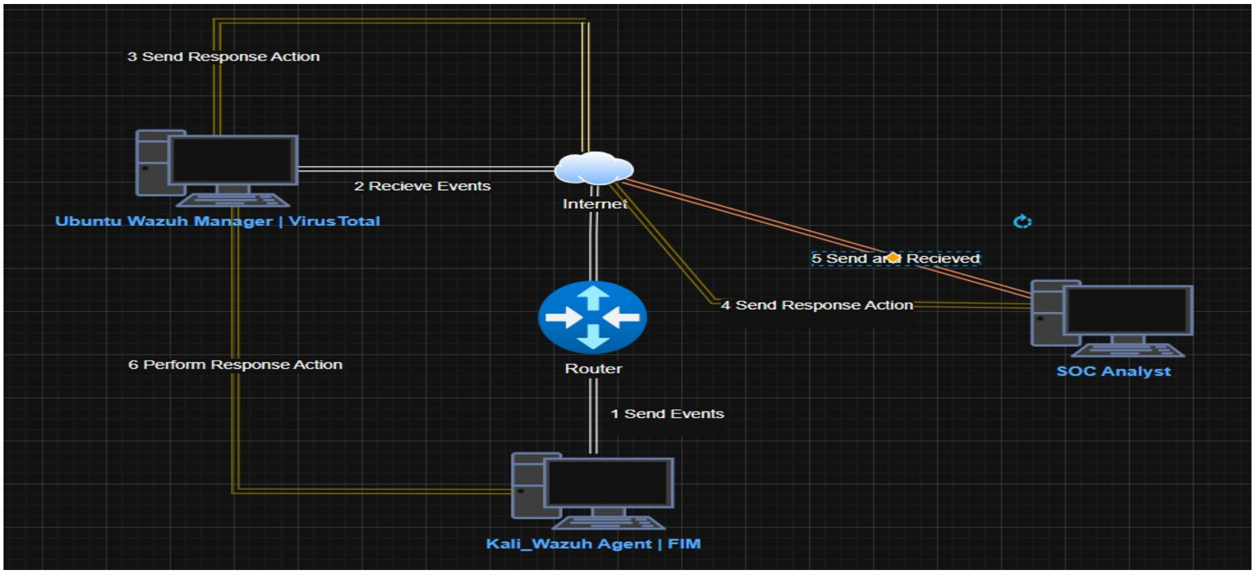
Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Project Name: Stop Malware INSTANTLY with Wazuh & VirusTotal Automation!



Project Objectives: Wazuh - VirusTotal Integration

This integration project enhances endpoint security by combining **Wazuh's File Integrity Monitoring (FIM)** with the **VirusTotal API** to automatically detect and eliminate malicious content. By continuously monitoring files and directories and leveraging VirusTotal's threat intelligence, the system proactively identifies and removes malware with minimal manual intervention.

Key Implementation Steps:

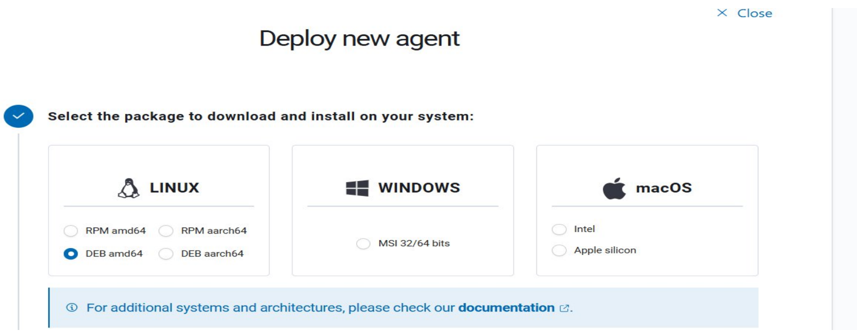
- **Deploy Wazuh Manager and Agent**
  Install and configure Wazuh components on both Ubuntu and Kali Linux environments to establish a robust monitoring infrastructure.
- **Enable File Integrity Monitoring (FIM)**
  Set up Wazuh's FIM module to track changes across critical files and directories, ensuring real-time visibility into potential tampering or unauthorized modifications.
- **Integrate VirusTotal API**
  Connect Wazuh with the VirusTotal API to scan monitored files against a vast database of known threats, enabling automated malware detection.
- **Automate Threat Response**
  Implement logic for automatic threat deletion and generate actionable threat analysis reports to support incident response and forensic review.

Prerequisites:

1. Install **Wazuh Manager in your Ubuntu** machine.
2. Install **Wazuh Agent in your Kali Linux** Machine.

2.1. In your Kali open a web browser and login to your Wazuh > Install the agent

2.2. Click the active one > click deploy new agent



Deploy new agent

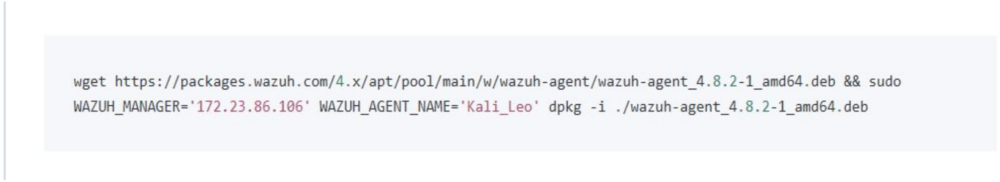
Select the package to download and install on your system:

LINUX: ○ RPM amd64 ○ RPM aarch64 ● DEB amd64 ○ DEB aarch64

WINDOWS: ○ MSI 32/64 bits

macOS: ○ Intel ○ Apple silicon

For additional systems and architectures, please check our **documentation**.



```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.2-1_amd64.deb && sudo
WAZUH_MANAGER='172.23.86.106' WAZUH_AGENT_NAME='Kali_Leo' dpkg -i ./wazuh-agent_4.8.2-1_amd64.deb
```

2.3 Start the Wazu-Agent

```
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
```

2.4 Verify the status

```
systemctl status wazuh-agent
```

Configure the FIM (File Integrity Monitoring)

1. **How it works:**
   - Wazuh **FIM** looks for any file addition, change, or deletion on the monitored folders. This module has the hash of these files stored and triggers alerts when it detects any changes.
   - If enabled, **Wazuh triggers the VirusTotal integration when an FIM alert occurs**. From this alert, the integration extracts the hash field of the file.
   - The integration then makes an **HTTP POST** request to the VirusTotal database using the VirusTotal API. This call sends the extracted file hash to compare it with the information in the VirusTotal database.

- The integration receives a **JSON response**, which is the result of the request. The response triggers one of the following Wazuh alerts:

  - ✓ Error: Check credentials.
  - ✓ Error: Public API request rate limit reached.
  - ✓ Alert: No records in VirusTotal database.
  - ✓ Alert: No positives found.
  - ✓ Alert: X engines detected this file. X is the number of antivirus engines.

2. In Kali where **Wazuh agent** installed create a directory /tmp/malware. Open your terminal in sudo mode.

```
# mkdir /tmp/malware
# chmod 777 /tmp/malware
```

3. In your **Wazuh manager Ubuntu** configure the **agent.conf** for **FIM** real monitoring

Click the Hamburger > Server Management > Endpoint Groups > click the pencil to edit the default and provide the configuration below > click Save.

This is for Linux:

```
<agent_config os="Linux">
        <!-- Shared agent configuration here -->
        <syscheck>
                <directories realtime="yes" check_all="yes"> /tmp/malware</directories>
        </syscheck>
</agent_config>
```

This is for Windows:

```
<agent_config os="Windows">
  <syscheck>
    <disabled>no</disabled>
    <scan_on_start>yes</scan_on_start>
    <frequency>43200</frequency> <!-- every 12 hours -->
    <directories check_all="yes" realtime="yes">C:\Windows</directories>
    <directories check_all="yes" realtime="yes">C:\Program Files</directories>
    <directories check_all="yes" realtime="yes">C:\Users</directories>
    <ignore>C:\Windows\Temp</ignore>
    <ignore>C:\Windows\Prefetch</ignore>
<registry>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</registry>
    <registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services</registry>
    <registry>HKEY_LOCAL_MACHINE\Security</registry>
```

<registry>HKEY_LOCAL_MACHINE\Software\Policies</registry>
<registry>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</registry> </syscheck>
</agent_config>

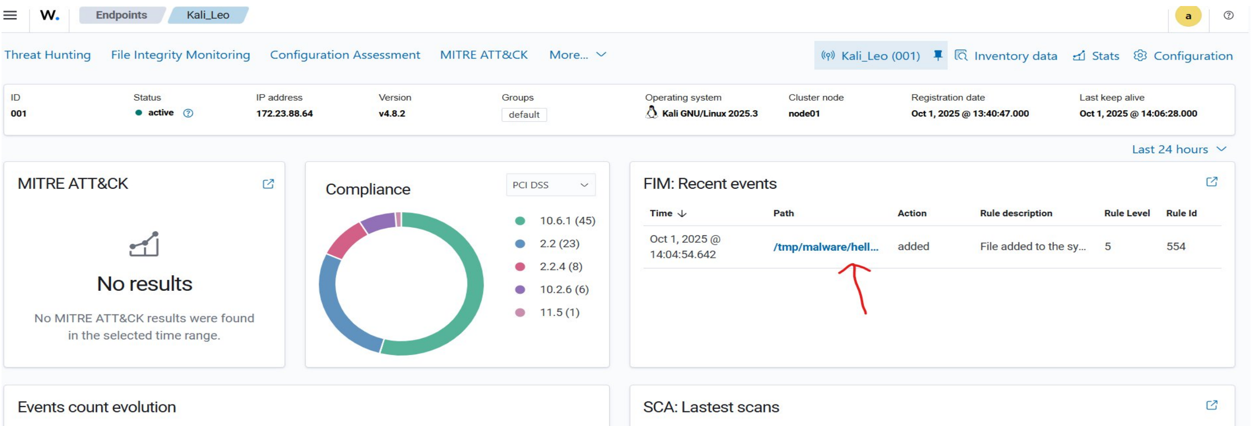
4. Now, go back to your **Wazuh agent Kali** and restart the Wazuh.

   Systemctl restart wazuh-agent

5. Now, we will test the FIM (**File Integrity Monitoring**) > in your agent **Kali** create a hello.txt in your terminal type below.

   Echo “hello” >> /tmp/malware/hello.txt

6. How to verify the FIM in your **Wazuh Manager** > click Agent Summary Active > click **Kali_Leo** > verify FIM:

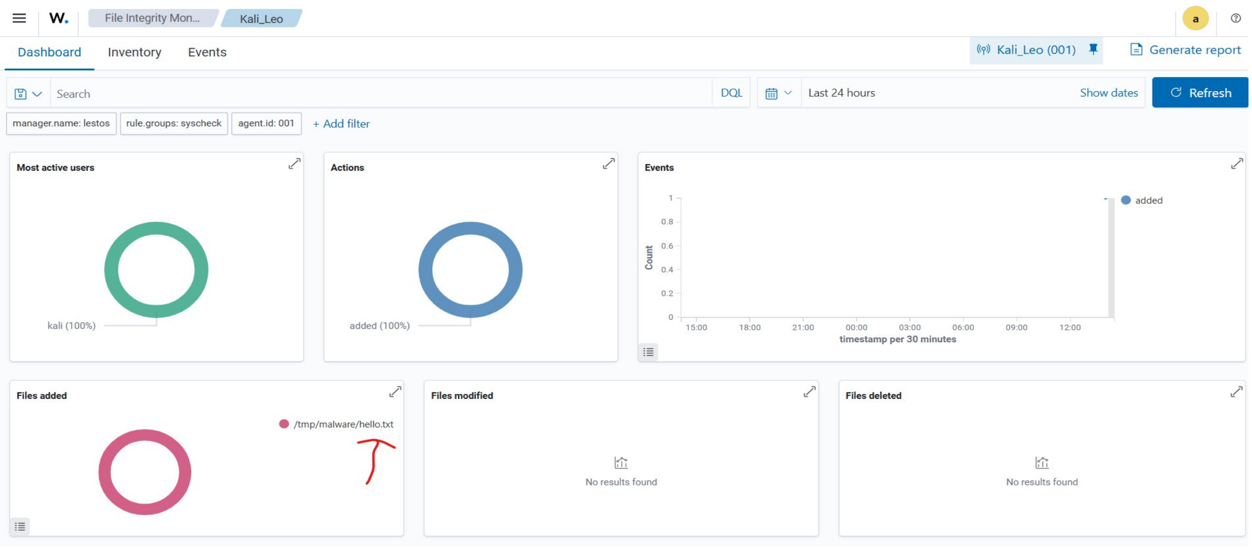


ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	active	172.23.88.64	v4.8.2	default	Kali GNU/Linux 2025.3	node01	Oct 1, 2025 @ 13:40:47.000	Oct 1, 2025 @ 14:06:28.000

FIM: Recent events

Time	Path	Action	Rule description	Rule Level	Rule Id
Oct 1, 2025 @ 14:04:54.642	/tmp/malware/hell...	added	File added to the sy...	5	554

7. Go to **File Integrity Monitoring** and verify the update:



manager.name: lestos | rule.groups: syscheck | agent.id: 001 | + Add filter

We will now configure the Virus Total Integration:

1. **What is Virustotal**. A powerful platform aggregating **multiple antivirus products** and an **online scanning engine**. Is an online service that analyzes files and URLs to detect **viruses, worms, trojans, and other malicious content** using antivirus engines and website scanners.
2. Go to https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/virus-total-integration.html to check the **VirusTotal Integration for Scanning a file.**
3. Follow the instructions from **External API integration** to enable the Integrator module and configure the VirusTotal integration.

   Below is an example of settings you must add to the **/var/ossec/etc/ossec.conf** file on the **Wazuh server Ubuntu**:

   ```
   <integration>
     <name>virustotal</name>
    <api_key>API_KEY</api_key> <!-- Replace with your VirusTotal API key -->
    <group>syscheck</group>
     <alert_format>json</alert_format>
   </integration>
   ```

4. Login to your Wazuh Manager Ubuntu machine > go to **ossec.conf**
   In your terminal provide a command > **sudo nano /var/ossec/etc/ossec.conf**
   Go all the way to the bottom and add the Virus Total Integration

   ```
   <integration>
     <name>virustotal</name>
    <api_key>API_KEY</api_key> <!-- Replace with your VirusTotal API key -->
    <group>syscheck</group>
     <alert_format>json</alert_format>
   </integration>
   ```

   CTRL X + Y = to save

5. To get your VirusTotal API Key > **Login to Virustotal** with your account and go to API Key

6. Restart your Wazuh Manager

   ```
   Systemctl daemon-reload
   Systemctl restart wazuh-manager
   Systemctl startus wazuh-manager
   ```

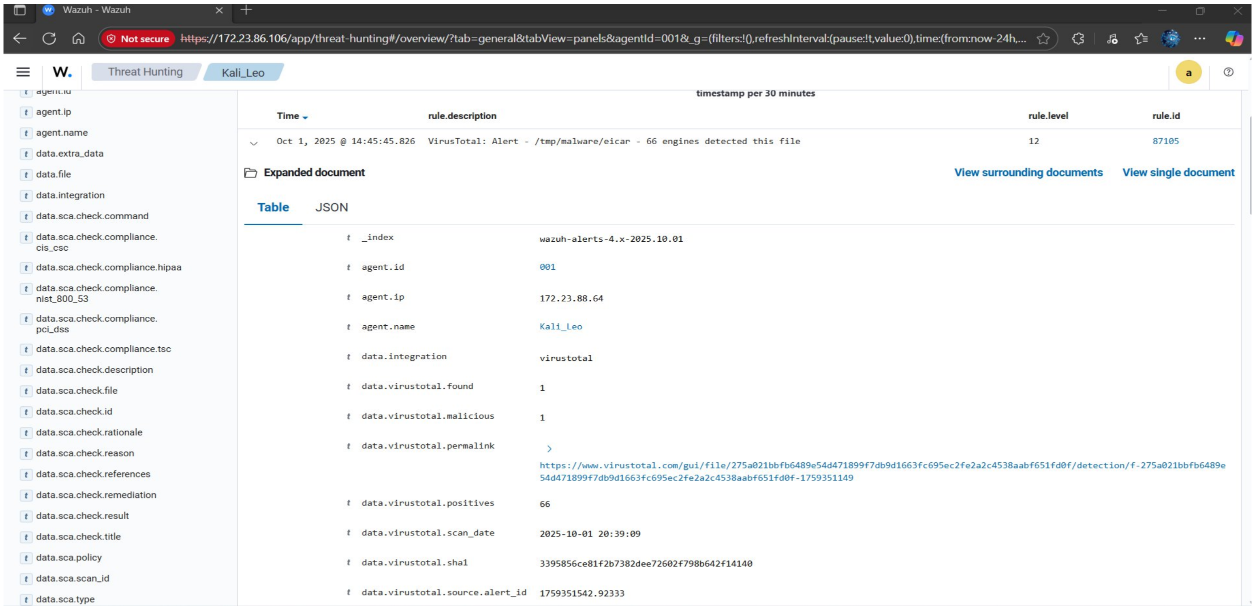
7. **Attack emulation:** We will now start to test using the malicious file. In your **Wazuh agent Kali** > Open the terminal and run below

   Go to your created folder cd /tmp/malware

   Run > sudo curl https://secure.eicar.org/eicar.com -o /tmp/malware/eicar

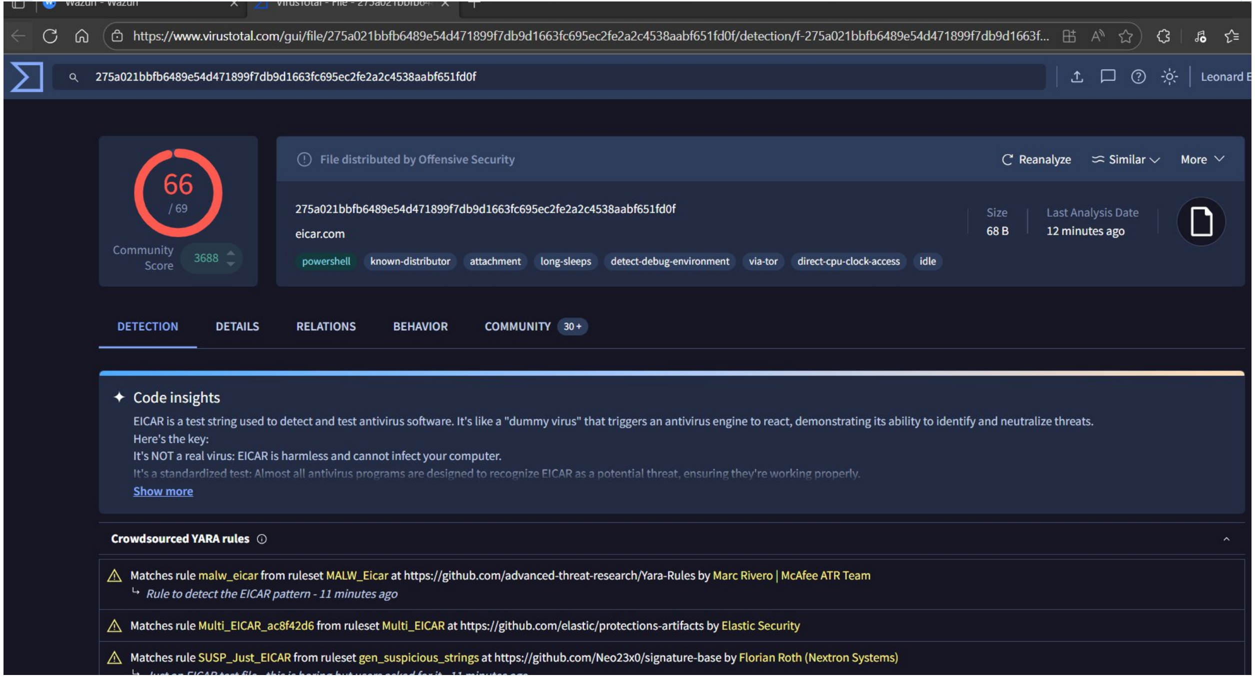
   https://secure.eicar.org/eicar.com = is a malicious website for testing only

8. Login to Wazuh Server Manager > Click Kali_Leo > click **Threat Hunting** > click Events


Wazuh - Wazuh
Not secure
https://172.23.86.106/app/threat-hunting#/overview/?tab=general&tabView=panels&agentId=001&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,...
W.
Threat Hunting
Kali_Leo
a
agent.id
agent.ip
agent.name
data.extra_data
data.file
data.integration
data.sca.check.command
data.sca.check.compliance.cis_csc
data.sca.check.compliance.hipaa
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.pci_dss
data.sca.check.compliance.tsc
data.sca.check.description
data.sca.check.file
data.sca.check.id
data.sca.check.rationale
data.sca.check.reason
data.sca.check.references
data.sca.check.remediation
data.sca.check.result
data.sca.check.title
data.sca.policy
data.sca.scan_id
data.sca.type
timestamp per 30 minutes
Expanded document
View surrounding documents
View single document
Table
JSON

Time	rule.description	rule.level	rule.id
Oct 1, 2025 @ 14:45:45.826	VirusTotal: Alert - /tmp/malware/eicar - 66 engines detected this file	12	87105

_index	wazuh-alerts-4.x-2025.10.01
agent.id	001
agent.ip	172.23.88.64
agent.name	Kali_Leo
data.integration	virustotal
data.virustotal.found	1
data.virustotal.malicious	1
data.virustotal.permalink	https://www.virustotal.com/gui/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f/detection/f-275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f-1759351149
data.virustotal.positives	66
data.virustotal.scan_date	2025-10-01 20:39:09
data.virustotal.sha1	3395856ce81f2b7382dee72602f798b642f14140
data.virustotal.source.alert_id	1759351542.92333



275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

File distributed by Offensive Security

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com

Size: 68 B

Last Analysis Date: 12 minutes ago

✦ Code insights

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats.
Here's the key:
It's NOT a real virus: EICAR is harmless and cannot infect your computer.
It's a standardized test: Almost all antivirus programs are designed to recognize EICAR as a potential threat, ensuring they're working properly.

Show more

Crowdsourced YARA rules

⚠ Matches rule malw_eicar from ruleset MALW_Eicar at https://github.com/advanced-threat-research/Yara-Rules by Marc Rivero | McAfee ATR Team
↳ *Rule to detect the EICAR pattern - 11 minutes ago*

⚠ Matches rule Multi_EICAR_ac8f42d6 from ruleset Multi_EICAR at https://github.com/elastic/protections-artifacts by Elastic Security

⚠ Matches rule SUSP_Just_EICAR from ruleset gen_suspicious_strings at https://github.com/Neo23x0/signature-base by Florian Roth (Nextron Systems)
↳ *Just an EICAR test file - this is boring but users asked for it - 11 minutes ago*

9. We need to create a script in the **Agent machine Kali to create or trigger when a malicious file is found** > Go to Wazuh site and check the **Wazuh Proof of Concept guide/ Detecting and removing malware using VirusTotal Integration.**

   Perform the following steps to configure Wazuh to monitor near real-time changes in the /root directory of the Ubuntu endpoint. These steps also install the necessary packages and create the active response script that removes malicious files. https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html

   Install **jq**, a utility that processes JSON input from the active response script:

   ```
   # sudo apt install jq
   # sudo su
   #nano /var/ossec/active-response/bin/remove-threat.sh
   ```

   - Now, paste the script of **#4** > ctrl + x then Y

   ```
   #!/bin/bash


   LOCAL=`dirname $0`;
   cd $LOCAL
   cd ../

   PWD=`pwd`

   read INPUT_JSON
   FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
   COMMAND=$(echo $INPUT_JSON | jq -r .command)
   LOG_FILE="${PWD}/../logs/active-responses.log"

   #------------------------ Analyze command -------------------------#
   if [ ${COMMAND} = "add" ]
   then
    # Send control message to execd
    printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"check_keys",
   "parameters":{"keys":[]}}\n'

    read RESPONSE
    COMMAND2=$(echo $RESPONSE | jq -r .command)
    if [ ${COMMAND2} != "continue" ]
    then
     echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Remove threat active response aborted" >> ${LOG_FILE}
     exit 0;
    fi
   fi

   # Removing file
   rm -f $FILENAME
   if [ $? -eq 0 ]; then
    echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Successfully removed threat" >> ${LOG_FILE}
   else
    echo "`date '+%Y/%m/%d %H:%M:%S'` $0: $INPUT_JSON Error removing threat" >> ${LOG_FILE}
   fi

   exit 0;
   ```

- Now change the permission: Change the /var/ossec/active-response/bin/remove-threat.sh file ownership, and permissions:

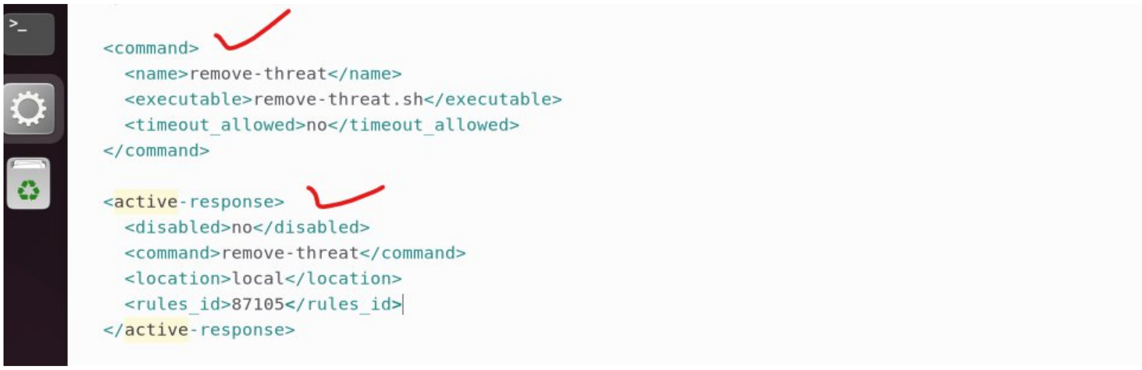
  # sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh
  # sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh

- Systemctl restart wasuh-agent

10. Now, go to **Wazuh Manager Ubuntu** and run below

    # Xdg-open /var/ossec/etc/ossec.conf

- Text editor will now open
- Search active response > copy and paste <name>netsh</name> and add below code and activate the response code.



```
<command>
  <name>remove-threat</name>
  <executable>remove-threat.sh</executable>
  <timeout_allowed>no</timeout_allowed>
</command>

<active-response>
  <disabled>no</disabled>
  <command>remove-threat</command>
  <location>local</location>
  <rules_id>87105</rules_id>
</active-response>
```

- Click Save and Close
- Now, restart the Wazuh Manager
  - # systemctl daemon-reload
  - # systemctl restart wazuh-manager
  - # systemctl status wazuh-manager

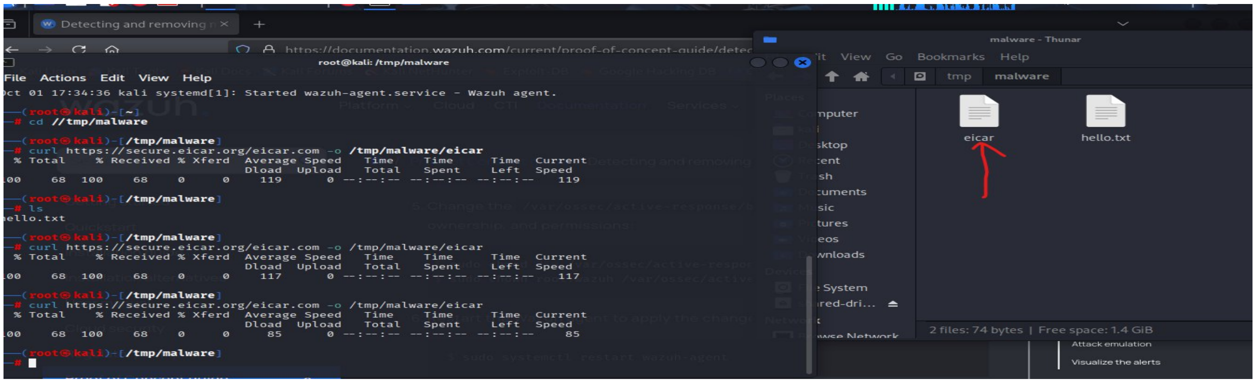
11. **Simulation and Testing**: We will now start to test using the malicious file again. In your **Wazuh agent Kali** > Open the terminal and run below.

- Go to your created folder cd /tmp/malware

  - Run > # curl https://secure.eicar.org/eicar.com -o /tmp/malware/eicar

- Go to Folder /tmp/malware/

- **Take a look and eicar.com it will automatically be deleted.**

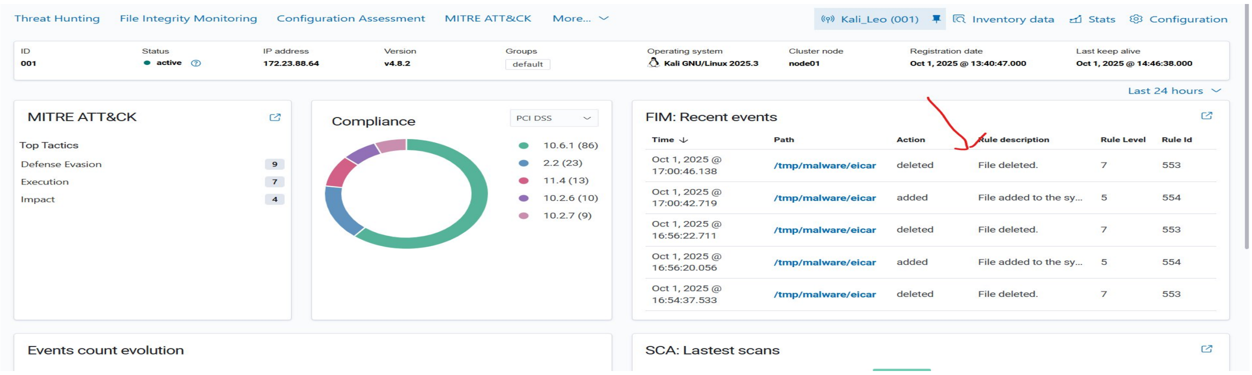


root@kali: /tmp/malware

```
Oct 01 17:34:36 kali systemd[1]: Started wazuh-agent.service - Wazuh agent.

┌──(root㉿kali)-[~]
└─# cd //tmp/malware

┌──(root㉿kali)-[/tmp/malware]
└─# curl https://secure.eicar.org/eicar.com -o /tmp/malware/eicar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    68  100    68    0     0    119      0 --:--:-- --:--:-- --:--:--   119

┌──(root㉿kali)-[/tmp/malware]
└─# ls
hello.txt

┌──(root㉿kali)-[/tmp/malware]
└─# curl https://secure.eicar.org/eicar.com -o /tmp/malware/eicar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    68  100    68    0     0    117      0 --:--:-- --:--:-- --:--:--   117

┌──(root㉿kali)-[/tmp/malware]
└─# curl https://secure.eicar.org/eicar.com -o /tmp/malware/eicar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    68  100    68    0     0     85      0 --:--:-- --:--:-- --:--:--    85

┌──(root㉿kali)-[/tmp/malware]
└─# 
```

2 files: 74 bytes | Free space: 1.4 GiB

12. Now, for testing and verification click Kali_Leo > See the **FIM** action below.



ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	● active	172.23.88.64	v4.8.2	default	Kali GNU/Linux 2025.3	node01	Oct 1, 2025 @ 13:40:47.000	Oct 1, 2025 @ 14:46:38.000

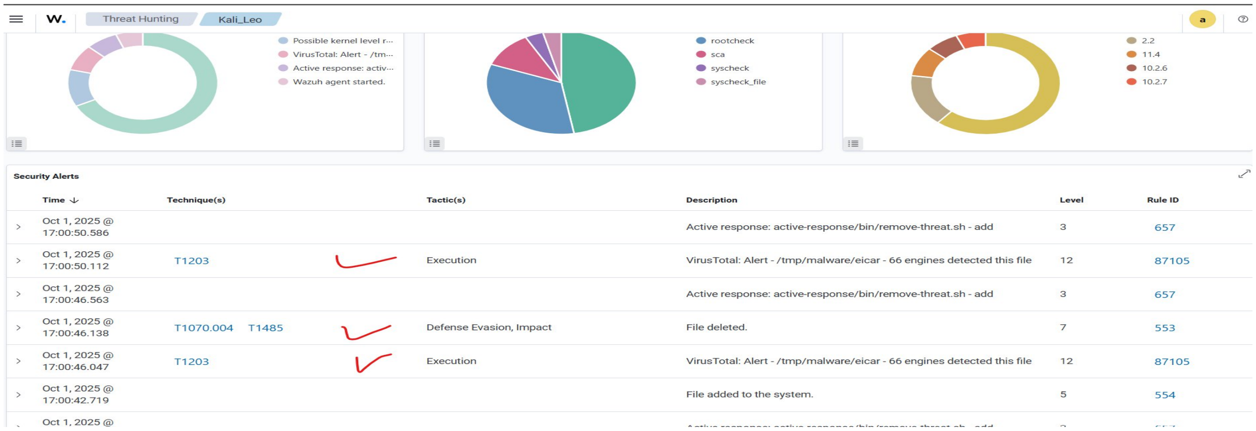
MITRE ATT&CK

Top Tactics	
Defense Evasion	9
Execution	7
Impact	4

FIM: Recent events

Time	Path	Action	Rule description	Rule Level	Rule Id
Oct 1, 2025 @ 17:00:46.138	/tmp/malware/eicar	deleted	File deleted.	7	553
Oct 1, 2025 @ 17:00:42.719	/tmp/malware/eicar	added	File added to the sy...	5	554
Oct 1, 2025 @ 16:56:22.711	/tmp/malware/eicar	deleted	File deleted.	7	553
Oct 1, 2025 @ 16:56:20.056	/tmp/malware/eicar	added	File added to the sy...	5	554
Oct 1, 2025 @ 16:54:37.533	/tmp/malware/eicar	deleted	File deleted.	7	553

- Now, click the Threat Hunting and see the **Technique, Tactic & Procedures (TTP's) | (MITRE ATT&CK) CVE.**



Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Oct 1, 2025 @ 17:00:50.586			Active response: active-response/bin/remove-threat.sh - add	3	657
Oct 1, 2025 @ 17:00:50.112	T1203	Execution	VirusTotal: Alert - /tmp/malware/eicar - 66 engines detected this file	12	87105
Oct 1, 2025 @ 17:00:46.563			Active response: active-response/bin/remove-threat.sh - add	3	657
Oct 1, 2025 @ 17:00:46.138	T1070.004 T1485	Defense Evasion, Impact	File deleted.	7	553
Oct 1, 2025 @ 17:00:46.047	T1203	Execution	VirusTotal: Alert - /tmp/malware/eicar - 66 engines detected this file	12	87105
Oct 1, 2025 @ 17:00:42.719			File added to the system.	5	554
Oct 1, 2025 @					

" When you train Smarter, you defend Stronger"
Leonard Estos