OSSEC Installation

Sunday, February 16, 2025 6:31 PM

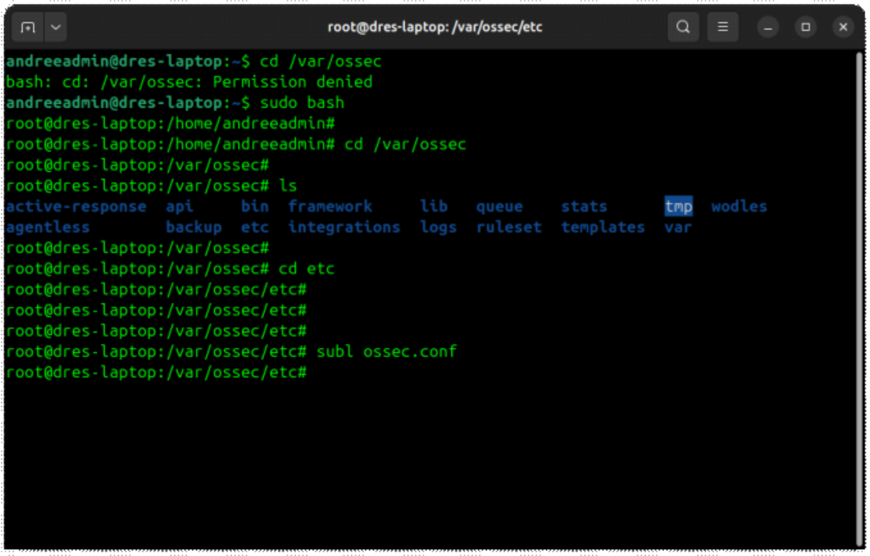
Explanation: On Ubuntu running the cd /var/ossec root directory, stores and configures files, logs, rules, and many other important components that are operational.

What the /var/ossec does?:

- **/var/ossec/logs/ > Stores logs generated by Wazuh, including alerts.**
- **/var/ossec/etc/ > Configures files (ossec.conf, rules, and decoders).**
- **/var/ossec/queue/ > This handles real-time events which proccess and communicate with agents.**

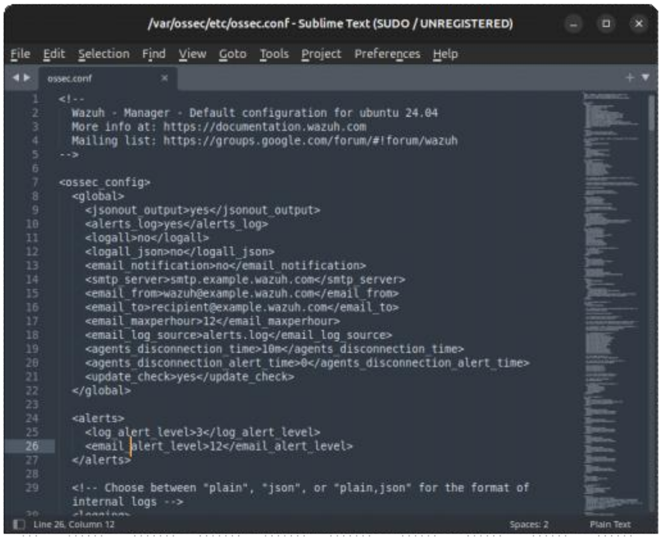
OSSEC terminal step by step guide:

- **On terminal by typing the command cd /var/ossec wouldn't work because its owned by root and will grant the permission being denied.**
- **To access the root user simply type the command > sudo bash**
- **Simply type ls > ls will show you all the list of directories**
- **What I focused on was typing cd etc directory> reason being is because I needed to get into the ossec.conf file**



```
andreeadmin@dres-laptop:~$ cd /var/ossec
bash: cd: /var/ossec: Permission denied
andreeadmin@dres-laptop:~$ sudo bash
root@dres-laptop:/home/andreeadmin#
root@dres-laptop:/home/andreeadmin# cd /var/ossec
root@dres-laptop:/var/ossec#
root@dres-laptop:/var/ossec# ls
active-response  api     bin  framework     lib   queue    stats      tmp  wodles
agentless        backup  etc  integrations  logs  ruleset  templates  var
root@dres-laptop:/var/ossec#
root@dres-laptop:/var/ossec# cd etc
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc# subl ossec.conf
root@dres-laptop:/var/ossec/etc#
```

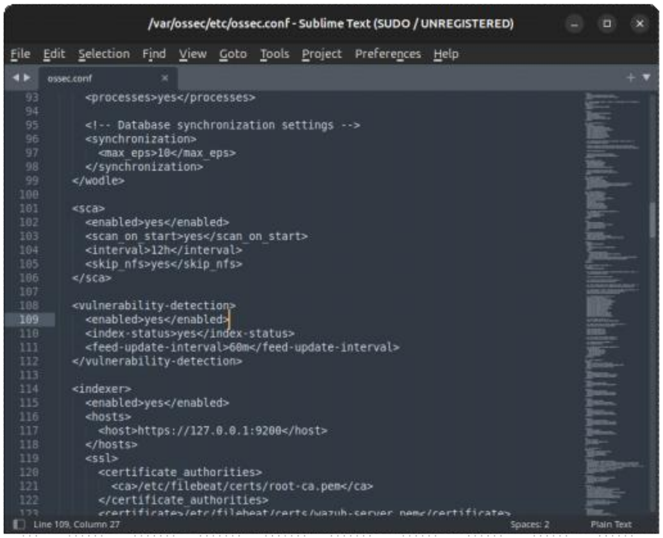
- **To open the file type > subl ossec.conf**
- **Once the file is open it will show you all configuration to configure your alerts, logging format, and how it will be communicated /var/ossec.conf file picture:**

- 
/var/ossec/etc/ossec.conf - Sublime Text (SUDO / UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
ossec.conf
Line 26, Column 12
Spaces: 2
Plain Text

```
<!--
  Wazuh - Manager - Default configuration for ubuntu 24.04
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>

  <!-- Choose between "plain", "json", or "plain,json" for the format of
  internal logs -->
  <logging>
```

Vulnerability detector:

Explanation: my key focus was on the Vulnerability Detector is because it helps identify security weaknesses in my system by scanning for known vulnerabilities in installed software.

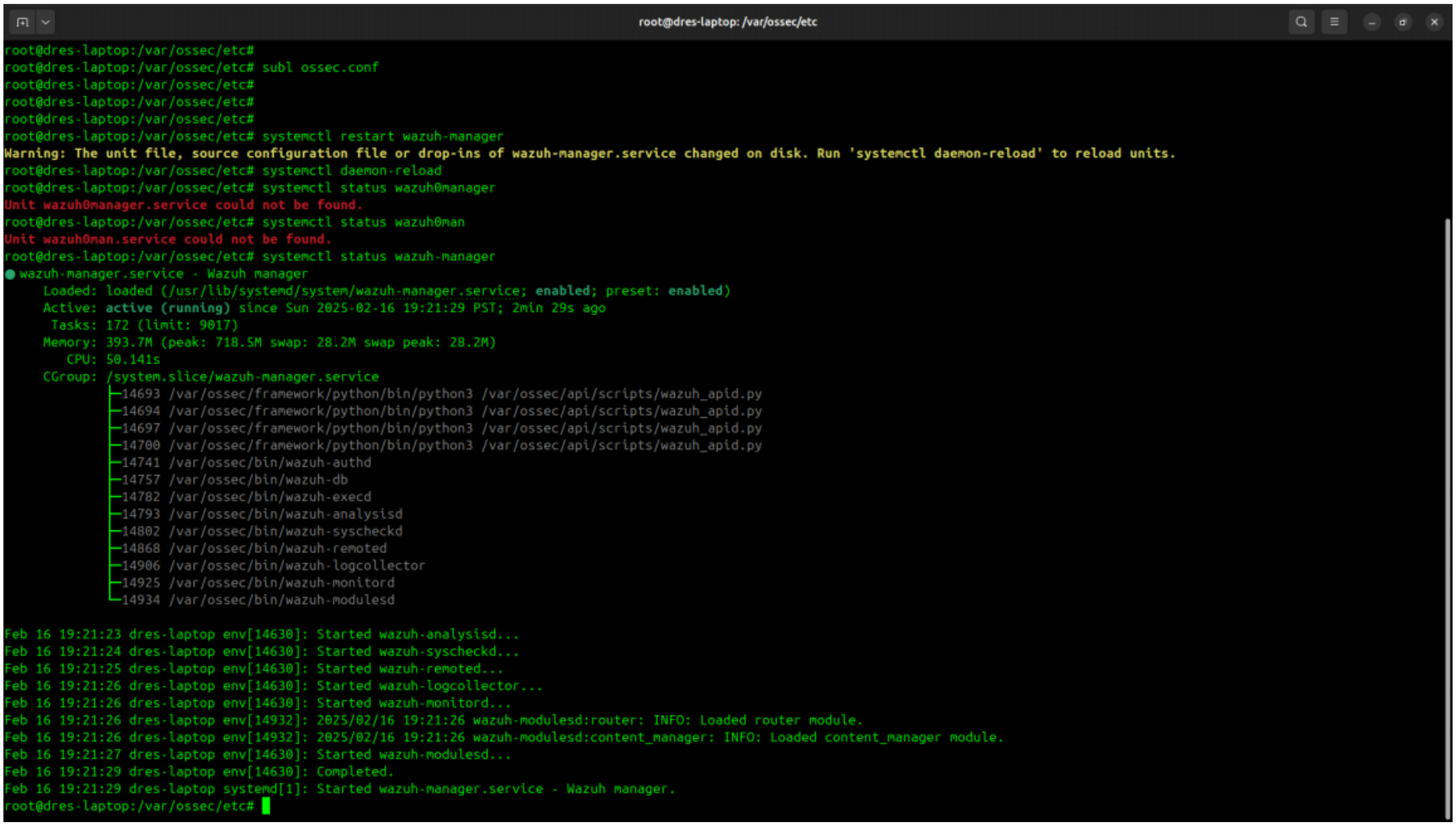

/var/ossec/etc/ossec.conf - Sublime Text (SUDO / UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
ossec.conf
Line 109, Column 27
Spaces: 2
Plain Text

```
      <processes>yes</processes>

      <!-- Database synchronization settings -->
      <synchronization>
        <max_eps>10</max_eps>
      </synchronization>
    </wodle>

    <sca>
      <enabled>yes</enabled>
      <scan_on_start>yes</scan_on_start>
      <interval>12h</interval>
      <skip_nfs>yes</skip_nfs>
    </sca>

    <vulnerability-detection>
      <enabled>yes</enabled>
      <index-status>yes</index-status>
      <feed-update-interval>60m</feed-update-interval>
    </vulnerability-detection>

    <indexer>
      <enabled>yes</enabled>
      <hosts>
        <host>https://127.0.0.1:9200</host>
      </hosts>
      <ssl>
        <certificate_authorities>
          <ca>/etc/filebeat/certs/root-ca.pem</ca>
        </certificate_authorities>
        <certificate>/etc/filebeat/certs/wazuh-server.pem</certificate>
```

Once everything has been done I did a a system restart for the wazuh-manager

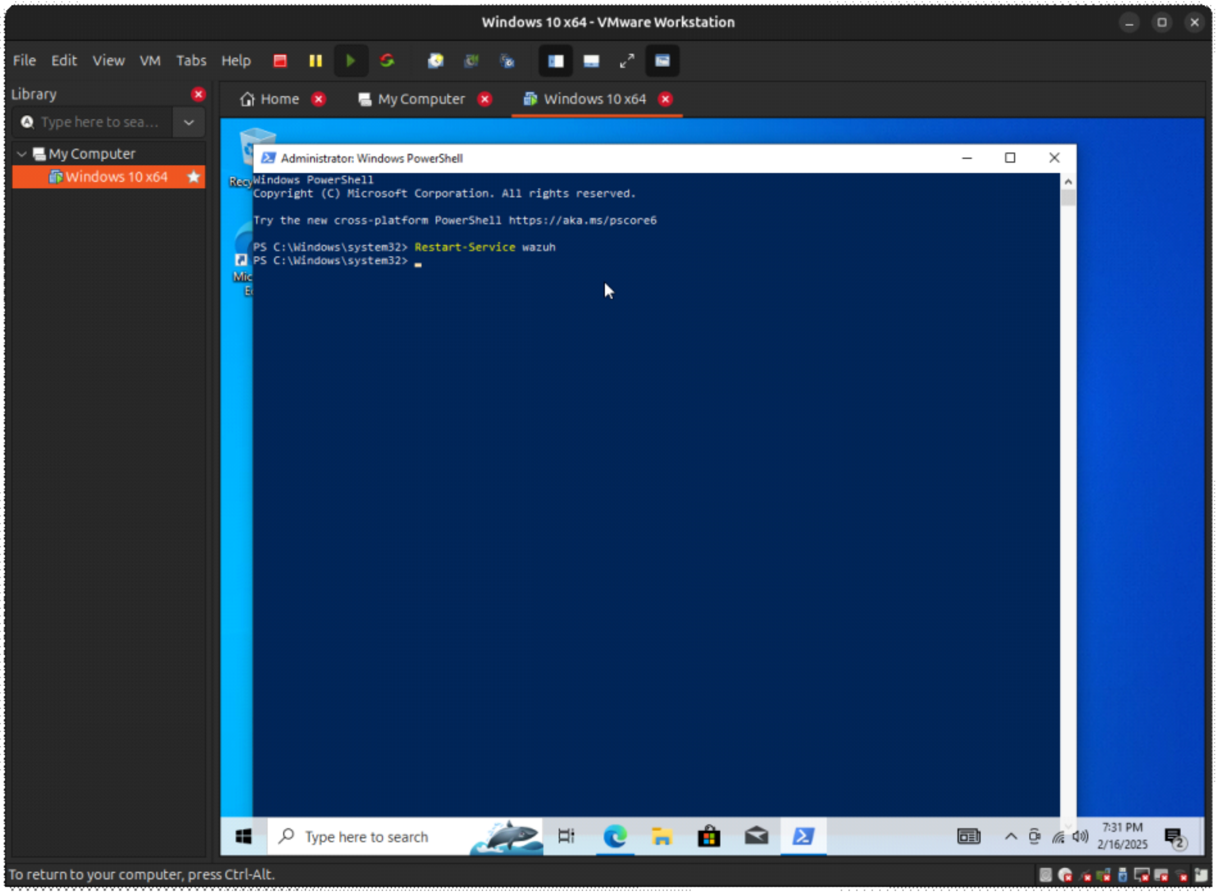
Commands:

- **Systemctl restart wazuh-manager (terminal)**
- **Restart-Service (Windows Powershell)**
- **There was no issues for me so the system was good and active and running**



```
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc# subl ossec.conf
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc#
root@dres-laptop:/var/ossec/etc# systemctl restart wazuh-manager
Warning: The unit file, source configuration file or drop-ins of wazuh-manager.service changed on disk. Run 'systemctl daemon-reload' to reload units.
root@dres-laptop:/var/ossec/etc# systemctl daemon-reload
root@dres-laptop:/var/ossec/etc# systemctl status wazuh0manager
Unit wazuh0manager.service could not be found.
root@dres-laptop:/var/ossec/etc# systemctl status wazuh0man
Unit wazuh0man.service could not be found.
root@dres-laptop:/var/ossec/etc# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-02-16 19:21:29 PST; 2min 29s ago
      Tasks: 172 (limit: 9017)
     Memory: 393.7M (peak: 718.5M swap: 28.2M swap peak: 28.2M)
        CPU: 50.141s
     CGroup: /system.slice/wazuh-manager.service
             ├─14693 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─14694 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─14697 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─14700 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             ├─14741 /var/ossec/bin/wazuh-authd
             ├─14757 /var/ossec/bin/wazuh-db
             ├─14782 /var/ossec/bin/wazuh-execd
             ├─14793 /var/ossec/bin/wazuh-analysisd
             ├─14802 /var/ossec/bin/wazuh-syscheckd
             ├─14868 /var/ossec/bin/wazuh-remoted
             ├─14906 /var/ossec/bin/wazuh-logcollector
             ├─14925 /var/ossec/bin/wazuh-monitord
             └─14934 /var/ossec/bin/wazuh-modulesd

Feb 16 19:21:23 dres-laptop env[14630]: Started wazuh-analysisd...
Feb 16 19:21:24 dres-laptop env[14630]: Started wazuh-syscheckd...
Feb 16 19:21:25 dres-laptop env[14630]: Started wazuh-remoted...
Feb 16 19:21:26 dres-laptop env[14630]: Started wazuh-logcollector...
Feb 16 19:21:26 dres-laptop env[14630]: Started wazuh-monitord...
Feb 16 19:21:26 dres-laptop env[14932]: 2025/02/16 19:21:26 wazuh-modulesd:router: INFO: Loaded router module.
Feb 16 19:21:26 dres-laptop env[14932]: 2025/02/16 19:21:26 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Feb 16 19:21:27 dres-laptop env[14630]: Started wazuh-modulesd...
Feb 16 19:21:29 dres-laptop env[14630]: Completed.
Feb 16 19:21:29 dres-laptop systemd[1]: Started wazuh-manager.service - Wazuh manager.
root@dres-laptop:/var/ossec/etc#
```

Windows Powershell:



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Restart-Service wazuh
PS C:\Windows\system32>
```

Installing software applications on windows 10:

Explanation: Once I restarted the agent in powershell, I went to

ninite.com to install a few software programs, to detect any possible vulnerabilities to my wazuh dashboard.

**As you can see on my wazuh dashboard, I clicked on my windows 10 vm desktop, The picture down below shows you what the agent had scanned on that vm and transferred the reports to my wazuh-manager. As you can see the vulnerabilities box, it scanned the detection of: **

- **5 = critical**
- **411 = high**
- **220 = medium**
- **3 = low**

It also scans like MITRE ATT&CKS, Compliance, Latest scans, and recent events

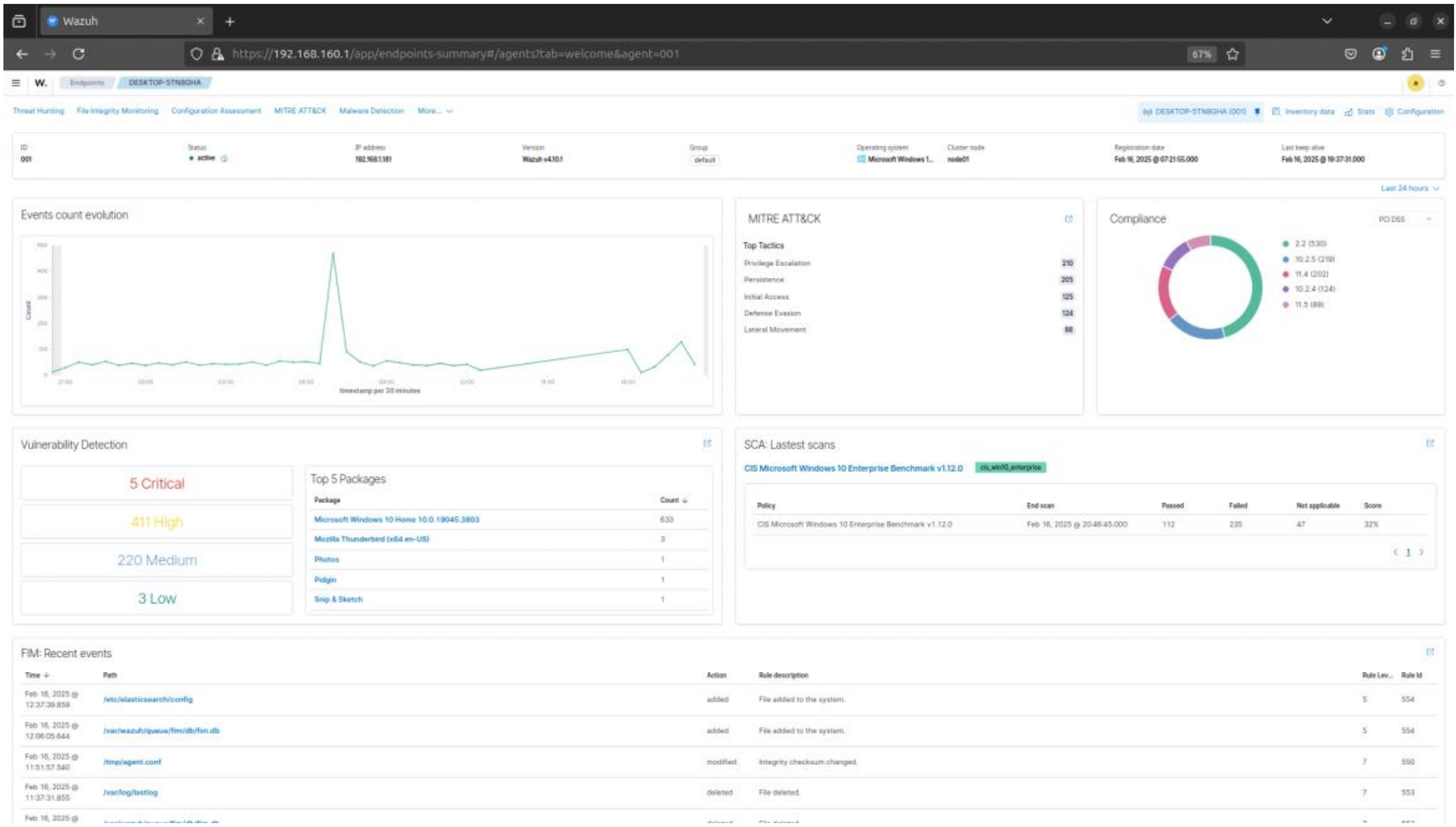
The FIM: Recent events, show you real-time File Integrity Monitoring (FIM) events, tracking any changes being made to critical system files and directories
What it does:

- **Detects file modification, deletion, and creations**
- **Monitors critical system files**
- **Provides a log of most recent file change events detected by Wazuh**

How it works:

1. **Wazuh scans monitored directories.**
2. **When a change occurs, Wazuh will log the events.**
3. **The FIM: Recent Events dashboard displays details such as.**

- **File Path (where the change happened).**
- **Change type (modified, created, and deleted).**
- **User & Process that made the change.**
- **Timestamp of the change.**



ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
001	● active	192.168.1.181	Wazuh v4.10.1	default	Microsoft Windows 1...	node01	Feb 16, 2025 @ 07:21:55.000	Feb 16, 2025 @ 19:37:31.000

MITRE ATT&CK

Top Tactics

Privilege Escalation	210
Persistence	205
Initial Access	125
Defense Evasion	124
Lateral Movement	88

Compliance

PCI DSS

- ● 2.2 (530)
- ● 10.2.5 (219)
- ● 11.4 (202)
- ● 10.2.4 (124)
- ● 11.5 (89)

Vulnerability Detection

5 Critical

411 High

220 Medium

3 Low

Top 5 Packages

Package	Count ↓
Microsoft Windows 10 Home 10.0.19045.3803	633
Mozilla Thunderbird (x64 en-US)	3
Photos	1
Pidgin	1
Snip & Sketch	1

SCA: Lastest scans

CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0 cis_win10_enterprise

Policy	End scan	Passed	Failed	Not applicable	Score
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0	Feb 16, 2025 @ 20:46:45.000	112	235	47	32%

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Feb 16, 2025 @ 12:37:39.859	/etc/elasticsearch/config	added	File added to the system.	5	554
Feb 16, 2025 @ 12:06:05.644	/var/wazuh/queue/fim/db/fim.db	added	File added to the system.	5	554
Feb 16, 2025 @ 11:51:57.540	/tmp/agent.conf	modified	Integrity checksum changed.	7	550
Feb 16, 2025 @ 11:37:31.855	/var/log/lastlog	deleted	File deleted.	7	553
Feb 16, 2025 @					