Endpoint Security & Threat Intelligence Integration

Name: Mahnoor Shafi
Email: mahnoorshafi88@gmail.com
Internship Batch: SOC [1-7-2025 – 1-8-2025]
Week: 3
Task Title: Endpoint Security & Threat Intelligence Integration

Table of Content:

Objective

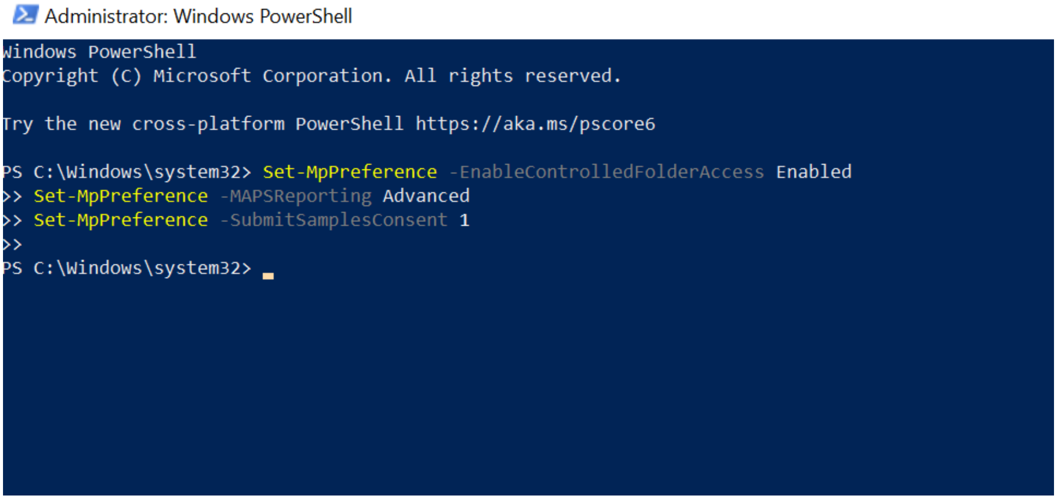
This week’s task was focused on enhancing endpoint visibility and enriching Wazuh alerts with external threat intelligence using VirusTotal. Key components included enabling Defender logs, integrating Wazuh with VirusTotal, and simulating alerts for testing.

Step 1: Enable Windows Defender Logs on Windows

To enable Defender logging:

Commands Used:

Set-MpPreference -EnableControlledFolderAccess Enabled
Set-MpPreference -MAPSReporting Advanced
Set-MpPreference -SubmitSamplesConsent 1

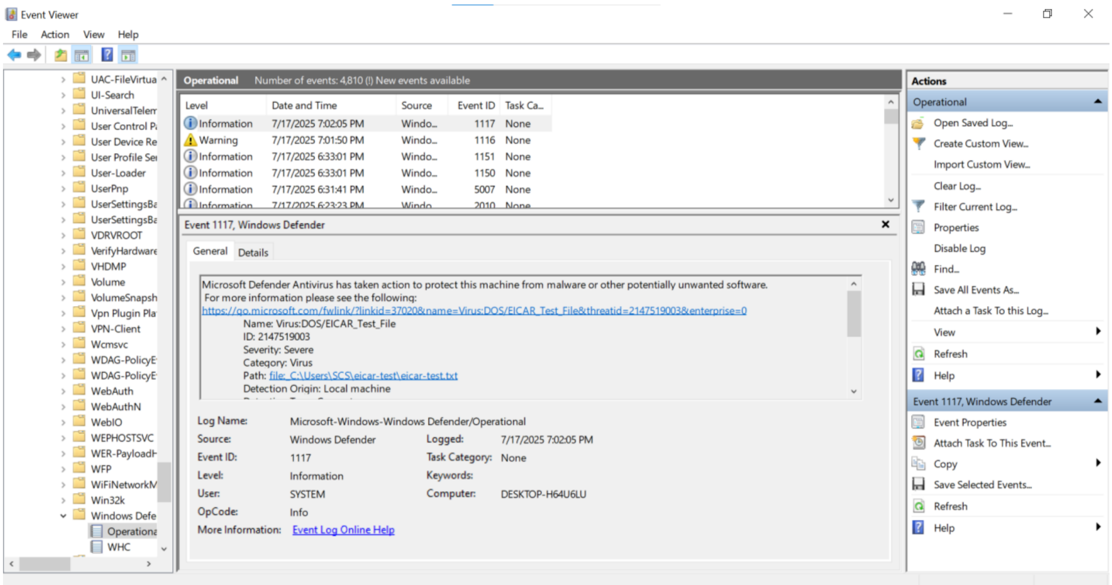


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-MpPreference -EnableControlledFolderAccess Enabled
>> Set-MpPreference -MAPSReporting Advanced
>> Set-MpPreference -SubmitSamplesConsent 1
>>
PS C:\Windows\system32> _
```

6

Enabled **Event Viewer > Applications and Services Logs > Microsoft > Windows > Windows Defender > Operational**

Defender Log in Event Viewer:



Operational Number of events: 4,810 (!) New events available

Level	Date and Time	Source	Event ID	Task Ca...
Information	7/17/2025 7:02:05 PM	Windo...	1117	None
Warning	7/17/2025 7:01:50 PM	Windo...	1116	None
Information	7/17/2025 6:33:01 PM	Windo...	1151	None
Information	7/17/2025 6:33:01 PM	Windo...	1150	None
Information	7/17/2025 6:31:41 PM	Windo...	5007	None
Information	7/17/2025 6:23:23 PM	Windo...	2010	None

Event 1117, Windows Defender

```
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0
 	Name: Virus:DOS/EICAR_Test_File
 	ID: 2147519003
 	Severity: Severe
 	Category: Virus
 	Path: file:_C:\Users\SCS\eicar-test\eicar-test.txt
 	Detection Origin: Local machine
```

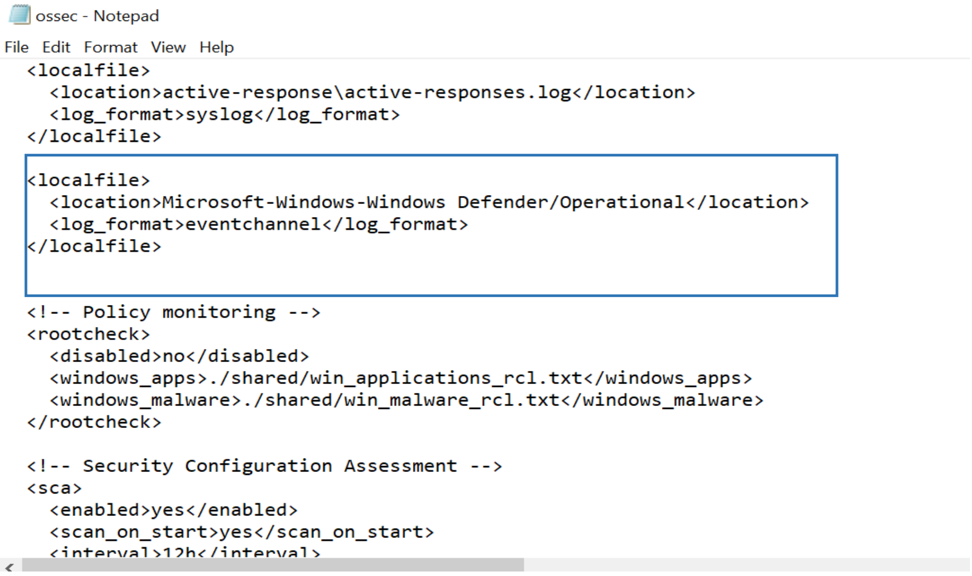
Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	7/17/2025 7:02:05 PM
Event ID:	1117	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-H64U6LU
OpCode:	Info		
More Information:	Event Log Online Help		

Step 2: Configure Wazuh Agent to Collect Defender Logs

Modified the ossec.conf file to include the Defender event channel.

Configuration:

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

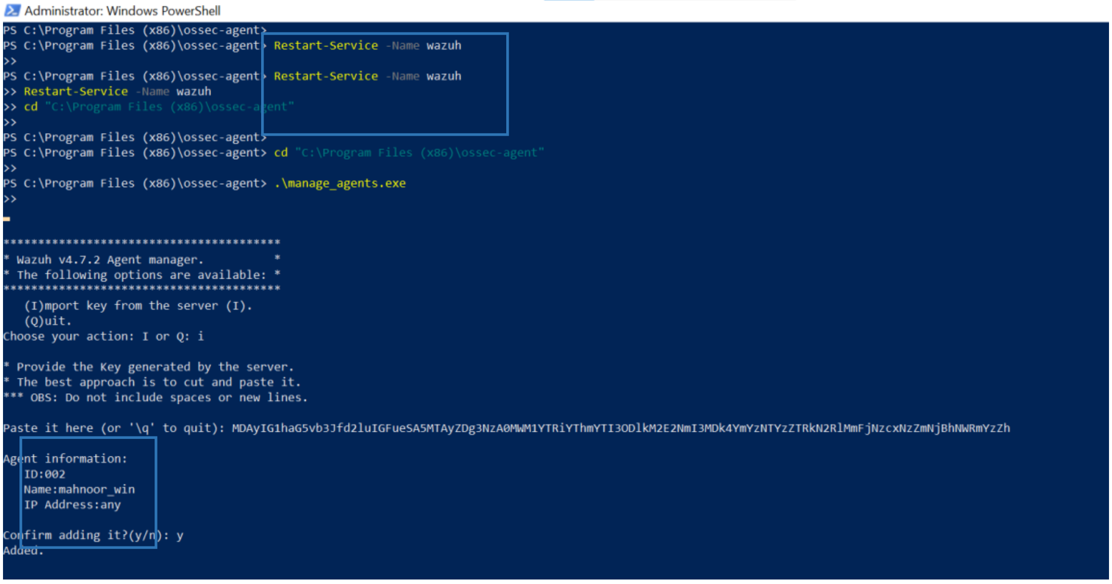


ossec - Notepad

```
<localfile>
  <location>active-response\active-responses.log</location>
  <log_format>syslog</log_format>
</localfile>

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

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
```

Restarted the agent with:

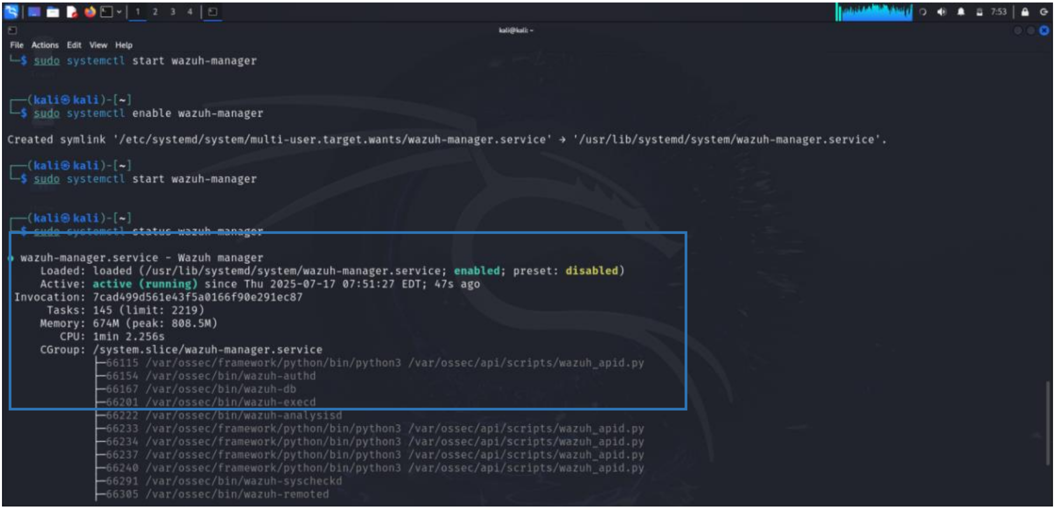
Restart-Service -Name wazuh



Administrator: Windows PowerShell

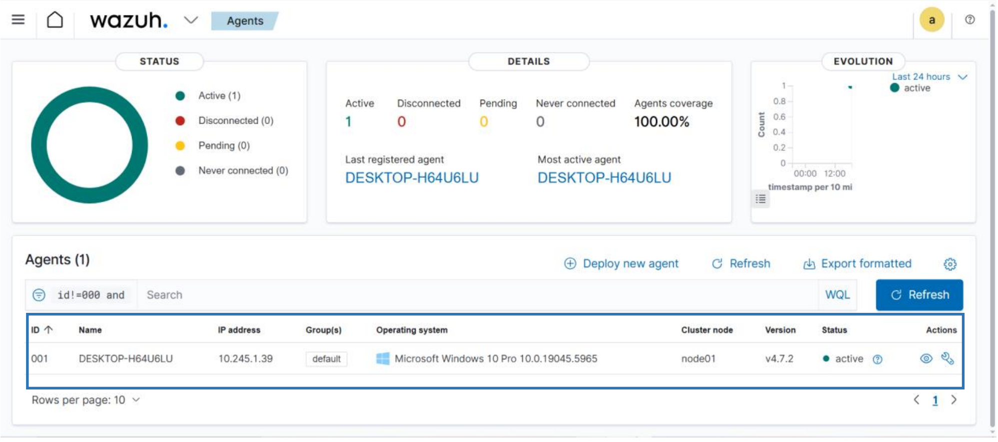
```
PS C:\Program Files (x86)\ossec-agent>
PS C:\Program Files (x86)\ossec-agent> Restart-Service -Name wazuh
>>
PS C:\Program Files (x86)\ossec-agent> Restart-Service -Name wazuh
>> Restart-Service -Name wazuh
>> cd "C:\Program Files (x86)\ossec-agent"
>>
PS C:\Program Files (x86)\ossec-agent>
PS C:\Program Files (x86)\ossec-agent> cd "C:\Program Files (x86)\ossec-agent"
>>
PS C:\Program Files (x86)\ossec-agent> .\manage_agents.exe
>>


****************************************
* Wazuh v4.7.2 Agent manager.          *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDAyIG1haG5vb3Jfd2luIGFueSA5MTAyZDg3NzA0MWM1YTRiYThmYTI3ODlkM2E2NmI3MDk4YmYzNTYzZTRkN2RlMmFjNzcxNzZmNjBhNWRmYzZh

Agent information:
   ID:002
   Name:mahnoor_win
   IP Address:any

Confirm adding it?(y/n): y
Added.
```

Wazuh Agent Running



```
└─$ sudo systemctl start wazuh-manager


┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable wazuh-manager

Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-manager.service' → '/usr/lib/systemd/system/wazuh-manager.service'.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start wazuh-manager


┌──(kali㉿kali)-[~]
└─$ sudo systemctl status wazuh-manager

● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-07-17 07:51:27 EDT; 47s ago
 Invocation: 7cad499d561e43f5a0166f90e291ec87
      Tasks: 145 (limit: 2219)
     Memory: 674M (peak: 808.5M)
        CPU: 1min 2.256s
     CGroup: /system.slice/wazuh-manager.service
             ├─66115 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─66154 /var/ossec/bin/wazuh-authd
             ├─66167 /var/ossec/bin/wazuh-db
             ├─66201 /var/ossec/bin/wazuh-execd
             ├─66222 /var/ossec/bin/wazuh-analysisd
             ├─66233 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─66234 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─66237 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─66240 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─66291 /var/ossec/bin/wazuh-syscheckd
             ├─66305 /var/ossec/bin/wazuh-remoted
```

:



Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent: DESKTOP-H64U6LU

Most active agent: DESKTOP-H64U6LU

Agents (1)

id!=000 and Search

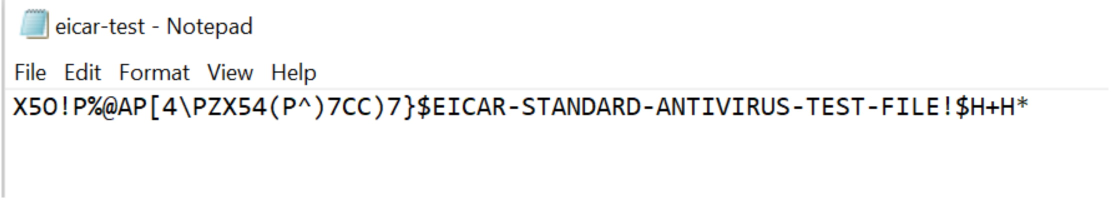
ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	DESKTOP-H64U6LU	10.245.1.39	default	Microsoft Windows 10 Pro 10.0.19045.5965	node01	v4.7.2	● active	

Step 3: Simulate Defender Alert Using EICAR Test File

Created a .txt file containing the EICAR test string to simulate a malware detection.

EICAR String:

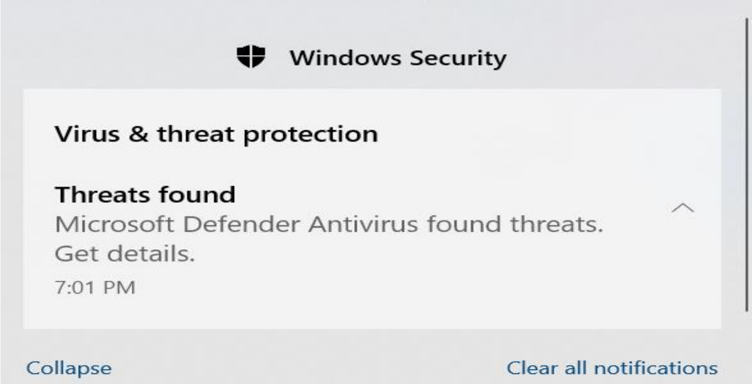
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*



eicar-test - Notepad

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Defender Alert triggered by EICAR

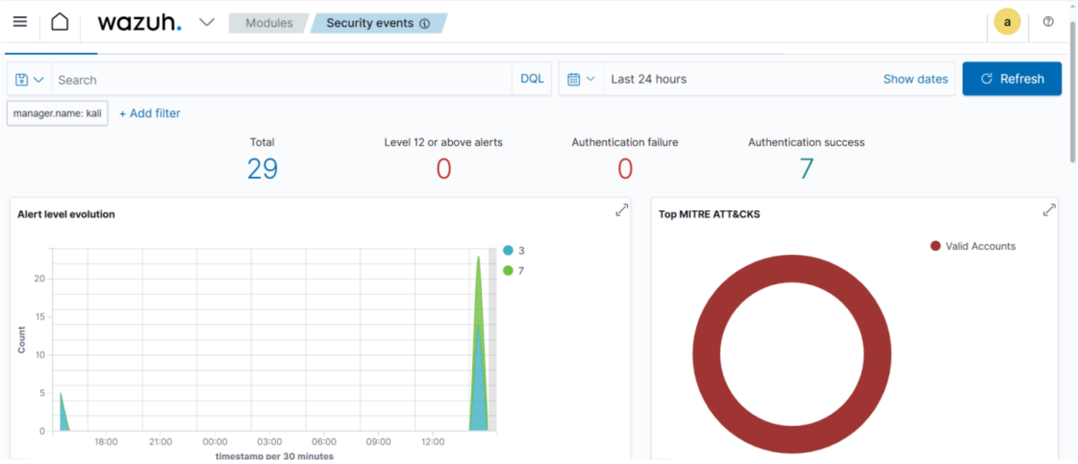


Windows Security

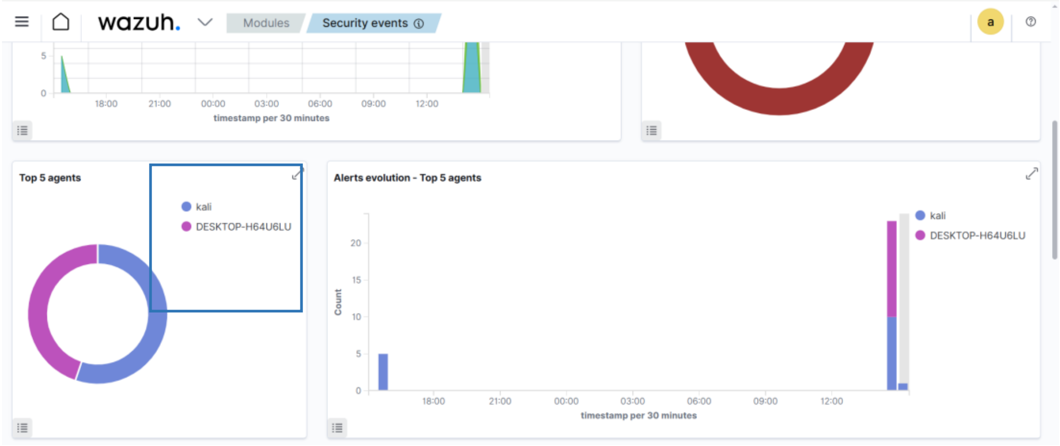
Virus & threat protection

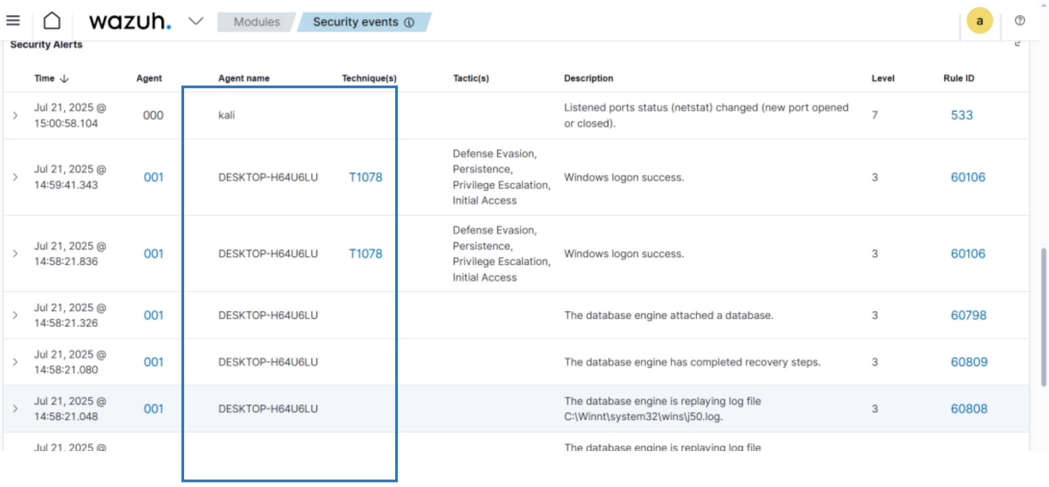
Threats found
Microsoft Defender Antivirus found threats. Get details.
7:01 PM

Wazuh Dashboard showing alert



Total 29
Level 12 or above alerts 0
Authentication failure 0
Authentication success 7



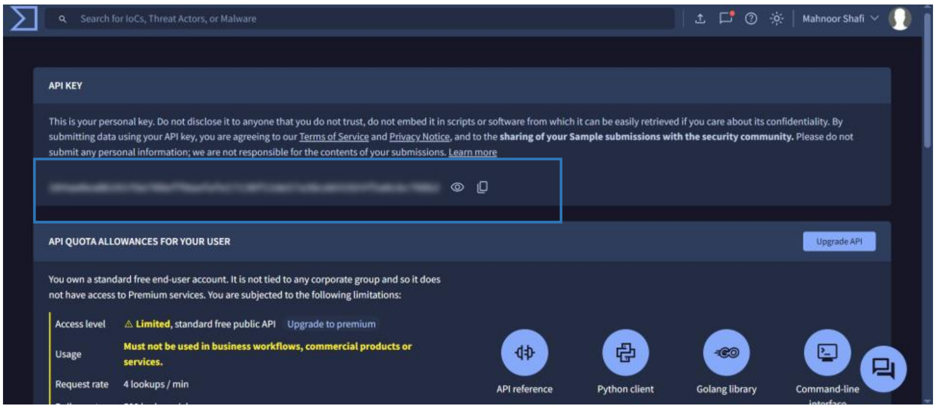


Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 21, 2025 @ 15:00:58.104	000	kali			Listened ports status (netstat) changed (new port opened or closed).	7	533
Jul 21, 2025 @ 14:59:41.343	001	DESKTOP-H64U6LU	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 21, 2025 @ 14:58:21.836	001	DESKTOP-H64U6LU	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 21, 2025 @ 14:58:21.326	001	DESKTOP-H64U6LU			The database engine attached a database.	3	60798
Jul 21, 2025 @ 14:58:21.080	001	DESKTOP-H64U6LU			The database engine has completed recovery steps.	3	60809
Jul 21, 2025 @ 14:58:21.048	001	DESKTOP-H64U6LU			The database engine is replaying log file C:\Winnt\system32\wins\j50.log.	3	60808
Jul 21, 2025 @					The database engine is replaying log file		

Step 4: Obtain VirusTotal API Key

Created a free account at https://virustotal.com and copied the API key from the user dashboard.



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

[redacted]

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	⚠ **Limited**, standard free public API Upgrade to premium
Usage	**Must not be used in business workflows, commercial products or services.**
Request rate	4 lookups / min

Step 5: Configure VirusTotal Integration in Wazuh

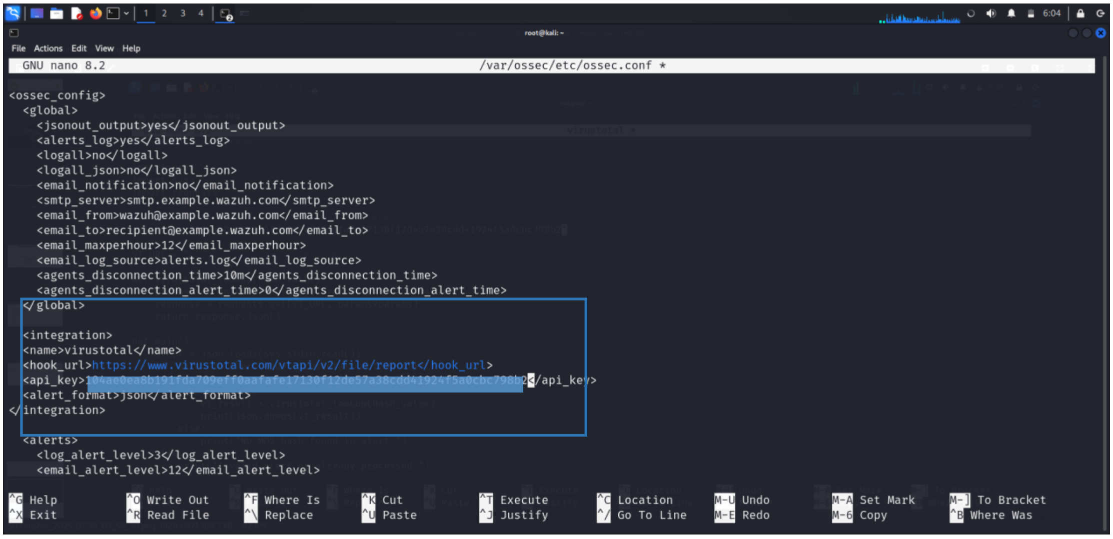
Edited virustotal integration script and ossec.conf to add the API key and hook.

Script Config:

```
api_key = "your_virustotal_api_key"
```

Wazuh Config:

```
<integration>
  <name>virustotal</name>

<hook_url>https://www.virustotal.com/vtapi/v2/file/report</hook_url>
  <api_key>your_virustotal_api_key</api_key>
  <alert_format>json</alert_format>
</integration>
```



root@kali: ~

File Actions Edit View Help

```
 GNU nano 8.2                       /var/ossec/etc/ossec.conf *

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <integration>
  <name>virustotal</name>
  <hook_url>https://www.virustotal.com/vtapi/v2/file/report</hook_url>
  <api_key>104ae0ea8b191fda709eff0aafafe17130f12de57a38cdd41924f5a0cbc798b2</api_key>
  <alert_format>json</alert_format>
</integration>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>

^G Help      ^O Write Out  ^F Where Is  ^K Cut    ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracket
^X Exit      ^R Read File  ^\ Replace   ^U Paste  ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^B Where Was
```

Restarted Wazuh:

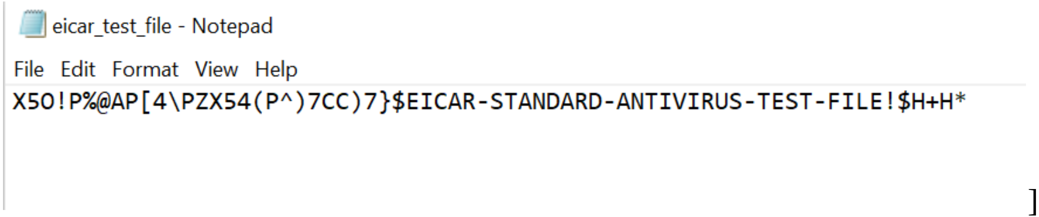
```
sudo systemctl restart wazuh-manager
```

Step 6: Generate File Hash

Used PowerShell to get SHA256 hash of a test file.

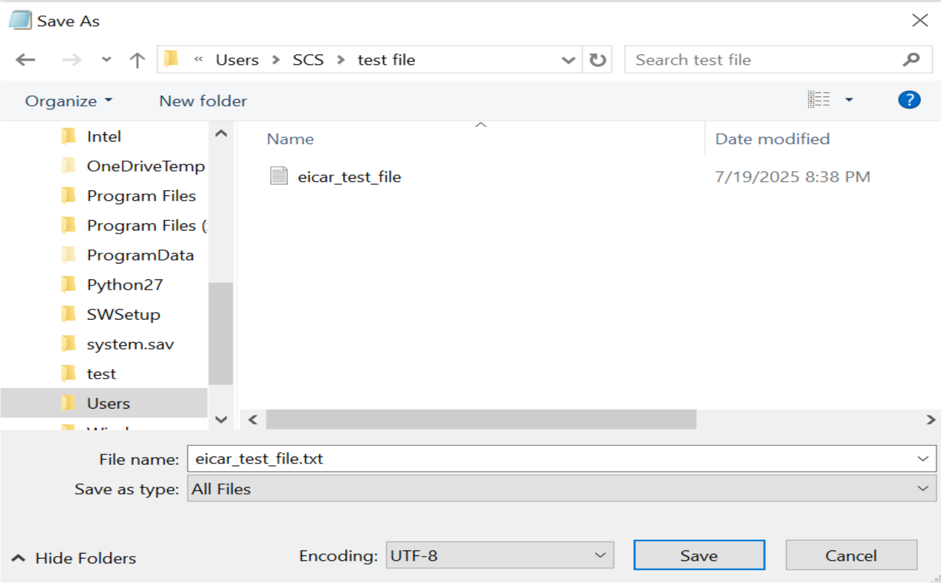
Command:

```
Get-FileHash C:\path\to\eicar.txt -Algorithm SHA256
```



```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

]

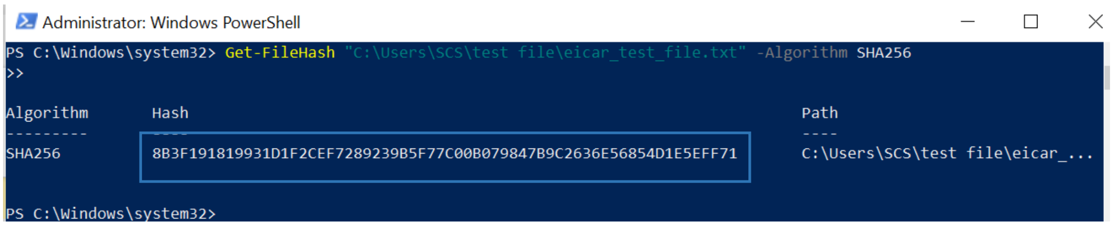


eicar_test_file 7/19/2025 8:38 PM

File name: eicar_test_file.txt

Save as type: All Files

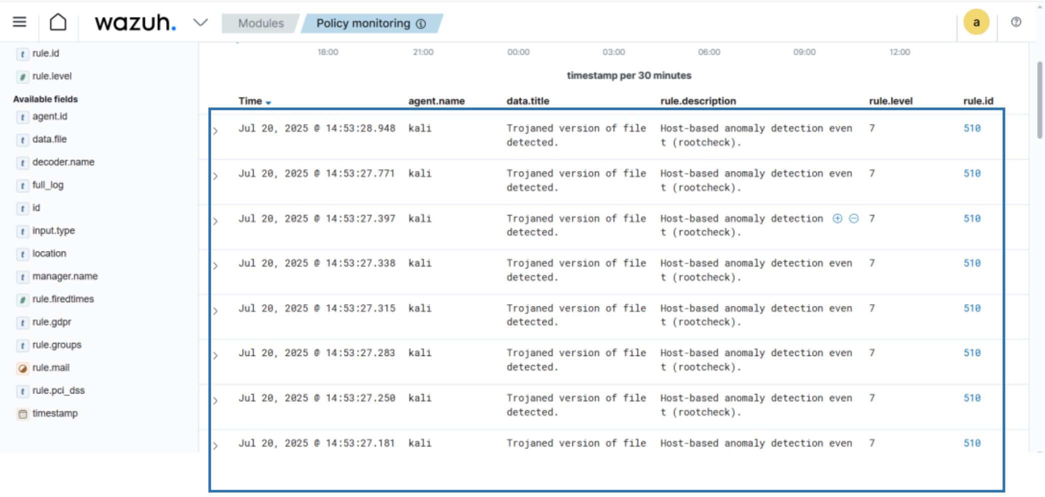
Encoding: UTF-8



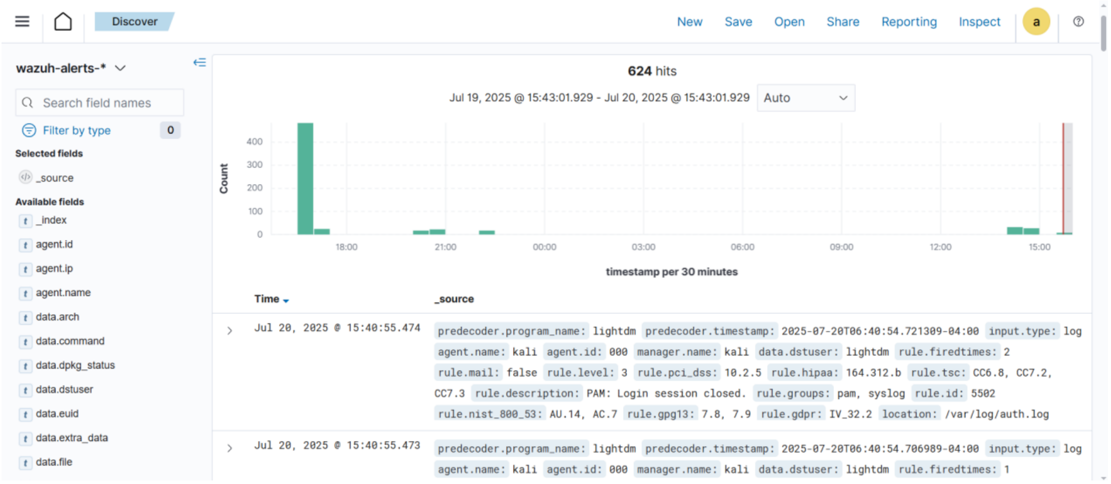
```
PS C:\Windows\system32> Get-FileHash "C:\Users\SCS\test file\eicar_test_file.txt" -Algorithm SHA256
>>

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          8B3F191819931D1F2CEF7289239B5F77C00B079847B9C2636E56854D1E5EFF71       C:\Users\SCS\test file\eicar_...


PS C:\Windows\system32>
```

Step 7: Submit Hash to VirusTotal via Wazuh

Wazuh sent the hash automatically upon detection. Observed enrichment in logs.



Time	agent.name	data.title	rule.description	rule.level	rule.id
Jul 20, 2025 @ 14:53:28.948	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.771	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.397	kali	Trojaned version of file detected.	Host-based anomaly detection ⊕ ⊖ t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.338	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.315	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.283	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.250	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.181	kali	Trojaned version of file	Host-based anomaly detection even	7	510

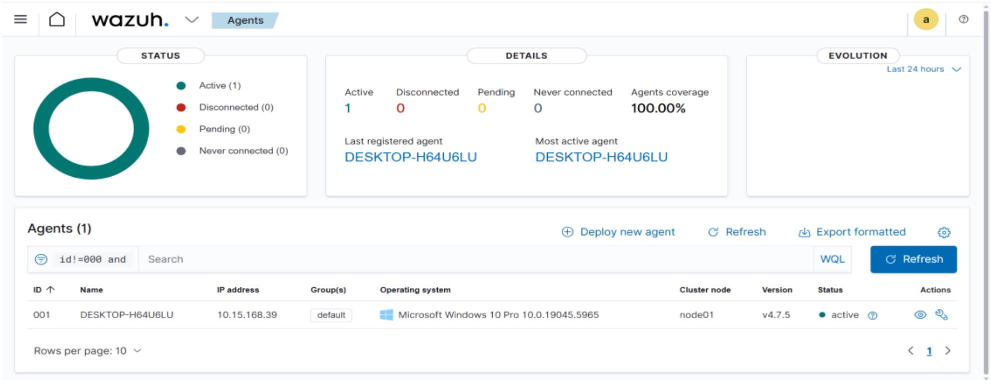


```
Jul 20, 2025 @ 15:40:55.474  predecoder.program_name: lightdm predecoder.timestamp: 2025-07-20T06:40:54.721309-04:00 input.type: log
                             agent.name: kali agent.id: 000 manager.name: kali data.dstuser: lightdm rule.firedtimes: 2
                             rule.mail: false rule.level: 3 rule.pci_dss: 10.2.5 rule.hipaa: 164.312.b rule.tsc: CC6.8, CC7.2,
                             CC7.3 rule.description: PAM: Login session closed. rule.groups: pam, syslog rule.id: 5502
                             rule.nist_800_53: AU.14, AC.7 rule.gpg13: 7.8, 7.9 rule.gdpr: IV_32.2 location: /var/log/auth.log

Jul 20, 2025 @ 15:40:55.473  predecoder.program_name: lightdm predecoder.timestamp: 2025-07-20T06:40:54.706989-04:00 input.type: log
                             agent.name: kali agent.id: 000 manager.name: kali data.dstuser: lightdm rule.firedtimes: 1
```

Step 8: Validate VirusTotal Intelligence in Logs

Searched for "virustotal" in Kibana/Wazuh Dashboard to c

confirm enrichment fields like positives, scan_date, etc.



Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

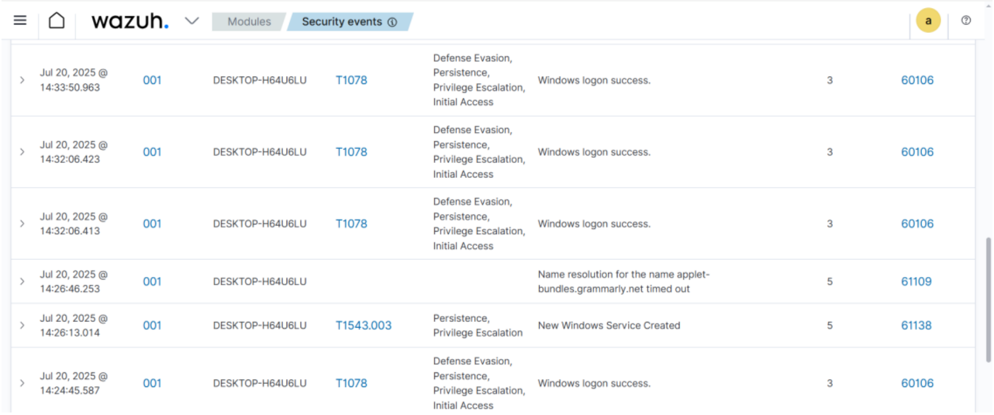
Last registered agent
DESKTOP-H64U6LU

Most active agent
DESKTOP-H64U6LU

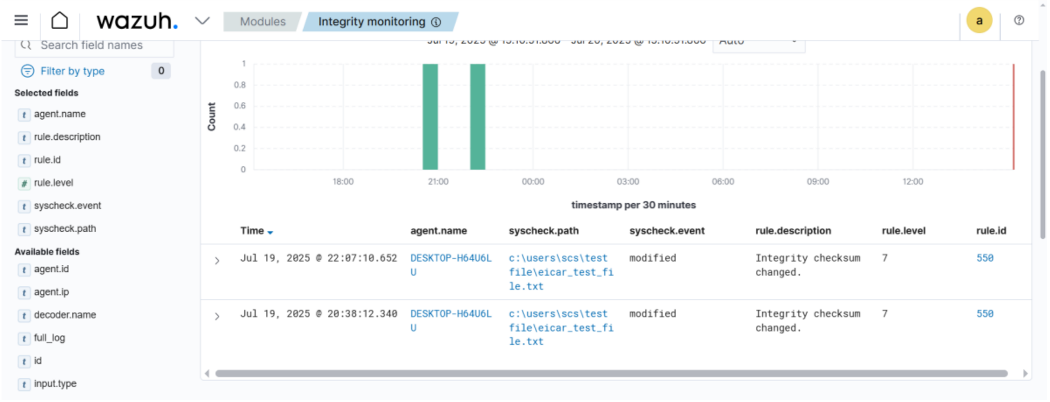
Agents (1)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	DESKTOP-H64U6LU	10.15.168.39	default	Microsoft Windows 10 Pro 10.0.19045.5965	node01	v4.7.5	● active	

Rows per page: 10



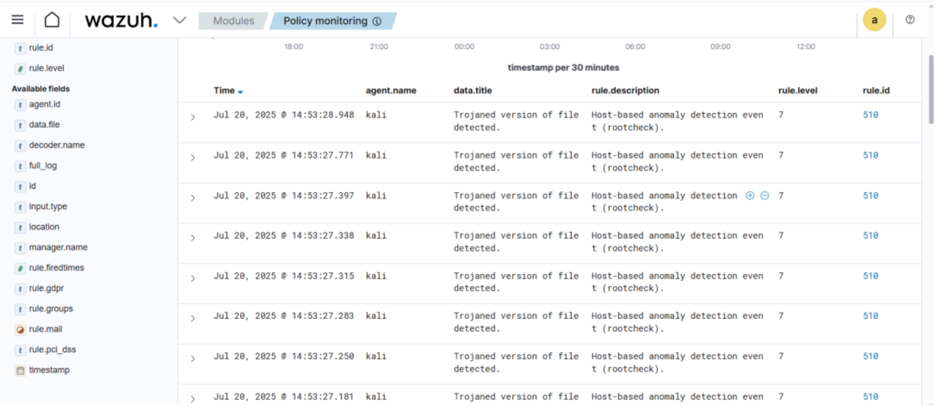
Jul 20, 2025 @ 14:33:50.963	001	DESKTOP-H64U6LU	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 20, 2025 @ 14:32:06.423	001	DESKTOP-H64U6LU	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 20, 2025 @ 14:32:06.413	001	DESKTOP-H64U6LU	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jul 20, 2025 @ 14:26:46.253	001	DESKTOP-H64U6LU			Name resolution for the name applet-bundles.grammarly.net timed out	5	61109
Jul 20, 2025 @ 14:26:13.014	001	DESKTOP-H64U6LU	T1543.003	Persistence, Privilege Escalation	New Windows Service Created	5	61138
Jul 20, 2025 @ 14:24:45.587	001	DESKTOP-H64U6LU	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106



Selected fields
- agent.name
- rule.description
- rule.id
- rule.level
- syscheck.event
- syscheck.path

Available fields
- agent.id
- agent.ip
- decoder.name
- full_log
- id
- input.type

Time	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jul 19, 2025 @ 22:07:10.652	DESKTOP-H64U6LU	c:\users\scs\test file\eicar_test_file.txt	modified	Integrity checksum changed.	7	550
Jul 19, 2025 @ 20:38:12.340	DESKTOP-H64U6LU	c:\users\scs\test file\eicar_test_file.txt	modified	Integrity checksum changed.	7	550



Time	agent.name	data.title	rule.description	rule.level	rule.id
Jul 20, 2025 @ 14:53:28.948	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.771	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.397	kali	Trojaned version of file detected.	Host-based anomaly detection t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.338	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.315	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.283	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.250	kali	Trojaned version of file detected.	Host-based anomaly detection even t (rootcheck).	7	510
Jul 20, 2025 @ 14:53:27.181	kali	Trojaned version of file	Host-based anomaly detection even	7	510

Summary

Defender logs were successfully integrated.
VirusTotal API was configured and tested.
Wazuh dashboard reflected alerts with external threat intel.
Screenshots were taken at each milestone.