

# **“Security event simulation and alerting using Elastic stack SIEM”**



# **“Security event simulation and alerting using Elastic stack SIEM”.**

A project report

submitted in partial fulfillment of the requirements

for the award of the degree of

**POST GRADUATE DIPLOMA IN CYBERSECURITY AND FORENSICS (PG-DCSF).**



Submitted by

<b>Nikita Pakhale</b>	<b>(230360940031)</b>
<b>Omkar Ingawale</b>	<b>(230360940032)</b>
<b>Jayraj Dinde</b>	<b>(230360940021)</b>
<b>Ritwik Mungale</b>	<b>(230360940021)</b>

Under the supervision of

**Hiron Bose**

Section Head (STDC) / Scientist E

C-DAC,

Thiruvananthapuram

# INDEX

SR no.	Topic	Page no.
1.	Introduction	3
2.	Chronology of Tasks.	4
3.	Set up a free Elastic account.	5
4.	Configure the Elastic Agent on the Linux VM to collect the logs and forward it to the SIEM.	6
5.	Generate Security events.	8
6.	Query to find the security events in the Elastic SIEM.	9
7.	Create a Dashboard to visualize security events.	10
8.	Create alerts for security events.	14
9.	Conclusion.	17
10.	References	17

# Introduction.

## **Our Aim:-**

This project oversees how to set up a home lab for Elastic Stack Security Information and Event Management (SIEM) using the Elastic Web portal and a Kali Linux VM. It also shows how to generate security events on the Kali VM, set up an agent to forward data to the SIEM, and query and analyse the logs in the SIEM.

## **What is SIEM?**

SIEM, or Security Information and Event Management collects logs and events, normalizing this data for further analysis that can manifest as visualizations, alerts, searches, reports, and more. Security teams will often use their SIEM as a central dashboard, conducting many of their day-to-day operations out of the platform. Security analysts can use SIEM solutions to take on advanced cybersecurity use cases such as continuous monitoring, threat hunting, and incident investigation and response.

## **How does SIEM work?**

A SIEM (security information and event management) platform works by collecting log and event data produced by these various technologies, and provides security analysts with a comprehensive view of their organization's IT environment. An effective SIEM will automatically remediate known threats within a system, while surfacing more nuanced situations to help security analysts identify whether further investigation and action is needed.

Devices, networks, servers, apps, systems... an organization's ecosystem produces a lot of data from daily operations. There's an abundance of context within this data that can be helpful for keeping the ecosystem secure. That's where SIEM comes in.

## **Why is SIEM important?**

SIEM is a critical component of any security team. It functions as a centralized hub through which massive amounts of data can be brought together for analysis, unifying the analyst experience by serving as the centralized mission-control base. With SIEM, a security team can identify and defend against threats that may have evaded perimeter security technologies and are active within the organization's ecosystem.

## **What is Elastic Stack SIEM?**

Elastic SIEM (Security Information and Event Management) is an extension of the Elastic Stack that equips security teams with powerful capabilities for detecting, investigating, and responding to advanced threats. Let's dive into the details:

### Unified Solution:

- Elastic SIEM provides a unified, open-source solution for security analytics. It combines data from various sources to give you a holistic view of your environment.
- With Elastic Common Schema (ECS), you can analyse data uniformly, regardless of its origin or format.

### Key Features:

- **Threat Detection:** Elastic SIEM automates detection of suspicious activity using behaviour-based rules. These rules are powered by research from Elastic Security Labs.
- **Anomaly Detection:** Uncover unknown threats with prebuilt machine learning (ML) jobs. Arm threat hunters with evidence-based hypotheses.
- **Entity Analytics:** Gain insight into entities at highest risk.
- **High-Fidelity Rules:** Prioritize potential threats based on risk and severity scores. Detections align with the MITRE ATT&CK framework.
- **Automated Incident Response:** Streamline inspection and invoke remote response actions.

### Chronology Of Tasks: -

- Set up a free Elastic account.
- Configure the Elastic Agent on the Linux VM to collect the logs and forward it to the SIEM.
- Generate security events on the Kali VM.
- Query to find the security events in the Elastic SIEM.
- Create a Dashboard to visualize security events.
- Create alerts for security events.
- Pre-requisites: -
  - Kali Linux VM.

### Objective:

- Learn to configure the Elastic Agent on the Linux VM to collect logs and forward them to the SIEM.
- Understand how to query Elastic SIEM to identify and analyze security events effectively.
- Gain experience in creating custom dashboards to visualize security events in Elastic SIEM.
- Learn to establish alerts within Elastic SIEM for proactive monitoring and incident response.

# 1.Set up a free Elastic account.

we need to create a free account to set up a cloud Elastic instance that we can run the SIEM on.

1. Sign up for a free trial to use Elastic Cloud at <https://cloud.elastic.co/registration>
2. Once you have an Elastic account, log in to the Elastic Cloud console at <https://cloud.elastic.co>.
3. Click on “Start your free trial.”
4. Click on the “Create Deployment” button and select “Elasticsearch” as the deployment type.
5. Choose a name and deployment size that fits your needs and click on “Create Deployment.”
6. Wait for the configuration to complete.
7. Once the deployment is ready, click “continue.” Below is an image for the reference. Name of our deployment is ‘SIEM project 0017’.

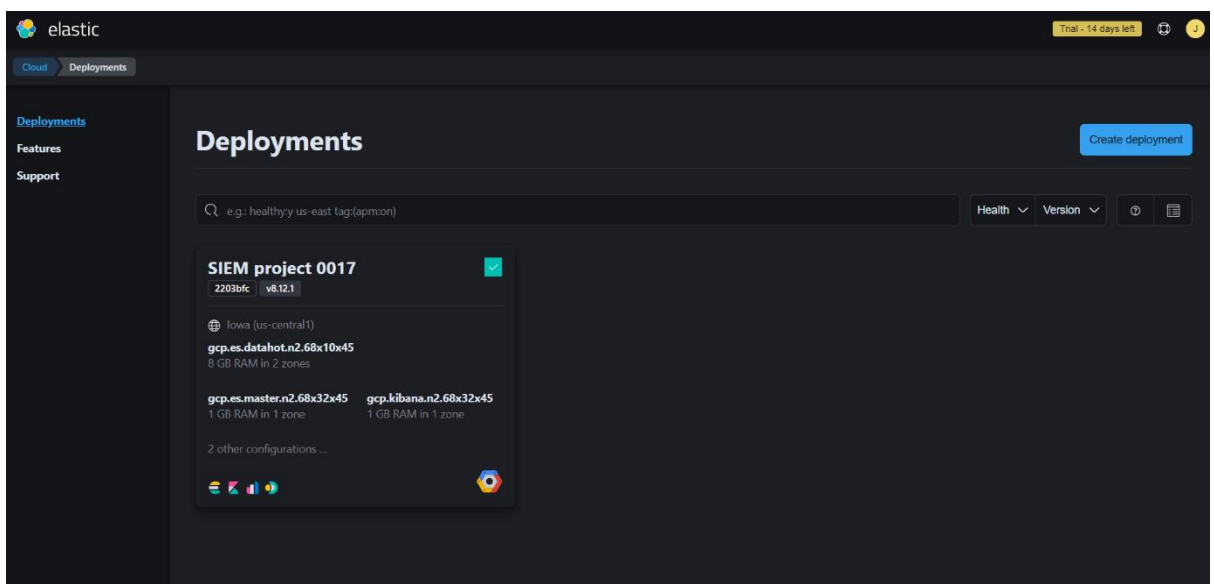


Fig.1

## 2. Configure the Elastic Agent on the Linux VM to collect the logs and forward it to the SIEM.

An agent is a software program that is installed on a device, such as a server or endpoint, to collect and send data to a centralized system for analysis and monitoring. In the context of Elastic SIEM, an agent is used to collect and forward security-related events from your endpoints to your Elastic SIEM instance.

To set up the agent to collect logs from your Kali VM and forward them to your Elastic SIEM instance, follow these steps:

- 1) Log in to your Elastic SIEM instance and navigate to the Integrations page by: clicking on the Kibana main menu bar at the top left, then selecting “Integrations” at the bottom.

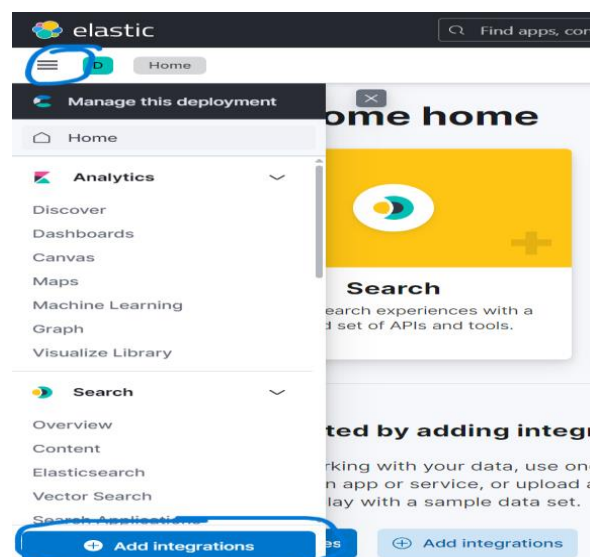


Fig.2

- 2) Search for “Elastic Defend” and click on it to open the integration page.

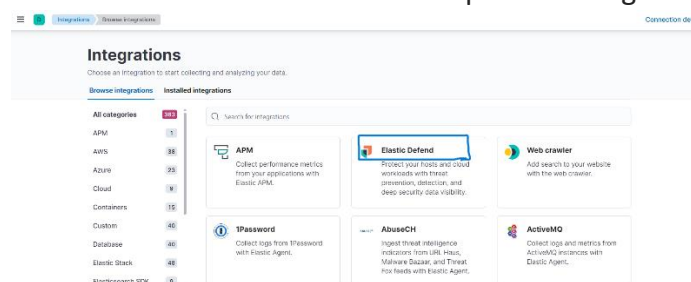


Fig.3

- 3) Click on “Install Elastic Defend” and follow the instructions provided on the integration page to install the agent on your Kali VM.

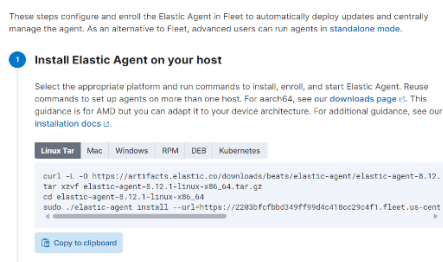


Fig.4

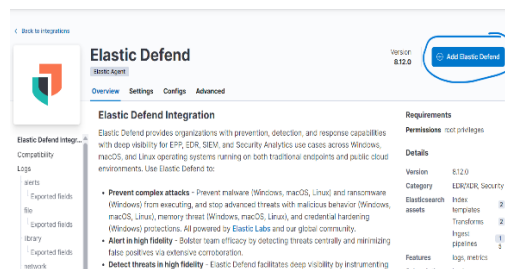


Fig.5

#### 4) Paste that command into the Kali terminal (command line).

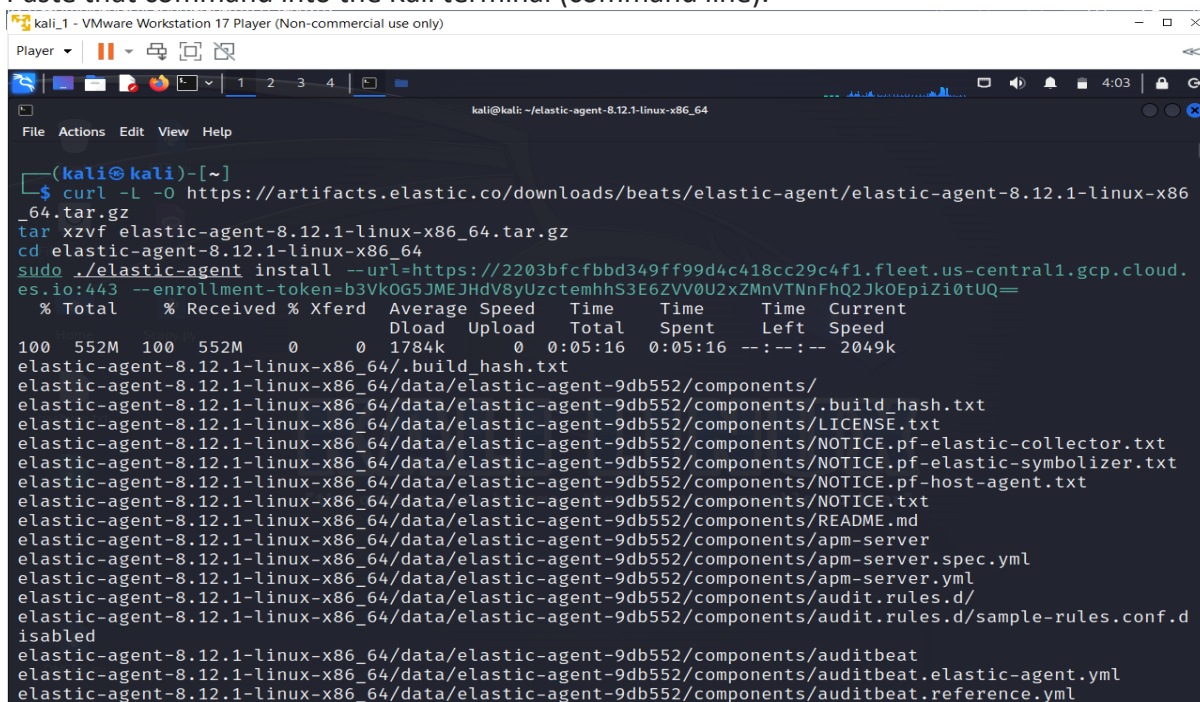


Fig.6

- 5) Once the agent is installed, which can take a few minutes, you'll see a message that says "Elastic Agent has been successfully installed." It will automatically start collecting and forwarding logs to your Elastic SIEM instance, although it might take a few minutes for the logs to appear in the SIEM. You can verify that the agent has been installed correctly by running this command:

**'sudo systemctl status elastic-agent.service'**

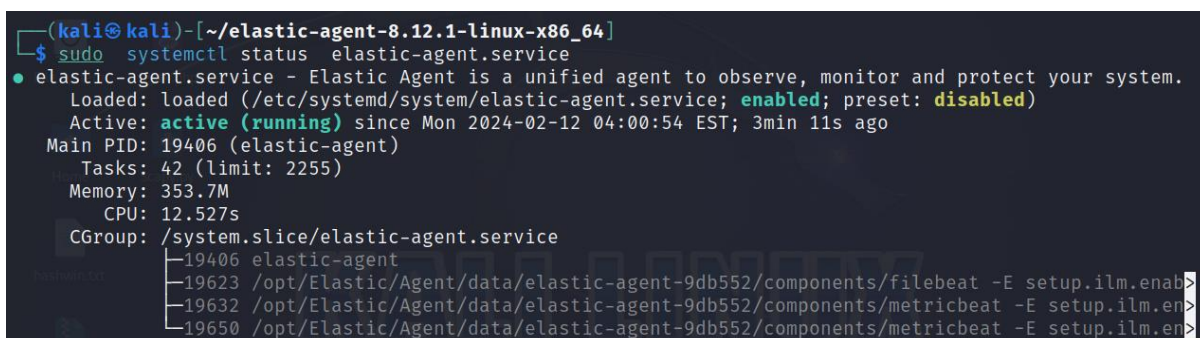


Fig.7



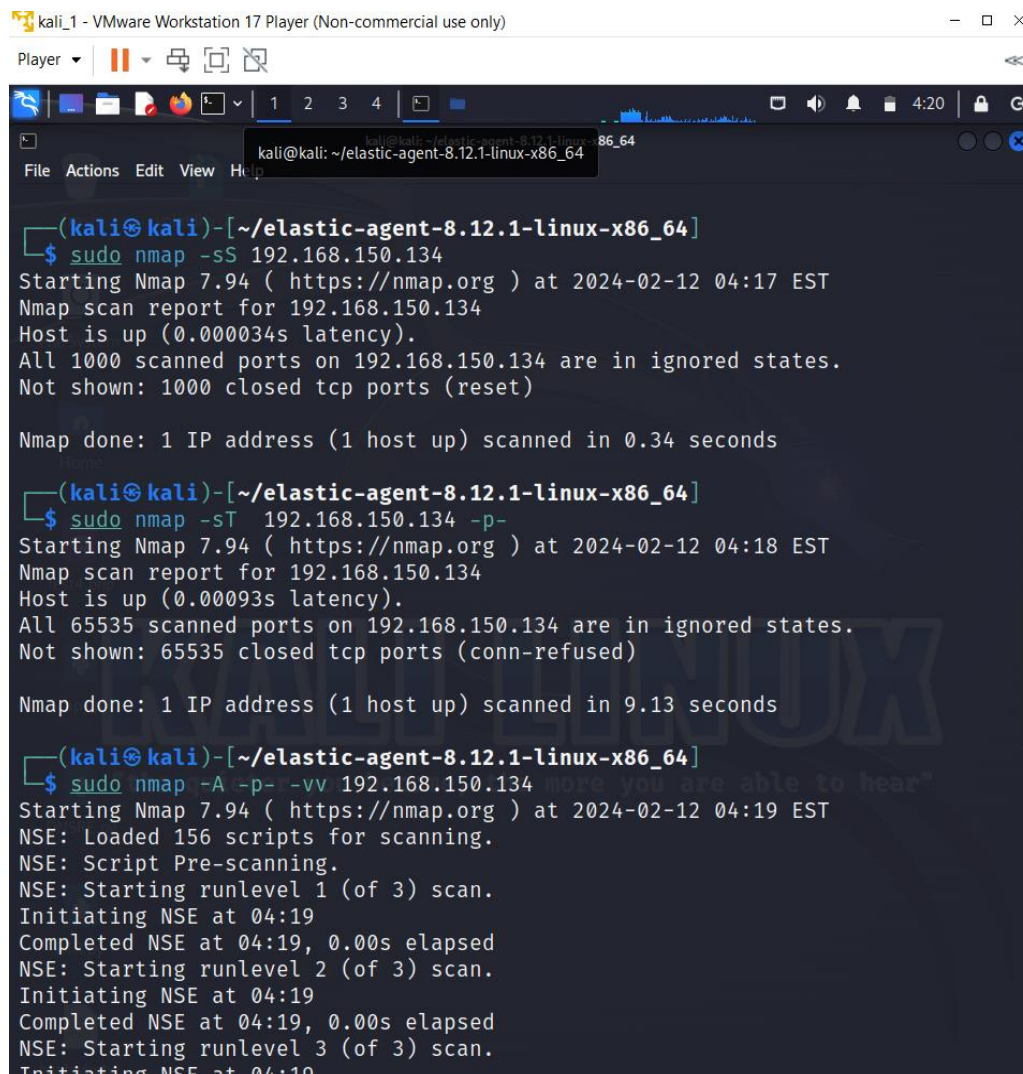
### 3. Generating security logs on Kali Linux VM.

To verify that the agent is working correctly, you can generate some security-related events on your Kali VM. To do this, we can use a tool like Nmap. Nmap (Network Mapper) is a free and open-source utility used for network exploration, management, and security auditing. It is designed to discover hosts and services on a computer network, thus creating a “map” of the network. Nmap can be used to scan hosts for open ports, determine the operating system and software running on the target system, and gather other information about the network.

Run a scan on Kali machine by running the command: **sudo nmap 192.168.150.134**  
You can also run a scan of your host machine if you place your Kali VM on a “bridged” network. This scan generates several security events, such as the detection of open ports and the identification of services running on those ports. Let us run a few more NMAP scans like

**Nmap -sS 192.168.150.134**

**Nmap -A 192.168.150.134**



```
kali_1 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
(kali@kali)-[~/elastic-agent-8.12.1-linux-x86_64]
$ sudo nmap -sS 192.168.150.134
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-12 04:17 EST
Nmap scan report for 192.168.150.134
Host is up (0.000034s latency).
All 1000 scanned ports on 192.168.150.134 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

(kali@kali)-[~/elastic-agent-8.12.1-linux-x86_64]
$ sudo nmap -sT 192.168.150.134 -p-
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-12 04:18 EST
Nmap scan report for 192.168.150.134
Host is up (0.00093s latency).
All 65535 scanned ports on 192.168.150.134 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 9.13 seconds

(kali@kali)-[~/elastic-agent-8.12.1-linux-x86_64]
$ sudo nmap -A -p- -vv 192.168.150.134
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-12 04:19 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 04:19
Completed NSE at 04:19, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 04:19
Completed NSE at 04:19, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 04:19
```

Fig.8

## 4. Examining the security events in Elastic SIEM.

Now that we have forwarded data from the Kali VM to the SIEM, we can start querying and analysing the logs in the SIEM.

1) Inside your Elastic Deployment, click on the menu icon at the top-left with the three horizontal lines and then click on the “Logs” tab under “Observability” to view the logs from the Kali VM.

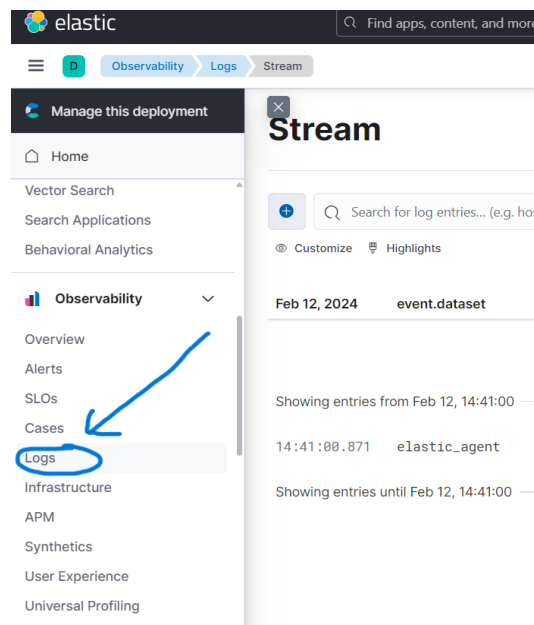


Fig.9

2) In the search bar, enter a search query to filter the logs.

to search for all logs related to Nmap scans, enter the query: **event.action: “nmap\_scan” or process.args: “sudo”**.

3) Click on the “Search” button to execute the search query.

4) The results of the search query will be displayed in the table below. You can click on the three dots next to each event to view more details.

**Stream**

Search bar: `process.args: 'nmap'`

Customize Highlights

Apr 30, 2023	event.action	event.dataset	Message
11:24:32.461	gid_change	endpoint.events.process	Endpoint process event
11:24:32.461	uid_change	endpoint.events.process	Endpoint process event
11:24:32.461	gid_change	endpoint.events.process	Endpoint process event
11:24:32.462	gid_change	endpoint.events.process	Endpoint process event
11:24:32.462	gid_change	endpoint.events.process	Endpoint process event
11:24:32.462	gid_change	endpoint.events.process	Endpoint process event
11:24:34.288	uid_change	endpoint.events.process	Endpoint process event

More details button (three dots) is highlighted next to the third row.

Fig.10

process.args	≡	sudo, nmap, -p-, 10.0.2.15
process.args_count	≡	4
process.command_line	≡	sudo nmap -p- 10.0.2.15
process.command_line.caseless	≡	sudo nmap -p- 10.0.2.15
process.command_line.text	≡	sudo nmap -p- 10.0.2.15

Fig.11

By generating and analysing different types of security events in Elastic SIEM like the one above, or generating authentication failures by typing in the wrong password for a user or attempting SSH logins an incorrect password, you can gain a better understanding of how security incidents are detected, investigated, and responded to in real-world environments.

## 5. Create a Dashboard to Visualize the Events.

You can also use the visualizations and dashboards in the SIEM app to analyse the logs and identify patterns or anomalies in the data. creating a dashboard in Elastic SIEM streamlines security operations, enhances threat visibility, and empowers analysts to proactively safeguard their systems and networks.

### **Advantages of a Dashboard: -**

- **Consolidated View:** Dashboards provide a consolidated view of security-related data, allowing analysts to quickly identify patterns, trends, and anomalies. By visualizing data from various sources, such as logs, network traffic, and system events, a dashboard helps security teams gain insights at first glance .
- **Early Threat Detection:** A well-designed dashboard enables early detection of threats. Analysts can monitor real-time events, track suspicious activities, and respond promptly. For example, visualizing failed login attempts, unusual network traffic, or system anomalies can help identify potential security breaches.
- **Compliance Reporting:** Dashboards facilitate compliance reporting by presenting relevant metrics and indicators. Security teams can track adherence to security policies, regulatory requirements, and industry standards. Having compliance-related visualizations ensures transparency and accountability.
- **Incident Response Support:** During security incidents, dashboards play a vital role. Analysts can quickly assess the situation, investigate alerts, and take necessary actions. Customized dashboards tailored to specific use cases (e.g., detecting malware, monitoring privileged access) enhance incident response efficiency.
- **User-Friendly Interface:** A well-organized dashboard simplifies data interpretation. Analysts can filter, drill down, and explore details without diving into raw

logs. Visualizations like bar charts, pie charts, and maps make complex information more accessible and actionable.

**Steps to create a Dashboard: -**

1. Navigate to the Elastic web portal at <https://cloud.elastic.co/>.
2. Click on the menu icon on the top-left, then under “Analytics,” click on “Dashboards.”

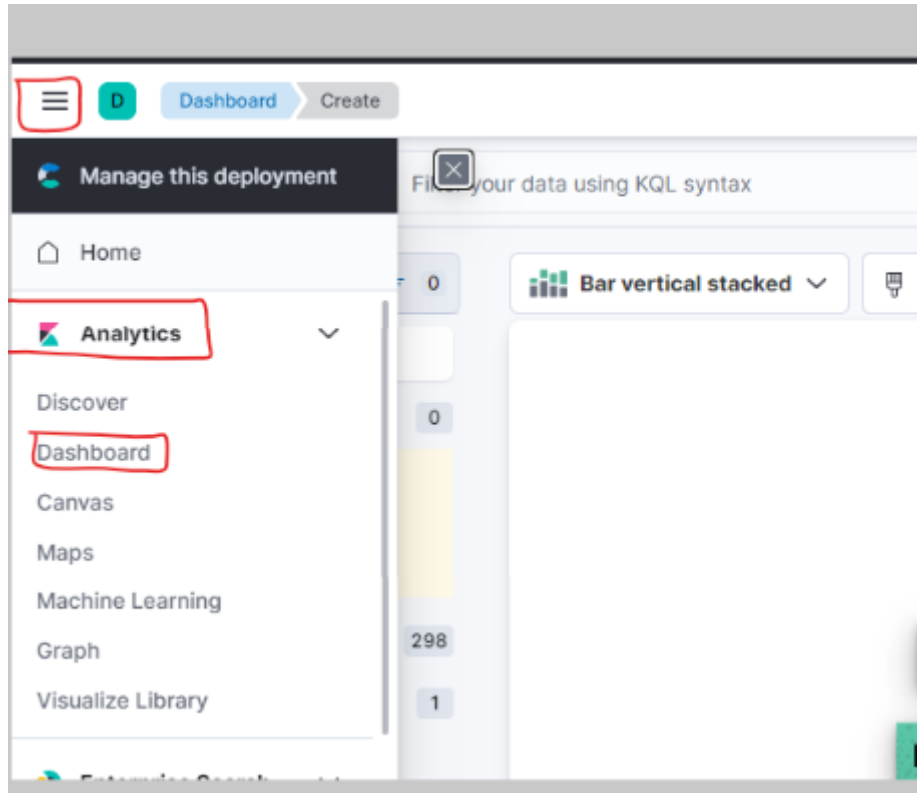


Fig.12

3. Click on the “Create dashboard” button on the top right to create a new dashboard.
4. Click on the “Create Visualization” button to add a new visualization to the dashboard.
5. Select “Area” or “Line” as the visualization type, depending on your preference. This will create a chart that shows the count of events over time.

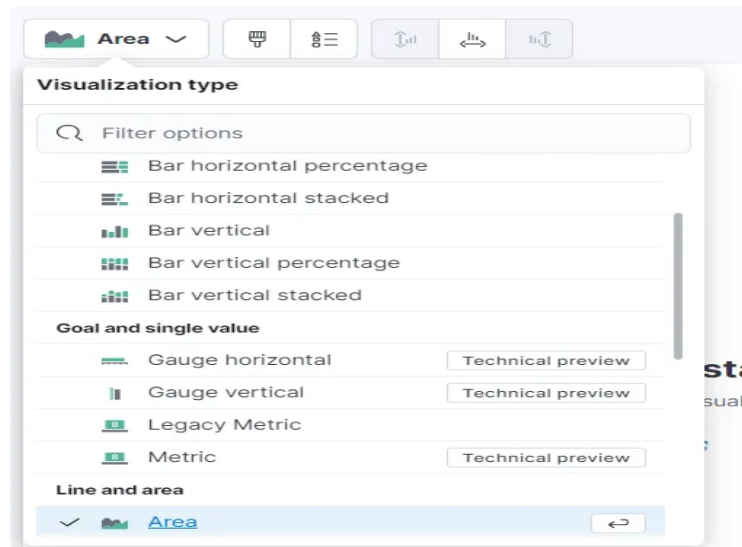


Fig.13

6. In the “Metrics” section of the visualization editor on the right, select “Count” as the vertical field type and “Timestamp” for the horizontal field. This will show the count of events over time.

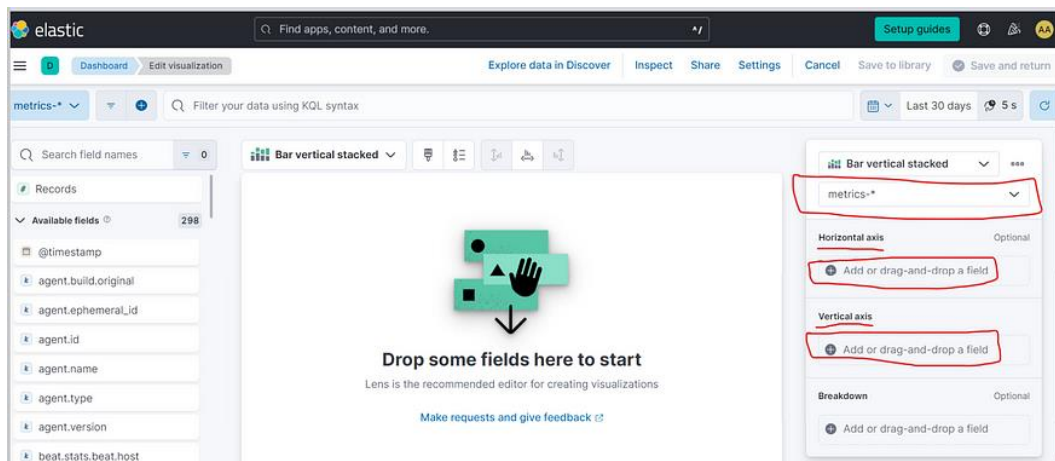


Fig.14

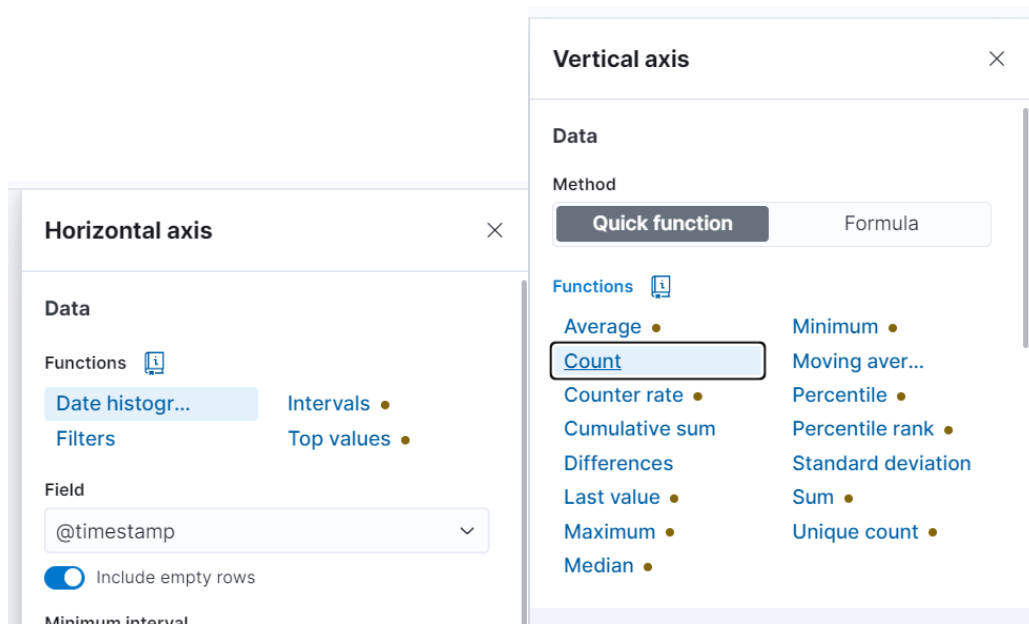


Fig.15

7. Click on the “Save” button to save the visualization and then complete the rest of the settings.

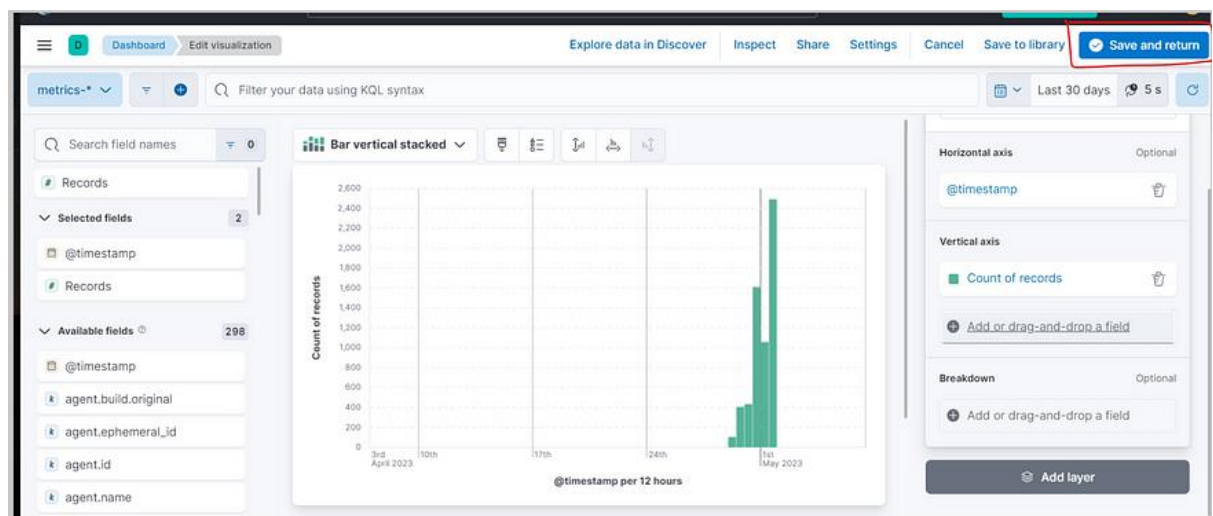


Fig.16

## **6. Create an Alert**

In a SIEM, alerts are a crucial feature for detecting security incidents and responding to them in a timely manner. Alerts are created based on predefined rules or custom queries, and can be configured to trigger specific actions when certain conditions are met. In this task, we will walk through the steps of creating an alert in the Elastic SIEM instance to detect Nmap scans. By following these steps, you can create an alert that will monitor your logs for Nmap scan events and then notify you when they are detected.

Advantages of alerting in Elastic SIEM: -

- **Unified Solution:** Elastic Security SIEM provides a unified, open platform for security analytics. It combines threat detection, investigation, and response capabilities, all powered by Elasticsearch. This holistic approach allows you to centralize environmental activity, analyse data from across your organization, and establish a comprehensive view of security events.
- **Fast and Scalable:** Elastic Security SIEM operates at cloud speed and scale. It can handle data by the petabyte, making it suitable for analysing details dispersed across continents and clouds. Whether you're monitoring historical data or quickly answering urgent questions, Elastic Security SIEM keeps pace with the quickest analysts.
- **Automated Detection:** Elastic Security SIEM automates detection with high-fidelity rules. Behaviour-based rules, backed by research from Elastic Security Labs, help identify suspicious activity and tools. These detections align with MITRE ATT&CK and are openly shared for review and activation.
- **Threat Intelligence Integration:** Enrich alerts by integrating threat intelligence. Elastic's machine learning and alerting features combined with other tools can help reduce false positives, prioritize threats, and mitigate alert fatigue.
- **Security Orchestration and Automation:** Elastic Security SIEM streamlines investigation and response. Native security orchestration, automation, and response (SOAR) capabilities accelerate workflows. You can iteratively hunt with piped queries, gather findings on an interactive timeline, and remotely inspect and invoke actions on distributed endpoints

### **Steps to create an alert:**

1. Click on the menu icon on the top-left, then under "Security," click on "Alerts."
2. Click on "Manage rules" at the top right.

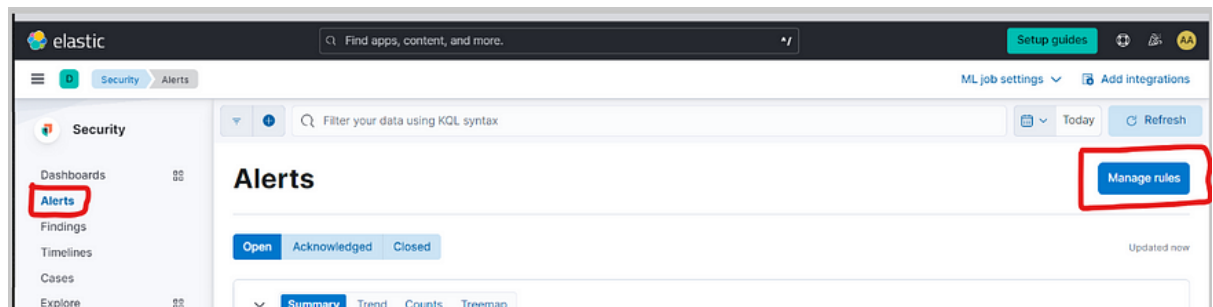


Fig.17

3. 3. Click on the “Create new rule” button at the top right.
4. 4. Under the “Define rule” section, select the “Custom query” option from the dropdown menu.
5. 5. Under “Custom query,” set the conditions for the rule. You can use the following query to detect Nmap scan events.

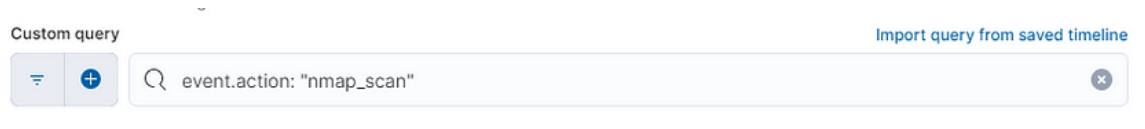


Fig.18

This query will match all events with the action “nmap\_scan.” Then click “Continue.”

6. Under the “About rule” section, give your rule a name and a description (Nmap Scan Detection).
7. Set the severity level for the alert, which can help you prioritize alerts based on their importance. Keep all the other default settings under “Schedule rule” and click “Continue.”



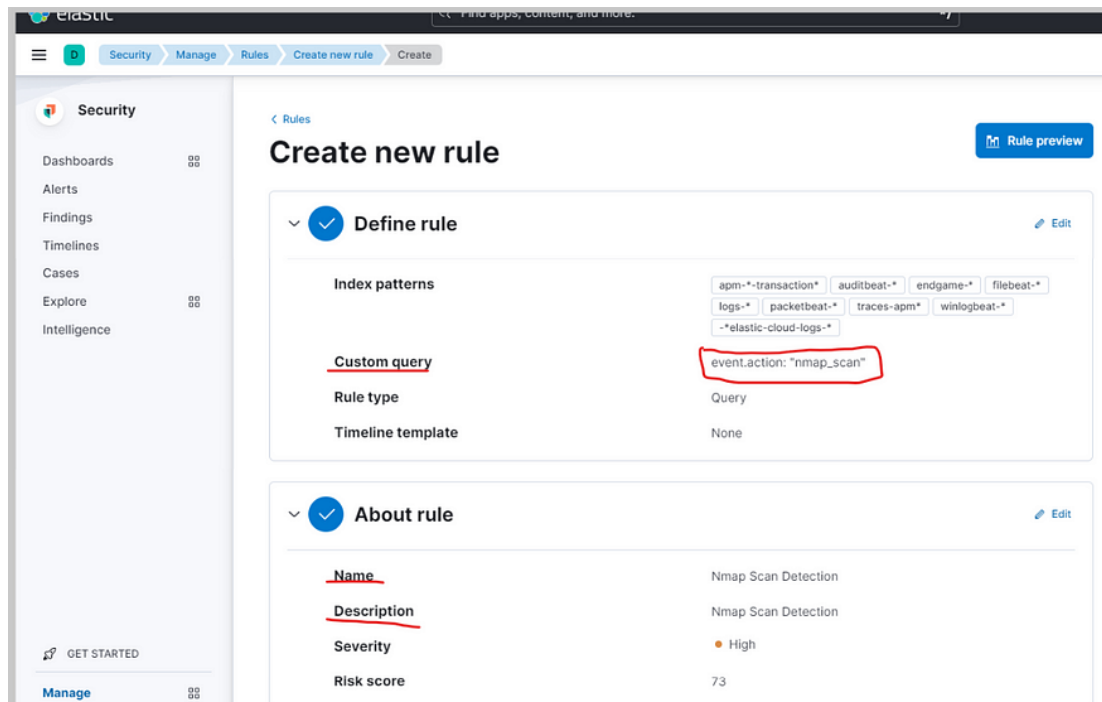


Fig.19

8. In the “Actions” section, select the action you want to take when the rule is triggered. You can choose to send an email notification, create a Slack message, or trigger a custom webhook.

9. Finally, click the “Create and enable rule” button to create the alert.

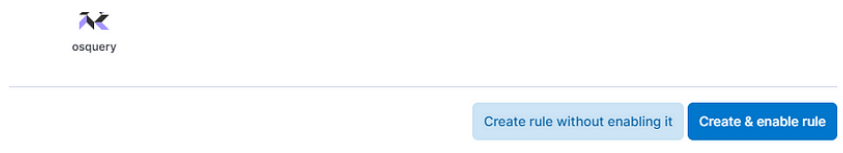


Fig.20

Once you’ve created the alert, it will monitor your logs for Nmap scan events. If an Nmap scan event is detected, the alert will be triggered and the selected action will be taken. You can view and manage your alerts on the “Alerts” section under “Security.”

# Conclusion.

## **Configuration of Elastic Stack SIEM: -**

- Successfully set up and configured Elastic stack SIEM in a home lab environment.
- Demonstrated proficiency in deploying a Kali Linux VM.
- Demonstrated proficiency in Configuring Elastic agent for log collection and forwarding of data to SIEM for Security Event monitoring.

## **Security Event Simulation and Analysis: -**

- Acquired hands-on experience in generating security events using NMAP on Kali Linux.
- Querying in Elastic SIEM was done to identify and investigate Security Incidents thereby enhancing skills in network security monitoring and Threat Detection.

## **Visualization and Alerting in SIEM: -**

- Developed a custom dashboard in elastic SIEM to visualize security events thereby enhancing data interpretation and pattern recognition skills.
- Successfully created and tested alert rules for detecting specific security events, showing competency in proactive incident response and alert management.

# References

1. [Setting Up a Home Lab for Elastic SIEM: A Step-by-Step Guide | by Christopher Elce | Medium](#)
2. [What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time \(freecodecamp.org\)](#)
3. [Elastic SIEM: free and open for security analysts everywhere | Elastic Blog](#)