Home-built SIEM System

Objective

To set up a home lab for Security Information and Event Management (SIEM) using Elastic Stack and Kali Linux, enabling skills development in security analytics and threat investigation.

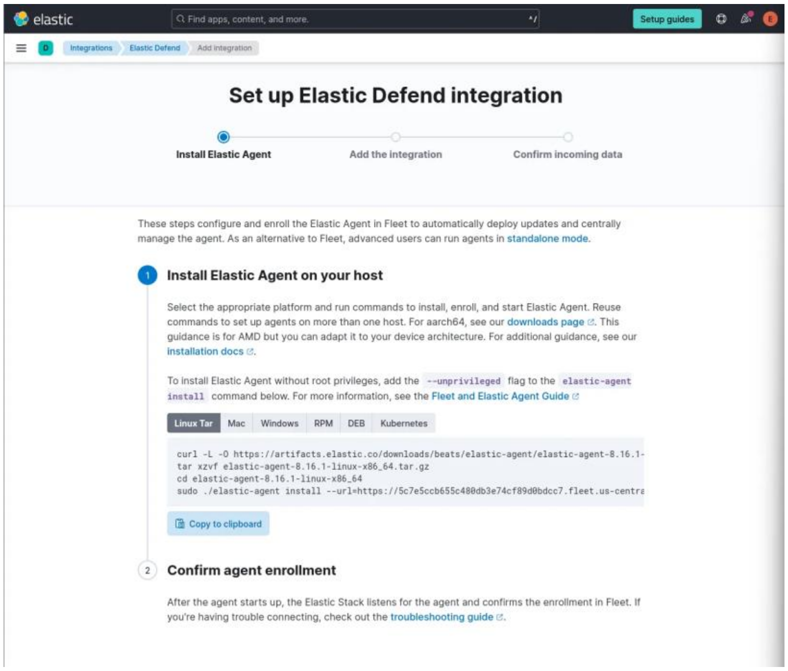
Tools and Technologies

- **Operating System:** Kali Linux (Virtual Machine)
- **SIEM Platform:** Elastic Stack (Elasticsearch, Logstash, Kibana)
- **Other Tools:** Nmap

Implementation Steps

1. Setting Up the Home Lab

- Configured Kali Linux VM as the primary system for generating and monitoring security events.
- Installed Elastic Stack on a separate virtual machine to manage log aggregation and analytics.



Set up Elastic Defend integration

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. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the Fleet and Elastic Agent Guide

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.16.1-
tar xzvf elastic-agent-8.16.1-linux-x86_64.tar.gz
cd elastic-agent-8.16.1-linux-x86_64
sudo ./elastic-agent install --url=https://5c7e5ccb655c480db3e74cf89d0bdcc7.fleet.us-centra
```

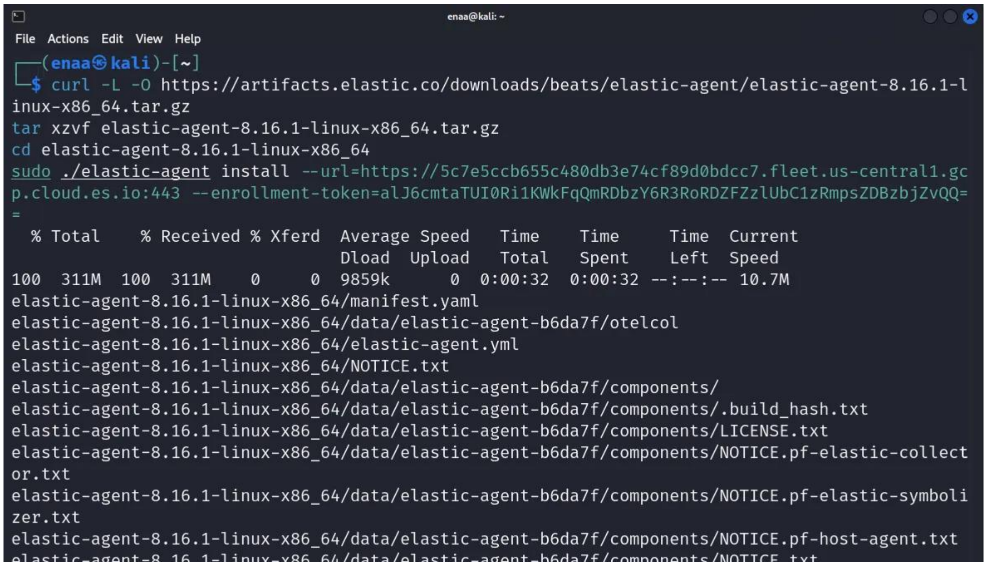
2 Confirm agent enrollment

After the agent starts up, the Elastic Stack listens for the agent and confirms the enrollment in Fleet. If you're having trouble connecting, check out the troubleshooting guide.

Figure 1: Setting up Elastic Agent

2. SIEM Integration

- Installed and configured an Elastic Agent on Kali Linux for log collection and event forwarding.
- Ensured seamless data transfer between Elastic Agent and Elasticsearch for indexing and analysis.

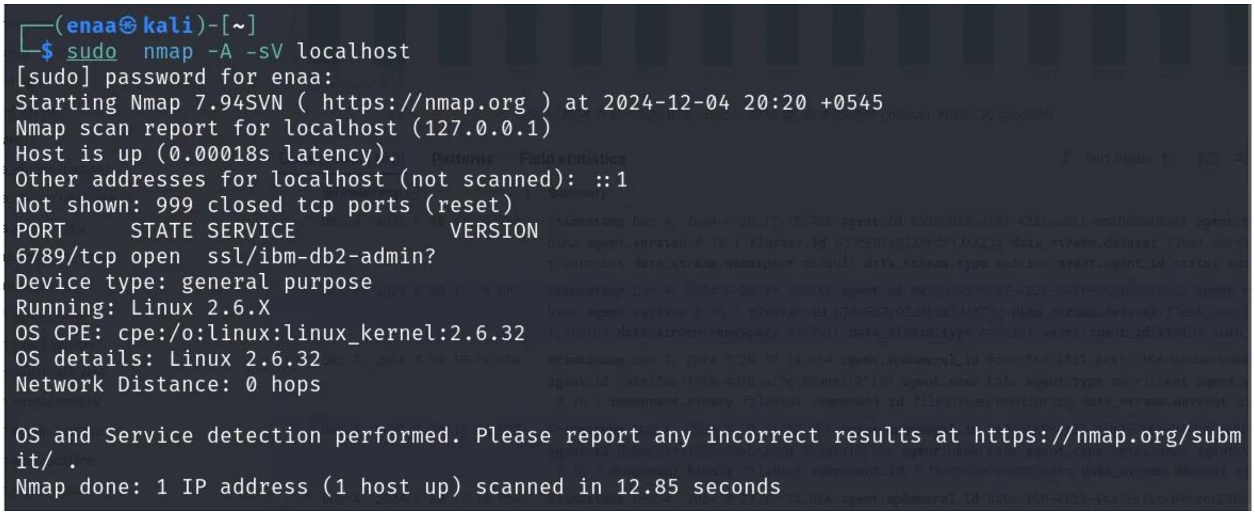


```
┌──(enaa㉿kali)-[~]
└─$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.16.1-l
inux-x86_64.tar.gz
tar xzvf elastic-agent-8.16.1-linux-x86_64.tar.gz
cd elastic-agent-8.16.1-linux-x86_64
sudo ./elastic-agent install --url=https://5c7e5ccb655c480db3e74cf89d0bdcc7.fleet.us-central1.gc
p.cloud.es.io:443 --enrollment-token=alJ6cmtaTUI0Ri1KWkFqQmRDbzY6R3RoRDZFZzlUbC1zRmpsZDBzbjZvQQ=
=
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  311M  100  311M    0     0  9859k      0  0:00:32  0:00:32 --:--:-- 10.7M
elastic-agent-8.16.1-linux-x86_64/manifest.yaml
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/otelcol
elastic-agent-8.16.1-linux-x86_64/elastic-agent.yml
elastic-agent-8.16.1-linux-x86_64/NOTICE.txt
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/.build_hash.txt
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/LICENSE.txt
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/NOTICE.pf-elastic-collect
or.txt
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/NOTICE.pf-elastic-symboli
zer.txt
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/NOTICE.pf-host-agent.txt
elastic-agent-8.16.1-linux-x86_64/data/elastic-agent-b6da7f/components/NOTICE.txt
```

Figure 2: Installing Elastic Agent on Kalil

3. Security Event Demonstration

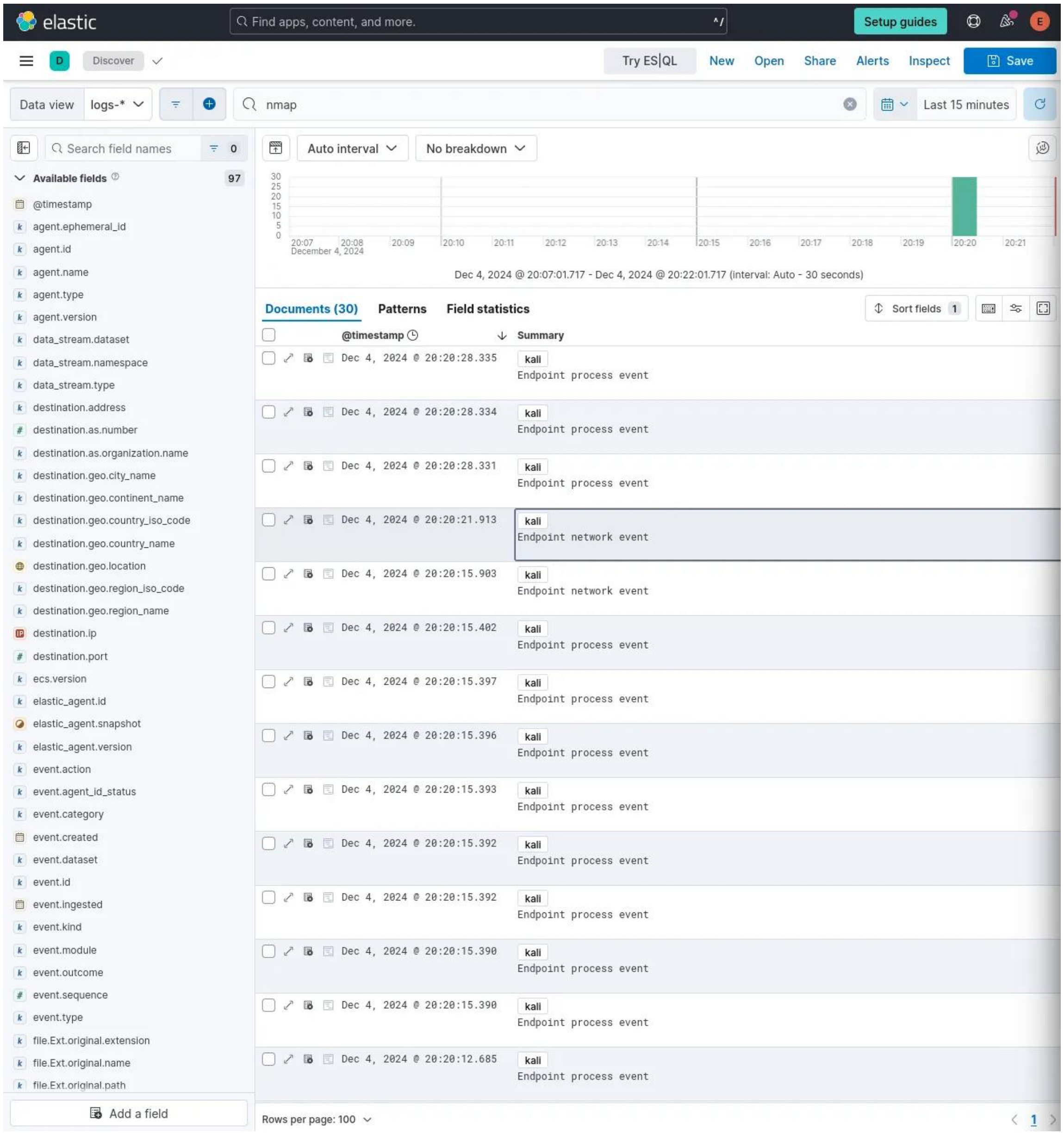
- Generated a security event using an Nmap scan targeting the Kali VM.
- Verified that the logs for the scan were captured and indexed by Elasticsearch.



```
┌──(enaa㉿kali)-[~]
└─$ sudo nmap -A -sV localhost
[sudo] password for enaa:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 20:20 +0545
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE            VERSION
6789/tcp open  ssl/ibm-db2-admin?
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 12.85 seconds
```

Figure 3: NMAP Scan



nmap

Dec 4, 2024 @ 20:07:01.717 - Dec 4, 2024 @ 20:22:01.717 (interval: Auto - 30 seconds)

@timestamp	Summary
Dec 4, 2024 @ 20:20:28.335	kali Endpoint process event
Dec 4, 2024 @ 20:20:28.334	kali Endpoint process event
Dec 4, 2024 @ 20:20:28.331	kali Endpoint process event
Dec 4, 2024 @ 20:20:21.913	kali Endpoint network event
Dec 4, 2024 @ 20:20:15.903	kali Endpoint network event
Dec 4, 2024 @ 20:20:15.402	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.397	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.396	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.393	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.392	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.392	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.390	kali Endpoint process event
Dec 4, 2024 @ 20:20:15.390	kali Endpoint process event
Dec 4, 2024 @ 20:20:12.685	kali Endpoint process event

Figure 4: NMAP Logs in Elastic

4. Custom Dashboard Creation

- Designed a Kibana dashboard to visualize logs and security events over time.
- Included key metrics such as event timestamps, sources, and event types.

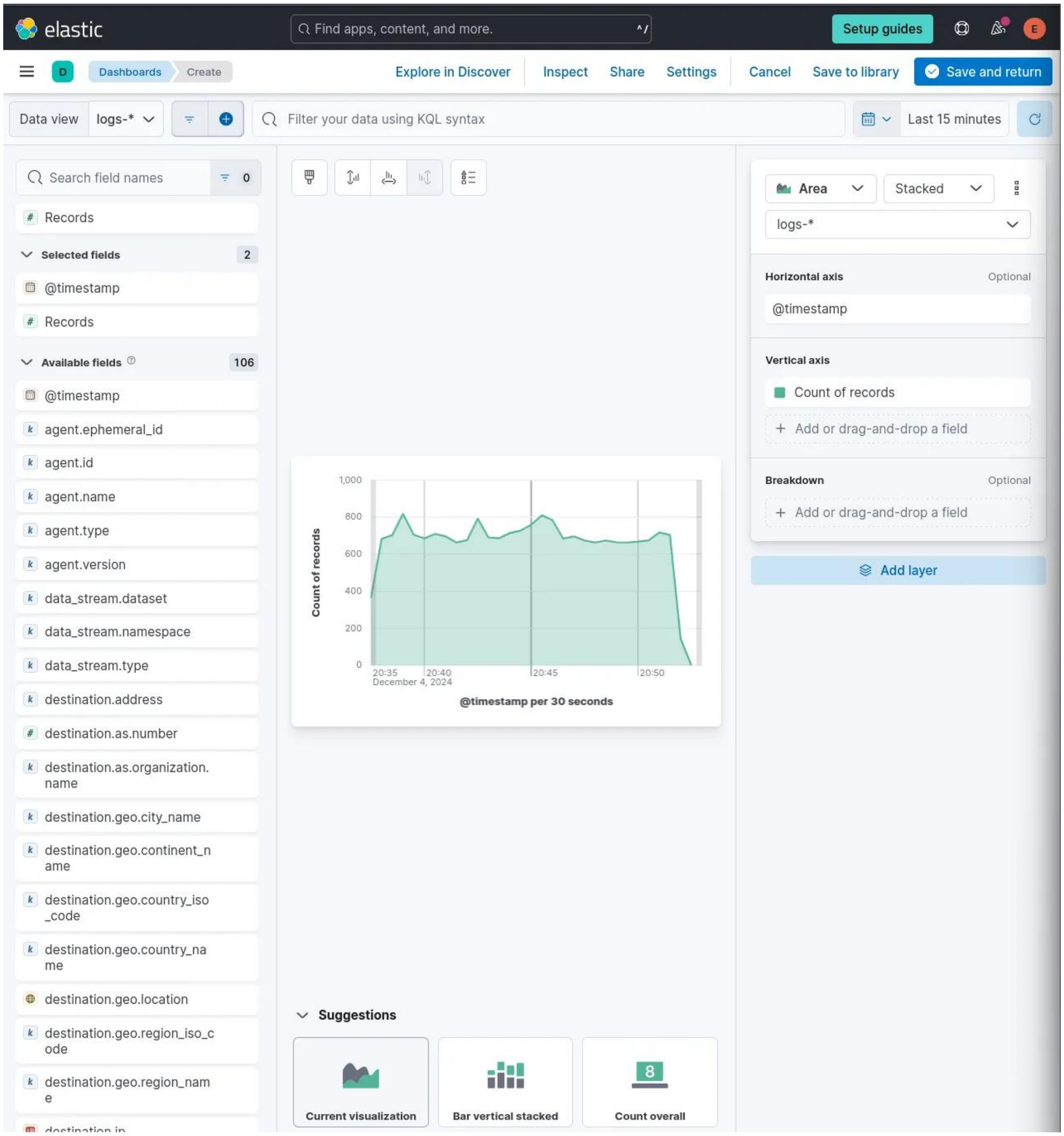
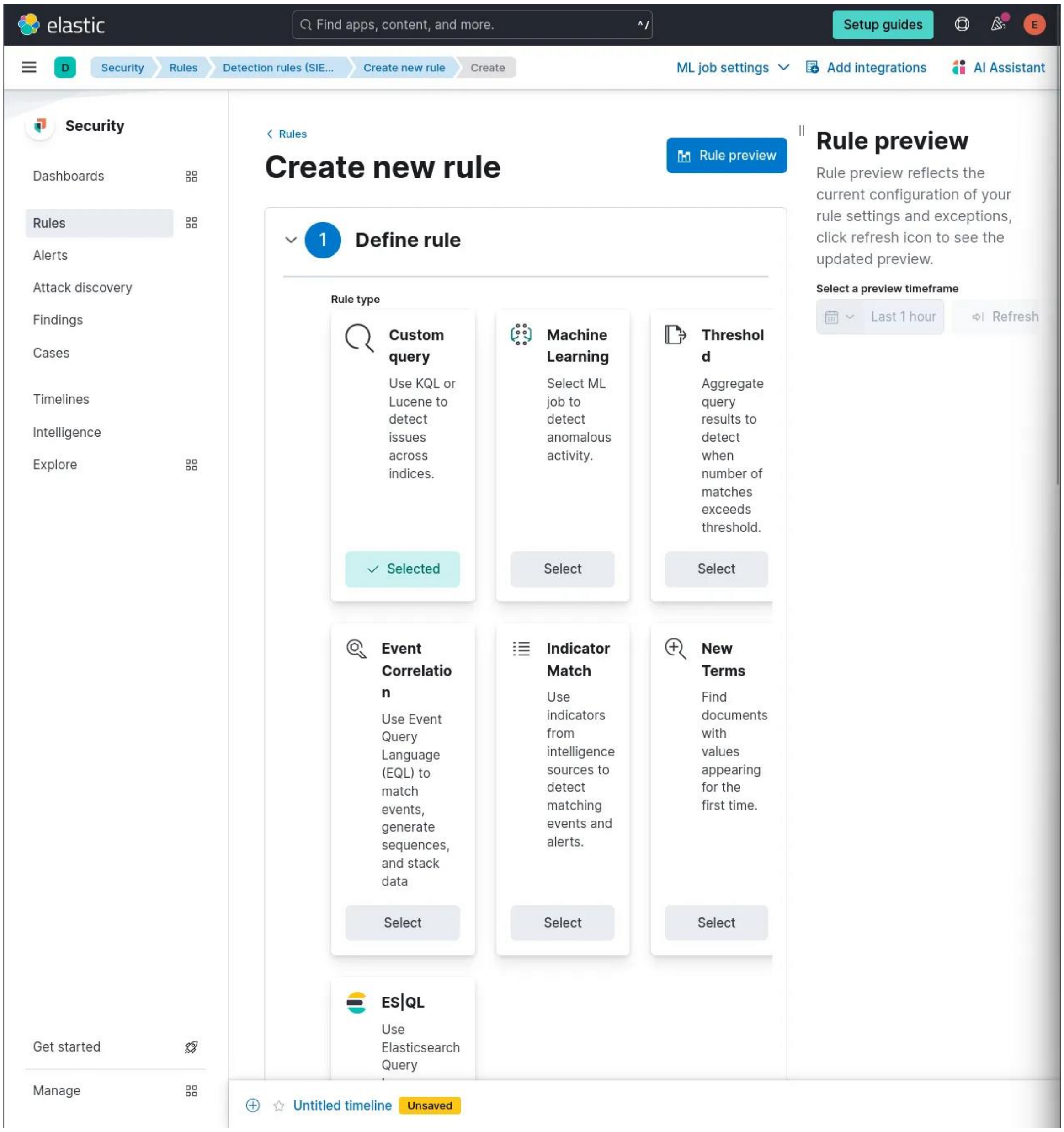


Figure 5: Create Dashboard

5. Custom Security Alert

- Created a security alert in Elastic SIEM to detect Nmap scanning activities.
- Configured the alert to trigger based on specific log patterns associated with Nmap scans.



Create new rule

1 Define rule

Custom query: Use KQL or Lucene to detect issues across indices.

Machine Learning: Select ML job to detect anomalous activity.

Threshold: Aggregate query results to detect when number of matches exceeds threshold.

Event Correlation: Use Event Query Language (EQL) to match events, generate sequences, and stack data

Indicator Match: Use indicators from intelligence sources to detect matching events and alerts.

New Terms: Find documents with values appearing for the first time.

ES|QL: Use Elasticsearch Query

Rule preview

Rule preview reflects the current configuration of your rule settings and exceptions, click refresh icon to see the updated preview.

Select a preview timeframe

Figure 6: Create Custom Rules for Alert

Key Features

- Real-time detection of network scanning activities.
- Comprehensive log analysis through a custom dashboard.
- Proactive alerting for potential threats using automated email notifications.

Results and Outcomes

- Successfully implemented a functional SIEM system in a home lab environment.
- Detected and analyzed security events, including Nmap scans, with actionable insights.
- Gained hands-on experience in security analytics and investigation.