Window Defender 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.

Why Integrate Windows Defender with Wazuh?

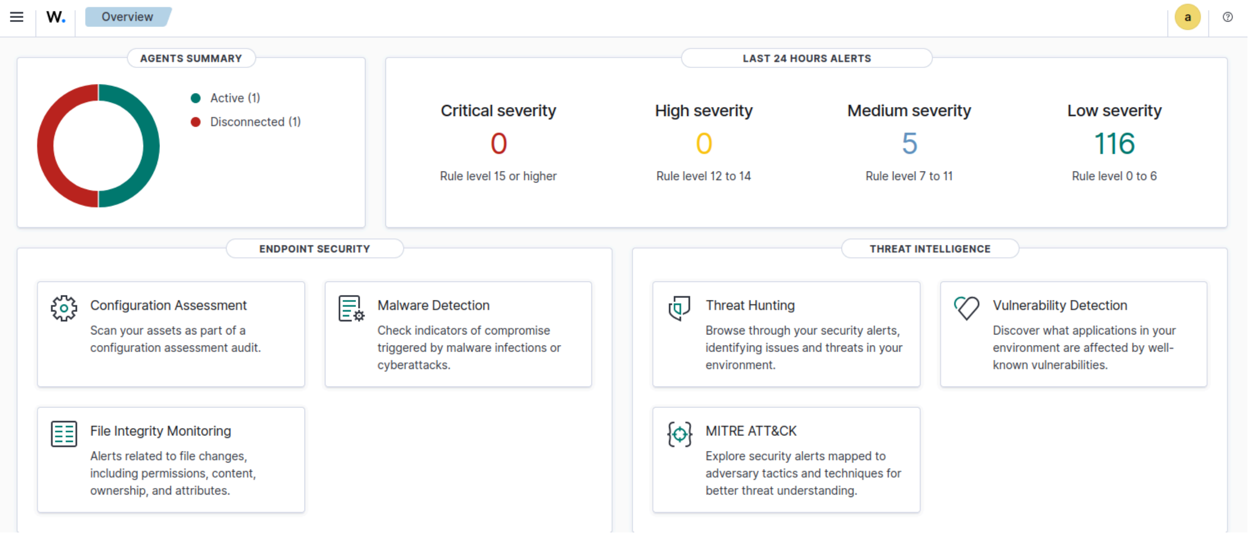
Wazuh is an open-source security monitoring platform that collects logs from various systems and generates security alerts. It helps organizations detect threats, monitor system activities, and take quick action in case of security incidents.

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.

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

Here is Wazuh Server Dashboard,



AGENTS SUMMARY

- Active (1)
- Disconnected (1)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	5	116
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

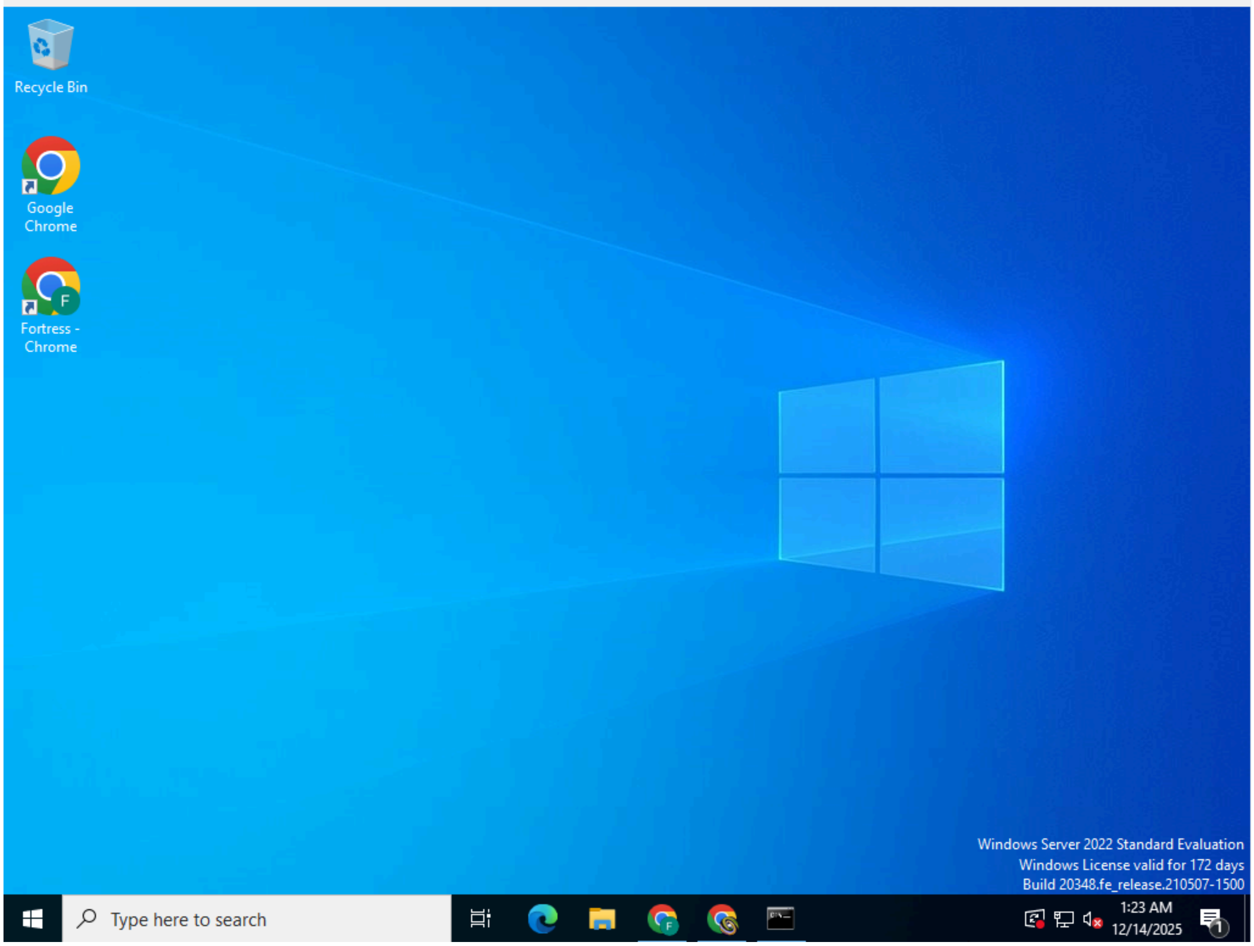
THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

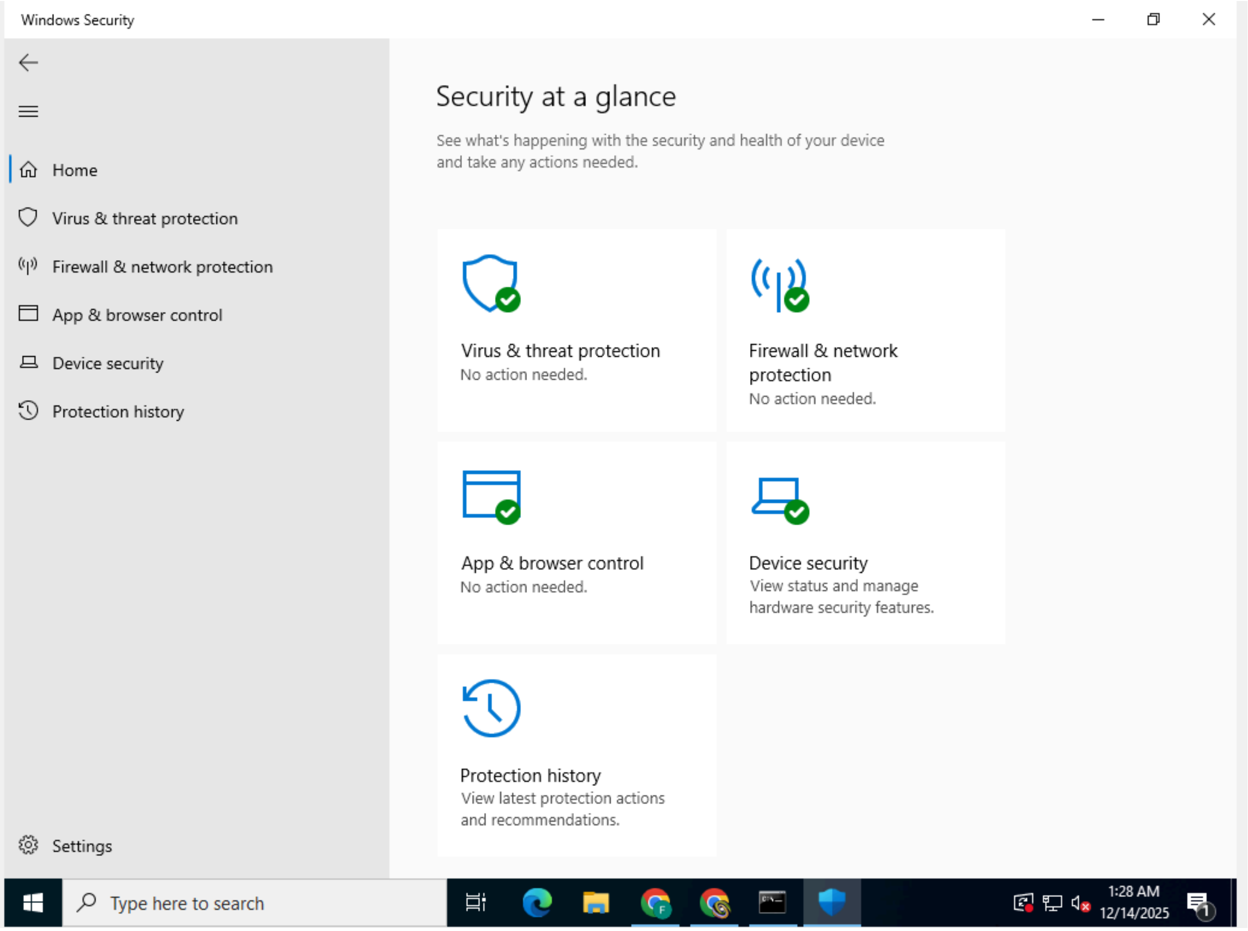
Here is our Window Server 2022 is running in Oracle Virtual Box where our agent is installed.



Windows Server 2022 Standard Evaluation
Windows License valid for 172 days
Build 20348.fe_release.210507-1500

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.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

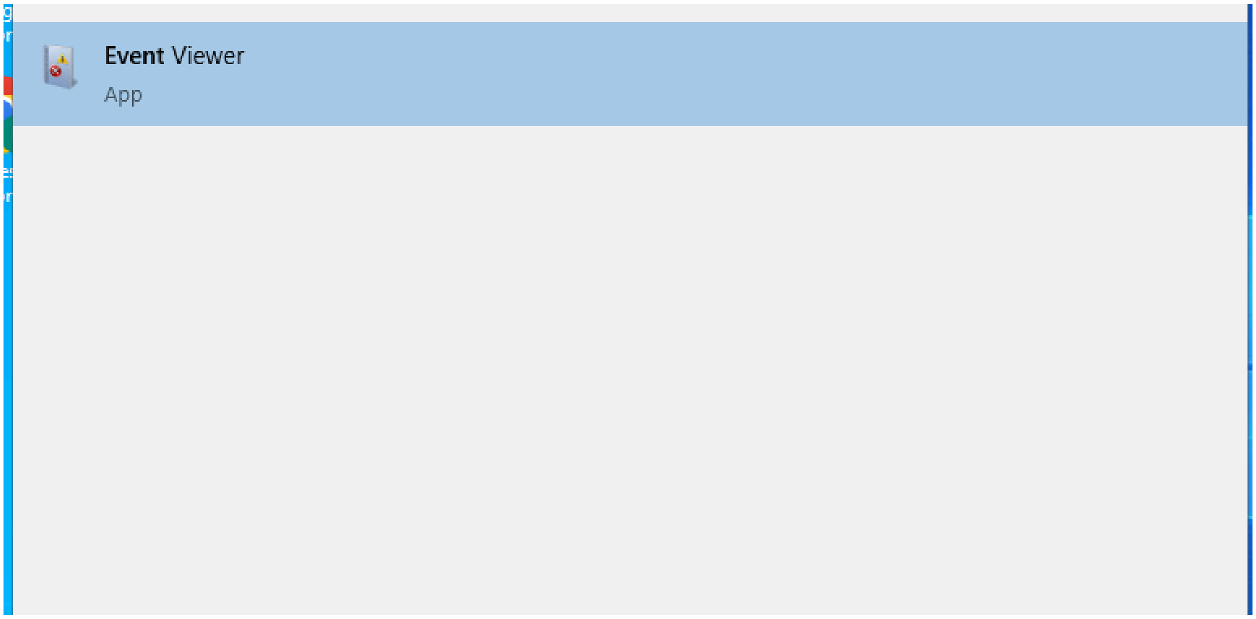
Firewall & network protection
No action needed.

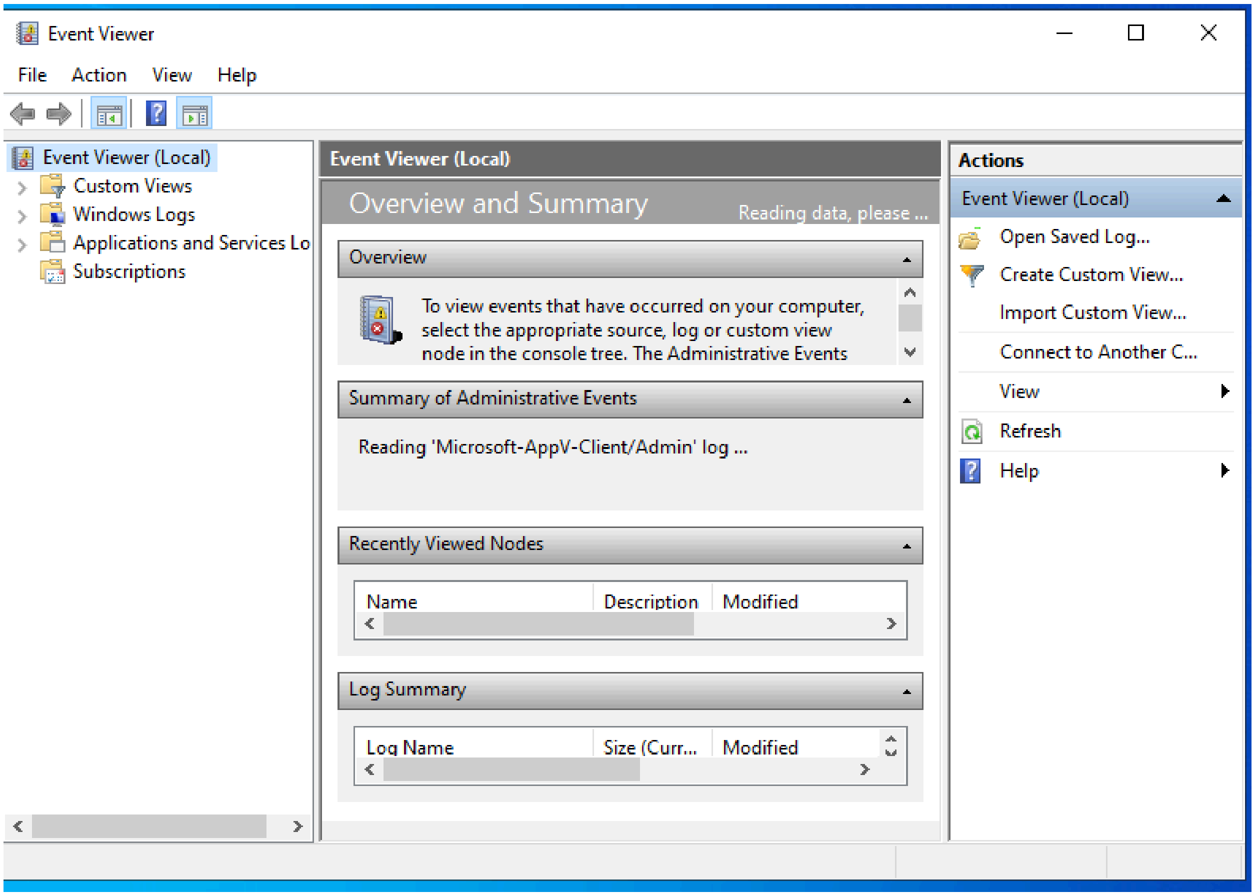
App & browser control
No action needed.

Device security
View status and manage hardware security features.

Protection history
View latest protection actions and recommendations.

Now I go to "Event Viewer" and open it.

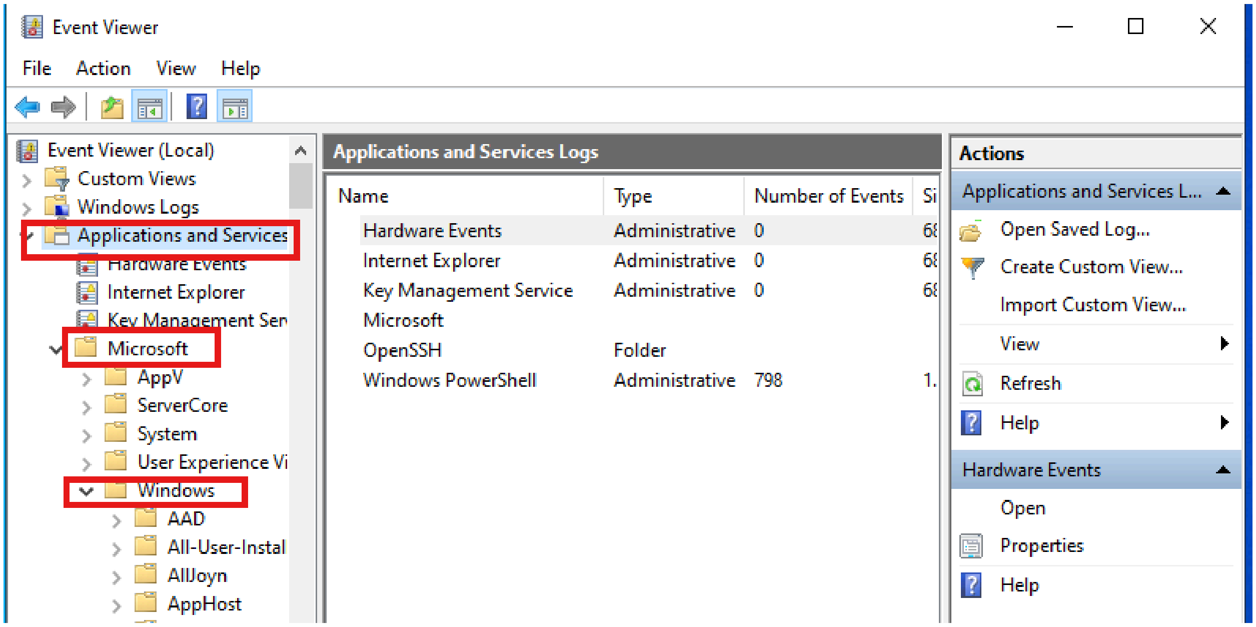




To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events

Reading 'Microsoft-AppV-Client/Admin' log ...

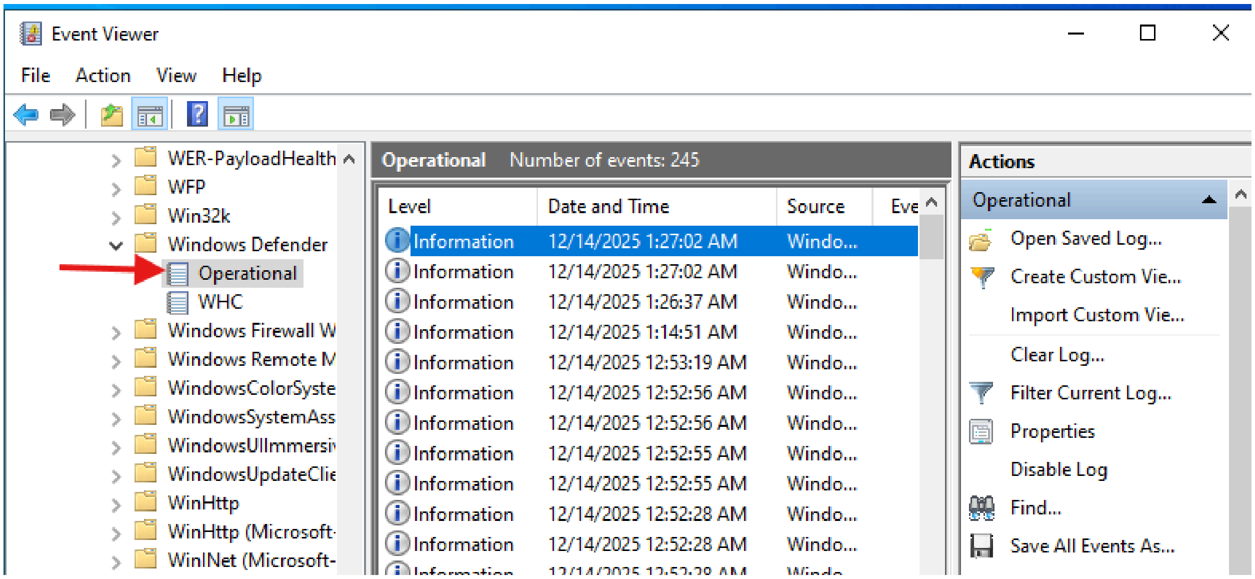
Now go to "Application and Services Logs" > "Microsoft" > "Windows".



Name	Type	Number of Events	Si
Hardware Events	Administrative	0	6٤
Internet Explorer	Administrative	0	6٤
Key Management Service	Administrative	0	6٤
Microsoft			
OpenSSH	Folder		
Windows PowerShell	Administrative	798	1.

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

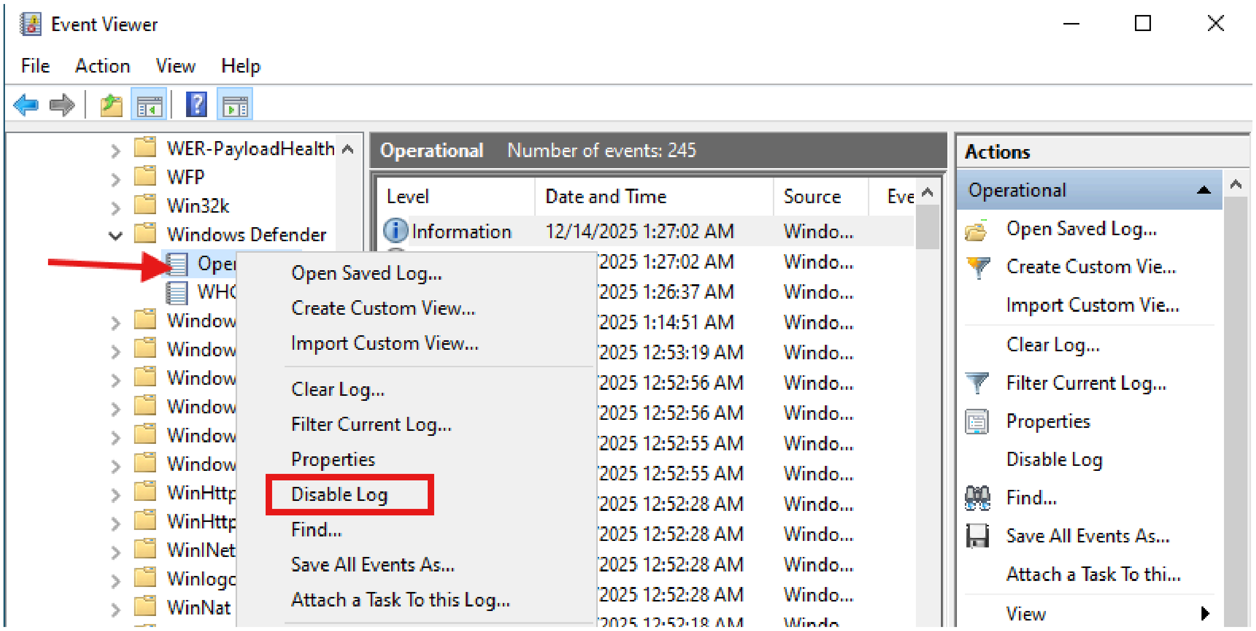
Here, you can view "Error" logs and other detailed events related to Windows Defender, including malware detections, scan results, and real-time protection activities.



Operational Number of events: 245

Level	Date and Time	Source	Eve
Information	12/14/2025 1:27:02 AM	Windo...	
Information	12/14/2025 1:27:02 AM	Windo...	
Information	12/14/2025 1:26:37 AM	Windo...	
Information	12/14/2025 1:14:51 AM	Windo...	
Information	12/14/2025 12:53:19 AM	Windo...	
Information	12/14/2025 12:52:56 AM	Windo...	
Information	12/14/2025 12:52:56 AM	Windo...	
Information	12/14/2025 12:52:55 AM	Windo...	
Information	12/14/2025 12:52:55 AM	Windo...	
Information	12/14/2025 12:52:28 AM	Windo...	
Information	12/14/2025 12:52:28 AM	Windo...	
Information	12/14/2025 12:52:28 AM	Windo...	

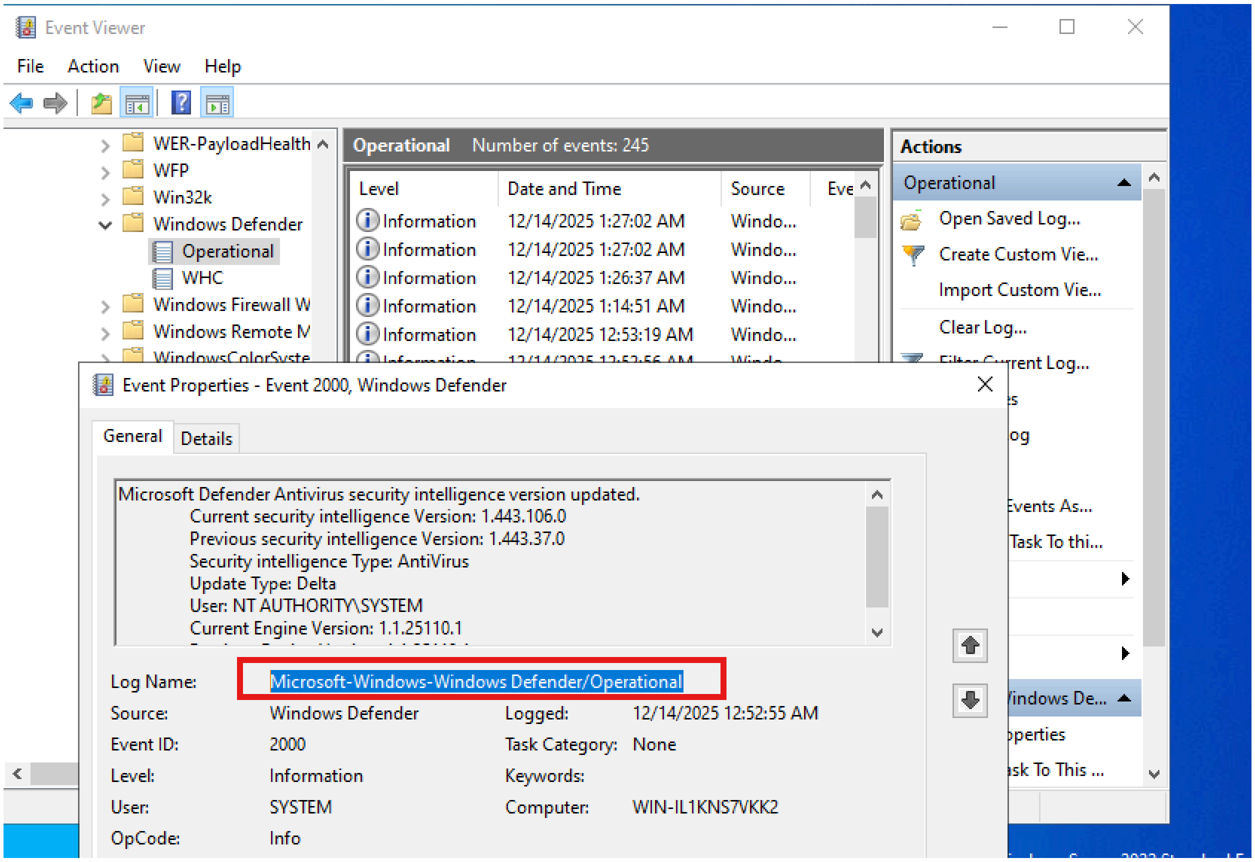
Right-click Operational, and select Enable Log (if not already enabled).



Operational Number of events: 245

Level	Date and Time	Source	Eve
Information	12/14/2025 1:27:02 AM	Windo...	
	2025 1:27:02 AM	Windo...	
	2025 1:26:37 AM	Windo...	
	2025 1:14:51 AM	Windo...	
	2025 12:53:19 AM	Windo...	
	2025 12:52:56 AM	Windo...	
	2025 12:52:56 AM	Windo...	
	2025 12:52:55 AM	Windo...	
	2025 12:52:55 AM	Windo...	
	2025 12:52:28 AM	Windo...	
	2025 12:52:28 AM	Windo...	
	2025 12:52:28 AM	Windo...	
	2025 12:52:28 AM	Windo...	

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



Level	Date and Time	Source	Eve
Information	12/14/2025 1:27:02 AM	Windo...	
Information	12/14/2025 1:27:02 AM	Windo...	
Information	12/14/2025 1:26:37 AM	Windo...	
Information	12/14/2025 1:14:51 AM	Windo...	
Information	12/14/2025 12:53:19 AM	Windo...	

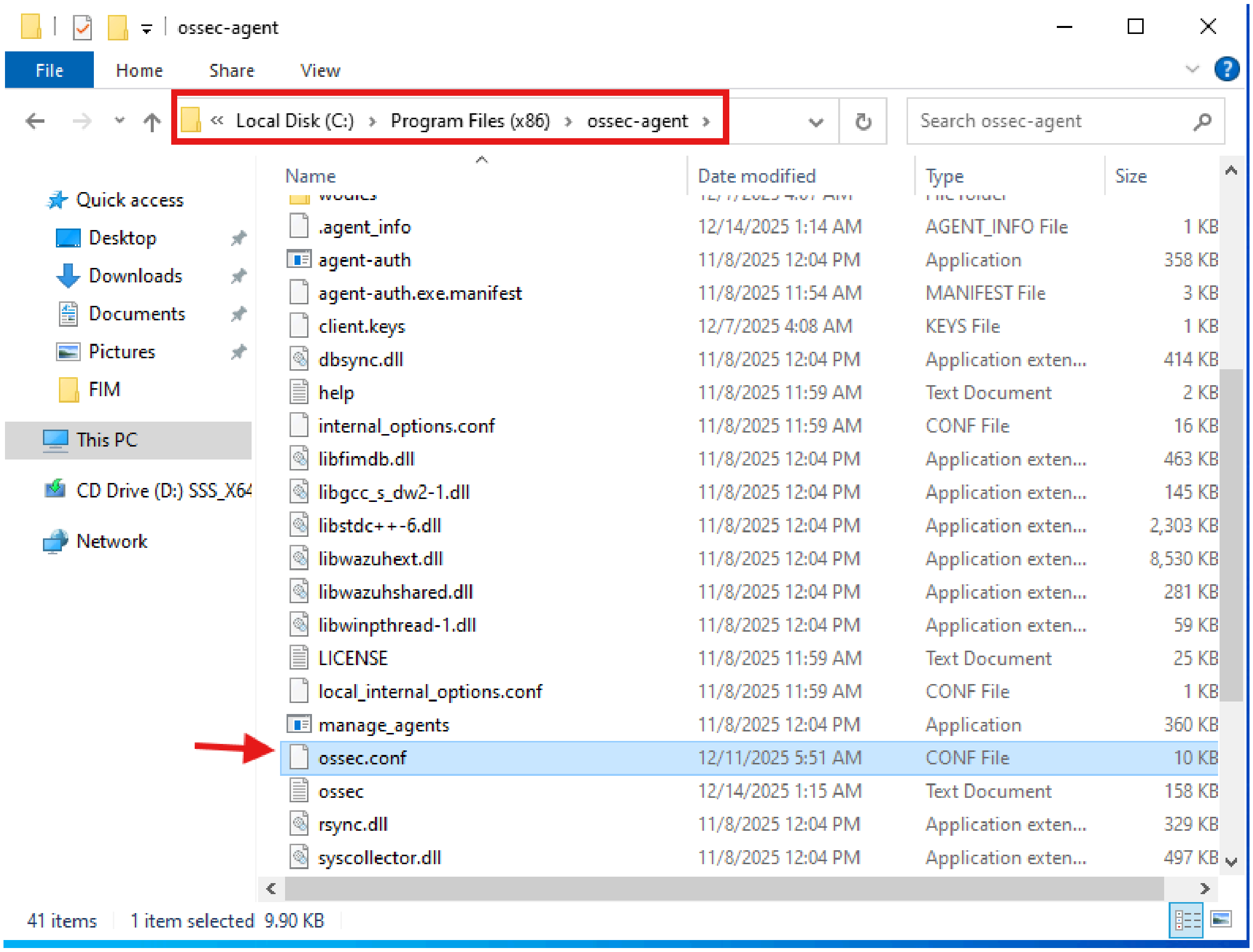
```
Microsoft Defender Antivirus security intelligence version updated.
        Current security intelligence Version: 1.443.106.0
        Previous security intelligence Version: 1.443.37.0
        Security intelligence Type: AntiVirus
        Update Type: Delta
        User: NT AUTHORITY\SYSTEM
        Current Engine Version: 1.1.25110.1
```

Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	12/14/2025 12:52:55 AM
Event ID:	2000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WIN-IL1KNS7VKK2
OpCode:	Info		

To ensure that the Wazuh agent running on our 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

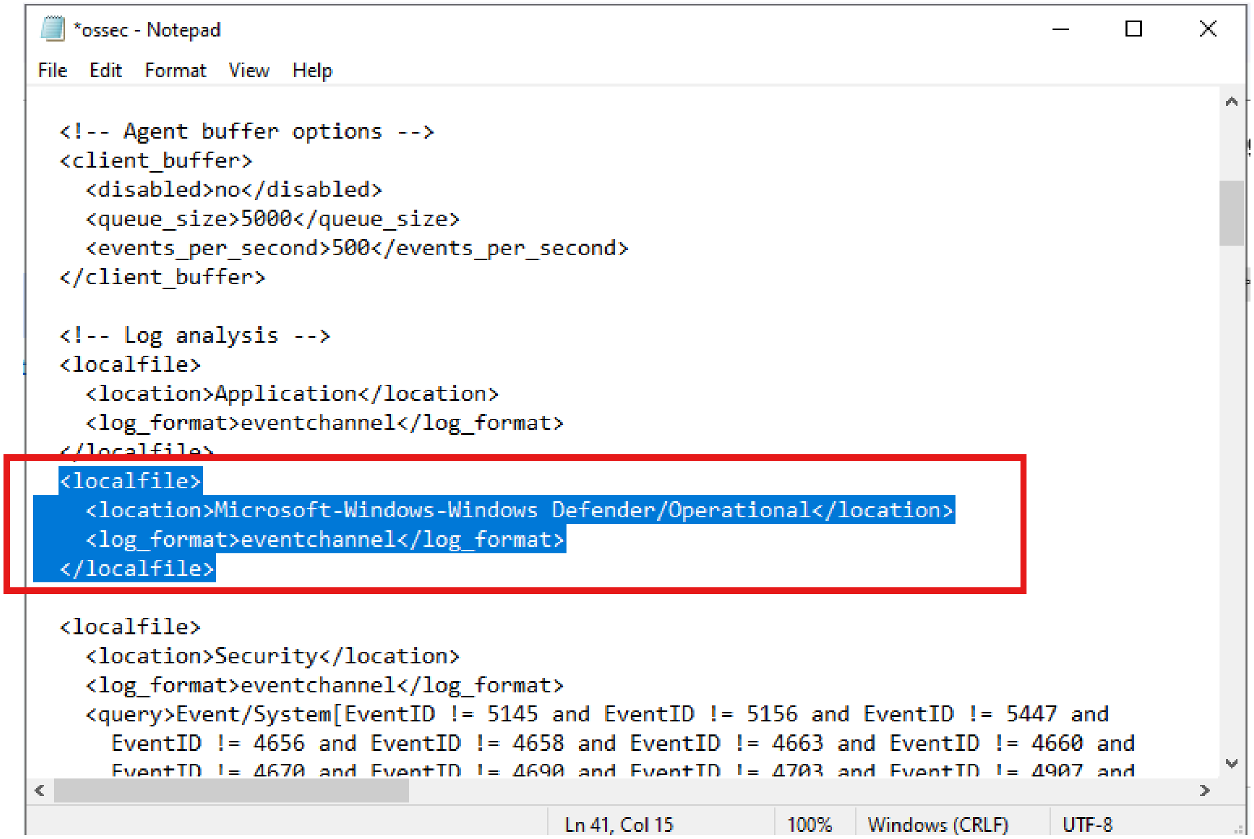
Locate the file named `ossec.conf` and open it in a text editor with administrator privileges.



Name	Date modified	Type	Size
.agent_info	12/14/2025 1:14 AM	AGENT_INFO File	1 KB
agent-auth	11/8/2025 12:04 PM	Application	358 KB
agent-auth.exe.manifest	11/8/2025 11:54 AM	MANIFEST File	3 KB
client.keys	12/7/2025 4:08 AM	KEYS File	1 KB
dbsync.dll	11/8/2025 12:04 PM	Application exten...	414 KB
help	11/8/2025 11:59 AM	Text Document	2 KB
internal_options.conf	11/8/2025 11:59 AM	CONF File	16 KB
libfimdb.dll	11/8/2025 12:04 PM	Application exten...	463 KB
libgcc_s_dw2-1.dll	11/8/2025 12:04 PM	Application exten...	145 KB
libstdc++-6.dll	11/8/2025 12:04 PM	Application exten...	2,303 KB
libwazuhext.dll	11/8/2025 12:04 PM	Application exten...	8,530 KB
libwazuhshared.dll	11/8/2025 12:04 PM	Application exten...	281 KB
libwinpthread-1.dll	11/8/2025 12:04 PM	Application exten...	59 KB
LICENSE	11/8/2025 11:59 AM	Text Document	25 KB
local_internal_options.conf	11/8/2025 11:59 AM	CONF File	1 KB
manage_agents	11/8/2025 12:04 PM	Application	360 KB
ossec.conf	12/11/2025 5:51 AM	CONF File	10 KB
ossec	12/14/2025 1:15 AM	Text Document	158 KB
rsync.dll	11/8/2025 12:04 PM	Application exten...	329 KB
syscollector.dll	11/8/2025 12:04 PM	Application exten...	497 KB

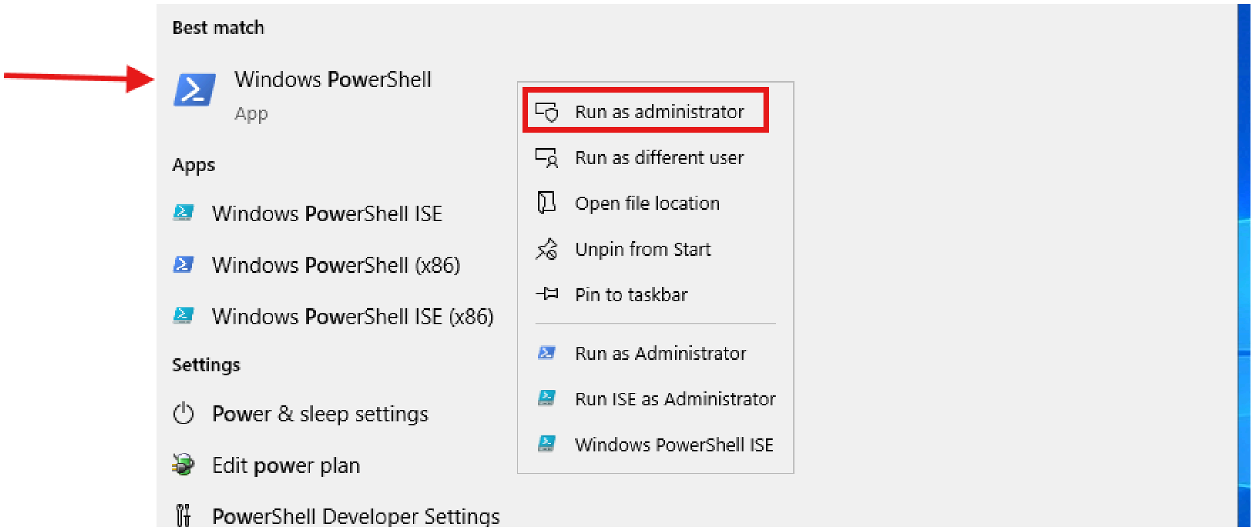
Inside the `<localfile>` section of the configuration file, add the following lines to enable log collection from Windows Defender's Operational log channel:

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

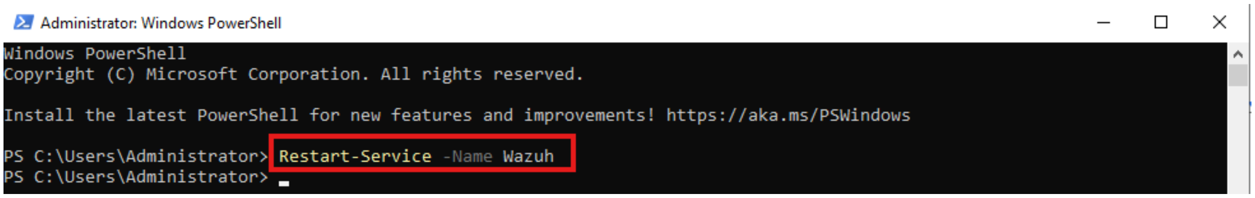


```
<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

<!-- Log analysis -->
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>Microsoft-Windows-Windows Defender/Operational</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
```

Now saved the configuration and restart the agent services.
Run the following command on Windows Powershell with administrator rights to restart the Wazuh agent service:



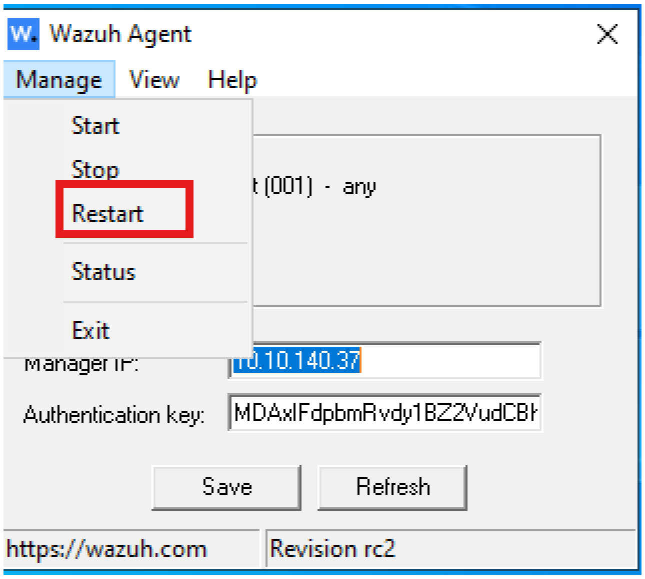
Restart-Service -Name WazuhRestart-Service -Name Wazuh



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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Restart-Service -Name Wazuh
PS C:\Users\Administrator> _
```

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

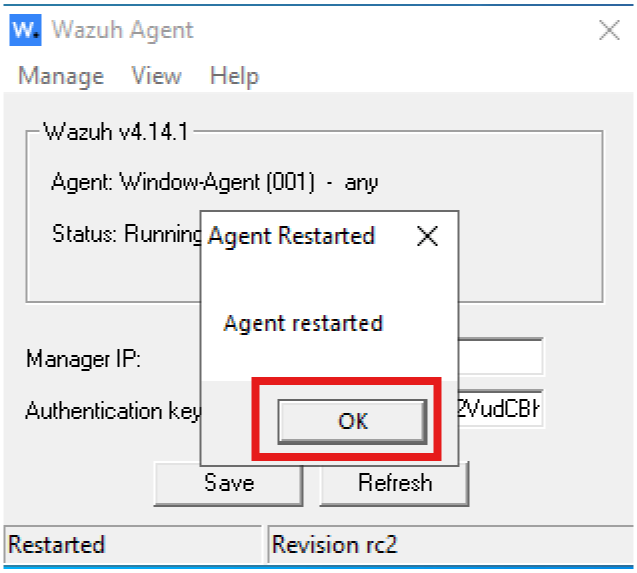


t (001) - any

Manager IP: 10.10.140.37

Authentication key: MDAxIFdpbmRvdy1BZ2VudCBI

https://wazuh.com | Revision rc2



Wazuh v4.14.1

Agent: Window-Agent (001) - any

Status: Running

Agent Restarted

Agent restarted

Manager IP:

Authentication key: 2VudCBI

Restarted | Revision rc2

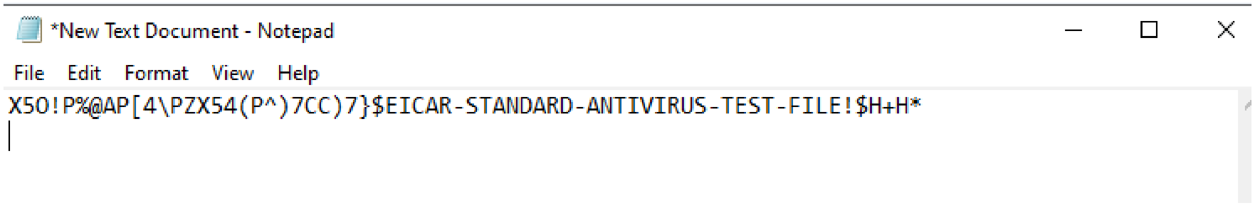
After restarting the wazuh-agent we need to perform some testing to verify the configuration work correctly.

Testing Phase:

To verify that our Wazuh agent is successfully collecting and forwarding Windows Defender logs, we can safely simulate a malware detection event using the EICAR test file. This file is specially designed for testing antivirus systems.

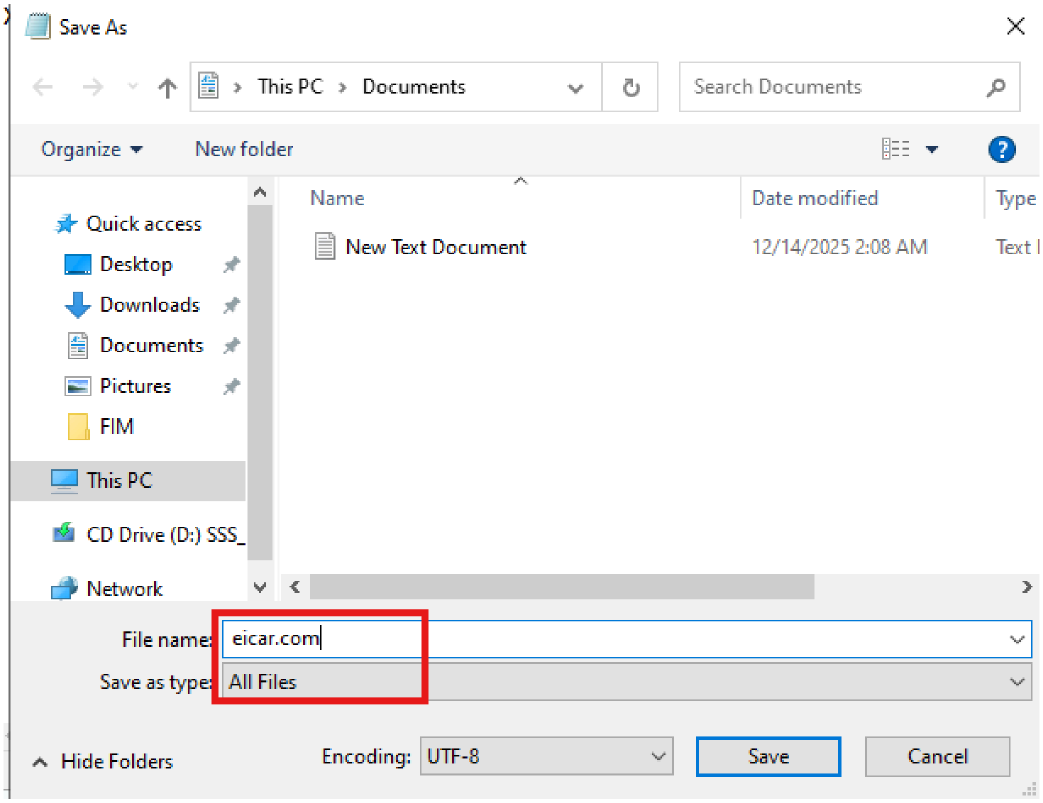
Open Notepad on our Windows machine and Paste the following line exactly as it is (this is the EICAR test string):

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



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

Save the file with the name eicar.com.
We may need to select "All Files" in the "Save as type" dropdown while saving in Notepad.



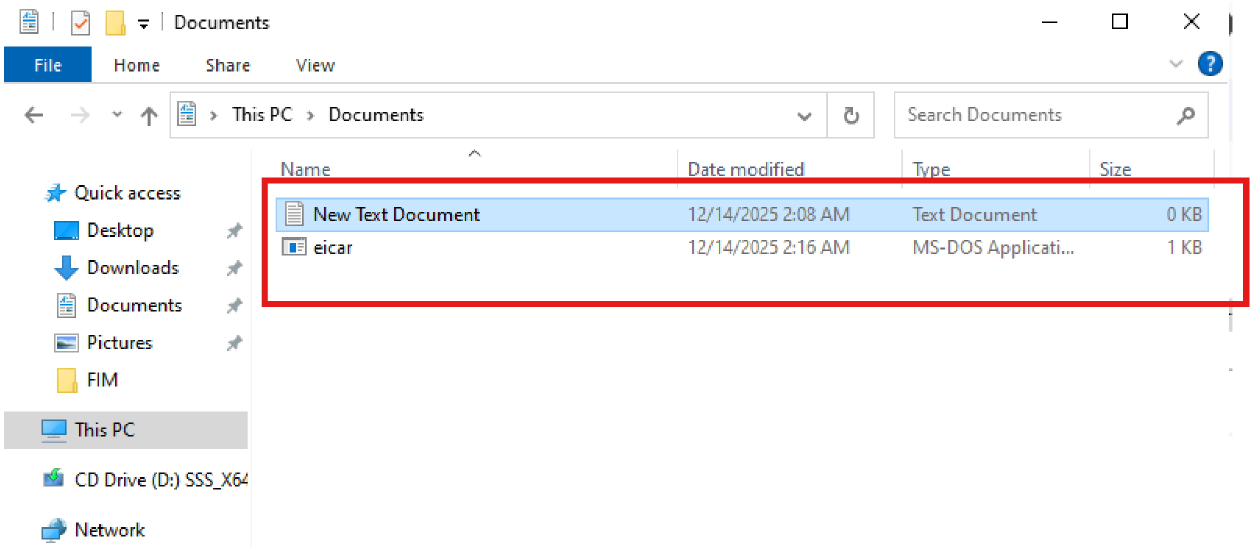
Name	Date modified	Type
New Text Document	12/14/2025 2:08 AM	Text I

File name: eicar.com

Save as type: All Files

Encoding: UTF-8

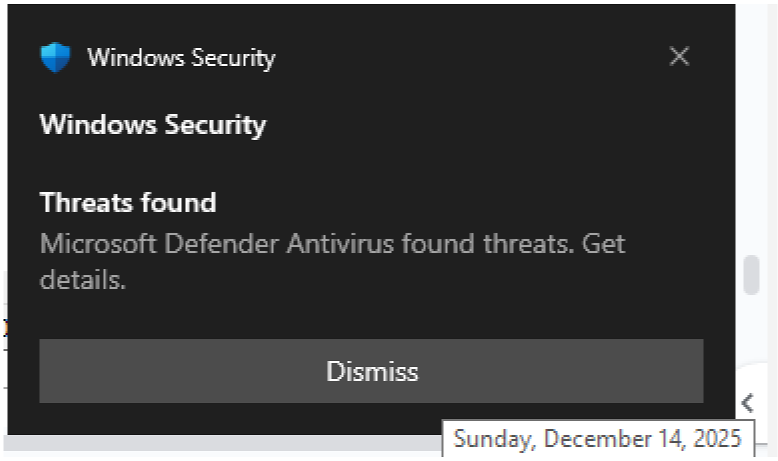
Saved file:



Name	Date modified	Type	Size
New Text Document	12/14/2025 2:08 AM	Text Document	0 KB
eicar	12/14/2025 2:16 AM	MS-DOS Applicati...	1 KB

Windows Defender Reaction:

As soon as we saved the file, Windows Defender should immediately detect and remove it.
We may receive a notification saying something like:

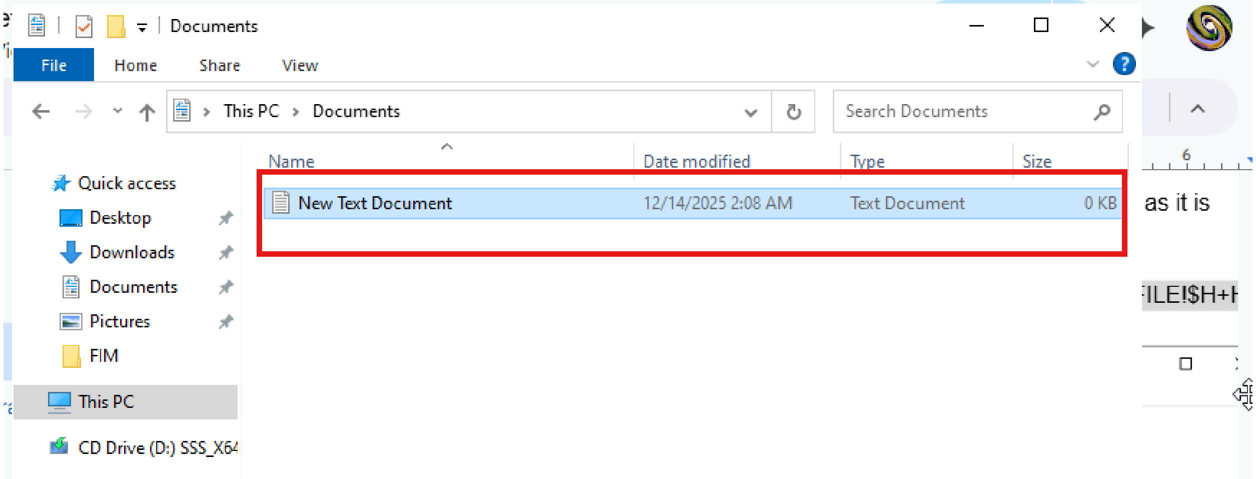


Windows Security

Windows Security

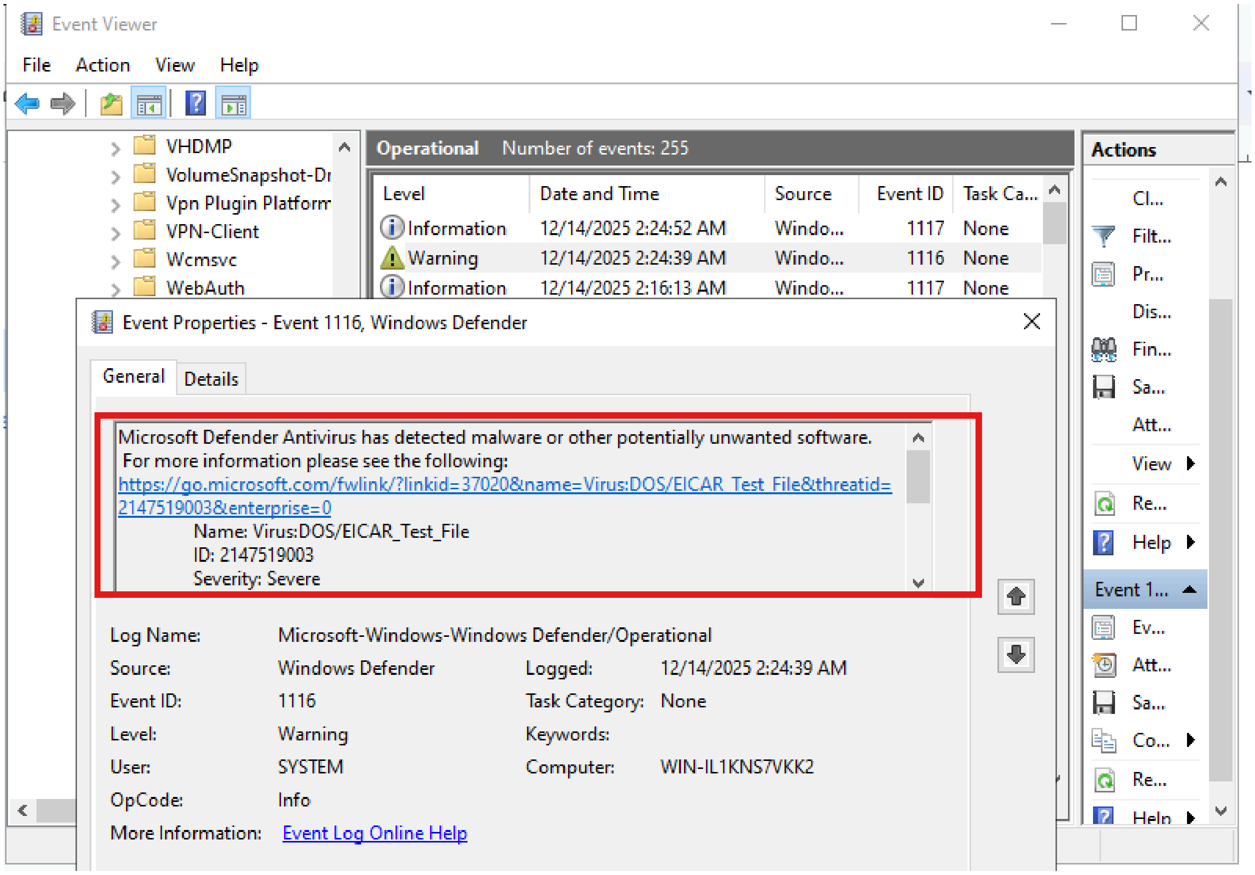
Threats found
Microsoft Defender Antivirus found threats. Get details.

Now the file is automatically removed and no file exist.



Name	Date modified	Type	Size
New Text Document	12/14/2025 2:08 AM	Text Document	0 KB

The place where logs are stored and agents collect them and forward towards manager.



Operational Number of events: 255

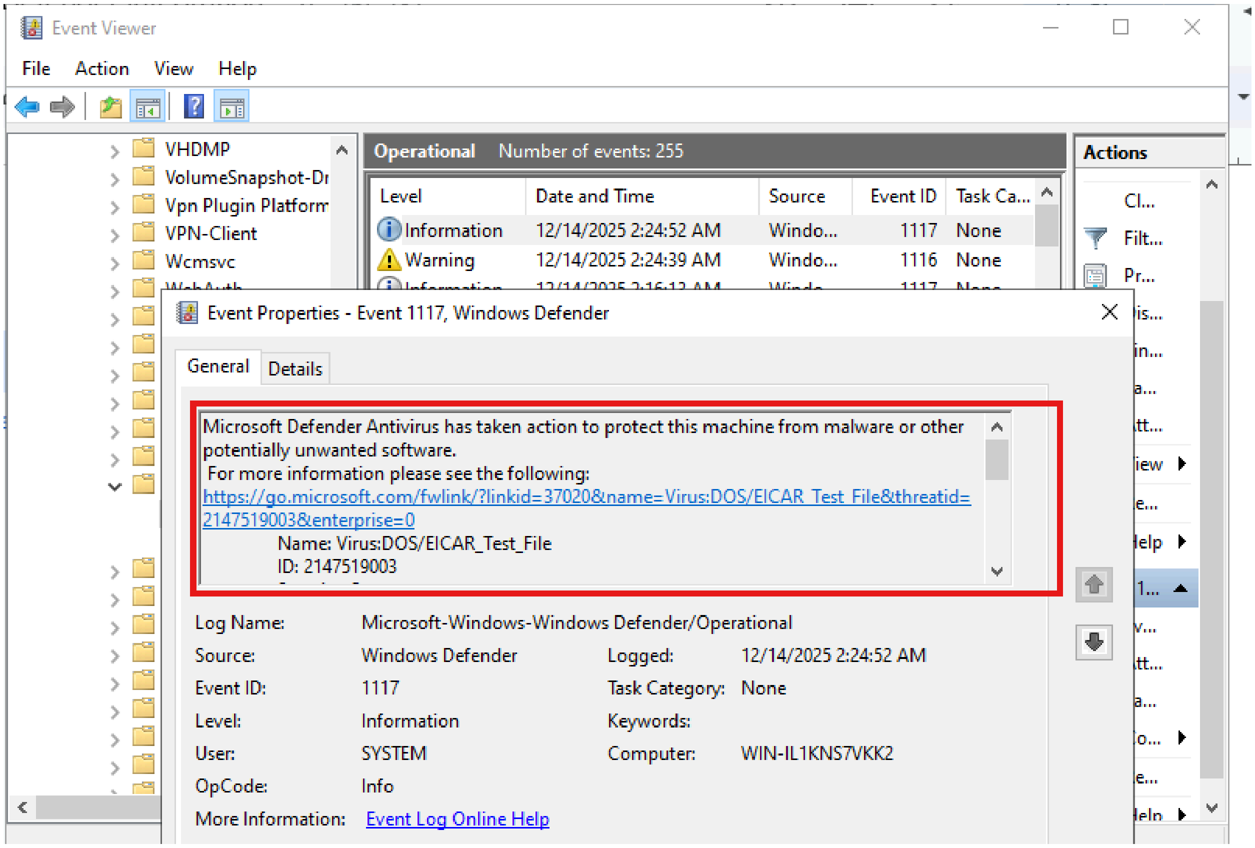
Level	Date and Time	Source	Event ID	Task Ca...
Information	12/14/2025 2:24:52 AM	Windo...	1117	None
Warning	12/14/2025 2:24:39 AM	Windo...	1116	None
Information	12/14/2025 2:16:13 AM	Windo...	1117	None

Event Properties - Event 1116, Windows Defender

```
Microsoft Defender Antivirus has detected 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
```

Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	12/14/2025 2:24:39 AM
Event ID:	1116	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	WIN-IL1KNS7VKK2
OpCode:	Info		
More Information:	Event Log Online Help		

And its removal logs



Operational Number of events: 255

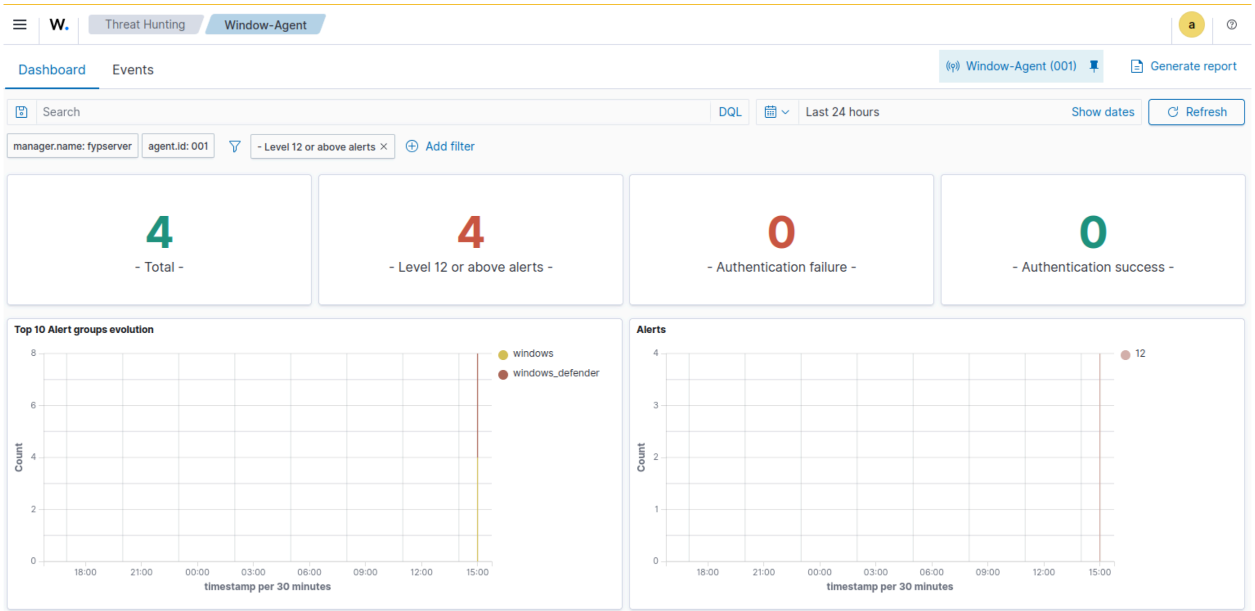
Level	Date and Time	Source	Event ID	Task Ca...
Information	12/14/2025 2:24:52 AM	Windo...	1117	None
Warning	12/14/2025 2:24:39 AM	Windo...	1116	None

Event Properties - 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

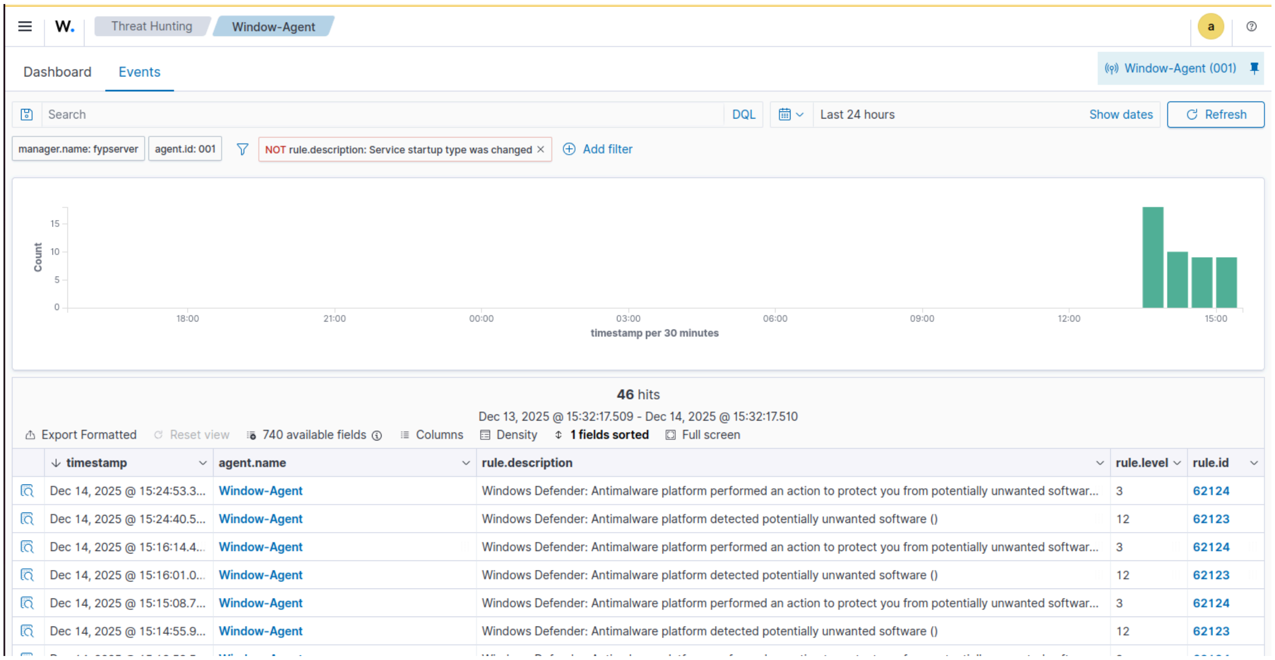
Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	12/14/2025 2:24:52 AM
Event ID:	1117	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WIN-IL1KNS7VKK2
OpCode:	Info		
More Information:	Event Log Online Help		

Now Agents collect these logs and send them to a manager.
And, now we see the alerts in Wazuh Dashboard in the “Threat Hunting” section in Dashboard and Events section.



Last 24 hours
manager.name: fypserver
agent.id: 001
- Level 12 or above alerts

4	4	0	0
- Total -	- Level 12 or above alerts -	- Authentication failure -	- Authentication success -

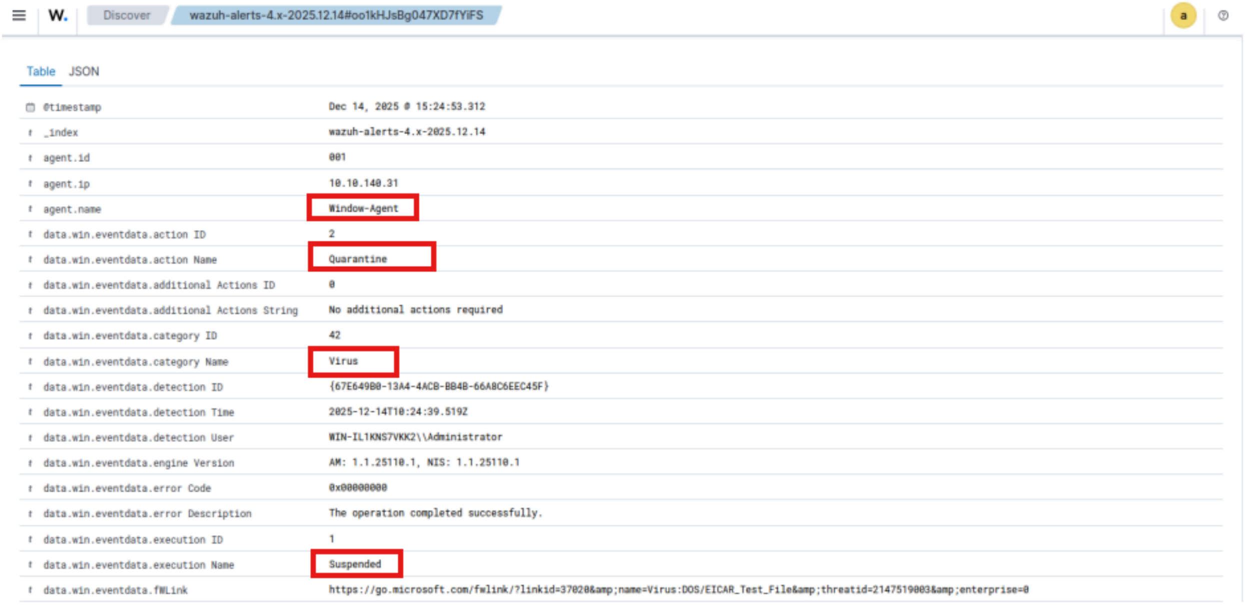


46 hits

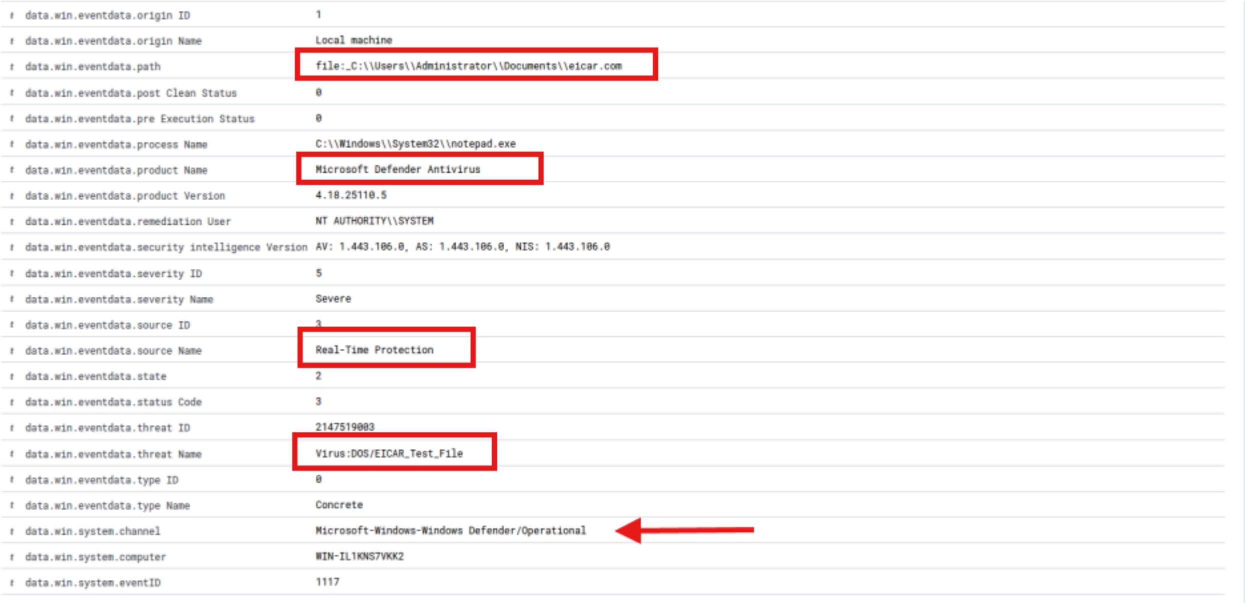
Dec 13, 2025 @ 15:32:17.509 - Dec 14, 2025 @ 15:32:17.510

timestamp	agent.name	rule.description	rule.level	rule.id
Dec 14, 2025 @ 15:24:53.3...	Window-Agent	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted softwar...	3	62124
Dec 14, 2025 @ 15:24:40.5...	Window-Agent	Windows Defender: Antimalware platform detected potentially unwanted software ()	12	62123
Dec 14, 2025 @ 15:16:14.4...	Window-Agent	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted softwar...	3	62124
Dec 14, 2025 @ 15:16:01.0...	Window-Agent	Windows Defender: Antimalware platform detected potentially unwanted software ()	12	62123
Dec 14, 2025 @ 15:15:08.7...	Window-Agent	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted softwar...	3	62124
Dec 14, 2025 @ 15:14:55.9...	Window-Agent	Windows Defender: Antimalware platform detected potentially unwanted software ()	12	62123

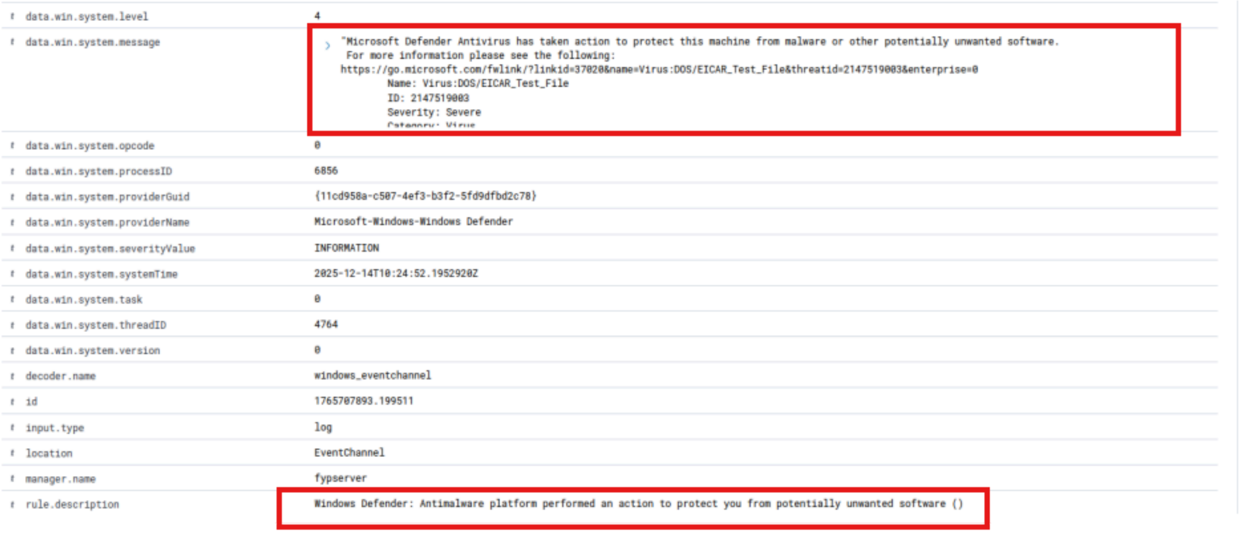
Now click on any alerts to see the details of alerts.



@timestamp	Dec 14, 2025 @ 15:24:53.312
_index	wazuh-alerts-4.x-2025.12.14
agent.id	001
agent.ip	10.10.140.31
agent.name	Window-Agent
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	{67E649B0-13A4-4ACB-BB4B-66A8C6EEC45F}
data.win.eventdata.detection Time	2025-12-14T10:24:39.519Z
data.win.eventdata.detection User	WIN-IL1KNS7VKK2\\Administrator
data.win.eventdata.engine Version	AM: 1.1.25110.1, NIS: 1.1.25110.1
data.win.eventdata.error Code	0x00000000
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&amp;name=Virus:DOS/EICAR_Test_File&amp;threatid=2147519003&amp;enterprise=0



data.win.eventdata.origin ID	1
data.win.eventdata.origin Name	Local machine
data.win.eventdata.path	file:_C:\\Users\\Administrator\\Documents\\eicar.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	4.18.25110.5
data.win.eventdata.remediation User	NT AUTHORITY\\SYSTEM
data.win.eventdata.security intelligence Version	AV: 1.443.106.0, AS: 1.443.106.0, NIS: 1.443.106.0
data.win.eventdata.severity ID	5
data.win.eventdata.severity Name	Severe
data.win.eventdata.source ID	3
data.win.eventdata.source Name	Real-Time Protection
data.win.eventdata.state	2
data.win.eventdata.status Code	3
data.win.eventdata.threat ID	2147519003
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	WIN-IL1KNS7VKK2
data.win.system.eventID	1117



data.win.system.level	4
data.win.system.message	"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
data.win.system.opcode	0
data.win.system.processID	6856
data.win.system.providerGuid	{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
data.win.system.providerName	Microsoft-Windows-Windows Defender
data.win.system.severityValue	INFORMATION
data.win.system.systemTime	2025-12-14T10:24:52.1952920Z
data.win.system.task	0
data.win.system.threadID	4764
data.win.system.version	0
decoder.name	windows_eventchannel
id	1765707893.199511
input.type	log
location	EventChannel
manager.name	fypserver
rule.description	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ()

Summary:

This task shows how Windows Defender works with the Wazuh SIEM system to monitor security events from one place.

In this task, the Wazuh Manager is installed on an Ubuntu server, and the Wazuh Agent is installed on a Windows Server 2022 that uses Windows Defender. Windows Defender logs were enabled so that security information such as virus detection, scanning activity, and protection actions could be collected.

The Wazuh agent was configured by modifying the ossec.conf file to include the Defender log source using the eventchannel format. After restarting the Wazuh Agent service, the connection between the Windows Server and the Wazuh Manager was checked using the command line and the Wazuh Dashboard.

To test the setup, a safe test virus file (EICAR file) was created on the Windows computer. Windows Defender quickly detected and removed the file. At the same time, this event was sent to the Wazuh Manager and appeared in the Wazuh Dashboard alerts section.

This task confirms that Wazuh can successfully receive and display Windows Defender security alerts in real time, helping in better security monitoring.