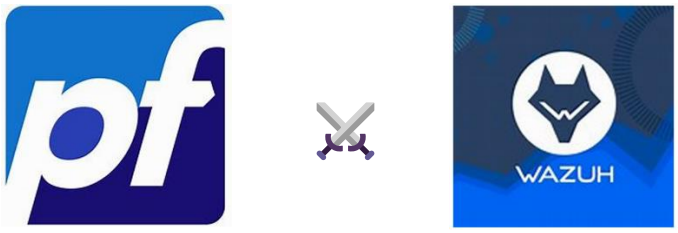
9/2/2025

Task # 03

Malware Download and Incident Response Plan.



Objective: Download a freely available malware via a VM with an active pfSense firewall, observe detection and log activities, analyze logs and malware, and create an incident response plan.

Submitted By:

Syed Muhammad Shah

SOC TEAM ~ OMEGA

ITSOLERA PVT LTD

STEP-1

Setup and Download Malware

Pre-requisites:

1) **Ensure that pfSense is properly installed and configured.**
   - Using the same pfsense & Network Topology (From Task 2).

2) **Make sure a virtual machine is prepared.**
   - Install new VM (Ubuntu), instead of using Kali Linux (Agent 1).

3) **Verify that Wazuh is installed and configured.**
   - installing Wazuh Agent in Ubuntu, setup File integrity monitoring (From Task 1).

4) **Ensure that pfSense is integrated With Wazuh.**
   - Setup Ubuntu network topology & configuring with pfsense (From Task 2).

Here are the details and IPs of components used in the task.

- Ubuntu: 192.168.0.103
- WazuhManager: 192.168.0.100
- pfSense LAN IP: 192.168.0.1/24
- pfSense WAN IP: 192.168.0.108/24 (DHCP)

For Ubuntu The Network Files For static ip is different , so setting up ,

i. Using "ip a" to see adapter name (enp0s3).
ii. Replace the file (**sudo gedit /etc/netplan/50-cloud-init.yaml**) content with below content.

```
network:
 version: 2
 renderer: networkd
 ethernets:
  enp0s3:            # check with `ip a` if your NIC has a different name
   dhcp4: no
   addresses:
    - 192.168.0.103/24
   routes:
    - to: default
      via: 192.168.0.1
   nameservers:
    addresses:
      - 192.168.0.1
```

iii. sudo netplan apply.
iv. sudo systemctl restart systemd-networkd.

5) Install ClamAV (AV) on Ubuntu and integrate its logs with Wazuh

We'll use ClamAV daemon + signatures and ingest /var/log/clamav/clamav.log into Wazuh. Wazuh ships ClamAV decoders/rules so detections become proper alerts.

1. sudo apt update
2. sudo apt install -y clamav clamav-daemon
3. sudo systemctl stop clamav-freshclam
4. sudo freshclam (it will show some warning cuz of command 3 so ignore)
5. sudo systemctl enable --now clamav-freshclam
6. sudo systemctl enable --now clamav-daemon

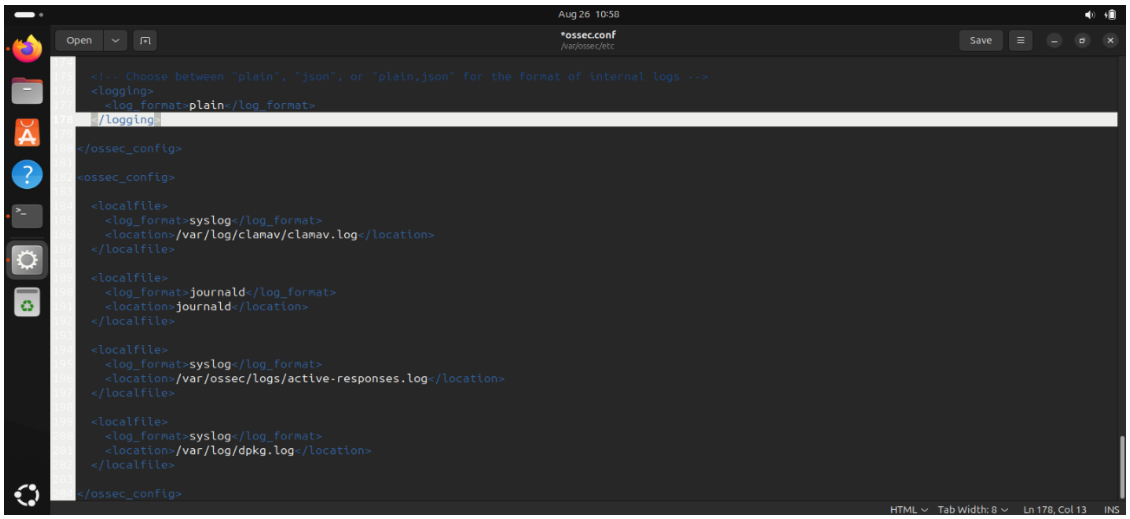
Tell Wazuh agent to read ClamAV log

Reference: [ClamAV logs collection - Malware detection · Wazuh documentation]

A. sudo gedit /var/ossec/etc/ossec.conf

➢ Add this block (anywhere among <localfile> items): “if not already present”

```
<localfile>
 <location>/var/log/syslog</location>
 <log_format>syslog</log_format>
</localfile>
```



B. Sudo gedit /etc/clamav/clamd.conf

➢ Arround line 20-22 , edit false to true “LogSyslog true”

```
#Automatically Generated by clamav-daemon postinst
#To reconfigure clamd run #dpkg-reconfigure clamav-daemon
#Please read /usr/share/doc/clamav-daemon/README.Debian.gz for details
LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
# TemporaryDirectory is not set to its default /tmp here to make overriding
# the default with environment variables TMPDIR/TMP/TEMP possible
User clamav
ScanMail true
ScanArchive true
ArchiveBlockEncrypted false
MaxDirectoryRecursion 15
FollowDirectorySymlinks false
FollowFileSymlinks false
ReadTimeout 180
MaxThreads 12
MaxConnectionQueueLength 15
LogSyslog true
LogRotate true
```

C. sudo chown -R clamav:clamav /home/ubuntu/malware
D. sudo chmod 755 /home/ubuntu
E. sudo systemctl restart clamav-daemon
F. sudo systemctl restart rsyslog
G. sudo systemctl restart wazuh-agent

.

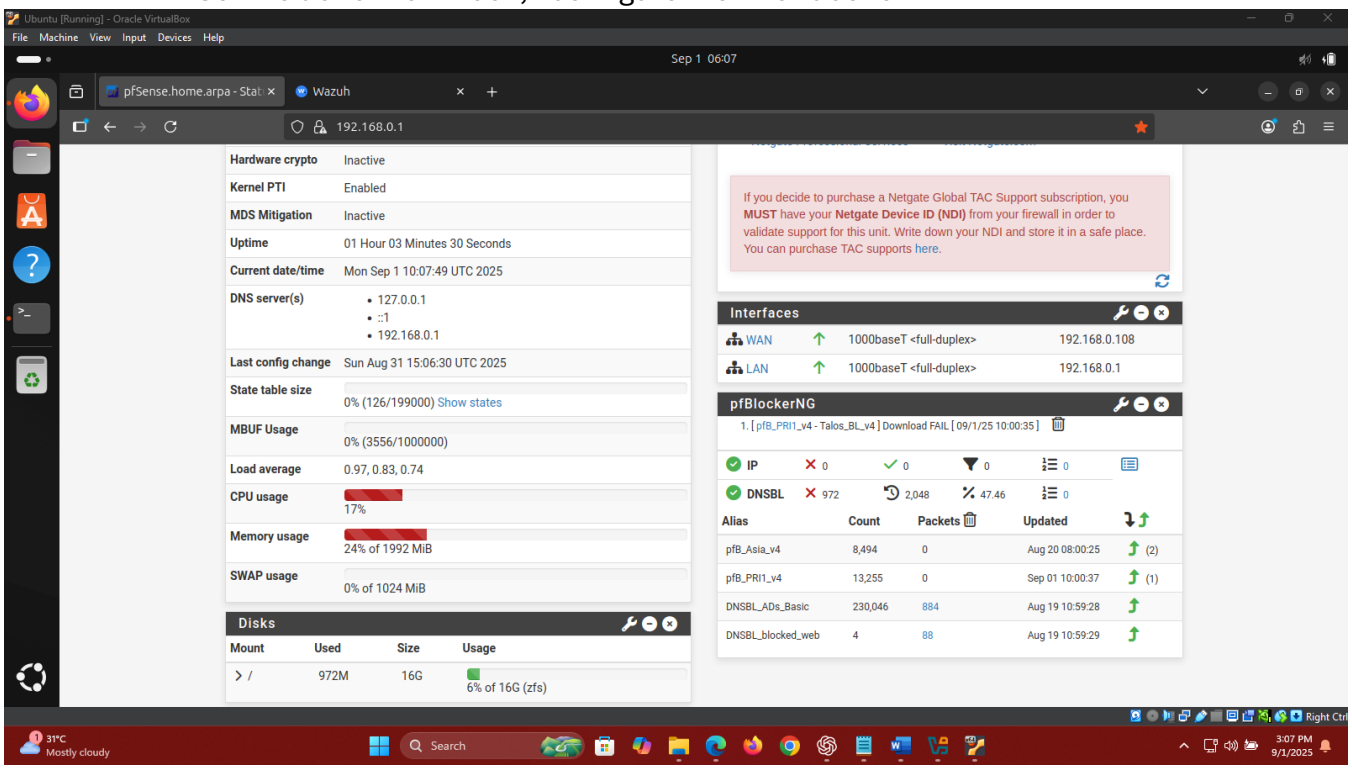
STEP-2

Detection and Observation

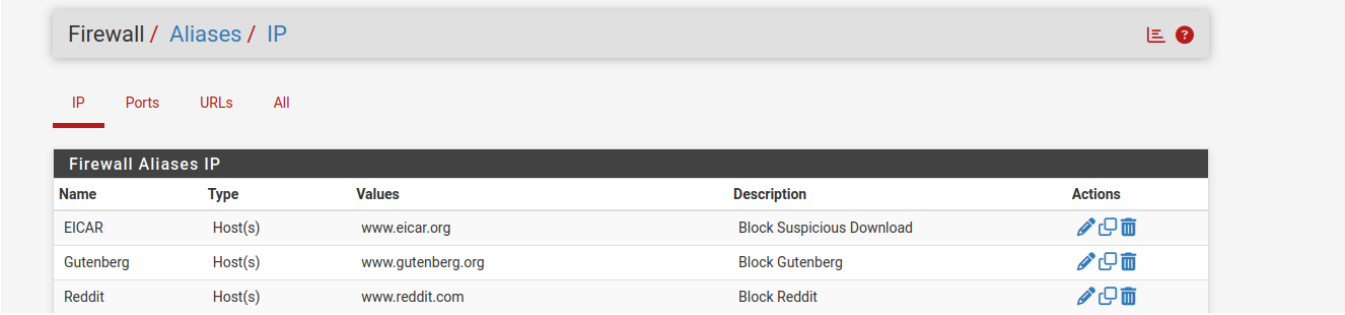
PRE-STEPS (FOR DETECTION & LOGS):

1) Go to Firewall → Aliases.
   - ➢ Select “Add” to create an alias. Assign a name to the alias, such as “EICAR.” Choose the “Host(s)” type to detect any domain related to the specified IP/FQDN, which in this case is “www.eicar.org.” Click “Save” to finalize the configuration.

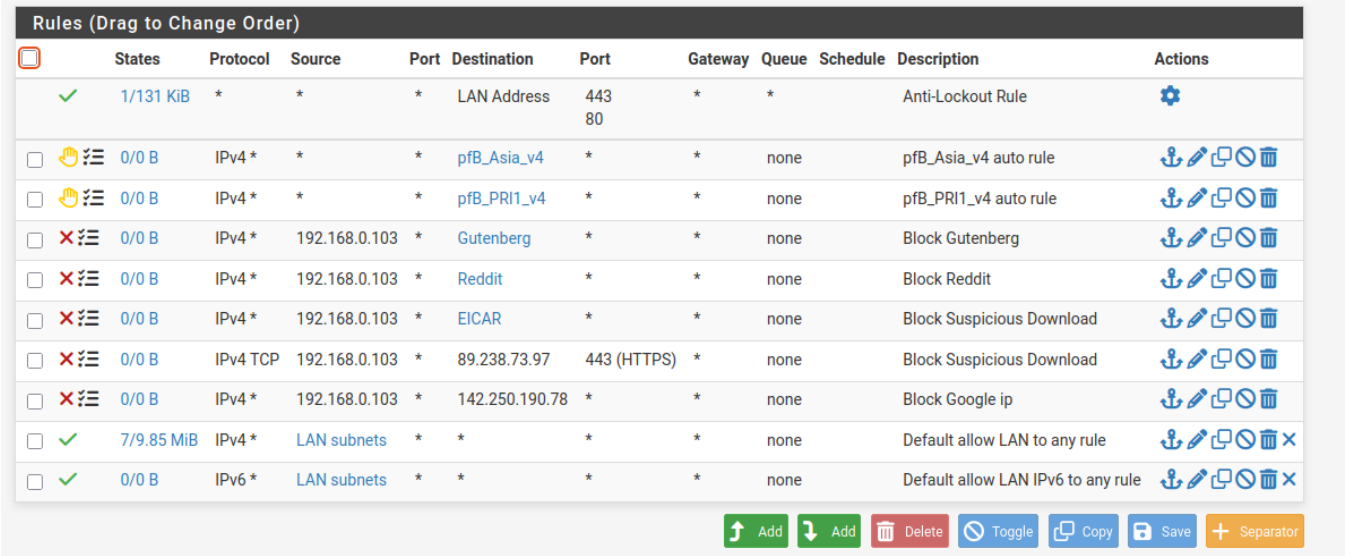
2) Go to Firewall → Rules → LAN and click on “Add” to add a new rule.
   - ➢ Set the action to “Block,” configure the interface to “LAN”.



.....

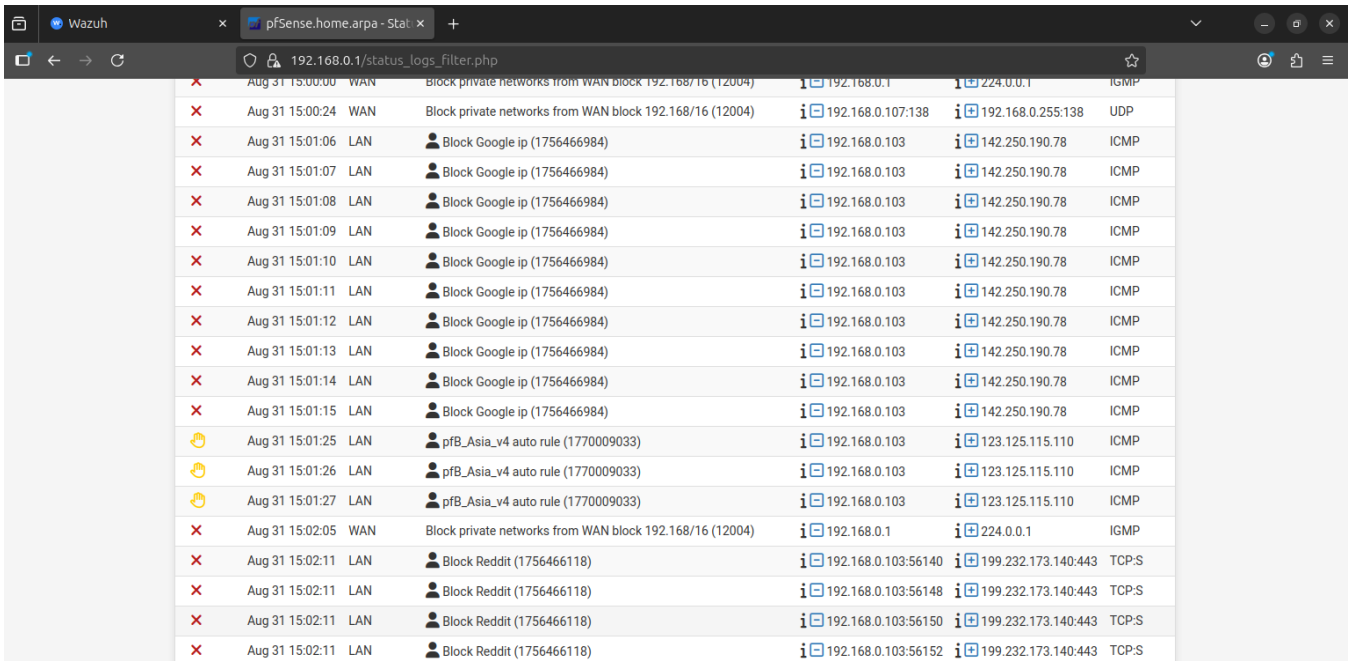


.....

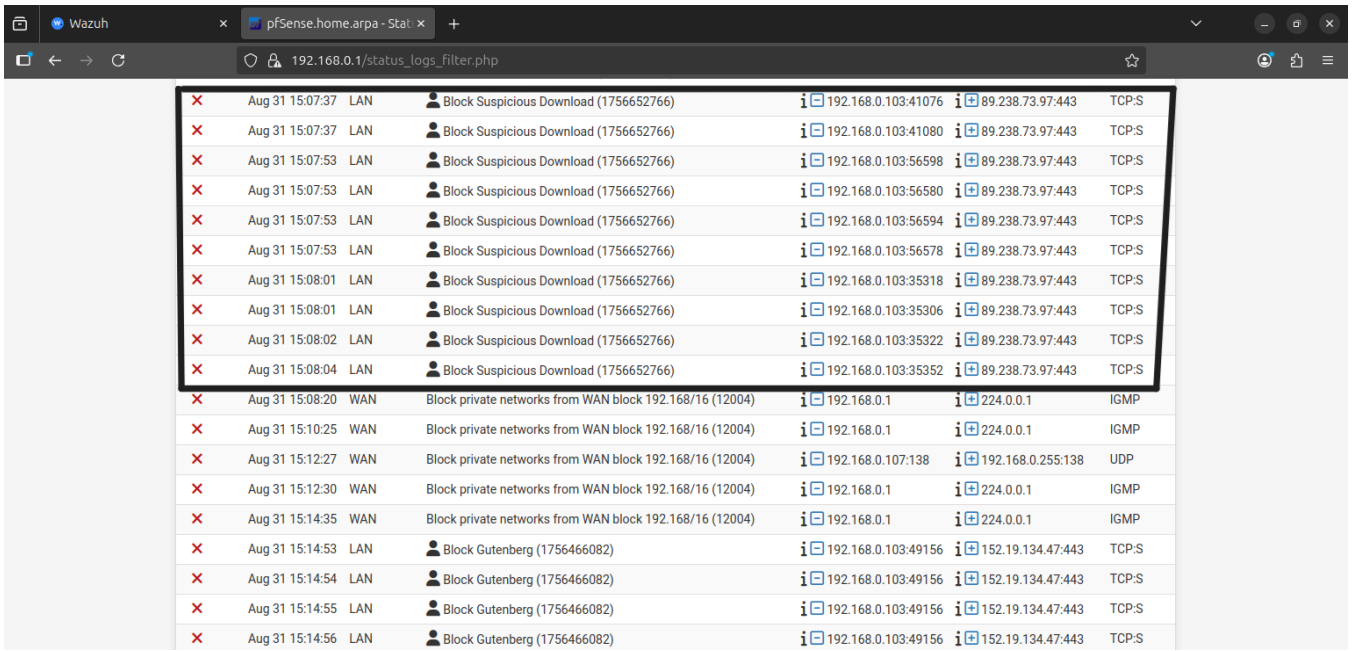


pfSense Monitoring:

The malware download attempt is successfully blocked by the firewall from the source IP 192.168.0.103 to the destination IP 89.238.73.97 (EICAR's IP) .



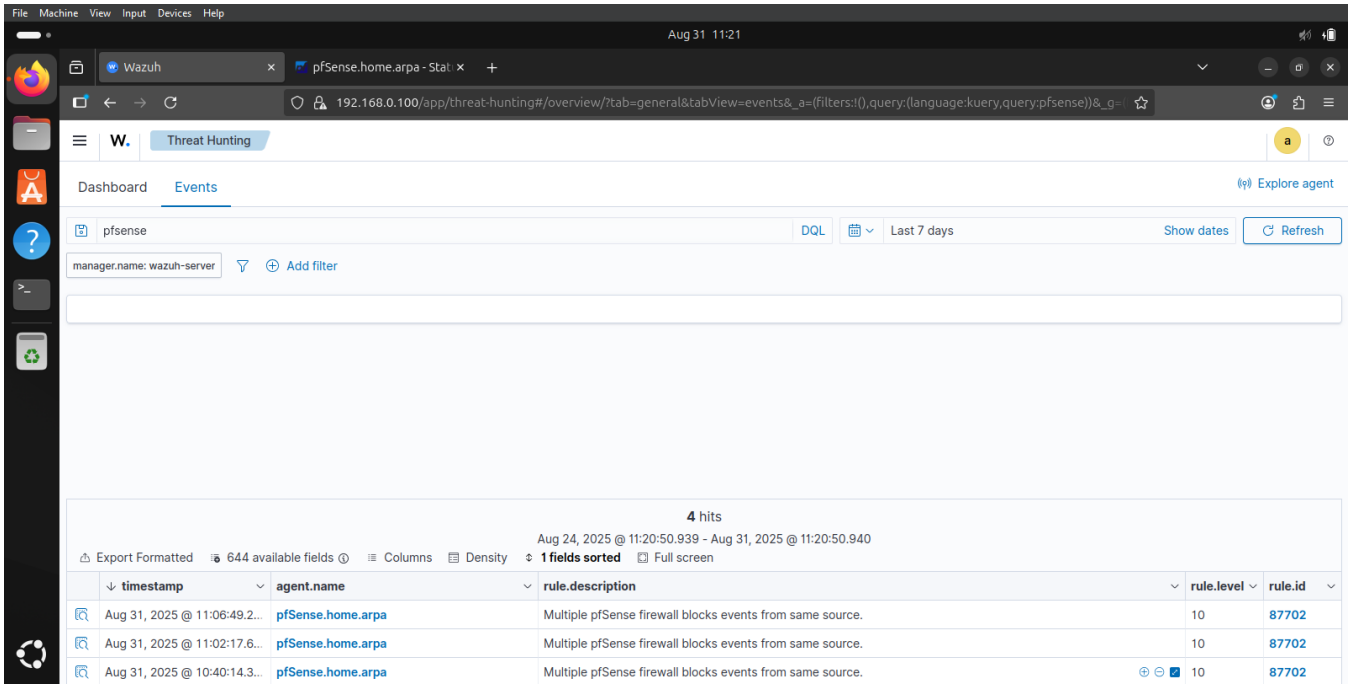
.....



.....

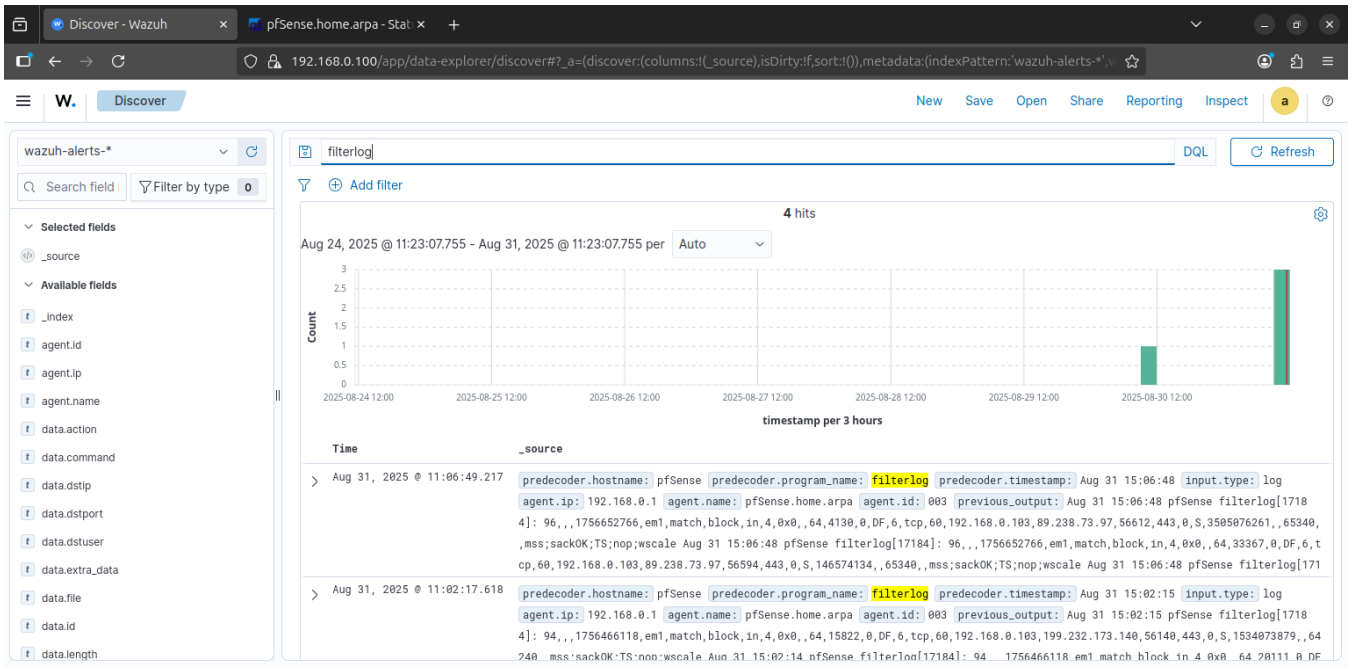
Wazuh Monitoring:

Here the logs in security events as “Multiple pfSense firewall blocks events from same source”.

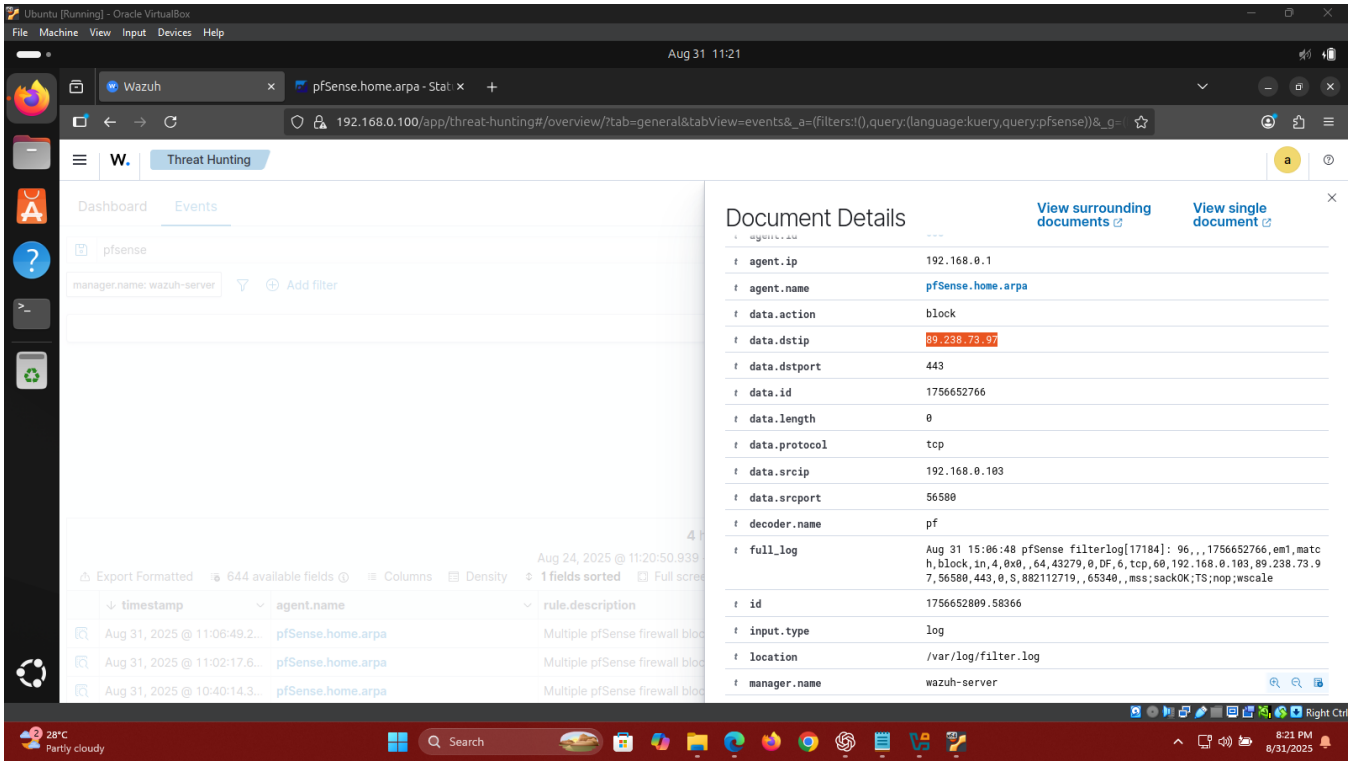


.....

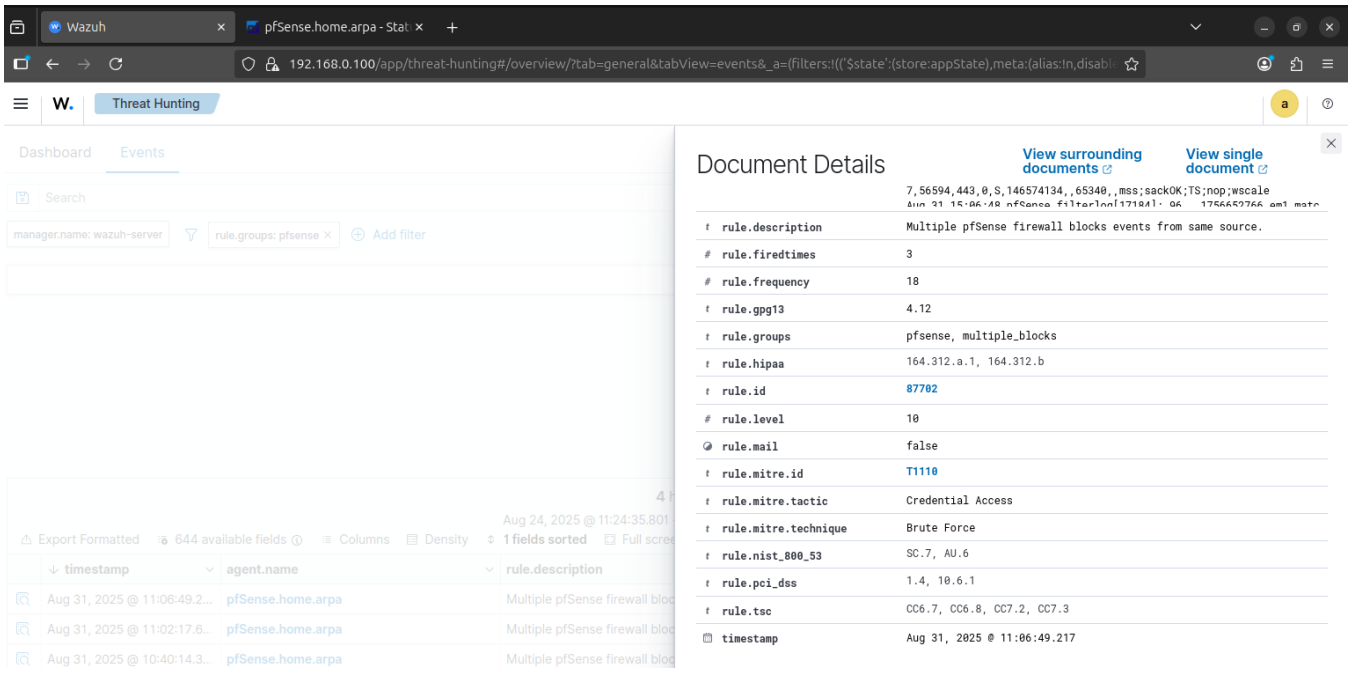
Examining the details reveals that access was blocked from the source IP 192.168.0.103 to the destination IP 89.238.73.97 (EICAR's IP), effectively stopping the malware to download.



On The Log Preview, By High lvl 10 rule , pfsense 87702 shows Clear Details What Actually Happened !

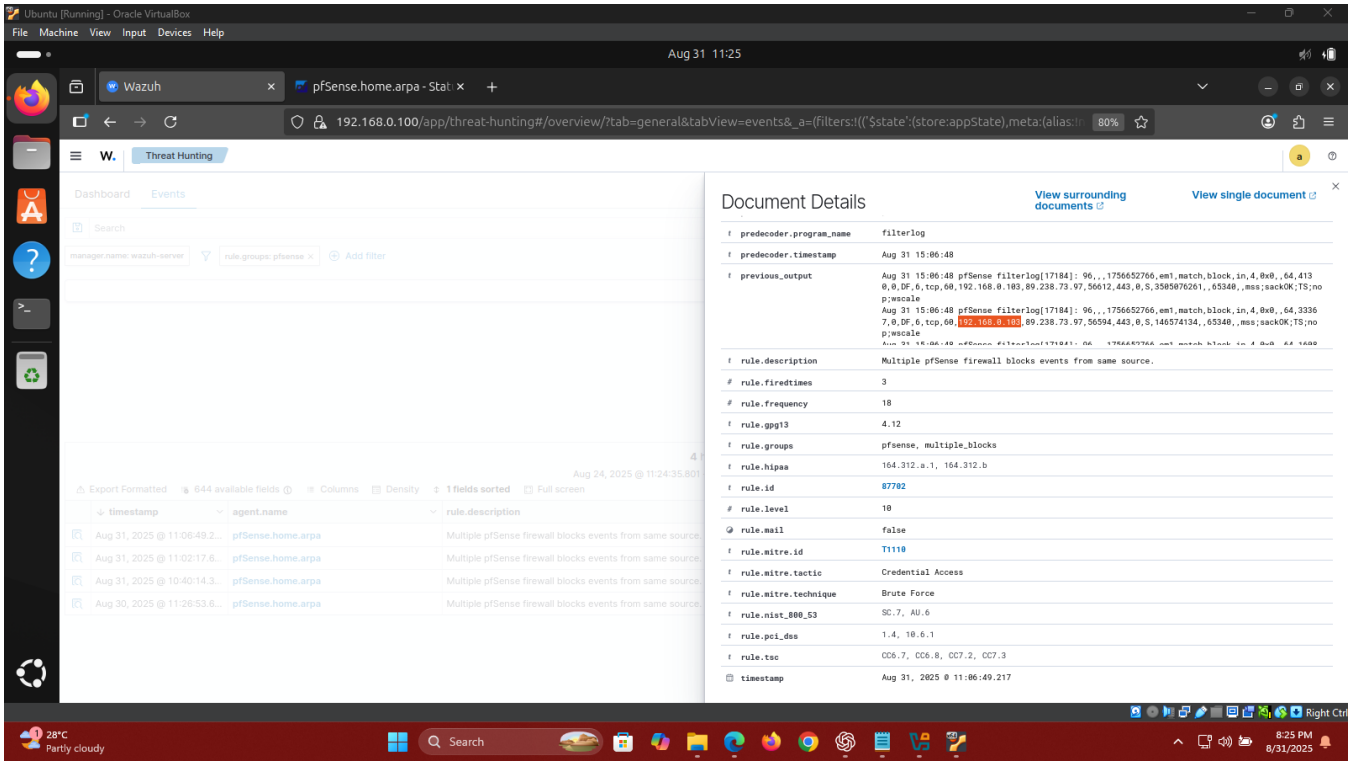


.....

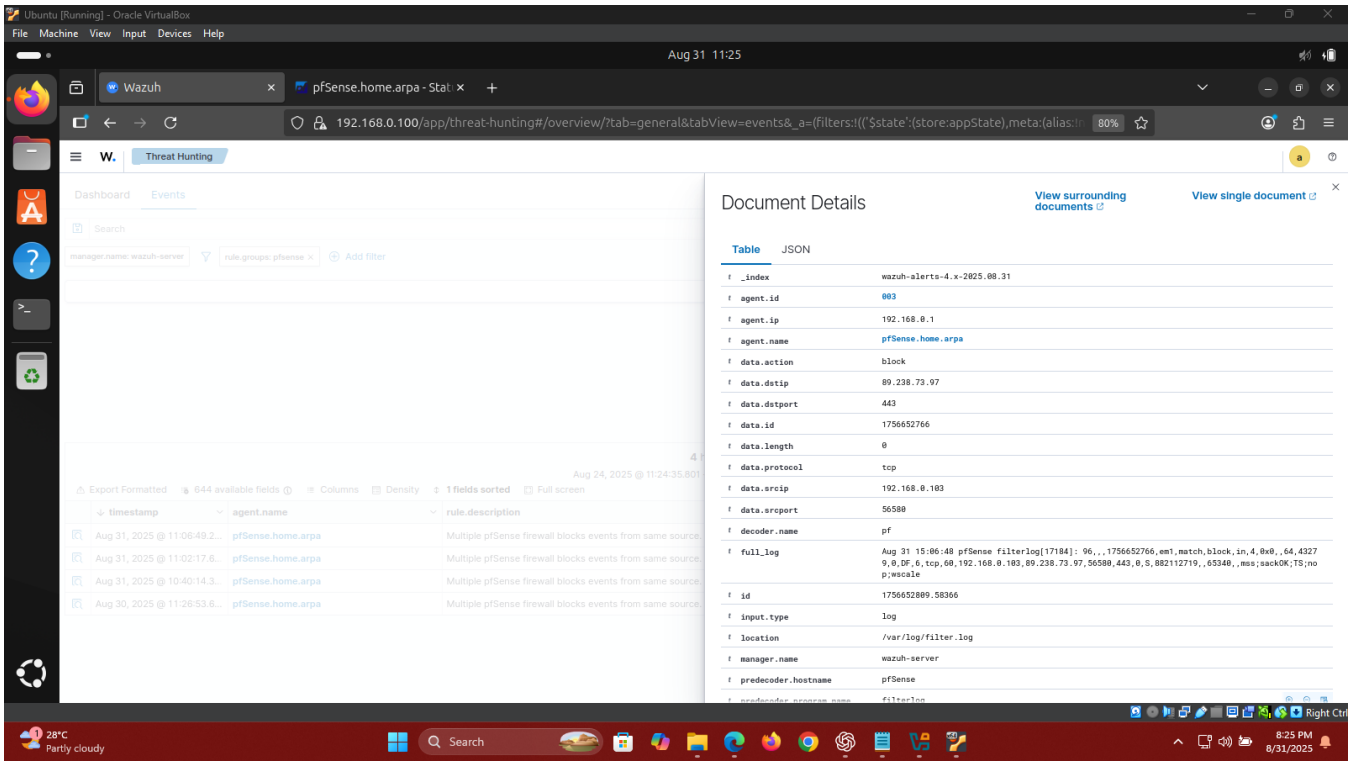


.....

Previous Attempts Collected and Mentioned With Agent ip , Source ip and Destination ip .


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 31 11:25
Wazuh
pfSense.home.arpa - Stat
192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(('$state':(store:appState),meta:(alias:!n
80%
Threat Hunting
Dashboard
Events
Document Details
View surrounding documents
View single document
predecoder.program_name filterlog
predecoder.timestamp Aug 31 15:06:48
previous_output Aug 31 15:06:48 pfSense filterlog[17184]: 96,,,1756652766,em1,match,block,in,4,0x0,,64,413 0,0,DF,6,tcp,60,192.168.0.103,89.238.73.97,56612,443,0,S,3505076261,,65340,,mss;sackOK;TS;no p;wscale
Aug 31 15:06:48 pfSense filterlog[17184]: 96,,,1756652766,em1,match,block,in,4,0x0,,64,3336 7,0,DF,6,tcp,60,192.168.0.103,89.238.73.97,56594,443,0,S,146574134,,65340,,mss;sackOK;TS;no p;wscale
rule.description Multiple pfSense firewall blocks events from same source.
rule.firedtimes 3
rule.frequency 18
rule.gpg13 4.12
rule.groups pfsense, multiple_blocks
rule.hipaa 164.312.a.1, 164.312.b
rule.id 87702
rule.level 10
rule.mail false
rule.mitre.id T1110
rule.mitre.tactic Credential Access
rule.mitre.technique Brute Force
rule.nist_800_53 SC.7, AU.6
rule.pci_dss 1.4, 10.6.1
rule.tsc CC6.7, CC6.8, CC7.2, CC7.3
timestamp Aug 31, 2025 @ 11:06:49.217
28°C Partly cloudy
Search
8:25 PM 8/31/2025

.....


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 31 11:25
Wazuh
pfSense.home.arpa - Stat
192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(('$state':(store:appState),meta:(alias:!n
80%
Threat Hunting
Dashboard
Events
Document Details
View surrounding documents
View single document
Table JSON
_index wazuh-alerts-4.x-2025.08.31
agent.id 003
agent.ip 192.168.0.1
agent.name pfSense.home.arpa
data.action block
data.dstip 89.238.73.97
data.dstport 443
data.id 1756652766
data.length 0
data.protocol tcp
data.srcip 192.168.0.103
data.srcport 56580
decoder.name pf
full_log Aug 31 15:06:48 pfSense filterlog[17184]: 96,,,1756652766,em1,match,block,in,4,0x0,,64,4327 9,0,DF,6,tcp,60,192.168.0.103,89.238.73.97,56580,443,0,S,882112719,,65340,,mss;sackOK;TS;no p;wscale
id 1756652809.58366
input.type log
location /var/log/filter.log
manager.name wazuh-server
predecoder.hostname pfSense
28°C Partly cloudy
Search
8:25 PM 8/31/2025

.....

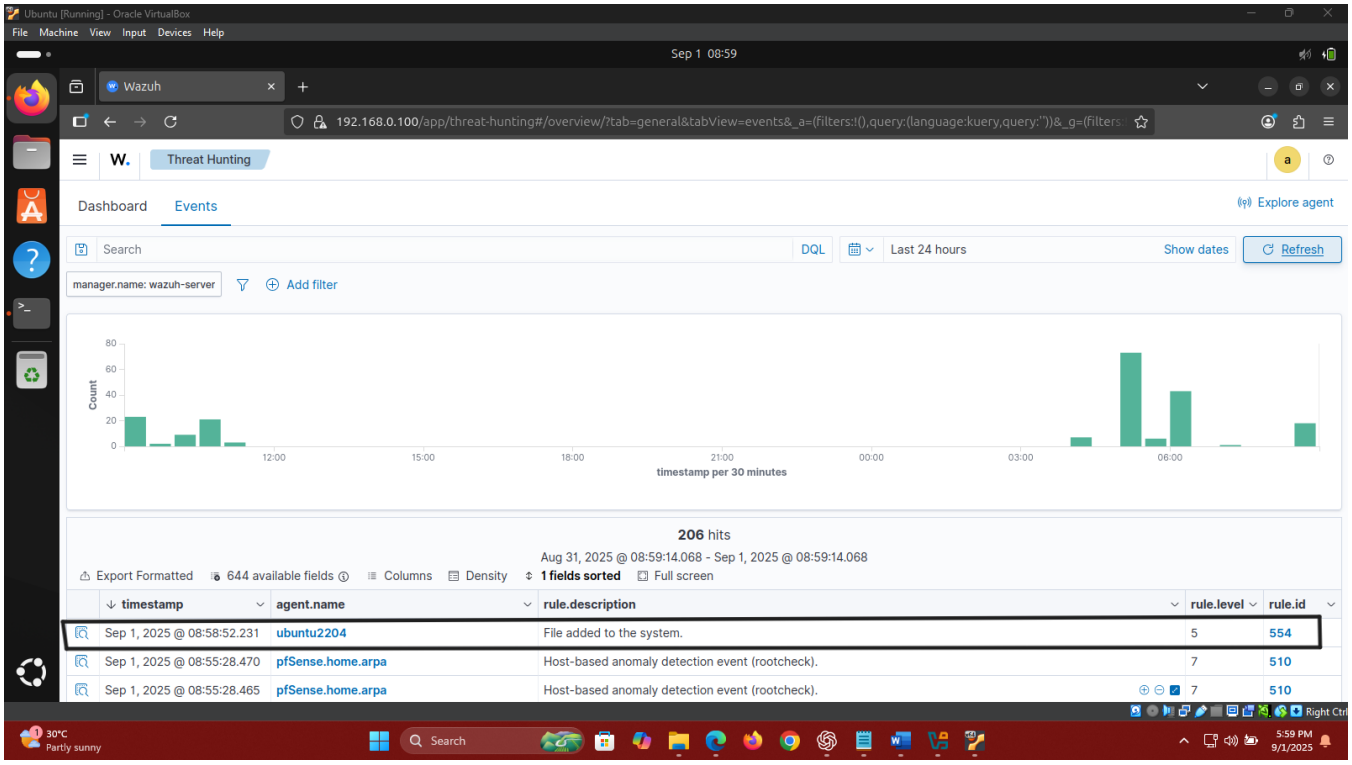
STEP-3

Logs and Malware Analysis

- Malware Was Pre-Downloaded For Lab Before The Detection Step !

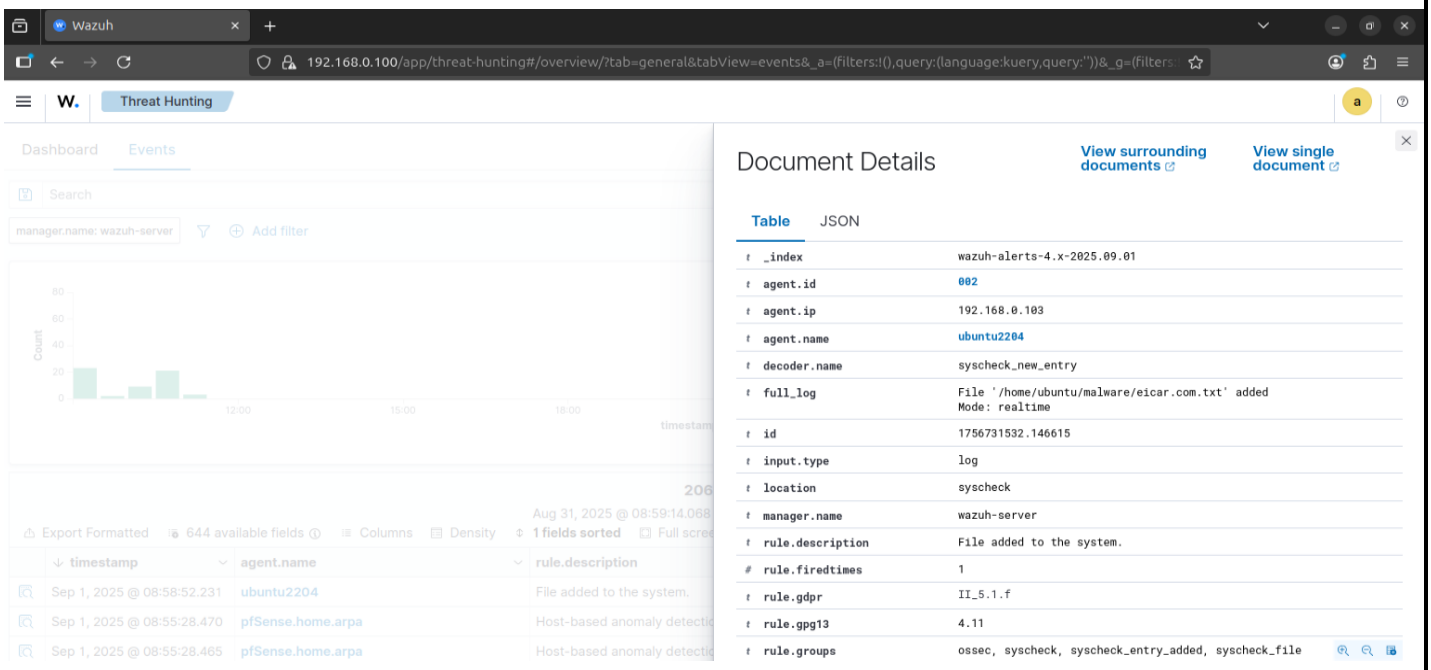
Phase-1

1) wazuh alerts us that a file was downloaded/Added in a known directory (malware) .

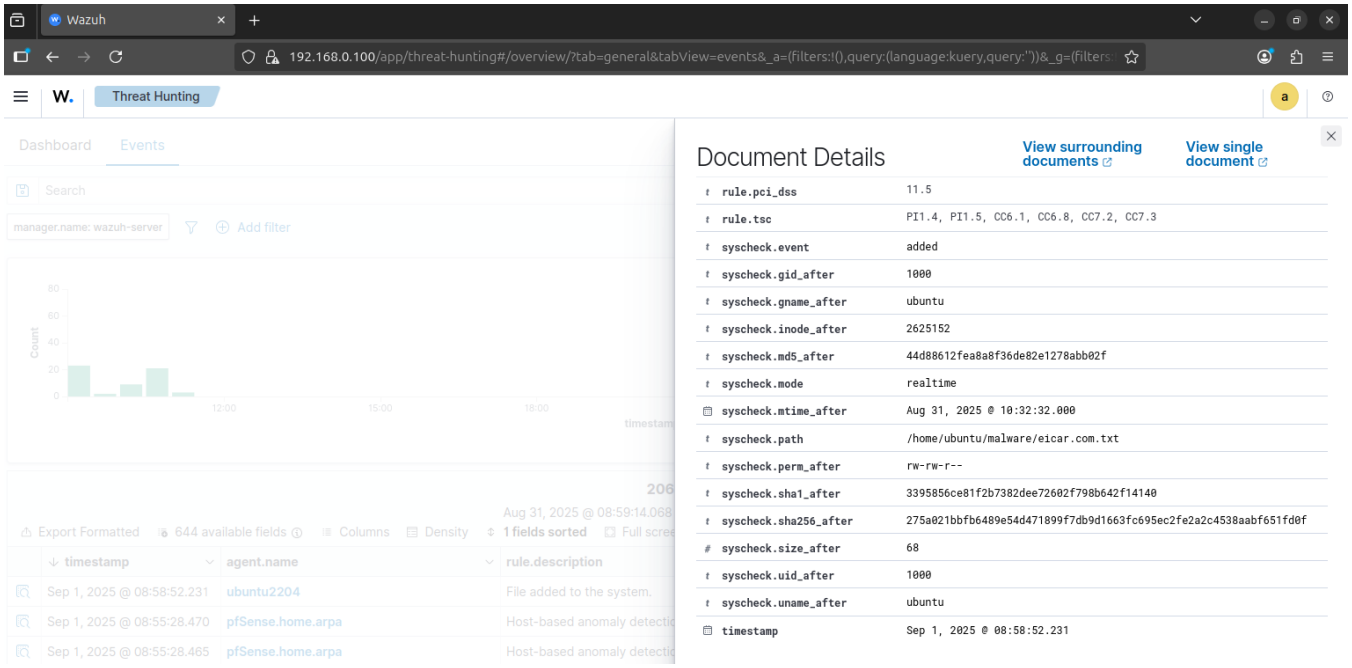


.....

2) I check the logs what actually happened . So , a file named “eicar.com.txt” was added in the directory “/home/ubuntu/malware/” with time-stamp “1 sept, 2025” .

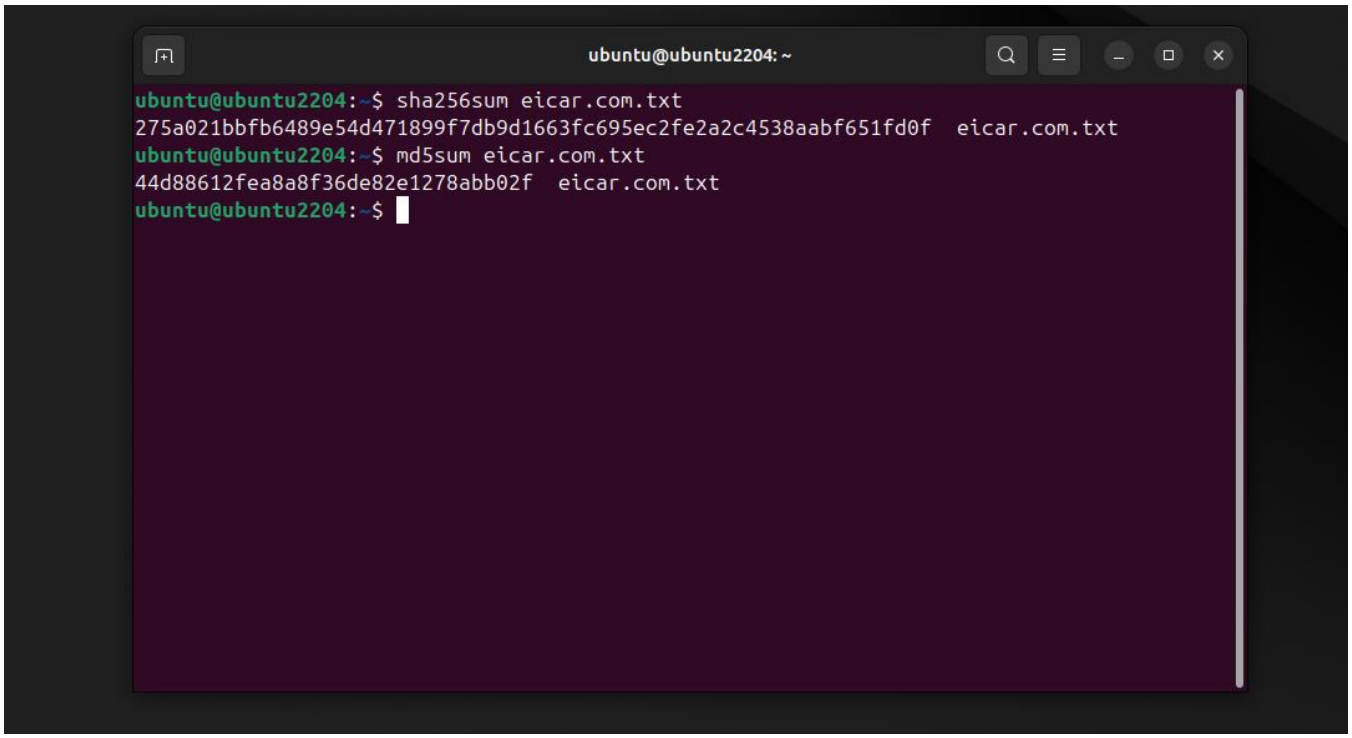


3) checking the file and malware with the given wazuh hashes to confirm the malware .



.....

4) The Hashes Confirmed The incident !



.....

SHA-256: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

MD5: 44d88612fea8a8f36de82e1278abb02f

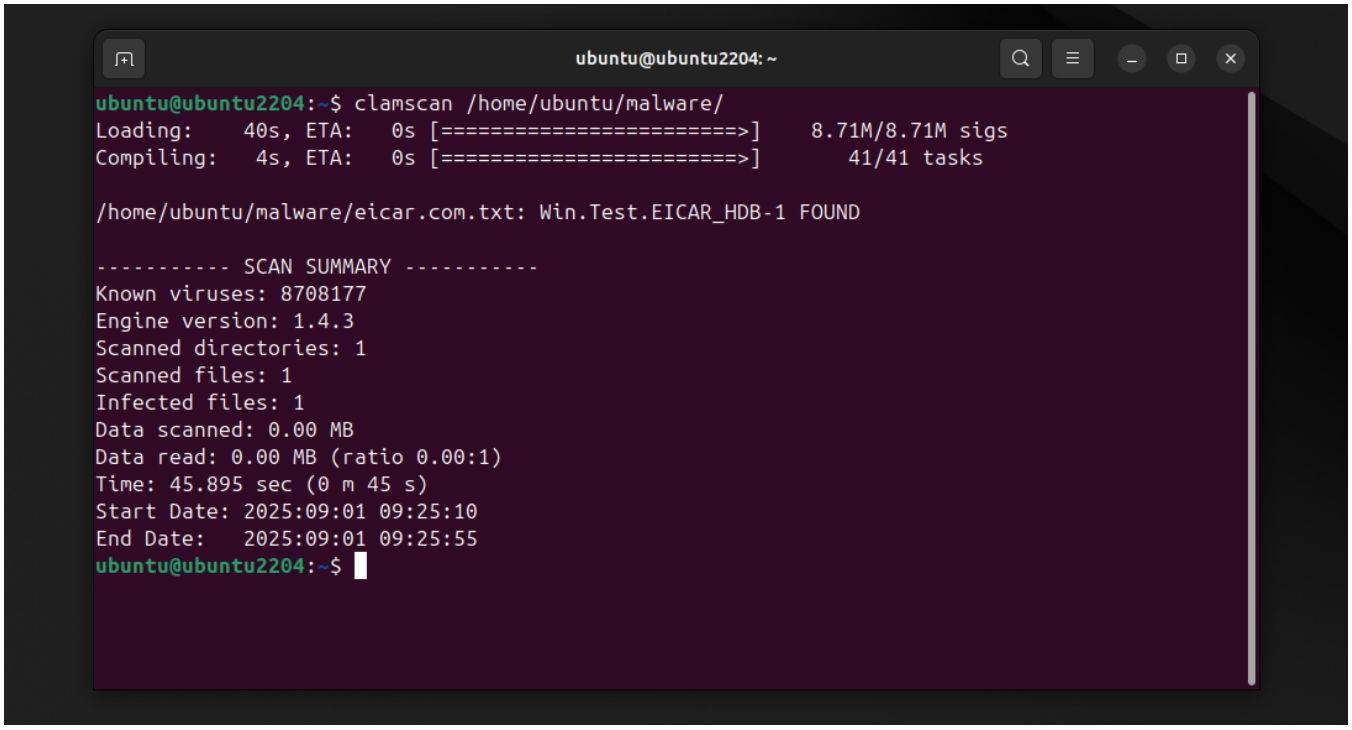
Phase-2

1) Scanning The Malware Behaviour With ClamAV .

- The malware behaviour was static as per lab .
- /home/ubuntu/malware/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
- Known viruses: 8708177
- Engine version: 1.4.3

I Did 2 Scans !

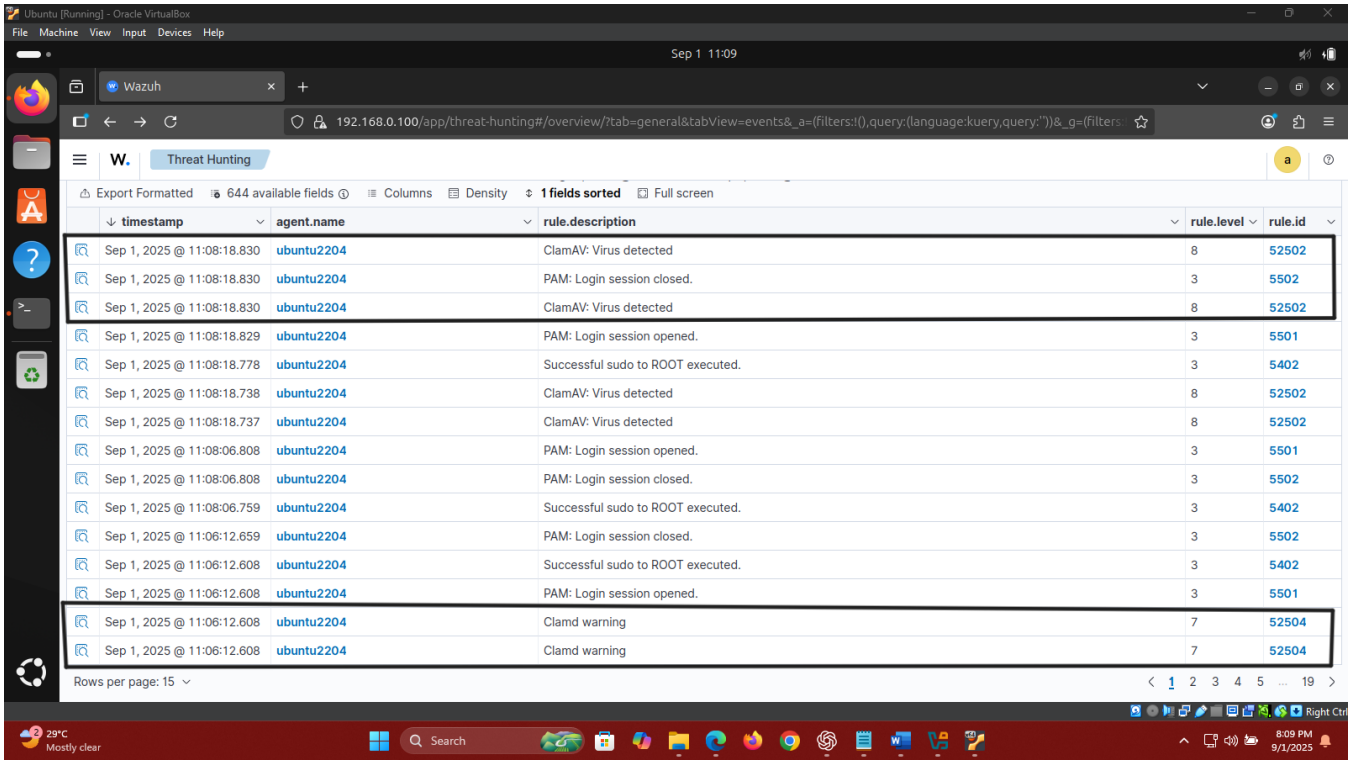
- sudo clamdscan /home/ubuntu/malware
- sudo clamscan /home/ubuntu/malware



.....

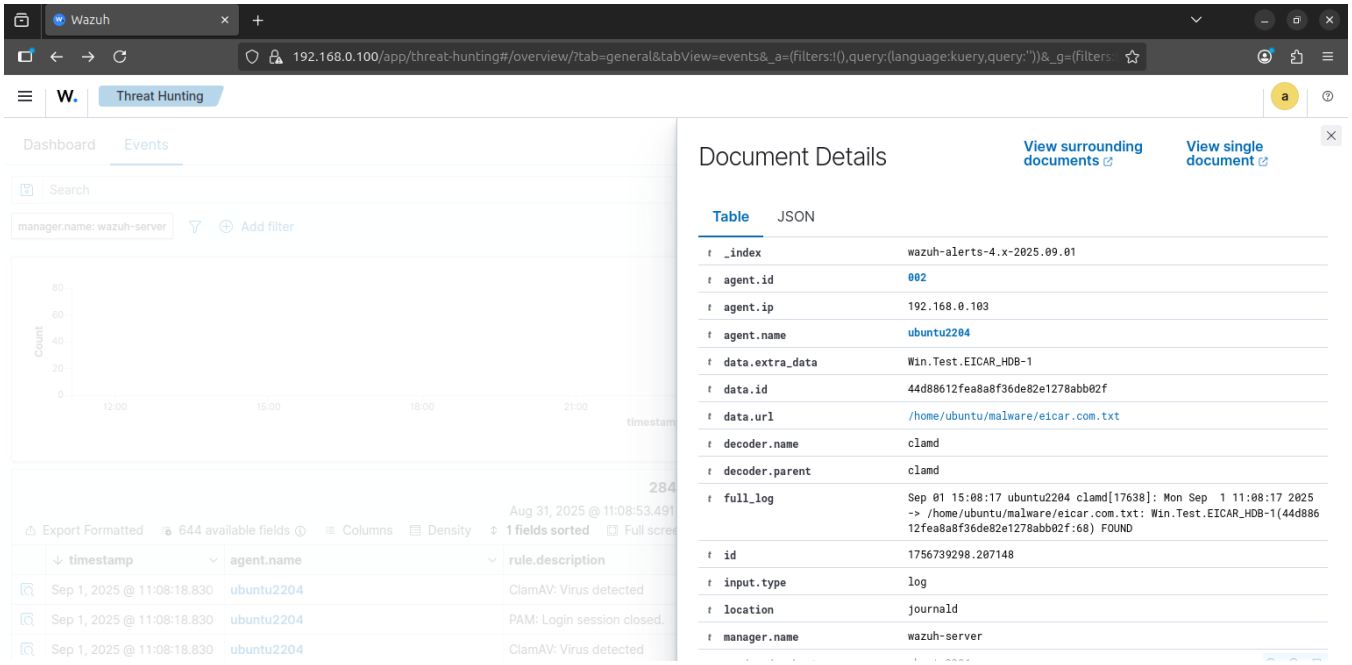
Phase-3

1) Wazuh Detection of Malware Behaviour.

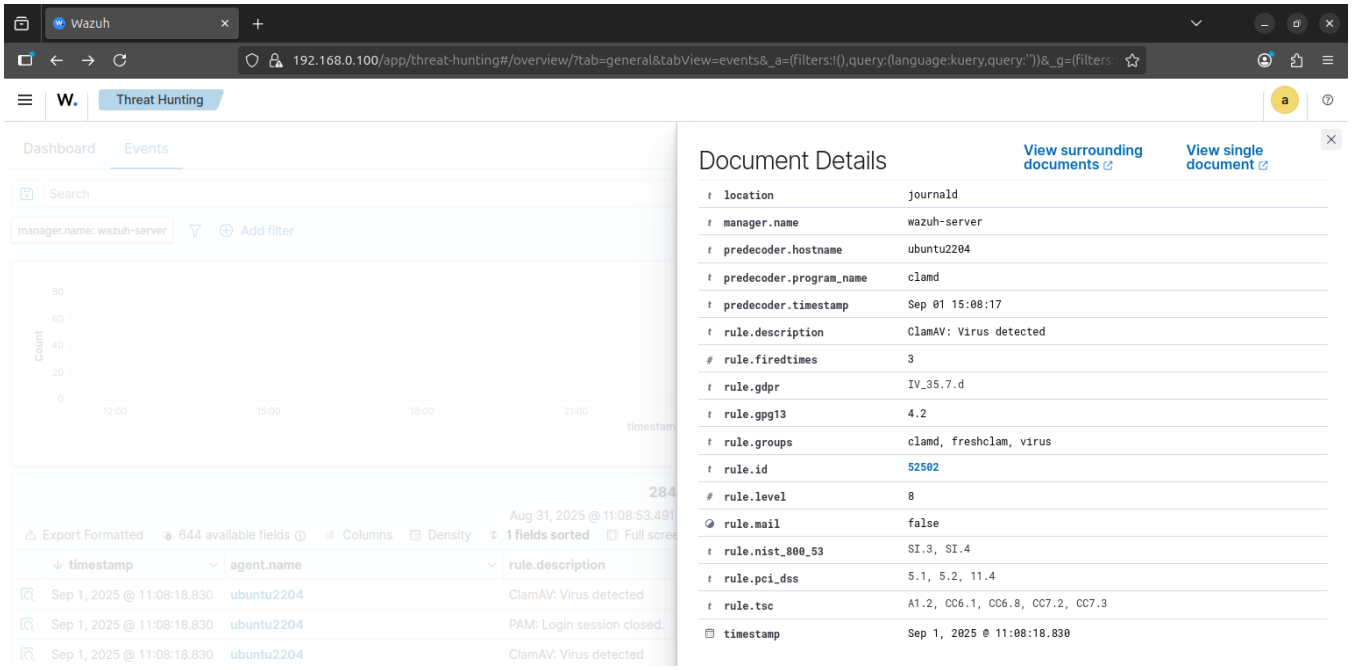


2) Wazuh Logs Analysis

1. **data.extra_data:** Win.Test.EICAR_HDB-1
2. **data.url:** /home/ubuntu/malware/eicar.com.txt
3. **full_log:** Sep 01 15:08:17 ubuntu2204 clamd[17638]: Mon Sep 1 11:08:17 2025 -> /home/ubuntu/malware/eicar.com.txt: Win.Test.EICAR_HDB-1(44d88612fea8a8f36de82e1278abb02f:68) FOUND
4. **decoder.name:** clamd
5. **rule.description:** ClamAV: Virus detected
6. **rule.id:** 52502
7. **timestamp:** Sep 1, 2025 @ 11:08:18.830



.....



.....

Phase-4

- ❖ Identify Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).

Incident overview

- **Date / time:** Sep 01, 2025 — detection logged at **11:08:17–11:08:18** (timestamps as recorded).
- **Affected asset:** ubuntu2204 VM (192.168.0.103).
- **Perimeter / SIEM:** pfSense (LAN: 192.168.0.1) forwarding syslog to Wazuh manager (192.168.0.100).
- **Outcome:** File was created on disk and detected by ClamAV; firewall logged the network attempt and Wazuh generated a ClamAV alert (52502) plus grouped pfSense firewall-block alerts.

Malware source / URL

- **Domain:** www.eicar.org (lab alias used / pfSense alias).

- **Standard test URL (used in this lab):** https://www.eicar.org/download/eicar.com.txt (the sample/file downloaded for AV testing).

Indicators of Compromise (IOCs)

Network IOCs

- Source (victim) IP: **192.168.0.103** (Ubuntu VM).
- Destination IP (EICAR host): **89.238.73.97**.
- Domain / Host: **www.eicar.org** (alias "EICAR" used in pfSense).
- Download URL: **https://www.eicar.org/download/eicar.com.txt** (observable in experiment/config).

File IOCs

- File name: **eicar.com.txt**
- File path: **/home/ubuntu/malware/eicar.com.txt**.
- MD5: **44d88612fea8a8f36de82e1278abb02f**.
- SHA-256: **275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f**.

Detection / log IOCs

- Wazuh/ClamAV detection rule: **rule.id = 52502**, **rule.description = "ClamAV: Virus detected"**.
- Full log excerpt (clamd → syslog):
- Sep 01 15:08:17 ubuntu2204 clamd[17638]: Mon Sep 1 11:08:17 2025 -> /home/ubuntu/malware/eicar.com.txt: Win.Test.EICAR_HDB-1(44d88612fea8a8f36de82e1278abb02f:68) FOUND

(This exact line is present in the Wazuh full_log field.)

Perimeter / firewall IOCs

- pfSense blocked connection entries: **Blocked from 192.168.0.103 → 89.238.73.97** (logged; Wazuh shows grouped "multiple pfSense firewall blocks from same source").
- pfSense log / Wazuh grouping reference: high-level **pfsense rule 87702** (as shown in Wazuh log preview).

Indicators of Attack (IOAs)

1. **Ingress tool transfer (download attempt)** — VM initiated an outbound HTTPS connection requesting eicar.com.txt from www.eicar.org (T1105 — Ingress Tool Transfer). Evidence:

pfSense filterlog for connection to 89.238.73.97 and Wazuh/clamd detection on the downloaded file.

2. **New artifact creation on host disk** — Creation of /home/ubuntu/malware/eicar.com.txt detected by FIM/agent. Evidence: Wazuh syscheck / file-add alert and file path in ClamAV full_log.

3. **Signature-based detection** — ClamAV reported Win.Test.EICAR_HDB-1 FOUND for the file (host-based detection). Evidence: full_log and rule id 52502.

4. **Perimeter defense activation** — pfSense firewall generated block logs (grouped in Wazuh), indicating the perimeter observed/block action against the same source/destination pair. Evidence: Wazuh grouped pfSense alert and pfsense rule 87702.

5. **Repeated/Grouped Attempts** — Wazuh shows "multiple pfSense firewall blocks from same source", indicating either repeated download attempts or multiple connections within a short window (useful to identify scanning or automated fetch behavior). Evidence: grouped firewall alerts in dashboard.

.

STEP-4

INCIDENT RESPONSE PLAN

✓ Following NIST SP 800-61 guidelines, the IR plan covers Detection/Analysis, Containment, Eradication, and Recovery.

Executive summary:

➢ On **2025-09-01** the lab Ubuntu VM (ubuntu2204, IP **192.168.0.103**) downloaded the EICAR test file (eicar.com.txt) from https://www.eicar.org/download/eicar.com.txt. Host AV (ClamAV/clamd) detected the file as **Win.Test.EICAR_HDB-1** and logged a detection event; pfSense logged outbound traffic to 89.238.73.97 and Wazuh correlated host and perimeter telemetry (ClamAV alert **52502** and grouped pfSense firewall blocks **87702**). This IR plan documents detection, evidence collection, containment, eradication, recovery, and lessons learned for this incident.

Scope & purpose:

➢ Single lab incident involving one Ubuntu VM (ubuntu2204 / 192.168.0.103), pfSense perimeter, and Wazuh SIEM. Provide clear, repeatable procedures to investigate, contain, remove, and recover from the detection; preserve forensic evidence; and update controls to prevent recurrence.

Incident Overview:

- **Date/Time:** 2025-09-01 ~11:08 (as per logs).
- **Victim Host:** Ubuntu VM (192.168.0.103).
- **Detection Systems:** ClamAV (host), pfSense (perimeter), Wazuh (SIEM).
- **Detection Rules:** ClamAV alert (**rule 52502**), grouped pfSense firewall blocks (**rule 87702**).
- **Outcome:** EICAR detected and contained. No real malicious payload.

Malware Source / URL:

- **Domain:** www.eicar.org
- **URL:** https://www.eicar.org/download/eicar.com.txt
- **Resolved IP:** 89.238.73.97

Indicators of Compromise (IOCs):

- **Source IP:** 192.168.0.103 (Ubuntu VM).
- **Destination IP:** 89.238.73.97 (EICAR host).
- **File Name/Path:** /home/ubuntu/malware/eicar.com.txt.
- **MD5 Hash:** 44d88612fea8a8f36de82e1278abb02f
- **SHA-256 Hash:** 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
- **Detection:** Win.Test.EICAR_HDB-1 — Wazuh rule **52502**.

Indicators of Attack (IOAs):

- **Download Attempt:** Outbound HTTPS request to www.eicar.org (observed in pfSense logs).
- **File Creation:** /home/ubuntu/malware/eicar.com.txt created on host.
- **AV Detection:** ClamAV flagged the file as malicious.
- **Perimeter Defense:** pfSense firewall blocked repeated connections to the EICAR IP.
- **Repeated Behavior:** Grouped pfSense alerts showed multiple connection attempts.

Incident Response Plan (NIST-Aligned)

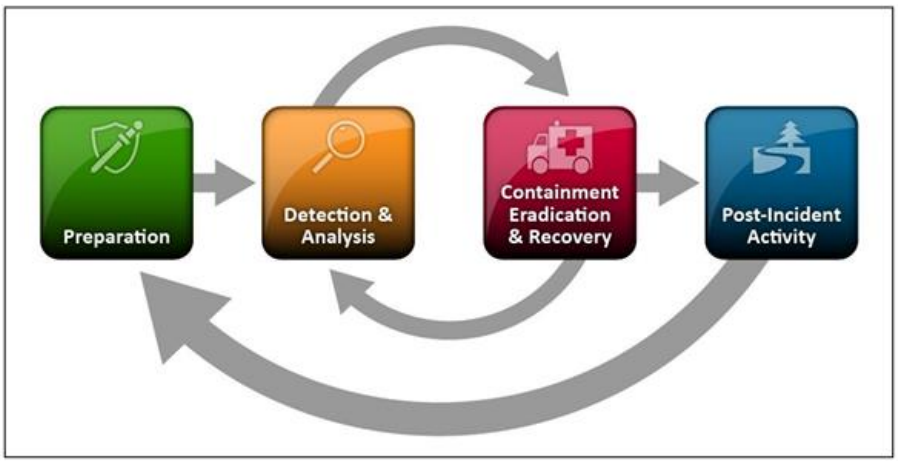


Figure 3-1. Incident Response Life Cycle

1. Detection & Analysis

- Alerts triggered by ClamAV and pfSense were ingested into Wazuh.
- Analyst confirmed the incident by reviewing Wazuh logs, ClamAV detection entry, and pfSense firewall logs.
- Severity assessed as **Low (lab test only)**.

2. Containment

- Isolated the affected Ubuntu VM by restricting its network access.
- pfSense firewall block rule prevented further communication with www.eicar.org.

3. Eradication

- Removed the test file (eicar.com.txt) from the host.
- Verified with a full **ClamAV scan** that no additional malicious files were present.

4. Recovery

- Restored the VM to a clean snapshot.
- Re-enabled network access and confirmed normal operations.
- Verified monitoring systems (Wazuh, ClamAV, pfSense) continued to detect and alert correctly.

5. Post-Incident (Lessons Learned)

- Detection pipeline (AV + FIM + Firewall + SIEM) worked as expected.
- For real malware, additional steps would include credential resets and system hardening.
- Improvement noted: maintain snapshots before malware testing, and consider creating Wazuh correlation rules to highlight repeated firewall blocks.

My Final Thoughts:

- This incident provided a safe and controlled opportunity to validate the effectiveness of our SOC lab environment. By simulating a real-world malware download with the harmless EICAR test file, we successfully demonstrated end-to-end detection and response capabilities across **pfSense**, **ClamAV**, and **Wazuh**. Each component played its role — pfSense blocked malicious traffic, ClamAV flagged the infected file, and Wazuh centralized the alerts for clear visibility. More importantly, the exercise reinforced a structured response workflow aligned with industry standards (NIST 800-61), ensuring that even in a training scenario, professional best practices were applied. The lessons learned here not only strengthen technical proficiency but also build the confidence and readiness to handle genuine threats in production environments. This practical experience stands as a strong step forward in becoming a capable SOC analyst.

THE END