

SOC Internship – Week 1 Report

Intern Name: Mahnoor Shafi

Email Address: mahnoorshafi88@gmail.com

Date: July 7, 2025

Task: Wazuh Installation & Agent Configuration

Organization: Cyborts

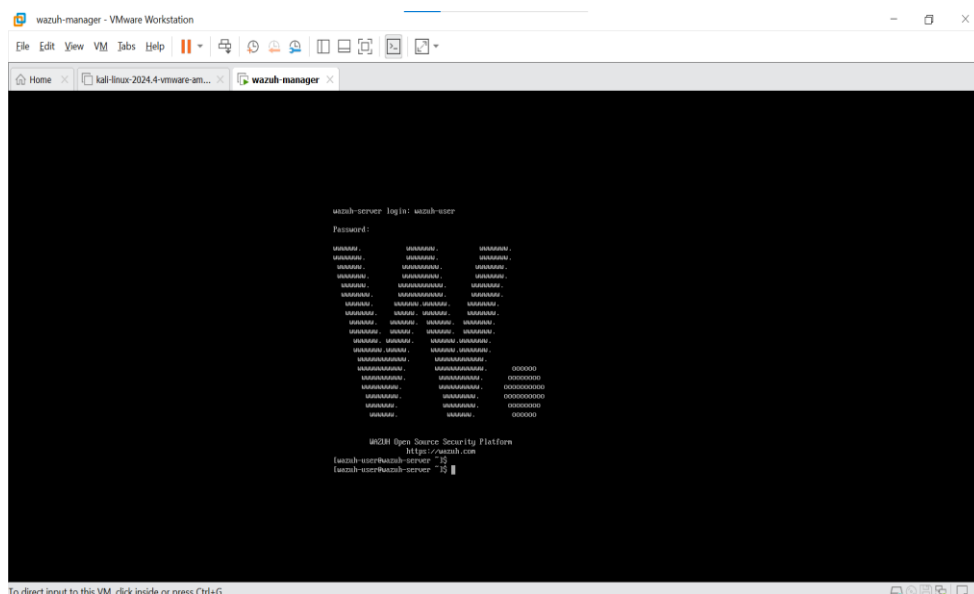
Table of Contents

- 1-Import the **Wazuh OVA file** into VirtualBox or VMware and start the Wazuh Manager.
- 2-Access the Wazuh web interface and take a **screenshot of the dashboard login page.**
- 3-Install the **Wazuh agent on a Windows machine** and connect it to the Wazuh Manager.
- 4-Install the **Wazuh agent on an Ubuntu machine** and connect it to the Wazuh Manager.
- 5-Enable **File Integrity Monitoring (FIM)** on the Ubuntu agent for the /etc directory.
- 6-Enable **FIM on the Windows agent** for the C:\Windows\System32 directory.
- 7-Create or modify a file in both monitored directories and **verify FIM alerts in the Wazuh dashboard.**

1. Wazuh Manager Setup in VirtualBox/VMware

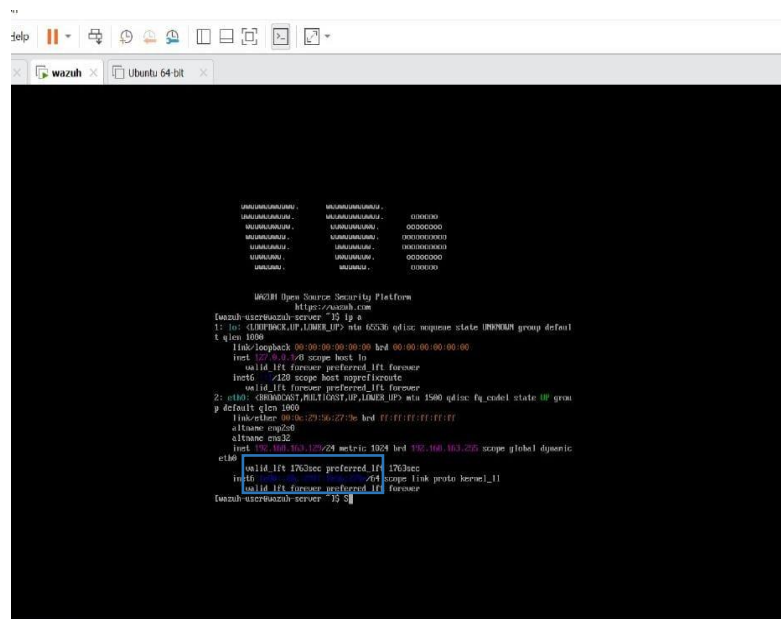
Step 1: Imported the Wazuh OVA file and started the virtual machine.

Step 2: **wazuh** is running



Enter command= ip a

It show ip of wazuh = **192.168.163.129**

A terminal window titled 'wazuh' and 'Ubuntu 64-bit' showing the output of the 'wazuh-ecsrwazuh-server' command. The output includes system information like IP address (192.168.163.129), hostname (kali), and various system metrics. A red box highlights the IP address '192.168.163.129' in the output.

```
Wazuh Open Source Security Platform
https://wazuh.com

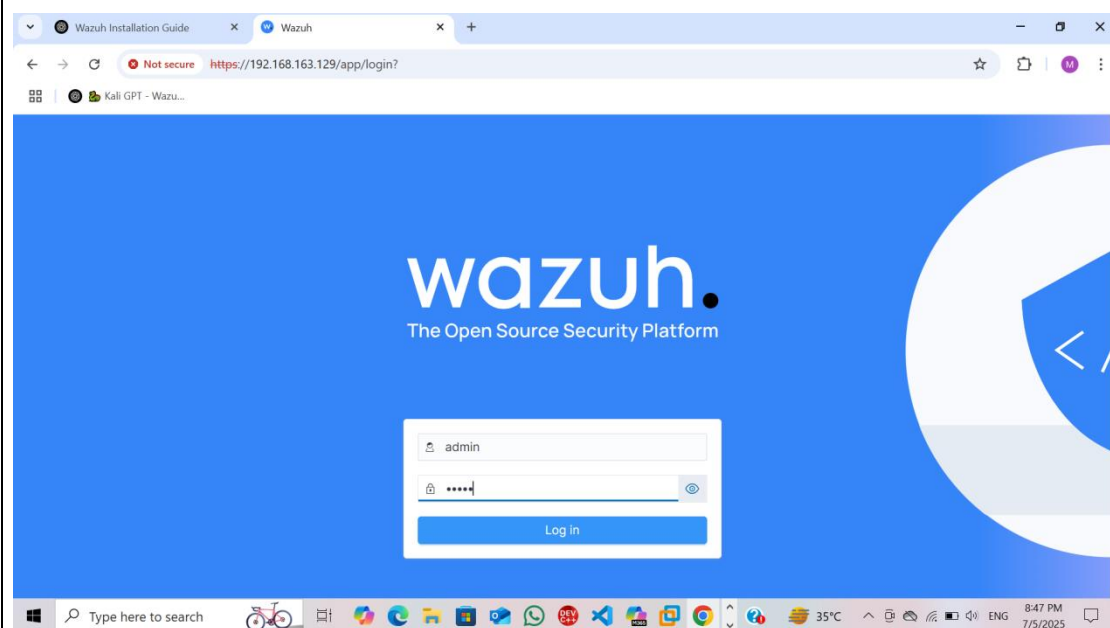
wazuh-ecsrwazuh-server ~$ ip a
1: eni: <UNDEFINED_IP,UNDEF_IP> mtu 65536 qlist: nupname state DOWN group default
    qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 192.168.163.129 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1:: scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <CHROMCAST,MLTICOST,IP,UNDEF_IP> mtu 1500 qlist: fq_codel state UP group
    p default qlen 1000
    link/ether 00:0c:29:56:22:7c brd ff:ff:ff:ff:ff:ff
    altname enp208
    altname eno32
    inet 192.168.163.129/24 metric 1024 brd 192.168.163.255 scope global dynamic
        ethtool
            valid_lft 1763sec preferred_lft 1763sec
            inet6 ::1:: scope link proto kernel_ll
            valid_lft forever preferred_lft forever
wazuh-ecsrwazuh-server ~$
```

2. Access Wazuh Web Interface

Step: Opened browser → navigated to <https://<Wazuh IP>:5601>

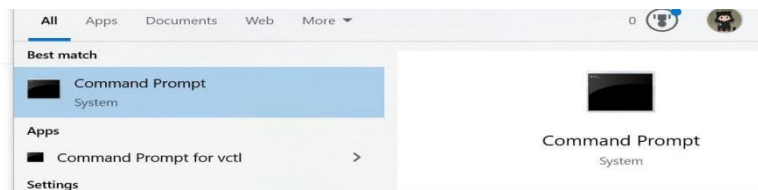
Username=admin

Password=admin

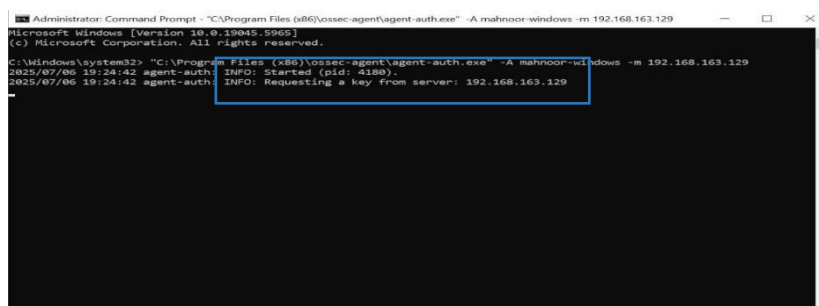


3. Install Wazuh Agent on Windows

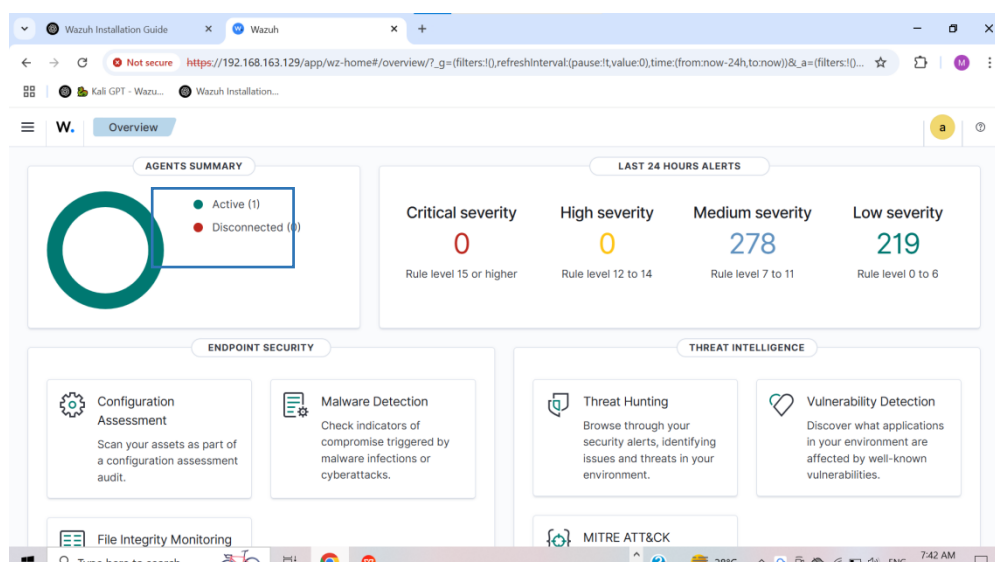
Step: Installed Wazuh agent and connected it to the Wazuh Manager.
Firstly, open **Command Prompt** and run as **administrator**



Run "**C:\Program Files (x86)\ossec-agent\agent-auth.exe**" -A mahnoor-windows -m 192.168.163.129

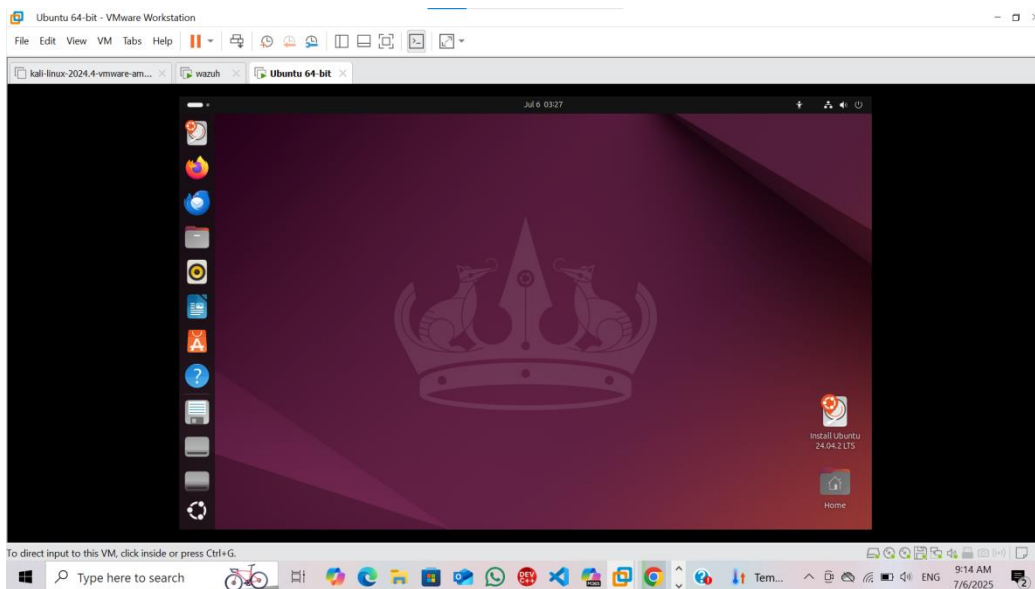


Now, Windows agent listed on the Wazuh dashboard



4. Install Wazuh Agent on Ubuntu

Step: Installed using script and connected agent to Wazuh Manager.
Firstly install ubuntu vm



Open terminal = **ctrl+alt+T**

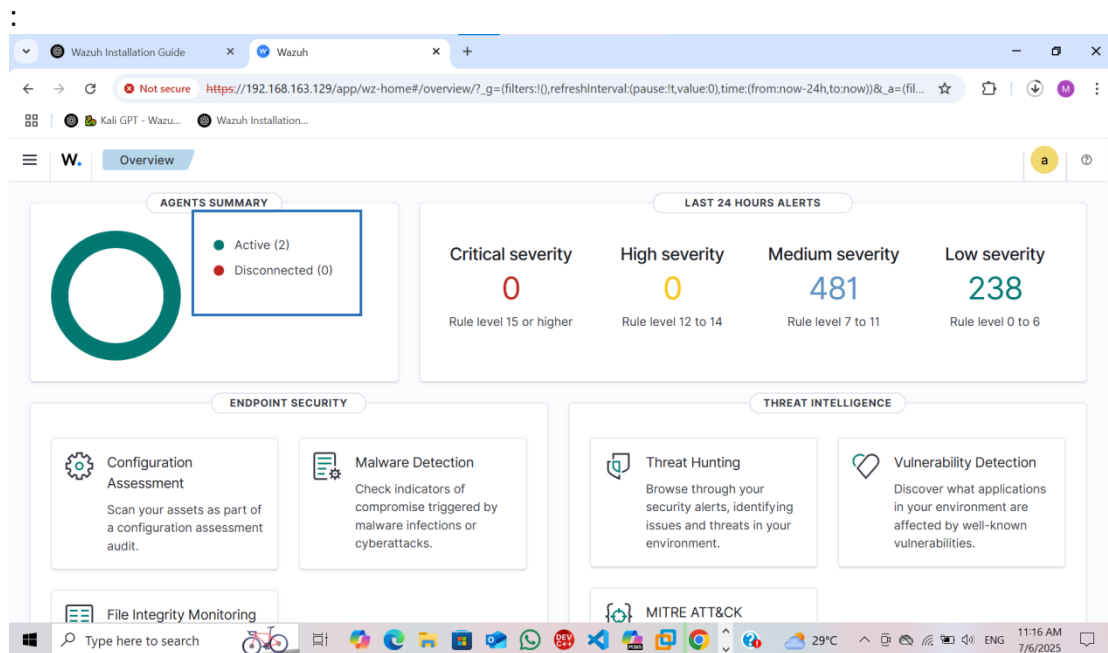
Run in terminal **curl -sO https://packages.wazuh.com/4.x/apt/wazuh-agent_4.x.x-1_amd64.deb**

Configure and then add your wazuh manager ip

<client>

<server-ip>192.168.163.129</server-ip>

</client>



5. Enable File Integrity Monitoring (FIM) – Ubuntu

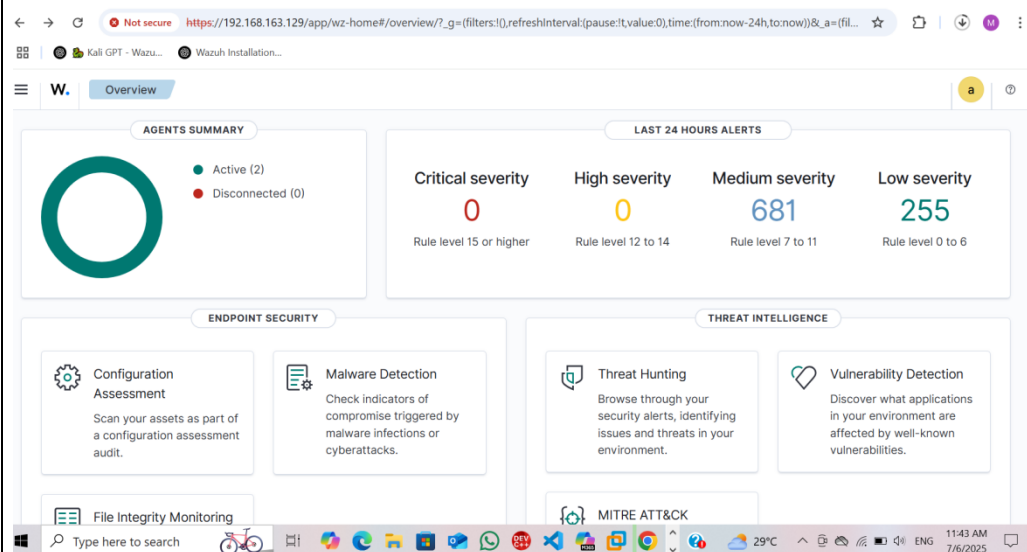
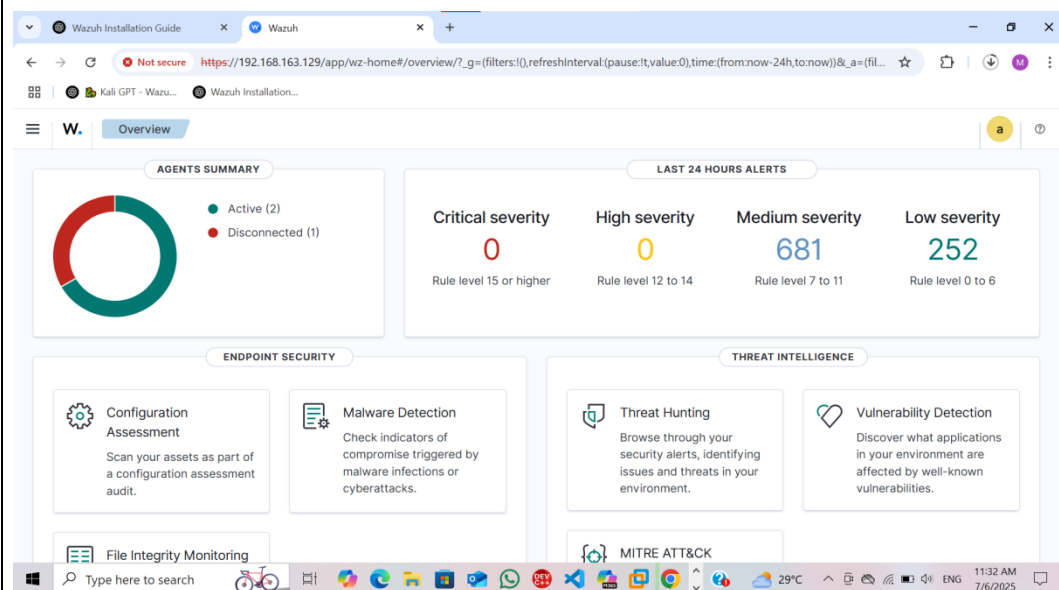
Step: Edited ossec.conf to include /etc directory under FIM.

On Ubuntu agent, edit configuration:

```
sudo nano /var/ossec/etc/ossec.conf
```

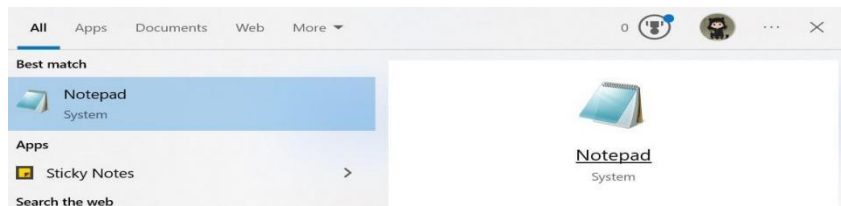
Inside <syscheck> block, add

```
<directories check_all="yes">/etc</directories>
```

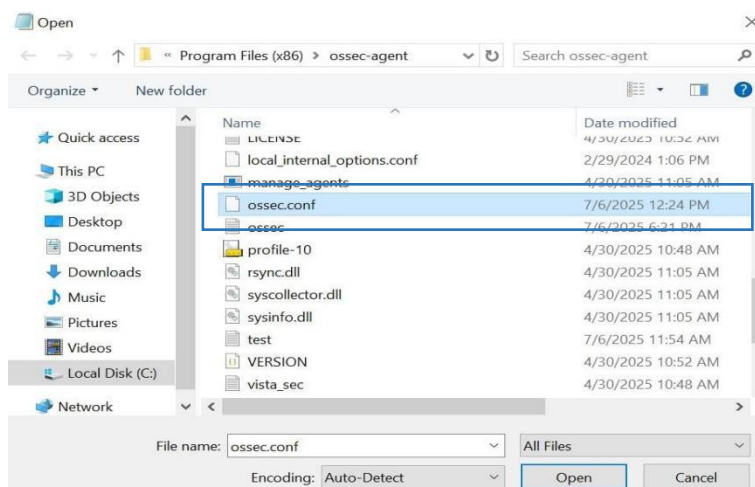


6. Enable File Integrity Monitoring – Windows

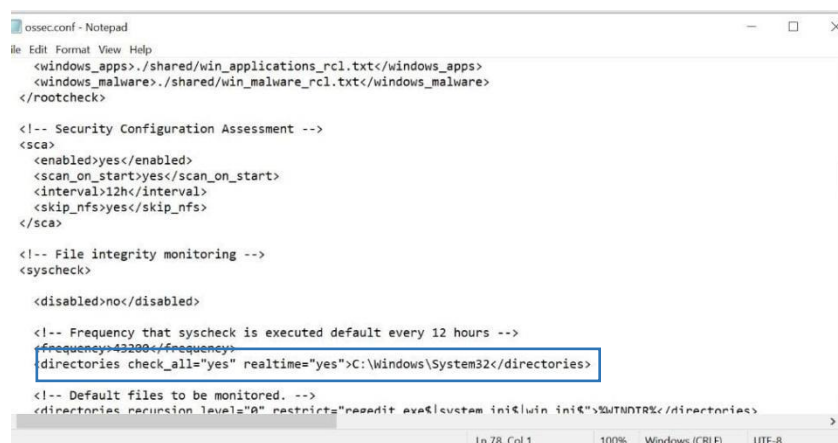
Step: Configured Wazuh agent to monitor C:\Windows\System32
Firstly, open **Notepad** as an **administrator**



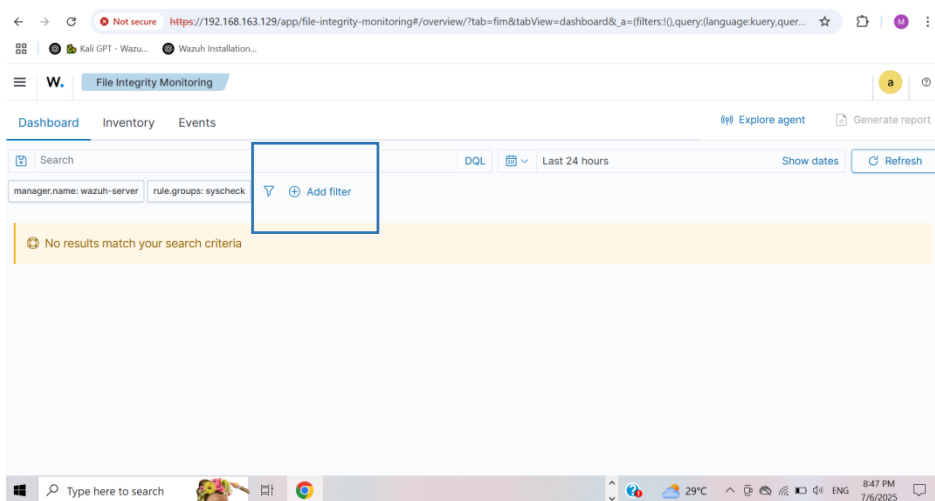
And then open file **C:\Program Files (x86)\ossec-agent\ossec.conf**



Add: **<directories**
check_all="yes">C:\Windows\System32</directories>



Restart agent from **Wazuh Agent Manager**



Add filter of your agent and laptop name

7. File Modification & Alert Verification

Step: Modified files in both monitored directories:

Ubuntu: Created testfile.txt in /etc

sudo nano/var/ossec/ossec.conf

```
<ossec_config>
<client>
  <server>
    <address>10.10.10.145</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
  <config-profile>ubuntu, ubuntu24, ubuntu24.04</config-profile>
  <notify_time>10</notify_time>
  <time-reconnect>60</time-reconnect>
  <auto_restart>yes</auto_restart>
  <crypto_method>aes</crypto_method>
  <enrollment>
    <enabled>yes</enabled>
    <agent_name>Ubuntu</agent_name>
    <authorization_pass_path>etc/authd.pass</authorization_pass_path>
  </enrollment>
</client>
<client_buffer>
```

Add: **<syscheck>**

<directories check_all="yes">/etc</directories>

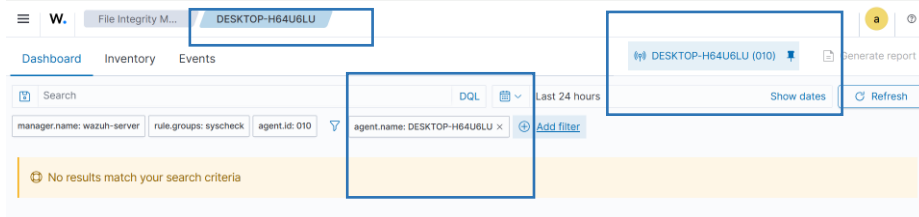
</syscheck>

And then restart agent

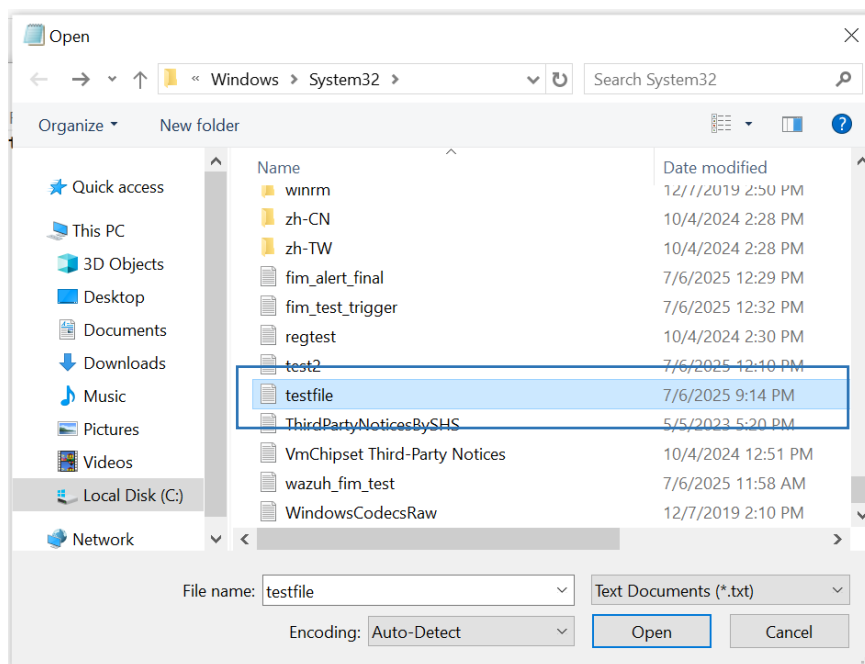
Windows: Created testfile.txt in C:\Windows\System32

Firstly they show no alerts

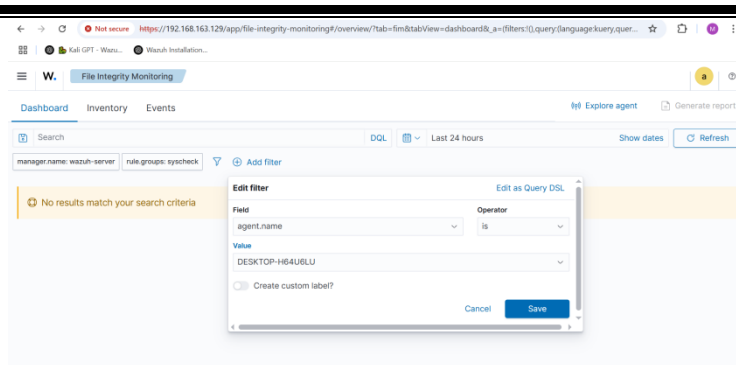
And then we add file which is given below



In notepad open **C:\Windows\System32\testfile.txt**



and then we add filter in wazuh and also generate agent

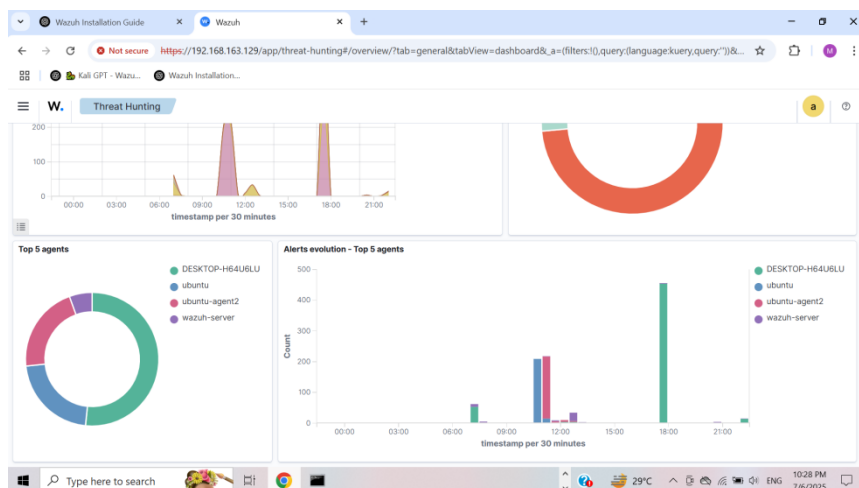


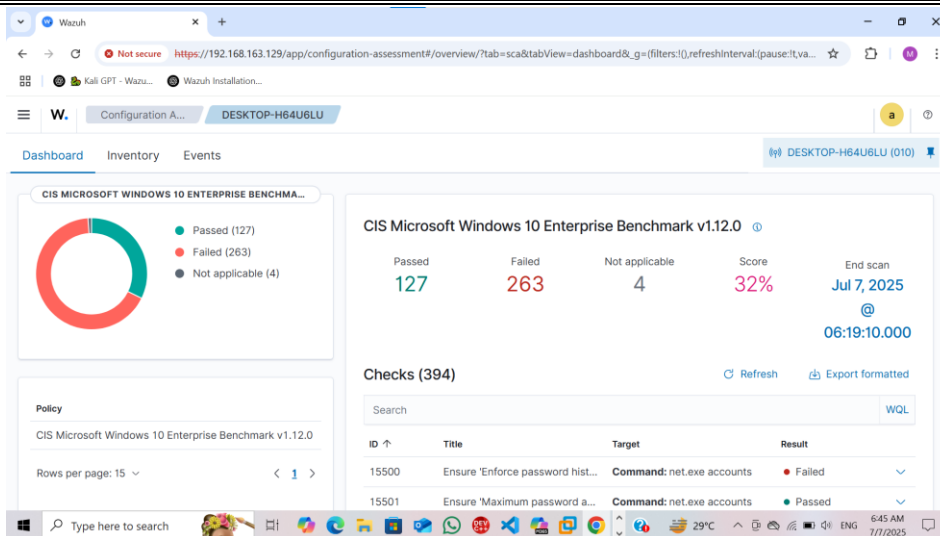
Threat Hunting:

Threat hunting in wazuh is actively searching through your security data to detect malicious activity like malware, reconnaissance etc.

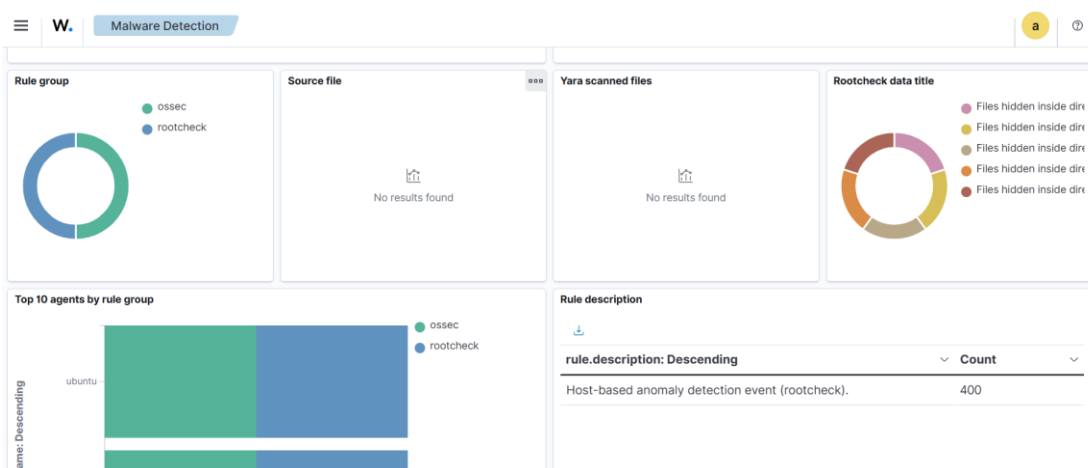
Go to:

Security events ->threat hunting

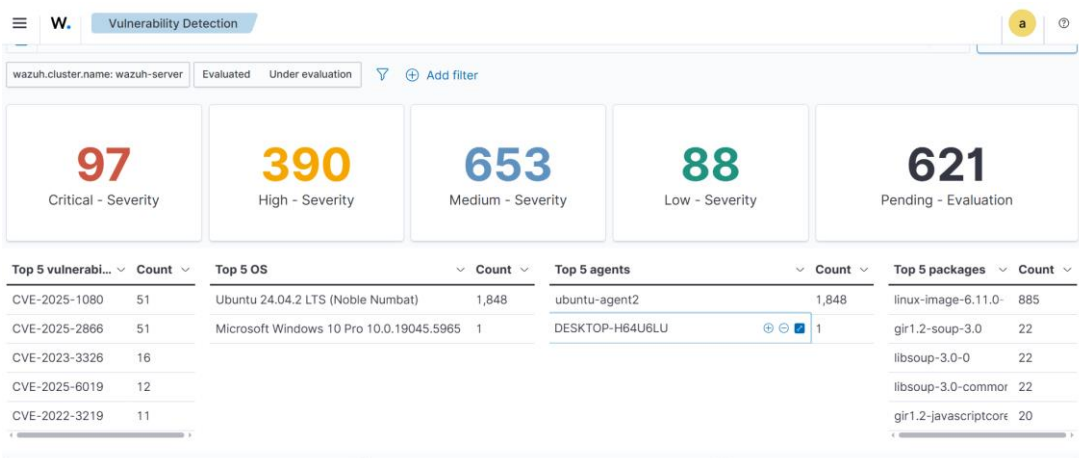




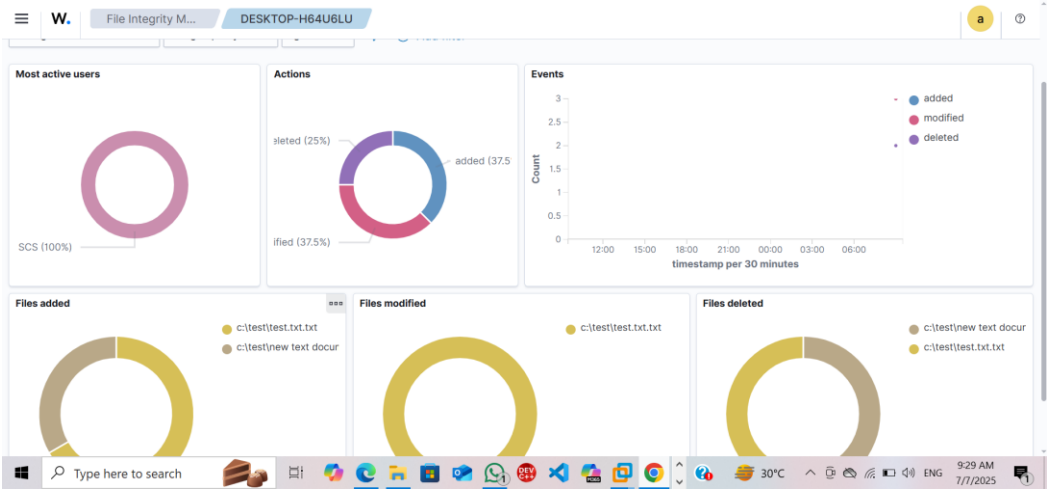
Malware Detection:



Vulnerability Detection:



File Modification:



Agents (4) ☐ Show only outdated (2) [Deploy new agent](#) [Refresh](#) [Export formatted](#) [More](#) [Settings](#)

Search [WQL](#)

| ID | Name | IP address | Group(s) | Operating system | Cluster node | Version | Status | Actions |
|-----|-----------------|-----------------|----------|--|--------------|---------|-----------------|---|
| 004 | ubuntu-agent2 | 192.168.163.130 | default | Ubuntu 24.04.2 LTS | node01 | v4.7.3 | disconnected | Info Refresh More |
| 006 | ubuntu | 192.168.163.130 | default | Ubuntu 24.04.2 LTS | node01 | v4.7.3 | disconnected | Info Refresh More |
| 008 | mahnoor-windows | any | default | - | - | - | never connected | Info Refresh More |
| 010 | DESKTOP-H64U6LU | 192.168.163.1 | default | Microsoft Windows 10 Pro 10.0.19045.5965 | node01 | v4.12.0 | active | Info Refresh More |

Rows per page: 10 [<](#) [1](#) [>](#)