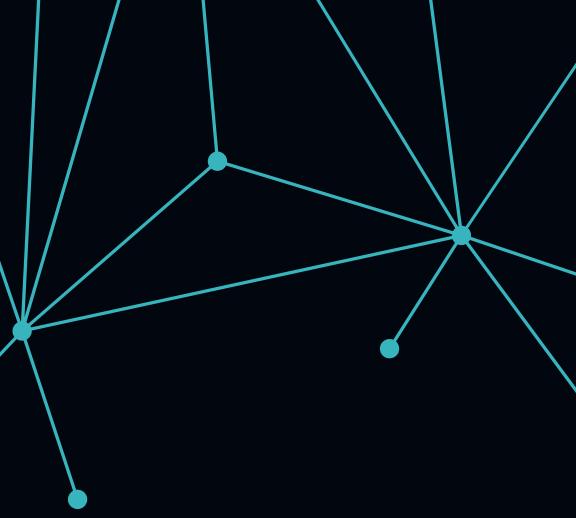


SIEM HOMELAB WITH ELASTIC CLOUD



Threat detection, Alerting and Log Monitoring

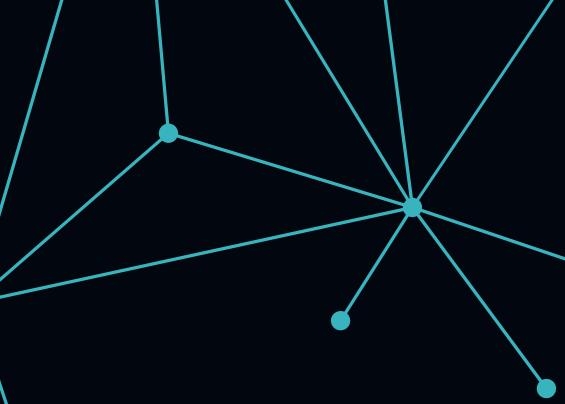
Prepared by Babajide Aina



THIS IS A GUIDE ON HOW I SET UP MY VERY OWN HOME LAB FOR ELASTIC STACK SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM). IN THIS PROJECT, I'LL TAKE YOU THROUGH THE STEPS ON HOW I CREATED MY SIEM ENVIRONMENT USING THE ELASTIC WEB PORTAL AND A KALI LINUX VM.

Threat detection, Alerting and Log Monitoring



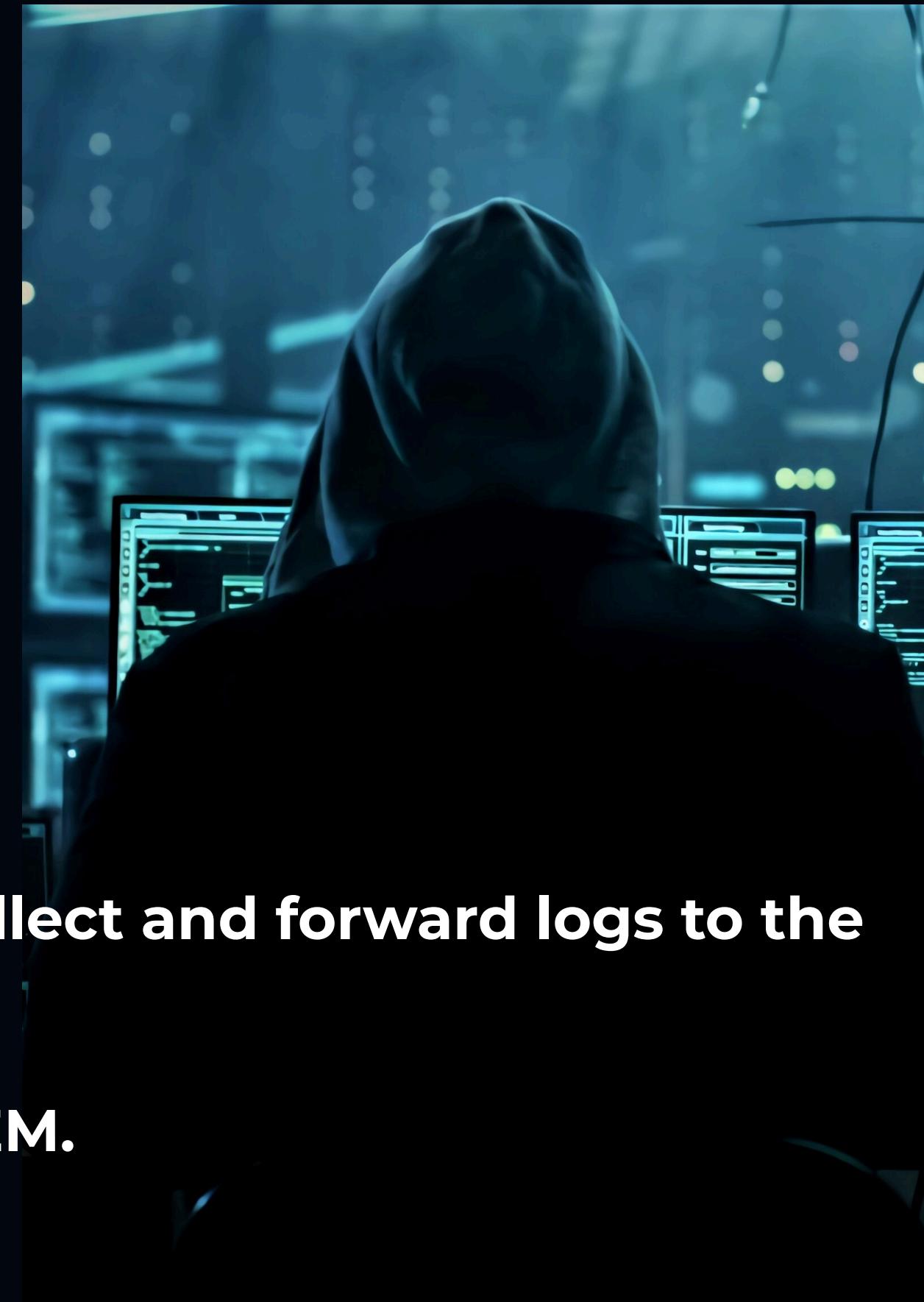


• Prerequisites:

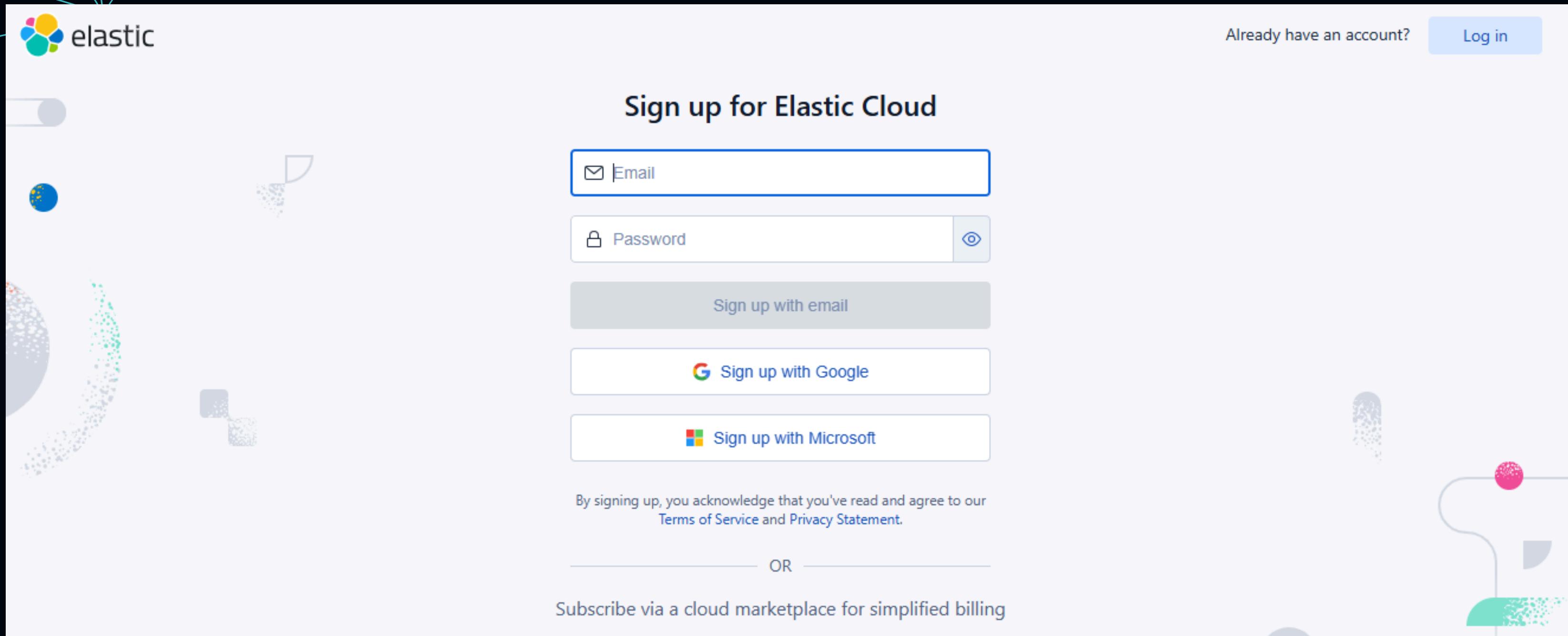
- **Virtualization software like VirtualBox or VMware.**
- **Basic familiarity with Linux and virtualization concepts**

Overview:

- **Setting up a free Elastic account.**
- **Provisioning the Kali VM.**
- **Configuring the Elastic Agent on the Kali Linux VM to collect and forward logs to the SIEM.**
- **Generating security events on the Kali VM.**
- **Querying and analyzing security events in the Elastic SIEM.**
- **Creating a dashboard to visualize security events.**
- **Setting up alerts for security events.**



Task 1



I Signed up for a free trial of Elastic Cloud by visiting <https://cloud.elastic.co/registration>. After registering, I logged into the Elastic Cloud console at <https://cloud.elastic.co>.

Task 1

The screenshot shows the Elastic Cloud interface. At the top left, there's a 'Cloud' tab. Below it, the main heading is 'Welcome to Elastic Cloud'. On the left, there's a section titled 'Hosted deployments' with a 'Create hosted deployment' button. It includes a circular icon with three icons (gear, padlock, magnifying glass) and a message stating 'You have no hosted deployments yet'. Below this, there's a 'Serverless projects' section with a 'Create serverless project' button. It lists one project: 'My Security project' (Type: Security, Cloud provider & region: GCP - US Central 1 (Iowa), Actions: Open, Manage). To the right, there's a 'News' section with several greyed-out news items and a 'Community' section with links to 'Join an ElasticON event' and 'Hear success stories, lessons learned, and tips from the Elastic community'.

I Clicked on "Start your free trial" to kick off the process. Next, hit the "Create Deployment" button and opt for "Elasticsearch" as my deployment type. I Selected a region , created a deployment and patiently waited for the configuration to finalize. Once the deployment was ready, I clicked on "continue" to proceed

Task 2

Setting up my Kali Linux VM

At this stage, I set up my kali and set up the agent to collect logs

```
(kali㉿kali)-[~]
$ curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-9.1.2-linux-x86_64.tar.gz
```

% Total	Time	Speed	Time	Time	Current	Google Hacking DB	OffSec
	Dload	Upload	Total	Spent	Left		
100	443M	100	443M	0	0	3527k	0:02:08 0:02:08 --:--:-- 1633k

```
(kali㉿kali)-[~]
$ tar xzvf elastic-agent-9.1.2-linux-x86_64.tar.gz
```

```
elastic-agent-9.1.2-linux-x86_64/data/elastic-agent-45007d/package.version-DB
elastic-agent-9.1.2-linux-x86_64/.elastic-agent.active.commit
elastic-agent-9.1.2-linux-x86_64/otel_samples/
elastic-agent-9.1.2-linux-x86_64/otel_samples/autoops_es.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/gateway.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/logs_metrics_traces.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/managed_otlp/
elastic-agent-9.1.2-linux-x86_64/otel_samples/managed_otlp/logs_metrics_traces.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/managed_otlp/platformlogs.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/managed_otlp/platformlogs_hostmetrics.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/platformlogs.yml
elastic-agent-9.1.2-linux-x86_64/otel_samples/platformlogs_hostmetrics.yml
elastic-agent-9.1.2-linux-x86_64/otelcol
elastic-agent-9.1.2-linux-x86_64/manifest.yaml
elastic-agent-9.1.2-linux-x86_64/README.md
elastic-agent-9.1.2-linux-x86_64/elastic-agent.reference.yml
elastic-agent-9.1.2-linux-x86_64/data/elastic-agent-45007d/otelcol
elastic-agent-9.1.2-linux-x86_64/data/elastic-agent-45007d/components/
elastic-agent-9.1.2-linux-x86_64/data/elastic-agent-45007d/components/.build_hash.txt
elastic-agent-9.1.2-linux-x86_64/data/elastic-agent-45007d/components/LICENSE +vt
```

Task 2

Setting up my Kali Linux VM

```
(kali㉿kali)-[~/elastic-agent-9.1.2-linux-x86_64]
$ sudo ./elastic-agent install --url=https://3e2e92beff2e4df5a94ad552a6d75228.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=cVhMUnpaZ0JXN2x2SnJSX1Z10Ws6Wmh4dmpLWUDyOTZ0dmJhRXNwbHQxUQ==
[sudo] password for kali:
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:y
[ == ] Service Started [20s] Elastic Agent successfully installed, starting enrollment.
[ == ] Waiting For Enroll ... [22s] {"log.level":"info","@timestamp":"2025-08-23T00:27:58.233-0400","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":536},"message":"Starting enrollment to URL: https://3e2e92beff2e4df5a94ad552a6d75228.fleet.us-central1.gcp.cloud.es.io:443/","ecs.version":"1.6.0"}
[ == ] Waiting For Enroll ... [28s] {"log.level":"info","@timestamp":"2025-08-23T00:28:04.391-0400","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":499},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-23T00:28:04.397-0400","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":317},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[ == ] Done [29s] bwsse... facebook flashscore downloads 127.0.0.1 student.lea... mail.google download
Elastic Agent has been successfully installed.
```

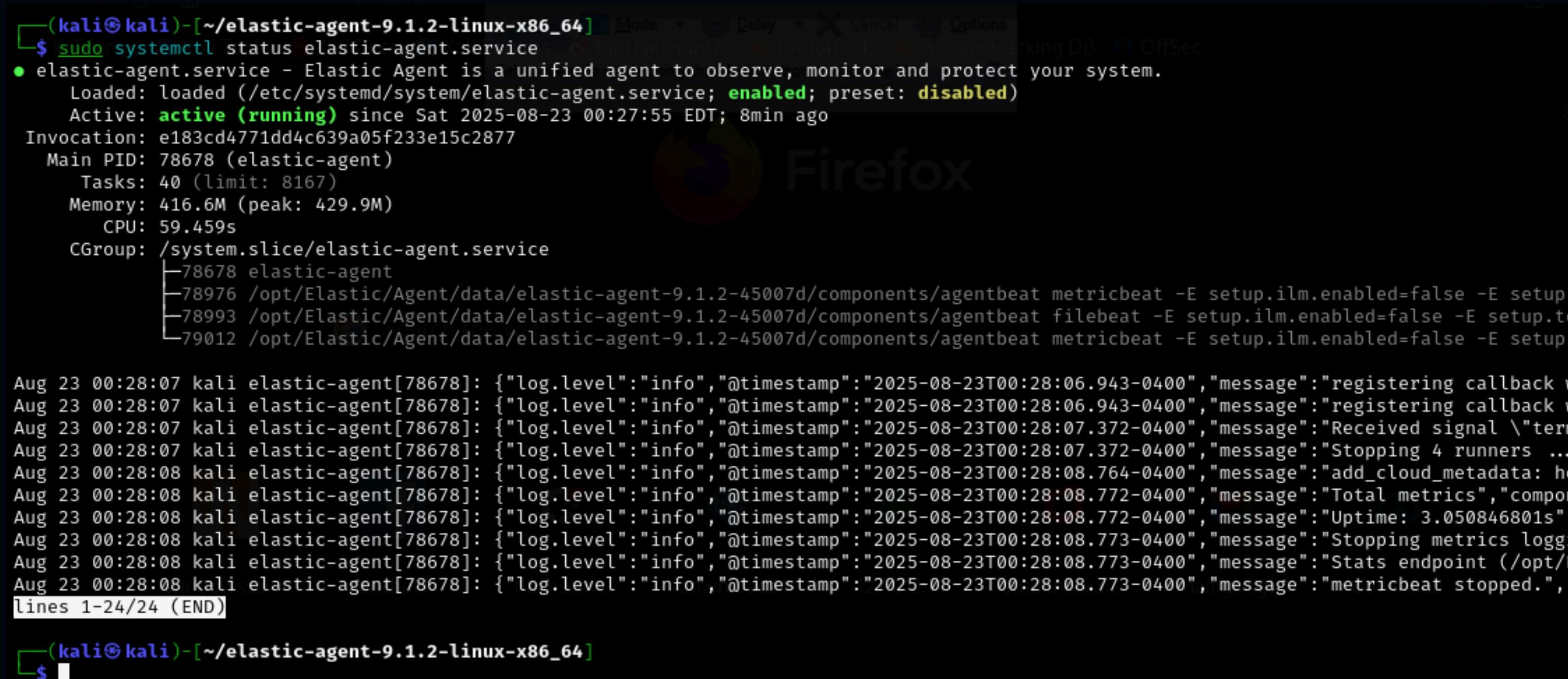
Once the installation process was completed, which took a few minutes, I received a confirmation message stating "Elastic Agent has been successfully installed." The agent will automatically start collecting and forwarding logs to my Elastic SIEM instance. However, it might take a few minutes for the logs to appear in the SIEM.

To verify that the agent was installed correctly, I ran the following command in my Kali terminal: `sudo systemctl status elastic-agent.service`

Task 2

Setting up my Kali Linux VM

To verify that the agent was installed correctly, I ran the following command in my Kali terminal: `sudo systemctl status elastic-agent.service`



```
(kali㉿kali)-[~/elastic-agent-9.1.2-linux-x86_64] $ sudo systemctl status elastic-agent.service
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
  Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
  Active: active (running) since Sat 2025-08-23 00:27:55 EDT; 8min ago
    Invocation: e183cd4771dd4c639a05f233e15c2877
      Main PID: 78678 (elastic-agent)
        Tasks: 40 (limit: 8167)
       Memory: 416.6M (peak: 429.9M)
         CPU: 59.459s
      CGroup: /system.slice/elastic-agent.service
              └─78678 elastic-agent
                  ├─78976 /opt/Elastic/Agent/data/elastic-agent-9.1.2-45007d/components/agentbeat metricbeat -E setupilm.enabled=false -E setup...
                  ├─78993 /opt/Elastic/Agent/data/elastic-agent-9.1.2-45007d/components/agentbeat filebeat -E setupilm.enabled=false -E setup...
                  ├─79012 /opt/Elastic/Agent/data/elastic-agent-9.1.2-45007d/components/agentbeat metricbeat -E setupilm.enabled=false -E setup...

Aug 23 00:28:07 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:06.943-0400", "message": "registering callback w
Aug 23 00:28:07 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:06.943-0400", "message": "registering callback w
Aug 23 00:28:07 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:07.372-0400", "message": "Received signal \"term
Aug 23 00:28:07 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:07.372-0400", "message": "Stopping 4 runners ...
Aug 23 00:28:08 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:08.764-0400", "message": "add_cloud_metadata: ho
Aug 23 00:28:08 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:08.772-0400", "message": "Total metrics", "compon
Aug 23 00:28:08 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:08.772-0400", "message": "Uptime: 3.050846801s",
Aug 23 00:28:08 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:08.773-0400", "message": "Stopping metrics loggi
Aug 23 00:28:08 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:08.773-0400", "message": "Stats endpoint (/opt/E
Aug 23 00:28:08 kali elastic-agent[78678]: {"log.level": "info", "@timestamp": "2025-08-23T00:28:08.773-0400", "message": "metricbeat stopped.", "
Lines 1-24/24 (END)

(kali㉿kali)-[~/elastic-agent-9.1.2-linux-x86_64] $
```

Task 2

The image consists of three vertically stacked screenshots from a web-based interface for managing cloud assets.

Screenshot 1: A flow diagram showing three steps: 1. Install Elastic Agent (with a sub-option to skip agent installation), 2. Add the integration, and 3. Confirm incoming data. Buttons for "Install Elastic Agent" and "Add integration only (skip agent installation)" are present.

Screenshot 2: A detailed guide for step 1 titled "Install Elastic Agent on your host". It includes instructions for selecting a platform (Linux aarch64 is selected) and running commands. A command line example is shown:

```
curl -L -0 https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-9.1.2-l  
tar xzvf elastic-agent-9.1.2-linux-arm64.tar.gz  
cd elastic-agent-9.1.2-linux-arm64  
sudo ./elastic-agent install --url=https://3e2e92beff2e4df5a94ad552a6d75228.fleet.us-cent
```

A "Copy to clipboard" button is available.

Screenshot 3: A confirmation screen showing "Agent enrollment confirmed" and "1 agent has been enrolled." It includes "Go back" and "Add the integration" buttons.

Task 3

Querying for Security Events in the Elastic SIEM

With data seamlessly forwarded from my Kali VM to the SIEM platform, it was time to dive into querying and analyzing the logs within the SIEM interface. I accessed my Elastic deployment ,created new rules and entered a search query for Nmap scans (searching for open ports, services and live machines on my workstation). I equally created rules for SSH and performed fake SSH logins by simulating authentication failures ,I attempted SSH logins with invalid credentials.

The screenshot shows the 'Create new rule' interface in the Elastic SIEM. On the left, a sidebar menu includes 'Discover', 'Dashboards', 'Rules' (selected), 'Alerts', 'Attack discovery', 'Findings', 'Cases', 'Explore', 'Investigations', 'Intelligence', 'Assets', 'Get started', and 'Developer tools'. The main area is titled 'Create new rule' and shows the first step: 'Define rule'. It has three options: 'Custom query' (selected, indicated by a green checkmark), 'Machine Learning' (with a 'Select' button), and 'Threshold' (with a 'Select' button). To the right, a 'Rule preview' section displays a summary of the current configuration, a preview timeframe ('Last 1 hour'), and a 'Refresh' button. A checkbox for 'Show Elasticsearch requests, ran during rule executions' is also present.

Task 3

Querying for Security Events in the Elastic SIEM

The screenshot shows the Elastic SIEM interface with a sidebar on the left and a main content area on the right.

Left Sidebar:

- Security
- Discover
- Dashboards
- Rules** (selected)
- Alerts
- Attack discovery
- Findings
- Cases
- Explore
- Investigations
- Intelligence
- Assets

Right Content Area:

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

ML job setting

Rule preview

Rule preview ref configuration of and exceptions, see the updated

Select a preview time

Last 1 hour

Show Elasticse during rule exe

Task 3

Querying for Security Events in the Elastic SIEM

The screenshot shows the Elastic SIEM interface with the following details:

- Navigation:** Deployment > Rules > Detection rules (SIEM) > nmap scan detection > Alerts.
- Header:** ML job settings, Add integrations, Data view, Alerts.
- Search Bar:** Filter your data using KQL syntax.
- Today:** Today button.
- Rule Title:** nmap scan detection.
- Created and Updated:** Created by: 3958785926 on Aug 23, 2025 @ 07:37:12.556 | Updated by: 3958785926 on Aug 23, 2025 @ 07:37:12.556.
- Status:** Enable switch is checked.
- Actions:** Edit rule settings, More options menu.
- Last response:** ● — (refresh icon) | Notify when alerts generated.
- About Section:**
 - Description:** Alert detection.
 - Severity:** Low (green dot).
 - Risk score:** 25.
- Definition Section:**
 - Index patterns:** apm-* transaction*, auditbeat*, endgame*, filebeat*, logs*, packetbeat*, traces-apm*, winlogbeat*, -*elastic-cloud-logs*.
 - Custom query:** event.action:"nmap scan"

Task 3

Querying for Security Events in the Elastic SIEM

The screenshot shows the Elastic Cloud interface for managing hosted deployments. The top navigation bar includes 'Cloud', 'Hosted deployments' (selected), and 'Babajide security deployment'. The main title 'Babajide security deployment' is displayed with a 'HEALTHY' status, location 'GCP - Iowa (us-central1)', and deployment ID '3e2e92'. Action buttons for 'Open AutoOps', 'Open Kibana', and 'Actions' are available.

The left sidebar for 'Babajide security deployment' includes options for 'Edit', 'Monitoring' (selected), 'Logs and metrics' (selected), and 'Performance'. A secondary sidebar lists 'Hosted deployments', 'Babajide security deployment' (selected), and other management options like 'Edit', 'Monitoring' (selected), 'Logs and metrics' (selected), 'Performance', 'Elasticsearch', 'Snapshots', and 'API console'. It also includes sections for 'Access and security', 'Network security', 'Trust management', 'Extensions', and 'Organization'.

The central content area is titled 'View last 24 hours standard logs'. It displays a search bar and a table of log entries. The table has columns for 'Timestamp', 'Level', 'Instance / Zone', and 'Message'. The first three log entries are shown:

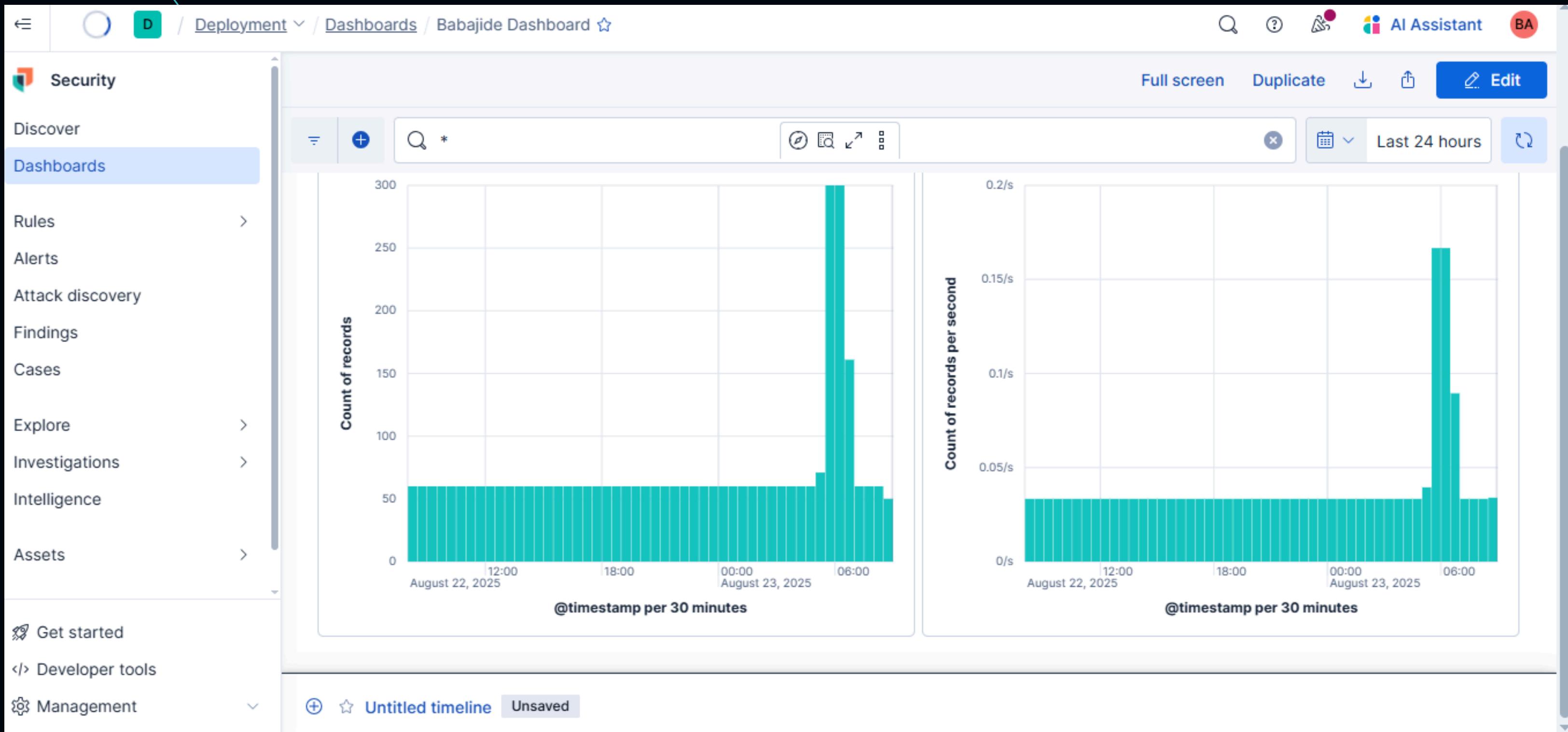
Timestamp	Level	Instance / Zone	Message
Aug 23, 2025, 4:28:34 AM UTC	INFO	i1@us-central1-b	[instance-0000000001] moving index [.ds-logs-elasticsearch-metricbeat-default-2025.08.23-000001] from [null] to [{"phase": "new", "action": "complete", "name": "complete"}] in policy [logs]
Aug 23, 2025, 4:28:34 AM UTC	INFO	i1@us-central1-b	[instance-0000000001] creating index [.ds-logs-elasticsearch-metricbeat-default-2025.08.23-000001] in project [default], cause [initialize_data_stream], templates [provided in request], shards [1]/[1]
Aug 23, 2025, 4:28:34 AM UTC	INFO	i1@us-central1-b	[instance-0000000001] adding data stream [logs-elasticsearch-metricbeat-default] with write index [.ds-logs-elasticsearch-metricbeat-default-2025.08.23-000001], backing indices [], and aliases []

A footer banner at the bottom reads 'Threat detection, Alerting and Log Monitoring'.

Prepared by Babajide Aina

Task 4

I Created a Dashboard to visualize the events



Task 4

Created a Dashboard to visualize the events

```
$ ssh Babajide@localhost
Babajide@localhost's password:
Permission denied, please try again.
Babajide@localhost's password:
Permission denied, please try again.
Babajide@localhost's password:facebook
Babajide@localhost's password:mail.google
Babajide@localhost: Permission denied (publickey,password).
```

The screenshot shows a security monitoring interface with a left sidebar and a main alert list.

Left Sidebar:

- Security
- Discover
- Dashboards
- Rules
- Alerts** (selected)
- Attack discovery
- Findings
- Cases
- Explore
- Investigations
- Intelligence
- Assets

Main Area:

Deployment / Alerts

ML job settings Add integrations Data view Alerts

Last 24 hours

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
SSH Alert	Aug 23, 2025 @ 08:59:22.912	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:59:22.911	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:58:22.924	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:58:22.922	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:57:22.891	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:57:22.890	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:56:22.938	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:56:22.937	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:55:22.931	SSH Alert		high	73	event cre...
SSH Alert	Aug 23, 2025 @ 08:55:22.928	SSH Alert		high	73	event cre...
CCU Alert	Aug 23, 2025 @ 08:54:22.919	CCU Alert		high	73	event cre...

Task 4

Created a Dashboard to visualize the events

```
└─$ ssh Babajide@localhost
Babajide@localhost's password:
Permission denied, please try again.
Babajide@localhost's password:
Permission denied, please try again.
Babajide@localhost's password:facebook
Babajide@localhost's password:mail.google
Babajide@localhost: Permission denied (publickey,password).
```

The screenshot shows a security monitoring interface with a left sidebar and a main dashboard area.

Left Sidebar:

- Security
- Discover
- Dashboards
- Rules
- Alerts** (selected)
- Attack discovery
- Findings
- Cases
- Explore
- Investigations
- Intelligence
- Assets

Main Dashboard:

Top navigation: Deployment / Alerts, ML job settings, Add integrations, Data view, Alerts (selected), Assignees, Manage rules.

Search bar: * Last 24 hours.

Alerts

Status: open (1), Severity, User, Host, ...

Summary tab (selected):

- Severity levels:

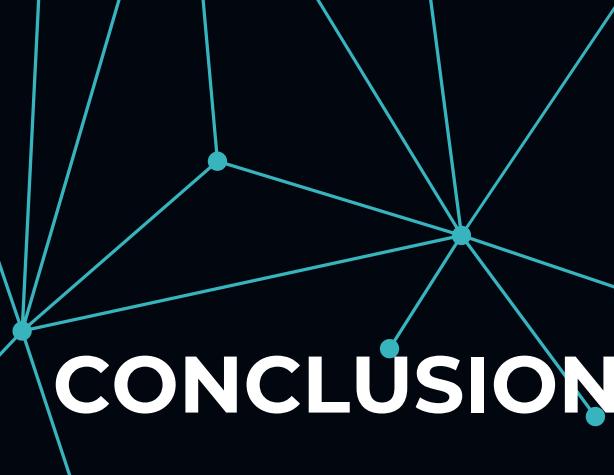
Levels	Count
High	28
- 28 alerts (indicated by a large orange circle)

Trend, Counts, Treemap tabs are also present.

Alerts by name table:

Rule name	Count
SSH Alert	28

Pagination: < 1 >



CONCLUSION

This project was more than just a technical exercise, it was a practical demonstration of how SIEM tools like Elastic Security and Kibana can be leveraged to strengthen digital defenses.

By building and testing detection rules, I showcased how raw system activity can be transformed into meaningful alerts that drive faster and smarter incident response.

In a world where cyber threats continue to evolve, projects like this reinforce the importance of proactive monitoring and continuous security improvement. My focus remains on applying these skills to contribute to a safer and more resilient digital environment for individuals and organizations alike.

