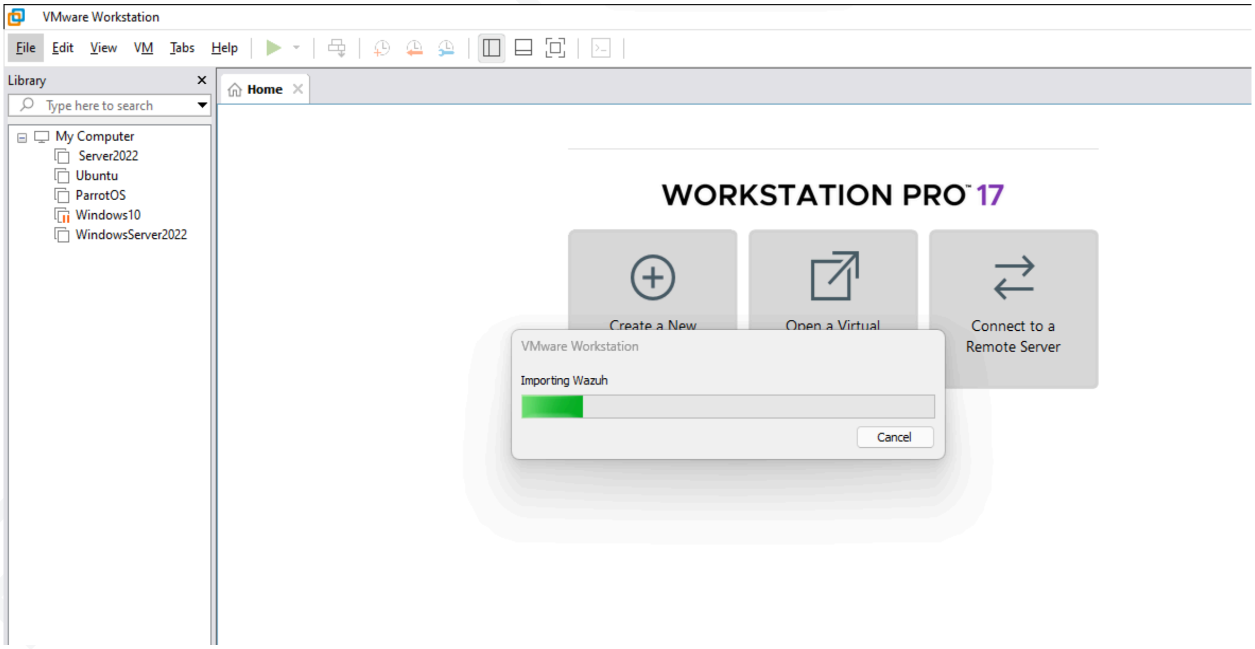
## Deployment of Wazuh Agent and File Integrity Monitoring Configuration

**Description**: This project details the deployment of a Windows Computer as a Wazuh agent on the Wazuh platform for endpoint security, as well as the configuration of File Integrity Monitoring (FIM) to monitor file changes and report them in the Wazuh dashboard.

Wazuh enhances security visibility by monitoring endpoints at the operating system and application levels. Its capabilities include log analysis, file integrity monitoring, intrusion detection, and compliance monitoring.

### PART 1: Deployment of Wazuh in VMware

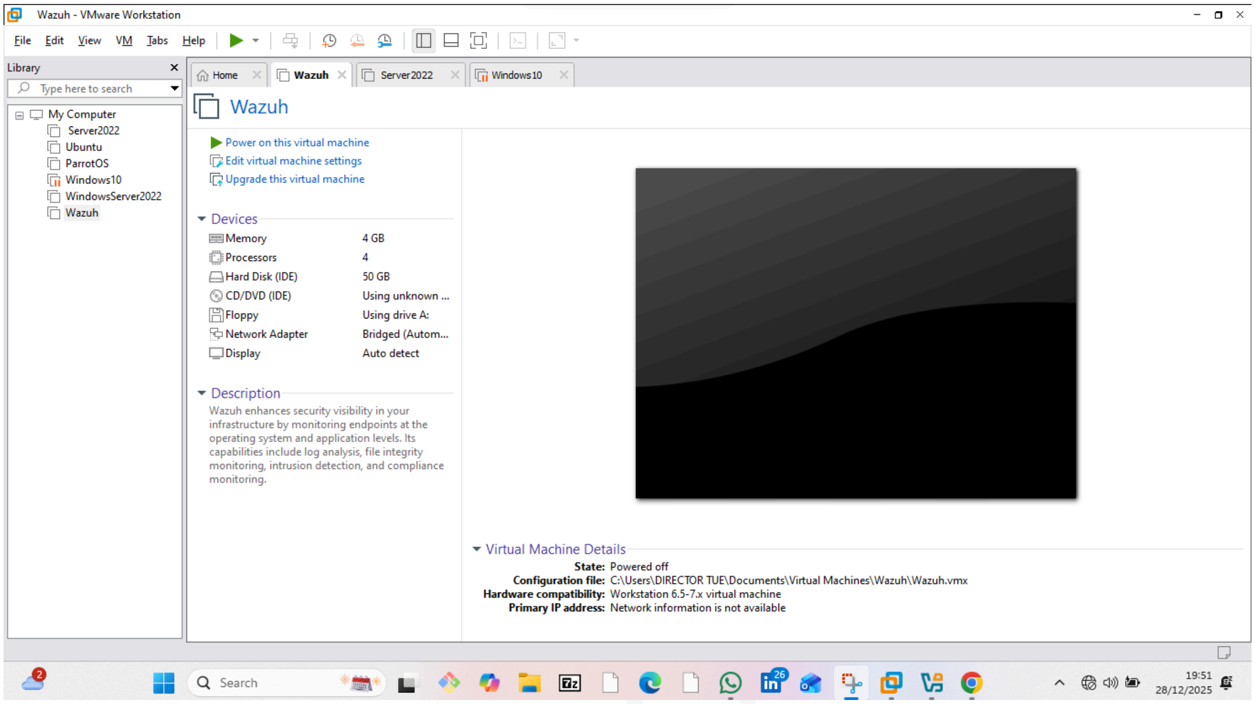
1. Download the Wazuh OVA from the Wazuh page (https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html)
2. Click on *"File"*, then click on Open, then import the Wazuh OVA into VMware



VMware Workstation

Importing Wazuh

3. After a successful import, the Wazuh VM would be in the list of VMs with the default requirement to run the Wazuh VM



Wazuh

Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

| | |
|---|---|
| Memory | 4 GB |
| Processors | 4 |
| Hard Disk (IDE) | 50 GB |
| CD/DVD (IDE) | Using unknown ... |
| Floppy | Using drive A: |
| Network Adapter | Bridged (Autom... |
| Display | Auto detect |

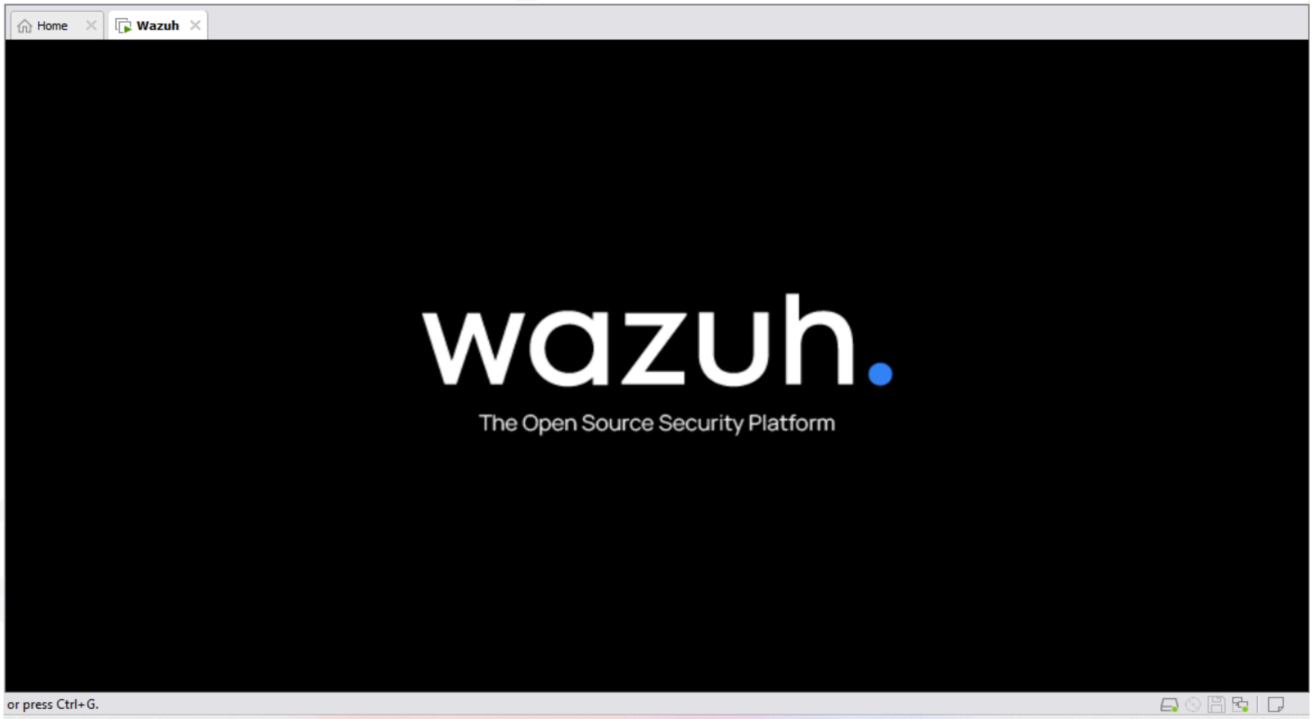
Description

Wazuh enhances security visibility in your infrastructure by monitoring endpoints at the operating system and application levels. Its capabilities include log analysis, file integrity monitoring, intrusion detection, and compliance monitoring.

Virtual Machine Details

State: Powered off
Configuration file: C:\Users\DIRECTOR TUE\Documents\Virtual Machines\Wazuh\Wazuh.vmx
Hardware compatibility: Workstation 6.5-7.x virtual machine
Primary IP address: Network information is not available

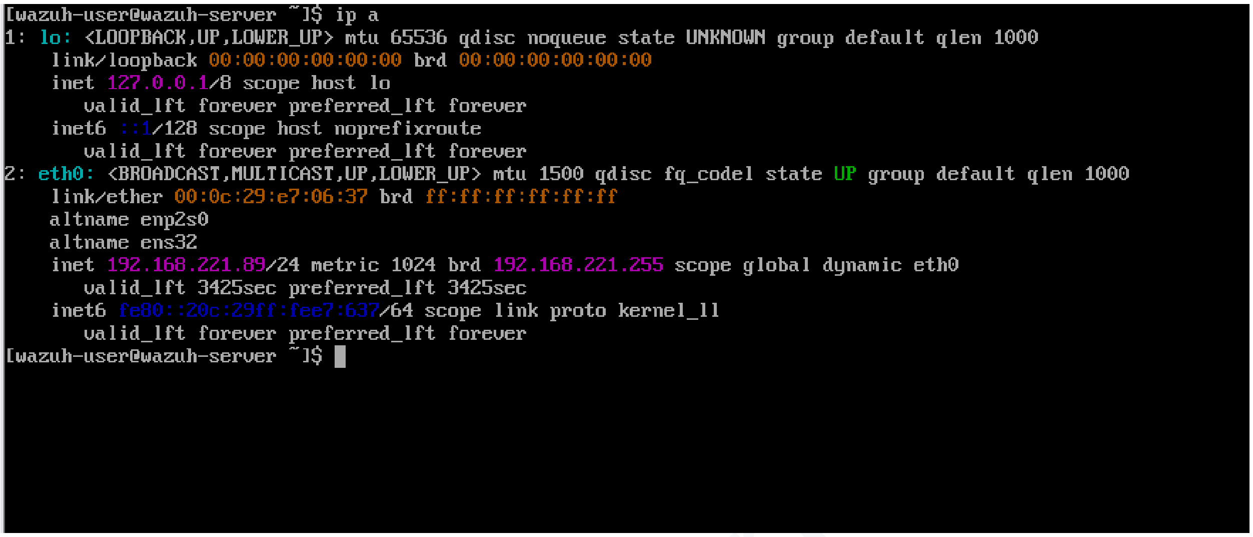
4. Run and start the Wazuh VM. I run mine with a baseline requirement of 4GB RAM and 4 CPUs



or press Ctrl+G.

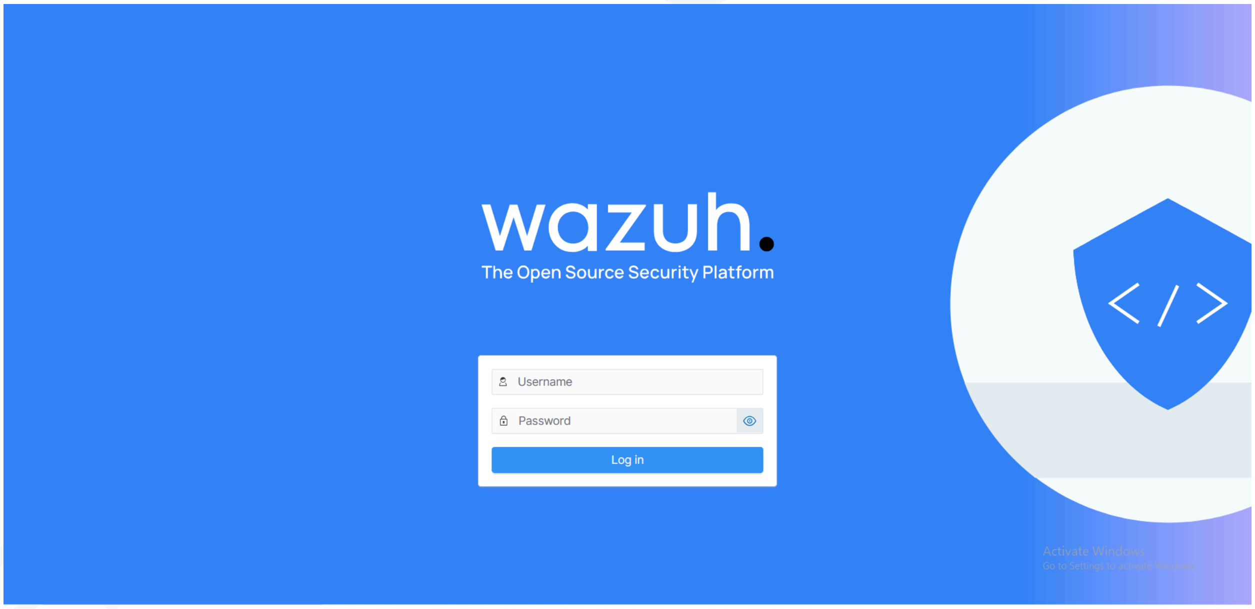
5. Check the IP allocated to the Wazuh VM to be able to access it through the browser (the network interface adapter is the bridged adapter; the IP address allocated in my case is 192.168.221.89).

The Wazuh VM CLI login credentials are username: wazuh-user and password:wazuh



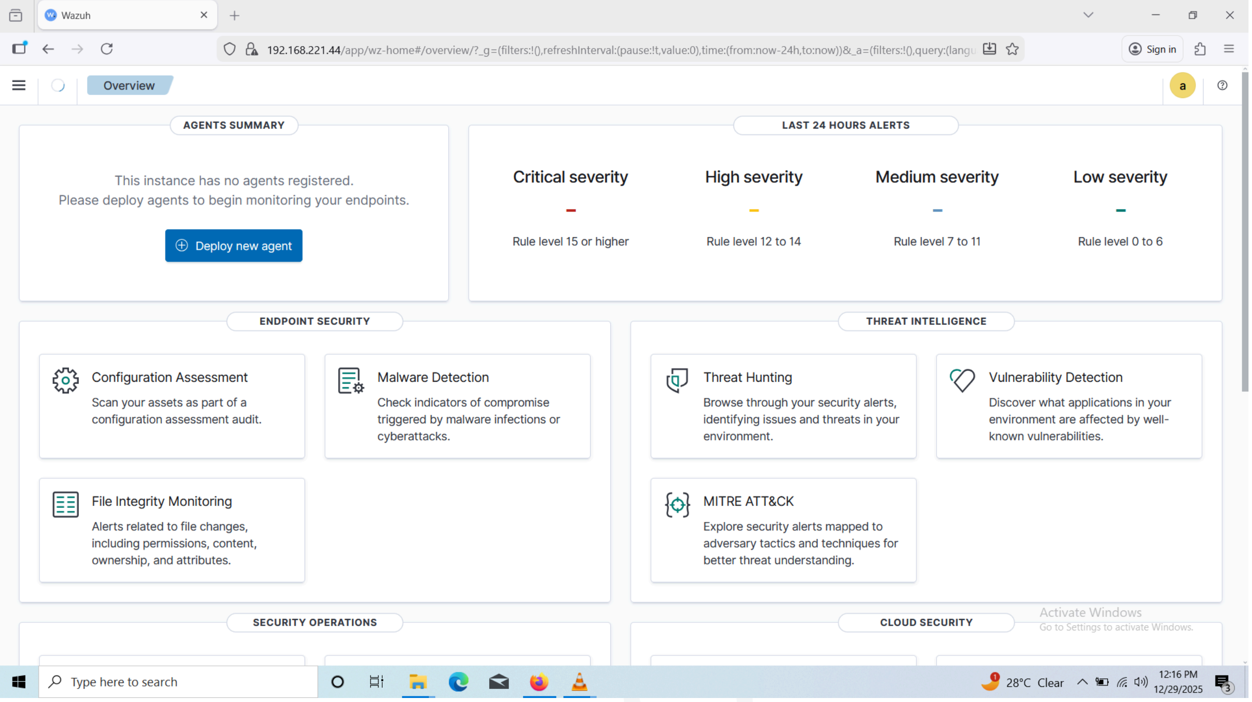
```
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e7:06:37 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname ens32
    inet 192.168.221.89/24 metric 1024 brd 192.168.221.255 scope global dynamic eth0
       valid_lft 3425sec preferred_lft 3425sec
    inet6 fe80::20c:29ff:fee7:637/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$ 
```

6. Access the Wazuh Dashboard through the browser using the IP address allocated to the Wazuh VM and logging in with the username: admin and password: admin


wazuh.
The Open Source Security Platform
Username
Password
Log in
Activate Windows
Go to Settings to activate Windows.

## Part 2: Agent Deployment

1. On the Wazuh Dashboard, click on the ***"Deploy new agent"***, which would bring up the prompt to determine the OS on which the agent would be installed on



Wazuh
192.168.221.44/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),query:(langu
Sign in
Overview
a
Type here to search
28°C Clear
12:16 PM
12/29/2025
Activate Windows
Go to Settings to activate Windows.

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

| Critical severity | High severity | Medium severity | Low severity |
|---|---|---|---|
| - | - | - | - |
| Rule level 15 or higher | Rule level 12 to 14 | Rule level 7 to 11 | Rule level 0 to 6 |

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

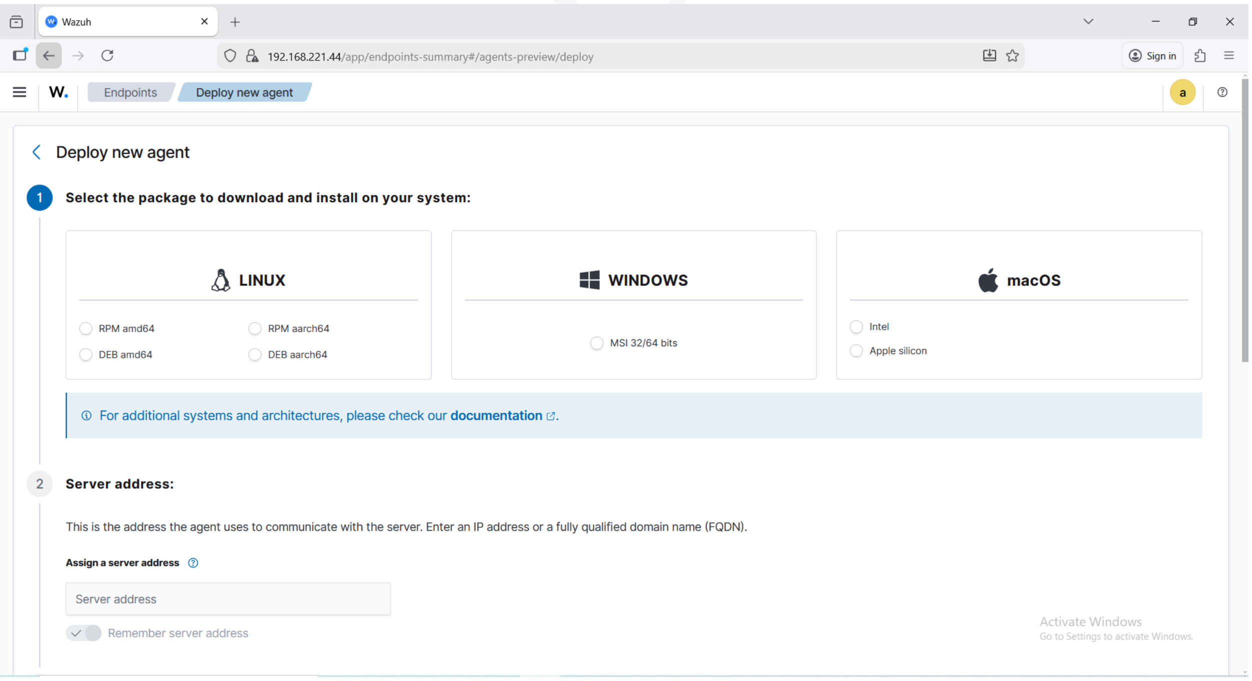
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

CLOUD SECURITY

2. For my own case, I clicked on the ***"Windows OS"*** as it is the OS that the agent would deploy on, then used the PowerShell command to install the Wazuh agent



Wazuh
192.168.221.44/app/endpoints-summary#/agents-preview/deploy
Sign in
W.
Endpoints
Deploy new agent
a
Activate Windows
Go to Settings to activate Windows.

Deploy new agent

1 Select the package to download and install on your system:

| LINUX | WINDOWS | macOS |
|---|---|---|
| ○ RPM amd64<br>○ DEB amd64<br>○ RPM aarch64<br>○ DEB aarch64 | ○ MSI 32/64 bits | ○ Intel<br>○ Apple silicon |

For additional systems and architectures, please check our **documentation**.

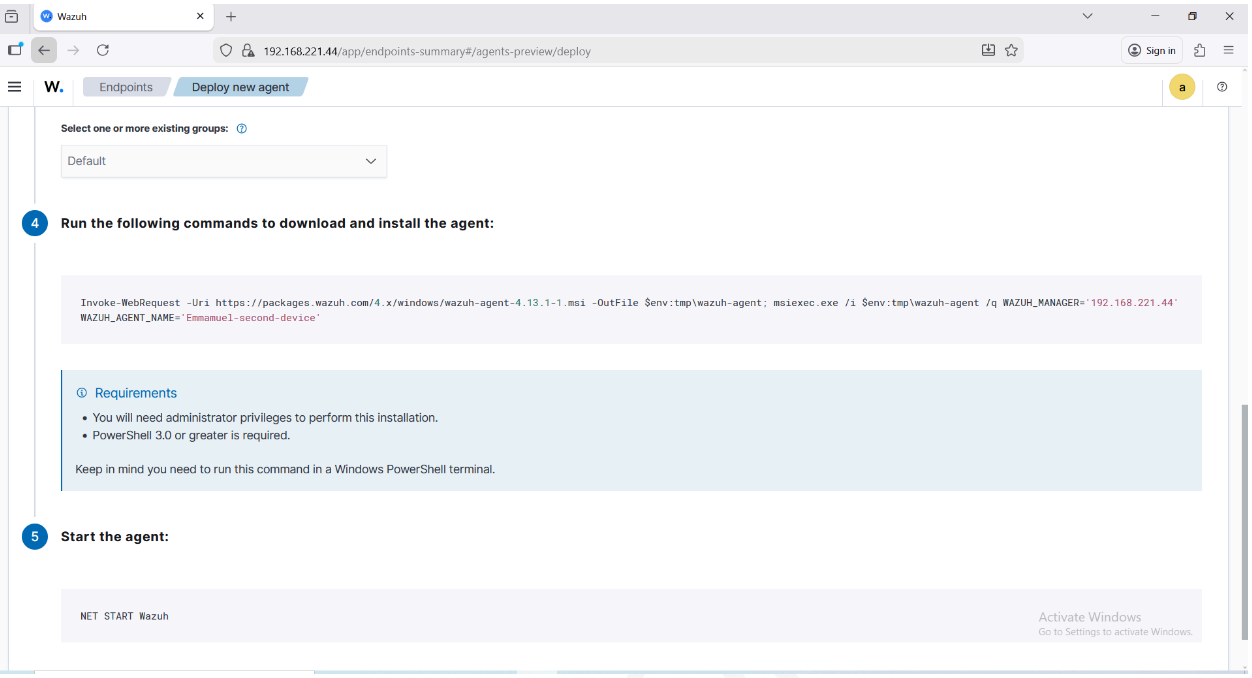
2 Server address:

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

**Assign a server address**

Server address

Remember server address


Wazuh
192.168.221.44/app/endpoints-summary#/agents-preview/deploy
Sign in
W.
Endpoints
Deploy new agent
a
Activate Windows
Go to Settings to activate Windows.

Select one or more existing groups:

Default

4 Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.13.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.221.44'
WAZUH_AGENT_NAME='Emmamuel-second-device'
```

Requirements

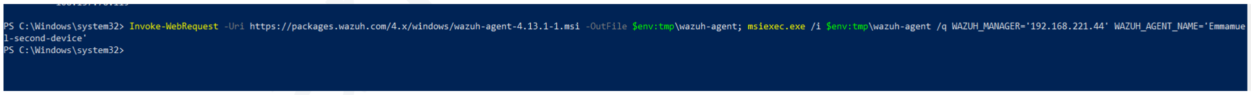
- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

5 Start the agent:

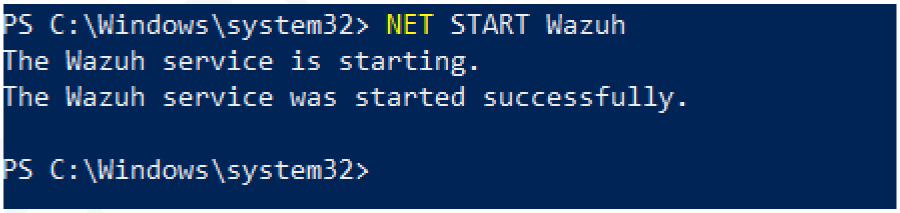
```
NET START Wazuh
```

3. Open PowerShell and run the command displayed by Wazuh to install the Windows agent and start the Wazuh agent
   In my case, the command is
   ***Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.13.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.221.44' WAZUH_AGENT_NAME='Emmamuel-second-device'***



```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.13.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.221.44' WAZUH_AGENT_NAME='Emmamue
l-second-device'
PS C:\Windows\system32>
```

4. Start the Wazuh agent using the command ***"NET START Wazuh"***

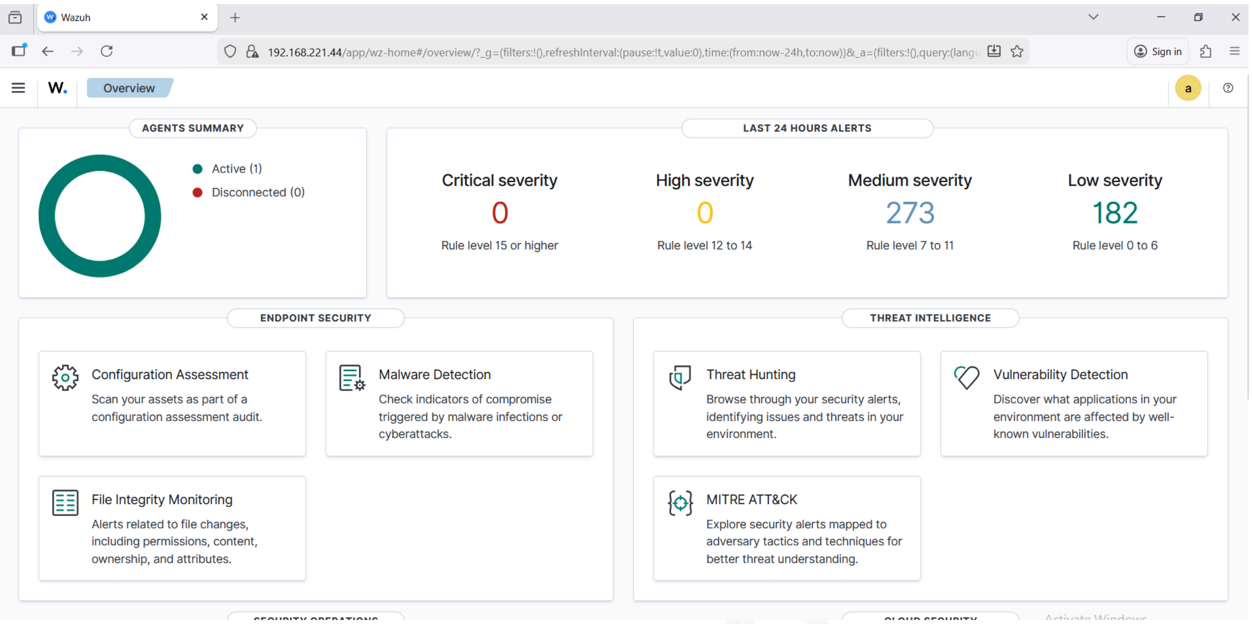


```
PS C:\Windows\system32> NET START Wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

5. Verification of the Agent being active

   After the agent is deployed, we can confirm the deployment status on the dashboard



| Critical severity | High severity | Medium severity | Low severity |
|---|---|---|---|
| 0 | 0 | 273 | 182 |
| Rule level 15 or higher | Rule level 12 to 14 | Rule level 7 to 11 | Rule level 0 to 6 |

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

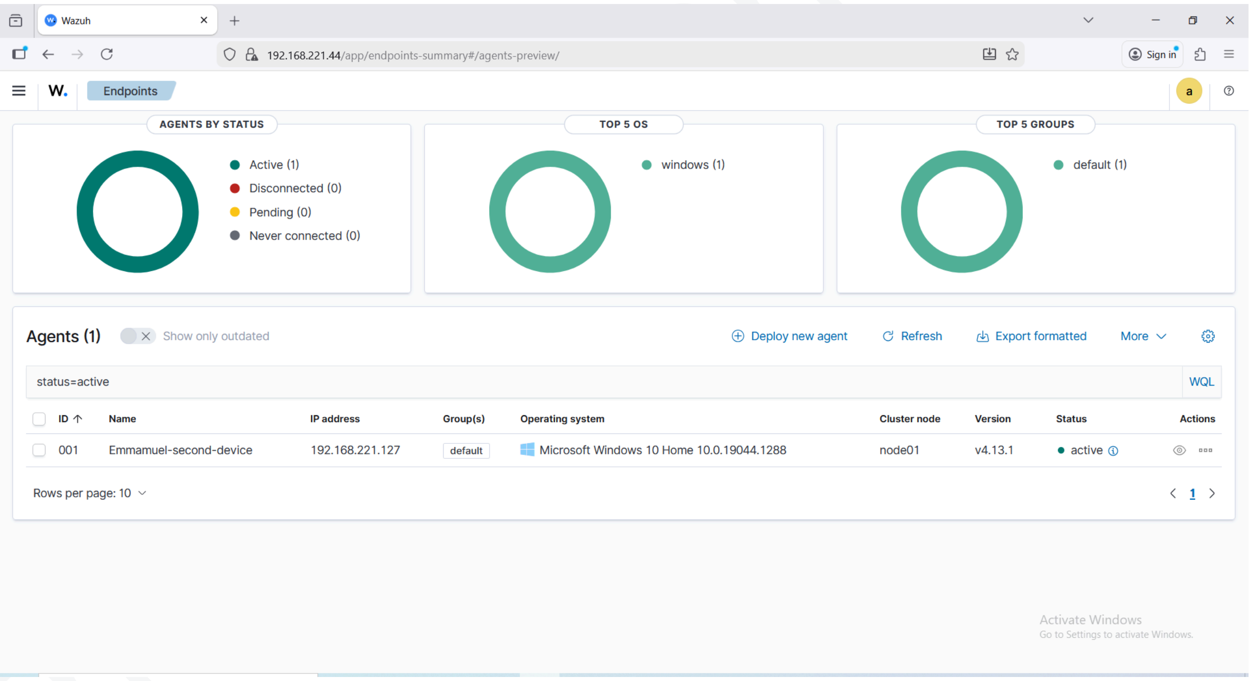
Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.



status=active

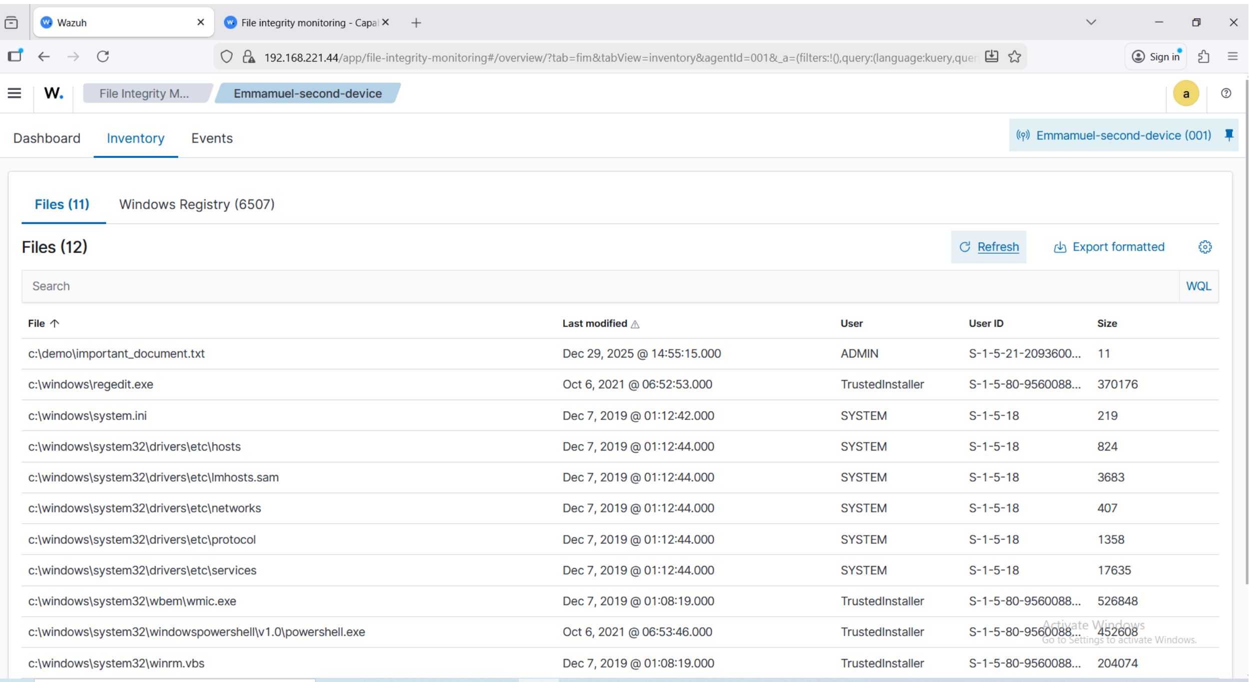
| ID ↑ | Name | IP address | Group(s) | Operating system | Cluster node | Version | Status | Actions |
|---|---|---|---|---|---|---|---|---|
| 001 | Emmamuel-second-device | 192.168.221.127 | default | Microsoft Windows 10 Home 10.0.19044.1288 | node01 | v4.13.1 | ● active | |

## Part 3: File Integrity Monitoring Configuration

1. To configure File Integrity Monitoring, we would need to modify the ossec.conf configuration file in the agent. For Windows, open Notepad in administrator mode, then navigate to the wazuh-agent file, then to the ossec.conf, and then scroll to the section that details File Monitoring, then change the frequency tags to 60 (this ensures faster results when observing change), and create a

new directories tag to contain the file to be monitored with attributes ***“check_all = “yes””*** under the ***“syscheck”*** block

2. The ***“Inventory”*** session of the File Integrity Monitoring dashboard shows that the ***“c/demo/important_document.txt”*** file has been added to be monitored



192.168.221.44/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&agentId=001&_a=(filters:!(),query:(language:kuery,quer

File Integrity M... / Emmamuel-second-device

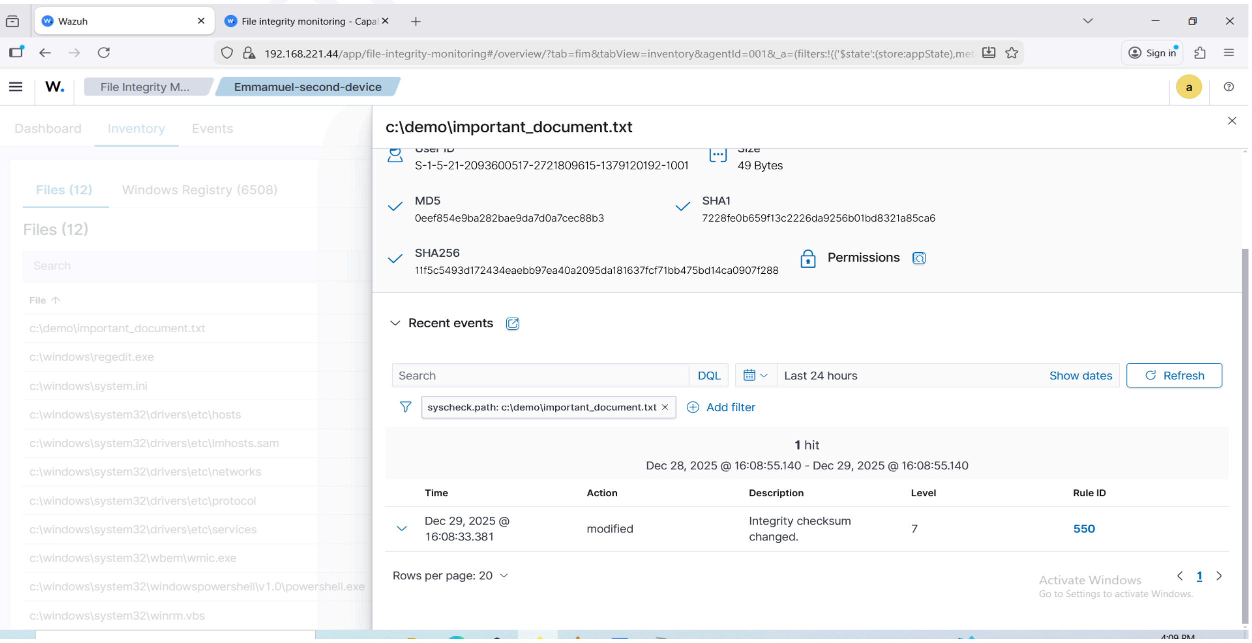
Dashboard | Inventory | Events — Emmamuel-second-device (001)

Files (11) | Windows Registry (6507)

Files (12) — Refresh | Export formatted

| File | Last modified | User | User ID | Size |
|---|---|---|---|---|
| c:\demo\important_document.txt | Dec 29, 2025 @ 14:55:15.000 | ADMIN | S-1-5-21-2093600... | 11 |
| c:\windows\regedit.exe | Oct 6, 2021 @ 06:52:53.000 | TrustedInstaller | S-1-5-80-9560088... | 370176 |
| c:\windows\system.ini | Dec 7, 2019 @ 01:12:42.000 | SYSTEM | S-1-5-18 | 219 |
| c:\windows\system32\drivers\etc\hosts | Dec 7, 2019 @ 01:12:44.000 | SYSTEM | S-1-5-18 | 824 |
| c:\windows\system32\drivers\etc\lmhosts.sam | Dec 7, 2019 @ 01:12:44.000 | SYSTEM | S-1-5-18 | 3683 |
| c:\windows\system32\drivers\etc\networks | Dec 7, 2019 @ 01:12:44.000 | SYSTEM | S-1-5-18 | 407 |
| c:\windows\system32\drivers\etc\protocol | Dec 7, 2019 @ 01:12:44.000 | SYSTEM | S-1-5-18 | 1358 |
| c:\windows\system32\drivers\etc\services | Dec 7, 2019 @ 01:12:44.000 | SYSTEM | S-1-5-18 | 17635 |
| c:\windows\system32\wbem\wmic.exe | Dec 7, 2019 @ 01:08:19.000 | TrustedInstaller | S-1-5-80-9560088... | 526848 |
| c:\windows\system32\windowspowershell\v1.0\powershell.exe | Oct 6, 2021 @ 06:53:46.000 | TrustedInstaller | S-1-5-80-9560088... | 452608 |
| c:\windows\system32\winrm.vbs | Dec 7, 2019 @ 01:08:19.000 | TrustedInstaller | S-1-5-80-9560088... | 204074 |

3. The document in the file was modified and deleted to observe and verify the configuration of the file integrity monitoring setup, and Policies matching **rule 550 and 553 observed a change**



192.168.221.44/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&agentId=001&_a=(filters:!(('$state':(store:appState),met

c:\demo\important_document.txt

User ID: S-1-5-21-2093600517-2721809615-1379120192-1001 — Size: 49 Bytes

MD5: 0eef854e9ba282bae9da7d0a7cec88b3

SHA1: 7228fe0b659f13c2226da9256b01bd8321a85ca6

SHA256: 11f5c5493d172434eaebb97ea40a2095da181637fcf71bb475bd14ca0907f288

Permissions

Recent events

Search | DQL | Last 24 hours | Show dates | Refresh

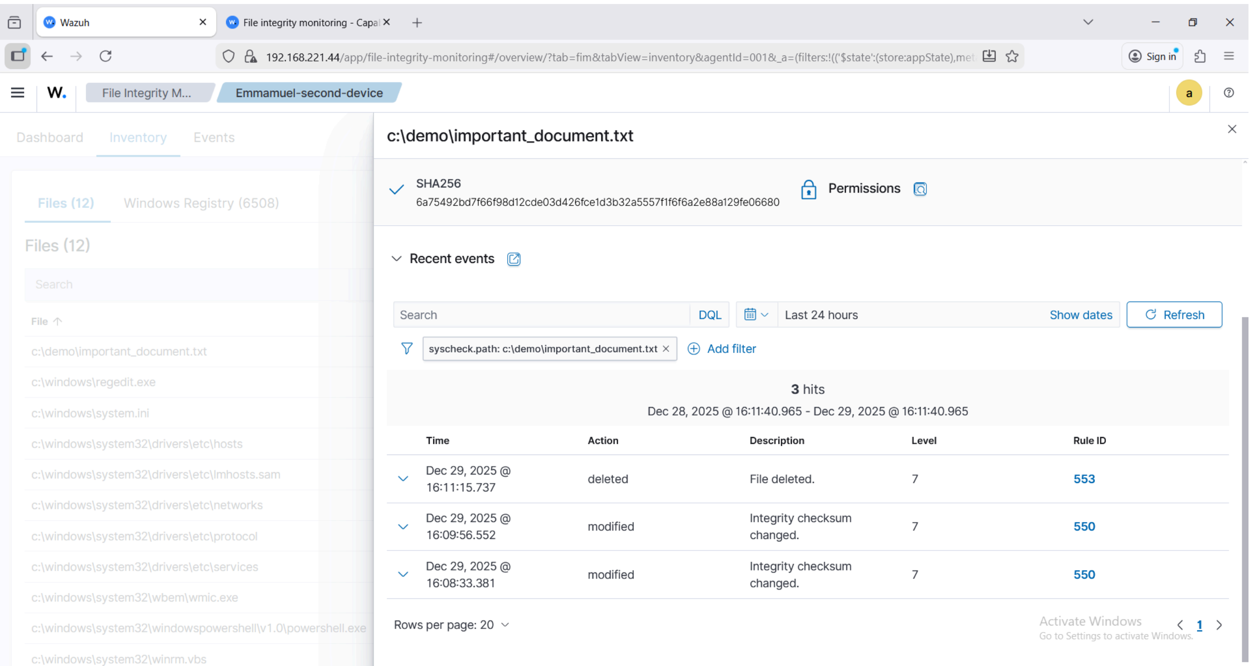
syscheck.path: c:\demo\important_document.txt — Add filter

1 hit

Dec 28, 2025 @ 16:08:55.140 - Dec 29, 2025 @ 16:08:55.140

| Time | Action | Description | Level | Rule ID |
|---|---|---|---|---|
| Dec 29, 2025 @ 16:08:33.381 | modified | Integrity checksum changed. | 7 | 550 |

Rows per page: 20



192.168.221.44/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&agentId=001&_a=(filters:!(('$state':(store:appState),me

File Integrity M... / Emmamuel-second-device

Dashboard | Inventory | Events

Files (12) | Windows Registry (6508)

Files (12)

| File |
|---|
| c:\demo\important_document.txt |
| c:\windows\regedit.exe |
| c:\windows\system.ini |
| c:\windows\system32\drivers\etc\hosts |
| c:\windows\system32\drivers\etc\lmhosts.sam |
| c:\windows\system32\drivers\etc\networks |
| c:\windows\system32\drivers\etc\protocol |
| c:\windows\system32\drivers\etc\services |
| c:\windows\system32\wbem\wmic.exe |
| c:\windows\system32\windowspowershell\v1.0\powershell.exe |
| c:\windows\system32\winrm.vbs |

c:\demo\important_document.txt

SHA256
6a75492bd7f66f98d12cde03d426fce1d3b32a5557f1f6f6a2e88a129fe06680

Permissions

Recent events

Search | DQL | Last 24 hours | Show dates | Refresh

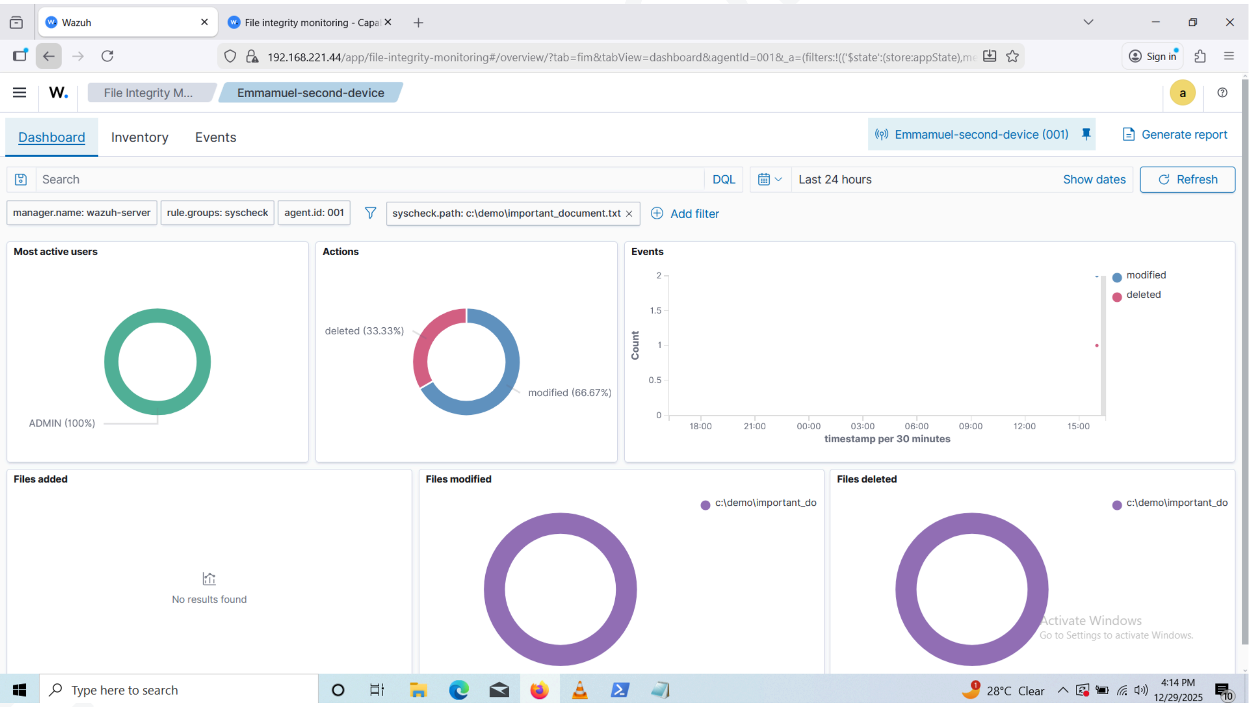
syscheck.path: c:\demo\important_document.txt | Add filter

3 hits
Dec 28, 2025 @ 16:11:40.965 - Dec 29, 2025 @ 16:11:40.965

| Time | Action | Description | Level | Rule ID |
|---|---|---|---|---|
| Dec 29, 2025 @ 16:11:15.737 | deleted | File deleted. | 7 | 553 |
| Dec 29, 2025 @ 16:09:56.552 | modified | Integrity checksum changed. | 7 | 550 |
| Dec 29, 2025 @ 16:08:33.381 | modified | Integrity checksum changed. | 7 | 550 |

Rows per page: 20

Activate Windows
Go to Settings to activate Windows.



192.168.221.44/app/file-integrity-monitoring#/overview/?tab=fim&tabView=dashboard&agentId=001&_a=(filters:!(('$state':(store:appState),m

File Integrity M... / Emmamuel-second-device

Dashboard | Inventory | Events | Emmamuel-second-device (001) | Generate report

Search | DQL | Last 24 hours | Show dates | Refresh

manager.name: wazuh-server | rule.groups: syscheck | agent.id: 001 | syscheck.path: c:\demo\important_document.txt | Add filter

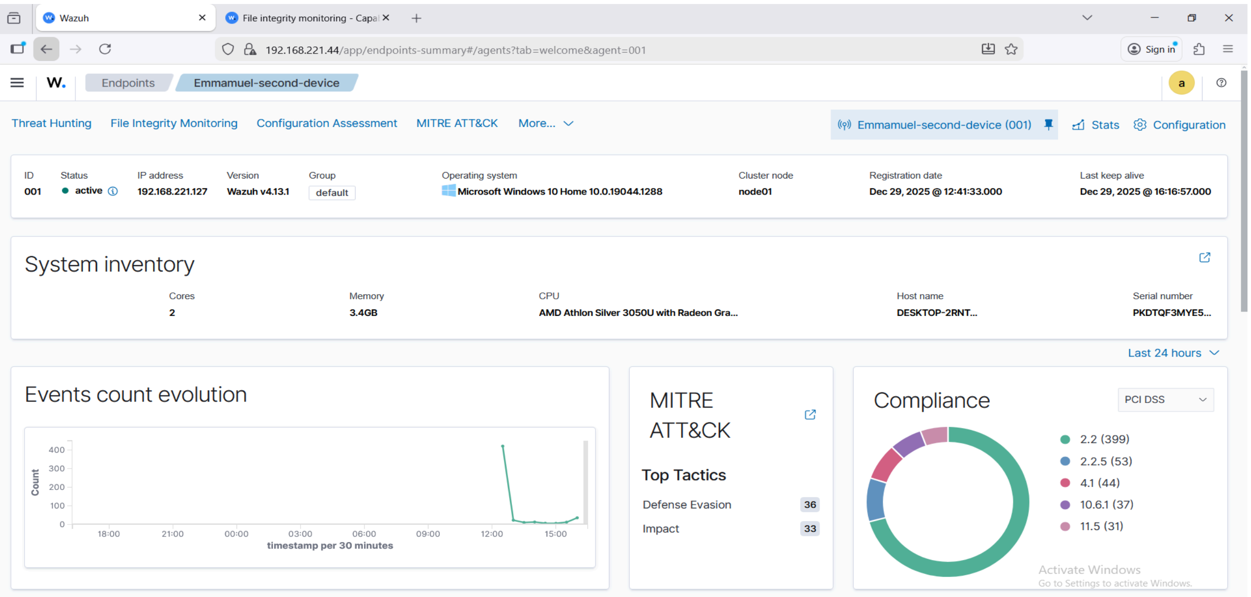
Activate Windows
Go to Settings to activate Windows.

Type here to search | 28°C Clear | 4:14 PM 12/29/2025

## Compliance Monitoring in Wazuh

Wazuh provides the capability to monitor compliance with various standards and regulations, such as PCI DSS and GDPR, through its compliance dashboard, allowing users to observe and generate compliance reports. Snippet below shows how FIM processes comply with

PCI DSS and GDPR; this report can then be used to understand how to be compliant



Wazuh | File integrity monitoring - Capa

192.168.221.44/app/endpoints-summary#/agents?tab=welcome&agent=001

Endpoints / Emmamuel-second-device

Threat Hunting | File Integrity Monitoring | Configuration Assessment | MITRE ATT&CK | More...

Emmamuel-second-device (001) | Stats | Configuration

| ID | Status | IP address | Version | Group | Operating system | Cluster node | Registration date | Last keep alive |
|---|---|---|---|---|---|---|---|---|
| 001 | active | 192.168.221.127 | Wazuh v4.13.1 | default | Microsoft Windows 10 Home 10.0.19044.1288 | node01 | Dec 29, 2025 @ 12:41:33.000 | Dec 29, 2025 @ 16:16:57.000 |

System inventory

| Cores | Memory | CPU | Host name | Serial number |
|---|---|---|---|---|
| 2 | 3.4GB | AMD Athlon Silver 3050U with Radeon Gra... | DESKTOP-2RNT... | PKDTQF3MYE5... |

Last 24 hours

Events count evolution

MITRE ATT&CK

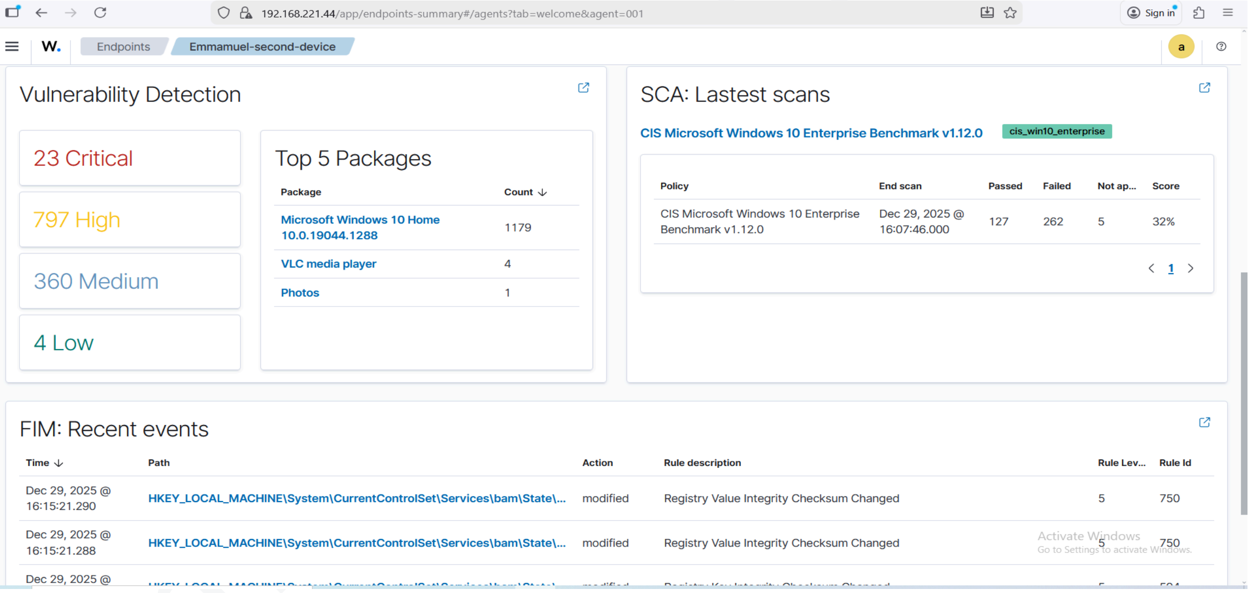
Top Tactics

| | |
|---|---|
| Defense Evasion | 36 |
| Impact | 33 |

Compliance

PCI DSS

Activate Windows
Go to Settings to activate Windows.



192.168.221.44/app/endpoints-summary#/agents?tab=welcome&agent=001

Endpoints / Emmamuel-second-device

Vulnerability Detection

23 Critical

797 High

360 Medium

4 Low

Top 5 Packages

| Package | Count ↓ |
|---|---|
| Microsoft Windows 10 Home 10.0.19044.1288 | 1179 |
| VLC media player | 4 |
| Photos | 1 |

SCA: Lastest scans

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 cis_win10_enterprise

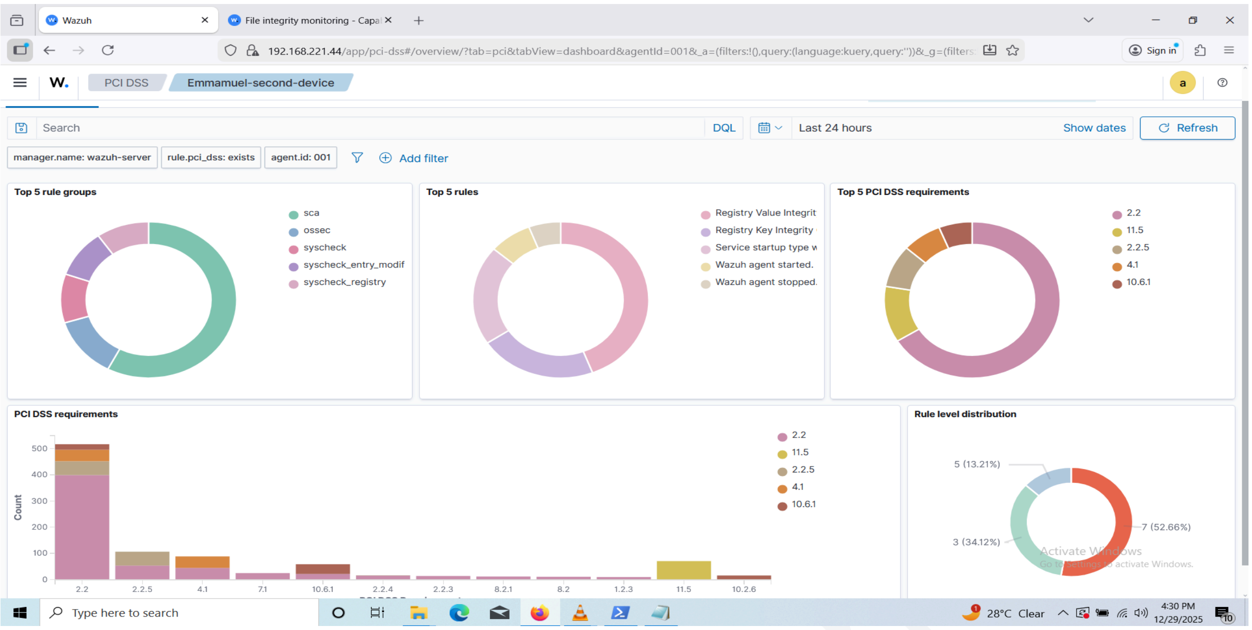
| Policy | End scan | Passed | Failed | Not ap... | Score |
|---|---|---|---|---|---|
| CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 | Dec 29, 2025 @ 16:07:46.000 | 127 | 262 | 5 | 32% |

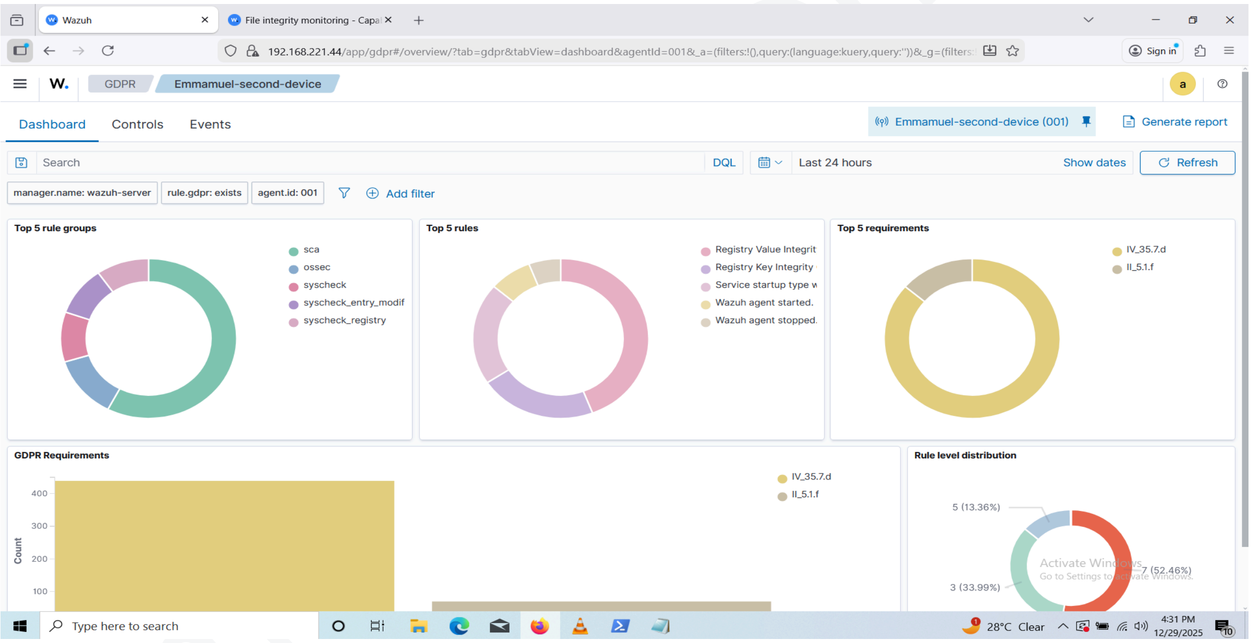
‹ 1 ›

FIM: Recent events

| Time ↓ | Path | Action | Rule description | Rule Lev... | Rule Id |
|---|---|---|---|---|---|
| Dec 29, 2025 @ 16:15:21.290 | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\... | modified | Registry Value Integrity Checksum Changed | 5 | 750 |
| Dec 29, 2025 @ 16:15:21.288 | HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\bam\State\... | modified | Registry Value Integrity Checksum Changed | 5 | 750 |
| Dec 29, 2025 @ | | | | | |

Activate Windows
Go to Settings to activate Windows.





**Summary:** This project successfully deployed a Windows Wazuh agent and configured File Integrity Monitoring (FIM). Wazuh was set up in a VMware environment, and the agent was installed on a Windows OS using PowerShell. FIM was then configured by modifying the ossec.conf file on the agent to monitor specific files (c/demo/important_document.txt). The modifications (edit and deletion) of the monitored file were successfully detected and reported on the Wazuh dashboard, confirming the FIM setup. The document also briefly highlights Wazuh's compliance monitoring capabilities (PCI DSS, GDPR).