Virustotal Integration with Wazuh

What is VirusTotal?

VirusTotal is an online malware analysis service that helps identify whether a file, URL, IP address, domain, or file hash is malicious or safe.

It scans files and links using multiple antivirus engines and security tools at the same time.

Instead of relying on a single antivirus, VirusTotal compares the data with global threat intelligence collected from cybersecurity companies around the world.

What We Achieved by Integrating VirusTotal with Wazuh

By integrating VirusTotal with Wazuh, we achieved the following benefits:

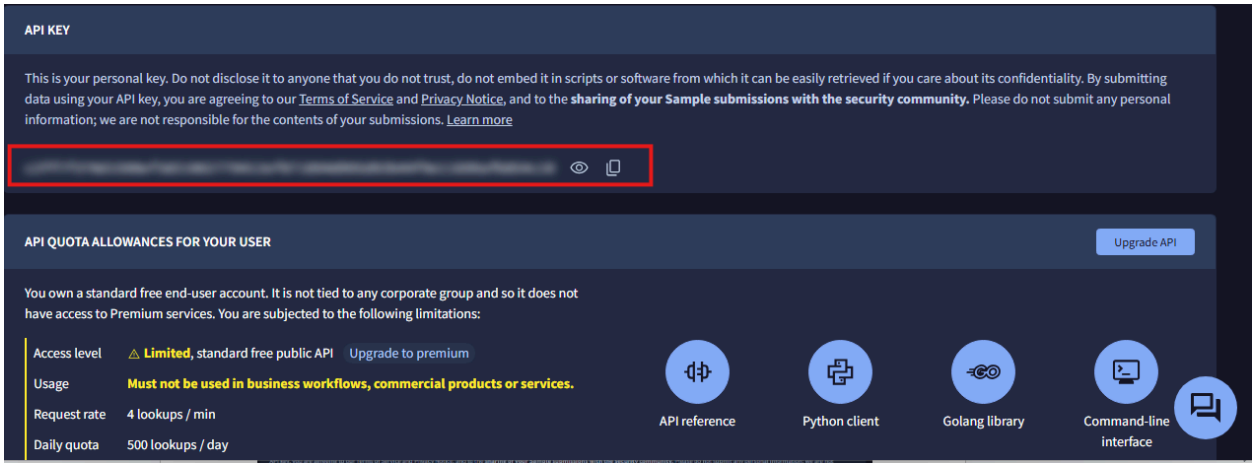
Wazuh detects suspicious files, and VirusTotal confirms whether those files are truly malicious or not using global antivirus data.
This integration allows Wazuh to detect not only local threats but also known worldwide malware, making detection more reliable.
Security teams receive verified results automatically, which helps them take quick action against threats.
VirusTotal helps distinguish between real malware and safe files, reducing unnecessary alerts.
VirusTotal provides intelligence collected from many security vendors, giving Wazuh real-world attack awareness.
File hashes are checked automatically without manual uploads, saving time and effort.
Combining Wazuh's detection capabilities with VirusTotal's analysis creates a more powerful and trusted security system.

Step by step Configuration

First I created the API key from VirusTotal.

Sign in at: https://www.virustotal.com

Click on the profile and select the API key.



Copy it and use it later.

The API key allows Wazuh to authenticate requests to VirusTotal's cloud services.

Configure ossec.conf for VirusTotal (Ubuntu Manager)

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, I added it just before the closing </ossec_config> tag.
I insert the following XML block.

```
<integration>
  <name>virustotal</name>
  <api_key>YOUR_API_KEY_HERE</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```

Make sure to replace YOUR_API_KEY_HERE with our actual VirusTotal API key.

By using following command:

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

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

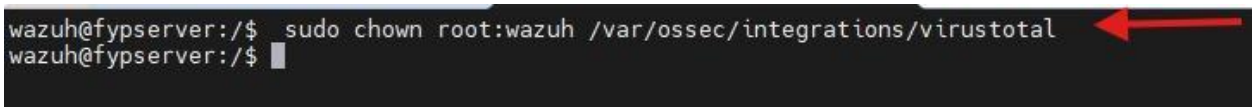
Open the VirusTotal Script for Editing:

sudo nano virustotal.py

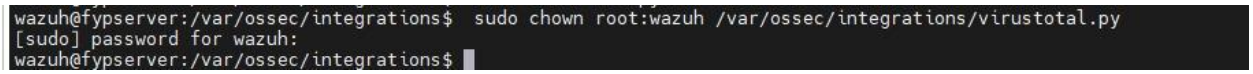
Apply Proper Permissions and Restart Wazuh Manager

Set the file ownership to root and group to Wazuh

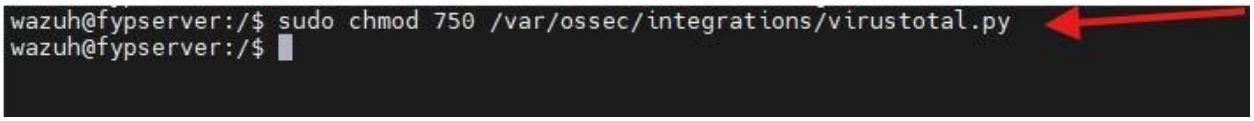
sudo chown root:wazuh /var/ossec/integrations/virustotal



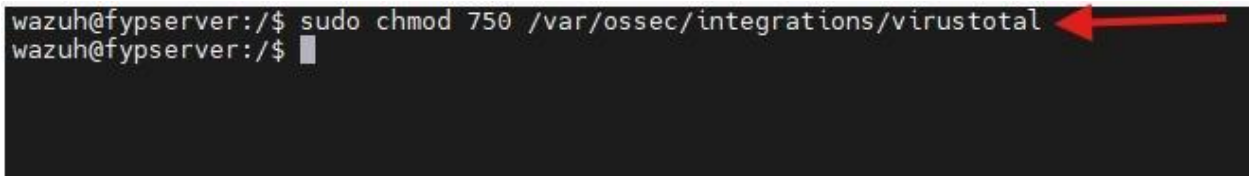
sudo chown root:wazuh /var/ossec/integrations/virustotal.py



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



sudo chmod 750 /var/ossec/integrations/virustotal



sudo systemctl restart wazuh-manager

```
wazuh@fypserver:/$ sudo systemctl restart wazuh-manager
wazuh@fypserver:/$
```

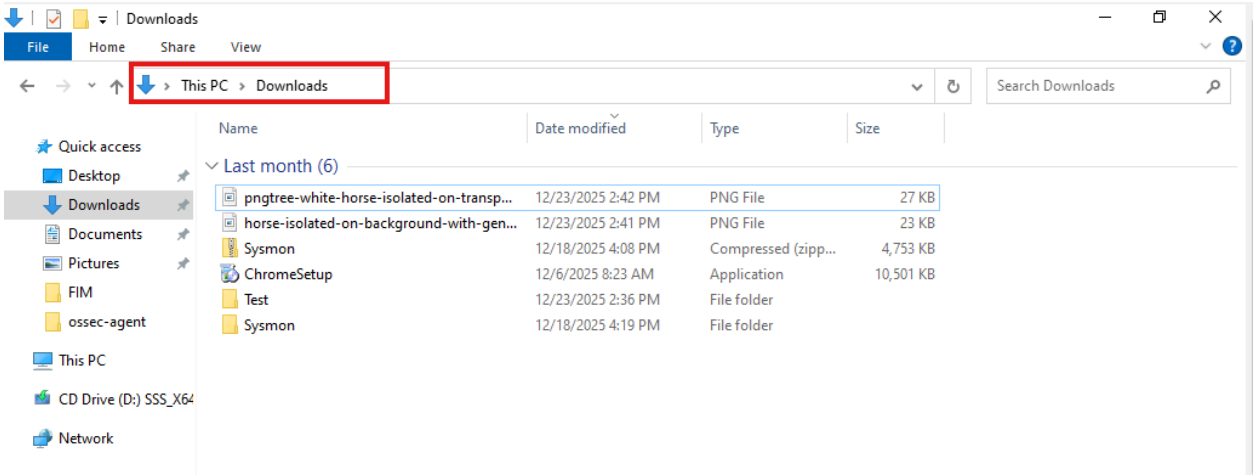
When a file change is detected by the Wazuh agent, the file hash is generated and sent to the Wazuh manager. The manager forwards this hash to VirusTotal, which returns the malware result. Based on this result, Wazuh generates a high-severity alert.

Testing Procedure:

First we create the malicious file in the monitored directory as we already enabled the FIM(File Integrity Monitoring) module in our project.

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

So, for this I go to my Window endpoint where my Agent is installed and given below is my monitored folder where I create the malicious file.



echo X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* > C:\Users\Administrator\Downloads\eicar.txt

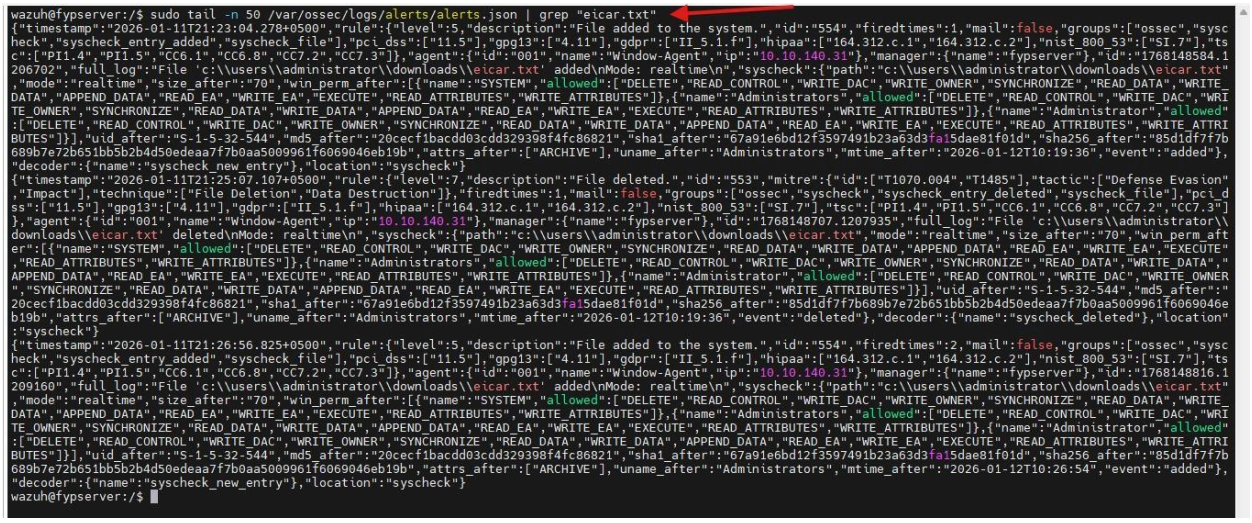
```
C:\Users\Administrator>echo X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* > C:\Users\Administrato
r\Downloads\eicar.txt

C:\Users\Administrator>
```

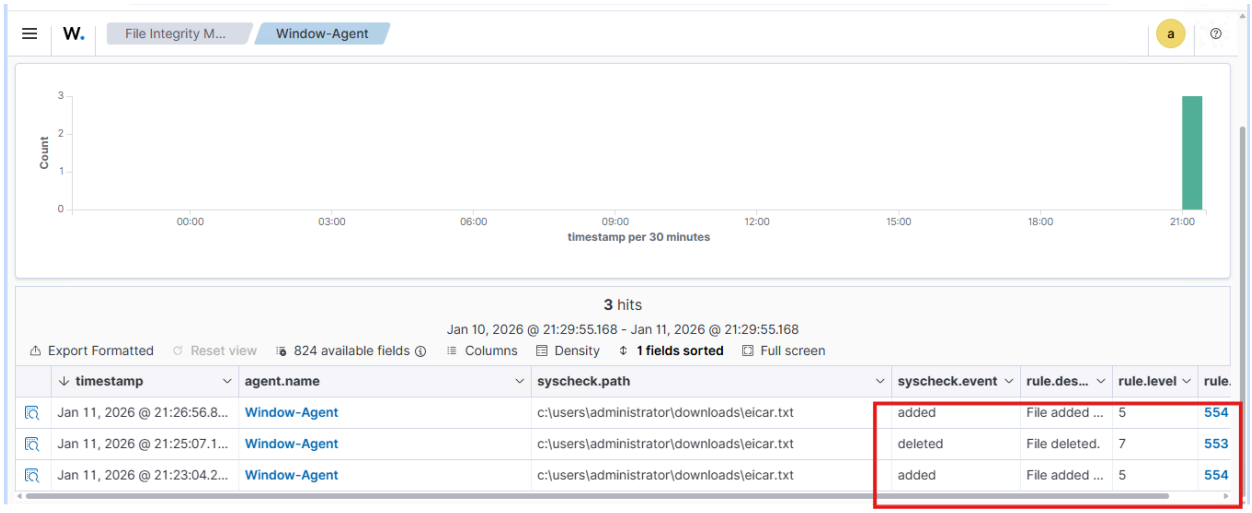
Verify alert in Wazuh logs

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"

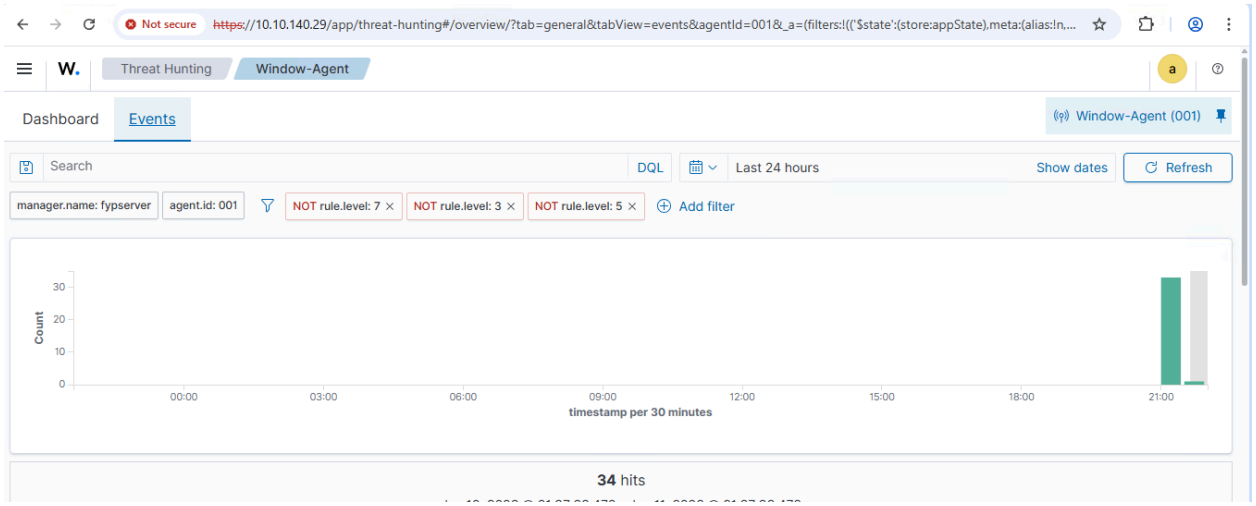


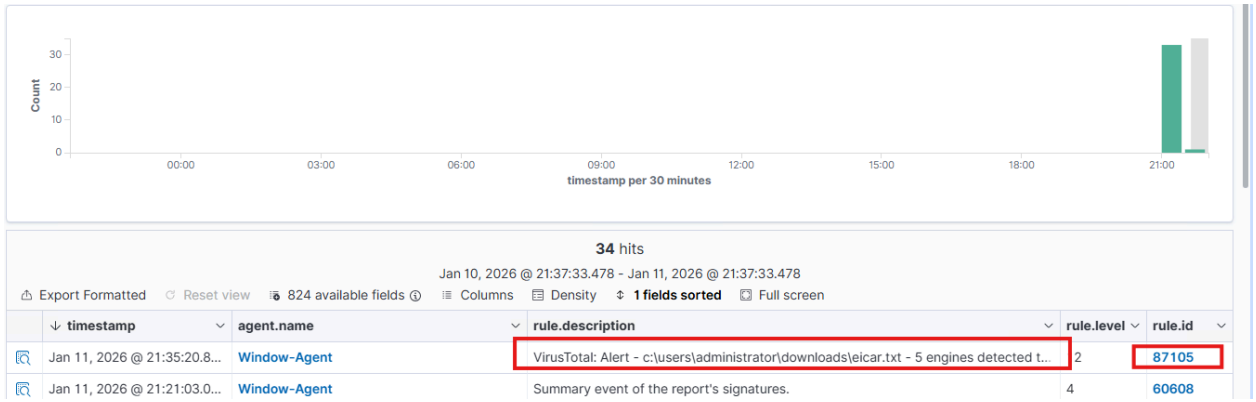
Before Virustotal Alerts:



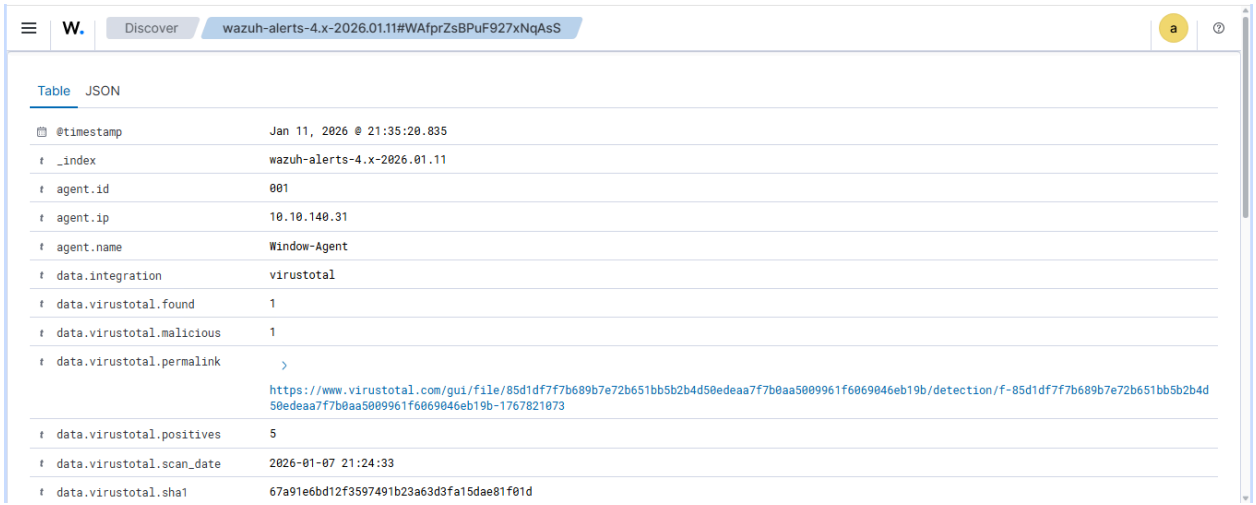
After VirusTotal result:

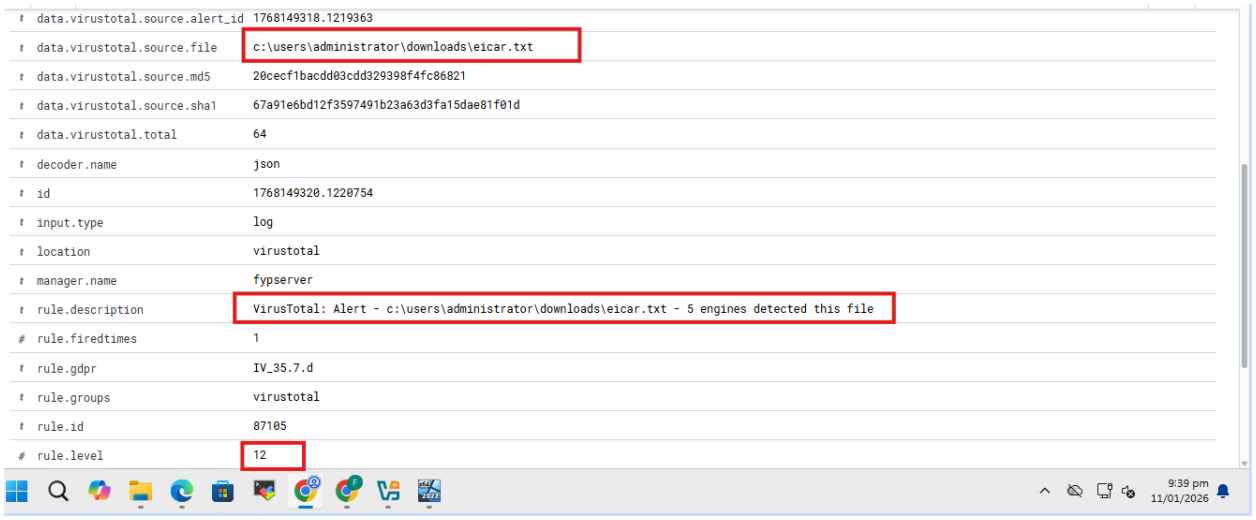
Now we see the alerts in the Threat Hunting section related to virustotal:





Details of alerts:





data.virustotal.source.alert_id	1768149318.1219363
data.virustotal.source.file	c:\users\administrator\downloads\eicar.txt
data.virustotal.source.md5	20cecf1bacdd03cdd329398f4fc86821
data.virustotal.source.sha1	67a91e6bd12f3597491b23a63d3fa15dae81f01d
data.virustotal.total	64
decoder.name	json
id	1768149320.1220754
input.type	log
location	virustotal
manager.name	fypserver
rule.description	VirusTotal: Alert - c:\users\administrator\downloads\eicar.txt - 5 engines detected this file
rule.firedtimes	1
rule.gdpr	IV_35.7.d
rule.groups	virustotal
rule.id	87105
rule.level	12

rule.mail	true
rule.mitre.id	T1203
rule.mitre.tactic	Execution
rule.mitre.technique	Exploitation for Client Execution
rule.pci_dss	10.6.1, 11.4
timestamp	Jan 11, 2026 @ 21:35:20.835

Summary:

VirusTotal is an online malware analysis service that checks files, URLs, IP addresses, domains, and file hashes for malicious activity. It uses multiple antivirus engines and global threat intelligence to determine whether something is safe or harmful.

Integrating VirusTotal with Wazuh enhances the malware detection capabilities of the system. When Wazuh detects a suspicious file, it generates the file's hash and sends it to VirusTotal. VirusTotal checks the hash and returns the result, allowing Wazuh to generate accurate alerts.

Through this integration, we achieved several benefits:

Wazuh can accurately verify malware using global intelligence.
It can detect both local and worldwide threats reliably.
Alerts are generated automatically, enabling faster incident response.

False positives are reduced, as safe files are distinguished from real threats.

Security teams gain real-world threat awareness from VirusTotal.

File hashes are checked automatically, saving time and effort.

Overall security monitoring becomes stronger and more trusted.

The integration was configured by creating a VirusTotal API key, updating the Wazuh `ossec.conf` file, modifying the integration script `virustotal.py`, setting correct permissions, and restarting the Wazuh manager. Testing was performed using the EICAR test file to ensure alerts were generated correctly.

A small limitation of the integration is the API request limit when using a free VirusTotal API key. Excessive file checks may be rate-limited, which could delay alert generation.

In conclusion, VirusTotal integration significantly improved the detection accuracy and response efficiency of Wazuh, making the system more reliable for monitoring and threat detection.