



Windows Defender Logs Integration

Created By: Amir Raza

Follow Me: www.linkedin.com/in/amirsoc

Windows Defender Logs Integration

What is Windows Defender?

Windows Defender, now called Microsoft Defender Antivirus, is a free antivirus program built into the Windows operating system. It protects computers from viruses, malware, ransomware, spyware, and other harmful threats.

According to the 2023 Antivirus Market Report, Windows Defender is the most widely used free antivirus software, with about 40% of the free antivirus market share.

Microsoft also offers an advanced version for businesses, called Windows Defender for Endpoint, which provides additional security features for enterprise environments.

Because of its popularity and importance, integrating Windows Defender with monitoring systems like Wazuh becomes very useful for improving security visibility.

Why Integrate Windows Defender with Wazuh?

Wazuh is an open-source security monitoring platform that collects logs from various systems and generates security alerts. It helps organizations detect threats, monitor system activities, and take quick action in case of security incidents.

However, by default, Wazuh cannot read Windows Defender logs. This means that even though Windows Defender may detect threats or perform scans, Wazuh will not be able to see or analyze that information unless we set up a proper integration.

To solve this, we need to configure the Windows system and Wazuh agent so that the Defender logs are collected and forwarded to the Wazuh manager.

Once integrated, security teams can:

- Collect logs from Windows Defender across multiple systems
- Analyze those logs in one centralized platform
- Get real-time alerts when malware is detected or a scan is performed
- Correlate Defender events with other system logs
- Make security monitoring and incident response more efficient and organized

This integration allows organizations to combine antivirus protection with powerful log analysis, making their systems more secure and easier to manage.

What You Achieve After Integration?

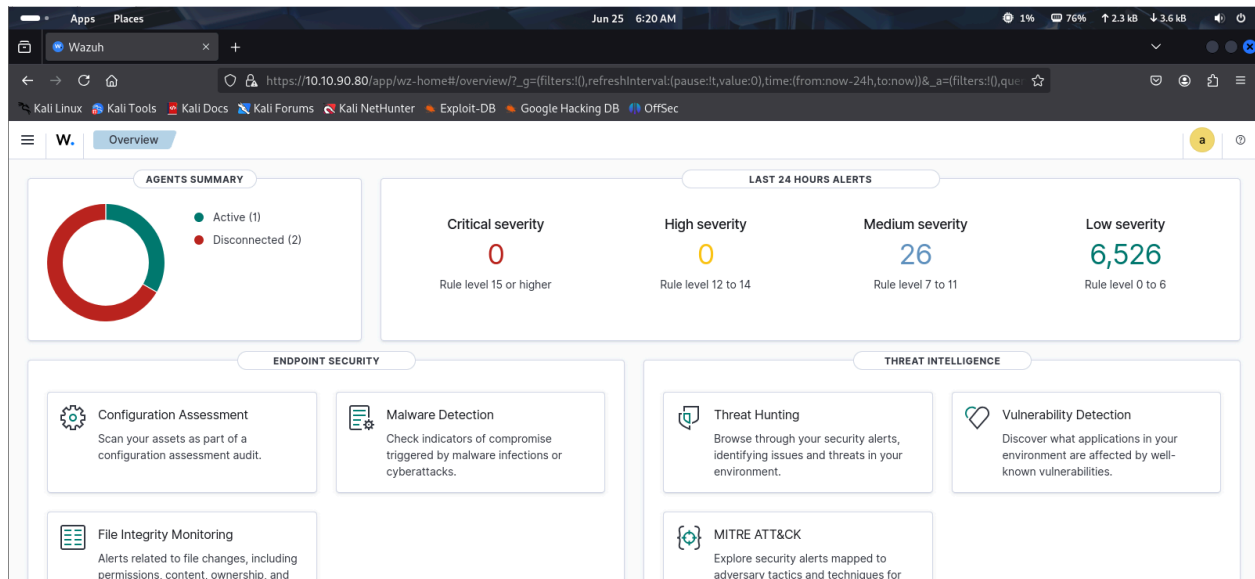
After integrating Windows Defender with Wazuh, you gain access to valuable security information that helps your team detect and respond to incidents more effectively.

Here's what Defender logs include, and what you gain by sending them to Wazuh:

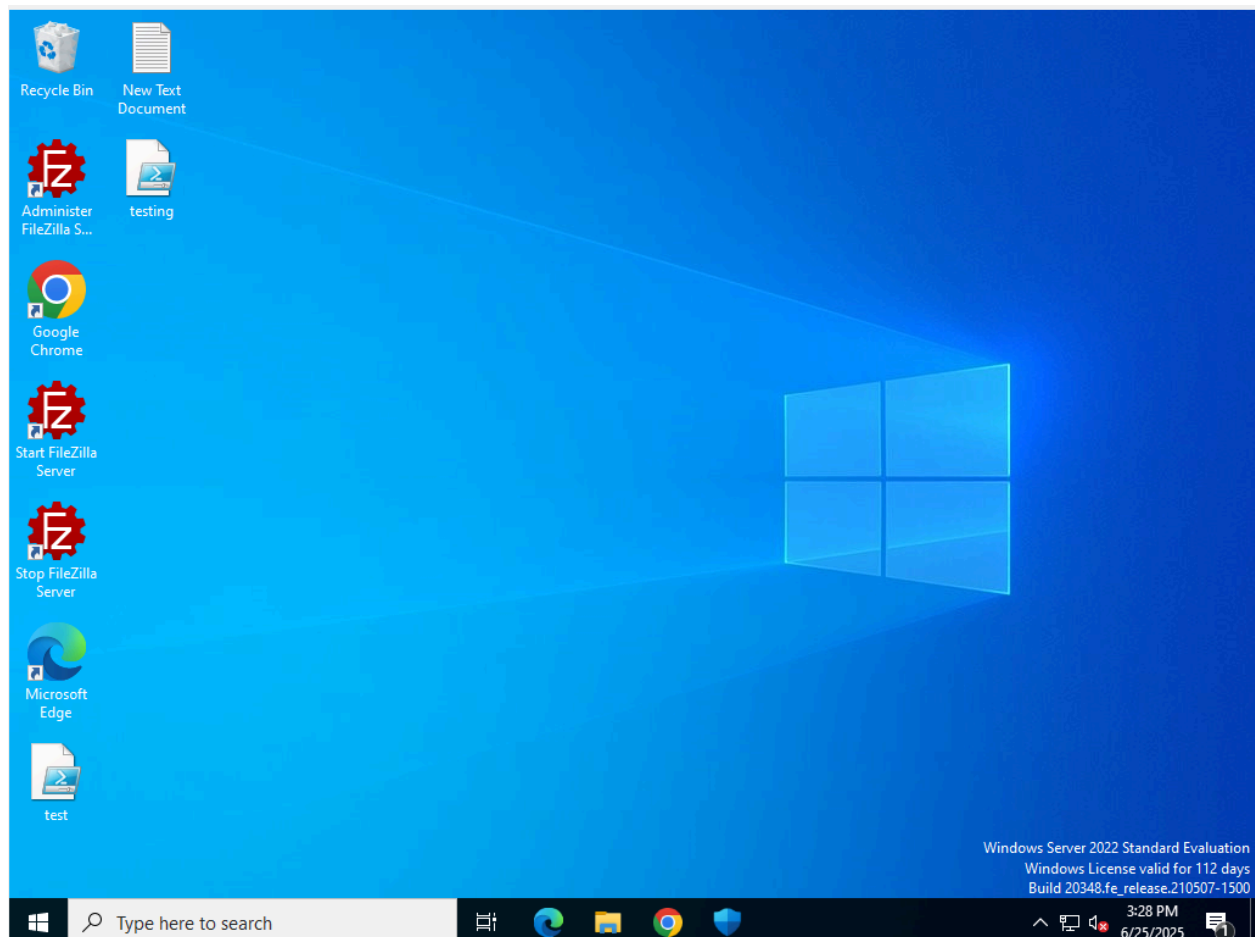
Defender Log Type	Benefit with Wazuh
Scan activities	View when and what files were scanned across all systems
Threat detections	Monitor detected threats in real-time
Remediation actions	See if threats were quarantined or removed
Update status	Ensure Defender is updated and active on all systems
Firewall/network alerts	Track suspicious traffic or blocked connections
Real-time protection events	Monitor events triggered by real-time antivirus protection

I have successfully set up a Wazuh server in my lab environment using Kali Linux. The Wazuh dashboard is accessible through a web browser by entering the server's IP address (e.g., `http://<IP_Address>`) in Firefox. This setup allows me to monitor security events in real-time and enhances my hands-on experience with centralized log management and threat detection.

Here is Wazuh Server dashboard.

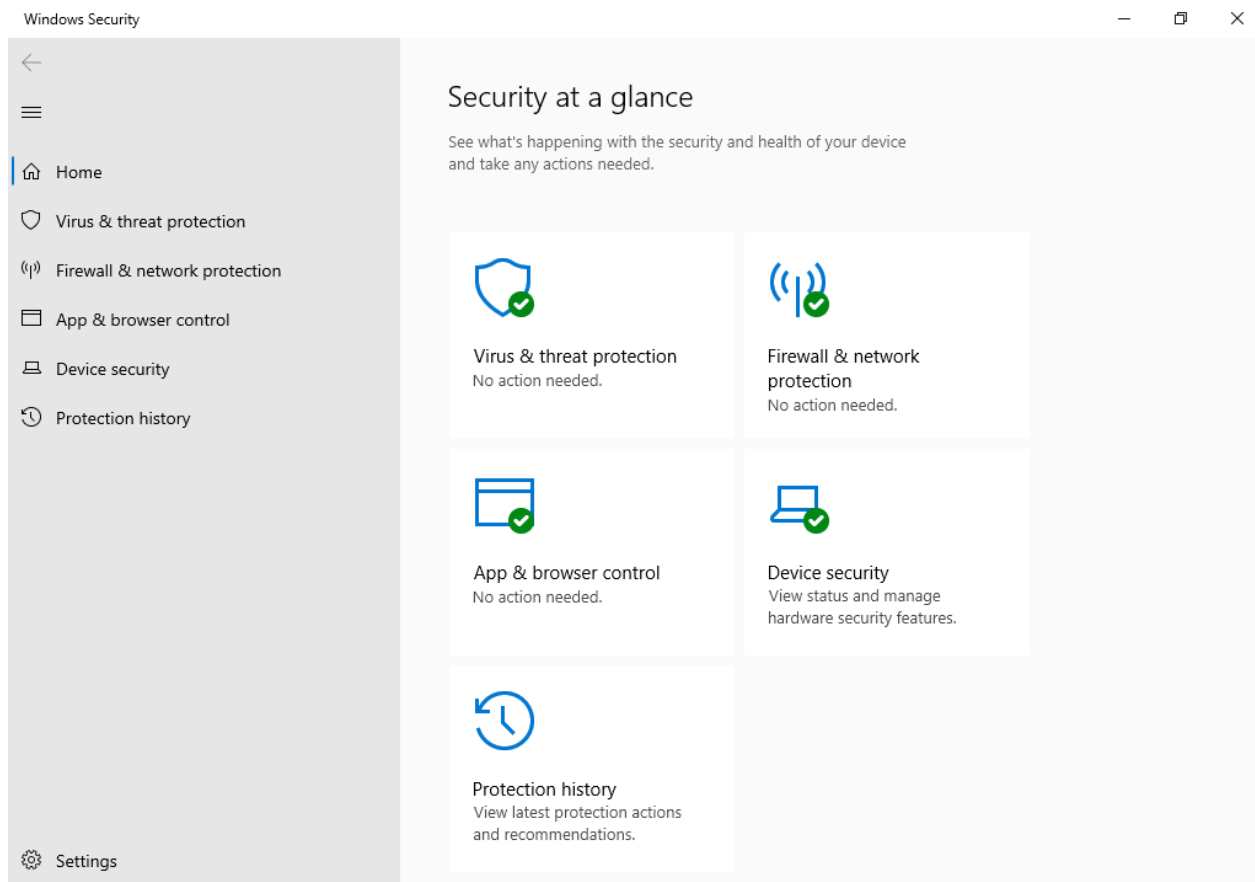


Here is window server 2022 is running on oracle virtual box.

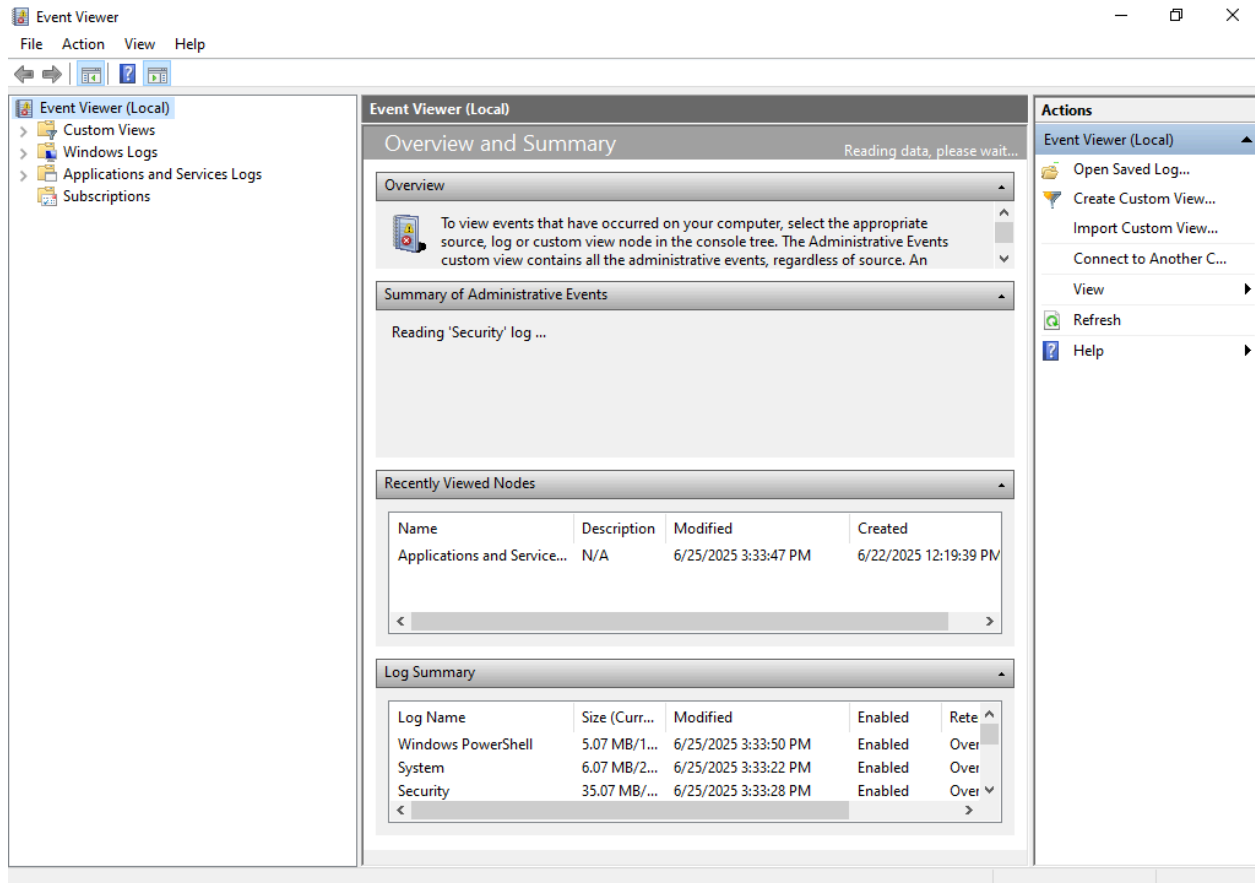


I searched for **"Windows Security"** from the **Start menu** to access the built-in antivirus and security settings on the Windows system.

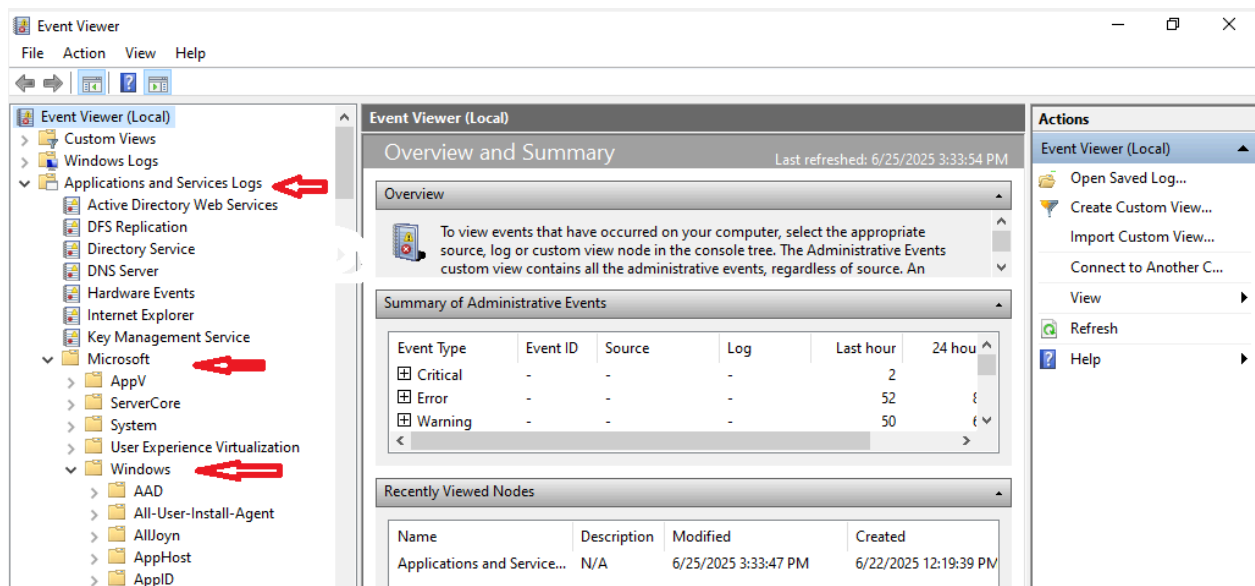
Windows Defender or real-time protection is ON and running actively.



Now go to "Event Viewer" and open it.



Now go to "Application and Services Logs" > "Microsoft" > "Windows".

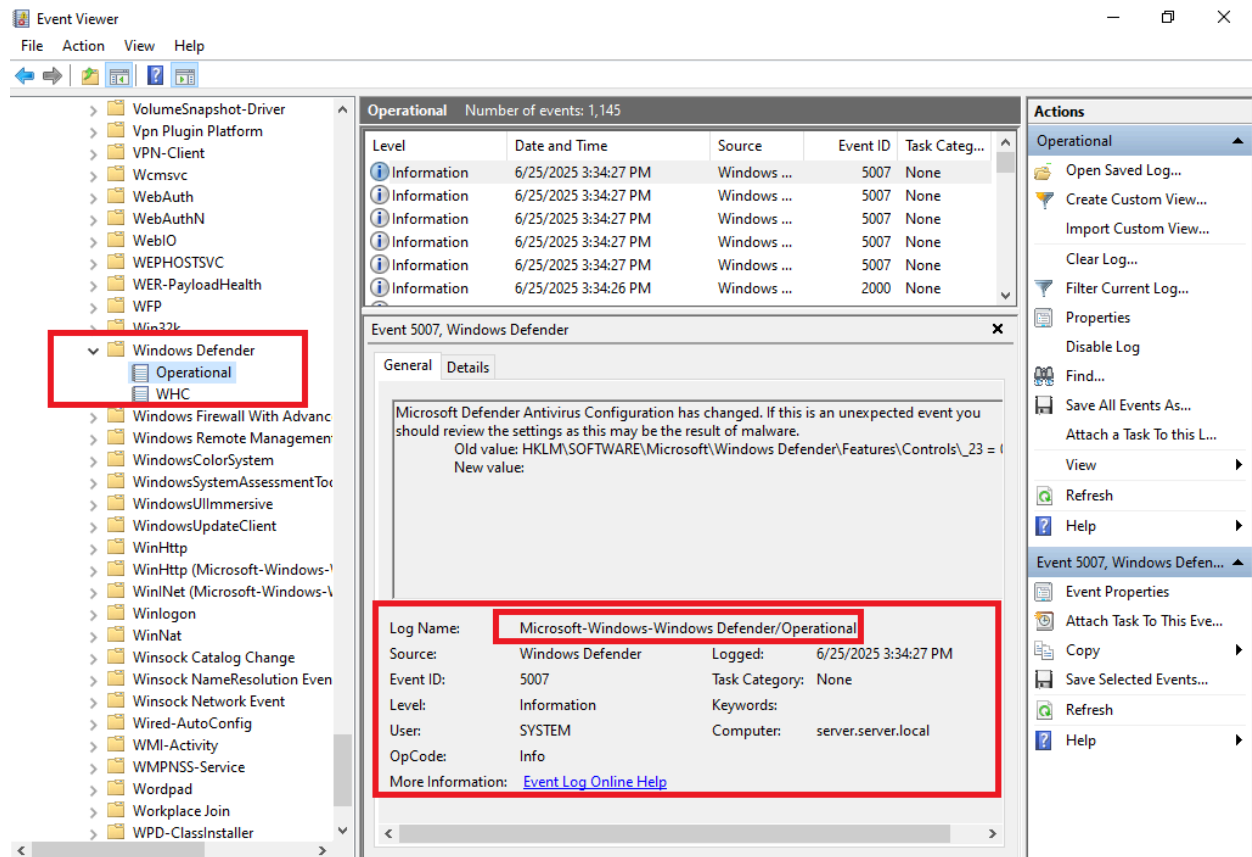


Scroll down little and click on "Windows Defender" > "Operational".

Here, you can view "Error" logs and other detailed events related to Windows Defender, including malware detections, scan results, and real-time protection activities.

Here is the configuration and the path of "Windows Defender" logs. Copy it and follow the same shown in figure.

Right-click Operational, and select Enable Log (if not already enabled).



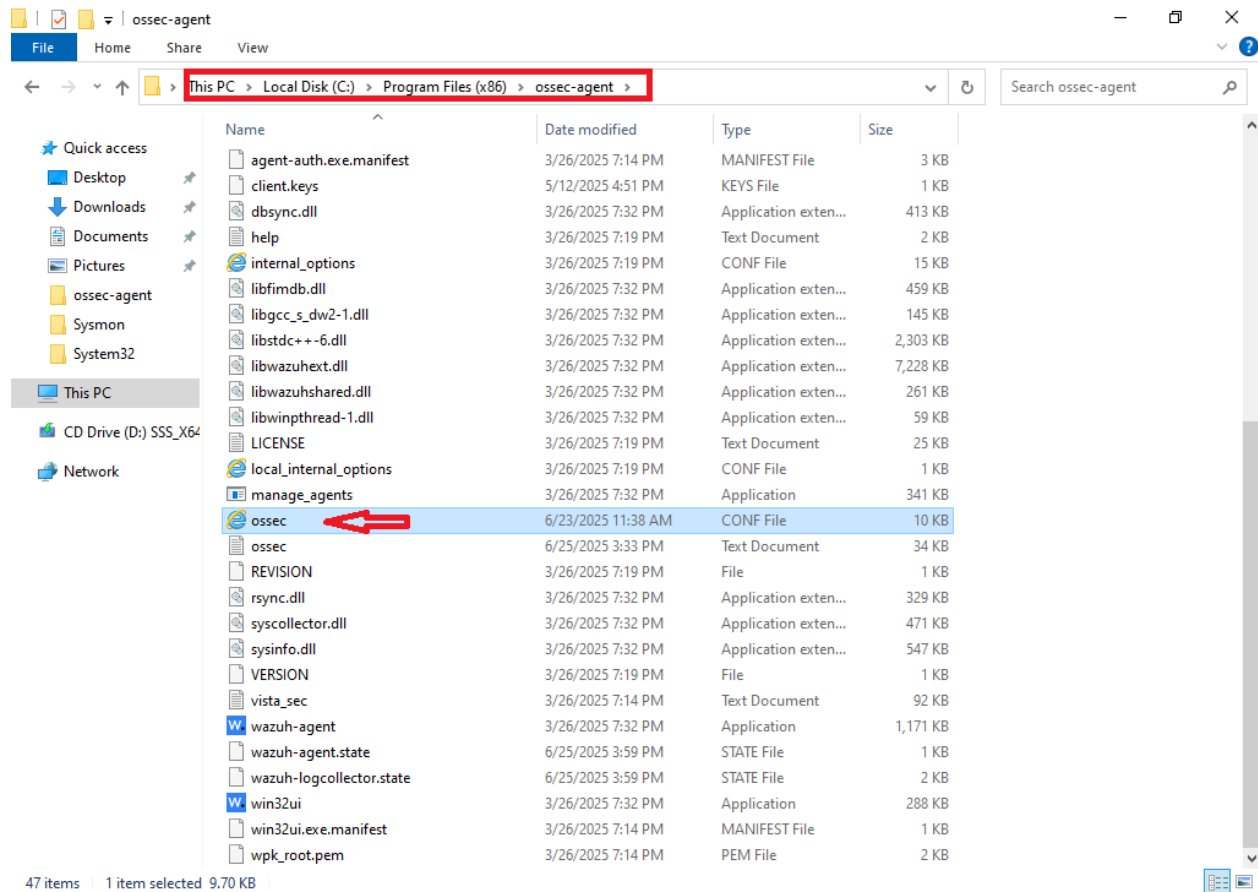
Configure Wazuh Agent to Collect Windows Defender Logs

To ensure that the Wazuh agent running on your Windows machine can read and forward Windows Defender logs to the Wazuh server, follow the steps below:

Navigate to the Wazuh agent installation directory:

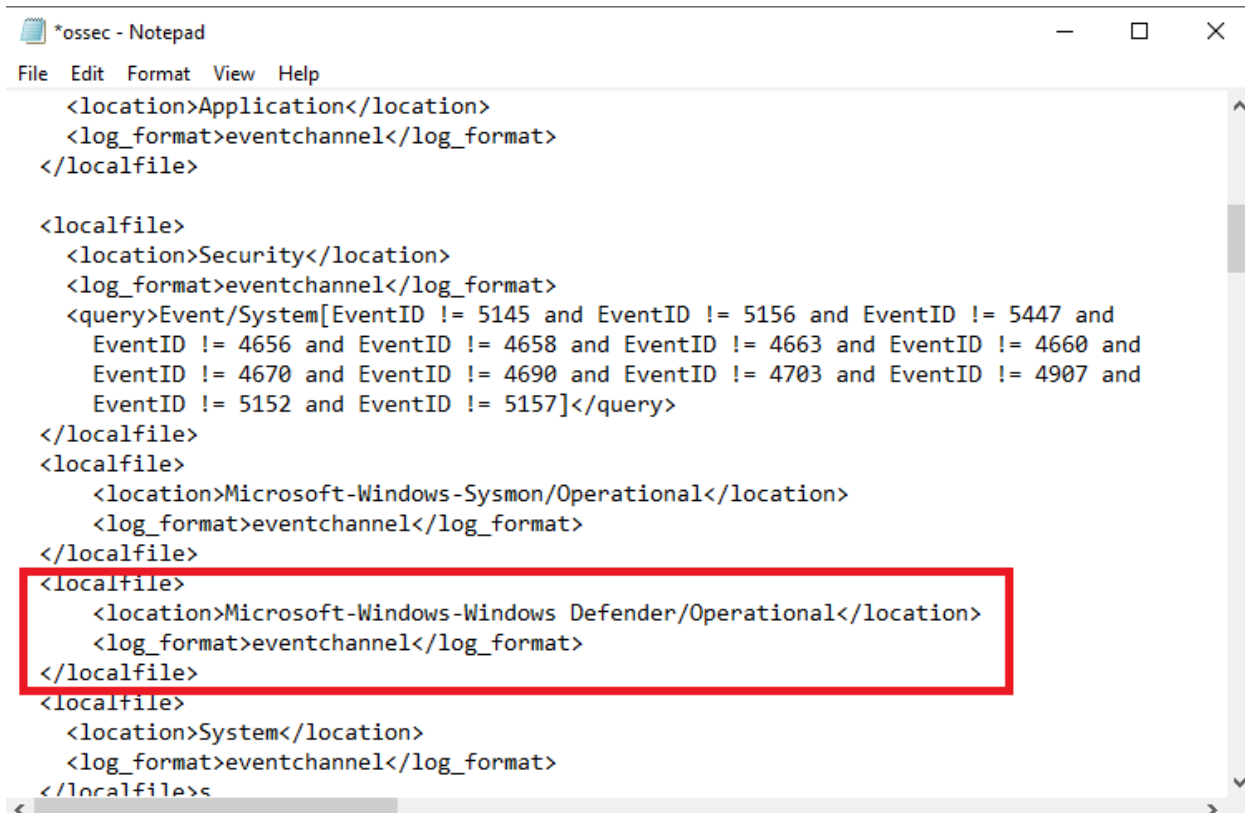
C:\Program Files (x86)\ossec-agent

Locate the file named `ossec.conf` and open it in a text editor with administrator privileges.



Inside the <localfile> section of the configuration file, add the following lines to enable log collection from Windows Defender's Operational log channel:

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

```
*ossec - Notepad
File Edit Format View Help

<location>Application</location>
<log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
  <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
    EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
    EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
    EventID != 5152 and EventID != 5157]</query>
</localfile>
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>
```

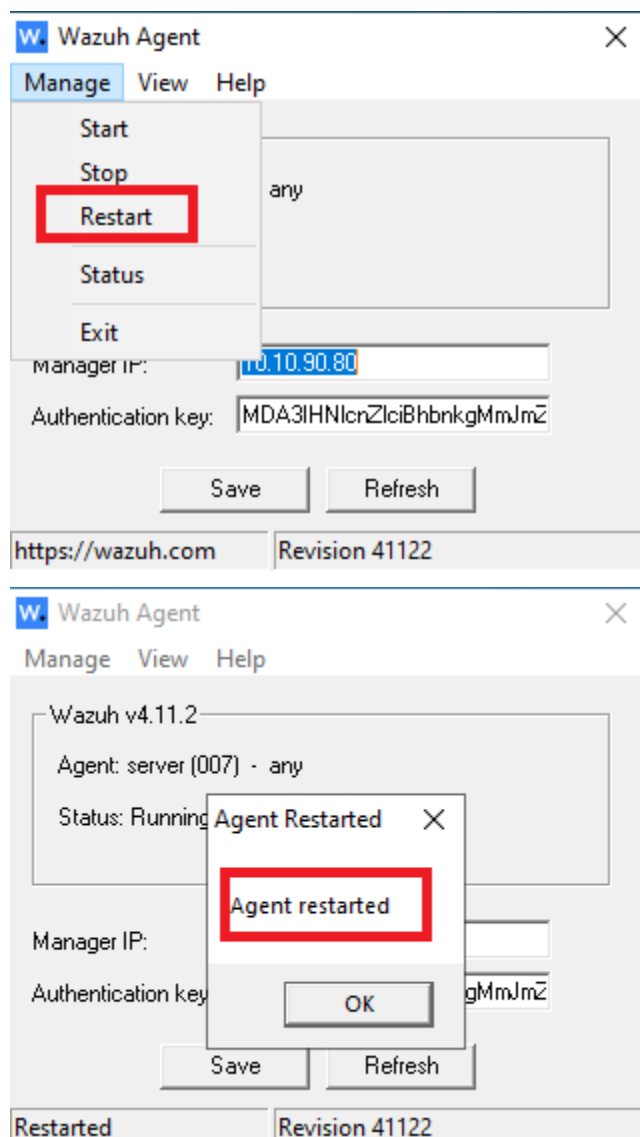
Now save the configuration and restart the agent services.

Run the following command on window powershell with administrator rights to restart the Wazuh agent service:

```
Restart-Service -Name wazuh
```

And there is also another way to restart the agent service :

First, search for "Wazuh Agent" in the Start menu, then click to open it



After restarted the wazuh-agent we have to download some malicious files form internet.

Testing Phase:

Simulate Threat Detection Using the EICAR Test File

To verify that your Wazuh agent is successfully collecting and forwarding Windows Defender logs, you can safely simulate a malware detection event using the EICAR test file. This file is specially designed for testing antivirus systems—it is harmless, but recognized by antivirus software as if it were malware.

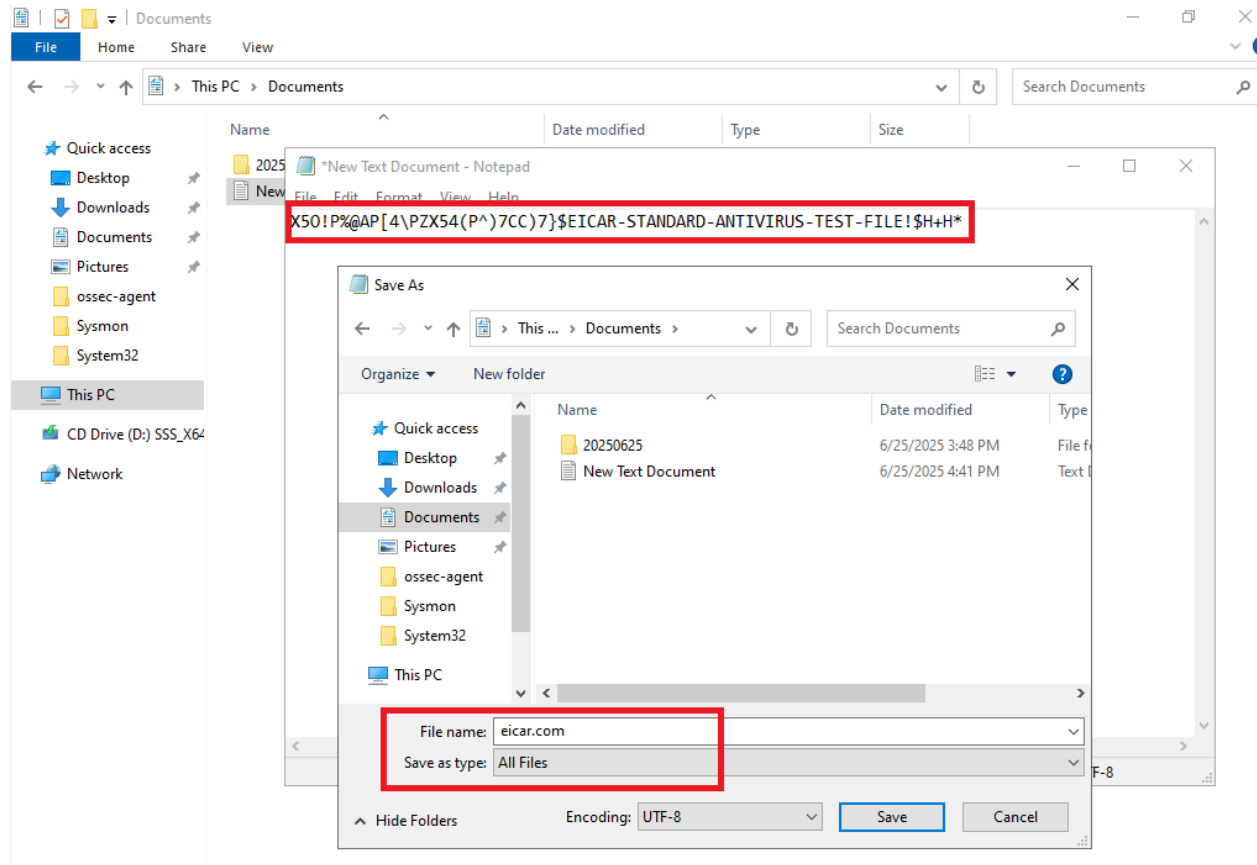
Open Notepad on your Windows machine.

Paste the following line exactly as it is (this is the EICAR test string):

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

Save the file with the name eicar.com.

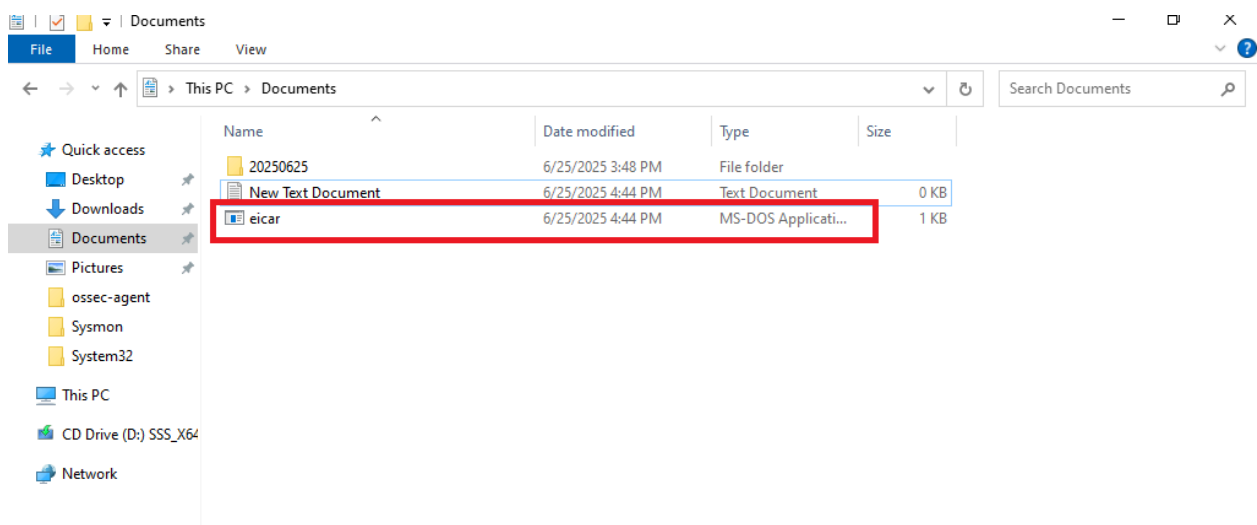
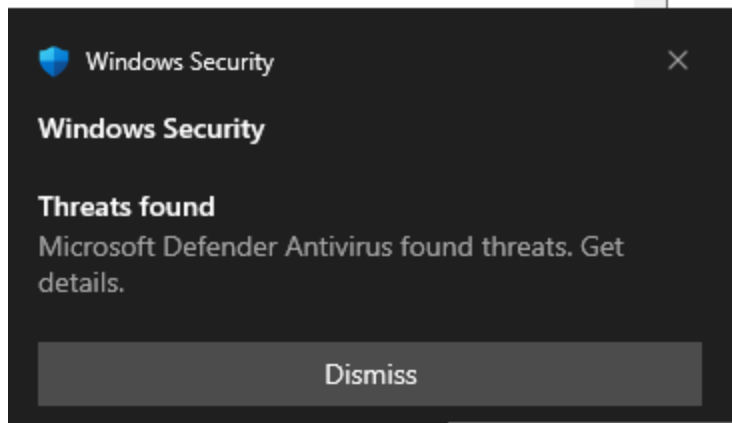
You may need to select "All Files" in the "Save as type" dropdown while saving in Notepad.



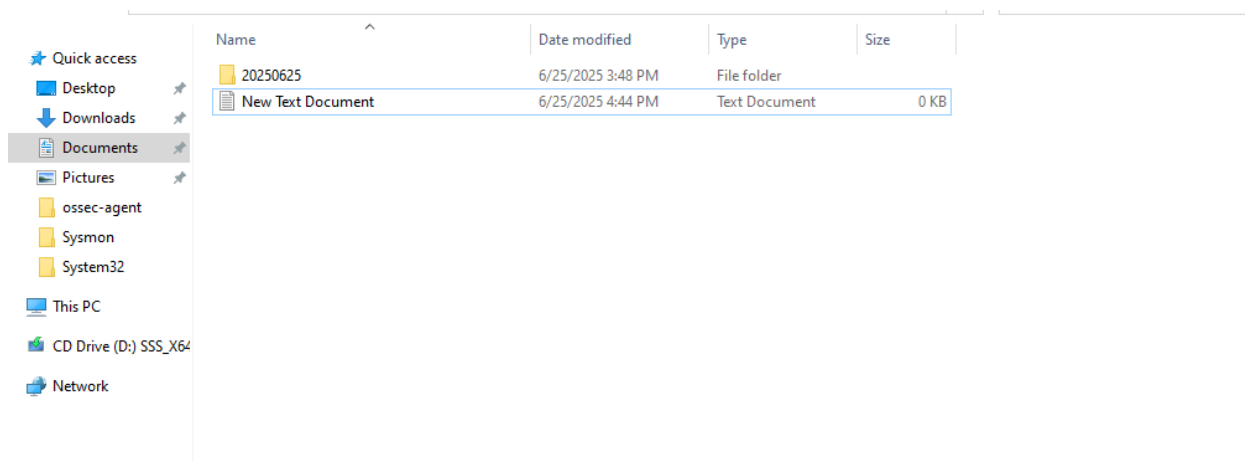
Windows Defender Reaction:

As soon as you save the file, Windows Defender should immediately detect and remove it.

You may receive a notification saying something like:
"Threat detected and removed – EICAR Test File".



After few seconds the file automatically removed from systems.



And now you see their logs in wazuh server Dashboard.

Here you can see windows defender antivirus or real-time protection blocked or remove malware file. And generate logs and send the logs details to Wazuh Server.

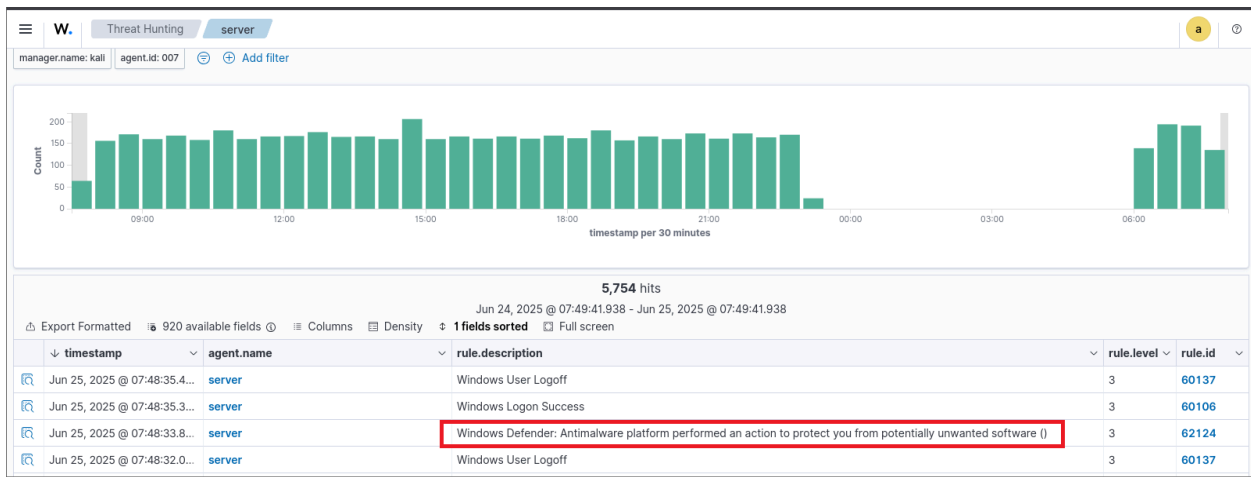


Table JSON

@timestamp	Jun 25, 2025 @ 07:48:33.837
_index	wazuh-alerts-4.x-2025.06.25
agent.id	007
agent.ip	10.0.2.15
agent.name	server
data.win.eventdata.action ID	2
data.win.eventdata.action Name	Quarantine
data.win.eventdata.additional Actions ID	0
data.win.eventdata.additional Actions String	No additional actions required
data.win.eventdata.category ID	42
data.win.eventdata.category Name	Virus
data.win.eventdata.detection ID	{46E9301F-3A75-412D-8F8E-B03AF5C828C7}
data.win.eventdata.detection Time	2025-06-25T11:50:44.044Z
data.win.eventdata.detection User	SERVER08\Administrator
data.win.eventdata.engine Version	AM: 1.1.25050.6, NIS: 1.1.25050.6

data.win.eventdata.error Description	The operation completed successfully.
data.win.eventdata.execution ID	1
data.win.eventdata.execution Name	Suspended
data.win.eventdata.fwLink	https://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003&enterprise=0
data.win.eventdata.origin ID	1
data.win.eventdata.origin Name	Local machine
data.win.eventdata.path	file:_C:\Users\administrator\Documents\leicar.com
data.win.eventdata.post Clean Status	0
data.win.eventdata.pre Execution Status	0
data.win.eventdata.process Name	C:\Windows\System32\notepad.exe
data.win.eventdata.product Name	Microsoft Defender Antivirus
data.win.eventdata.product Version	4.18.25050.5
data.win.eventdata.remediation User	NT AUTHORITY\SYSTEM
data.win.eventdata.security intelligence Version	AV: 1.431.211.0, AS: 1.431.211.0, NIS: 1.431.211.0
data.win.eventdata.severity ID	5
data.win.eventdata.severity Name	Severe
data.win.eventdata.source ID	3

data.win.eventdata.threat Name	Virus:DOS/EICAR_Test_File
data.win.eventdata.type ID	0
data.win.eventdata.type Name	Concrete
data.win.system.channel	Microsoft-Windows-Windows Defender/Operational
data.win.system.computer	server.server.local
data.win.system.eventID	1117
data.win.system.eventRecordID	1160
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	<p>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 Potentially Unwanted Software</p>
data.win.system.opcode	0
data.win.system.processID	3424
data.win.system.providerGuid	{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
data.win.system.providerName	Microsoft-Windows-Windows Defender

input.type	log
location	EventChannel
manager.name	kali
rule.description	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ()
# rule.firedtimes	5
rule.gdpr	IV_35.7.d
rule.gpg13	4.2
rule.groups	windows, windows_defender
rule.hipaa	164.312.b
rule.id	62124
# rule.level	3
rule.mail	false
rule.nist_800_53	SI.3, AU.6, SI.4
rule.pci_dss	5.1, 5.2, 10.6.1, 11.4
rule.tsc	A1.2, CC7.2, CC7.3, CC6.1, CC6.8
timestamp	Jun 25, 2025 @ 07:48:33.837

Summary

This lab successfully demonstrates the integration of Windows Defender, the built-in antivirus solution for Windows, with the Wazuh SIEM platform to achieve centralized security monitoring and enhanced threat visibility.

The process began with preparing the lab environment, where the Wazuh server was already deployed on Kali Linux, and the Wazuh agent was installed on a Windows machine running Windows Defender. Logging was enabled from Windows Defender's Operational event log, which contains critical security data such as scan activities, threat detections, real-time protection events, and remediation actions.

The Wazuh agent was configured by modifying the `ossec.conf` file to include the Defender log source using the eventchannel format. After restarting the agent service, communication between the Windows agent and the Wazuh manager was verified using both the command line and the Wazuh Dashboard.

To validate the integration, a safe test threat (EICAR test file) was created and saved on the Windows system. As expected, Windows Defender immediately detected and quarantined the file, and the corresponding log entry appeared in the Wazuh Dashboard under the agent's alert section. This confirmed that Wazuh was successfully receiving and parsing Defender logs in real-time.

Key Outcomes:

- Successfully enabled Windows Defender Operational logs
- Configured Wazuh agent to collect and forward logs to the server
- Validated threat detection using an industry-standard test method (EICAR)
- Verified log visibility and alert generation in the Wazuh Dashboard
- Achieved centralized monitoring, making endpoint security data visible in one place

This integration enhances endpoint visibility, enables real-time alerting, and helps security teams detect, analyze, and respond to threats more efficiently. It also demonstrates the practical application of combining antivirus protection with a SIEM solution like Wazuh for improved security monitoring in enterprise or lab environments.

