Cybersecurity Project

SOC Analysis

Home Lab for Elastic Stack SIEM (Security Information and Event Management)

Prepared by:

Anouar MOUDAD

February 23, 2025

1. Project Overview

This project demonstrates the setup and usage of the **Elastic Stack** as a Security Information and Event Management (**SIEM**) solution in a home lab environment. The setup is virtualized using **VMware ESXi**, with **Ubuntu** as the primary system for generating security events. An Elastic Agent is configured to forward logs to the **SIEM**, allowing real-time monitoring and analysis. Additionally, email alerts are configured to provide instant notifications of significant security events, enhancing threat detection and response capabilities.

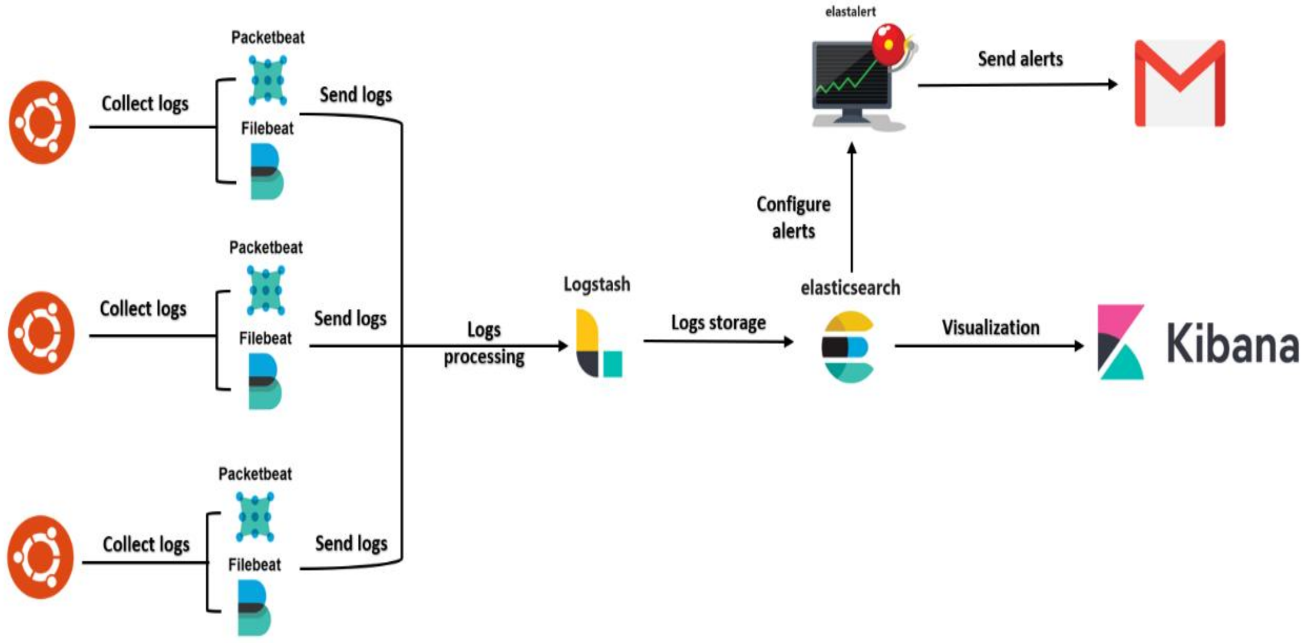
2. Tools Used

2. Objectives

- Set up and configure a SIEM environment with Elastic Stack.
- Generate and forward security events to Elastic SIEM for analysis.
- Monitor and visualize security data through dashboards in Kibana.
- Configure email alerts for real-time incident monitoring.
- Deepen understanding of SIEM capabilities through hands-on implementation.

3. Architecture

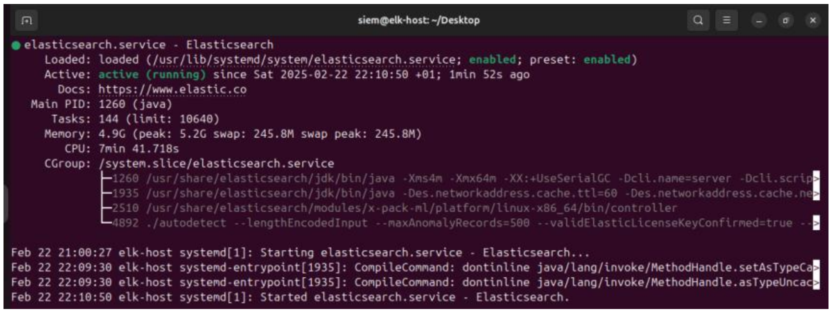
An Elastic Stack-based SIEM setup where Ubuntu agents collect logs using **Packetbeat** and **Filebeat**. Logs are forwarded to **Logstash** for processing, then stored in **Elasticsearch** and visualized in **Kibana**. **ElastAlert** monitors logs and sends alerts via email when anomalies are detected.



4. Tasks Overview

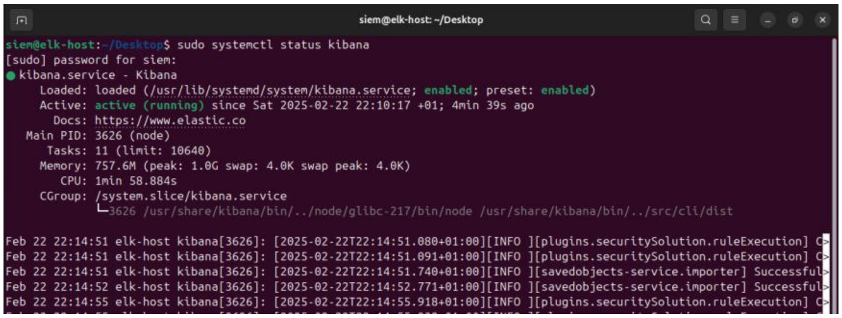
1. Set up Elastic and logs forwarders

Install **Elasticsearch** and verify that it's running:



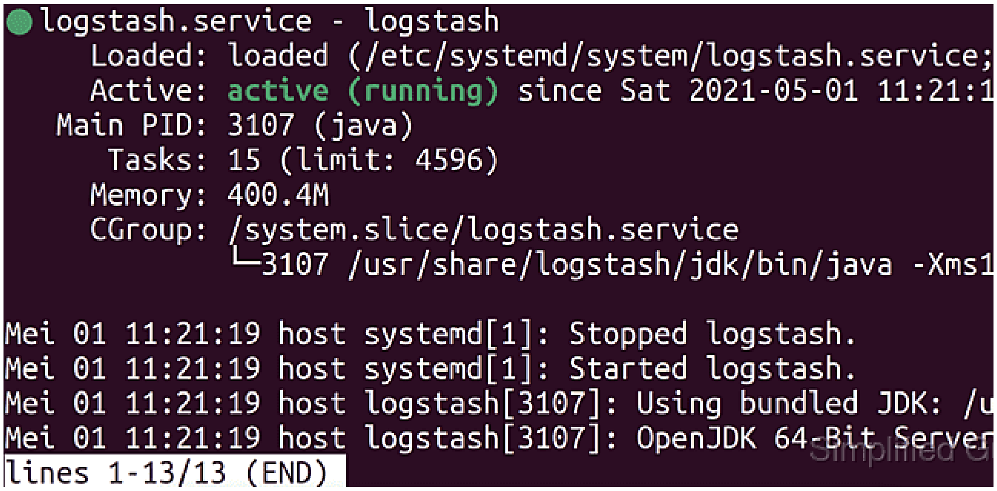
```
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-02-22 22:10:50 +01; 1min 52s ago
       Docs: https://www.elastic.co
   Main PID: 1260 (java)
      Tasks: 144 (limit: 10640)
     Memory: 4.9G (peak: 5.2G swap: 245.8M swap peak: 245.8M)
        CPU: 7min 41.718s
     CGroup: /system.slice/elasticsearch.service
             ├─1260 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.scrip>
             ├─1935 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.ne>
             ├─2510 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
             └─4892 ./autodetect --lengthEncodedInput --maxAnomalyRecords=500 --validElasticLicenseKeyConfirmed=true -->

Feb 22 21:00:27 elk-host systemd[1]: Starting elasticsearch.service - Elasticsearch...
Feb 22 22:09:30 elk-host systemd-entrypoint[1935]: CompileCommand: dontinline java/lang/invoke/MethodHandle.setAsTypeCa>
Feb 22 22:09:30 elk-host systemd-entrypoint[1935]: CompileCommand: dontinline java/lang/invoke/MethodHandle.asTypeUncac>
Feb 22 22:10:50 elk-host systemd[1]: Started elasticsearch.service - Elasticsearch.
```

Install **Kibana** and verify that it's running:



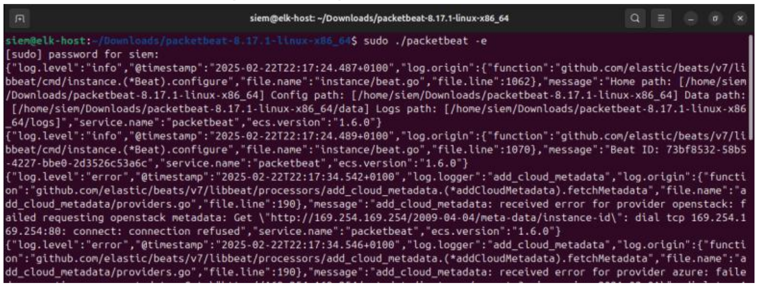
```
siem@elk-host:~/Desktop$ sudo systemctl status kibana
[sudo] password for siem:
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-02-22 22:10:17 +01; 4min 39s ago
       Docs: https://www.elastic.co
   Main PID: 3626 (node)
      Tasks: 11 (limit: 10640)
     Memory: 757.6M (peak: 1.0G swap: 4.0K swap peak: 4.0K)
        CPU: 1min 58.884s
     CGroup: /system.slice/kibana.service
             └─3626 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Feb 22 22:14:51 elk-host kibana[3626]: [2025-02-22T22:14:51.080+01:00][INFO ][plugins.securitySolution.ruleExecution] C>
Feb 22 22:14:51 elk-host kibana[3626]: [2025-02-22T22:14:51.091+01:00][INFO ][plugins.securitySolution.ruleExecution] C>
Feb 22 22:14:51 elk-host kibana[3626]: [2025-02-22T22:14:51.740+01:00][INFO ][savedobjects-service.importer] Successful>
Feb 22 22:14:52 elk-host kibana[3626]: [2025-02-22T22:14:52.771+01:00][INFO ][savedobjects-service.importer] Successful>
Feb 22 22:14:55 elk-host kibana[3626]: [2025-02-22T22:14:55.918+01:00][INFO ][plugins.securitySolution.ruleExecution] C>
```

Install **Logstash** and verify that t's running:



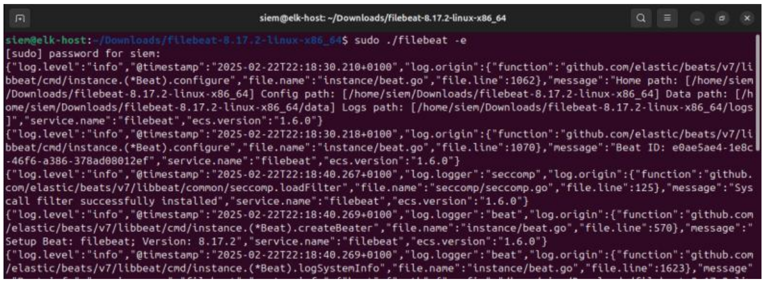
```
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service;
     Active: active (running) since Sat 2021-05-01 11:21:1
   Main PID: 3107 (java)
      Tasks: 15 (limit: 4596)
     Memory: 400.4M
     CGroup: /system.slice/logstash.service
             └─3107 /usr/share/logstash/jdk/bin/java -Xms1

Mei 01 11:21:19 host systemd[1]: Stopped logstash.
Mei 01 11:21:19 host systemd[1]: Started logstash.
Mei 01 11:21:19 host logstash[3107]: Using bundled JDK: /u
Mei 01 11:21:19 host logstash[3107]: OpenJDK 64-Bit Server
lines 1-13/13 (END)
```

Start and configure log forwarders: **Packetbeat** and **Filebeat** on the three agents:



siem@elk-host: ~/Downloads/packetbeat-8.17.1-linux-x86_64

```
siem@elk-host:~/Downloads/packetbeat-8.17.1-linux-x86_64$ sudo ./packetbeat -e
[sudo] password for siem:
{"log.level":"info","@timestamp":"2025-02-22T22:17:24.487+0100","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1062},"message":"Home path: [/home/siem
/Downloads/packetbeat-8.17.1-linux-x86_64] Config path: [/home/siem/Downloads/packetbeat-8.17.1-linux-x86_64] Data path:
 [/home/siem/Downloads/packetbeat-8.17.1-linux-x86_64/data] Logs path: [/home/siem/Downloads/packetbeat-8.17.1-linux-x86
_64/logs]","service.name":"packetbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-02-22T22:17:24.489+0100","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1070},"message":"Beat ID: 73bf8532-58b5
-4227-bbe0-2d3526c53a6c","service.name":"packetbeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2025-02-22T22:17:34.542+0100","log.logger":"add_cloud_metadata","log.origin":{"functi
on":"github.com/elastic/beats/v7/libbeat/processors/add_cloud_metadata.(*addCloudMetadata).fetchMetadata","file.name":"a
dd_cloud_metadata/providers.go","file.line":190},"message":"add_cloud_metadata: received error for provider openstack: f
ailed requesting openstack metadata: Get \"http://169.254.169.254/2009-04-04/meta-data/instance-id\": dial tcp 169.254.1
69.254:80: connect: connection refused","service.name":"packetbeat","ecs.version":"1.6.0"}
{"log.level":"error","@timestamp":"2025-02-22T22:17:34.546+0100","log.logger":"add_cloud_metadata","log.origin":{"functi
on":"github.com/elastic/beats/v7/libbeat/processors/add_cloud_metadata.(*addCloudMetadata).fetchMetadata","file.name":"a
dd_cloud_metadata/providers.go","file.line":190},"message":"add_cloud_metadata: received error for provider azure: faile
```

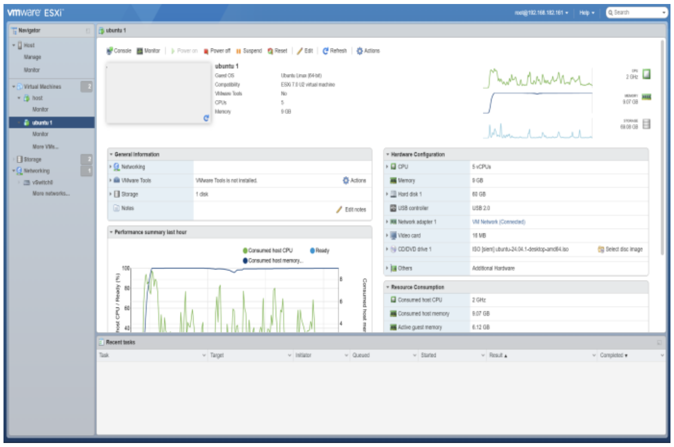


siem@elk-host: ~/Downloads/filebeat-8.17.2-linux-x86_64

```
siem@elk-host:~/Downloads/filebeat-8.17.2-linux-x86_64$ sudo ./filebeat -e
[sudo] password for siem:
{"log.level":"info","@timestamp":"2025-02-22T22:18:30.210+0100","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1062},"message":"Home path: [/home/siem
/Downloads/filebeat-8.17.2-linux-x86_64] Config path: [/home/siem/Downloads/filebeat-8.17.2-linux-x86_64] Data path: [/h
ome/siem/Downloads/filebeat-8.17.2-linux-x86_64/data] Logs path: [/home/siem/Downloads/filebeat-8.17.2-linux-x86_64/logs
]","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-02-22T22:18:30.218+0100","log.origin":{"function":"github.com/elastic/beats/v7/li
bbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":1070},"message":"Beat ID: e0ae5ae4-1e8c
-46f6-a386-378ad08012ef","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-02-22T22:18:40.267+0100","log.logger":"seccomp","log.origin":{"function":"github.
com/elastic/beats/v7/libbeat/common/seccomp.loadFilter","file.name":"seccomp/seccomp.go","file.line":125},"message":"Sys
call filter successfully installed","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-02-22T22:18:40.269+0100","log.logger":"beat","log.origin":{"function":"github.com
/elastic/beats/v7/libbeat/cmd/instance.(*Beat).createBeater","file.name":"instance/beat.go","file.line":570},"message":"
Setup Beat: filebeat; Version: 8.17.2","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-02-22T22:18:40.269+0100","log.logger":"beat","log.origin":{"function":"github.com
/elastic/beats/v7/libbeat/cmd/instance.(*Beat).logSystemInfo","file.name":"instance/beat.go","file.line":1623},"message"
```

2. Install VMs

I used **VMware ESXi** to install the two **Ubuntu agents**.



ubuntu 1

Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 7.0 U2 virtual machine
VMware Tools: No
CPUs: 5
Memory: 9 GB

General Information

Networking	
VMware Tools	VMware Tools is not installed.
Storage	1 disk
Notes	

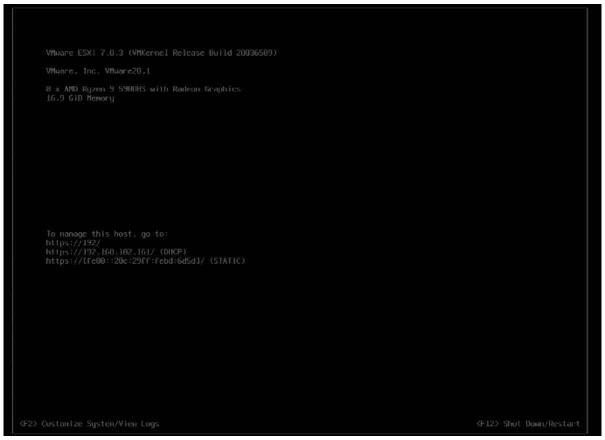
Performance summary last hour

Hardware Configuration

CPU	5 vCPUs
Memory	9 GB
Hard disk 1	60 GB
USB controller	USB 2.0
Network adapter 1	VM Network (Connected)
Video card	16 MB
CD/DVD drive 1	ISO [siem] ubuntu-24.04.1-desktop-amd64.iso
Others	Additional Hardware

Resource Consumption

Consumed host CPU	2 GHz
Consumed host memory	9.07 GB
Active guest memory	6.12 GB

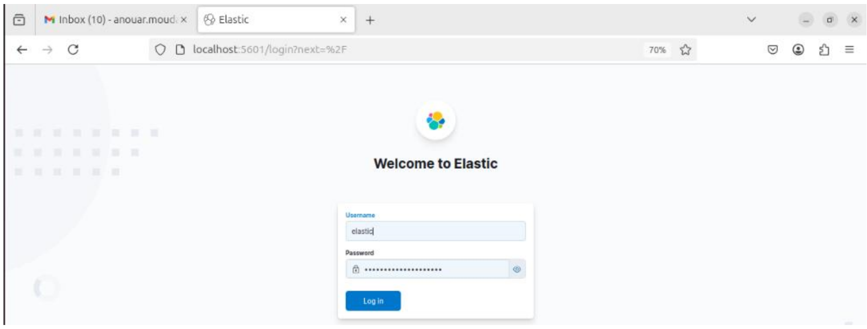


```
VMware ESXi 7.0.3 (VMKernel Release Build 20036589)

VMware, Inc. VMware20,1

8 x AMD Ryzen 9 5900HS with Radeon Graphics
16.9 GiB Memory




To manage this host, go to:
https://192/
https://192.168.182.161/ (DHCP)
https://[fe80::20c:29ff:febd:6d5d]/ (STATIC)



<F2> Customize System/View Logs                                  <F12> Shut Down/Restart
```

3. Configure Elastic Agent

To receive logs in **Elastic Stack** and visualize them in **Kibana**, you need to configure the relevant services properly. This includes updating the configuration files for **Filebeat**, **Packetbeat**, and **Logstash** to specify the **Elasticsearch host URL** and authentication credentials (such as username and password).

Additionally, you must ensure that **Kibana** is connected to **Elasticsearch** by setting the correct **Elasticsearch URL** in its configuration file. Proper configuration allows logs to be forwarded, processed, stored, and visualized seamlessly in **Kibana dashboards**.



Welcome to Elastic

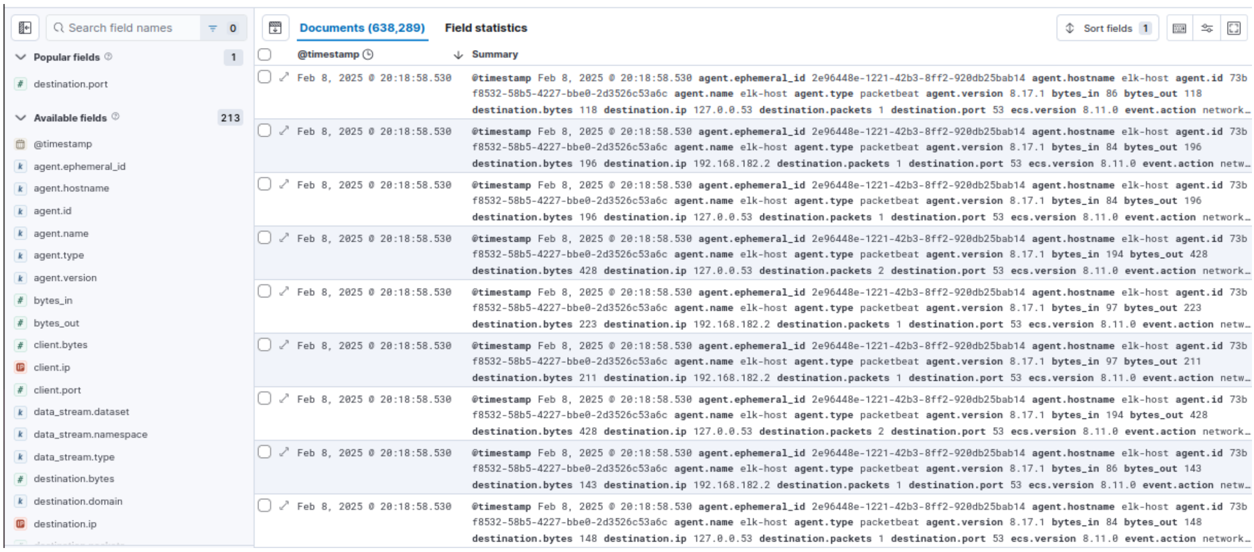
Username: elastic

Password: ••••••••••••••••••••

Log in

4. KQL syntax

In Elasticsearch, **KQL** (Kibana Query Language) is used for querying and searching data in Kibana. KQL is simpler to use than Lucene query syntax and provides a more intuitive approach to searching and filtering your data.

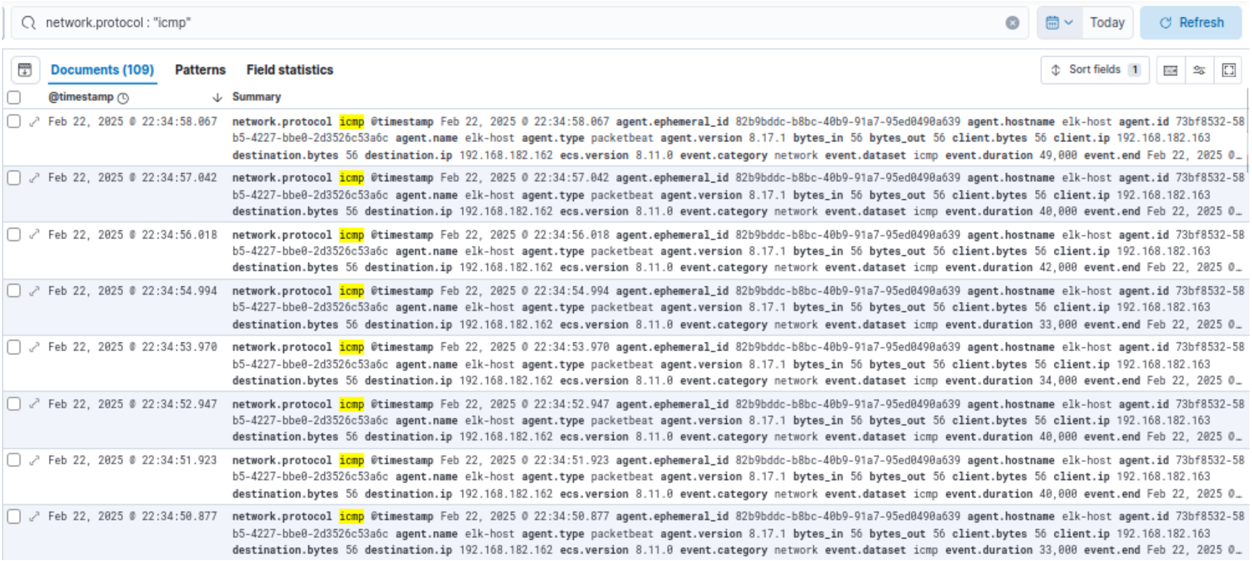


Popular fields 1
- destination.port

Available fields 213
- @timestamp
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- bytes_in
- bytes_out
- client.bytes
- client.ip
- client.port
- data_stream.dataset
- data_stream.namespace
- data_stream.type
- destination.bytes
- destination.domain
- destination.ip

@timestamp	Summary
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 86 **bytes_out** 118 **destination.bytes** 118 **destination.ip** 127.0.0.53 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** network…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 84 **bytes_out** 196 **destination.bytes** 196 **destination.ip** 192.168.182.2 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** netw…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 84 **bytes_out** 196 **destination.bytes** 196 **destination.ip** 127.0.0.53 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** network…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 194 **bytes_out** 428 **destination.bytes** 428 **destination.ip** 127.0.0.53 **destination.packets** 2 **destination.port** 53 **ecs.version** 8.11.0 **event.action** network…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 97 **bytes_out** 223 **destination.bytes** 223 **destination.ip** 192.168.182.2 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** netw…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 97 **bytes_out** 211 **destination.bytes** 211 **destination.ip** 192.168.182.2 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** netw…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 194 **bytes_out** 428 **destination.bytes** 428 **destination.ip** 127.0.0.53 **destination.packets** 2 **destination.port** 53 **ecs.version** 8.11.0 **event.action** network…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 86 **bytes_out** 143 **destination.bytes** 143 **destination.ip** 192.168.182.2 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** netw…
Feb 8, 2025 @ 20:18:58.530	**@timestamp** Feb 8, 2025 @ 20:18:58.530 **agent.ephemeral_id** 2e96448e-1221-42b3-8ff2-920db25bab14 **agent.hostname** elk-host **agent.id** 73bf8532-58b5-4227-bbe0-2d3526c53a6c **agent.name** elk-host **agent.type** packetbeat **agent.version** 8.17.1 **bytes_in** 84 **bytes_out** 148 **destination.bytes** 148 **destination.ip** 127.0.0.53 **destination.packets** 1 **destination.port** 53 **ecs.version** 8.11.0 **event.action** network…

For example, we want to see the **ICPM** packet received:

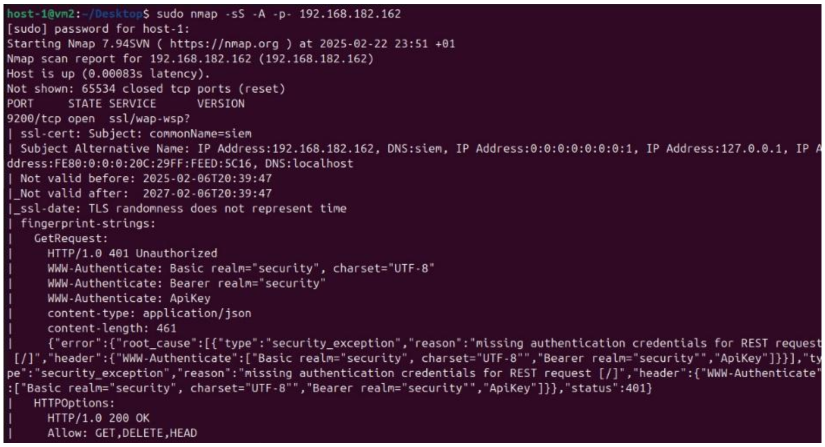


network.protocol : "icmp"

@timestamp	Summary
Feb 22, 2025 @ 22:34:58.067	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:58.067 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 49,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:57.042	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:57.042 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 40,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:56.018	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:56.018 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 42,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:54.994	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:54.994 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 33,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:53.970	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:53.970 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 34,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:52.947	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:52.947 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 40,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:51.923	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:51.923 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 40,000 event.end Feb 22, 2025 0…
Feb 22, 2025 @ 22:34:50.877	network.protocol icmp @timestamp Feb 22, 2025 @ 22:34:50.877 agent.ephemeral_id 82b9bddc-b8bc-40b9-91a7-95ed0490a639 agent.hostname elk-host agent.id 73bf8532-58b5-4227-bbe0-2d3526c53a6c agent.name elk-host agent.type packetbeat agent.version 8.17.1 bytes_in 56 bytes_out 56 client.bytes 56 client.ip 192.168.182.163 destination.bytes 56 destination.ip 192.168.182.162 ecs.version 8.11.0 event.category network event.dataset icmp event.duration 33,000 event.end Feb 22, 2025 0…

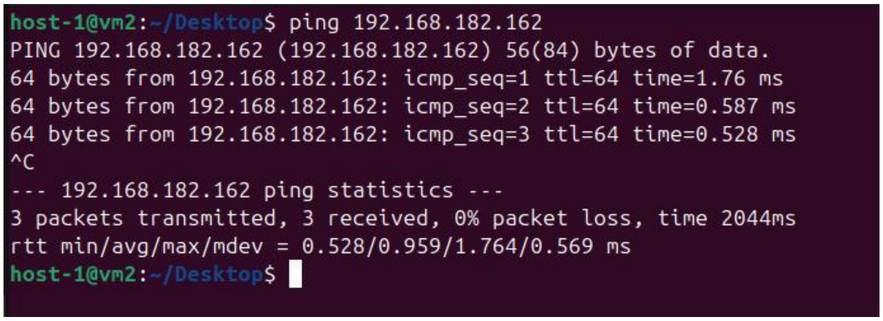
5. Generate Security Events

Conducted Nmap scans from one VM to another



```
host-1@vm2:~/Desktop$ sudo nmap -sS -A -p- 192.168.182.162
[sudo] password for host-1:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-22 23:51 +01
Nmap scan report for 192.168.182.162 (192.168.182.162)
Host is up (0.00083s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
9200/tcp open  ssl/wap-wsp?
| ssl-cert: Subject: commonName=siem
| Subject Alternative Name: IP Address:192.168.182.162, DNS:siem, IP Address:0:0:0:0:0:0:0:1, IP Address:127.0.0.1, IP A
ddress:FE80:0:0:0:20C:29FF:FEED:5C16, DNS:localhost
| Not valid before: 2025-02-06T20:39:47
|_Not valid after:  2027-02-06T20:39:47
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 401 Unauthorized
|     WWW-Authenticate: Basic realm="security", charset="UTF-8"
|     WWW-Authenticate: Bearer realm="security"
|     WWW-Authenticate: ApiKey
|     content-type: application/json
|     content-length: 461
|     {"error":{"root_cause":[{"type":"security_exception","reason":"missing authentication credentials for REST request
 [/]","header":{"WWW-Authenticate":["Basic realm="security", charset="UTF-8"","Bearer realm="security"","ApiKey"]}}],"ty
pe":"security_exception","reason":"missing authentication credentials for REST request [/]","header":{"WWW-Authenticate"
:["Basic realm="security", charset="UTF-8"","Bearer realm="security"","ApiKey"]}},"status":401}
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: GET,DELETE,HEAD
```

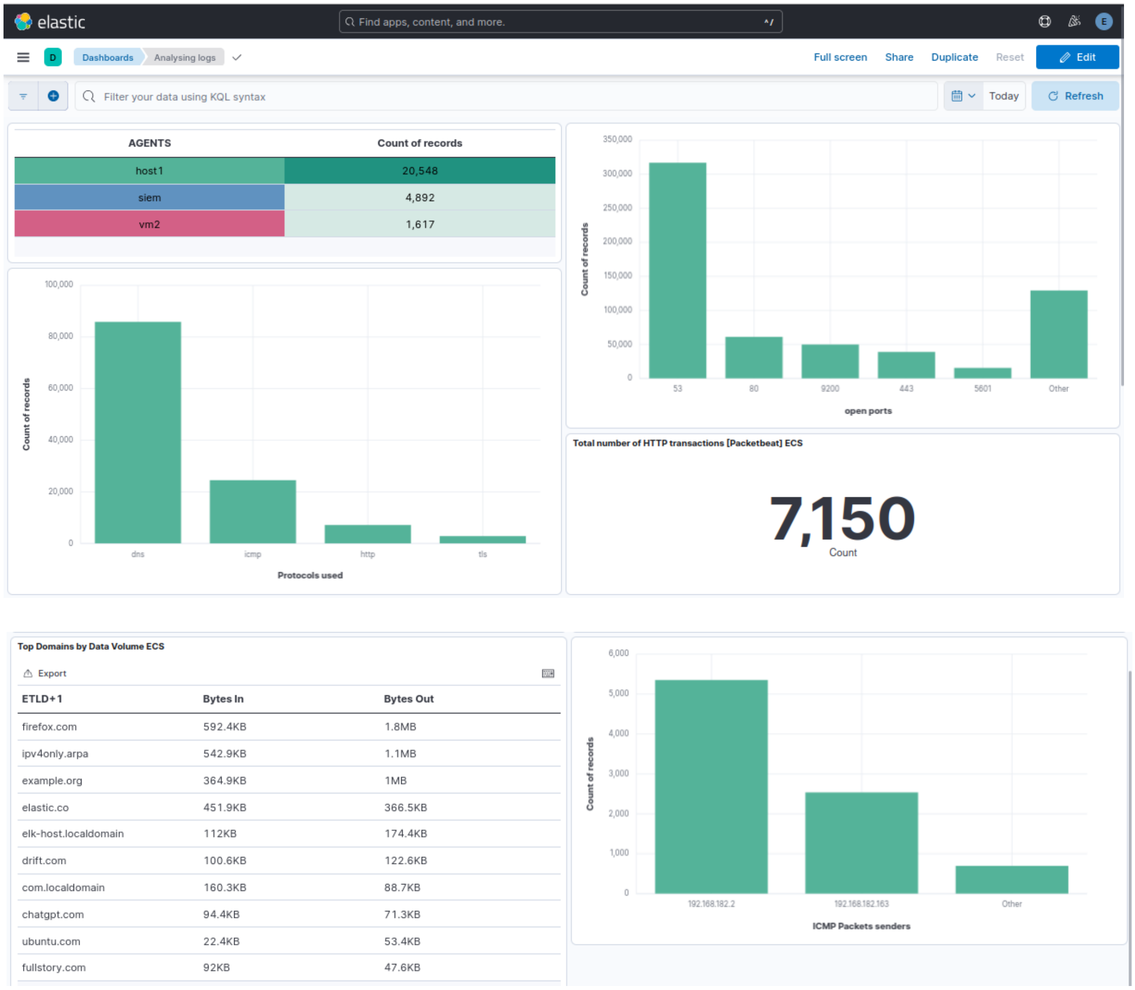
Sent ICMP packets from one VM to another



```
host-1@vm2:~/Desktop$ ping 192.168.182.162
PING 192.168.182.162 (192.168.182.162) 56(84) bytes of data.
64 bytes from 192.168.182.162: icmp_seq=1 ttl=64 time=1.76 ms
64 bytes from 192.168.182.162: icmp_seq=2 ttl=64 time=0.587 ms
64 bytes from 192.168.182.162: icmp_seq=3 ttl=64 time=0.528 ms
^C
--- 192.168.182.162 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2044ms
rtt min/avg/max/mdev = 0.528/0.959/1.764/0.569 ms
host-1@vm2:~/Desktop$ 
```

6. Create Dashboards using Kibana

Kibana is an advanced data visualization tool designed to transform complex datasets into interactive and insightful dashboards. As illustrated in the image, a **Kibana** dashboard effectively displays key metrics such as host-specific data, open ports, and protocol usage through various visualizations. These visualizations are instrumental in uncovering trends, detecting anomalies, and facilitating data-driven decision-making. With features like filtering, editing, and resetting, users can tailor their dashboards to gain deeper insights and enhance their analytical capabilities.



AGENTS	Count of records
host1	20,548
siem	4,892
vm2	1,617

Total number of HTTP transactions [Packetbeat] ECS

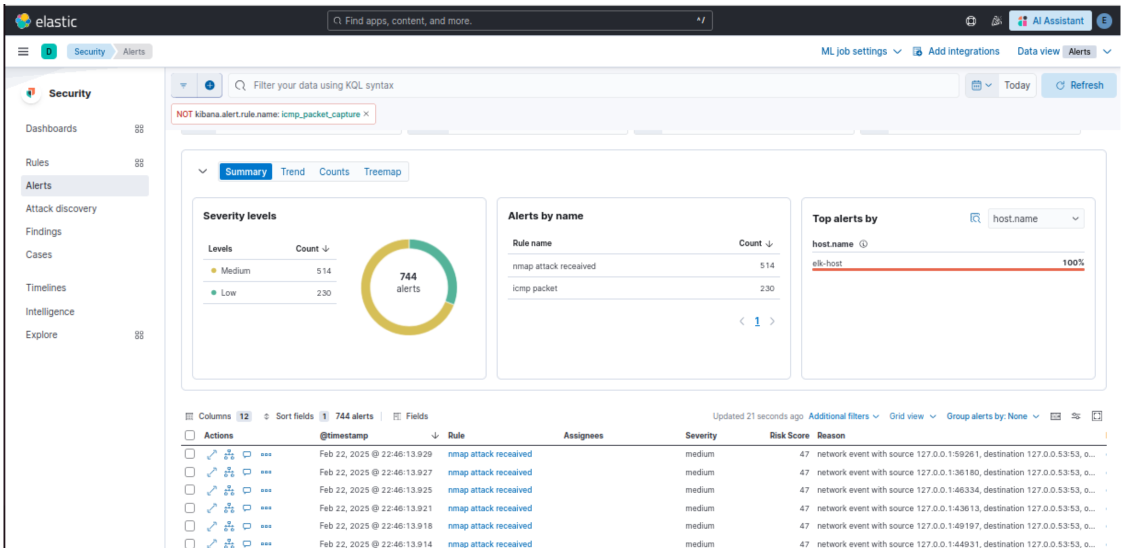
7,150
Count

Top Domains by Data Volume ECS

ETLD+1	Bytes In	Bytes Out
firefox.com	592.4KB	1.8MB
ipv4only.arpa	542.9KB	1.1MB
example.org	364.9KB	1MB
elastic.co	451.9KB	366.5KB
elk-host.localdomain	112KB	174.4KB
drift.com	100.6KB	122.6KB
com.localdomain	160.3KB	88.7KB
chatgpt.com	94.4KB	71.3KB
ubuntu.com	22.4KB	53.4KB
fullstory.com	92KB	47.6KB

7. Configure Alerts

In this section, we have established specific rules to generate alerts based on predefined conditions. For instance, an alert can be triggered whenever a host receives an **ICMP** packet or when an **NMAP** scan is detected targeting that host. These alerts are seamlessly integrated into the dashboard, allowing for real-time monitoring and immediate response to potential security events. This proactive approach enhances our ability to detect and mitigate threats efficiently, ensuring robust network security.



NOT kibana.alert.rule.name: icmp_packet_capture

Severity levels

Levels	Count
● Medium	514
● Low	230

Alerts by name

Rule name	Count
nmap attack receaived	514
icmp packet	230

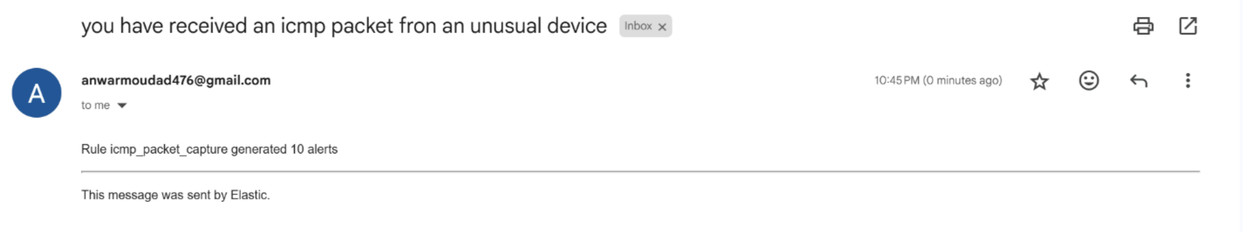
Top alerts by host.name

host.name	
elk-host	100%

Columns 12 · Sort fields 1 · 744 alerts · Fields · Updated 21 seconds ago · Additional filters · Grid view · Group alerts by: None

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
□	Feb 22, 2025 @ 22:46:13.929	nmap attack receaived		medium	47	network event with source 127.0.0.1:59261, destination 127.0.0.53:53, o...
□	Feb 22, 2025 @ 22:46:13.927	nmap attack receaived		medium	47	network event with source 127.0.0.1:36180, destination 127.0.0.53:53, o...
□	Feb 22, 2025 @ 22:46:13.925	nmap attack receaived		medium	47	network event with source 127.0.0.1:46334, destination 127.0.0.53:53, o...
□	Feb 22, 2025 @ 22:46:13.921	nmap attack receaived		medium	47	network event with source 127.0.0.1:43613, destination 127.0.0.53:53, o...
□	Feb 22, 2025 @ 22:46:13.918	nmap attack receaived		medium	47	network event with source 127.0.0.1:49197, destination 127.0.0.53:53, o...
□	Feb 22, 2025 @ 22:46:13.914	nmap attack receaived		medium	47	network event with source 127.0.0.1:44931, destination 127.0.0.53:53, o...

And we can receive these alerts via **email** (there are other options):

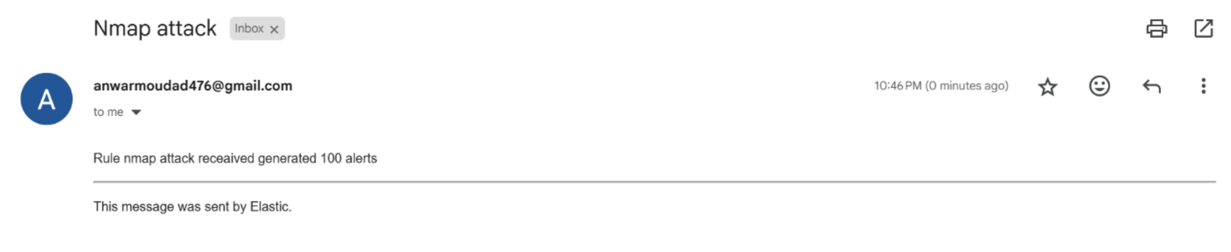


you have received an icmp packet fron an unusual device

anwarmoudad476@gmail.com
to me
10:45 PM (0 minutes ago)

Rule icmp_packet_capture generated 10 alerts

This message was sent by Elastic.



Nmap attack

anwarmoudad476@gmail.com
to me
10:46 PM (0 minutes ago)

Rule nmap attack receaived generated 100 alerts

This message was sent by Elastic.

5. Results

- Successfully configured and forwarded logs from the Ubuntu VM to the Elastic SIEM, ensuring seamless data integration and real-time monitoring.

- Implemented real-time detection of Nmap scans, with immediate email notifications triggered to alert the security team of potential reconnaissance activities.
- Developed a custom, user-friendly dashboard that provided clear and actionable insights into security events, simplifying the analysis process and enhancing decision-making.
- The project effectively showcased the critical role of SIEM systems in detecting, analyzing, and responding to security incidents within a controlled environment, highlighting its importance in maintaining robust cybersecurity defenses.

6. Conclusion

This project underscores the efficiency of the Elastic Stack as a comprehensive SIEM solution for monitoring and analyzing security events. The setup offered practical experience in log forwarding, querying, visualization, and alerting, demonstrating the stack's versatility. The addition of email notifications significantly improved the system's responsiveness, enabling swift action on potential security incidents.

7. Future Enhancements

- **Integrate Machine Learning with Elastic Stack**: Automate threat detection by leveraging machine learning algorithms to identify patterns and anomalies in real-time data.
- **Enhance Alerting Mechanisms**: Implement more sophisticated alerting rules and integrate with additional communication platforms like Slack or Microsoft Teams for broader team awareness.
- **Expand Data Sources**: Incorporate logs and metrics from a wider range of devices and applications, including cloud services and IoT devices, to provide a more comprehensive security overview.

- **Develop Custom Dashboards**: Create more specialized dashboards tailored to different roles within the organization, such as security analysts, to streamline their workflows and improve efficiency. Test these dashboards with real-world data and simulated attack scenarios to ensure they provide actionable insights and enhance situational awareness.