Project Title

Wazuh-Based SIEM and File Integrity Monitoring Home Lab

Project Description

This project focuses on building a complete **Security Information and Event Management (SIEM)** and **File Integrity Monitoring (FIM)** environment using **Wazuh**. The setup includes deploying a Wazuh Manager on an Ubuntu Virtual Machine and configuring a Wazuh Agent on a Windows host system.

The project demonstrates how logs, system events, and file-change activities from a Windows machine can be collected, analyzed, and visualized in real time using the Wazuh Dashboard. It also includes configuring file integrity monitoring to detect unauthorized file modifications, deletions, and creations. The system provides real-time alerts and serves as a practical demonstration of endpoint monitoring, intrusion detection, and security automation — essential skills in cybersecurity and SOC operations.

The setup consists of two main components:

1.Wazuh Manager installed on an Ubuntu virtual machine

2.Wazuh Agent installed on a Windows host machine

The Wazuh Manager collects logs and security data from the agent, processes it, and displays insights through the Wazuh Dashboard. The Windows agent continuously monitors activities such as logins, system events, configuration changes, and any modification to sensitive folders.

A major part of this project is implementing File Integrity Monitoring (FIM). A specific directory on the Windows system was configured for real-time monitoring. Any file creation, deletion, or modification in this folder triggers alerts in the Wazuh dashboard. This demonstrates how SIEM tools help detect suspicious activity or unauthorized access.

Overall, this project provides hands-on experience with endpoint security, log analysis, threat detection, and real-time security operations — skills crucial in cybersecurity and SOC analyst roles.

Objective of the Project

To build and configure a real SIEM environment using Wazuh.

To understand how security logs are collected and analyzed.

To implement File Integrity Monitoring for detecting unauthorized changes.

To simulate a basic SOC workflow and observe real-time alerts.

To gain practical exposure to SIEM dashboards and security event correlation.

Scope of the Project

Installation and configuration of Wazuh Manager on Ubuntu.

Deployment and registration of the Wazuh Agent on Windows.

Monitoring Windows logs, events, system health, and processes.

Implementation of real-time File Integrity Monitoring (FIM).

Testing by generating file changes and observing alert generation.

Viewing logs and alerts through the Wazuh Dashboard.

Understanding how SIEM tools detect unusual activity.

Problem Statement

Modern endpoints face threats such as unauthorized file access, malware activity, insider misuse, and configuration tampering. Organizations need automated systems that continuously monitor endpoints, detect suspicious actions, and generate security alerts.
This project solves this problem by implementing a Wazuh-based SIEM and FIM setup to monitor a Windows machine in real time.

Use Case Model

Log Monitoring: Collect Windows event logs and detect abnormal patterns.

File Integrity Monitoring: Detect changes to sensitive files or directories.

Intrusion Detection: Identify suspicious activity such as failed logins or privilege misuse.

Alerting: Real-time notifications for security violations.

Dashboard Analysis: SOC-like visual analysis of system events and alerts.

Key Features Implemented

SIEM setup with Wazuh

Windows agent onboarding

Generated agent connection keys

Real-time file and folder monitoring

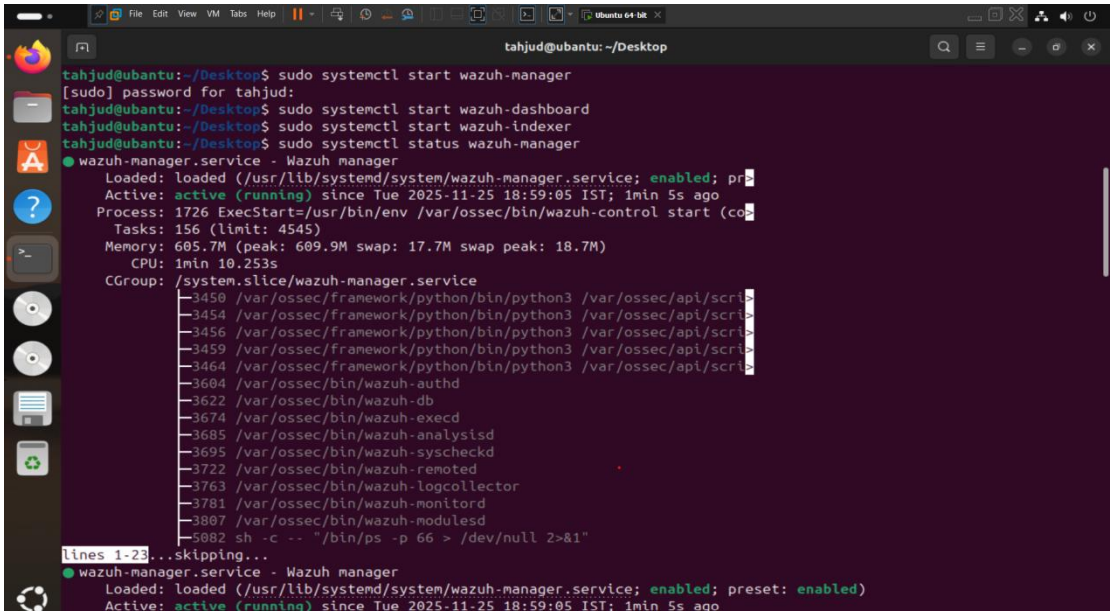
Event log collection

Wazuh dashboard usage

Real-time alerts for file creation/deletion/modification

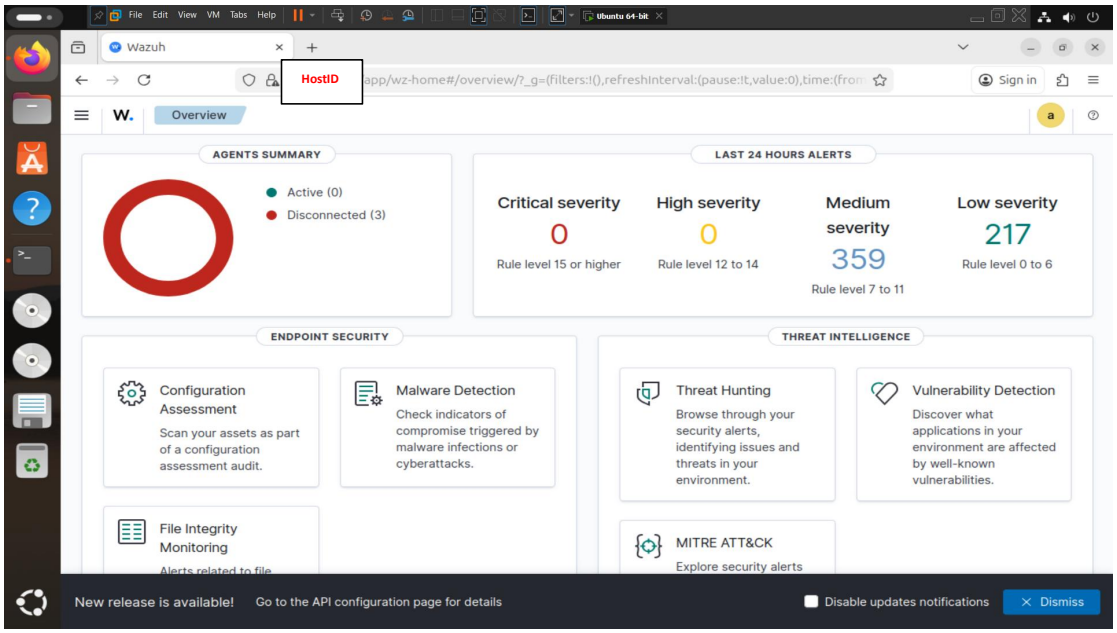
Hands-on SOC analysis workflow

1.Install wazuh in Ubantu

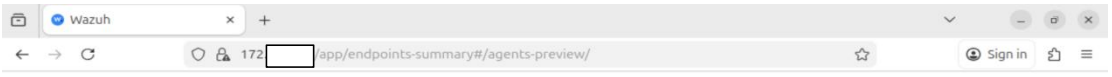


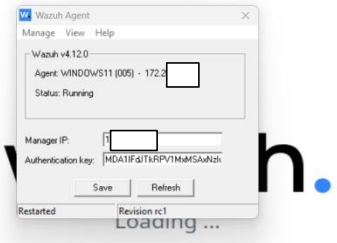
On your Ubuntu server, open a browser and go to: https://localhost

1. Accept any browser security warning due to the self-signed certificate.
2. Log in using the credentials displayed at the end of the installation script.



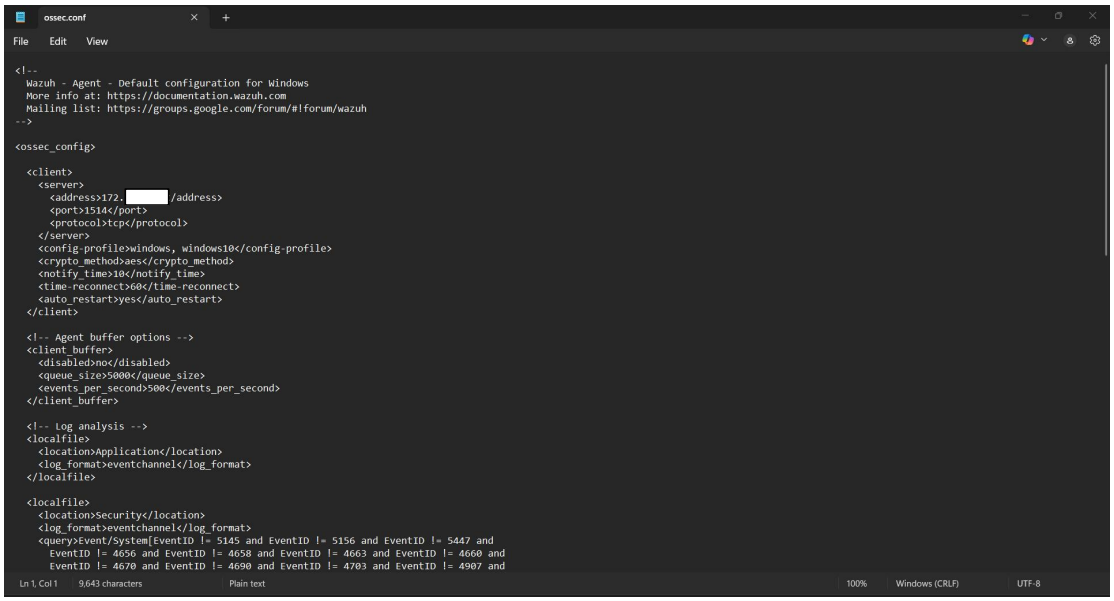
Install the Wazuh Agent (Windows Host)



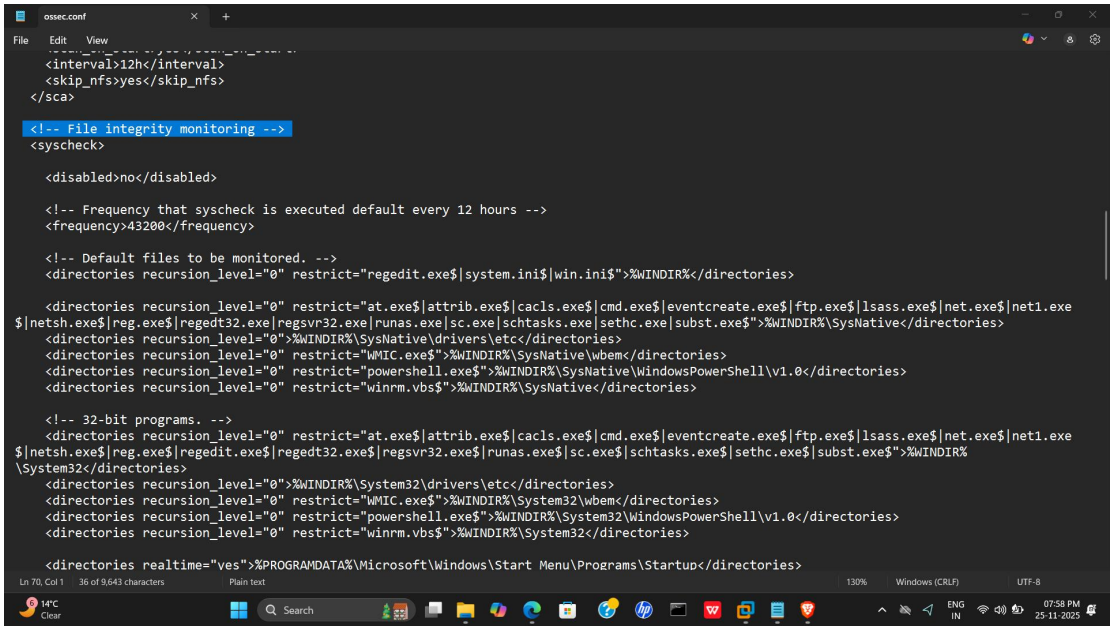


Registering the Agent with the Manager
(sudo /var/ossec/bin/manage_agents)

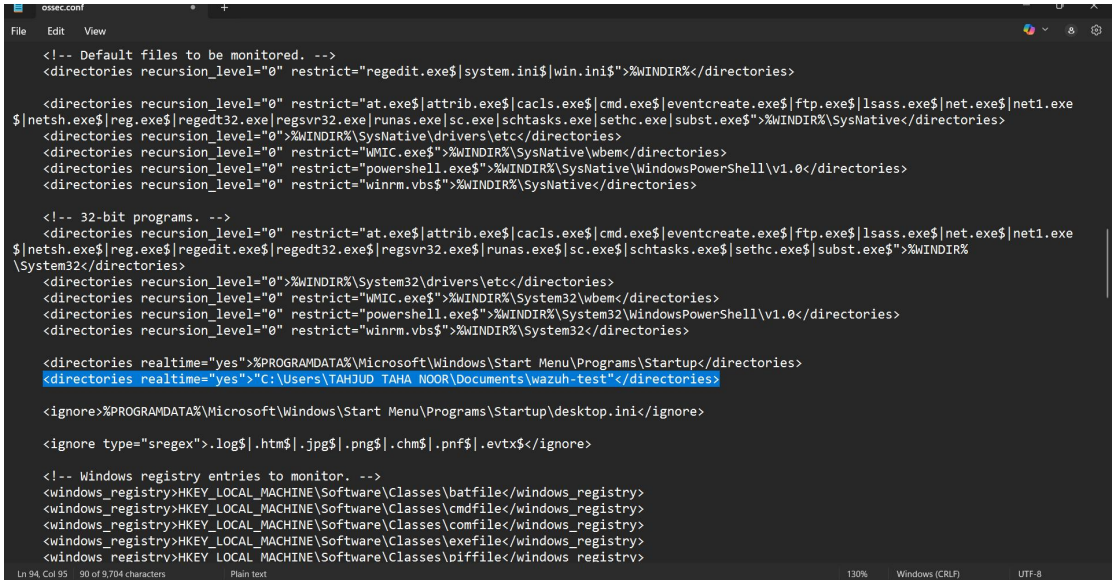
File Integrity Monitoring on Windows Wazuh supports real-time monitoring of file and folder changes using Syscheck.
Edit Agent Configuration Open the following configuration file: C:\Program Files (x86)\ossec-agent\ossec.conf

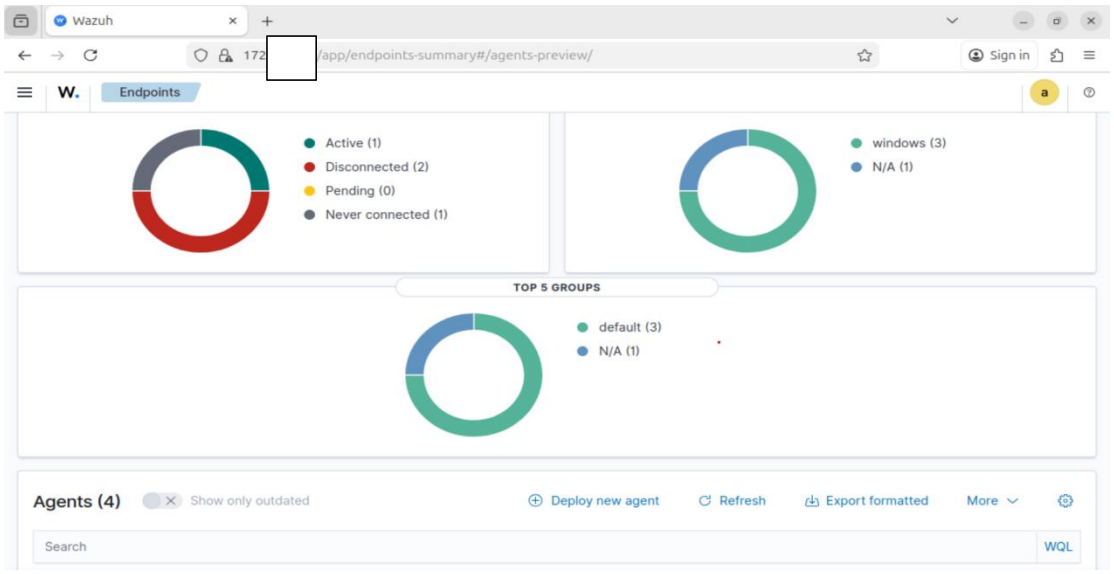


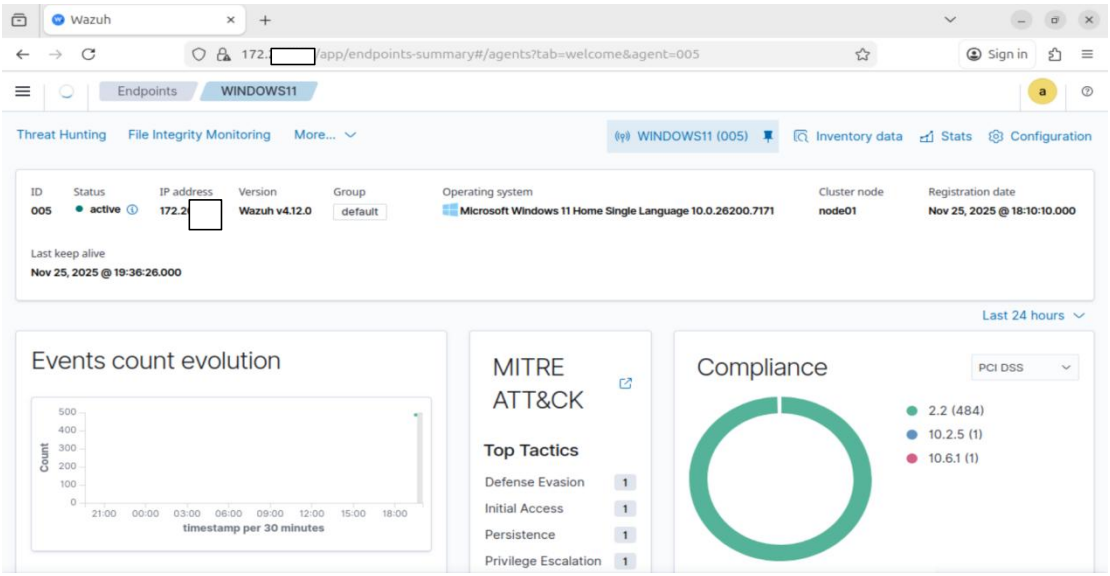
```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>172.[redacted]/address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
  </client>

  <!-- Agent buffer options -->
  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Log analysis -->
  <localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
      EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
      EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
```



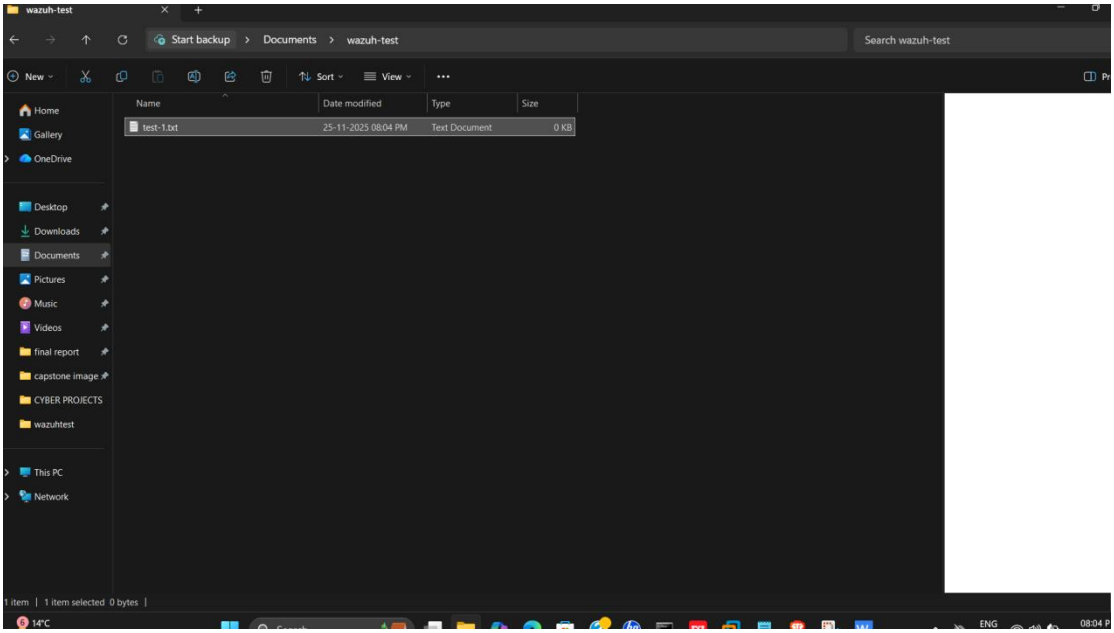
```
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
  </sca>

  <!-- File integrity monitoring -->
  <syscheck>

    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</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$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%\SysNative</directories>
    <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</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$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%
\System32</directories>
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
```


ossec.conf
File Edit View
<!-- 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$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%\SysNative</directories>
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%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$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\System32</directories>
<directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>
<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
<directories realtime="yes">"C:\Users\TAHJUD TAHA NOOR\Documents\wazuh-test"</directories>
<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>
<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
<!-- Windows registry entries to monitor. -->
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\batfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\cmdfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\comfile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\exefile</windows_registry>
<windows_registry>HKEY_LOCAL_MACHINE\Software\Classes\piffile</windows_registry>
Ln 94, Col 95 90 of 9,704 characters Plain text 130% Windows (CRLF) UTF-8


Wazuh
/app/endpoints-summary#/agents-preview/
Sign in
Endpoints
Active (1)
Disconnected (2)
Pending (0)
Never connected (1)
windows (3)
N/A (1)
TOP 5 GROUPS
default (3)
N/A (1)
Agents (4)
Show only outdated
Deploy new agent
Refresh
Export formatted
More
Search
WQL



Create a folder and add a text file then delete it



This is the detail of the file deleted in host