Elastic SIEM Lab

Welcome to the Elastic SIEM Home Lab Documentation! This guide provides instructions for setting up and utilizing a basic Elastic Stack Security Information and Event Management (SIEM) environment. It covers configuring agents, generating security events, analyzing logs, visualizing data, and setting up alerts within Elastic SIEM.

Prerequisites

- **Virtualization Software**: VirtualBox or VMware
- **Basic Linux Knowledge**

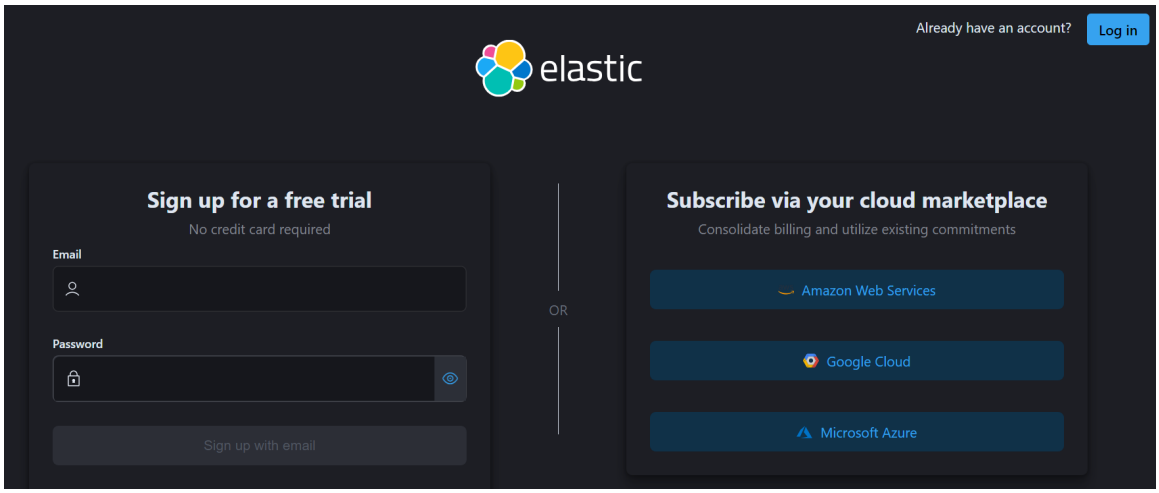
Overview of Tasks

- Set up a free Elastic account
- Install the Kali VM
- 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

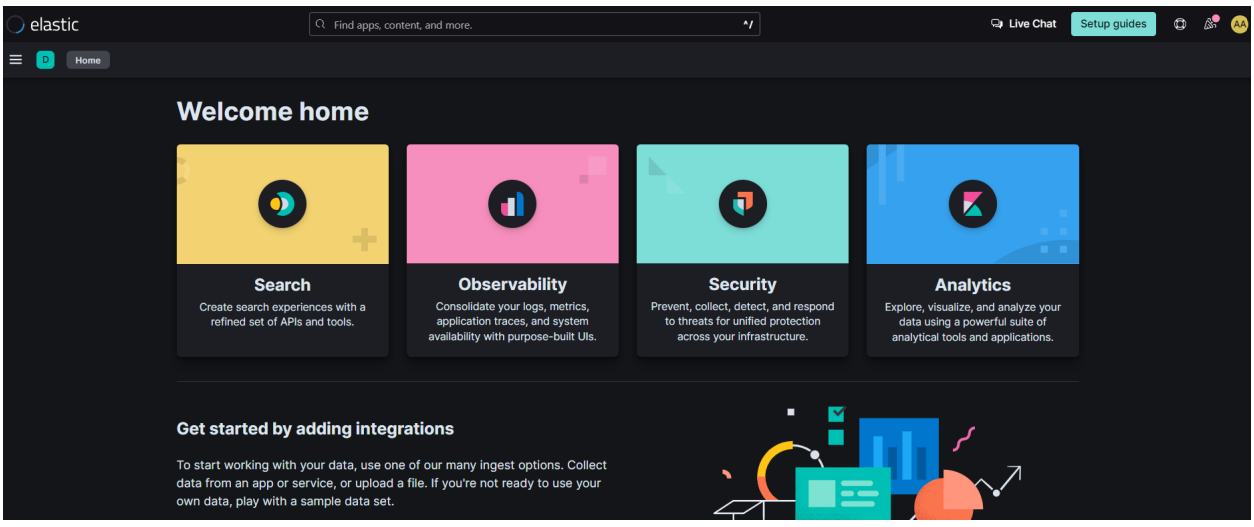
Task 1: Set up an Elastic Account

Create an Elastic account to create a cloud instance conducive to SIEM operation.

1. Sign up for a free trial to use Elastic Cloud at https://cloud.elastic.co/registration



1. Once the account is created, log in to the Elastic Cloud console at https://cloud.elastic.co.
2. Click on the “Create Deployment” button and select “Elasticsearch” as the deployment type.
3. Wait for the configuration to complete.
4. Once the deployment is ready, click “Continue.”

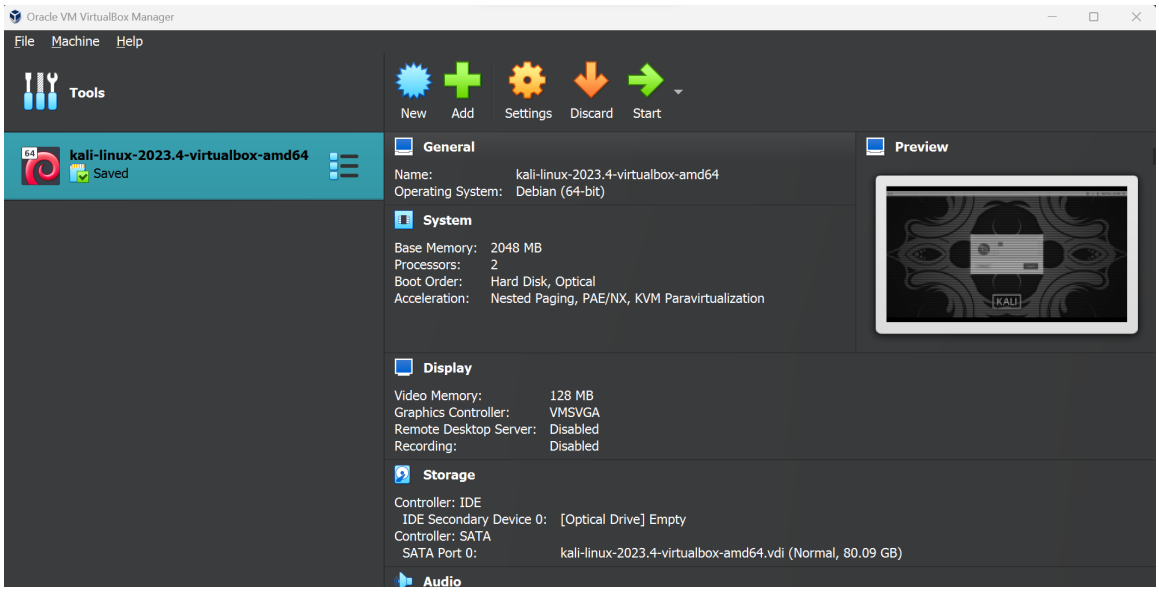


Task 2: Setting up the Linux VM

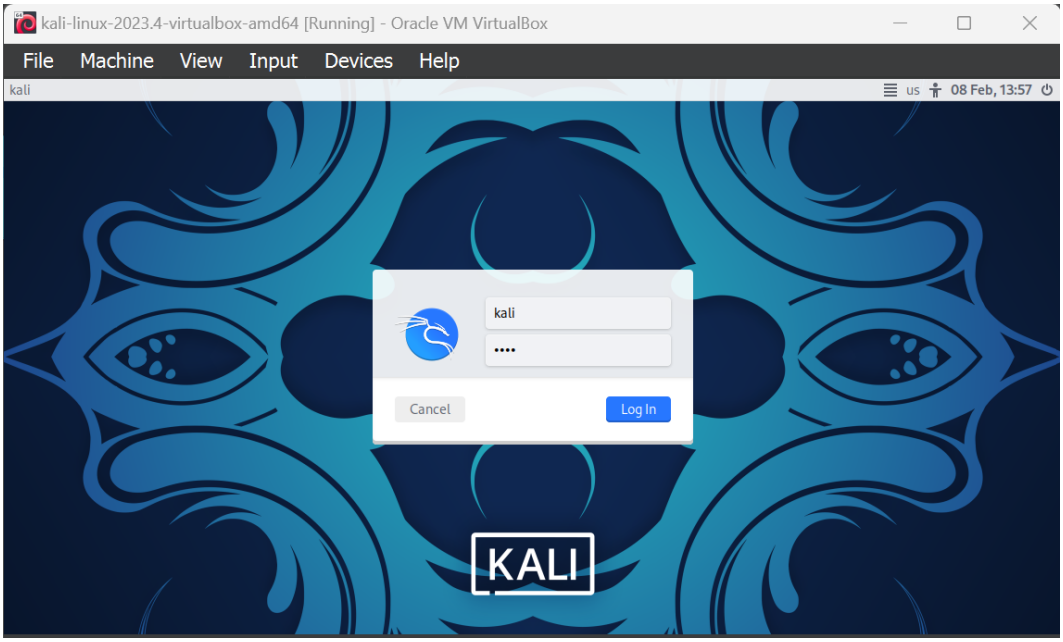
Setting up the Linux VM involves the following steps:

1. **Download Kali Linux VM**: Obtain the Kali Linux VM from the official website here.

2. **Create a new VM**: Utilize your preferred virtualization platform (e.g., VirtualBox or VMware) to create a new VM using the downloaded Kali VM file.
3. **Initiate installation**: Start the VM and proceed with the installation of Kali Linux by following the on-screen instructions.



4. **Log in to the VM**: Upon completion of the installation, log in to the Kali VM using the default credentials: username and password both set as "kali".

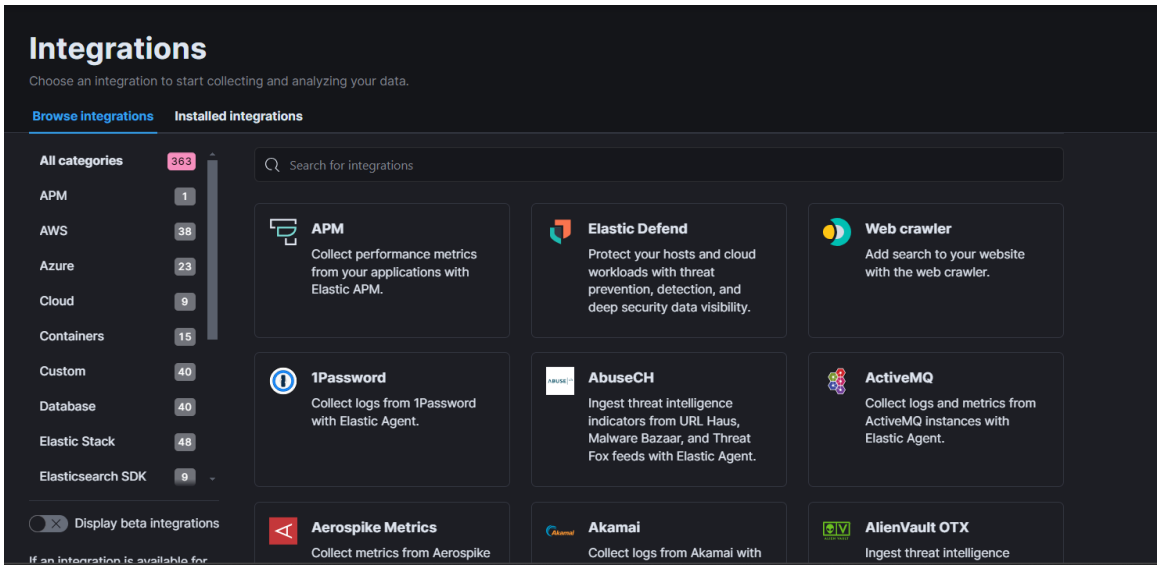


Task 3: Setting up the Agent to Collect Logs

An integral aspect of security monitoring entails deploying agents, which are software components responsible for gathering and transmitting data from endpoints to a central system for analysis. Within the framework of Elastic SIEM, agents play a vital role in facilitating the collection and forwarding of security-related events to the Elastic SIEM instance.

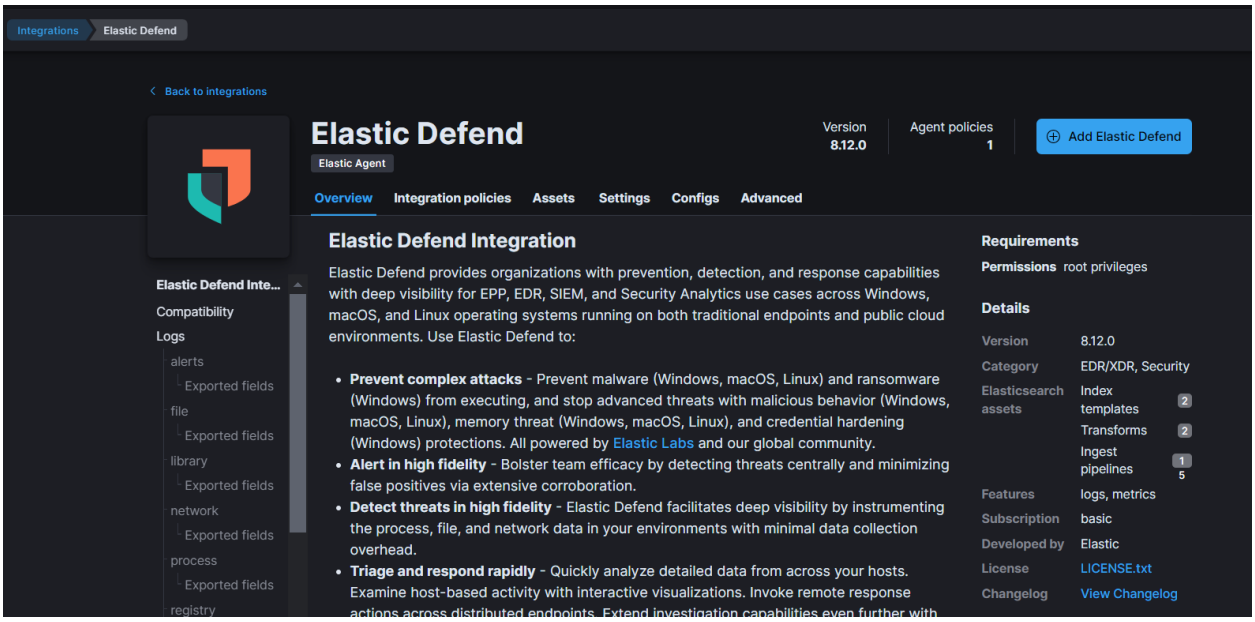
To configure the agent to get logs from the Kali VM and relay them to the Elastic SIEM instance, adhere to the following methodical steps:

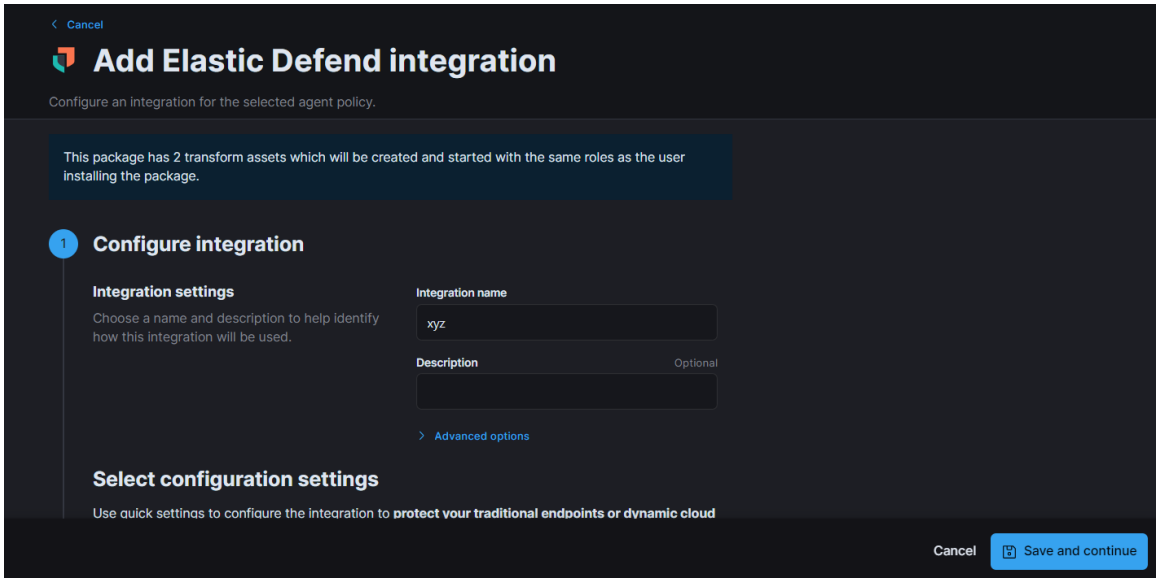
1. **Access the Integrations Page**: Commence by logging into your Elastic SIEM instance and accessing the Integrations page. This can be accomplished by navigating to the Kibana main menu located at the top left corner, followed by selecting "Integrations" situated at the bottom.



2. **Install Elastic Defend**: Upon accessing the Integrations page, initiate a search for "Elastic Defend" and proceed to select it, thereby opening the integration page.
3. **Initiate Installation**: Subsequently, click on "Install Elastic Defend" and meticulously follow the provided instructions on the integration page to facilitate the installation of the agent on your Kali VM.

- Ensure the "Linux" option is selected and meticulously copy the provided command to your clipboard for subsequent execution.





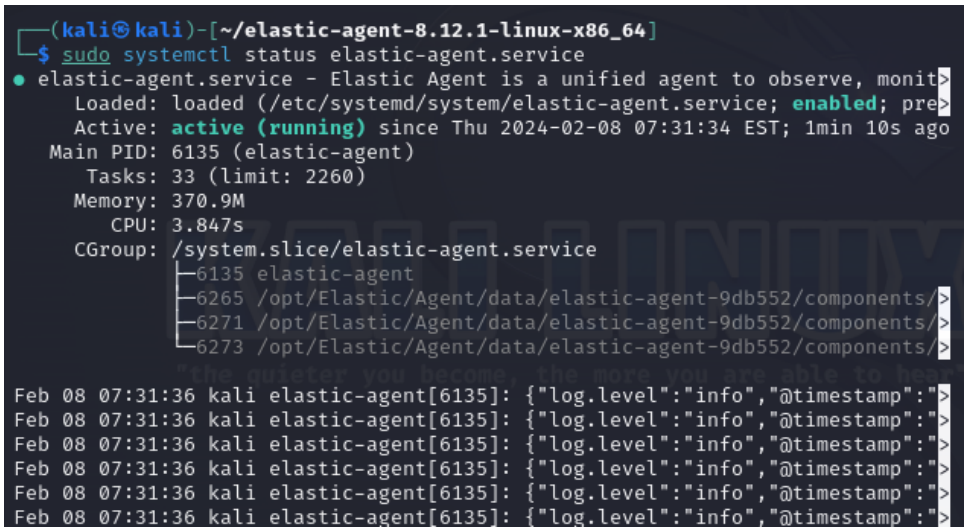
4. **Execute Installation Command**: Transfer the copied command to the terminal (command line) of your Kali VM and execute it accordingly.

```
┌──(kali㉿kali)-[~]
└─$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/ela
stic-agent-8.12.1-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.1-linux-x86_64.tar.gz
cd elastic-agent-8.12.1-linux-x86_64
sudo ./elastic-agent install --url=https://4c52c78079184c5ca9bf323064c02d1e.f
leet.us-central1.gcp.cloud.es.io:443 --enrollment-token=ajk2dmlJMEJvYkFQRFhHZ
HFRWnA6MHl0T3VhMDJUclNSa05MT3dYeUZ2QQ==
  % 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  552M    0 98129    0     0  98253      0  1:38:15 --:--:--  1:38:15 9862
  0  552M    0 4551k    0     0  2315k      0  0:04:04  0:00:01  0:04:03 2320
  2  552M    2 11.7M    0     0  4043k      0  0:02:19  0:00:02  0:02:17 4048
  3  552M    3 18.7M    0     0  4830k      0  0:01:57  0:00:03  0:01:54 4835
  4  552M    4 25.8M    0     0  5330k      0  0:01:46  0:00:04  0:01:42 5333
  5  552M    5 31.3M    0     0  5387k      0  0:01:44  0:00:05  0:01:39 6451
  7  552M    7 38.6M    0     0  5687k      0  0:01:39  0:00:06  0:01:33 7012
  8  552M    8 45.6M    0     0  5863k      0  0:01:36  0:00:07  0:01:29 6944
  9  552M    9 52.7M    0     0  6023k      0  0:01:33  0:00:08  0:01:25 6970
 10  552M   10 58.9M    0     0  6056k      0  0:01:33  0:00:09  0:01:24 6777
 11  552M   11 65.9M    0     0  6160k      0  0:01:31  0:00:10  0:01:21 7083
 13  552M   13 73.5M    0     0  6297k      0  0:01:29  0:00:11  0:01:18 7147
 14  552M   14 81.2M    0     0  6414k      0  0:01:28  0:00:12  0:01:16 7291
```

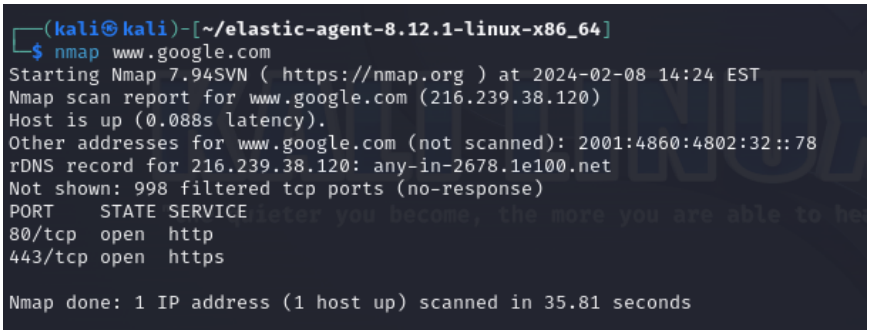
```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a servi
ce. Do you want to continue? [Y/n]:Y
[ ==] Service Started  [27s] Elastic Agent successfully installed, starting
enrollment.
[== ] Waiting For Enroll...  [27s] {"log.level":"info","@timestamp":"2024-02
-08T07:31:34.185-0500","log.origin":{"file.name":"cmd/enroll_cmd.go","file.li
ne":496},"message":"Starting enrollment to URL: https://4c52c78079184c5ca9bf3
23064c02d1e.fleet.us-central1.gcp.cloud.es.io:443/","ecs.version":"1.6.0"}
[=  ] Waiting For Enroll...  [30s] {"log.level":"info","@timestamp":"2024-02
-08T07:31:36.714-0500","log.origin":{"file.name":"cmd/enroll_cmd.go","file.li
ne":461},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"
}
{"log.level":"info","@timestamp":"2024-02-08T07:31:36.718-0500","log.origin":
{"file.name":"cmd/enroll_cmd.go","file.line":285},"message":"Successfully tri
ggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=  ] Done  [30s]
Elastic Agent has been successfully installed.
```

5. **Verification**: Upon the completion of the installation process, a confirmation message will be displayed, signaling the successful installation of the Elastic Agent. The agent will promptly commence the collection and transmission of logs to your Elastic SIEM instance. However, it may take a brief period for the logs to manifest within the SIEM interface.

- Validate the installation's success by executing the command: `sudo systemctl status elastic-agent.service`.



- In the event of encountering installation errors, it is imperative to ascertain that your Kali VM possesses an active internet connection, which can be verified by pinging `www.google.com`.



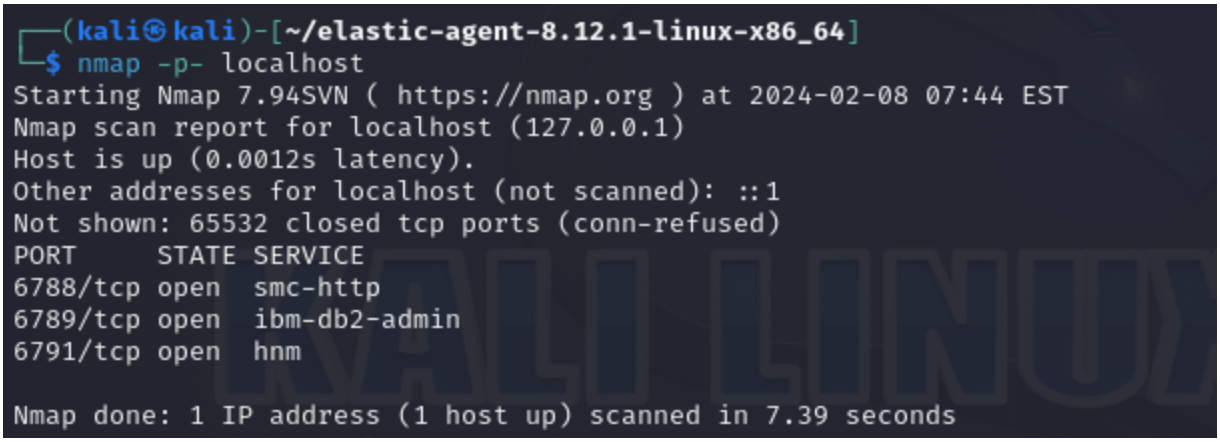
By meticulously adhering to these sequential steps, we can configure the agent to diligently get and transmit logs from the Kali VM to the Elastic SIEM instance, thereby fortifying the security monitoring capabilities.

Task 4: Generating Security Events on the Kali VM

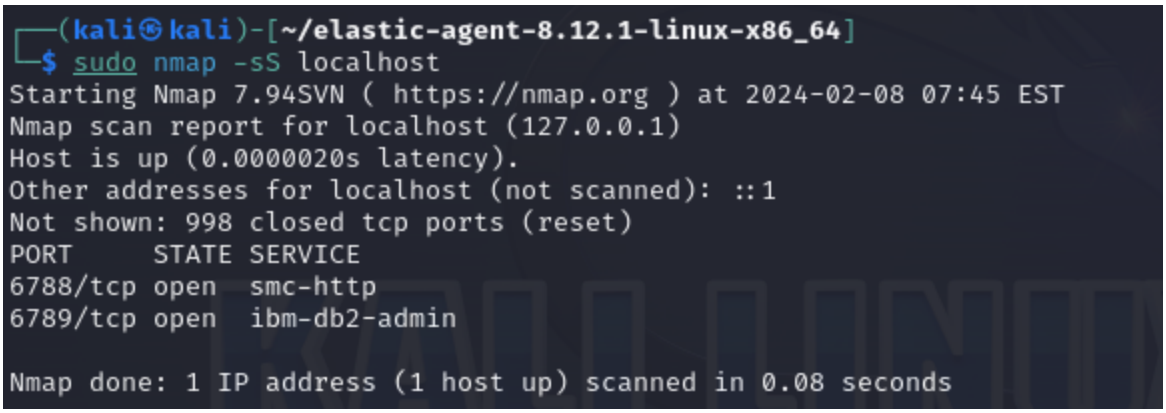
To verify the agent's functionality, security-related events must be generated on the Kali VM. Nmap, a versatile open-source utility, is suitable for this purpose. Nmap, or Network Mapper, is adept at network exploration, management, and security auditing. It facilitates host and service discovery on a network, aiding in the creation of a comprehensive network "map." Nmap scans can detect open ports, identify operating systems and services, and gather crucial network information.

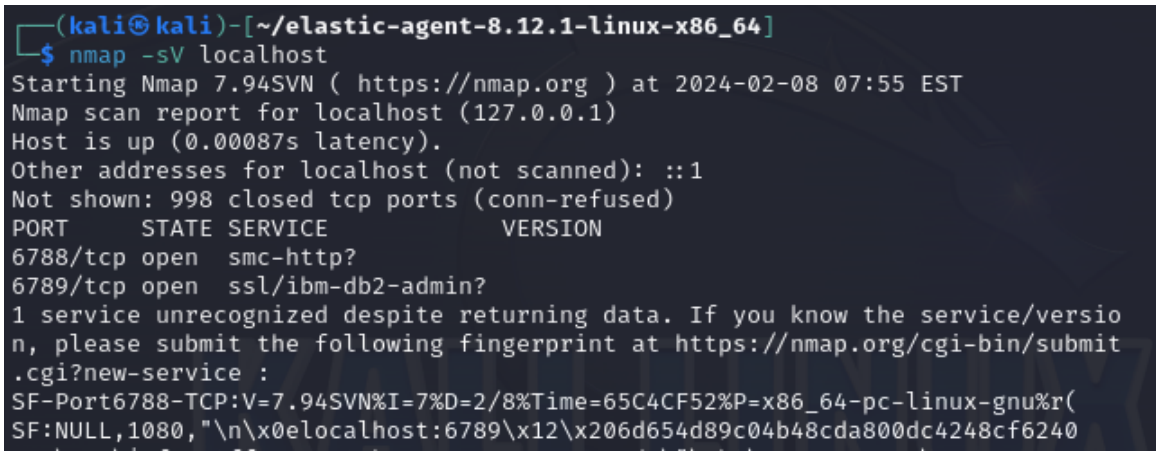
To conduct an Nmap scan, follow these steps:

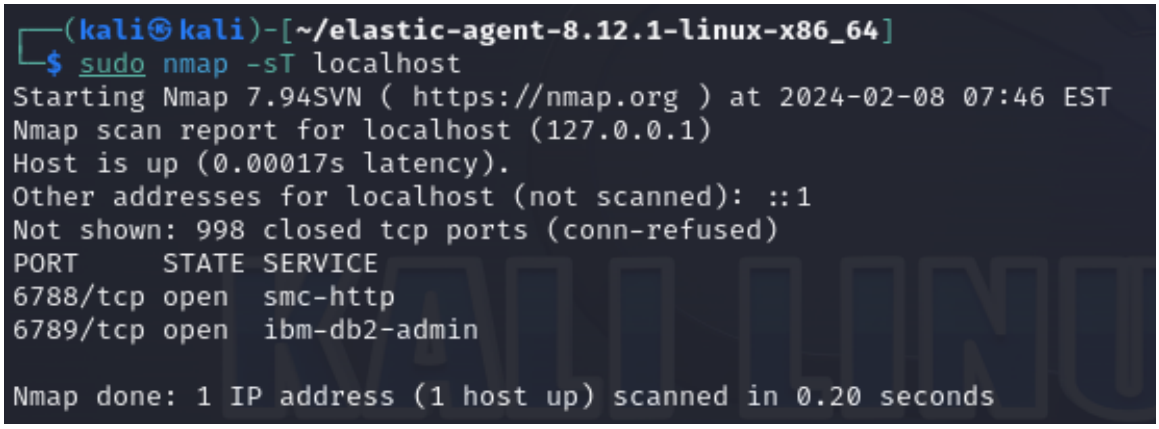
1. **Install Nmap (if necessary)**: If Nmap is not preinstalled, install it on the Linux VM by executing the following command in a new Terminal: `sudo apt-get install nmap`.
2. **Run Nmap Scan**: Execute an Nmap scan on the Kali machine by entering the command: `sudo nmap -p- localhost`. Alternatively, perform a scan on the host machine by placing the Kali VM on a "bridged" network.



3. **Generate Security Events**: The Nmap scan generates various security events, including the detection of open ports and identification of services running on those ports. To enhance event generation, conduct additional Nmap scans using different scan options, such as "nmap -sS localhost", "nmap -sV localhost", and "nmap -sT localhost", among others.





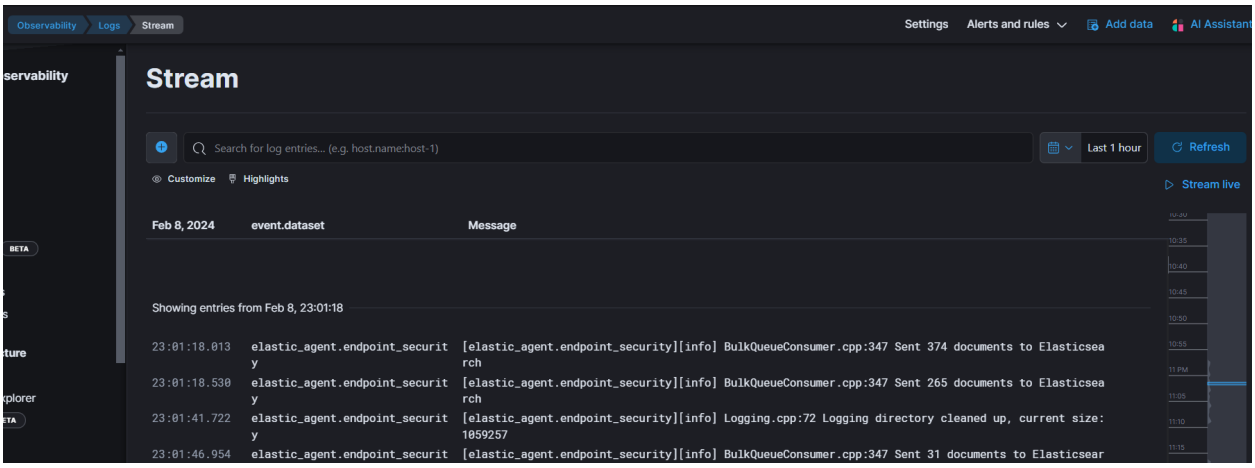


Following these steps effectively generates a diverse range of security events on the Kali VM, providing valuable data for testing and validation.

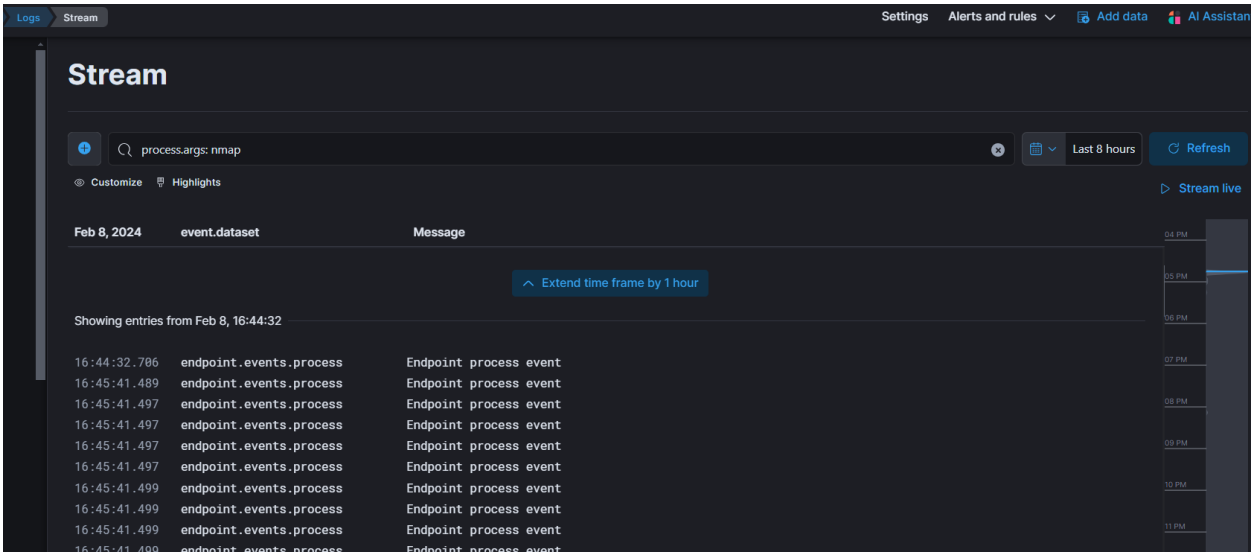
Task 5: Querying for Security Events in the Elastic SIEM

With data forwarded from the Kali VM to the SIEM, querying and analyzing logs within the SIEM interface can commence. Follow these steps to proceed:

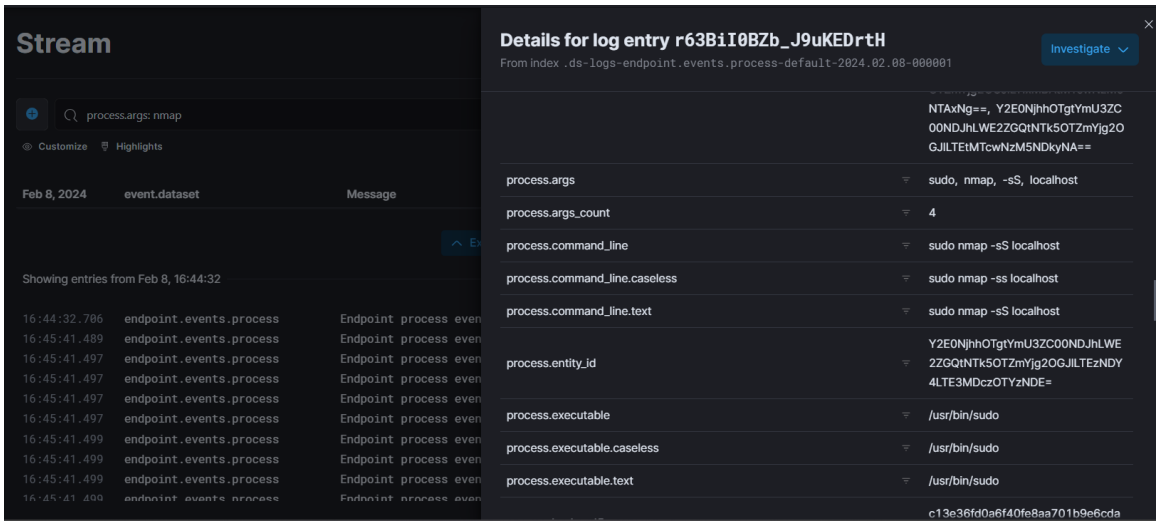
1. **Access the Logs Interface**: Within the Elastic Deployment, navigate to the "Logs" tab under "Observability." Click on the menu icon at the top-left corner with the three horizontal lines to access the Logs tab.



2. **Enter Search Query**: In the search bar, input a search query to filter the logs. For instance, to retrieve logs pertaining to Nmap scans, utilize a query such as: `process.args: "nmap"` or `process.args: "sudo"`.



3. **Execute Search**: Click on the "Search" button to execute the search query. Please note that it may take some time for the events to populate and appear in the SIEM interface, so the results might not be immediate.
4. **Review Results**: The results of the search query will be displayed in the table below. Further details can be explored by clicking on the three dots next to each event.



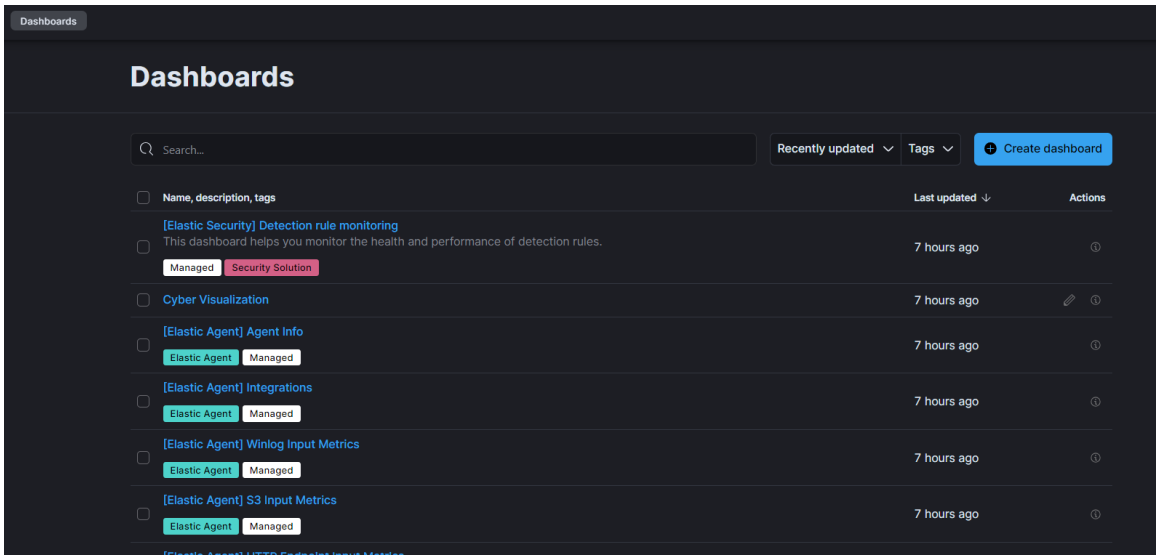
By conducting various queries and analyzing different types of security events within Elastic SIEM, such as authentication failures or SSH login attempts with incorrect passwords, a better understanding of how security incidents are identified, investigated, and responded to in real-world scenarios can be gained.

Task 6: Create a Dashboard to Visualize the Events

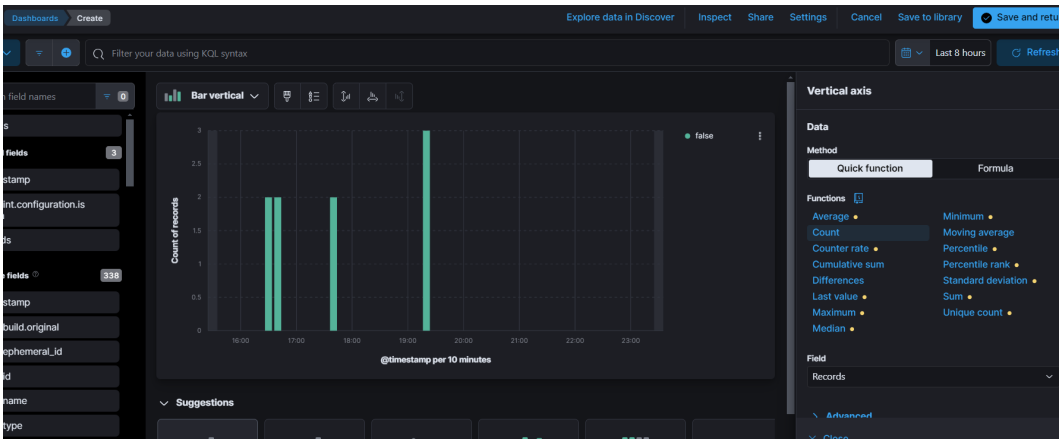
Utilize the visualizations and dashboards within the SIEM app to analyze logs and identify patterns or anomalies in the data. For instance, a simple dashboard displaying a count of security events over time can be created.

Follow these steps to accomplish this:

1. **Access the Elastic Web Portal**: Navigate to the Elastic web portal at cloud.elastic.co.
2. **Navigate to Dashboards**: Click on the menu icon located at the top-left corner. Under "Analytics," select "Dashboards."



3. **Create a New Dashboard**: Click on the "Create dashboard" button situated at the top-right corner to initiate the creation of a new dashboard.
4. **Add Visualization**: Click on the "Create Visualization" button to add a new visualization to the dashboard.
5. **Select Visualization Type**: Choose either "Area" or "Line" as the visualization type, depending on preference. This selection will generate a chart illustrating the count of events over time.
6. **Configure Metrics**: In the "Metrics" section of the visualization editor on the right, designate "Count" as the vertical field type and "Timestamp" for the horizontal field. This configuration will display the count of events over time.
7. **Save Visualization**: Click on the "Save" button to preserve the visualization and proceed to complete the remaining settings.



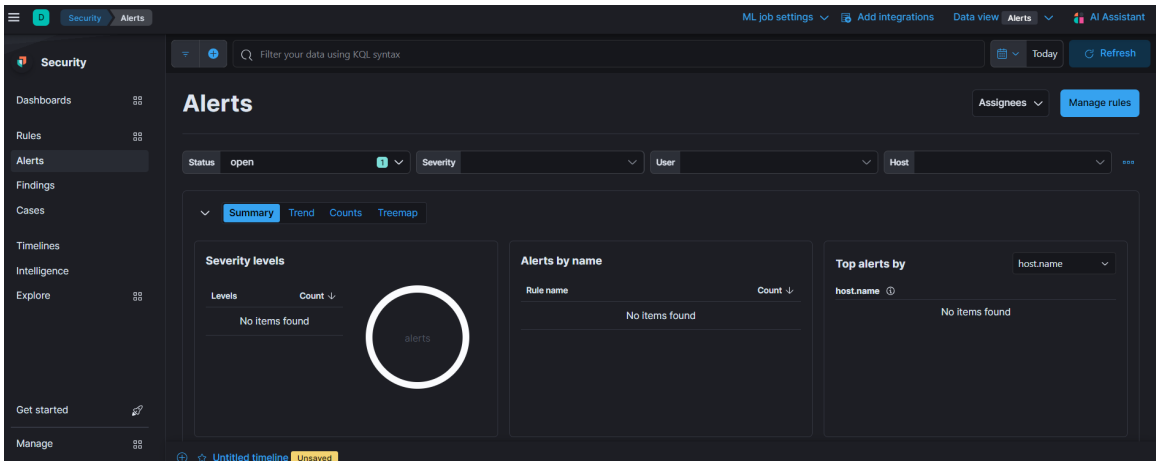
By adhering to these steps, a dashboard capable of visualizing security events over time can be created within the SIEM app, facilitating enhanced analysis and comprehension of logged data.

Task 7: Create an Alert

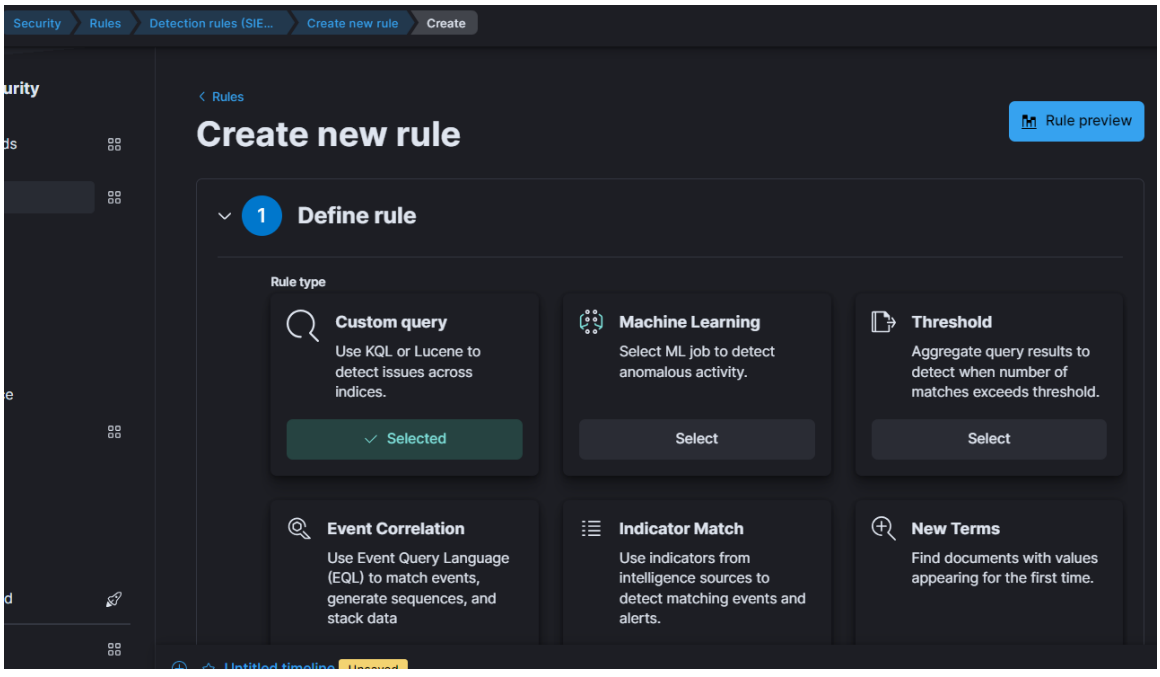
Within a SIEM environment, alerts serve as critical tools for detecting security incidents and responding promptly. These alerts are crafted based on predefined rules or custom queries, capable of triggering specific actions upon meeting specified conditions. In this task, we will outline the steps for creating an alert within the Elastic SIEM instance to detect Nmap scans. By adhering to these steps, an alert can be established to monitor logs for Nmap scan events, thereby facilitating timely notification upon detection.

Follow these steps to create the alert:

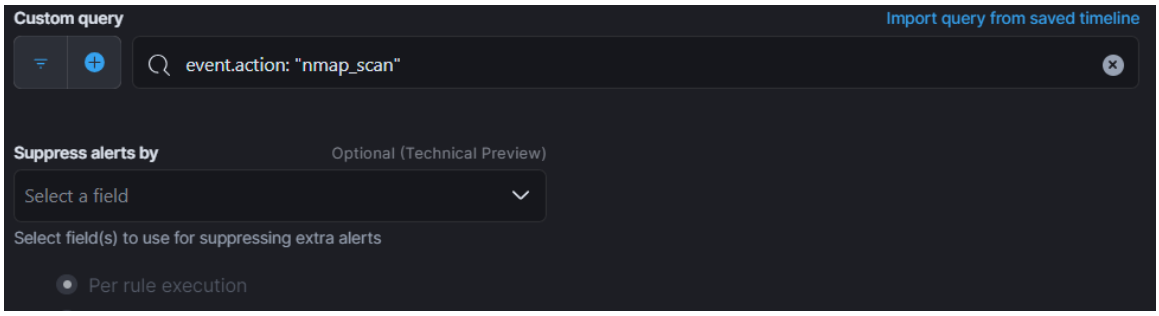
1. **Access Alert Management**: Click on the menu icon located at the top-left corner. Under "Security," select "Alerts."



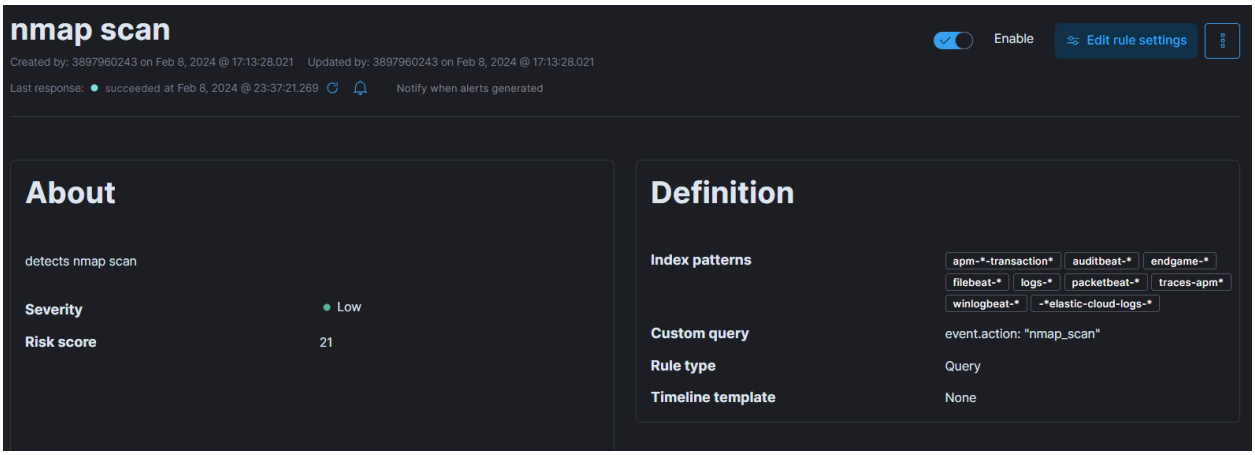
2. **Navigate to Rule Management**: Click on "Manage rules" situated at the top-right corner.



1. **Define Query Conditions**: Craft a query to match all events with the action "nmap_scan." Then proceed by clicking "Continue."



2. **Provide Rule Details**: Under the "About rule" section, furnish your rule with a name and description (e.g., Nmap Scan Detection).
3. **Set Severity Level**: Determine the severity level for the alert, aiding in prioritizing alerts based on their significance. Retain the default settings under "Schedule rule" and proceed by clicking "Continue."
4. **Configure Actions**: In the "Actions" section, designate the action to be executed upon rule triggering. Options include email notification, Slack message creation, or triggering a custom webhook.
5. **Create and Enable Rule**: Finally, click the "Create and enable rule" button to instantiate the alert.



Upon successful creation, the alert will actively monitor logs for Nmap scan events. Upon detection of such an event, the alert will be triggered, prompting the execution of the selected action. Alert management and oversight can be performed within the "Alerts" section under "Security."

Conclusion

In conclusion, this lab provided a comprehensive hands-on experience in setting up and utilizing the Elastic SIEM for security monitoring purposes. Through a series of sequential tasks, including the establishment of an Elastic account, installation and configuration of necessary components such as the Elastic Agent on the Kali VM, and the creation of alerts and dashboards within the SIEM interface, participants gained valuable insights into the process of security event detection, analysis, and response.

By leveraging tools like Nmap for event generation and exploring the functionalities of Elastic SIEM for log querying, visualization, and alert creation, participants were equipped with practical skills essential for effective security monitoring and incident response.