Integrating Windows Defender with Wazuh SIEM

Created by:Jean Chrysostome NDAYISABYE

Introduction

In today's rapidly evolving threat landscape, organizations require comprehensive visibility into endpoint security activities to maintain robust cybersecurity postures. While Windows Defender provides excellent built-in protection against malware, viruses, and other security threats, its defensive capabilities are significantly enhanced when integrated with centralized Security Information and Event Management (SIEM) solutions.

This comprehensive guide demonstrates the integration of Windows Defender with Wazuh, an open-source SIEM platform, enabling security teams to centrally monitor, analyze, and respond to endpoint security events. By forwarding Windows Defender logs to Wazuh, organizations can achieve unified security monitoring, correlate events across multiple endpoints, and implement automated incident response workflows.

Objectives

The primary objectives of this integration are:

Security Monitoring Enhancement

- Centralize Windows Defender security events from multiple endpoints
- Enable real-time monitoring of malware detection and remediation activities
- Provide comprehensive visibility into endpoint security posture

Incident Response Improvement

- Accelerate threat detection and response times
- Enable correlation of security events across the enterprise
- Facilitate forensic analysis and investigation workflows

Compliance and Reporting

- Generate compliance reports for security frameworks
- Maintain audit trails of security events and responses
- Support regulatory requirements for security monitoring

Operational Efficiency

- Reduce manual monitoring overhead
- Automate alert generation and notification processes
- Enable proactive threat hunting capabilities

Prerequisites

Before implementing this integration, ensure the following requirements are met:

Infrastructure Requirements

- **Wazuh Server**: Properly configured and operational Wazuh manager
- **Windows Endpoints**: Windows 10/11 machines with Windows Defender enabled
- **Network Connectivity**: Reliable network connection between endpoints and Wazuh server
- **Wazuh Agent**: Installed and configured on target Windows machines

Software Versions

- Wazuh Manager: Version 4.0 or later recommended
- Windows Defender: Current version with real-time protection enabled
- Wazuh Agent: Compatible version with Wazuh Manager

1. Enable Windows Defender logs on a Windows machine.

In today's threat landscape, having visibility into endpoint activity is a key requirement for maintaining a secure environment. **Windows Defender**, a built-in antivirus tool in Windows operating systems, provides real-time protection against malware, viruses, and other security threats. While Defender effectively handles local detection and response, its true potential is unlocked when integrated with a centralized security monitoring solution.

Step 1.1: Access Event Viewer

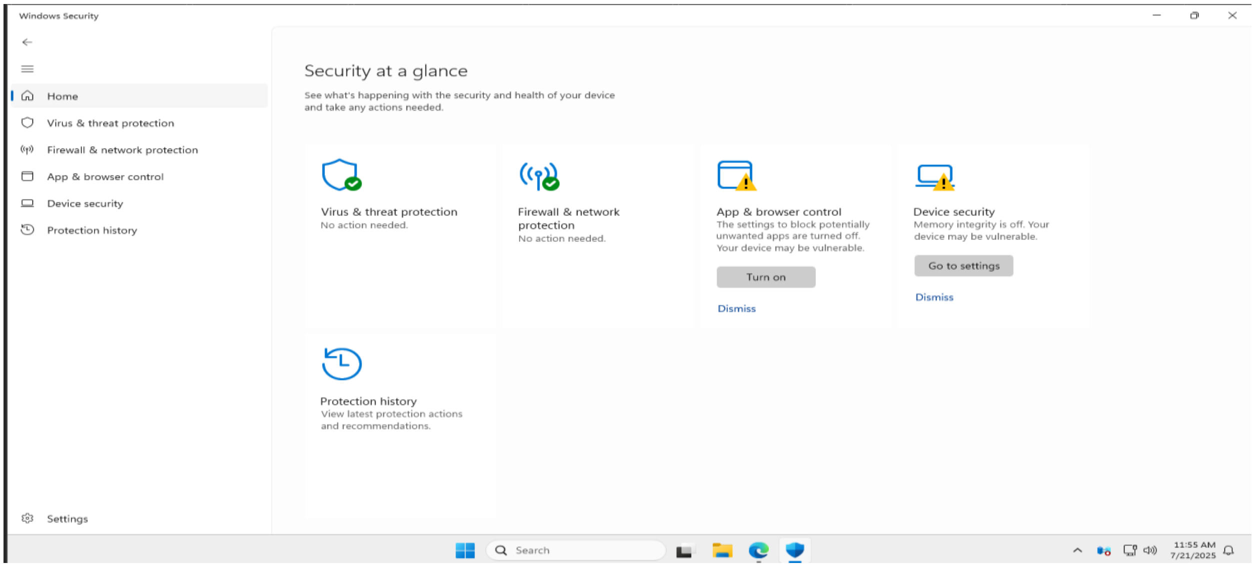
1. Press Windows Key + R to open the Run dialog
2. Type eventvwr.msc and press Enter
3. If prompted by UAC, click "Yes" to run as administrator

Step 1.2: Navigate to Windows Defender Logs

1. In Event Viewer, expand "Applications and Services Logs"
2. Navigate to: Microsoft → Windows → Windows Defender
3. Right-click on "Operational" and select "Properties"
4. Ensure "Enable logging" is checked
5. Set maximum log size (recommended: 20MB minimum)
6. Click "OK" to save settings

Technical Note: The Windows Defender Operational log path is:

```
Microsoft-Windows-Windows Defender/Operational
```



Security at a glance

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

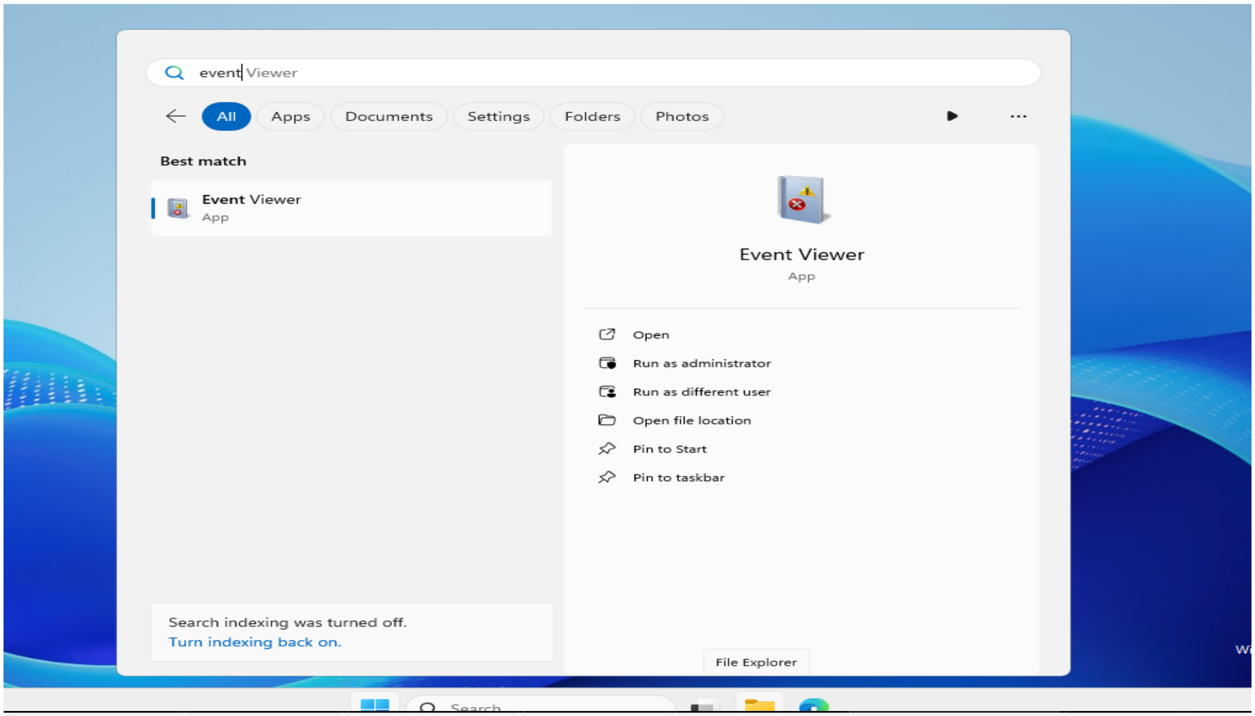
Virus & threat protection
No action needed.

Firewall & network protection
No action needed.

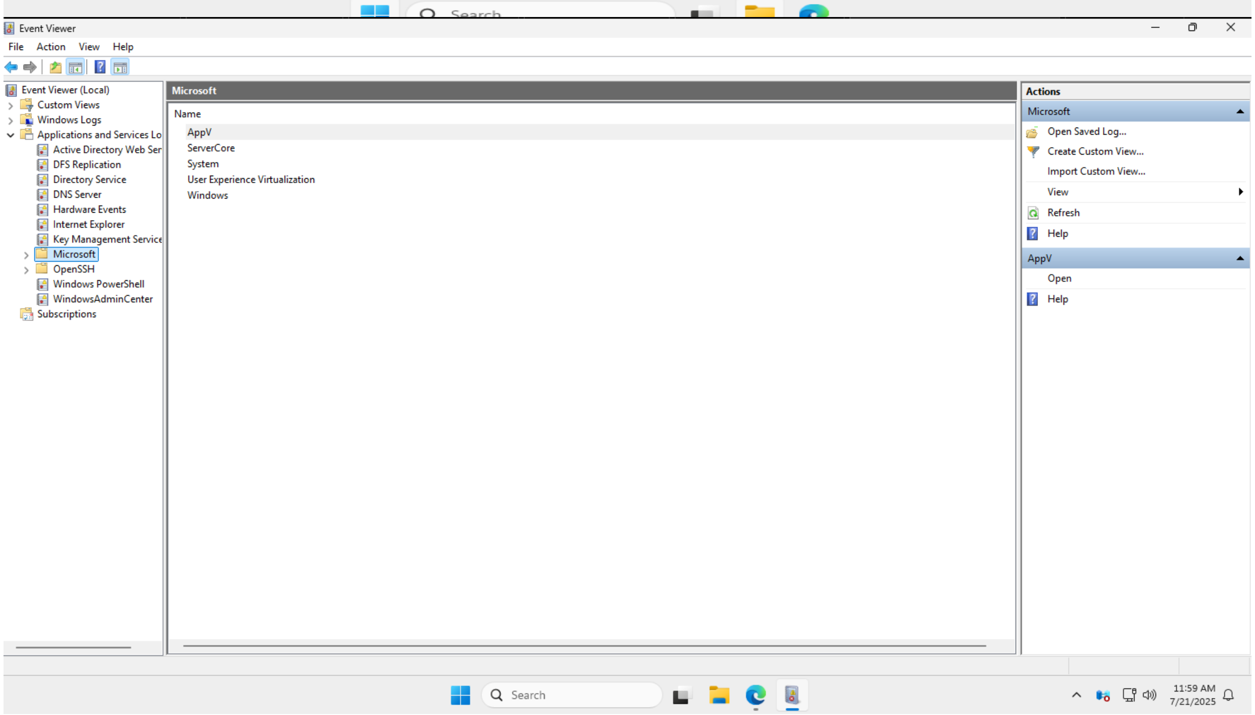
App & browser control
The settings to block potentially unwanted apps are turned off. Your device may be vulnerable.

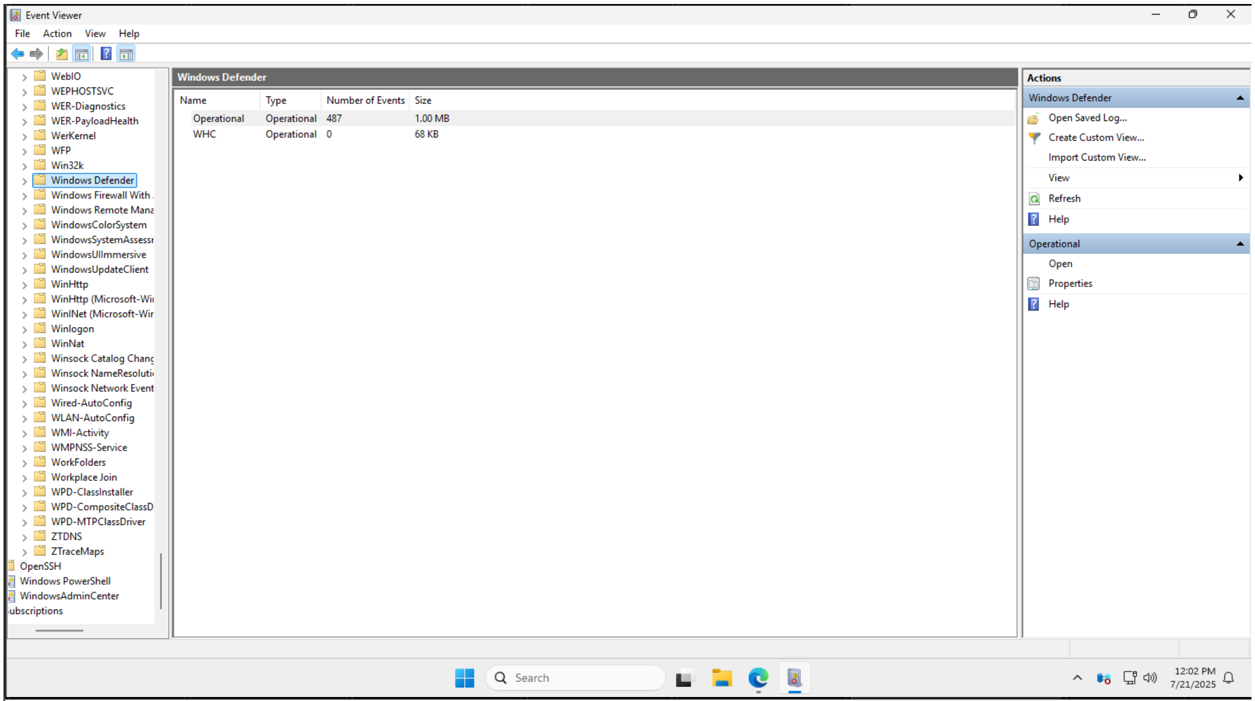
Device security
Memory integrity is off. Your device may be vulnerable.

Protection history
View latest protection actions and recommendations.



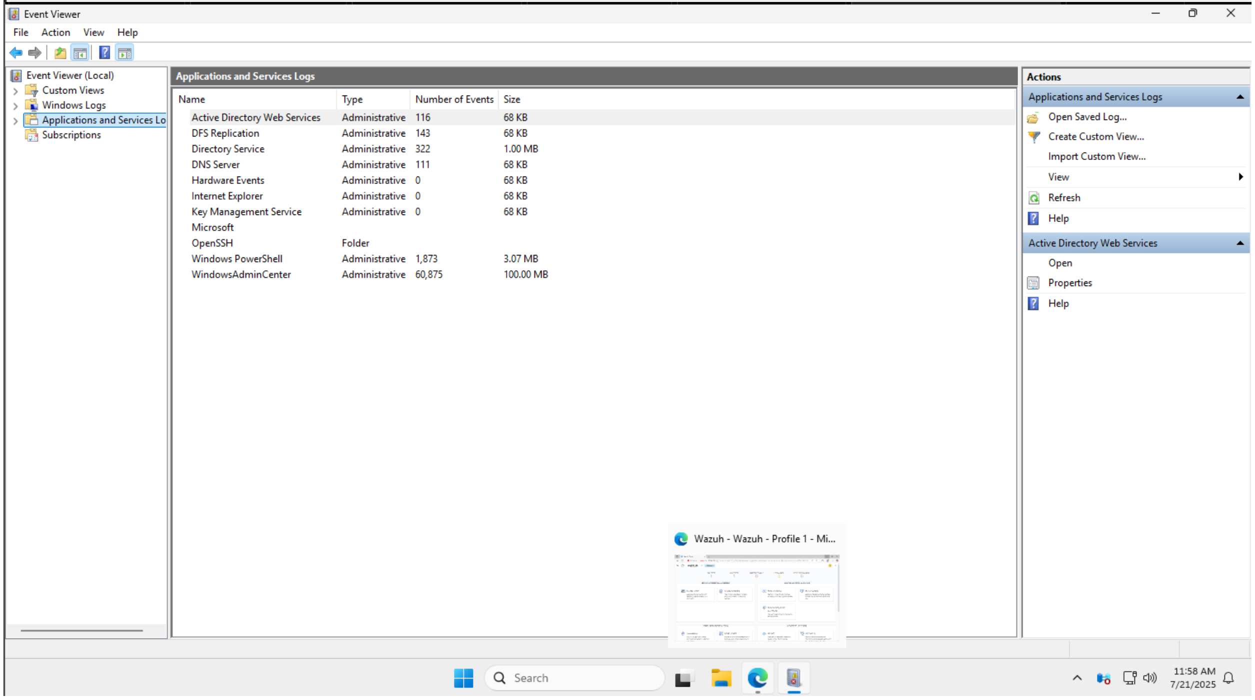
Search indexing was turned off.
Turn indexing back on.





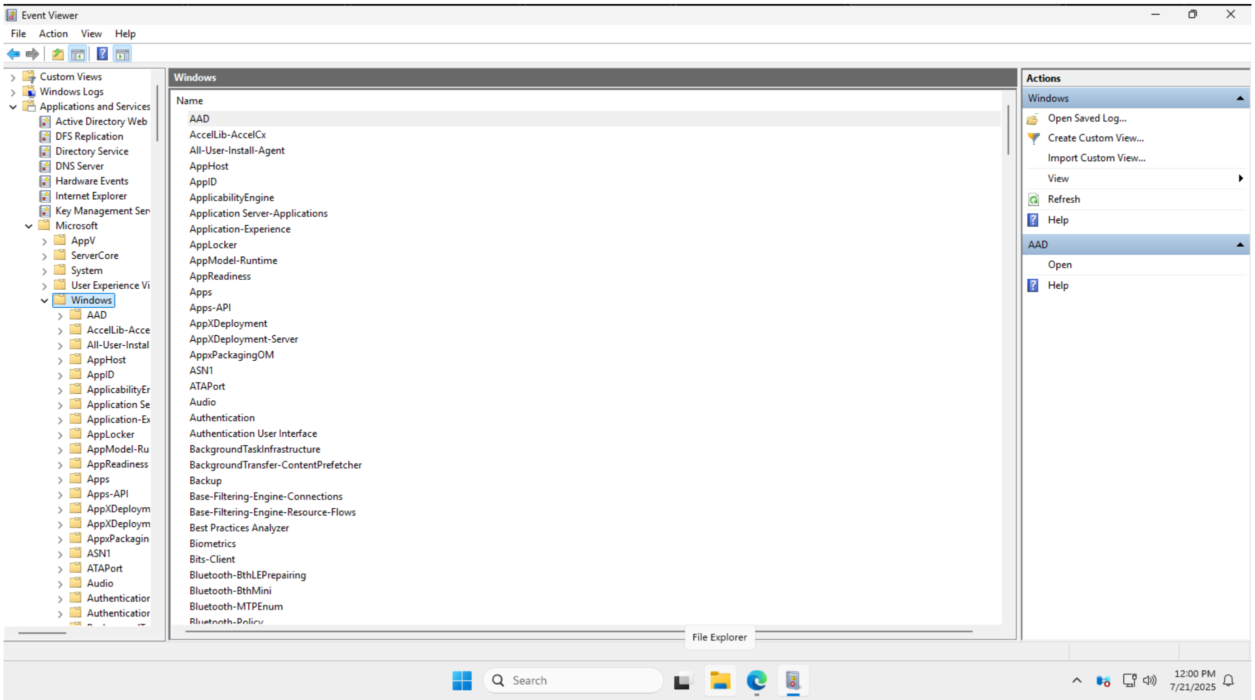
Windows Defender

Name	Type	Number of Events	Size
Operational	Operational	487	1.00 MB
WHC	Operational	0	68 KB



Applications and Services Logs

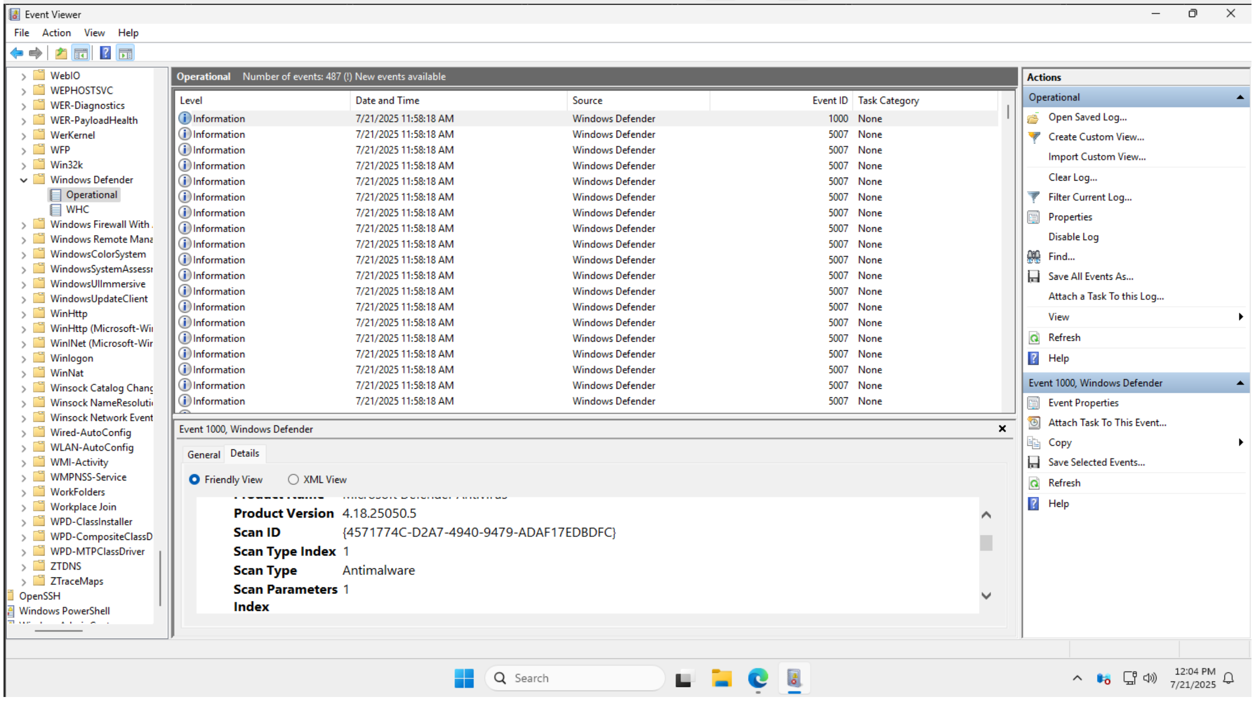
Name	Type	Number of Events	Size
Active Directory Web Services	Administrative	116	68 KB
DFS Replication	Administrative	143	68 KB
Directory Service	Administrative	322	1.00 MB
DNS Server	Administrative	111	68 KB
Hardware Events	Administrative	0	68 KB
Internet Explorer	Administrative	0	68 KB
Key Management Service	Administrative	0	68 KB
Microsoft			
OpenSSH	Folder		
Windows PowerShell	Administrative	1,873	3.07 MB
WindowsAdminCenter	Administrative	60,875	100.00 MB



Windows

Name

AAD
AccelLib-AccelCx
All-User-Install-Agent
AppHost
AppID
ApplicabilityEngine
Application Server-Applications
Application-Experience
AppLocker
AppModel-Runtime
AppReadiness
Apps
Apps-API
AppXDeployment
AppXDeployment-Server
AppxPackagingOM
ASN1
ATAPort
Audio
Authentication
Authentication User Interface
BackgroundTaskInfrastructure
BackgroundTransfer-ContentPrefetcher
Backup
Base-Filtering-Engine-Connections
Base-Filtering-Engine-Resource-Flows
Best Practices Analyzer
Biometrics
Bits-Client
Bluetooth-BthLEPrepairing
Bluetooth-BthMini
Bluetooth-MTPEnum
Bluetooth-Policy



Operational Number of events: 487 (!) New events available

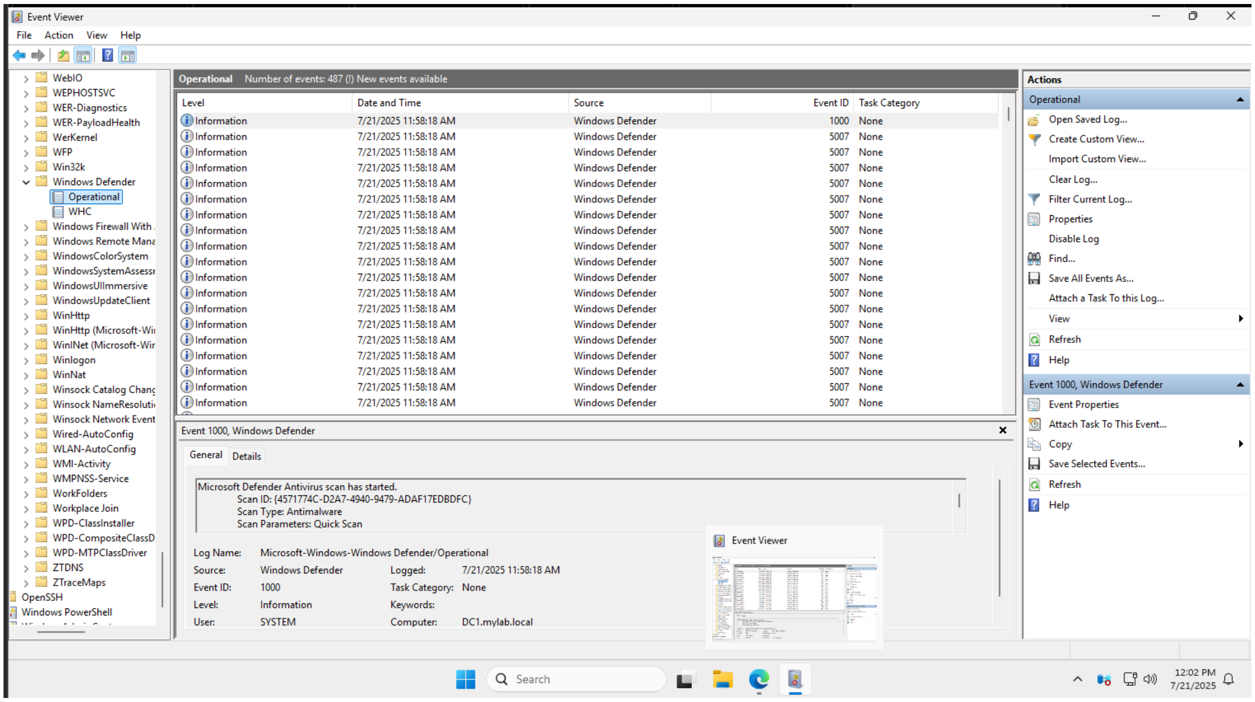
Level	Date and Time	Source	Event ID	Task Category
Information	7/21/2025 11:58:18 AM	Windows Defender	1000	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None

Event 1000, Windows Defender

General Details

● Friendly View ○ XML View

Product Name	Microsoft Defender Antivirus
Product Version	4.18.25050.5
Scan ID	{4571774C-D2A7-4940-9479-ADAF17EDBDFC}
Scan Type Index	1
Scan Type	Antimalware
Scan Parameters Index	1



Operational Number of events: 487 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	7/21/2025 11:58:18 AM	Windows Defender	1000	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None
Information	7/21/2025 11:58:18 AM	Windows Defender	5007	None

Event 1000, Windows Defender

General Details

```
Microsoft Defender Antivirus scan has started.
        Scan ID: {4571774C-D2A7-4940-9479-ADAF17EDBDFC}
        Scan Type: Antimalware
        Scan Parameters: Quick Scan
```

Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	7/21/2025 11:58:18 AM
Event ID:	1000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DC1.mylab.local

2: Configure Wazuh Agent

Step 2.1: Modify Agent Configuration

1. Access the Wazuh server terminal
2. Navigate to the agent configuration directory:

```
cd /var/ossec/etc/shared/
```

3. Open the agent configuration file:

```
sudo nano agent.conf
```

Step 2.2: Add Windows Defender Log Collection

Add the following configuration block to the agent.conf file:

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

Configuration Explanation:

- <location>: Specifies the Windows Event Log channel to monitor
- <log_format>: Defines the format as Windows Event Channel for proper parsing
- This configuration enables the Wazuh agent to collect all Windows Defender operational events

Step 2.3: Apply Configuration Changes

1. Save the configuration file
2. Restart the Wazuh manager to apply changes:

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

3. Verify the service is running:

```
sudo systemctl status wazuh-manager
```

Phase 3: Update Windows Endpoint

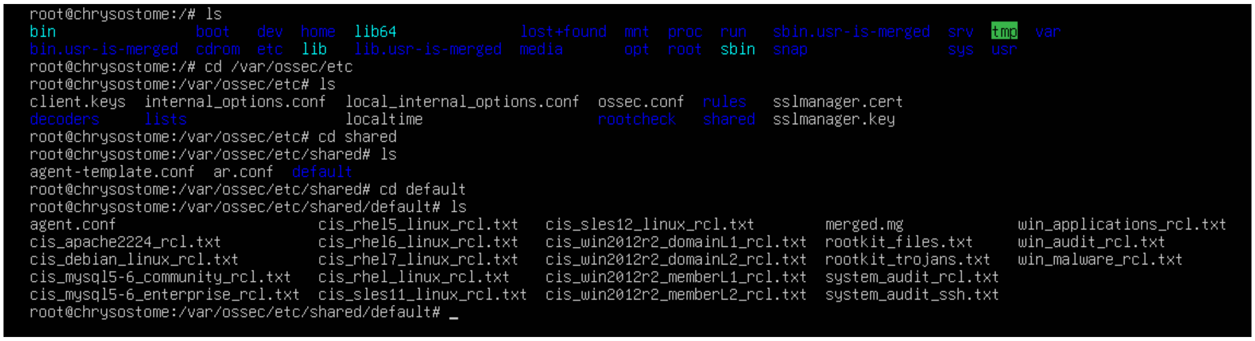
Step 3.1: Restart Wazuh Agent

On the Windows machine:

1. Open Services management console (services.msc)
2. Locate "Wazuh Agent" service
3. Right-click and select "Restart"
4. Verify the service status shows "Running"

Step 3.2: Verify Agent Connectivity

1. Check agent status in Wazuh dashboard
2. Verify last keep-alive timestamp is recent
3. Review agent logs for any connection issue



```
root@chrysostome:/# ls
bin                boot   dev  home  lib64             lost+found  mnt  proc  run   sbin.usr-is-merged  srv  tmp  var
bin.usr-is-merged  cdrom  etc  lib   lib.usr-is-merged  media       opt  root  sbin  snap                sys  usr
root@chrysostome:/# cd /var/ossec/etc
root@chrysostome:/var/ossec/etc# ls
client.keys  internal_options.conf  local_internal_options.conf  ossec.conf  rules   sslmanager.cert
decoders     lists                  localtime                    rootcheck   shared  sslmanager.key
root@chrysostome:/var/ossec/etc# cd shared
root@chrysostome:/var/ossec/etc/shared# ls
agent-template.conf  ar.conf  default
root@chrysostome:/var/ossec/etc/shared# cd default
root@chrysostome:/var/ossec/etc/shared/default# ls
agent.conf                        cis_rhel5_linux_rcl.txt   cis_sles12_linux_rcl.txt        merged.mg            win_applications_rcl.txt
cis_apache2224_rcl.txt            cis_rhel6_linux_rcl.txt   cis_win2012r2_domainL1_rcl.txt  rootkit_files.txt    win_audit_rcl.txt
cis_debian_linux_rcl.txt          cis_rhel7_linux_rcl.txt   cis_win2012r2_domainL2_rcl.txt  rootkit_trojans.txt  win_malware_rcl.txt
cis_mysql5-6_community_rcl.txt    cis_rhel_linux_rcl.txt    cis_win2012r2_memberL1_rcl.txt  system_audit_rcl.txt
cis_mysql5-6_enterprise_rcl.txt   cis_sles11_linux_rcl.txt  cis_win2012r2_memberL2_rcl.txt  system_audit_ssh.txt
root@chrysostome:/var/ossec/etc/shared/default# _
```

2. **Configure Wazuh to collect Windows Security logs related to Defender events.**

After open “agent.conf” file we have to add configuration here.

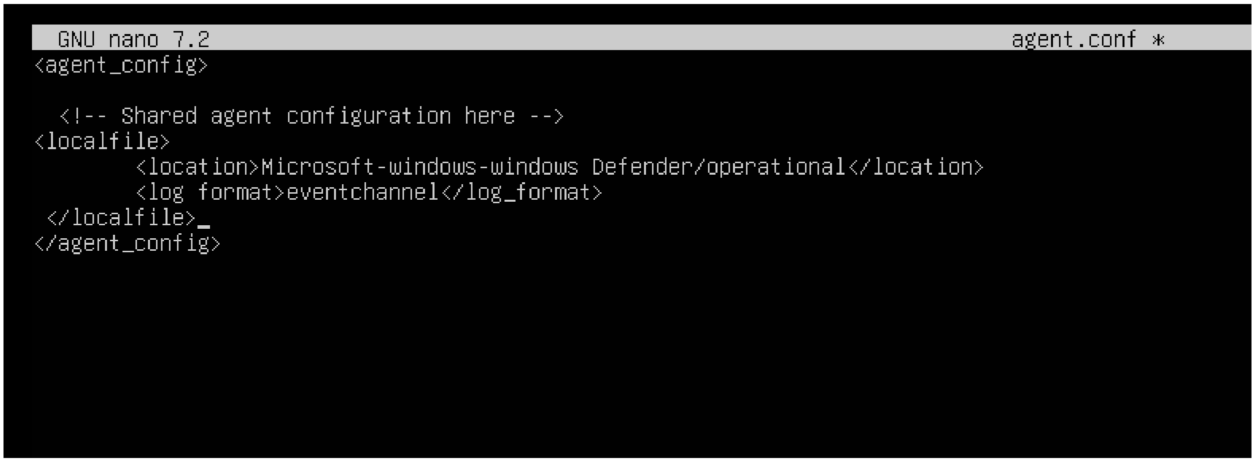
Add this configuration here.

<localfile>

<location>Microsoft-Windows-Windows Defender/Operational</location>

<log_format>eventchannel</log_format>

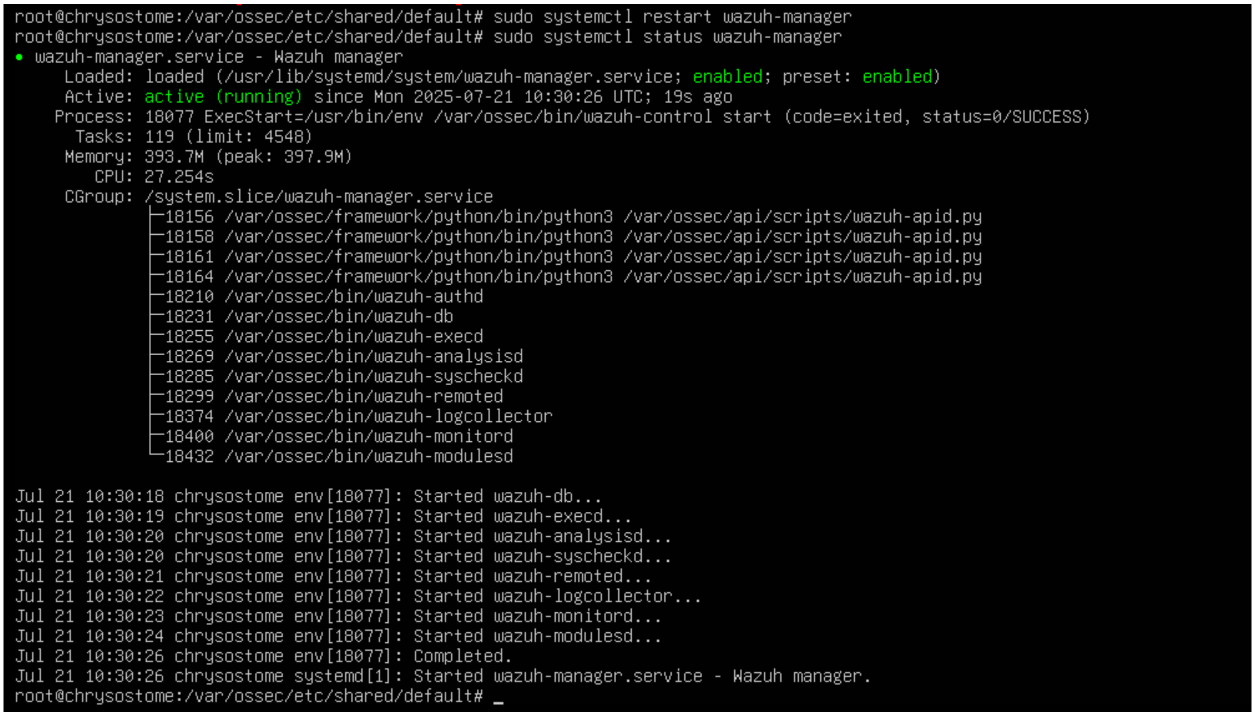
</localfile>



```
  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>
```

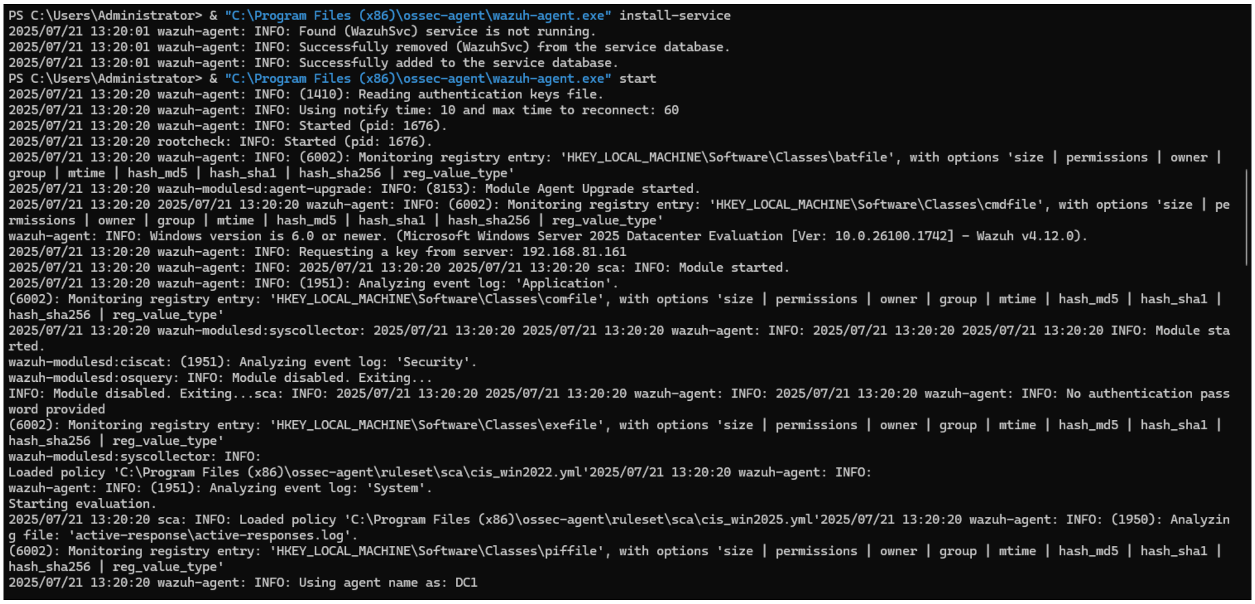
Then save this configuration and run restart wazuh manager and also you can check its status.



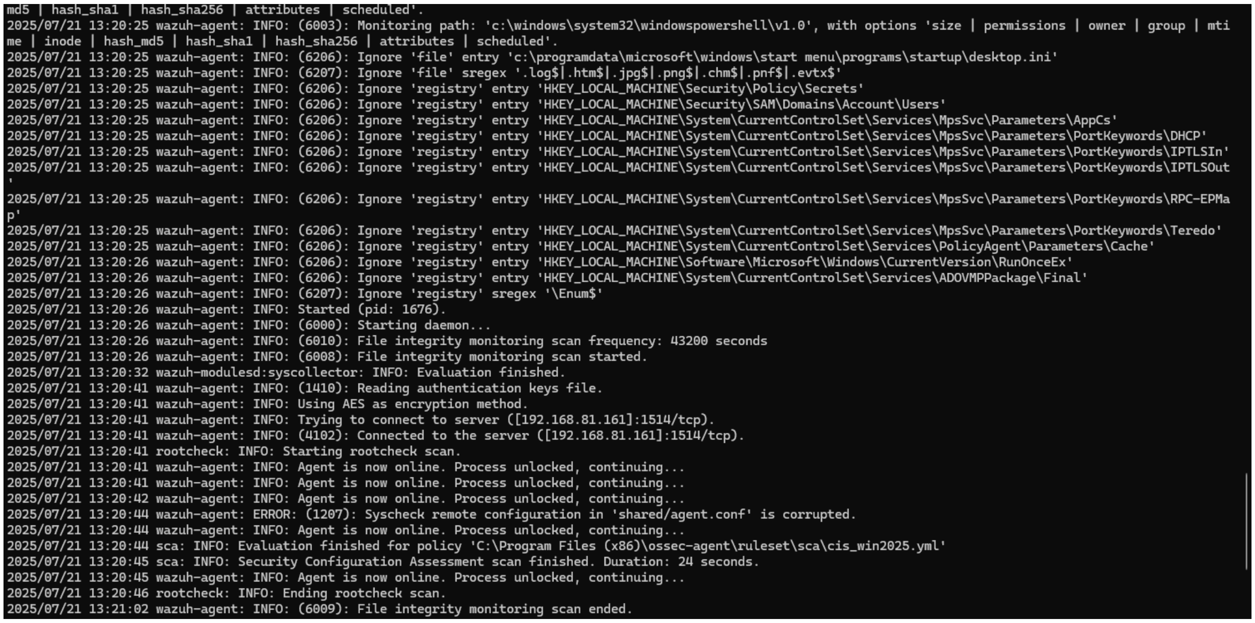
```
root@chrysostome:/var/ossec/etc/shared/default# sudo systemctl restart wazuh-manager
root@chrysostome:/var/ossec/etc/shared/default# sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-07-21 10:30:26 UTC; 19s ago
    Process: 18077 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 119 (limit: 4548)
     Memory: 393.7M (peak: 397.9M)
        CPU: 27.254s
     CGroup: /system.slice/wazuh-manager.service
             ├─18156 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─18158 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─18161 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─18164 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─18210 /var/ossec/bin/wazuh-authd
             ├─18231 /var/ossec/bin/wazuh-db
             ├─18255 /var/ossec/bin/wazuh-execd
             ├─18269 /var/ossec/bin/wazuh-analysisd
             ├─18285 /var/ossec/bin/wazuh-syscheckd
             ├─18299 /var/ossec/bin/wazuh-remoted
             ├─18374 /var/ossec/bin/wazuh-logcollector
             ├─18400 /var/ossec/bin/wazuh-monitord
             └─18432 /var/ossec/bin/wazuh-modulesd

Jul 21 10:30:18 chrysostome env[18077]: Started wazuh-db...
Jul 21 10:30:19 chrysostome env[18077]: Started wazuh-execd...
Jul 21 10:30:20 chrysostome env[18077]: Started wazuh-analysisd...
Jul 21 10:30:20 chrysostome env[18077]: Started wazuh-syscheckd...
Jul 21 10:30:21 chrysostome env[18077]: Started wazuh-remoted...
Jul 21 10:30:22 chrysostome env[18077]: Started wazuh-logcollector...
Jul 21 10:30:23 chrysostome env[18077]: Started wazuh-monitord...
Jul 21 10:30:24 chrysostome env[18077]: Started wazuh-modulesd...
Jul 21 10:30:26 chrysostome env[18077]: Completed.
Jul 21 10:30:26 chrysostome systemd[1]: Started wazuh-manager.service - Wazuh manager.
root@chrysostome:/var/ossec/etc/shared/default# _
```

Now go to“Windows10”and restart“Wazuh-agent”.

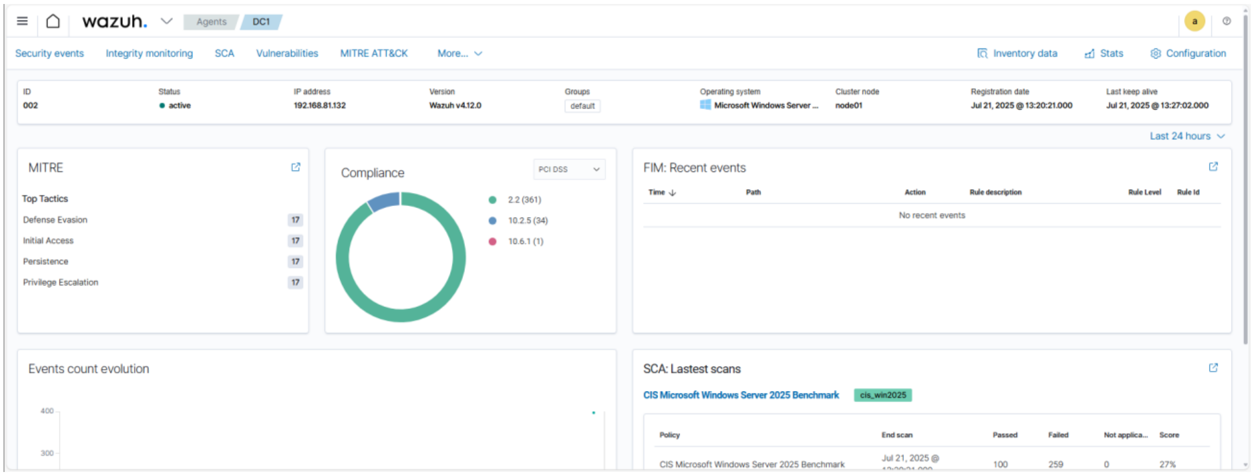


```
PS C:\Users\Administrator> & "C:\Program Files (x86)\ossec-agent\wazuh-agent.exe" install-service
2025/07/21 13:20:01 wazuh-agent: INFO: Found (WazuhSvc) service is not running.
2025/07/21 13:20:01 wazuh-agent: INFO: Successfully removed (WazuhSvc) from the service database.
2025/07/21 13:20:01 wazuh-agent: INFO: Successfully added to the service database.
PS C:\Users\Administrator> & "C:\Program Files (x86)\ossec-agent\wazuh-agent.exe" start
2025/07/21 13:20:20 wazuh-agent: INFO: (1410): Reading authentication keys file.
2025/07/21 13:20:20 wazuh-agent: INFO: Using notify time: 10 and max time to reconnect: 60
2025/07/21 13:20:20 wazuh-agent: INFO: Started (pid: 1676).
2025/07/21 13:20:20 rootcheck: INFO: Started (pid: 1676).
2025/07/21 13:20:20 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\batfile', with options 'size | permissions | owner |
group | mtime | hash_md5 | hash_sha1 | hash_sha256 | reg_value_type'
2025/07/21 13:20:20 wazuh-modulesd:agent-upgrade: INFO: (8153): Module Agent Upgrade started.
2025/07/21 13:20:20 2025/07/21 13:20:20 wazuh-agent: INFO: (6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\cmdfile', with options 'size | pe
rmissions | owner | group | mtime | hash_md5 | hash_sha1 | hash_sha256 | reg_value_type'
wazuh-agent: INFO: Windows version is 6.0 or newer. (Microsoft Windows Server 2025 Datacenter Evaluation [Ver: 10.0.26100.1742] - Wazuh v4.12.0).
2025/07/21 13:20:20 wazuh-agent: INFO: Requesting a key from server: 192.168.81.161
2025/07/21 13:20:20 wazuh-agent: INFO: 2025/07/21 13:20:20 2025/07/21 13:20:20 sca: INFO: Module started.
2025/07/21 13:20:20 wazuh-agent: INFO: (1951): Analyzing event log: 'Application'.
(6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\comfile', with options 'size | permissions | owner | group | mtime | hash_md5 | hash_sha1 |
hash_sha256 | reg_value_type'
2025/07/21 13:20:20 wazuh-modulesd:syscollector: 2025/07/21 13:20:20 2025/07/21 13:20:20 wazuh-agent: INFO: 2025/07/21 13:20:20 2025/07/21 13:20:20 INFO: Module sta
rted.
wazuh-modulesd:ciscat: (1951): Analyzing event log: 'Security'.
wazuh-modulesd:osquery: INFO: Module disabled. Exiting...
INFO: Module disabled. Exiting...sca: INFO: 2025/07/21 13:20:20 2025/07/21 13:20:20 wazuh-agent: INFO: 2025/07/21 13:20:20 wazuh-agent: INFO: No authentication pass
word provided
(6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\exefile', with options 'size | permissions | owner | group | mtime | hash_md5 | hash_sha1 |
hash_sha256 | reg_value_type'
wazuh-modulesd:syscollector: INFO:
Loaded policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_win2022.yml'2025/07/21 13:20:20 wazuh-agent: INFO:
wazuh-agent: INFO: (1951): Analyzing event log: 'System'.
Starting evaluation.
2025/07/21 13:20:20 sca: INFO: Loaded policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_win2025.yml'2025/07/21 13:20:20 wazuh-agent: INFO: (1950): Analyzin
g file: 'active-response\active-responses.log'.
(6002): Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes\piffile', with options 'size | permissions | owner | group | mtime | hash_md5 | hash_sha1 |
hash_sha256 | reg_value_type'
2025/07/21 13:20:20 wazuh-agent: INFO: Using agent name as: DC1
```



```
md5 | hash_sha1 | hash_sha256 | attributes | scheduled'.
2025/07/21 13:20:25 wazuh-agent: INFO: (6003): Monitoring path: 'c:\windows\system32\windowspowershell\v1.0', with options 'size | permissions | owner | group | mti
me | inode | hash_md5 | hash_sha1 | hash_sha256 | attributes | scheduled'.
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'file' entry 'c:\programdata\microsoft\windows\start menu\programs\startup\desktop.ini'
2025/07/21 13:20:25 wazuh-agent: INFO: (6207): Ignore 'file' sregex '.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Security\Policy\Secrets'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Security\SAM\Domains\Account\Users'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\AppCs'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\DHCP'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSIn'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\IPTLSOut
'

2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\RPC-EPMa
p'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MpsSvc\Parameters\PortKeywords\Teredo'
2025/07/21 13:20:25 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent\Parameters\Cache'
2025/07/21 13:20:26 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx'
2025/07/21 13:20:26 wazuh-agent: INFO: (6206): Ignore 'registry' entry 'HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ADOVMPPackage\Final'
2025/07/21 13:20:26 wazuh-agent: INFO: (6207): Ignore 'registry' sregex '\Enum$'
2025/07/21 13:20:26 wazuh-agent: INFO: Started (pid: 1676).
2025/07/21 13:20:26 wazuh-agent: INFO: (6000): Starting daemon...
2025/07/21 13:20:26 wazuh-agent: INFO: (6010): File integrity monitoring scan frequency: 43200 seconds
2025/07/21 13:20:26 wazuh-agent: INFO: (6008): File integrity monitoring scan started.
2025/07/21 13:20:32 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/07/21 13:20:41 wazuh-agent: INFO: (1410): Reading authentication keys file.
2025/07/21 13:20:41 wazuh-agent: INFO: Using AES as encryption method.
2025/07/21 13:20:41 wazuh-agent: INFO: Trying to connect to server ([192.168.81.161]:1514/tcp).
2025/07/21 13:20:41 wazuh-agent: INFO: (4102): Connected to the server ([192.168.81.161]:1514/tcp).
2025/07/21 13:20:41 rootcheck: INFO: Starting rootcheck scan.
2025/07/21 13:20:41 wazuh-agent: INFO: Agent is now online. Process unlocked, continuing...
2025/07/21 13:20:41 wazuh-agent: INFO: Agent is now online. Process unlocked, continuing...
2025/07/21 13:20:42 wazuh-agent: INFO: Agent is now online. Process unlocked, continuing...
2025/07/21 13:20:44 wazuh-agent: ERROR: (1207): Syscheck remote configuration in 'shared/agent.conf' is corrupted.
2025/07/21 13:20:44 wazuh-agent: INFO: Agent is now online. Process unlocked, continuing...
2025/07/21 13:20:44 sca: INFO: Evaluation finished for policy 'C:\Program Files (x86)\ossec-agent\ruleset\sca\cis_win2025.yml'
2025/07/21 13:20:45 sca: INFO: Security Configuration Assessment scan finished. Duration: 24 seconds.
2025/07/21 13:20:45 wazuh-agent: INFO: Agent is now online. Process unlocked, continuing...
2025/07/21 13:20:46 rootcheck: INFO: Ending rootcheck scan.
2025/07/21 13:21:02 wazuh-agent: INFO: (6009): File integrity monitoring scan ended.
```



ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
002	● active	192.168.81.132	Wazuh v4.12.0	default	Microsoft Windows Server ...	node01	Jul 21, 2025 @ 13:20:21.000	Jul 21, 2025 @ 13:27:02.000

Last 24 hours

MITRE

Top Tactics

Defense Evasion	17
Initial Access	17
Persistence	17
Privilege Escalation	17

Compliance

PCI DSS

FIM: Recent events

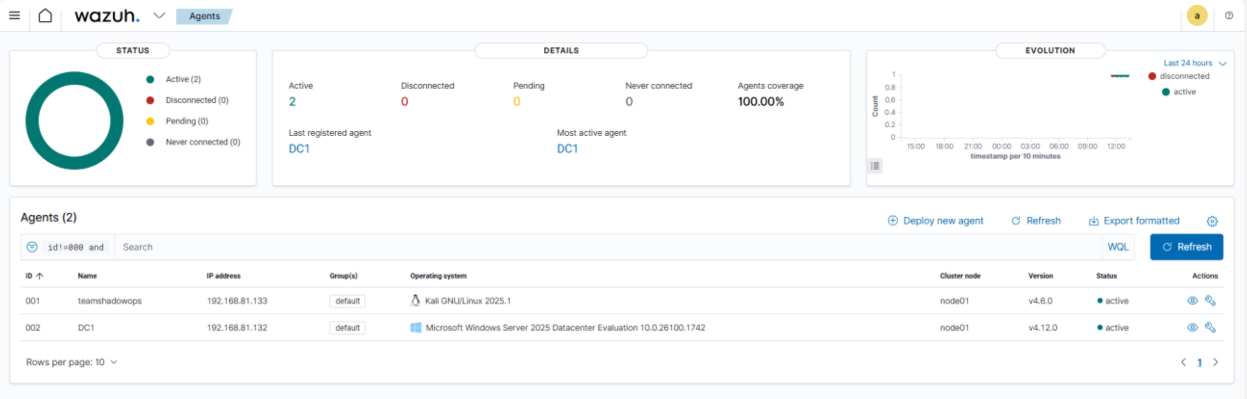
Time ↓	Path	Action	Rule description	Rule Level	Rule Id
No recent events					

Events count evolution

SCA: Lastest scans

CIS Microsoft Windows Server 2025 Benchmark cis_win2025

Policy	End scan	Passed	Failed	Not applica...	Score
CIS Microsoft Windows Server 2025 Benchmark	Jul 21, 2025 @	100	259	0	27%



DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last registered agent DC1

Most active agent DC1

Agents (2)

id!=000 and Search

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	teamshadowops	192.168.81.133	default	Kali GNU/Linux 2025.1	node01	v4.6.0	● active	
002	DC1	192.168.81.132	default	Microsoft Windows Server 2025 Datacenter Evaluation 10.0.26100.1742	node01	v4.12.0	● active	

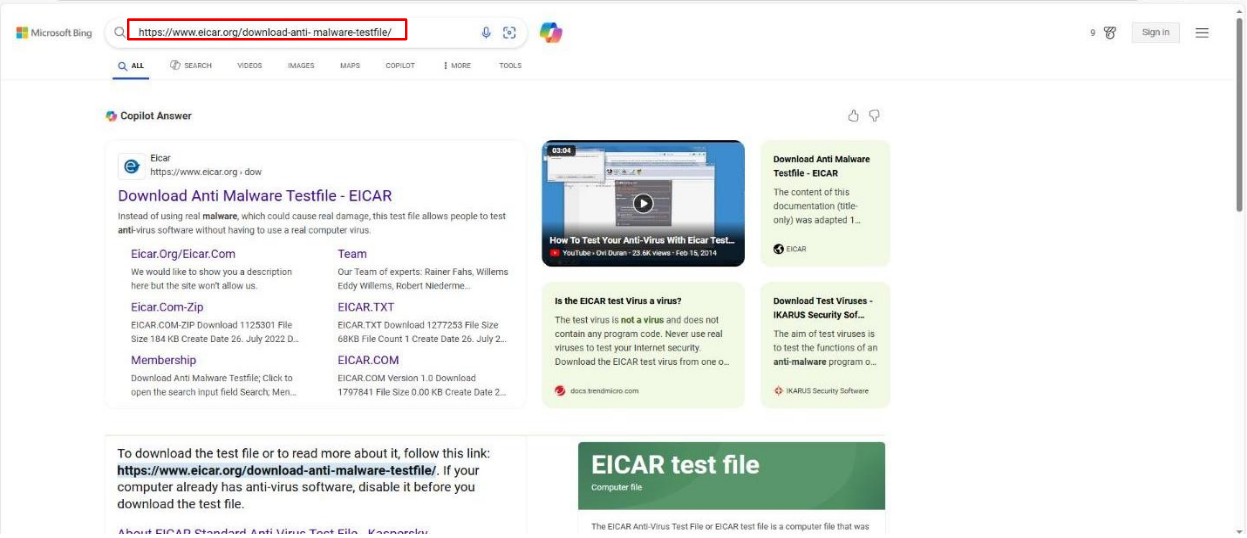
Rows per page: 10

1

After restarting the Wazuh agent, I temporarily disabled Windows Defender’s real-time Protection to allow the download of a malicious test file onto my Windows 11 machine. I then proceeded to access the Wazuh dashboard to monitor and analyze the generated alerts.

Downloading Malware files form:

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



Eicar
https://www.eicar.org › dow

Download Anti Malware Testfile - EICAR

Instead of using real **malware**, which could cause real damage, this test file allows people to test **anti**-virus software without having to use a real computer virus.

Eicar.Org/Eicar.Com
We would like to show you a description here but the site won't allow us.

Team
Our Team of experts: Rainer Fahs, Willems Eddy Willems, Robert Niederme...

Eicar.Com-Zip
EICAR.COM-ZIP Download 1125301 File Size 184 KB Create Date 26. July 2022 D...

EICAR.TXT
EICAR.TXT Download 1277253 File Size 68KB File Count 1 Create Date 26. July 2...

Membership
Download Anti Malware Testfile; Click to open the search input field Search; Men...

EICAR.COM
EICAR.COM Version 1.0 Download 1797841 File Size 0.00 KB Create Date 2...

03:04
How To Test Your Anti-Virus With Eicar Test...
YouTube · Ovi Duran · 23.6K views · Feb 15, 2014

Download Anti Malware Testfile - EICAR
The content of this documentation (title-only) was adapted 1...
EICAR

Is the EICAR test Virus a virus?
The test virus is **not a virus** and does not contain any program code. Never use real viruses to test your Internet security. Download the EICAR test virus from one o...
docs.trendmicro.com

Download Test Viruses - IKARUS Security Sof...
The aim of test viruses is to test the functions of an **anti-malware** program o...
IKARUS Security Software

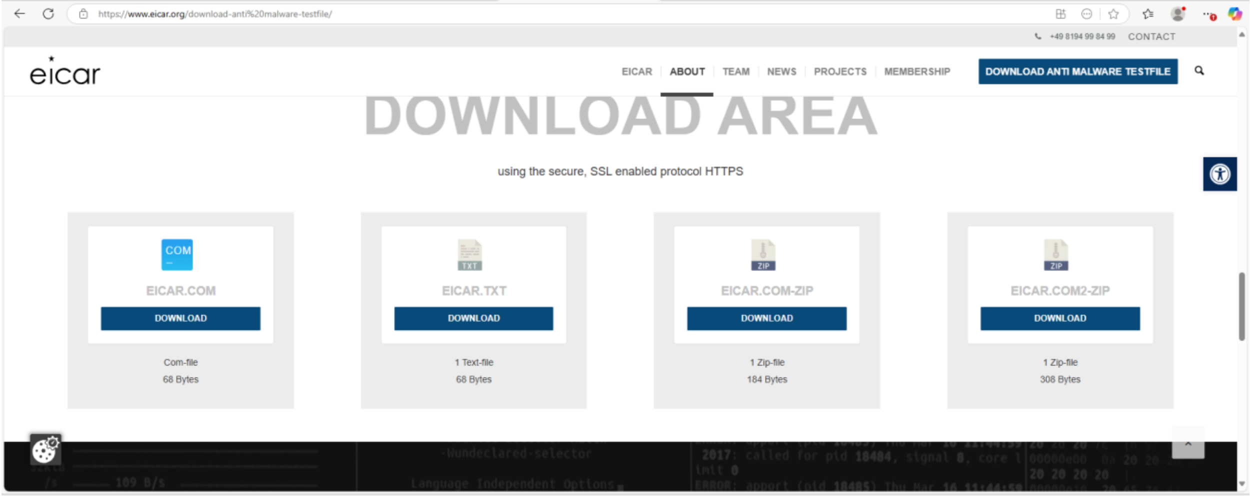
To download the test file or to read more about it, follow this link: **https://www.eicar.org/download-anti-malware-testfile/**. If your computer already has anti-virus software, disable it before you download the test file.

About EICAR Standard Anti Virus Test File - Kaspersky

EICAR test file
Computer file

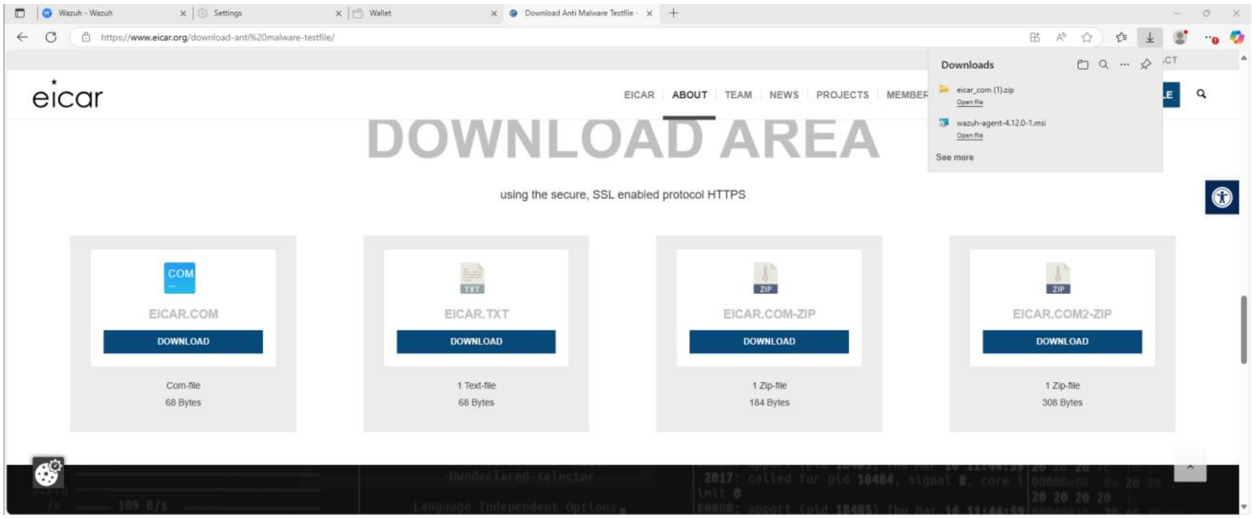
The EICAR Anti-Virus Test File or EICAR test file is a computer file that was

Download any file but I downloaded eicar.zip file

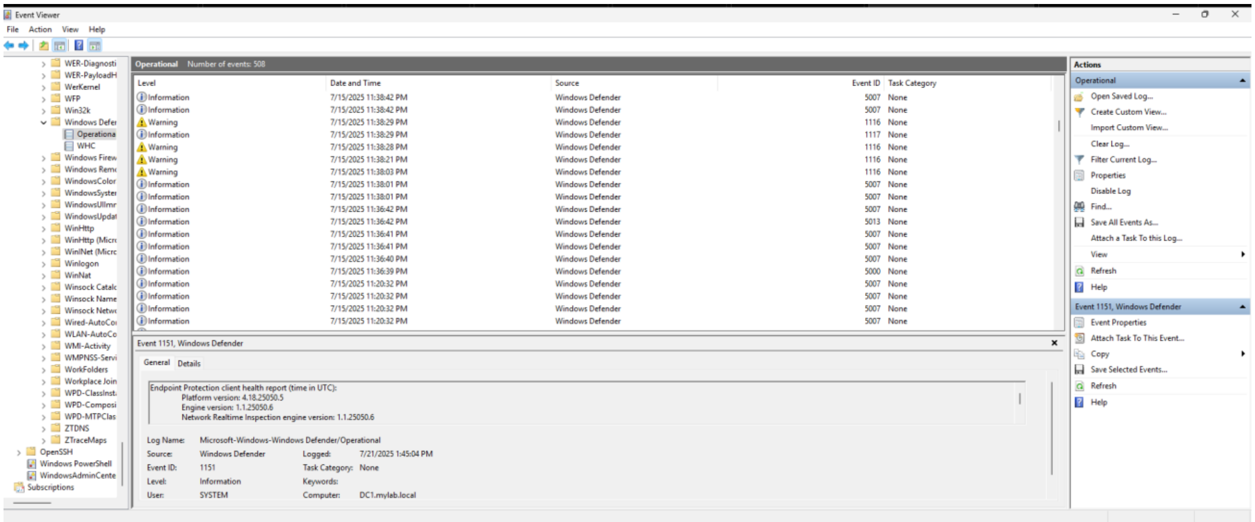

https://www.eicar.org/download-anti%20malware-testfile/
+49 8194 99 84 99
CONTACT
eicar
EICAR
ABOUT
TEAM
NEWS
PROJECTS
MEMBERSHIP
DOWNLOAD ANTI MALWARE TESTFILE
DOWNLOAD AREA

using the secure, SSL enabled protocol HTTPS

EICAR.COM	EICAR.TXT	EICAR.COM-ZIP	EICAR.COM2-ZIP
DOWNLOAD	DOWNLOAD	DOWNLOAD	DOWNLOAD
Com-file 68 Bytes	1 Text-file 68 Bytes	1 Zip-file 184 Bytes	1 Zip-file 308 Bytes



You can see the warning from Microsoft defender here.



Operational Number of events: 508

Level	Date and Time	Source	Event ID	Task Category
Information	7/15/2025 11:38:42 PM	Windows Defender	5007	None
Information	7/15/2025 11:38:42 PM	Windows Defender	5007	None
Warning	7/15/2025 11:38:29 PM	Windows Defender	1116	None
Information	7/15/2025 11:38:29 PM	Windows Defender	1117	None
Warning	7/15/2025 11:38:28 PM	Windows Defender	1116	None
Warning	7/15/2025 11:38:21 PM	Windows Defender	1116	None
Warning	7/15/2025 11:38:03 PM	Windows Defender	1116	None
Information	7/15/2025 11:38:01 PM	Windows Defender	5007	None
Information	7/15/2025 11:38:01 PM	Windows Defender	5007	None
Information	7/15/2025 11:36:42 PM	Windows Defender	5007	None
Information	7/15/2025 11:36:42 PM	Windows Defender	5013	None
Information	7/15/2025 11:36:41 PM	Windows Defender	5007	None
Information	7/15/2025 11:36:41 PM	Windows Defender	5007	None
Information	7/15/2025 11:36:40 PM	Windows Defender	5007	None
Information	7/15/2025 11:36:39 PM	Windows Defender	5000	None
Information	7/15/2025 11:20:32 PM	Windows Defender	5007	None
Information	7/15/2025 11:20:32 PM	Windows Defender	5007	None
Information	7/15/2025 11:20:32 PM	Windows Defender	5007	None
Information	7/15/2025 11:20:32 PM	Windows Defender	5007	None

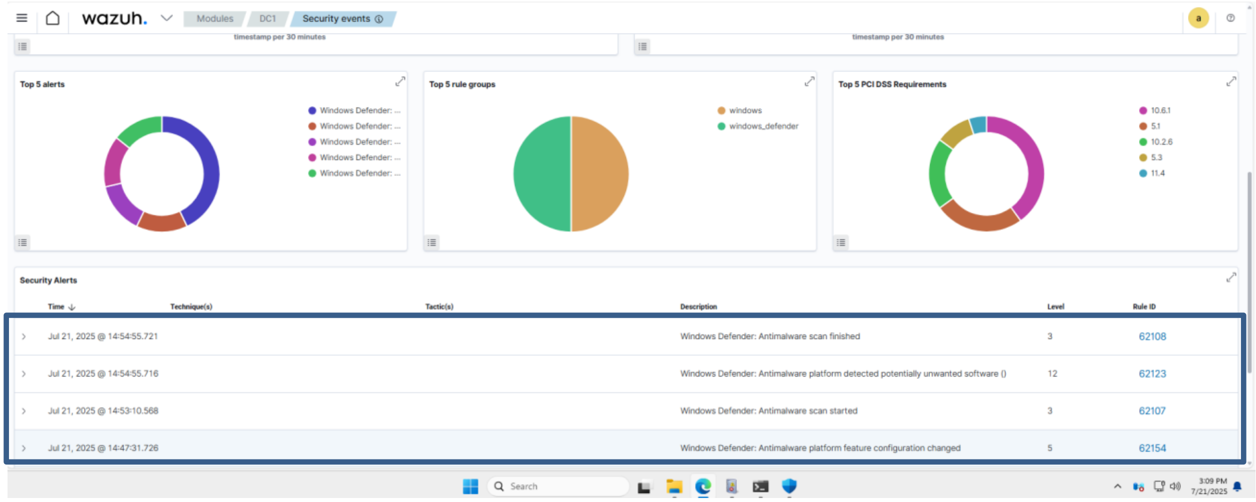
Event 1151, Windows Defender

General Details

```
Endpoint Protection client health report (time in UTC):
        Platform version: 4.18.25050.5
        Engine version: 1.1.25050.6
        Network Realtime Inspection engine version: 1.1.25050.6
```

Log Name:	Microsoft-Windows-Windows Defender/Operational		
Source:	Windows Defender	Logged:	7/21/2025 1:45:04 PM
Event ID:	1151	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DC1.mylab.local

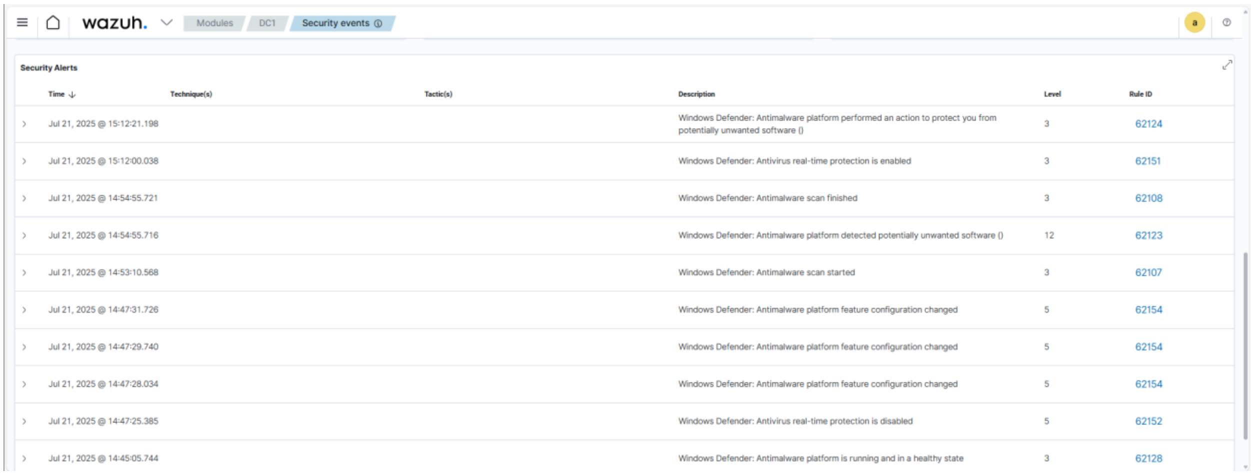
3. **Observe the detection is forwarded to the Wazuh dashboard.**



Security Alerts

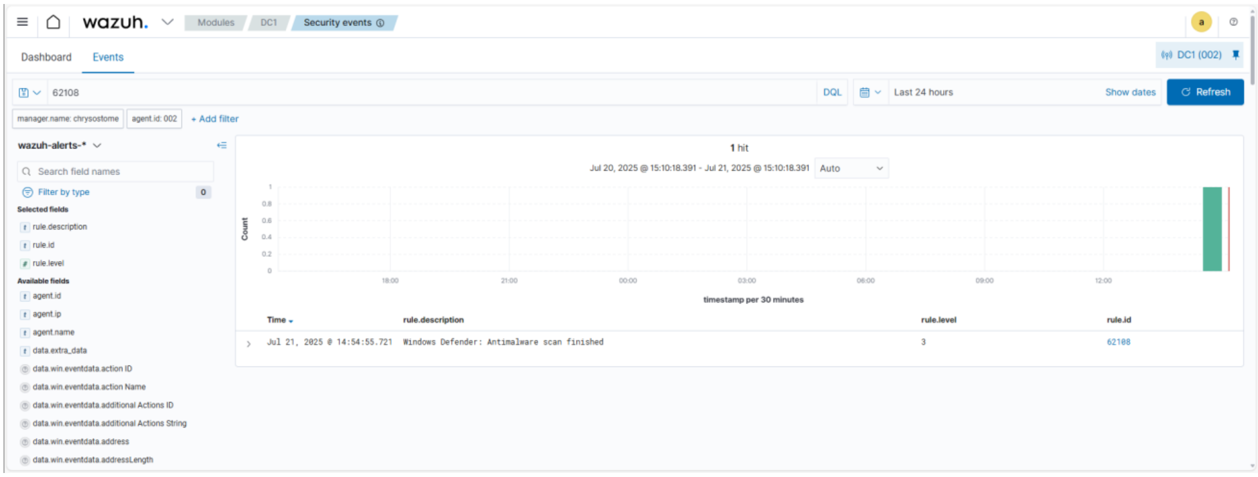
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 21, 2025 @ 14:54:55.721			Windows Defender: Antimalware scan finished	3	62108
Jul 21, 2025 @ 14:54:55.716			Windows Defender: Antimalware platform detected potentially unwanted software ()	12	62123
Jul 21, 2025 @ 14:53:10.568			Windows Defender: Antimalware scan started	3	62107
Jul 21, 2025 @ 14:47:31.726			Windows Defender: Antimalware platform feature configuration changed	5	62154

Here you can see the alert from Microsoft defender in Events Section



Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 21, 2025 @ 15:12:21.198			Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ()	3	62124
Jul 21, 2025 @ 15:12:00.038			Windows Defender: Antivirus real-time protection is enabled	3	62151
Jul 21, 2025 @ 14:54:55.721			Windows Defender: Antimalware scan finished	3	62108
Jul 21, 2025 @ 14:54:55.716			Windows Defender: Antimalware platform detected potentially unwanted software ()	12	62123
Jul 21, 2025 @ 14:53:10.568			Windows Defender: Antimalware scan started	3	62107
Jul 21, 2025 @ 14:47:31.726			Windows Defender: Antimalware platform feature configuration changed	5	62154
Jul 21, 2025 @ 14:47:29.740			Windows Defender: Antimalware platform feature configuration changed	5	62154
Jul 21, 2025 @ 14:47:28.034			Windows Defender: Antimalware platform feature configuration changed	5	62154
Jul 21, 2025 @ 14:47:25.385			Windows Defender: Antivirus real-time protection is disabled	5	62152
Jul 21, 2025 @ 14:45:05.744			Windows Defender: Antimalware platform is running and in a healthy state	3	62128



62108

Last 24 hours

manager.name: chrysostome

agent.id: 002

wazuh-alerts-*

Selected fields
- rule.description
- rule.id
- rule.level

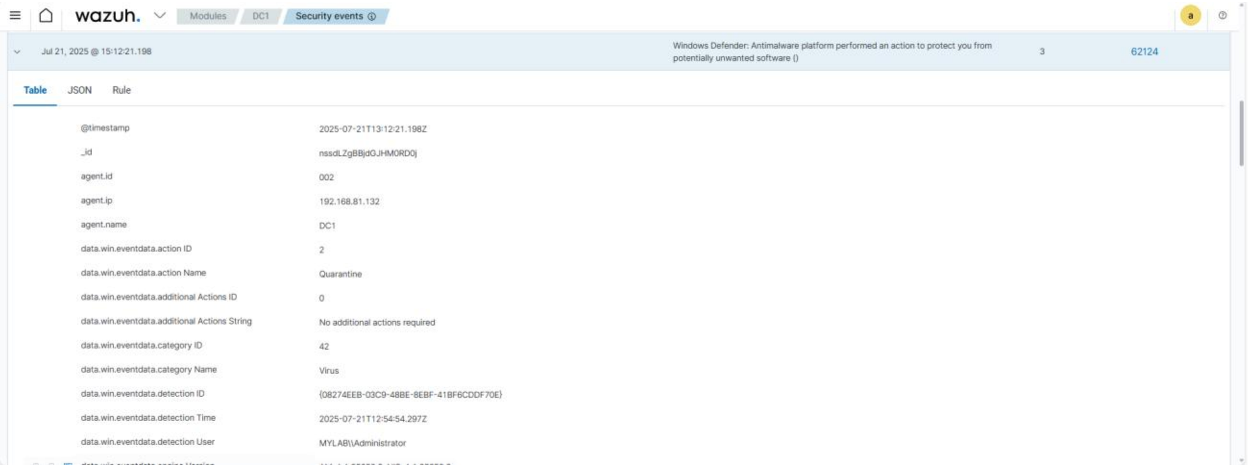
Available fields
- agent.id
- agent.ip
- agent.name
- data.extra_data
- data.win.eventdata.action ID
- data.win.eventdata.action Name
- data.win.eventdata.additional Actions ID
- data.win.eventdata.additional Actions String
- data.win.eventdata.address
- data.win.eventdata.addressLength

1 hit

Jul 20, 2025 @ 15:10:18.391 - Jul 21, 2025 @ 15:10:18.391 Auto

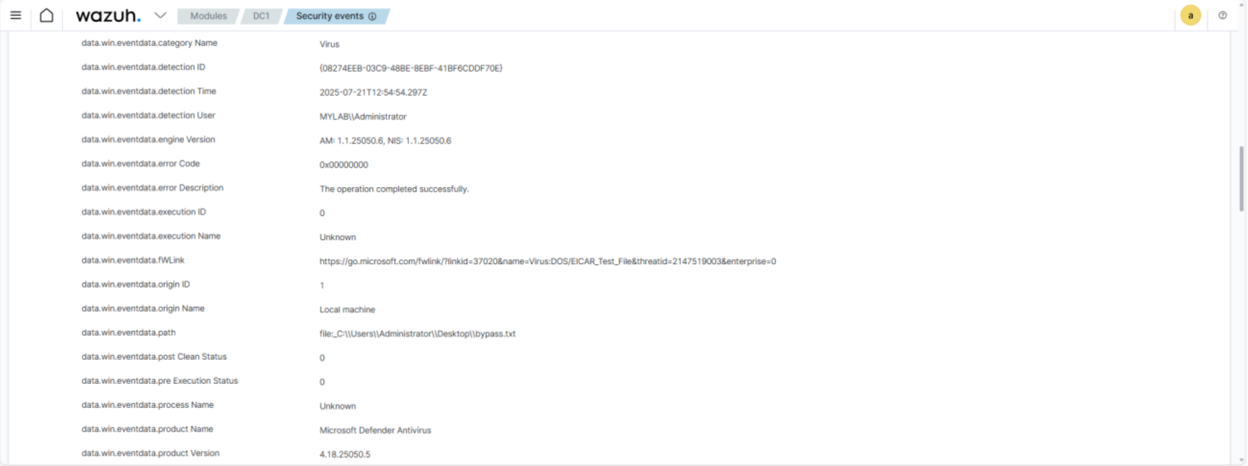
Time	rule.description	rule.level	rule.id
Jul 21, 2025 @ 14:54:55.721	Windows Defender: Antimalware scan finished	3	62108

And we can do some analysis basing on the details we have



Jul 21, 2025 @ 15:12:21.198 Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software () 3 62124

@timestamp	2025-07-21T13:12:21.198Z
_id	nssdLZgBBjdGJHM0RD0j
agent.id	002
agent.ip	192.168.81.132
agent.name	DC1
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	{08274EEB-03C9-48BE-8EBF-41BF6CDDF70E}
data.win.eventdata.detection Time	2025-07-21T12:54:54.297Z
data.win.eventdata.detection User	MYLAB\\Administrator



data.win.eventdata.category Name	Virus
data.win.eventdata.detection ID	{08274EEB-03C9-48BE-8EBF-41BF6CDDF70E}
data.win.eventdata.detection Time	2025-07-21T12:54:54.297Z
data.win.eventdata.detection User	MYLAB\\Administrator
data.win.eventdata.engine Version	AM: 1.1.25050.6, NIS: 1.1.25050.6
data.win.eventdata.error Code	0x00000000
data.win.eventdata.error Description	The operation completed successfully.
data.win.eventdata.execution ID	0
data.win.eventdata.execution Name	Unknown
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\\Desktop\\bypass.txt
data.win.eventdata.post Clean Status	0
data.win.eventdata.pre Execution Status	0
data.win.eventdata.process Name	Unknown
data.win.eventdata.product Name	Microsoft Defender Antivirus
data.win.eventdata.product Version	4.18.25050.5

Key Event Types

- **Event ID 1116**: Malware detection and quarantine
- **Event ID 1117**: Protective action taken
- **Event ID 1118**: Real-time protection state changes
- **Event ID 5001**: Real-time protection disabled
- **Event ID 5010**: Scanning engine configuration changes

Conclusions

Implementation Success Metrics

The successful integration of Windows Defender with Wazuh provides significant security advantages:

Enhanced Threat Detection

- **Centralized Visibility**: Unified view of endpoint security across the organization
- **Real-time Monitoring**: Immediate notification of security threats and responses
- **Historical Analysis**: Comprehensive threat pattern analysis and trend

identification

Operational Benefits

- **Reduced Response Time**: Faster incident detection and response capabilities
- **Automated Workflows**: Streamlined security incident handling processes
- **Resource Optimization**: More efficient allocation of security resources

Strategic Advantages

- **Scalable Architecture**: Easy expansion to additional endpoints and security tools
- **Compliance Support**: Enhanced ability to meet regulatory requirements
- **Risk Reduction**: Improved overall security posture and risk management

This comprehensive integration of Windows Defender with Wazuh establishes a robust foundation for endpoint security monitoring and incident response. The centralized visibility and automated alerting capabilities significantly enhance the organization's ability to detect, analyze, and respond to security threats while maintaining operational efficiency and regulatory compliance.

By following this guide and implementing the recommended best practices, organizations can achieve a mature, scalable security monitoring solution that adapts to evolving threat landscapes and business requirements.