How I built a powerful home SIEM tool with Elastic

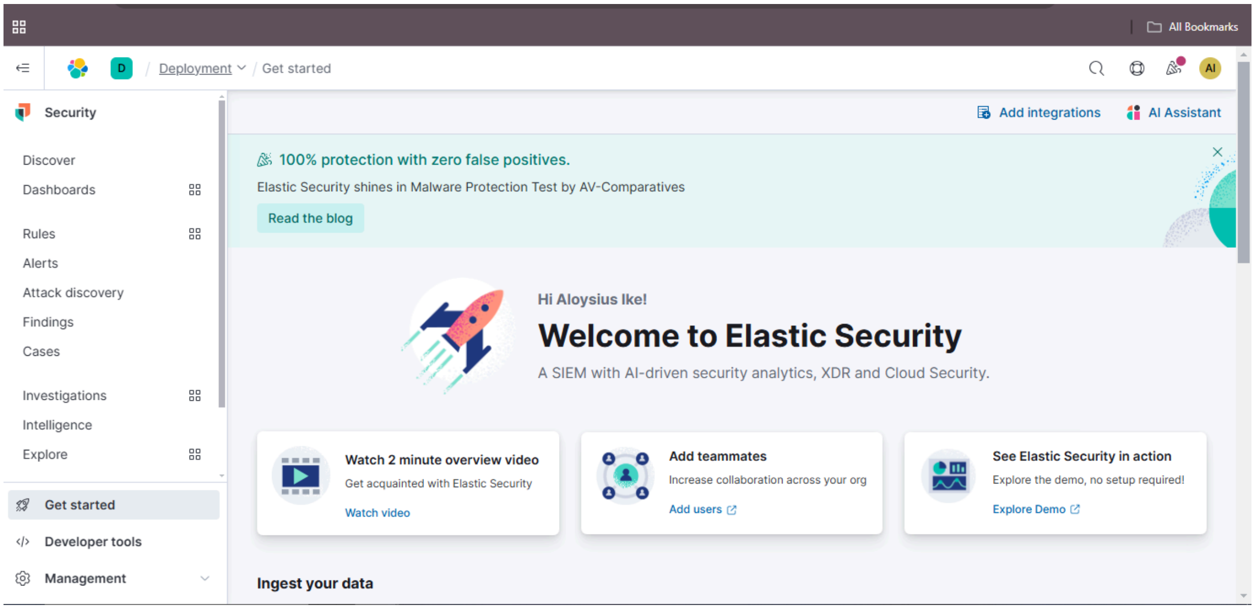
Overview

This report covers the process of setting up a home SIEM lab using Elastic, giving me hands-on experience with tools and workflows essential for a SOC analyst. The goal was to create a realistic lab environment where I could collect, analyze, and interact with telemetry data through a SIEM platform, simulating scenarios a SOC analyst might encounter in the field. Elastic was my tool of choice because it's flexible, user-friendly, and offers powerful analytics.

I set up the lab by installing Elastic Agent on a Kali Linux machine to serve as the main source of telemetry. This setup enabled me to track security events and simulate adversarial activity, like running a network scan using Nmap. Along the way, I verified that the Elastic Agent was successfully capturing data, built a dashboard to make the telemetry easier to visualize, and configured alerts to detect and respond to suspicious behavior.

Building this lab wasn't just about getting the technical setup right; it was also a practical exercise in learning blue team skills. It gave me hands-on experience with monitoring, threat detection, and incident response—the core responsibilities of a SOC analyst. This project was a big step toward understanding how to work effectively with SIEM tools and handle security events in a real-world setting.

1.0 Creation of Elastic Account and Configuration of Elastic Agent on Kali Linux



100% protection with zero false positives.

Elastic Security shines in Malware Protection Test by AV-Comparatives

Hi Aloysius Ike!

Welcome to Elastic Security

A SIEM with AI-driven security analytics, XDR and Cloud Security.

Watch 2 minute overview video

Get acquainted with Elastic Security

Add teammates

Increase collaboration across your org

See Elastic Security in action

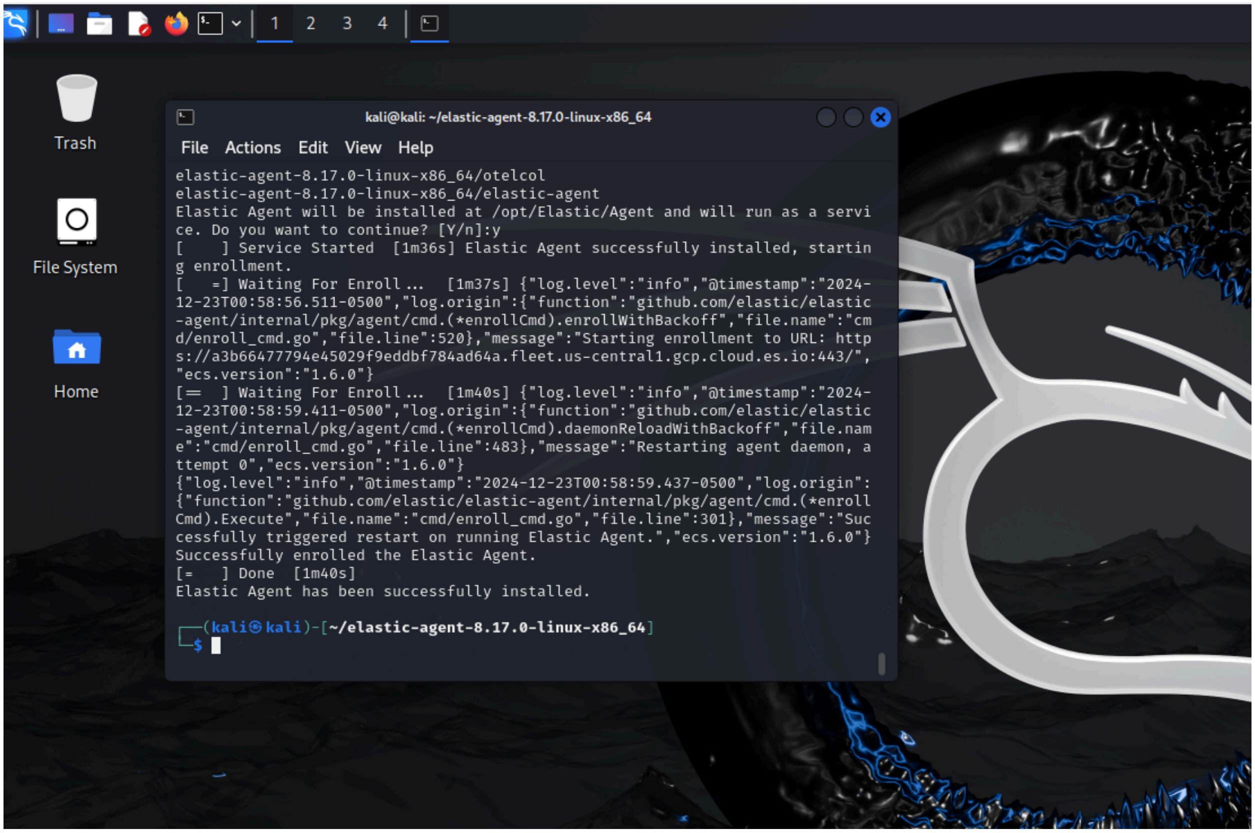
Explore the demo, no setup required!

Ingest your data

Fig 1. Successful account creation on Elastic Security

Started by creating a free account to set up a cloud Elastic instance on which the SIEM will run. After creating the Elastic account, I created a Deployment and its configuration. Once the deployment was ready, I proceeded to configure Kali Linux VM.

2.0 Collection of Logs

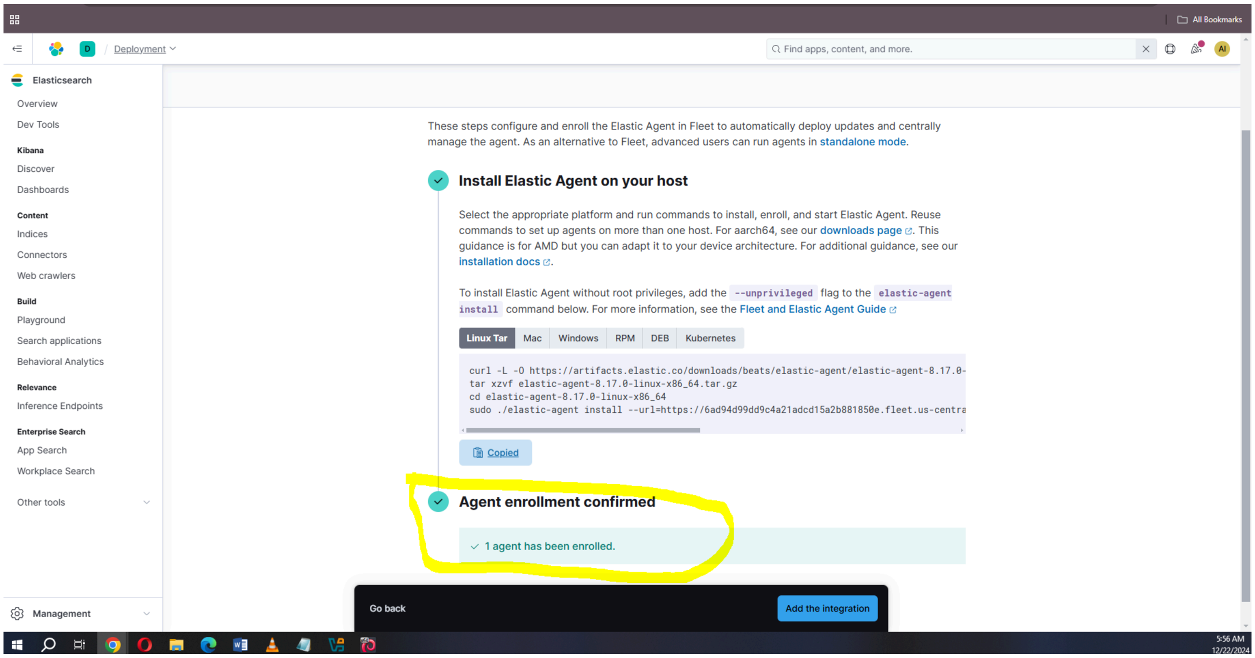


```
elastic-agent-8.17.0-linux-x86_64/otelcol
elastic-agent-8.17.0-linux-x86_64/elastic-agent
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a servi
ce. Do you want to continue? [Y/n]:y
[    ] Service Started  [1m36s] Elastic Agent successfully installed, startin
g enrollment.
[   =] Waiting For Enroll ...  [1m37s] {"log.level":"info","@timestamp":"2024-
12-23T00:58:56.511-0500","log.origin":{"function":"github.com/elastic/elastic
-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cm
d/enroll_cmd.go","file.line":520},"message":"Starting enrollment to URL: http
s://a3b66477794e45029f9eddbf784ad64a.fleet.us-central1.gcp.cloud.es.io:443/",
"ecs.version":"1.6.0"}
[==  ] Waiting For Enroll ...  [1m40s] {"log.level":"info","@timestamp":"2024-
12-23T00:58:59.411-0500","log.origin":{"function":"github.com/elastic/elastic
-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.nam
e":"cmd/enroll_cmd.go","file.line":483},"message":"Restarting agent daemon, a
ttempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-12-23T00:58:59.437-0500","log.origin":
{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enroll
Cmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":301},"message":"Suc
cessfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=   ] Done  [1m40s]
Elastic Agent has been successfully installed.

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ 
```

Fig 2. Installation of Elastic Agent to Kali Linux

Kali Linux is used as an endpoint or a server where the SIEM collects and sanes data to a centralised system from, for analysis and monitoring. An agent is also required to be installed on the endpoint or server to enable telemetry of security-related incidents from the endpoints to Elastic SIEM.

I configured my agent to collect logs from my Kali Linux VM and forward them to Elastic SIEM instance.



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.

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

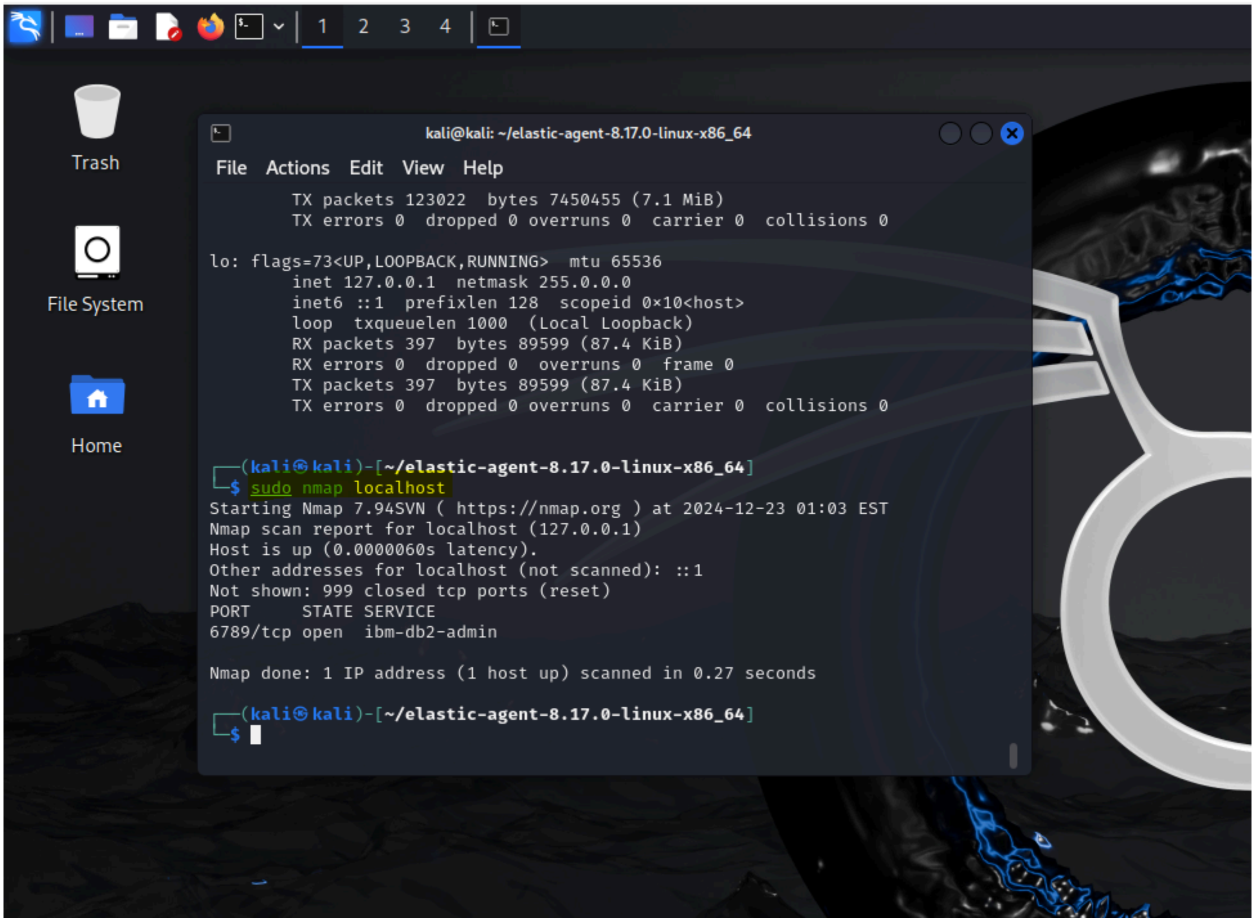
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://6ad94d99dd9c4a21adcd15a2b881850e.fleet.us-centra
```

Agent enrollment confirmed

✓ 1 agent has been enrolled.

Fig 3. Confirmation of the Agent successfully installed and communicating with the endpoint.

3.0 Queried for Nmap events

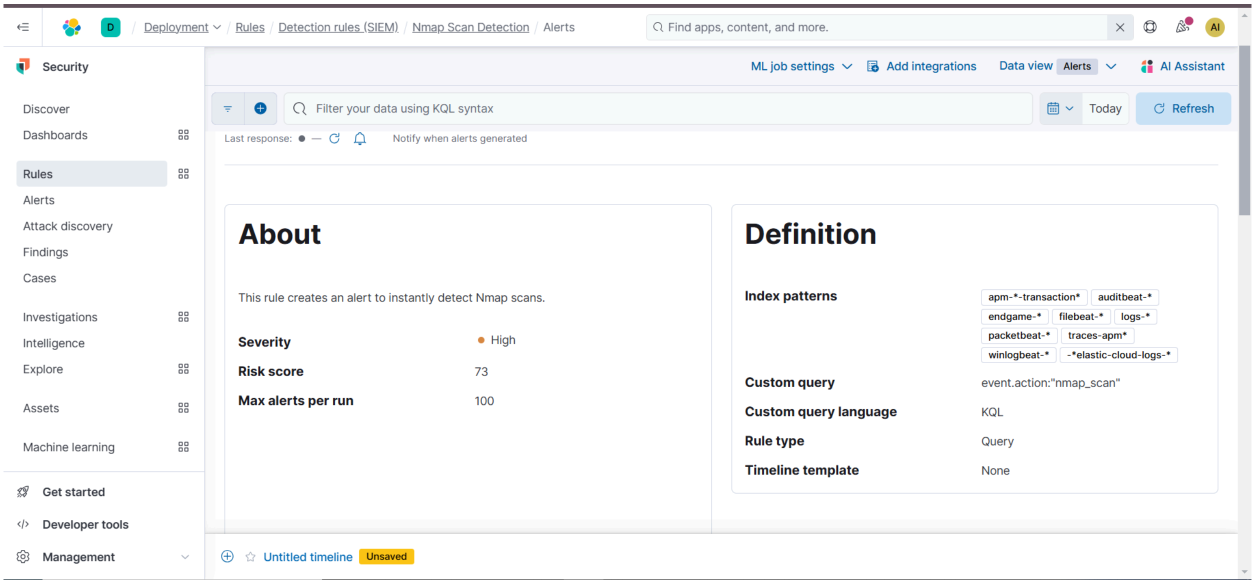


```
        TX packets 123022  bytes 7450455 (7.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 397  bytes 89599 (87.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 397  bytes 89599 (87.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ sudo nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-23 01:03 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s 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 0.27 seconds

┌──(kali㉿kali)-[~/elastic-agent-8.17.0-linux-x86_64]
└─$ 
```

Fig 4. Ran an Nmap scan to generate traffic on the network

To generate traffic to the SIEM tool and create a simulation of a potential network scanning activity, I ran Nmap on the endpoint to generate network traffic.

5.0 Alert Configuration and Creation



About

This rule creates an alert to instantly detect Nmap scans.

Severity ● High
Risk score 73
Max alerts per run 100

Definition

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

Fig 5. Configuration of alerts to be triggered once an Nmap scan is initiated

Configured an alert to trigger when an Nmap scan is detected which also sends email notification to alert about the potential scanning activity.

Once I've created the alert, it will monitor logs for Nmap scan events. If an Nmap scan event is detected, the alert will be triggered and the selected action will be taken. I can view and manage the alerts on the "Alerts" section under "Security."

6.0 Conclusion

Building a home SIEM lab with Elastic was a highly rewarding experience that provided practical, hands-on exposure to the tools and techniques used by SOC analysts. The process involved setting up Elastic Agent on a Kali Linux host, configuring data collection, visualizing telemetry through custom dashboards, and simulating adversarial activity to test detection and alerting capabilities.

This lab not only deepened my understanding of SIEM platforms but also honed my ability to monitor, analyze, and respond to security events—key skills for any blue team professional. I gained valuable insights into the workflows and challenges of security operations, by working through real-world scenarios, such as detecting network scans with Nmap.

Overall, this project solidified my foundational knowledge of Elastic as a SIEM tool and enhanced my readiness to contribute to SOC operations. It underscored the importance of continuous learning and experimentation in building a strong skill set in cybersecurity.

Lastly, i'd like to refer to Abdulahi Ali, for providing a detailed guide and Gerald Auger for his YouTube video on this.