



## Windows Defender Integration with Wazuh

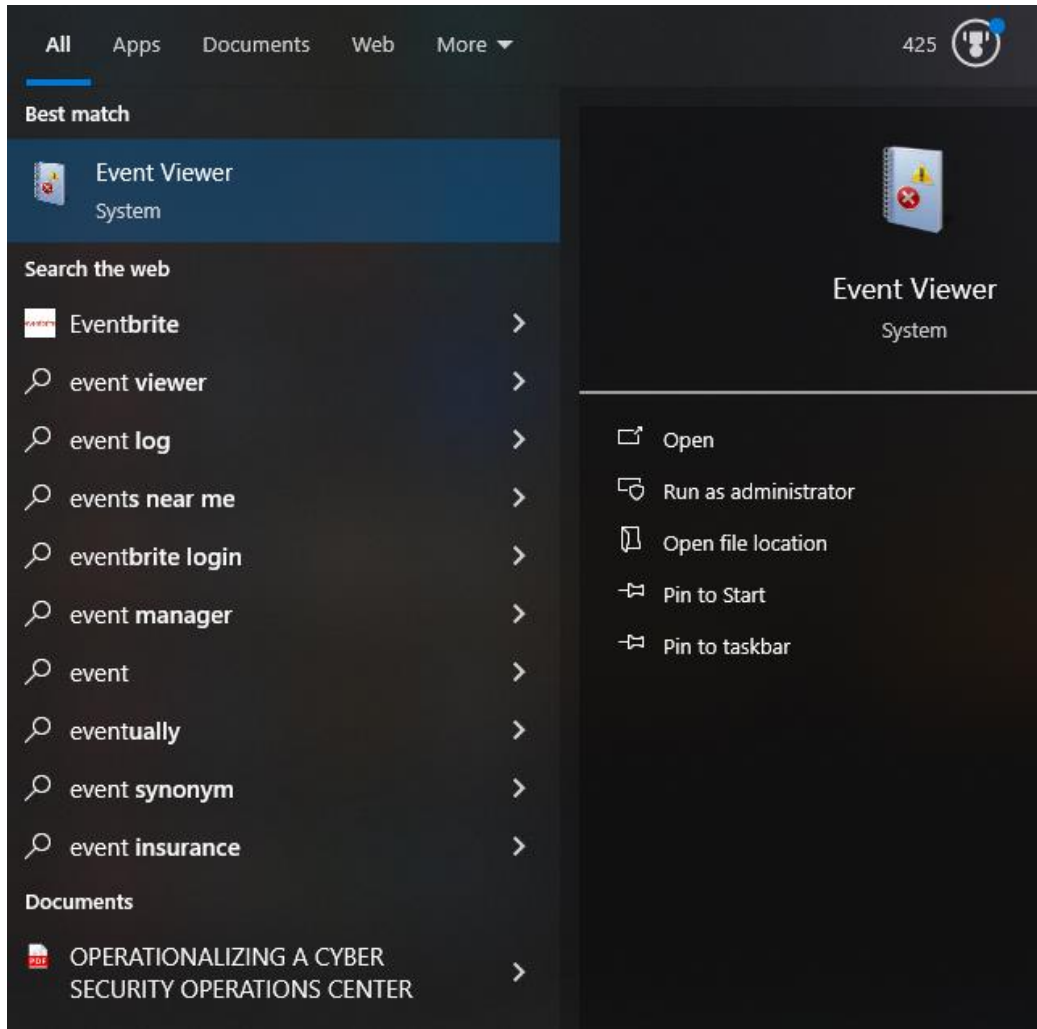
Lab Created by : Sayed Waqar Ali Bacha

LinkedIn: [www.linkedin.com/in/waqar-ali-8a5b6b228](https://www.linkedin.com/in/waqar-ali-8a5b6b228)

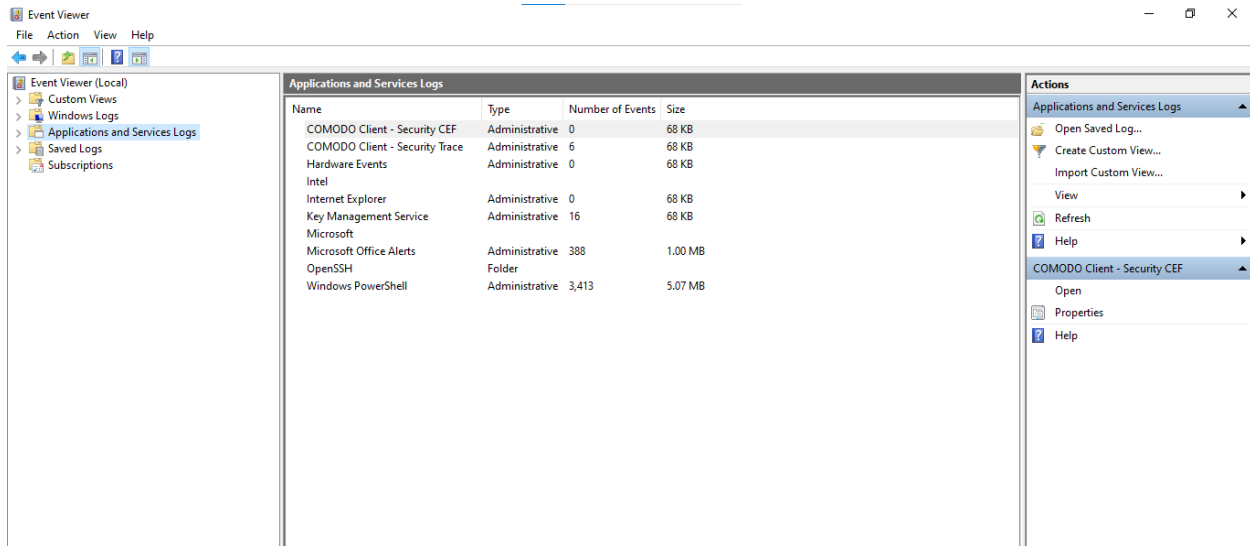
GitHub: <https://github.com/waqar5289>

## 1. Enable Windows Defender logs on a Windows machine.

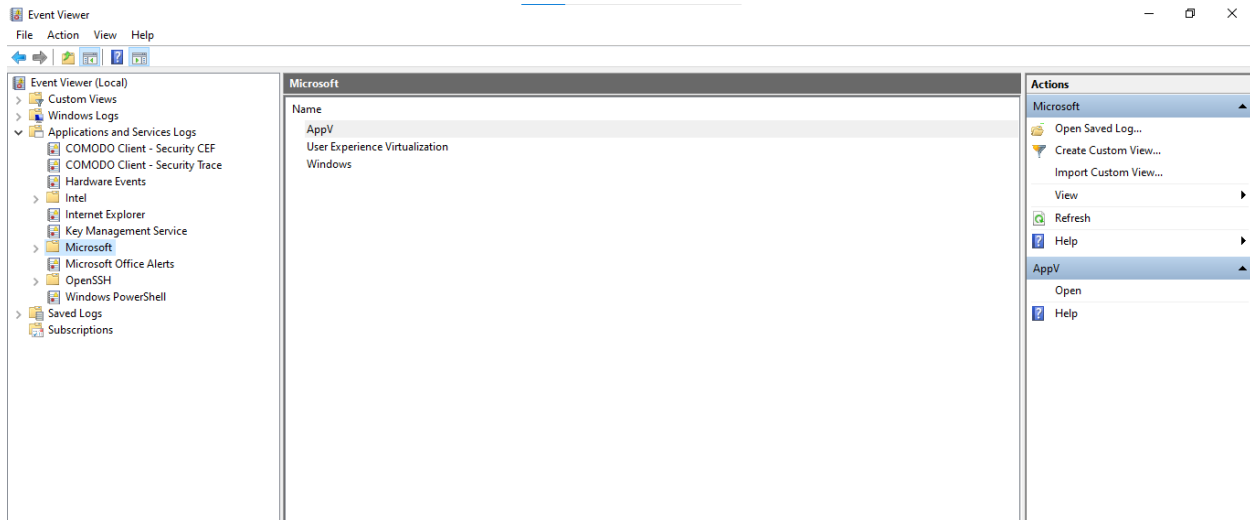
### Open Event Viewer



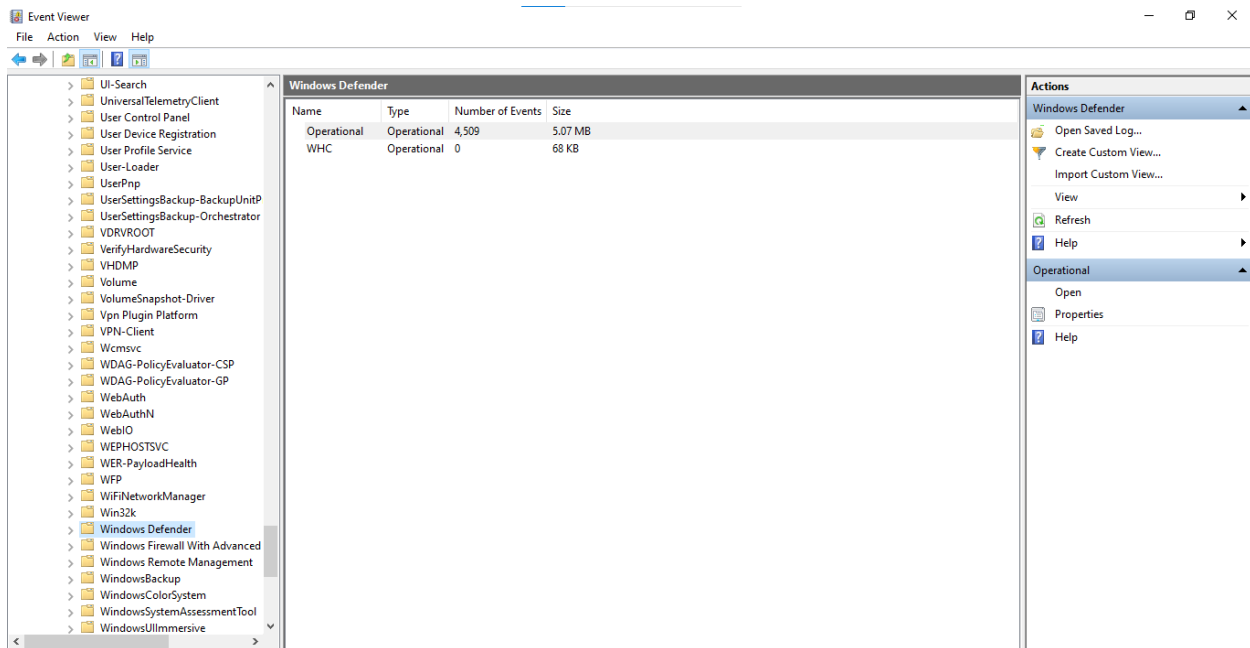
## Click On Open And services Logs



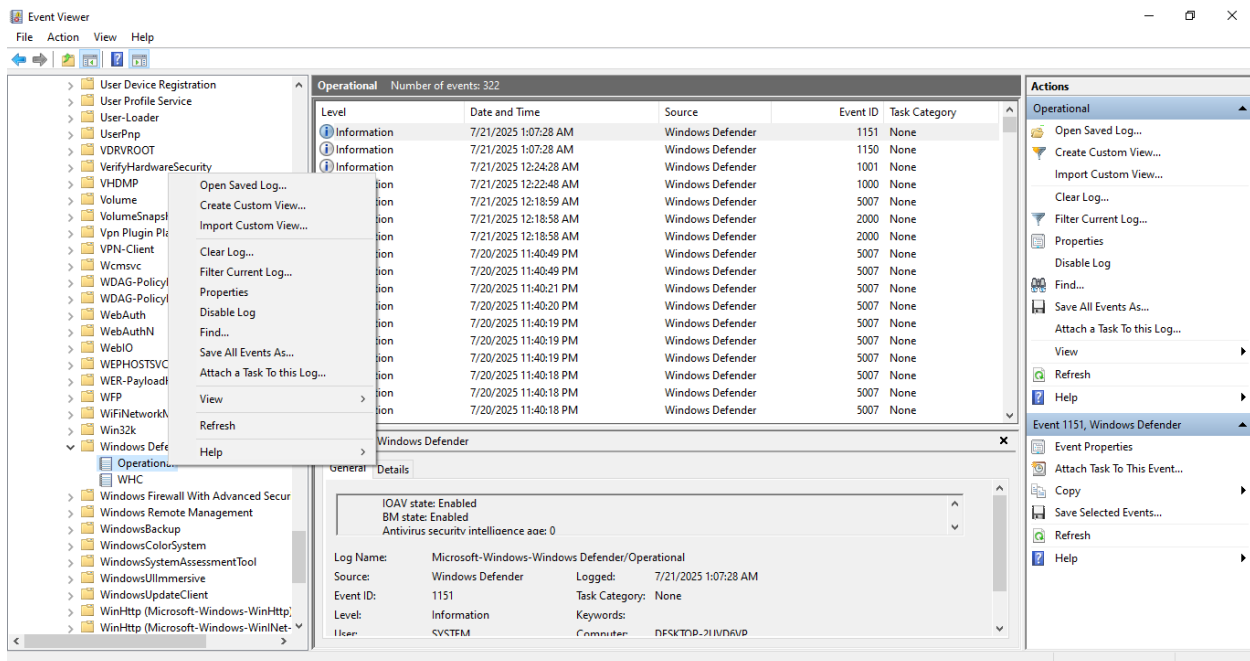
## Click on Microsoft and Then on Windows



After clicking windows Then open Windows defender:



In windows Defender Enabled Operational Field



## 2. Configure Wazuh to collect Windows Security logs related to

### Defender events.

- On your Windows endpoint (with the Wazuh agent installed)
- Open (ossec.conf) file and add these lines inside it.

**<localfile>**

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

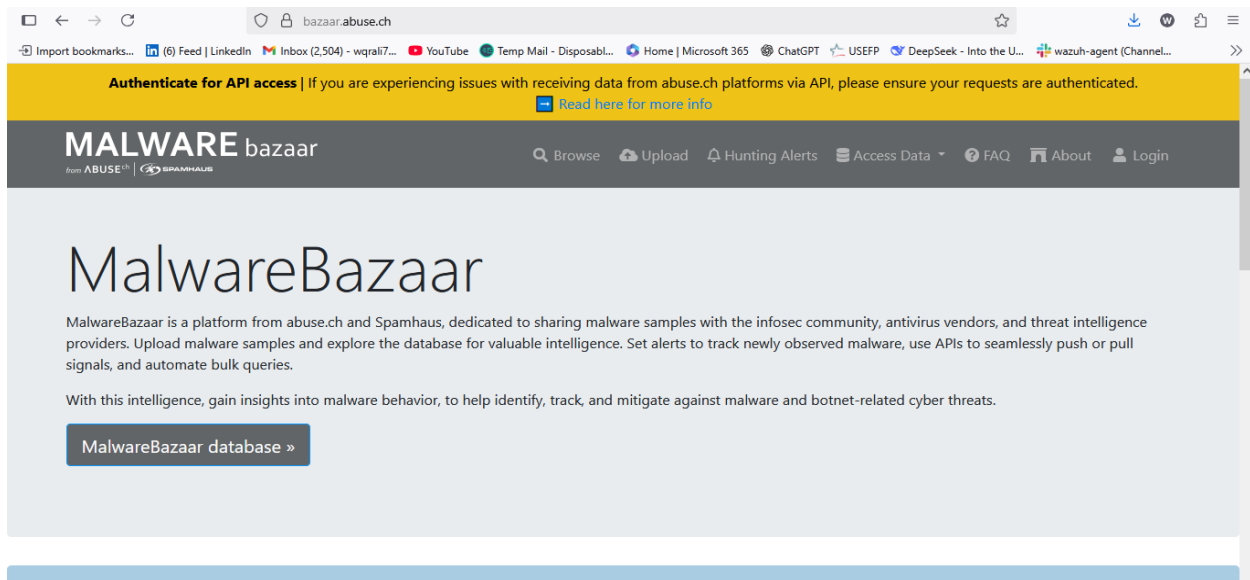
**<log\_format>eventchannel</log\_format>**

**</localfile>**

- Restart Wazuh Agent

### 3. Simulate a Defender alert by downloading or scanning an EICAR test file.

Download a sample from Malware Bazar Then Execute It But Safe One.



### 4. After Running The Malware You Will See Alerts On wazuh Dashboard.

Successfully Analyze Alerts On Wazuh Dashboard

🔍	🔍	📄	🔖	🔍	_index	wazuh-alerts-4.x-2025.07.20
🔍	🔍	📄	🔖	🔍	agent.id	001
🔍	🔍	📄	🔖	🔍	agent.ip	192.168.71.134
🔍	🔍	📄	🔖	🔍	agent.name	windows
🔍	🔍	📄	🔖	🔍	data.win.eventdata.action ID	9
🔍	🔍	📄	🔖	🔍	data.win.eventdata.action Name	Not Applicable
🔍	🔍	📄	🔖	🔍	data.win.eventdata.category ID	8
🔍	🔍	📄	🔖	🔍	data.win.eventdata.category Name	Trojan
🔍	🔍	📄	🔖	🔍	data.win.eventdata.detection ID	{F1B09206-12D7-4AC0-A554-06FFA1250651}
🔍	🔍	📄	🔖	🔍	data.win.eventdata.detection Time	2025-07-20T20:44:08.827Z
🔍	🔍	📄	🔖	🔍	data.win.eventdata.detection User	DESKTOP-2UVD6VP\\Laptop Valley
🔍	🔍	📄	🔖	🔍	data.win.eventdata.engine Version	AM: 1.1.25050.6, NIS: 1.1.25050.6
🔍	🔍	📄	🔖	🔍	data.win.eventdata.error Code	0x00000000

data.win.e	data.win.eventdata.origin Name	4
data.win.eventdata.origin Name	Internet	
data.win.eventdata.path	file:_C:\Users\Laptop Valley\Downloads\f98d7197ef78ba5c70dc5da3a4ba5a74e1195ff50be60bcb2599836554b27e4f.zip; webfile:_C:\Users\Laptop Valley\Downloads\f98d7197ef78ba5c70dc5da3a4ba5a74e1195ff50be60bcb2599836554b27e4f.zip https://bazaar.abuse.ch/download/9195dfe4f2048be1fa20/pid:4976,ProcessStart:133975178450990168	
data.win.system.message	timestamp per 10 minutes > "Microsoft Defender Antivirus has detected malware or other potentially unwanted software. For more information please see the following: <a href="https://go.microsoft.com/fwlink/?linkid=37020&amp;name=Trojan:Script/Wacatac.B!ml&amp;threatid=2147735503&amp;enterprise=0">https://go.microsoft.com/fwlink/?linkid=37020&amp;name=Trojan:Script/Wacatac.B!ml&amp;threatid=2147735503&amp;enterprise=0</a> Name: Trojan:Script/Wacatac.B!ml TD: 2147735503	
decoder.name	windows_eventchannel	
id	1753043552.1622733	
input.type	log	
location	EventChannel	
manager.name	wazuh-server	
rule.description	Windows Defender: Antimalware platform detected potentially unwanted software ()	

THE END