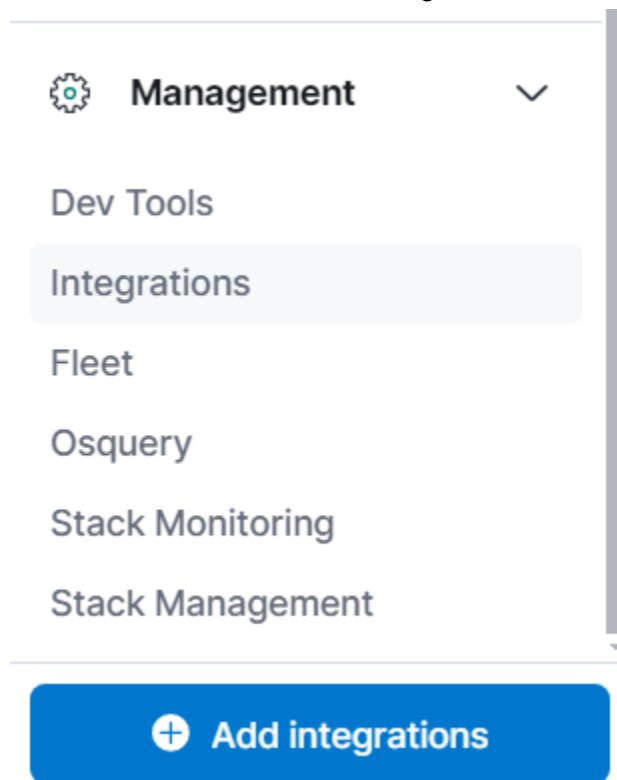


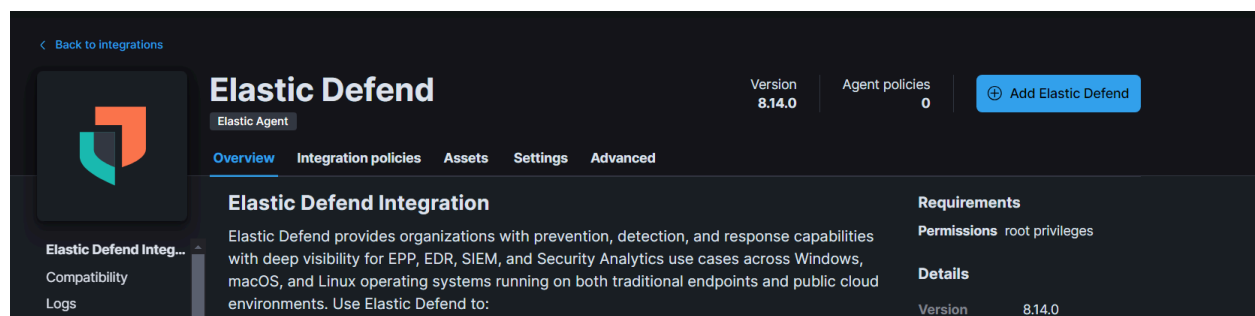
**Description:** The goal of this project is to demonstrate how to perform Nmap scans using Kali Linux and set up an SIEM Lab with Elastic SIEM to detect and monitor these scans. The project includes creating custom dashboards to visualize the events and setting up alerts that trigger whenever a Nmap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

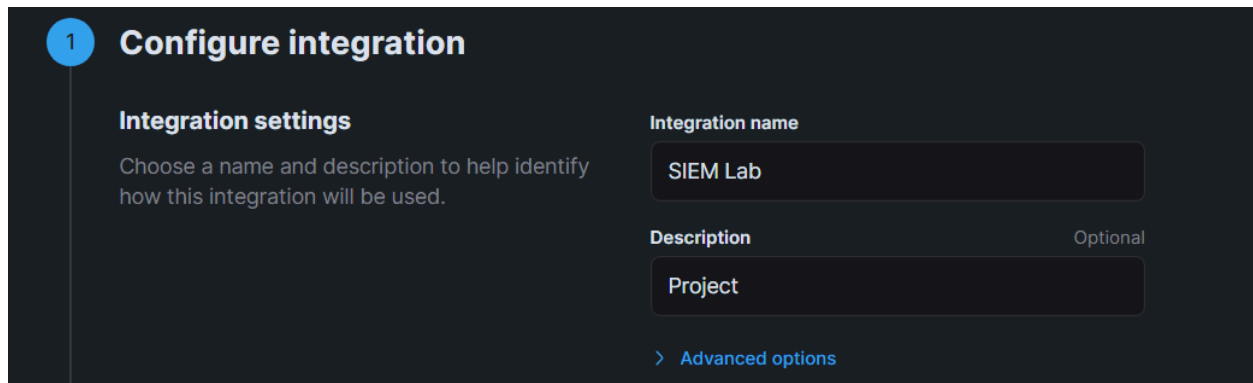
**Project:** First I need to log in to Elastic in the browser and on the left option, I will click and go to the bottom and choose Add integrations.



I will add Elastic Defend.

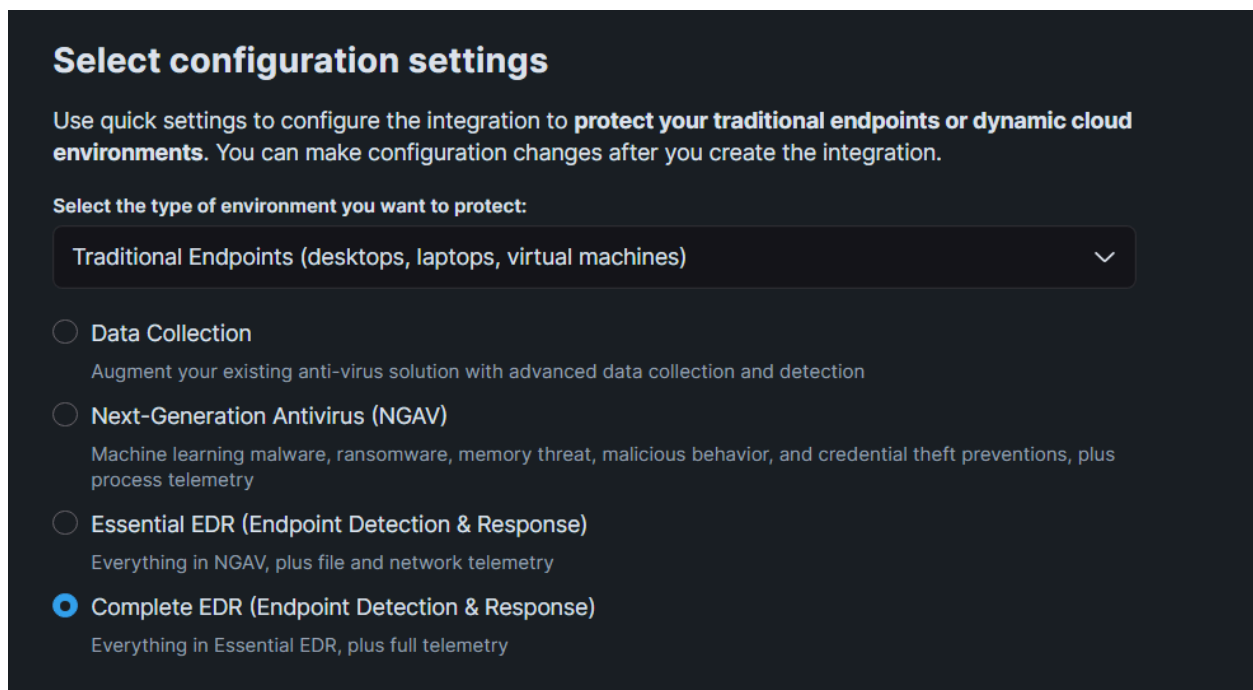


I have to choose the Integration name and description name. For this project, I will name it “SIEM Lab” and “Project”.



The screenshot shows a dark-themed interface for configuring an integration. On the left, a blue circle with the number '1' is next to the heading 'Configure integration'. Below this, the section 'Integration settings' is followed by a descriptive text: 'Choose a name and description to help identify how this integration will be used.' To the right, there are two input fields. The first is labeled 'Integration name' and contains the text 'SIEM Lab'. The second is labeled 'Description' and contains the text 'Project'; it is also marked as 'Optional'. At the bottom right of the form, there is a link that says '> Advanced options'.

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



The screenshot shows a dark-themed interface for selecting configuration settings. The heading is 'Select configuration settings', followed by a paragraph: '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.' Below this, a dropdown menu is labeled 'Select the type of environment you want to protect:' and currently shows 'Traditional Endpoints (desktops, laptops, virtual machines)'. Underneath the dropdown are four radio button options. The first is 'Data Collection' with the subtext 'Augment your existing anti-virus solution with advanced data collection and detection'. The second is 'Next-Generation Antivirus (NGAV)' with the subtext 'Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry'. The third is 'Essential EDR (Endpoint Detection & Response)' with the subtext 'Everything in NGAV, plus file and network telemetry'. The fourth is 'Complete EDR (Endpoint Detection & Response)', which is selected (indicated by a blue dot) and has the subtext '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.

[Add Elastic Agent later](#)

[Add Elastic Agent to your hosts](#)

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](#).

Linux Tar

Mac

Windows

RPM

DEB

Kubernetes

```
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

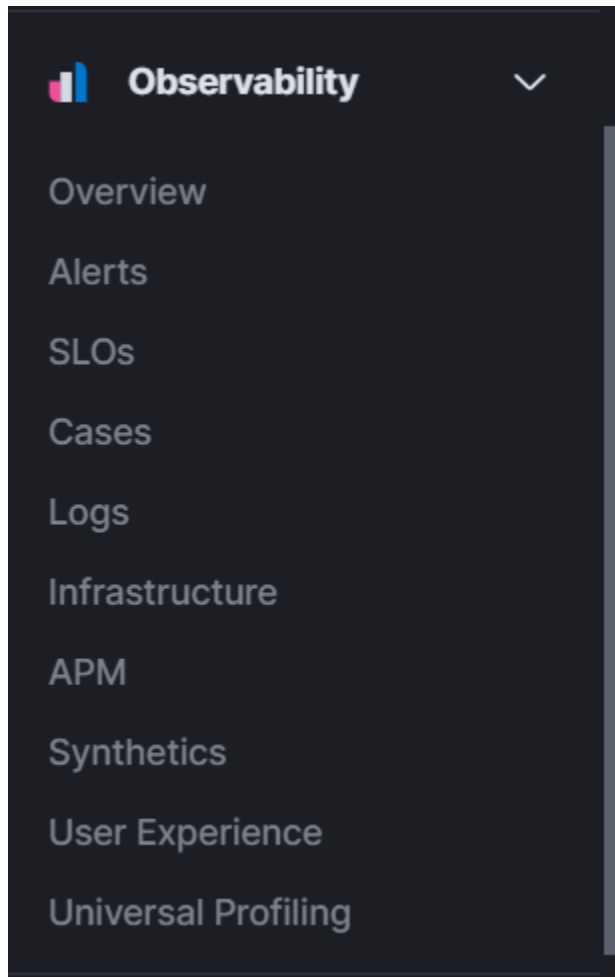
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 18:01 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.49% done; ETC: 18:01 (0:00:03 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan 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'.

# Stream

event.action nmap

Customize

Highlights

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'.

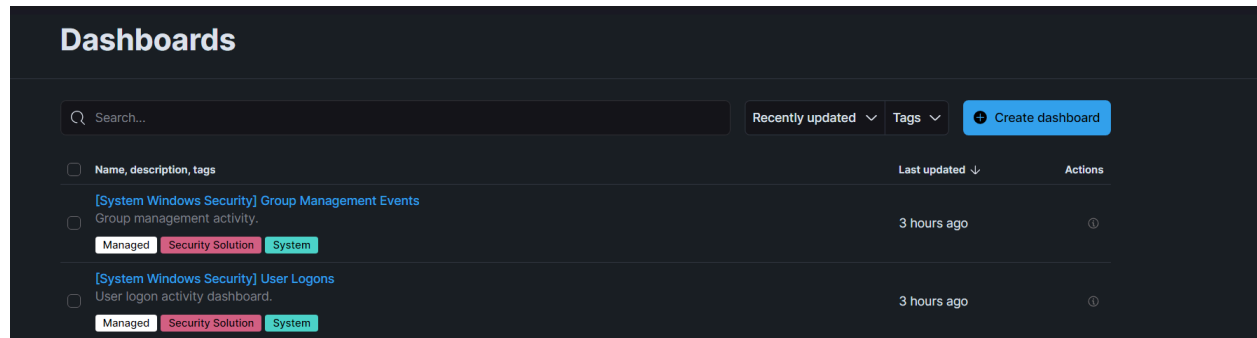
## Details for log entry WNa6KZEBaytPrfXXjY5M

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

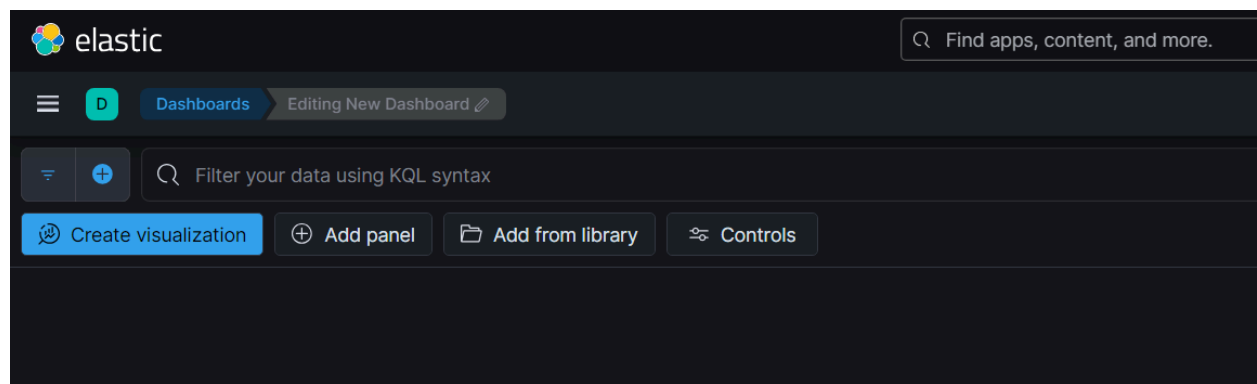
Investigate

	S0xNzIyOTc0OTgx, NDFmYzc0MzYtZjM4OC00YmE3LWE2MmQtZTE2NjBmOTE5ODZmLTI0MTcyMjk3NDk3NW==
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	NDFmYzc0MzYtZjM4OC00YmE3LWE2MmQtZTE2NjBmOTE5ODZmLTYwMjM2LTE3MjI5ODU5Mzk=

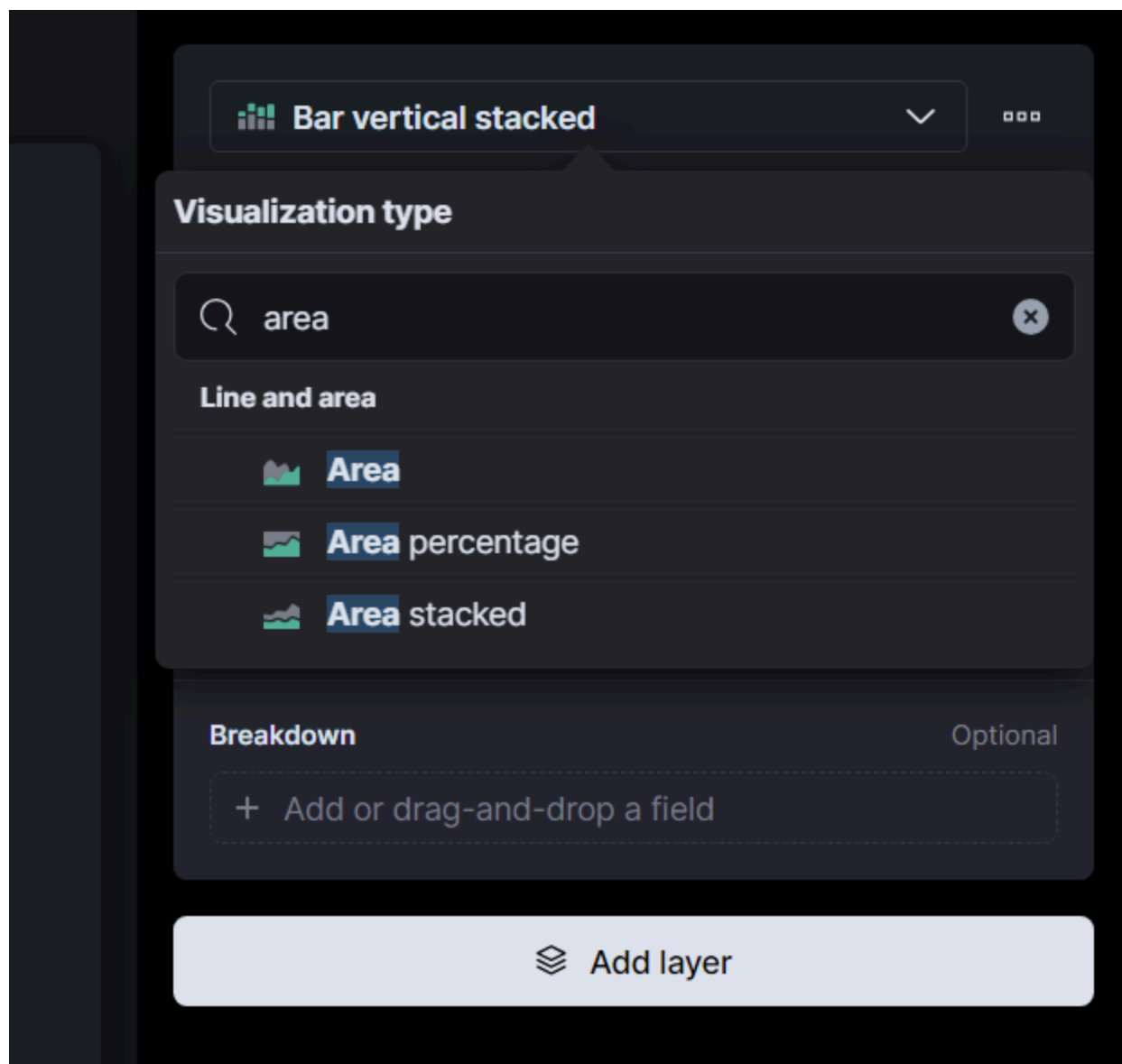
I can see the command that I used 'sudo nmap -sS localhost'. Now I will create a Dashboard to Visualize the Events. To do that, I will open the dashboard. Then I will click 'create dashboard'.



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



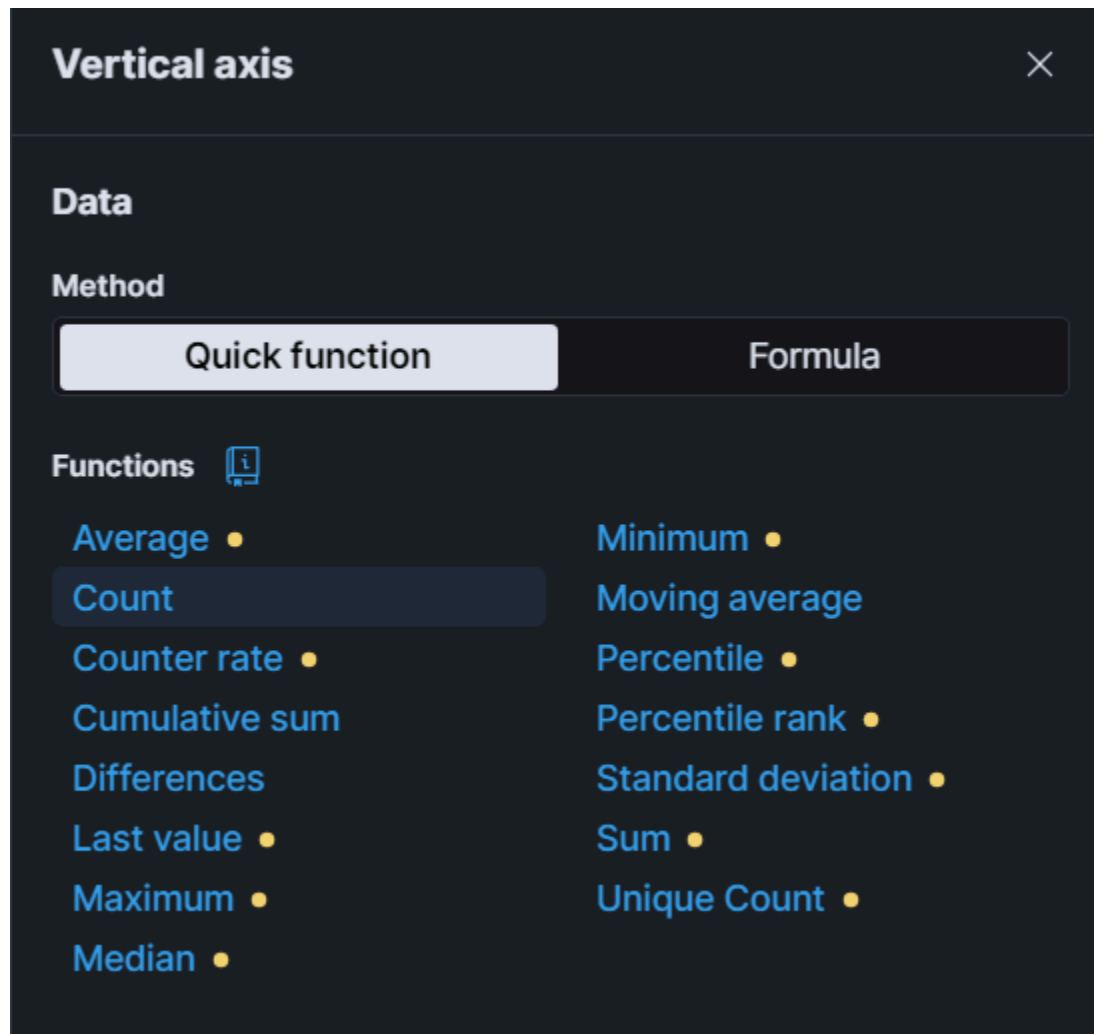
Drop partial intervals

### Appearance

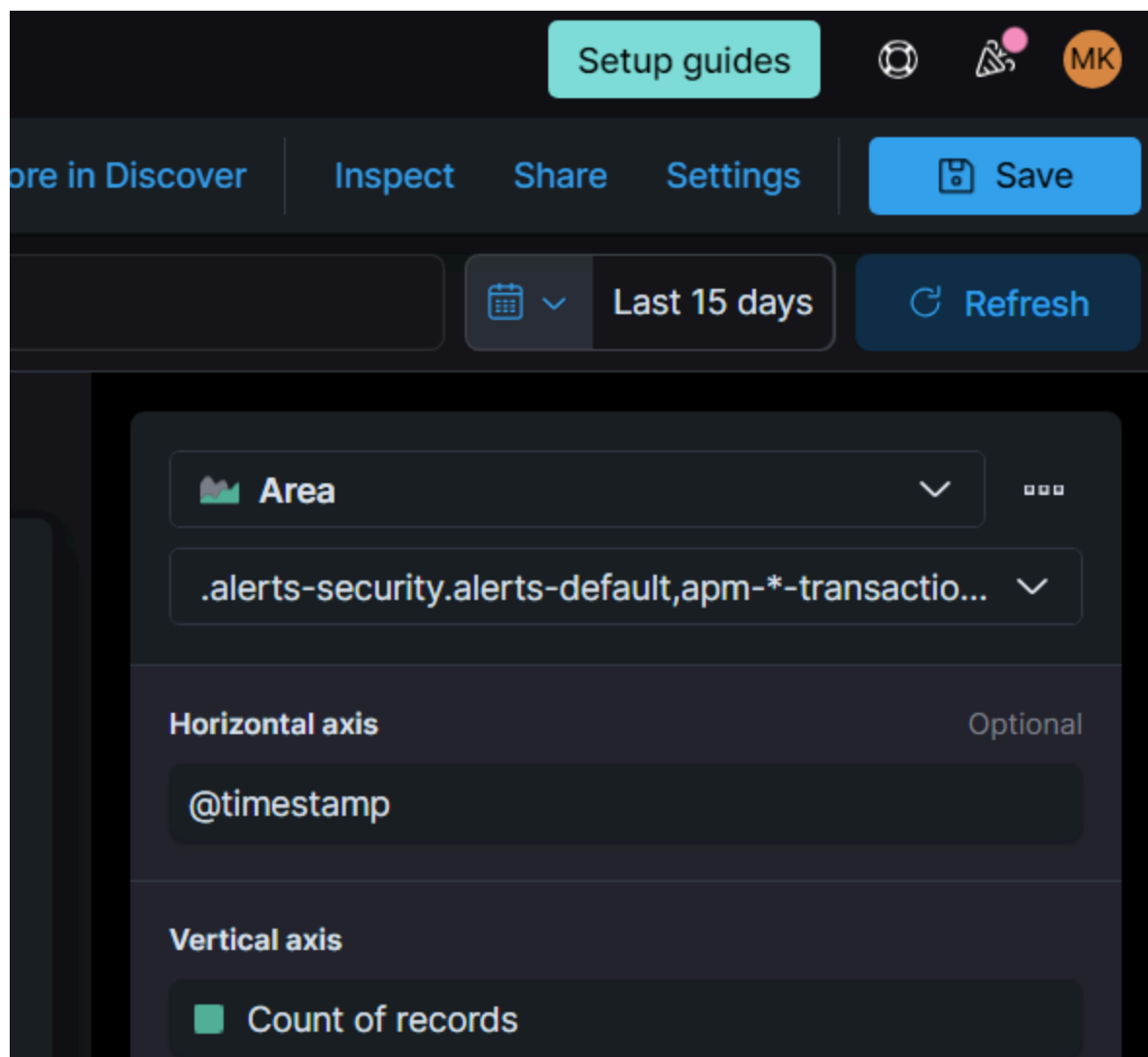
Name

@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'.

# Save Lens visualization

Title

Cyber visualization

Description

Optional

Add to dashboard

☒ Existing

Select dashboard

☐ New

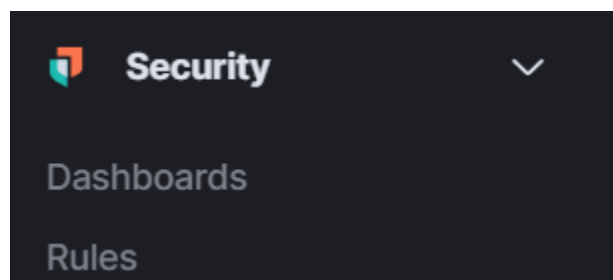
☐ None

☐ Add to library ⓘ

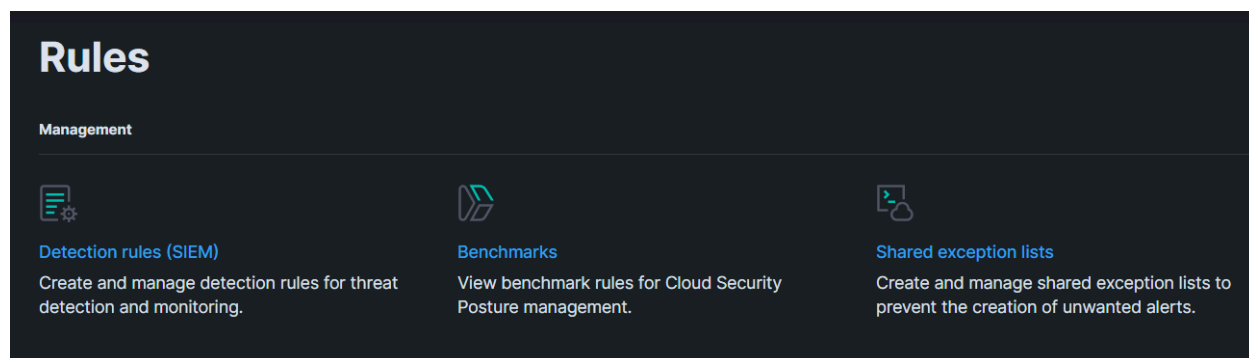
Cancel

Save and go to Dashboard

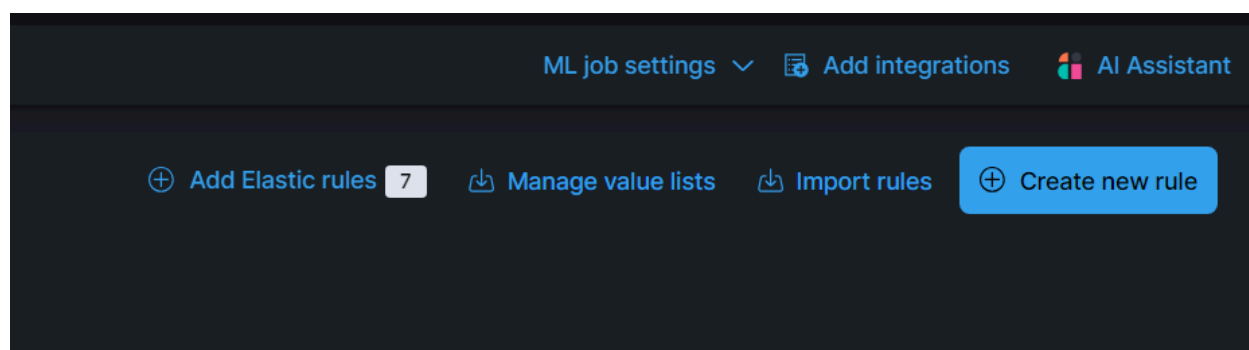
Now I will create an alert to monitor my logs for Nmap scan events and notify me if they are detected. In the Security section, I will click on the 'Rules' from the toggle menu.



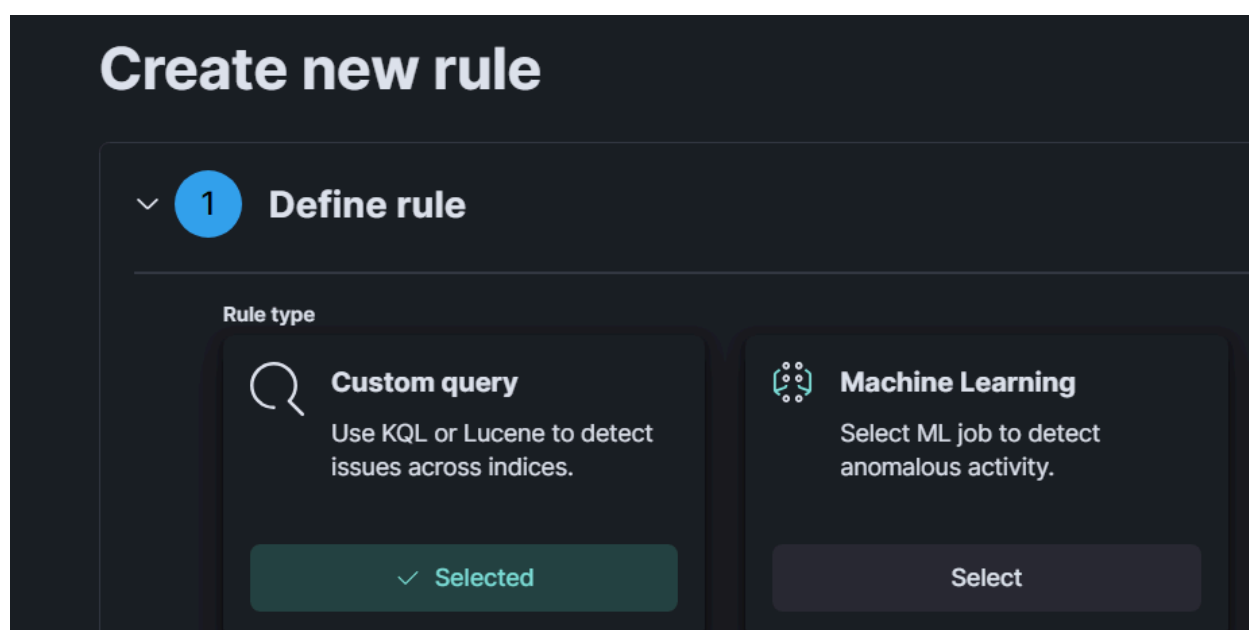
I will click the 'Detection rules (SIEM)'.



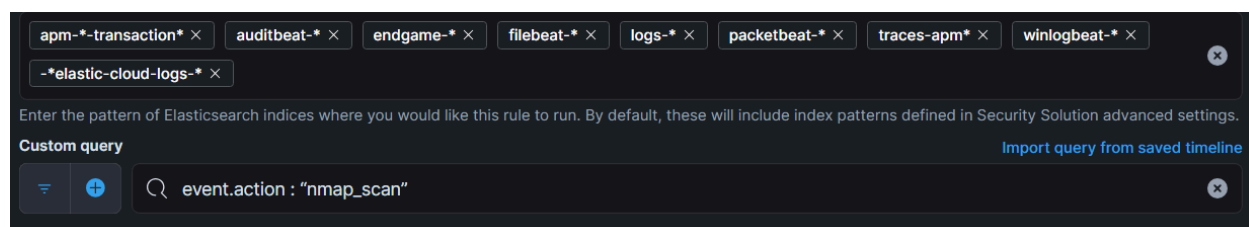
I will click the 'Create new rule' on the right.



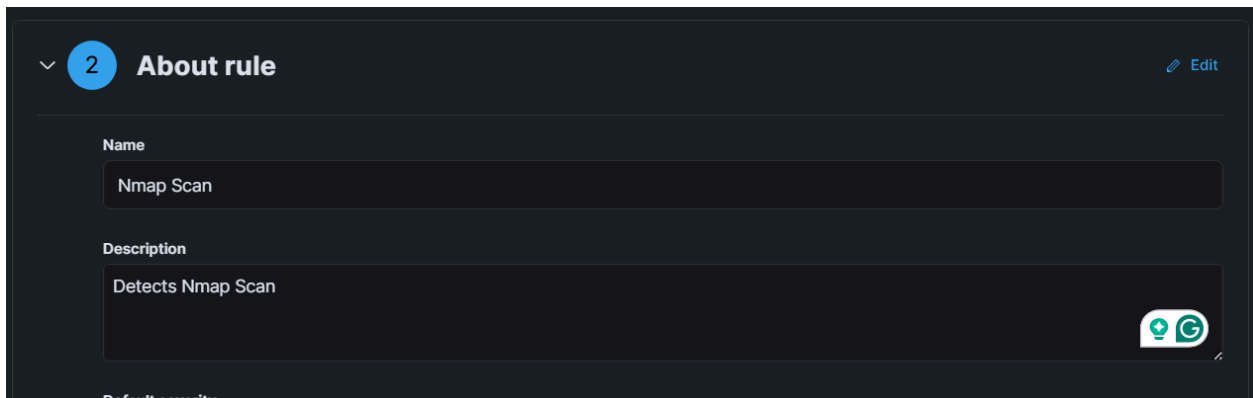
I will click 'Custom query'.



If I scroll down, I will see the Custom query section. I will type 'event.action: "nmap\_scan"' and click 'Continue'.

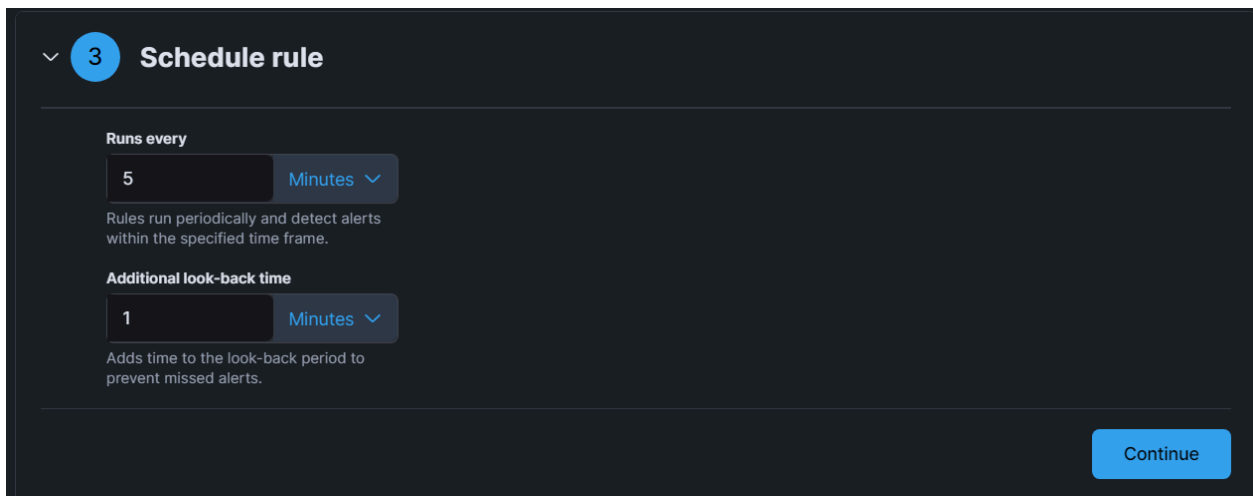


In the About rule section, I will name it 'Nmap Scan' and in the description section, I will name it 'Detects Nmap Scan'. Then I will click 'Continue'.



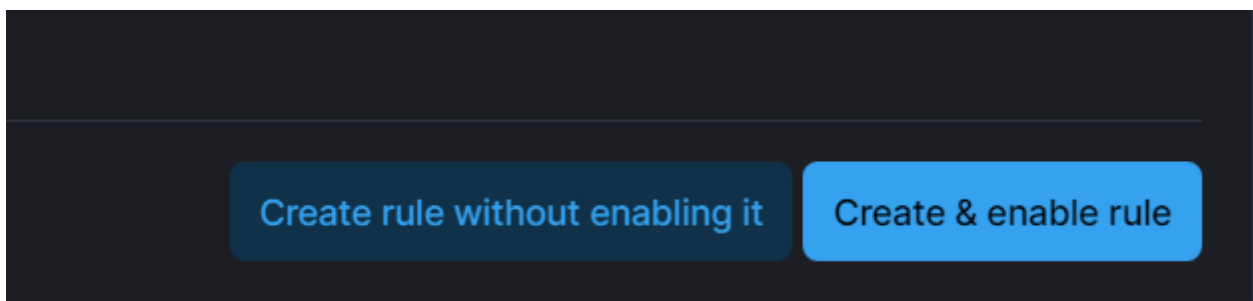
The screenshot shows the 'About rule' configuration screen. At the top, there is a header with a dropdown arrow, a blue circle containing the number '2', and the text 'About rule'. To the right of this header is an 'Edit' link with a pencil icon. Below the header, there are two input fields. The first is labeled 'Name' and contains the text 'Nmap Scan'. The second is labeled 'Description' and contains the text 'Detects Nmap Scan'. To the right of the description field is a small icon of a lightbulb and a green circle with a 'G'. At the bottom of the screen, the text 'Default severity' is partially visible.

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



The screenshot shows the 'Schedule rule' configuration screen. At the top, there is a header with a dropdown arrow, a blue circle containing the number '3', and the text 'Schedule rule'. Below the header, there are two sections. The first section is labeled 'Runs every' and contains a dropdown menu with the value '5' and a 'Minutes' dropdown with a downward arrow. Below this is a small text box that says 'Rules run periodically and detect alerts within the specified time frame.' The second section is labeled 'Additional look-back time' and contains a dropdown menu with the value '1' and a 'Minutes' dropdown with a downward arrow. Below this is a small text box that says 'Adds time to the look-back period to prevent missed alerts.' At the bottom right of the screen is a blue button labeled 'Continue'.

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



The screenshot shows the Rule actions screen. It features two large buttons. The first button is dark blue and labeled 'Create rule without enabling it'. The second button is light blue and labeled '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.

