****

**Wazuh + VirusTotal Integration**

## **Introduction**

This comprehensive guide demonstrates how to integrate WazuhSecurity Information and Event Management (SIEM) with VirusTotal's threat intelligence platform to create an automated malware detection and removal system. The setup uses a Kali Linux manager and Ubuntu agent configuration for real-world security monitoring.

## **What is Wazuh?**

Wazuh is a free, open-source Security Information and Event Management (SIEM) tool. It provides:

Intrusion Detection  
Log Data Analysis  
File Integrity Monitoring  
Vulnerability Detection  
Compliance Reporting  
 Wazuh collects and analyzes security data from different systems and centralizes it in a dashboard for monitoring and alerting.

## **What is VirusTotal?**

VirusTotal is a free online platform that analyzes suspicious files, URLs, domains, and IPs. It aggregates results from:

70+ antivirus scanners  
URL blacklisting services  
Sandbox environments  
 It helps in identifying malware, phishing, and other security threats by checking submitted items against known threat databases.

## **Why Integrate Wazuh with VirusTotal?**

Integrating Wazuh with VirusTotal provides enhanced security intelligence. This integration allows:

Automated scanning of files or URLs found in Wazuh alerts.

Cross-checking hashes or indicators of compromise (IoCs) with VirusTotal.  
More accurate threat detection by correlating Wazuh logs with VirusTotal results.  
Faster incident response by providing VirusTotal report links directly in Wazuh alerts.

## **Benefits of Integration**

**Advanced Threat Intelligence** Real-time access to VirusTotal's large threat database enhances Wazuh's analysis.  
 **Improved Detection Accuracy** Cross-verification reduces false positives and highlights real threats.  
 **Faster Response Time** Security teams get immediate context and can act quickly.  
 **Automated Workflows** Integration automates the checking of suspicious items, saving time.  
 **Comprehensive Alerts** Alerts become more informative with VirusTotal verdicts and links.

**Real-Time Scenario**

**Scenario:** An attacker uploads a suspicious .exe file on a public-facing web server. Wazuh is monitoring the directory with file integrity monitoring. When the file is created, Wazuh detects the change and triggers a custom script.

**The script:**

Extracts the hash of the file  
Sends it to VirusTotal via API  
Gets the result: **"Detected as malware by 55/70 engines"  
Wazuh:**

Tags this event as **high severity**Sends alert to the SOC team via email or Slack  
The team immediately quarantines the file and blocks the IP  
 This happens **within seconds**, providing **real-time response**.

## **System Architecture**

### **Infrastructure Overview**

┌─────────────────┐ API Calls ┌──────────────────┐

│ Kali Linux │◄────────────────┤ VirusTotal │

│ Wazuh Manager │ │ Cloud API │

│ │ │ │

└─────────────────┘ └──────────────────┘

▲

│ Agent Communications

│ (Port 1514)

▼

┌─────────────────┐

│ Ubuntu 22.04 │

│ Wazuh Agent │

│ (File Monitor) │

└─────────────────┘

**Step by step Configuration**

**Wazuh Version Compatibility Statement**

The following steps (Step 1 to Step 3) describe how VirusTotal integration is typically enabled via the Wazuh Dashboard by navigating through Threat Detection and Response and Settings > Modules.

However, in Wazuh version 4.11.2, these options are not available, and the VirusTotal module cannot be activated via the dashboard.

In this version, integration with VirusTotal must be performed manually through direct modifications in the ossec.conf configuration file.

These steps are still included here for the following purposes:

To illustrate the standard UI-based activation method available in earlier versions (e.g., 4.2.x, 4.3.x).  
To provide clarity for users working in mixed-version environments.

To emphasize the manual setup requirement for version 4.11.2 and onward.  
 For version 4.11.2 users, you may skip the dashboard steps below and proceed directly to the manual VirusTotal configuration section.

**Steps to Enable VirusTotal via Wazuh Dashboard**

**Step 1: Access the Wazuh Environment**

Action: Open a terminal and connect via SSH to the Wazuh server, or log in to the Wazuh web dashboard.  
Purpose: This grants access to the SIEM platform where further configuration will be carried out.

**Step 2: Locate the VirusTotal Module**

Action: Navigate to the Wazuh Dashboard:  
 Dashboard → Threat Detection and Response  
 Scroll to find VirusTotal listed (it is disabled by default).  
Purpose: This verifies that the VirusTotal module is available and ready to be enabled.

**Step 3: Activate the VirusTotal Integration**

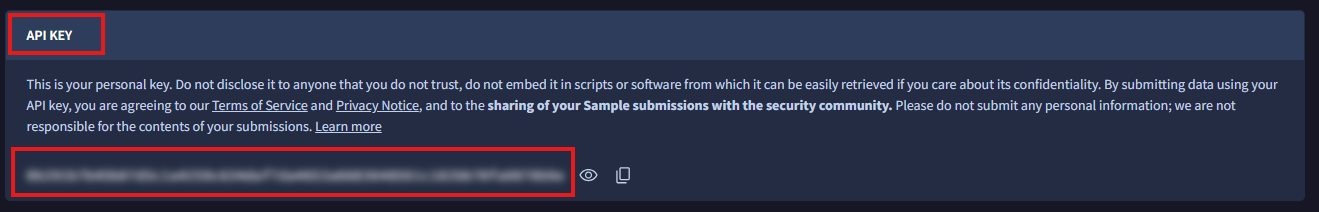
Action:  
 Go to: Settings → Modules  
 Locate the VirusTotal option and toggle it ON.  
Purpose: This action enables VirusTotal as a backend integration, allowing Wazuh to perform hash lookups for threat intelligence.

**Step 4: Retrieve VirusTotal API Key**

Action:  
 Sign in at:<https://www.virustotal.com>



Get API key from your profile section.



Reason:  
 The API key allows Wazuh to authenticate requests to VirusTotal’s cloud services.

**Step 5: Configure ossec.conf for VirusTotal**

**Edit the config file:**

Using following command

sudo nano /var/ossec/etc/ossec.conf

Inside the file, scroll to or locate the <integration> section. If it doesn't exist, you may add it just before the closing </ossec\_config> tag.  
Insert the following XML block.

Make sure to replace YOUR\_API\_KEY\_HERE with your actual VirusTotal API key:

<integration>

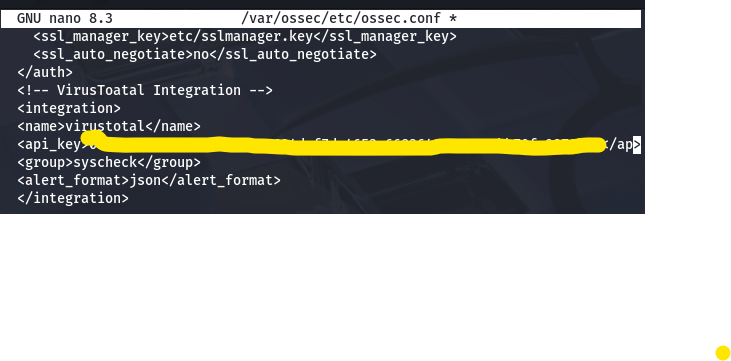
<name>virustotal</name>

<api\_key>YOUR\_API\_KEY\_HERE</api\_key>

<group>syscheck</group>

<alert\_format>json</alert\_format>

</integration>



name: Specifies the integration name (must be set to virustotal).  
api\_key: Your personal or enterprise VirusTotal API key.  
group: Defines which alert group will trigger VirusTotal lookups (e.g., syscheck).  
alert\_format: Indicates the format in which the alert will be sent (json is recommended).  
After saving the changes, proceed to restart the Wazuh manager to apply the new integration settings.

This links the VirusTotal service with Wazuh’s file integrity monitoring alerts.

**Step 6: Access and Modify the VirusTotal Integration Script**

To customize or inspect the behavior of the VirusTotal integration, access its script within the Wazuh directory.

Navigate to the Integrations Folder:

cd /var/ossec/integrations

List the Available Integration Scripts:

ls

Expected output may include:

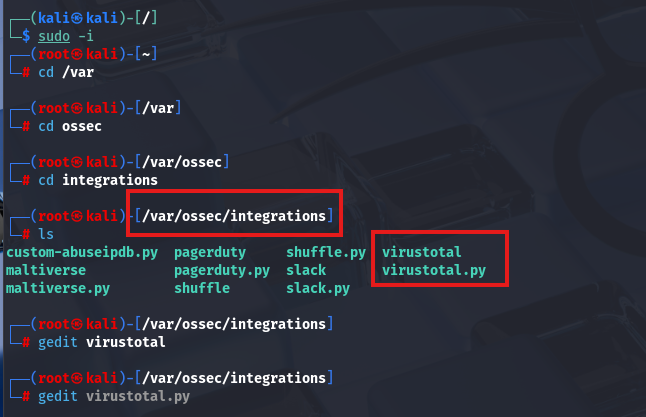
virustotal.py shuffle.py pagerduty.py custom-abuseipdb.py

Open the VirusTotal Script for Editing:

Use your preferred text editor to open the script:

nano virustotal.py

gedit [virustotal.py](http://virustotal.py)



### **Step 7: Apply Proper Permissions and Restart Wazuh Manager**

To ensure the VirusTotal integration script is secure and executable by the appropriate user, apply the following permissions:

Set the file ownership to root and group to Wazuh

sudo chown root:wazuh /var/ossec/integrations/virustotal

If the file is a script or symbolic link (e.g., virustotal.py), ensure both the original script and link have correct permissions and restrict write permissions for group and others

sudo chmod 750 /var/ossec/integrations/virustotal.py

sudo chmod 750 /var/ossec/integrations/virustotal



Finally, restart the Wazuh Manager to apply the integration changes:

sudo systemctl restart wazuh-manager

**Testing Procedure:**

#### **Step 1: Create a monitored directory**

Ensure that the directory /home/amir/Downloads/fileIntegrity is being monitored by Wazuh FIM (File Integrity Monitoring).

sudo mkdir -p /home/amir/Downloads/fileIntegrity

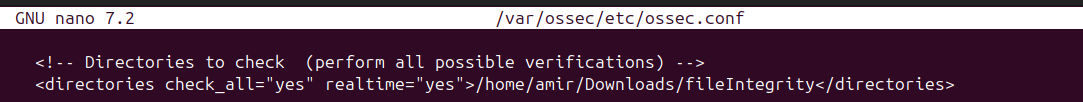
Add this

<directories check\_all="yes" realtime="yes">/home/amir/Downloads/fileIntegrity</directories>

Using following command for monitoring:

Sudo nano /var/ossec/etc/ossec.conf





#### **Step 2: Generate a test malicious file using EICAR**

Create the EICAR antivirus test fil**e** which is globally recognized as a harmless file used for testing antivirus and malware detection systems.

echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\*' > /home/amir/Downloads/fileIntegrity/eicar.txt

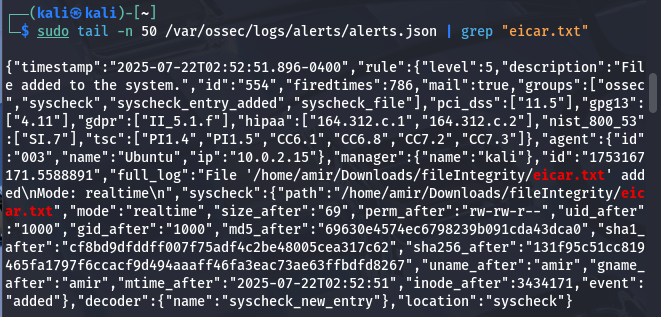
**Expected Behavior:**

* Wazuh detects the new file and triggers a **Syscheck alert**.
* Wazuh queries VirusTotal using the file hash.
* If the hash is not found in VirusTotal, the alert will indicate:

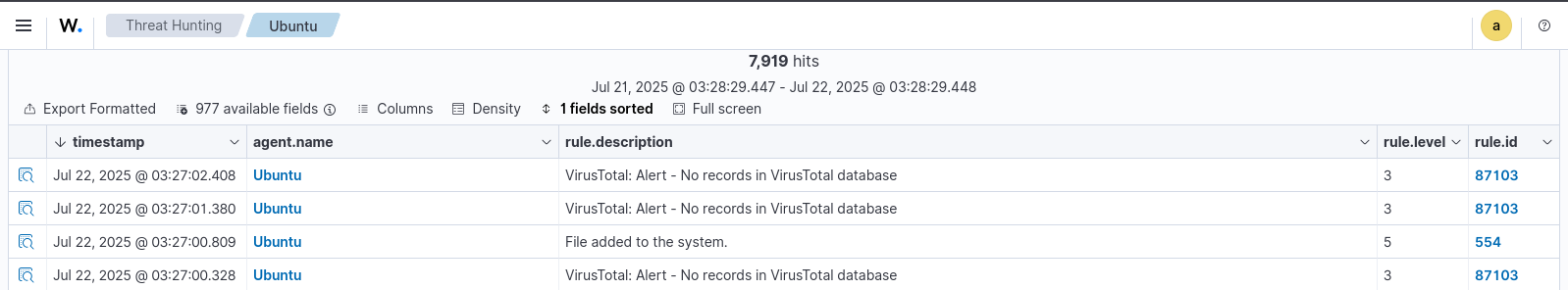
#### **Step 3: Verify alert in Wazuh logs**

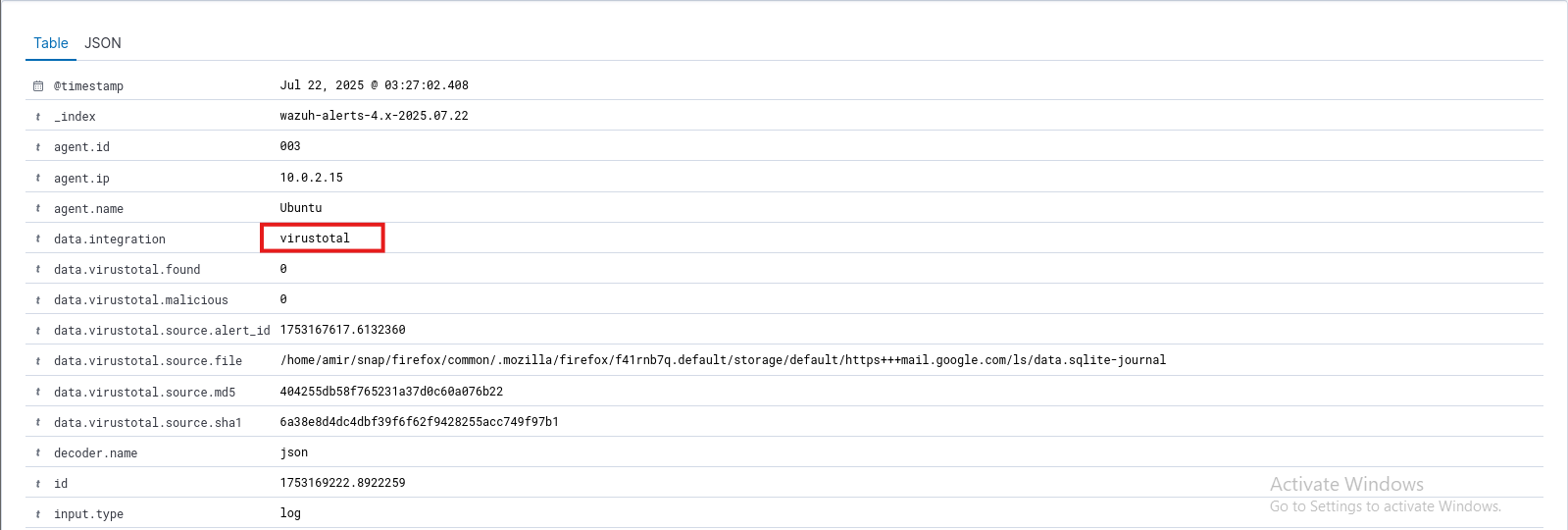
Check the Wazuh alerts to confirm that the file addition was detected and logged correctly:

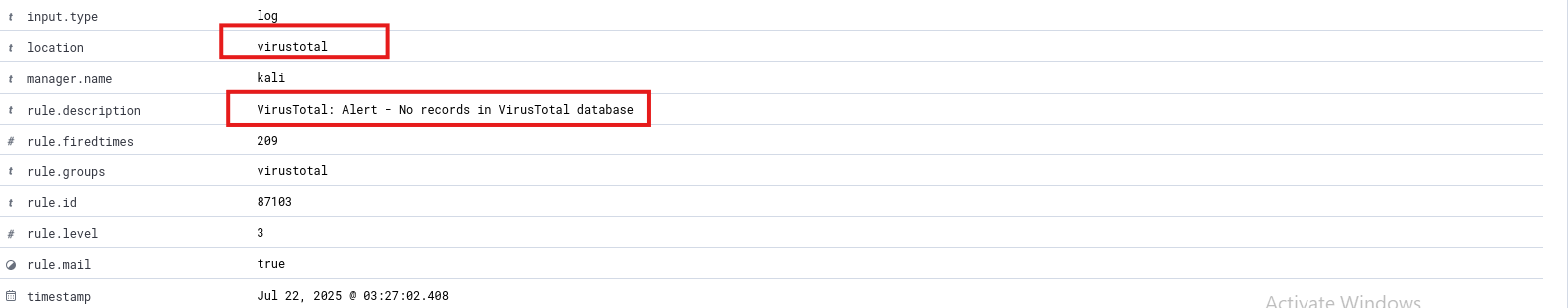
sudo tail -n 50 /var/ossec/logs/alerts/alerts.json | grep "eicar.txt"



Check Dashboard:







### **Summary**

In this project, I successfully implemented an integration between Wazuh SIEM and VirusTotal to enable real-time detection, analysis, and response to potential malware threats. The environment was set up using a Wazuh Manager on Kali Linux and an Ubuntu-based Wazuh Agent, with File Integrity Monitoring (FIM) configured to observe specific directories for any file modifications or additions.

When a suspicious file—such as the standard test malware file eicar.txt—was placed in the monitored directory, Wazuh generated a security alert. This alert automatically triggered the custom VirusTotal integration script (virustotal.py), which extracted the file’s hash and submitted it to the VirusTotal platform using a valid API key. The script then retrieved and displayed the analysis results, including detection ratios from over 70 antivirus engines. These results were visible in both Wazuh log files and the Wazuh dashboard, enhancing the overall visibility of threats.

To maintain security and proper functionality, I ensured correct permissions were applied to the integration scripts and API key files. I also validated the integration thoroughly using the EICAR test file, confirming that the process worked as expected—from alert generation to VirusTotal response.

This integration significantly strengthened the threat detection and response capabilities of the Wazuh environment. It allowed for automated correlation between local file-based alerts and global threat intelligence, improving both the speed and accuracy of incident analysis and enhancing the organization’s cybersecurity posture.