SIEM HOMELAB WITH ELASTIC CLOUD

Threat detection, Alerting and Log Monitoring

Prepared by Babajide Aina

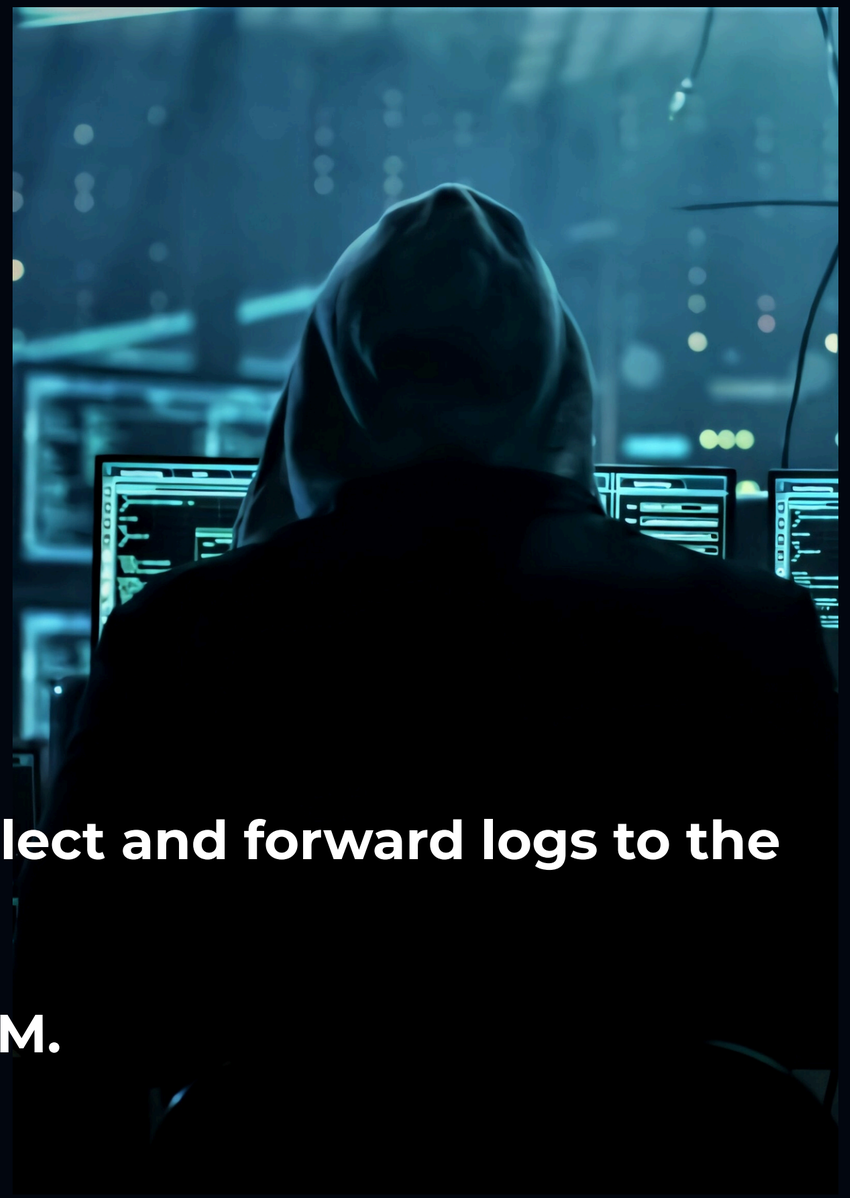
THIS IS A GUIDE ON HOW I SET UP MY VERY OWN HOME LAB FOR ELASTIC STACK SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM). IN THIS PROJECT, I'LL TAKE YOU THROUGH THE STEPS ON HOW I CREATED MY SIEM ENVIRONMENT USING THE ELASTIC WEB PORTAL AND A KALI LINUX VM.

Threat detection, Alerting and Log Monitoring

Prepared by Babajide Aina

Prerequisites:

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

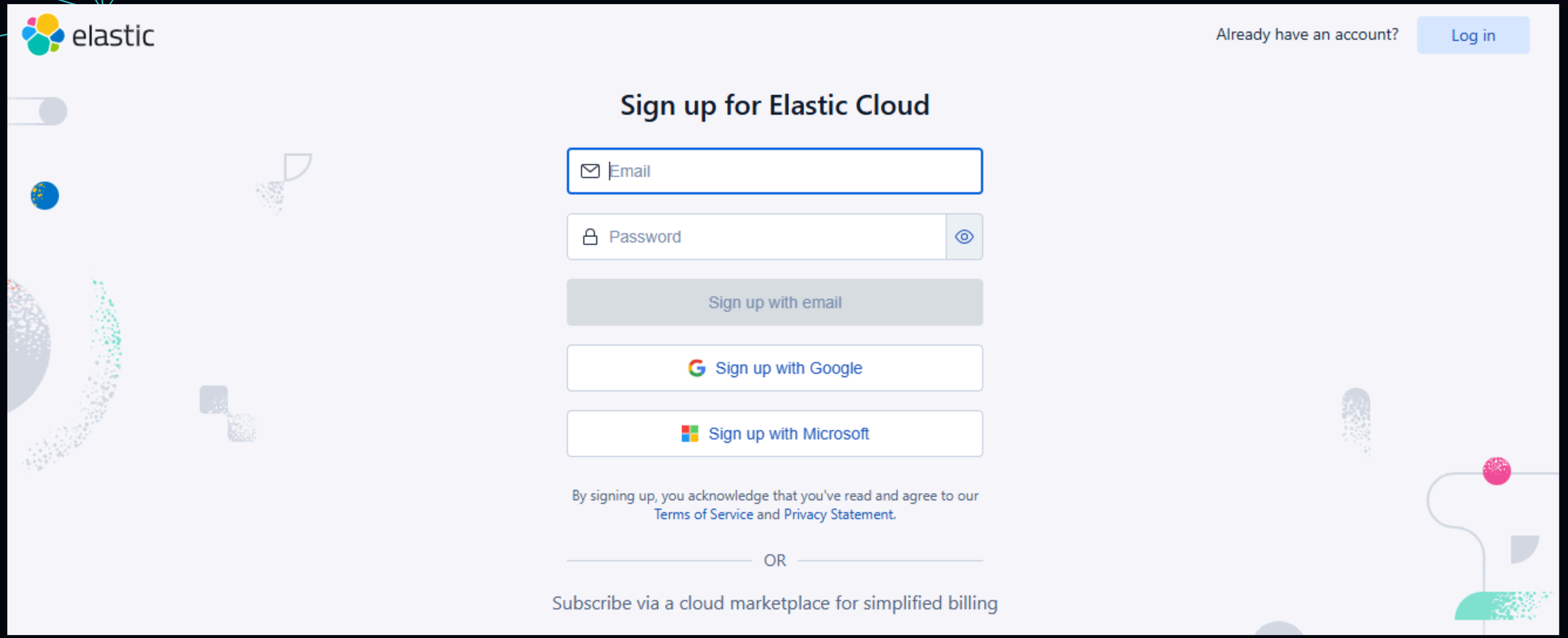


Overview:

- 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.

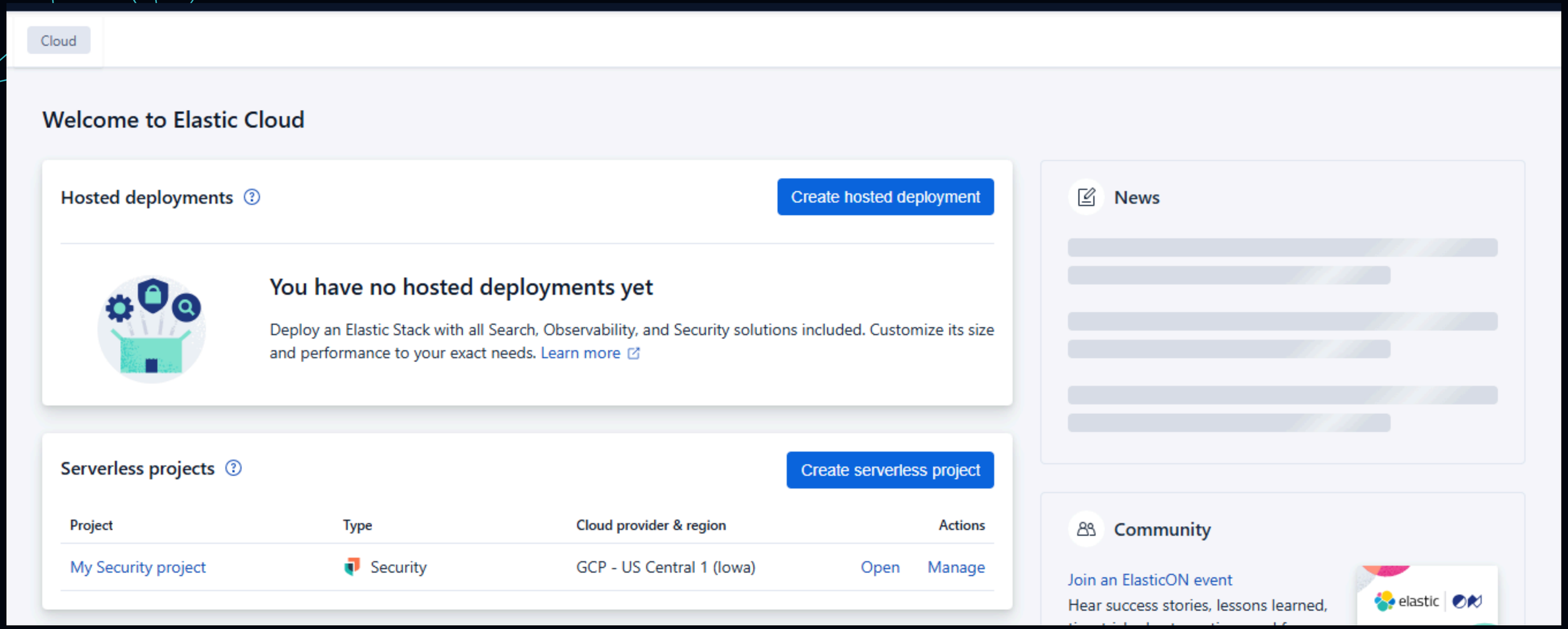
Prepared by Babajide Aina

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



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    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  443M  100  443M    0     0  3527k      0  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
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.txt
```

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=cVhMU
npaZ0JXN2×2SnJSX1Z1OWs6Wmh4dmpLWUdYOTZ0dmJhRXNwbHQxUQ==
[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/elast
ic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":536},"message":"Starting e
nrollment 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/elast
ic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":499},"message":"Rest
arting 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]
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

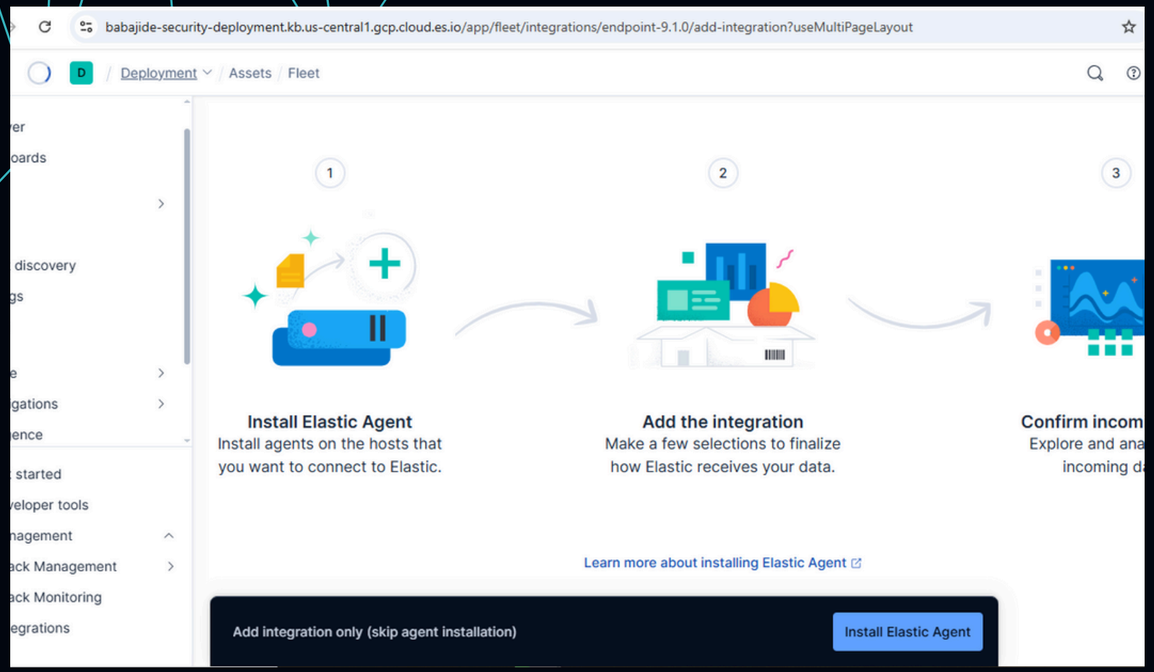
Task 2

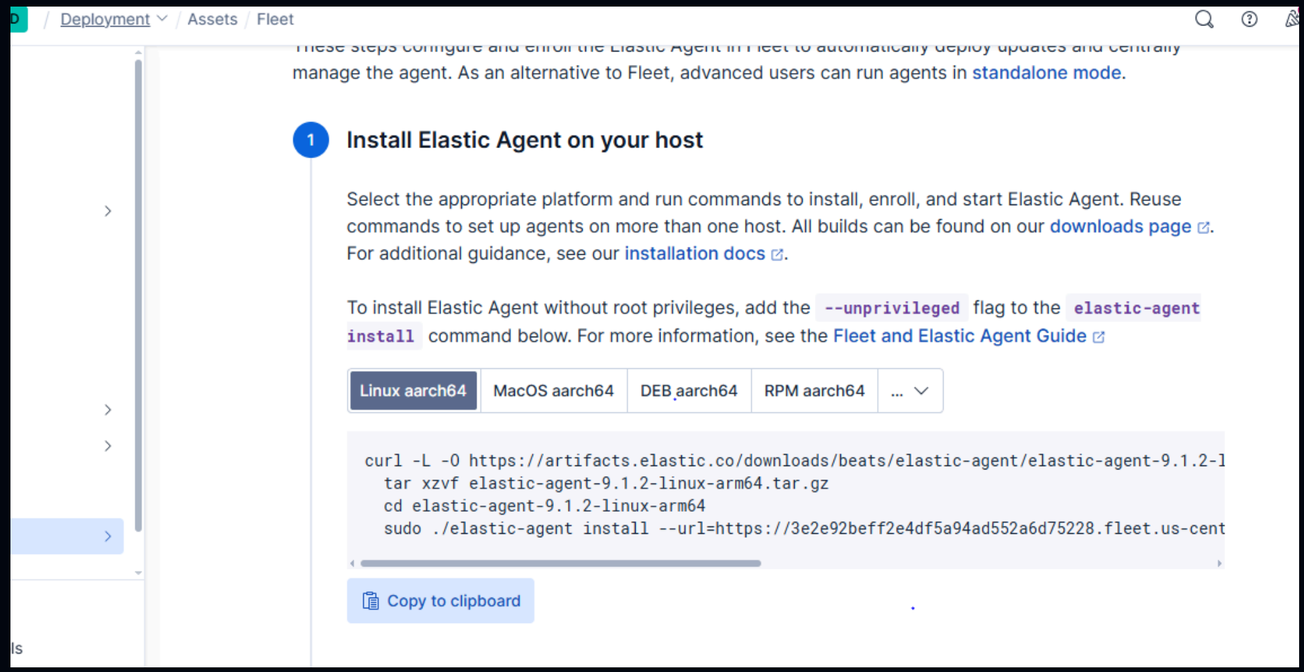
Setting up my Kali Linux VM

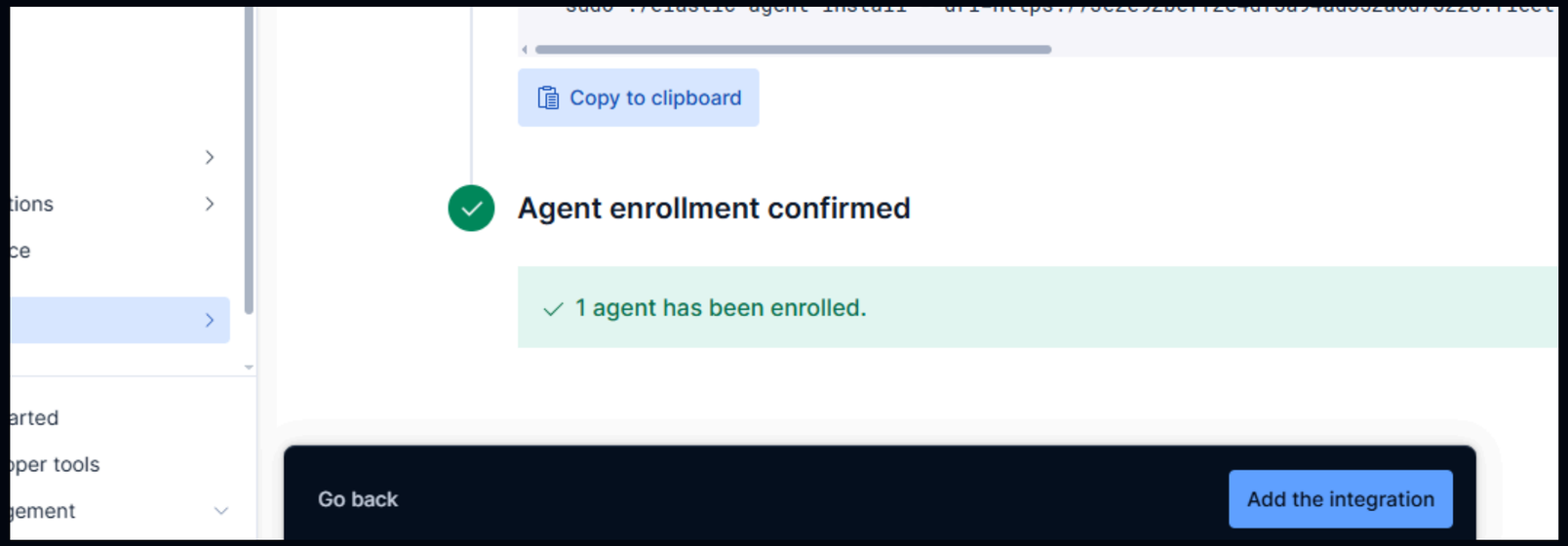
To verify that the agent was installed correctly,I ran the following command in my Kali terminal: sudo systemctl status elastic-agent.service

```
┌──(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 setup.ilm.enabled=false -E setup.
             ├─78993 /opt/Elastic/Agent/data/elastic-agent-9.1.2-45007d/components/agentbeat filebeat -E setup.ilm.enabled=false -E setup.te
             └─79012 /opt/Elastic/Agent/data/elastic-agent-9.1.2-45007d/components/agentbeat metricbeat -E setup.ilm.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





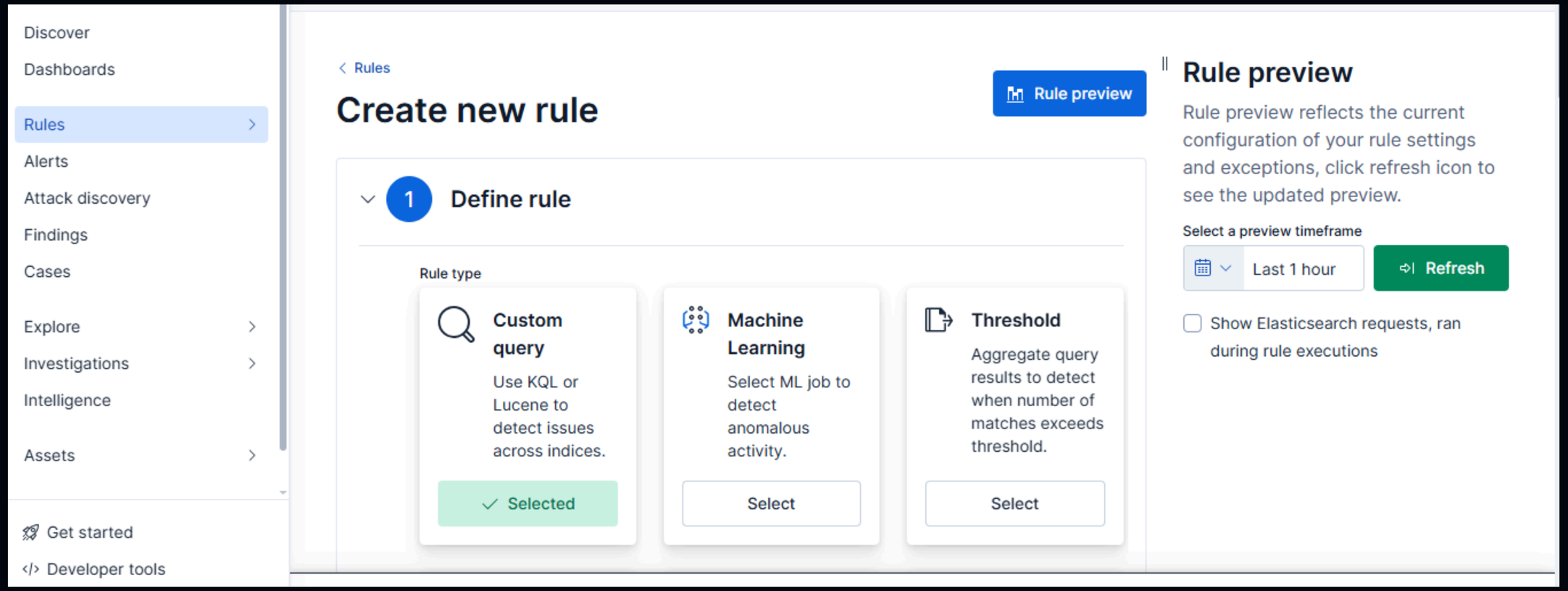


Prepared by Babajide Aina

Task 3

Querying for Security Events in the Elastic SIEM

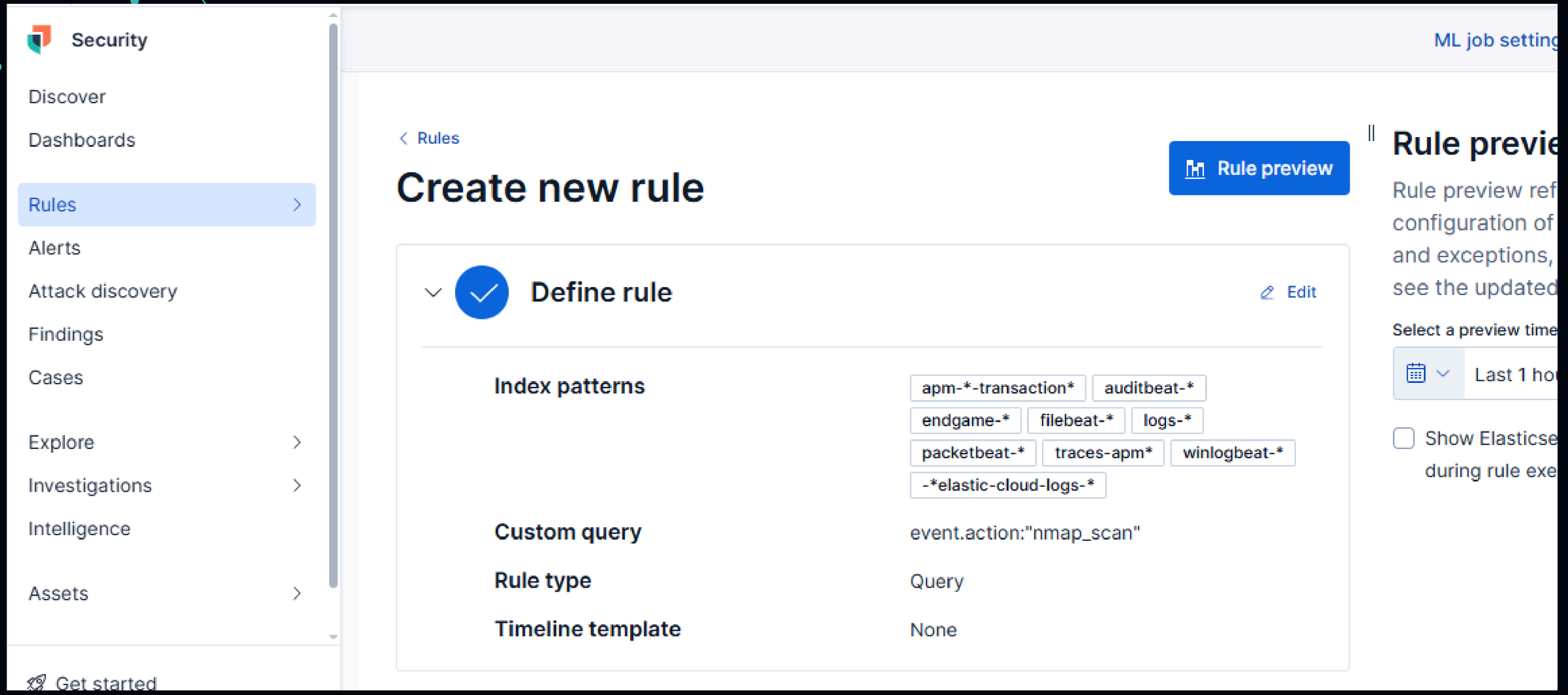
With data seamlessly forwarded from my Kali VM to the SIEM platform, it was time to dive into querying and analyzing the logs within the SIEM interface. I accessed my Elastic deployment ,created new rules and entered a search query for Nmap scans (searching for open ports, services and live machines 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.



Prepared by Babajide Aina

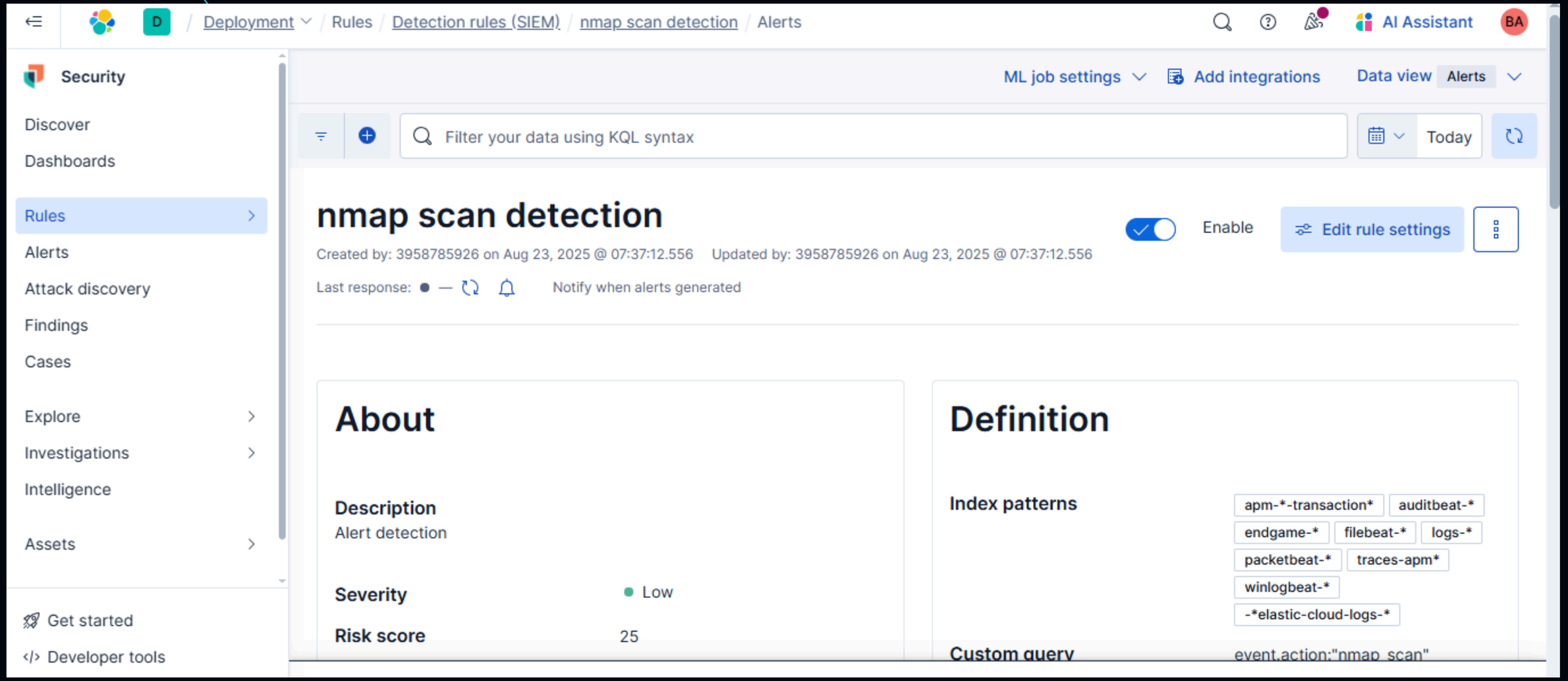
Task 3

Querying for Security Events in the Elastic SIEM



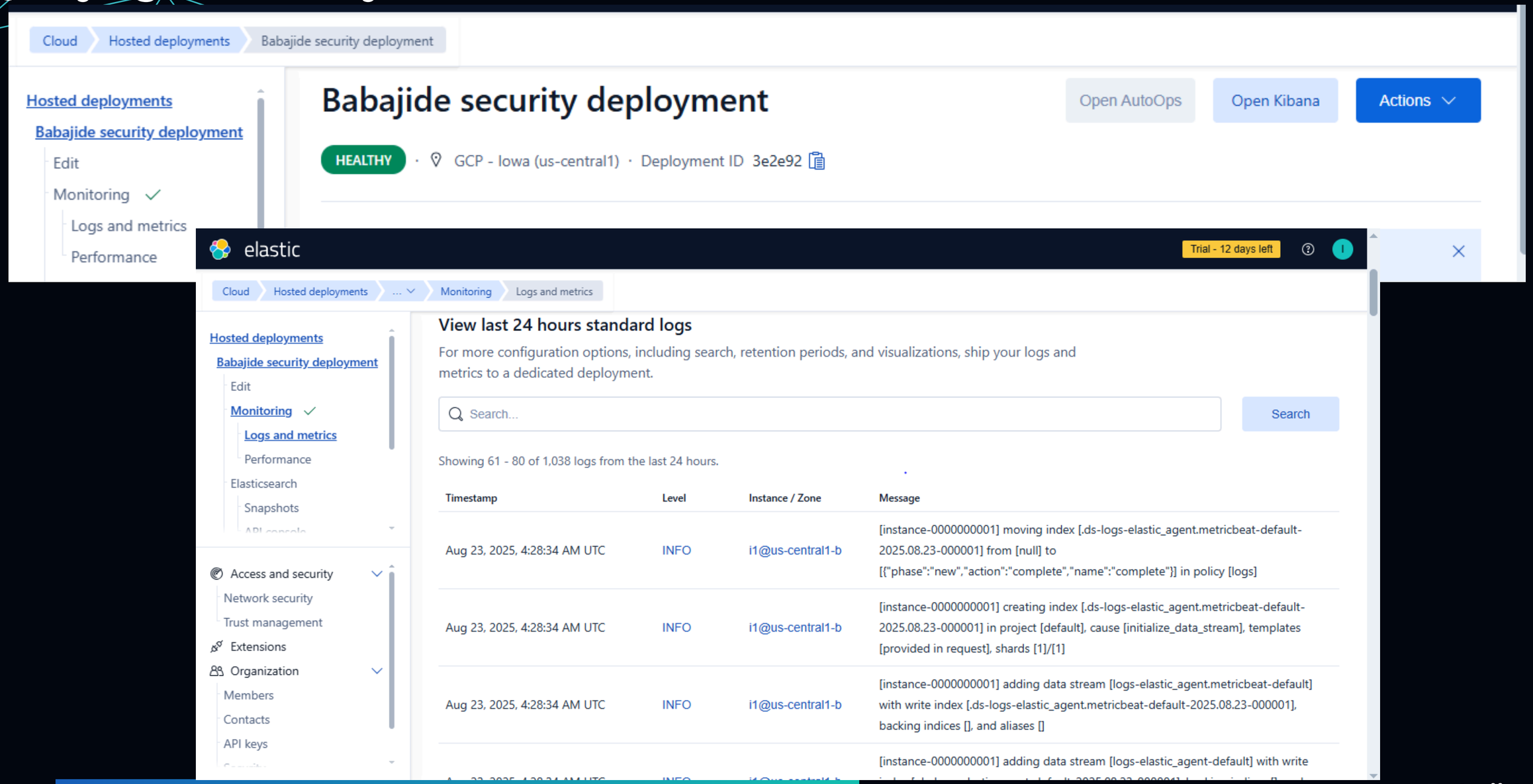
Task 3

Querying for Security Events in the Elastic SIEM



Task 3

Querying for Security Events in the Elastic SIEM

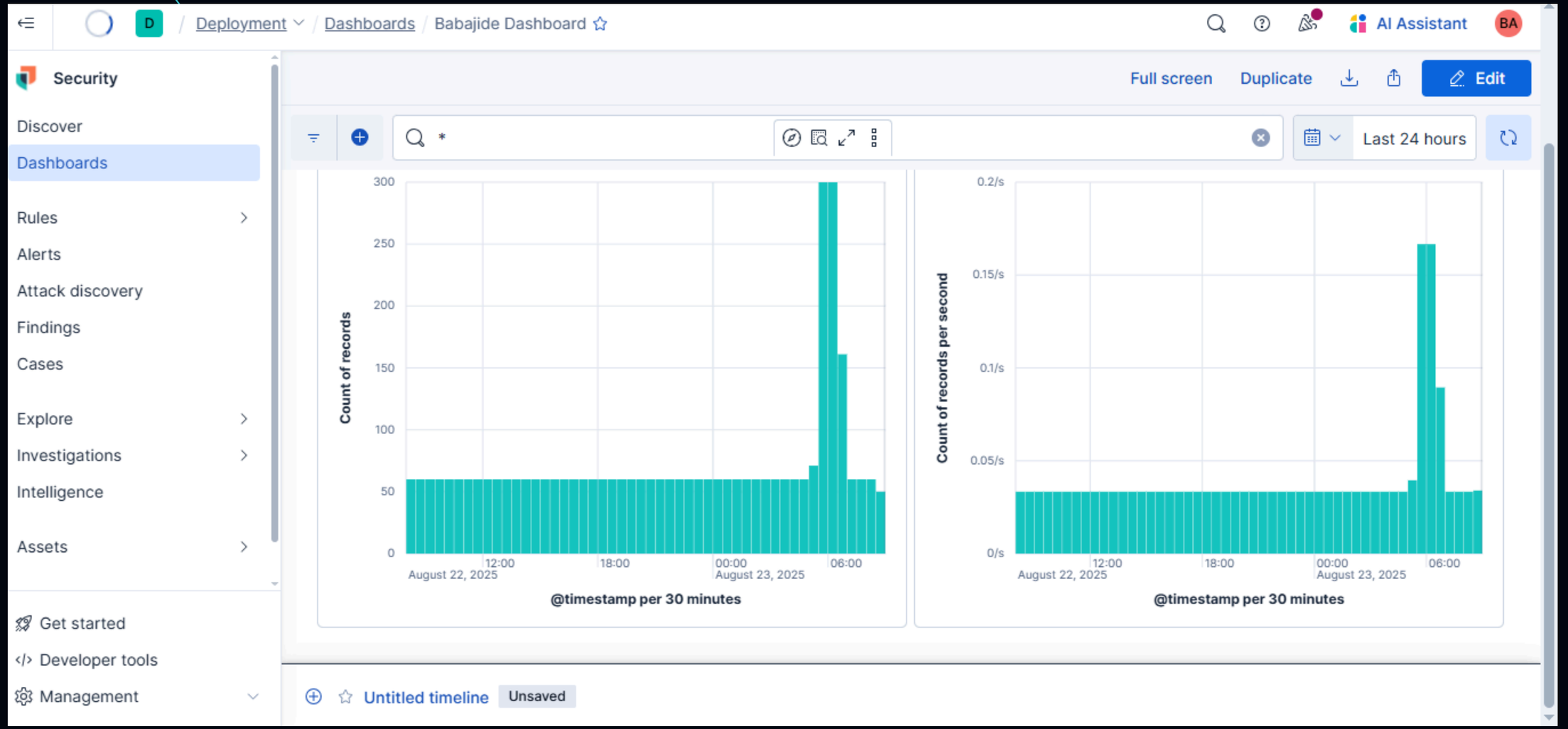


Threat detection, Alerting and Log Monitoring

Prepared by Babajide Aina

Task 4

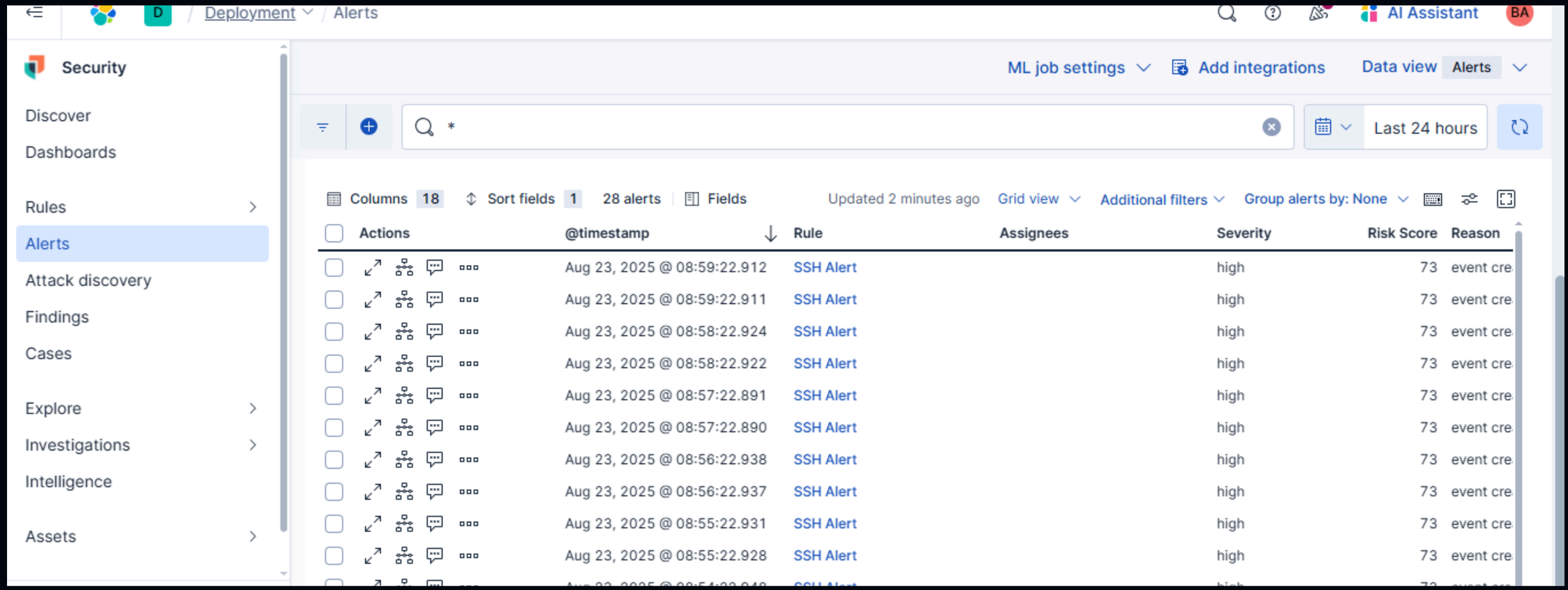
I Created a Dashboard to visualize the events



Prepared by Babajide Aina

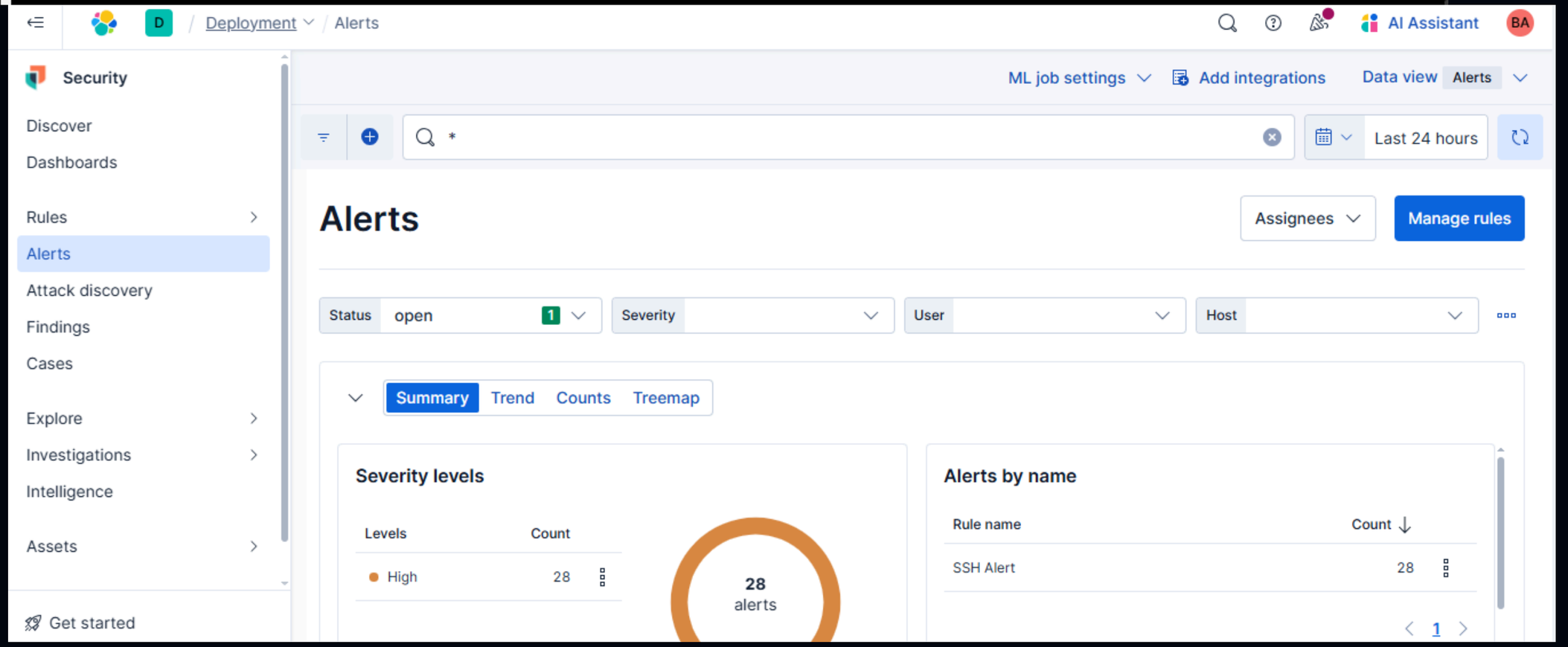
Task 4
Created a Dashboard to visualize the events

```
└─$ 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:
Babajide@localhost: Permission denied (publickey,password).

┌──(kali㉿kali)-[~]
└─$
```



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:
Babajide@localhost: Permission denied (publickey,password).

┌──(kali㉿kali)-[~]
```

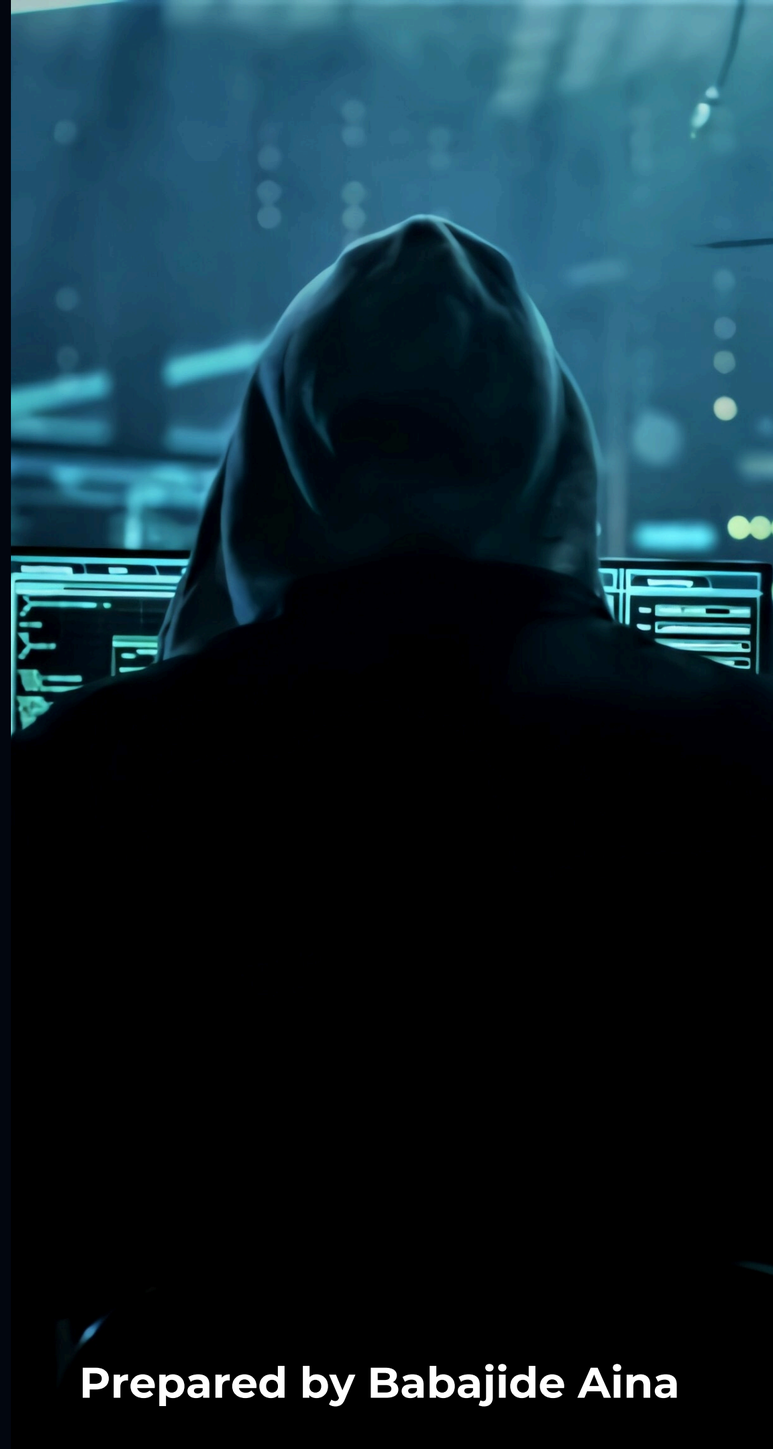


CONCLUSION

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.



Threat detection, Alerting and Log Monitoring

Prepared by Babajide Aina