

Configuration Manual

MSc Research Project
MSc Cybersecurity

Sachin Radder
Student ID: x23305371

School of Computing
National College of Ireland

Supervisor: Prof. Kamil Mahajan

**National College of Ireland
Project Submission Sheet
School of Computing**



Student Name:	Sachin Radder
Student ID:	x23305371
Programme:	MSc Cybersecurity
Year:	2024-25
Module:	MSc Research Project
Supervisor:	Prof. Kamil Mahajan
Submission Due Date:	31/08/2025
Project Title:	Comparative study of IDS Solutions for Small and Medium Enterprises: A metric-focused Performance Study Identification
Word Count:	XXX
Page Count:	8

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Sachin Radder
Date:	31st August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Sachin Radder

x23305371

1 Introduction

This configuration manual documents the setup and deployment of three open-source IDS tools like Snort, Suricata, and Zeek in a virtualized environment. This was done with the objective of replicating a SME's network to make comparative analyses of intrusion detection and prevention capabilities. As a mimicking malicious traffic, a Kali Linux machine was applied in generating attack traffic (port scans, brute force attempts, SSH authentication) against Ubuntu-based IDS systems. Detection efficiency, resource consumption and integration ease were then measured with logs collected and compared.

The installation of Zeek was successful but was found to have limitations in configuration, notably in dependency management and integration with SIEM dashboards. This is observed as a limitation and one of the gaps in the research.

2 System Configuration

2.1 VirtualBox

The simulation of the test environment was carried out using VirtualBox on several VMs simulating attacker, IDS nodes and SIEM collector. To assure consistency in repeated tests, snapshots were taken.

2.2 Internet access on VMs

Internet connectivity was required for downloading and updating IDS systems on VM and for integration with ELK for logs and alerts creation which was hosted on cloud.

2.3 Operating Systems

- Kali Linux - Attacker machine (Nmap, hping3, Hydra)
- Ubuntu 22.04 LTS (Snort, Suricata, Zeek)

2.4 Virtual machine configurations

Parameter	Ubuntu IDS Nodes	Kali (Attacker)
OS Version	Ubuntu 22.04 LTS	Kali 2024.2
RAM	4 GB	4 GB
CPU	2 vCPU	1 vCPU
Disk	70 GB SSD	40 GB SSD
Network	NAT + Host Adapter	NAT + Host Adapter

Table 1: System Configurations of VMs

3 Tool Setup Overview

Tool	Deployment Type	Tested OS	Traffic Source
Snort	On-prem VM	Ubuntu	Kali-generated
Suricata	On-prem VM	Ubuntu	Kali-generated
Zeek	On-prem VM	Ubuntu	Kali-generated

Table 2: IDS/IPS Tools Setup overview

4 Configuration Steps

4.1 Snort (Signature-based IDS)

4.1.1 Environment

- Installed Snort 2.9 on Ubuntu via source packages.

4.1.2 Steps

- Installed Depends (libpcap-dev, libpcre3-dev, etc.)
- Built Snort from source.
- Configured /etc/snort/snort.conf with community rules.
- Traffic in enp0s8 was captured and Nmap scans, and other traffic were sent for test from Kali.

4.1.3 Verification

- Alerts on attempts for port scanning, ICMP flooding and SSH authentication attempts.
- The logs are written on to /var/log/snort/alert.

```

root@root1404:/# systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
   Loaded: loaded (/etc/init.d/snort; generated)
   Active: active (running) since Thu 2025-08-28 11:07:25 UTC; 31min ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 4 (limit: 3426)
   Memory: 138.6M
      CPU: 2.706s
   CGroup: /system.slice/snort.service
           └─3622 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --pid-path /run/snort/ -c /etc/snort/snort.conf -S "\"HOME_NET=[192.168.
           └─3644 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --pid-path /run/snort/ -c /etc/snort/snort.conf -S "\"HOME_NET=[192.168.
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: appid Version 1.1 <Build 5>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Aug 28 11:07:25 root1404 snort[3644]: Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Aug 28 11:07:25 root1404 snort[3644]: Commencing packet processing (pid=3644)

```

Fig 1: The screenshot shows snort running on the VM

```

root@root1404:/# sudo snort -q -l /var/log/snort -t enp0s8 -A console -c /etc/snort/snort.conf
08/28-11:25:37.237679 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:37.249858 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:37.294209 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:37.424262 [[*]] [1:5421:1] ICMP Traffic Detected [[*]] [Priority: 0] {ICMP} 192.168.56.10 -> 192.168.56.105
08/28-11:25:37.424380 [[*]] [1:5421:1] ICMP Traffic Detected [[*]] [Priority: 0] {ICMP} 192.168.56.105 -> 192.168.56.10
08/28-11:25:38.251966 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:38.278492 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:38.292419 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:38.309989 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:38.425451 [[*]] [1:5421:1] ICMP Traffic Detected [[*]] [Priority: 0] {ICMP} 192.168.56.10 -> 192.168.56.105
08/28-11:25:38.425492 [[*]] [1:5421:1] ICMP Traffic Detected [[*]] [Priority: 0] {ICMP} 192.168.56.105 -> 192.168.56.10
08/28-11:25:39.275358 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:39.320066 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:39.331794 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:39.357662 [[*]] [1:123:1] SSH Authentication Attempt Detected [[*]] [Priority: 0] {TCP} 192.168.56.1:60968 -> 192.168.56.105:22
08/28-11:25:39.425953 [[*]] [1:5421:1] ICMP Traffic Detected [[*]] [Priority: 0] {ICMP} 192.168.56.10 -> 192.168.56.105
08/28-11:25:39.425987 [[*]] [1:5421:1] ICMP Traffic Detected [[*]] [Priority: 0] {ICMP} 192.168.56.105 -> 192.168.56.10

```

Fig 2: The screenshot shows snort capturing logs for custom rules set

```

$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.

alert icmp any any -> $HOME_NET any (msg: "ICMP Traffic Detected"; sid: 5421; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg: "SSH Authentication Attempt Detected"; sid: 123; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg: "Command Execution Attempt"; content:"GET"; content:"/etc/passwd"; sid:100003;)

```

Fig 3: The screenshot shows custom rules set for traffic detection

4.2 Suricata (Signature + Protocol Analysis IDS)

4.2.1 Environment

- Installed Suricata from PPA

4.2.2 Steps

- Installation package Suricata - apt install suricata.
- Configured suricata.yaml with custom ruleset.
- Kali simulated SYN flood and Hydra simulated SSH brute force with used hping3.

4.2.3 Verification

- Suricata produced eve.json alerts that are highly detailed (protocol metadata).
- Logs sent over Filebeat to be analyzed.

```
root@root1404:/home/root1404# sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS/NSM/FW daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-08-28 23:15:29 UTC; 11s ago
     Docs: man:suricata(8)
           man:suricata-sc(8)
           https://suricata.io/documentation/
   Process: 38340 ExecStartPre=/bin/rm -f /run/suricata.pid (code=exited, status=0/SUCCESS)
   Main PID: 38341 (Suricata-Main)
    Tasks: 8 (limit: 3426)
   Memory: 36.0M
      CPU: 604ms
   CGroup: /system.slice/suricata.service
           └─38341 /usr/bin/suricata --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid --user suricata --group suricata

Aug 28 23:15:29 root1404 systemd[1]: Starting Suricata IDS/IPS/NSM/FW daemon...
Aug 28 23:15:29 root1404 systemd[1]: Started Suricata IDS/IPS/NSM/FW daemon.
Aug 28 23:15:29 root1404 suricata[38341]: i: suricata: This is Suricata version 8.0.0 RELEASE running in SYSTEM mode
Aug 28 23:15:29 root1404 suricata[38341]: i: mpm-hs: Rule group caching - loaded: 2 newly cached: 0 total cacheable: 2
Aug 28 23:15:29 root1404 suricata[38341]: i: threads: Threads created -> W: 2 FM: 1 FR: 1 Engine started.
```

Figure 1: The screenshot shows suricata running on the VM

```
root@root1404:/var/log/suricata# tail -f fast.log
08/28/2025-23:14:09.099265  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:09.293936  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:09.335900  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:09.488844  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:09.531646  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:10.112984  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:10.117076  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:10.120907  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:10.129757  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:14:10.458241  [**] [1:1000001:1] SSH Authentication Attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 19
2.168.56.1:52699 -> 192.168.56.105:22
08/28/2025-23:32:44.189675  [**] [1:123:1] ICMP Alert [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.56.10:8 -> 192.168.56.105:0
08/28/2025-23:32:44.189675  [**] [1:1234:1] NMAP ping Sweep Scan Detected [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.56.10:8 -> 192.168.56.105
:0
```

Fig 2: The screenshot shows suricata capturing logs for custom rules set

```
root@root1404:/etc/suricata/rules# cat local.rules
alert icmp any any -> $HOME_NET any ( msg: "ICMP Alert"; sid:123; rev:1;)
alert icmp any any -> 192.168.56.105 any (msg: "NMAP ping Sweep Scan Detected"; sid:1234; rev:1;)
alert tcp any any -> 192.168.56.105 22 (msg:"SSH Authentication Attempt"; sid:1000001; rev:1; flow:to_server,established; classtype:attempted-admin;)
alert tcp any any -> any 80 (msg:"Access to Suspicious Website"; content:"example.com"; sid:1000002; rev:1; http_host;)
alert tcp any any -> any 21 (msg:"FTP Login Attempt"; sid:1000005; rev:1; content:"USER"; nocase;)
```

Fig 3: The screenshot shows custom rules set for traffic detection

4.3 Zeek (Anomaly-based IDS)

4.3.1 Environment

- Installed Zeek from source (/usr/local/zeek)

4.3.2 Steps

- Compiled ./configure and make and make install.
- Ran test with Zeek -i enp0s8 local.
- Some dependency and log parsing problems were experienced when integrating with SIEM.

4.3.3 Limitations

- Zeekctl needs to be setup manually tuned.
- Integration with ELK is not straightforward while pulling logs.

```
Unpacking zeek-core-dev (8.0.1-0) ...
dpkg: error processing archive /tmp/apt-dpkg-install-Q0FZrg/3-zeek-core-dev_8.0.1-0_amd64.deb (--unpack):
 trying to overwrite '/opt/zeek/bin/bifcl', which is also in package zeek-8.0-core-dev 8.0.1-0
No apport report written because MaxReports is reached already
dpkg-deb: error: paste subprocess was killed by signal (Broken pipe)
Preparing to unpack .../4-zeek-spicy-dev_8.0.1-0_amd64.deb ...
Unpacking zeek-spicy-dev (8.0.1-0) ...
dpkg: error processing archive /tmp/apt-dpkg-install-Q0FZrg/4-zeek-spicy-dev_8.0.1-0_amd64.deb (--unpack):
 trying to overwrite '/opt/zeek/bin/hilti-config', which is also in package zeek-8.0-spicy-dev 8.0.1-0
No apport report written because MaxReports is reached already
dpkg-deb: error: paste subprocess was killed by signal (Broken pipe)
Preparing to unpack .../5-zeek-btest_8.0.1-0_all.deb ...
Unpacking zeek-btest (8.0.1-0) ...
dpkg: error processing archive /tmp/apt-dpkg-install-Q0FZrg/5-zeek-btest_8.0.1-0_all.deb (--unpack):
 trying to overwrite '/opt/zeek/bin/btest', which is also in package zeek-8.0-btest 8.0.1-0
No apport report written because MaxReports is reached already
Preparing to unpack .../6-zeek-btest-data_8.0.1-0_all.deb ...
Unpacking zeek-btest-data (8.0.1-0) ...
dpkg: error processing archive /tmp/apt-dpkg-install-Q0FZrg/6-zeek-btest-data_8.0.1-0_all.deb (--unpack):
 trying to overwrite '/opt/zeek/share/btest/data/Scripts/README', which is also in package zeek-8.0-btest-data 8.0.1-0
No apport report written because MaxReports is reached already
dpkg-deb: error: paste subprocess was killed by signal (Broken pipe)
Preparing to unpack .../7-zeek-zkg_8.0.1-0_all.deb ...
Unpacking zeek-zkg (8.0.1-0) ...
dpkg: error processing archive /tmp/apt-dpkg-install-Q0FZrg/7-zeek-zkg_8.0.1-0_all.deb (--unpack):
 trying to overwrite '/opt/zeek/bin/zkg', which is also in package zeek-8.0-zkg 8.0.1-0
No apport report written because MaxReports is reached already
Preparing to unpack .../8-zeek-client_8.0.1-0_all.deb ...
Unpacking zeek-client (8.0.1-0) ...
dpkg: error processing archive /tmp/apt-dpkg-install-Q0FZrg/8-zeek-client_8.0.1-0_all.deb (--unpack):
 trying to overwrite '/opt/zeek/bin/zeek-client', which is also in package zeek-8.0-client 8.0.1-0
No apport report written because MaxReports is reached already
Errors were encountered while processing:
 /tmp/apt-dpkg-install-Q0FZrg/0-zeek-core_8.0.1-0_amd64.deb
 /tmp/apt-dpkg-install-Q0FZrg/1-zeekctl_8.0.1-0_amd64.deb
 /tmp/apt-dpkg-install-Q0FZrg/2-libbroker-dev_8.0.1-0_amd64.deb
 /tmp/apt-dpkg-install-Q0FZrg/3-zeek-core-dev_8.0.1-0_amd64.deb
 /tmp/apt-dpkg-install-Q0FZrg/4-zeek-spicy-dev_8.0.1-0_amd64.deb
 /tmp/apt-dpkg-install-Q0FZrg/5-zeek-btest_8.0.1-0_all.deb
 /tmp/apt-dpkg-install-Q0FZrg/6-zeek-btest-data_8.0.1-0_all.deb
 /tmp/apt-dpkg-install-Q0FZrg/7-zeek-zkg_8.0.1-0_all.deb
 /tmp/apt-dpkg-install-Q0FZrg/8-zeek-client_8.0.1-0_all.deb
needrestart is being skipped since dpkg has failed
E: Sub-process /usr/bin/dpkg returned an error code (1)
```

Fig 1: Zeek Installation failed due to multiple errors which were tried to fix but never got fixed due to broken dependencies

4.4 Elastic Cloud

4.4.1 Environment

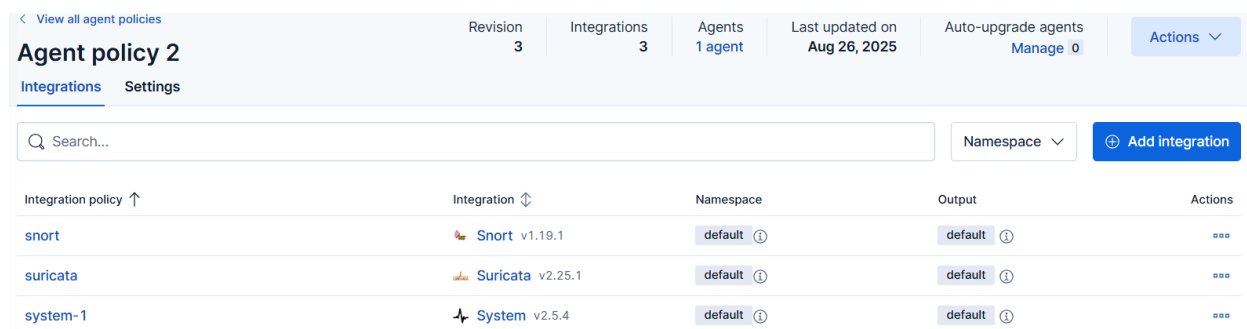
- Elastic cloud was installed to pull the logs, and a free trial version was being used.

4.4.2 Steps

- Registered account on Elastic cloud platform with MFA.
- Downloaded Agents to Ubuntu machine where logs of IDS tools are collected.
- In Kibana → Fleet → Agent Policies → Add Integration for IDS systems
- Added the below integrations:
 - 1) Suricata Integration: Automatically parsed eve.json logs.
 - 2) Zeek Integration: Monitored conn.log, dns.log, and http.log.
 - 3) Custom Logs Integration: For Snort alerts (/var/log/snort/alert).
- Verified the logs are pulled to the Elastic cloud.
- Created alerts and cases rule for malicious traffic which is being detected.

4.4.3 Verification

- Suricata dashboards filled with events of attacks (port scan, brute force).
- Under custom logs index, Snort alerts were shown.
- The timestamps confirmed the significant delay in traffic being logged.



The screenshot shows the 'Agent policy 2' configuration page in Kibana. At the top, there are tabs for 'Integrations' and 'Settings', with 'Integrations' selected. Below the tabs is a search bar and a 'Namespace' dropdown. The main table lists the integrations for this policy:

Integration policy ↑	Integration ⇅	Namespace	Output	Actions
snort	Snort v1.19.1	default ⓘ	default ⓘ	...
suricata	Suricata v2.25.1	default ⓘ	default ⓘ	...
system-1	System v2.5.4	default ⓘ	default ⓘ	...

Fig 1: Snort and Suricata Integration added to Agent policy

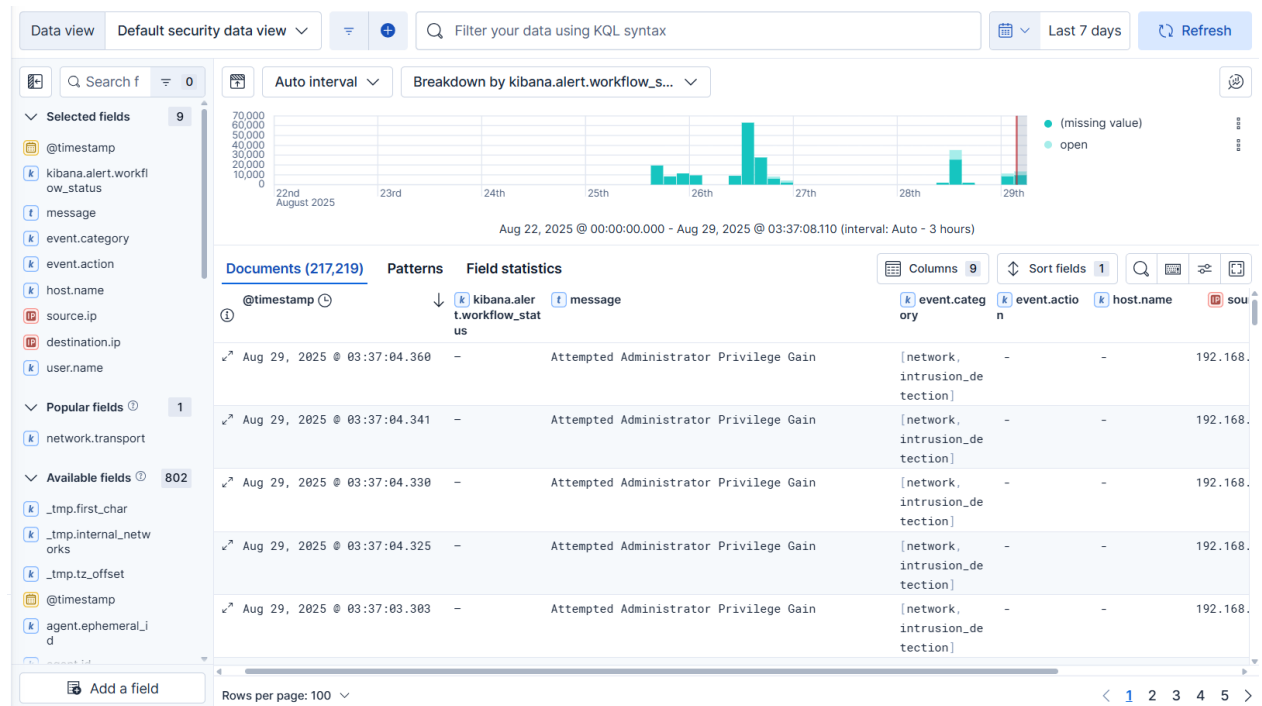


Fig 2: Logs getting populated in Elastic cloud

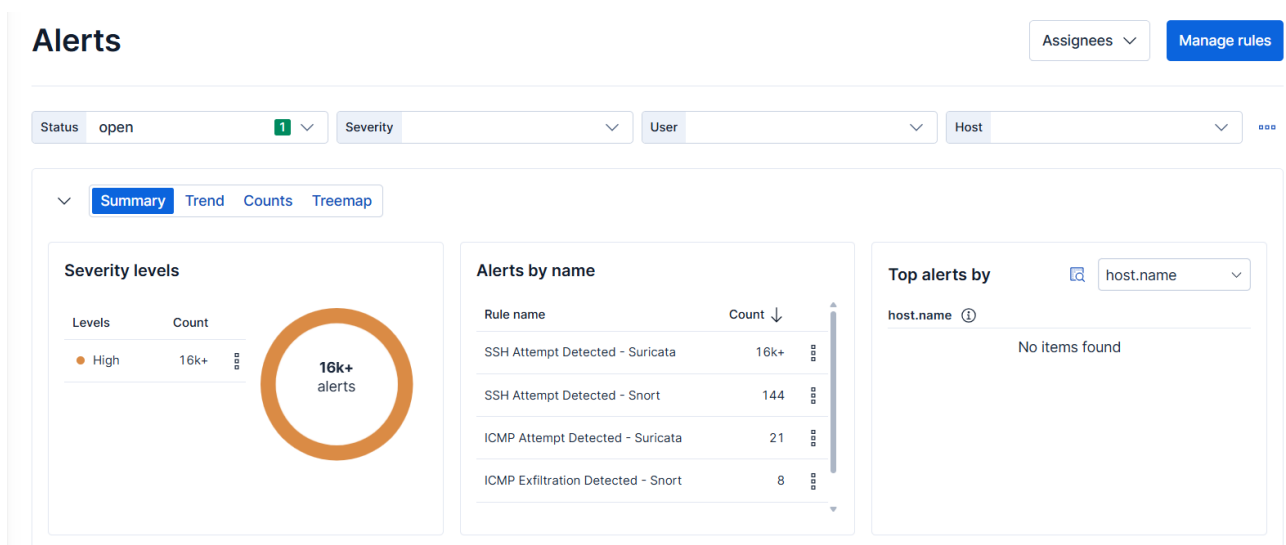


Fig 3: Alert rules are made to correlate logs which are getting populated

5 Tool Results

5.1 MTTD and MTTR Metrics

Tool	Test Type	Action Time	MTTD (Time)	MTTD (sec)	MTTR Time (Alert Creation)	MTTR (sec)
Snort	ICMP Traffic	29/08/2025 3:52:00 PM	15:52:24	24	15:53:18	54
	SSH Attempt	29/08/2025 3:53:00 PM	15:53:30	30	15:54:23	53
	Command Execution	29/08/2025 3:55:00 PM	15:55:21	21	15:56:05	44
Suricata	ICMP Traffic	29/8/2025 12:38:00 PM	12:38:35	35	12:39:42	67
	SSH Attempt	26/8/2025 03:53:00 AM	3:54:35	35	3:55:23	48
	NMAP Scan Detected	29/8/2025 12:54:00 PM	12:54:19	19	12:55:10	70

Table 3: MTTD and MTTR across IDS Tools

5.2 Resource Utilization Comparison

Tool	OS	CPU Usage	Memory Usage	Agent Disk Size
Snort	Ubuntu	10%	102.9 MB	51 MB
Suricata	Ubuntu	8%	67.9 MB	214 MB

Table 4: IDS tool Resource Utilization

References

Ahmet Aytemiz (2024). *How to Install and Configure Suricata on Ubuntu*. [online] Letsdefend.io. Available at: <https://letsdefend.io/blog/how-to-install-and-configure-suricata-on-ubuntu>.

Ahmet Numan Aytemiz (2024). *How to Install and Configure Snort on Ubuntu*. [online] Letsdefend.io. Available at: <https://letsdefend.io/blog/how-to-install-and-configure-snort-on-ubuntu>.

Kali (2025). *Kali Tools / Kali Linux Tools*. [online] Kali Linux. Available at: <https://www.kali.org/tools/>.

Oracle (2023). *Oracle VM VirtualBox*. [online] VirtualBox. Available at: <https://www.virtualbox.org/>.

Snort (2019). *Snort - Network Intrusion Detection & Prevention System*. [online] Snort.org.

Available at: <https://www.snort.org/>.

Suricata (2024). *Home*. [online] Suricata. Available at: <https://suricata.io/>.

Zeek (2024). *The Zeek Network Security Monitor*. [online] Zeek. Available at: <https://zeek.org/>.