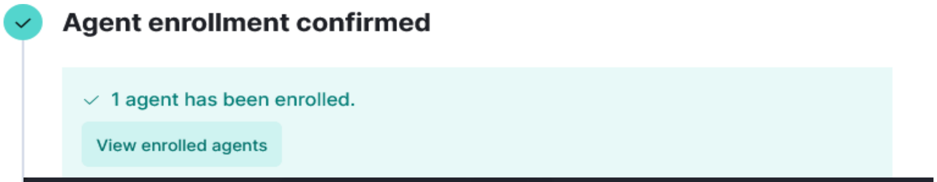
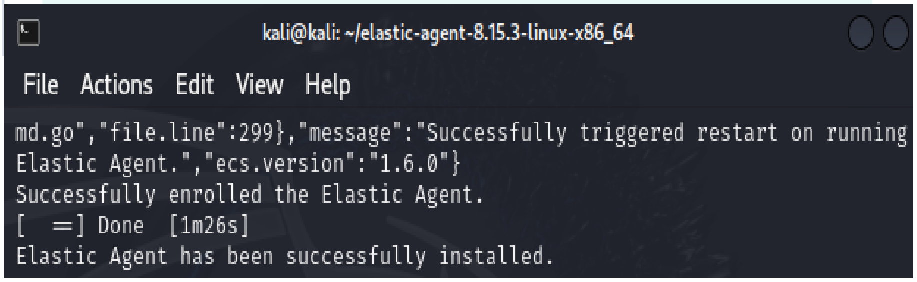
SIEM Home Lab Setup

- **Project Summary:** Configured a customized SIEM to monitor, analyze, and forward security events
- **Setup Components**: Kali Linux VM, Elastic SIEM
- **Pre-Configuration Setup**:
  - I set up a Kali Linux VM using Virtualbox and a prebuilt image from https://www.kali.org. I then deployed a SIEM using Elastic Defend, and added our VM as the agent to be monitored.



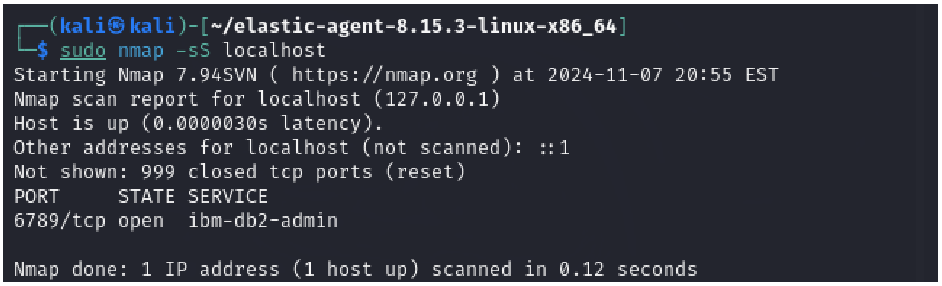
Agent enrollment confirmed

✓ 1 agent has been enrolled.



```
md.go","file.line":299},"message":"Successfully triggered restart on running
Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[  =] Done  [1m26s]
Elastic Agent has been successfully installed.
```

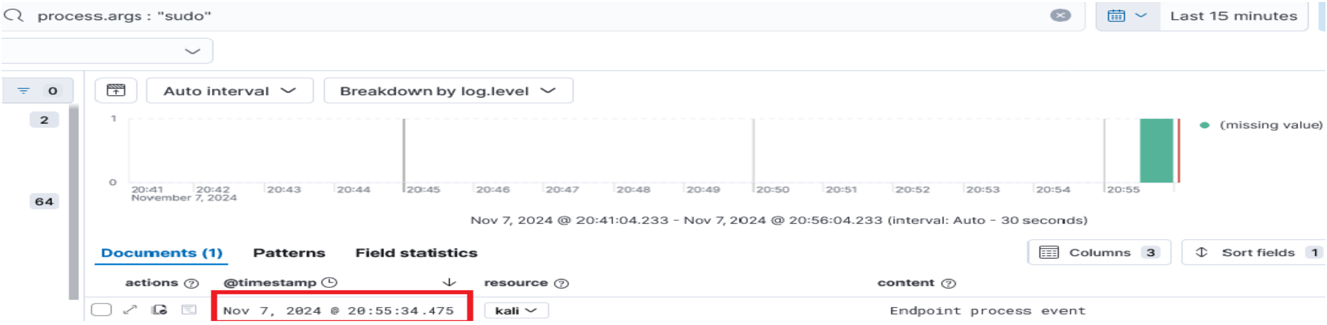
- **Simulating Security Events:**
  - Verified agent was working correctly by creating events on the monitored VM.
  - In order to generate our first event, I used Nmap, a common utility for network discovery.



```
┌──(kali㉿kali)-[~/elastic-agent-8.15.3-linux-x86_64]
└─$ sudo nmap -sS localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 20:55 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
6789/tcp open  ibm-db2-admin

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

  - As you can see above, the Nmap scan was ran at 20:55. Below, we see that the SIEM has record of the Nmap scan occurring at 20:55.



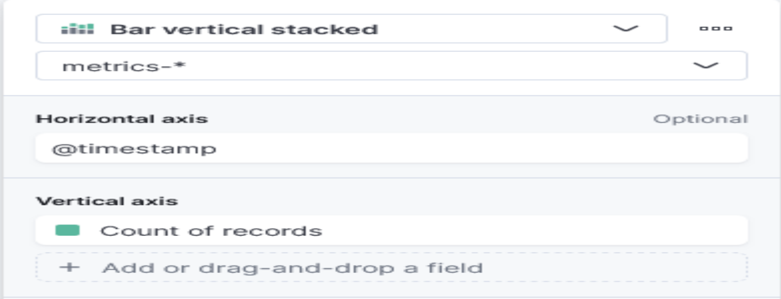
process.args : "sudo"

Last 15 minutes

Nov 7, 2024 @ 20:41:04.233 - Nov 7, 2024 @ 20:56:04.233 (interval: Auto - 30 seconds)

actions	@timestamp	resource	content
□	Nov 7, 2024 @ 20:55:34.475	kali	Endpoint process event

- **Creating a Visualized Dashboard**:
  - Created a custom dashboard using the number of events(aka the metrics) for our vertical axis, and the timestamps of the events for our horizontal axis



Bar vertical stacked

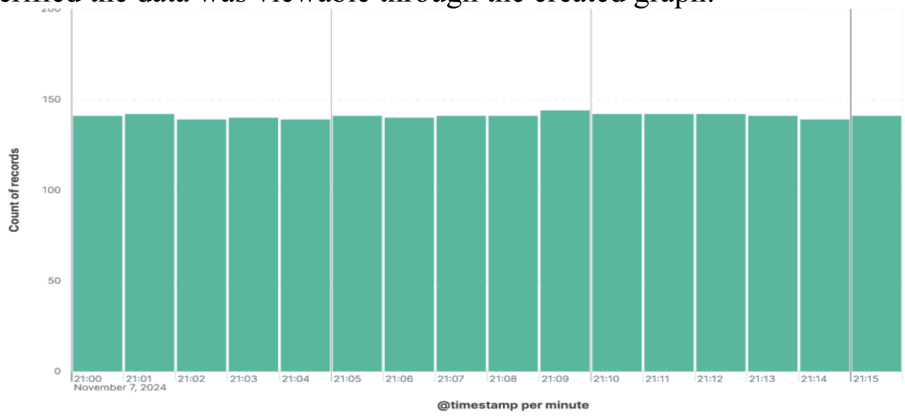
metrics-*

Horizontal axis — Optional: @timestamp

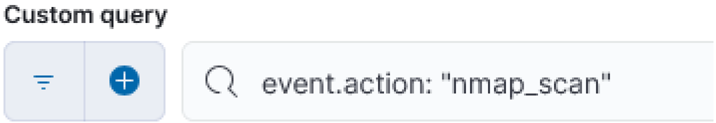
Vertical axis: 🟩 Count of records

+ Add or drag-and-drop a field

  - Verified the data was viewable through the created graph:



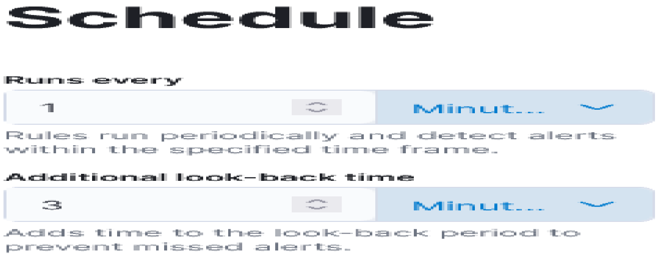
- **Creating Alerts**:
  - Defined rules in the Elastic SIEM to alert when an Nmap scan occurred, or when a user ran a command using Sudo.



Custom query

event.action: "nmap_scan"

  - Had the SIEM check for these events every 1 minute, and to look back 3 minutes. This ensured no events were missed.



Schedule

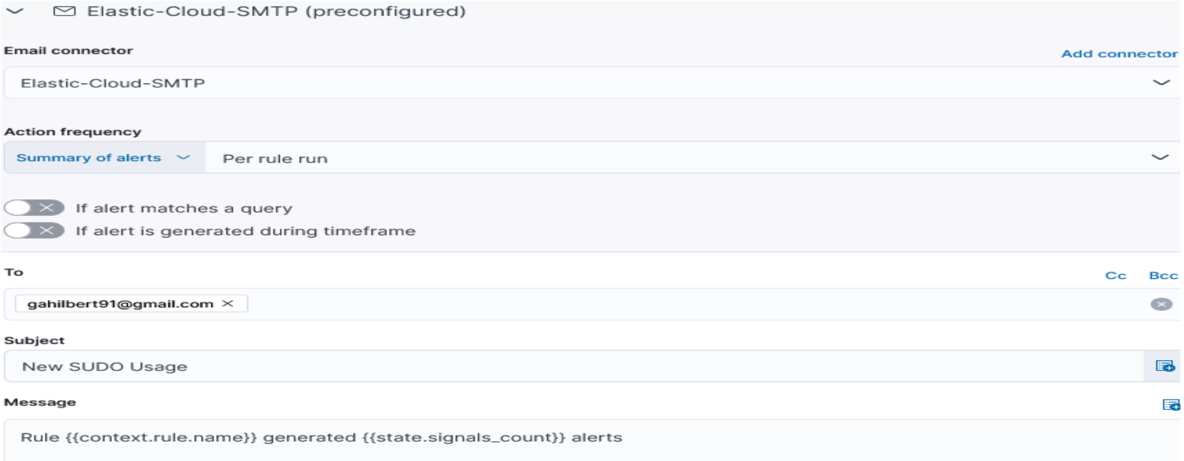
Runs every: 1 Minut...

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

Additional look-back time: 3 Minut...

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

- **Receiving Alerts**:
  - Based on the above parameters, used the pre-configured Elastic-Cloud-SMTP to alert email of choice when the conditions were met.



Elastic-Cloud-SMTP (preconfigured)

Email connector

Elastic-Cloud-SMTP

Action frequency

Summary of alerts | Per rule run

If alert matches a query

If alert is generated during timeframe

To

gahilbert91@gmail.com ×

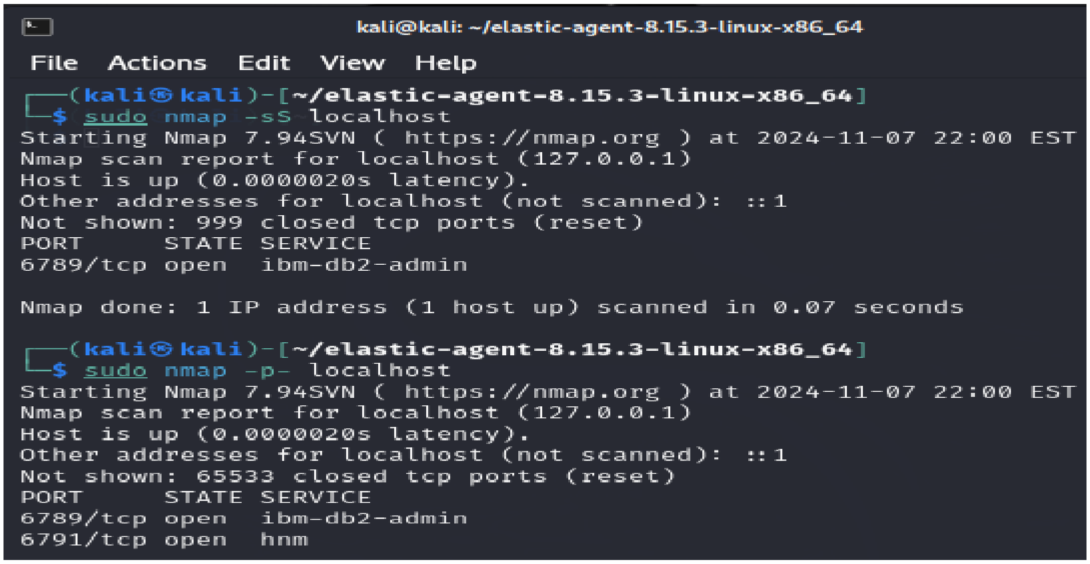
Subject

New SUDO Usage

Message

Rule {{context.rule.name}} generated {{state.signals_count}} alerts

- Ran another Nmap scan, which was followed by a successful email alert. As you can see below, a Sudo Nmap scan occurs at 22:00(10:00 PM). I received an email alert about the scan at 10:01 PM.

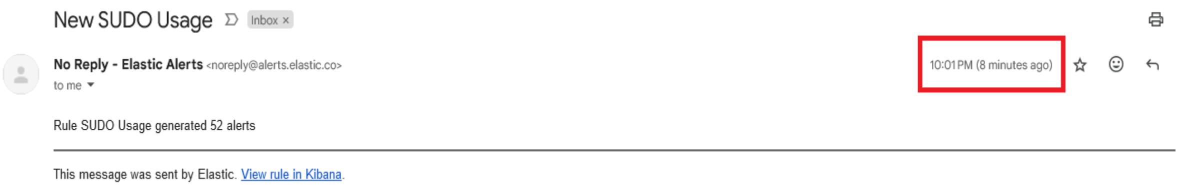


kali@kali: ~/elastic-agent-8.15.3-linux-x86_64
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/elastic-agent-8.15.3-linux-x86_64]
└─$ sudo nmap -sS localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 22:00 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
6789/tcp open  ibm-db2-admin

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

┌──(kali㉿kali)-[~/elastic-agent-8.15.3-linux-x86_64]
└─$ sudo nmap -p- localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 22:00 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
6789/tcp open  ibm-db2-admin
6791/tcp open  hnm
```



New SUDO Usage

No Reply - Elastic Alerts <noreply@alerts.elastic.co>

to me

10:01 PM (8 minutes ago)

Rule SUDO Usage generated 52 alerts

This message was sent by Elastic. View rule in Kibana.

- **Outcome**: Configured a home lab using Elastic SIEM and a Kali VM as the agent. Utilized Nmap and Sudo commands to generate events. Used the SIEM's interface to query and analyze the events. Created a custom dashboard to visualize events. Additionally, I set up email alerts to detect specific security incidents.