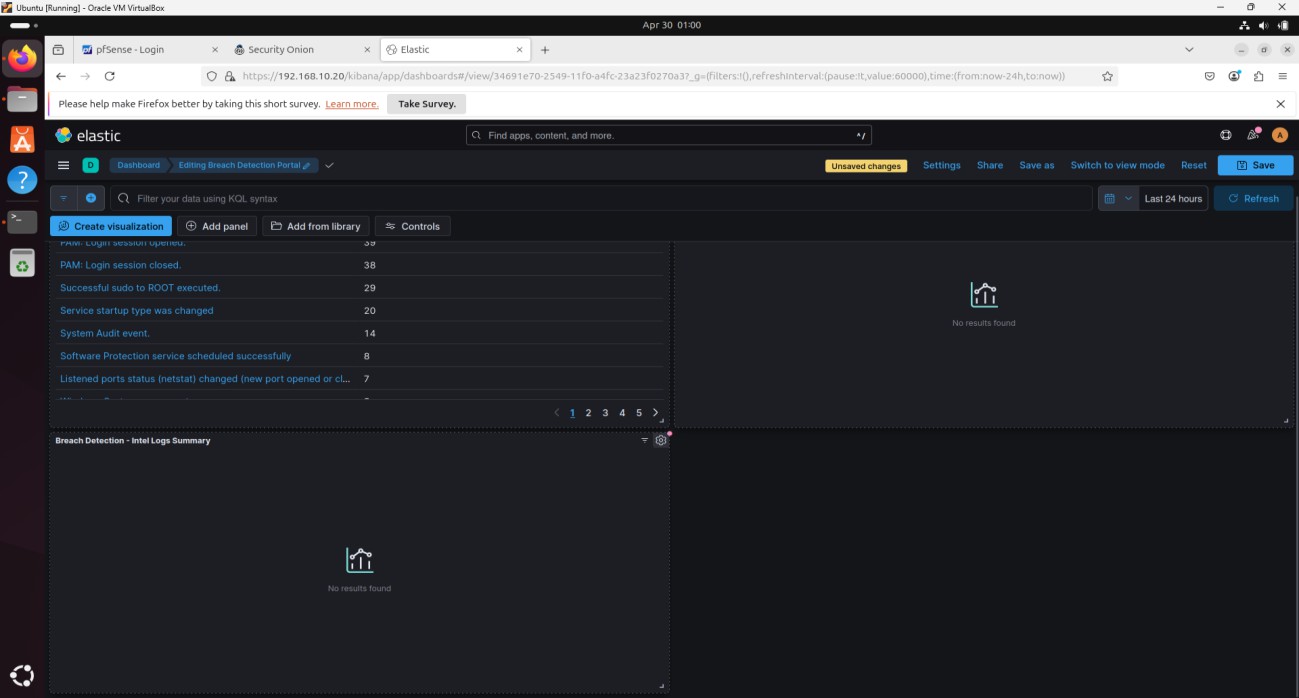


I filtered with event.dataset:intel.



I used Split Rows: intel.sources.keyword and source.ip, each with Size: 50.

I saved it as "Breach Detection – Intel Logs Summary."

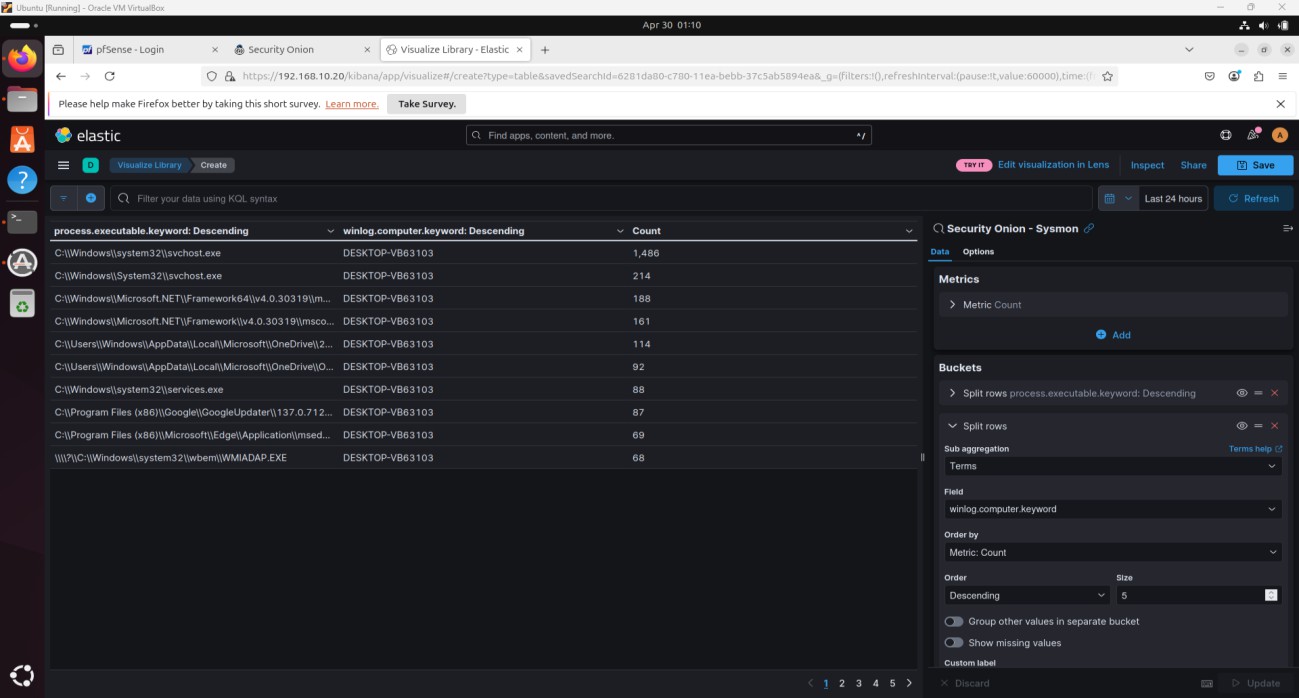


**Suspicious Process and File Creation**

I added a new Data Table using the Sysmon data source.

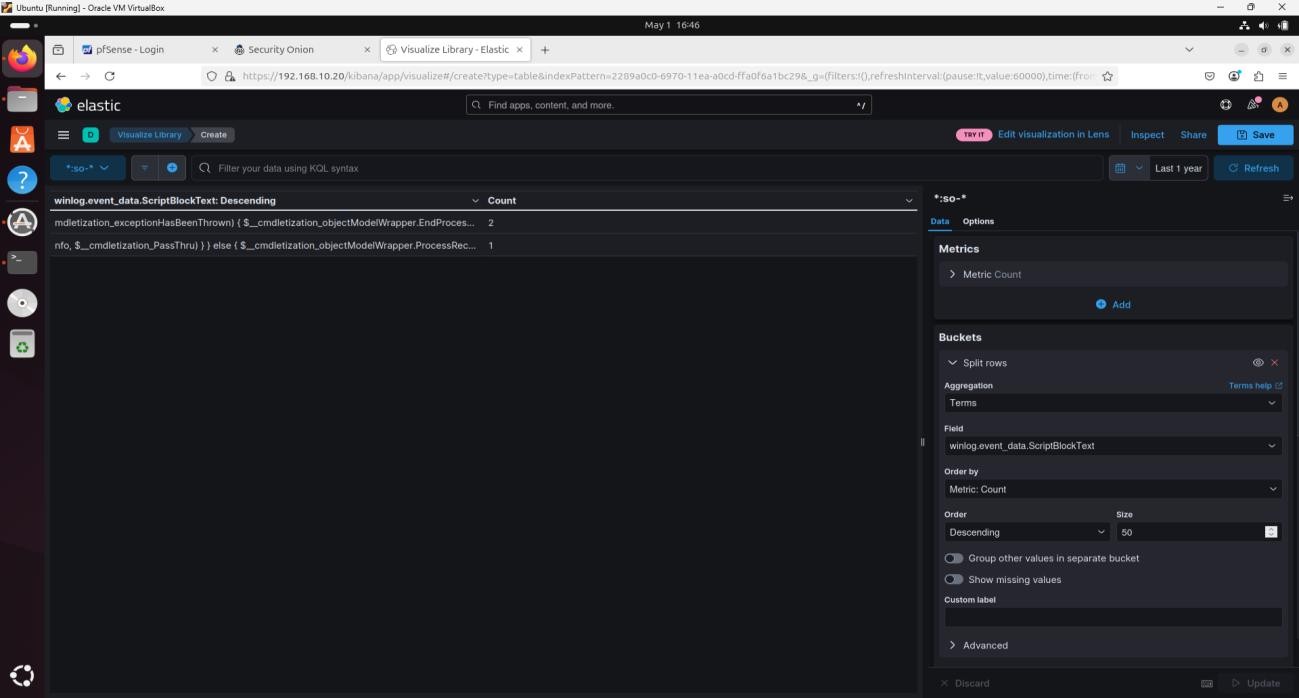
I split rows by process.executable.keyword.

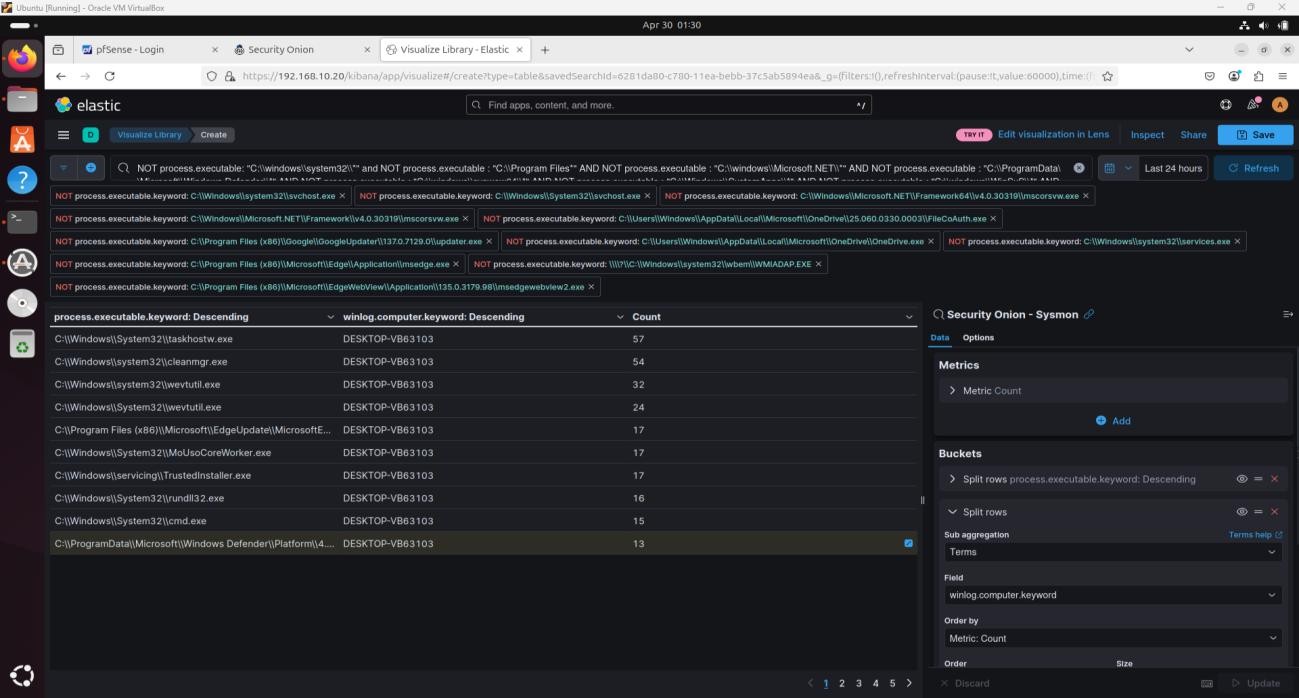
I added winlog.computer.keyword as another Split Rows field.



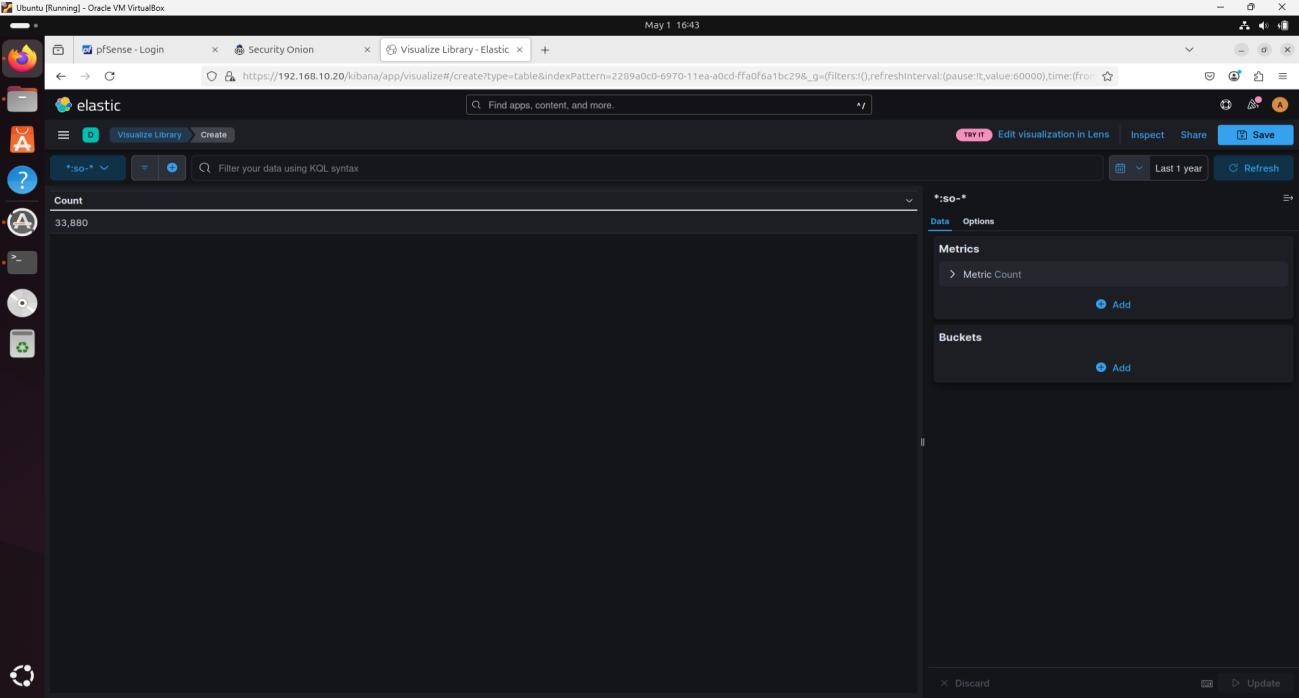
I filtered out standard file paths like C:\Windows\System32.

I removed safe executables such as explorer.exe.





I saved the widget as "Breach Detection – Suspicious Image Paths."

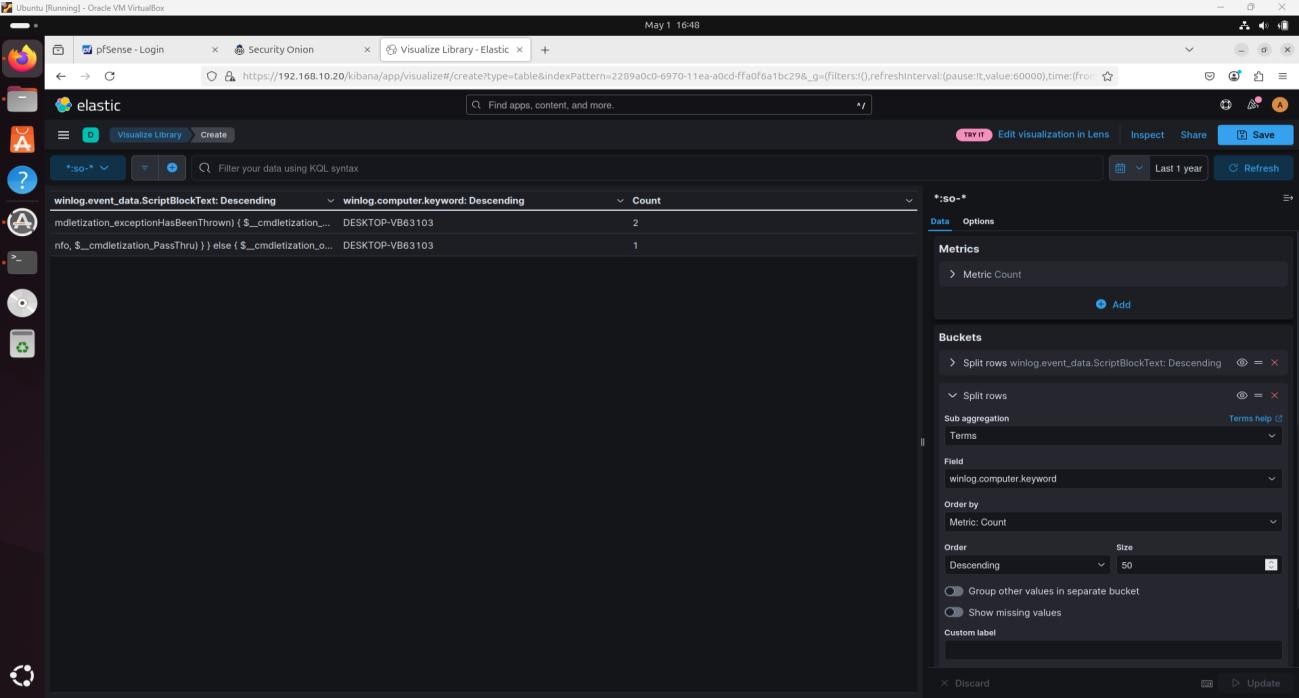


**Suspicious PowerShell Commands**

I added a Data Table using the :so- data source.

I split rows by winlog.event\_data.scriptBlockText.keyword.

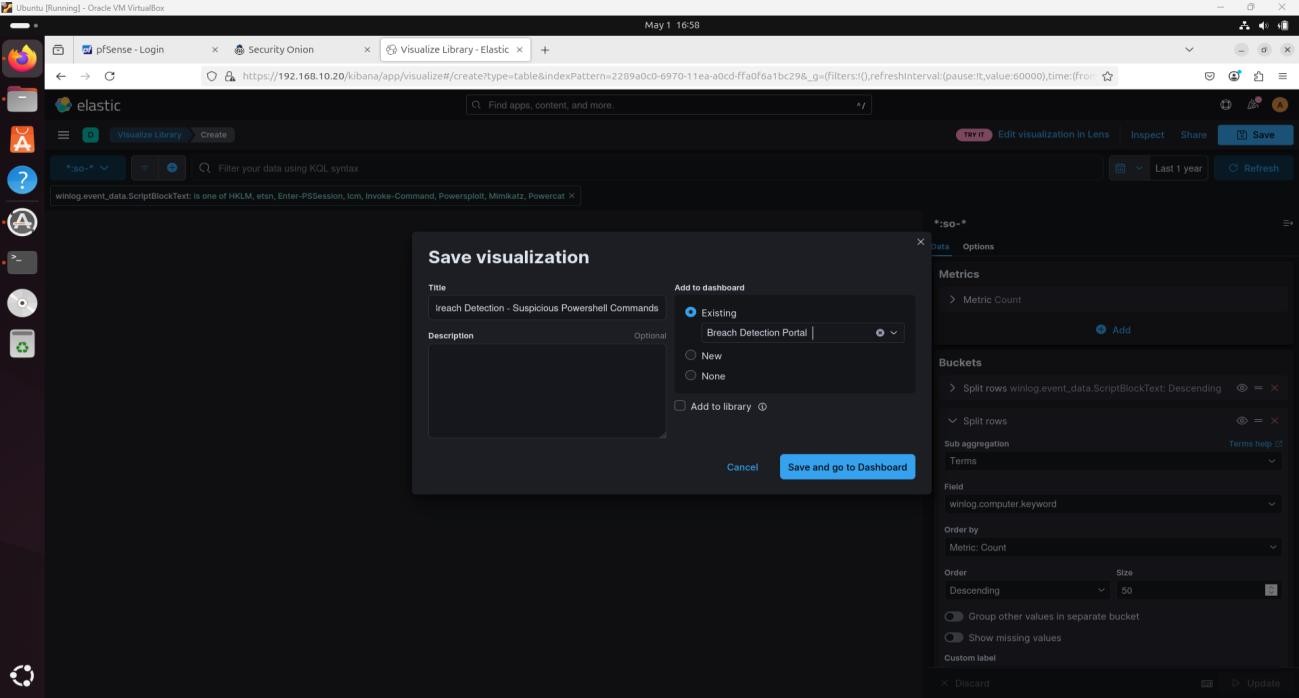
I added winlog.computer.keyword as a secondary field.



I applied a filter with known suspicious script commands.

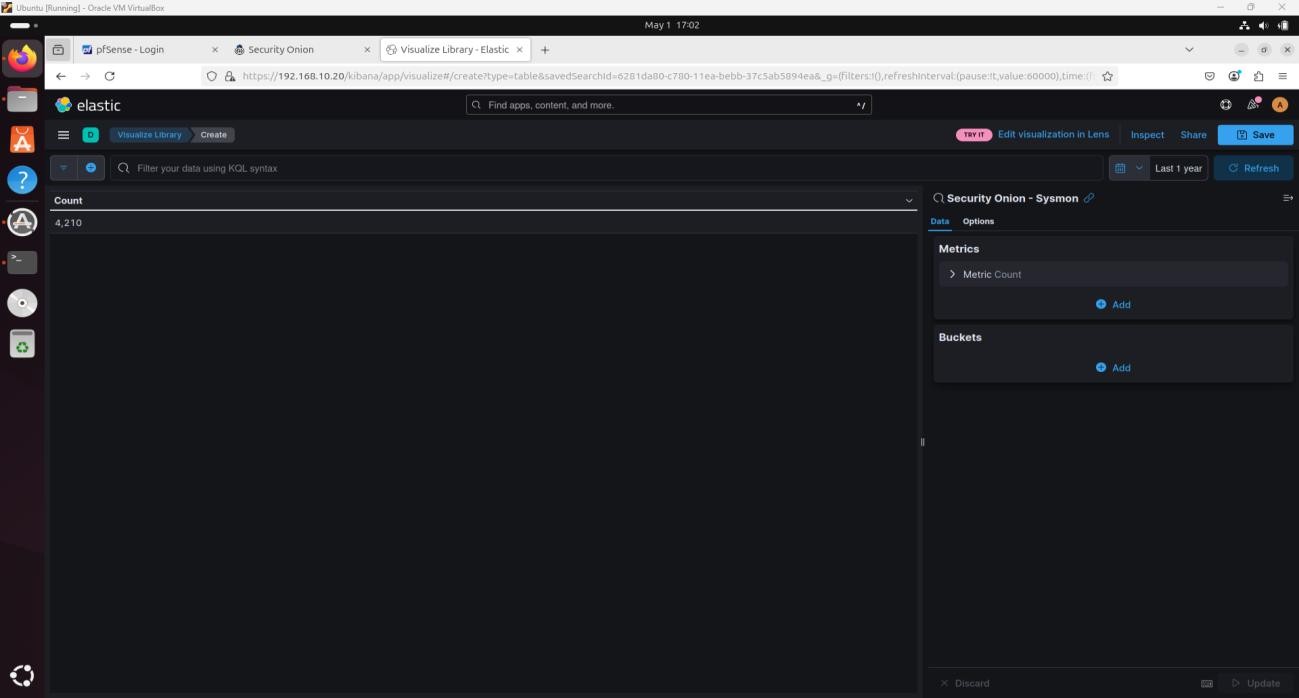


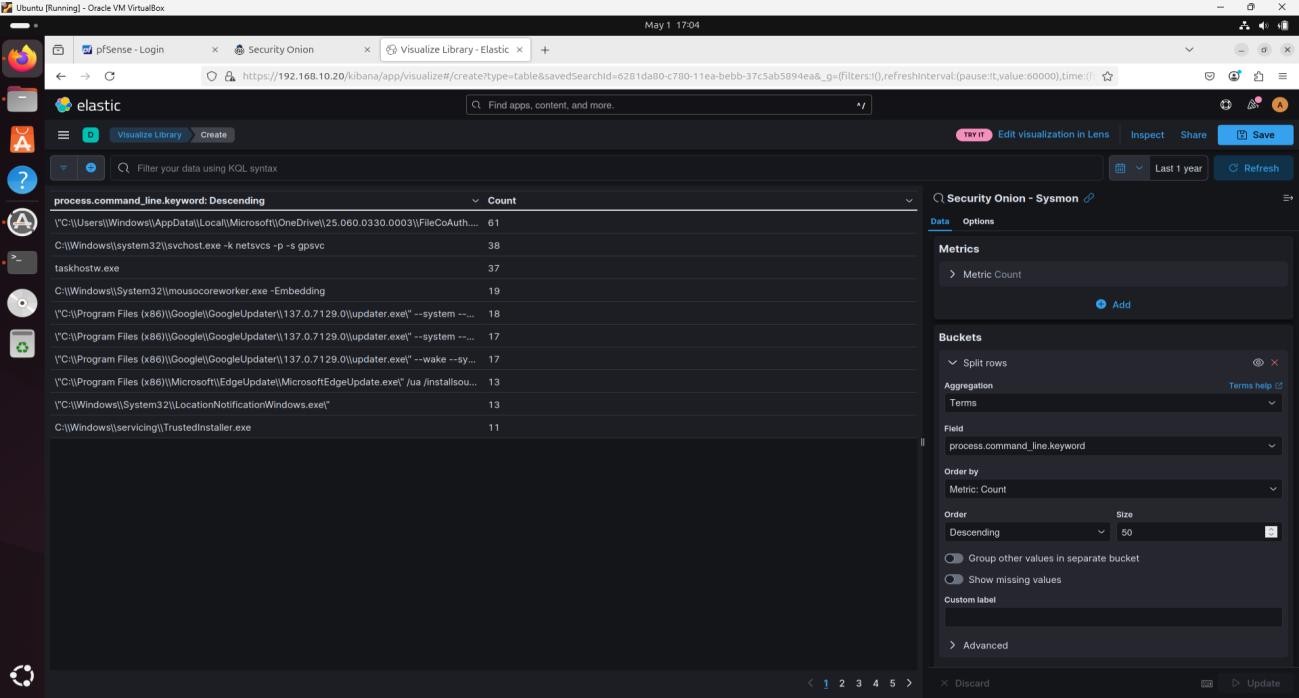
I saved the visualization as "Breach Detection – Suspicious PowerShell Commands."

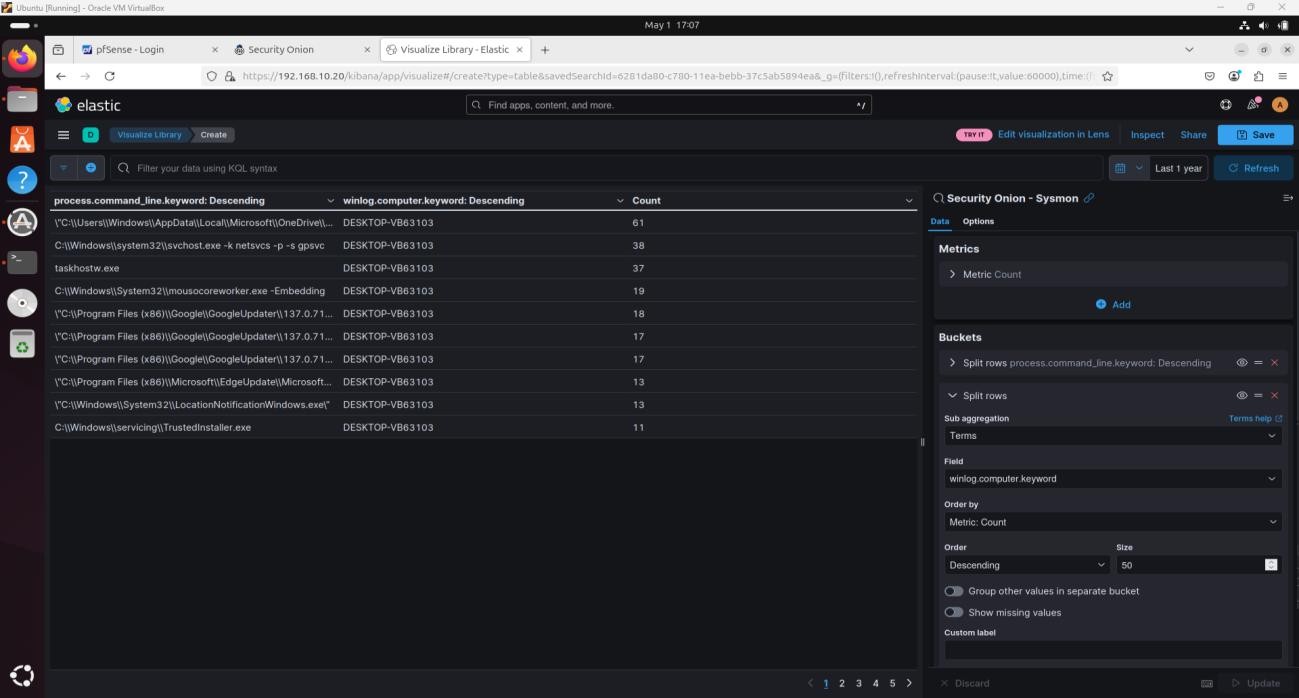


**Suspicious PowerShell Invocation**

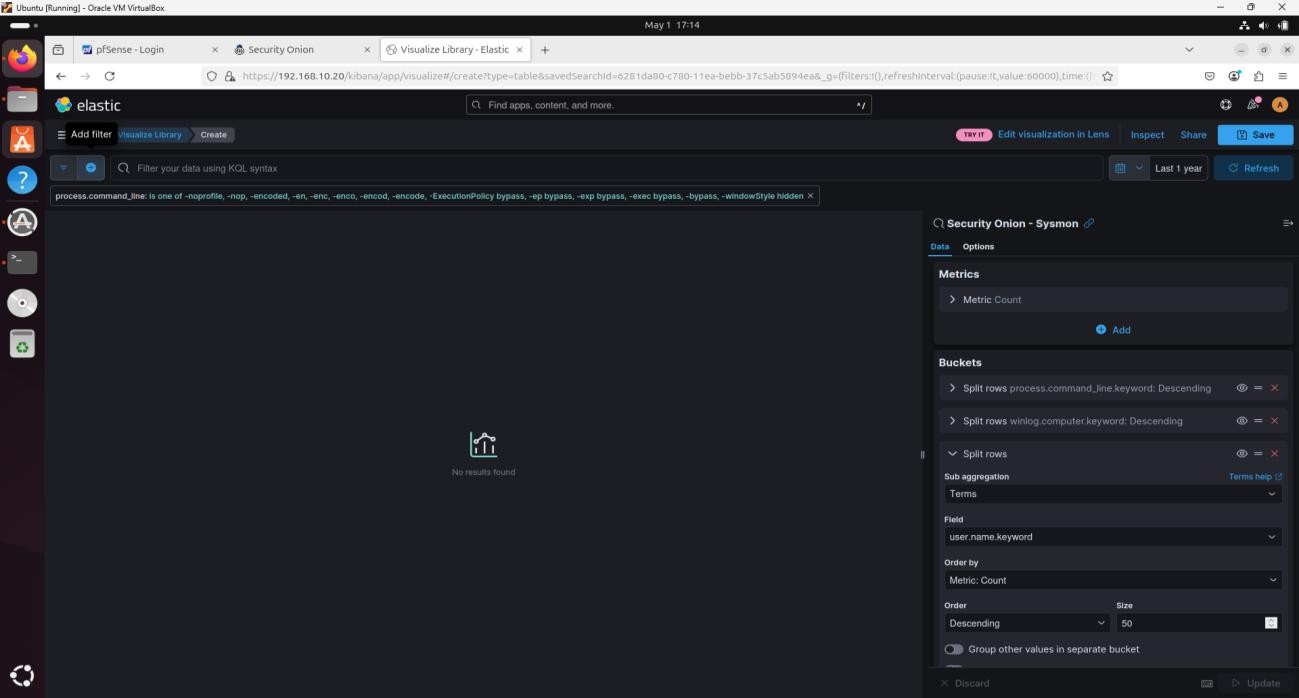
I added a Data Table with the Sysmon data source.

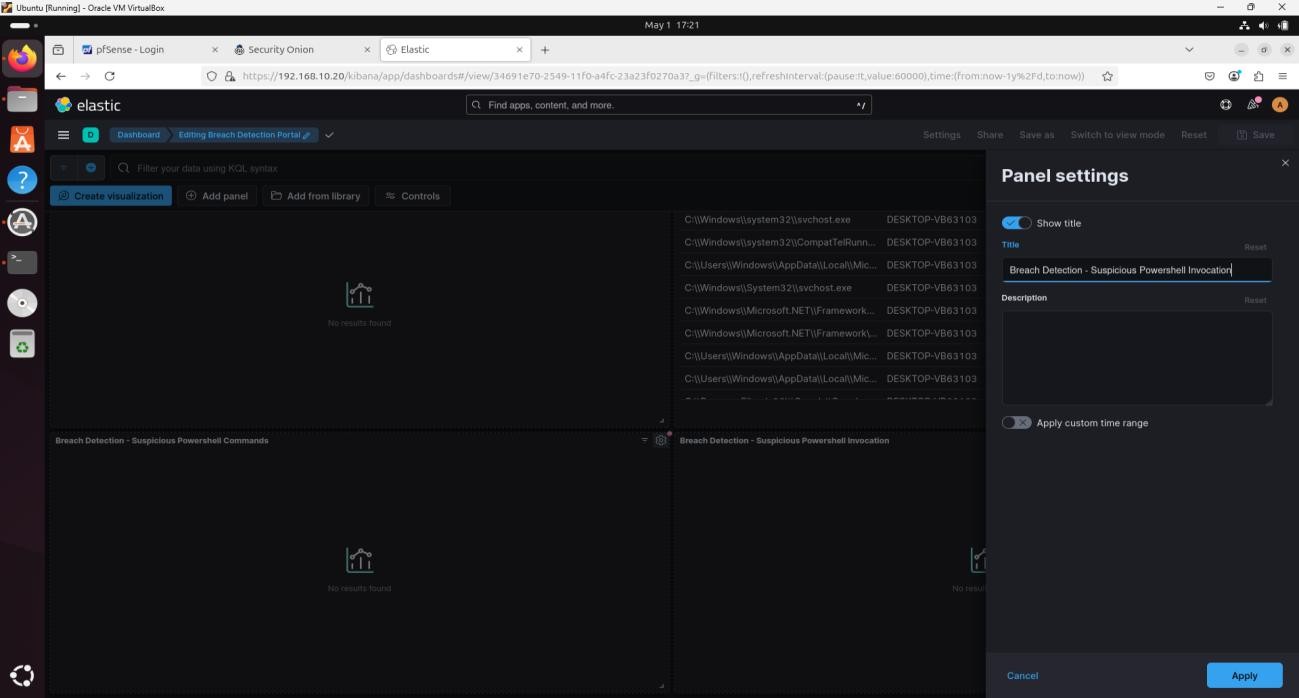
I split rows by process.command\_line.keyword.

I added winlog.computer.keyword and user.name.keyword as additional split fields.



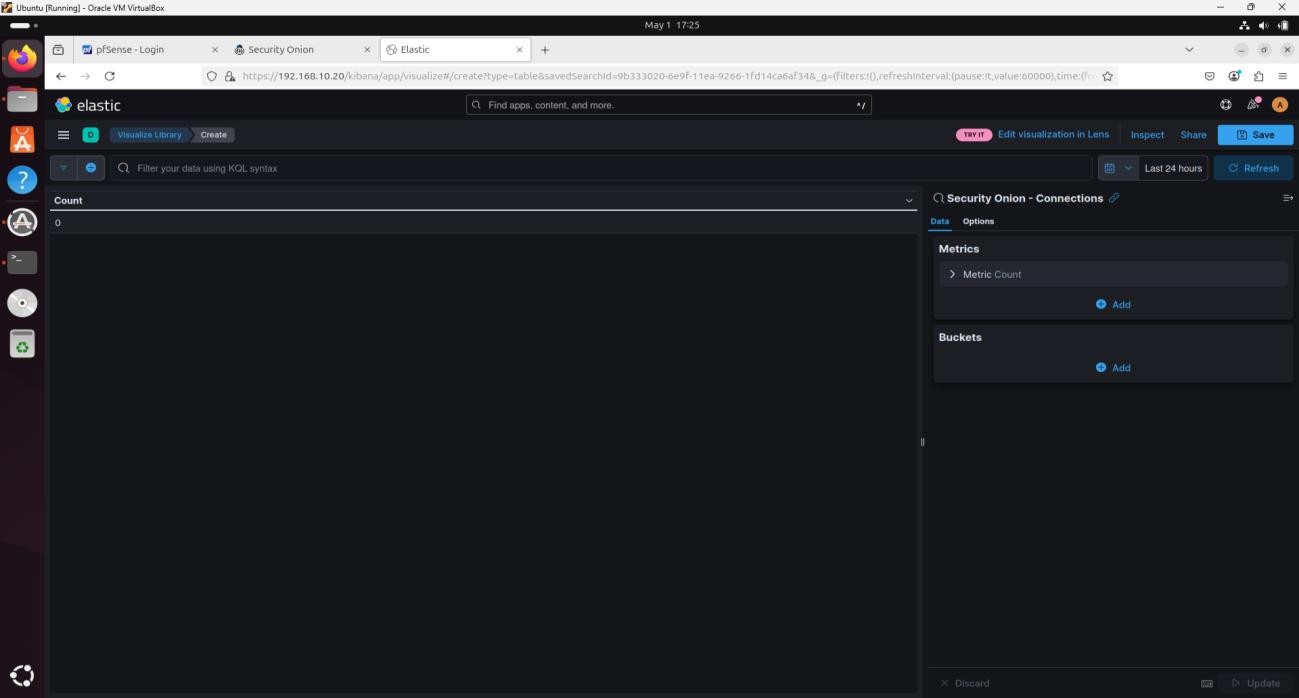
I filtered for known malicious PowerShell invocation commands.

I saved it as "Breach Detection – Suspicious PowerShell Invocation."

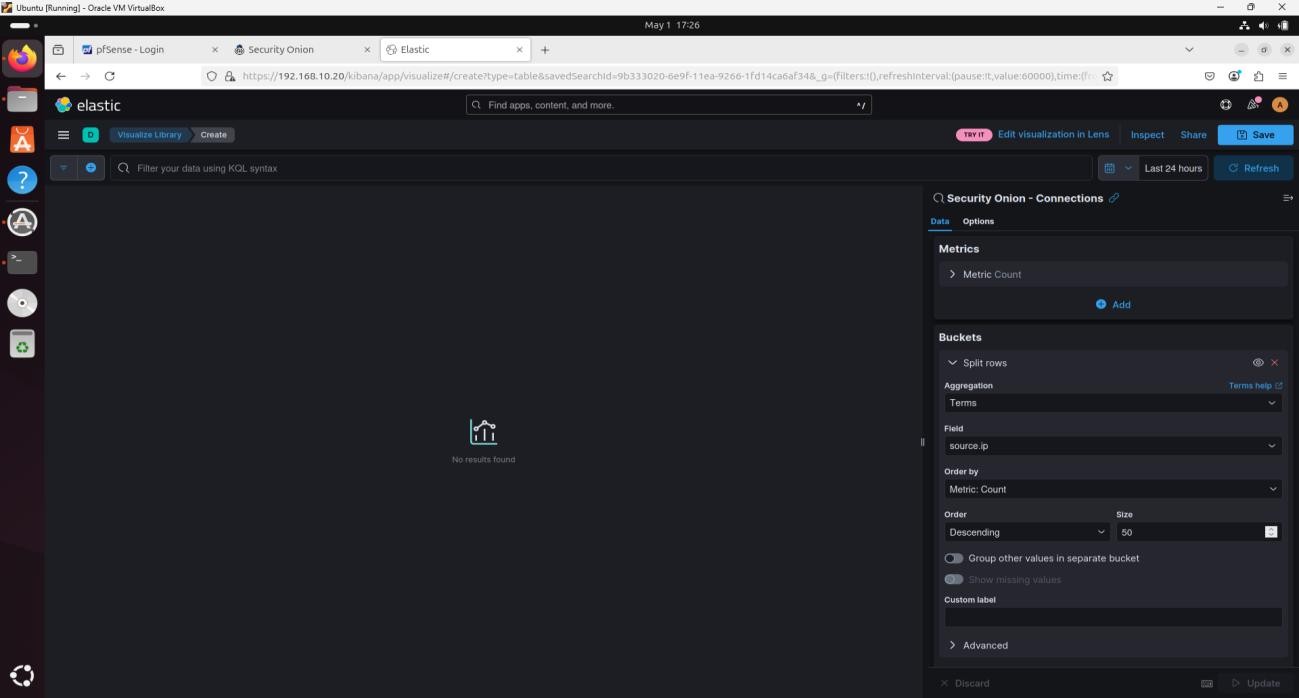
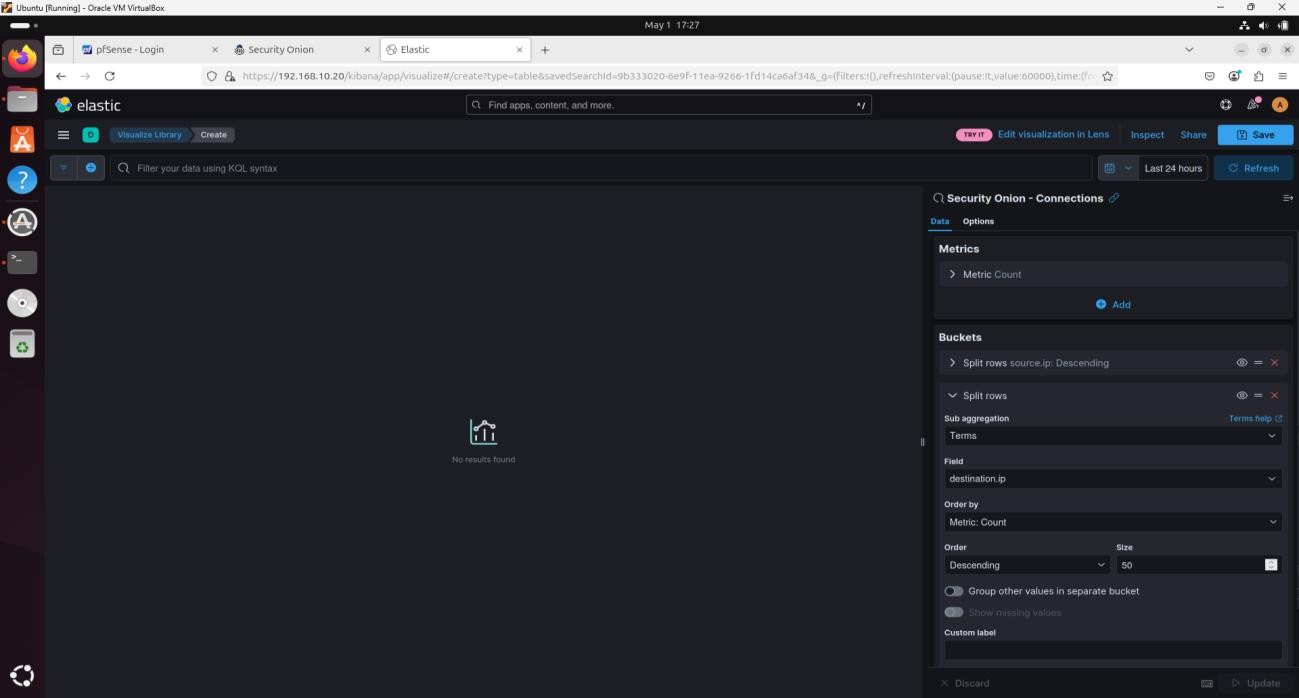


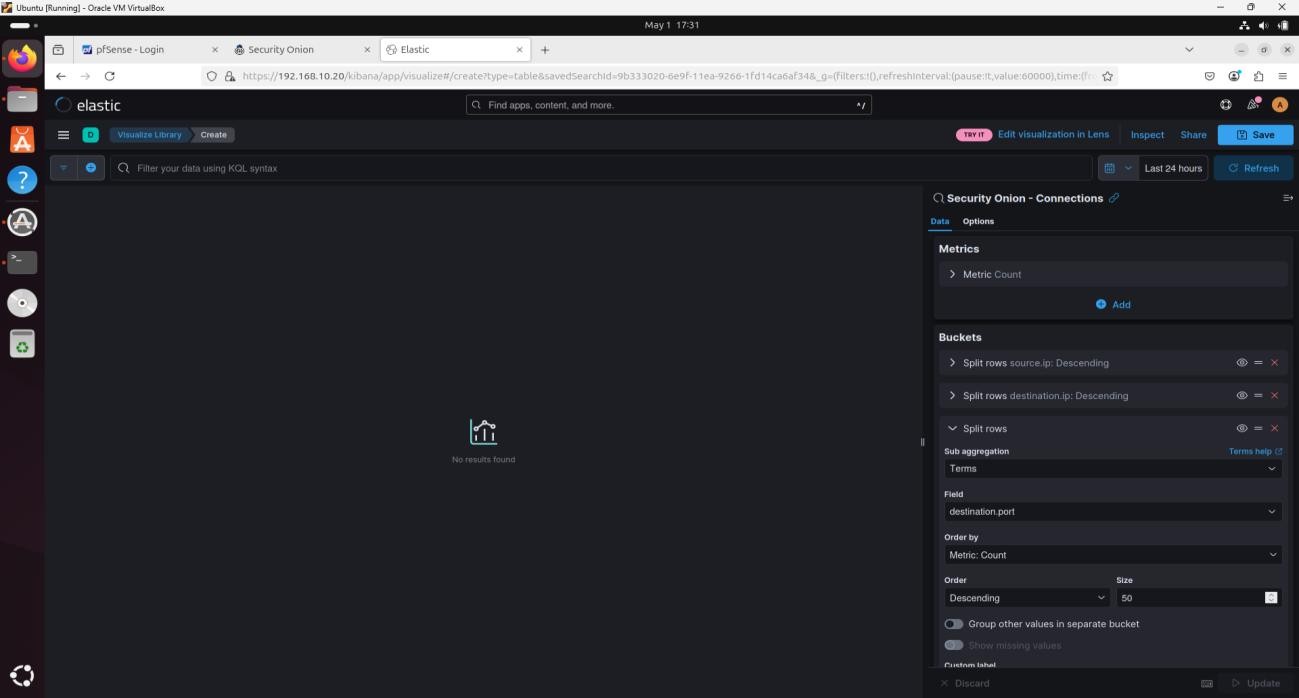
**Suspicious Egress Connections**

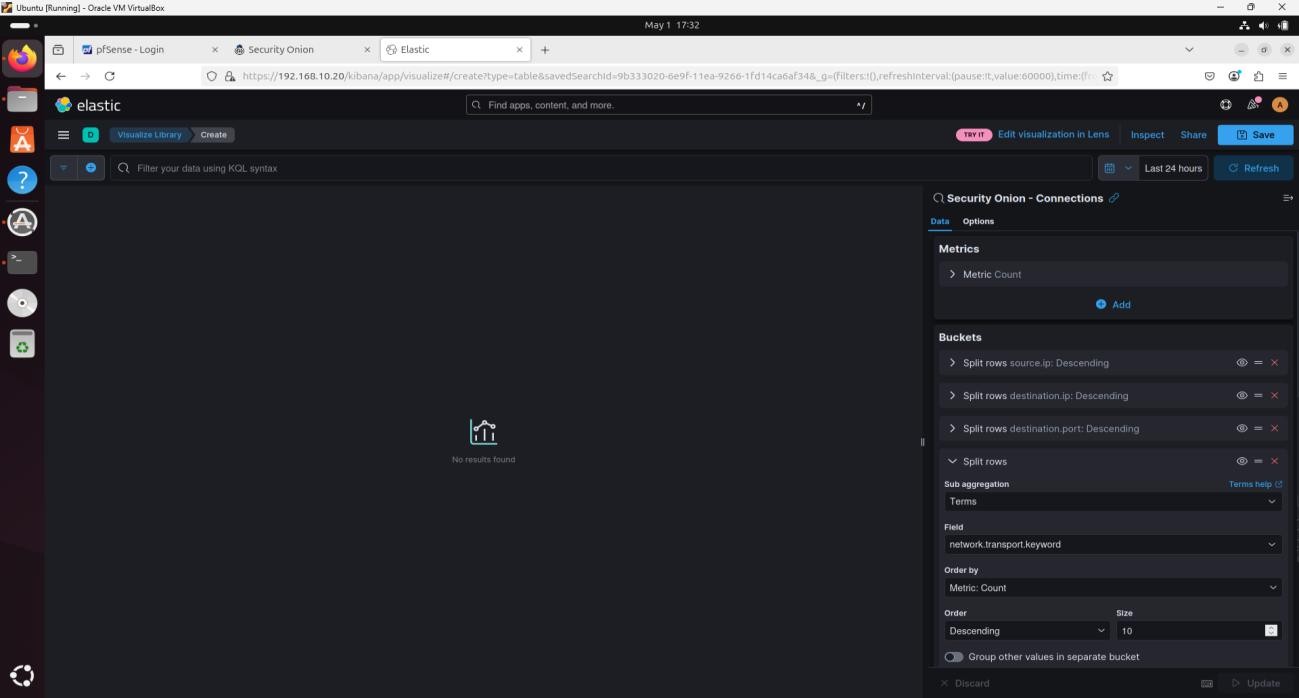
I added a Data Table using the Security Onion – Connections data source.

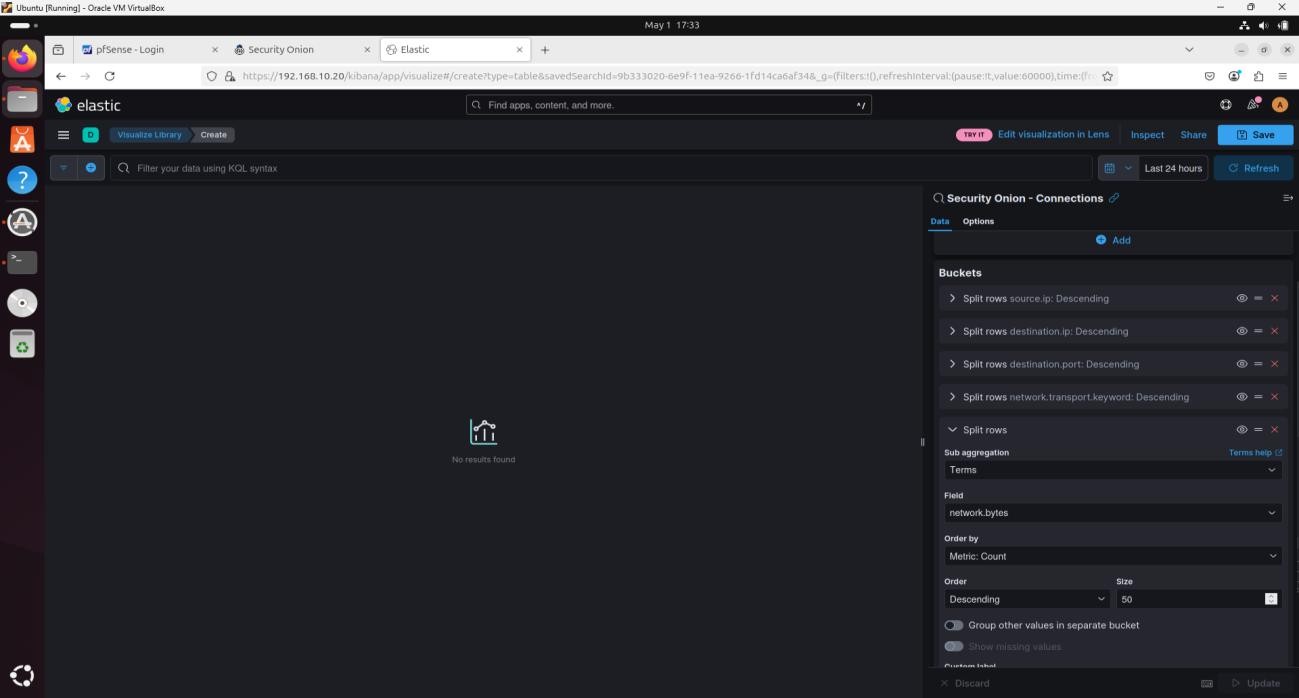


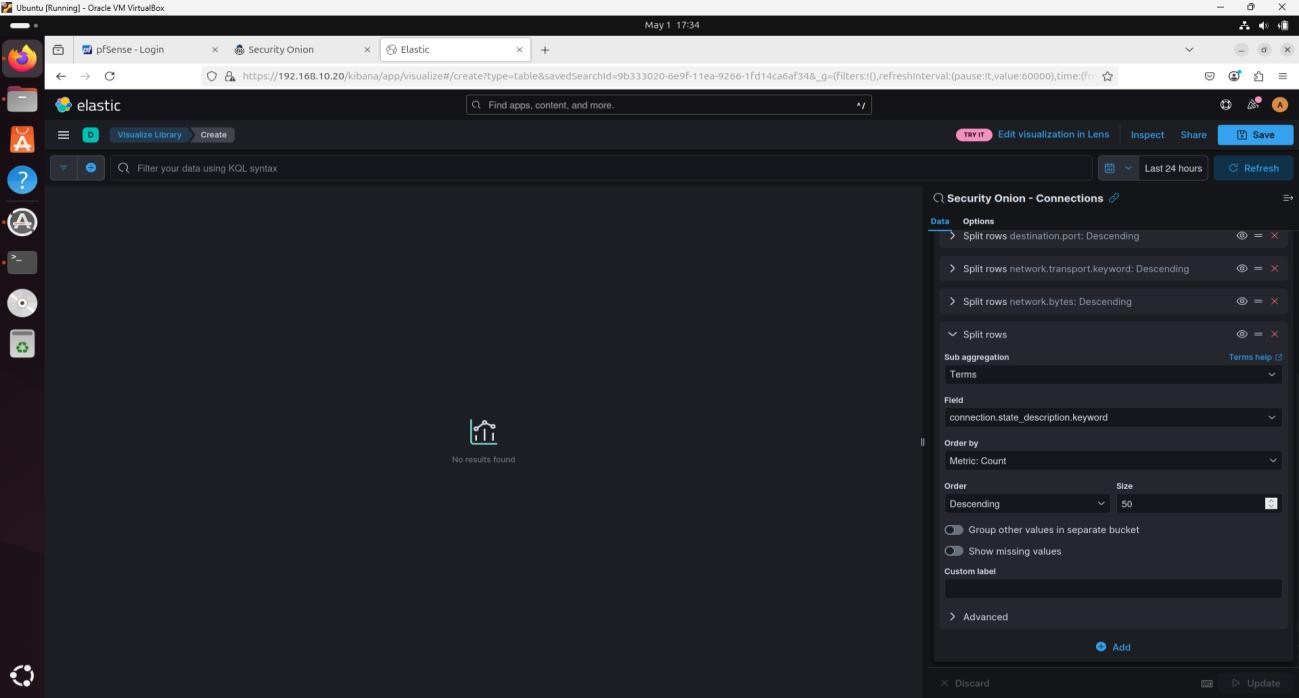
I split rows by: source.ip, destination.ip, destination.port, network.transport.keyword, network.bytes, and connection.state\_description.keyword.







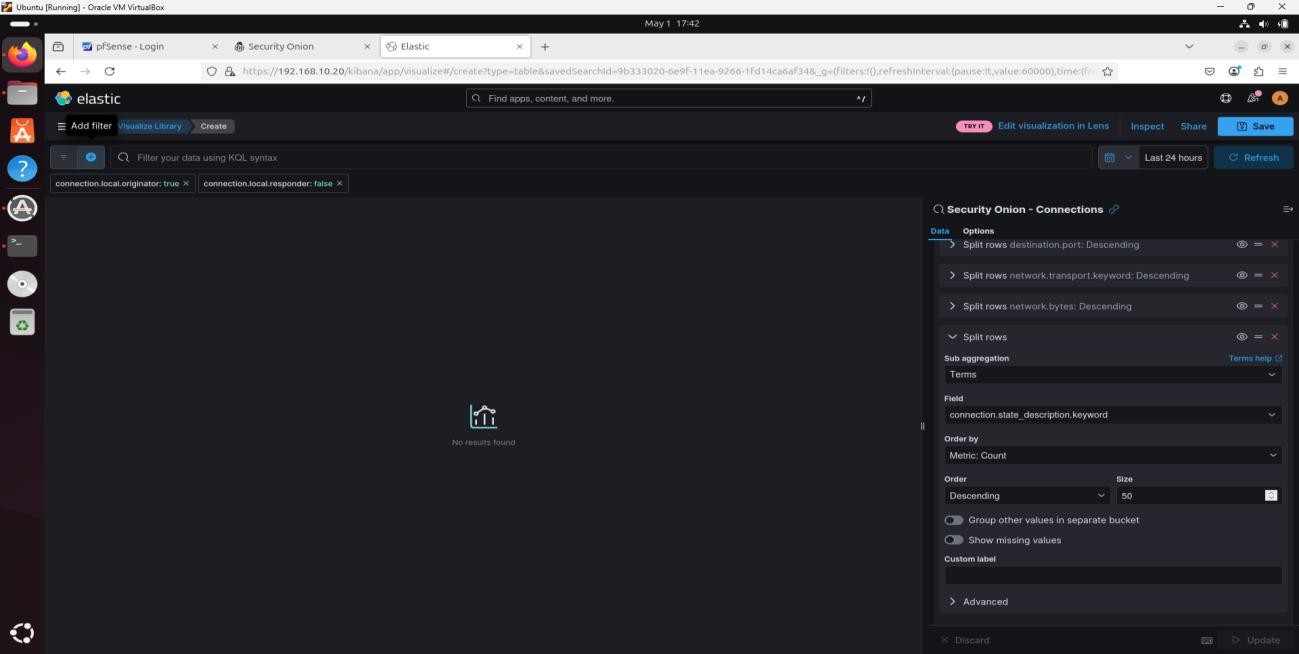


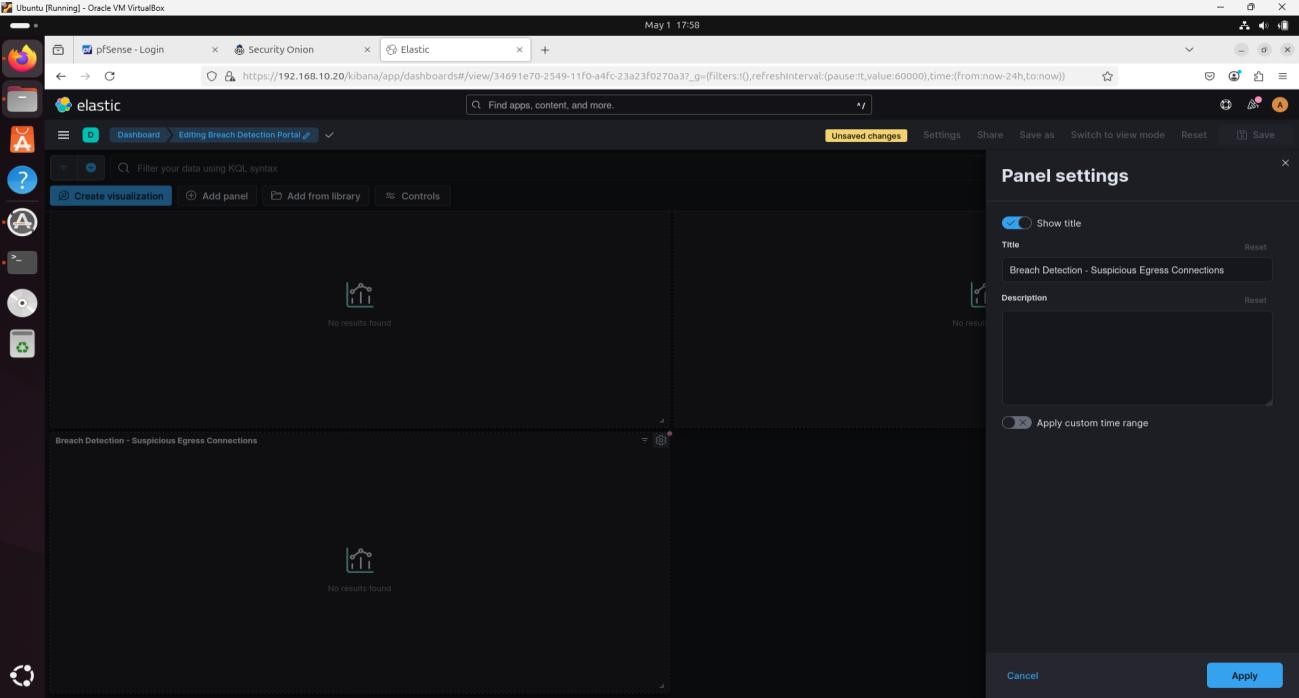


I applied filters for connection.local.originator: true and connection.local.responder: false.

I sorted by Count (descending).

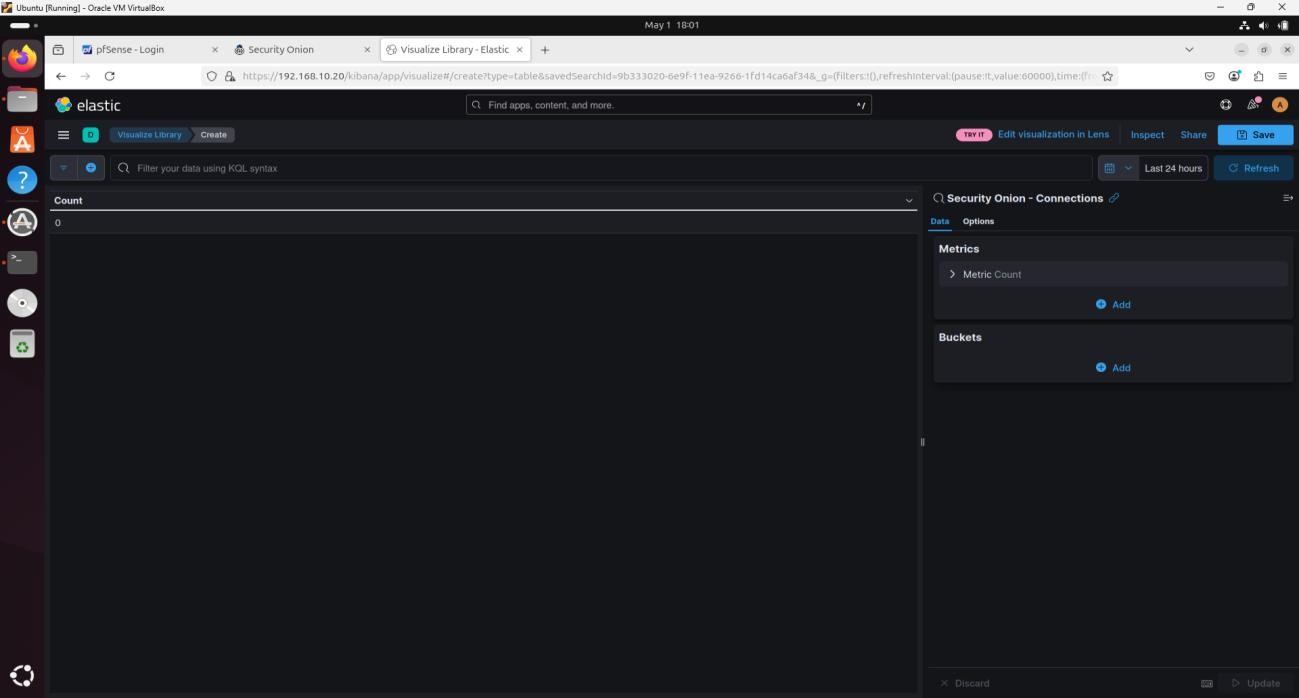
I saved the visualization as "Breach Detection – Suspicious Egress Connections."





**Suspicious Ingress Connections**

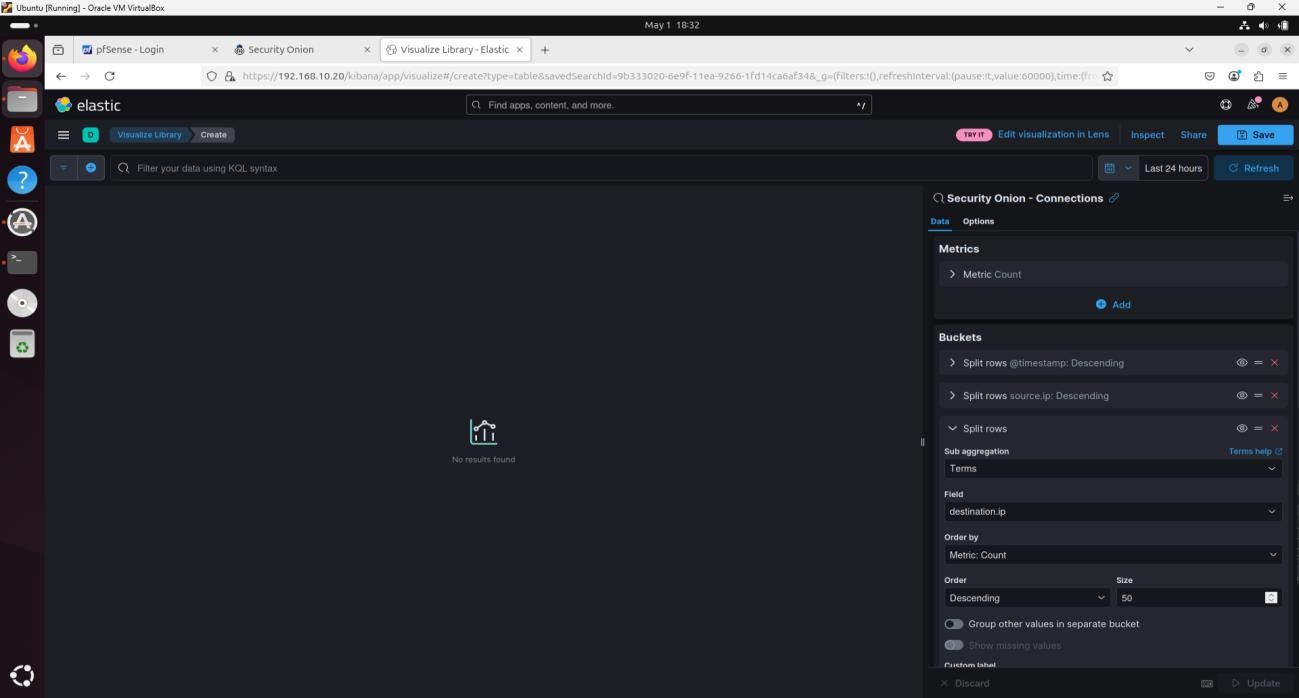
I added another Data Table using the same data source.

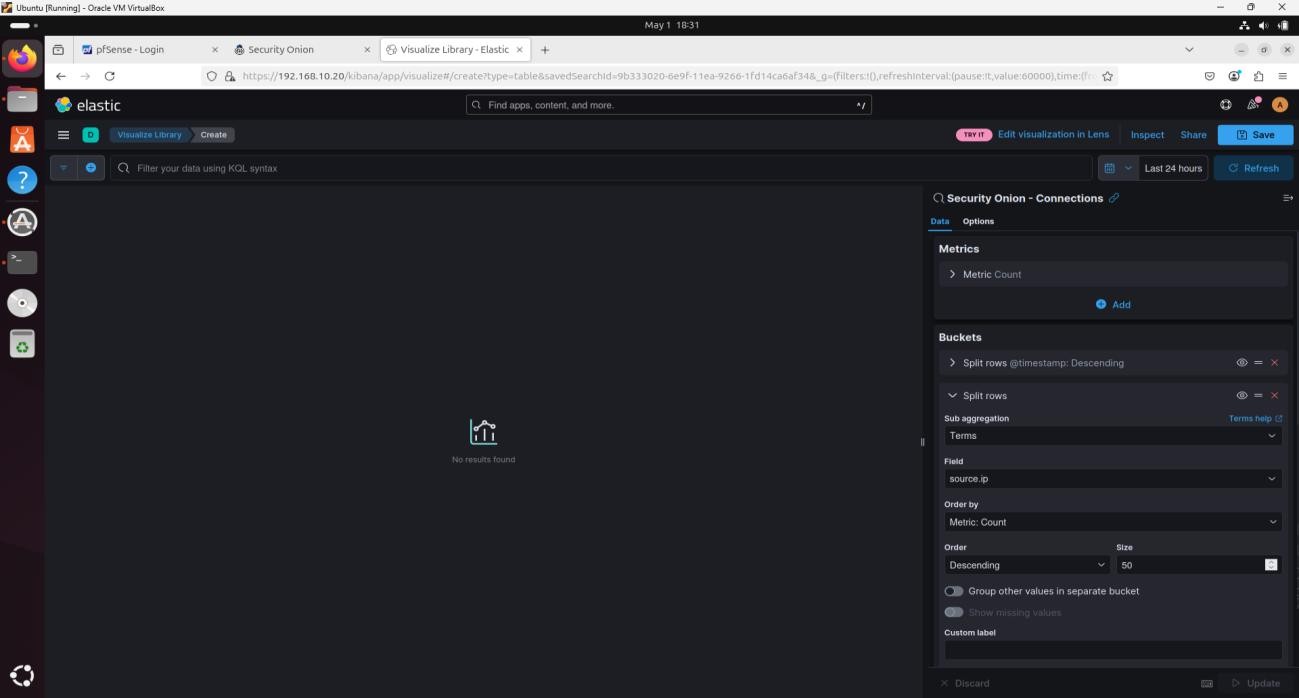


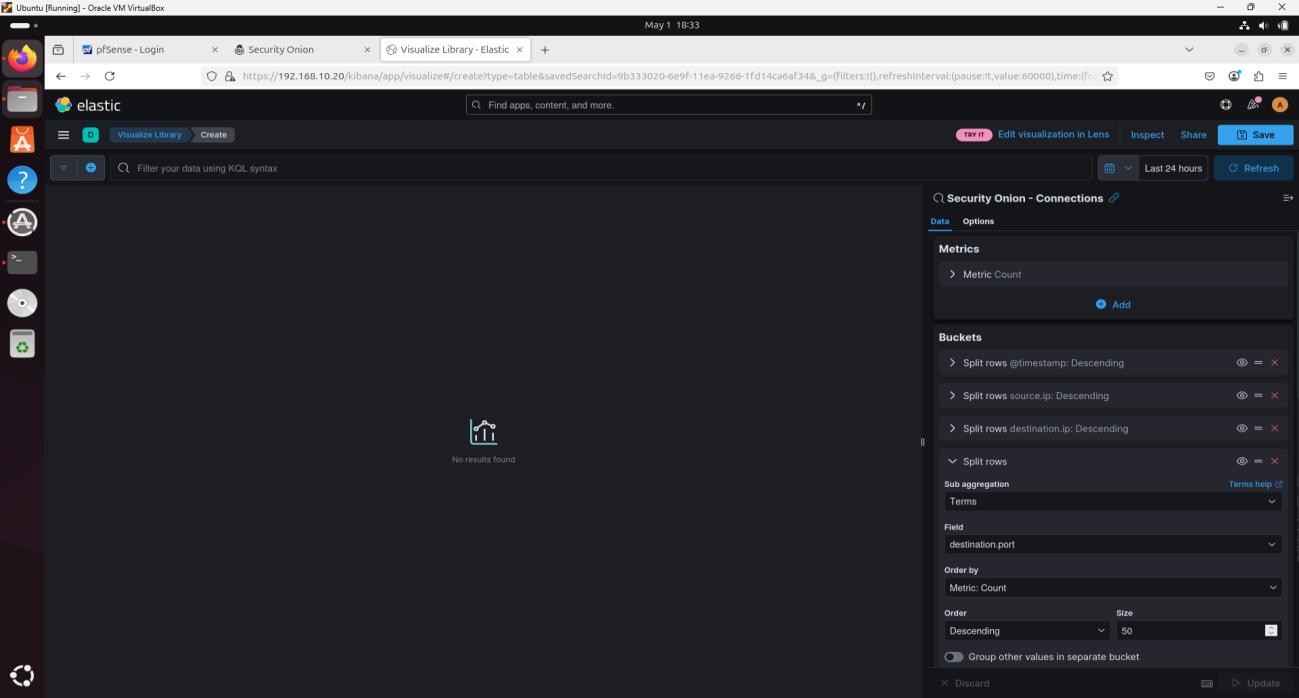
I split rows by: @timestamp, source.ip, destination.ip, destination.port, network.transport.keyword, event.duration, network.bytes, and connection.state\_description.keyword.

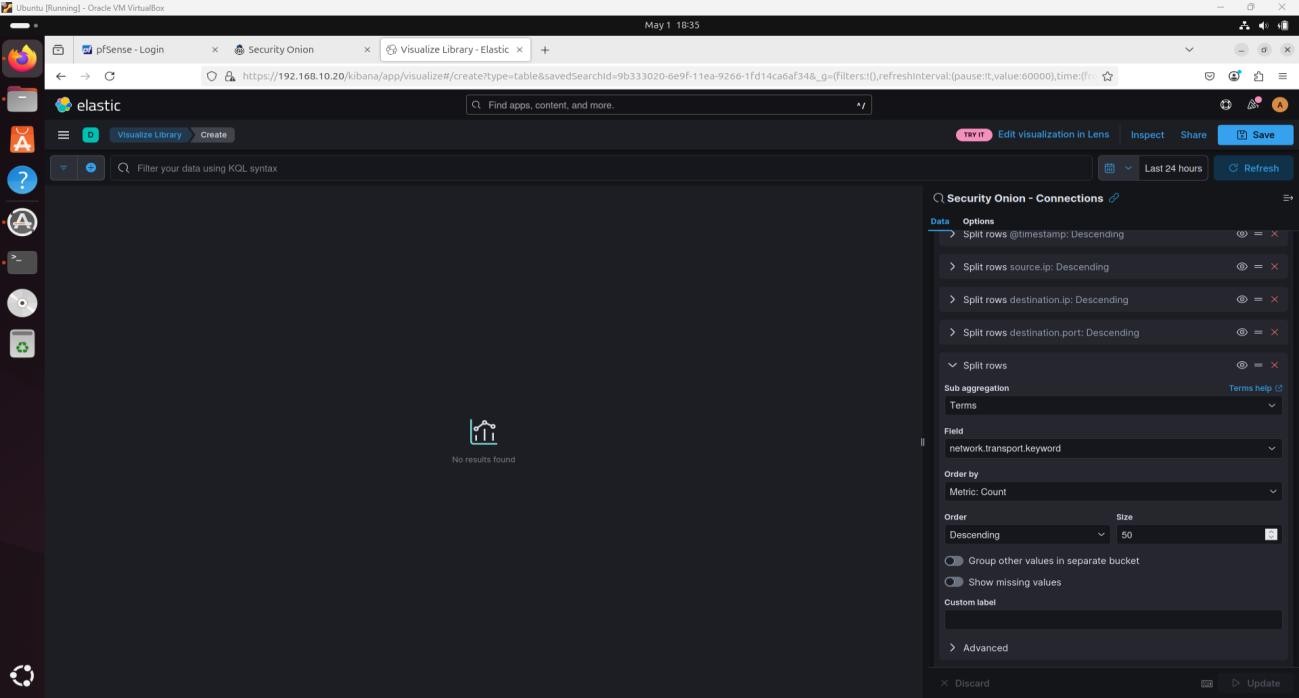


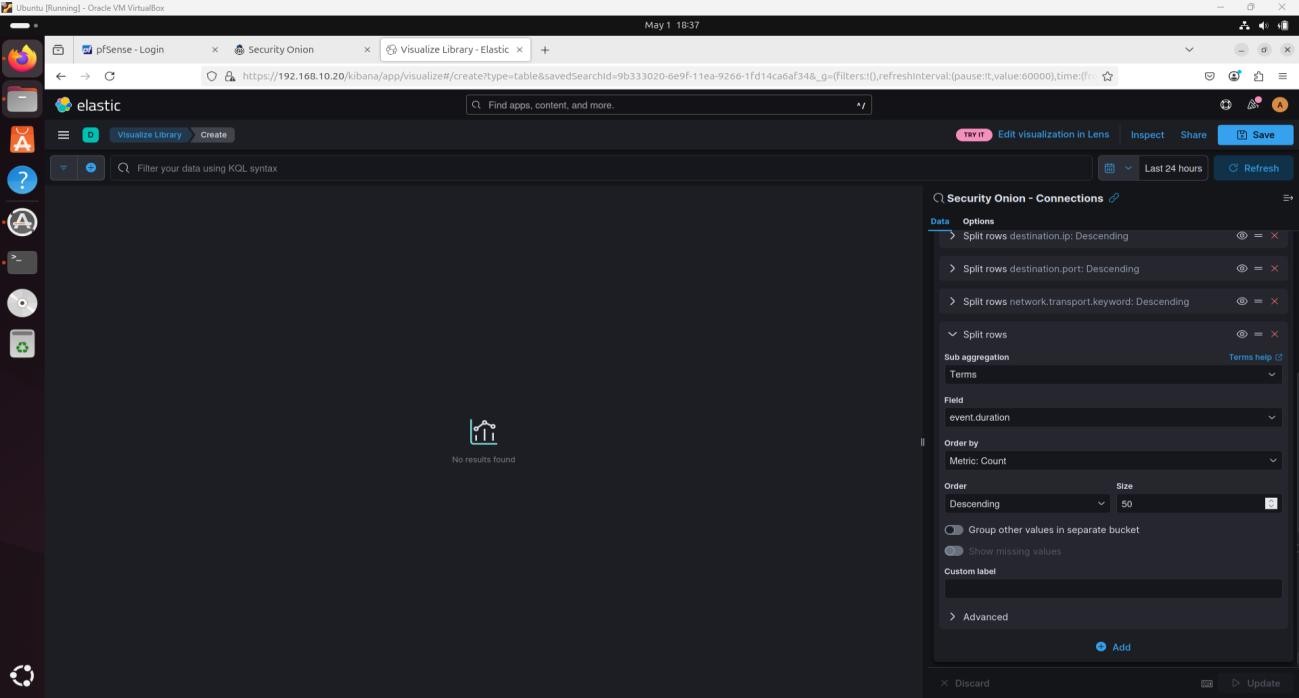


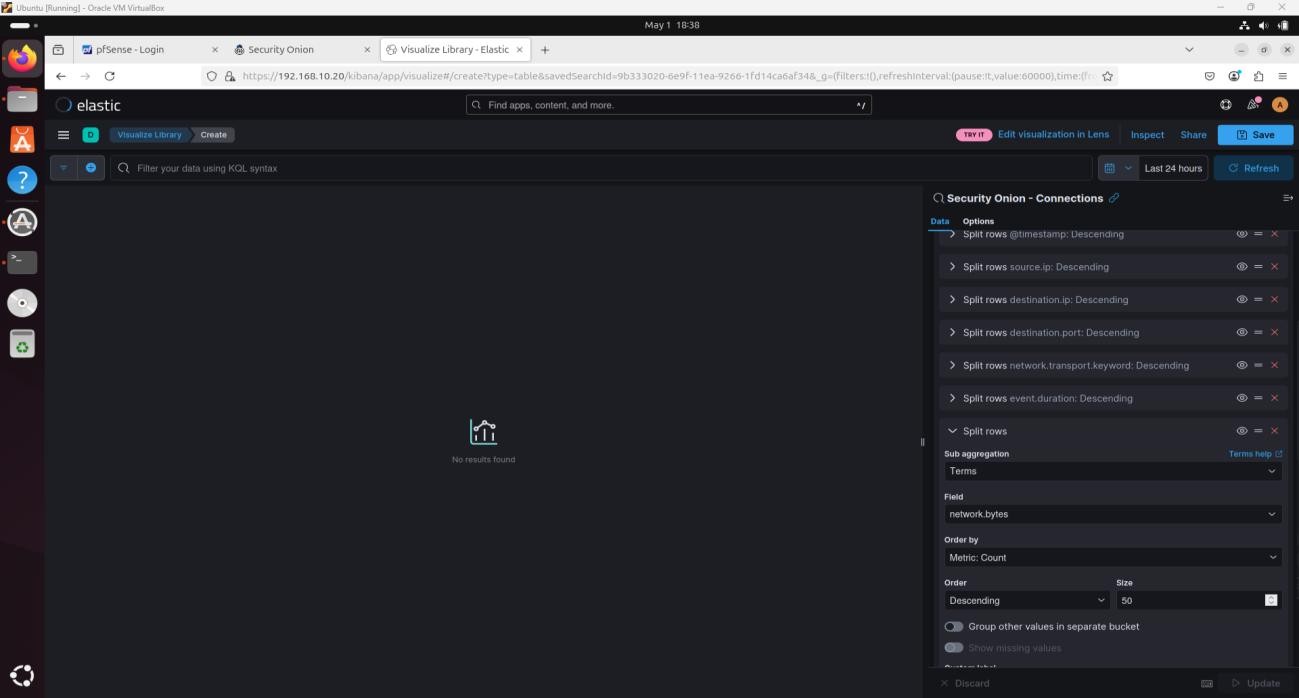
****

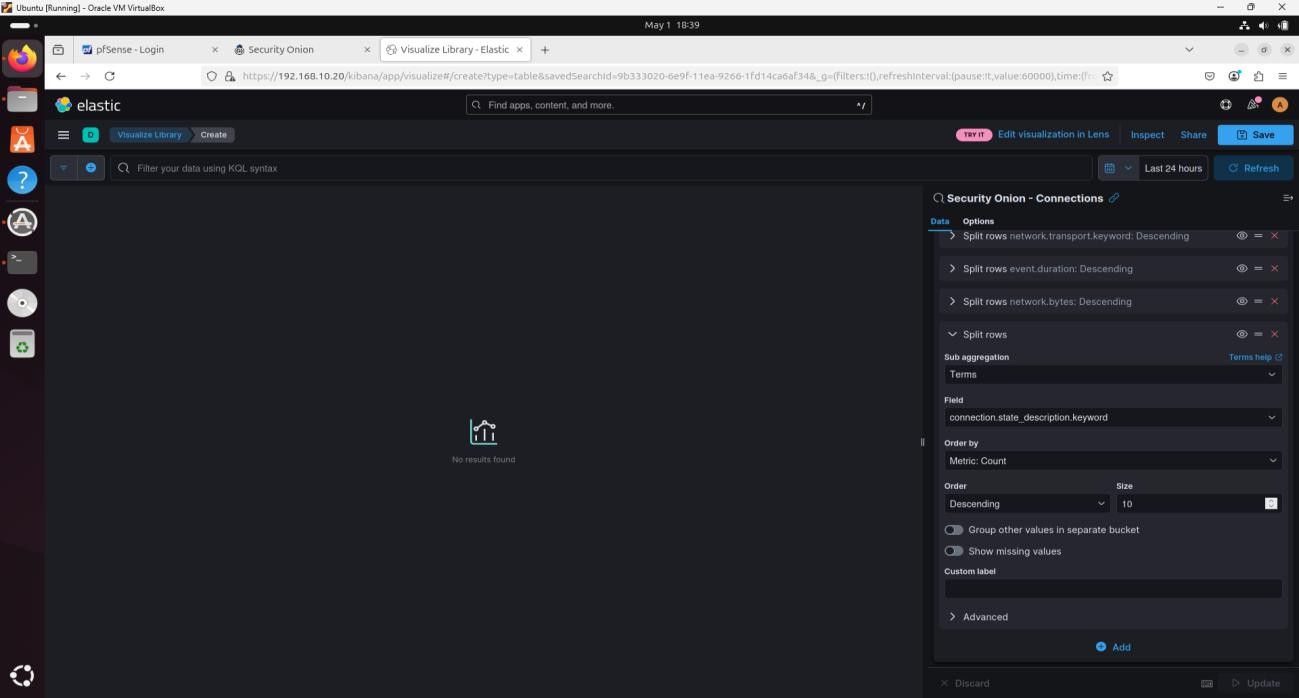


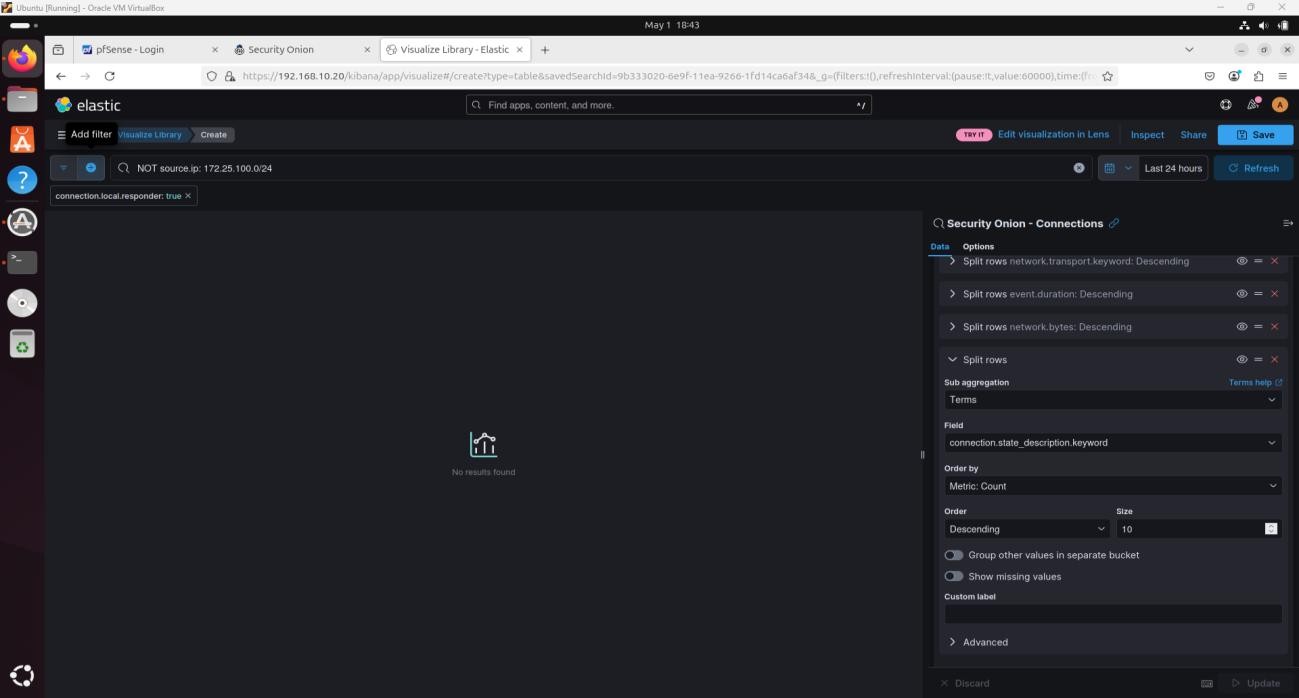








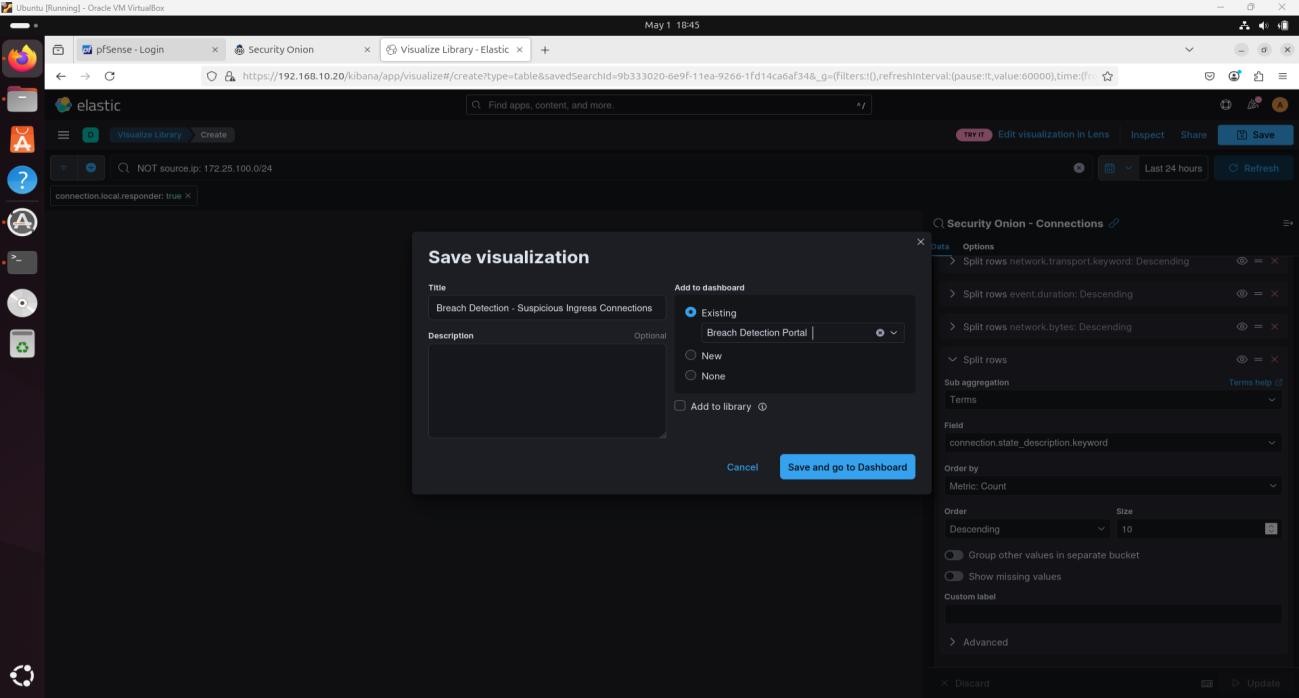




I applied filters: NOT source.ip: 172.25.100.0/24 and connection.local.responder: true.

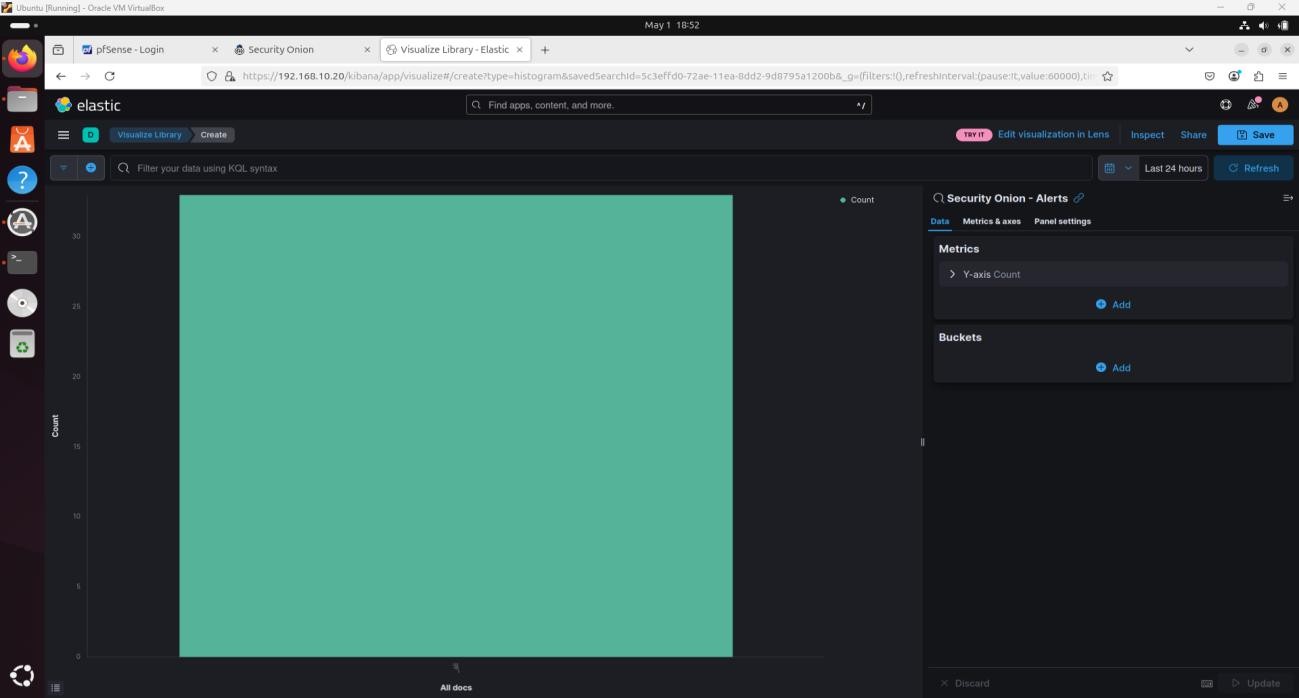
I sorted by Duration (descending).

I saved the widget as "Breach Detection – Suspicious Ingress Connections."

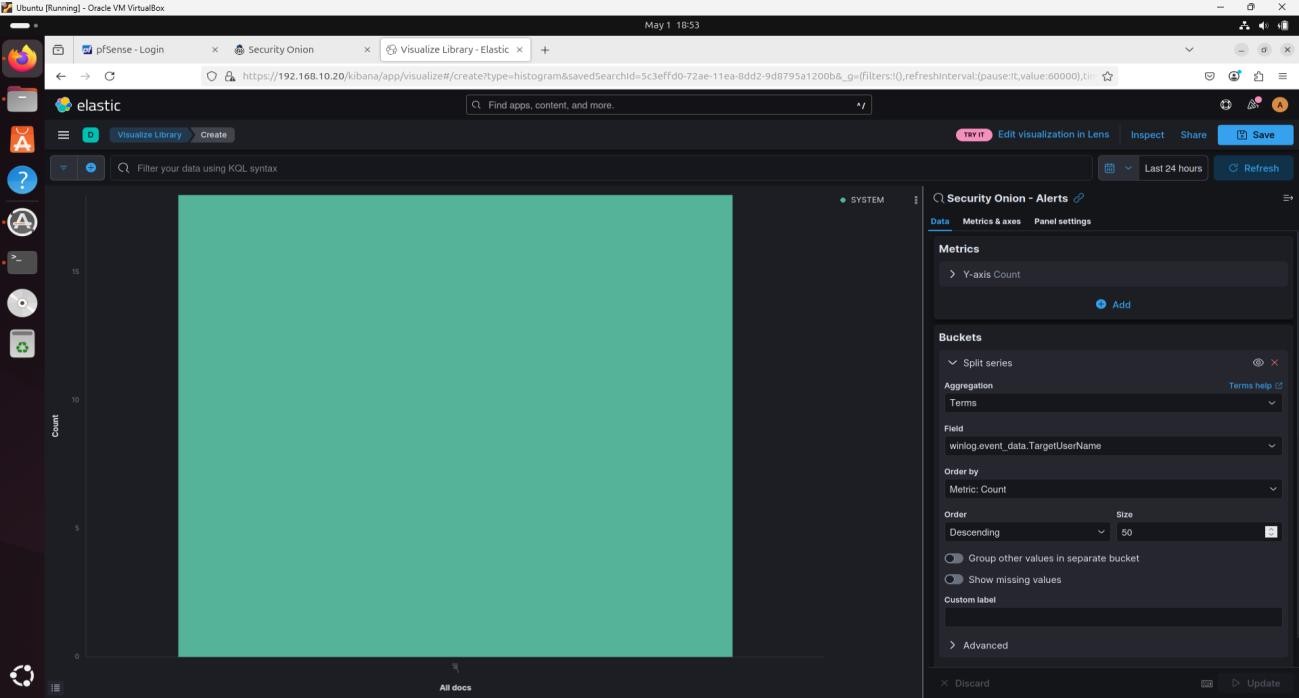


**Failed User Login Attempts**

I added a Vertical Bar visualization.

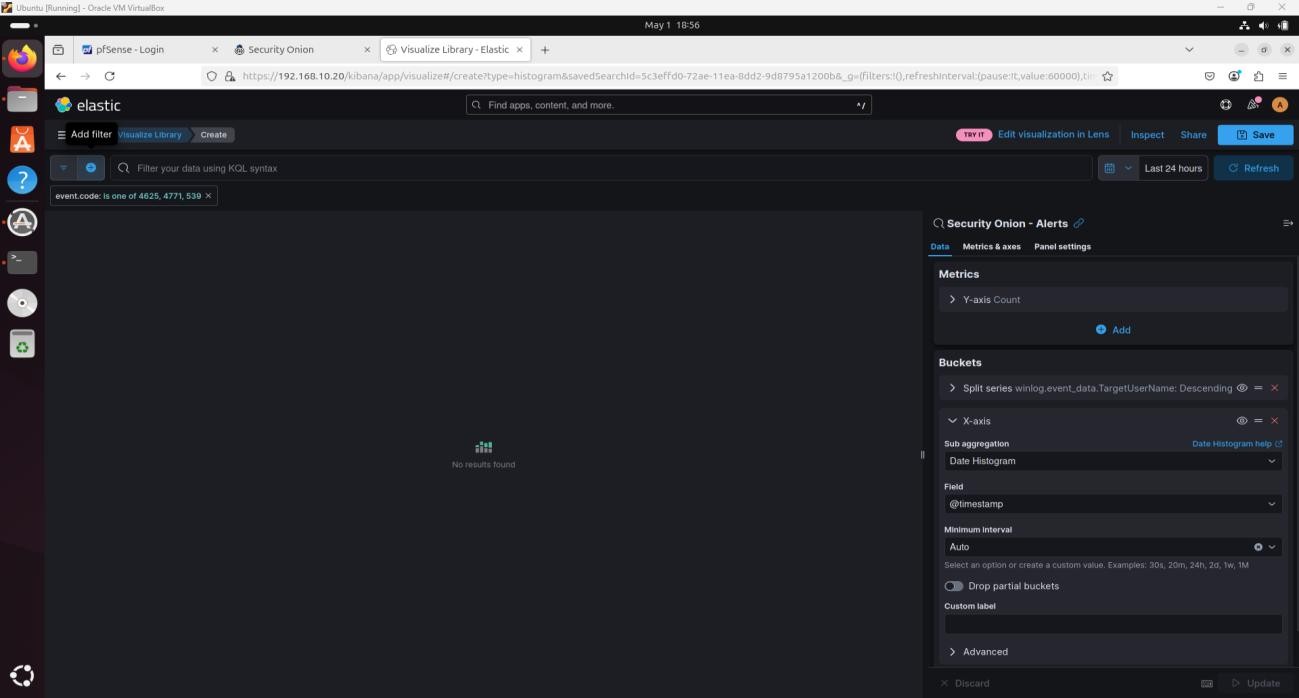


I used winlog.event\_data.targetUserName.keyword for the split series.

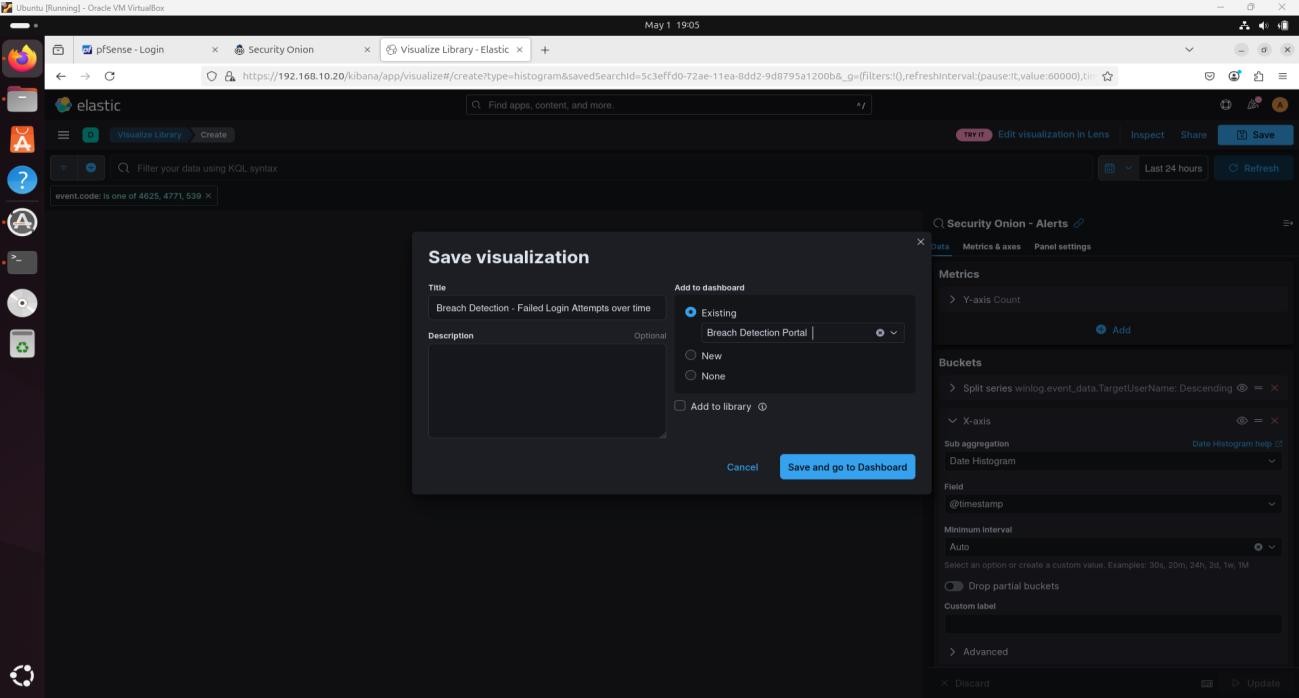


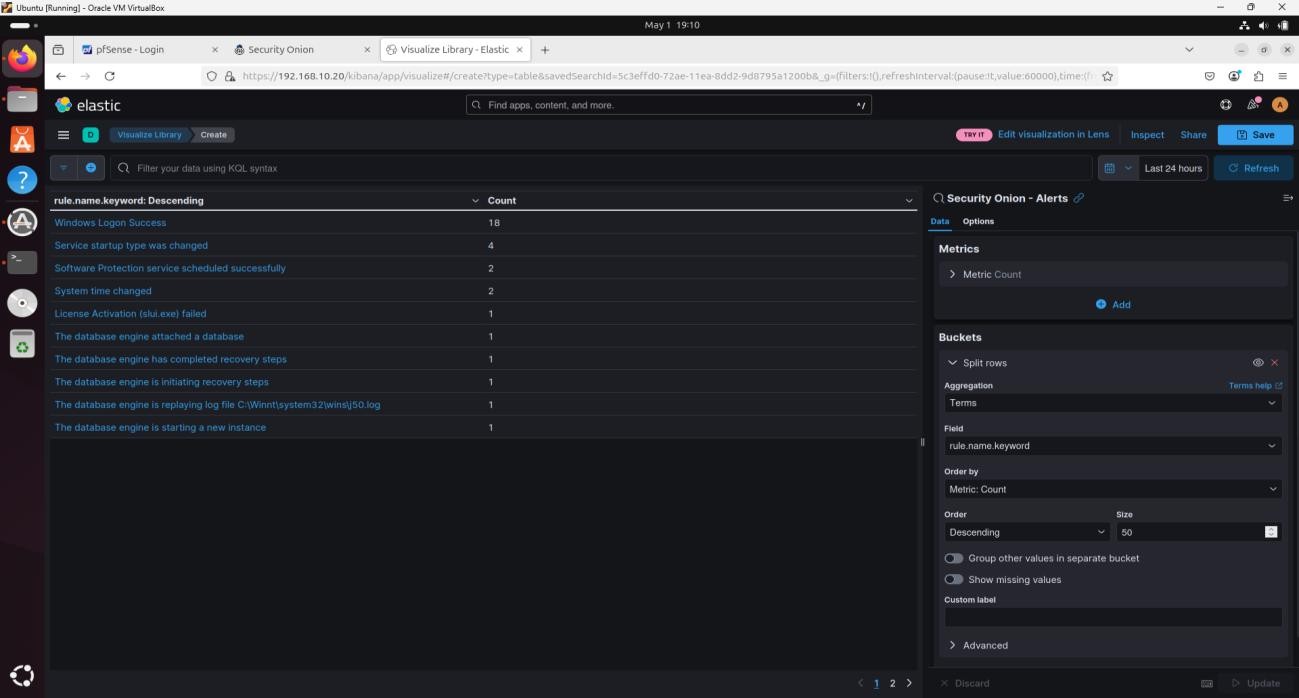
I added a Date Histogram as the X-axis.

I filtered by event codes 4625, 4771, and 539.



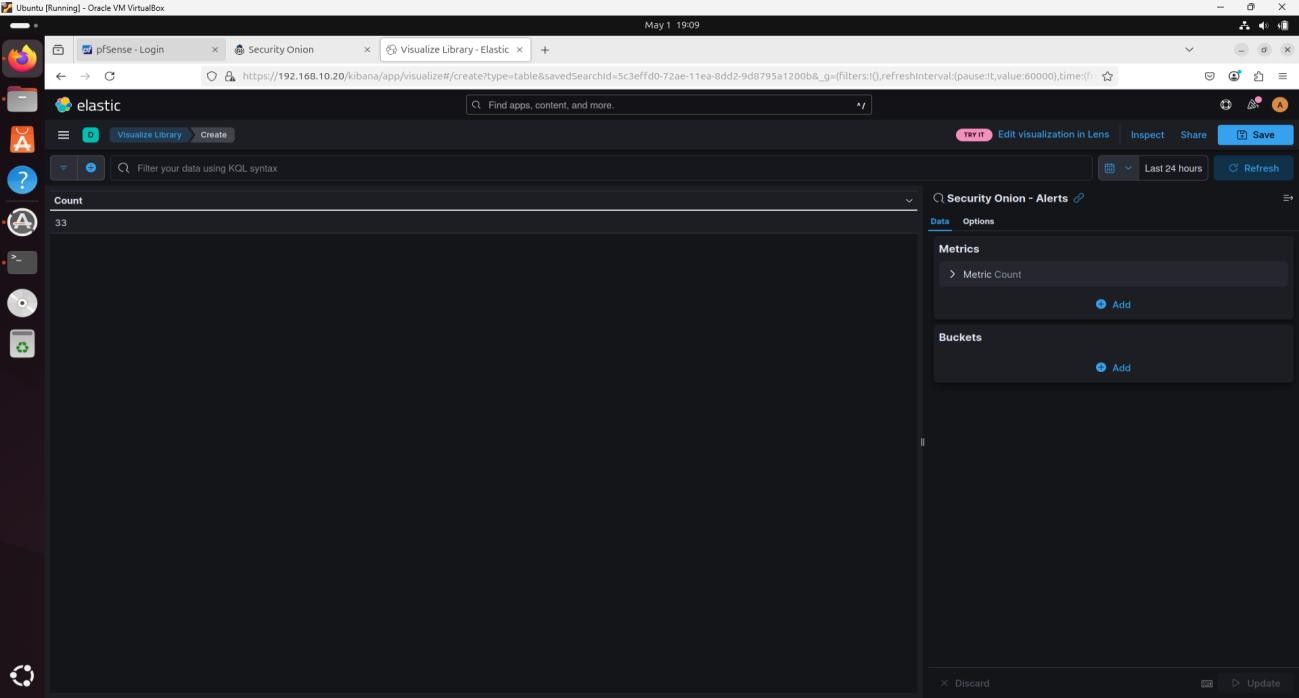
I saved the visualization as "Breach Detection – Failed Login Attempts Over Time."



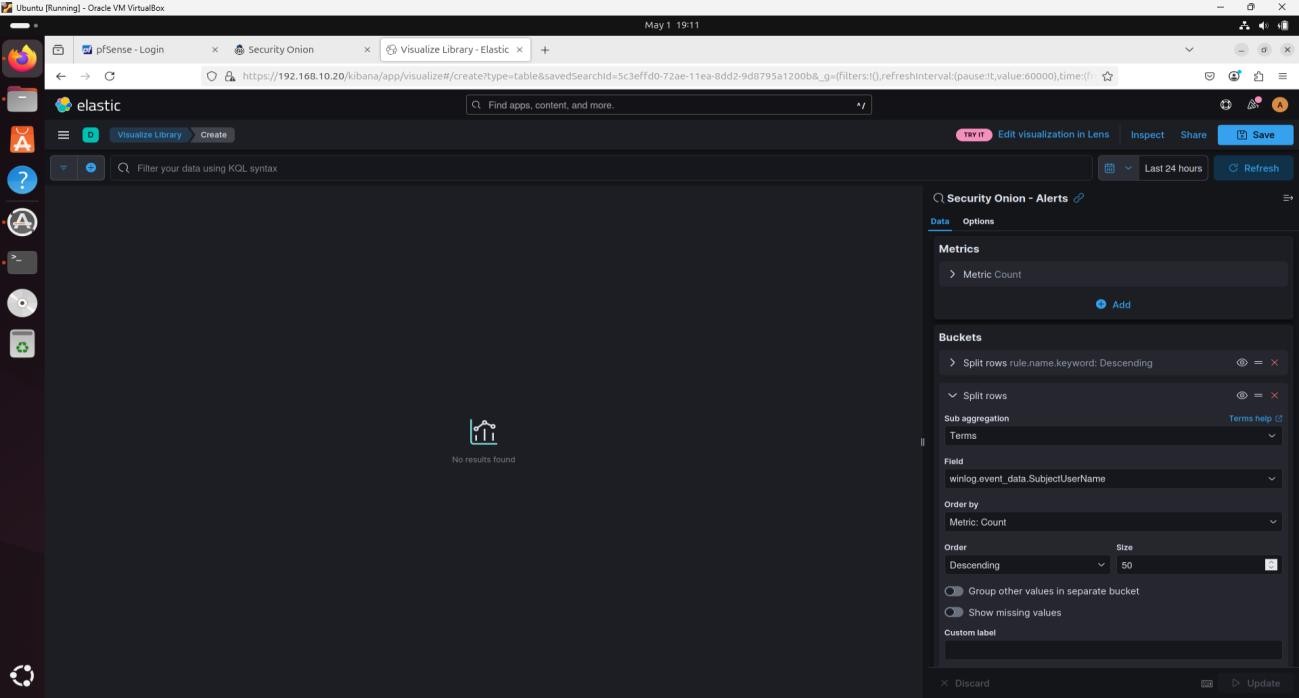


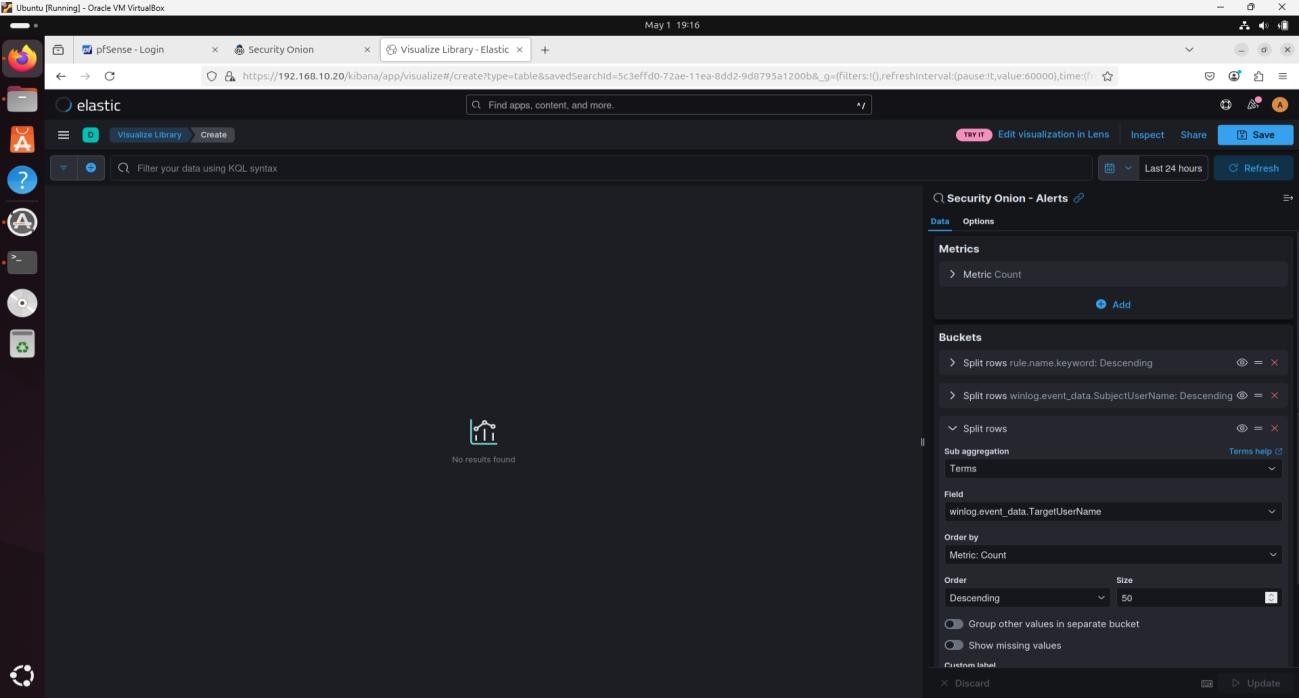
**New User Creation and Changes**

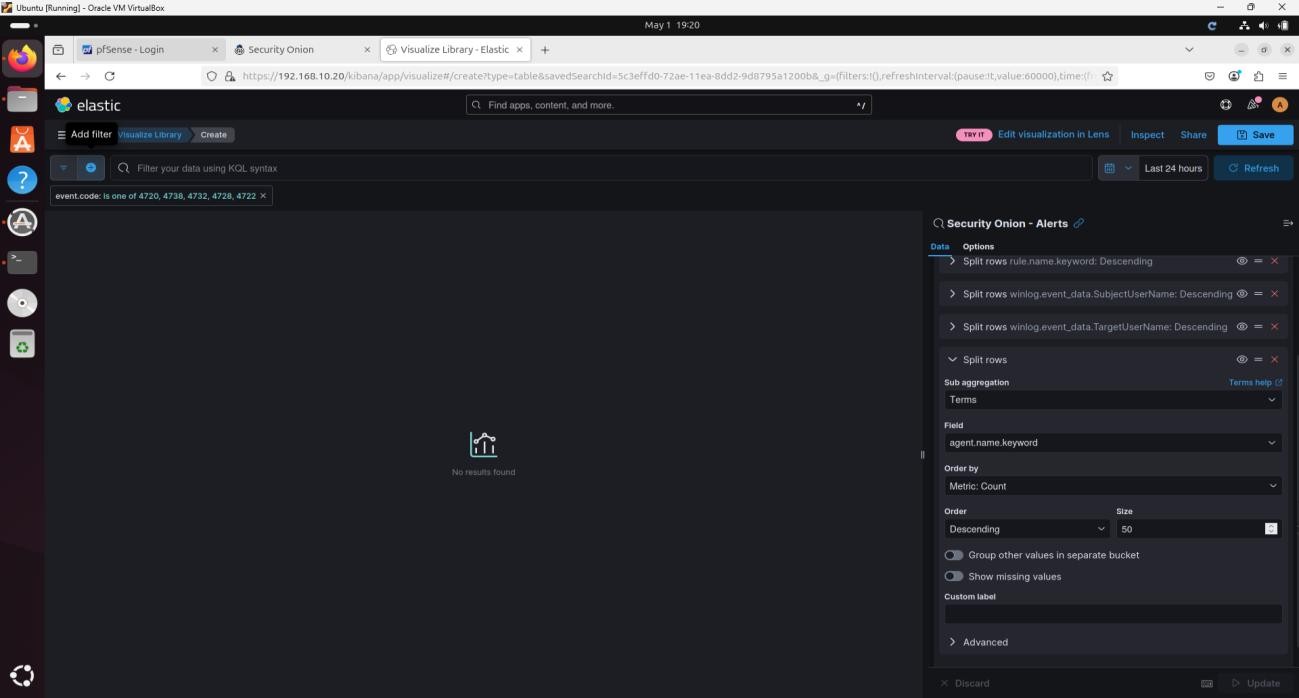
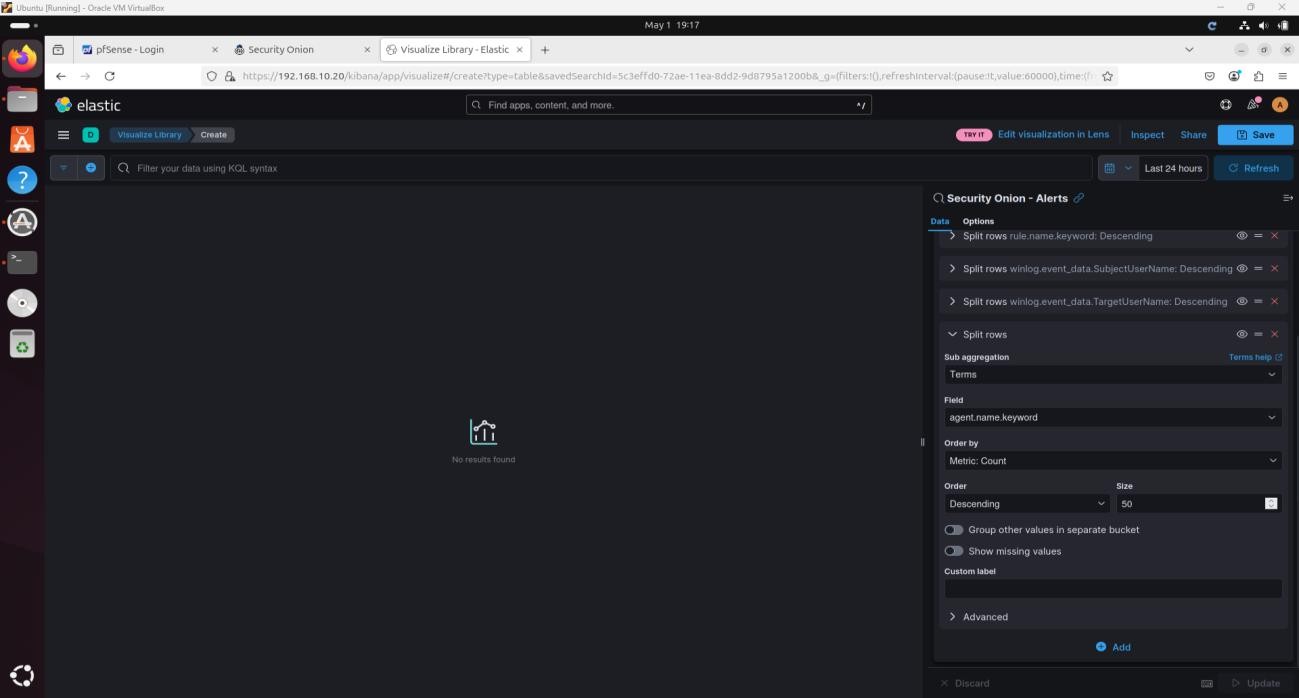
I created a Data Table with the Alerts data source.



I split rows by: rule.name.keyword, winlog.event\_data.subjectUserName.keyword, winlog.event\_data.targetUserName.keyword, and agent.name.keyword.



****



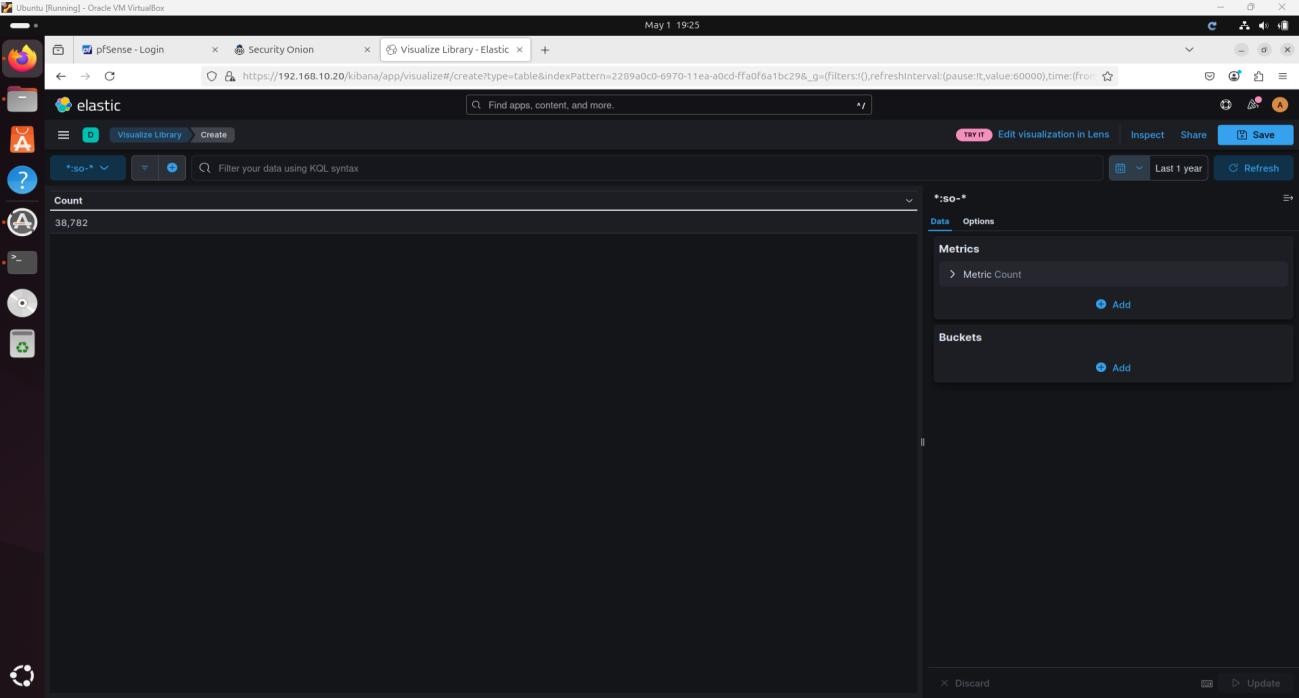
I applied a filter for event codes: 4720, 4738, 4732, 4728, and 4722.

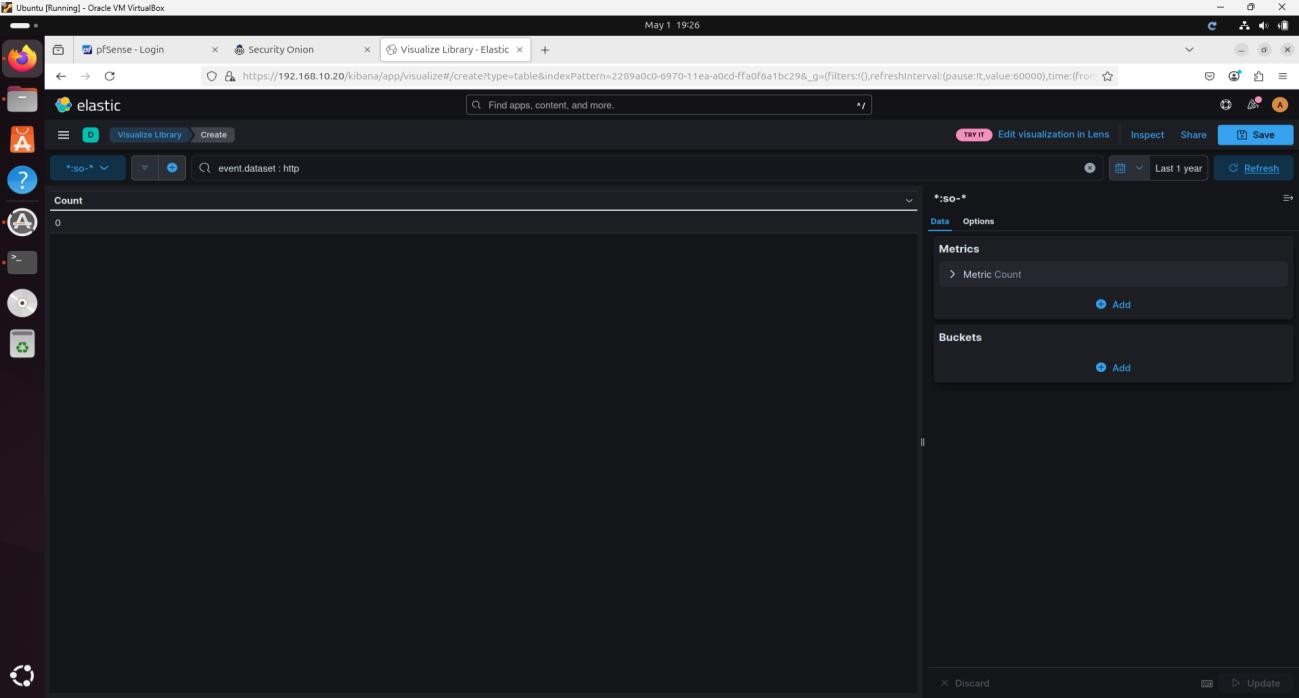
I saved the widget as "Breach Detection – User Account Alerts Summary."



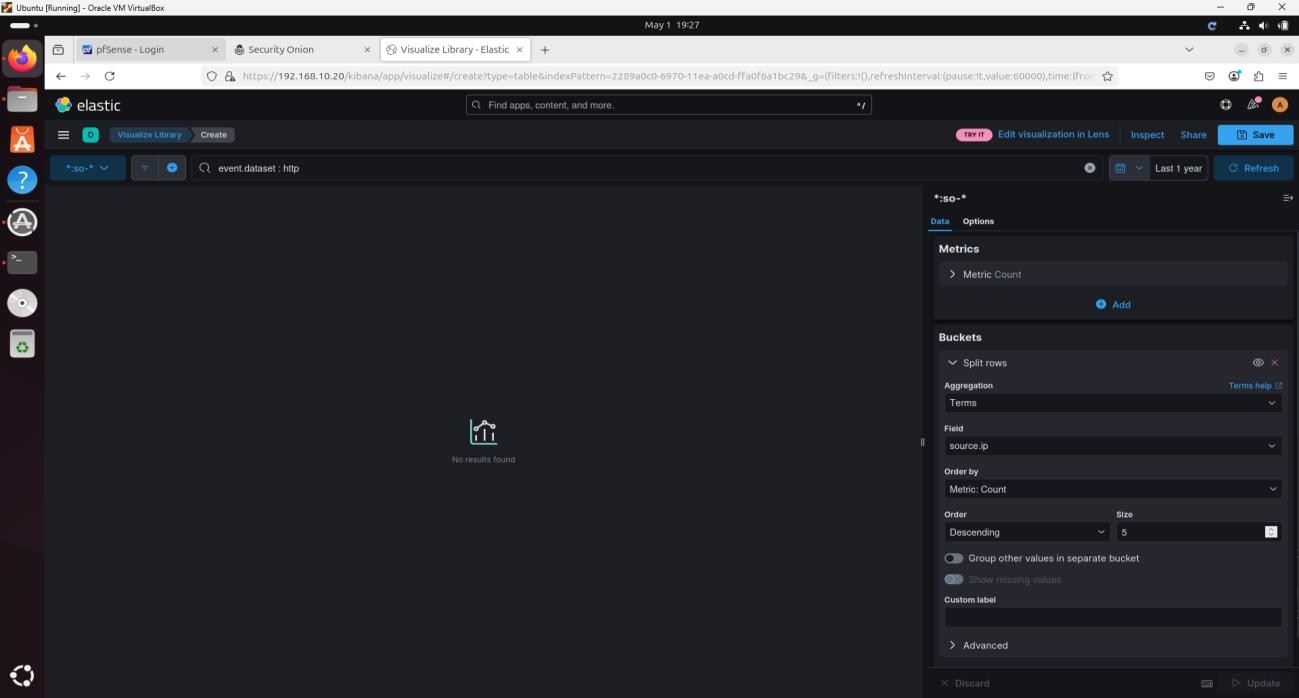
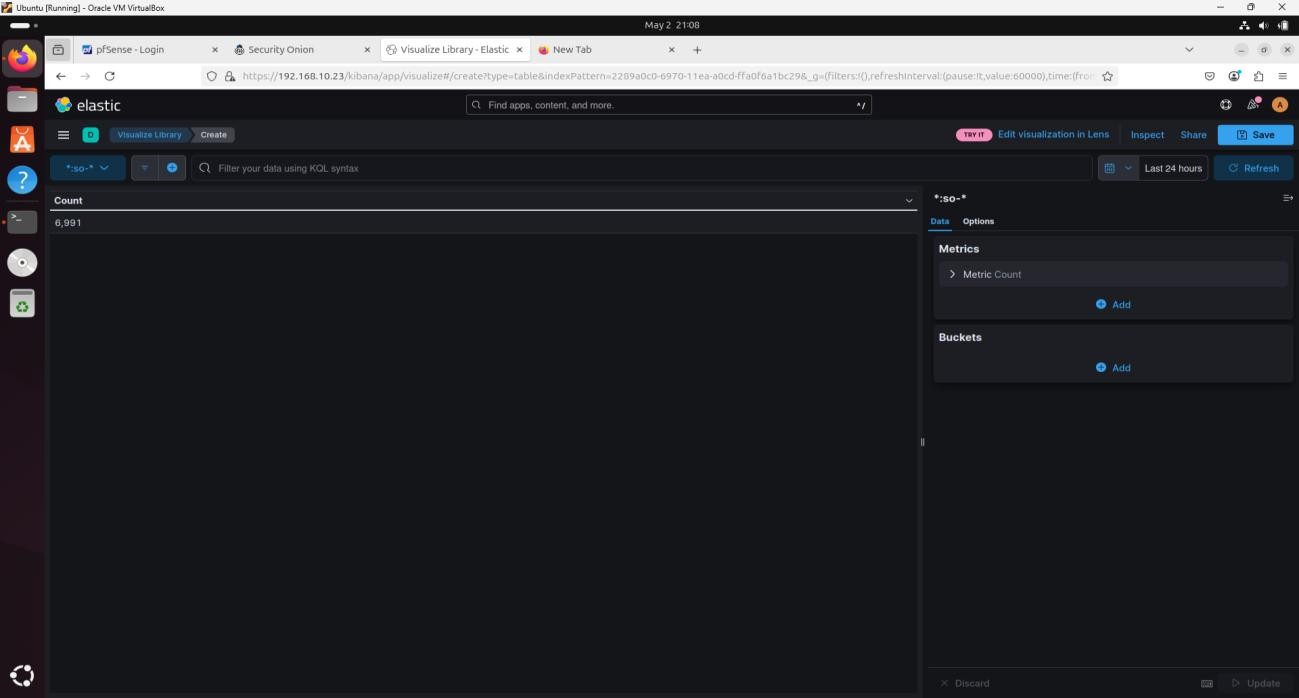
**Downloaded Executable Files**

I added a Data Table using :so- data source.

I filtered for event.dataset:http.



I split rows by: source.ip, http.virtual\_host.keyword, http.uri.keyword, and http.user\_agent.keyword.



I searched for file extensions like .exe, .bat, .cmd.

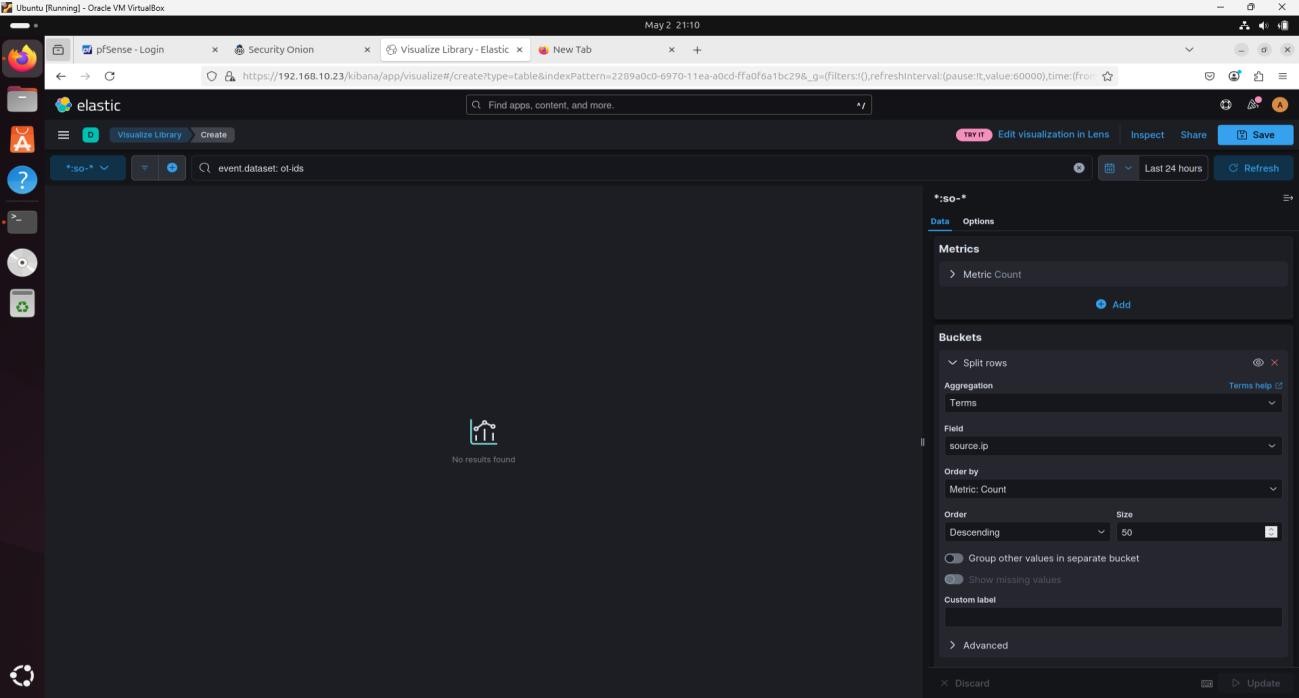
I saved it as "Breach Detection – Download of Executable Files."

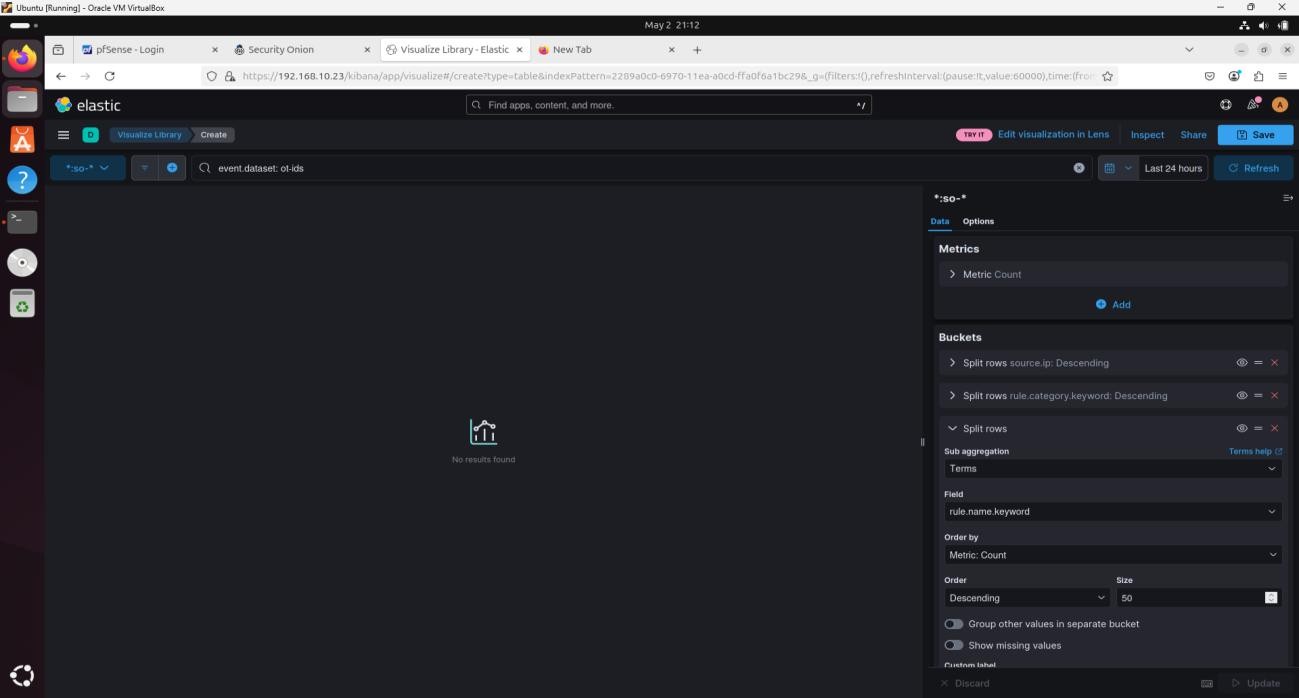
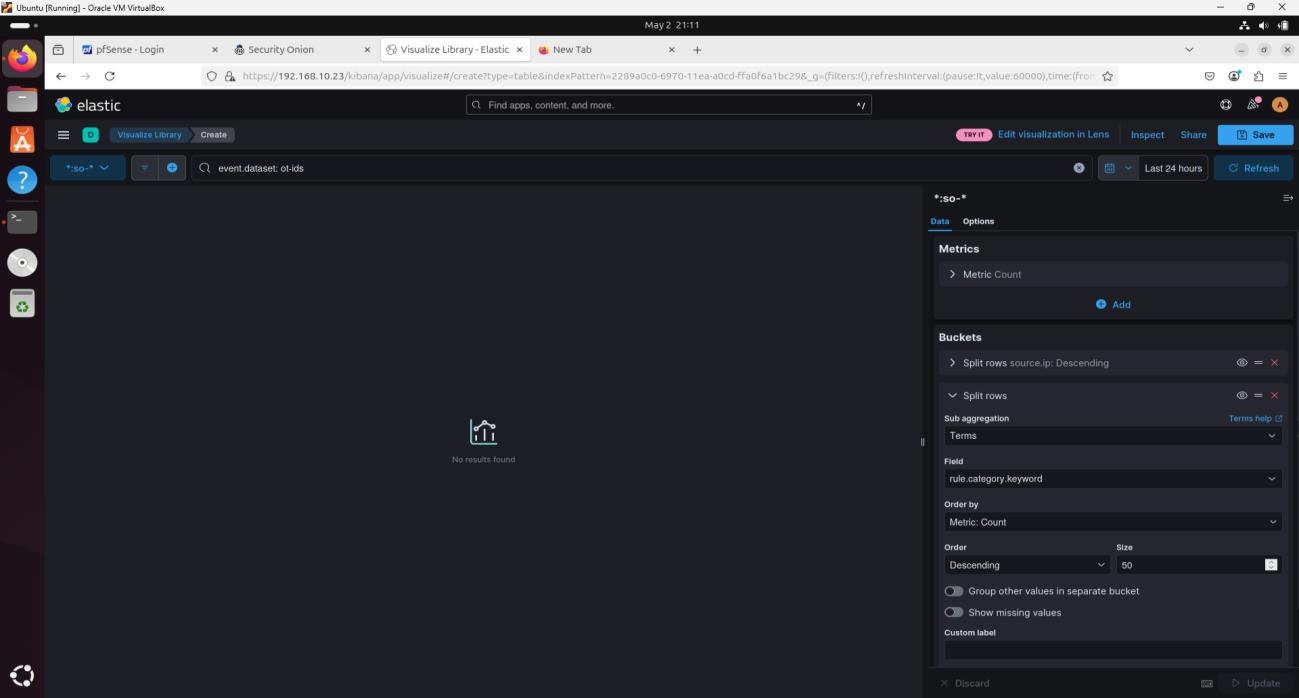
**SilentDefense Alerts**

I created a Data Table using :so- as the source.

I filtered for event.dataset:ot-ids.****

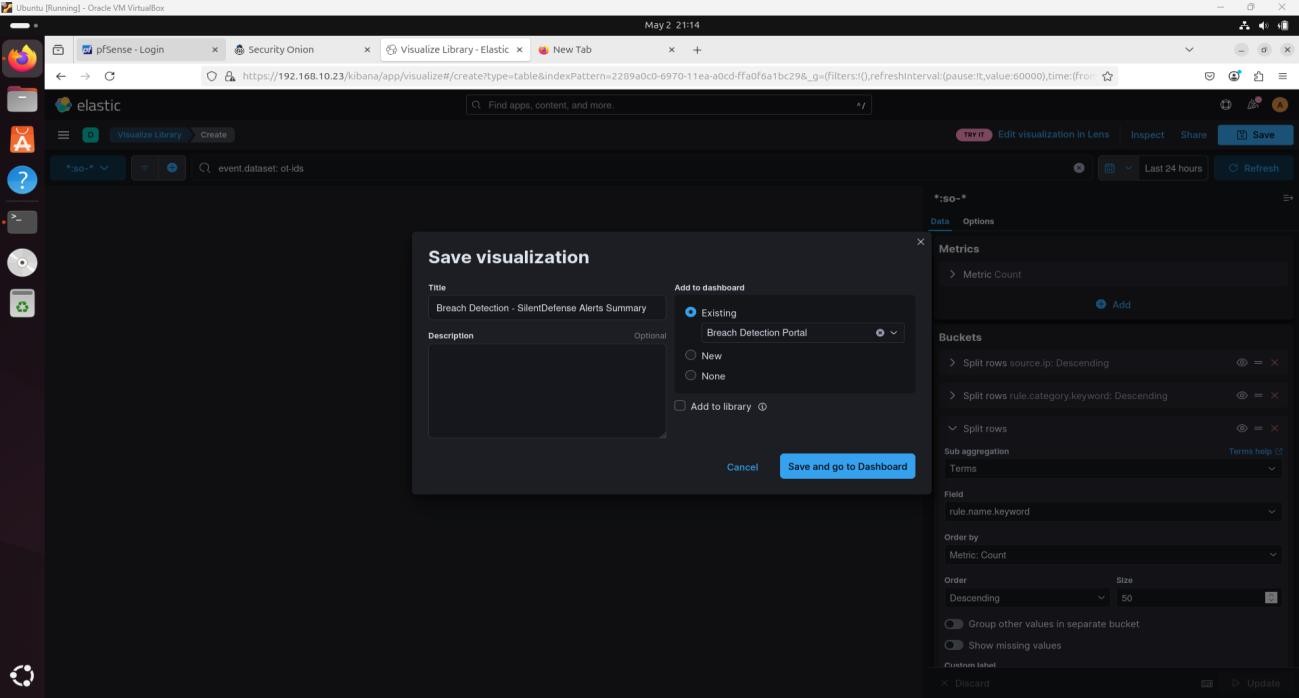
I split rows by: source.ip, rule.category.keyword, and rule.name.keyword.



****

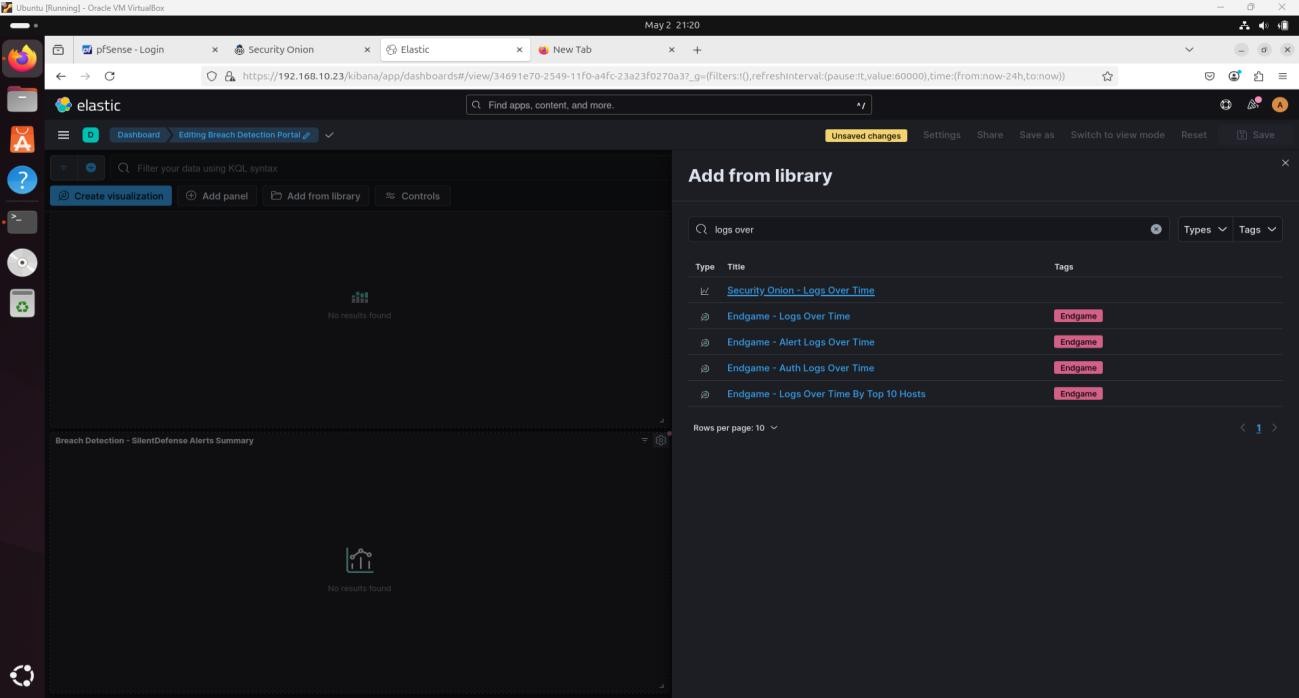
I filtered out noisy categories like NameResolution.

I saved the widget as "Breach Detection – SilentDefense Alerts Summary."

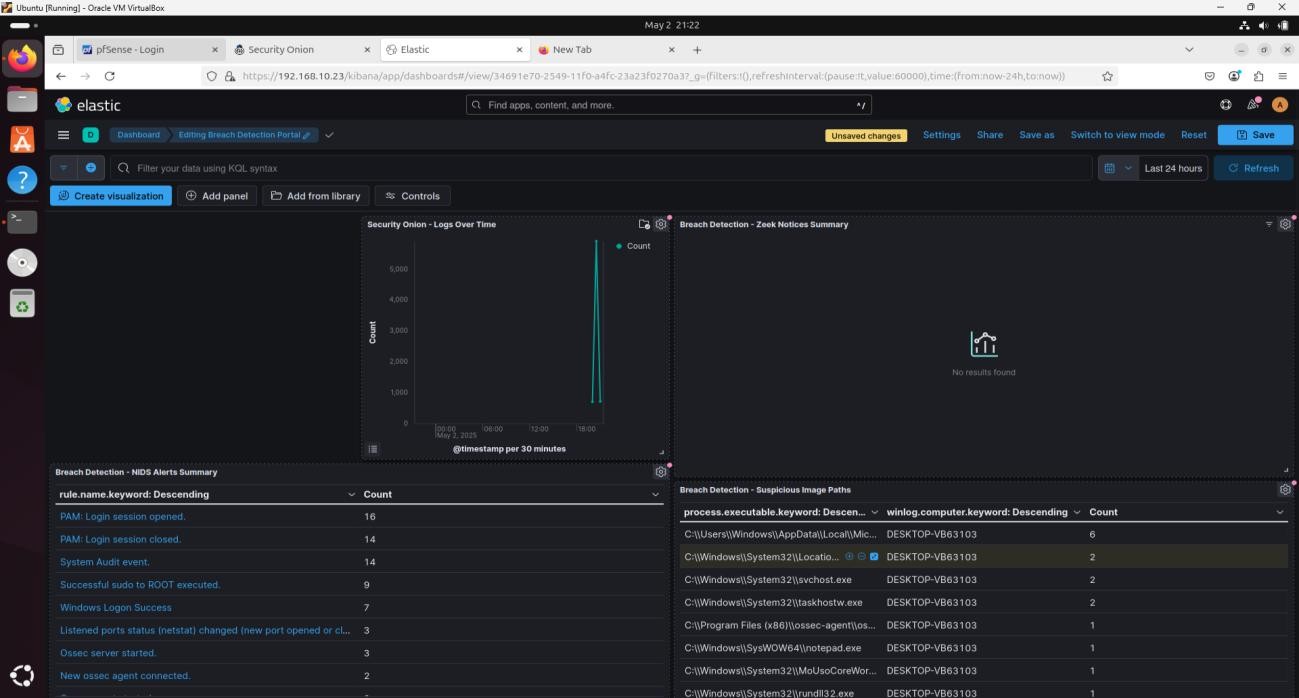
****

**Finishing the Dashboard**

I added the "Logs Over Time" bar graph from Security Onion.



I placed it at the top of the dashboard.



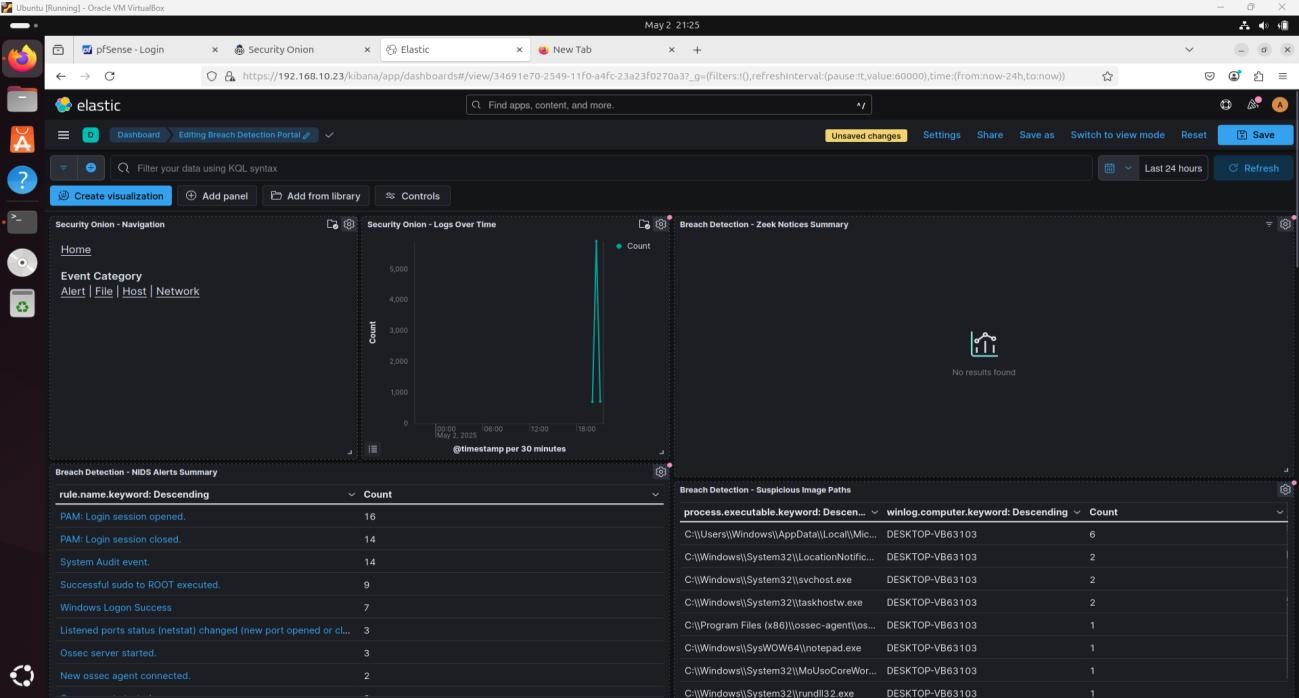
I added the Security Onion – Navigation panel and placed it on the left.

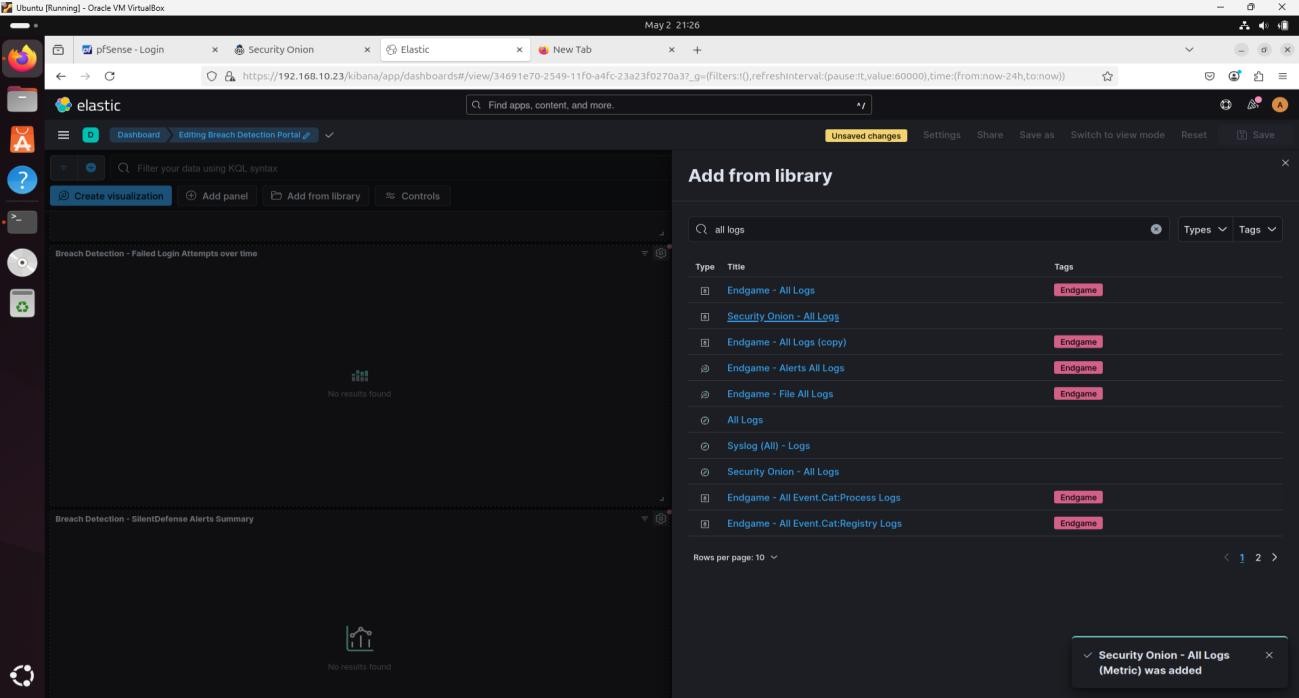
I included the "All Logs" view at the bottom of the dashboard.

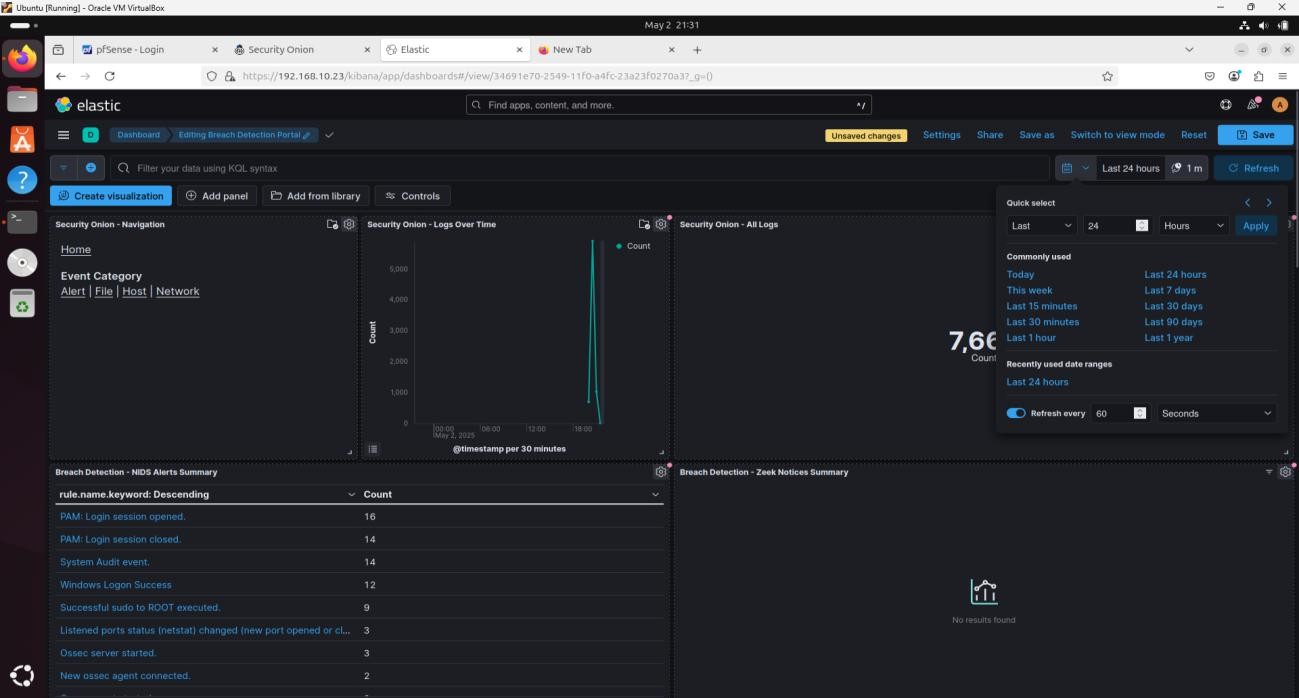
I adjusted the layout of widgets for readability.

I set the dashboard time range to 24 hours and enabled auto-refresh every minute.







++

This completed my breach detection dashboard. It provided a real-time, interactive overview of my environment’s security posture. When I observed anomalies like recurring alerts or IP addresses, I used the filter tools to investigate them further using the widgets and log viewer.

