

## Wazuh - Windows Defender Integration {Windows Defender Logs Integration}

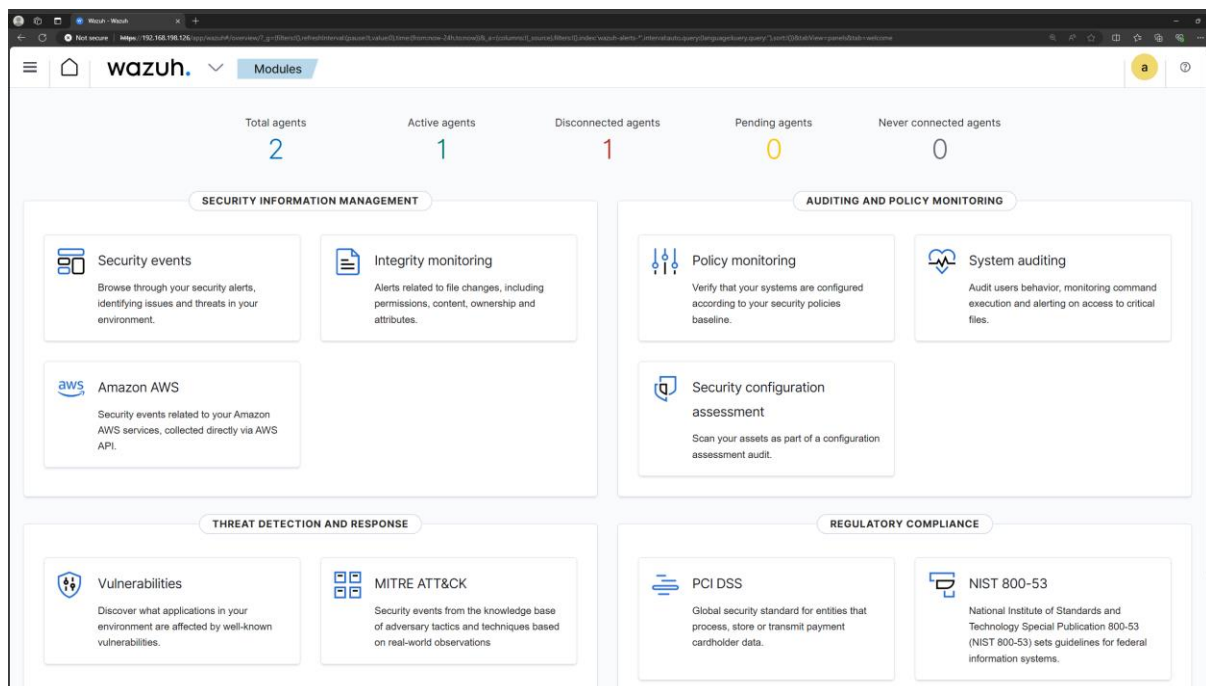
Microsoft offers endpoint security solutions for enterprises called windows Defender with wazuh.

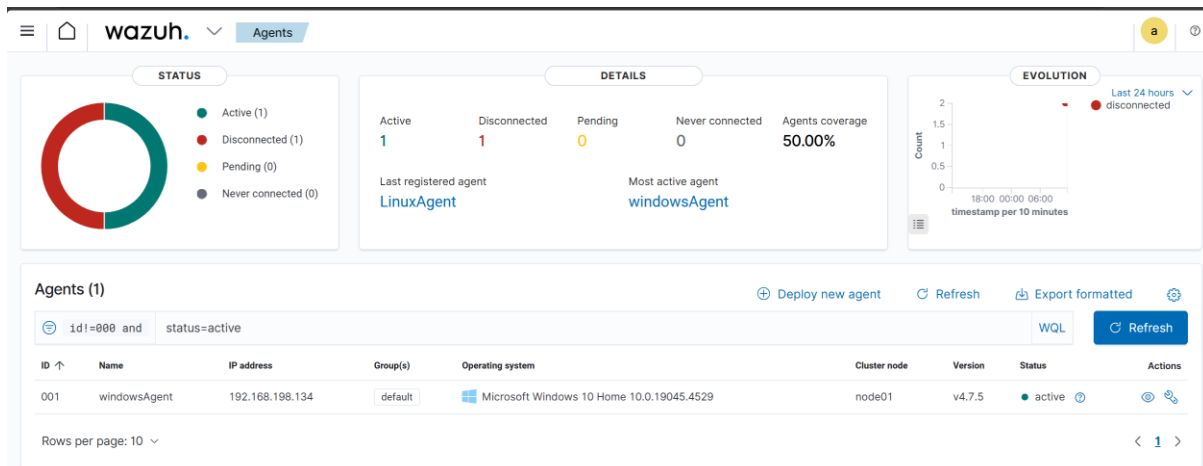
Windows Defender is the anti-malware component of the Microsoft Windows operating system. You can configure Wazuh agents installed on Windows endpoints to collect Windows Defender logs. This provides visibility on malware infections detected by Windows Defender on Windows endpoints. These logs can also provide information about:

- The status of the Windows Defender service.
- Results of Windows Defender scans that the users run on these endpoints.

Setup:

Here I have accessed my Wazuh console via SSH connection in my kali





To collect Windows Defender logs, you must configure the Wazuh agent using centralized configuration, or locally using the agent C:\Program Files (x86)\ossec-agent\ossec.conf file. Centralized configuration allows the instructions to be shared with a group of agents.


For that,

Go to

Event Viewer → Application and Services Logs → Microsoft → Windows → Windows Defender → Operational → search for “error”

AllAppsDocumentsWebMore

Best match



Event Viewer

System

Search the web

Event Viewer - See more search results

Event Viewer

event viewer logs

event viewer command

event viewer.exe

event viewer windows 10


event viewer cmd

event viewer windows 11

event viewer shortcut

event viewer download

event viewer event id 4672



Event Viewer

System

Open

Run as administrator

Open file location

Pin to Start

Pin to taskbar

name	type	number of events	size
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	103	1.07 MB

Information	02-07-2024 10:30:41	Windows Defender	5007	None
Information	02-07-2024 10:32:40	Windows Defender	5007	None
Warning	02-07-2024 10:51:04	Windows Defender	1002	None
Information	02-07-2024 10:49:05	Windows Defender	1000	None
Information	02-07-2024 10:39:56	Windows Defender	1151	None
Information	02-07-2024 09:30:21	Windows Defender	5007	None
Information	02-07-2024 09:58:21	Windows Defender	5007	None
Information	02-07-2024 09:58:20	Windows Defender	2000	None
Information	02-07-2024 09:58:20	Windows Defender	2000	None
Information	02-07-2024 09:52:07	Windows Defender	5007	None
Error	02-07-2024 09:52:07	Windows Defender	2001	None
Information	02-07-2024 09:40:19	Windows Defender	5007	None
Information	02-07-2024 09:40:19	Windows Defender	5007	None



```
agent_config> linux-core (2024-2-18) ...
system-gui (2024-2-18) ...
setting up libdpd-protocol-headers-devel (6-14-1) ...
<!-- Shared agent configuration here --> ...
<localfile>oneid-plugin-domecrandom (1-17-0-3x61) ...
<location>Microsoft-Windows-Windows Defender/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
...
triggers for tex-common (5-18) ...
running mktexlsr. This may take some time ... done.
</agent_config> This may take some time ... done.
running mktexlsr /var/lib/texmf ... done.
building format(s) --all.
This may take some time ... done.
processing triggers for cracklib-runtime (2-9-0-5-1x61) ...
```

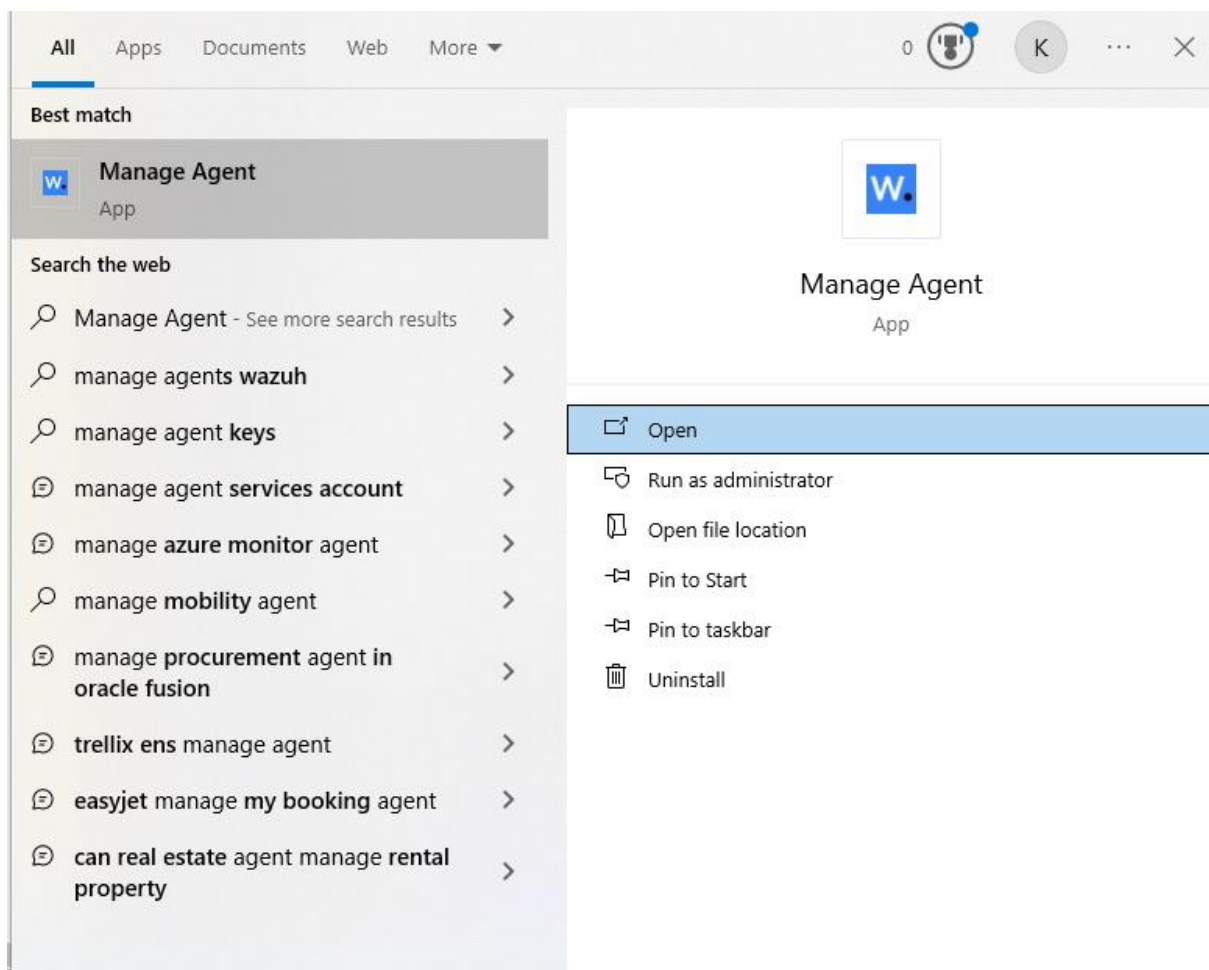
Now, in order to save the changes made, restart your wazuh manager

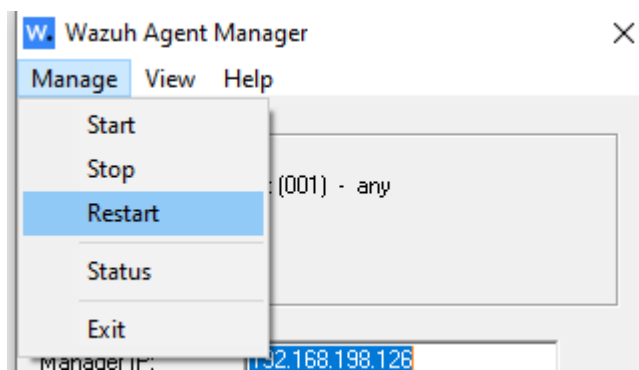
Command: `sudo systemctl restart wazuh-manager`

Now, after successfully restarting your wazuh-manager, its time to restart your agent in windows.

Go to your windows endpoint

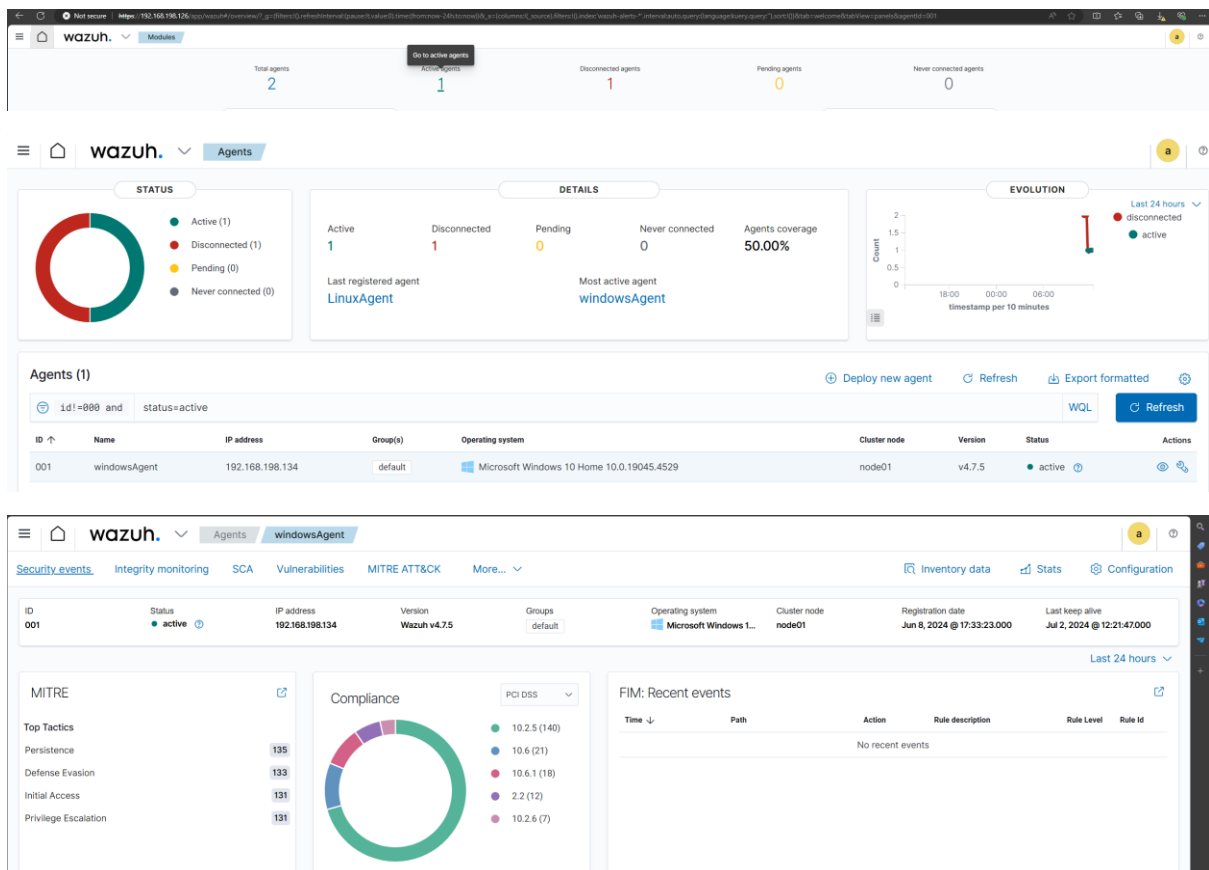
Manage Agent → Manage → restart

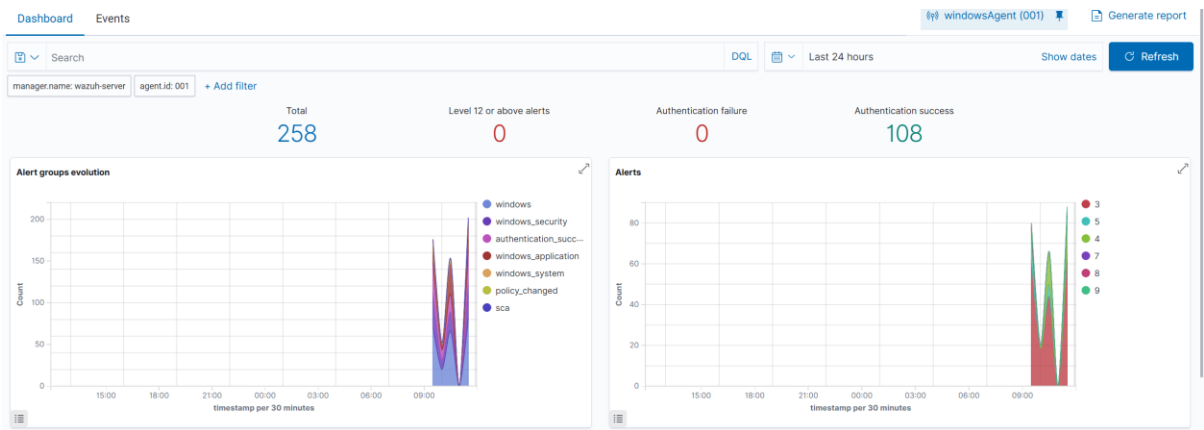




Now, after successful restarting your windows agent, access your wazuh-dashboard

Click on the active agents → select your windows agent → security events



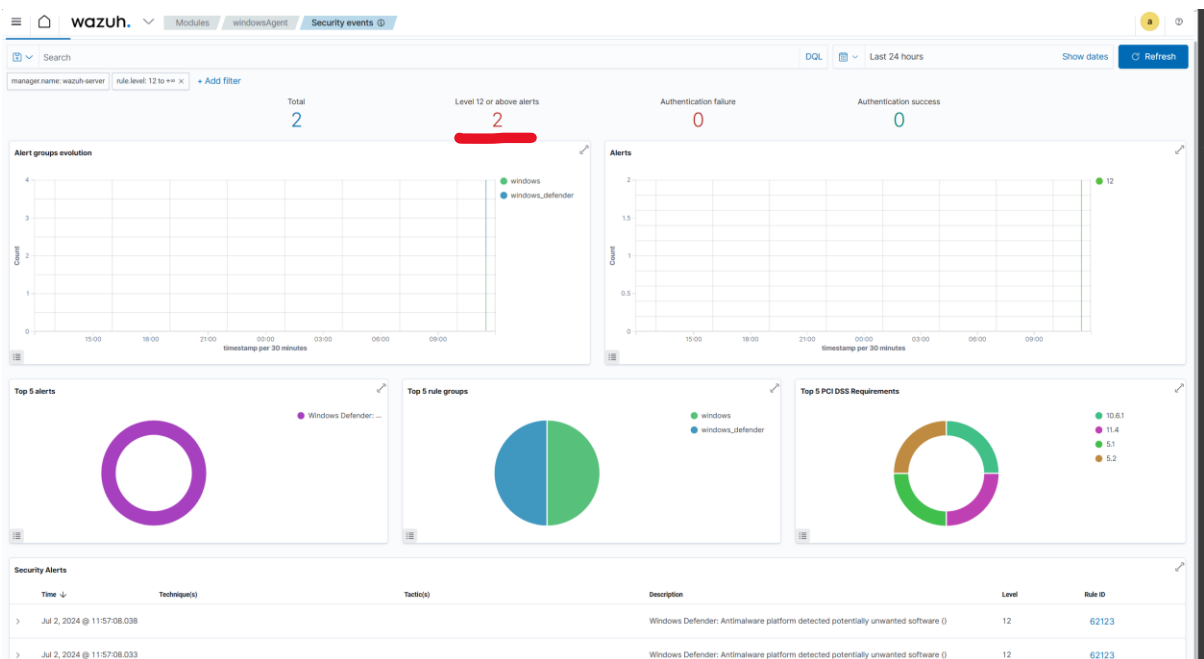


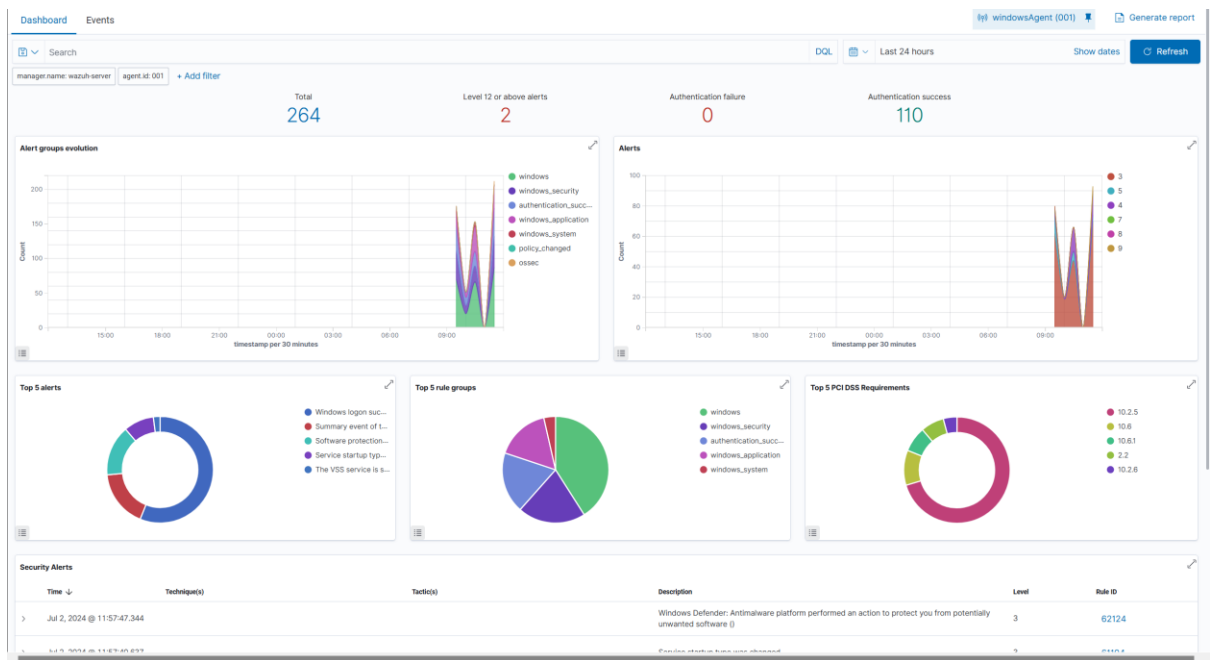
Now, its time to test our setup, for this you can either create your own malware or you can install some test-malwares that are freely available from the internet

Note:

Install malwares at your own risk.

After installing malwares, you can see that there's a notification in the alerts





You can view the security alerts by just clicking on the event and continue your analysis there by

Security Alerts					
Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 2, 2024 @ 11:57:08.038			Windows Defender: Antimalware platform detected potentially unwanted software ( )	12	62123
Jul 2, 2024 @ 11:57:08.033			Windows Defender: Antimalware platform detected potentially unwanted software ( )	12	62123

```
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
Path: containerfile_C:\Users\kusha\Downloads\3e8ae7be-3178-47c4-8b07-5c11972e561.tmp; file_C:\Users\kusha\Downloads\3e8ae7be-3178-47c4-8b07-5c11972e561.tmp->IZip; file_C:\Users\kusha\downloads\d02acc48-0dd9d-4d13-837c-527ab1ae0578.tmp->IZip)
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: NT AUTHORITY\SYSTEM
Process Name: C:\Program Files (x86)\ossec-agent\wazuh-agent.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x80580023
Error description: The program could not find the malware and other potentially unwanted software on this device.
Security Intelligence Version: AV: 1.413.641.0, AS: 1.413.641.0, NS: 1.413.641.0
Engine Version: AM: 1.1.24050.5, NS: 1.1.24050.5"
```

```
data.win.system.opcode
0
data.win.system.processID
3012
data.win.system.providerGuid
{11cd958a-c507-4ef3-b3f2-5f5b9fdb2c78}
data.win.system.providerName
Microsoft-Windows-Windows Defender
data.win.system.severityValue
INFORMATION
data.win.system.systemTime
2024-07-02T10:57:09.9527500Z
data.win.system.task
0
data.win.system.threadID
4348
data.win.system.version
0
decoder.name
windows_eventchannel
id
1719917867.1275069
```