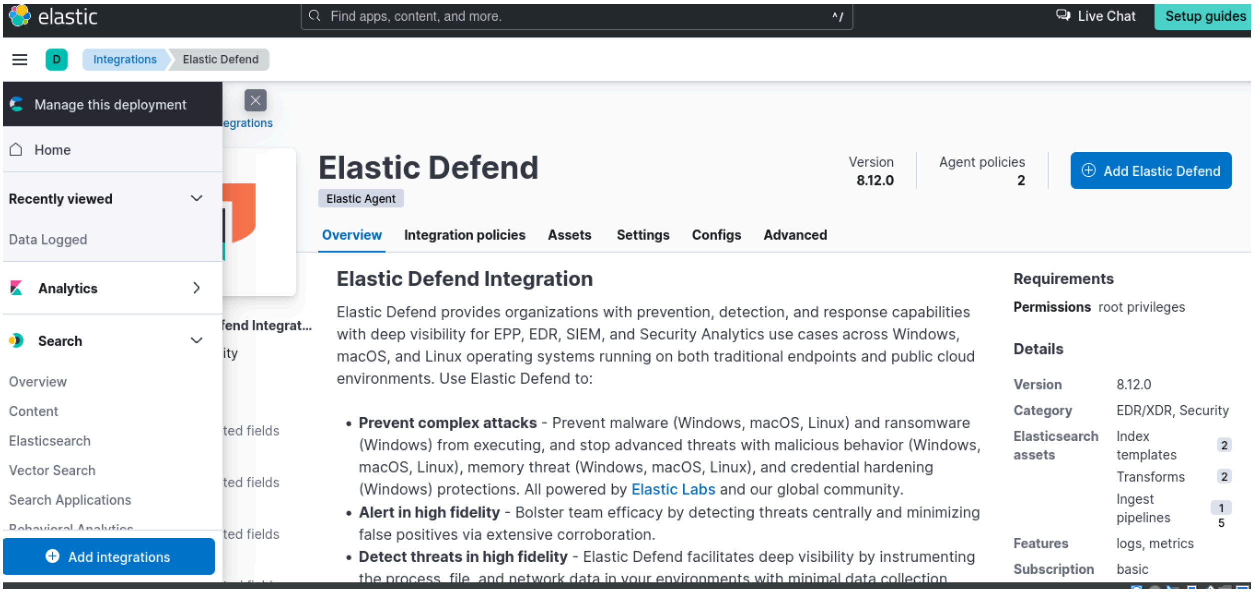
Elastic SIEM Lab

In this Home Lab I set up for Elastic Stack Security Information Event Management using the elastic web portal and Kali VM. Within this lab I was able to generate security events on Kali VM, set up an agent that forwards data to the SIEM as well as query and analyze logs in the SIEM. Very beneficial lab that continues to provide me with hands-on experience in working with different tools to help sharpen my analyst skills.

1. Set up agent “Elastic Defend” that will collect logs from my Kali VM and push data to Elastic SIEM



Elastic Defend

Elastic Agent

Version 8.12.0 | Agent policies 2

Elastic Defend Integration

Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. Use Elastic Defend to:

- **Prevent complex attacks** - Prevent malware (Windows, macOS, Linux) and ransomware (Windows) from executing, and stop advanced threats with malicious behavior (Windows, macOS, Linux), memory threat (Windows, macOS, Linux), and credential hardening (Windows) protections. All powered by Elastic Labs and our global community.
- **Alert in high fidelity** - Bolster team efficacy by detecting threats centrally and minimizing false positives via extensive corroboration.
- **Detect threats in high fidelity** - Elastic Defend facilitates deep visibility by instrumenting the process, file, and network data in your environments with minimal data collection

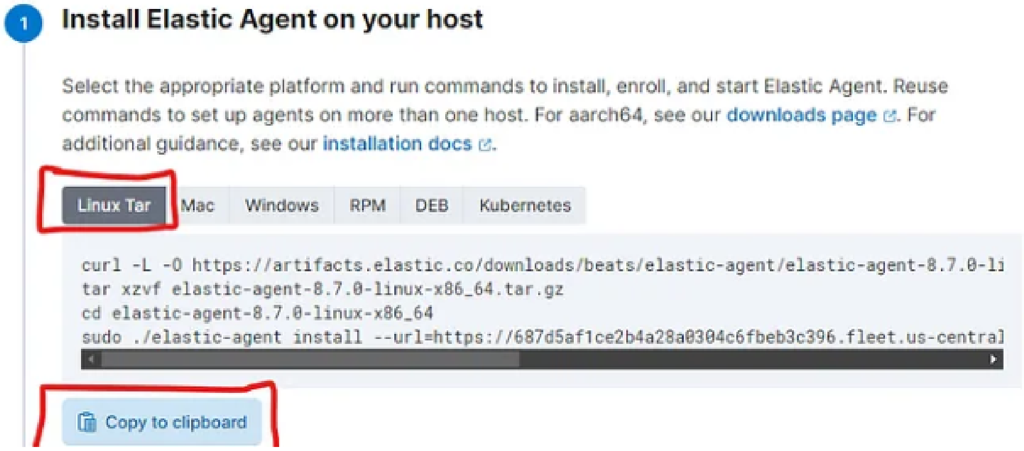
Requirements

Permissions root privileges

Details

Version	8.12.0
Category	EDR/XDR, Security
Elasticsearch assets	Index templates 2 Transforms 2 Ingest pipelines 15
Features	logs, metrics
Subscription	basic

Next was to copy command to enter into LInux terminal

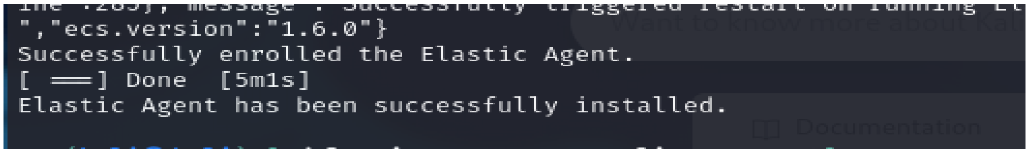


Install Elastic Agent on your host

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. For additional guidance, see our installation docs.

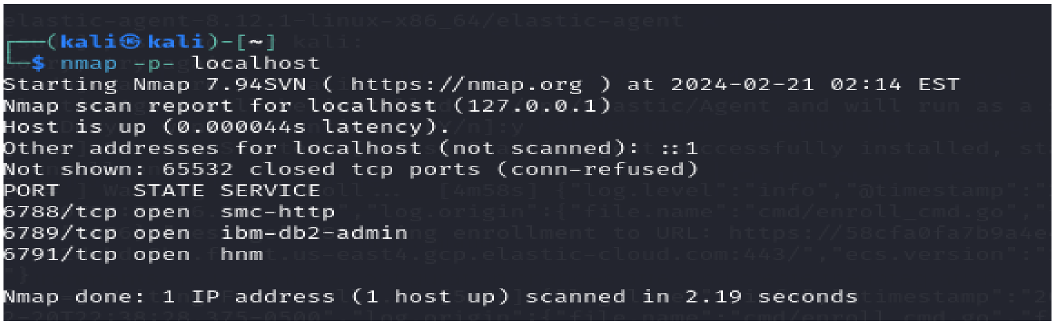
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.7.0-li
tar xzvf elastic-agent-8.7.0-linux-x86_64.tar.gz
cd elastic-agent-8.7.0-linux-x86_64
sudo ./elastic-agent install --url=https://687d5af1ce2b4a28a0304c6fbeb3c396.fleet.us-central
```

Entered and successfully installed Elastic agent into Linux VM

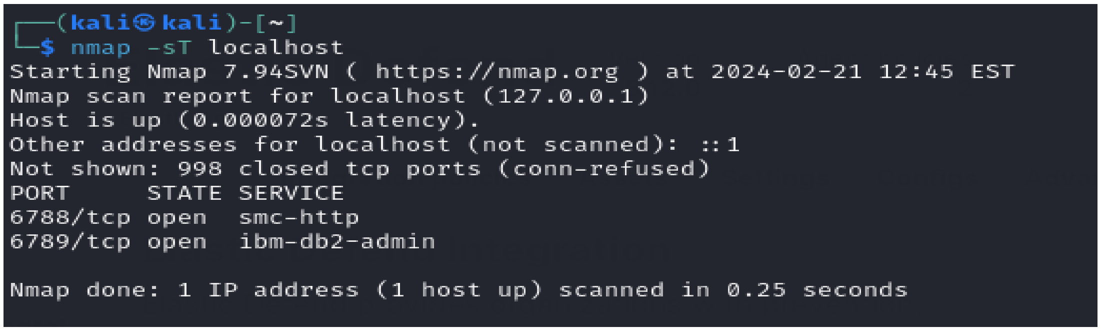


```
ine":283},"message":"Successfully triggered restart on running El
","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[ ══] Done  [5m1s]
Elastic Agent has been successfully installed.
```

After installing Elastic agent next I was able to able generate Security events on Kali VM, this was done using Network analyzer Nmap so I ran the following commands to generate security events:

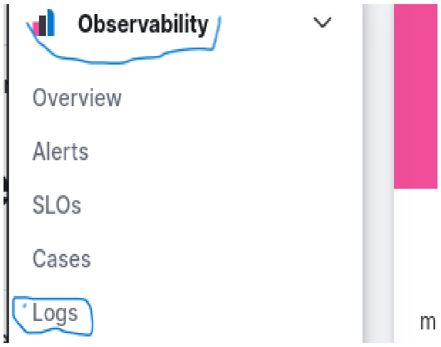


```
┌──(kali㉿kali)-[~]
└─$ nmap -p- localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 02:14 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE
6788/tcp open  smc-http
6789/tcp open  ibm-db2-admin
6791/tcp open  hnm

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
```

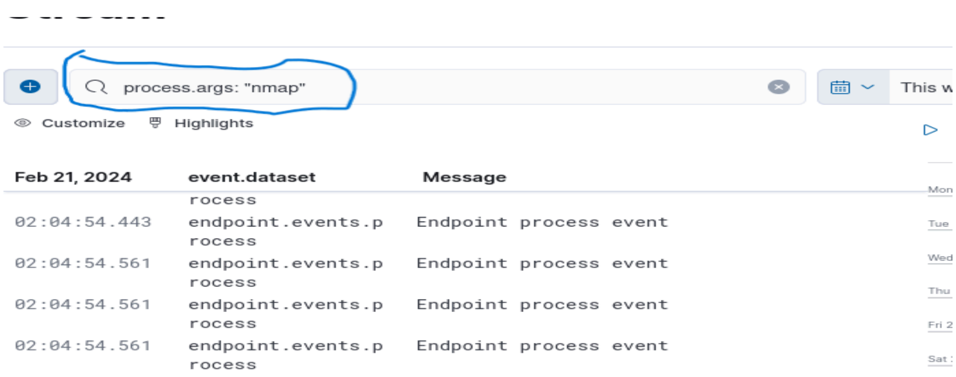


```
┌──(kali㉿kali)-[~]
└─$ nmap -sT localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 12:45 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000072s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
6788/tcp open  smc-http
6789/tcp open  ibm-db2-admin

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Now I have forwarded data from kali VM to the SIEM im able to query and analyze logs within the SIEM

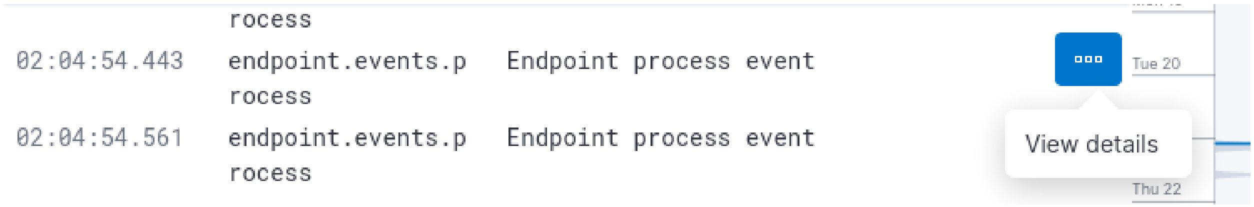


Next was to enter search query to filter the logs that was generated with our scans

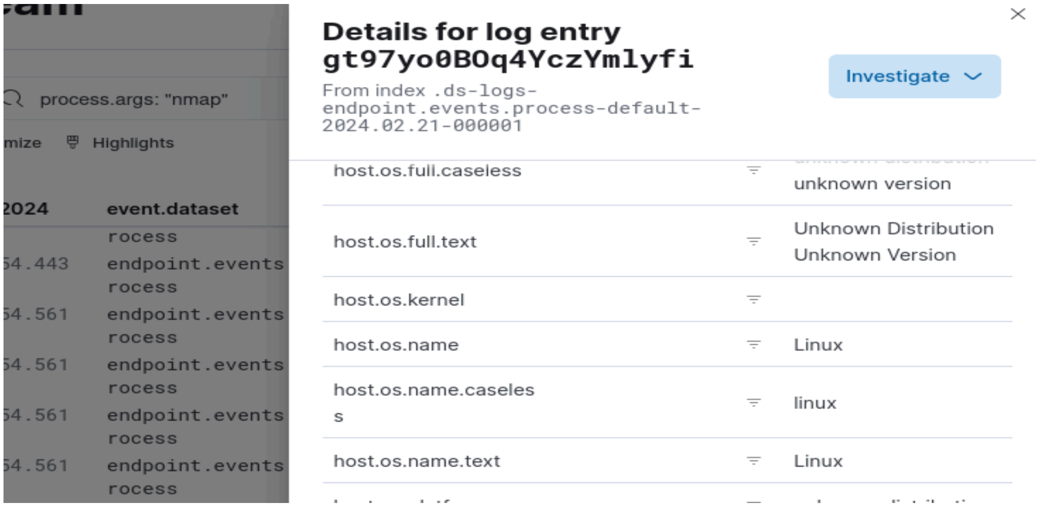


```
Feb 21, 2024   event.dataset          Message
               rocess
02:04:54.443   endpoint.events.p      Endpoint process event
               rocess
02:04:54.561   endpoint.events.p      Endpoint process event
               rocess
02:04:54.561   endpoint.events.p      Endpoint process event
               rocess
02:04:54.561   endpoint.events.p      Endpoint process event
               rocess
```

With Security events on display I was able to gather details on Security events giving me more details on the events.



```
               rocess
02:04:54.443   endpoint.events.p   Endpoint process event
               rocess
02:04:54.561   endpoint.events.p   Endpoint process event
               rocess
```



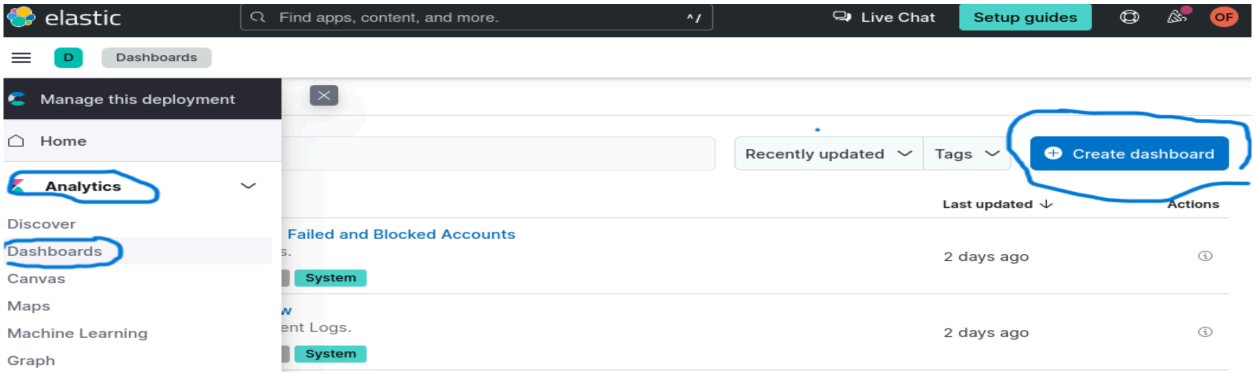
```
2024   event.dataset
       rocess
54.443 endpoint.events
       rocess
54.561 endpoint.events
       rocess
54.561 endpoint.events
       rocess
54.561 endpoint.events
       rocess
54.561 endpoint.events
       rocess
```

Details for log entry gt97yo0BOq4YczYmlyfi

From index .ds-logs-endpoint.events.process-default-2024.02.21-000001

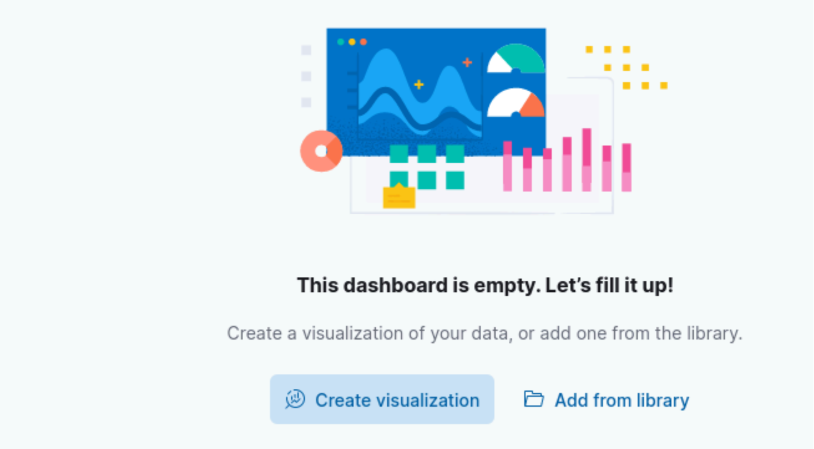
host.os.full.caseless	unknown version
host.os.full.text	Unknown Distribution Unknown Version
host.os.kernel	
host.os.name	Linux
host.os.name.caseless	linux
host.os.name.text	Linux

Next tasks was to create dashboards and visualizations within the SIEM to further analyze logs and identify if they may be patterns to be aware of data that's just not of the norm.



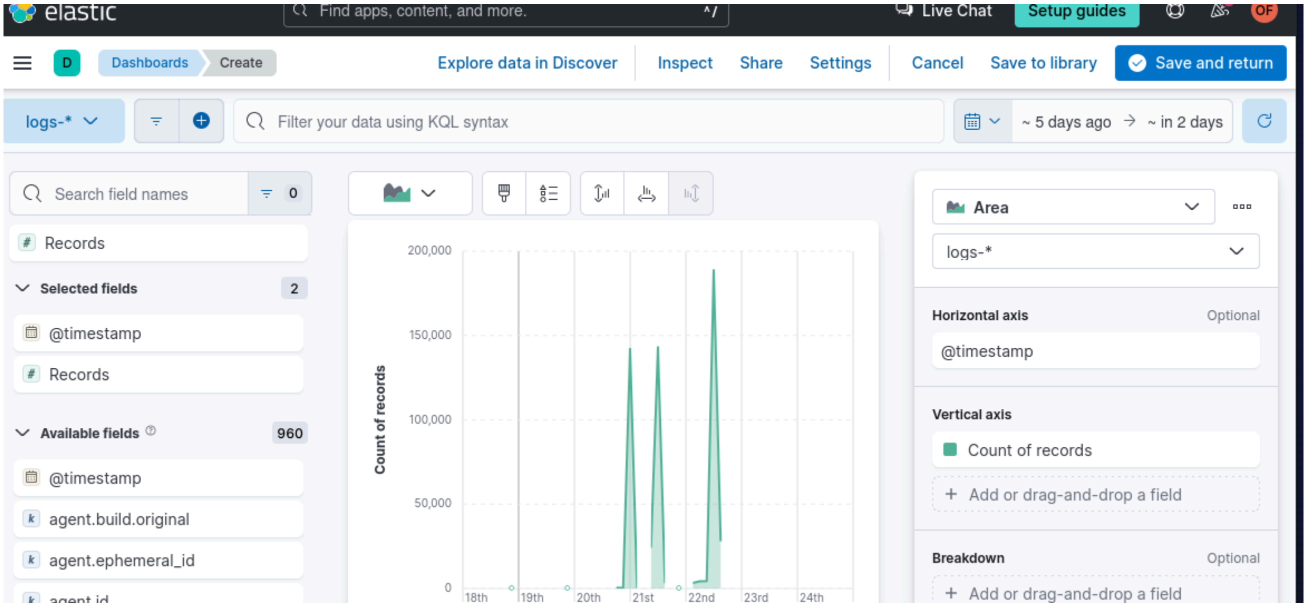
	Last updated	Actions
Failed and Blocked Accounts s. System	2 days ago	
w ent Logs. System	2 days ago	

Next I added Visualization to the dashboard to help see a visual of the data of events



This dashboard is empty. Let's fill it up!

Create a visualization of your data, or add one from the library.



logs-*

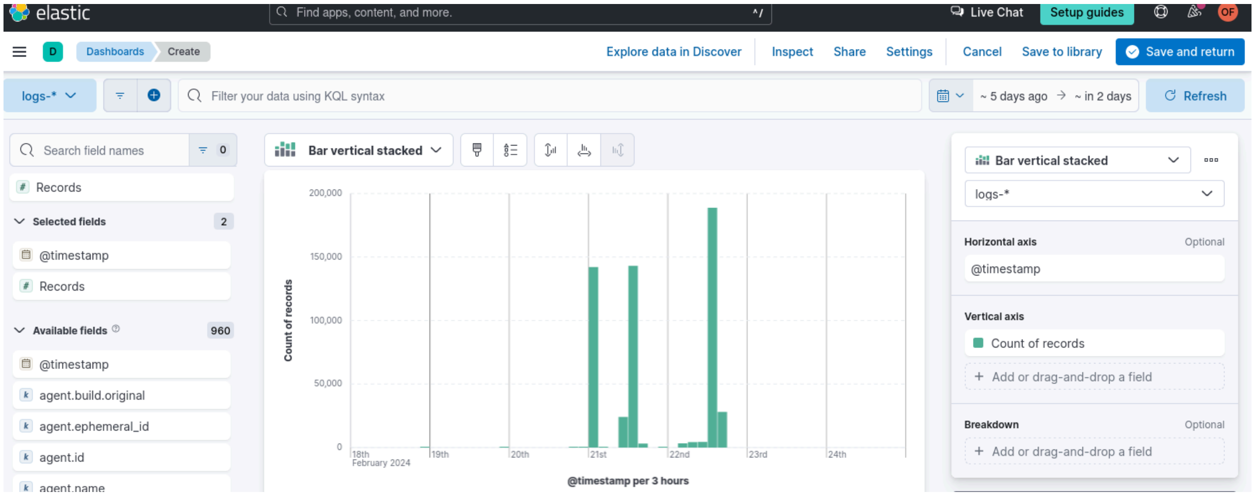
Area

logs-*

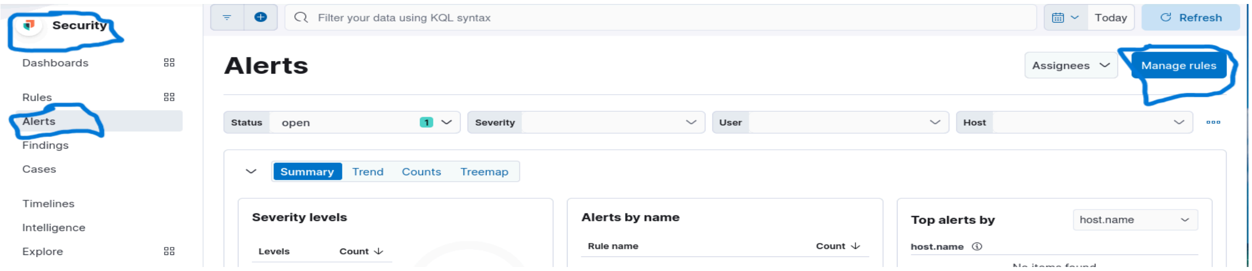
Horizontal axis Optional
@timestamp

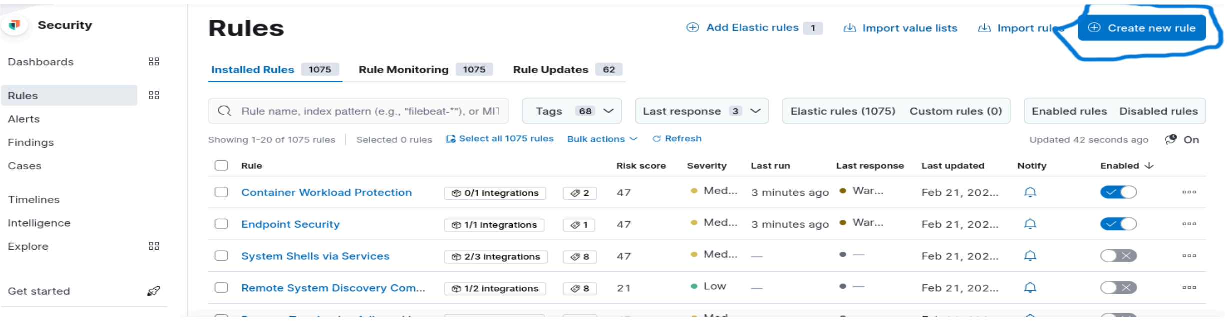
Vertical axis
Count of records

Breakdown Optional



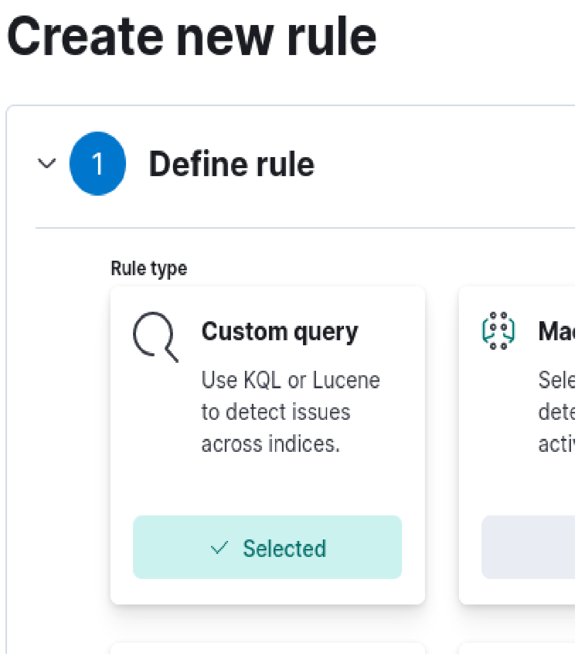
The next task was to create an alert which can be a critical feature used to detect security incidents and being able to respond in a timely manner, and can be configured to trigger specific actions when conditions of alert are met.





Rule			Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
Container Workload Protection	0/1 integrations	2	47	● Med...	3 minutes ago	● War...	Feb 21, 202...	🔔	✓
Endpoint Security	1/1 integrations	1	47	● Med...	3 minutes ago	● War...	Feb 21, 202...	🔔	✓
System Shells via Services	2/3 integrations	8	47	● Med...	—	● —	Feb 21, 202...	🔔	✗
Remote System Discovery Com...	1/2 integrations	8	21	● Low	—	● —	Feb 21, 202...	🔔	✗

Next step was create new rule within the custom query selection to detect all Nmap scan events



Create new rule

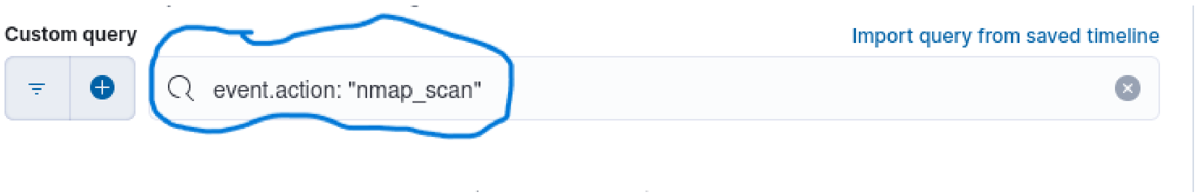
1 Define rule

Rule type

Custom query

Use KQL or Lucene to detect issues across indices.

✓ Selected

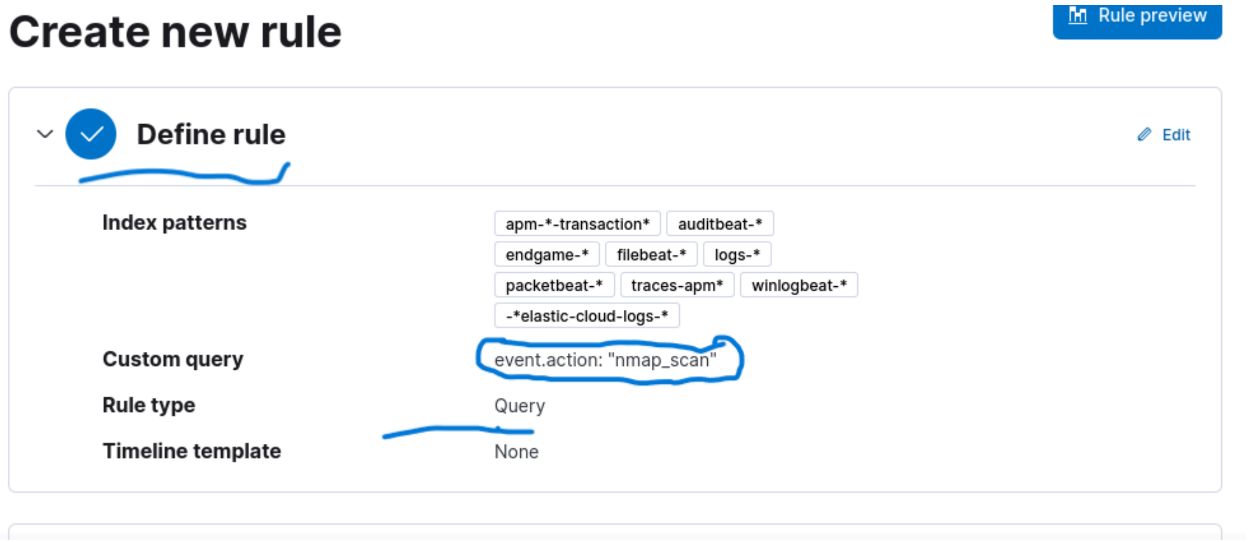


Custom query

Import query from saved timeline

```
event.action: "nmap_scan"
```

Next leading up to final tasks we defined the rule

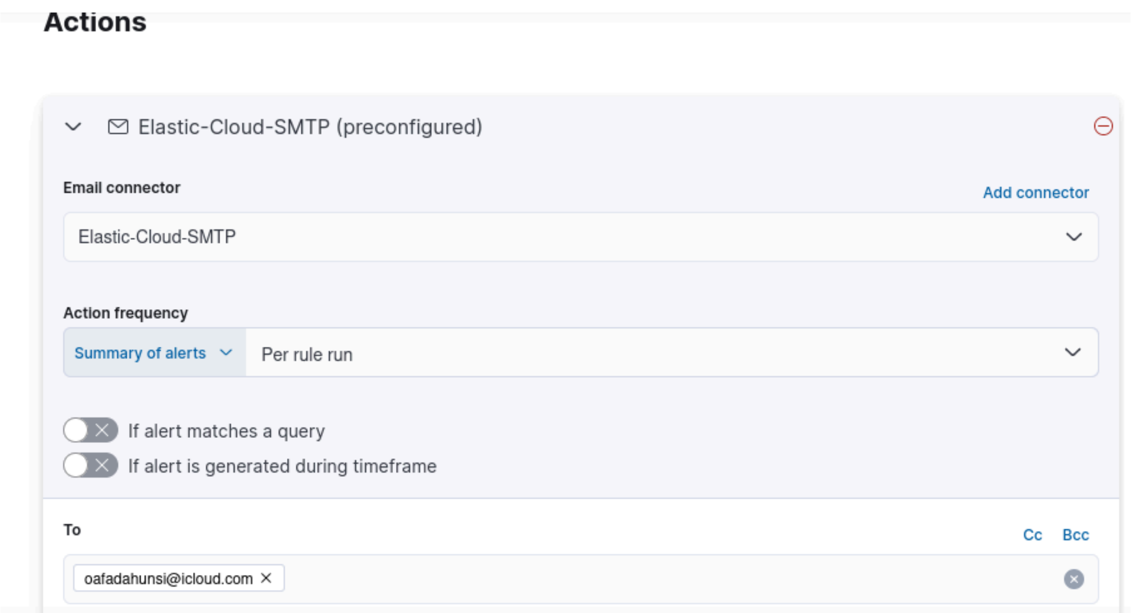


Create new rule

✓ 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

The last few steps before finalizing the rule was to give my rule a name and description and notify me by email once the alert is triggered.



Actions

Elastic-Cloud-SMTP (preconfigured)

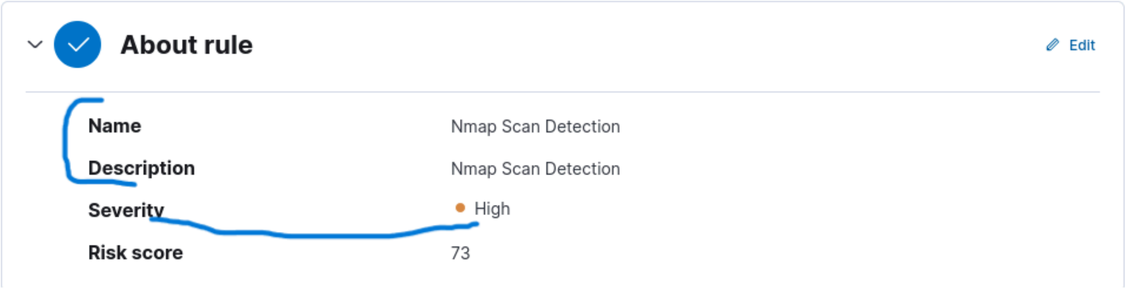
Email connector: Elastic-Cloud-SMTP

Action frequency: Summary of alerts — Per rule run

○ If alert matches a query
○ If alert is generated during timeframe

To: oafadahunsi@icloud.com

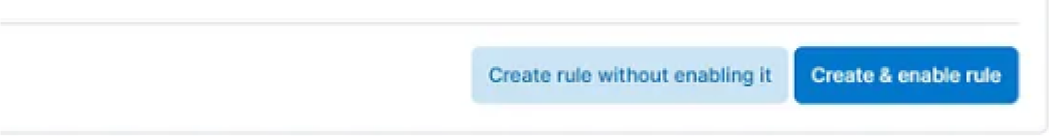
Before the final task was to create name and description of the rule along with the severity of importance which will help prioritize what needs to be done



About rule

Name	Nmap Scan Detection
Description	Nmap Scan Detection
Severity	● High
Risk score	73

Final task is to click create and enable the rule button to finally create the rule.



Once a rule is created it will monitor logs for Nmap scan events if an alert is triggered the selected action that is chosen will be implemented.

In this Lab, I was able to set up a home lab using Elastic SIEM and a Kali VM. The data was forwarded from the Kali VM to the SIEM using the Elastic agent, generated security events on the Kali VM using Nmap, queried and analyzed the logs in the SIEM using the Elastic web interface. Also I created a dashboard to visualize security events and then create an alert to detect security events.

This home lab provided me with a valuable environment for learning and practicing the skills necessary for effective security monitoring and incident response using Elastic SIEM.