Elastic SIEM Lab Setup for Threat Detection and Log Analysis

Table of Contents

Overview

This is a step by step guide explains how to set up a Security Information and Event Management (SIEM) lab at home using Elastic Stack and a Kali Linux virtual machine. The goal of the lab is to generate, forward, and analyze security events in Elastic SIEM, helping users learn about security monitoring, incident response, and analysis.

Prerequisites

1. **Virtualization Software**: VirtualBox or VMware
2. **Basic Knowledge**: Familiarity with Linux commands and virtualization setup
3. **Elastic Cloud Account**: A free Elastic account for cloud deployment
4. **Internet Connection**: Necessary for downloading tools and setting up the cloud environment

Project Tasks

Task 1: Set up an Elastic Account

1. **Sign Up**: Visit Elastic Cloud and sign up for a free trial.
2. **Log In**: Access the Elastic Cloud console at Elastic Cloud Console.
3. **Create Deployment**: Choose **"Start your free trial"**, click **"Create Deployment"**, select **"Elasticsearch"** as the deployment type, and configure the region and size as per requirements.
4. **Wait for Setup**: Allow the deployment setup to finish, then click **"Continue"**.

Task 2: Set up the Kali Linux VM

1. **Download Kali**: Download the Kali Linux VM image from Kali’s website.

2. **Create the VM**: Use VirtualBox or VMware to create a VM from the downloaded Kali image.

3. **Configuration**: Allocate at least 2 CPU cores and sufficient memory (e.g., 2GB) to the VM. Ensure network configuration is set to **"Bridged"** or **"Host-Only"** mode.

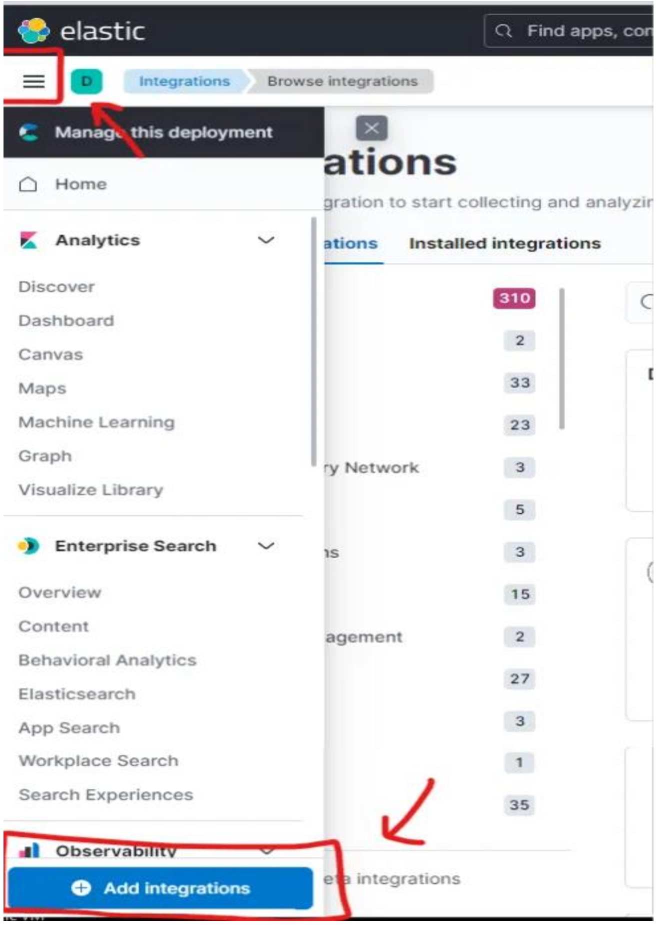
4. **First Run**: Start the VM, log in with credentials (default username/password: kali/kali), and update the system with sudo apt update && sudo apt upgrade.

Task 3: Setting up the Agent to Collect Logs

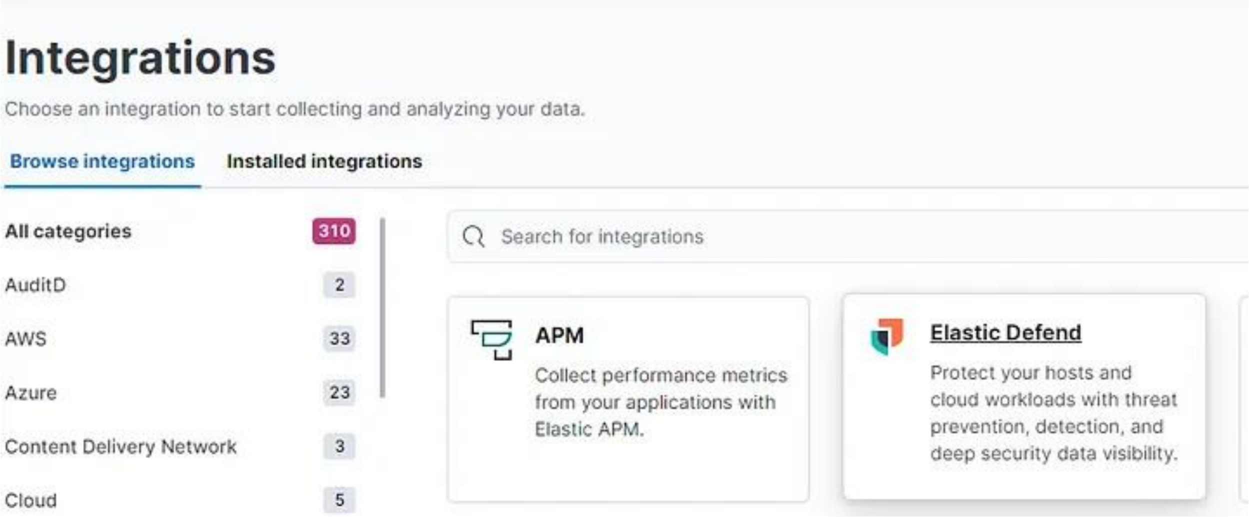
An agent is a software program that is installed on a device, such as a server or endpoint, to collect and send data to a centralized system for analysis and monitoring. In the context of Elastic SIEM, an agent is used to collect and forward security-related events from your endpoints to your Elastic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

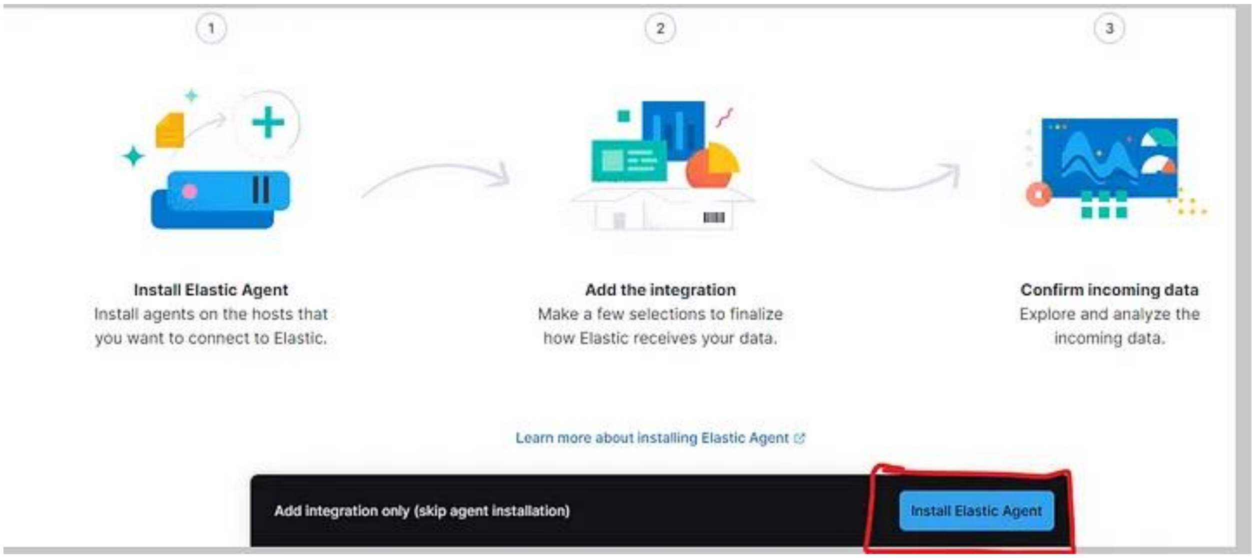
1. Log in to your Elastic SIEM instance and navigate to the Integrations page by: clicking on the Kibana main menu bar at the top left, then selecting "Integrations" at the bottom.



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


Integrations
Choose an integration to start collecting and analyzing your data.
Browse integrations
Installed integrations
All categories 310
AuditD 2
AWS 33
Azure 23
Content Delivery Network 3
Cloud 5
Search for integrations
APM
Collect performance metrics from your applications with Elastic APM.
Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

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



1

Install Elastic Agent
Install agents on the hosts that you want to connect to Elastic.

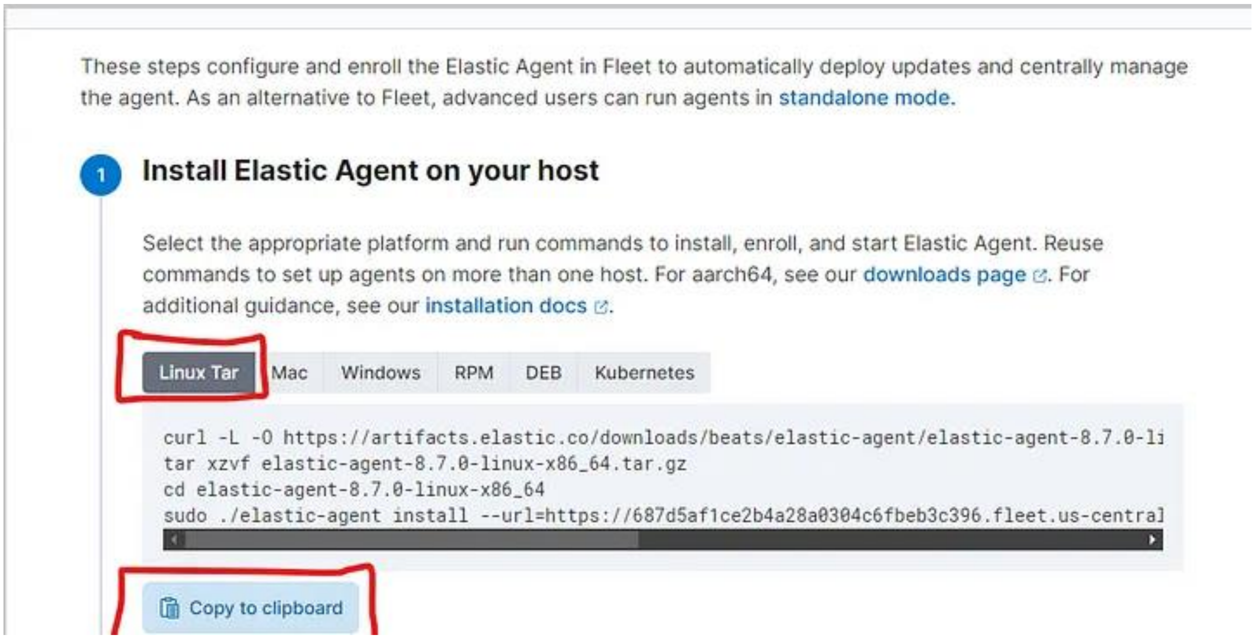
2

Add the integration
Make a few selections to finalize how Elastic receives your data.

3

Confirm incoming data
Explore and analyze the incoming data.

Learn more about installing Elastic Agent



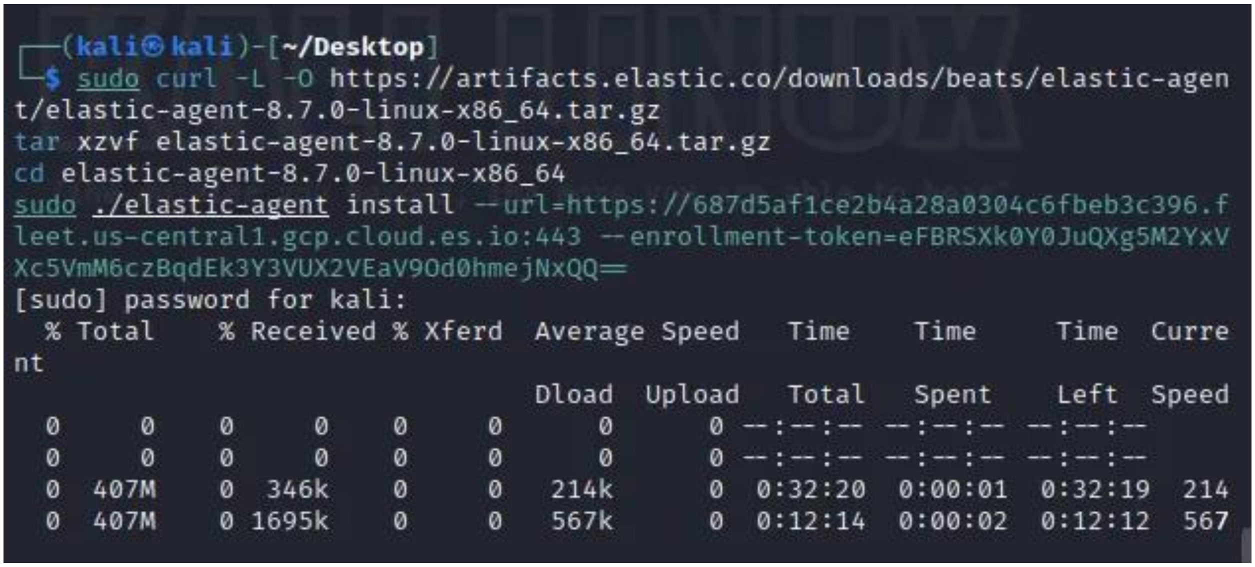
These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in standalone mode.

1 **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. For additional guidance, see our installation docs.

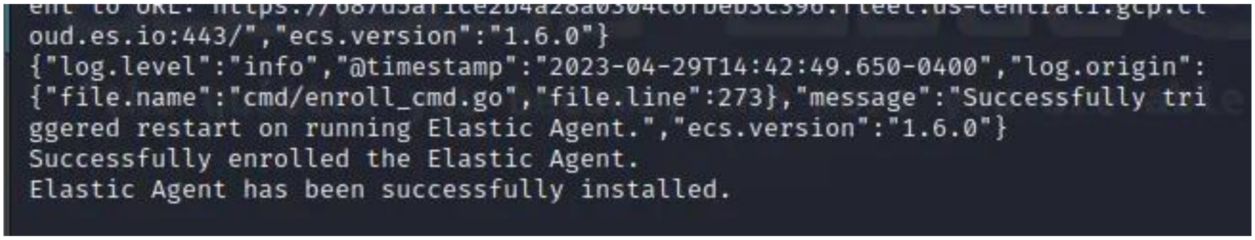
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-li
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://687d5af1ce2b4a28a0304c6fbeb3c396.fleet.us-central
```

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



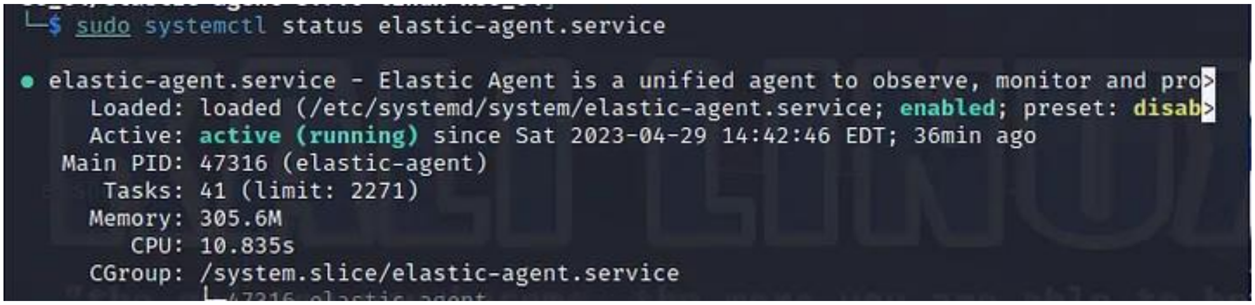
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agen
t/elastic-agent-8.7.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://687d5af1ce2b4a28a0304c6fbeb3c396.f
leet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFBRSXk0Y0JuQXg5M2YxV
Xc5VmM6czBqdEk3Y3VUX2VEaV9Od0hmejNxQQ==
[sudo] password for kali:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curre
nt
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
  0  407M    0  346k    0     0   214k      0  0:32:20  0:00:01  0:32:19  214
  0  407M    0 1695k    0     0   567k      0  0:12:14  0:00:02  0:12:12  567
```

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.
6.



```
ent to URL: https://687d5af1ce2b4a28a0304c6fbeb3c396.fleet.us-central1.gcp.cl
oud.es.io:443/","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-04-29T14:42:49.650-0400","log.origin":
{"file.name":"cmd/enroll_cmd.go","file.line":273},"message":"Successfully tri
ggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
```

You can verify that the agent has been installed correctly by running this command: sudo systemctl status elastic-agent.service.



```
└─$ sudo systemctl status elastic-agent.service

● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and pro>
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disab>
     Active: active (running) since Sat 2023-04-29 14:42:46 EDT; 36min ago
   Main PID: 47316 (elastic-agent)
      Tasks: 41 (limit: 2271)
     Memory: 305.6M
        CPU: 10.835s
     CGroup: /system.slice/elastic-agent.service
             └─47316 elastic-agent
```

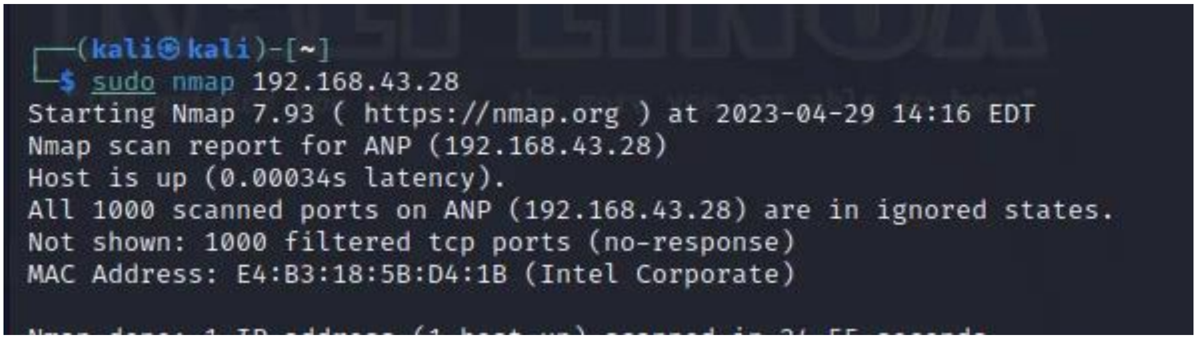
If you get an error installing the agent, make sure that your Kali is connected to the internet before proceeding by pinging google.com.

Task 4: Generating Security Events on the Kali 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.

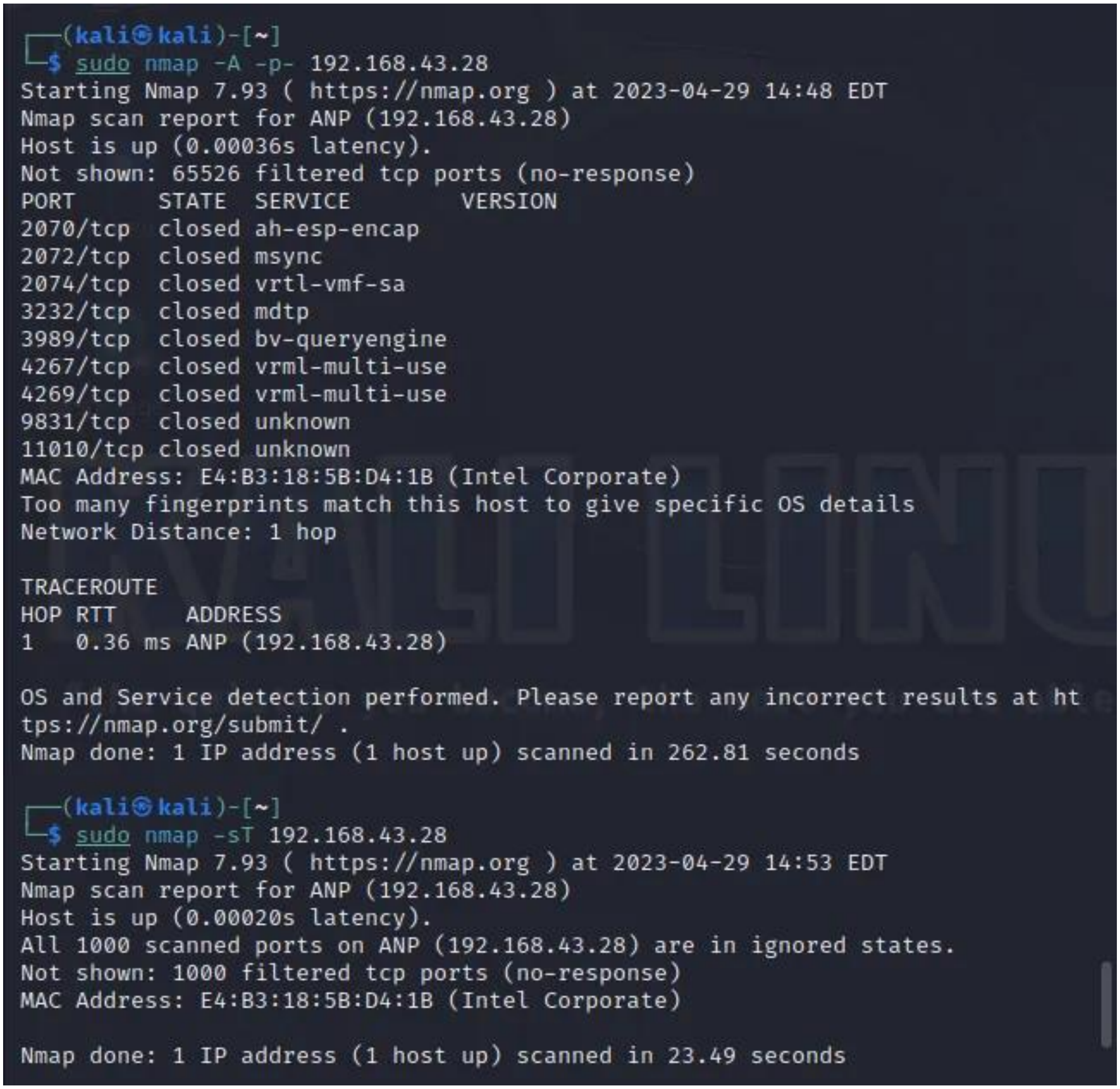
To run an Nmap scan, follow these steps:

1. Install Nmap on the Linux VM if you’re not using Kali, Nmap already comes preinstalled in Kali. Open a new Terminal and run this command to install it: sudo apt-get install nmap.
2. Run a scan on Kali machine by running the command: sudo nmap <vm-ip>. You can also run a scan of your host machine if you place your Kali VM on a “bridged” network.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-29 14:16 EDT
Nmap scan report for ANP (192.168.43.28)
Host is up (0.00034s latency).
All 1000 scanned ports on ANP (192.168.43.28) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E4:B3:18:5B:D4:1B (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 34.55 seconds
```

3. This scan generates several security events, such as the detection of open ports and the identification of services running on those ports. **Run a few more Nmap scans** (“nmap -sS <ip address>”, “nmap -sT <ip address>”, “nmap -p- <ip address>”etc..”



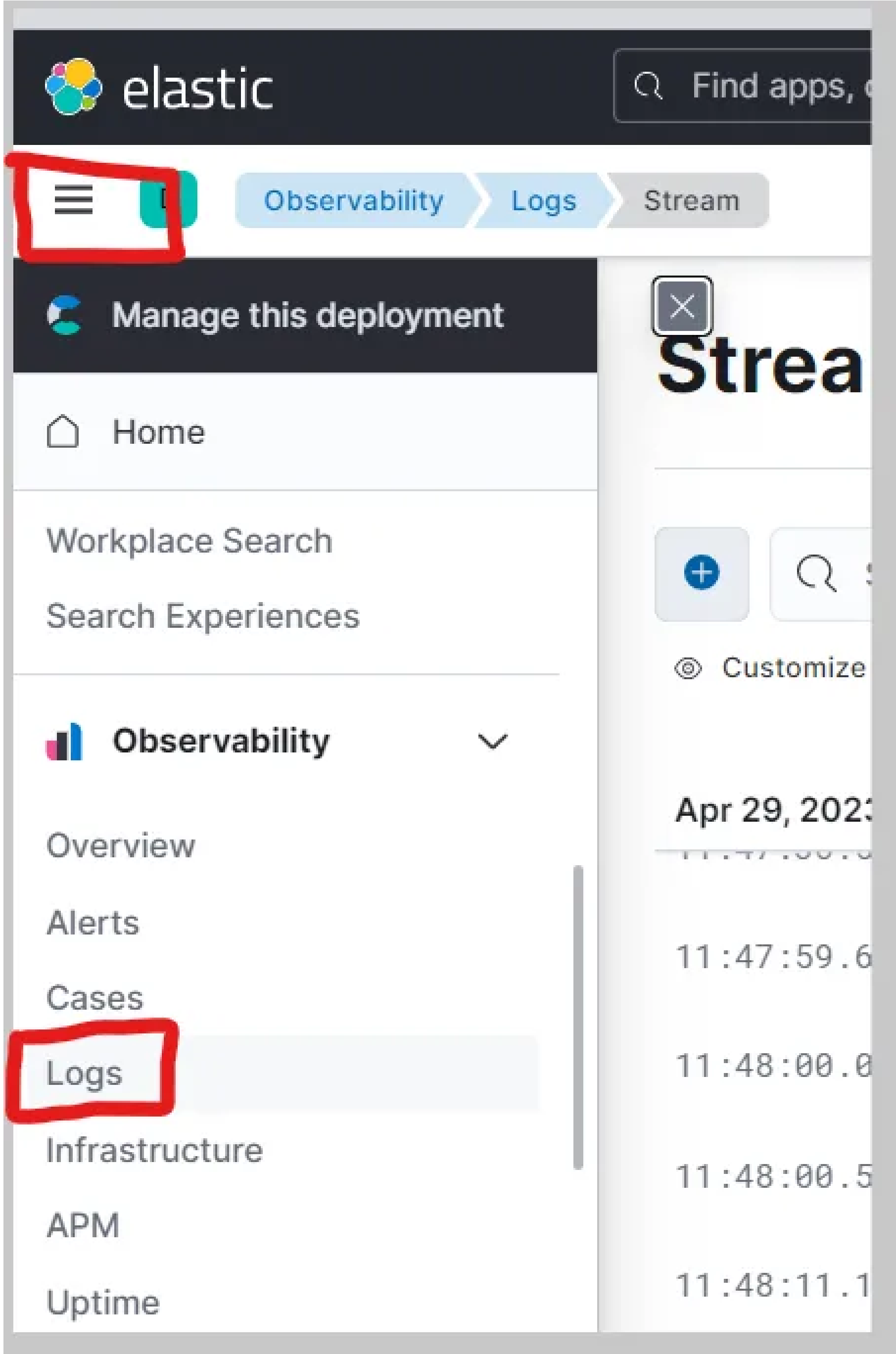
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -p- 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-29 14:48 EDT
Nmap scan report for ANP (192.168.43.28)
Host is up (0.00036s latency).
Not shown: 65526 filtered tcp ports (no-response)
PORT      STATE  SERVICE        VERSION
2070/tcp  closed ah-esp-encap
2072/tcp  closed msync
2074/tcp  closed vrtl-vmf-sa
3232/tcp  closed mdtp
3989/tcp  closed bv-queryengine
4267/tcp  closed vrml-multi-use
4269/tcp  closed vrml-multi-use
9831/tcp  closed unknown
11010/tcp closed unknown
MAC Address: E4:B3:18:5B:D4:1B (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms ANP (192.168.43.28)

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 262.81 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.43.28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-29 14:53 EDT
Nmap scan report for ANP (192.168.43.28)
Host is up (0.00020s latency).
All 1000 scanned ports on ANP (192.168.43.28) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E4:B3:18:5B:D4:1B (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 23.49 seconds
```

Task 5: Querying for Security Events in the Elastic SIEM

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

To do this, follow these steps:

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.

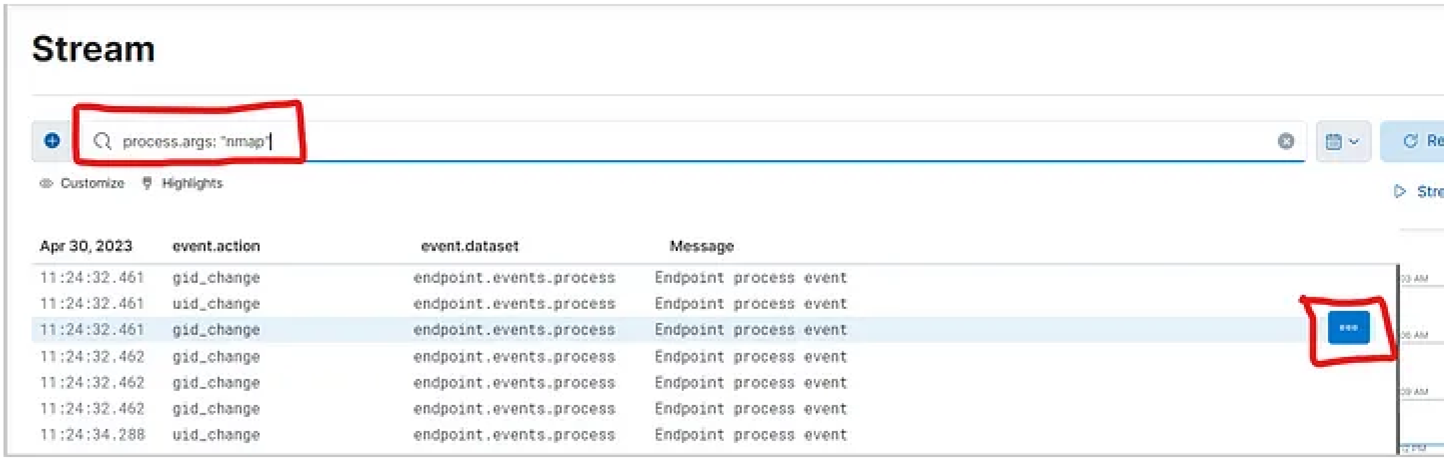


2. In the search bar, enter a search query to filter the logs. For example, to search for all logs related to Nmap scans, enter the query: event.action: “nmap_scan” or process.args: “sudo”.

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

But please note that it can sometimes take a while for the events to populate and show up on the SIEM, so this query might not work right away.

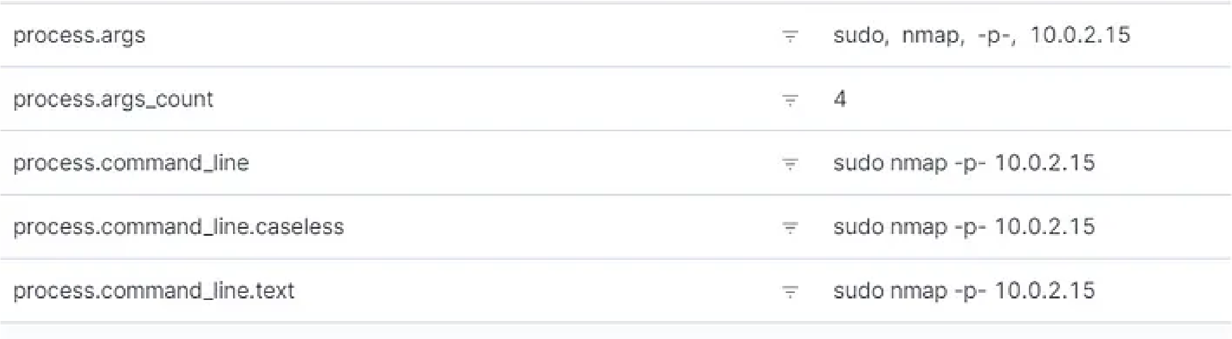
4.The results of the search query will be displayed in the table below. You can click on the three dots next to each event to view more details.



Stream

process.args: "nmap"

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



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

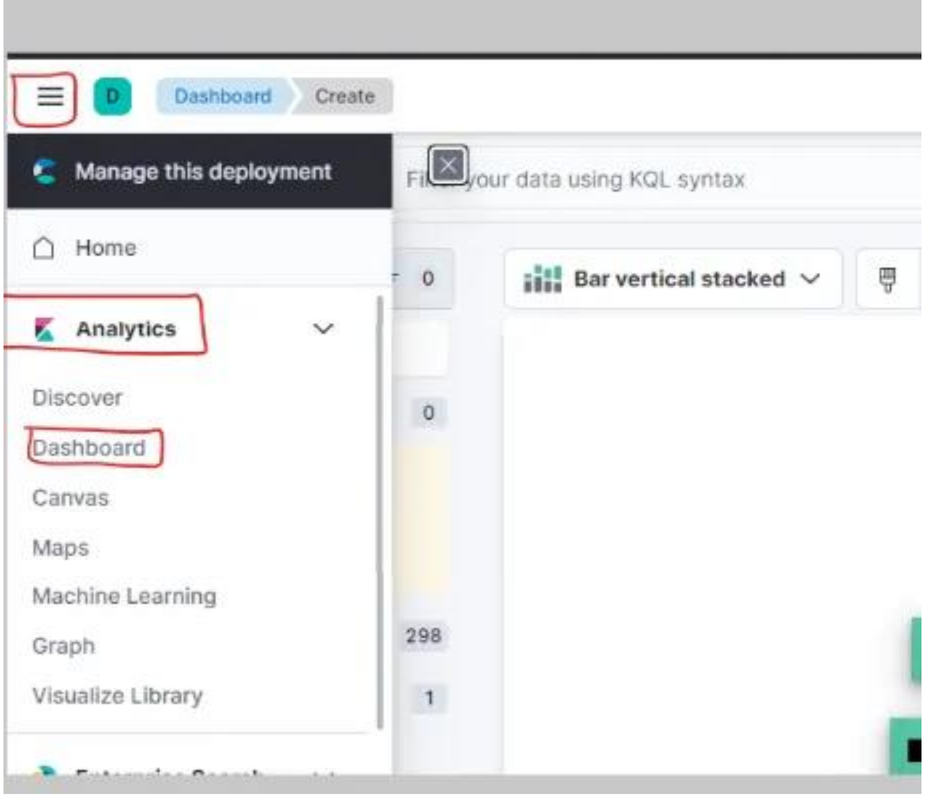
By generating and analyzing different types of security events in Elastic SIEM like the one above, or generating authentication failures by typing in the wrong password for a user or attempting SSH logins an incorrect password, you can gain a better understanding of how security incidents are detected,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

Task 6: Create a Dashboard to Visualize the Events

You can also use the visualizations and dashboards in the SIEM app to analyze the logs and identify patterns or anomalies in the data. For example, you can create a simple dashboard that shows a count of security events over time.

Here’s how you can do that:

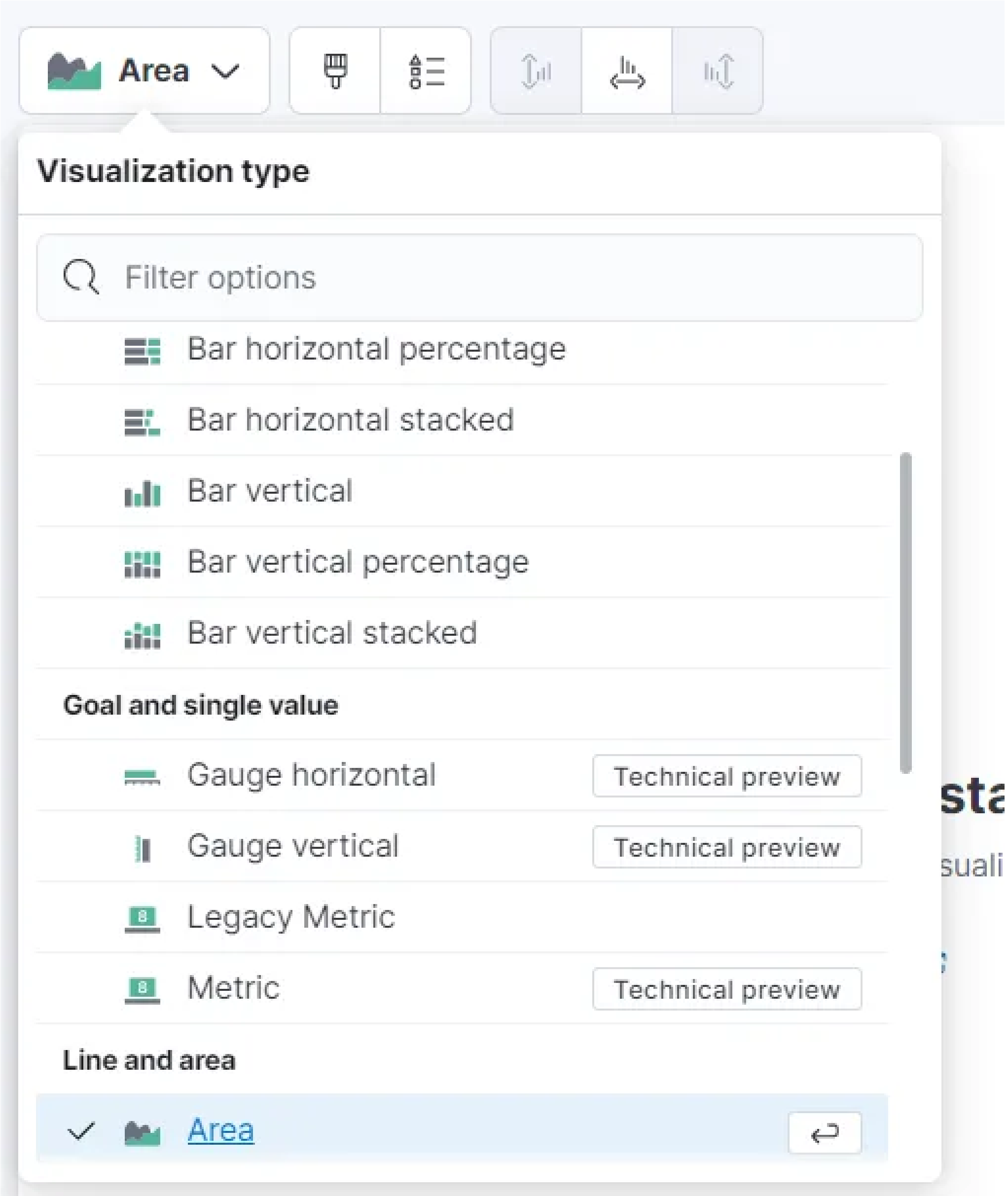
1. Navigate to the Elastic web portal at https://cloud.elastic.co/.
2. Click on the menu icon on the top-left, then under “Analytics,” click on “Dashboards.”



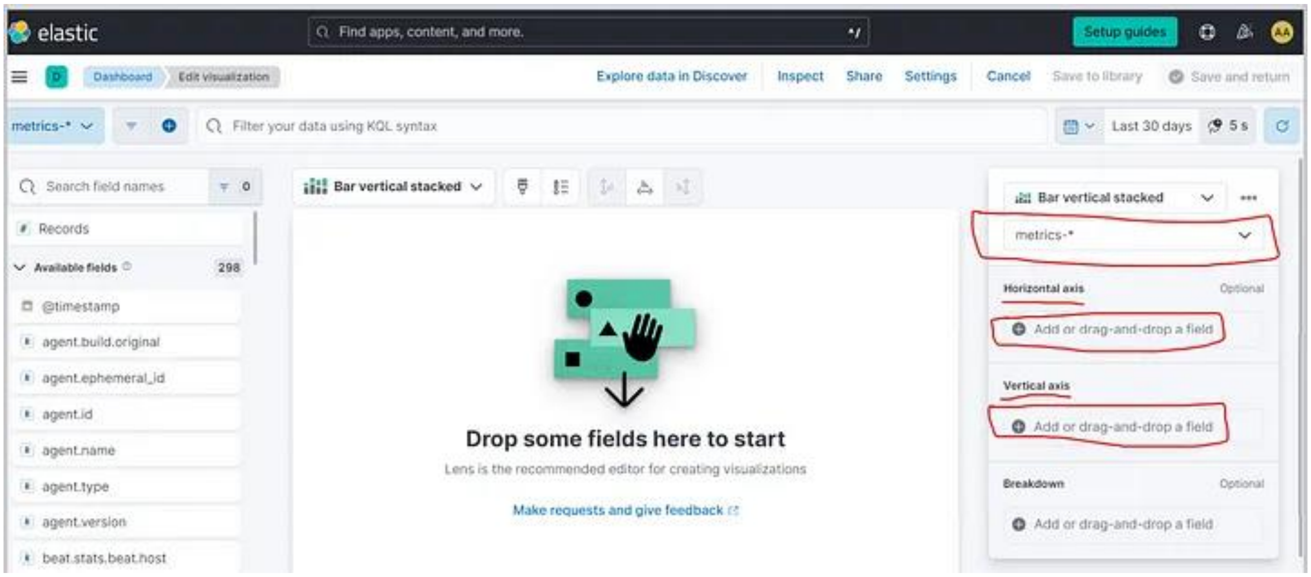
3. Click on the “Create dashboard” button on the top right to create a new dashboard.

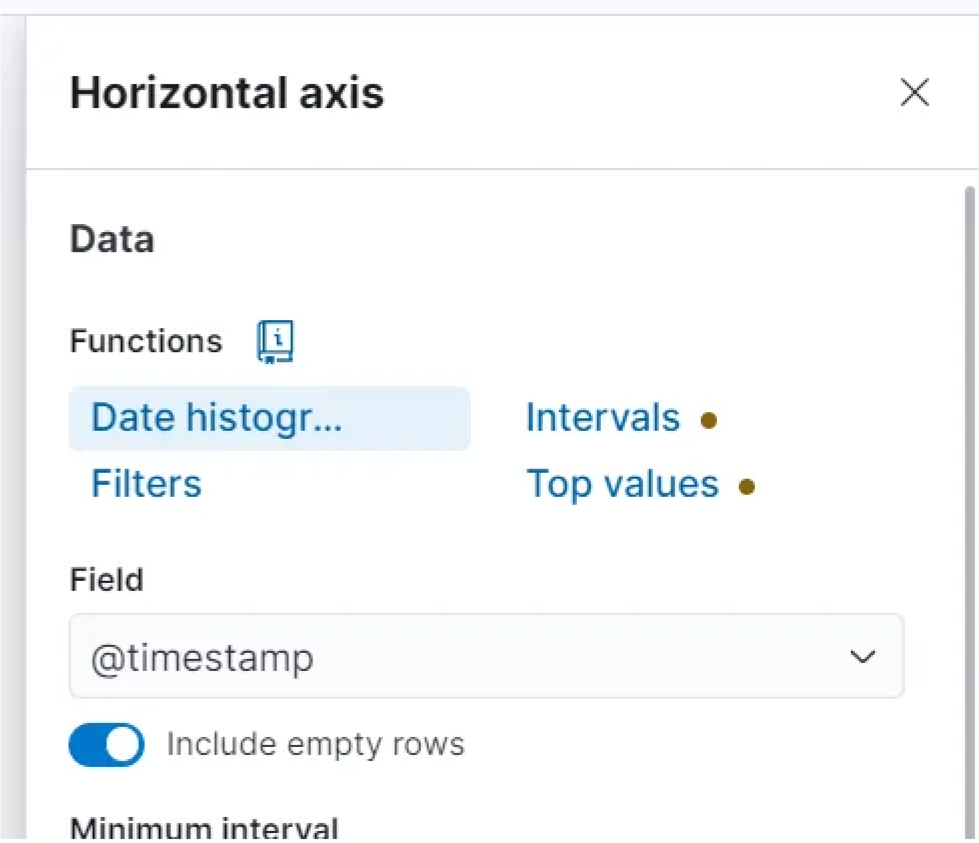
4. Click on the “Create Visualization” button to add a new visualization to the dashboard.

4. 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.



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.




Horizontal axis

Data

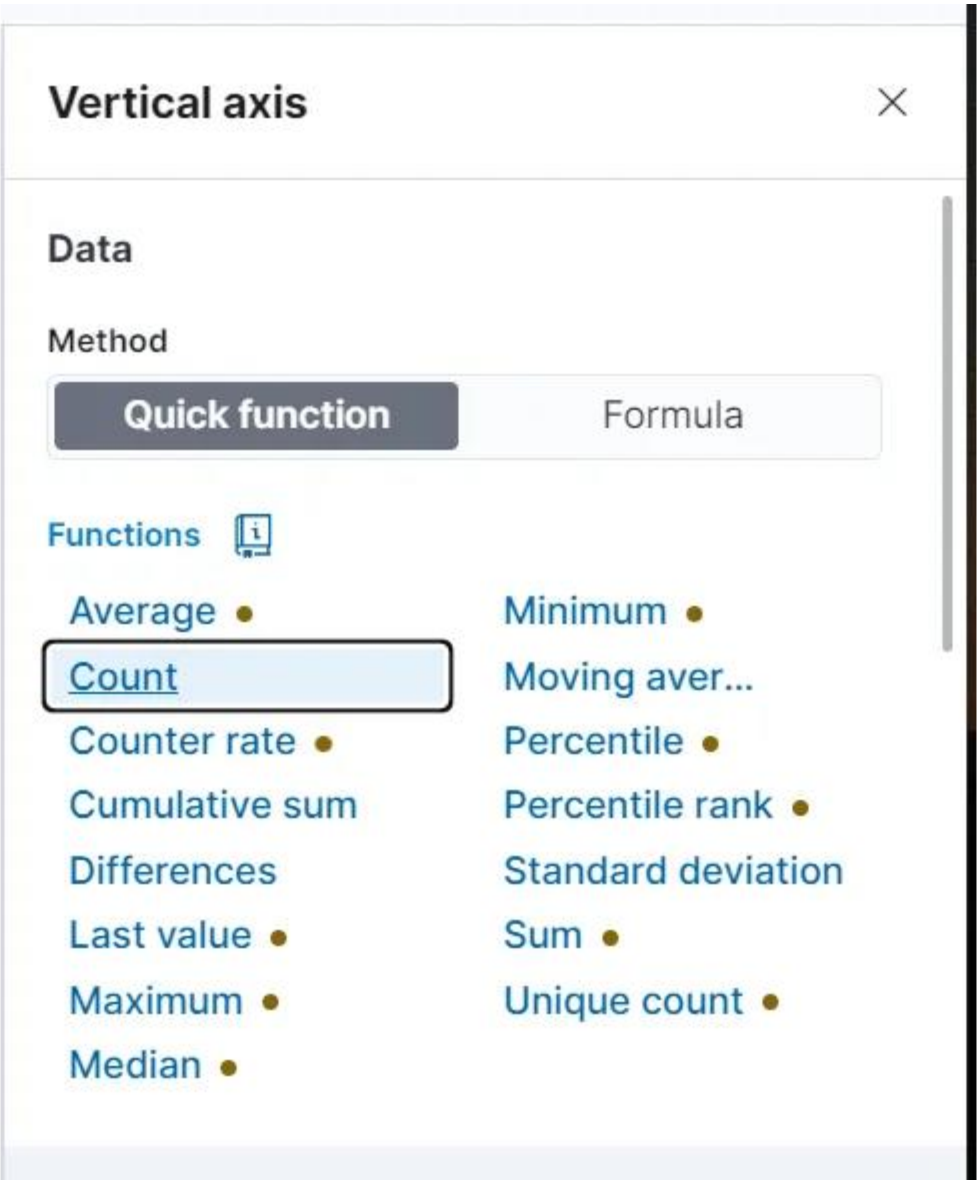
Functions

Date histogr... | Intervals ● | Filters | Top values ●

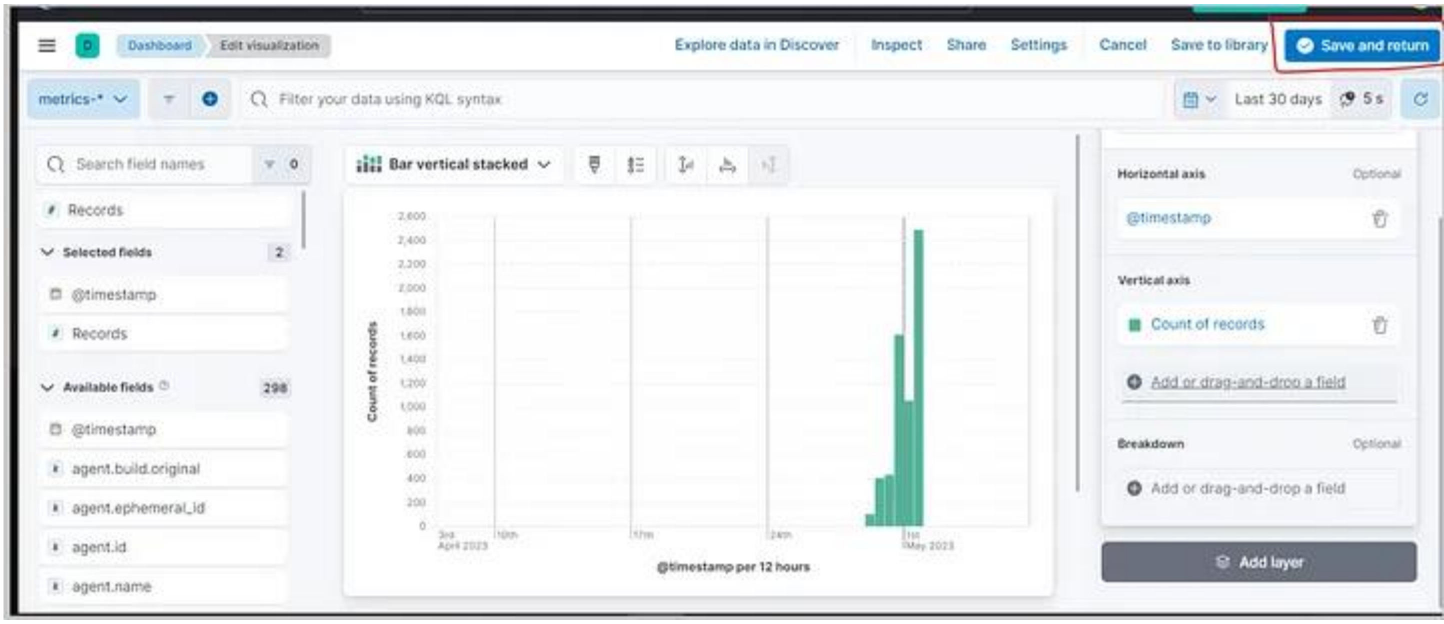
Field: @timestamp

Include empty rows (on)

Minimum interval



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

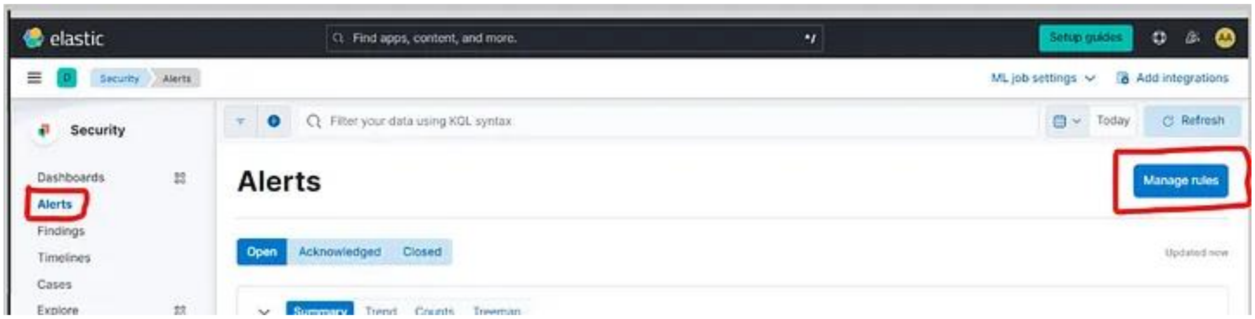


Task 7: Create an Alert

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.

Here are the steps:

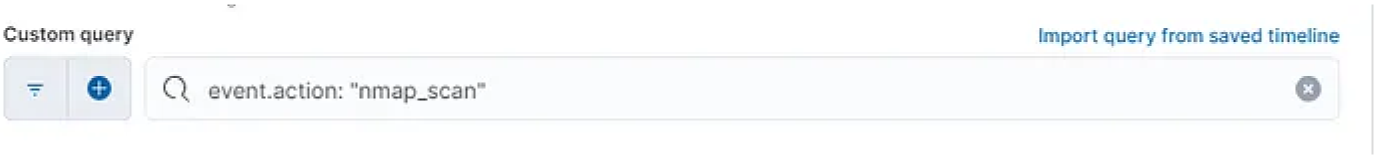
1. Click on the menu icon on the top-left, then under "Security," click on "Alerts."
2. Click on "Manage rules" at the top right.



3. Click on the “Create new rule” button at the top right.

4. Under the “Define rule” section, select the “Custom query” option from the dropdown menu.

5. Under “Custom query,” set the conditions for the rule. You can use the following query to detect Nmap scan events.



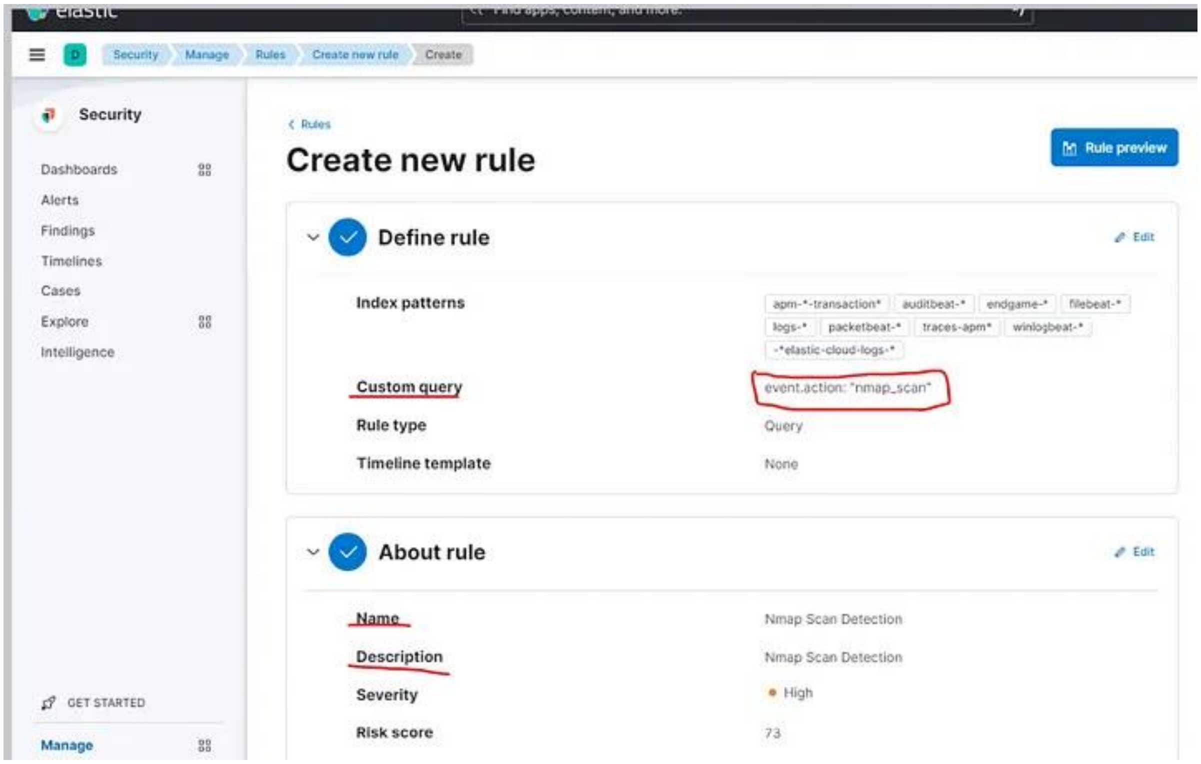
Custom query

```
event.action: "nmap_scan"
```

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.”



Create new rule

Define rule

Index patterns	apm-*-transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* traces-apm* winlogbeat-* -*elastic-cloud-logs-*
Custom query	event.action: "nmap_scan"
Rule type	Query
Timeline template	None

About rule

Name	Nmap Scan Detection
Description	Nmap Scan Detection
Severity	● High
Risk score	73

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.

Conclusion

In this project, we have set up a home lab using Elastic SIEM and a Kali VM. We forwarded data from the Kali VM to the SIEM using the Elastic Beats agent, generated security events on the Kali VM using Nmap, and queried and analyzed the logs in the SIEM using the Elastic web interface. We also created a dashboard to visualize security events and then created an alert to detect security events.

This home lab provides a valuable environment for learning and practicing the skills necessary for effective security monitoring and incident response using Elastic SIEM. By following these steps, you can gain hands-on experience with using a SIEM and improve your security monitoring skills to help you become a successful security analyst or engineer.

Contact Information

If you have any questions, feedback, or would like to connect, feel free to reach out to me:

- **LinkedIn: linkedin.com/in/r-rafi-cybersecurity**

Thank you for reviewing my project.