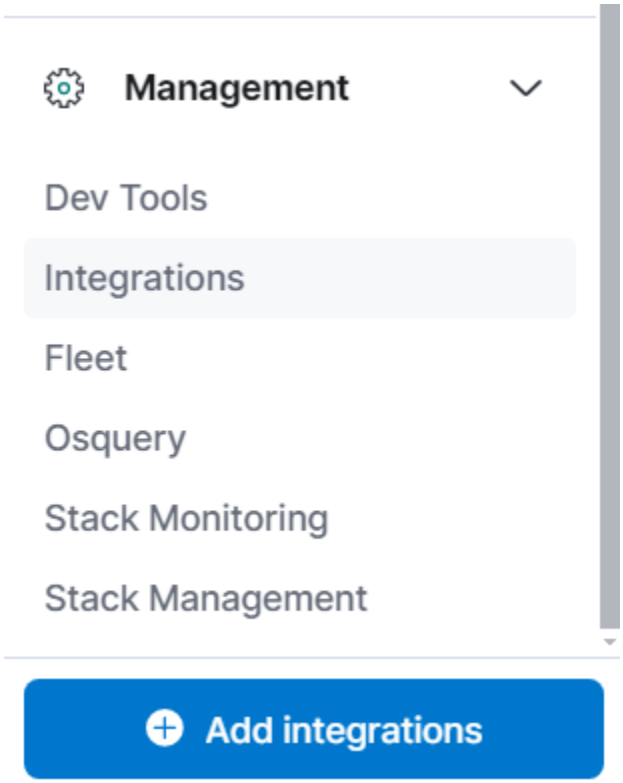
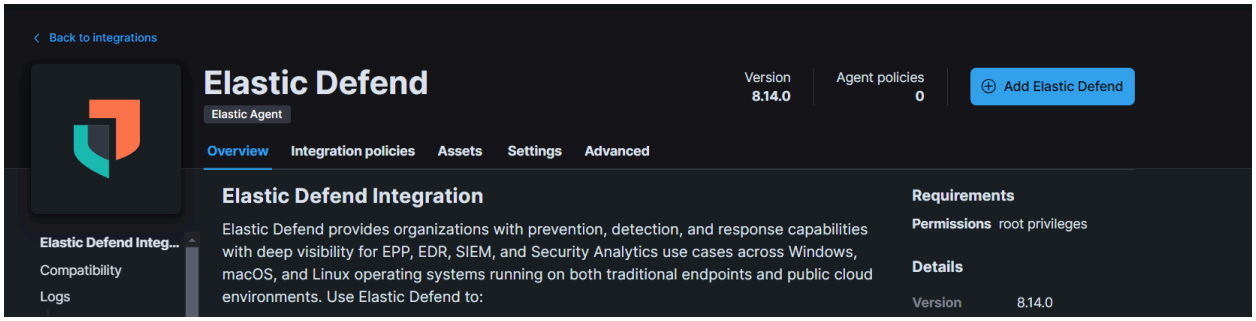
Description: The goal of this project is to demonstrate how to perform Nmap scans using Kali Linux and set up an SIEM Lab with Elastic SIEM to detect and monitor these scans. The project includes creating custom dashboards to visualize the events and setting up alerts that trigger whenever a Nmap scan is detected, providing real-time insights into potential security threats.

Software and tools I use: Vmware Workstation Pro, Elastic (SIEM, Windows 11(victim), Sliver Command (Offensive tool).

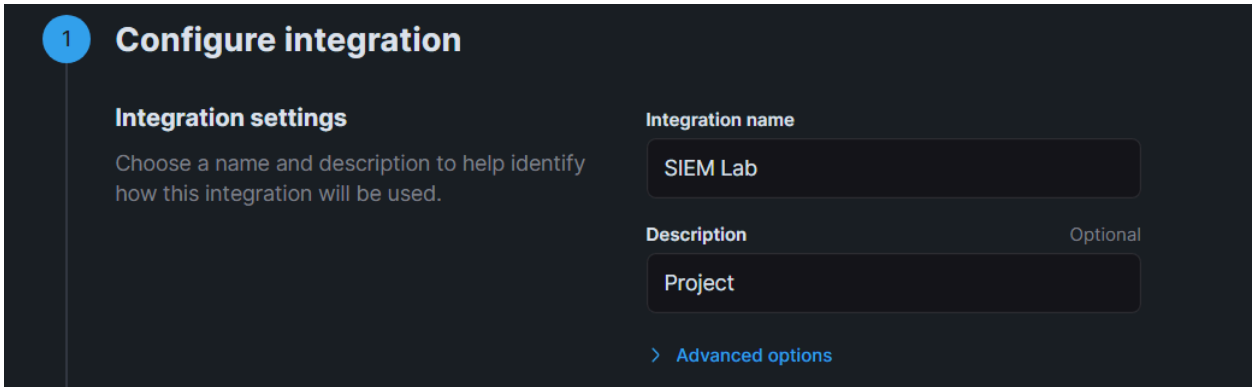
Project: First I need to log in to Elastic in the browser and on the left option, I will click and go to the bottom and choose Add integrations.



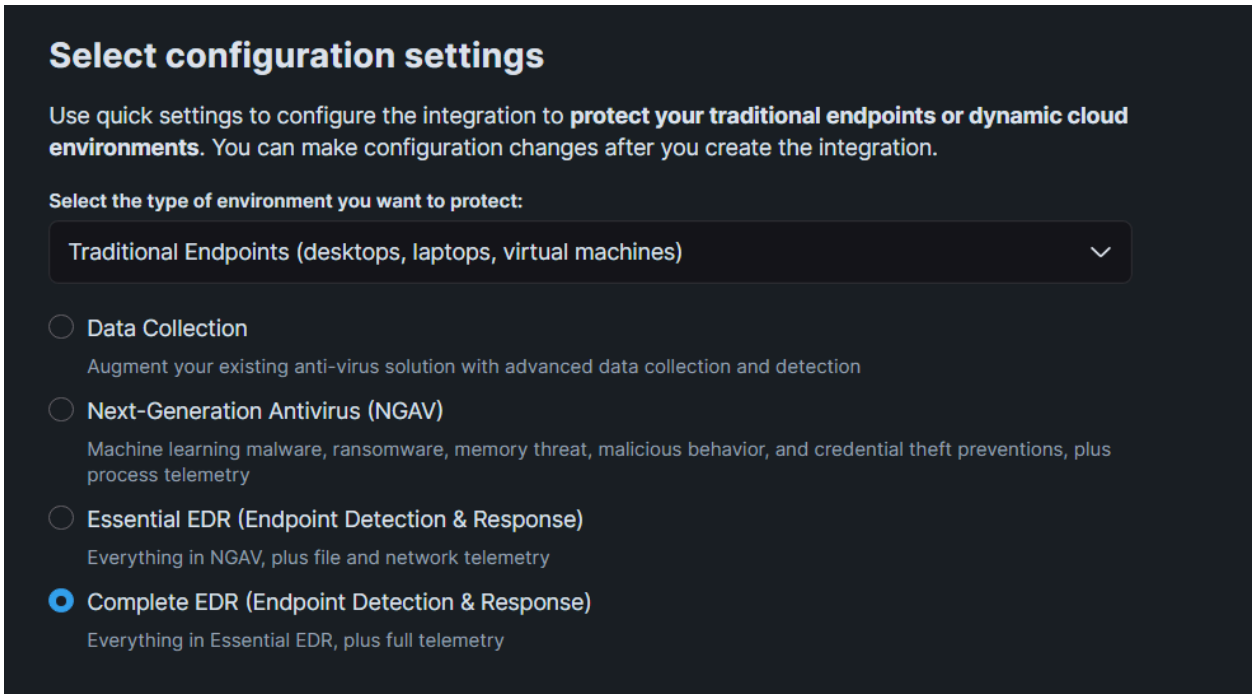
I will add Elastic Defend.



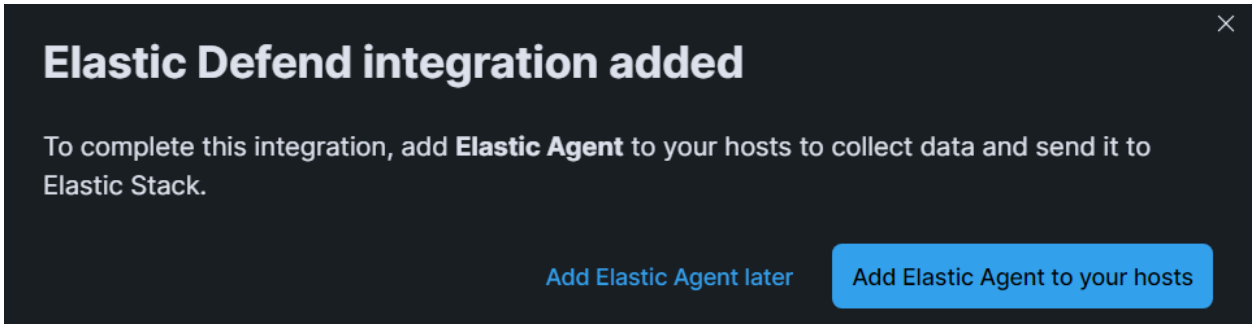
I have to choose the Integration name and description name. For this project, I will name it “SIEM Lab” and “Project”.



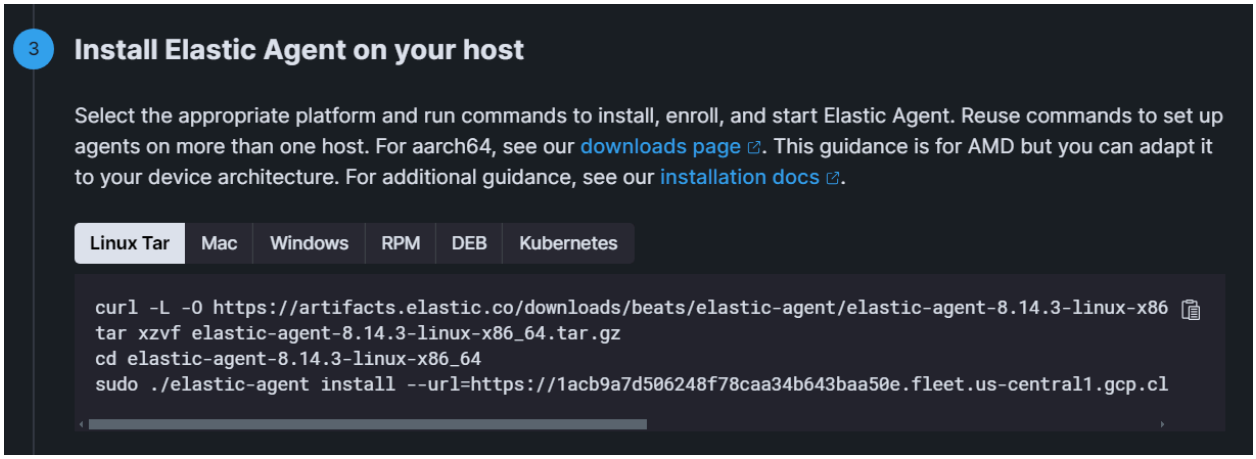
I will choose EDR (Endpoint Detection & Response) for configuration settings and click ‘save and continue’.



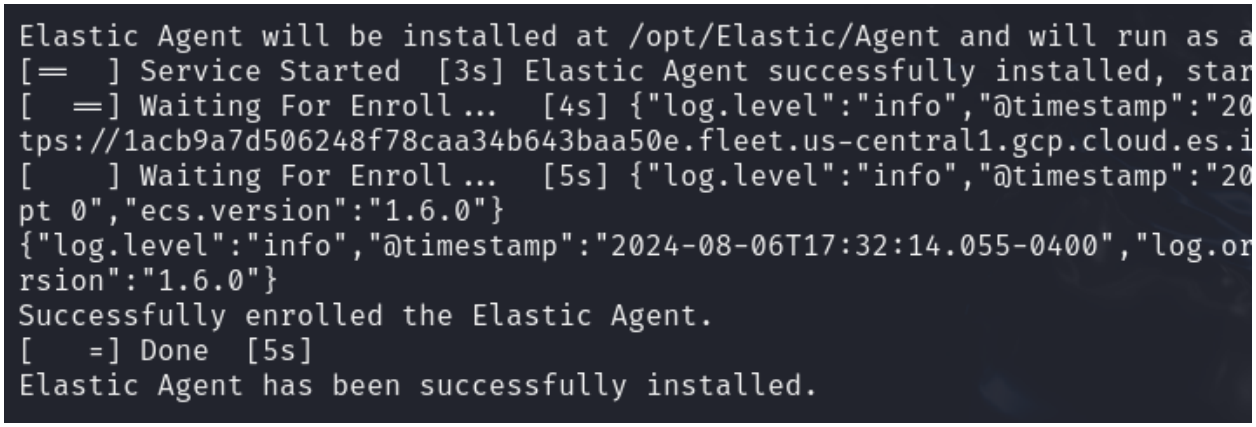
I will click ‘Add Elastic Agent to your hosts’.



I am using Kali Linux, so I have to copy the Linux commands.



I will open up Kali Linux and paste the commands in the terminal.



I can verify the installation by typing this command ‘sudo systemctl status elastic-agent.service’

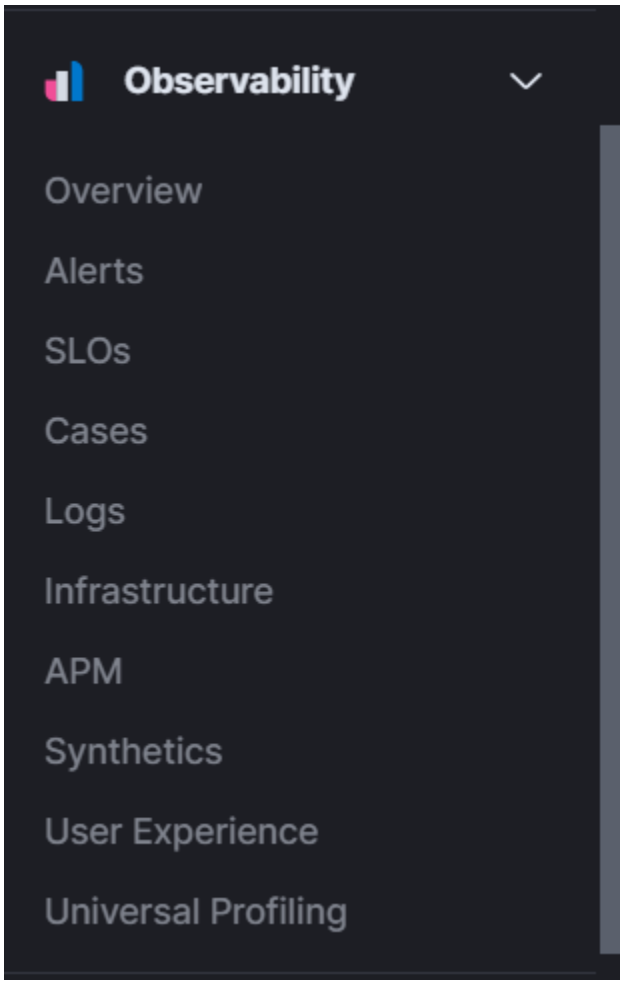
```
└─$ sudo systemctl status elastic-agent.service
[sudo] password for kali:
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-08-06 17:32:12 EDT; 13min ago
   Main PID: 43268 (elastic-agent)
      Tasks: 64 (limit: 2262)
     Memory: 637.8M (peak: 663.4M)
        CPU: 26.569s
     CGroup: /system.slice/elastic-agent.service
```

It will say ‘active (running)’ in a different color. Now I will generate security events on the Kali VM. I will run ‘nmap -p- localhost’ to scan the localhost for all open ports and ‘nmap -sS localhost’ to scan TCP SYN on the localhost.

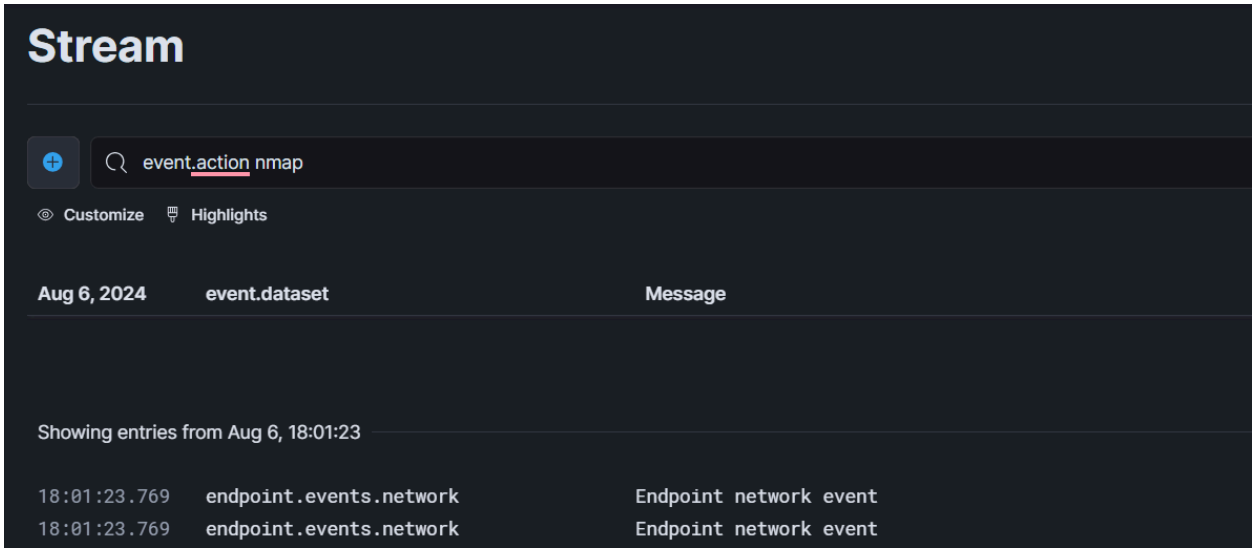
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- localhost

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 18:01 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.49% done; ETC: 18:01 (0:00:03 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.56% done; ETC: 18:01 (0:00:03 remaining)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00039s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE
6788/tcp open  smc-http
6789/tcp open  ibm-db2-admin
6791/tcp open  hnm

Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS localhost
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 18:05 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
6788/tcp open  smc-http
6789/tcp open  ibm-db2-admin

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

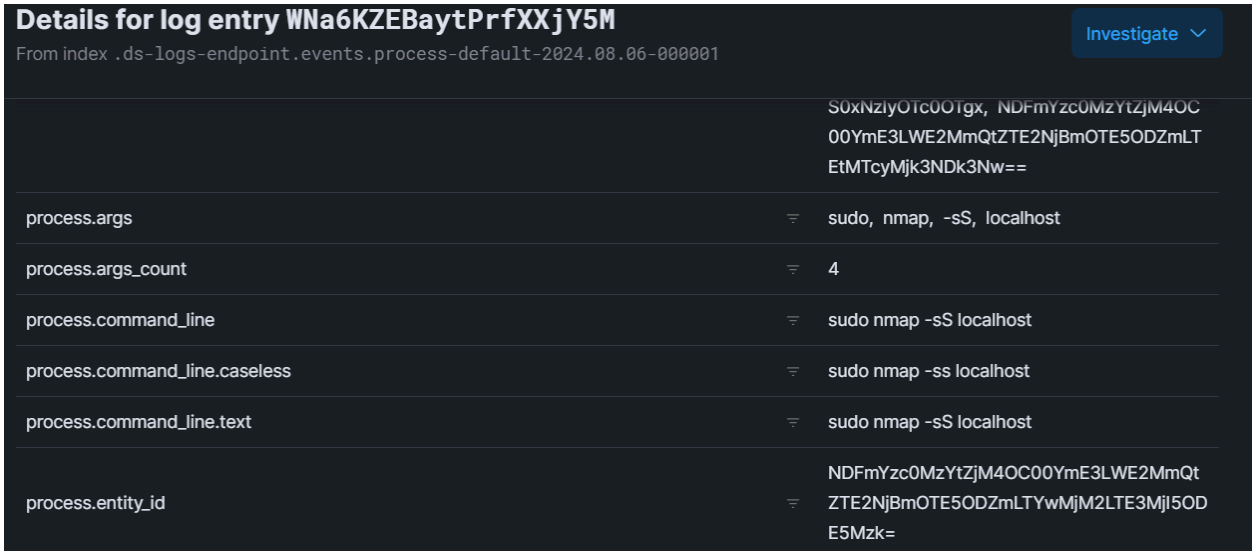
I will go to the elastic and click the toggle menu. In the observability section, I will click logs.



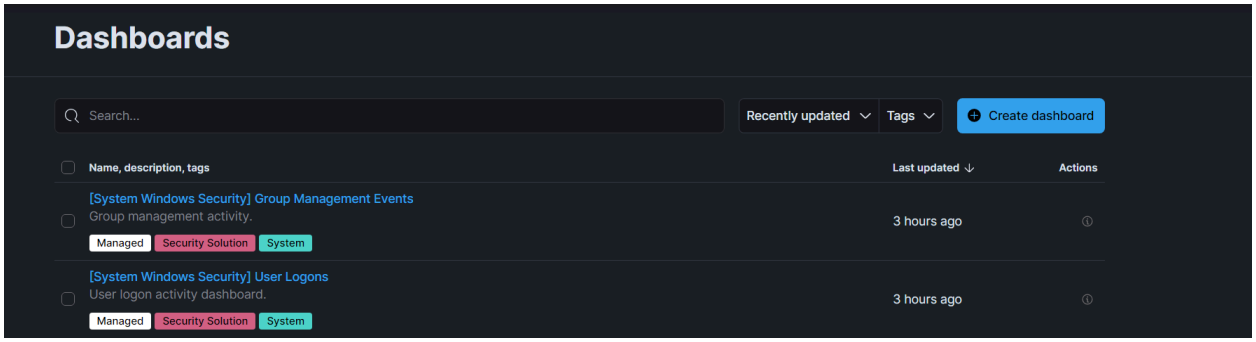
In the search option, I will search for ‘event.action nmap’.



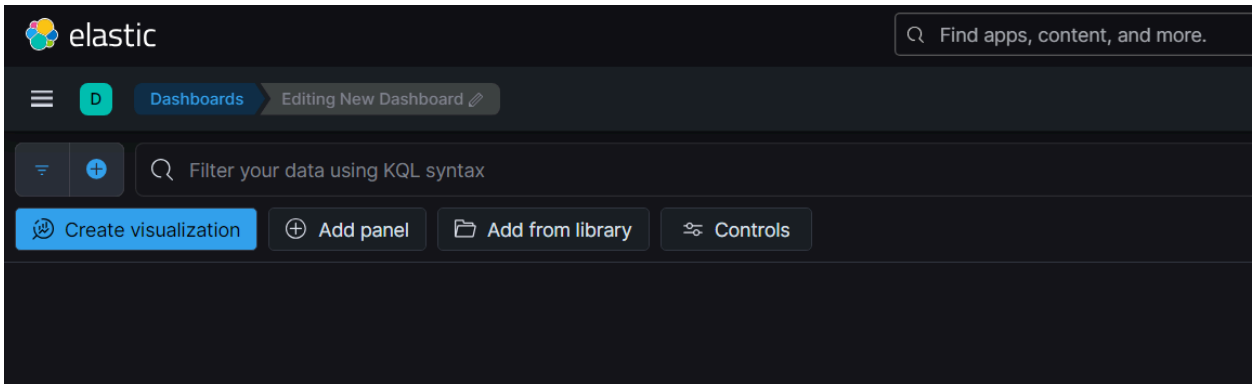
I will scroll down and go to the last event. I will click on the right side of the toggle menu and click ‘view details’.



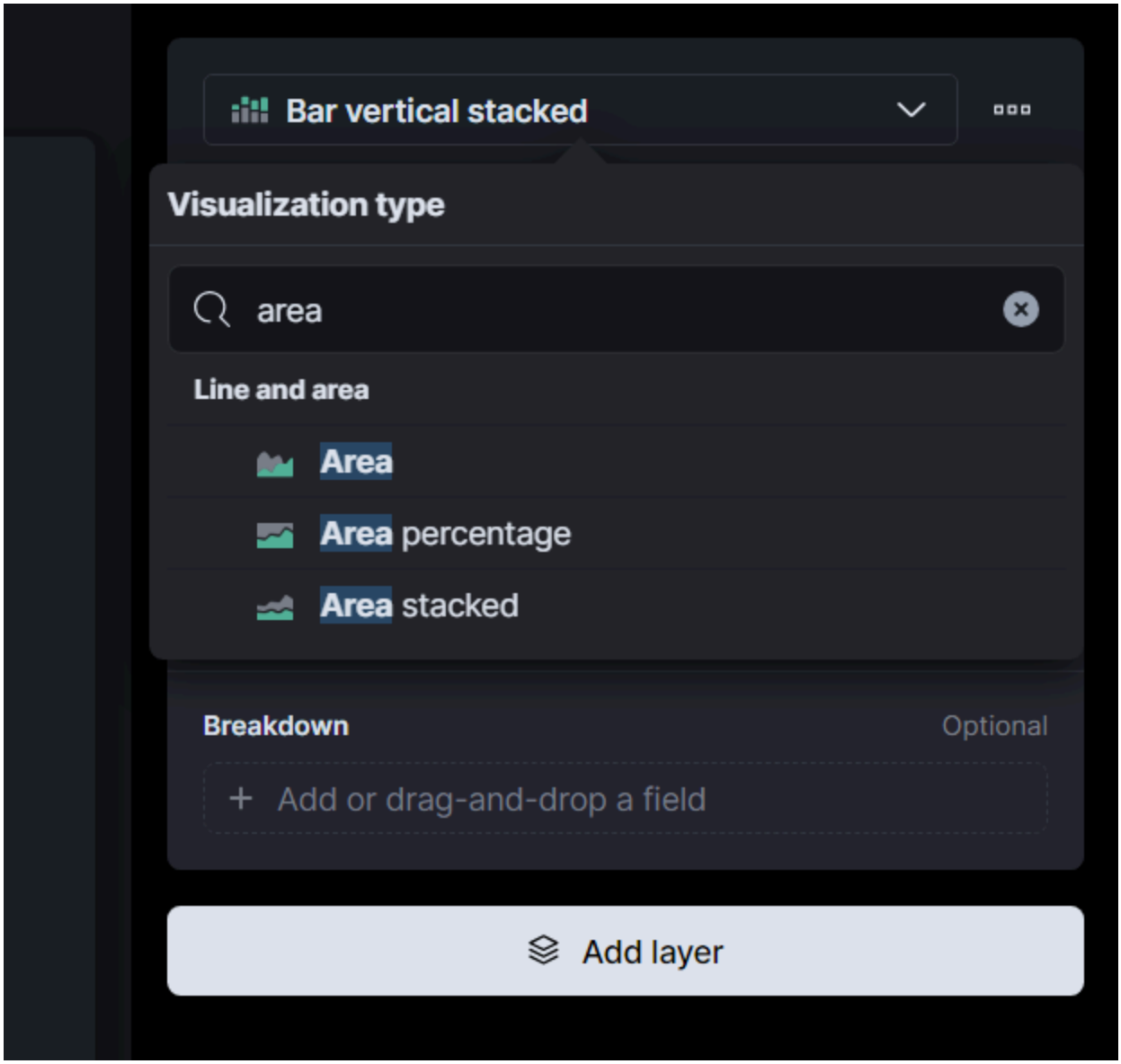
I can see the command that I used ‘sudo nmap -sS localhost’’. Now I will create a Dashboard to Visualize the Events. To do that, I will open the dashboard. Then I will click ‘create dashboard’.



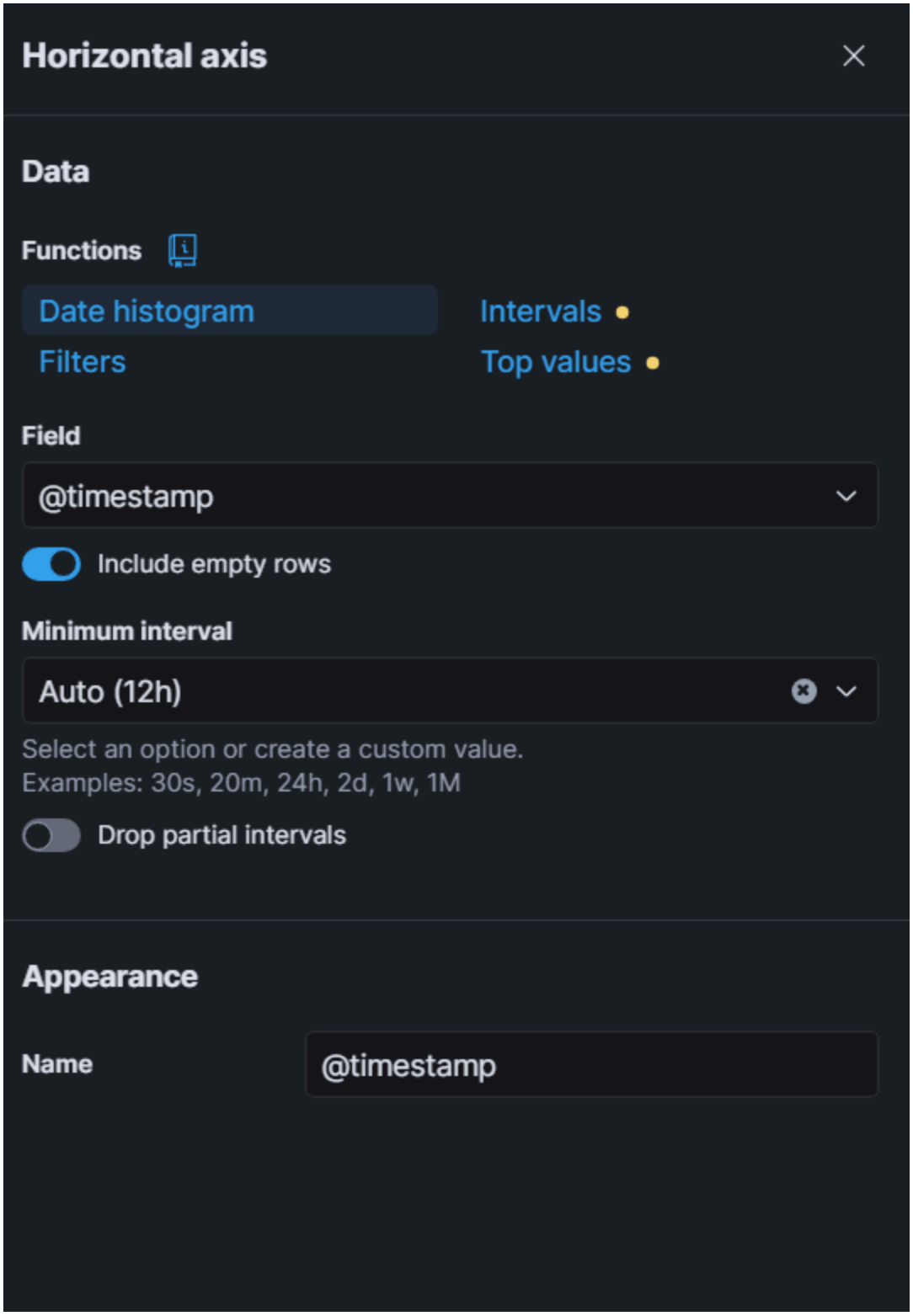
I will click the “Create Visualization” button to create a new visualization.



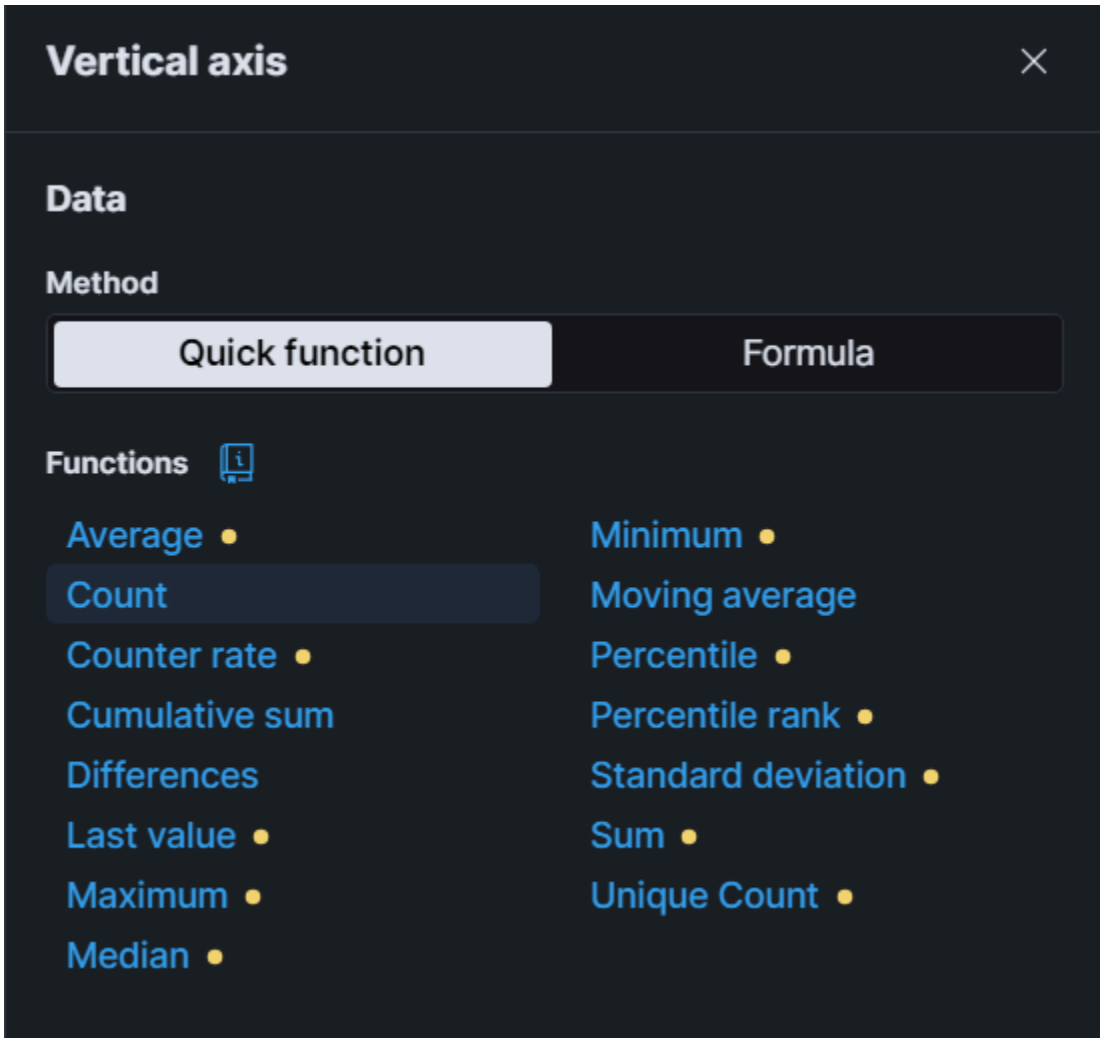
On the right side, I will click the drop-down menu and choose ‘area’.



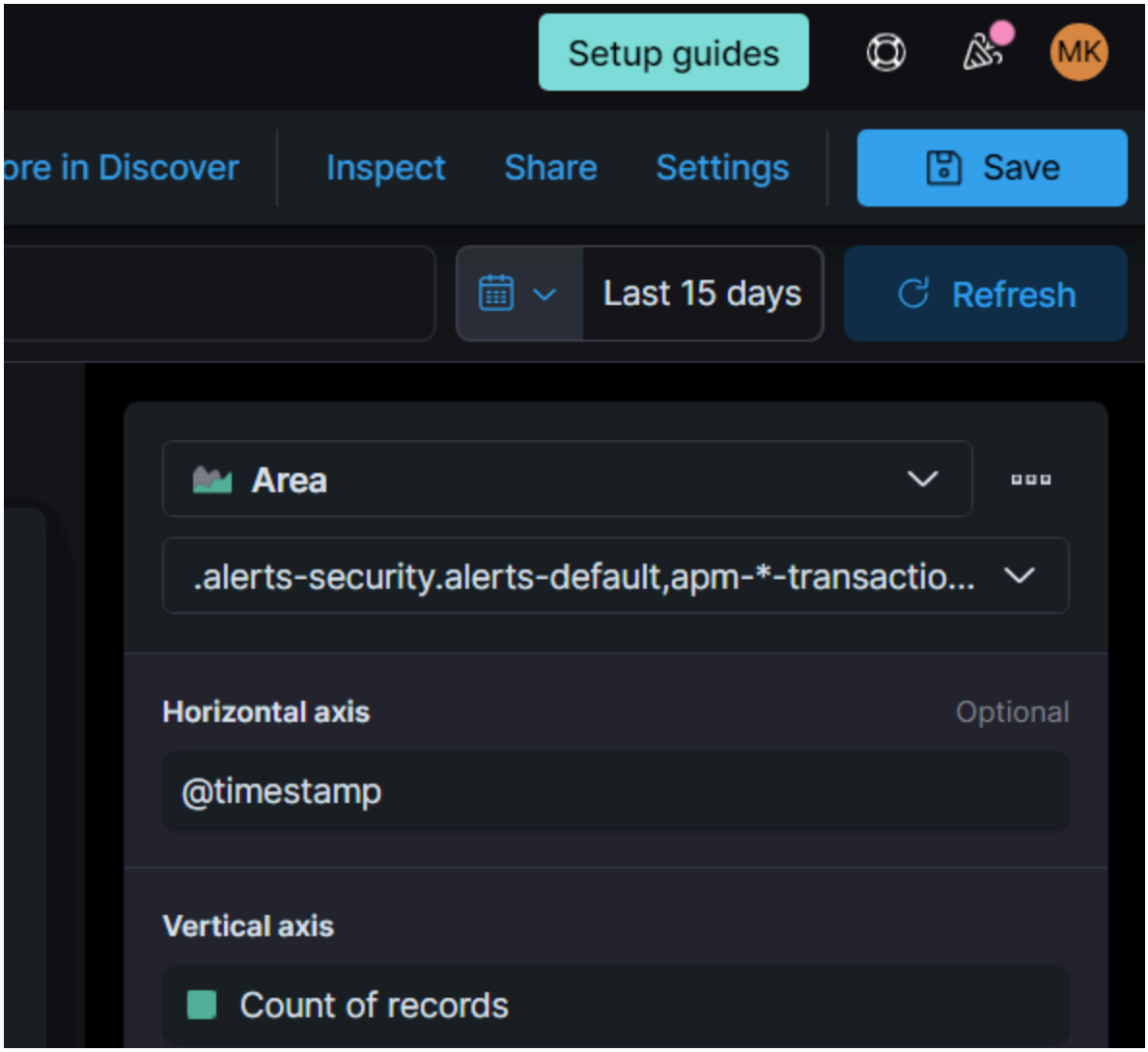
In the ‘Horizontal axis’ option on the right, I will add ‘timestamp’.


Horizontal axis
Data
Functions
Date histogram
Intervals
Filters
Top values
Field
@timestamp
Include empty rows
Minimum interval
Auto (12h)
Select an option or create a custom value.
Examples: 30s, 20m, 24h, 2d, 1w, 1M
Drop partial intervals
Appearance
Name
@timestamp

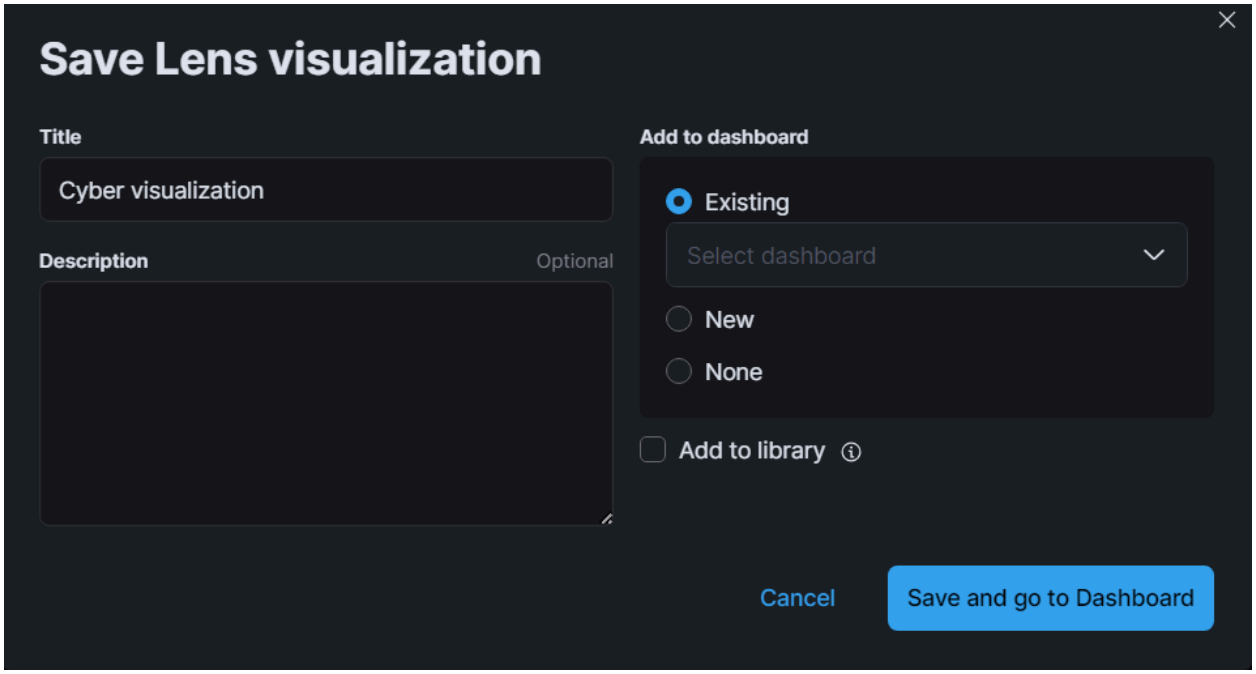
I will add the ‘count'' function in the ‘Vertical axis’ option on the right.



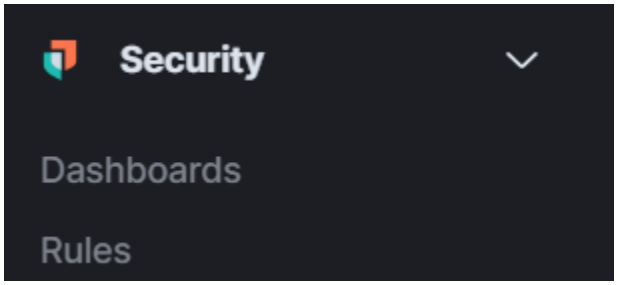
After choosing the ‘timestamp’ and count function, I will save it.



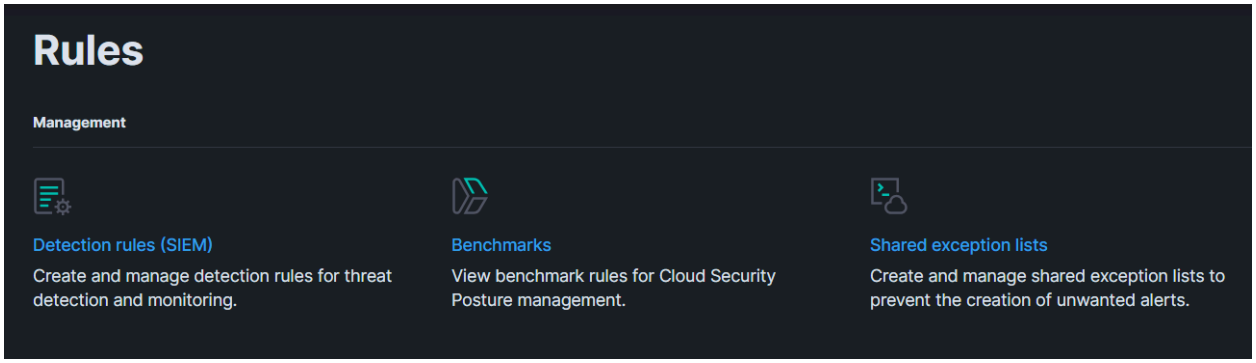
To save it, I will save the title as ‘Cyber visualization’.



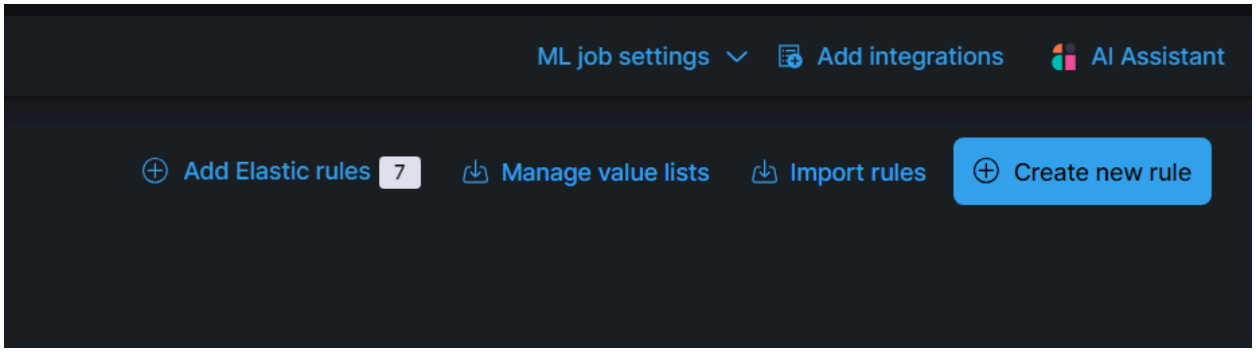
Now I will create an alert to monitor my logs for Nmap scan events and notify me if they are detected. In the Security section, I will click on the ‘Rules’ from the toggle menu.



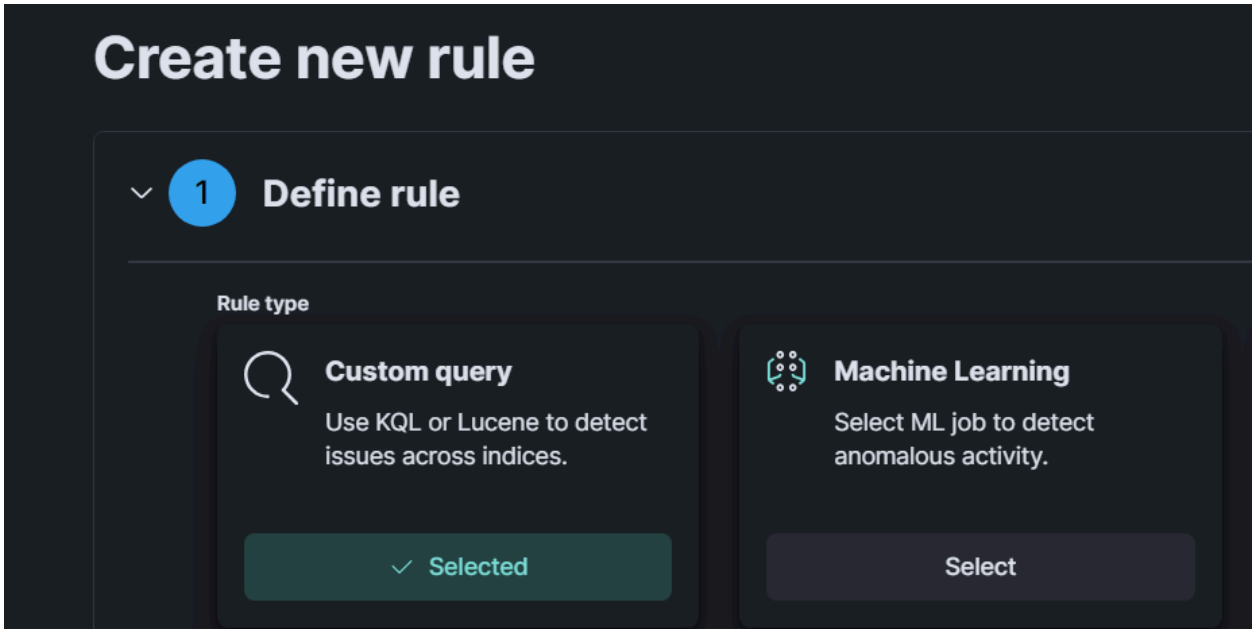
I will click the ‘Detection rules (SIEM)’.



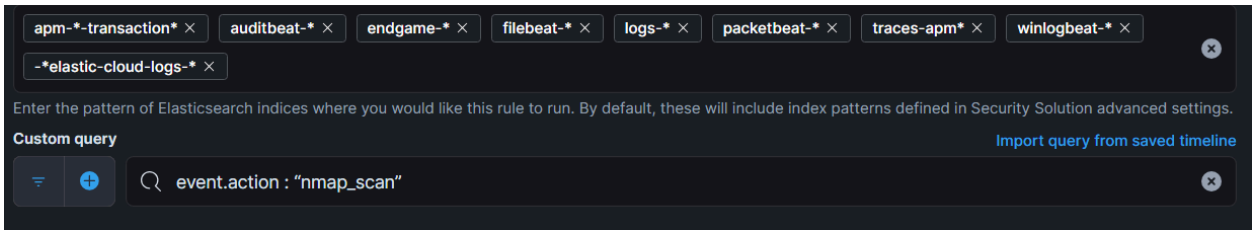
I will click the ‘Create new rule’ on the right.



I will click ‘Custom query’.

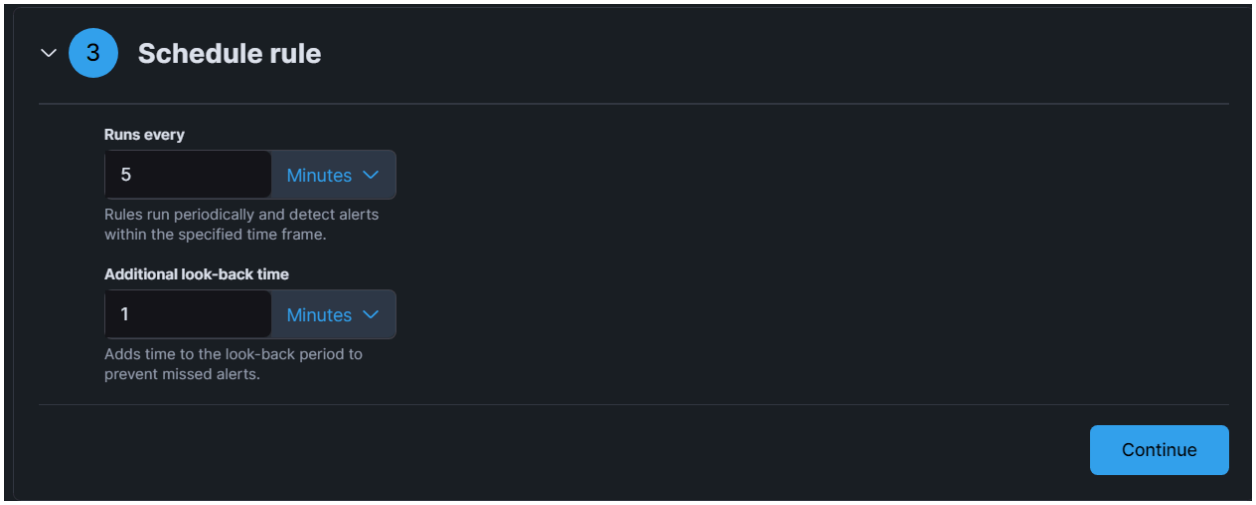


If I scroll down, I will see the Custom query section. I will type ‘event.action: “nmap_scan” ’ and click ‘Continue’.

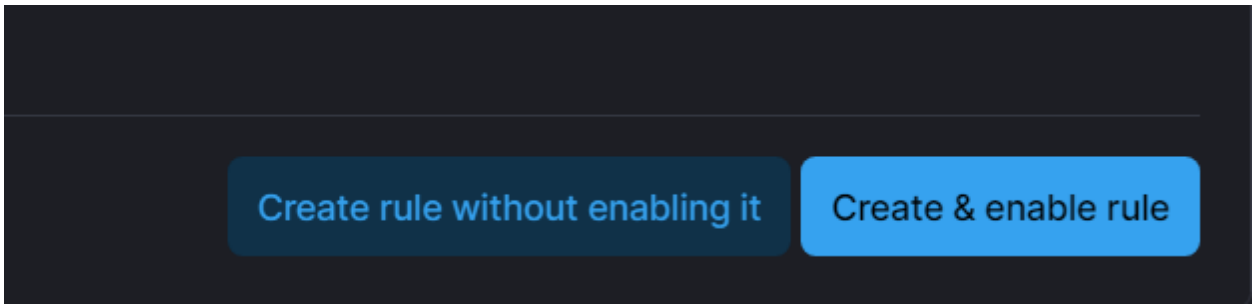


In the About rule section, I will name it ‘Nmap Scan’ and in the description section, I will name it ‘Detects Nmap Scan’. Then I will click ‘Continue’.

In the Schedule rule, I will choose the default option and click ‘Continue’.



In the Rule actions, I will click ‘create & enable rule’.



It will successfully create an alert. Now, I will use Nmap scan again. Now I will go to the dashboard that I created and I see the high spike for Nmap scan.