🔐 SOC Analyst Hands-on Project

File Integrity Monitoring (FIM) using Wazuh

Prepared by Faizanullah Syed
Email: faizanulla.syed19@gmail.com
SOC Analyst Learner | Cybersecurity Enthusiast

🧠 Objective

The objective of this lab was to implement **File Integrity Monitoring (FIM)** using **Wazuh SIEM**. This helped me monitor critical system files for any unauthorized changes, detect suspicious behavior like file tampering, and learn how SOC teams respond to these events in real-world environments.

🛠 Setup Requirements

- **Wazuh Manager:** Already installed and running on the server
- **Wazuh Agent:** Installed on the target machine (Linux or Windows)
- **Kali Linux or any attacker machine** for simulating file tampering
- Basic access to Wazuh Dashboard

⚙ Step-by-Step Configuration

🔧 Step 1: Enable File Integrity Monitoring on Wazuh Manager

1. **Open the configuration file**:

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

   ```
   [wazuh-user@wazuh-server ~]$ sudo nano /var/ossec/etc/ossec.conf
   ```

2. **Make sure FIM is enabled**:
   Check the logall lines are “Yes” as shown in snap shot bellow.

```
  GNU nano 8.3                                                    /var/ossec/etc/ossec.conf
<!--
  Wazuh - Manager - Default configuration for amzn 2023
  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>yes</logall>
    <logall_json>yes</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>
```

3. **Restart Wazuh Manager to apply changes:**

   sudo systemctl restart wazuh-manager

4. **Open Wazuh Agent Configuration:**

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

```
wazuh-user@wazuhagent:~$ sudo nano /var/ossec/etc/ossec.conf
[sudo] password for wazuh-user:
wazuh-user@wazuhagent:~$ sudo nano /var/ossec/etc/ossec.conf
```

5. **Make sure FIM is enabled and Add Path (Directory) to be monitored :**

   Add or verify FIM settings under the `<syscheck>` section.

<directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

```
GNU nano 7.2                                                    /var/ossec/etc/ossec.conf *
    <enabled>yes</enabled>
    <scan_on_start>yes</scan_on_start>
    <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>

    <scan_on_start>yes</scan_on_start>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories>/etc,/usr/bin,/usr/sbin</directories>
    <directories>/bin,/sbin,/boot</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
    <ignore>/etc/random-seed</ignore>
    <ignore>/etc/random.seed</ignore>
    <ignore>/etc/adjtime</ignore>
    <ignore>/etc/httpd/logs</ignore>
    <ignore>/etc/utmpx</ignore>
    <ignore>/etc/wtmpx</ignore>
    <ignore>/etc/cups/certs</ignore>
    <ignore>/etc/dumpdates</ignore>
    <ignore>/etc/svc/volatile</ignore>
    <directories check_all="yes" report_changes="yes" realtime="yes">/root</directories>

    <!-- File types to ignore -->
    <ignore type="sregex">.log$|.swp$</ignore>
```

6. **Restart Wazuh Agent to apply changes:**

   sudo systemctl restart wazuh-agent

```
[sudo] password for wazuh-user:
wazuh-user@wazuhagent:~$ sudo systemctl restart wazuh-agent
wazuh-user@wazuhagent:~$
```

⍰ Attack Simulation – Unauthorized File Change

On Kali Linux (Simulating Attacker) or Switch to root user in Agent server :

1. Create a new file in the monitored directory (/root)

echo "Sensitive data" > faizan.txt

```
wazuh-user@wazuhagent:~$ echo "sensitive data" > faizan.txt
wazuh-user@wazuhagent:~$
```

2. Modify the content:(/root)

   echo "Unauthorized modification detected" >> faizan.txt

```
wazuh-user@wazuhagent:~$ echo "Unauthorized modification detected" >> faizan.txt
wazuh-user@wazuhagent:~$
```

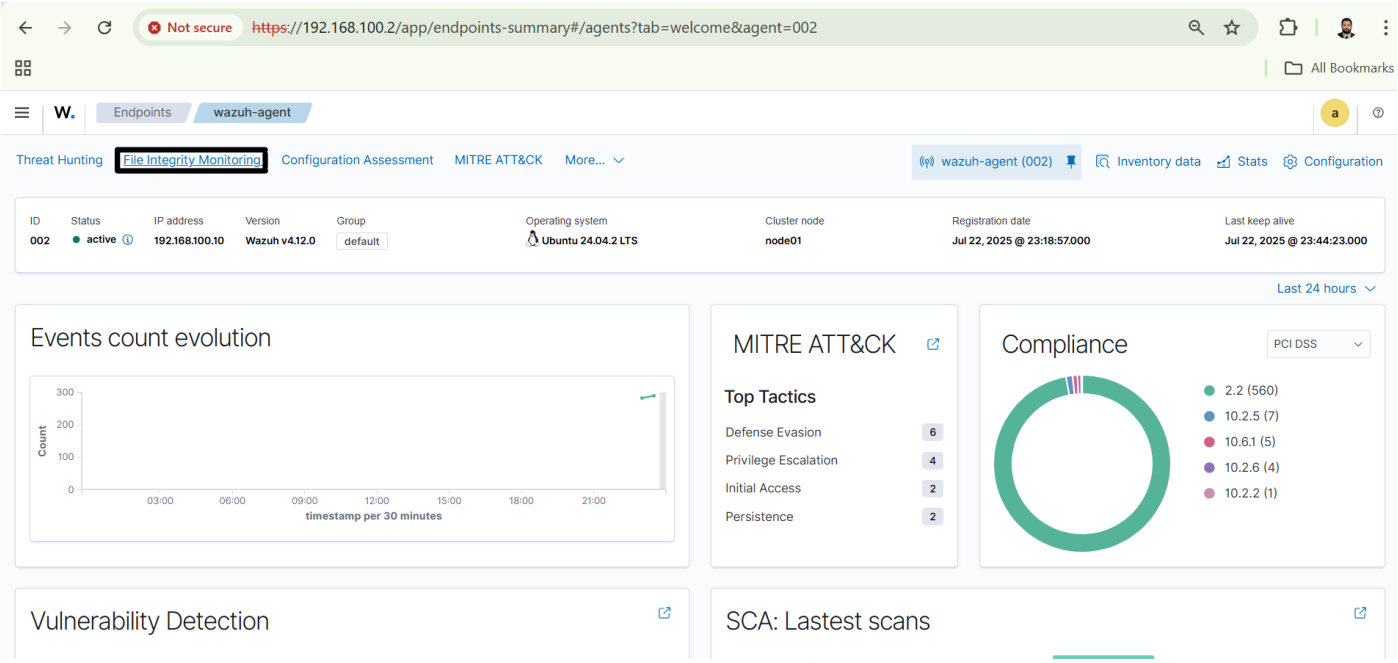
3. Delete the file: (/root)

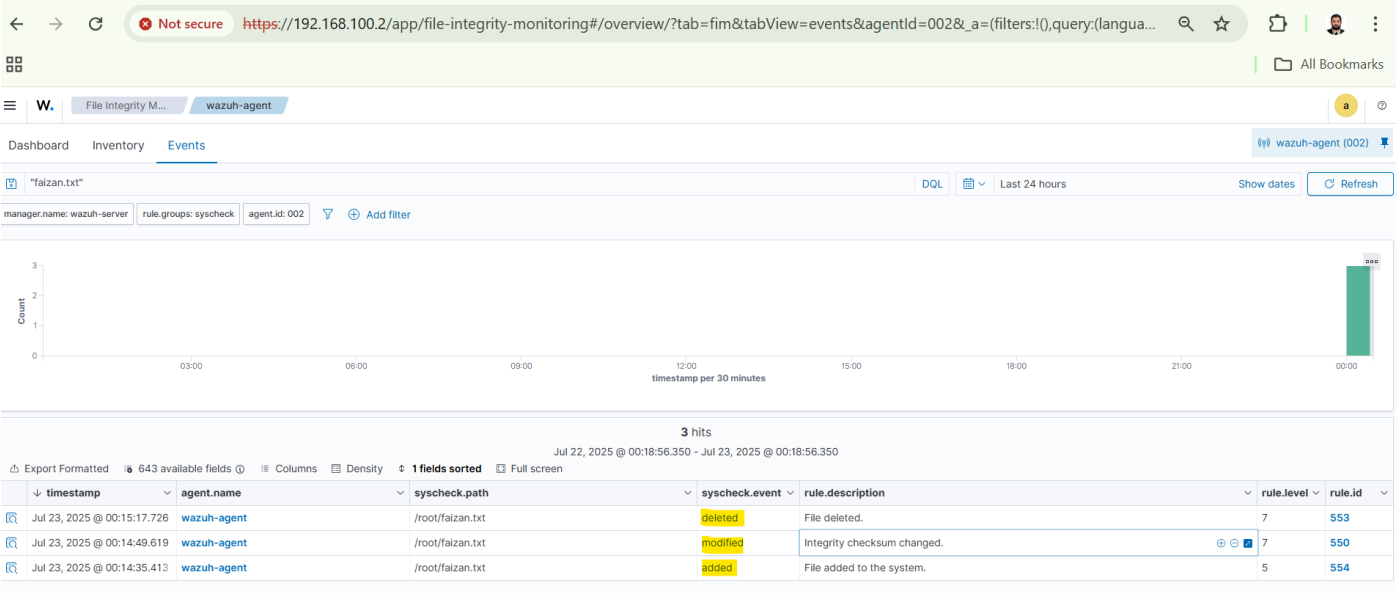
   rm -f faizan.txt

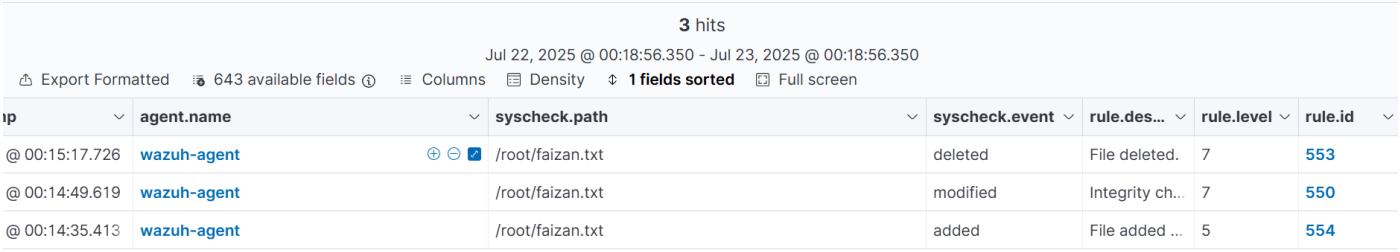
```
wazuh@wazuh-agent:~$ rm -f faizan.txt
wazuh@wazuh-agent:~$
```

🔍 Detection in Wazuh

1. Open your **Wazuh Dashboard**
2. Go to:
   Security Events → File Integrity Monitoring
3. Search using:







4. Look for logs indicating: • File Created • File Modified • File Deleted

✅ Outcome

By the end of this project, I was able to:

- ✅ Successfully configure **File Integrity Monitoring** in Wazuh
- ✅ Simulate file-based attacks on a Linux machine
- ✅ View real-time alerts for file modifications, deletions, and creations
- ✅ Understand how **SOC teams investigate and respond** to FIM alerts

🧠 Observation

Wazuh's File Integrity Monitoring is one of the most important tools for detecting suspicious activity on endpoints. It continuously monitors sensitive files and generates alerts when unauthorized changes are made.

This makes FIM a key element in **threat detection, compliance monitoring, and forensic investigations**. It helps SOC analysts:

- Detect insider threats or malware tampering
- Trace the timeline of a breach
- Build a proactive detection strategy