MAC-DONALD ONYEWUCHI EGBUNA

WAZUH ENDPOINT SECURITY MONITORING

ALT/SOE/025/4248

macdonalde2000@gmail.com

Wazuh Manager VM Setup on Windows Host & Endpoint

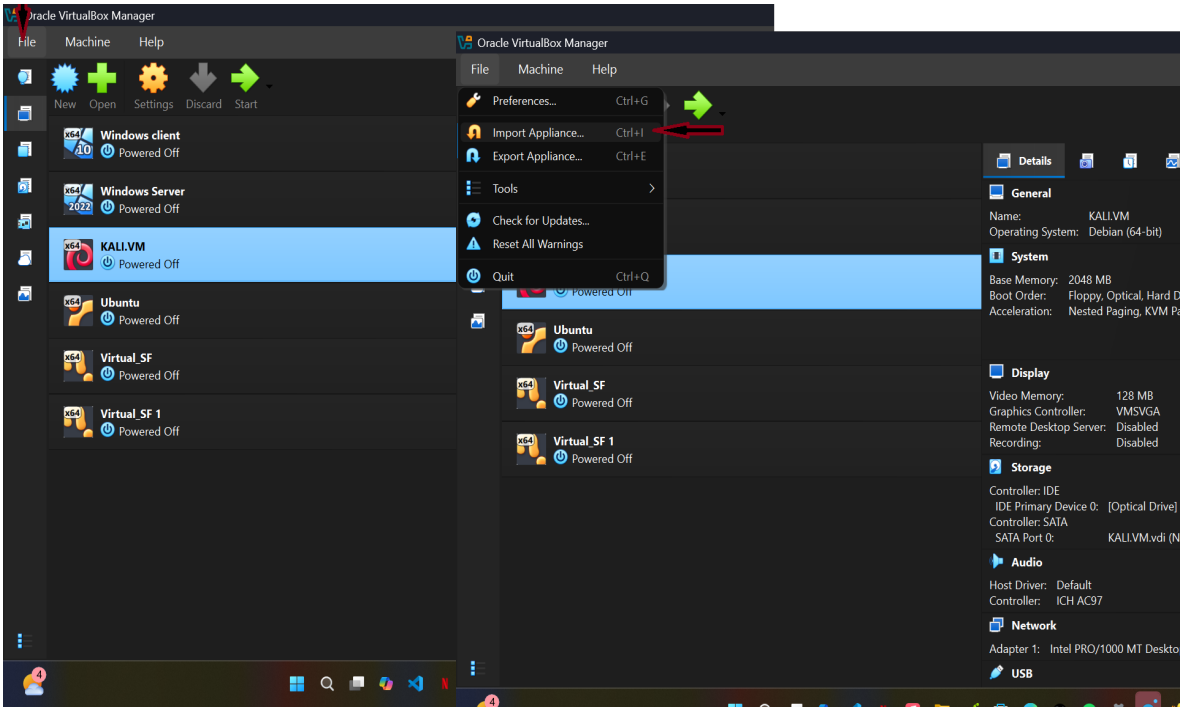
Policy Configuration

Part 1: Initial Setup - Deploying the Wazuh VM

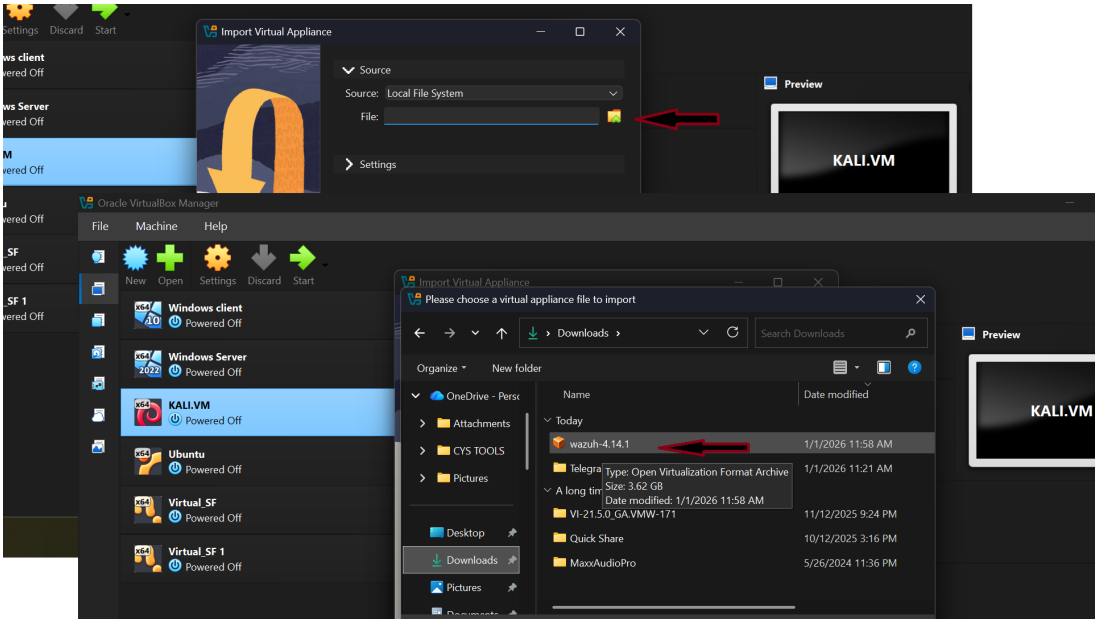
1. Prerequisites and Environment
   - Host PC: Windows 11 with Hardware Virtualization (VT-x/AMD-V) enabled in the BIOS.
   - Software: Oracle VirtualBox installed.
   - Appliance: The official Wazuh OVA (Open Virtualization Appliance) file downloaded.

1.1. Importing the Wazuh OVA into VirtualBox

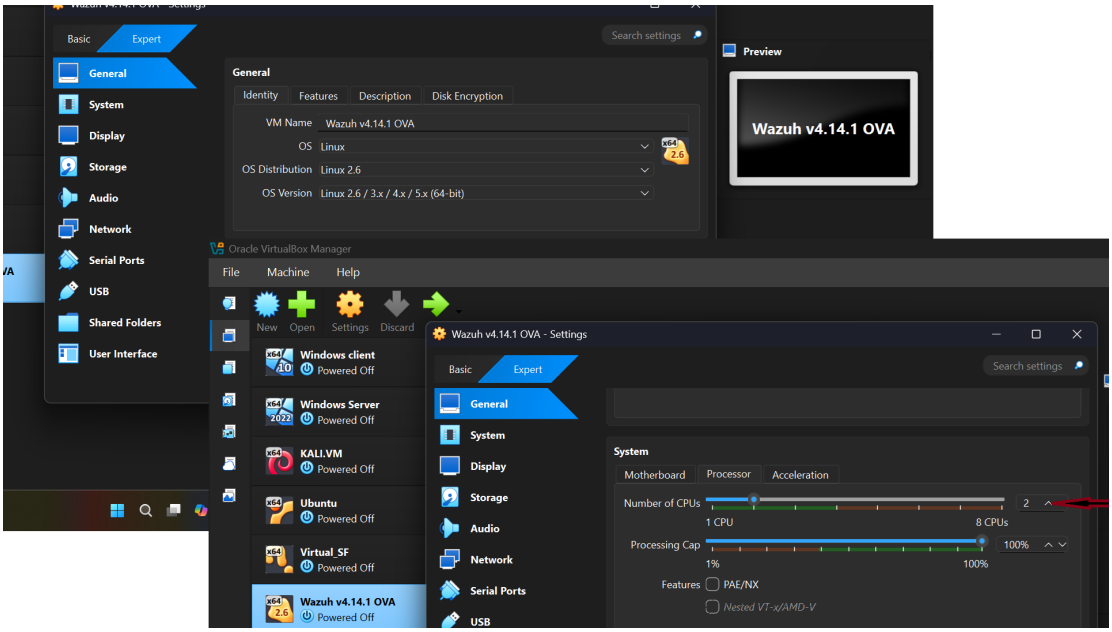
1. Using Oracle VirtualBox
2. Click on - Files -Import Appliance



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

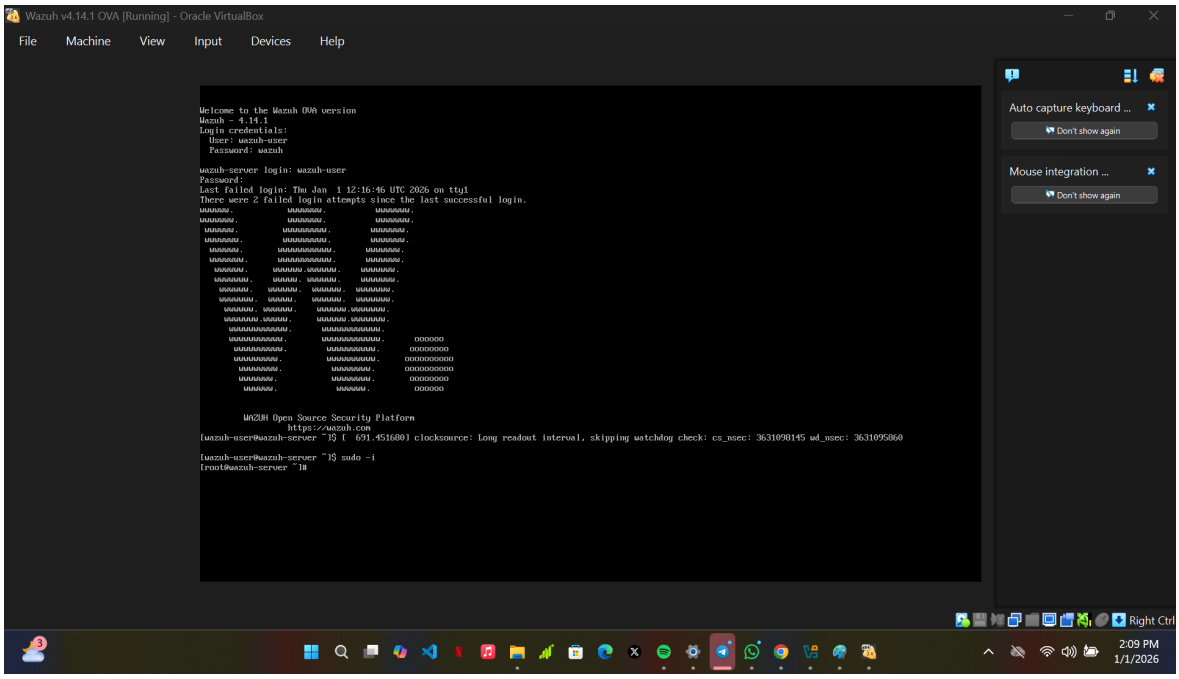


4. Review Settings: Allocate at least 4GB of RAM and 2 CPUs. Adjust the hard disk location if necessary. and Import.

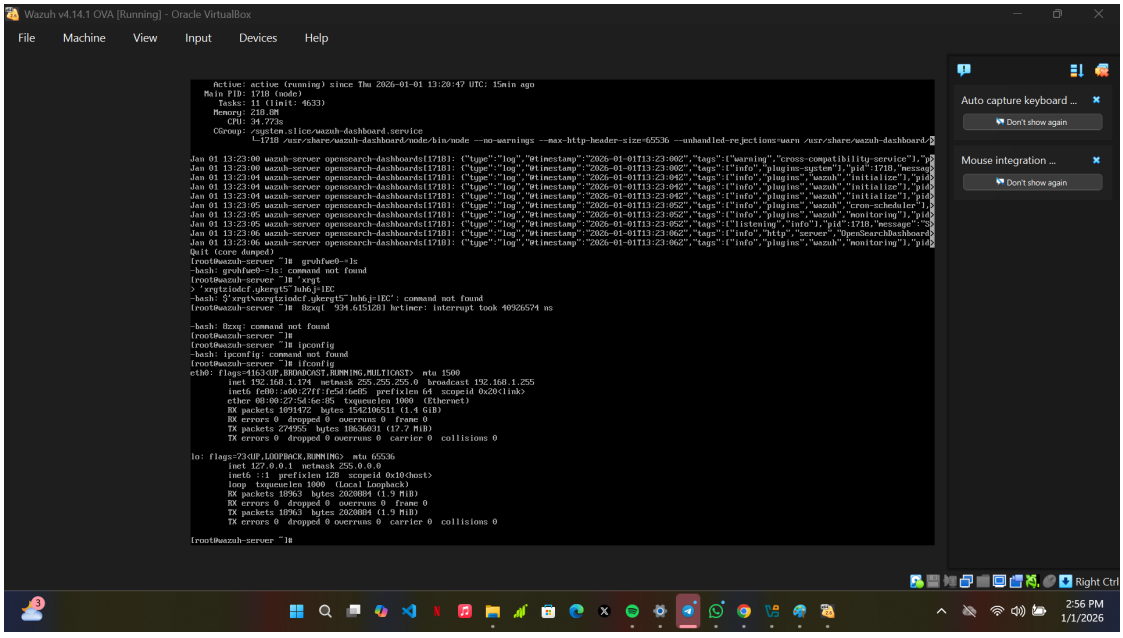


1.2. Starting the VM and Retrieving the IP:

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

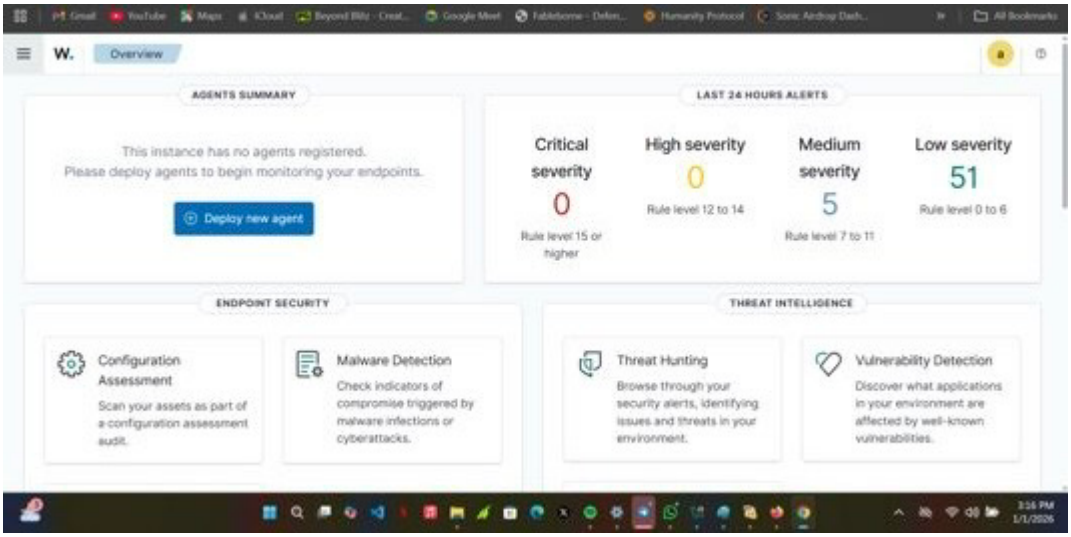


Agent Installation on the Windows Endpoint

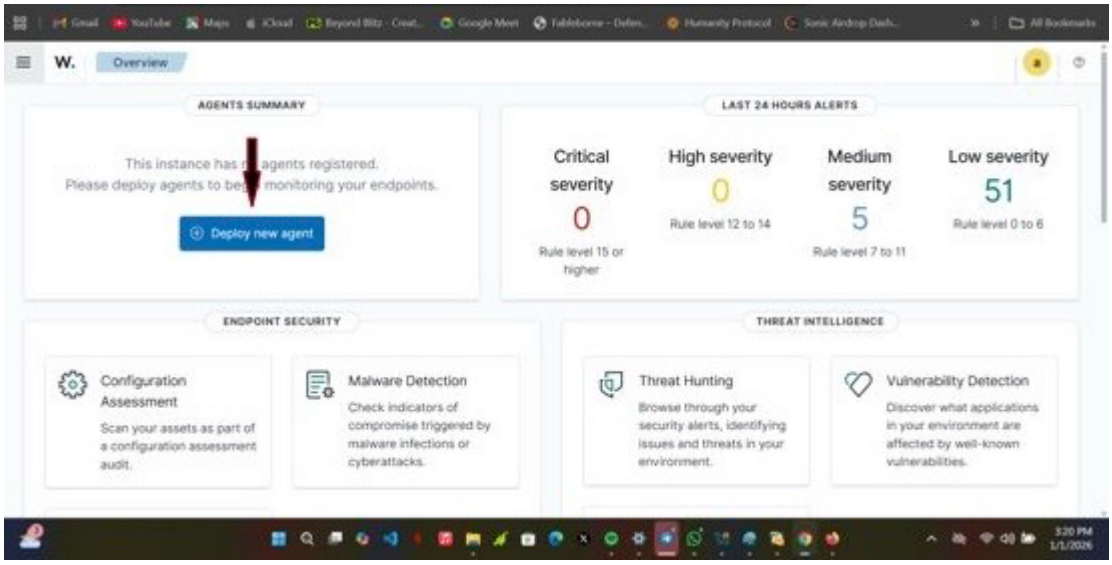
Part 2:

2.1: Generating the Deployment Command in the Dashboard

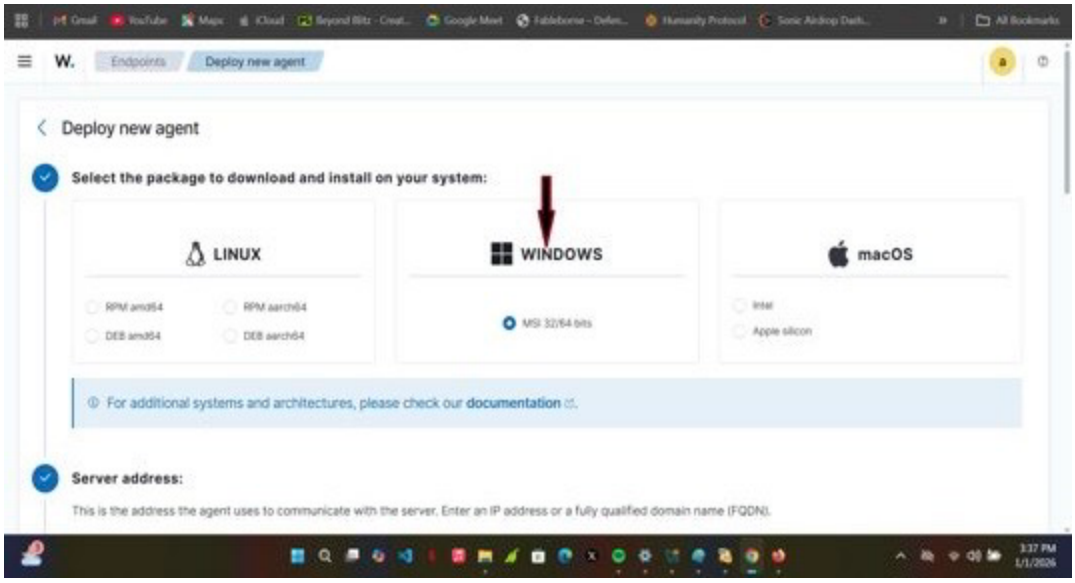
1. Open a web browser on the host pc and navigate to Wazuh Dashboard(https://192.168.1.178). Log in



2. Click **"Deploy agent"**

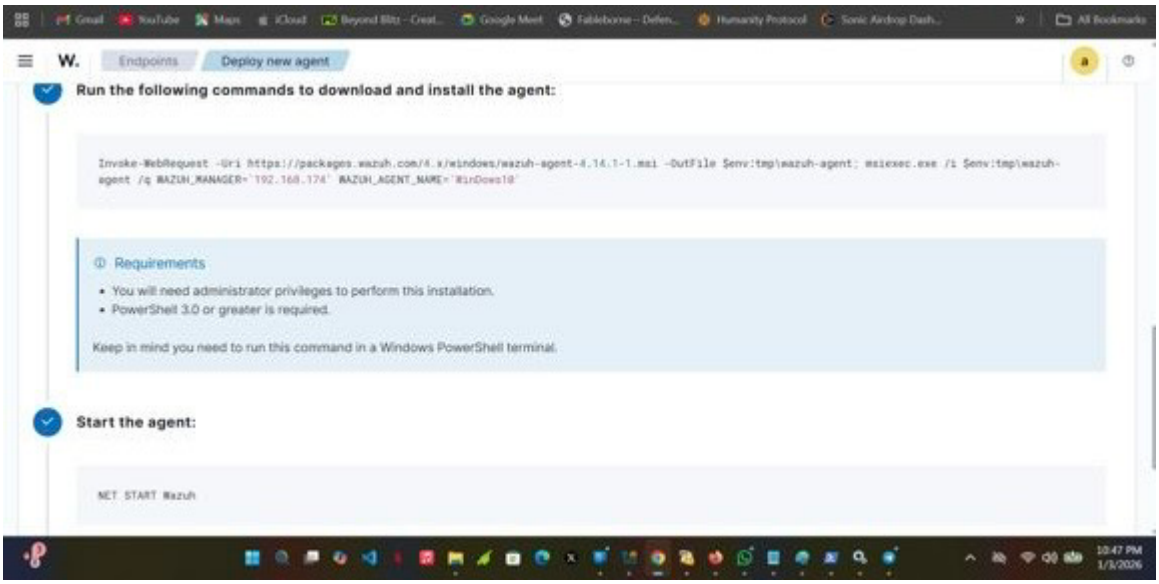


3. Select **OS** of choice (Windows)



4. Configure the Manager Connection:
    - Target Architecture: Select 64-bit (most common).
    - Manager address: (192.168.1.178).

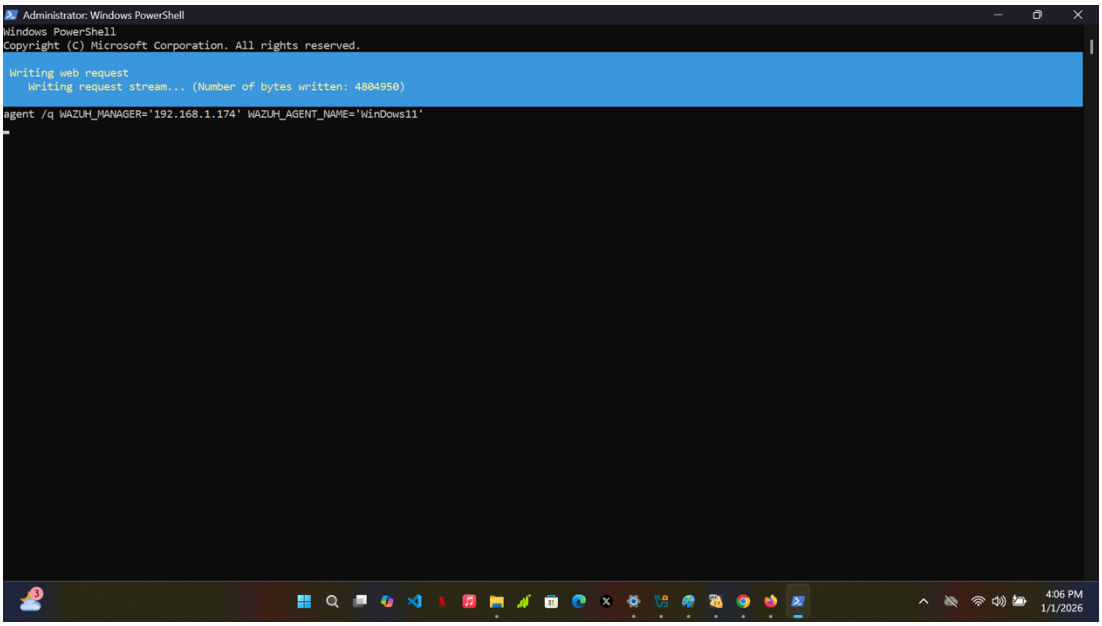
5. Leave existing group at default
6. Copy the command displayed on the dashboard and run on powershell.



2.2 Executing the Deployment Command

1. Open Powershell
2. Run as Administrator (crucial)

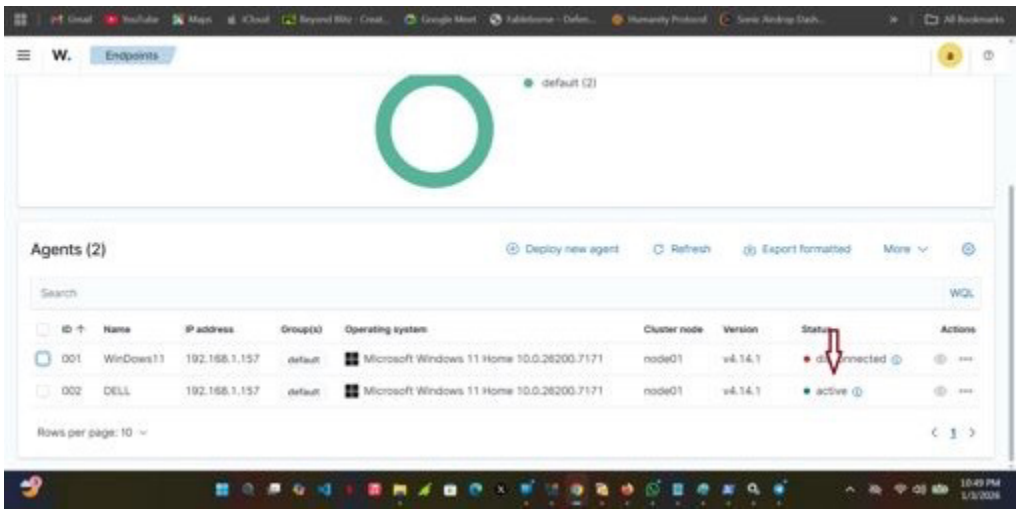
3. Paste the long command copied from the agent dashboard



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

2.3 Verifying Agent Connection in the Dashboard:

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



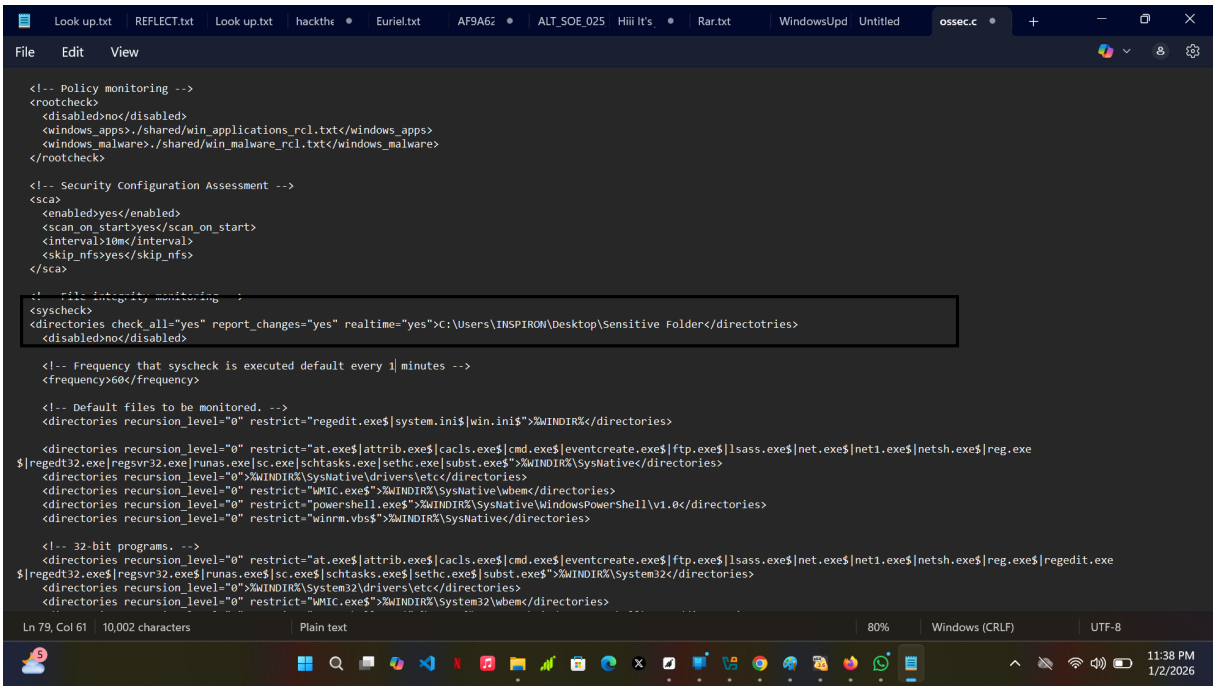
Policy Configuration - File Integrity Monitoring (FIM)

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>

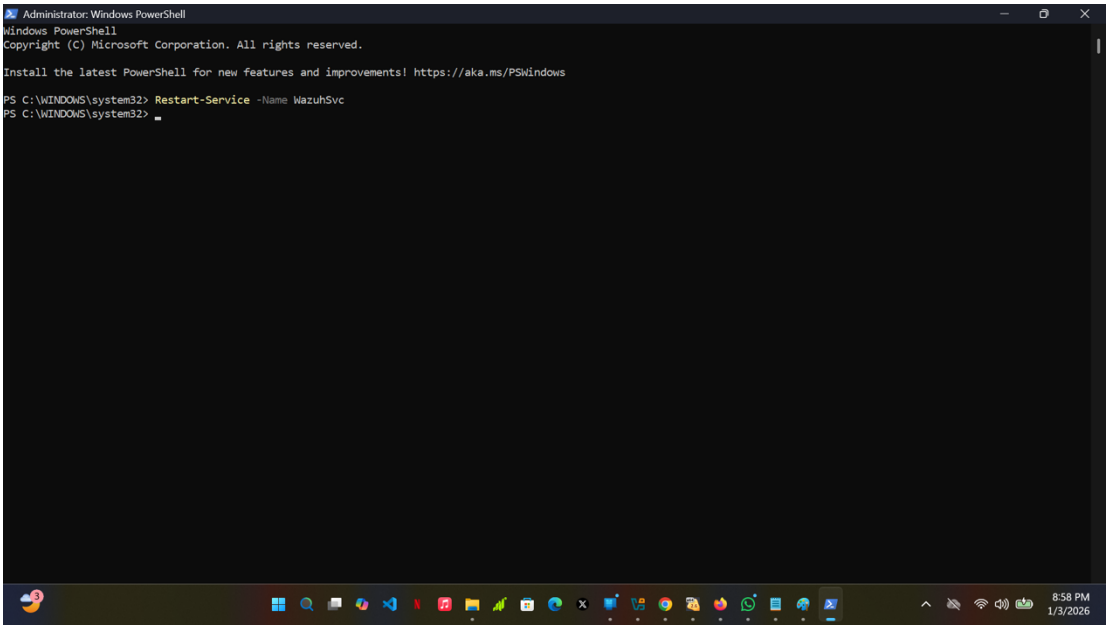


- Modify the **ossec.conf** file to speed up the detection of your file modifications

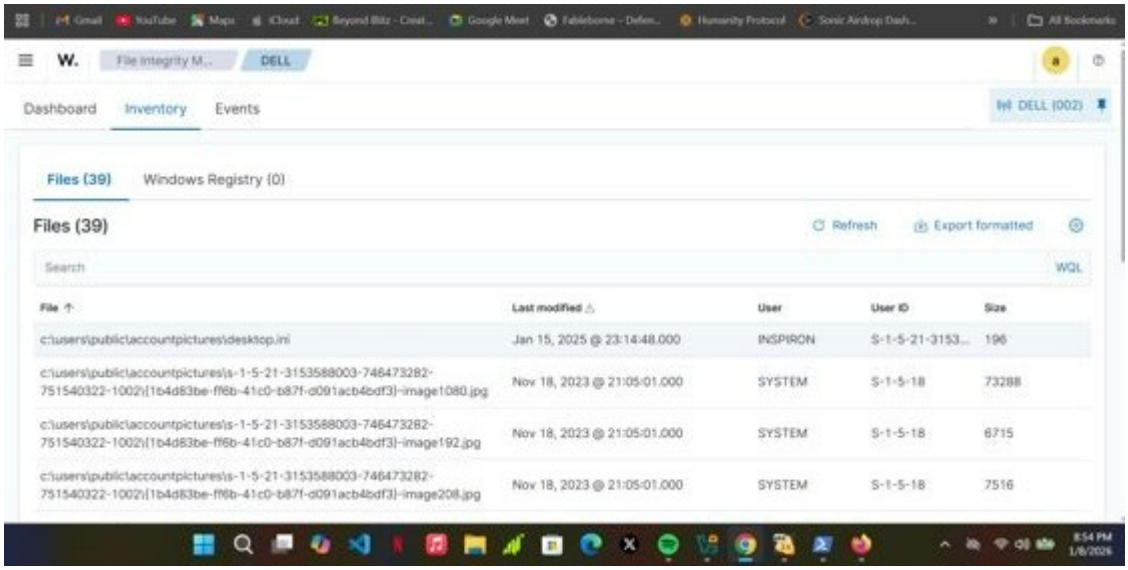
```
<!-- File integrity monitoring -->
<syscheck>
<directories check_all="yes" report_changes="yes" realtime="yes">C:\Users\INSPIRON\Desktop\Sensitive Folder</directotries>
  <disabled>no</disabled>

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

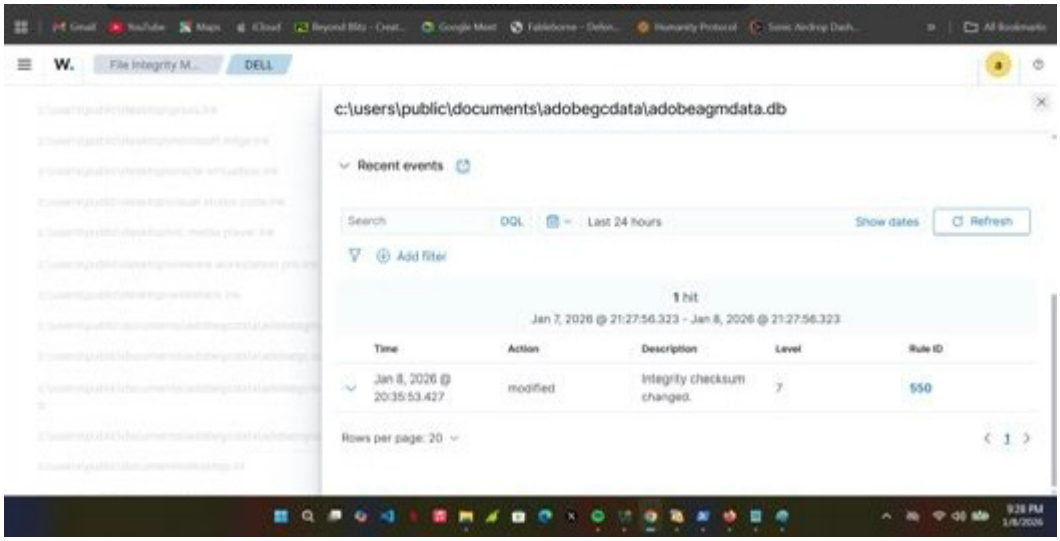
- Save File
- Restart Wazuh manager service using **Restart-Service -Name WazuhSvc** on powershell, after running as administrator.



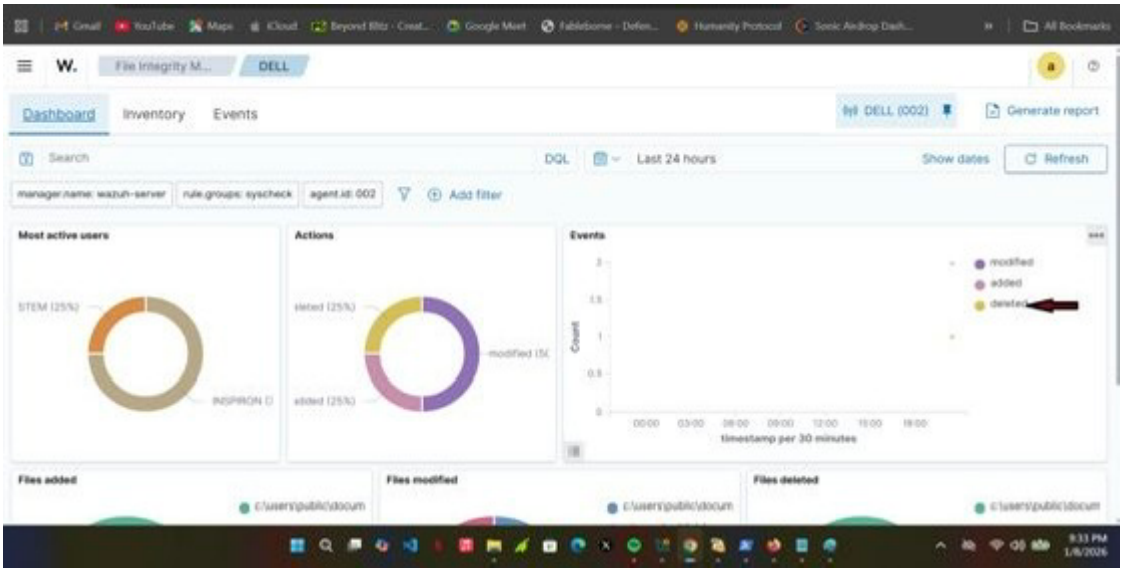
8. In the Wazuh web console (via the web browser), Go to the **File Integrity Monitoring** page
   Menu >> Endpoint Security >> **File Integrity Monitoring** (It will be on the Dashboard tab by default.
9. Navigate to the **Inventory** tab.
10. Click the **Select agent** button.
11. Select your agent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



- **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



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



4 hits

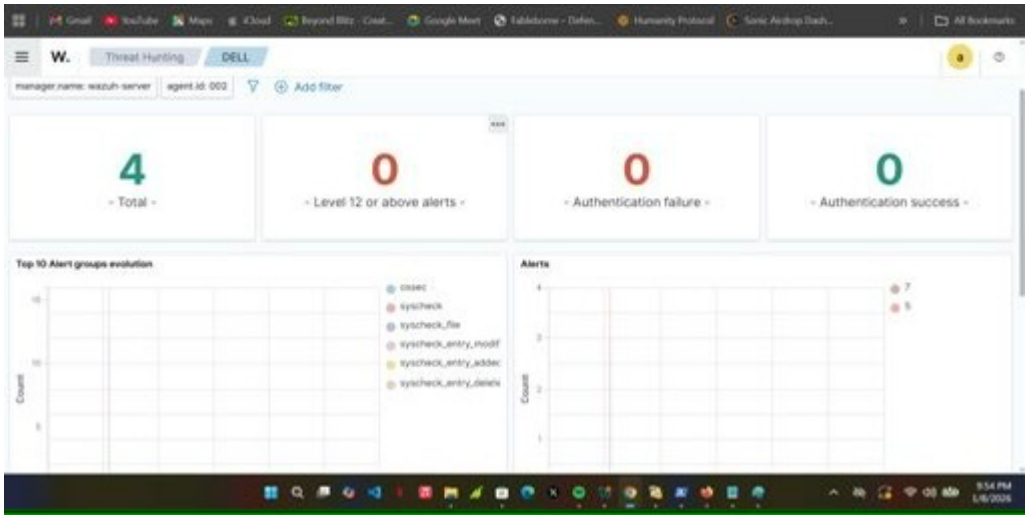
Jan 8, 2026 @ 20:30:00.000 - Jan 8, 2026 @ 21:00:00.000

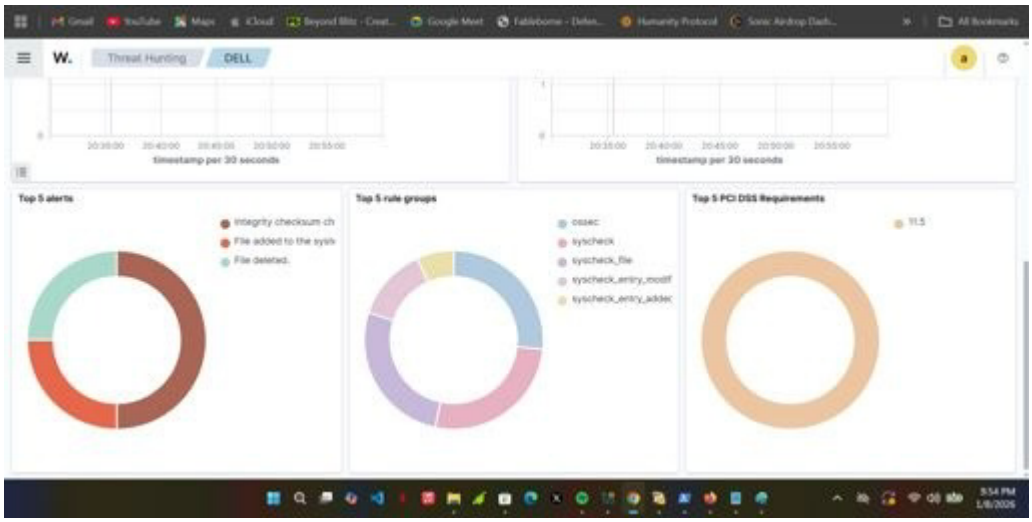
Export Formatted | Reset view | 704 available fields | Columns | Density | **1 fields sorted** | Full screen

ıp	agent.name	syscheck.path	syscheck.event	rule.des...	rule.level	rule.id
@ 20:35:55.404	DELL	c:\users\public\documents\adobegc\adobegc_a23032	added	File added ...	5	554
@ 20:35:53.713	DELL	c:\users\public\documents\adobegc\adobegc_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\adobeagmdat...	modified	Integrity ch...	7	550

Checking General Security Alerts

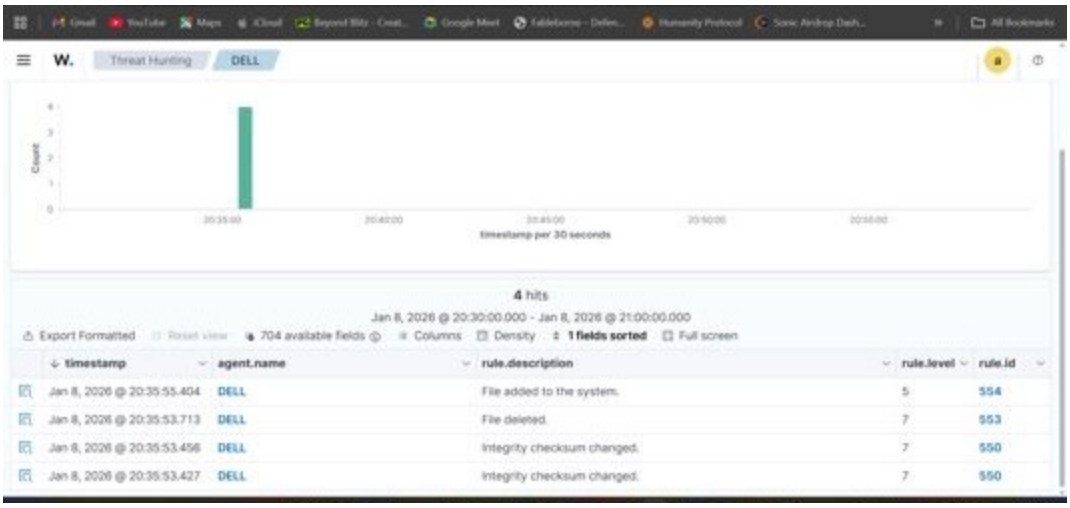
1. Threat Hunting Page on Wazuh: (Menu button (top left) >> Threat Intelligence >> Threat Hunting).





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.

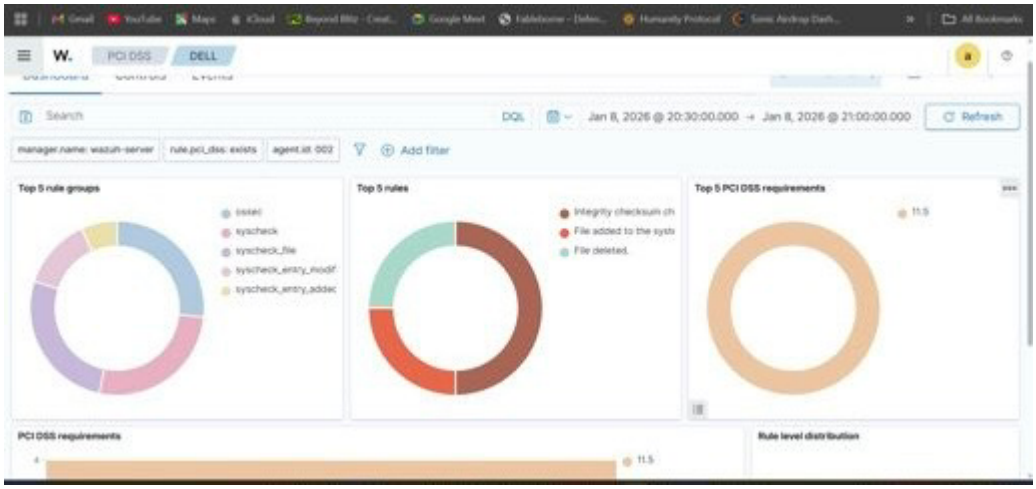
2. On the Event tab:

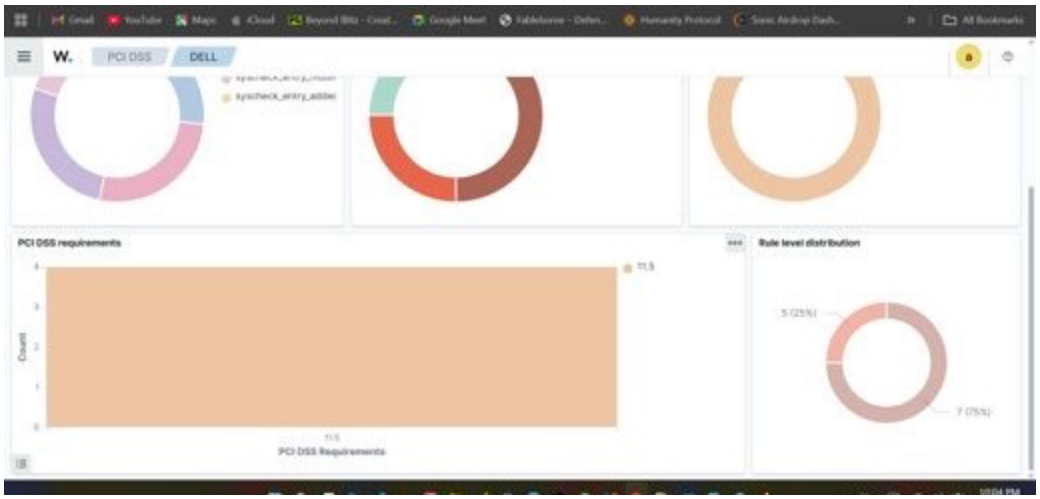


N/B: The Events Tab is the granular engine of the threat hunting process. While the dashboard provides the big picture, the Events tab provides the raw, searchable data. This page lists individual telemetry logs and security occurrences captured from endpoints, network traffic, and cloud environments.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

Viewing PCI DSS Compliance

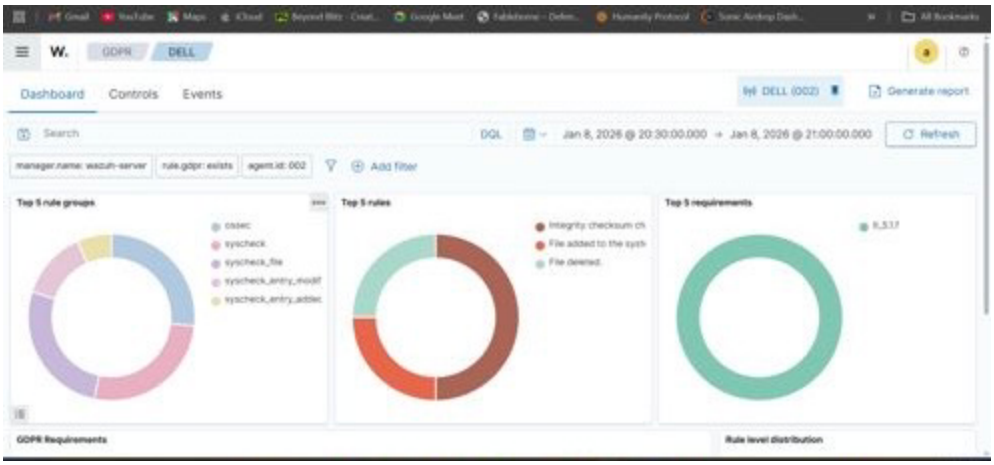
1. Click on the Wazuh Menu (top left) > Security operations > PCI DSS.
2. Dashboard View: Summary of requirements met/failed based on recent alerts will be displayed

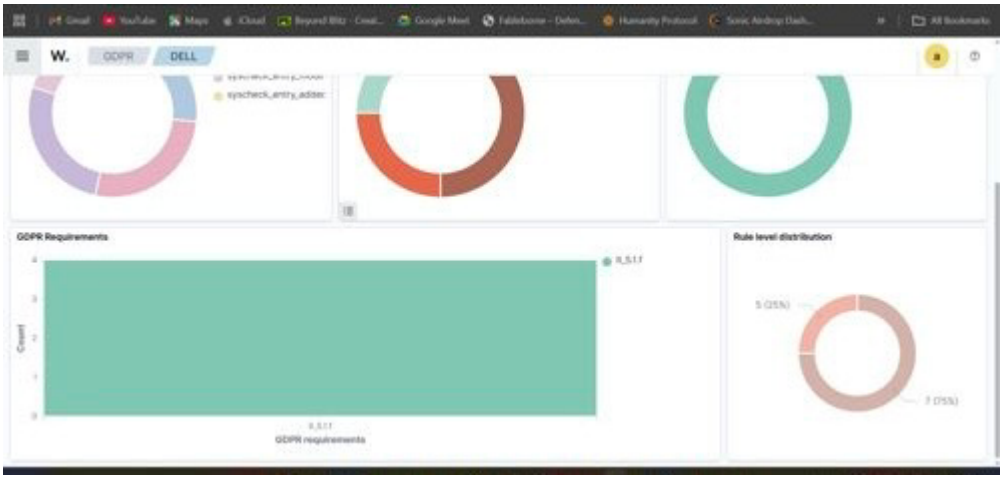




Viewing GDPR Compliance

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


W.
GDPR
DELL
Dashboard
Controls
Events
DELL (002)
Generate report
Search
DQL
Jan 8, 2026 @ 20:30:00.000 → Jan 8, 2026 @ 21:00:00.000
Refresh
manager.name: wazuh-server
rule.gdpr: exists
agent.id: 002
Add filter
Top 5 rule groups
Top 5 rules
Top 5 requirements
GDPR Requirements
Rule level distribution


W.
GDPR
DELL
GDPR Requirements
Rule level distribution
Count
GDPR requirements