

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.

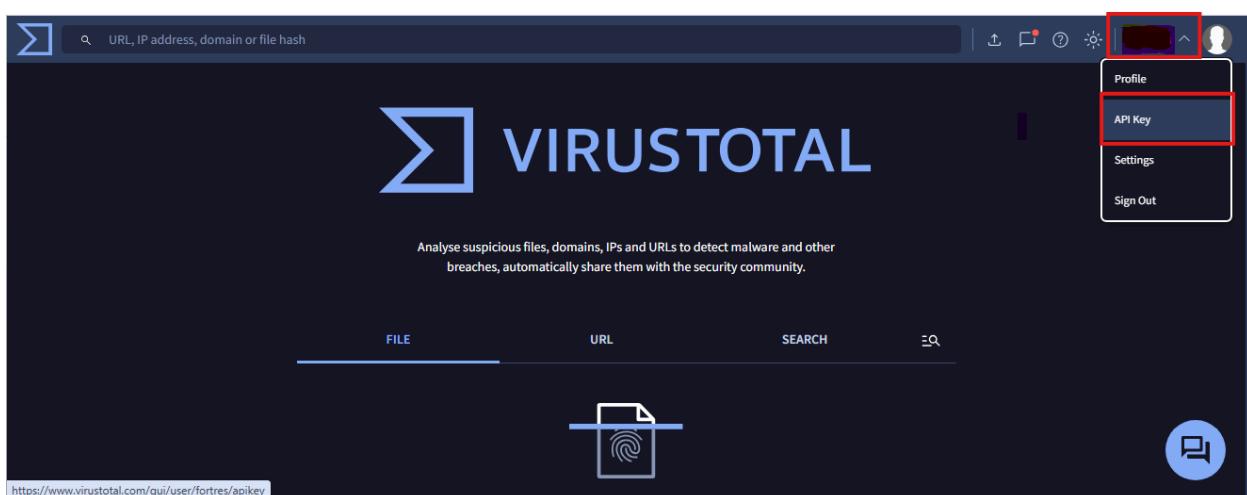
Step by step Configuration

First I created the API key from VirusTotal.

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



Click on the profile and select the API key.



A screenshot of the 'API KEY' page. At the top, it says 'API KEY'. Below that is a warning: 'This is your personal key. Do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality. By submitting data using your API key, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submissions with the security community. Please do not submit any personal information; we are not responsible for the contents of your submissions. Learn more'. A red box highlights a copy icon next to the key text. Below this is a section titled 'API QUOTA ALLOWANCES FOR YOUR USER'. It states: 'You own a standard free end-user account. It is not tied to any corporate group and so it does not have access to Premium services. You are subjected to the following limitations:'. It lists: 'Access level: Limited, standard free public API' (with a 'Upgrade to premium' link), 'Usage: Must not be used in business workflows, commercial products or services.', 'Request rate: 4 lookups / min', and 'Daily quota: 500 lookups / day'. To the right, there are icons for 'API reference', 'Python client', 'Golang library', and 'Command-line interface'. A 'Upgrade API' button is also visible.

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
```



```
GNU nano 6.2                               /var/ossec/etc/ossec.conf *
<timeout_allowed>yes</timeout_allowed>
</command>
<command>
  <name>win_route-null</name>
  <executable>route-null.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
<command>
  <name>nets</name>
  <executable>nets.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
<integration>
  <name>virustotal</name>
  <api_key>YOUR_API_KEY_HERE</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>
```

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
```

```
wazuh@fypserver:/var$ cd /var/ossec/integrations
wazuh@fypserver:/var/ossec/integrations$ ls
multiverse  multiverse.py  pagerduty  pagerduty.py  shuffle  shuffle.py  slack  slack.py  virustotal  virustotal.py
wazuh@fypserver:/var/ossec/integrations$
```

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
```

```
wazuh@fypserver:/$ sudo chown root:wazuh /var/ossec/integrations/virustotal ←
wazuh@fypserver:/$
```

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

```
wazuh@fypserver:/var/ossec/integrations$ sudo chown root:wazuh /var/ossec/integrations/virustotal.py
[sudo] password for wazuh:
wazuh@fypserver:/var/ossec/integrations$
```

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

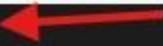
```
wazuh@fypserver:/$ sudo chmod 750 /var/ossec/integrations/virustotal.py ←
wazuh@fypserver:/$
```

```
sudo chmod 750 /var/ossec/integrations/virustotal
```

```
wazuh@fypserver:/$ sudo chmod 750 /var/ossec/integrations/virustotal ←
wazuh@fypserver:/$
```

```
sudo systemctl restart wazuh-manager
```

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



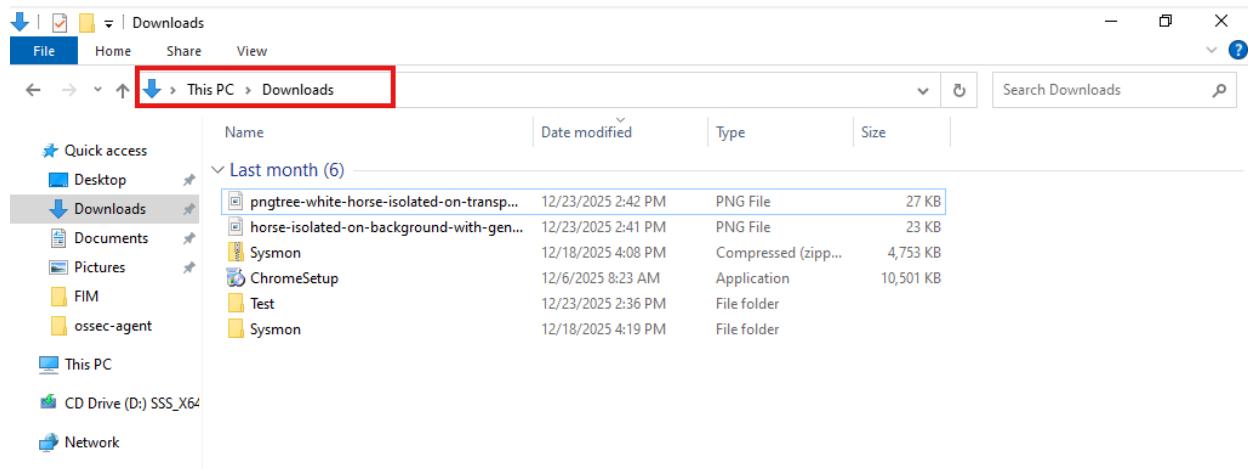
When a file change is detected by the Wazuh agent, the file hash is generated and sent to the Wazuh manager. The manager forwards this hash to VirusTotal, which returns the malware result. Based on this result, Wazuh generates a high-severity alert.

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\leicar.txt
```

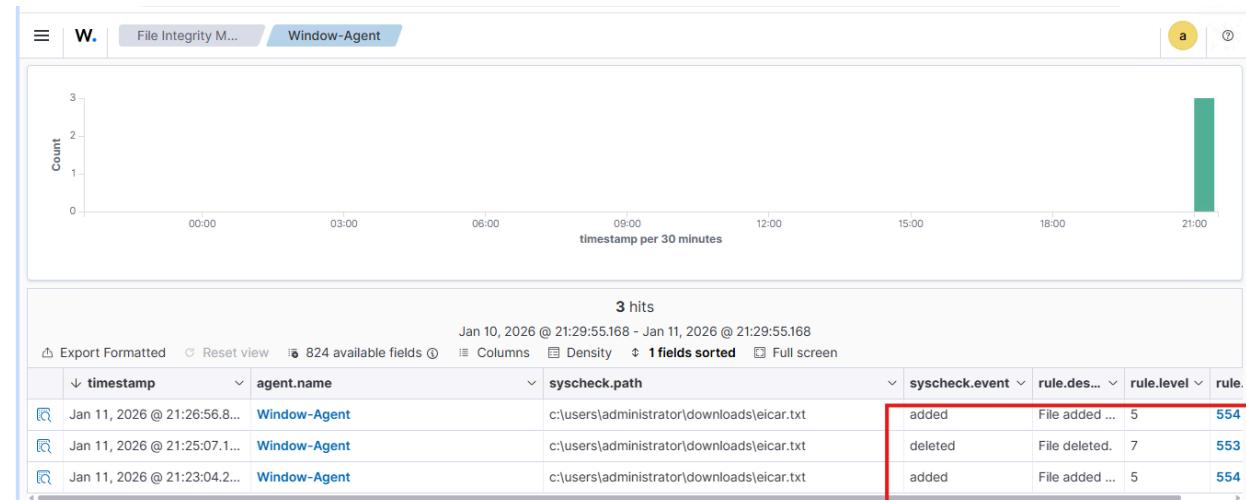
```
C:\Users\Administrator>echo X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* > C:\Users\Administrato  
r\Downloads\leicar.txt  
C:\Users\Administrator>
```

Verify alert in Wazuh logs

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

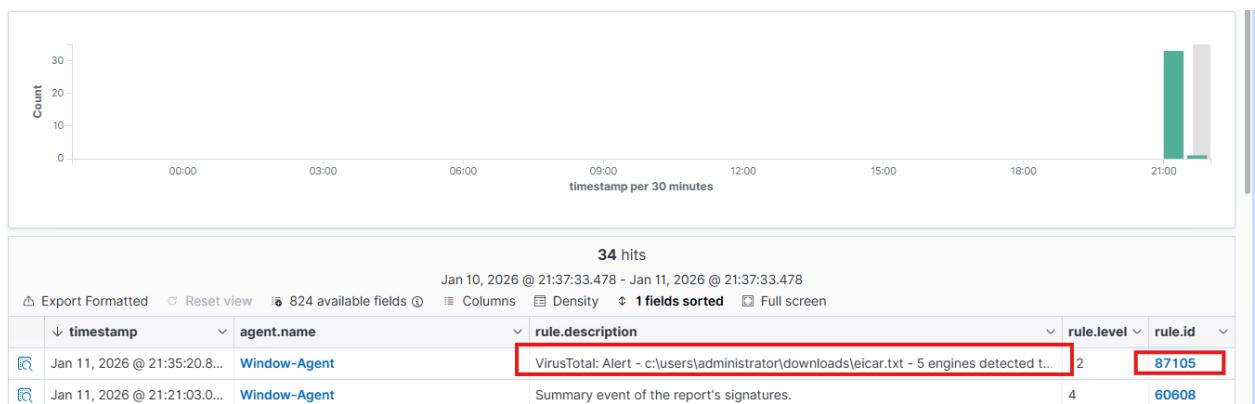
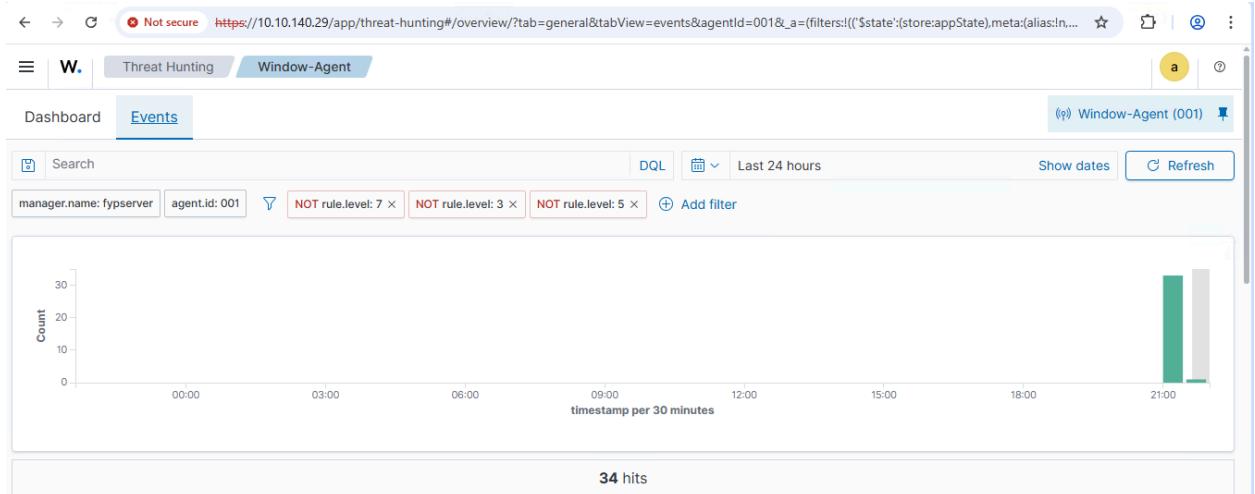
```
sudo tail -n 50 /var/ossec/logs/alerts/alerts.json | grep "eicar.txt"
```

Before Virustotal Alerts:



After VirusTotal result:

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



Details of alerts:

Table JSON	
@timestamp	Jan 11, 2026 @ 21:35:20.835
_index	wazuh-alerts-4.x-2026.01.11#WAfprZsBPuF927xNqAsS
agent.id	001
agent.ip	10.10.140.31
agent.name	Window-Agent
data.integration	virustotal
data.virustotal.found	1
data.virustotal.malicious	1
data.virustotal.permalink	> https://www.virustotal.com/gui/file/85d1df7f7b689b7e72b651bb5b2b4d50edeaa7f7b0aa5009961f6069046eb19b/detection/f-85d1df7f7b689b7e72b651bb5b2b4d50edeaa7f7b0aa5009961f6069046eb19b-1767821073
data.virustotal.positives	5
data.virustotal.scan_date	2026-01-07 21:24:33
data.virustotal.sha1	67a91e6bd12f3597491b23a63d3fa15dae81f01d

t	data.virustotal.source.alert_id	1768149318.1219363
t	data.virustotal.source.file	c:\users\administrator\downloads\eicar.txt
t	data.virustotal.source.md5	20cecf1bacdd03ddd29398f4fc86821
t	data.virustotal.source.sha1	67a91e6bd12f3597491b23a63d3fa15dae81f01d
t	data.virustotal.total	64
t	decoder.name	json
t	id	1768149320.1220754
t	input.type	log
t	location	virustotal
t	manager.name	fypserver
t	rule.description	VirusTotal: Alert - c:\users\administrator\downloads\eicar.txt - 5 engines detected this file
#	rule.firedtimes	1
t	rule.gdpr	IV_35.7.d
t	rule.groups	virustotal
t	rule.id	87105
#	rule.level	12

rule.mail	true
t rule.mitre.id	T1203
t rule.mitre.tactic	Execution
t rule.mitre.technique	Exploitation for Client Execution
t rule.poi_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.