

MAC-DONALD ONYEWUCHI EGBUNA

WAZUH ENDPOINT SECURITY MONITORING

ALT/SOE/025/4248

[macdonalde2000@gmail.com](mailto:macdonalde2000@gmail.com)

## Wazuh Manager VM Setup on Windows Host & Endpoint

### Policy Configuration

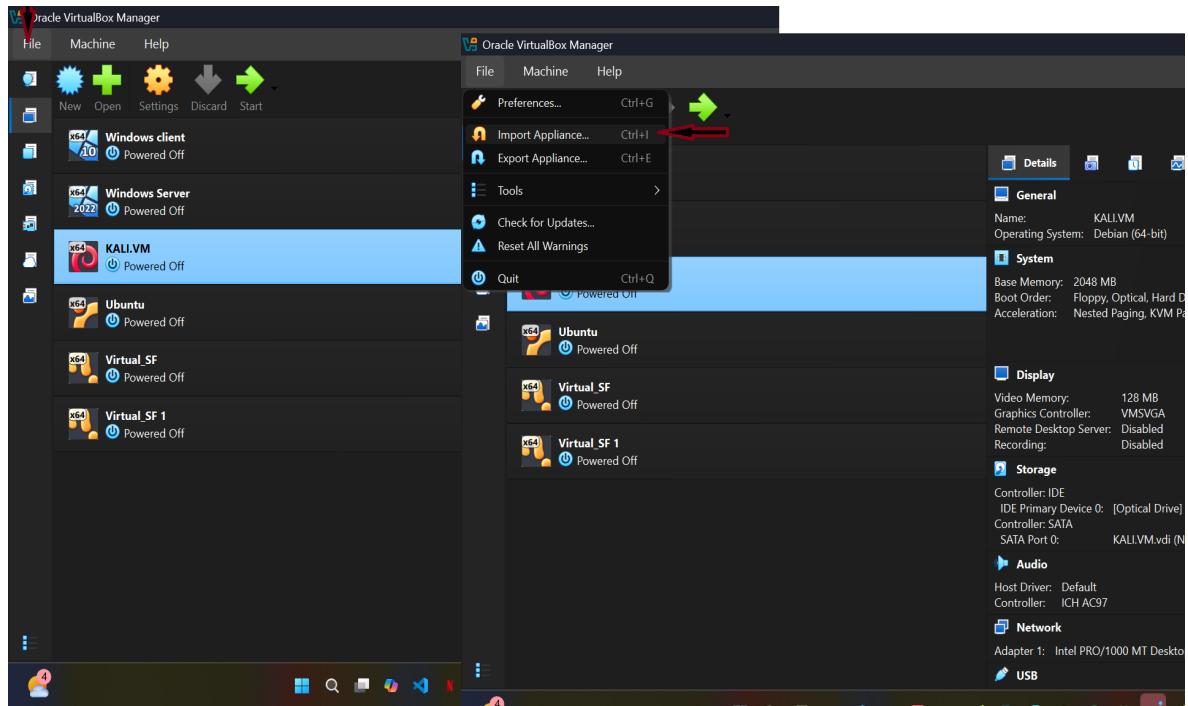
#### Part 1: Initial Setup - Deploying the Wazuh VM

##### 1. Prerequisites and Environment

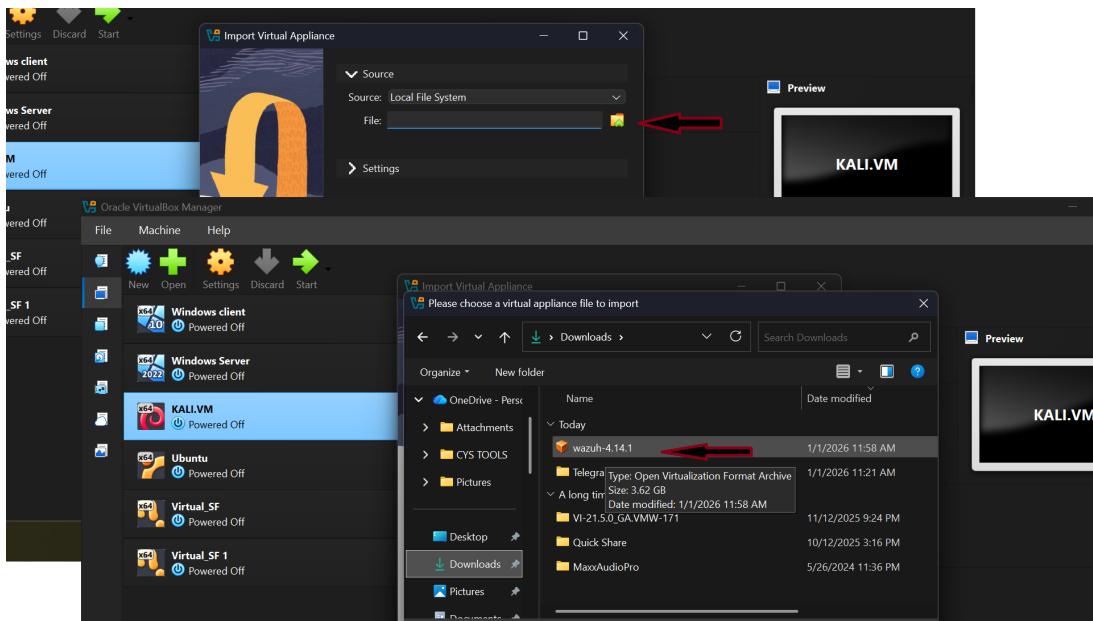
- Host PC: Windows 11 with Hardware Virtualization (VT-x/AMD-V) enabled in the BIOS.
- Software: Oracle VirtualBox installed.
- Appliance: The official Wazuh OVA (Open Virtualization Appliance) file downloaded.

##### 1.1. Importing the Wazuh OVA into VirtualBox

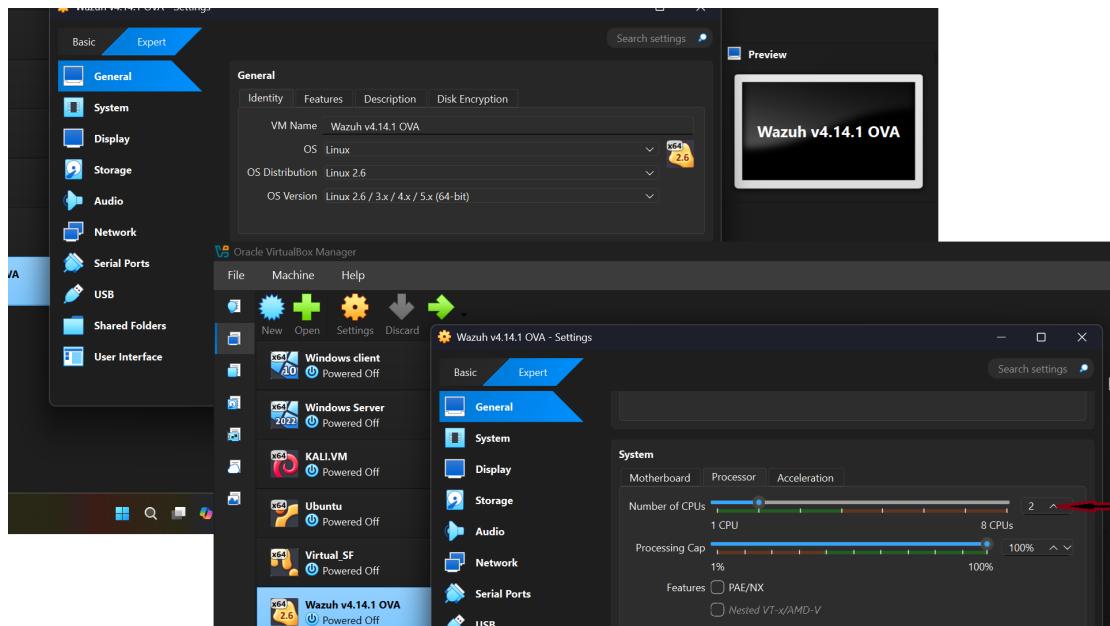
1. Using Oracle VirtualBox
2. Click on - Files -Import Appliance



3. Click the folder icon and select the downloaded Wazuh OVA file.

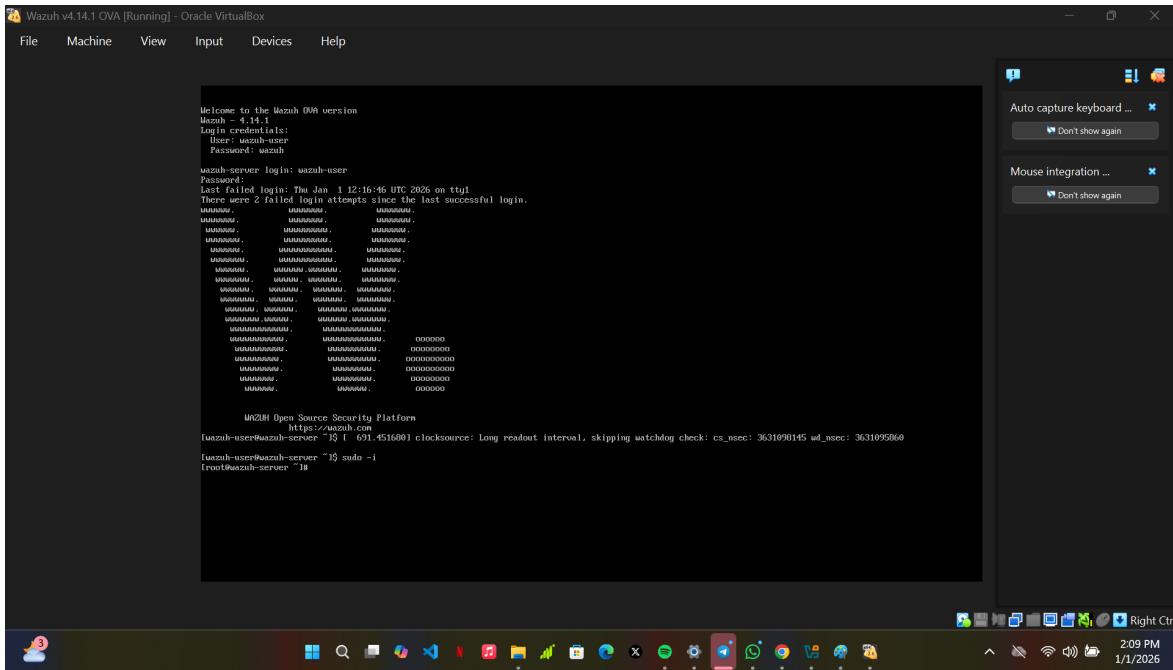


4. Review Settings: Allocate at least 4GB of RAM and 2 CPUs. Adjust the hard disk location if necessary. and Import.

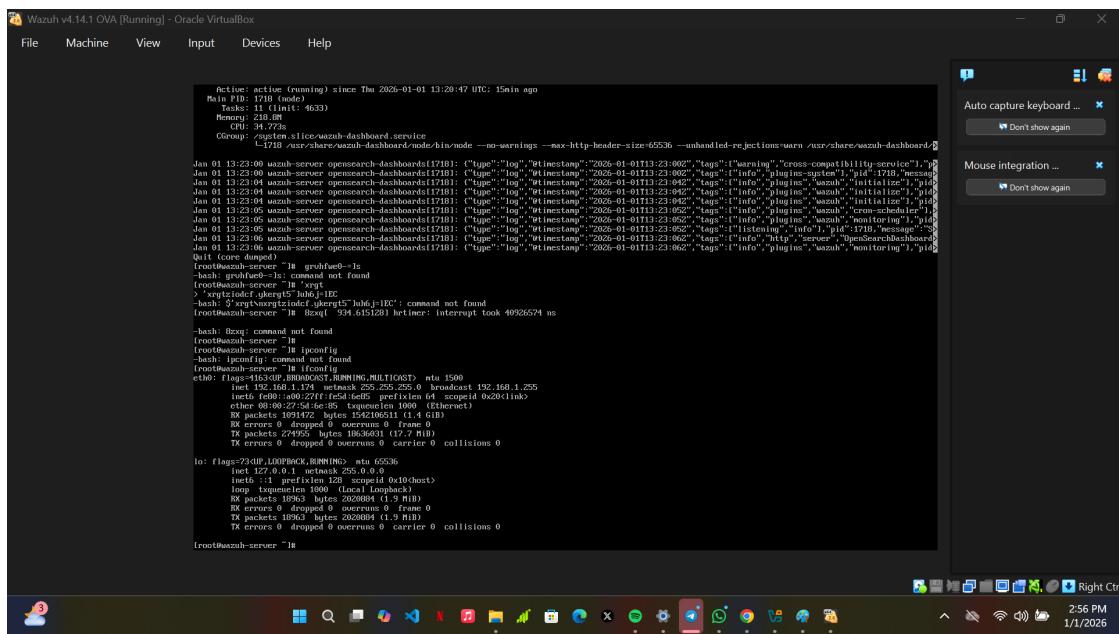


## 1.2. Starting the VM and Retrieving the IP:

1. Start the Wazuh VM. Log in using the default credentials (check the official documentation for the OVA's default login).



2. Using Linux, check for Vm assigned network address using the `ifconfig` command



## Agent Installation on the Windows Endpoint

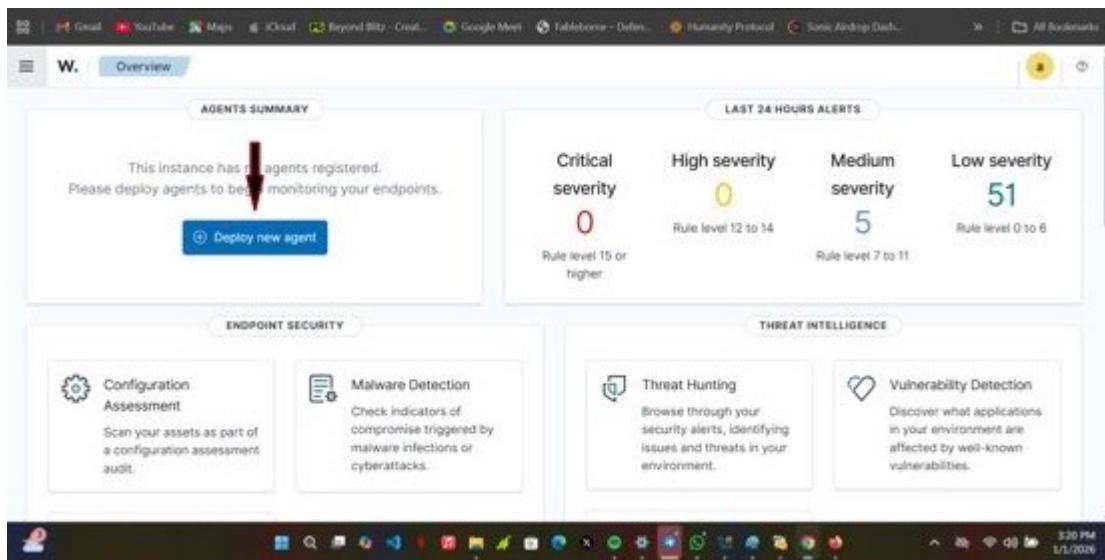
Part 2:

### 2.1: Generating the Deployment Command in the Dashboard

1. Open a web browser on the host pc and navigate to Wazuh Dashboard(<https://192.168.1.178>). Log in

The image shows two screenshots of a web browser displaying the Wazuh dashboard. The top screenshot is a login screen with fields for 'admin' and a password, and a 'Log in' button. The bottom screenshot shows the main 'Overview' page. The 'OVERVIEW' section displays a message: 'This instance has no agents registered. Please deploy agents to begin monitoring your endpoints.' It includes a 'Deploy new agent' button. The 'AGENTS SUMMARY' section shows 0 agents with 'Critical severity' and 0 with 'High severity'. The 'LAST 24 HOURS ALERTS' section shows 0 alerts with 'High severity', 5 with 'Medium severity', and 51 with 'Low severity'. The 'ENDPOINT SECURITY' section includes 'Configuration Assessment' and 'Malware Detection' modules. The 'THREAT INTELLIGENCE' section includes 'Threat Hunting' and 'Vulnerability Detection' modules. The browser's address bar shows the URL <https://192.168.1.178/app/login?nextUrl=%2Fapp%2Fendpoints-summary%2Fagents-preview>.

2. Click "Deploy agent"



This instance has 0 agents registered.  
Please deploy agents to begin monitoring your endpoints.

**LAST 24 HOURS ALERTS**

Severity	Count	Rule level
Critical severity	0	Rule level 12 to 14
High severity	0	Rule level 12 to 14
Medium severity	5	Rule level 7 to 11
Low severity	51	Rule level 0 to 6

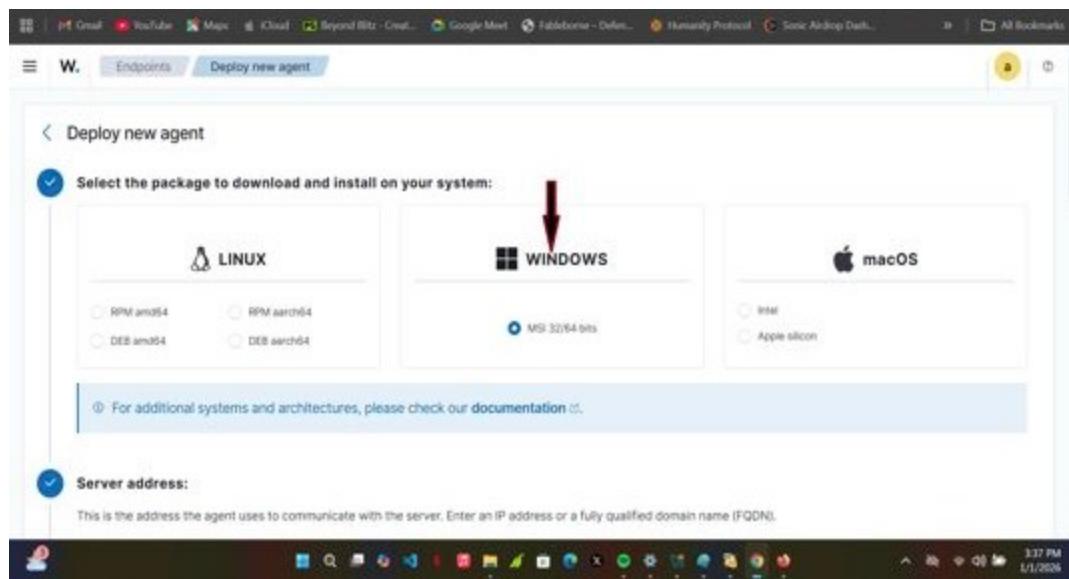
**ENDPOINT SECURITY**

- Configuration Assessment
- Malware Detection

**THREAT INTELLIGENCE**

- Threat Hunting
- Vulnerability Detection

### 3. Select OS of choice (Windows)



Select the package to download and install on your system:

**LINUX**

- RPM/amd64
- DEB/amd64

**WINDOWS**

- MSI 32/64 bits

**macOS**

- Intel
- Apple silicon

For additional systems and architectures, please check our documentation.

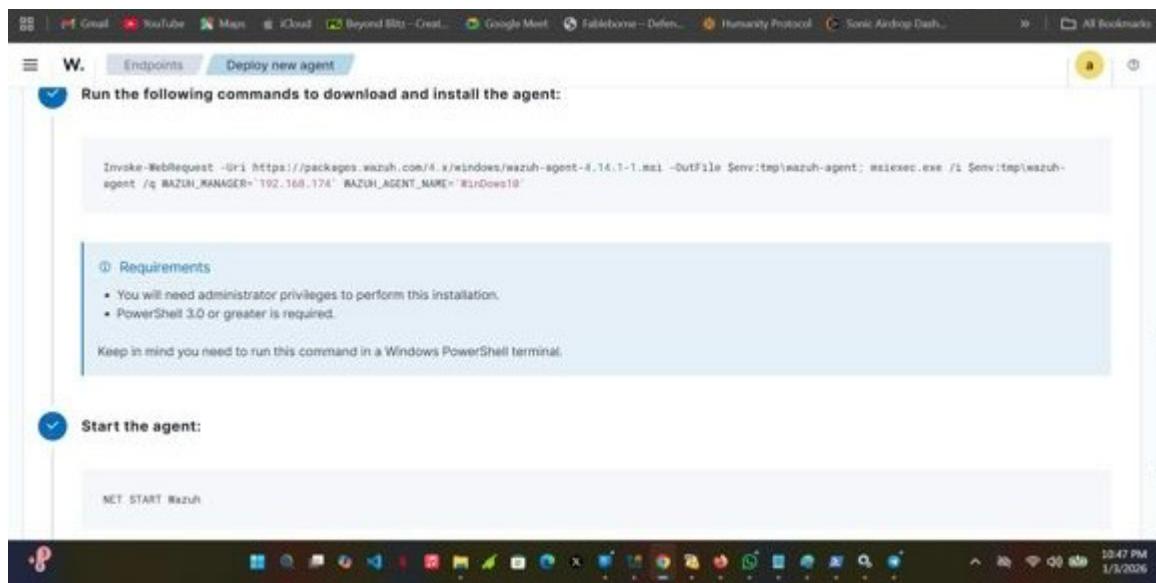
**Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

### 4. Configure the Manager Connection:

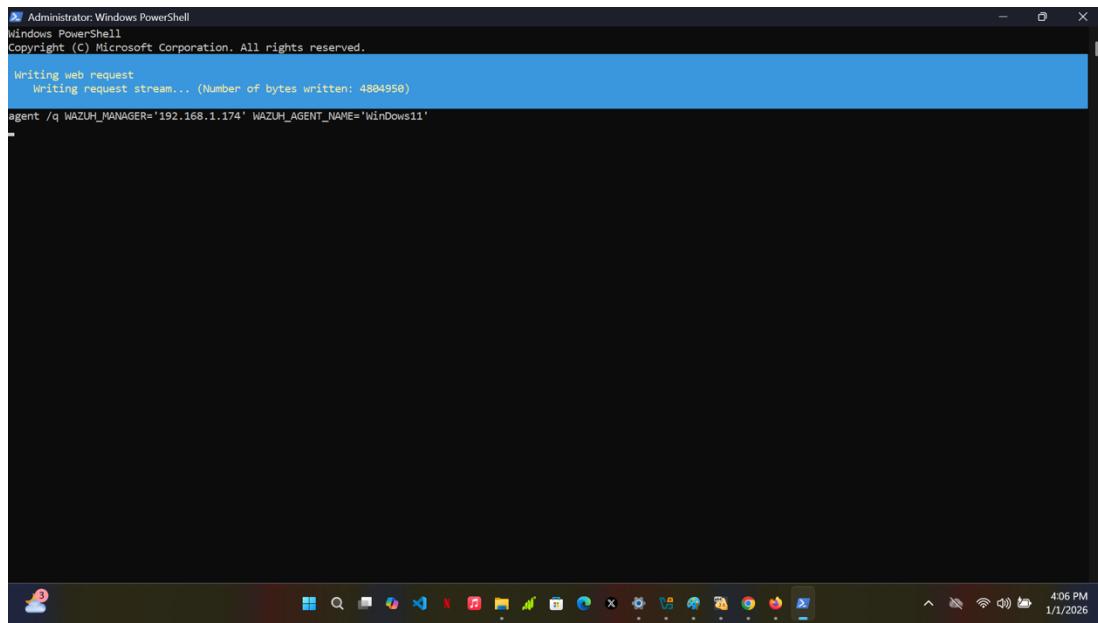
- Target Architecture: Select 64-bit (most common).
- Manager address: (192.168.1.178).

5. Leave existing group at default
6. Copy the command displayed on the dashboard and run on powershell.



## 2.2 Executing the Deployment Command

1. Open Powershell
2. Run as Administrator (crucial)
3. Paste the long command copied from the agent dashboard



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

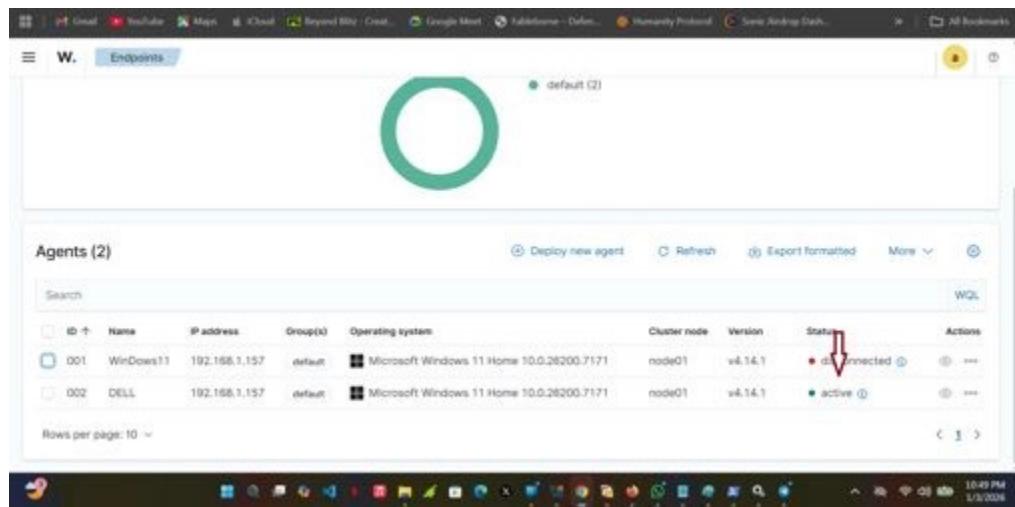
Writing web request
Writing request stream... (Number of bytes written: 4804950)

agent /q WAZUM_MANAGER='192.168.1.174' WAZUM_AGENT_NAME='WinDows11'
```

4. And then copy the next command and start the agent.

### 2.3 Verifying Agent Connection in the Dashboard:

1. Return to Wazuh Dashboard.
2. Go to Modules – Agents.
3. Windows laptop should appear in the list with a green Active status.



ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	WinDows11	192.168.1.157	default	Microsoft Windows 11 Home 10.0.26200.7171	node01	v4.14.1	disconnected	
002	DELL	192.168.1.157	default	Microsoft Windows 11 Home 10.0.26200.7171	node01	v4.14.1	active	

## Policy Configuration - File Integrity

### Monitoring (FIM)

Part 3:

#### 3.1 Configure File Integrity Monitoring (FIM) on Windows Agent

1. On the **Windows Endpoint**, create a unique folder and rename it.
2. Open the **SensitiveData** folder.
3. Inside the folder, create a file to be monitored.
4. Open that monitored text file. To be opened in a **Notepad** window.(type in a random text).  
And close the notepad.
5. Open **ossec.conf** file
  - I. Open **Start Menu** on the endpoint/agent machine (Windows host).
  - II. Search for **Notepad**.
  - III. Right-click the **Notepad** icon and select “Run as Administrator. This opens a **Notepad** window.
  - IV. Click **File >> Open**. This opens the **Open** dialog/window.
  - V. Navigate to the **ossec-agent** folder:  
**C:\Program Files (x86)\ossec-agent\**  
**This PC >> C: (Local Disk) >> Program Files (x86) >> ossec-agent**
  - VI. At the bottom right of the “**Open** window,” the dropdown menu is currently on **Text Documents (\*.txt)**. Click it and select **All files**.
  - VII. This makes all the files in the folder visible.
  - VIII. Find the **ossec.conf** file. Click it.
  - IX. Click the **Open** button. This opens the **ossec.conf** file in a **Notepad** window.
6. Inside Locate the **<syscheck>** block inside the **Notepad** window.
7. Under **<syscheck>** add a directory you want to monitor. For example, for the **SensitiveData** folder, add the following:  
**<directories check\_all="yes" report\_changes="yes" realtime="yes">C:\Users\Administrator\Desktop\SensitiveFolder</directories>**

```

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
  <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

<!-- Security Configuration Assessment -->
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>10m</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring :>
<syscheck>
  <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\INSPIRON\Desktop\Sensitive Folder</directories>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 1 minutes -->
  <frequency>60</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\sysNative</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\sysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\sysNative</directories>

  <!-- 32-bit programs -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe$|reg.exe$|regedit.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\System32\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>

```

- ❖ Modify the **ossec.conf** file to speed up the detection of your file modifications

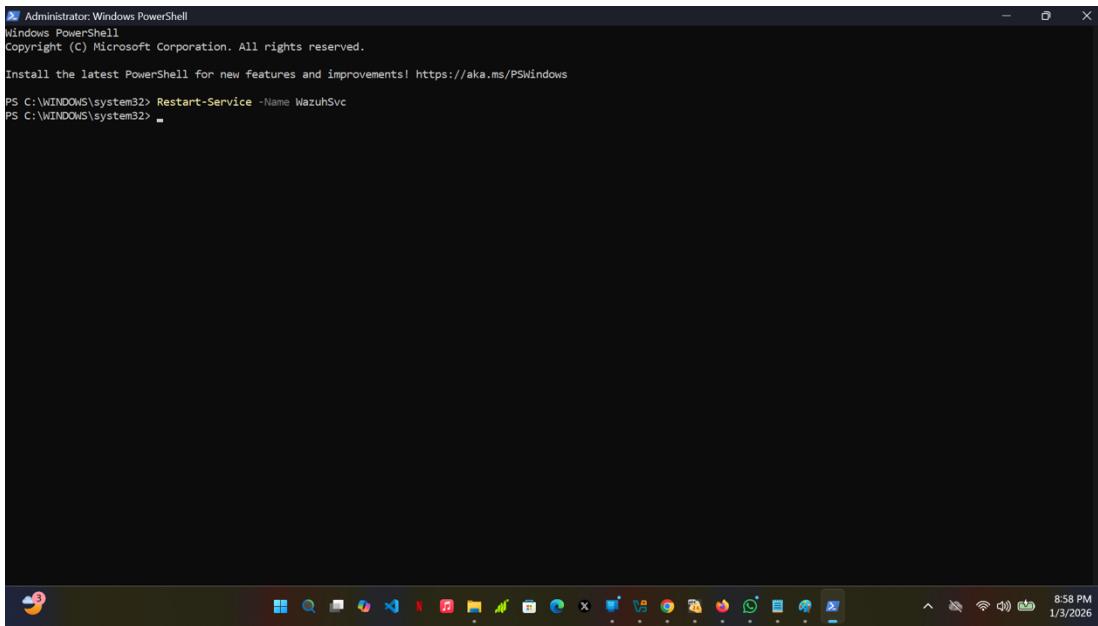
```

<!-- File integrity monitoring -->
<syscheck>
  <directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\INSPIRON\Desktop\Sensitive Folder</directories>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 1 minutes -->
  <frequency>60</frequency>

```

- ❖ Save File
- ❖ Restart Wazuh manager service using **Restart-Service -Name WazuhSvc** on powershell, after running as administrator.

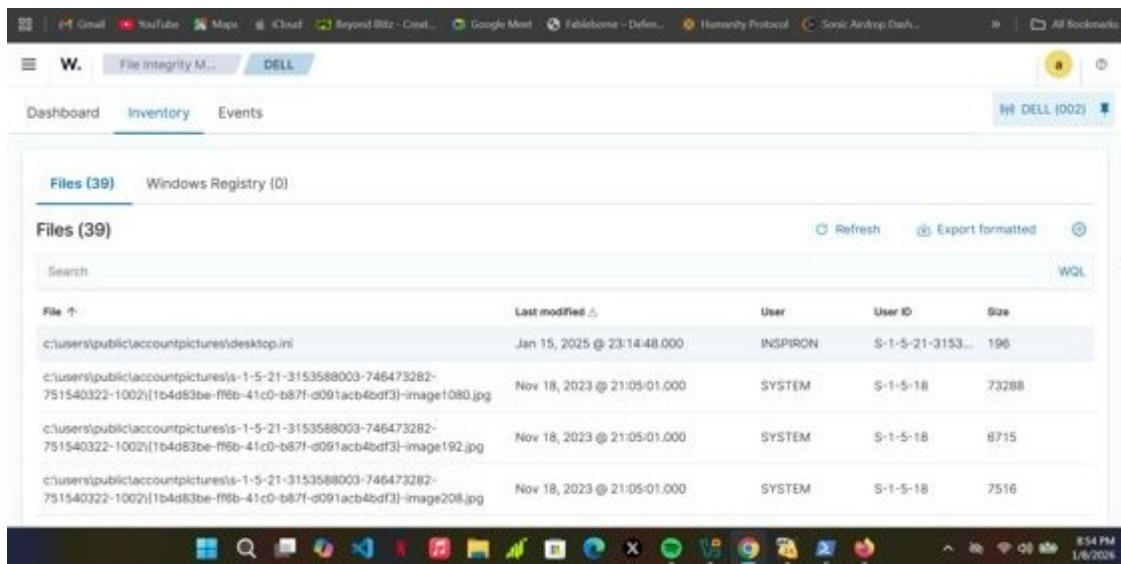


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\WINDOWS\system32> Restart-Service -Name WazuhSvc
PS C:\WINDOWS\system32> -
```

8. In the Wazuh web console (via the web browser), Go to the **File Integrity Monitoring** page  
Menu >> Endpoint Security >> **File Integrity Monitoring** (It will be on the Dashboard tab by default.)
9. Navigate to the **Inventory** tab.
10. Click the **Select agent** button.
11. Select your agent
12. Search the name of your monitored file (Mine did not appear as saved on the agent)

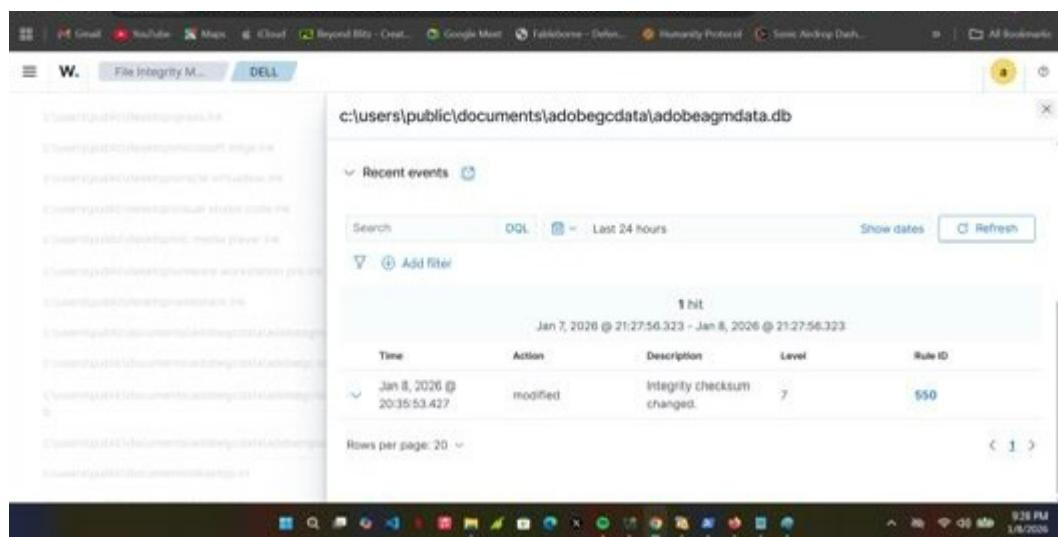


The screenshot shows the FIM interface with the following details:

- Header:** Shows browser tabs for Gmail, YouTube, Maps, iCloud, Beyond Blitz - Create, Google Meet, FileIntegrity - Detect, Humanity Protocol, and Sonic Airdrop Dash. The title bar includes "W. File Integrity M..." and "DELL".
- Top Navigation:** Buttons for Dashboard, Inventory (which is selected), and Events. A status bar shows "DELL (002)" and a battery icon.
- Left Sidebar:** A tree view showing "File Integrity M..." and "DELL".
- Main Content:** A table titled "Files (39) Windows Registry (0)".

File	Last modified	User	User ID	Size
c:\users\public\account\pictures\desktop.ini	Jan 15, 2025 @ 23:14:48.000	INSPIRON	S-1-5-21-3153...	196
c:\users\public\account\pictures\{a-1-5-21-3153588003-746473282-751540322-1002}\{1b4d83be-ff6b-41c0-b87f-d091acb46df3}-image1080.jpg	Nov 18, 2023 @ 21:05:01.000	SYSTEM	S-1-5-18	73288
c:\users\public\account\pictures\{a-1-5-21-3153588003-746473282-751540322-1002}\{1b4d83be-ff6b-41c0-b87f-d091acb46df3}-image192.jpg	Nov 18, 2023 @ 21:05:01.000	SYSTEM	S-1-5-18	8715
c:\users\public\account\pictures\{a-1-5-21-3153588003-746473282-751540322-1002}\{1b4d83be-ff6b-41c0-b87f-d091acb46df3}-image208.jpg	Nov 18, 2023 @ 21:05:01.000	SYSTEM	S-1-5-18	7516
- Bottom:** A taskbar with various icons and the system tray showing the date and time.

- **Test 1 (on Windows Agent):** Go to your Windows laptop and open the monitored file (`C:\Demo\Sensitive_Folder`). Type one letter and save it

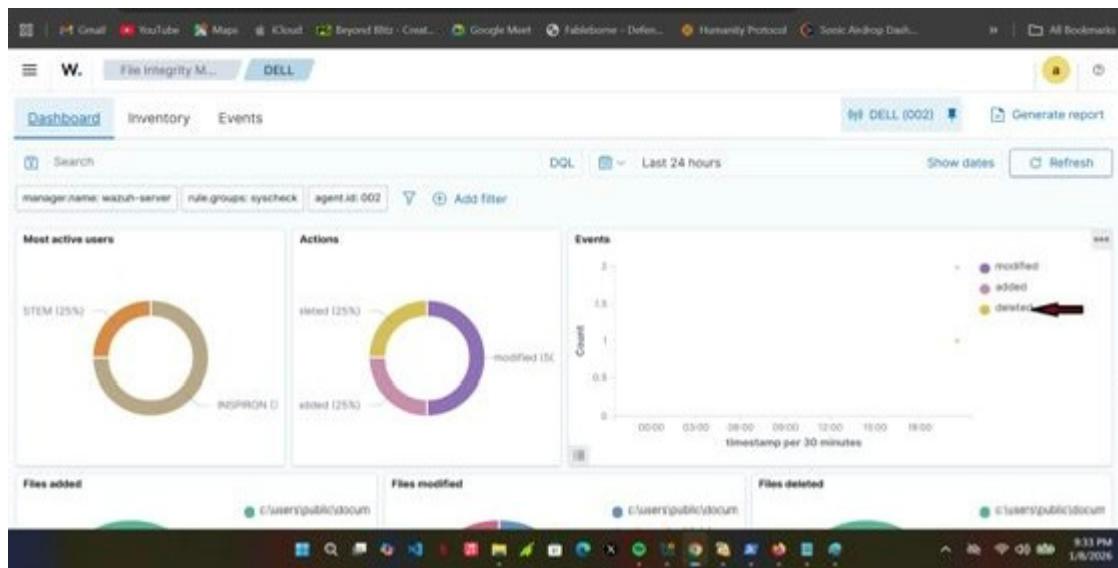


The screenshot shows the FIM interface with the following details:

- Header:** Shows browser tabs for Gmail, YouTube, Maps, iCloud, Beyond Blitz - Create, Google Meet, FileIntegrity - Detect, Humanity Protocol, and Sonic Airdrop Dash. The title bar includes "W. File Integrity M..." and "DELL".
- Top Navigation:** Buttons for Dashboard, Inventory (which is selected), and Events. A status bar shows "DELL (002)" and a battery icon.
- Left Sidebar:** A tree view showing "File Integrity M..." and "DELL".
- Main Content:** A table titled "Recent events" for the file `c:\users\public\documents\adobegcdatal\adobeagmdata.db`.

Time	Action	Description	Level	Rule ID
Jan 8, 2026 @ 20:35:53.427	modified	Integrity checksum changed.	7	550
- Bottom:** A taskbar with various icons and the system tray showing the date and time.

- **Test 2 (on Windows Agent):** Delete the file entirely.



4 hits

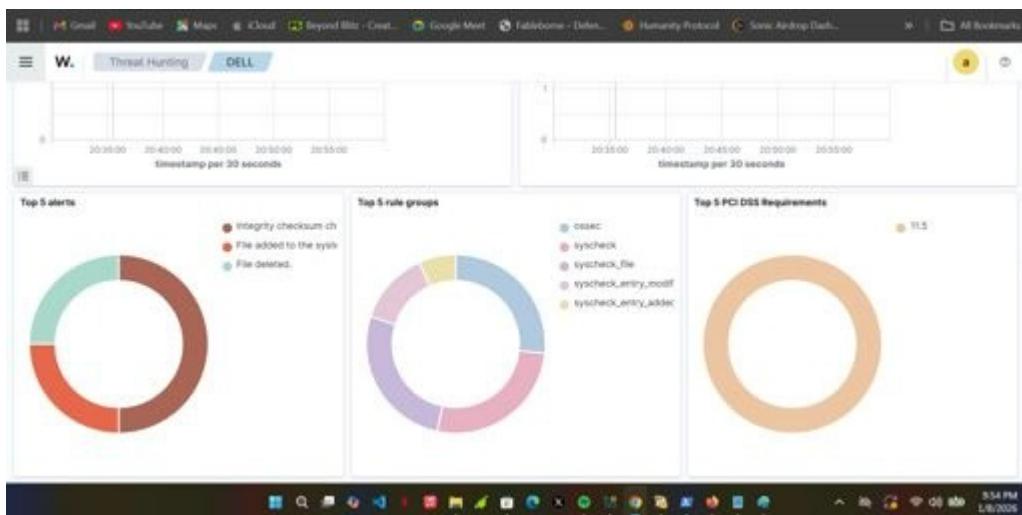
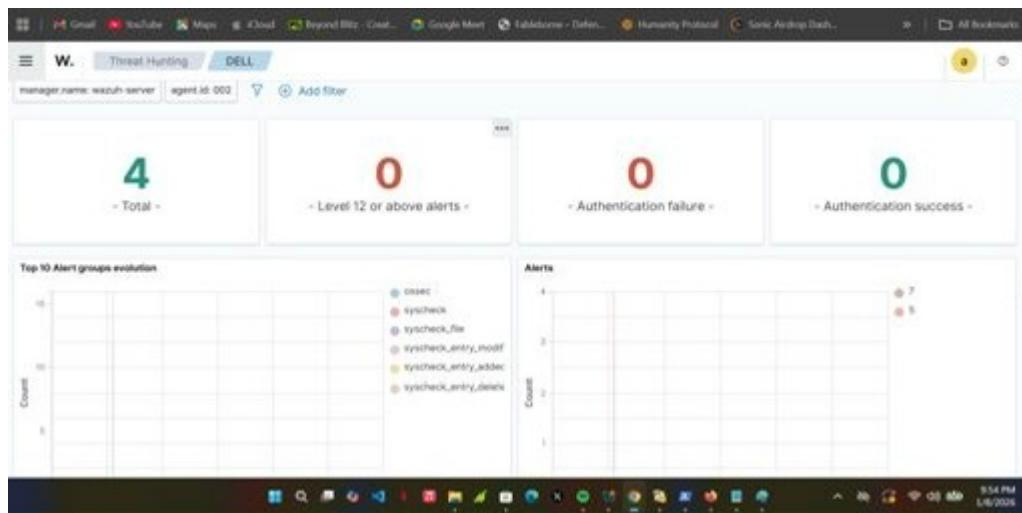
Jan 8, 2026 @ 20:30:00.000 - Jan 8, 2026 @ 21:00:00.000

Export Formatted Reset view 704 available fields Columns Density 1 fields sorted Full screen

ip	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
@ 20:35:55.404	DELL	c:\users\public\documents\adobegcadobegc_a23032	added	File added ...	5	554
@ 20:35:53.713	DELL	c:\users\public\documents\adobegcadobegc_a23032	deleted	File deleted...	7	553
@ 20:35:53.456	DELL	c:\users\public\documents\adobegcdata\adobenglappi...	modified	Integrity ch...	7	550
@ 20:35:53.427	DELL	c:\users\public\documents\adobegcdata\adobeagmdata...	modified	Integrity ch...	7	550

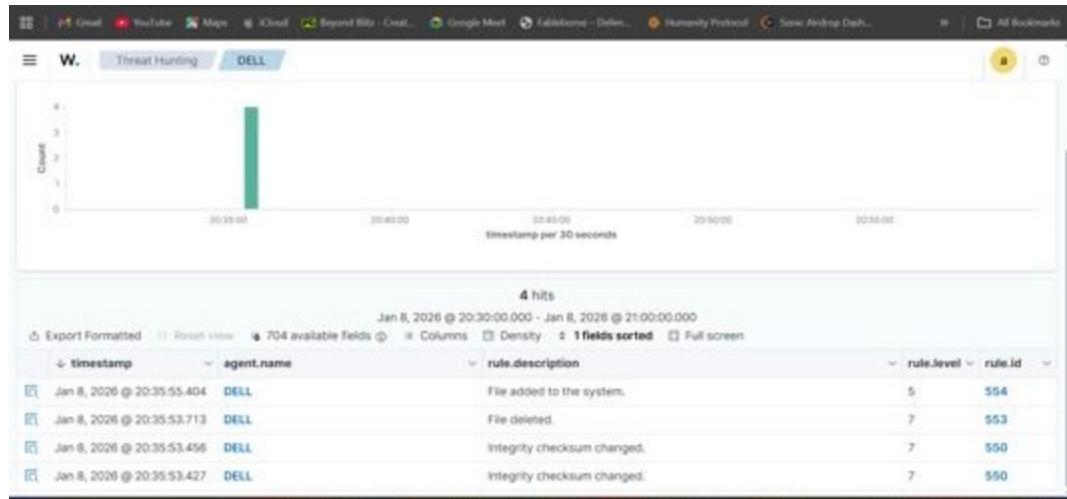
## Checking General Security Alerts

1. Threat Hunting Page on Wazuh: (Menu button (top left) >> Threat Intelligence >> Threat Hunting).



**N/B:** The Threat Hunting Dashboard provides a high-level, visual overview of the organization's security posture. It serves as a central hub for identifying trends and anomalies across the environment. By aggregating data into interactive widgets, it allows security analysts to quickly spot spikes in suspicious activity, see which MITRE ATT&CK techniques are being triggered most frequently, and identify Top Talkers or high-risk assets.

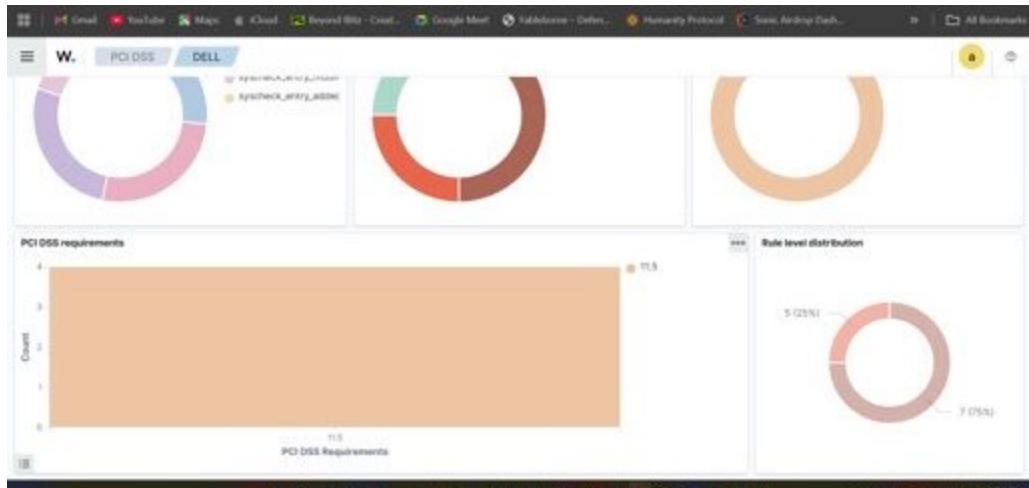
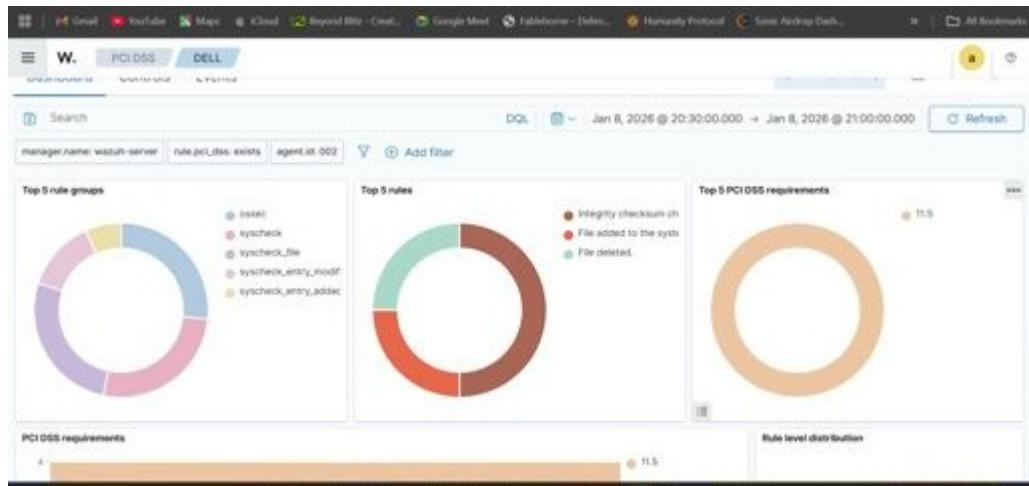
2. On the Event tab:



**N/B:** The Events Tab is the granular engine of the threat hunting process. While the dashboard provides the big picture, the Events tab provides the raw, searchable data. This page lists individual telemetry logs and security occurrences captured from endpoints, network traffic, and cloud environments. It is designed for deep-dive investigations where an analyst needs to reconstruct the specific timeline of an incident.

## Viewing PCI DSS Compliance

1. Click on the Wazuh Menu (top left) > Security operations > PCI DSS.
2. Dashboard View: Summary of requirements met/failed based on recent alerts will be displayed



## Viewing GDPR Compliance

1. Click on Wazuh Menu (top left) > Security operations > GDPR.
2. Dashboard View: Similar to PCI DSS, this maps alerts to GDPR articles.

