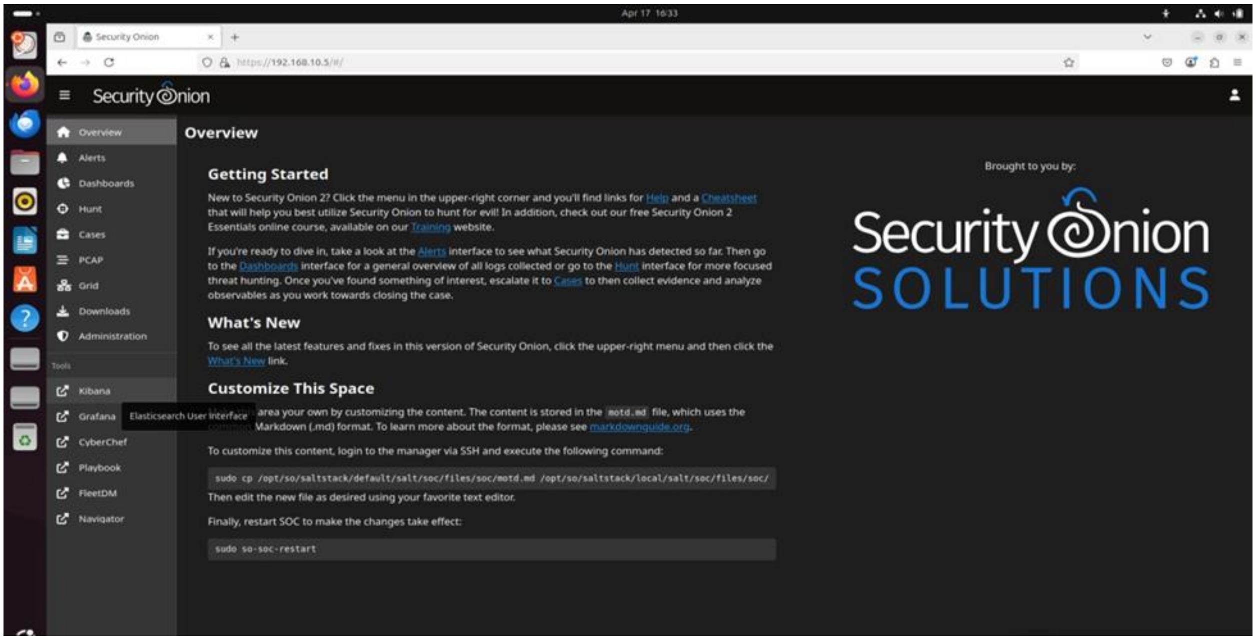
BFOR 650 – LAB REPORT 7 :- Creating a pfsense Firewall event dashboard in Kibana

Name: Phanindhar Reddy Karnati
ID: 001667635

I. In the VM, I logged in to security Onion and open the Kibana tool from the left side selection panel.



Overview

Getting Started

New to Security Onion 2? Click the menu in the upper-right corner and you'll find links for Help and a Cheatsheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion 2 Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. Then go to the Dashboards interface for a general overview of all logs collected or go to the Hunt interface for more focused threat hunting. Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Customize This Space

area your own by customizing the content. The content is stored in the `motd.md` file, which uses the Markdown (.md) format. To learn more about the format, please see markdownguide.org.

To customize this content, login to the manager via SSH and execute the following command:

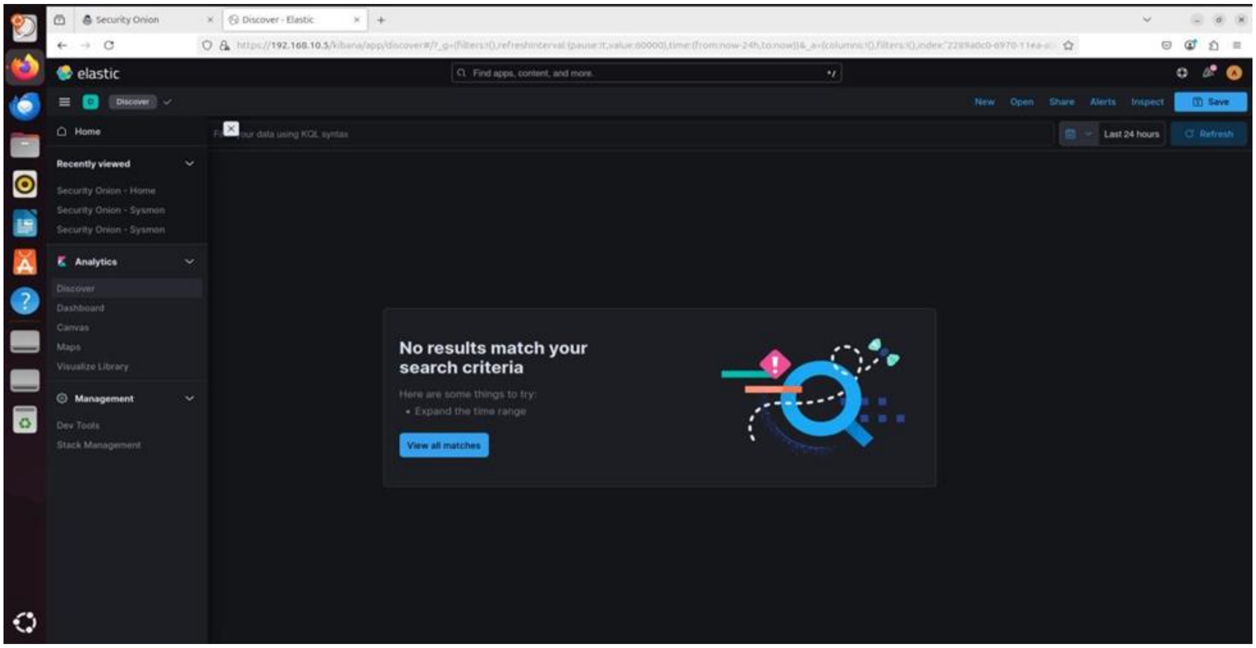
```
sudo cp /opt/so/saltstack/default/salt/soc/files/soc/motd.md /opt/so/saltstack/local/salt/soc/files/soc/
```

Then edit the new file as desired using your favorite text editor.

Finally, restart SOC to make the changes take effect:

```
sudo so-soc-restart
```

II. Once Kibana opened in a new tab, I clicked the hamburger icon at the top-left and navigated to the Discover section. This area allowed me to search and explore event logs in detail.



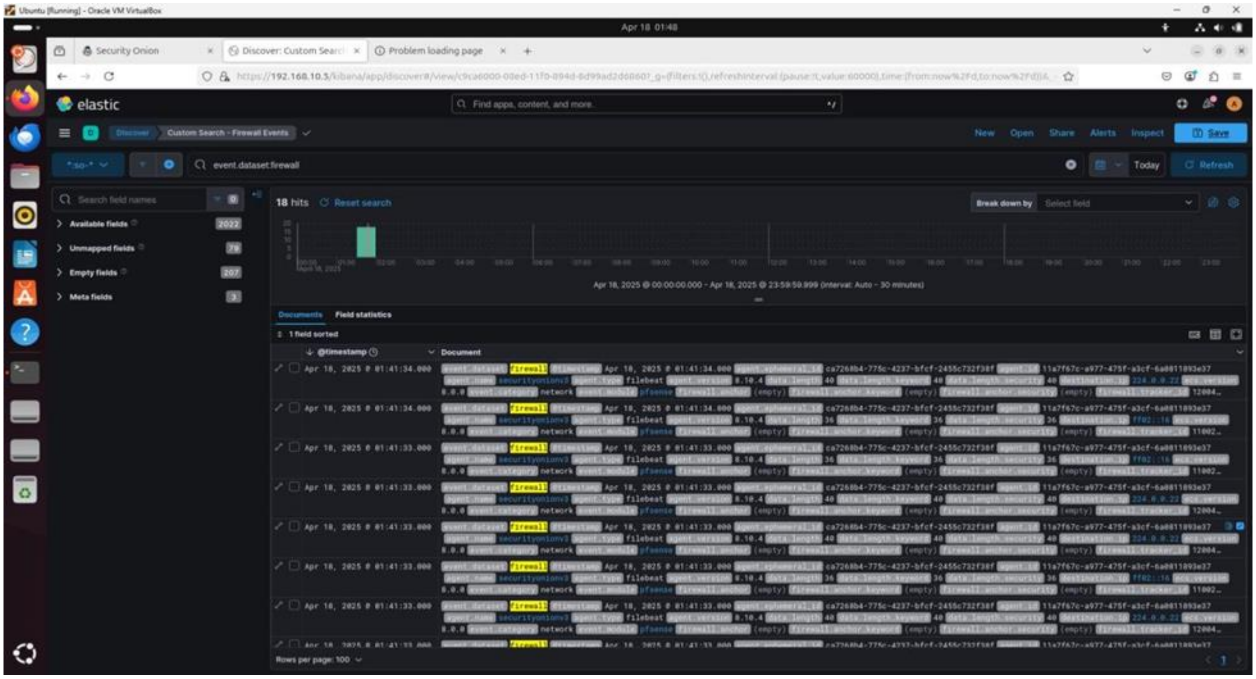
No results match your search criteria

Here are some things to try:

- Expand the time range

View all matches

III. I entered the search query event.dataset:firewall to filter events tagged by Zeek as related to firewall activity.



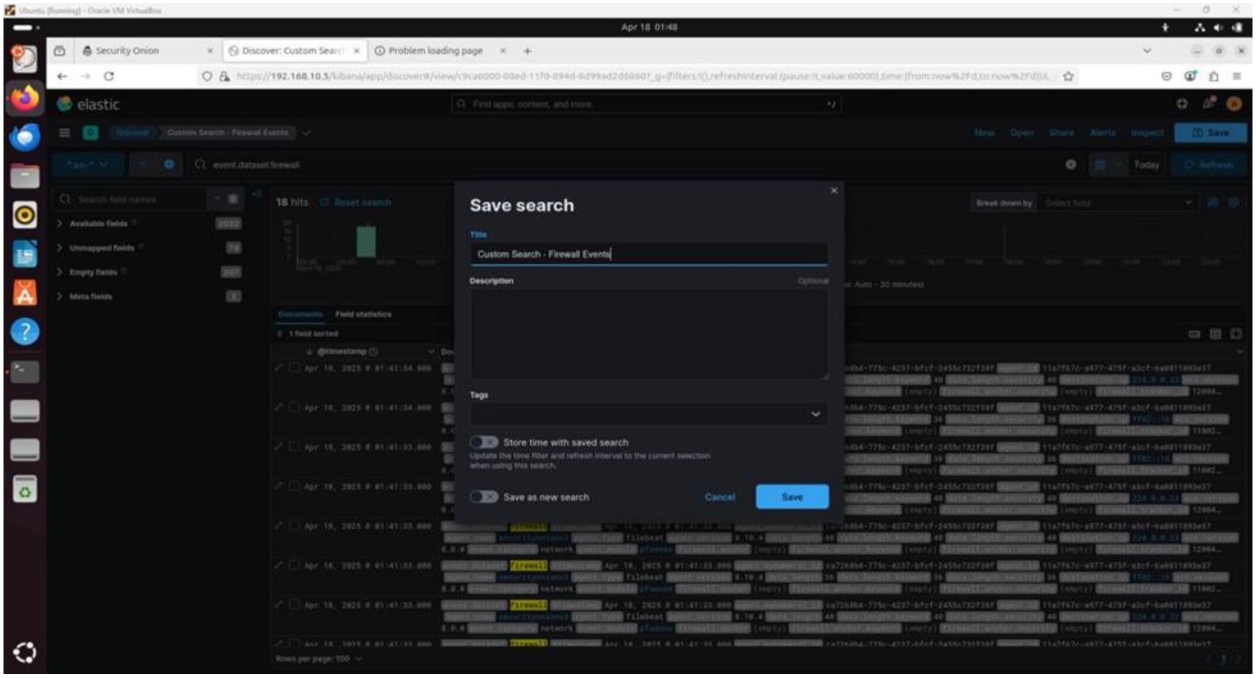
```
event.dataset:firewall
```

18 hits

Apr 18, 2025 @ 00:00:00.000 - Apr 18, 2025 @ 23:59:59.999 (interval: Auto - 30 minutes)

```
@timestamp                   Document
Apr 18, 2025 @ 01:41:34.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:34.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 40 data.length.keyword 40 data.length.security 40 destination.ip 224.0.0.22 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 12004…
Apr 18, 2025 @ 01:41:34.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:34.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 36 data.length.keyword 36 data.length.security 36 destination.ip ff02::16 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 11002…
Apr 18, 2025 @ 01:41:33.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 36 data.length.keyword 36 data.length.security 36 destination.ip ff02::16 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 11002…
Apr 18, 2025 @ 01:41:33.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 40 data.length.keyword 40 data.length.security 40 destination.ip 224.0.0.22 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 12004…
Apr 18, 2025 @ 01:41:33.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 40 data.length.keyword 40 data.length.security 40 destination.ip 224.0.0.22 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 12004…
Apr 18, 2025 @ 01:41:33.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 36 data.length.keyword 36 data.length.security 36 destination.ip ff02::16 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 11002…
Apr 18, 2025 @ 01:41:33.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
                             agent.name securityonionv3 agent.type filebeat agent.version 8.10.4 data.length 40 data.length.keyword 40 data.length.security 40 destination.ip 224.0.0.22 ecs.version
                             8.0.0 event.category network event.module pfsense firewall.anchor (empty) firewall.anchor.keyword (empty) firewall.anchor.security (empty) firewall.tracker_id 12004…
Apr 18, 2025 @ 01:41:33.000  event.dataset firewall @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37
```

IV. After confirming the results, I saved this search with the name Custom Search – Firewall Event using the Save option in the top-right corner.



Save search

Title: Custom Search - Firewall Events

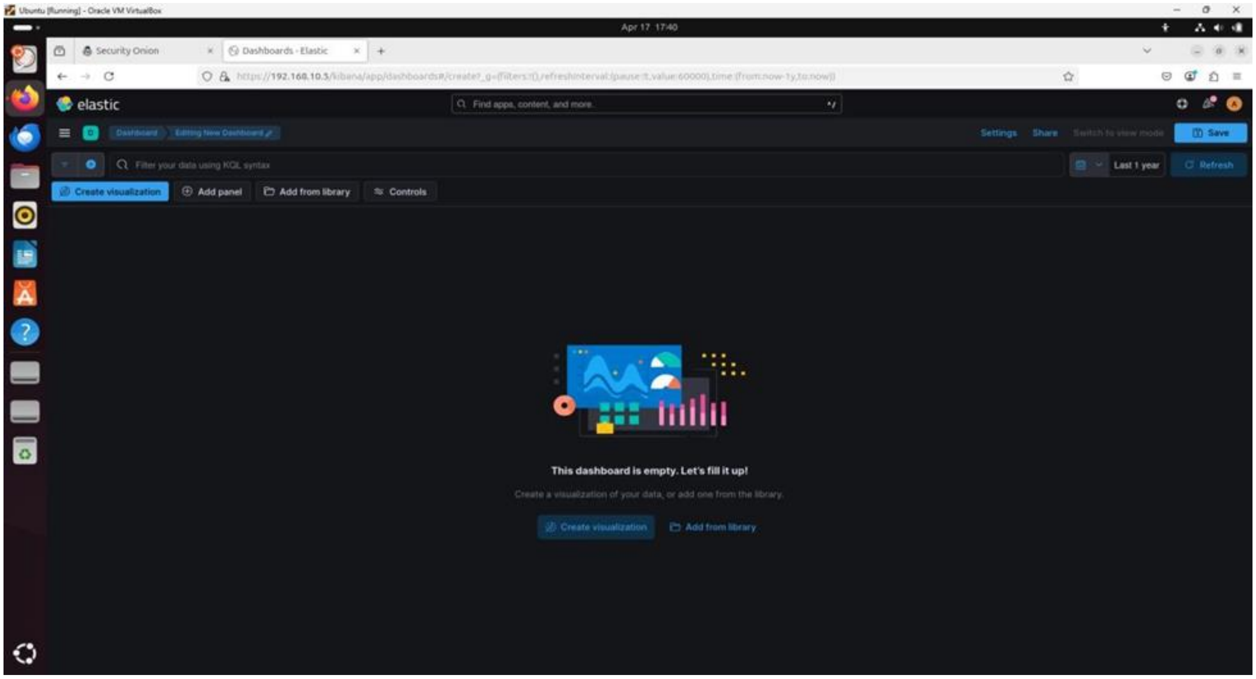
Description: Optional

Tags

Store time with saved search
Update the time filter and refresh interval to the current selection when using this search.

Save as new search

V. Returning to the Kibana menu, I selected Dashboard, then clicked Create dashboard, which opened a blank dashboard editing space.



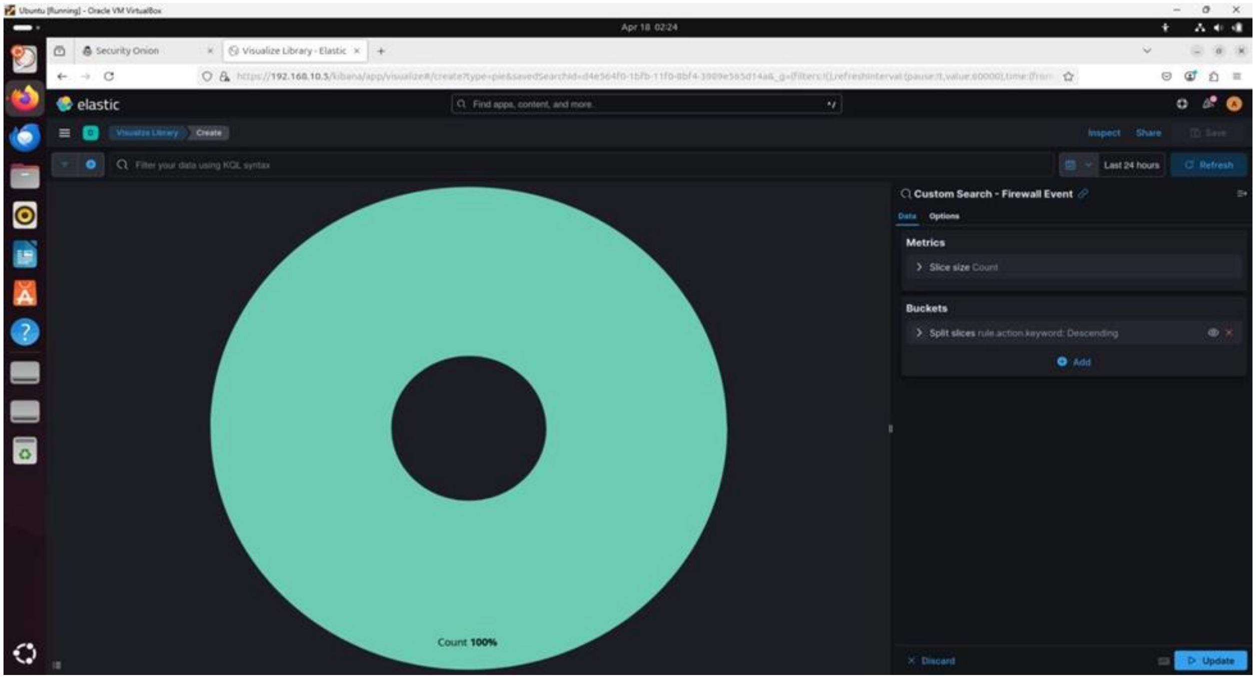
This dashboard is empty. Let's fill it up!

Create a visualization of your data, or add one from the library.

Ubuntu [Running] - Oracle VM VirtualBox
Apr 17 17:40
Security Onion
Dashboards - Elastic
https://192.168.10.5/kibana/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-1y,to:now))
elastic
Find apps, content, and more
Dashboard
Editing New Dashboard
Settings
Share
Switch to view mode
Save
Filter your data using KQL syntax
Last 1 year
Refresh
Create visualization
Add panel
Add from library
Controls
Create visualization
Add from library

VII. In the visualization settings, I added a bucket, chose Split slices, and configured it to aggregate Terms on the field rule.action.keyword. I set the order by Metric:

Count, in Descending order, and limited it to the top 50 results. After updating, I saved this as Firewall – Rule Action Summary.


Ubuntu [Running] - Oracle VM VirtualBox
Apr 18 02:24
Security Onion
Visualize Library - Elastic
elastic
Find apps, content, and more.
Visualize Library
Create
Inspect
Share
Save
Filter your data using KQL syntax
Last 24 hours
Refresh
Count 100%
Discard
Update

Custom Search - Firewall Event

Data Options

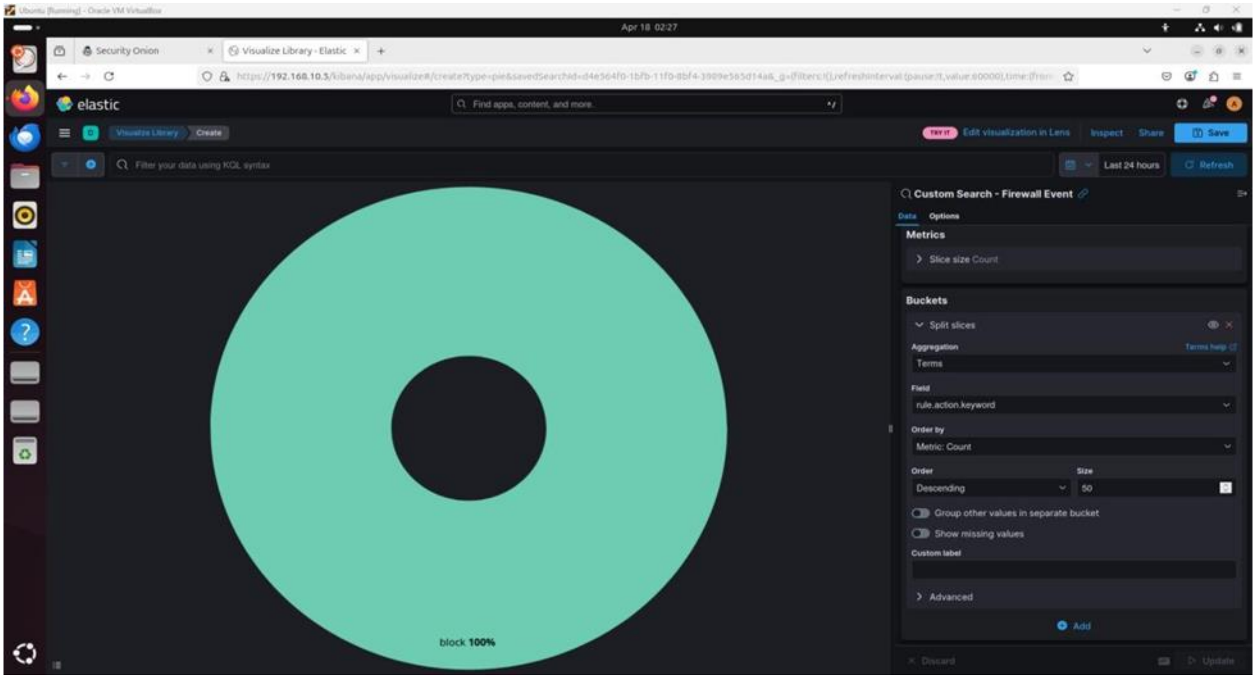
Metrics

Slice size Count

Buckets

Split slices rule.action.keyword: Descending

Add


Ubuntu [Running] - Oracle VM VirtualBox
Apr 18 02:27
Security Onion
Visualize Library - Elastic
elastic
Find apps, content, and more.
Visualize Library
Create
TRY IT
Edit visualization in Lens
Inspect
Share
Save
Filter your data using KQL syntax
Last 24 hours
Refresh
block 100%
Discard
Update

Custom Search - Firewall Event

Data Options

Metrics

Slice size Count

Buckets

Split slices

Aggregation: Terms

Field: rule.action.keyword

Order by: Metric: Count

Order: Descending

Size: 50

Group other values in separate bucket

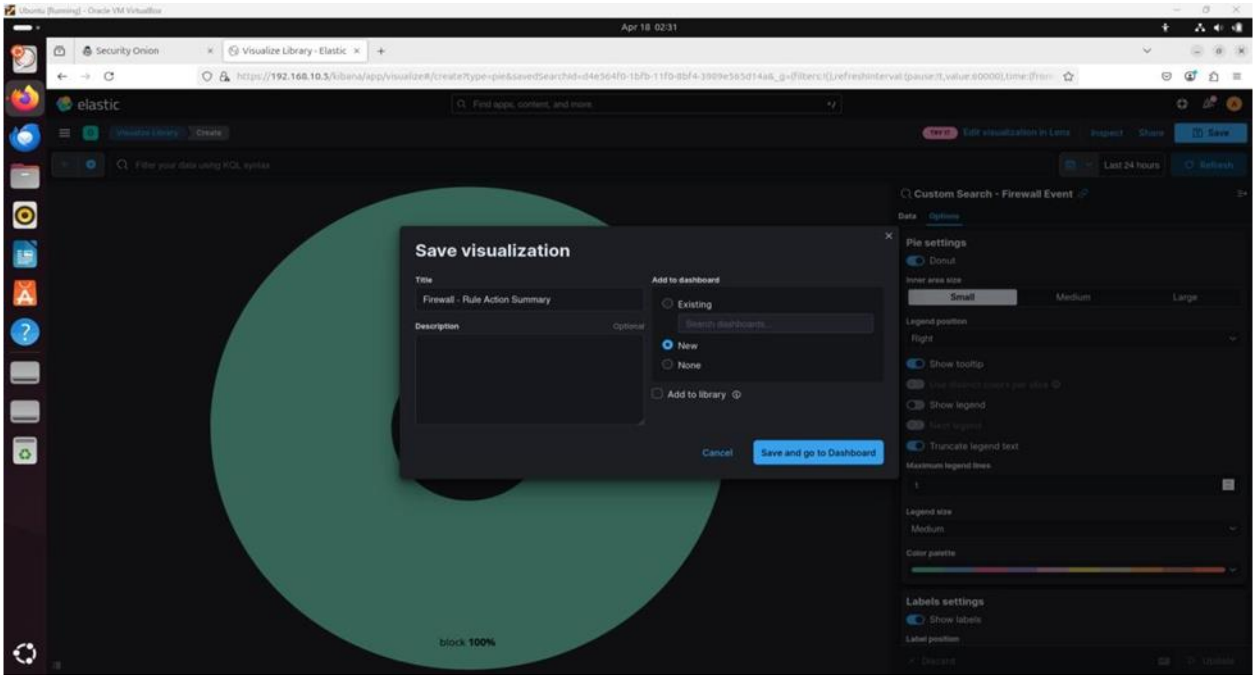
Show missing values

Custom label

Advanced

Add

VIII. I was redirected back to the dashboard editor, where I resized the pie chart widget to improve the layout.



Apr 18 02:31

Visualize Library - Elastic

https://192.168.10.5/kibana/app/visualize#/create?type=pie&savedSearchId=d4e564f0-1bfb-11f0-8bf4-3989e565d14a&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:

Custom Search - Firewall Event

Save visualization

Title: Firewall - Rule Action Summary

Description (Optional):

Add to dashboard

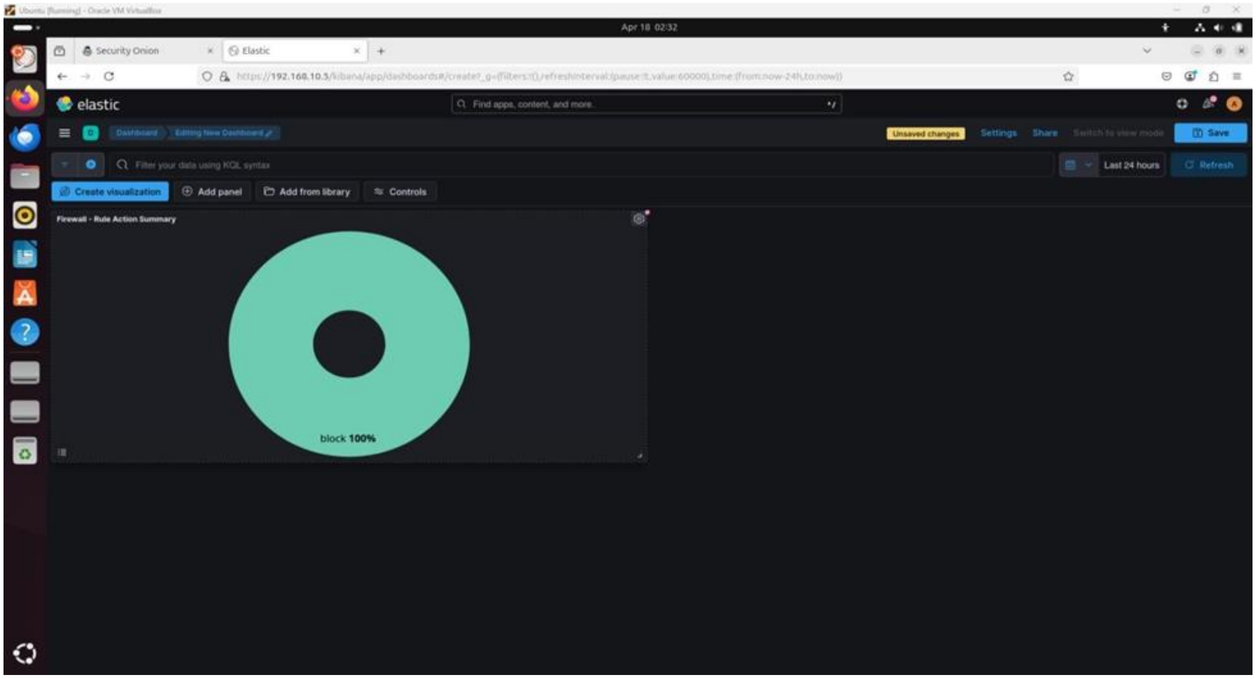
○ Existing

● New

○ None

□ Add to library

Cancel | Save and go to Dashboard



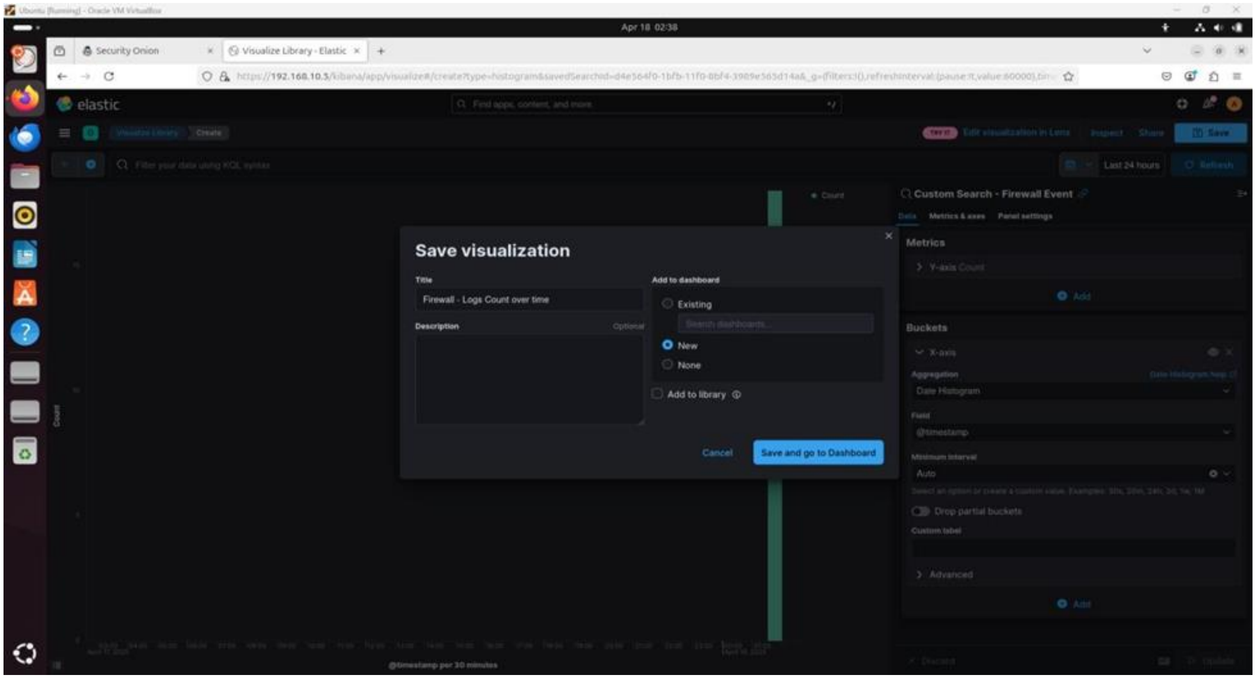
Apr 18 02:32

https://192.168.10.5/kibana/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-24h,to:now))

Dashboard / Editing New Dashboard

Unsaved changes

Firewall - Rule Action Summary



Save visualization

Title: Firewall - Logs Count over time

Description (Optional)

Add to dashboard: ○ Existing ● New ○ None

□ Add to library

Custom Search - Firewall Event

Metrics: Y-axis Count

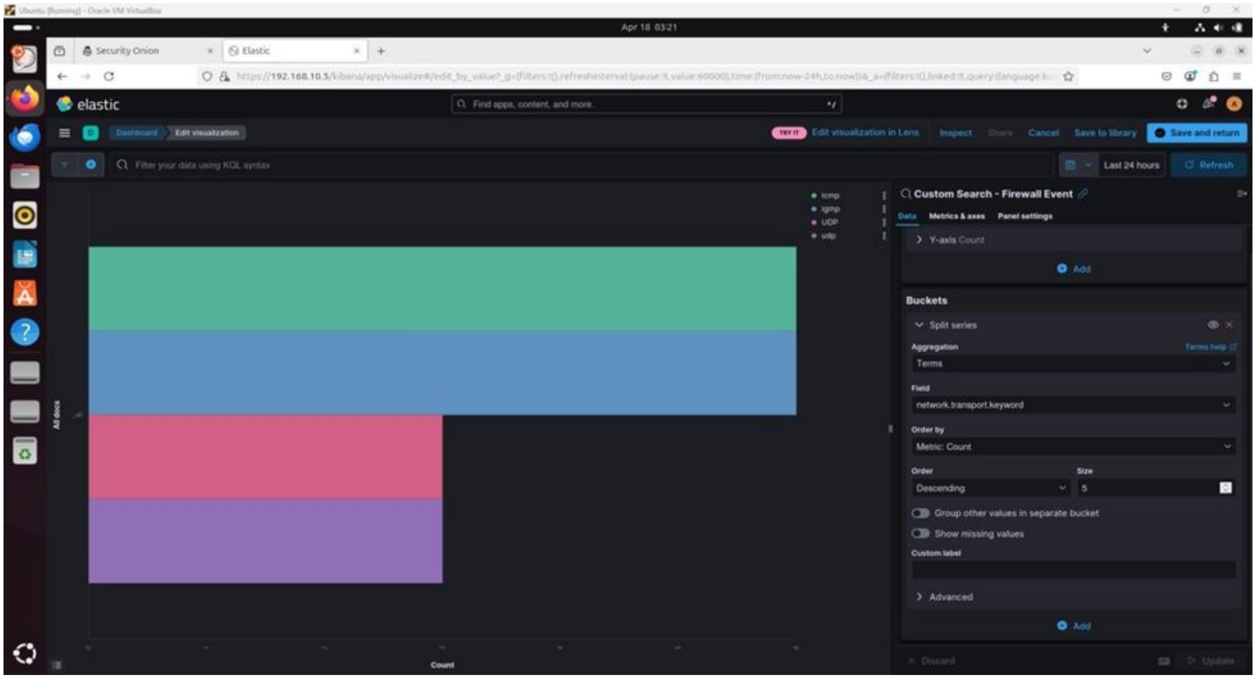
Buckets: X-axis

Aggregation: Date Histogram

Field: @timestamp

Minimum interval: Auto

IX. Next, I created a Vertical Bar chart using the same custom search. I configured the X-axis as a Date Histogram using the @timestamp field and saved this visualization as Firewall – Logs Count over Time.



Custom Search - Firewall Event

Metrics: Y-axis Count

Buckets: Split series

Aggregation: Terms

Field: network.transport.keyword

Order by: Metric: Count

Order: Descending

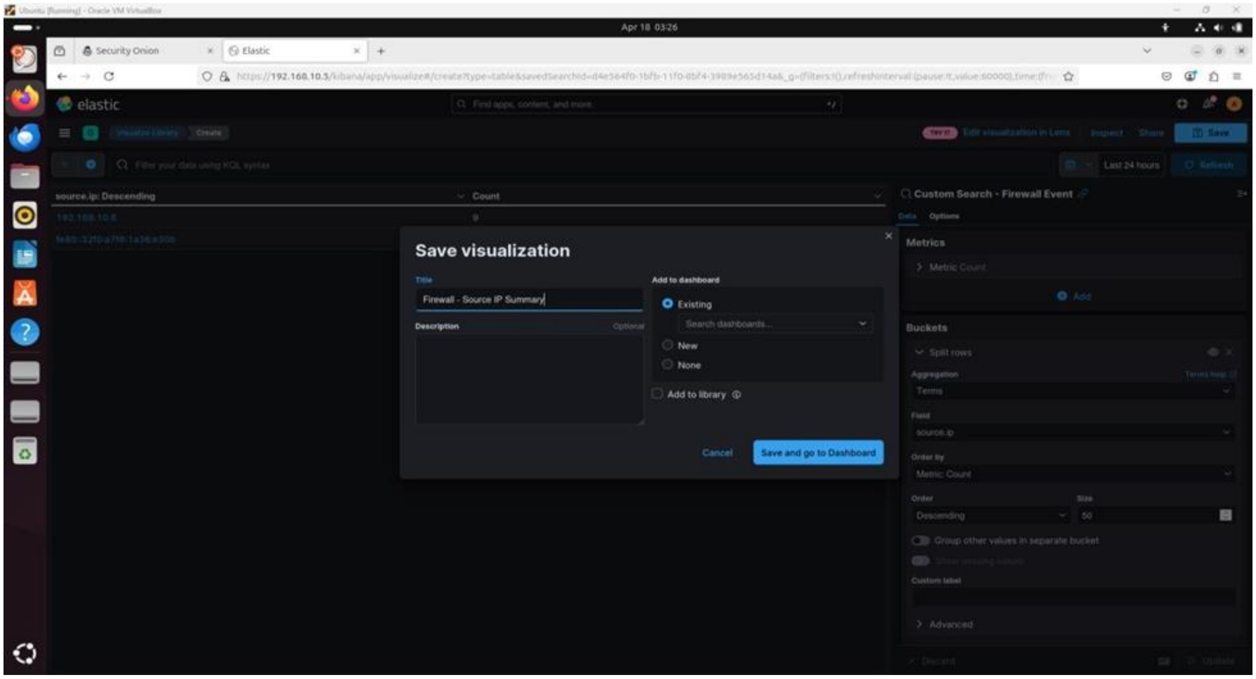
Size: 5

Group other values in separate bucket

Show missing values

Custom label

X. Then I built a Horizontal Bar chart, again using the custom firewall event search. I split the series using the Terms aggregation on the network.transport.keyword field and saved it as Firewall – Network Protocol Summary.



Custom Search - Firewall Event

source.ip: Descending	Count
192.168.10.8	9

Save visualization

Title: Firewall - Source IP Summary

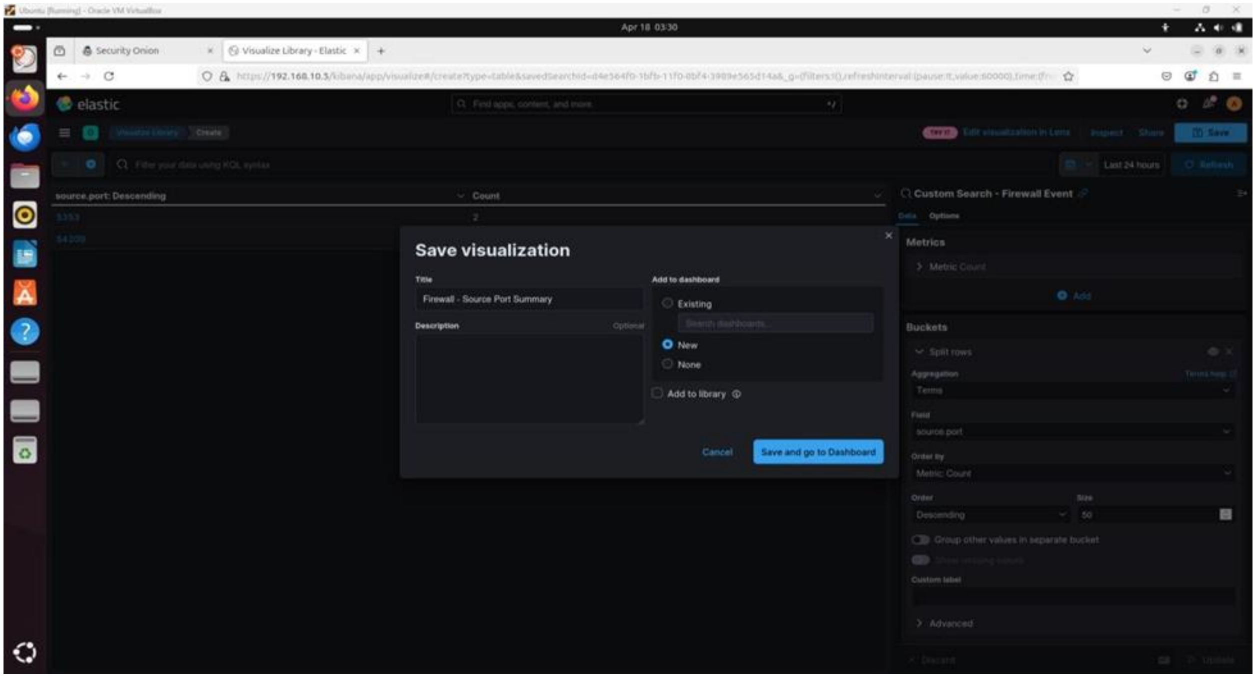
Description (Optional)

Add to dashboard: ● Existing ○ New ○ None

□ Add to library

Aggregation: Terms · Field: source.ip · Order by: Metric: Count · Order: Descending · Size: 50

XII. Similarly, I built another Data Table focusing on source.port, again using Terms with a size limit of 50. I saved this as Firewall – Source Port Summary.



Custom Search - Firewall Event

source.port: Descending	Count
3353	2

Save visualization

Title: Firewall - Source Port Summary

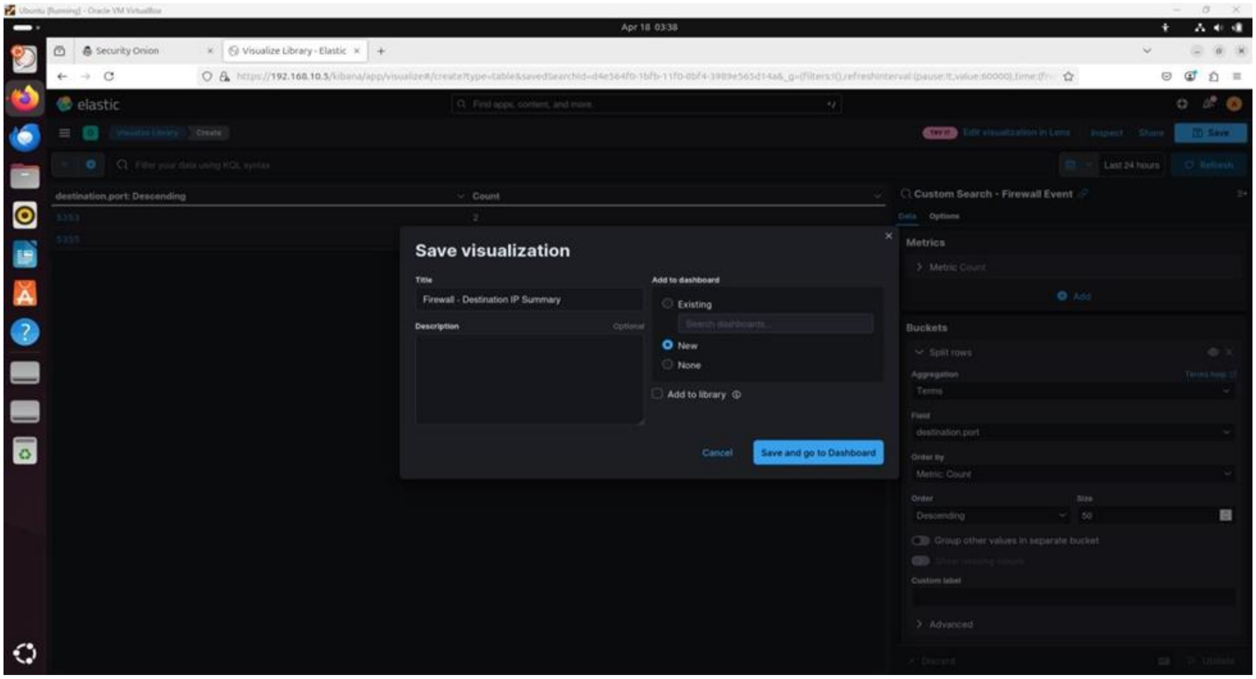
Description (Optional)

Add to dashboard: ○ Existing ● New ○ None

□ Add to library

Aggregation: Terms · Field: source.port · Order by: Metric: Count · Order: Descending · Size: 50

XIII. For destination traffic details, I created another Data Table split by destination.ip, naming it Firewall – Destination IP Summary.



destination.port: Descending	Count
5353	2
5355	

Save visualization

Title: Firewall - Destination IP Summary

Description (Optional):

Add to dashboard: ○ Existing ● New ○ None

□ Add to library

Custom Search - Firewall Event

Metrics: Metric Count

Buckets: Split rows

Aggregation: Terms

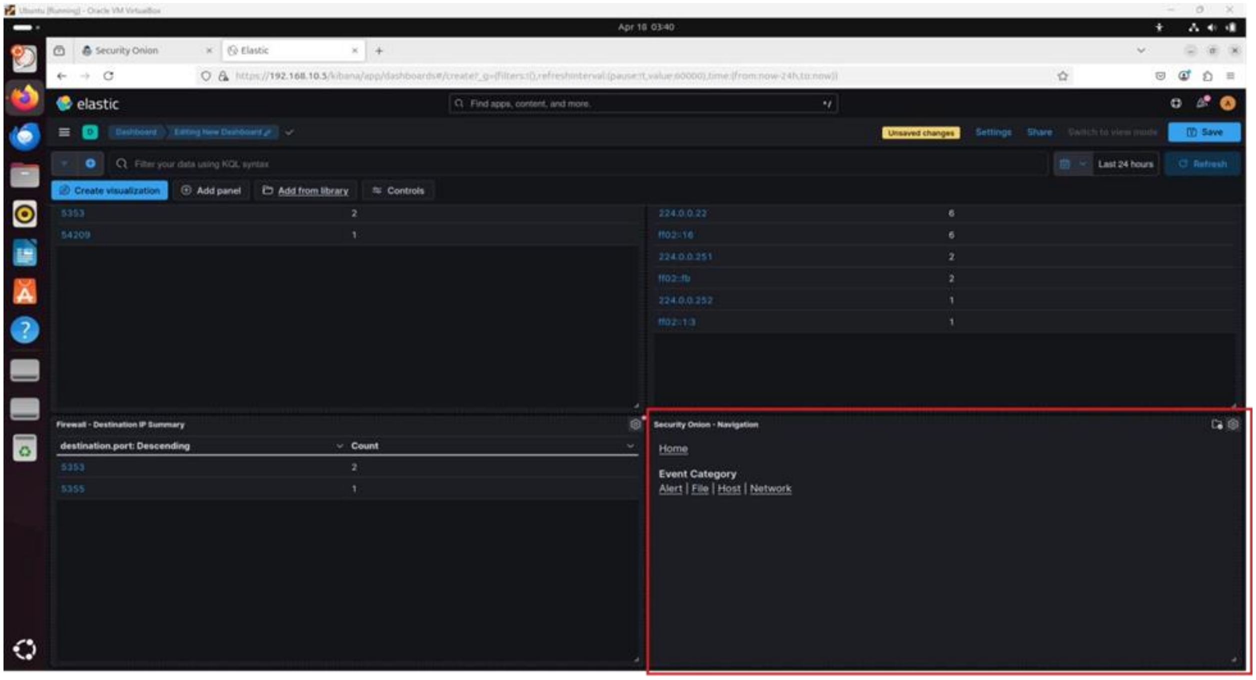
Field: destination.port

Order by: Metric: Count

Order: Descending

Size: 50

XIV. I also added a final Data Table visualization using destination.port as the split field and saved it as Firewall – Destination Port Summary.



5353	2
54209	1

224.0.0.22	6
ff02::16	6
224.0.0.251	2
ff02::fb	2
224.0.0.252	1
ff02::1:3	1

Firewall - Destination IP Summary

destination.port: Descending	Count
5353	2
5355	1

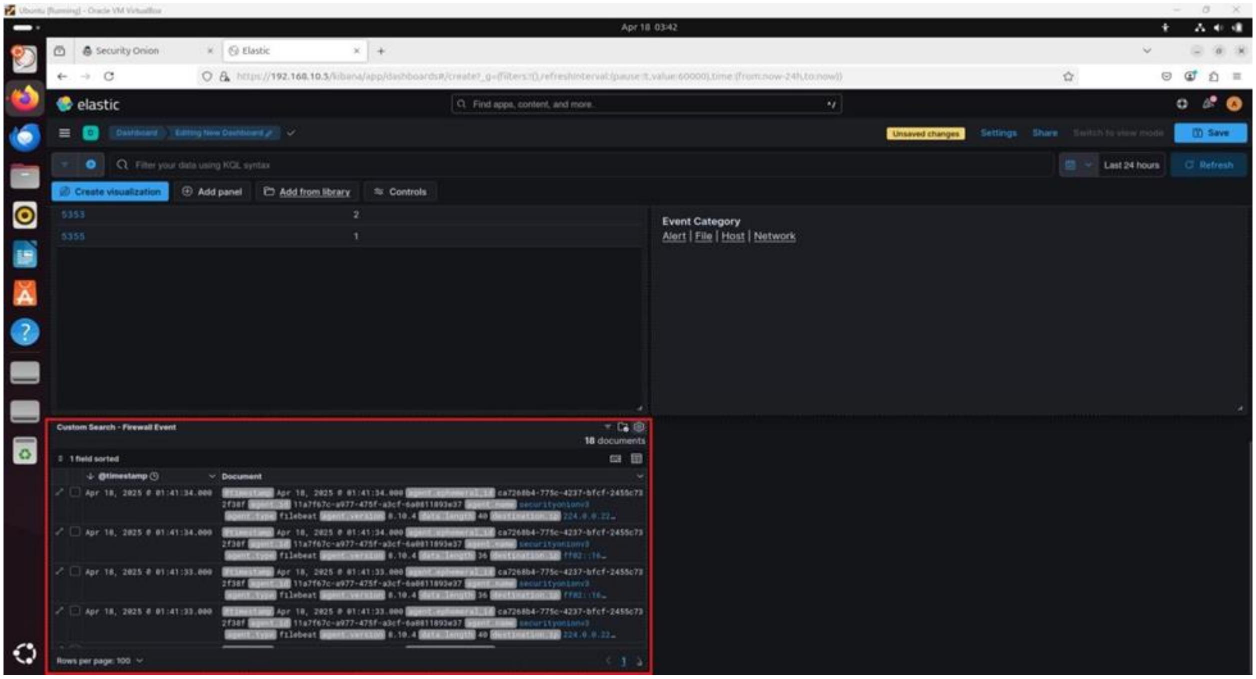
Security Onion - Navigation

Home

Event Category

Alert | File | Host | Network

XV. To enhance the dashboard, I added pre-built panels by clicking Add from library, where I selected the Security Onion Navigation panel.



Event Category
Alert | File | Host | Network

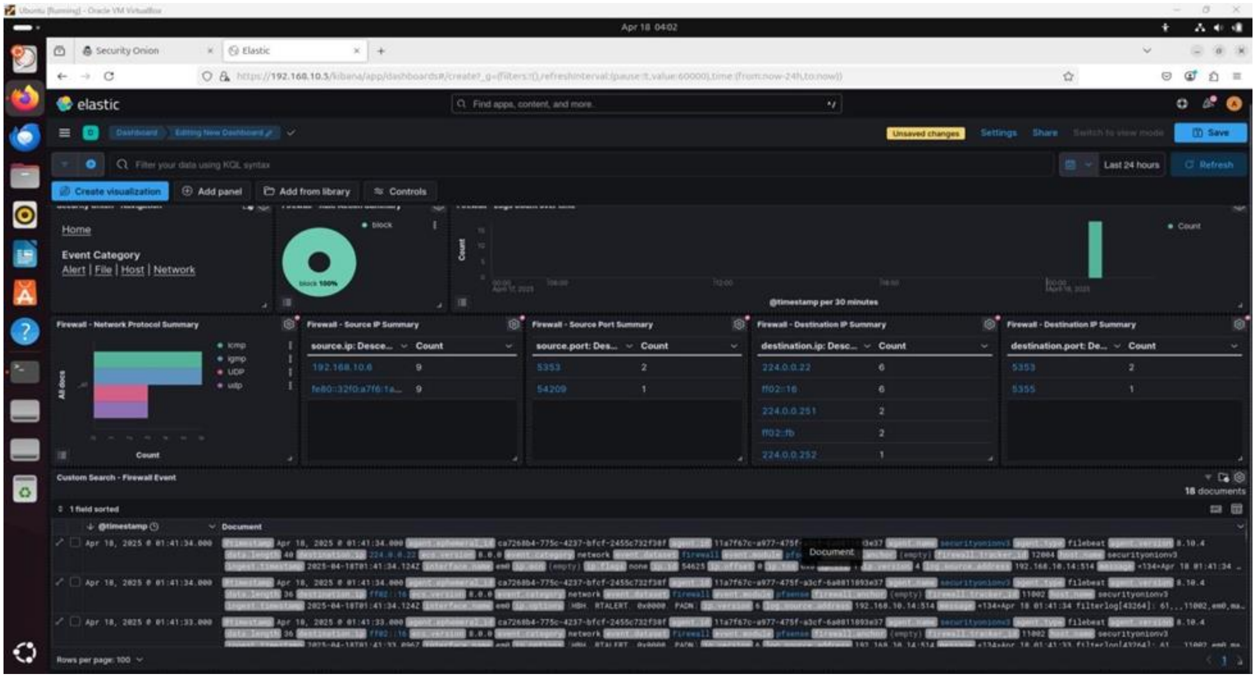
5353	2
5355	1

Custom Search - Firewall Event
18 documents
1 field sorted

```
@timestamp                   Document
Apr 18, 2025 @ 01:41:34.000  @timestamp Apr 18, 2025 @ 01:41:34.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c73
                             2f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37 agent.name securityonionv3
                             agent.type filebeat agent.version 8.10.4 data_length 40 destination.ip 224.0.0.22…
Apr 18, 2025 @ 01:41:34.000  @timestamp Apr 18, 2025 @ 01:41:34.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c73
                             2f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37 agent.name securityonionv3
                             agent.type filebeat agent.version 8.10.4 data_length 36 destination.ip ff02::16…
Apr 18, 2025 @ 01:41:33.000  @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c73
                             2f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37 agent.name securityonionv3
                             agent.type filebeat agent.version 8.10.4 data_length 36 destination.ip ff02::16…
Apr 18, 2025 @ 01:41:33.000  @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c73
                             2f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37 agent.name securityonionv3
                             agent.type filebeat agent.version 8.10.4 data_length 40 destination.ip 224.0.0.22…
```

Rows per page: 100

XVI. I also added the saved custom search panel, allowing real-time firewall event viewing similar to what's available in the Discover section.



Home

Event Category
Alert | File | Host | Network

@timestamp per 30 minutes

Firewall - Network Protocol Summary

Firewall - Source IP Summary

source.ip: Desce...	Count
192.168.10.6	9
fe80::32f0:a7f6:1a...	9

Firewall - Source Port Summary

source.port: Des...	Count
5353	2
54209	1

Firewall - Destination IP Summary

destination.ip: Desc...	Count
224.0.0.22	6
ff02::16	6
224.0.0.251	2
ff02::fb	2
224.0.0.252	1

Firewall - Destination IP Summary

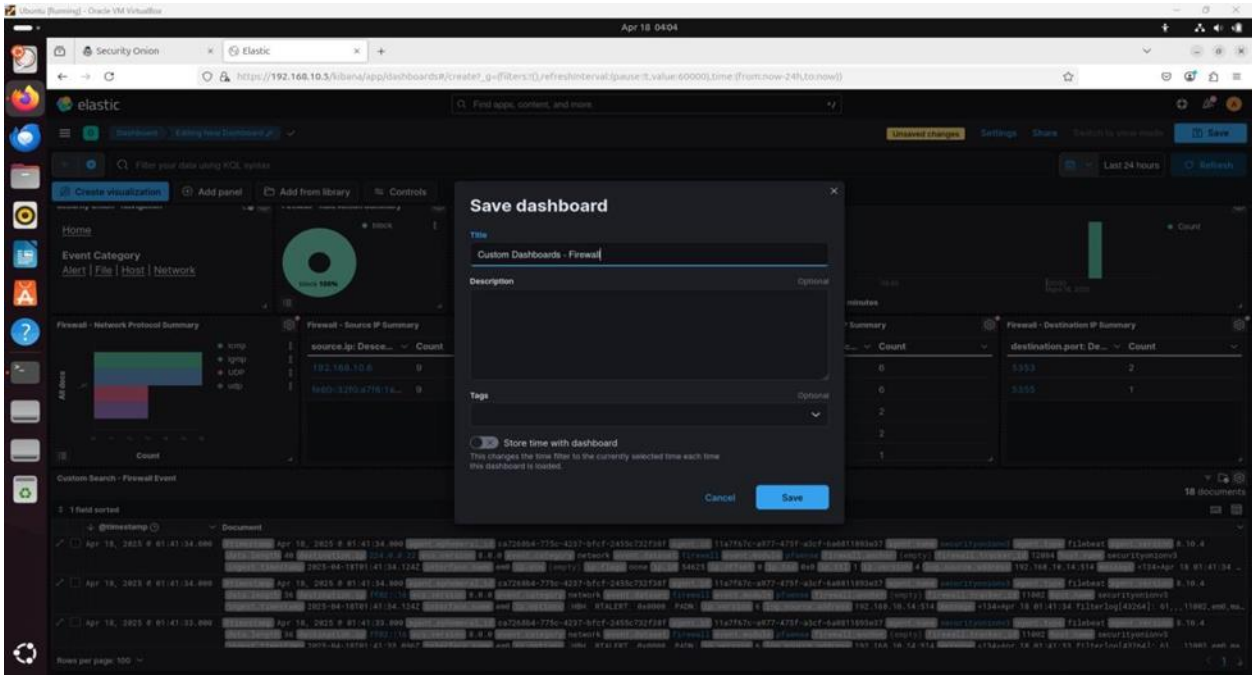
destination.port: De...	Count
5353	2
5355	1

Custom Search - Firewall Event
18 documents
1 field sorted

```
@timestamp                   Document
Apr 18, 2025 @ 01:41:34.000  @timestamp Apr 18, 2025 @ 01:41:34.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f- … 3e37 agent.name securityonionv3 agent.type filebeat agent.version 8.10.4
                             data_length 40 destination.ip 224.0.0.22 ecs.version 8.0.0 event.category network event.dataset firewall event.module pf… anchor (empty) firewall.tracker_id 12004 host.name securityonionv3
                             ingest.timestamp 2025-04-18T01:41:34.124Z interface.name em0 ip.ecn (empty) ip.flags none ip.id 54625 ip.offset 0 ip.tos … ip.version 4 log.source.address 192.168.10.14:514 message <134>Apr 18 01:41:34 …
Apr 18, 2025 @ 01:41:34.000  @timestamp Apr 18, 2025 @ 01:41:34.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37 agent.name securityonionv3 agent.type filebeat agent.version 8.10.4
                             data_length 36 destination.ip ff02::16 ecs.version 8.0.0 event.category network event.dataset firewall event.module pfsense firewall.anchor (empty) firewall.tracker_id 11002 host.name securityonionv3
                             ingest.timestamp 2025-04-18T01:41:34.124Z interface.name em0 ip.options HBH, RTALERT, 0x0000, PADN ip.version 6 log.source.address 192.168.10.14:514 message <134>Apr 18 01:41:34 filterlog[43264]: 61,,,11002,em0,ma…
Apr 18, 2025 @ 01:41:33.000  @timestamp Apr 18, 2025 @ 01:41:33.000 agent.ephemeral_id ca7268b4-775c-4237-bfcf-2455c732f38f agent.id 11a7f67c-a977-475f-a3cf-6a0811893e37 agent.name securityonionv3 agent.type filebeat agent.version 8.10.4
                             data_length 36 destination.ip ff02::16 ecs.version 8.0.0 event.category network event.dataset firewall event.module pfsense firewall.anchor (empty) firewall.tracker_id 11002 host.name securityonionv3
                             ingest.timestamp 2025-04-18T01:41:33.096Z interface.name em0 ip.options HBH, RTALERT, 0x0000, PADN ip.version 6 log.source.address 192.168.10.14:514 message <134>Apr 18 01:41:33 filterlog[43264]: 61,,,11002,em0,ma…
```

Rows per page: 100

XVII. I then reorganized and resized all widgets on the dashboard to ensure clarity and logical layout.



Save dashboard

Title: Custom Dashboards - Firewall

Description (Optional)

Tags (Optional)

Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Security Onion
Elastic
https://192.168.10.5/kibana/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-24h,to:now))
elastic
Unsaved changes
Save
Create visualization
Add panel
Add from library
Controls
Home
Event Category
Alert | File | Host | Network
Firewall - Network Protocol Summary
icmp
igmp
UDP
udp
Count
Firewall - Source IP Summary
source.ip: Desce...
Count
192.168.10.6
Firewall - Destination IP Summary
destination.port: De...
Count
Custom Search - Firewall Event
18 documents
@timestamp
Document
Rows per page: 100
Cancel
Save

XVIII. Finally, I clicked the Save button to preserve the full dashboard setup.

I have successfully completed the Lab.

-- Phanindhar Reddy Karnati
-- 001667635