Design and Implementation of a Mini Security Operations Center (SOC) Using Suricata and Splunk

Project Overview

Modern Security Operations Centers (SOCs) rely on continuous visibility into network activity, centralized log analysis, and structured incident response workflows. The objective of this project was to design and implement a mini SOC environment capable of detecting, analyzing, and responding to network-based threats using open-source security tools.

Objective:

The objective of this project was to design and implement a functional mini SOC environment capable of detecting, analyzing, and responding to network-based threats using open-source tools.

Scope:

This project focuses on:

- Network intrusion detection
- Log forwarding and SIEM ingestion
- Threat analysis and visualization
- Incident response classification

Goal:

Detect, visualize, and investigate malicious network activity using IDS + SIEM.

- Suricata detects malicious traffic
- Logs forwarded to Splunk
- Custom dashboards and alerts
- Simulated attacks detected

- SOC investigation walkthrough

PROJECT ARCHITECTURE

Attacker Activity (Nmap Scan)

↓

Suricata IDS (Kali Linux)

↓

Suricata Logs (JSON / Alerts)

↓

Splunk Universal Forwarder

↓

Splunk Enterprise (Windows Host)

↓

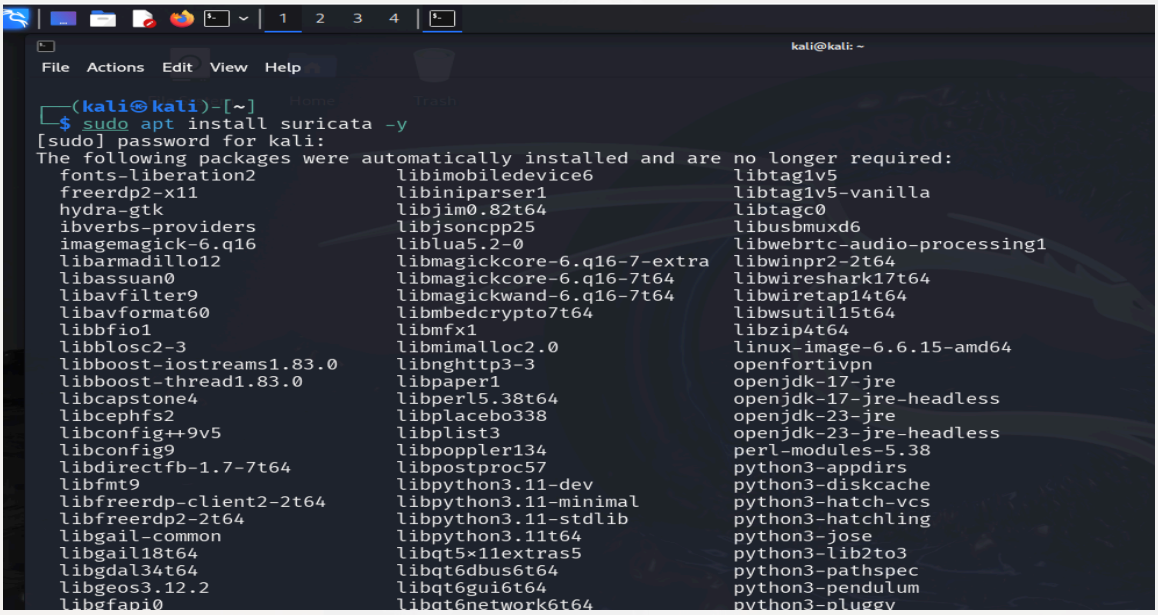
Detection, Analysis, Dashboards, Response Classification

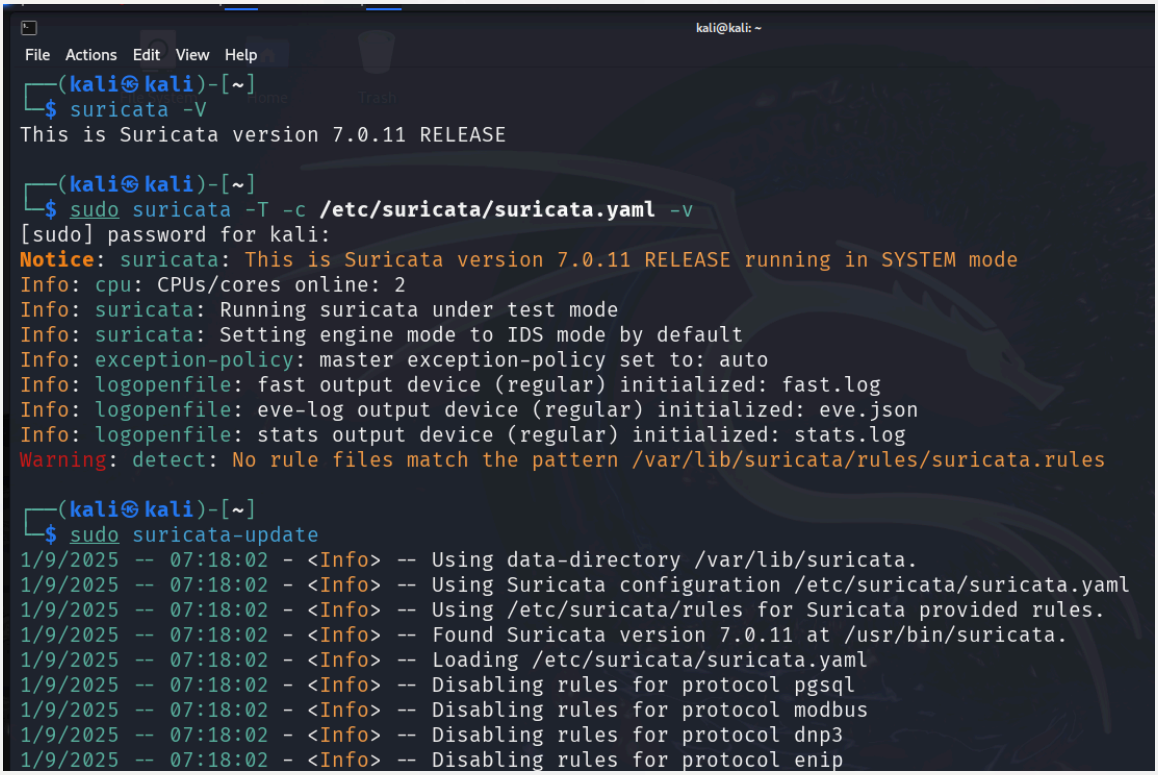
Implementation and Configuration

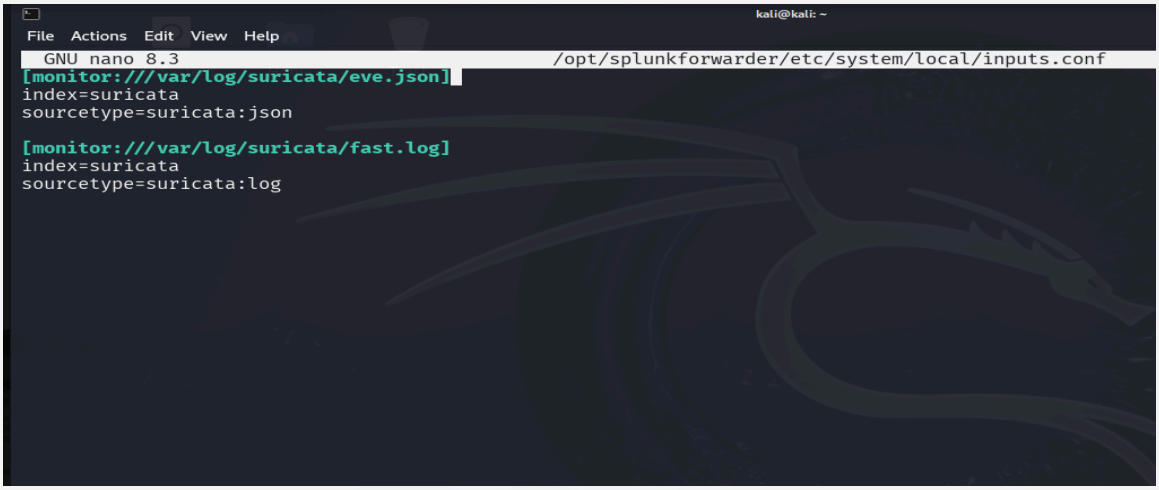
Suricata Deployment

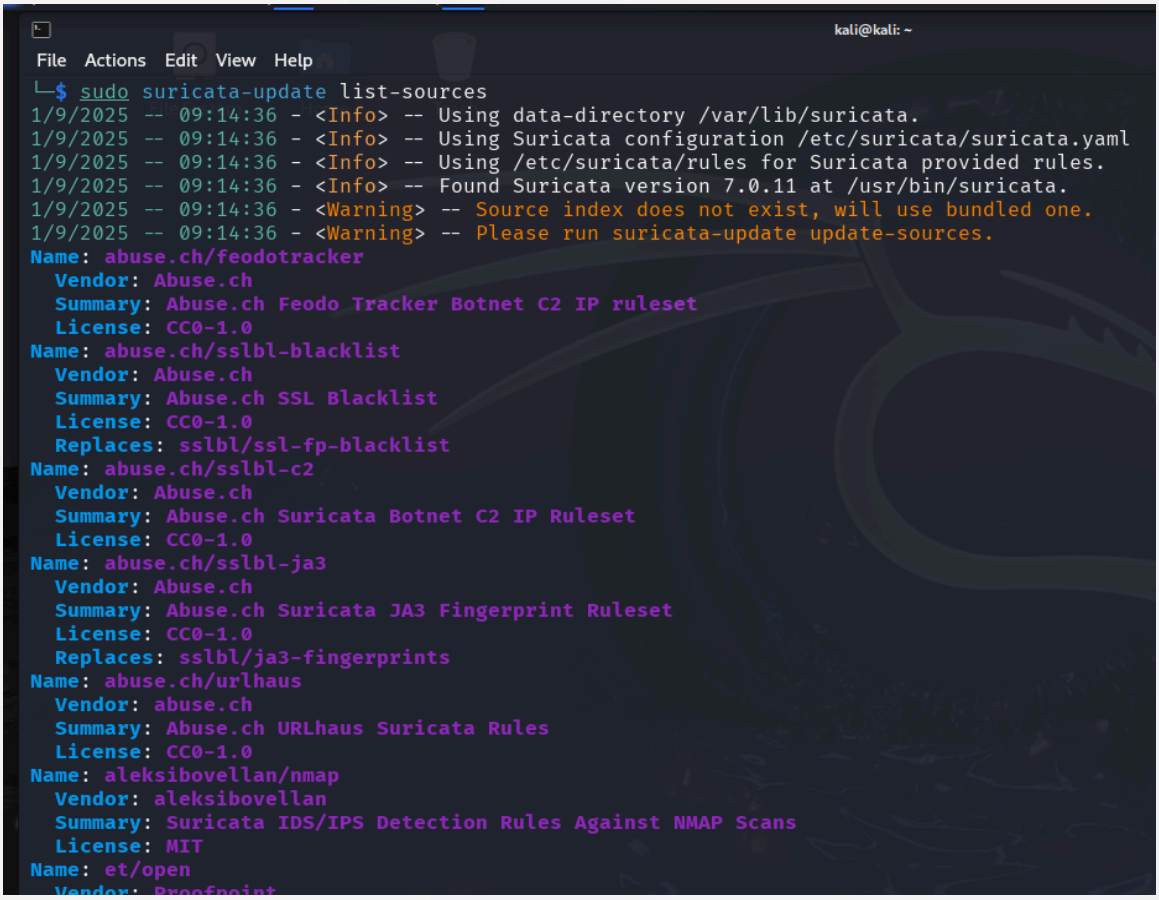
Suricata was installed and configured on the Kali Linux virtual machine to operate in IDS mode. The monitored network interface was specified in the Suricata configuration file, and JSON logging was enabled to ensure compatibility with SIEM ingestion.

After deployment, Suricata was tested to confirm it was actively monitoring traffic and generating alerts.


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo apt install suricata -y
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
fonts-liberation2 libimobiledevice6 libtag1v5
freerdp2-x11 libiniparser1 libtag1v5-vanilla
hydra-gtk libjim0.82t64 libtagc0
ibverbs-providers libjsoncpp25 libusbmuxd6
imagemagick-6.q16 liblua5.2-0 libwebrtc-audio-processing1
libarmadillo12 libmagickcore-6.q16-7-extra libwinpr2-2t64
libassuan0 libmagickcore-6.q16-7t64 libwireshark17t64
libavfilter9 libmagickwand-6.q16-7t64 libwiretap14t64
libavformat60 libmbedcrypto7t64 libwsutil15t64
libbfio1 libmfx1 libzip4t64
libblosc2-3 libmimalloc2.0 linux-image-6.6.15-amd64
libboost-iostreams1.83.0 libnghttp3-3 openfortivpn
libboost-thread1.83.0 libpaper1 openjdk-17-jre
libcapstone4 libperl5.38t64 openjdk-17-jre-headless
libcephfs2 libplacebo338 openjdk-23-jre
libconfig++9v5 libplist3 openjdk-23-jre-headless
libconfig9 libpoppler134 perl-modules-5.38
libdirectfb-1.7-7t64 libpostproc57 python3-appdirs
libfmt9 libpython3.11-dev python3-diskcache
libfreerdp-client2-2t64 libpython3.11-minimal python3-hatch-vcs
libfreerdp2-2t64 libpython3.11-stdlib python3-hatchling
libgail-common libpython3.11t64 python3-jose
libgail18t64 libqt5x11extras5 python3-lib2to3
libgdal34t64 libqt6dbus6t64 python3-pathspec
libgeos3.12.2 libqt6gui6t64 python3-pendulum
libgfapi0 libqt6network6t64 python3-pluggy

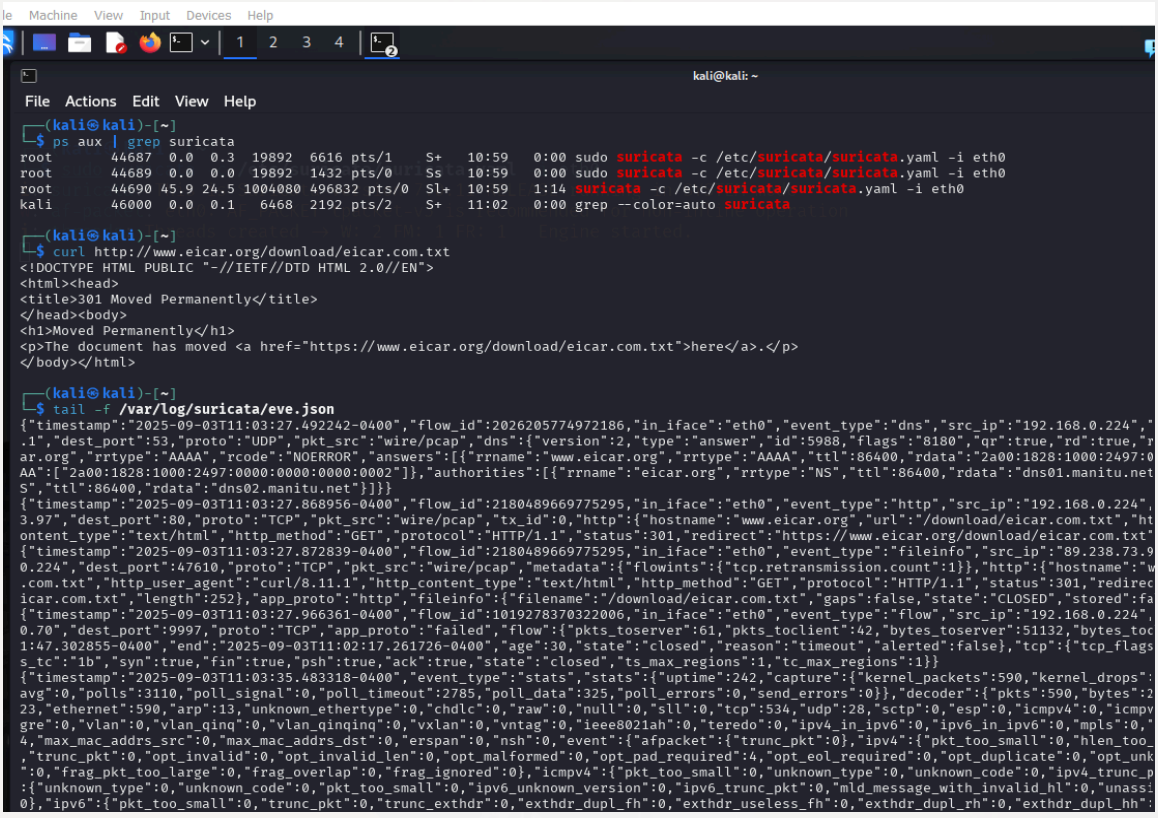

kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ suricata -V
This is Suricata version 7.0.11 RELEASE
┌──(kali㉿kali)-[~]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
[sudo] password for kali:
Notice: suricata: This is Suricata version 7.0.11 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 2
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Warning: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
┌──(kali㉿kali)-[~]
└─$ sudo suricata-update
1/9/2025 -- 07:18:02 - <Info> -- Using data-directory /var/lib/suricata.
1/9/2025 -- 07:18:02 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
1/9/2025 -- 07:18:02 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
1/9/2025 -- 07:18:02 - <Info> -- Found Suricata version 7.0.11 at /usr/bin/suricata.
1/9/2025 -- 07:18:02 - <Info> -- Loading /etc/suricata/suricata.yaml
1/9/2025 -- 07:18:02 - <Info> -- Disabling rules for protocol pgsql
1/9/2025 -- 07:18:02 - <Info> -- Disabling rules for protocol modbus
1/9/2025 -- 07:18:02 - <Info> -- Disabling rules for protocol dnp3
1/9/2025 -- 07:18:02 - <Info> -- Disabling rules for protocol enip

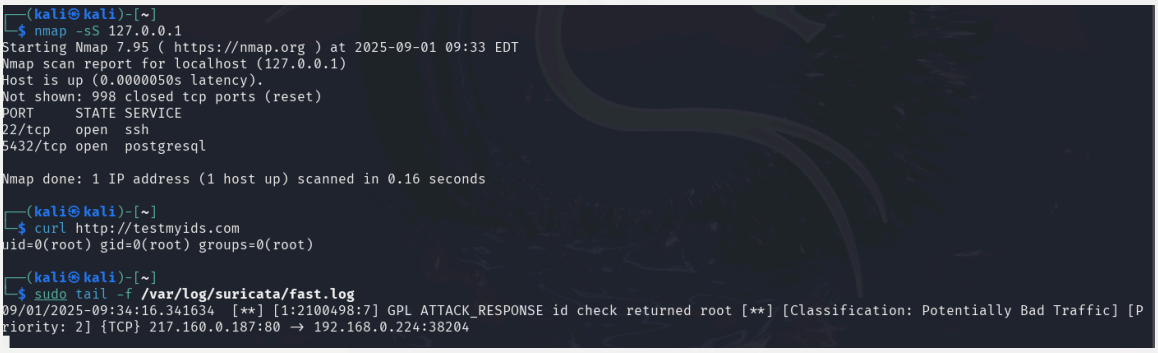

kali@kali: ~
File Actions Edit View Help
GNU nano 8.3 /opt/splunkforwarder/etc/system/local/inputs.conf
[monitor:///var/log/suricata/eve.json]
index=suricata
sourcetype=suricata:json
[monitor:///var/log/suricata/fast.log]
index=suricata
sourcetype=suricata:log


kali@kali: ~
File Actions Edit View Help
└─$ sudo suricata-update list-sources
1/9/2025 -- 09:14:36 - <Info> -- Using data-directory /var/lib/suricata.
1/9/2025 -- 09:14:36 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
1/9/2025 -- 09:14:36 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
1/9/2025 -- 09:14:36 - <Info> -- Found Suricata version 7.0.11 at /usr/bin/suricata.
1/9/2025 -- 09:14:36 - <Warning> -- Source index does not exist, will use bundled one.
1/9/2025 -- 09:14:36 - <Warning> -- Please run suricata-update update-sources.
Name: abuse.ch/feodotracker
Vendor: Abuse.ch
Summary: Abuse.ch Feodo Tracker Botnet C2 IP ruleset
License: CC0-1.0
Name: abuse.ch/sslbl-blacklist
Vendor: Abuse.ch
Summary: Abuse.ch SSL Blacklist
License: CC0-1.0
Replaces: sslbl/ssl-fp-blacklist
Name: abuse.ch/sslbl-c2
Vendor: Abuse.ch
Summary: Abuse.ch Suricata Botnet C2 IP Ruleset
License: CC0-1.0
Name: abuse.ch/sslbl-ja3
Vendor: Abuse.ch
Summary: Abuse.ch Suricata JA3 Fingerprint Ruleset
License: CC0-1.0
Replaces: sslbl/ja3-fingerprints
Name: abuse.ch/urlhaus
Vendor: abuse.ch
Summary: Abuse.ch URLhaus Suricata Rules
License: CC0-1.0
Name: aleksibovellan/nmap
Vendor: aleksibovellan
Summary: Suricata IDS/IPS Detection Rules Against NMAP Scans
License: MIT
Name: et/open

```
┌──(kali㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.11 RELEASE running in SYSTEM mode
W: af-packet: eth0: AF_PACKET tpacket-v3 is recommended for non-inline operation
i: threads: Threads created → W: 2 FM: 1 FR: 1   Engine started.
```

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-09-01 09:20:05 EDT; 12min ago
 Invocation: a611c606f01748268a799a4e30f3f1bb
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 6383 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suric
   Main PID: 6392 (Suricata-Main)
      Tasks: 8 (limit: 2218)
     Memory: 479.4M (peak: 481.1M)
        CPU: 1min 42.945s
     CGroup: /system.slice/suricata.service
             └─6392 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid

Sep 01 09:20:04 kali systemd[1]: Starting suricata.service - Suricata IDS/IDP daemon...
Sep 01 09:20:04 kali suricata[6383]: i: suricata: This is Suricata version 7.0.11 RELEASE running in SYSTEM mode
Sep 01 09:20:05 kali systemd[1]: Started suricata.service - Suricata IDS/IDP daemon.
lines 1-18/18 (END)
```

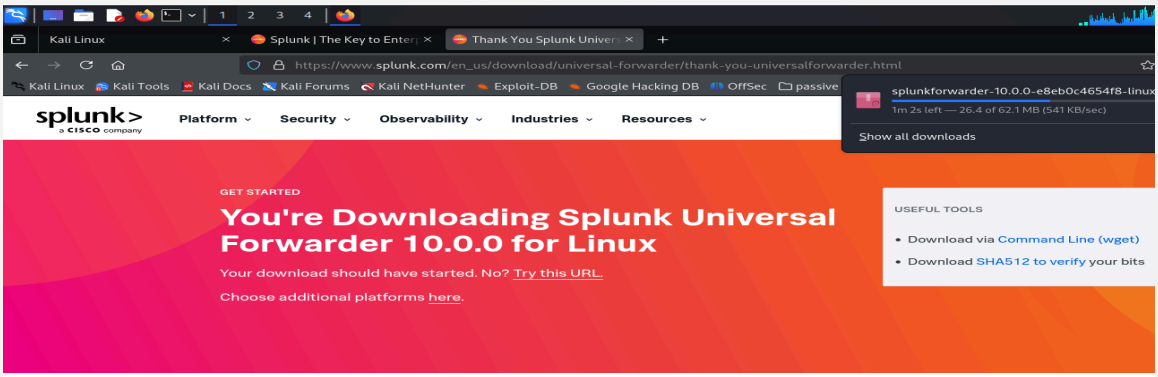




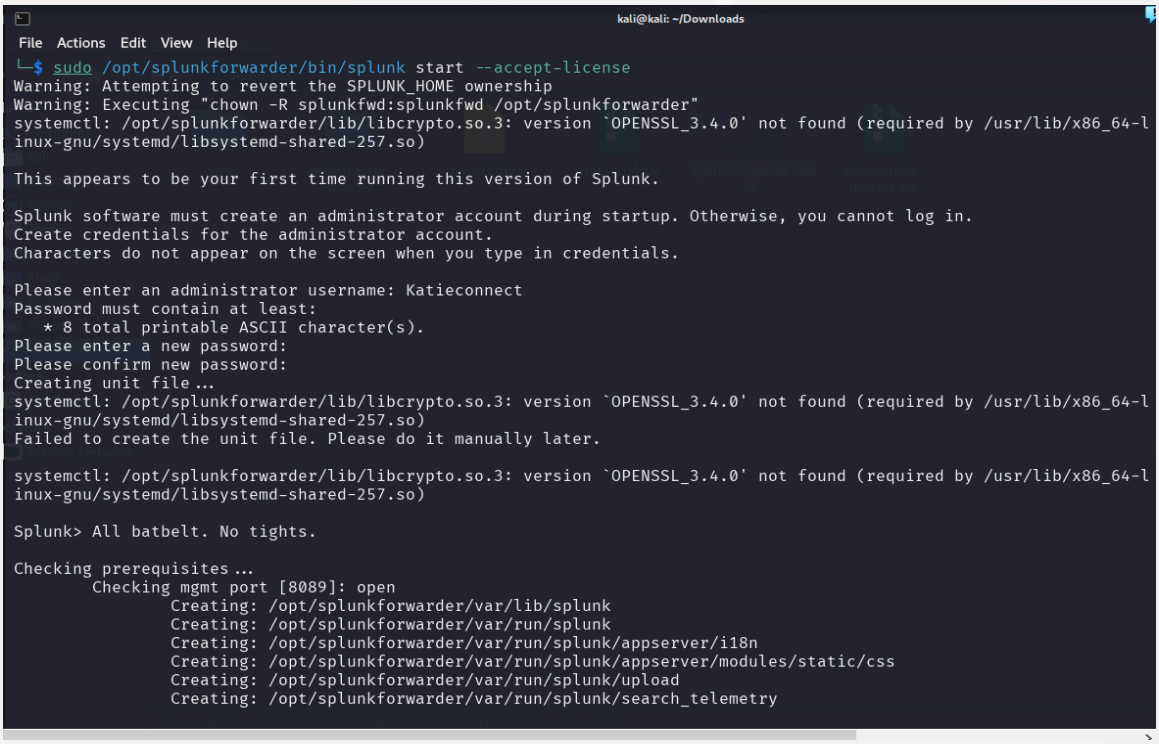
1. Log Forwarding Configuration

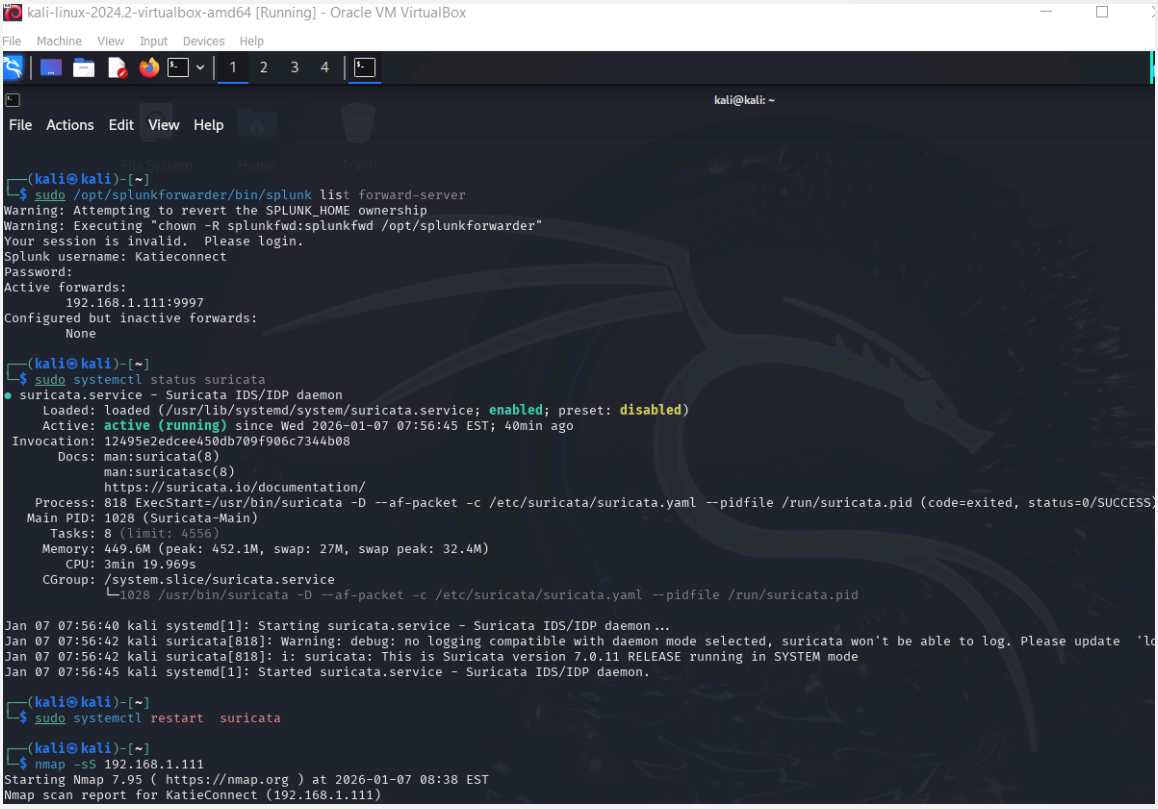
To centralize alert analysis, the Splunk Universal Forwarder was installed on the Kali Linux system. The forwarder was configured to monitor Suricata log files and forward them to the Splunk Enterprise instance running on the Windows host.

Connectivity between the forwarder and the SIEM was verified to ensure logs were successfully transmitted and indexed.




```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i splunkforwarder.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 461404 files and directories currently installed.)
Preparing to unpack splunkforwarder.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunkforwarder (10.0.0) ...
Setting up splunkforwarder (10.0.0) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
```



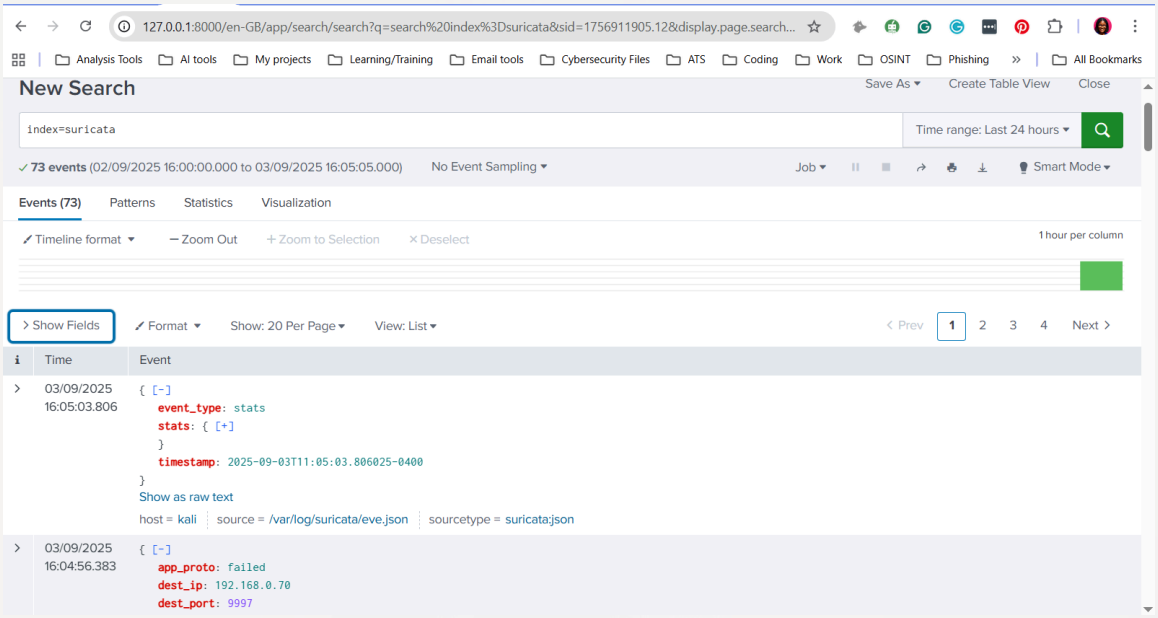


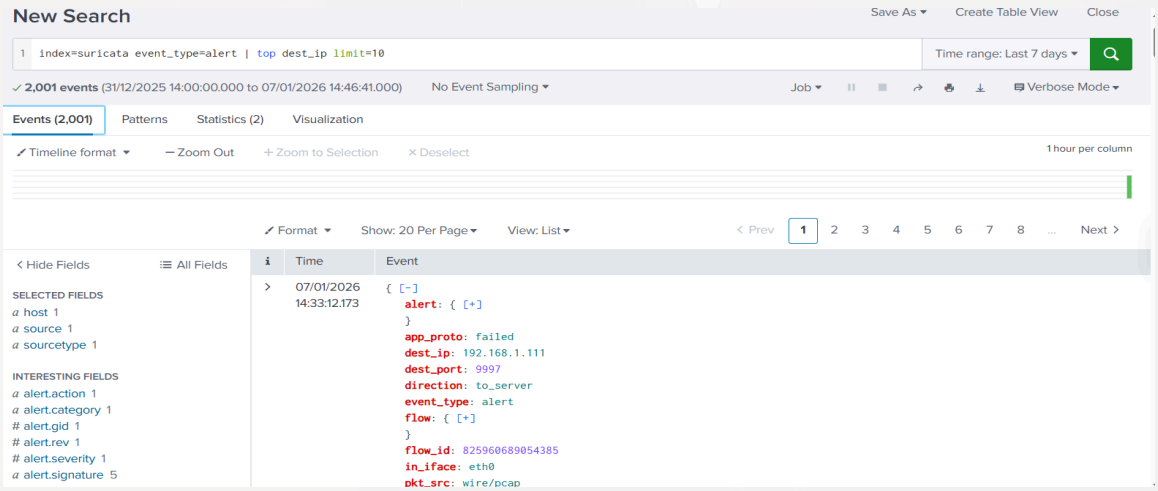
2. SIEM Configuration

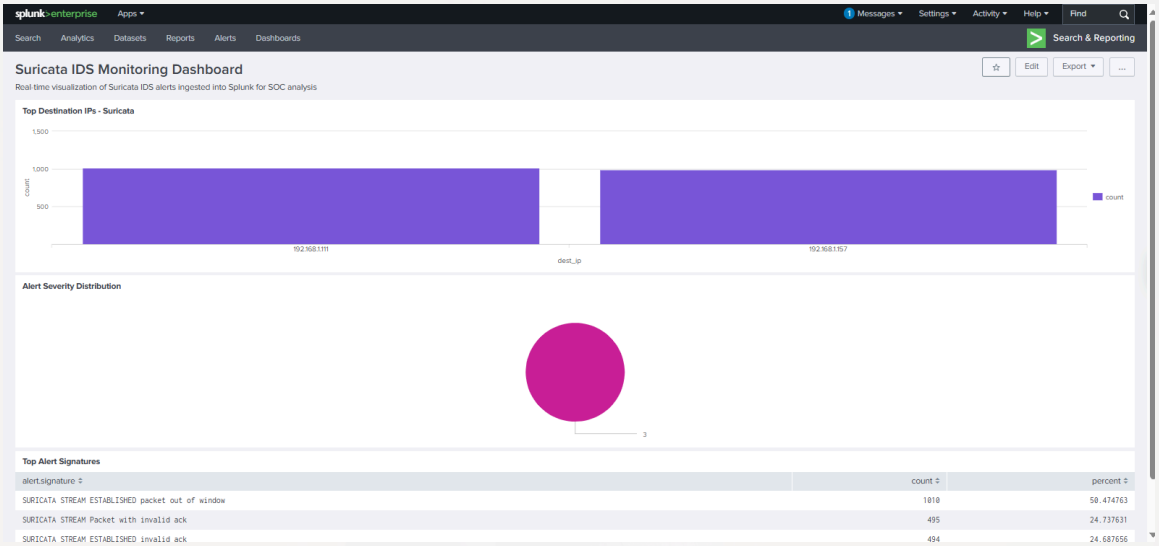
Within Splunk, a dedicated index was configured to receive Suricata logs. JSON fields were parsed to extract relevant information such as alert signatures, severity, source IP, and destination IP.

Test events were generated to confirm:

- Logs were being ingested
- Fields were correctly extracted
- Events were searchable using SPL


127.0.0.1:8000/en-GB/app/search/search?q=search%20index%3Dsuricata&sid=1756911905.12&display.page.search...
Analysis Tools
AI tools
My projects
Learning/Training
Email tools
Cybersecurity Files
ATS
Coding
Work
OSINT
Phishing
All Bookmarks
New Search
Save As
Create Table View
Close
index=suricata
Time range: Last 24 hours
73 events (02/09/2025 16:00:00.000 to 03/09/2025 16:05:05.000)
No Event Sampling
Job
Smart Mode
Events (73)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Show Fields
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
Next
Time
Event
03/09/2025 16:05:03.806
{ [-]
event_type: stats
stats: { [+]
}
timestamp: 2025-09-03T11:05:03.806025-0400
}
Show as raw text
host = kali
source = /var/log/suricata/eve.json
sourcetype = suricata:json
03/09/2025 16:04:56.383
{ [-]
app_proto: failed
dest_ip: 192.168.0.70
dest_port: 9997


New Search
Save As
Create Table View
Close
1 index=suricata event_type=alert | top dest_ip limit=10
Time range: Last 7 days
2,001 events (31/12/2025 14:00:00.000 to 07/01/2026 14:46:41.000)
No Event Sampling
Job
Verbose Mode
Events (2,001)
Patterns
Statistics (2)
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a alert.action 1
a alert.category 1
alert.gid 1
alert.rev 1
alert.severity 1
a alert.signature 5
Time
Event
07/01/2026 14:33:12.173
{ [-]
alert: { [+]
}
app_proto: failed
dest_ip: 192.168.1.111
dest_port: 9997
direction: to_server
event_type: alert
flow: { [+]
}
flow_id: 825960689054385
in_iface: eth0
pkt_src: wire/pcap



3. Attack Simulation

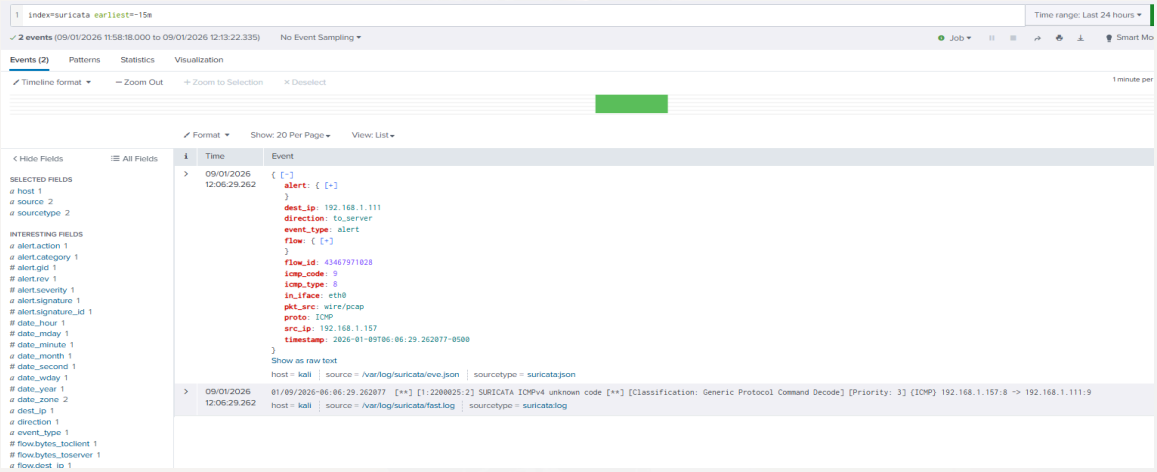
To simulate malicious activity, reconnaissance-based attacks were launched using Nmap from the Kali Linux environment. The attacks included: SYN scans and Service detection scans.

```
┌──(kali㉿kali)-[~]
└─$ ping -c5  192.168.1.111
PING 192.168.1.111 (192.168.1.111) 56(84) bytes of data.
64 bytes from 192.168.1.111: icmp_seq=1 ttl=64 time=11.6 ms
64 bytes from 192.168.1.111: icmp_seq=2 ttl=64 time=1.12 ms
64 bytes from 192.168.1.111: icmp_seq=3 ttl=64 time=1.17 ms
64 bytes from 192.168.1.111: icmp_seq=4 ttl=64 time=3.38 ms
64 bytes from 192.168.1.111: icmp_seq=5 ttl=64 time=1.42 ms

── 192.168.1.111 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4015ms
rtt min/avg/max/mdev = 1.121/3.730/11.566/4.006 ms

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A 192.168.1.111
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-09 06:06 EST
Nmap scan report for KatieConnect (192.168.1.111)
Host is up (0.0010s latency).
All 1000 scanned ports on KatieConnect (192.168.1.111) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E8:2A:EA:D1:68:7F (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.00 ms KatieConnect (192.168.1.111)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.06 seconds
```

4. Expected Outcome

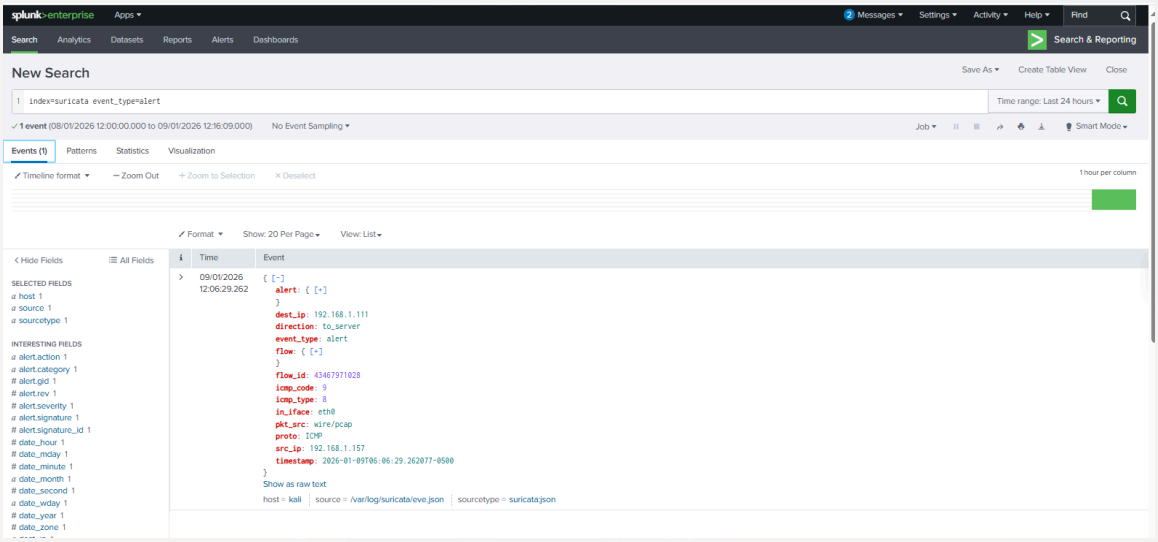
The expected behavior of the SOC environment was:

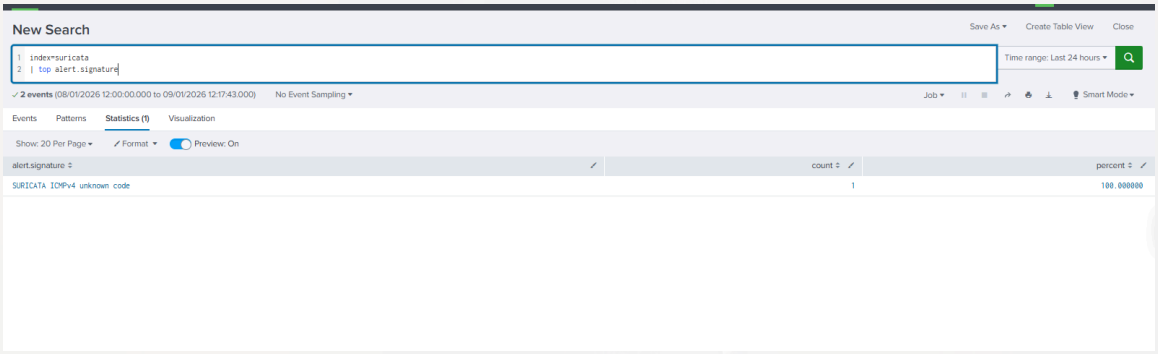
- Suricata detects suspicious scanning behavior
- Alerts are generated with defined signatures and severity
- Logs are forwarded to Splunk in near real-time



5. Observed Outcome

The attacks successfully triggered multiple Suricata alerts. These alerts were forwarded to Splunk and indexed correctly. Analysis showed repeated alerts originating from the same source IP, confirming reconnaissance activity.





6. Detection and Analysis

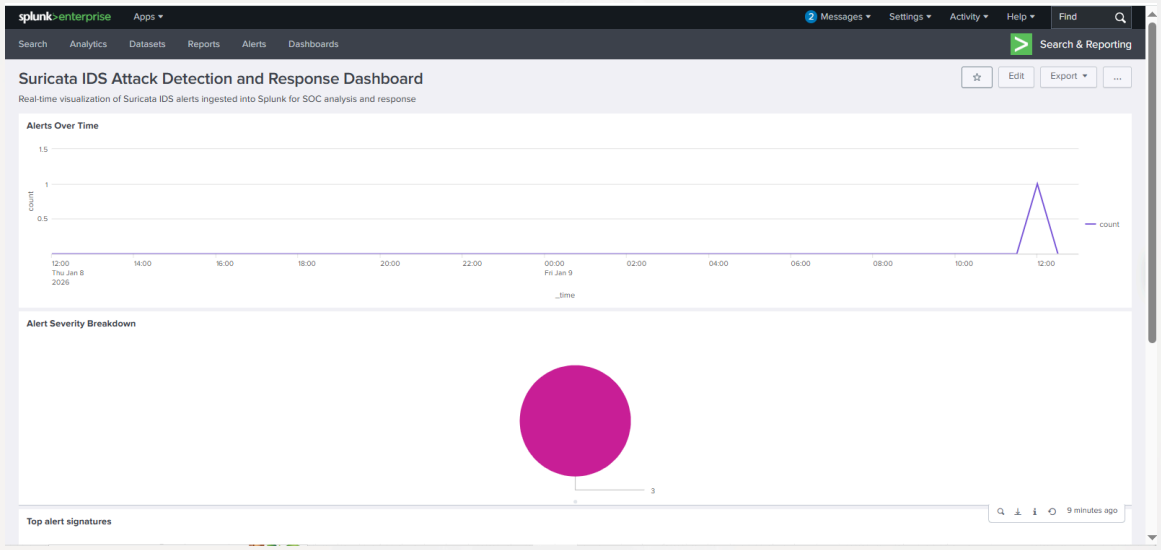
Using Splunk, alerts were analyzed to identify:

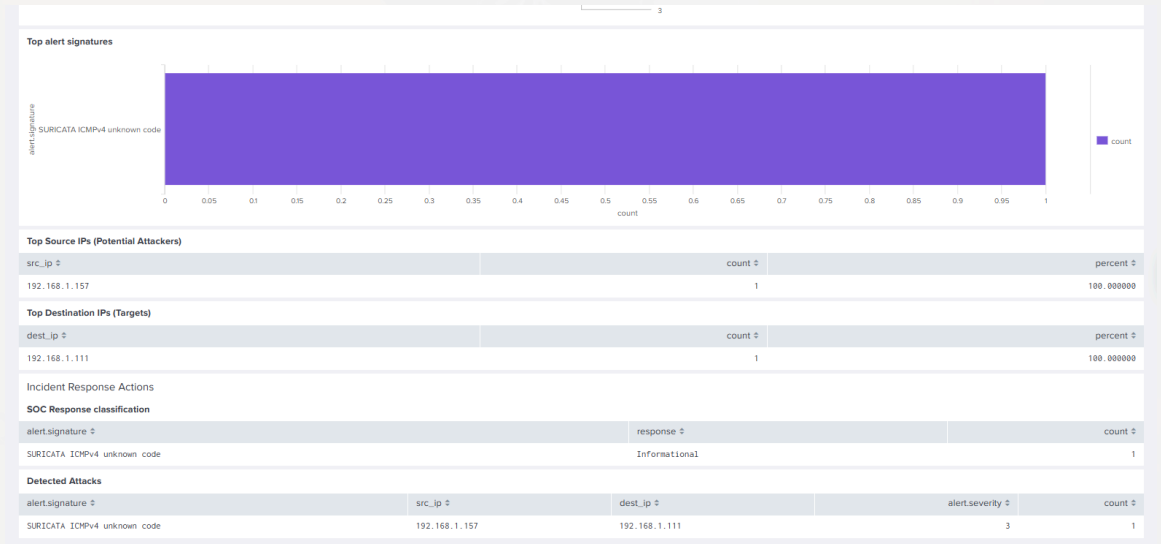
- The source IP responsible for the activity
- Alert signatures triggered by the scans
- Severity levels assigned by Suricata

Correlation across multiple alerts confirmed that the activity was reconnaissance rather than a single benign event.

Some SPL queries used during analysis:

- index=suricata event_type=alert
- index=suricata | top alert.signature
- index=suricata | stats count by src_ip





Top Source IPs (Potential Attackers)

src_ip	count	percent
192.168.1.157	1	100.000000

Top Destination IPs (Targets)

dest_ip	count	percent
192.168.1.111	1	100.000000

Incident Response Actions

SOC Response classification

alert.signature	response	count
SURICATA ICMPv4 unknown code	Informational	1

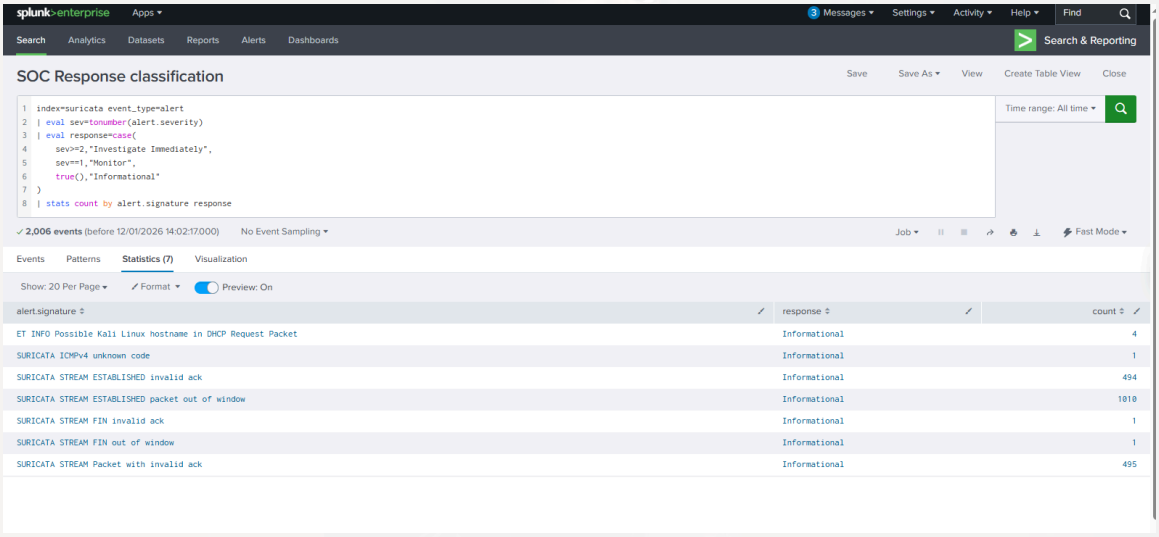
Detected Attacks

alert.signature	src_ip	dest_ip	alert.severity	count
SURICATA ICMPv4 unknown code	192.168.1.157	192.168.1.111	3	1

7. Incident Response and Analyst Decision-Making

Based on the detected alerts, the activity was identified as reconnaissance behavior originating from a single source IP. Multiple SYN scan alerts and service detection signatures were correlated in Splunk, confirming repeated scanning activity rather than a one-off benign event.

The incident was classified as **medium severity**, requiring investigation and monitoring. Since the source IP was confirmed as an internal test system, no blocking action was taken.



8. **Challenges Encountered and Resolutions**

- Log parsing issues affecting severity classification
- SIEM ingestion and connectivity troubleshooting
- Tool compatibility and configuration failures

Conclusion

This project successfully demonstrated the design and operation of a mini Security Operations Center using Suricata and Splunk. The environment enabled end-to-end visibility from attack simulation to detection, analysis, and response classification.

Through this project, I gained hands-on experience with IDS deployment, SIEM ingestion, SPL querying, dashboard creation, and incident response reasoning.