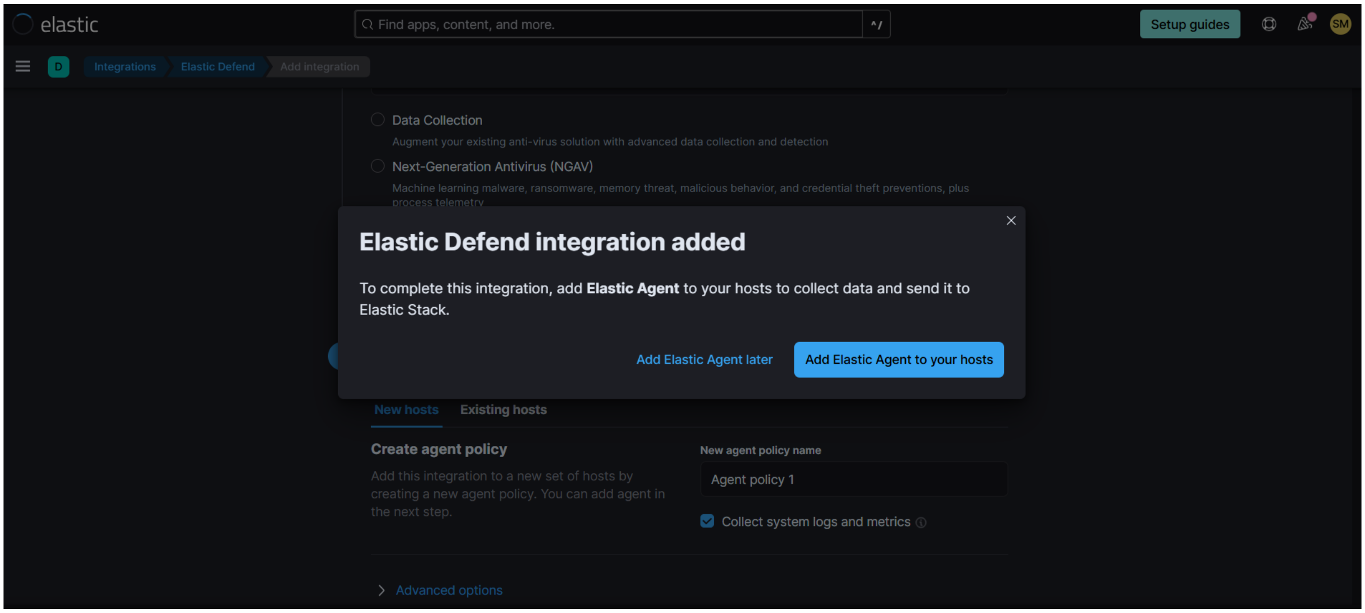
Home Lab for Elastic SIEM

This lab focuses on building a home Security Information and Event Management (SIEM) system using the Elastic Stack and a Kali Linux virtual machine. It allows us to collect, analyze, and visualize security logs in real-time, simulating and detecting threats.

We begin by setting up the environment with the following steps:

1- Create a free trial Elastic account
2- Set up the Linux virtual machine
3- Configure the agent to collect logs



○ 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

Elastic Defend integration added

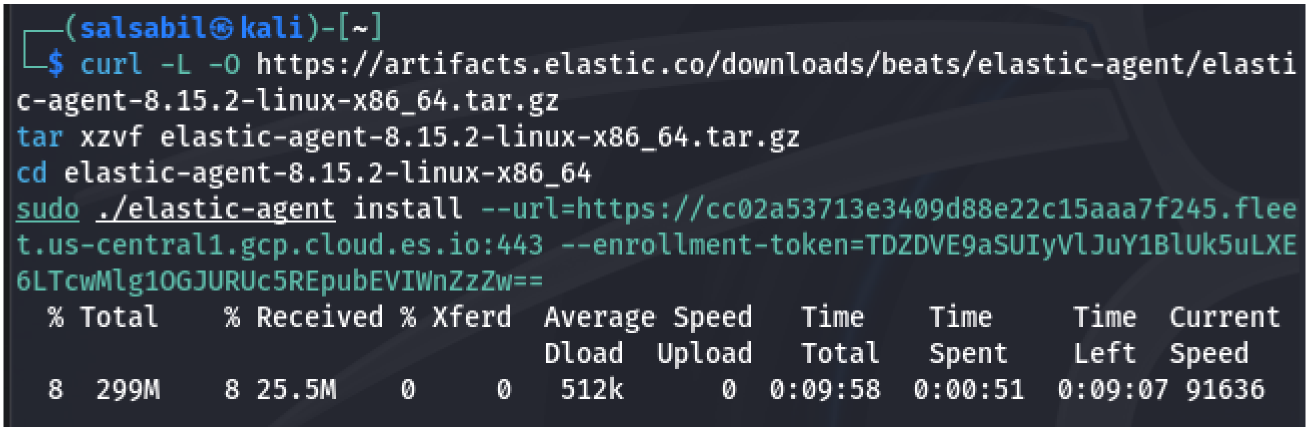
To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack.

Add Elastic Agent later | Add Elastic Agent to your hosts

Create agent policy
Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

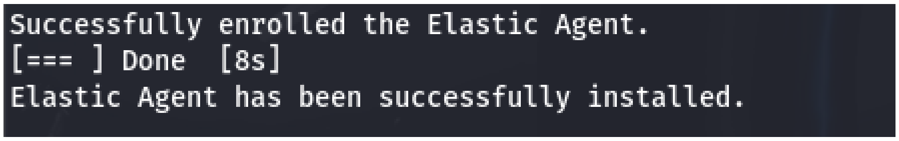
New agent policy name: Agent policy 1

☑ Collect system logs and metrics



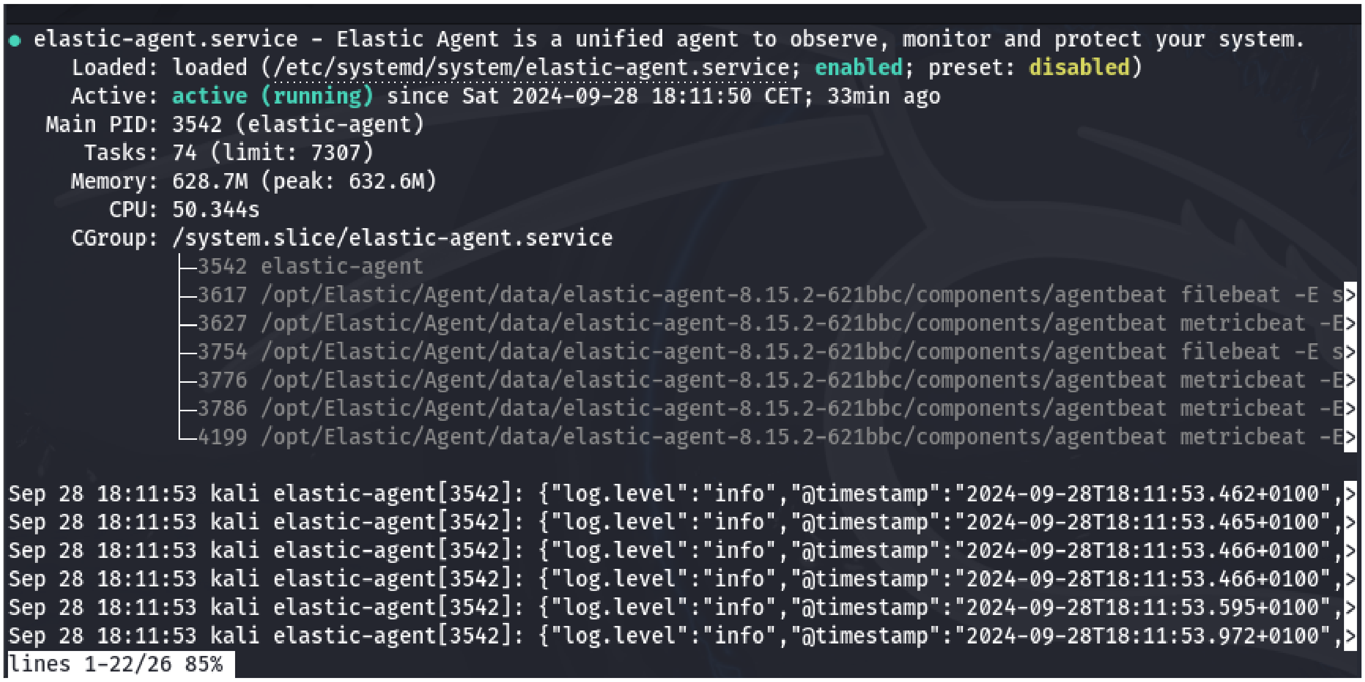
```
┌──(salsabil㉿kali)-[~]
└─$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elasti
c-agent-8.15.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.15.2-linux-x86_64.tar.gz
cd elastic-agent-8.15.2-linux-x86_64
sudo ./elastic-agent install --url=https://cc02a53713e3409d88e22c15aaa7f245.flee
t.us-central1.gcp.cloud.es.io:443 --enrollment-token=TDZDVE9aSUIyVlJuY1BlUk5uLXE
6LTcwMlg1OGJURUc5REpubEVIWnZzZw==
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  8  299M    8 25.5M    0     0   512k      0  0:09:58  0:00:51  0:09:07 91636
```

- The agent was installed successfully



```
Successfully enrolled the Elastic Agent.
[=== ] Done  [8s]
Elastic Agent has been successfully installed.
```

- To confirm that the agent has been downloaded successfully, run the following terminal command:



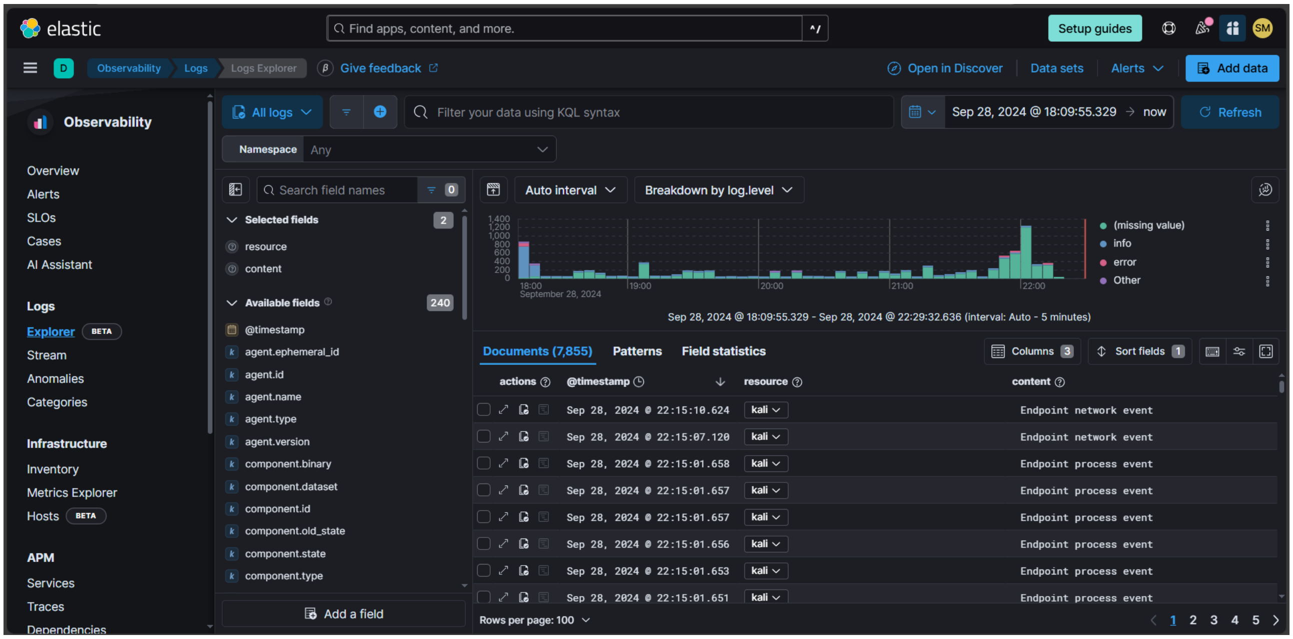
```
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
     Active: active (running) since Sat 2024-09-28 18:11:50 CET; 33min ago
   Main PID: 3542 (elastic-agent)
      Tasks: 74 (limit: 7307)
     Memory: 628.7M (peak: 632.6M)
        CPU: 50.344s
     CGroup: /system.slice/elastic-agent.service
             ├─3542 elastic-agent
             ├─3617 /opt/Elastic/Agent/data/elastic-agent-8.15.2-621bbc/components/agentbeat filebeat -E s>
             ├─3627 /opt/Elastic/Agent/data/elastic-agent-8.15.2-621bbc/components/agentbeat metricbeat -E>
             ├─3754 /opt/Elastic/Agent/data/elastic-agent-8.15.2-621bbc/components/agentbeat filebeat -E s>
             ├─3776 /opt/Elastic/Agent/data/elastic-agent-8.15.2-621bbc/components/agentbeat metricbeat -E>
             ├─3786 /opt/Elastic/Agent/data/elastic-agent-8.15.2-621bbc/components/agentbeat metricbeat -E>
             └─4199 /opt/Elastic/Agent/data/elastic-agent-8.15.2-621bbc/components/agentbeat metricbeat -E>

Sep 28 18:11:53 kali elastic-agent[3542]: {"log.level":"info","@timestamp":"2024-09-28T18:11:53.462+0100",>
Sep 28 18:11:53 kali elastic-agent[3542]: {"log.level":"info","@timestamp":"2024-09-28T18:11:53.465+0100",>
Sep 28 18:11:53 kali elastic-agent[3542]: {"log.level":"info","@timestamp":"2024-09-28T18:11:53.466+0100",>
Sep 28 18:11:53 kali elastic-agent[3542]: {"log.level":"info","@timestamp":"2024-09-28T18:11:53.466+0100",>
Sep 28 18:11:53 kali elastic-agent[3542]: {"log.level":"info","@timestamp":"2024-09-28T18:11:53.595+0100",>
Sep 28 18:11:53 kali elastic-agent[3542]: {"log.level":"info","@timestamp":"2024-09-28T18:11:53.972+0100",>
lines 1-22/26 85%
```

4-Creating security events on the Kali VM with Nmap

At this stage, the environment is set up, and we now need to generate some security events on the Kali VM using Nmap.

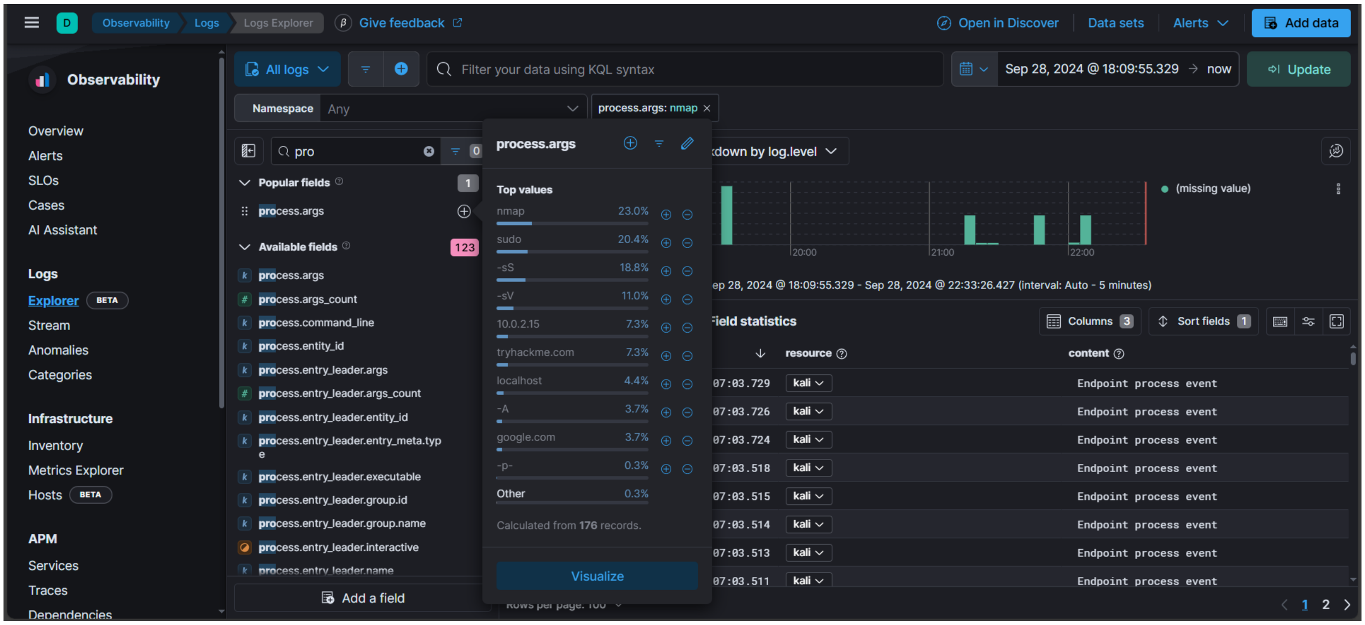
- Here are the sent logs



Sep 28, 2024 @ 18:09:55.329 → now

Sep 28, 2024 @ 18:09:55.329 - Sep 28, 2024 @ 22:29:32.636 (interval: Auto - 5 minutes)

actions	@timestamp	resource	content
□	Sep 28, 2024 @ 22:15:10.624	kali	Endpoint network event
□	Sep 28, 2024 @ 22:15:07.120	kali	Endpoint network event
□	Sep 28, 2024 @ 22:15:01.658	kali	Endpoint process event
□	Sep 28, 2024 @ 22:15:01.657	kali	Endpoint process event
□	Sep 28, 2024 @ 22:15:01.657	kali	Endpoint process event
□	Sep 28, 2024 @ 22:15:01.656	kali	Endpoint process event
□	Sep 28, 2024 @ 22:15:01.653	kali	Endpoint process event
□	Sep 28, 2024 @ 22:15:01.651	kali	Endpoint process event



Top values

nmap	23.0%
sudo	20.4%
-sS	18.8%
-sV	11.0%
10.0.2.15	7.3%
tryhackme.com	7.3%
localhost	4.4%
-A	3.7%
google.com	3.7%
-p-	0.3%
Other	0.3%

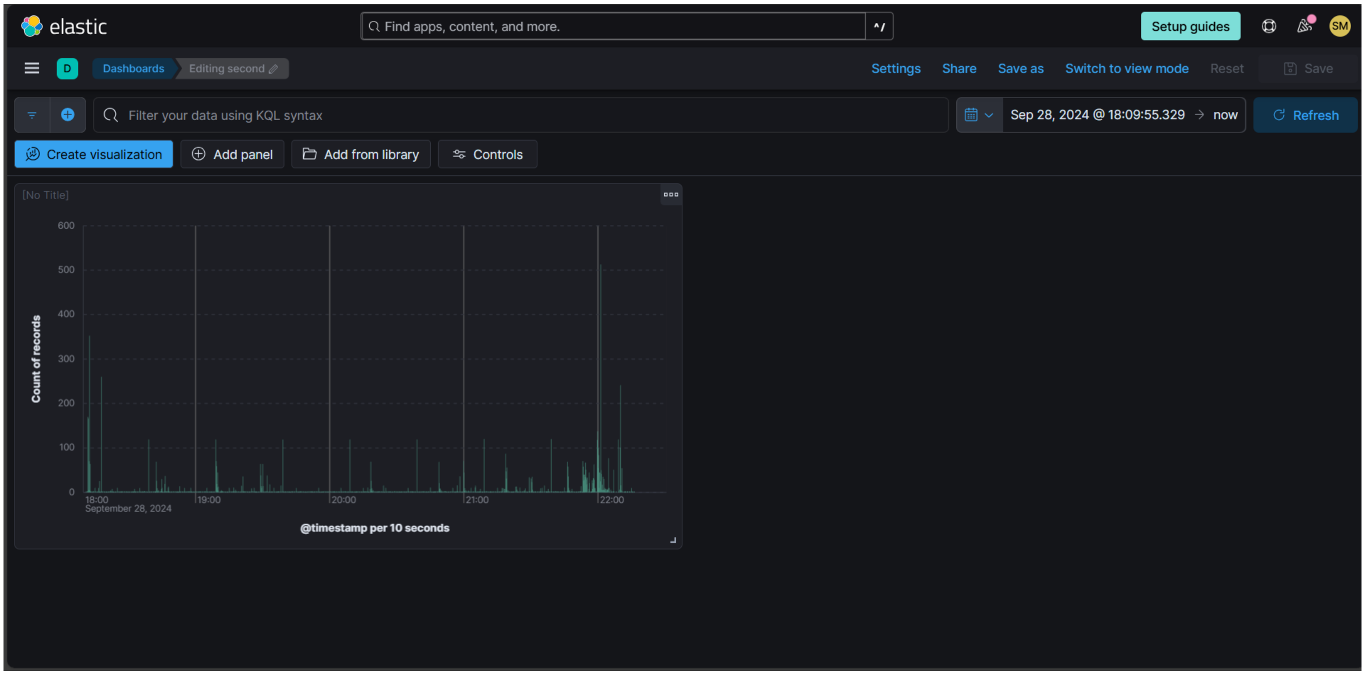
Calculated from 176 records.

	resource	content
07:03.729	kali	Endpoint process event
07:03.726	kali	Endpoint process event
07:03.724	kali	Endpoint process event
07:03.518	kali	Endpoint process event
07:03.515	kali	Endpoint process event
07:03.514	kali	Endpoint process event
07:03.513	kali	Endpoint process event
07:03.511	kali	Endpoint process event

Analyzing diverse security events in Elastic SIEM provides valuable insights into real-world security incident detection, investigation, and response procedures

5-Create a Dashboard to Visualize the Events

- Create a simple dashboard to visualize the count of security events over time

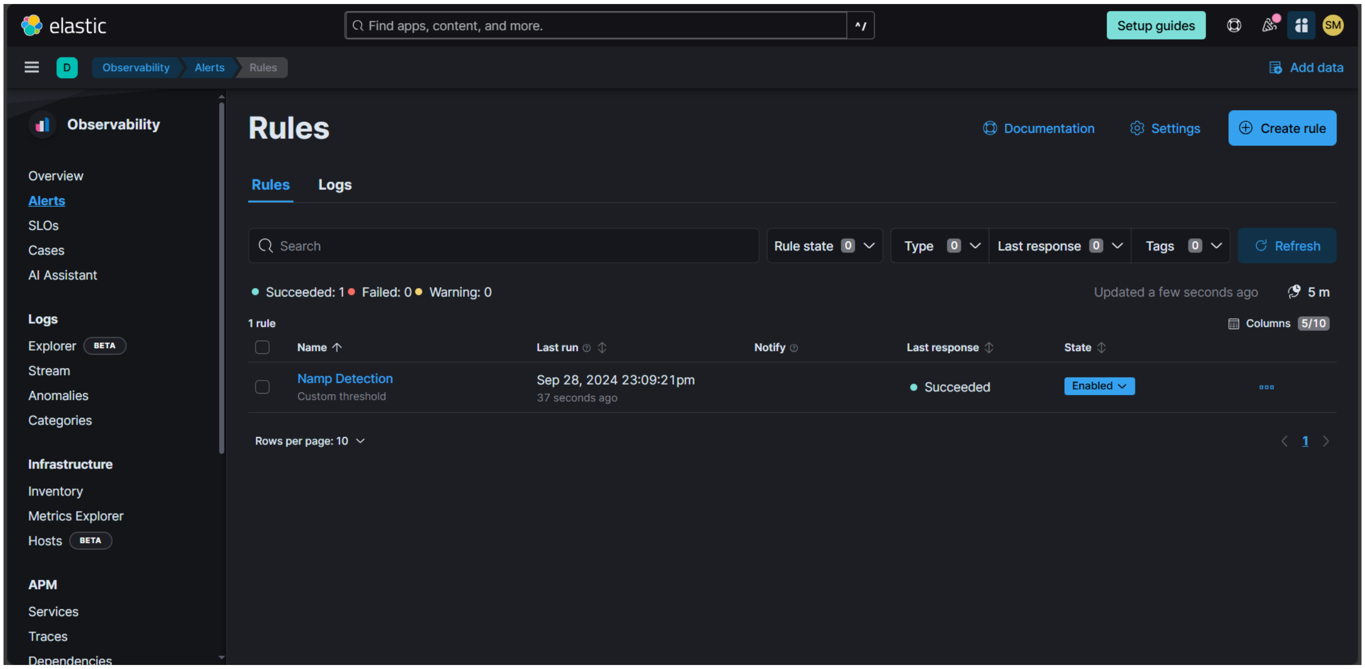


6-Create an Alert

- Create an alert in Elastic SIEM to detect Nmap scans based on custom queries.

Alerts play a crucial role in a SIEM system by facilitating the swift detection and response to security incidents. These alerts are generated from predefined rules or custom queries, specifically designed to initiate targeted actions when certain conditions are fulfilled.

- We set up our alert, named "Nmap Detection"



Rules

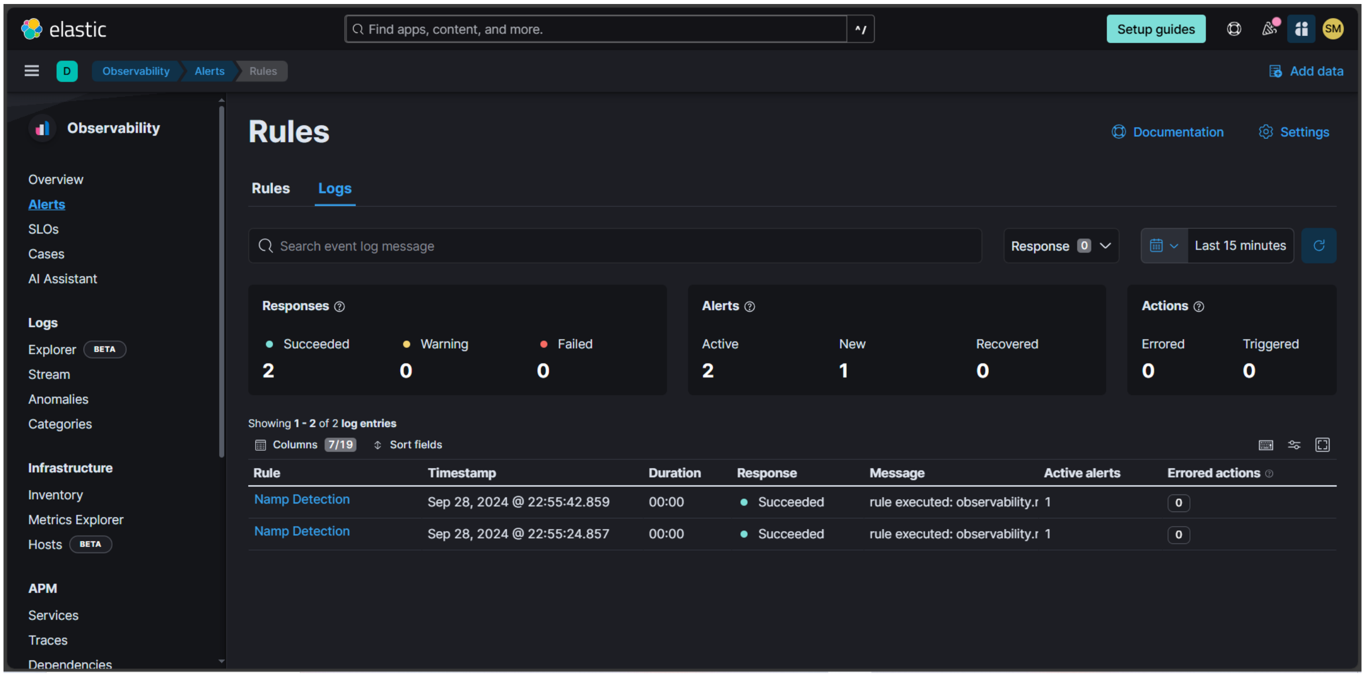
● Succeeded: 1 ● Failed: 0 ● Warning: 0

Updated a few seconds ago 5 m

1 rule

	Name	Last run	Notify	Last response	State
□	Namp Detection Custom threshold	Sep 28, 2024 23:09:21pm 37 seconds ago		● Succeeded	Enabled

- As we can see, the alert was successfully generated (we ran Nmap twice, which is why there are two alerts).



Rules

Responses			Alerts			Actions	
● Succeeded	● Warning	● Failed	Active	New	Recovered	Errored	Triggered
2	0	0	2	1	0	0	0

Showing 1 - 2 of 2 log entries

Rule	Timestamp	Duration	Response	Message	Active alerts	Errored actions
Namp Detection	Sep 28, 2024 @ 22:55:42.859	00:00	● Succeeded	rule executed: observability.r	1	0
Namp Detection	Sep 28, 2024 @ 22:55:24.857	00:00	● Succeeded	rule executed: observability.r	1	0

Conclusion

In this lab, we’ve set up a home lab to practice Elastic SIEM and gain hands-on experience in security monitoring and incident response. we’ve learned how to forward data, generate and analyze security events, create dashboards, and set up alerts.