Project: Using a SIEM to monitor Ubuntu traffic and generate alerts

Clay Jones

Objective:

Connect a Ubuntu virtual machine to a SIEM and monitor the traffic. Run some Nmap scans to generate network traffic. Analyze the traffic and find the commands that were run. Create a chart monitoring based on the traffic. Create an alert that sends an email and triggers when a specific command is run.

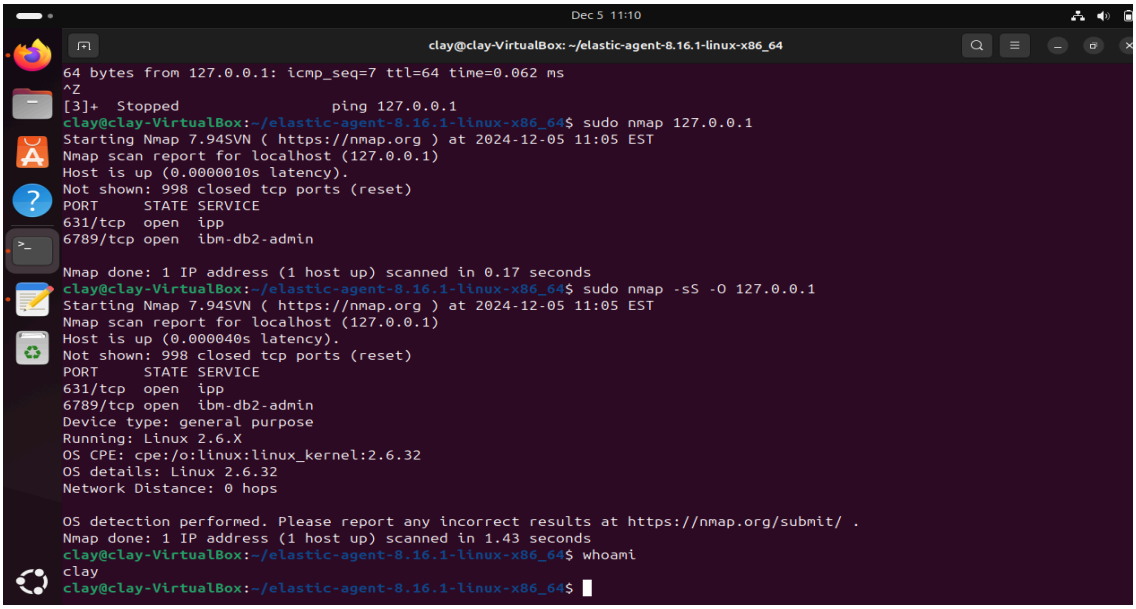
Connecting the VM with Elastic Stack:

```
{"log.level":"info","@timestamp":"2024-12-05T11:01:05.270-0500","log.origin":{"function":"github.com/elastic/elast
nt/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":301},"message":"Succes
 triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=   ] Done  [26s]
Elastic Agent has been successfully installed.
clay@clay-VirtualBox:~/elastic-agent-8.16.1-linux-x86_64$ sudo systemctl status elastic-agent.service
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor >
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset>
     Active: active (running) since Thu 2024-12-05 11:01:01 EST; 2min 25s ago
   Main PID: 7877 (elastic-agent)
      Tasks: 71 (limit: 2278)
     Memory: 705.7M (peak: 774.6M swap: 35.0M swap peak: 49.2M)
        CPU: 18.269s
     CGroup: /system.slice/elastic-agent.service
             ├─7877 elastic-agent
             ├─7955 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compone>
             ├─7964 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compone>
             ├─7976 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compone>
             ├─7986 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compone>
             ├─8151 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compone>
             └─8675 /opt/Elastic/Agent/data/elastic-agent-8.16.1-b6da7f/compone>

Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
Dec 05 11:01:03 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
Dec 05 11:01:04 clay-VirtualBox elastic-agent[7877]: {"log.level":"info","@time>
lines 1-23
clay@clay-VirtualBox:~/elastic-agent-8.16.1-linux-x86_64$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
```

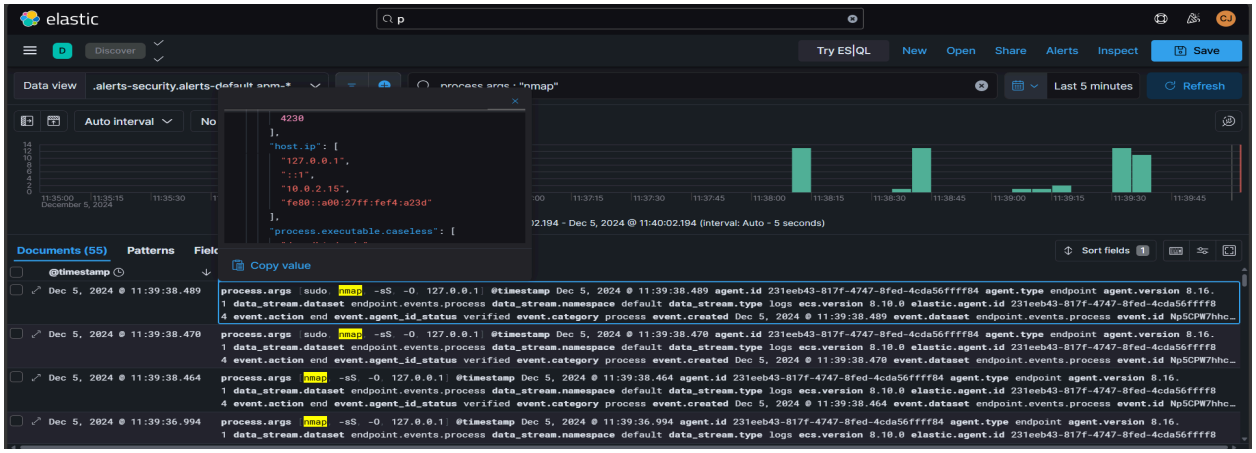
Create an integration and connected Ubuntu to elastic.

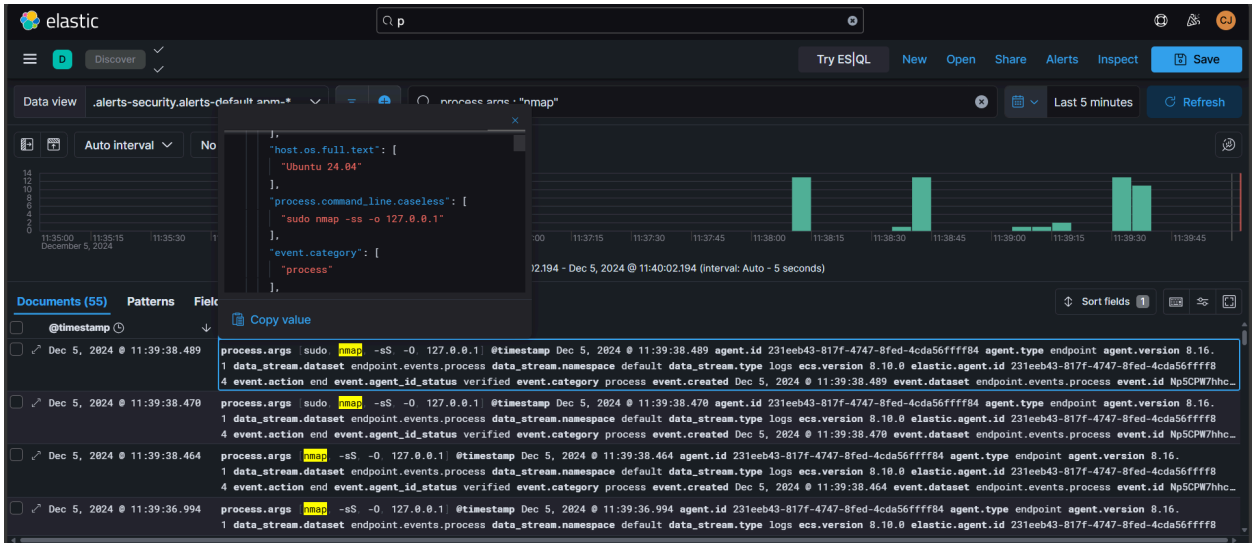
Generating Traffic using Nmap:

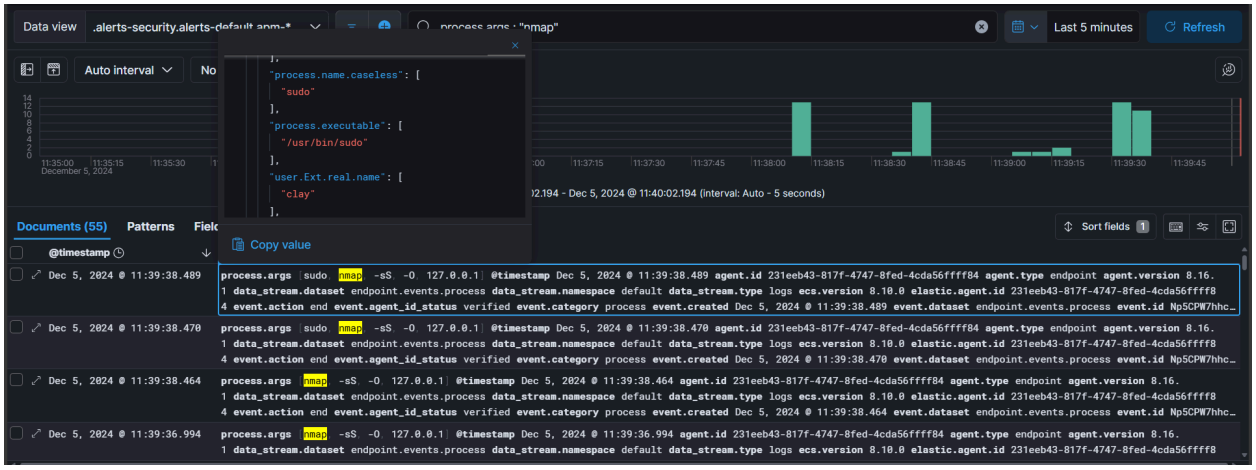


I ran several Nmap scans on the host to generate network traffic.

Nmap scans found in elastic logs:

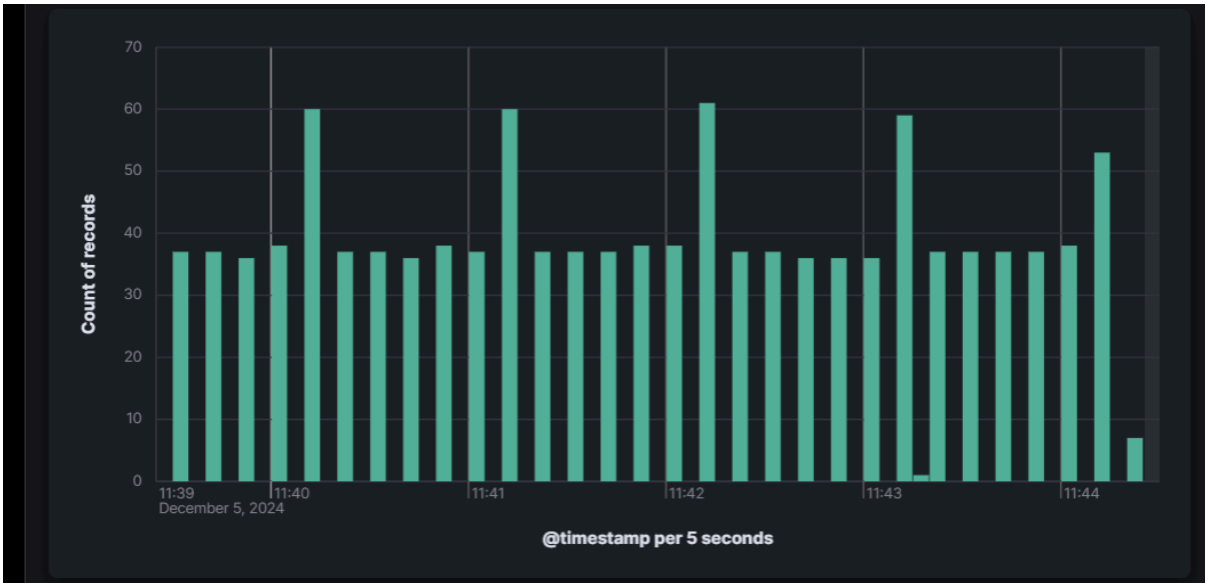


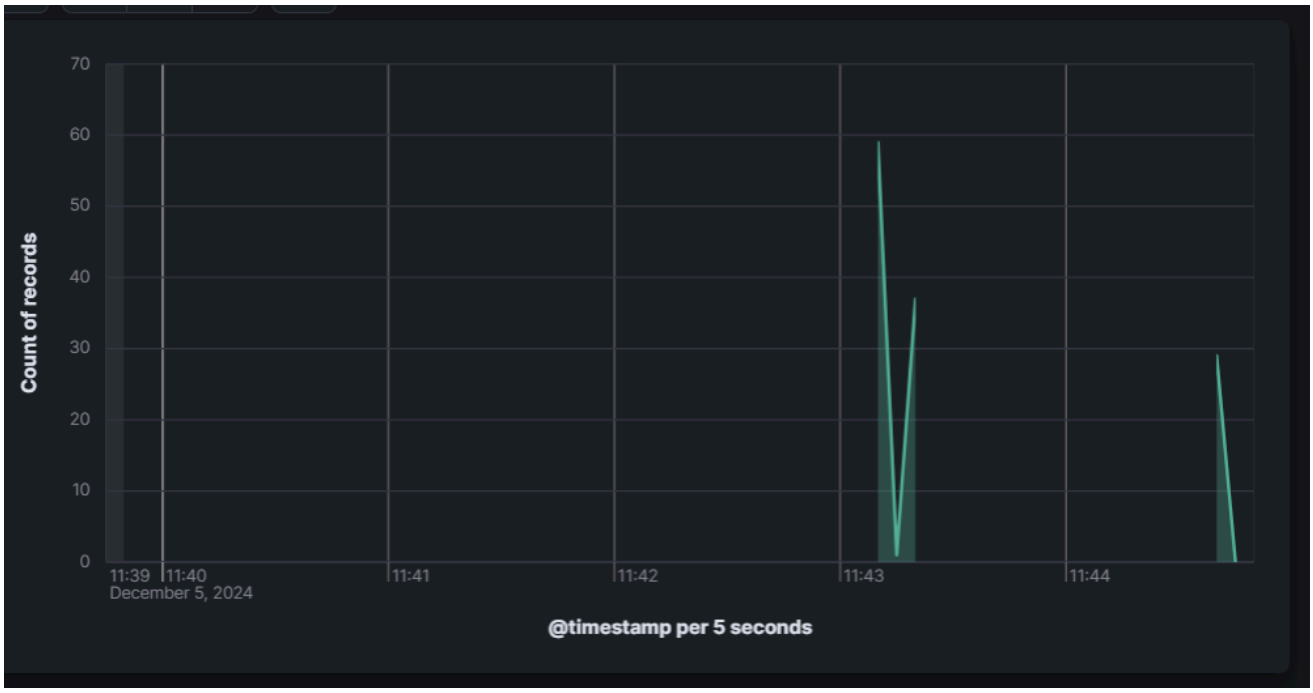




The scans that I ran were shown in the logs. The command that generated the most traffic was "sudo nmap -sS -O localhost." This also shows metadata off the host that generated this traffic.

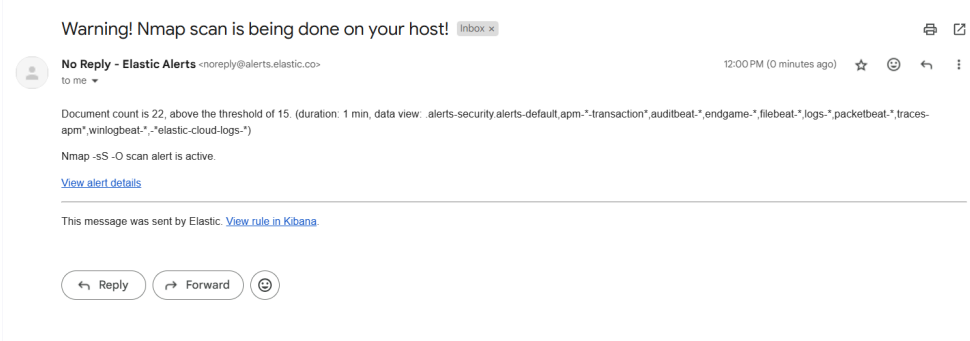
Charts based on traffic:

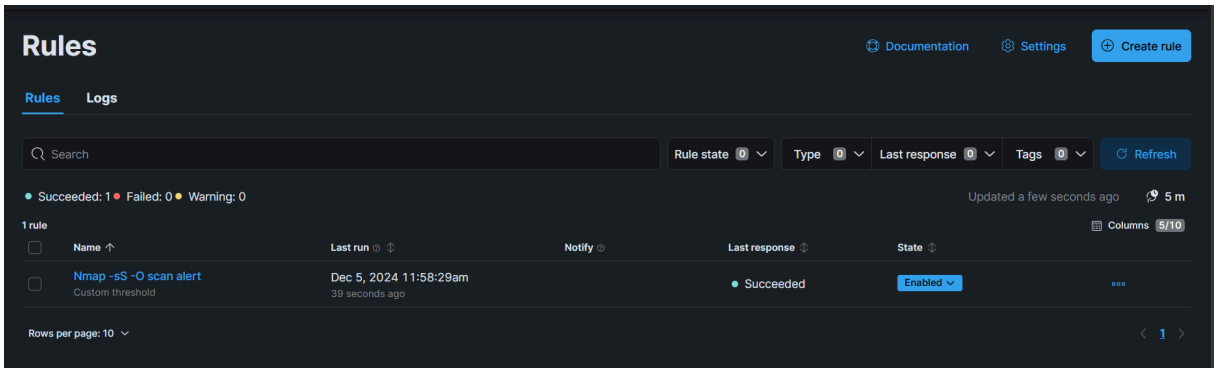




These charts were created based on the time and count of records.

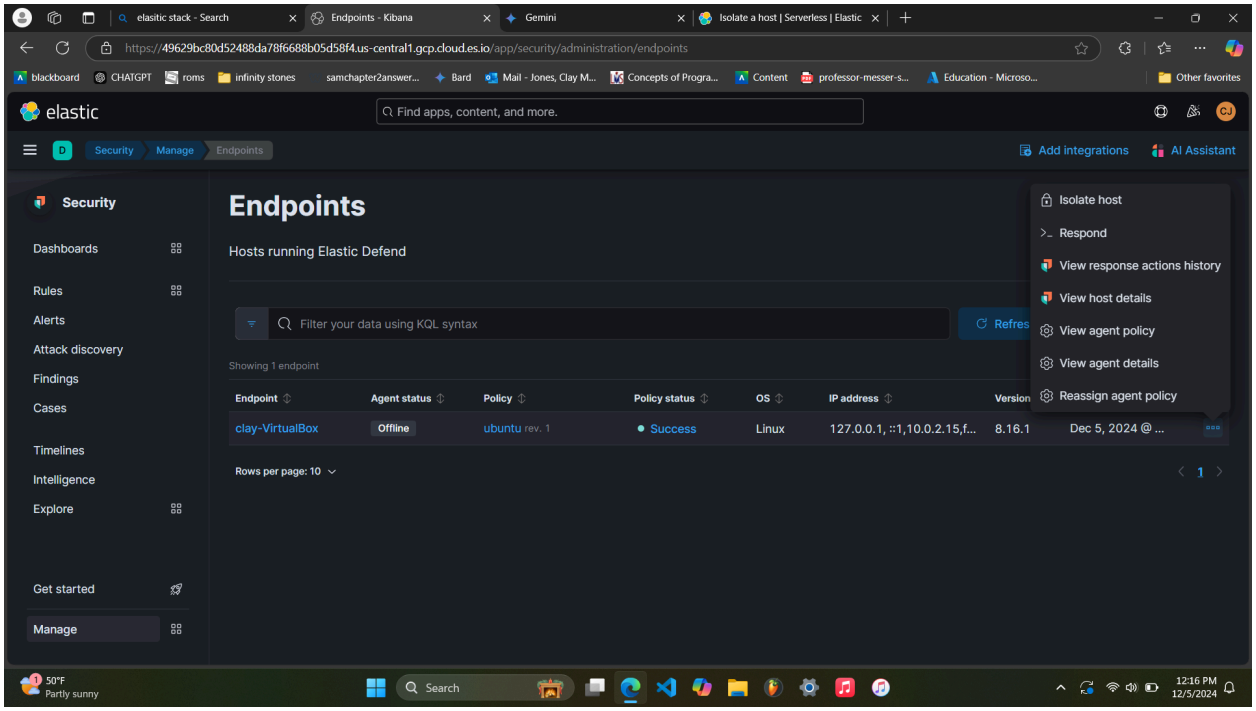
Creating an alert





I created an alert that sends an email every time the “sudo nmap -sS -O localhost” command is run on the host.

Isolation and Response:



I have the option of isolating the host or responding to the incident in the endpoint manager.