

WAZUH – SIEM and File Integrity Monitoring

Step-by-Step Installation and Configuration Guide



Contents

Wazuh – SIEM and File Integrity Monitoring.....	3
Step 1: Installing Prerequisite Packages	3
Step 2: Installing GPG Key on Ubuntu Server	3
Step 3: Add Wazuh Repository.....	4
Step 4: Update Package Information	4
Step 5: Execute Installation Script.....	5
Step 6: Wazuh Console	6
Step 7: Agent Deployment.....	6
Step 8: Setting up File Integrity Monitoring	10
Step 9: Creating a Sample File	11
Step 10: Verifying File Integrity Monitoring Events.....	12



Wazuh – SIEM and File Integrity Monitoring

Wazuh is a free and open-source security platform that unifies XDR and SIEM capabilities. It protects workloads across on-premises, virtualized, containerized, and cloud environments.

This document provides a step-by-step guide to install and configure Wazuh File Integrity Monitoring.

Step 1: Installing Prerequisite Packages

Install the required packages.

```
sudo apt update && sudo apt install curl apt-transport-https unzip wget gnupg -y
```

```
root@wazuh-s:/home/kboopathi# apt-get install gnupg apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.4.4-2ubuntu17.3).
gnupg set to manually installed.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
Need to get 3970 B of archives.
After this operation, 36.9 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 apt-transport-https all 2.8.3
Fetched 3970 B in 1s (3081 B/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package apt-transport-https.
(Reading database ... 73190 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.8.3_all.deb ...
Unpacking apt-transport-https (2.8.3) ...
Setting up apt-transport-https (2.8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
```

Figure 1: Package installation

Step 2: Installing GPG Key on Ubuntu Server

Ensure that packages from the Wazuh repository are trusted by the server.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor -o
/usr/share/keyrings/wazuh.gpg
```



```

root@wazhu-s: /home/kboopathi
root@wazhu-s:/home/kboopathi# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: keyring '/usr/share/keyrings/wazuh.gpg' created
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:          imported: 1
root@wazhu-s:/home/kboopathi#

```

Figure 2: Installing GPG key

Step 3: Add Wazuh Repository

Add the Wazuh repository to your server.

```

echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee -a
/etc/apt/sources.list.d/wazuh.list

```

Step 4: Update Package Information

sudo apt update

```

root@wazhu-s: /home/kboopathi
root@wazhu-s:/home/kboopathi# apt-get update
Hit:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1497 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [288 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2084 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [471 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:10 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [378 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:12 http://in.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7136 B]
Get:13 http://in.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:14 http://in.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.0 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:16 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:17 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [48.0 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:20 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:21 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.2 kB]
Get:22 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 5431 kB in 13s (409 kB/s)
Reading package lists... Done
root@wazhu-s:/home/kboopathi#

```

Figure 3: Update packages



Step 5: Execute Installation Script

Download and execute the Wazuh installation script.

```
curl -sO https://packages.wazuh.com/4.13/wazuh-install.sh
chmod +x wazuh-install.sh
sudo ./wazuh-install.sh
```

It takes 5–10 minutes to complete. The username and password appear in the logs.

```
-rwxr-xr-x 1 root root 199376 Oct 13 21:11 wazuh-install.sh
root@wazhu-s:/home/kboopathi# ./wazuh-install.sh -a -i
13/10/2025 21:12:19 INFO: Starting Wazuh installation assistant. Wazuh version: 4.13.1
13/10/2025 21:12:19 INFO: Verbose logging redirected to /var/log/wazuh-install.log
13/10/2025 21:12:35 WARNING: Hardware checks ignored.
13/10/2025 21:12:35 INFO: Wazuh web interface port will be 443.
13/10/2025 21:12:52 INFO: --- Dependencies ---
13/10/2025 21:12:52 INFO: Installing debhelper.
13/10/2025 21:13:25 INFO: Wazuh repository added.
13/10/2025 21:13:25 INFO: --- Configuration files ---
13/10/2025 21:13:25 INFO: Generating configuration files.
13/10/2025 21:13:26 INFO: Generating the root certificate.
13/10/2025 21:13:26 INFO: Generating Admin certificates.
13/10/2025 21:13:26 INFO: Generating Wazuh indexer certificates.
13/10/2025 21:13:27 INFO: Generating Filebeat certificates.
13/10/2025 21:13:27 INFO: Generating Wazuh dashboard certificates.
13/10/2025 21:13:28 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation
13/10/2025 21:13:28 INFO: --- Wazuh indexer ---
13/10/2025 21:13:28 INFO: Starting Wazuh indexer installation.
13/10/2025 21:16:47 INFO: Wazuh indexer installation finished.
13/10/2025 21:16:47 INFO: Wazuh indexer post-install configuration finished.
13/10/2025 21:16:47 INFO: Starting service wazuh-indexer.
13/10/2025 21:17:02 INFO: wazuh-indexer service started.
13/10/2025 21:17:02 INFO: Initializing Wazuh indexer cluster security settings.
13/10/2025 21:17:06 INFO: Wazuh indexer cluster security configuration initialized.
13/10/2025 21:17:06 INFO: Wazuh indexer cluster initialized.
13/10/2025 21:17:06 INFO: --- Wazuh server ---
13/10/2025 21:17:06 INFO: Starting the Wazuh manager installation.
13/10/2025 21:19:57 INFO: Wazuh manager installation finished.
13/10/2025 21:19:57 INFO: Wazuh manager vulnerability detection configuration finished.
13/10/2025 21:19:57 INFO: Starting service wazuh-manager.
13/10/2025 21:20:13 INFO: wazuh-manager service started.
13/10/2025 21:20:13 INFO: Starting Filebeat installation.
13/10/2025 21:21:16 INFO: Filebeat installation finished.
13/10/2025 21:21:22 INFO: Filebeat post-install configuration finished.
13/10/2025 21:21:22 INFO: Starting service filebeat.
13/10/2025 21:21:23 INFO: filebeat service started.
13/10/2025 21:21:23 INFO: --- Wazuh dashboard ---
13/10/2025 21:21:23 INFO: Starting Wazuh dashboard installation.
13/10/2025 21:26:50 INFO: Wazuh dashboard installation finished.
13/10/2025 21:26:50 INFO: Wazuh dashboard post-install configuration finished.
13/10/2025 21:26:50 INFO: Starting service wazuh-dashboard.
13/10/2025 21:26:50 INFO: wazuh-dashboard service started.
13/10/2025 21:26:52 INFO: Updating the internal users.
13/10/2025 21:26:55 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
13/10/2025 21:27:05 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
13/10/2025 21:27:36 INFO: Initializing Wazuh dashboard web application.
13/10/2025 21:27:38 INFO: Wazuh dashboard web application initialized.
13/10/2025 21:27:38 INFO: --- Summary ---
13/10/2025 21:27:38 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: wMHa+FTY7rx?cYD*Qn7FBLxzQCS3iXGp
13/10/2025 21:27:38 INFO: Installation finished.
root@wazhu-s:/home/kboopathi#
```

4: Installation process



Step 6: Wazuh Console

This is how the Wazuh console looks after a fresh installation.

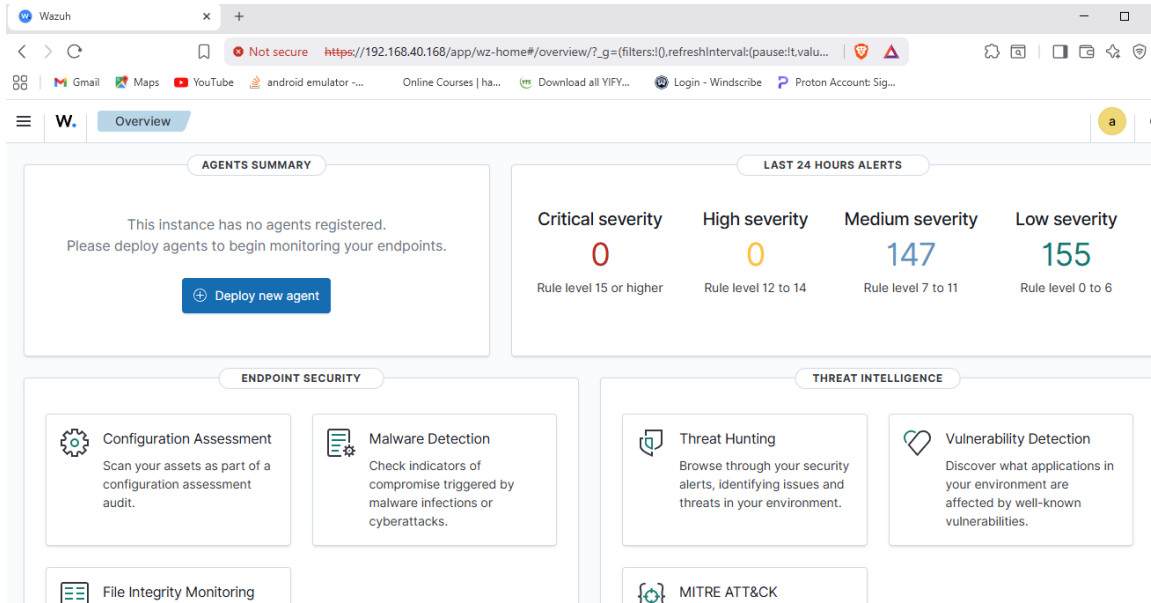


Figure5: Wazuh console

Step 7: Agent Deployment

Download the Wazuh agent from the Deploy New Agent section or from the official site. Install it on Windows.



Wazuh

Not secure <https://192.168.40.129/app/endpoints-summary#/agents-preview/deploy>

Endpoints Deploy new agent

Deploy new agent

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

LINUX

☐ RPM amd64 ☐ RPM aarch64

☐ DEB amd64 ☐ DEB aarch64

WINDOWS

☒ MSI 32/64 bits

For additional systems and architectures, please check our [documentation](#).

✓ 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

192.168.40.129

☐ Remember server address

Figure 6a: Wazuh agent deployment

Run the agent configuration interface and provide the Wazuh server IP address and authentication key.



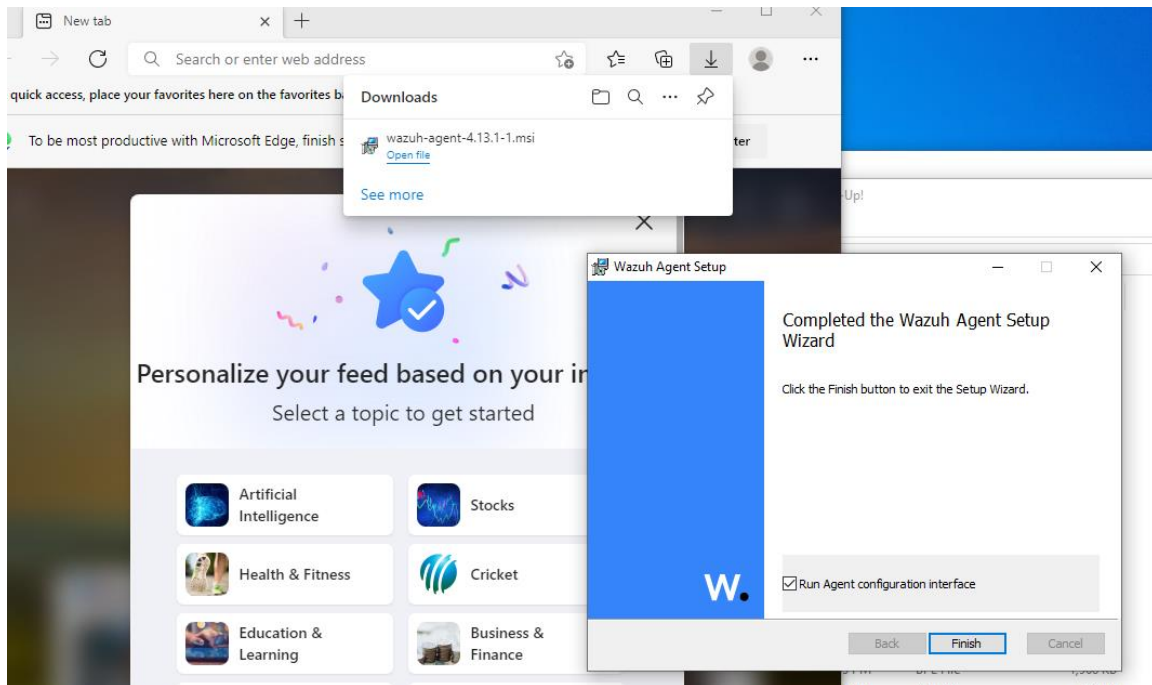


Figure 6b: Wazuh agent deployment

To retrieve the key:

```
/var/ossec/bin/manage_agents
```

Use the E option to extract the key by entering the agent name and IP.




```

root@wazhu-s:/home/kboopathi# /var/ossec/bin/manage_agents

*****
* Wazuh v4.13.1 Agent manager.          *
* The following options are available:  *
*****

  (A)dd an agent (A).
  (E)xtract key for an agent (E).
  (L)ist already added agents (L).
  (R)emove an agent (R).
  (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: THEPUNISHER, IP: 192.168.10.129
  ID: 002, Name: SPIDERMAN, IP: 192.168.10.130
  ID: 003, Name: HYDRA-DC, IP: 192.168.10.128
Provide the ID of the agent to extract the key (or '\q' to quit): █

```

Figure 6c: Wazuh agent deployment

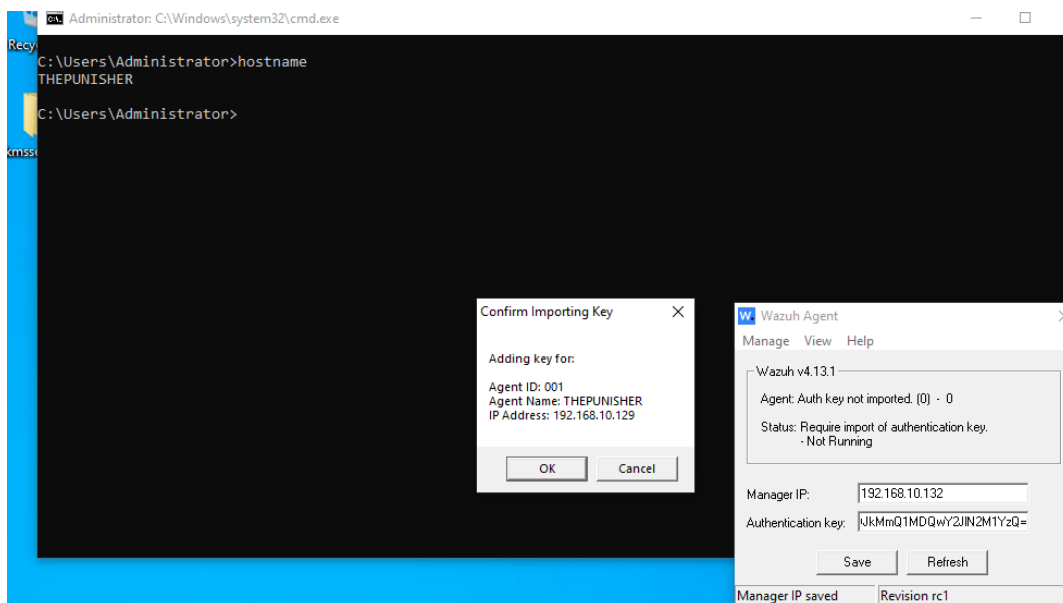


Figure 6d: Wazuh agent deployment



Step 8: Setting up File Integrity Monitoring

Wazuh supports real-time monitoring of file and folder changes using Syscheck.

Edit ossec.conf on the client machine:

C:\Program Files (x86)\ossec-agent\ossec.conf

Add:

```
<syscheck>
  <directories realtime="yes">C:\Users\Administrator\Desktop\wazuh-FIM</directories>
</syscheck>
```

Save and restart the Wazuh agent.



```
*ossec.conf - Notepad
File Edit Format View Help
  <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.e
  <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>

  <directories realtime="yes">C:\Users\Administrator\Desktop\wazuh-FIM</directories>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.e
```

Figure 7: FIM setup



Step 9: Creating a Sample File

Create a test file in C:\Users\Administrator\Desktop\wazuh-FIM.

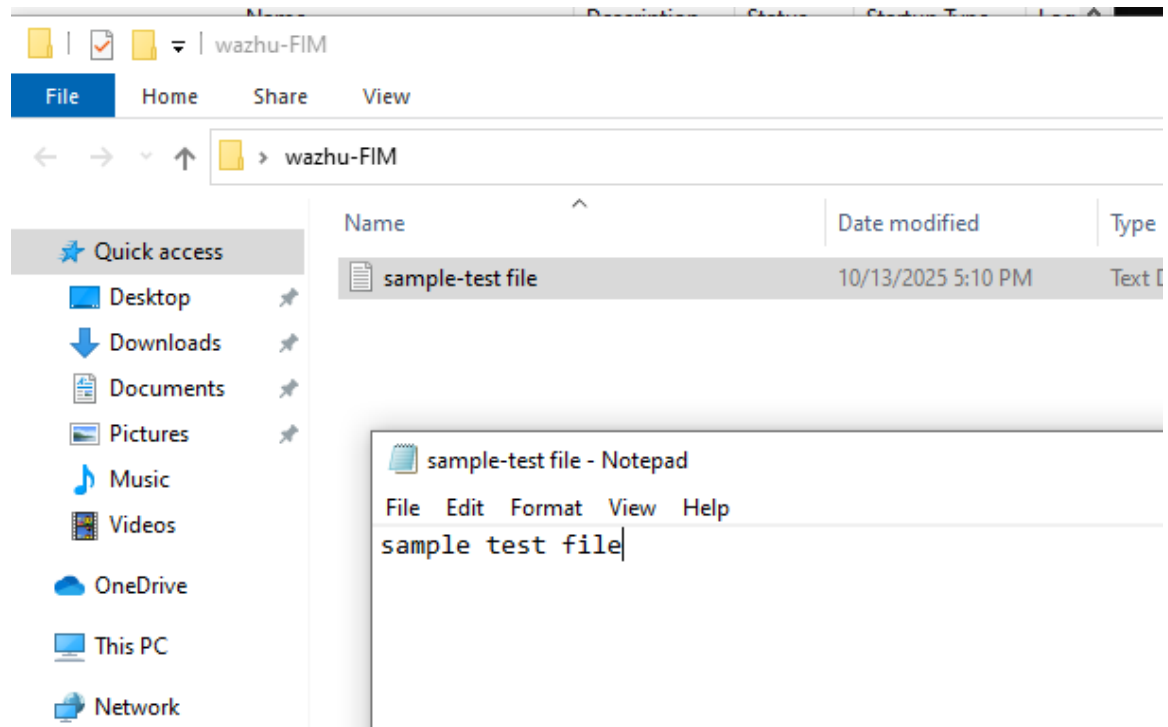


Figure 8: Sample file creation



Step 10: Verifying File Integrity Monitoring Events

When a file is created or modified, alerts appear on the Wazuh dashboard. Directory changes are recorded and reported in real time.

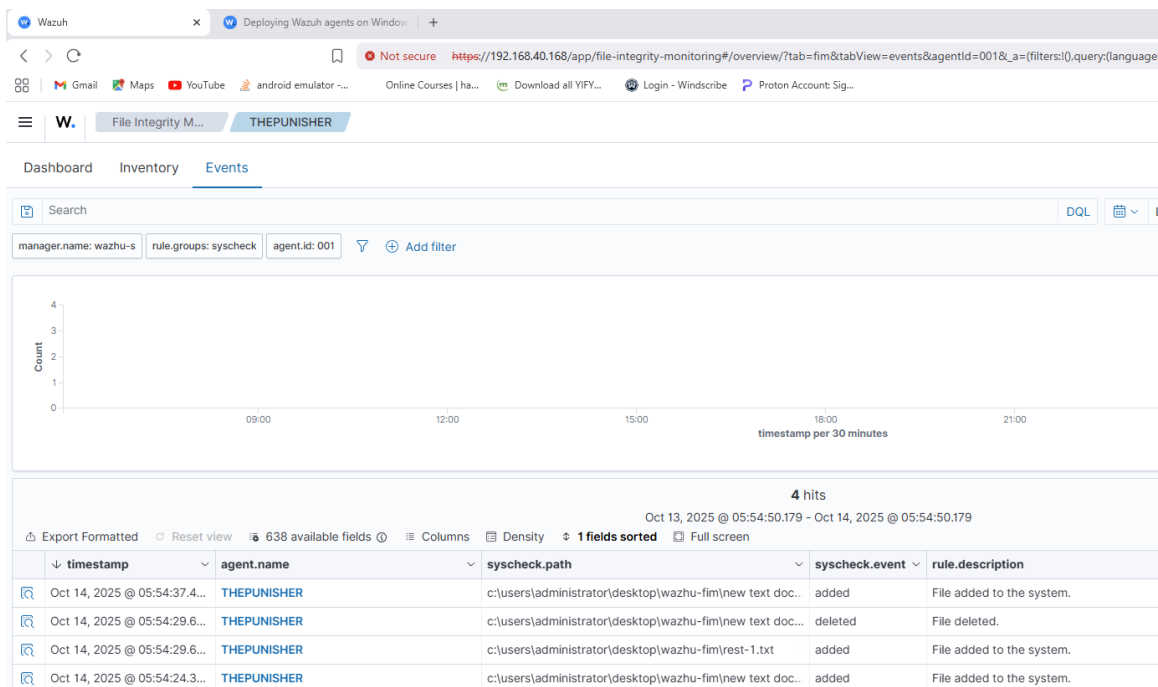


Figure 9: File integrity alert

