



# wazuh.

## **Wazuh – Windows Defender**

### **Windows Defender Logs Integration**

**Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY**

**Follow Me: [linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)**

## Integrating Windows Defender logs

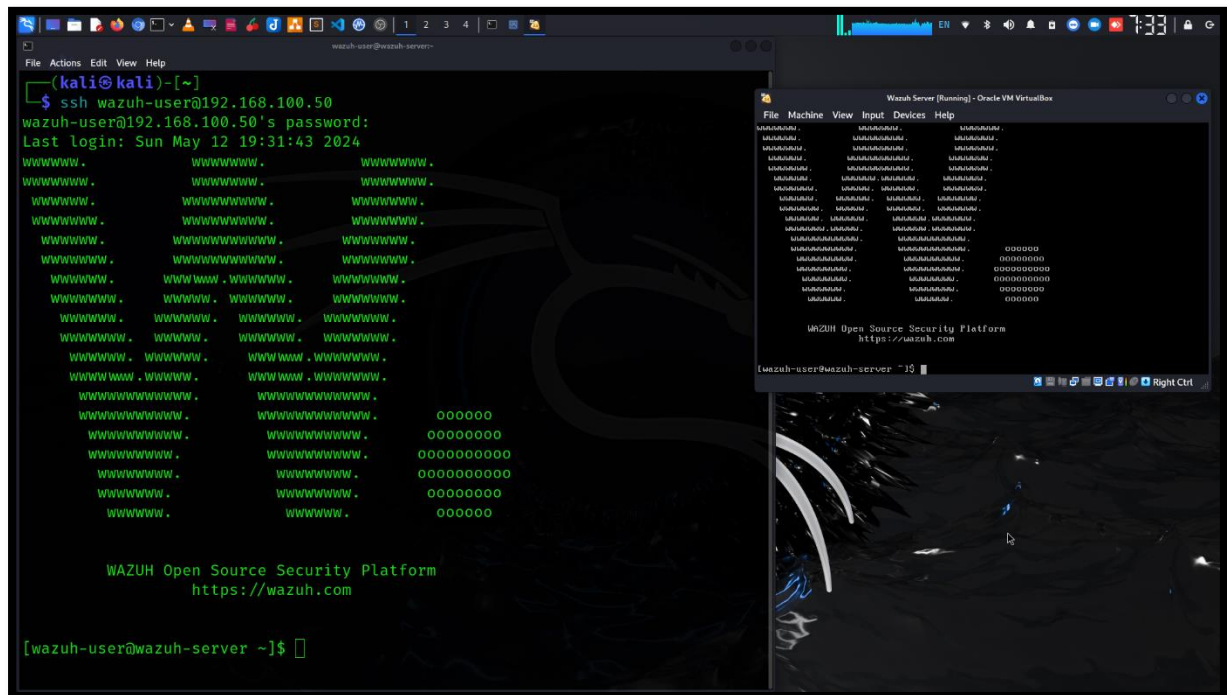
Windows Defender is an antivirus software module of Microsoft Windows. As per the *2023 Antivirus Market Report*, Windows Defender is the most common free antivirus product for PC users, with around 40% of the market share of free antivirus software. For more information on this, you can check the following link: <https://www.security.org/antivirus/antivirus-consumer-report-annual/>.

Additionally, Microsoft also offers endpoint security solutions for enterprises called Windows Defender for Endpoint. This makes us put more attention on integrating Windows Defender with Wazuh. By default, Wazuh cannot read the Windows Defender logs. Hence, it is important for us to put extra effort into making it possible.

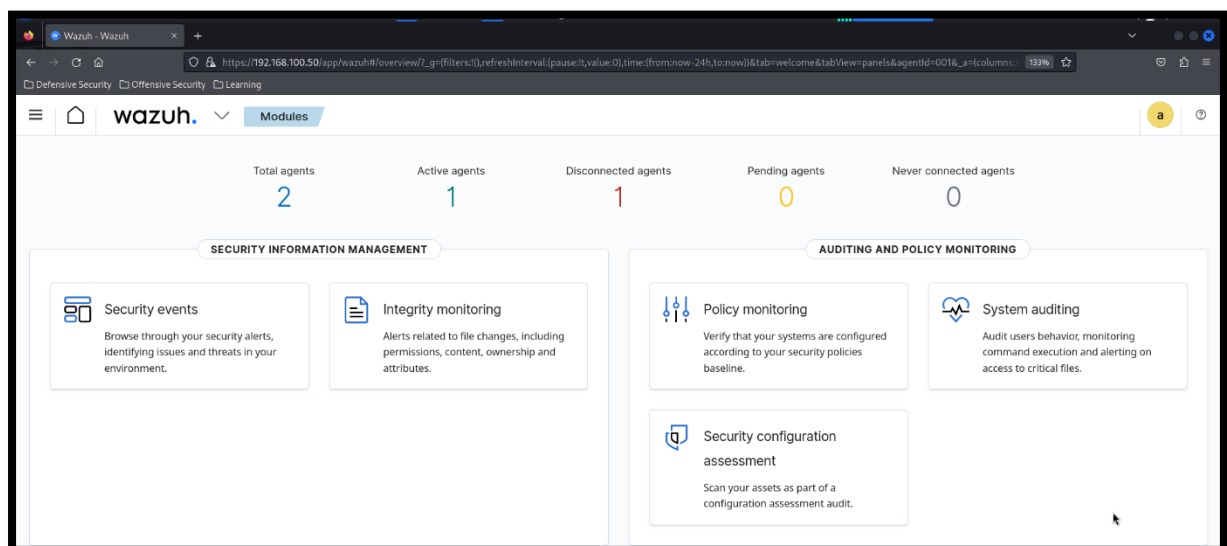
**Understand Windows Defender Logs:** Before setting up the integration, it's essential to understand the types of logs generated by Windows Defender. Windows Defender logs contain valuable information about security events such as malware detections, system scans, and updates.

**Windows Defender** logs help SOC analysts understand the security status of endpoints, identify potential cyber threats, and also help them investigate any security incidents. Windows Defender logs encompass several pieces of information such as scan activities, threat detection, updates, quarantine, remediation, firewall and network activities, and real-time protection.

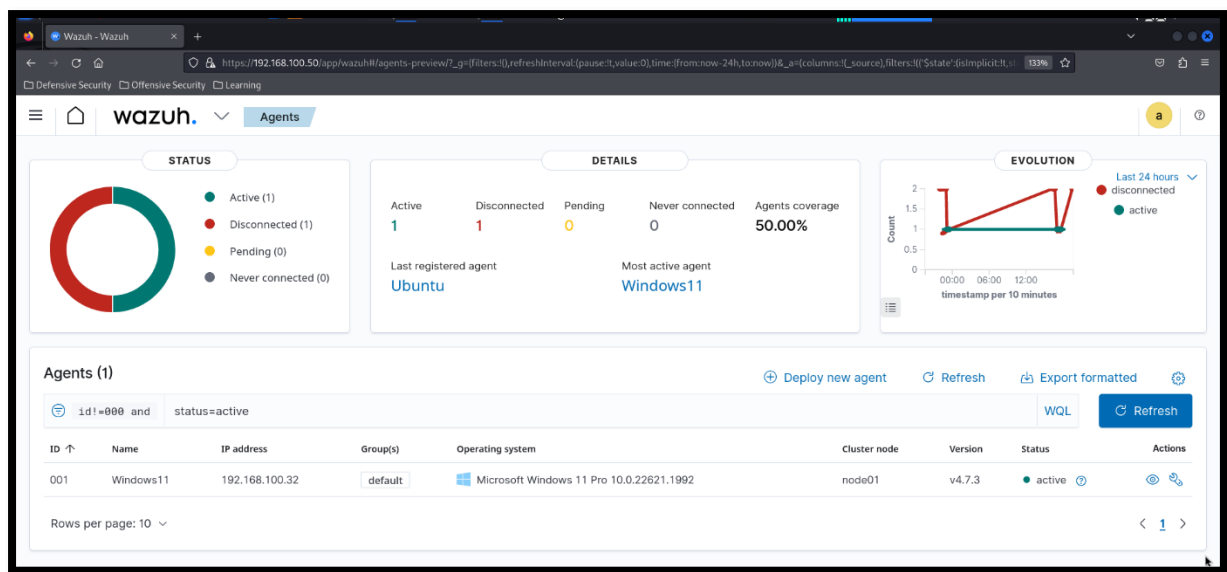
Here is Wazuh Server running on my lab environment. I access Wazuh console via SSH connection.



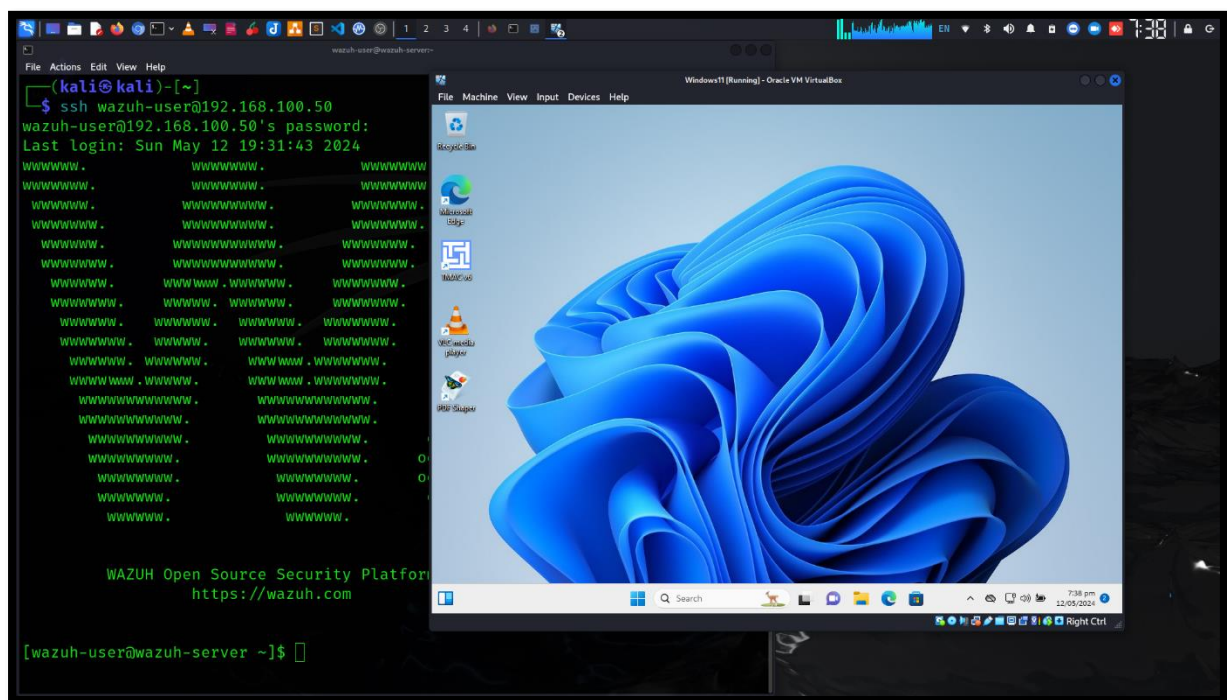
Here is Wazuh Server dashboard.



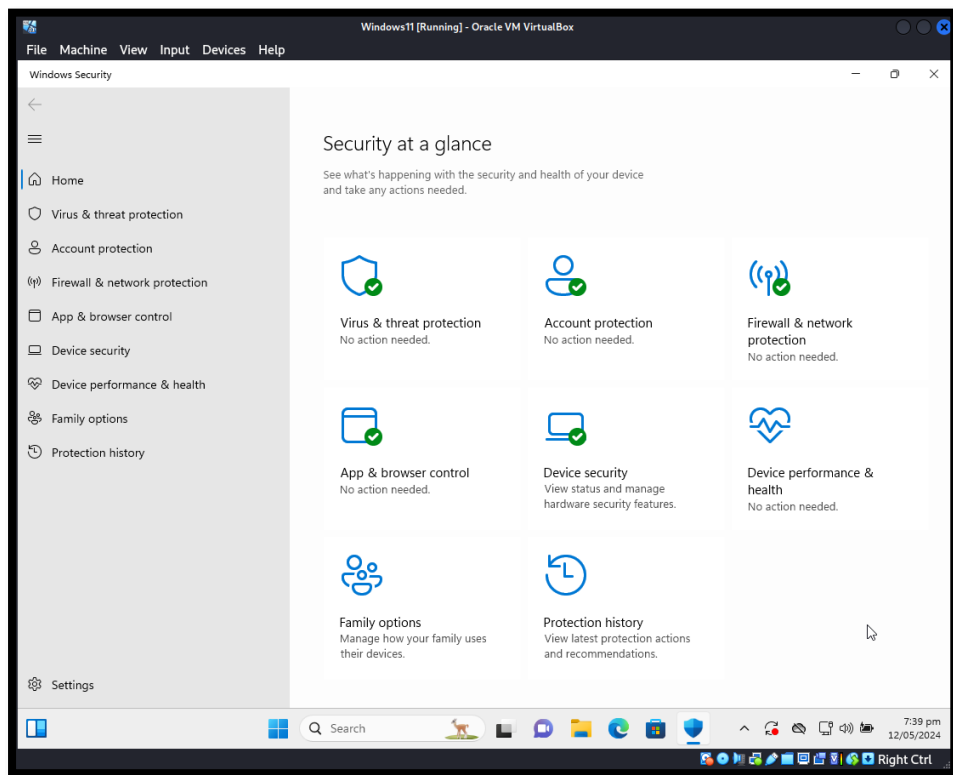
### Selecting the Active agent (Windows 11)



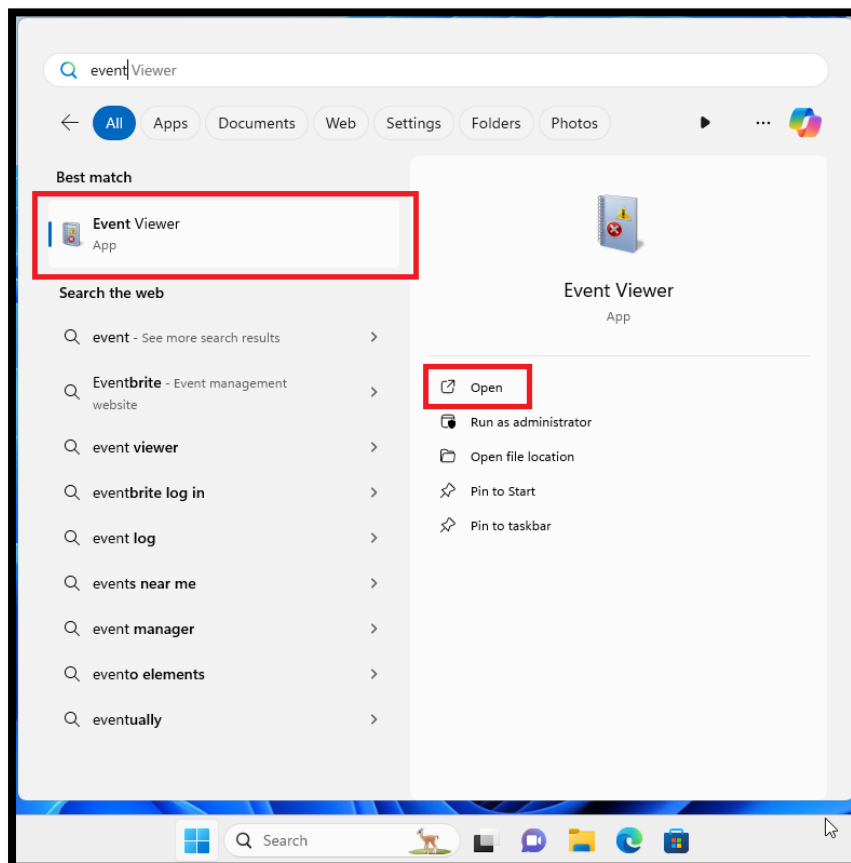
Here is Windows 11 is running in VirtualBox



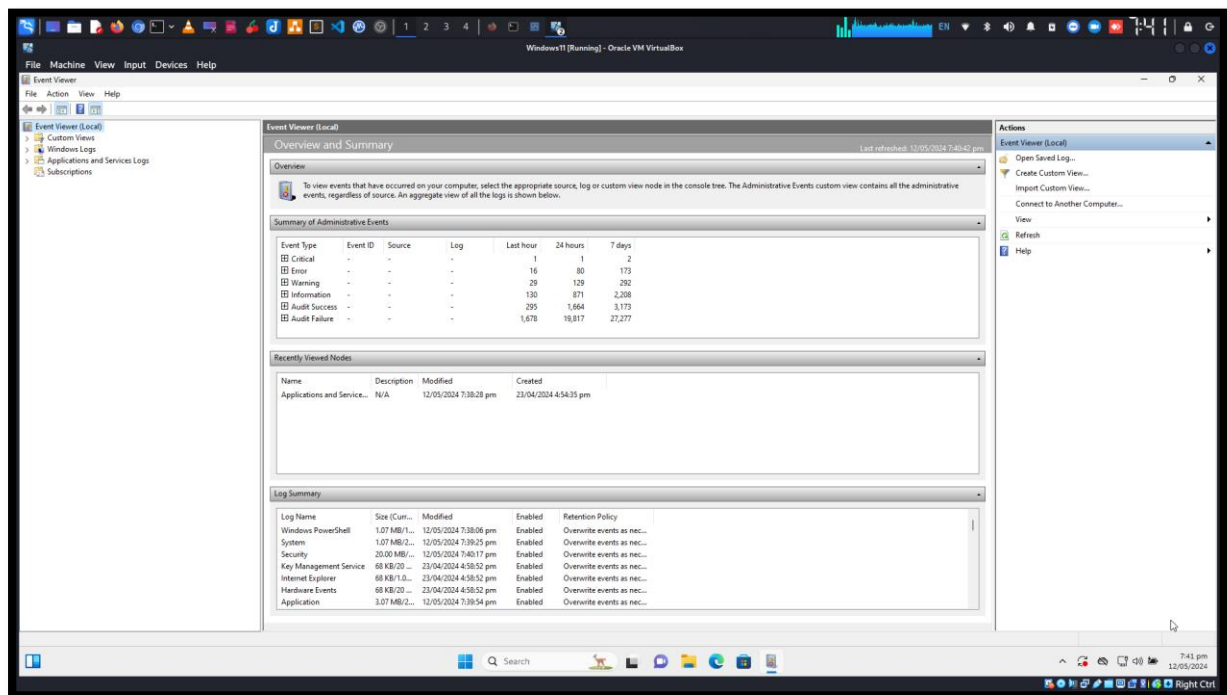
Windows Defender or real-time protection is ON and running actively.



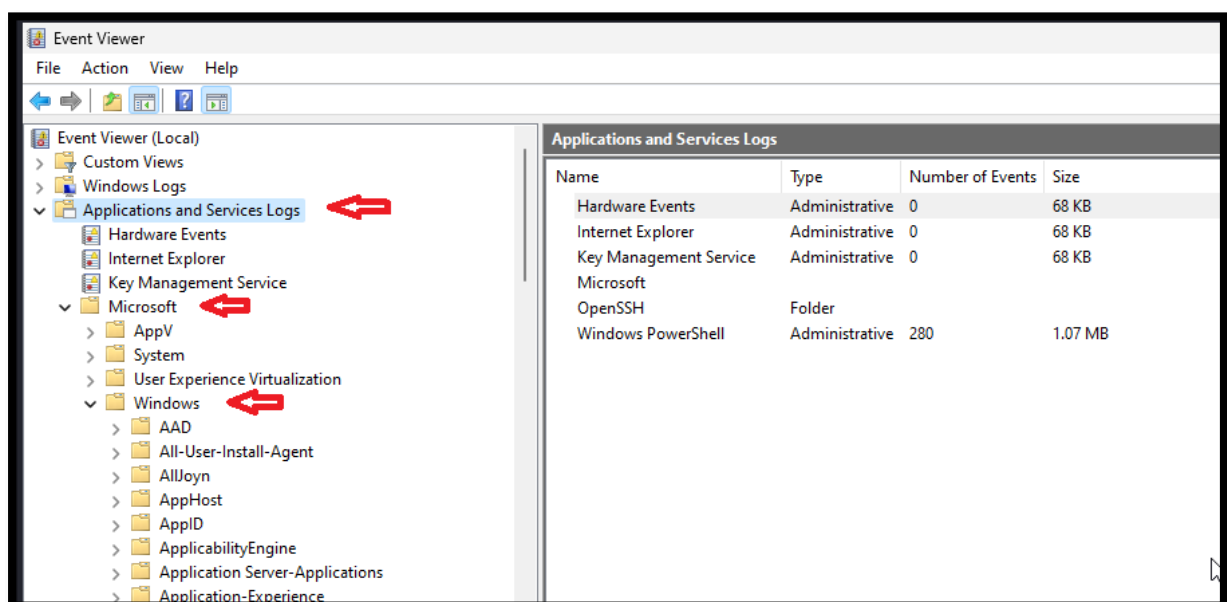
Now go to “Event Viewer” and open it.



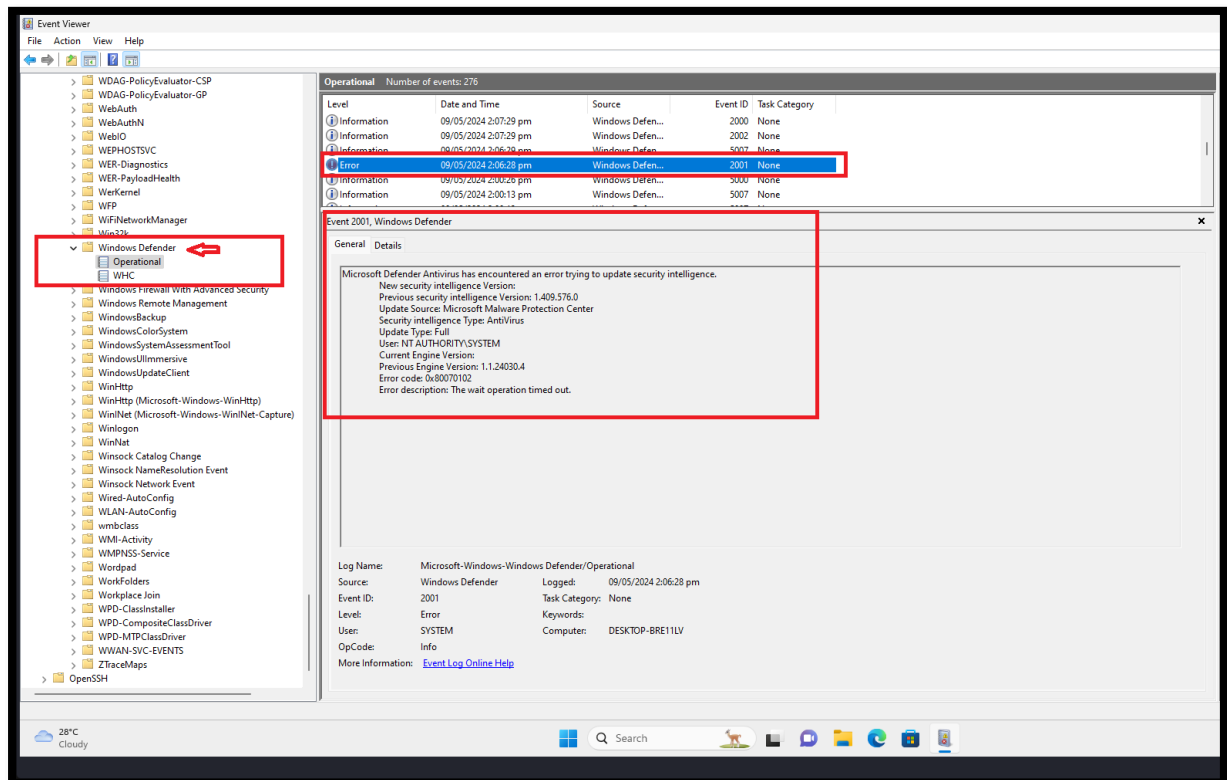
Here is windows “Event Viewer”



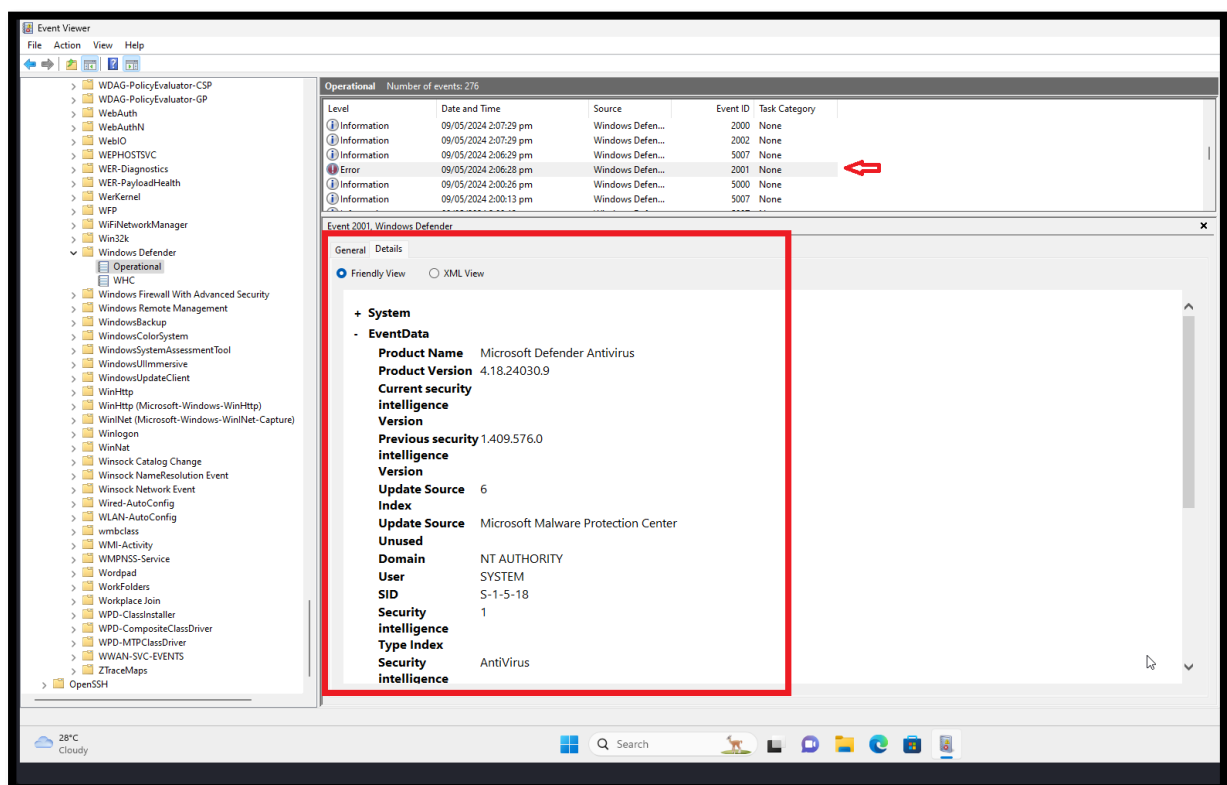
Now go to “Application and Services Logs” > “Microsoft” > “Windows”.



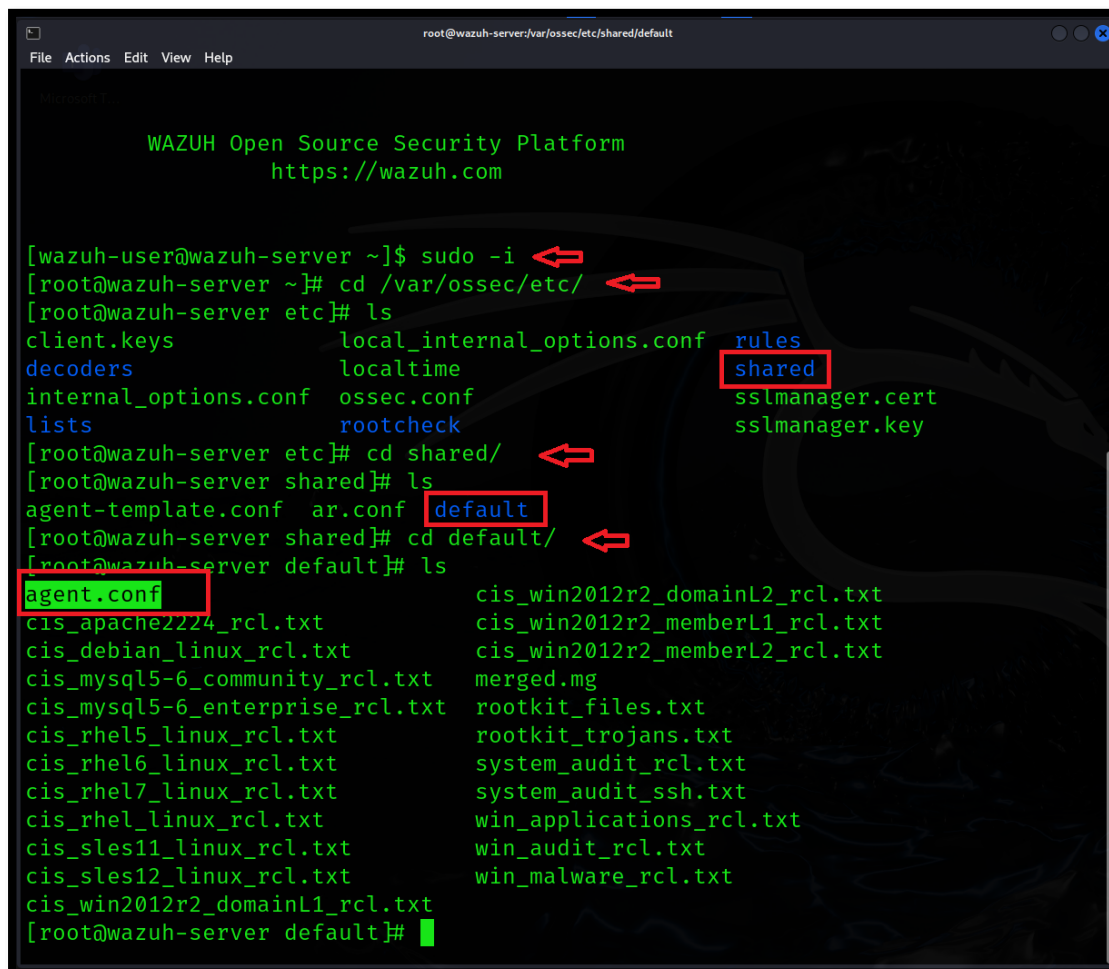
Scroll down little and click on “Windows Defender” > “Operational”. Here you can see “Error” logs and details.



Click on “Details”



Now we have to add configuration in “agent.conf” file. Follow same as shown in figure.

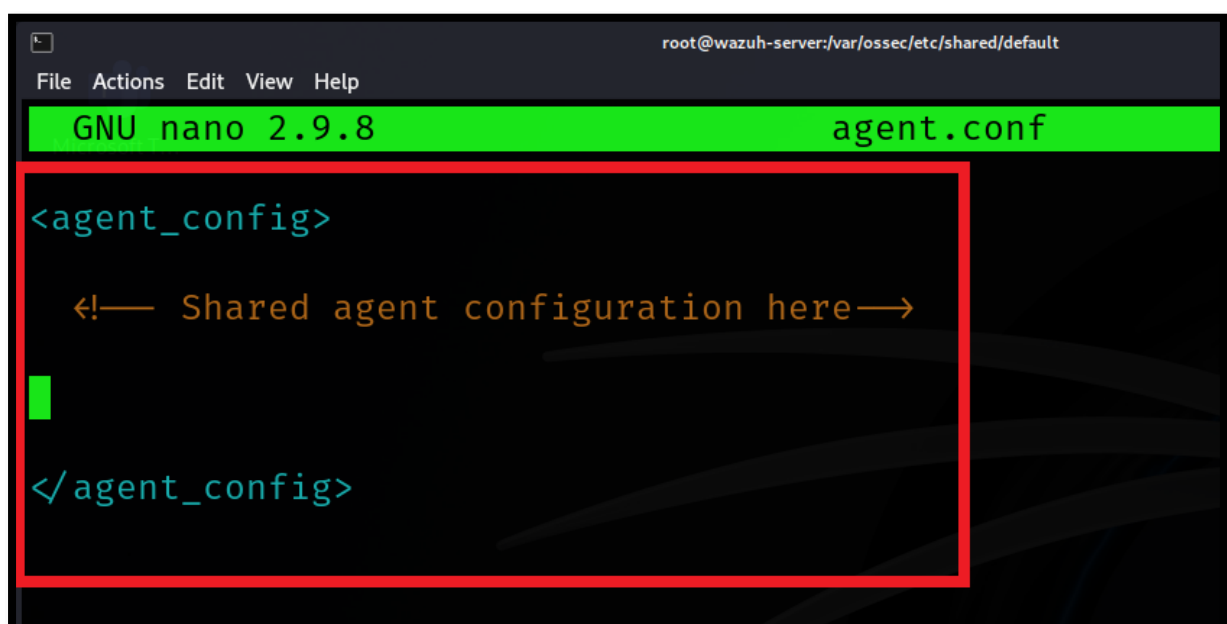


```
root@wazuh-server:/var/ossec/etc/shared/default
File Actions Edit View Help

WAZUH Open Source Security Platform
https://wazuh.com

[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /var/ossec/etc/
[root@wazuh-server etc]# ls
client.keys          local_internal_options.conf  rules
decoders             localtime                   shared
internal_options.conf ossec.conf                  sslmanager.cert
lists               rootcheck                   sslmanager.key
[root@wazuh-server etc]# cd shared/
[root@wazuh-server shared]# ls
agent-template.conf  ar.conf  default
[root@wazuh-server shared]# cd default/
[root@wazuh-server default]# ls
agent.conf          cis_win2012r2_domainL2_rcl.txt
cis_apache2224_rcl.txt  cis_win2012r2_memberL1_rcl.txt
cis_debian_linux_rcl.txt  cis_win2012r2_memberL2_rcl.txt
cis_mysql5-6_community_rcl.txt  merged.mg
cis_mysql5-6_enterprise_rcl.txt  rootkit_files.txt
cis_rhel5_linux_rcl.txt          rootkit_trojans.txt
cis_rhel6_linux_rcl.txt          system_audit_rcl.txt
cis_rhel7_linux_rcl.txt          system_audit_ssh.txt
cis_rhel_linux_rcl.txt           win_applications_rcl.txt
cis_sles11_linux_rcl.txt         win_audit_rcl.txt
cis_sles12_linux_rcl.txt         win_malware_rcl.txt
cis_win2012r2_domainL1_rcl.txt
[root@wazuh-server default]#
```

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



```
root@wazuh-server:/var/ossec/etc/shared/default
File Actions Edit View Help

GNU nano 2.9.8 agent.conf

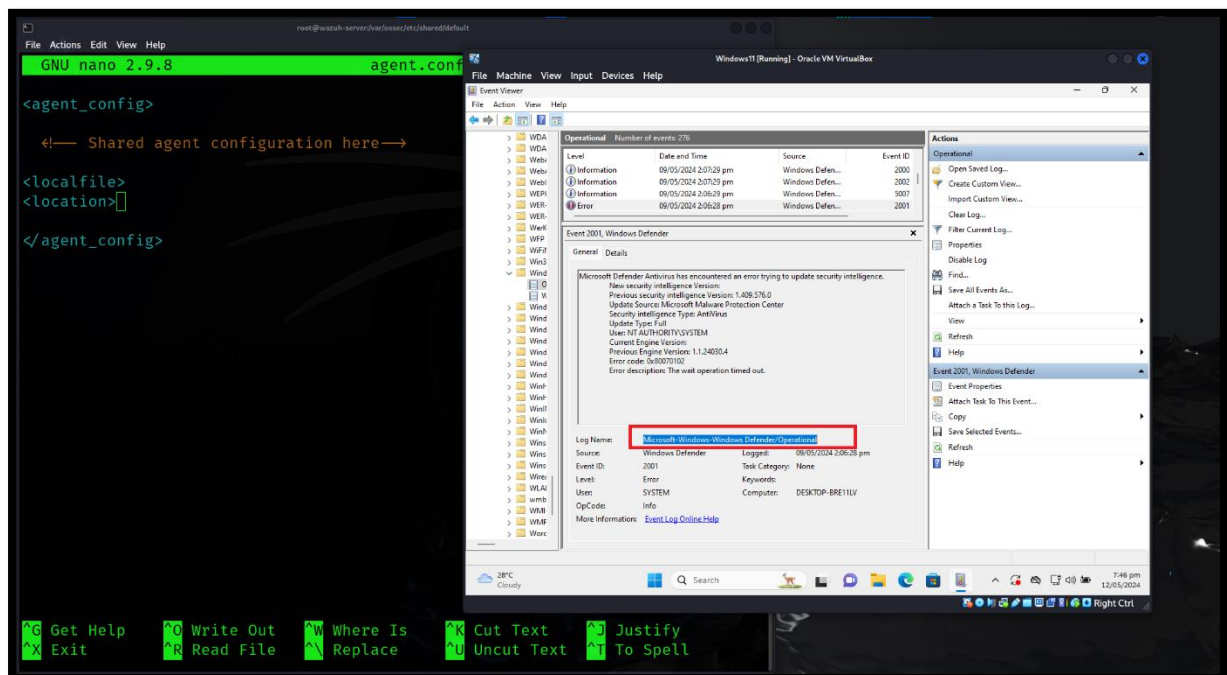
<agent_config>

  <!-- Shared agent configuration here -->

</agent_config>
```

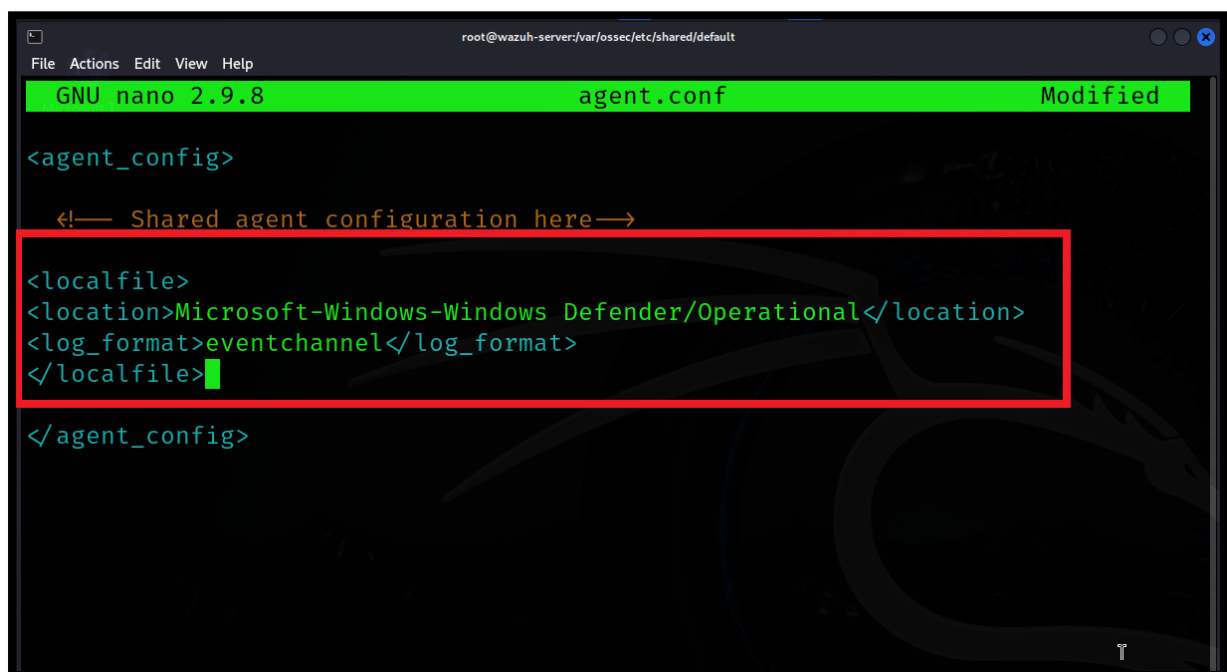


Here is the configuration and the path of “Windows Defender” logs. Copy it and follow the same shown in figure.



Here is the full configuration:

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



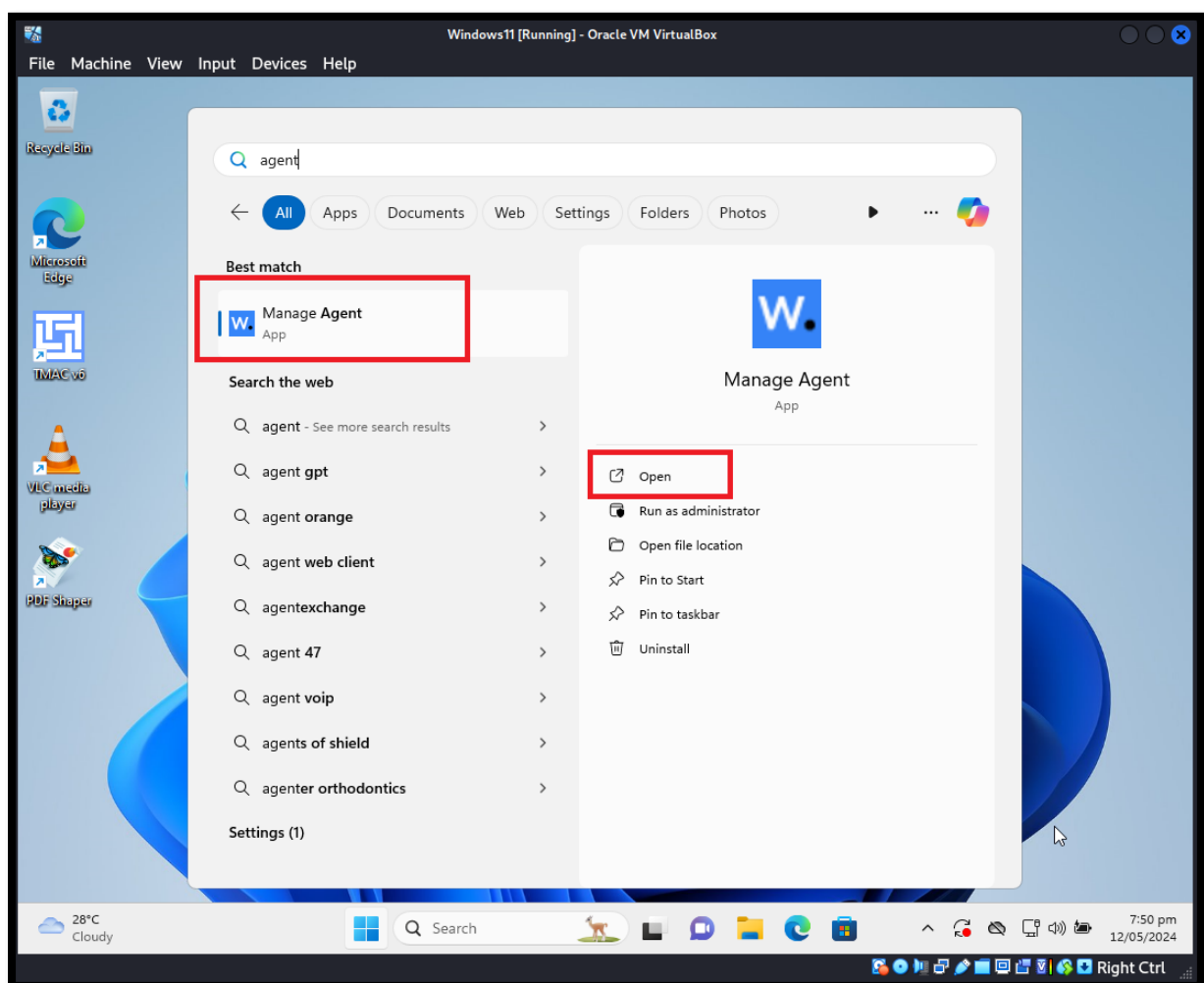
Now save the configuration and restart wazuh-manager.

Command: systemctl restart Wazuh-manager

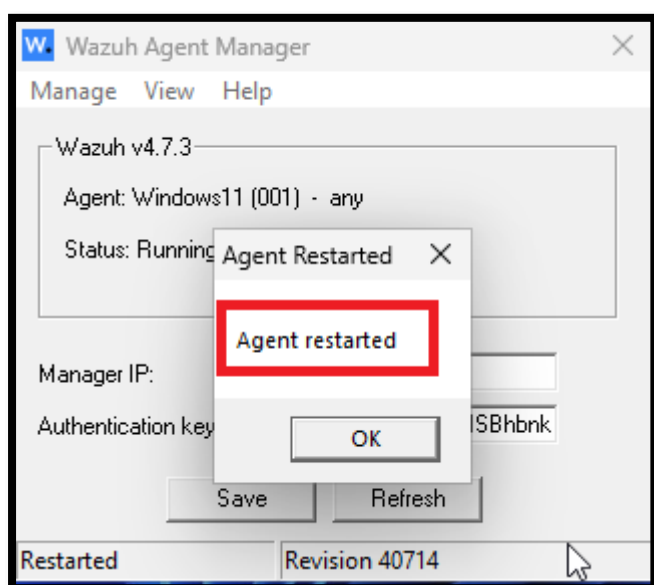
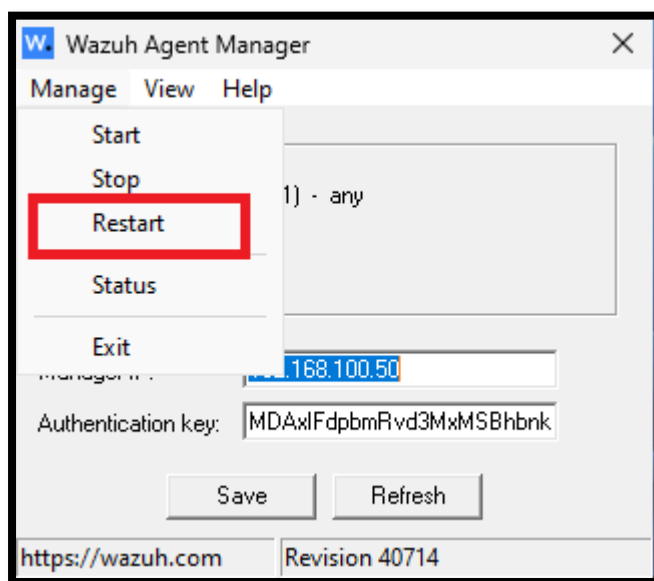
```
[root@wazuh-server default]# sudo nano agent.conf
[root@wazuh-server default]# sudo nano agent.conf
[root@wazuh-server default]# systemctl restart wazuh-manager

[root@wazuh-server default]#
[root@wazuh-server default]#
[root@wazuh-server default]#
```

Now go to “Windows 11” and restart “Wazuh-agent”.



Restarting wazuh-agent.



After restarted the wazuh-agent we have to download some malicious files form internet I am going to turn off windows real-time protection to allow download malicious file or malware into my "Windows 11" machine.

Now go to “Security events” tab after selection the “Windows11” agent.

The screenshot shows the Wazuh dashboard interface. The 'Security events' tab is selected and highlighted with a red box. The dashboard displays the following information:

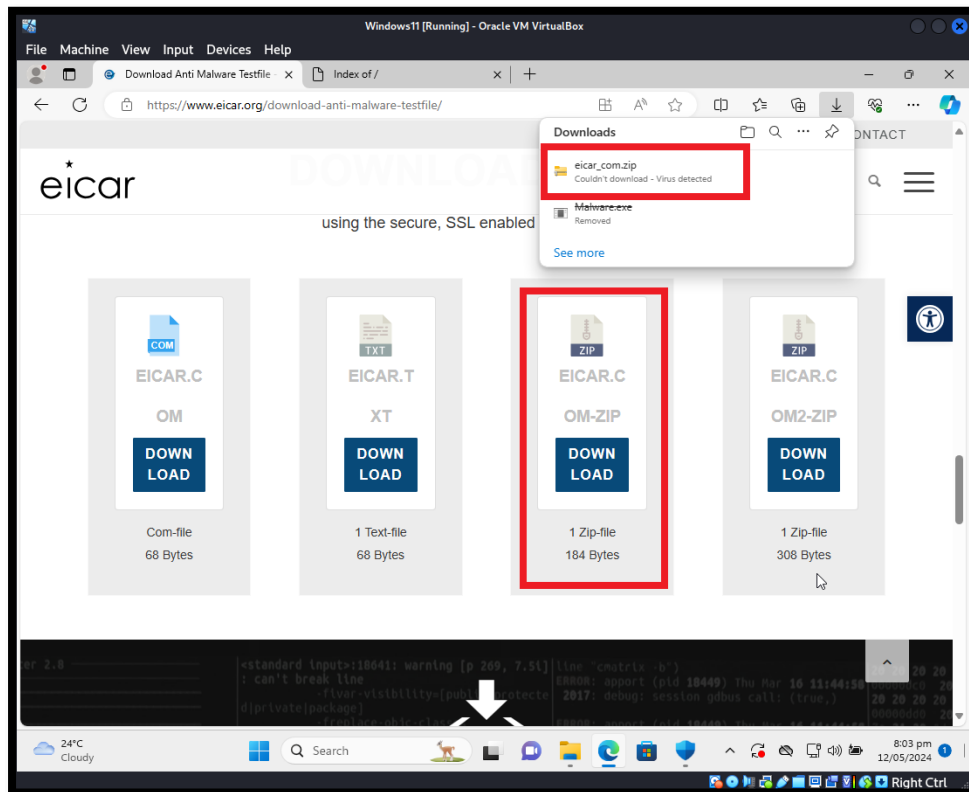
- Agent Information:** ID 001, Status active, IP address 192.168.100.32, Version Wazuh v4.7.3, Groups default, Operating system Microsoft Windows 11, Cluster node node01, Registration date May 9, 2024 @ 14:37:24.000, Last keep alive May 12, 2024 @ 19:52:17.000.
- MITRE Top Tactics:** Defense Evasion (29811), Initial Access (29790), Persistence (29790), Privilege Escalation (29790), Execution (35).
- Compliance:** A donut chart showing compliance status for PCI DSS, with a score of 10.2.2 (29611).
- FIM: Recent events:** A table listing recent File Integrity Monitoring events, including file deletions and additions.

The screenshot shows the Wazuh dashboard interface, specifically the 'Security events' tab for the 'Windows11' agent. The dashboard displays the following information:

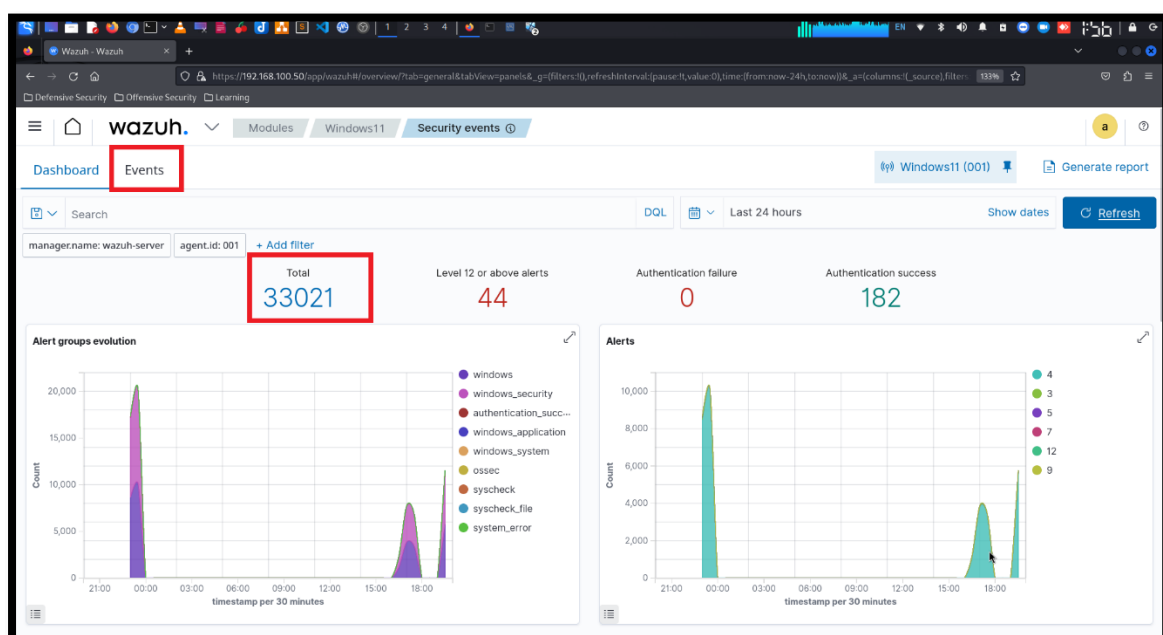
- Alert Statistics:** Total 30048, Level 12 or above alerts 36, Authentication failure 0, Authentication success 179.
- Alert groups evolution:** A line chart showing the count of alert groups over time, with a peak around 00:00.
- Alerts:** A line chart showing the count of alerts over time, with a peak around 00:00.

Downloading Malware files form: <https://www.eicar.org/download-anti-malware-testfile/>

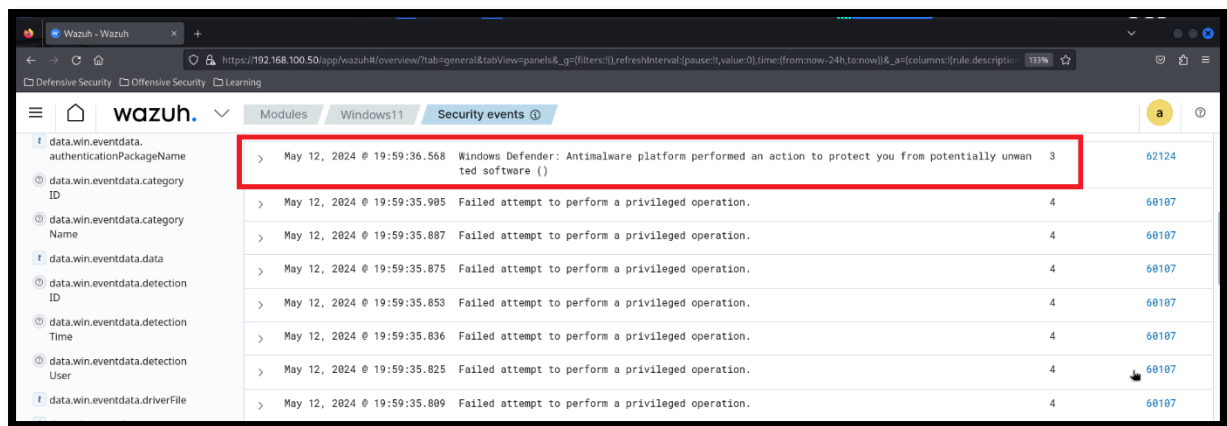
Also, we can test our “Malware.exe” or other malwares as well. Try it by your own. After download the malware file in turned on Windows real-time protection.



Now go to “Events” tab.



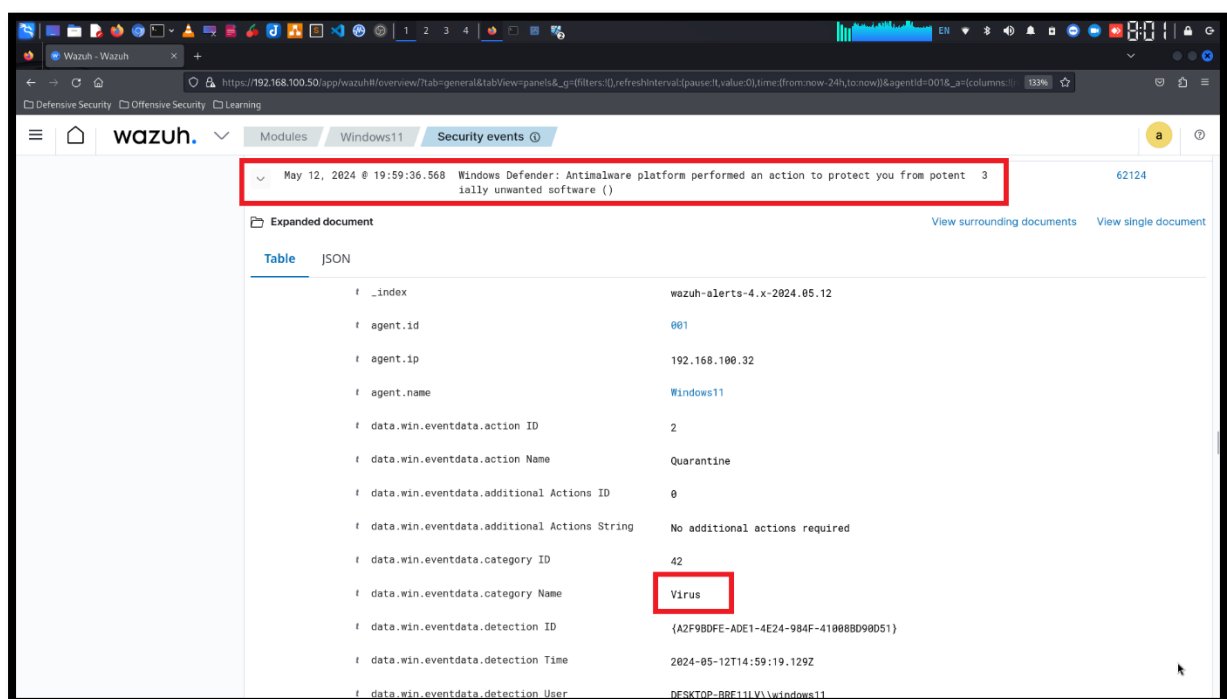
Here you can see windows defender antivirus or real-time protection blocked or remove malware file. And generate logs and send the logs details to Wazuh Server.



The screenshot shows the Wazuh Security events page. The first event is highlighted with a red box. The event details are as follows:

Timestamp	Event Description	Score	Alert ID
May 12, 2024 @ 19:59:36.568	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ( )	3	62124
May 12, 2024 @ 19:59:35.985	Failed attempt to perform a privileged operation.	4	60107
May 12, 2024 @ 19:59:35.887	Failed attempt to perform a privileged operation.	4	60107
May 12, 2024 @ 19:59:35.875	Failed attempt to perform a privileged operation.	4	60107
May 12, 2024 @ 19:59:35.853	Failed attempt to perform a privileged operation.	4	60107
May 12, 2024 @ 19:59:35.836	Failed attempt to perform a privileged operation.	4	60107
May 12, 2024 @ 19:59:35.825	Failed attempt to perform a privileged operation.	4	60107
May 12, 2024 @ 19:59:35.809	Failed attempt to perform a privileged operation.	4	60107

Now explore the events and see the details.



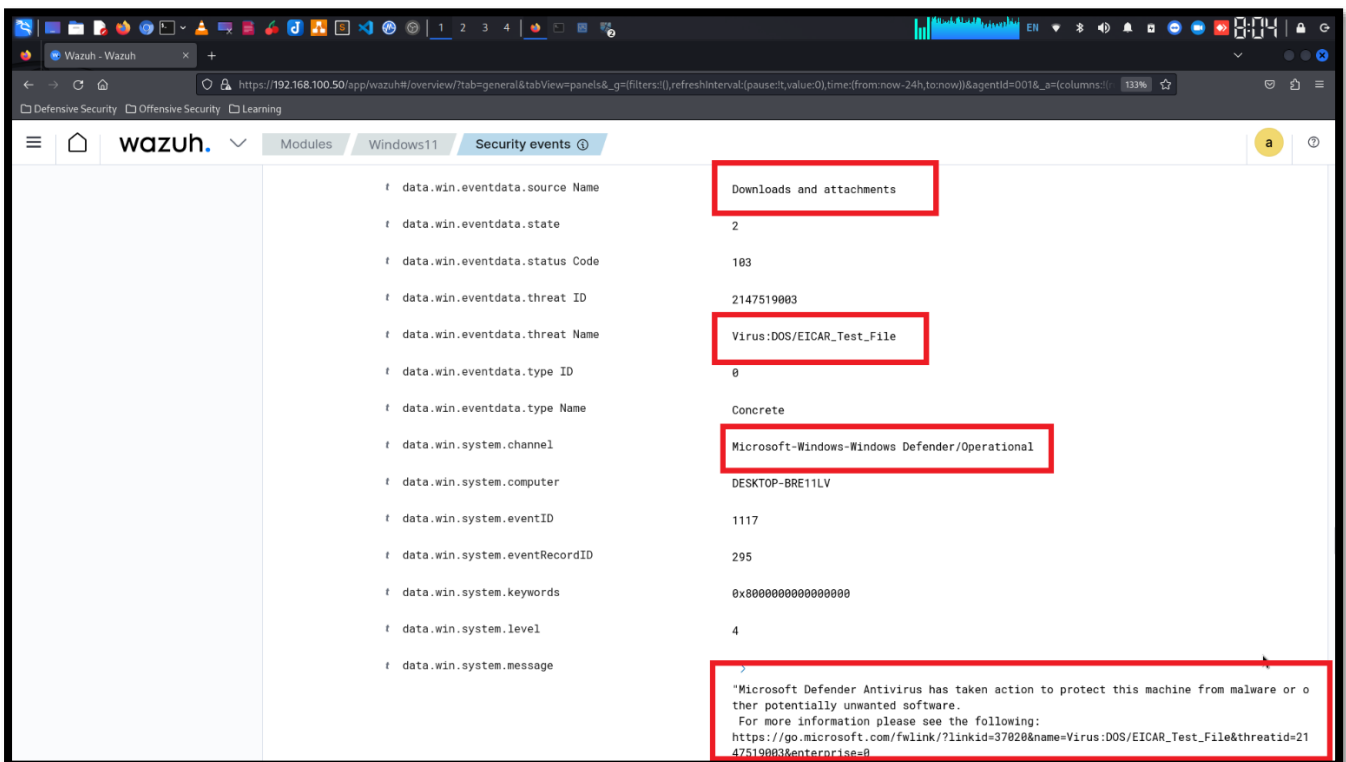
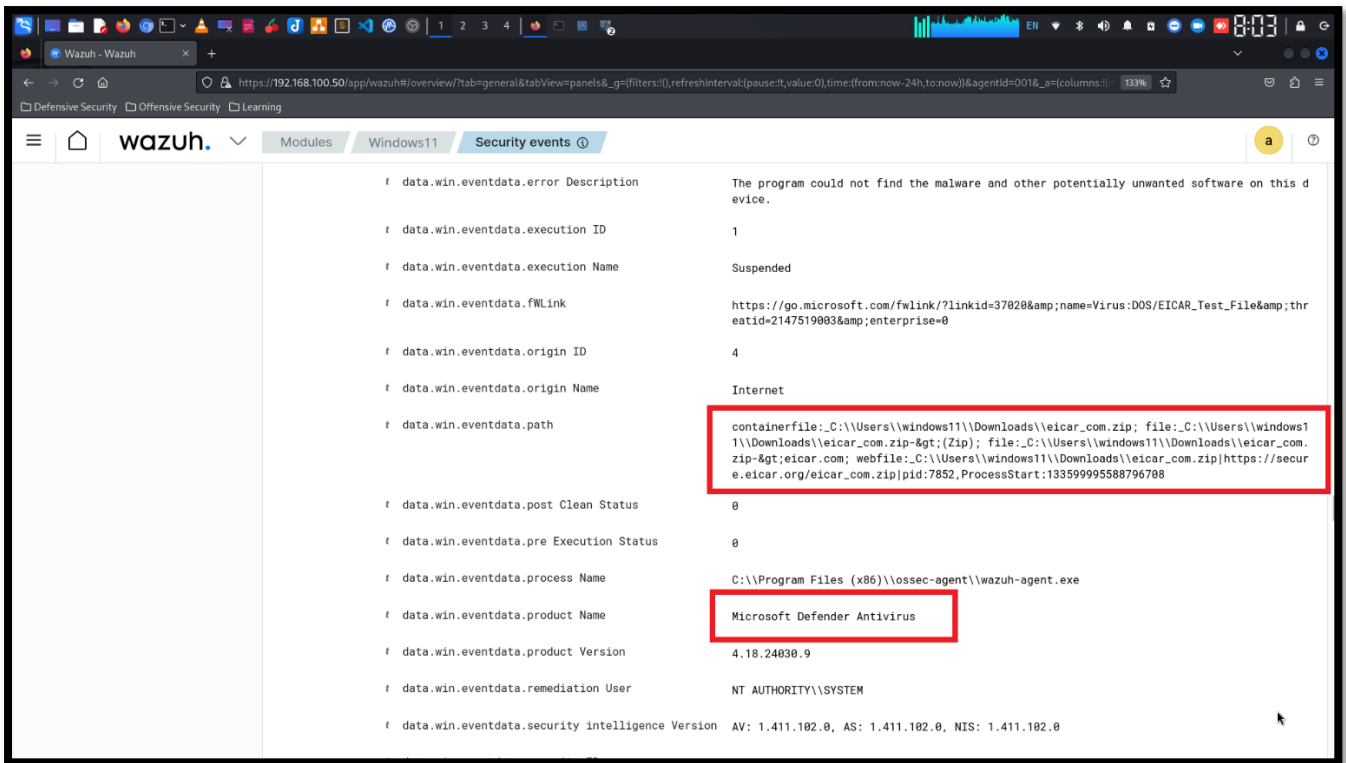
The screenshot shows the Wazuh Security events page with the details of the first event expanded. The event details are as follows:

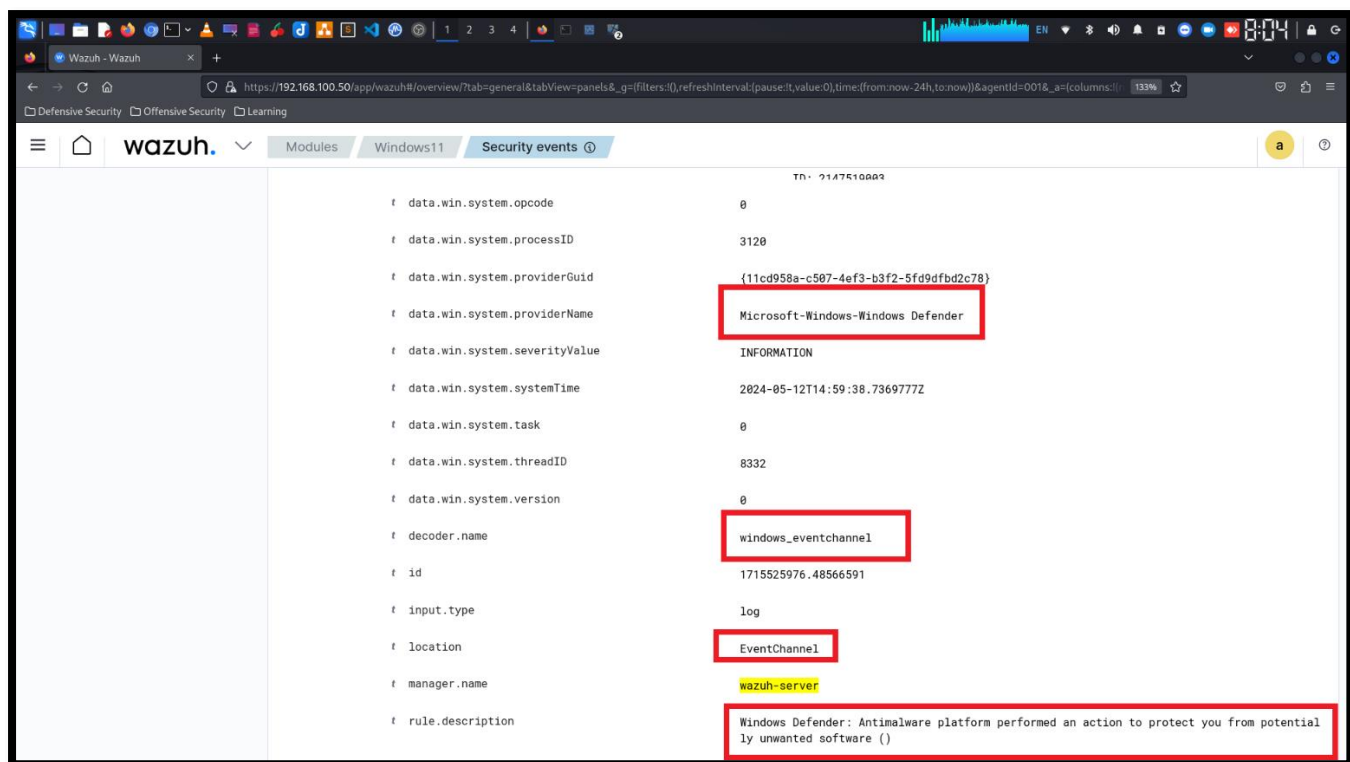
Timestamp	Event Description	Score	Alert ID
May 12, 2024 @ 19:59:36.568	Windows Defender: Antimalware platform performed an action to protect you from potentially unwanted software ( )	3	62124

Expanded document

Field	Value
_index	wazuh-alerts-4.x-2024.05.12
agent.id	001
agent.ip	192.168.100.32
agent.name	Windows11
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	{A2F9B0FE-ADE1-4E24-984F-410088D90D51}
data.win.eventdata.detection Time	2024-05-12T14:59:19.129Z
data.win.eventdata.detection User	DESKTOP-BBF1111\Windows11

See the more details in next page.





## SUMMARY

In summary, Sending Windows Defender logs to Wazuh can significantly enhance your security monitoring capabilities. Wazuh, an open-source security monitoring platform, offers centralized log management and real-time analysis, allowing you to efficiently detect and respond to security incidents. By integrating Windows Defender logs into Wazuh, you gain a comprehensive view of your network's security posture. This integration enables you to correlate events from multiple sources, detect threats more effectively, and take timely action to mitigate risks. Additionally, leveraging Wazuh's alerting and reporting functionalities enhances your ability to maintain a secure environment. Overall, sending Windows Defender logs to Wazuh empowers your organization to bolster its defense against cyber threats and ensure the integrity of your IT infrastructure.