

# Task 3 Submission

## Syed Hasa Raza Rizvi

### Questions:

1. Enable Windows Defender logs on a Windows machine.
2. Configure Wazuh to collect Windows Security logs related to Defender events.
3. Simulate a Defender alert by downloading or scanning an EICAR test file. o Observe if the detection is forwarded to the Wazuh dashboard.
4. Obtain and configure a VirusTotal API key.
5. Integrate VirusTotal with Wazuh using the provided Wazuh module or custom script.
6. Generate a test file or hash from a suspicious file.
7. Submit the file hash to VirusTotal via Wazuh and observe the reputation score and classification.
8. Verify VirusTotal results in Wazuh alerts or logs, showing external intelligence enrichment.
9. Take screenshots of logs/alerts from both Defender and VirusTotal in the Wazuh dashboard.

Accessing wazuh manager with ubuntu:

ubuntu's ip that will be used to access the dashboard from windows:

```
hasanraza@hasanraza-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:50:89:83 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86317sec preferred_lft 86317sec
    inet6 2400:adc1:171:6500:6d48:ad43:4ae0:6975/64 scope global temporary dynamic
        valid_lft 604719sec preferred_lft 85968sec
    inet6 2400:adc1:171:6500:5079:5c2e:8f23:55ac/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 2591995sec preferred_lft 604795sec
    inet6 fe80::a10f:64b9:db85:129/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b9:33:7f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s8
        valid_lft 86317sec preferred_lft 86317sec
    inet6 fd00::b830:b02a:dc64:b18/64 scope global temporary dynamic
        valid_lft 86318sec preferred_lft 14318sec
    inet6 fd00::a00:27ff:feb9:337f/64 scope global dynamic mngtmpaddr
        valid_lft 86318sec preferred_lft 14318sec
    inet6 fe80::a00:27ff:feb9:337f/64 scope link
        valid_lft forever preferred_lft forever
```

Run this command to see if every service is running smoothly:

```
hasanraza@hasanraza-VirtualBox:~$ sudo systemctl status wazuh-manager wazuh-indexer wazuh-dashboard filebeat
[sudo] password for hasanraza:
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-07-22 01:04:57 PKT; 1min 38s ago
   Process: 1412 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   Tasks: 174 (limit: 4609)
   Memory: 590.0M (peak: 781.6M swap: 24.0K swap peak: 24.0K)
   CPU: 1min 16.258s
   CGroup: /system.slice/wazuh-manager.service
           └─2258 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             └─2259 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               └─2260 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                 └─2263 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                   └─2266 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                     └─2312 /var/ossec/bin/wazuh-authd
                       └─2330 /var/ossec/bin/wazuh-db
                         └─2358 /var/ossec/bin/wazuh-execd
                           └─2376 /var/ossec/bin/wazuh-analysisd
                             └─2389 /var/ossec/bin/wazuh-syscheckd
                               └─2409 /var/ossec/bin/wazuh-remoted
                                 └─2445 /var/ossec/bin/wazuh-logcollector
                                   └─2464 /var/ossec/bin/wazuh-monitord
                                     └─2486 /var/ossec/bin/wazuh-modulesd

lines 1-23...skipping...
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-07-22 01:04:57 PKT; 1min 38s ago
   Process: 1412 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   Tasks: 174 (limit: 4609)
   Memory: 590.0M (peak: 781.6M swap: 24.0K swap peak: 24.0K)
   CPU: 1min 16.258s
   CGroup: /system.slice/wazuh-manager.service
           └─2258 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
```

```
● wazuh-indexer.service - wazuh-indexer
   Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-07-22 01:05:21 PKT; 1min 14s ago
     Docs: https://documentation.wazuh.com
   Main PID: 1411 (java)
```

lines 1-39

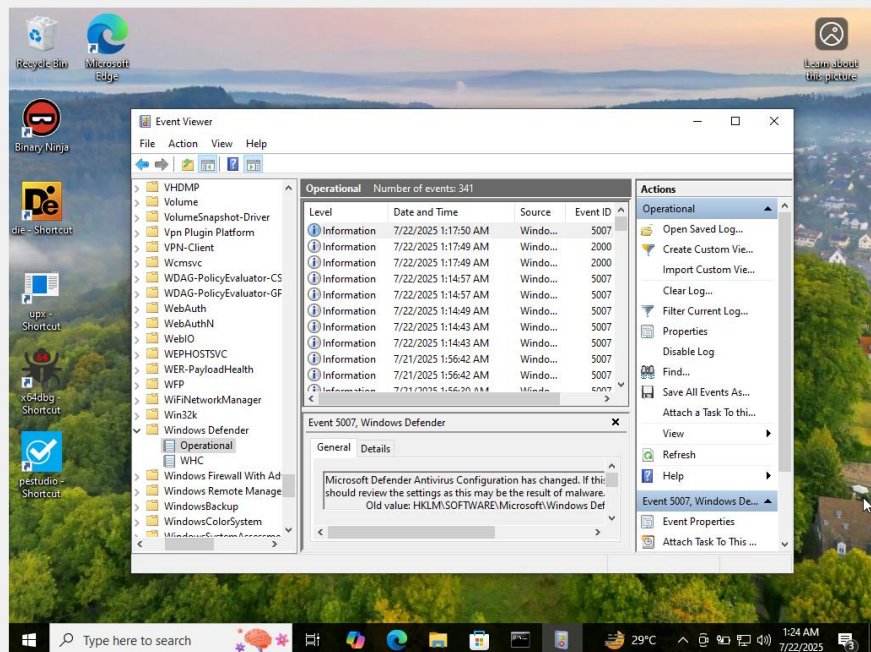
Booted windows vm:

followed this path and enabled operational log

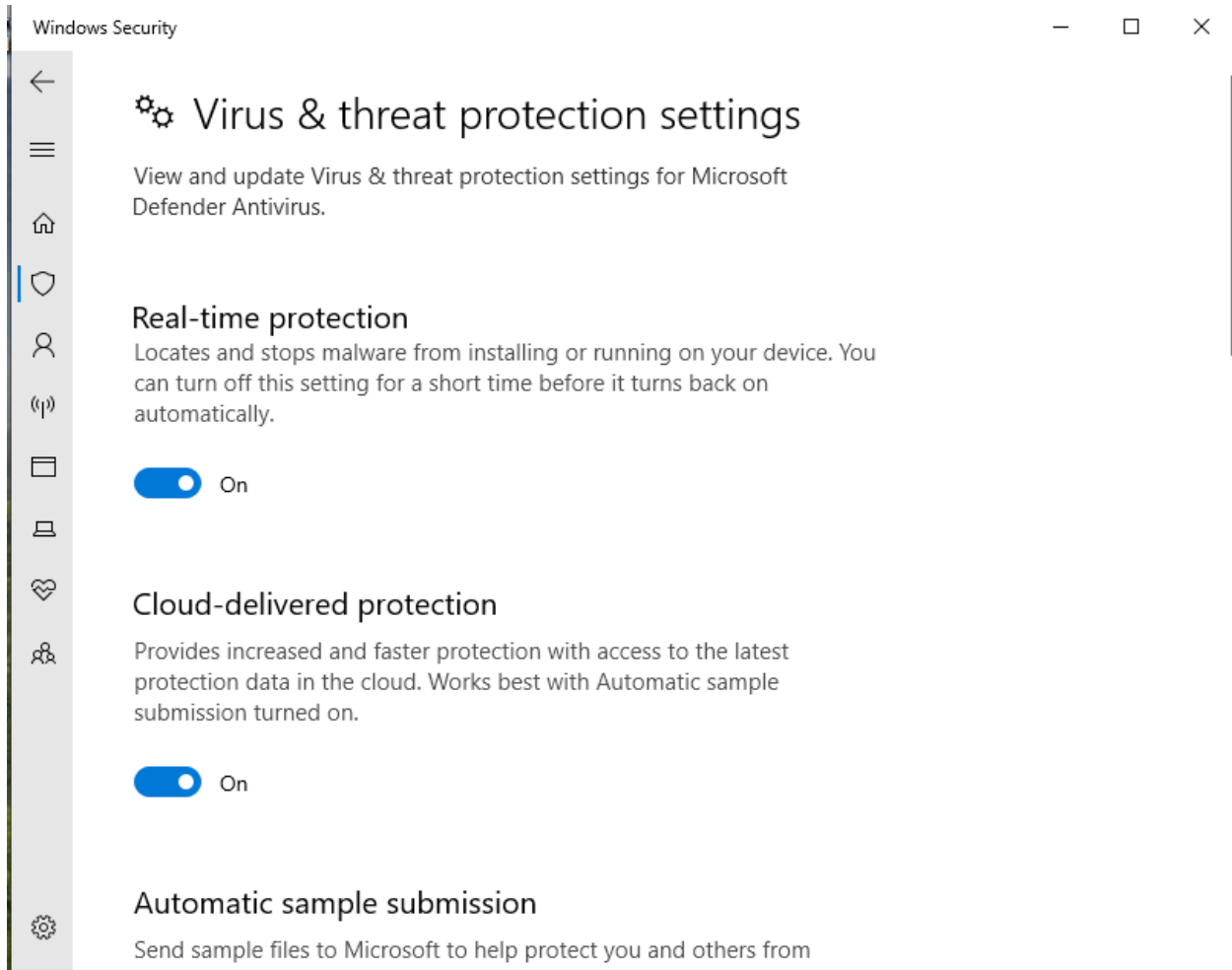
Applications and Services Logs > Microsoft > Windows > Windows Defender > Operational

windows10 [Running] - Oracle VirtualBox

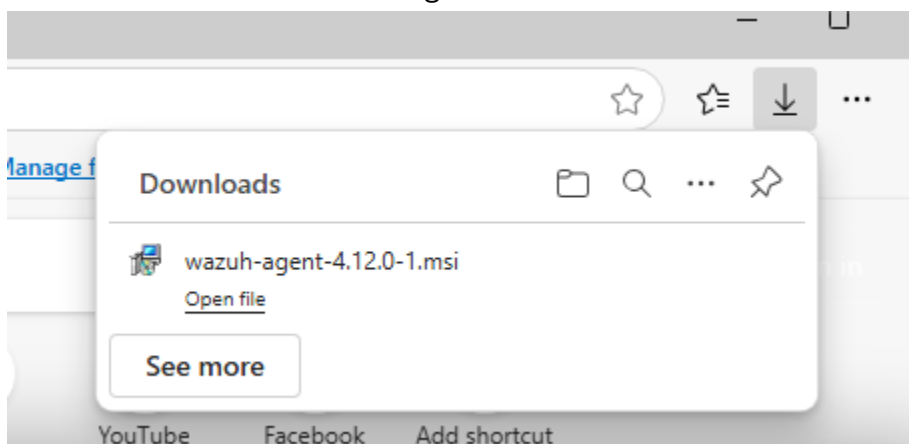
File Machine View Input Devices Help

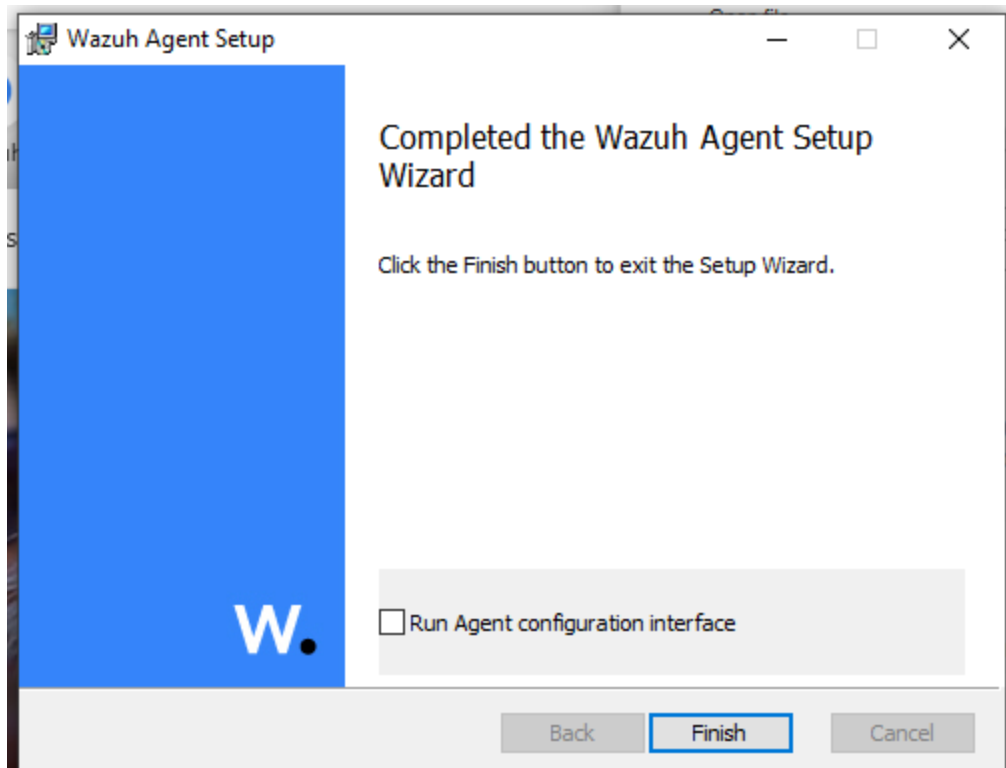


Also made sure that Real-time protection is on in Virus & threat protection settings

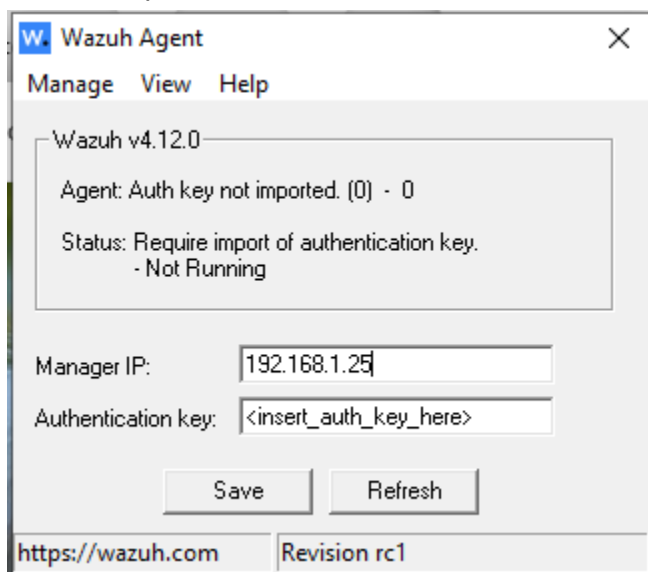


Then downloaded the wazuh agent on windows vm:





Gave the ip of ubuntu



Deployed a new agent:

```
hasanraza@hasanraza-VirtualBox:~$ sudo /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
  ID: 000, Name: hasanraza-VirtualBox (server), IP: 127.0.0.1, Active/Local
  ID: 004, Name: hasan-windows10, IP: any, Active
```

Agents (1)

[Deploy new agent](#) [Refresh](#) [Export formatted](#) [More](#) [Settings](#)

☐ Show only outdated

status=active [WQL](#)

<input type="checkbox"/>	ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
<input type="checkbox"/>	004	hasan-windows10	192.168.1.23	<a href="#">default</a>	Microsoft Windows 10 Pro 10.0.19045.6093	node01	v4.12.0	<span style="color: green;">●</span> <a href="#">i</a> <a href="#">👁</a> <a href="#">⋮</a>	

Rows per page: 10 [1](#)

```
hasanraza@hasanraza-VirtualBox:~$ sudo -i
root@hasanraza-VirtualBox:~# cd /var/ossec/etc
root@hasanraza-VirtualBox:/var/ossec/etc# ls
client.keys      lists            ossec.conf      shared
decoders         local_internal_options.conf  rootcheck      sslmanager.cert
internal_options.conf  localtime       rules           sslmanager.key
root@hasanraza-VirtualBox:/var/ossec/etc# cd shared
root@hasanraza-VirtualBox:/var/ossec/etc/shared# ls
agent-template.conf  ar.conf  default
root@hasanraza-VirtualBox:/var/ossec/etc/shared# cd default
root@hasanraza-VirtualBox:/var/ossec/etc/shared/default# ls
agent.conf          cis_win2012r2_domainL2_rcl.txt
cis_apache2224_rcl.txt  cis_win2012r2_memberL1_rcl.txt
cis_debian_linux_rcl.txt  cis_win2012r2_memberL2_rcl.txt
cis_mysql5-6_community_rcl.txt  merged.mg
cis_mysql5-6_enterprise_rcl.txt  rootkit_files.txt
cis_rhel5_linux_rcl.txt  rootkit_trojans.txt
cis_rhel6_linux_rcl.txt  system_audit_rcl.txt
cis_rhel7_linux_rcl.txt  system_audit_ssh.txt
cis_rhel_linux_rcl.txt  win_applications_rcl.txt
cis_sles11_linux_rcl.txt  win_audit_rcl.txt
cis_sles12_linux_rcl.txt  win_malware_rcl.txt
cis_win2012r2_domainL1_rcl.txt
root@hasanraza-VirtualBox:/var/ossec/etc/shared/default#
```

```
root@hasanraza-VirtualBox: /var/ossec/etc/shared/default
GNU nano 7.2 agent.conf
<agent_config>

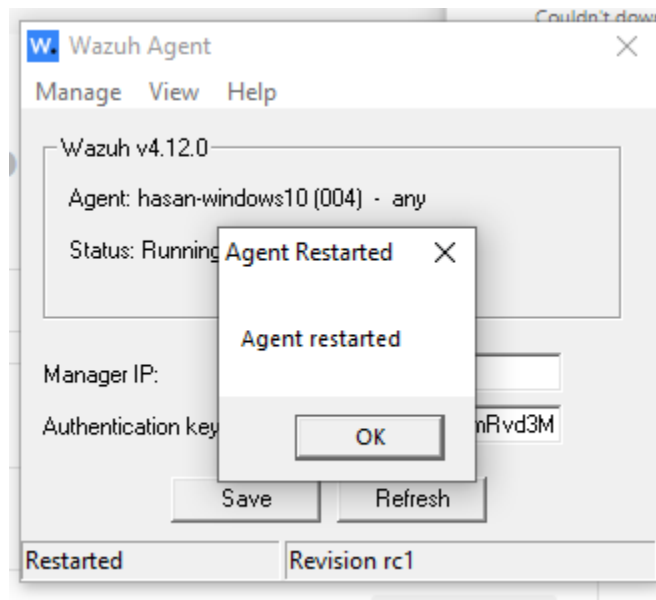
  <!-- Shared agent configuration here -->

<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>

</agent_config>
```

Then restarted all the services:

```
hasanraza@hasanraza-VirtualBox:~$ sudo systemctl restart wazuh-manager
[sudo] password for hasanraza:
Warning: The unit file, source configuration file or drop-ins of wazuh-manager.s
ervice changed on disk. Run 'systemctl daemon-reload' to reload units.
hasanraza@hasanraza-VirtualBox:~$ sudo systemctl daemon-reload
hasanraza@hasanraza-VirtualBox:~$ sudo systemctl restart wazuh-manager
```



Then edited the config file on the windows using this command  
notepad "C:\Program Files (x86)\ossec-agent\ossec.conf"

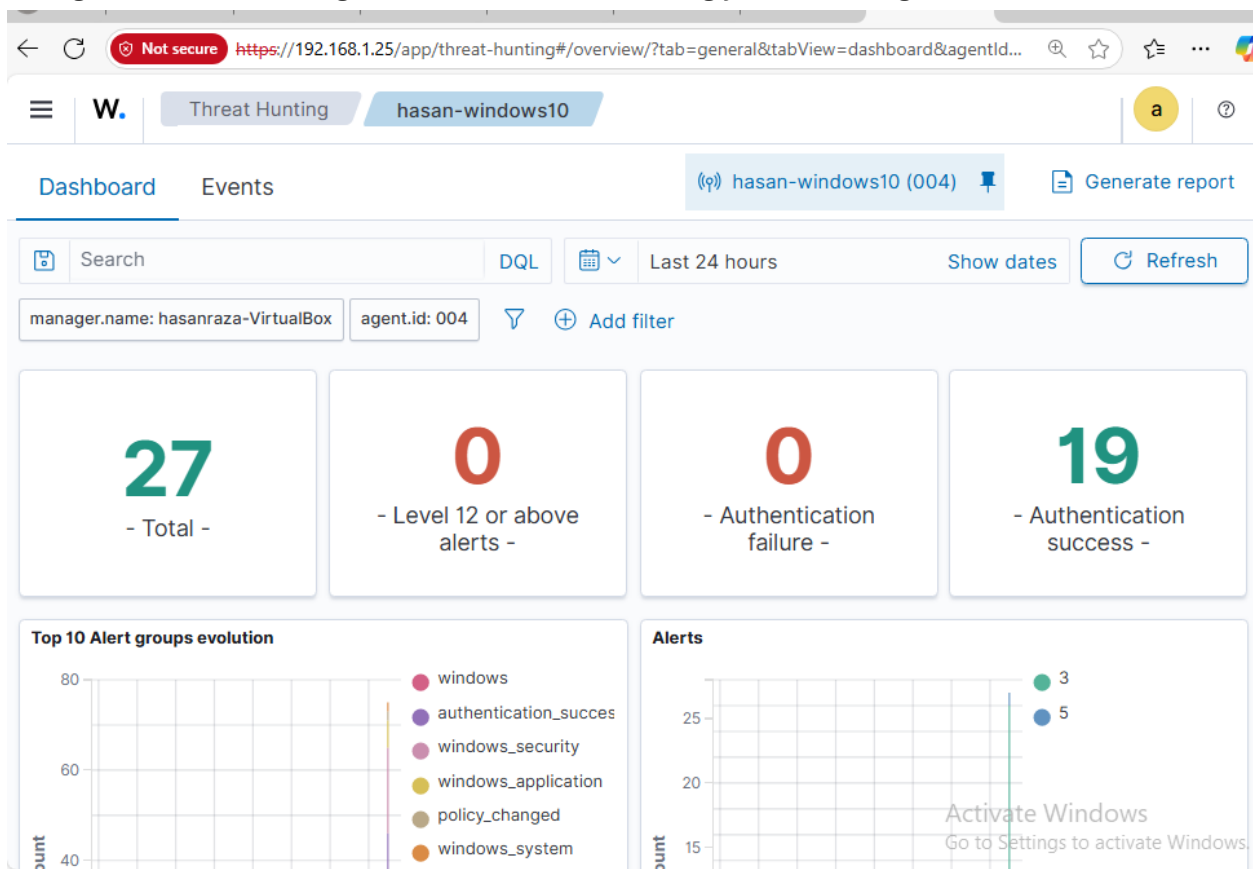
Added this part to the file:

```
<!-- ☒ Added: Windows Defender Operational Log -->
<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

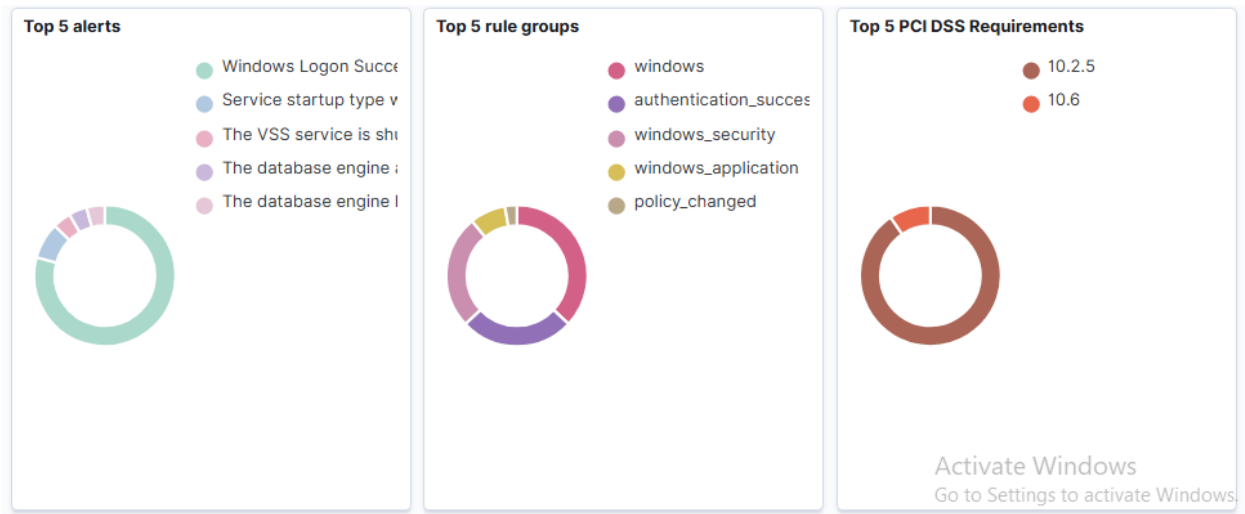
And then restarted the wazuh services using this command:

Restart-Service -Name Wazuh

Now goto “Threat Hunting events” tab after selecting your active agent:







Now it's time to download Ecar file to check if the system show alerts

<https://www.eicar.org/download-anti-malware-testfile/>

Downloaded this file:

The screenshot shows a web browser window at [https://www.eicar.org/download/eicar\\_com-zip/](https://www.eicar.org/download/eicar_com-zip/). The page features the EICAR logo and a section titled "EICAR.COM-ZIP" with a search bar and a table of download statistics. A Windows "Downloads" pop-up is visible, showing that the file "eicar\_com.zip" could not be downloaded because a virus was detected. The table on the page provides the following information:

EICAR.COM-ZIP	
Download	1139309
File Size	184 KB
Create Date	26. July 2022
<a href="#">Download</a>	

On the right side of the page, there is a "LATEST NEWS" section with a thumbnail image and the text: "Objective, history, addressees, application notes. Without sufficiently secure products, there can be no sufficiently secure processes: Cyber".

I tried everything but the windows defender logs were not forwarded to wazuh

```
hasanraza@hasanraza-VirtualBox:~$ sudo tail -f /var/ossec/logs/ossec.log
2025/07/22 17:05:07 wazuh-csyslogd: INFO: Remote syslog server not configured. Clean exit.
2025/07/22 17:05:07 wazuh-dbd: INFO: Database not configured. Clean exit.
2025/07/22 17:05:07 wazuh-integrator: INFO: Remote integrations not configured. Clean exit.
2025/07/22 17:05:07 wazuh-agentlessd: INFO: Not configured. Exiting.
2025/07/22 17:28:19 wazuh-modulesd:router: INFO: Loaded router module.
2025/07/22 17:28:19 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
2025/07/22 17:28:22 wazuh-csyslogd: INFO: Remote syslog server not configured. Clean exit.
2025/07/22 17:28:22 wazuh-dbd: INFO: Database not configured. Clean exit.
2025/07/22 17:28:22 wazuh-integrator: INFO: Remote integrations not configured. Clean exit.
2025/07/22 17:28:22 wazuh-agentlessd: INFO: Not configured. Exiting.
```

It should show something like this :

Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ( )	3
Windows Defender: Antimalware platform detected potentially unwanted software ( )	12
Windows Defender: Antimalware platform feature configuration changed	5
Windows Defender: Antimalware definitions updated successfully	3
Windows Defender: Antimalware definitions updated successfully	3
Service startup type was changed	3
Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ( )	3
Windows Defender: Antimalware platform detected potentially unwanted software ( )	12

# Virus Total Task:

## Obtain a VirusTotal API Key

1. Go to: <https://www.virustotal.com/gui/join-us>
2. Sign up or log in with your Google account.
3. After logging in, go to:  
[https://www.virustotal.com/gui/user/<your\\_username>/apikey](https://www.virustotal.com/gui/user/<your_username>/apikey)  
Or navigate to **API Key** in your account settings.
4. Copy the API key (you'll need it in the next step).

API KEY

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](#)

API QUOTA ALLOWANCES FOR YOUR USER

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:

Access level	⚠️ <b>Limited</b> , standard free public API	<a href="#">Upgrade to premium</a>
Usage	<b>Must not be used in business workflows, commercial products or services.</b>	
Request rate	4 lookups / min	
Daily quota	500 lookups / day	

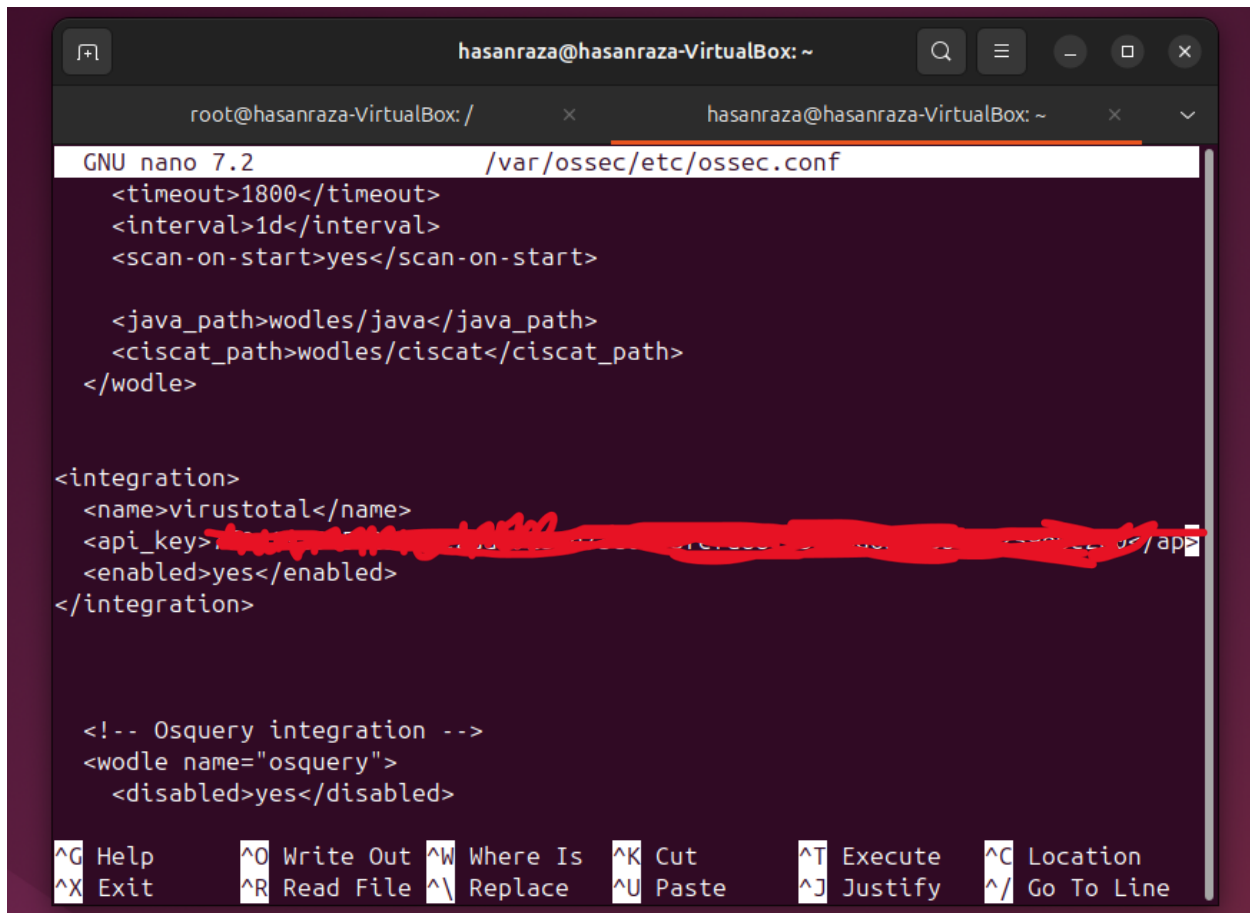
API reference Python client Golang library Command-line interface

Activate Windows Go to Settings to activate Windows interface

Now Integrate VirusTotal with Wazuh:

**Ubuntu Wazuh server**, edit the VirusTotal configuration file:

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



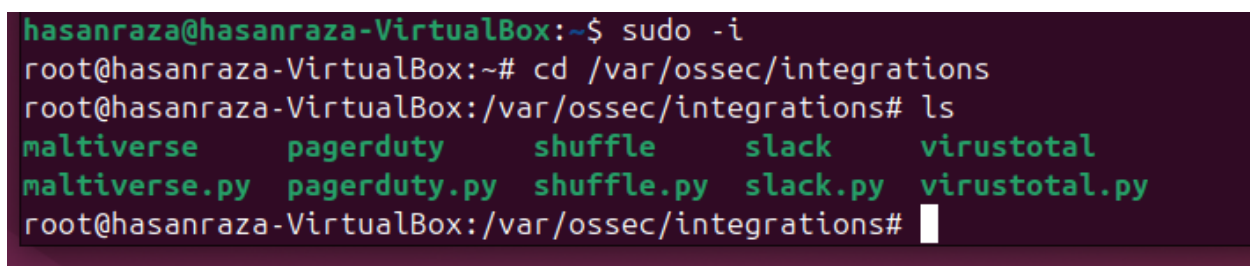
```
hasanraza@hasanraza-VirtualBox: ~
root@hasanraza-VirtualBox: /
GNU nano 7.2 /var/ossec/etc/ossec.conf
<timeout>1800</timeout>
<interval>1d</interval>
<scan-on-start>yes</scan-on-start>

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

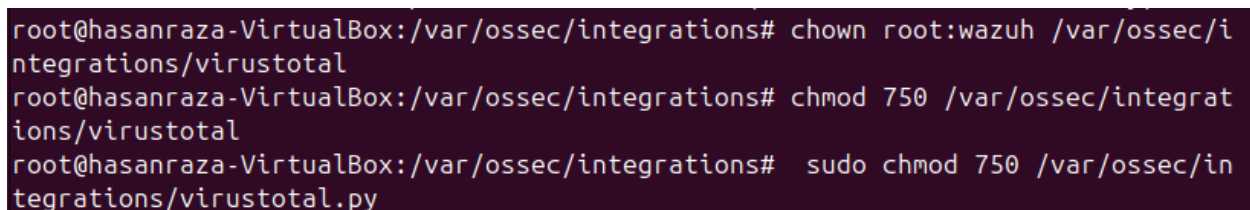
<integration>
  <name>virustotal</name>
  <api_key>[REDACTED]
  <enabled>yes</enabled>
</integration>

<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>

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



```
hasanraza@hasanraza-VirtualBox:~$ sudo -i
root@hasanraza-VirtualBox:~# cd /var/ossec/integrations
root@hasanraza-VirtualBox:/var/ossec/integrations# ls
maltiverse      pagerduty      shuffle        slack          virustotal
maltiverse.py   pagerduty.py   shuffle.py     slack.py       virustotal.py
root@hasanraza-VirtualBox:/var/ossec/integrations#
```



```
root@hasanraza-VirtualBox:/var/ossec/integrations# chown root:wazuh /var/ossec/integrations/virustotal
root@hasanraza-VirtualBox:/var/ossec/integrations# chmod 750 /var/ossec/integrations/virustotal
root@hasanraza-VirtualBox:/var/ossec/integrations# sudo chmod 750 /var/ossec/integrations/virustotal.py
```

Then saved the file and restarted the wazuh manager:

```
hasanraza@hasanraza-VirtualBox:~$ sudo systemctl restart wazuh-manager
hasanraza@hasanraza-VirtualBox:~$
```

## Used a Known Public Malware Hash

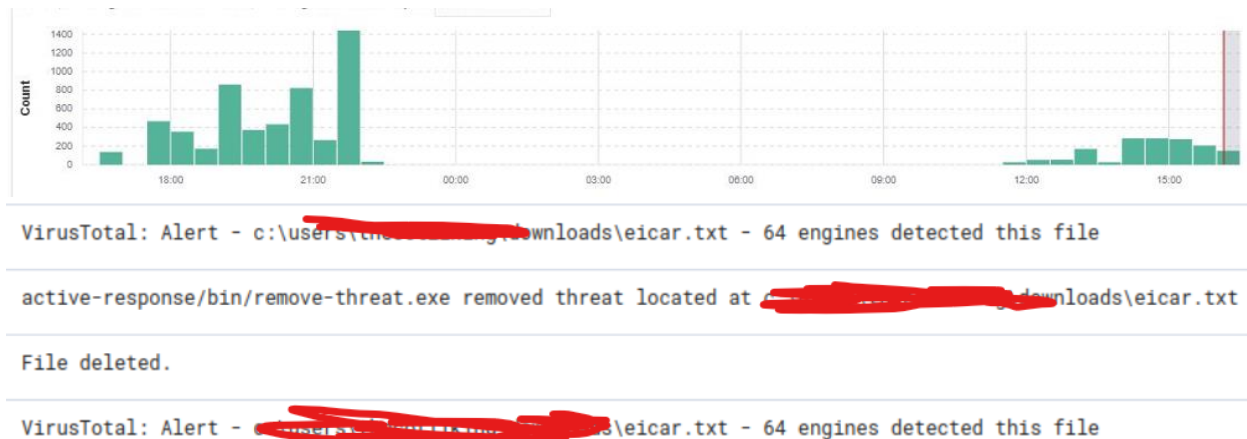
### EICAR test hash:

- **SHA1 of EICAR test file:**

3395856ce81f2b7382dee72602f798b642f14140

```
hasanraza@hasanraza-VirtualBox:~$ sudo /var/ossec/integrations/virustotal -a 7f0
[REDACTED] -q 3395856ce81f2b7
382dee72602f798b642f14140
```

### Results:



t	data.virustotal.total	68
t	decoder.name	json
t	id	1751368842.1417546
t	input.type	log
t	location	virustotal
t	manager.name	kali
t	rule.description	VirusTotal: Alert - c:\users\ [REDACTED] \downloads\eicar_com\eicar.com - 64 engines detected this file
#	rule.firedtimes	3
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