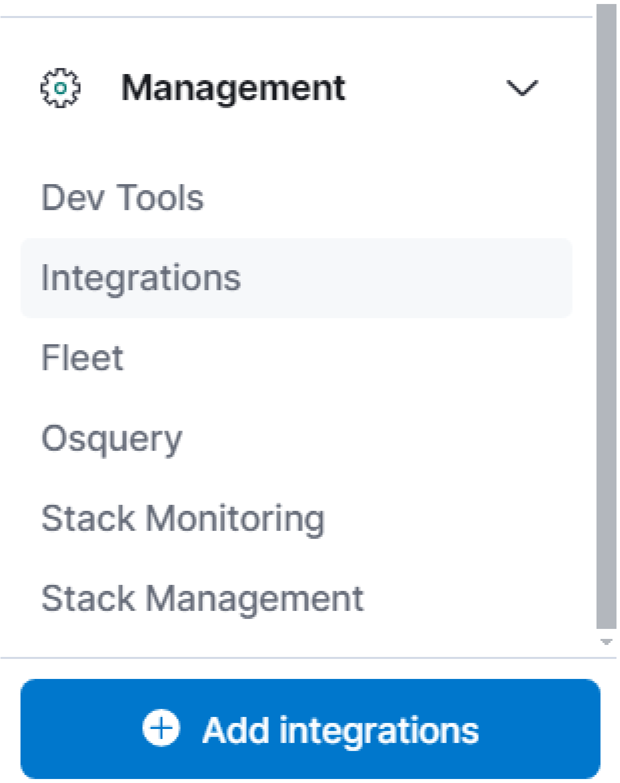
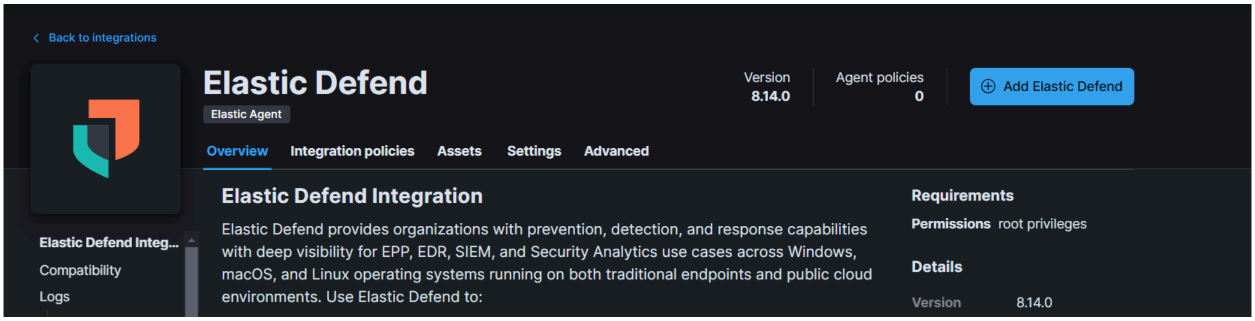
Description: The goal of this project is to demonstrate how to perform Nmap scans using Kali Linux and set up an SIEM Lab with Elastic SIEM to detect and monitor these scans. The project includes creating custom dashboards to visualize the events and setting up alerts that trigger whenever a Nmap scan 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.



Elastic Defend Integration

Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. Use Elastic Defend to:

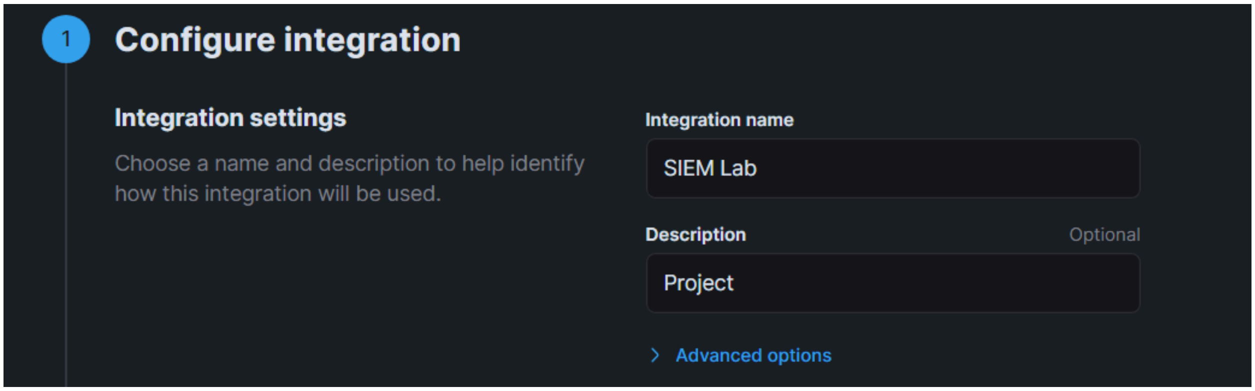
Requirements

Permissions root privileges

Details

Version 8.14.0

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



1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

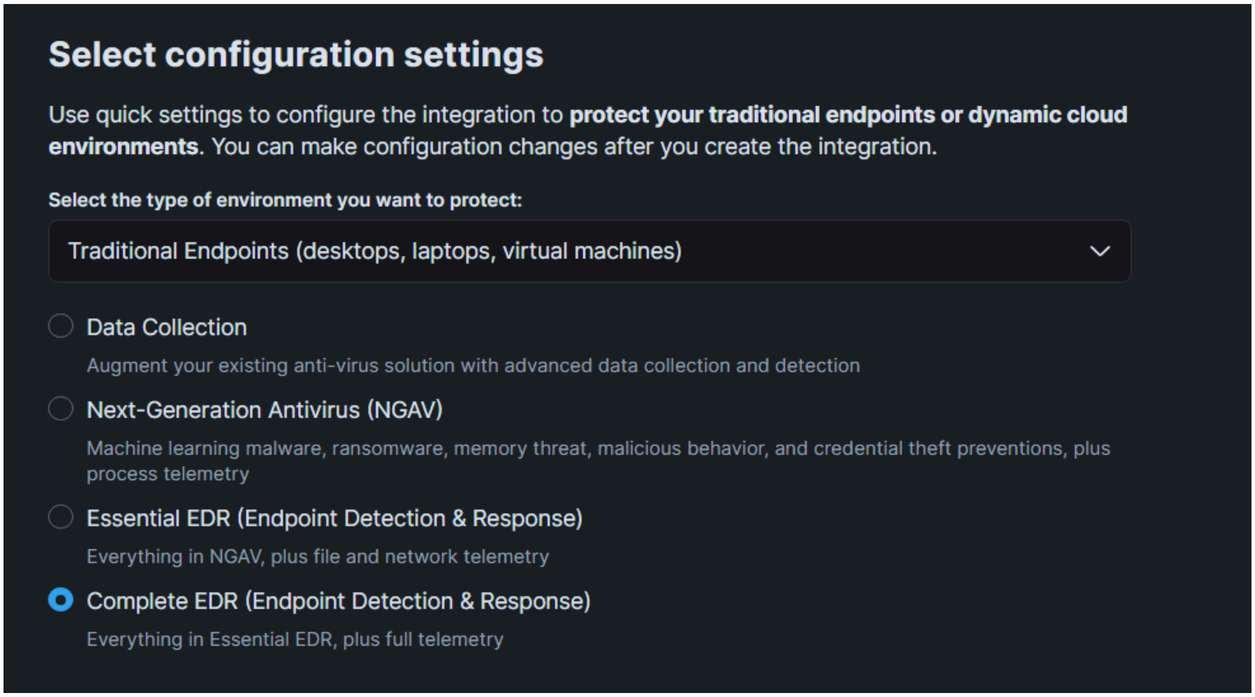
Integration name

SIEM Lab

Description Optional

Project

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



Select configuration settings

Use quick settings to configure the integration to **protect your traditional endpoints or dynamic cloud environments.** You can make configuration changes after you create the integration.

Select the type of environment you want to protect:

Traditional Endpoints (desktops, laptops, virtual machines)

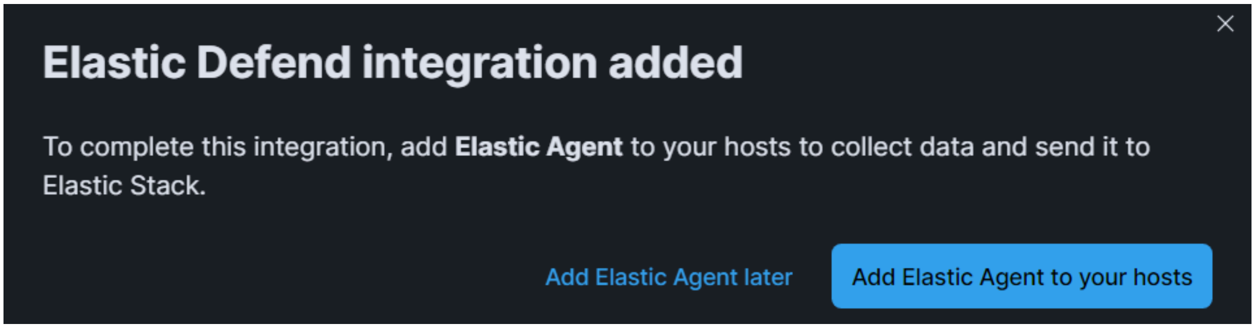
○ Data Collection
Augment your existing anti-virus solution with advanced data collection and detection

○ Next-Generation Antivirus (NGAV)
Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry

○ Essential EDR (Endpoint Detection & Response)
Everything in NGAV, plus file and network telemetry

● Complete EDR (Endpoint Detection & Response)
Everything in Essential EDR, plus full telemetry

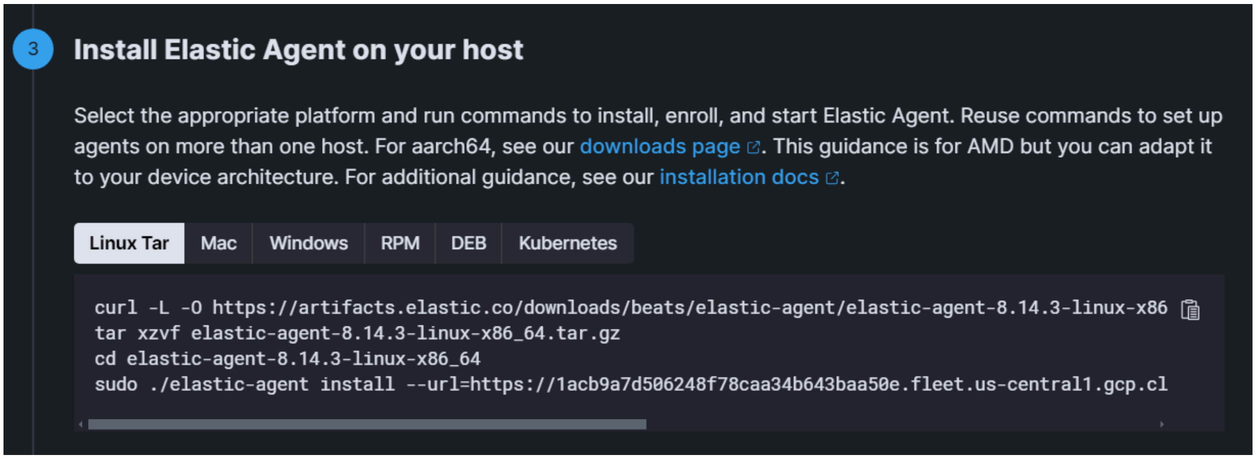
I will click ‘Add Elastic Agent to your hosts’.



Elastic Defend integration added

To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack.

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

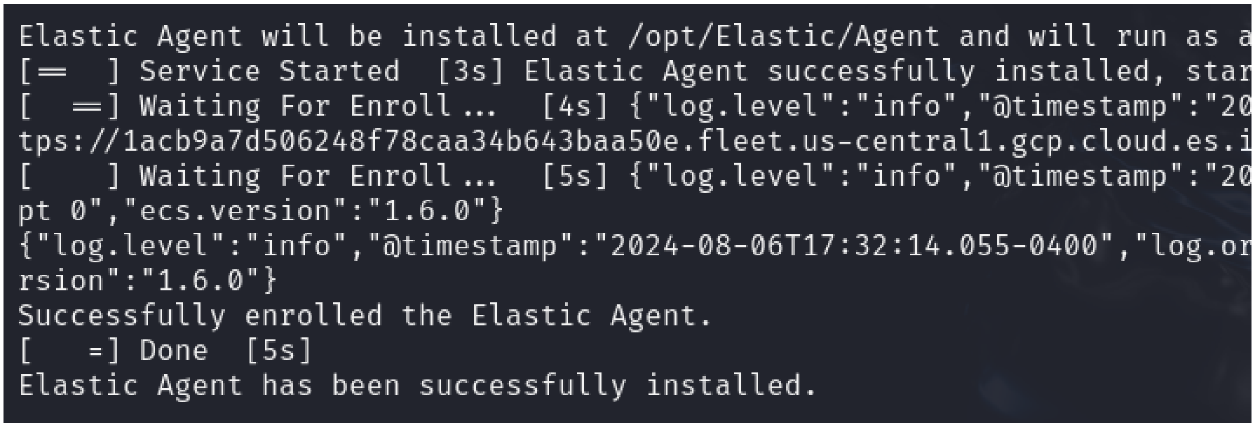


3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

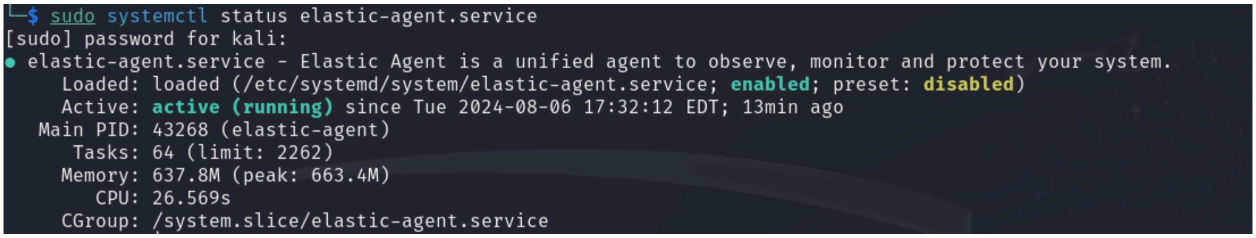
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.14.3-linux-x86
tar xzvf elastic-agent-8.14.3-linux-x86_64.tar.gz
cd elastic-agent-8.14.3-linux-x86_64
sudo ./elastic-agent install --url=https://1acb9a7d506248f78caa34b643baa50e.fleet.us-central1.gcp.cl
```

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



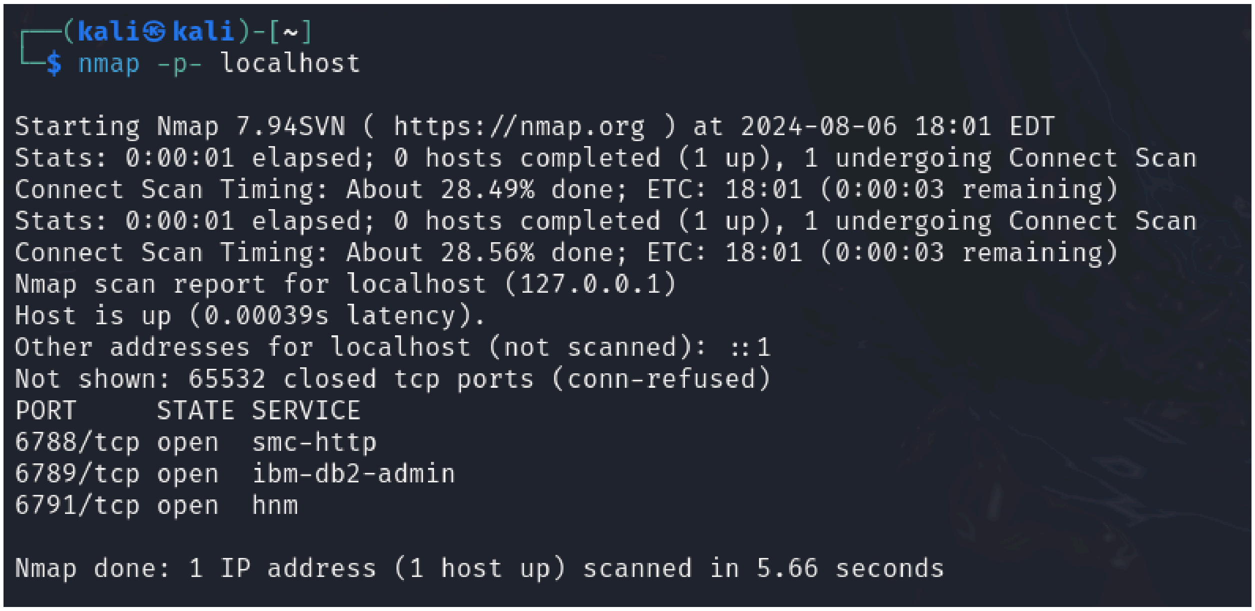
```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a
[==  ] Service Started  [3s] Elastic Agent successfully installed, star
[  ==] Waiting For Enroll ...  [4s] {"log.level":"info","@timestamp":"20
tps://1acb9a7d506248f78caa34b643baa50e.fleet.us-central1.gcp.cloud.es.i
[    ] Waiting For Enroll ...  [5s] {"log.level":"info","@timestamp":"20
pt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-08-06T17:32:14.055-0400","log.or
rsion":"1.6.0"}
Successfully enrolled the Elastic Agent.
[   =] Done  [5s]
Elastic Agent has been successfully installed.
```

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

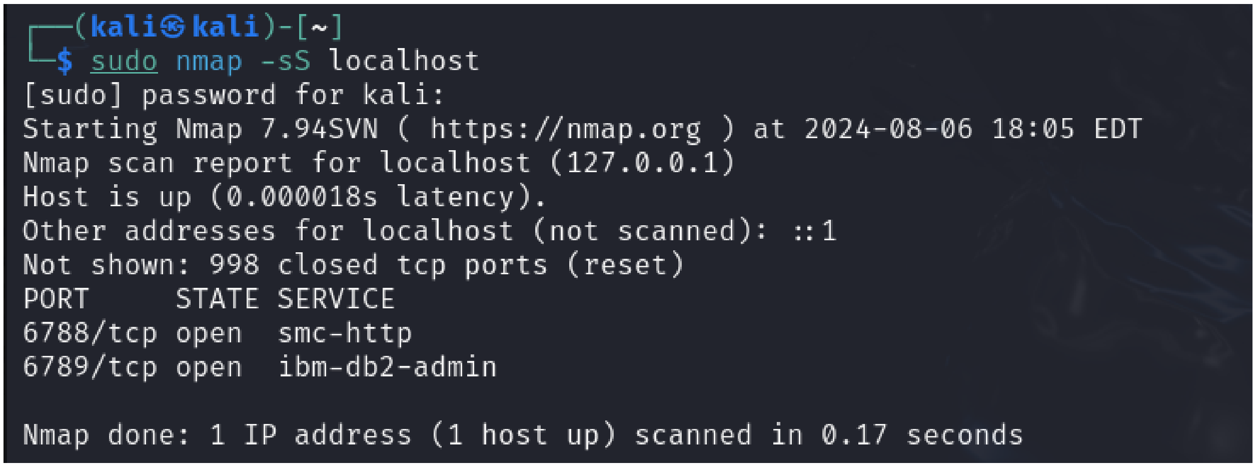


```
└─$ sudo systemctl status elastic-agent.service
[sudo] password for kali:
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
     Active: active (running) 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.

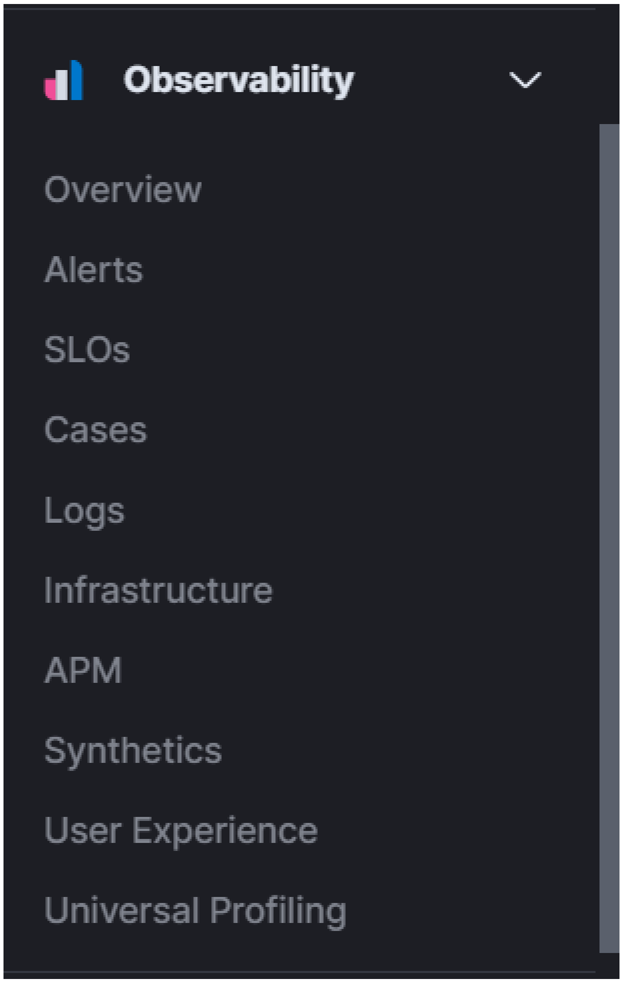


```
┌──(kali㉿kali)-[~]
└─$ nmap -p- localhost

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
```

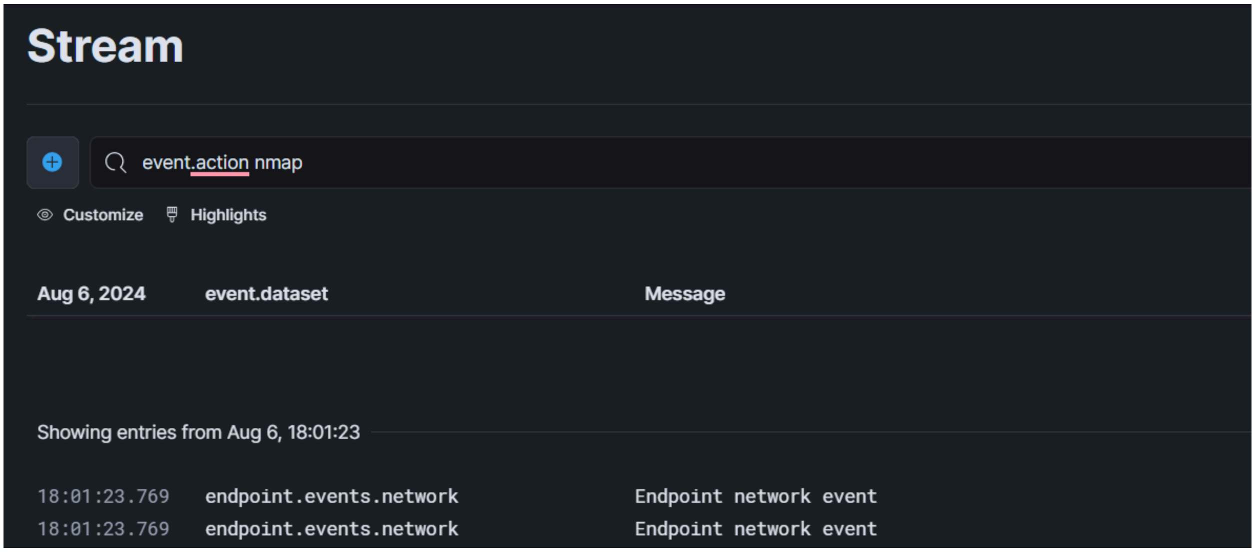


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS localhost
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 18:05 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (reset)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

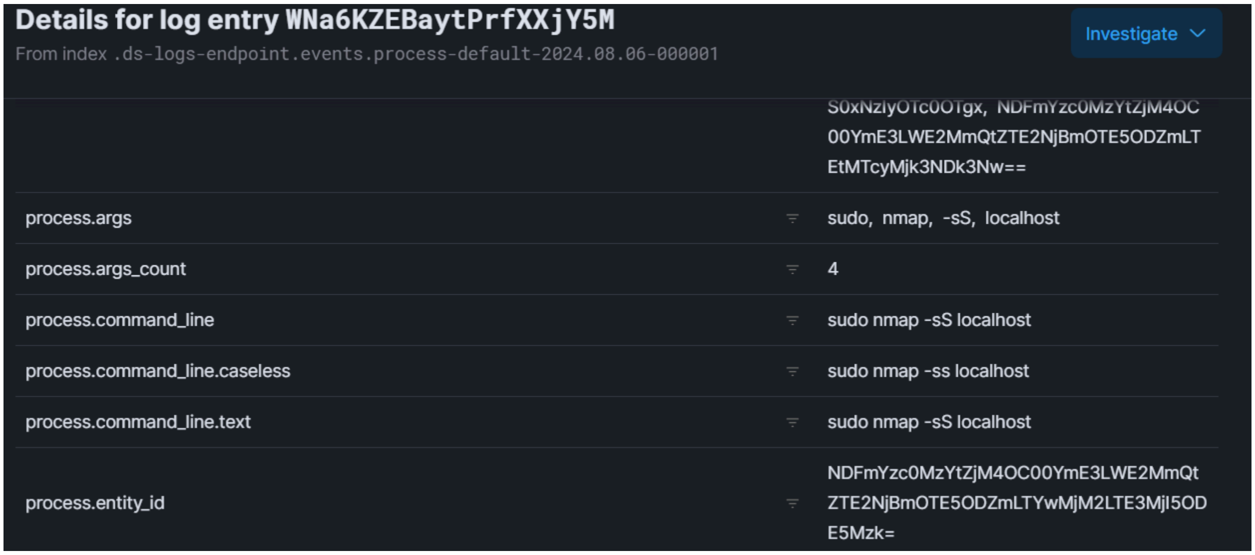


In the search option, I will search for ‘event.action nmap’.



```
event.action nmap

Aug 6, 2024    event.dataset                   Message

Showing entries from Aug 6, 18:01:23

18:01:23.769   endpoint.events.network         Endpoint network event
18:01:23.769   endpoint.events.network         Endpoint network event
```

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’.

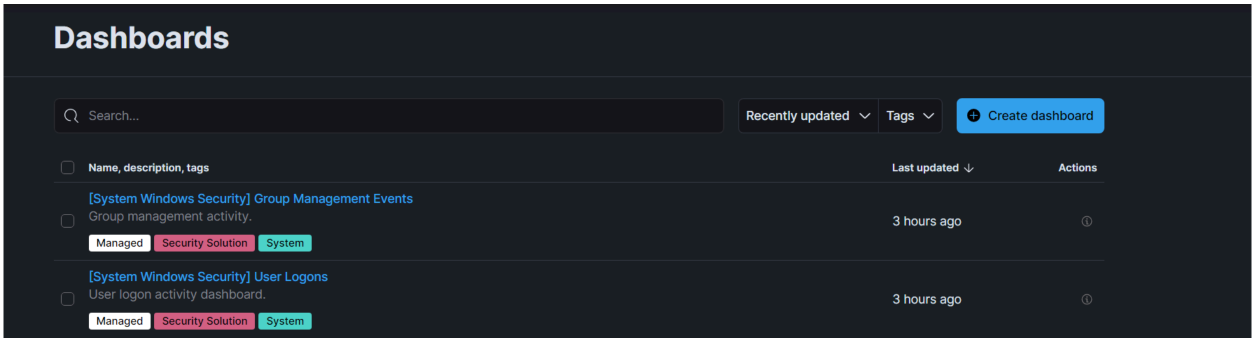


Details for log entry WNa6KZEBaytPrfXXjY5M

From index .ds-logs-endpoint.events.process-default-2024.08.06-000001

	S0xNzIyOTc0OTgx, NDFmYzc0MzYtZjM4OC00YmE3LWE2MmQtZTE2NjBmOTE5ODZmLTEtMTcyMjk3NDk3Nw==
process.args	sudo, nmap, -sS, localhost
process.args_count	4
process.command_line	sudo nmap -sS localhost
process.command_line.caseless	sudo nmap -ss localhost
process.command_line.text	sudo nmap -sS localhost
process.entity_id	NDFmYzc0MzYtZjM4OC00YmE3LWE2MmQtZTE2NjBmOTE5ODZmLTYwMjM2LTE3MjI5ODE5Mzk=

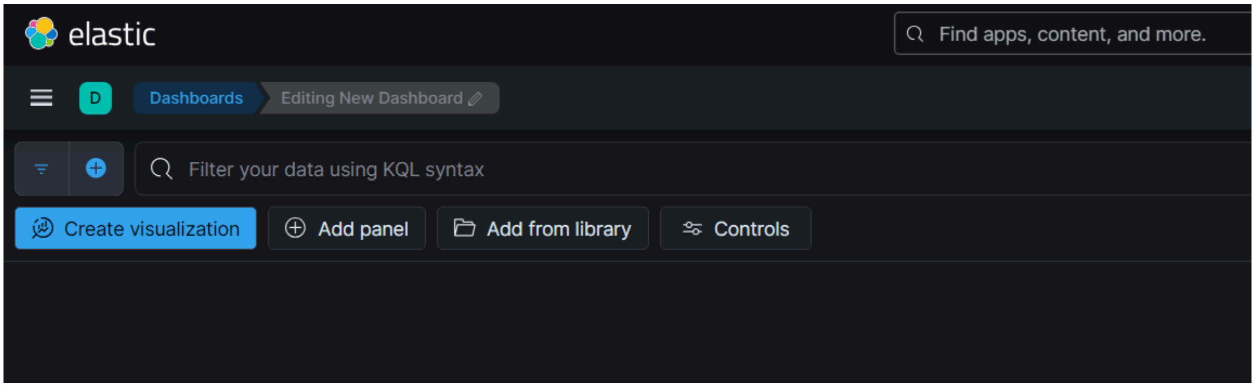
I can see the command that I used ‘sudo nmap -sS localhost’’. Now I will create a Dashboard to Visualize the Events. To do that, I will open the dashboard. Then I will click ‘create dashboard’.



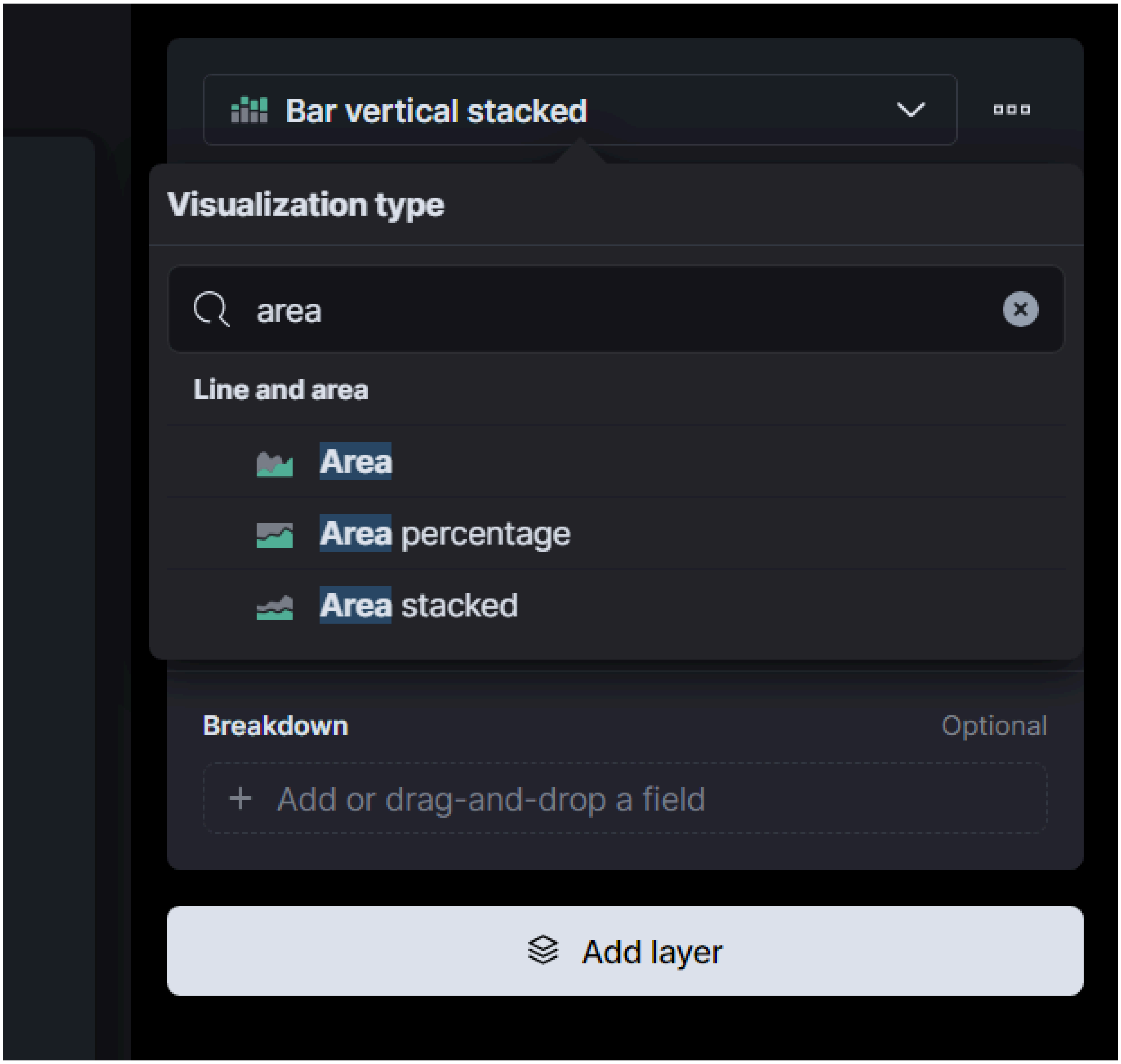
Dashboards

Name, description, tags	Last updated	Actions
[System Windows Security] Group Management Events Group management activity. Managed Security Solution System	3 hours ago	ⓘ
[System Windows Security] User Logons User logon activity dashboard. Managed Security Solution System	3 hours ago	ⓘ

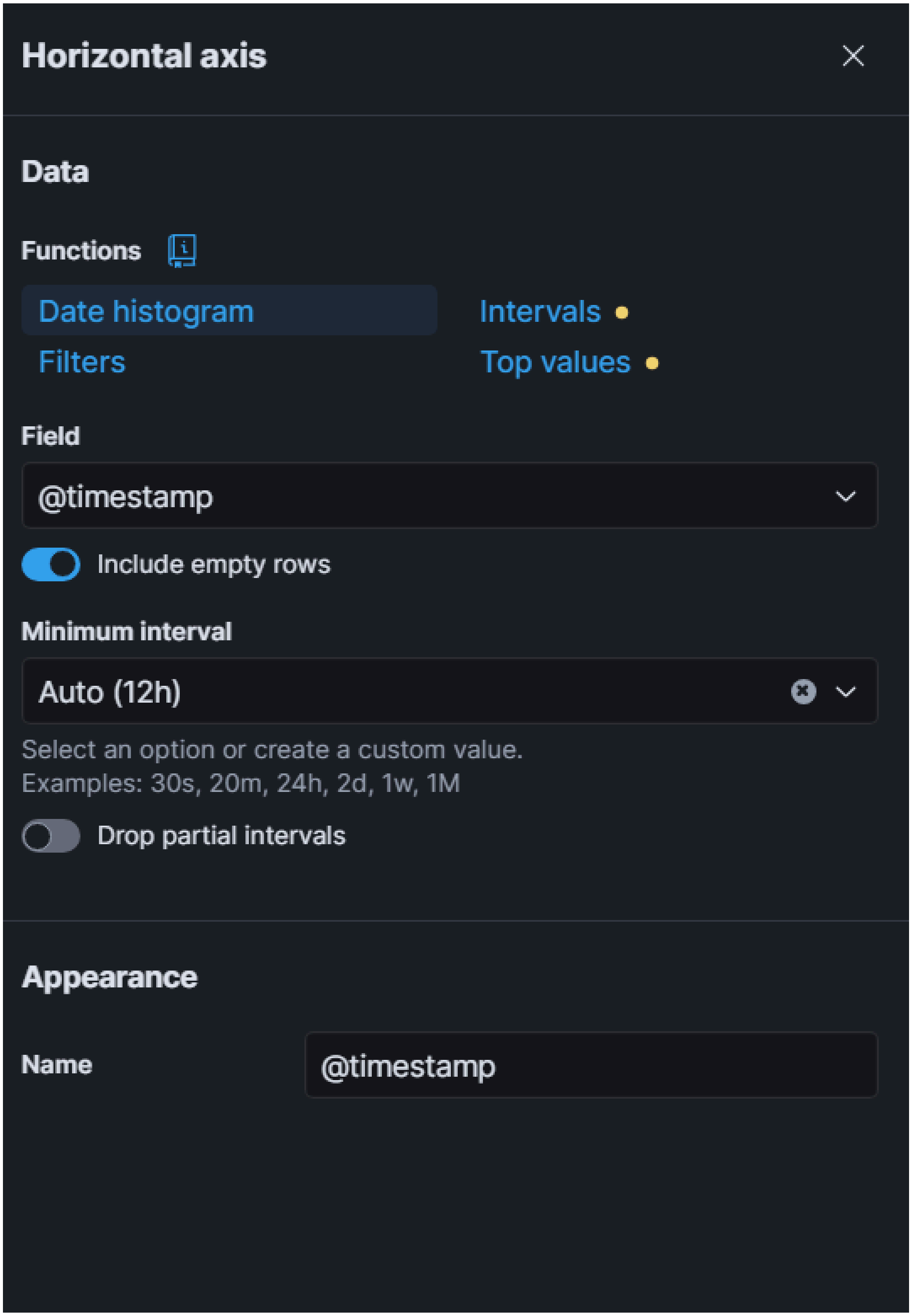
I will click the “Create Visualization” button to create a new visualization.



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

Field

@timestamp

Include empty rows

Minimum interval

Auto (12h)

Select an option or create a custom value.
Examples: 30s, 20m, 24h, 2d, 1w, 1M

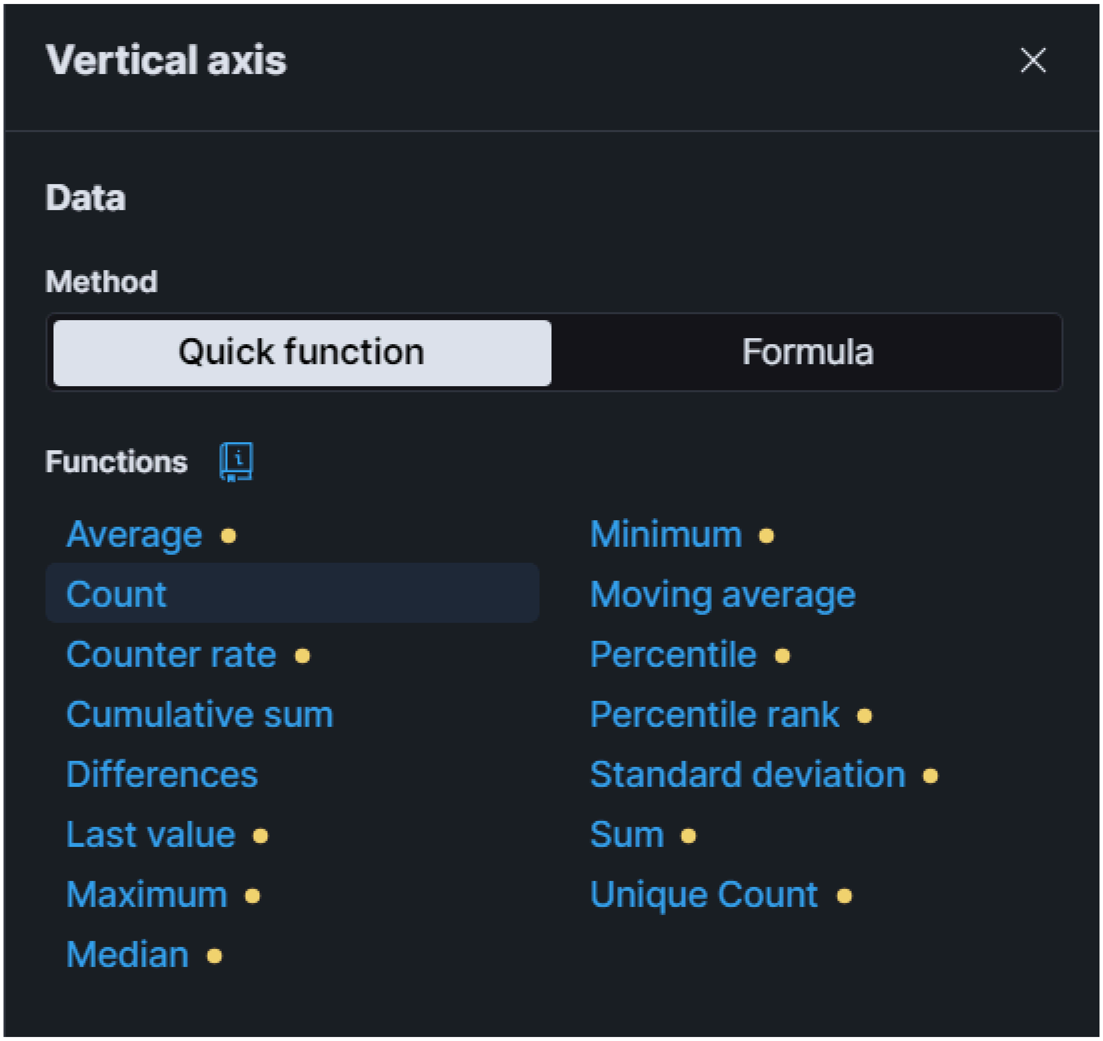
Drop partial intervals

Appearance

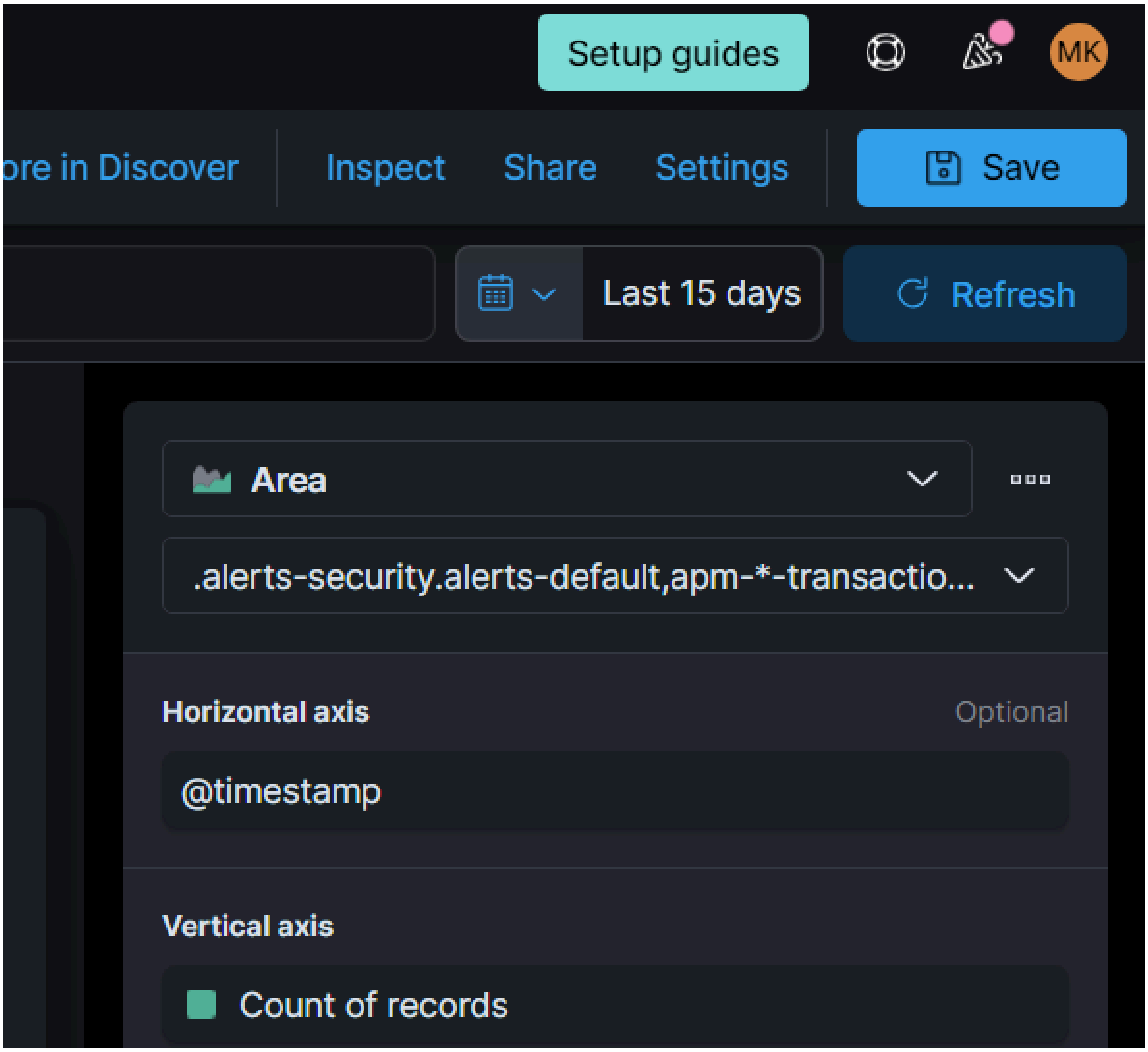
Name

@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.



Area

.alerts-security.alerts-default,apm-*-transactio...

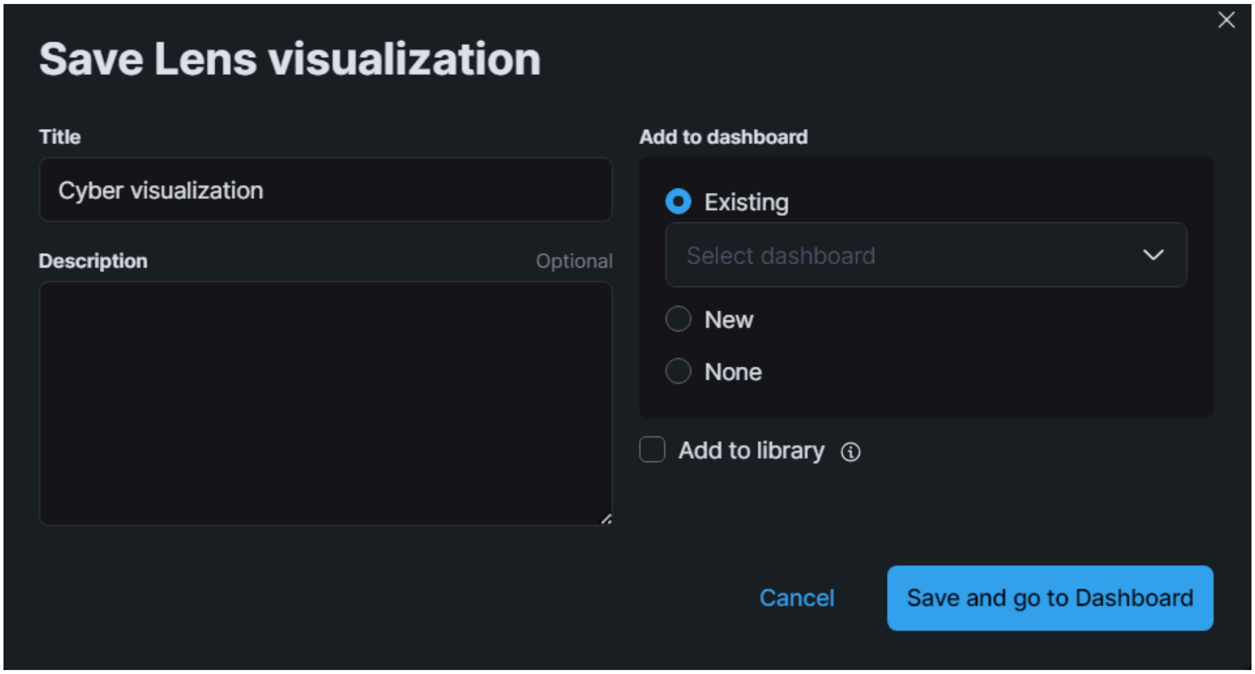
Horizontal axis Optional

@timestamp

Vertical axis

🟩 Count of records

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



Save Lens visualization

Title

Cyber visualization

Description

Optional

Add to dashboard

● Existing

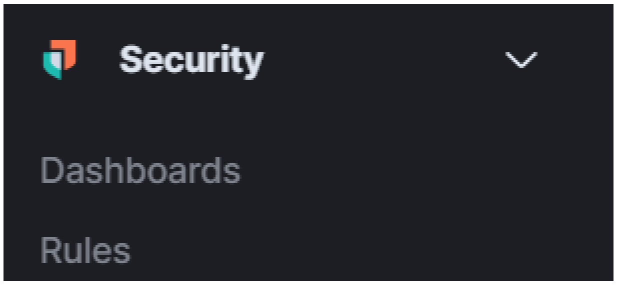
Select dashboard

○ New

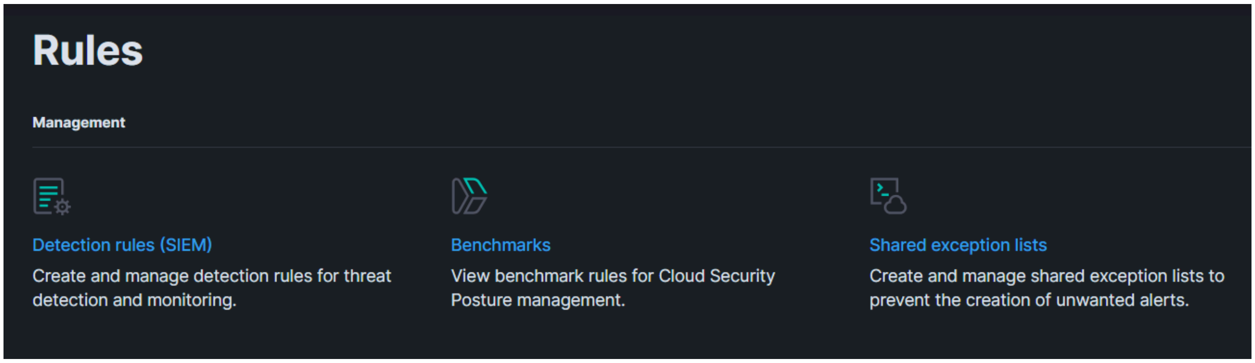
○ None

□ Add to library

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)’.



Rules

Management

Detection rules (SIEM)

Create and manage detection rules for threat detection and monitoring.

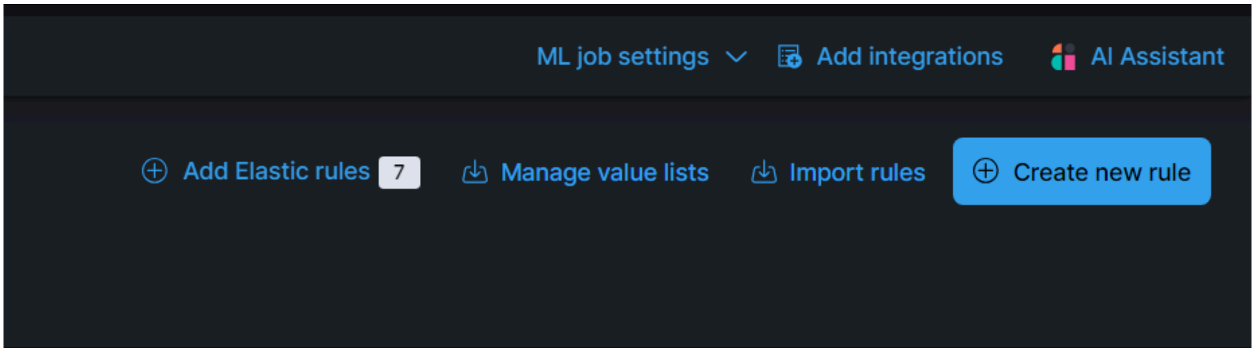
Benchmarks

View benchmark rules for Cloud Security Posture management.

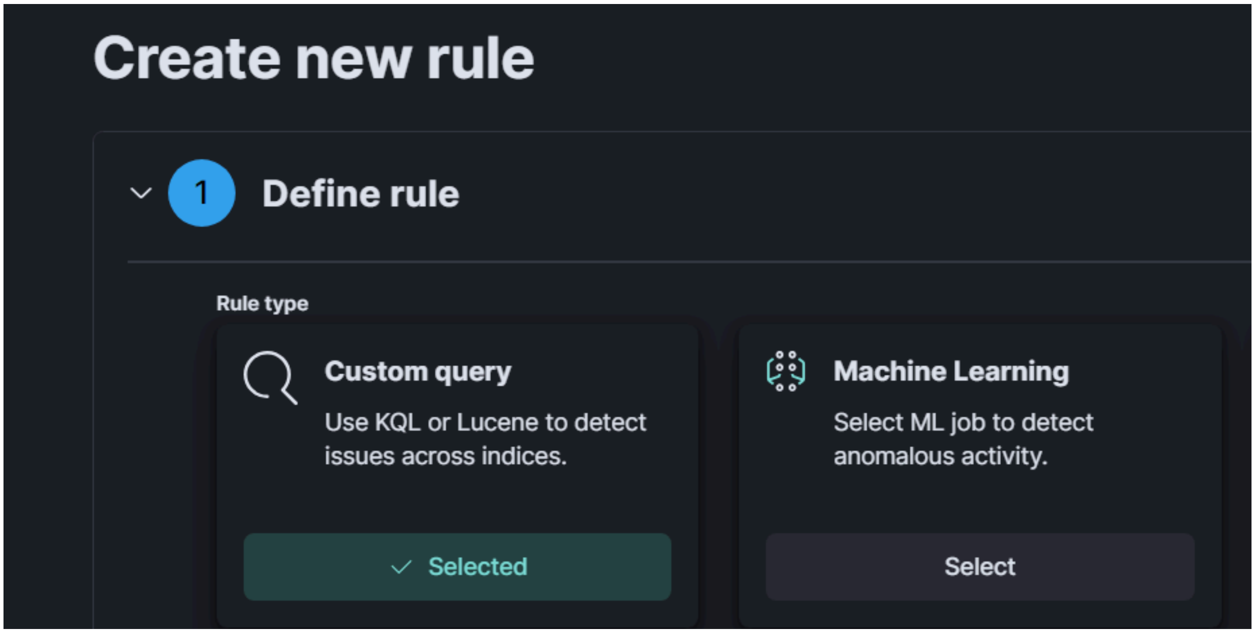
Shared exception lists

Create and manage shared exception lists to prevent the creation of unwanted alerts.

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



I will click ‘Custom query’.


Create new rule

1 Define rule

Rule type

Custom query

Use KQL or Lucene to detect issues across indices.

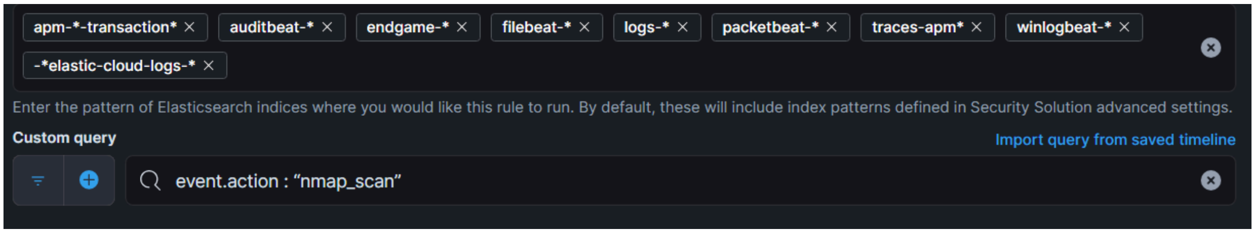
✓ Selected

Machine Learning

Select ML job to detect anomalous activity.

Select

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

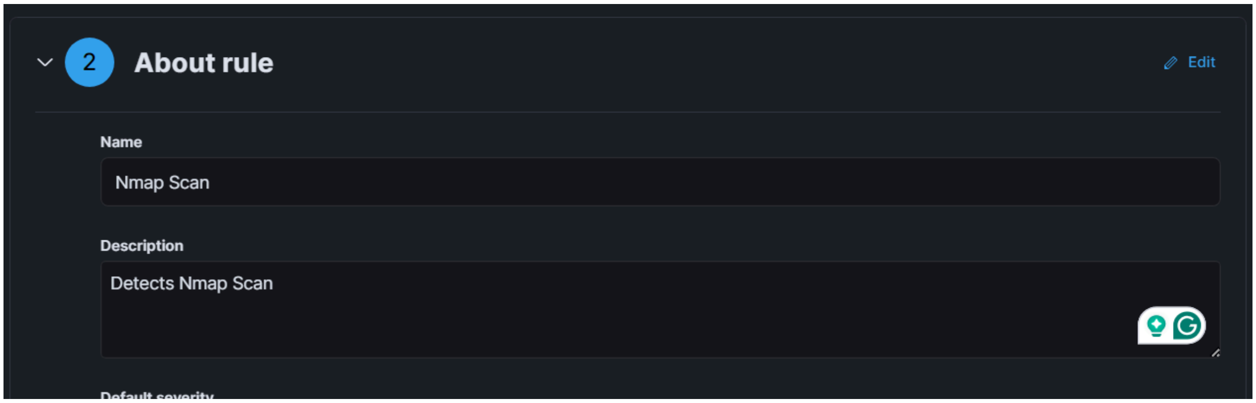


Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query

```
event.action : “nmap_scan”
```

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’.

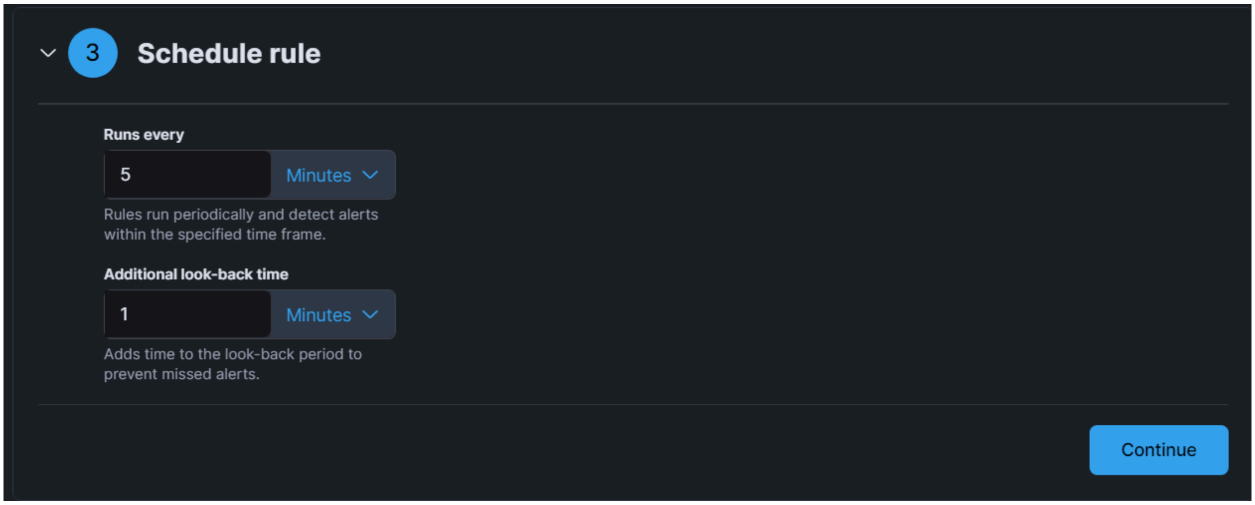


Name: Nmap Scan

Description: Detects Nmap Scan

Default severity

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



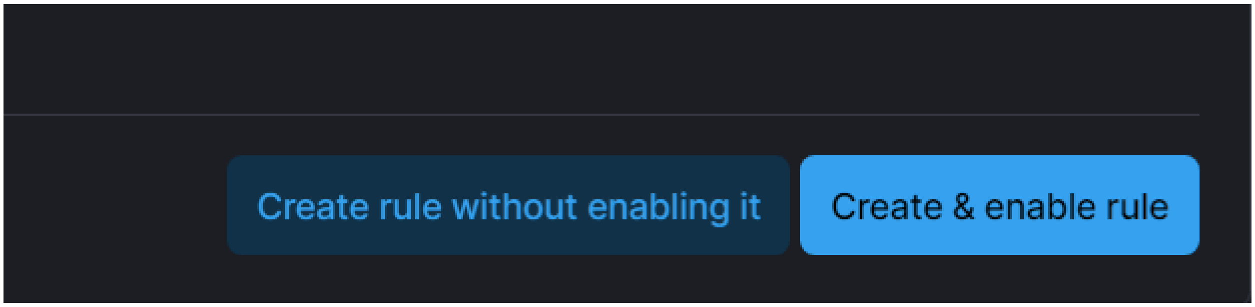
Runs every: 5 Minutes

Rules run periodically and detect alerts within the specified time frame.

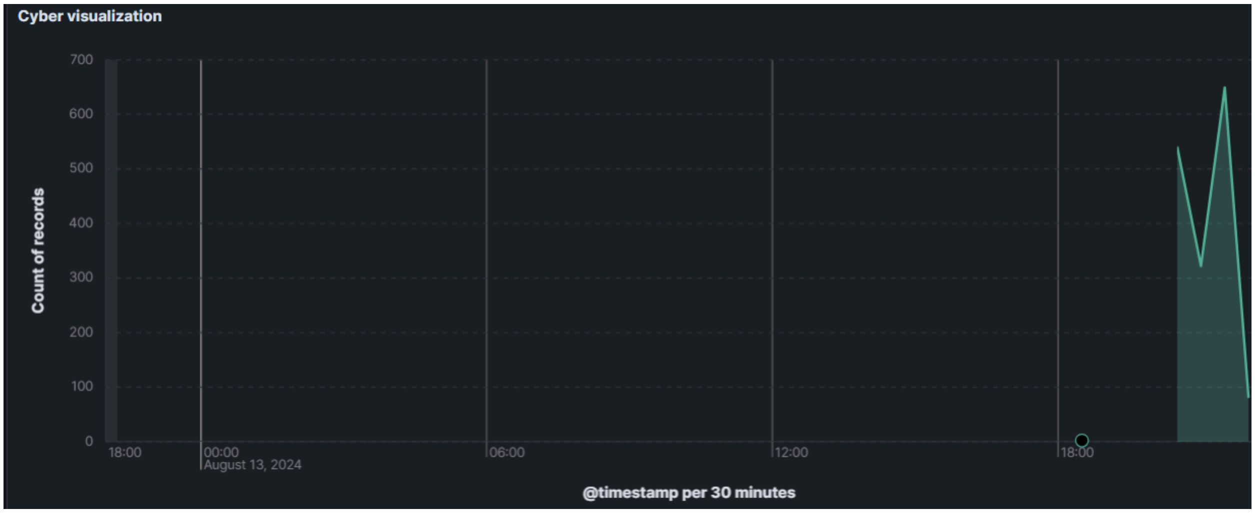
Additional look-back time: 1 Minutes

Adds time to the look-back period to prevent missed alerts.

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.


Cyber visualization
Count of records
18:00
00:00
August 13, 2024
06:00
12:00
18:00
@timestamp per 30 minutes