

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



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

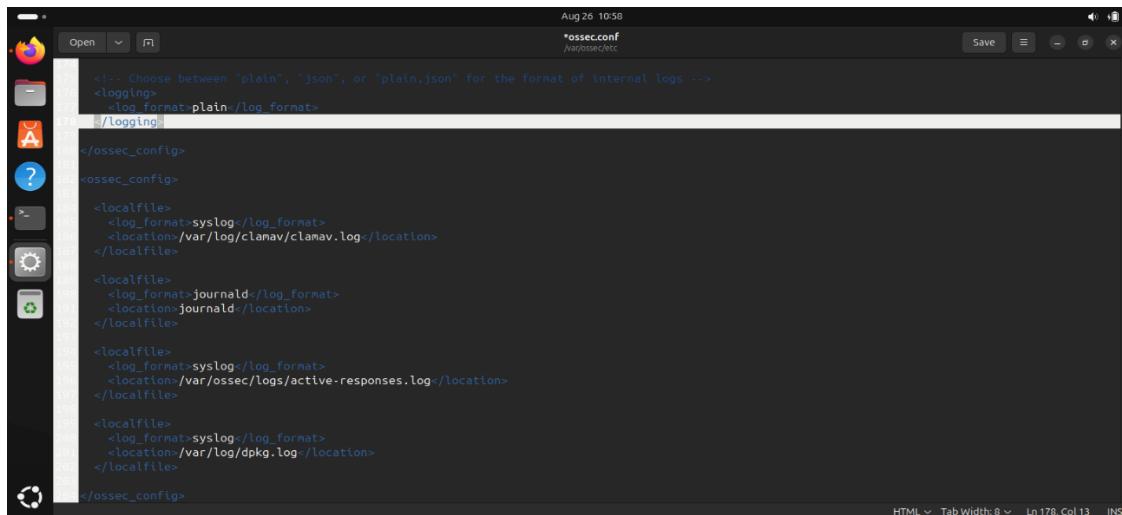
Tell Wazuh agent to read ClamAV log

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

- Around 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
-

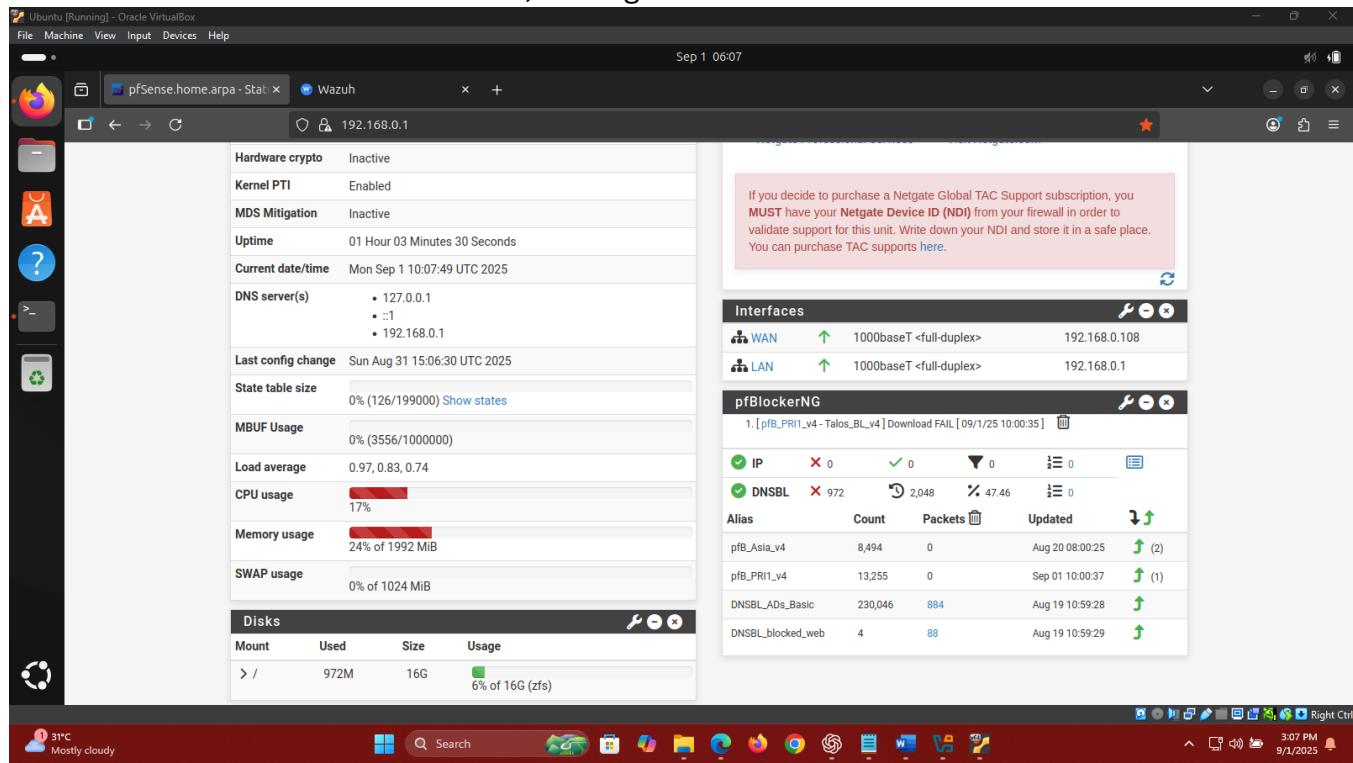
STEP-2

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”.



The screenshot shows the pfSense Firewall configuration interface. At the top, there are tabs for Firewall, Aliases, and IP. The IP tab is selected, showing a list of Firewall Aliases. Below that is a list of Rules.

Firewall Aliases IP

Name	Type	Values	Description	Actions
EICAR	Host(s)	www.eicar.org	Block Suspicious Download	
Gutenberg	Host(s)	www.gutenberg.org	Block Gutenberg	
Reddit	Host(s)	www.reddit.com	Block Reddit	

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/131 kB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4	*	*	pfB_Asia_v4	*	*	none		pfB_Asia_v4 auto rule	
<input type="checkbox"/>	0/0 B	IPv4	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4 auto rule	
<input type="checkbox"/>	0/0 B	IPv4	*	192.168.0.103	*	Gutenberg	*	*	none	Block Gutenberg	
<input type="checkbox"/>	0/0 B	IPv4	*	192.168.0.103	*	Reddit	*	*	none	Block Reddit	
<input type="checkbox"/>	0/0 B	IPv4	*	192.168.0.103	*	EICAR	*	*	none	Block Suspicious Download	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.0.103	*	89.238.73.97	443 (HTTPS)	*	none		Block Suspicious Download	
<input type="checkbox"/>	0/0 B	IPv4	*	192.168.0.103	*	142.250.190.78	*	*	none	Block Google ip	
<input checked="" type="checkbox"/>	✓ 7/9.85 MiB	IPv4	*	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv6	*	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Buttons at the bottom: Add, Add, Delete, Toggle, Copy, Save, Separator.

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).

The screenshot displays two separate browser sessions, both titled "Wazuh" and "pfSense.home.arpa - Stat". Both sessions are viewing the URL 192.168.0.1/status_logs_filter.php. The content of both pages is identical, showing a list of security events from the pfSense firewall. The events are listed in a table format:

Date	Time	Interface	Action	Source IP	Destination IP	Protocol
Aug 31	15:00:00	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.1	224.0.0.1	IGMP
Aug 31	15:00:24	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.107:138	192.168.0.255.138	UDP
Aug 31	15:01:06	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:07	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:08	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:09	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:10	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:11	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:12	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:13	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:14	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:15	LAN	Block Google ip (1756466984)	192.168.0.103	142.250.190.78	ICMP
Aug 31	15:01:25	LAN	pfb_Asia_v4 auto rule (1770009033)	192.168.0.103	123.125.115.110	ICMP
Aug 31	15:01:26	LAN	pfb_Asia_v4 auto rule (1770009033)	192.168.0.103	123.125.115.110	ICMP
Aug 31	15:01:27	LAN	pfb_Asia_v4 auto rule (1770009033)	192.168.0.103	123.125.115.110	ICMP
Aug 31	15:02:05	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.1	224.0.0.1	IGMP
Aug 31	15:02:11	LAN	Block Reddit (1756466118)	192.168.0.103:56140	199.232.173.140:443	TCP:S
Aug 31	15:02:11	LAN	Block Reddit (1756466118)	192.168.0.103:56148	199.232.173.140:443	TCP:S
Aug 31	15:02:11	LAN	Block Reddit (1756466118)	192.168.0.103:56150	199.232.173.140:443	TCP:S
Aug 31	15:02:11	LAN	Block Reddit (1756466118)	192.168.0.103:56152	199.232.173.140:443	TCP:S
Aug 31	15:07:37	LAN	Block Suspicious Download (1756652766)	192.168.0.103:41076	89.238.73.97:443	TCP:S
Aug 31	15:07:37	LAN	Block Suspicious Download (1756652766)	192.168.0.103:41080	89.238.73.97:443	TCP:S
Aug 31	15:07:53	LAN	Block Suspicious Download (1756652766)	192.168.0.103:56598	89.238.73.97:443	TCP:S
Aug 31	15:07:53	LAN	Block Suspicious Download (1756652766)	192.168.0.103:56580	89.238.73.97:443	TCP:S
Aug 31	15:07:53	LAN	Block Suspicious Download (1756652766)	192.168.0.103:56594	89.238.73.97:443	TCP:S
Aug 31	15:07:53	LAN	Block Suspicious Download (1756652766)	192.168.0.103:56578	89.238.73.97:443	TCP:S
Aug 31	15:08:01	LAN	Block Suspicious Download (1756652766)	192.168.0.103:35318	89.238.73.97:443	TCP:S
Aug 31	15:08:01	LAN	Block Suspicious Download (1756652766)	192.168.0.103:35306	89.238.73.97:443	TCP:S
Aug 31	15:08:02	LAN	Block Suspicious Download (1756652766)	192.168.0.103:35322	89.238.73.97:443	TCP:S
Aug 31	15:08:04	LAN	Block Suspicious Download (1756652766)	192.168.0.103:35352	89.238.73.97:443	TCP:S
Aug 31	15:08:20	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.1	224.0.0.1	IGMP
Aug 31	15:10:25	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.1	224.0.0.1	IGMP
Aug 31	15:12:27	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.107:138	192.168.0.255.138	UDP
Aug 31	15:12:30	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.1	224.0.0.1	IGMP
Aug 31	15:14:35	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.0.1	224.0.0.1	IGMP
Aug 31	15:14:53	LAN	Block Gutenberg (1756466082)	192.168.0.103:49156	152.19.134.47:443	TCP:S
Aug 31	15:14:54	LAN	Block Gutenberg (1756466082)	192.168.0.103:49156	152.19.134.47:443	TCP:S
Aug 31	15:14:55	LAN	Block Gutenberg (1756466082)	192.168.0.103:49156	152.19.134.47:443	TCP:S
Aug 31	15:14:56	LAN	Block Gutenberg (1756466082)	192.168.0.103:49156	152.19.134.47:443	TCP:S

Wazuh Monitoring:

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

File Machine View Input Devices Help

Wazuh Threat Hunting

Dashboard Events

manager.name: wazuh-server Add filter

DQL Last 7 days Show dates Refresh

4 hits Aug 24, 2025 @ 11:20:50.939 - Aug 31, 2025 @ 11:20:50.940

Export Formatted 644 available fields Columns Density Fields sorted Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Aug 31, 2025 @ 11:06:49.2...	pfSense.home.arpa	Multiple pfSense firewall blocks events from same source.	10	87702
Aug 31, 2025 @ 11:02:17.6...	pfSense.home.arpa	Multiple pfSense firewall blocks events from same source.	10	87702
Aug 31, 2025 @ 10:40:14.3...	pfSense.home.arpa	Multiple pfSense firewall blocks events from same source.	10	87702

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.

Discover - Wazuh

Discover

wazuh-alerts-* filterlog

Search field Filter by type 0

Selected fields: _source, _index, agent.id, agent.ip, agent.name, data.action, data.command, data.dstip, data.dsport, data.dsuser, data.extra_data, data.file, data.id, data.length

Available fields: _index, agent.id, agent.ip, agent.name, data.action, data.command, data.dstip, data.dsport, data.dsuser, data.extra_data, data.file, data.id, data.length

filterlog

4 hits Aug 24, 2025 @ 11:23:07.755 - Aug 31, 2025 @ 11:23:07.755 per Auto

Count timestamp per 3 hours

Time _source

> Aug 31, 2025 @ 11:06:49.217 predecoder.hostname: pfSense predecoder.program_name: **filterlog** predecoder.timestamp: Aug 31 15:06:48 input.type: log agent.ip: 192.168.0.1 agent.name: pfSense.home.arpa agent.id: 003 previous_output: Aug 31 15:06:48 pfSense filterlog[17184]: 96.,,1756652766,em1,match,block,in,4,0x0.,64,4130,0,DF,6,tcp,68,192.168.0.103,89.238.73.97,56612,443,0,S,3585076261,,65340, ,mss,sackOK,TS;nop;wscale Aug 31 15:06:48 pfSense filterlog[17184]: 96.,,1756652766,em1,match,block,in,4,0x0.,64,33367,0,DF,6,t cp,68,192.168.0.103,89.238.73.97,56594,443,0,S,146574134.,65348,,mss,sackOK,TS;nop;wscale Aug 31 15:06:48 pfSense filterlog[17184]: 94.,,1756466118,em1,match,block,in,4,0x0.,64,15822,0,DF,6,tcp,60,192.168.0.103,199.232.173.140,56140,443,0,S,1534073879.,64 240_mss:sackOK:TS:nop;wscale Aug 31 15:02:14_pfSense.filterlog[17184]: 94.,,1756466118,em1,match,block,in,4,0x0.,64,20111,0,DF

> Aug 31, 2025 @ 11:02:17.618 predecoder.hostname: pfSense predecoder.program_name: **filterlog** predecoder.timestamp: Aug 31 15:02:15 input.type: log agent.ip: 192.168.0.1 agent.name: pfSense.home.arpa agent.id: 003 previous_output: Aug 31 15:02:15 pfSense filterlog[17184]: 94.,,1756466118,em1,match,block,in,4,0x0.,64,15822,0,DF,6,tcp,60,192.168.0.103,199.232.173.140,56140,443,0,S,1534073879.,64 240_mss:sackOK:TS:nop;wscale Aug 31 15:02:14_pfSense.filterlog[17184]: 94.,,1756466118,em1,match,block,in,4,0x0.,64,20111,0,DF

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

Ubuntu [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 31 11:21

Wazuh pfSense.home.arpa - Stats

192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),query:(language:kuery,query:pfSense))&_g=(

Threat Hunting

Dashboard Events

pfsense

manager.name: wazuh-server Add filter

Document Details

View surrounding documents View single document

t agent.ip	192.168.0.1
t agent.name	pfSense.home.arpa
t data.action	block
t data.dstip	89.238.73.97
t data.dstport	443
t data.id	1756652766
t data.length	0
t data.protocol	tcp
t data.srcip	192.168.0.103
t data.srcport	56580
t decoder.name	pf
t full_log	Aug 31 15:06:48 pfSense filterlog[17184]: 96.,,1756652766,em1,matc h,block,in,4,0x0,,64,43279,0,DF,6,tcp,69,192.168.0.103,89,238.73.9 7,56580,443,0,S,882112719,,65340,,mss;sackOK;TS:nop;wscale
t id	1756652809_58366
t input.type	log
t location	/var/log/filter.log
t manager.name	wazuh-server

Export Formatted 644 available fields Columns Density 1 fields sorted Full screen

timestamp agent.name rule.description

Aug 31, 2025 @ 11:06:49.2... pfSense.home.arpa Multiple pfSense firewall blo...
Aug 31, 2025 @ 11:02:17.6... pfSense.home.arpa Multiple pfSense firewall blo...
Aug 31, 2025 @ 10:40:14.3... pfSense.home.arpa Multiple pfSense firewall blo...

28°C Partly cloudy Search 8:21 PM 8/31/2025 Right Ctrl

Ubuntu [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 31 15:06:48

Wazuh pfSense.home.arpa - Stats

192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:('\$state':(store:appState),meta:(alias:In,disabled:Out)),query:(language:kuery,query:pfSense))&_g=(

Threat Hunting

Dashboard Events

Search

manager.name: wazuh-server rule.groups: pfsense Add filter

Document Details

View surrounding documents View single document

t rule.description	Multiple pfSense firewall blocks events from same source.
# rule.firedtimes	3
# rule.frequency	18
t rule.gpg13	4.12
t rule.groups	pfsense, multiple_blocks
t rule.hipaa	164.312.a.1, 164.312.b
t rule.id	87702
# rule.level	10
rule.mail	false
t rule.mitre.id	T1110
t rule.mitre.tactic	Credential Access
t rule.mitre.technique	Brute Force
t rule.nist_800_53	SC.7, AU.6
t rule.pci_dss	1.4, 10.6.1
t rule.tsc	CC6.7, CC6.8, CC7.2, CC7.3
timestamp	Aug 31, 2025 @ 11:06:49.217

Export Formatted 644 available fields Columns Density 1 fields sorted Full screen

timestamp agent.name rule.description

Aug 31, 2025 @ 11:06:49.2... pfSense.home.arpa Multiple pfSense firewall blo...
Aug 31, 2025 @ 11:02:17.6... pfSense.home.arpa Multiple pfSense firewall blo...
Aug 31, 2025 @ 10:40:14.3... pfSense.home.arpa Multiple pfSense firewall blo...

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 Threat Hunting

Dashboard Events

manager.name: wazuh-server rule-groups: pfSense

Export Formatted 644 available fields Columns Density 1 fields sorted Full screen

Aug 31, 2025 @ 11:06:49... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Aug 31, 2025 @ 11:02:17... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Aug 31, 2025 @ 10:40:14... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Aug 30, 2025 @ 11:26:53... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Document Details

View surrounding documents View single document

t predecoder.program_name	filterlog
t predecoder.timestamp	Aug 31 15:06:48
t 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,68,192.168.0.183,89.238.73.97,56612,443,B,S,3585076261,,65348,,mss;sackOK;TS:no p;wscale
t rule.description	Multiple pfSense firewall blocks events from same source.
# rule.firetimes	3
# rule.frequency	18
t rule.gpg13	4.12
t rule.groups	pfSense, multiple_blocks
t rule.hipaa	164.312.a.1, 164.312.b
t rule.id	87782
# rule.level	10
rule.mail	false
t rule.mitre.id	T1110
t rule.mitre.tactic	Credential Access
t rule.mitre.technique	Brute Force
t rule.nist_800_53	SC.7, AU.6
t rule.poi_dss	1.4, 10.6.1
t rule.tsc	CC6.7, CC6.8, CC7.2, CC7.3
t timestamp	Aug 31, 2025 @ 11:06:49.217

28°C Partly cloudy 8:25 PM 8/31/2025

Ubuntu [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 31 11:25

Wazuh Threat Hunting

Dashboard Events

manager.name: wazuh-server rule-groups: pfSense

Export Formatted 644 available fields Columns Density 1 fields sorted Full screen

Aug 31, 2025 @ 11:06:49... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Aug 31, 2025 @ 11:02:17... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Aug 31, 2025 @ 10:40:14... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Aug 30, 2025 @ 11:26:53... pfSense.home.arpa

Multiple pfSense firewall blocks events from same source.

Document Details

View surrounding documents View single document

Table JSON

t _index	wazuh-alerts-4.x-2025.08.31
t agent.id	003
t agent.ip	192.168.0.1
t agent.name	pfSense.home.arpa
t data.action	block
t data.dstip	89.238.73.97
t data.dsport	443
t data.id	1756652766
t data.length	0
t data.protocol	tcp
t data.srcip	192.168.0.183
t data.sport	56580
t decoder.name	pf
t 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,68,192.168.0.183,89.238.73.97,56580,443,B,S,882112719,,65348,,mss;sackOK;TS:no p;wscale
t id	1756652766.58366
t input.type	log
t location	/var/log/filter.log
t manager.name	wazuh-server
t predecoder.hostname	pfSense
t predecoder.program_name	filterlog

28°C Partly cloudy 8:25 PM 8/31/2025

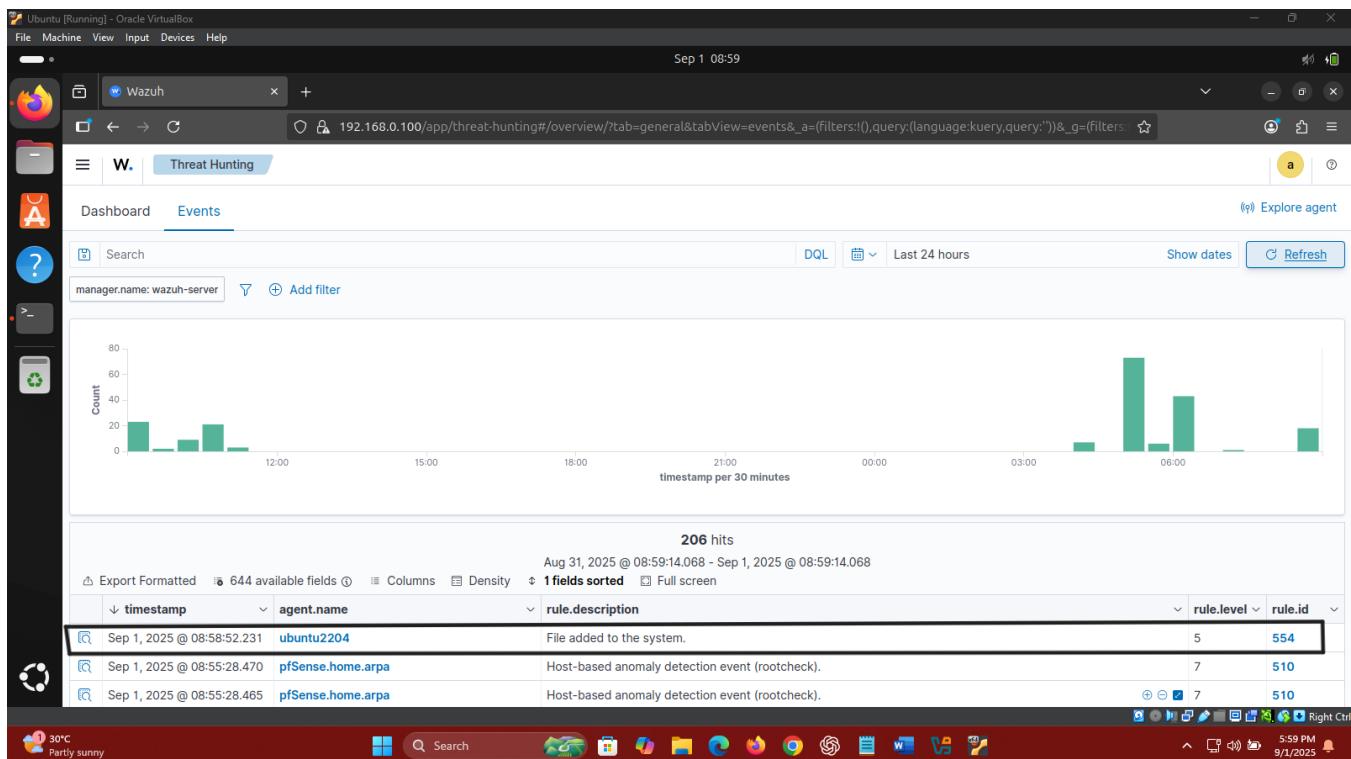
STEP-3

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” .

The screenshot shows the Wazuh Threat Hunting interface. On the left, there's a search bar with 'manager.name: wazuh-server' and a chart showing event counts over time. On the right, the 'Document Details' section displays a table of event fields and their values.

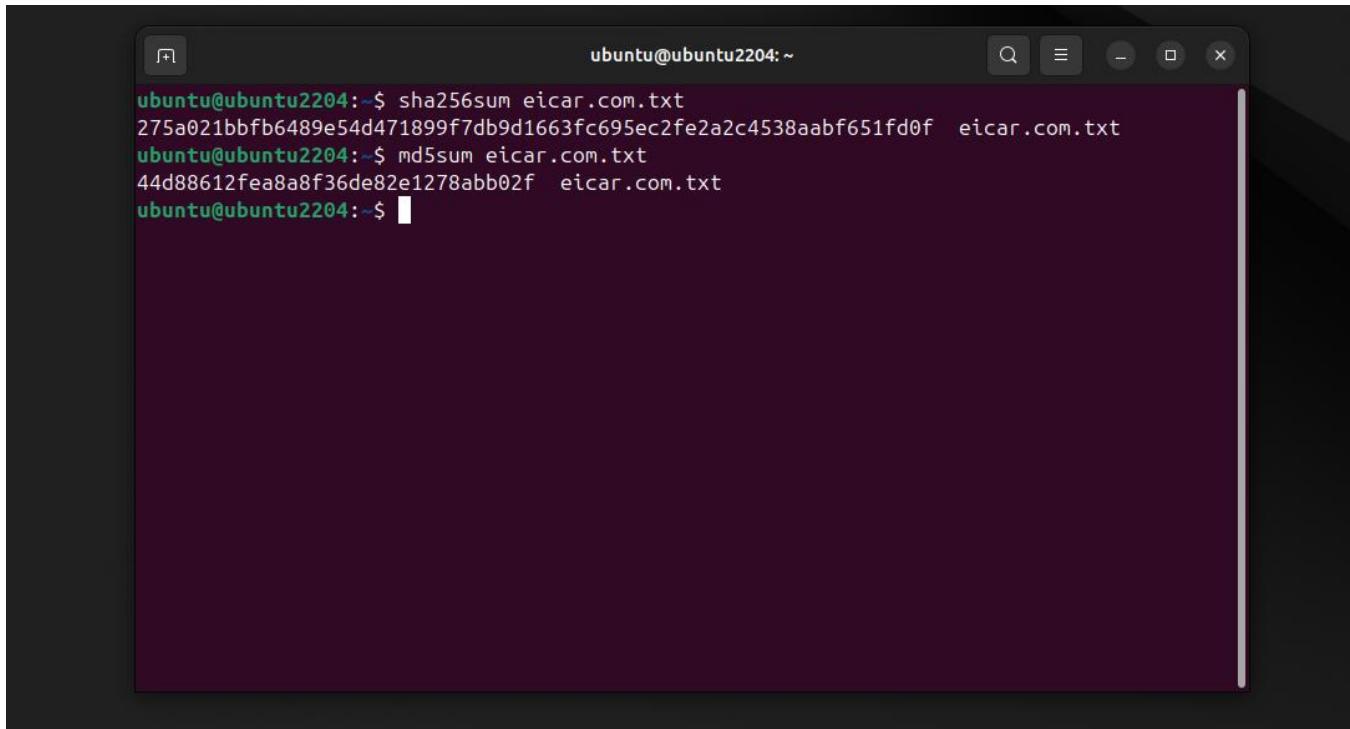
Table	JSON
t _index	wazuh-alerts-4.x-2025.09.01
t agent.id	002
t agent.ip	192.168.0.103
t agent.name	ubuntu2204
t decoder.name	syscheck_new_entry
t full_log	File '/home/ubuntu/malware/eicar.com.txt' added Mode: realtime
t id	1756731532.146615
t input.type	log
t location	syscheck
t manager.name	wazuh-server
t rule.description	File added to the system.
# rule.firedtimes	1
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file

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

This screenshot is identical to the one above, showing the same Wazuh Threat Hunting interface with event details for a malware detection. The 'Document Details' table contains the same information as the first screenshot.

Table	JSON
t rule.pci_dss	11.5
t rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3
t syscheck.event	added
t syscheck.gid_after	1000
t syscheck.gname_after	ubuntu
t syscheck.inode_after	2625152
t syscheck.md5_after	44d88612fea8a8f36de82e1278abb02f
t syscheck.mode	realtime
✉ syscheck.mtime_after	Aug 31, 2025 @ 10:32:32.000
t syscheck.path	/home/ubuntu/malware/eicar.com.txt
t syscheck.perm_after	rw-rw-r--
t syscheck.sha1_after	3395856ce81f2b7382dee72602f798b642f14140
t syscheck.sha256_after	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
# syscheck.size_after	68
t syscheck.uid_after	1000
t syscheck.uname_after	ubuntu
✉ timestamp	Sep 1, 2025 @ 08:58:52.231

4) The Hashes Confirmed The incident !



A terminal window titled "ubuntu@ubuntu2204: ~" showing command-line output. The user runs "sha256sum eicar.com.txt" and "md5sum eicar.com.txt", both of which return the same results as the ones listed below.

```
ubuntu@ubuntu2204:~$ sha256sum eicar.com.txt
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f  eicar.com.txt
ubuntu@ubuntu2204:~$ md5sum eicar.com.txt
44d88612fea8a8f36de82e1278abb02f  eicar.com.txt
ubuntu@ubuntu2204:~$
```

.....

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

```
ubuntu@ubuntu2204:~$ clamscan /home/ubuntu/malware/
Loading: 40s, ETA: 0s [=====>] 8.71M/8.71M sigs
Compiling: 4s, ETA: 0s [=====>] 41/41 tasks

/home/ubuntu/malware/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Known viruses: 8708177
Engine version: 1.4.3
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 45.895 sec (0 m 45 s)
Start Date: 2025:09:01 09:25:10
End Date: 2025:09:01 09:25:55
ubuntu@ubuntu2204:~$
```

.....

Phase-3

1) Wazuh Detection of Malware Behaviour.

timestamp	agent.name	rule.description	rule.level	rule.id
Sep 1, 2025 @ 11:08:18.830	ubuntu2204	ClamAV: Virus detected	8	52502
Sep 1, 2025 @ 11:08:18.830	ubuntu2204	PAM: Login session closed.	3	5502
Sep 1, 2025 @ 11:08:18.830	ubuntu2204	ClamAV: Virus detected	8	52502
Sep 1, 2025 @ 11:08:18.829	ubuntu2204	PAM: Login session opened.	3	5501
Sep 1, 2025 @ 11:08:18.778	ubuntu2204	Successful sudo to ROOT executed.	3	5402
Sep 1, 2025 @ 11:08:18.738	ubuntu2204	ClamAV: Virus detected	8	52502
Sep 1, 2025 @ 11:08:18.737	ubuntu2204	ClamAV: Virus detected	8	52502
Sep 1, 2025 @ 11:08:06.808	ubuntu2204	PAM: Login session opened.	3	5501
Sep 1, 2025 @ 11:08:06.808	ubuntu2204	PAM: Login session closed.	3	5502
Sep 1, 2025 @ 11:08:06.759	ubuntu2204	Successful sudo to ROOT executed.	3	5402
Sep 1, 2025 @ 11:08:12.659	ubuntu2204	PAM: Login session closed.	3	5502
Sep 1, 2025 @ 11:08:12.608	ubuntu2204	Successful sudo to ROOT executed.	3	5402
Sep 1, 2025 @ 11:08:12.608	ubuntu2204	PAM: Login session opened.	3	5501
Sep 1, 2025 @ 11:08:12.608	ubuntu2204	Clamd warning	7	52504
Sep 1, 2025 @ 11:08:12.608	ubuntu2204	Clamd warning	7	52504

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

The screenshot shows the Wazuh Threat Hunting interface. On the left, there's a search bar with the filter "manager.name: wazuh-server". Below it is a chart showing event counts over time, with a peak of 284 at 11:08:18.830. To the right, a table lists log entries. One entry is expanded, showing detailed information in a "Document Details" panel.

	Value
_index	wazuh-alerts-4.x-2025.09.01
agent.id	002
agent.ip	192.168.0.103
agent.name	ubuntu2204
data.extra_data	Win.Test.EICAR_HDB-1
data.id	44d88612fea8a8f36de82e1278abb02f
data.url	/home/ubuntu/malware/eicar.com.txt
decoder.name	clamd
decoder.parent	clamd
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
id	1756739298.207148
input.type	log
location	journald
manager.name	wazuh-server

The screenshot shows the Wazuh Threat Hunting interface. On the left, there's a timeline chart with a search bar and filter options. Below the chart, a table lists events with columns for timestamp, agent.name, and rule.description. One event is highlighted: "Sep 1, 2025 @ 11:08:18.830 ubuntu2204 ClamAV: Virus detected". On the right, a detailed view of this event is shown under "Document Details".

Field	Value
t location	journald
t manager.name	wazuh-server
t predecoder.hostname	ubuntu2204
t predecoder.program_name	clamd
t predecoder.timestamp	Sep 01 15:08:17
t rule.description	ClamAV: Virus detected
# rule.firetimes	3
t rule.gdpr	IV_35.7.d
t rule.gpp13	4.2
t rule.groups	clamd, freshclam, virus
t rule.id	52502
# rule.level	8
rule.mail	false
t rule.nist_800_53	SI.3, SI.4
t rule.pci_dss	5.1, 5.2, 11.4
t rule.tsc	A1.2, C06.1, C06.8, C07.2, C07.3
timestamp	Sep 1, 2025 @ 11:08:18.830

Phase-4

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

IOCS & 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)

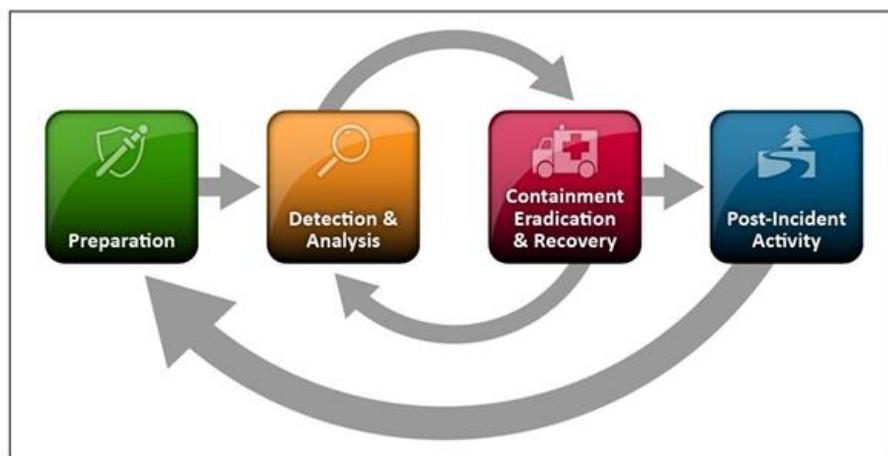


Figure 3-1. Incident Response Life Cycle

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