In essence, SIEM is like a security radar that helps organizations detect, investigate, and respond to potential cyber threats more efficiently.

### **How SIEM Fits into Cybersecurity**

* Works as a command center for cybersecurity teams.
* Combines automation (alerting, reports) and human intervention (analysis, response).
* Integrated with other tools like firewalls, IDS/IPS, and endpoint protection systems.

There are various SIEM tools available as an open source such as

* Wazuh
* Splunk
* Microsoft sentinel
* Etc

We will give more insight on **Wazuh**  as an open source SIEM tools

**WAZUH**

**Wazuh** is an open-source security platform that provides capabilities for **Security Information and Event Management (SIEM)**. It integrates multiple security features into a single solution, making it an accessible and versatile choice for SIEM implementation.

Features such as

* Log collection
* Threat detection
* Real time alert
* Centralize monitoring
* Log analysis
* Compliance report
* Incidence response

It consists of the following components

* Wazuh Agent - Installed on monitored endpoints (servers, workstations, cloud instances). Collects logs and system activity data, performs file integrity monitoring (FIM), vulnerability detection, and other local security tasks.

Sends collected data to the Wazuh Manager.

* Wazuh Manager- The central component of Wazuh.Processes and analyzes data received from Wazuh Agents. Applies rules for threat detection, generates alerts, and stores collected data.
* Wazuh indexer- Handles the indexing and storage of logs and alerts.
* Wazuh dashboar - A user interface integrated with Wazuh for visualization.Provides dashboards for real-time monitoring, threat analysis, and compliance reporting.

Description of components

1. Wazuh Agent- this was installed on my window computer

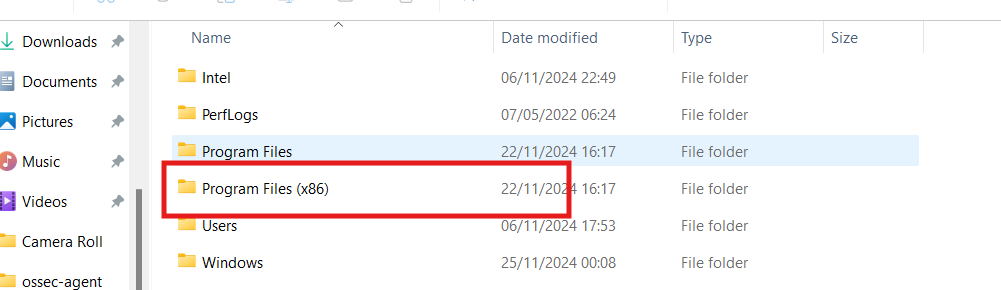


Fig 1



Fig 2

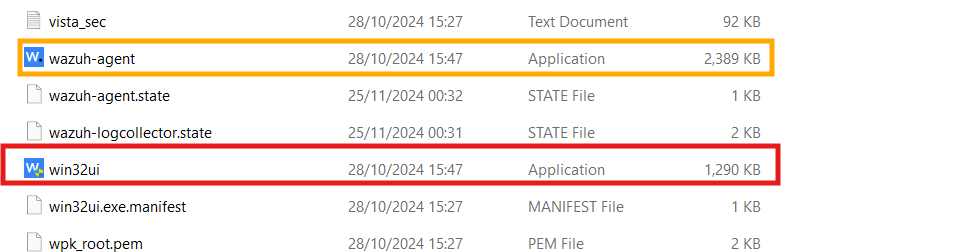
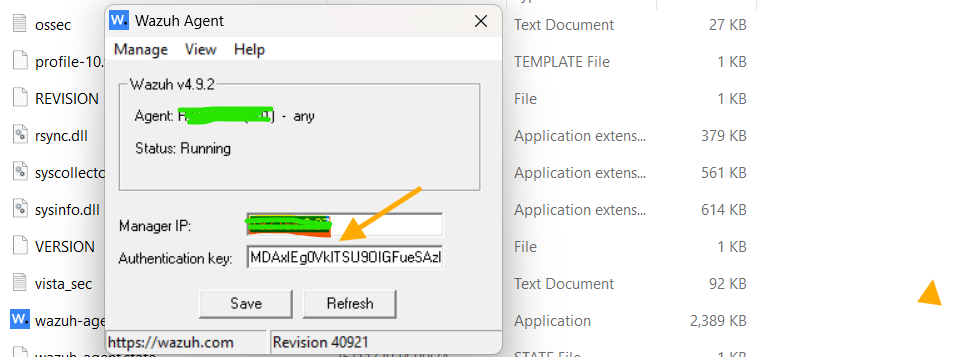
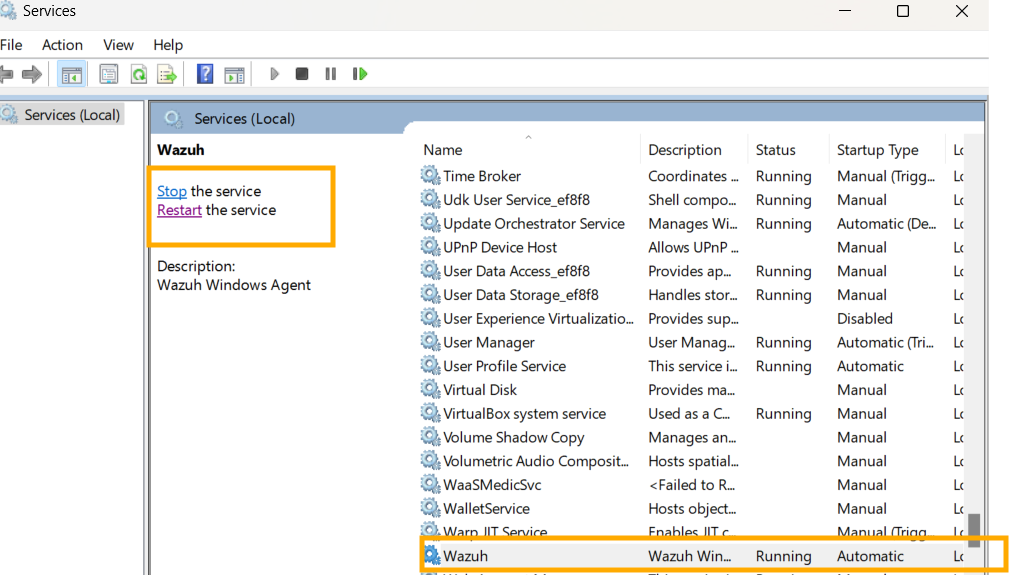


Fig 3

Fig 4

Fig 5

1. Wazuh Manager setups

The firefox browser in our Ubuntu server was use to open the wazuh manager by using the Ubuntu IP address in this format ‘ https:// ip address:443

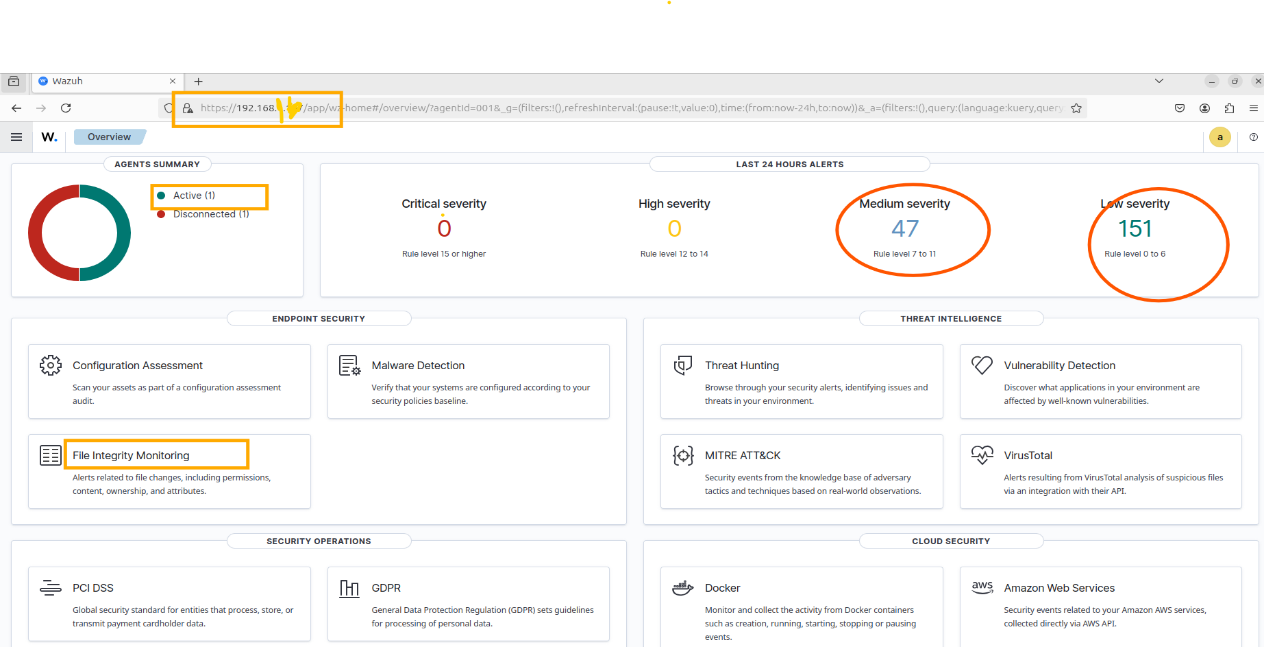


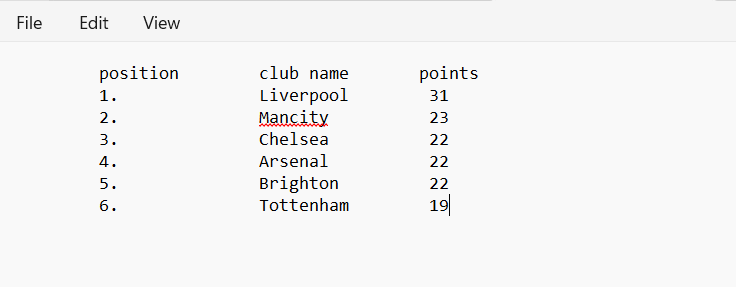
Fig 6

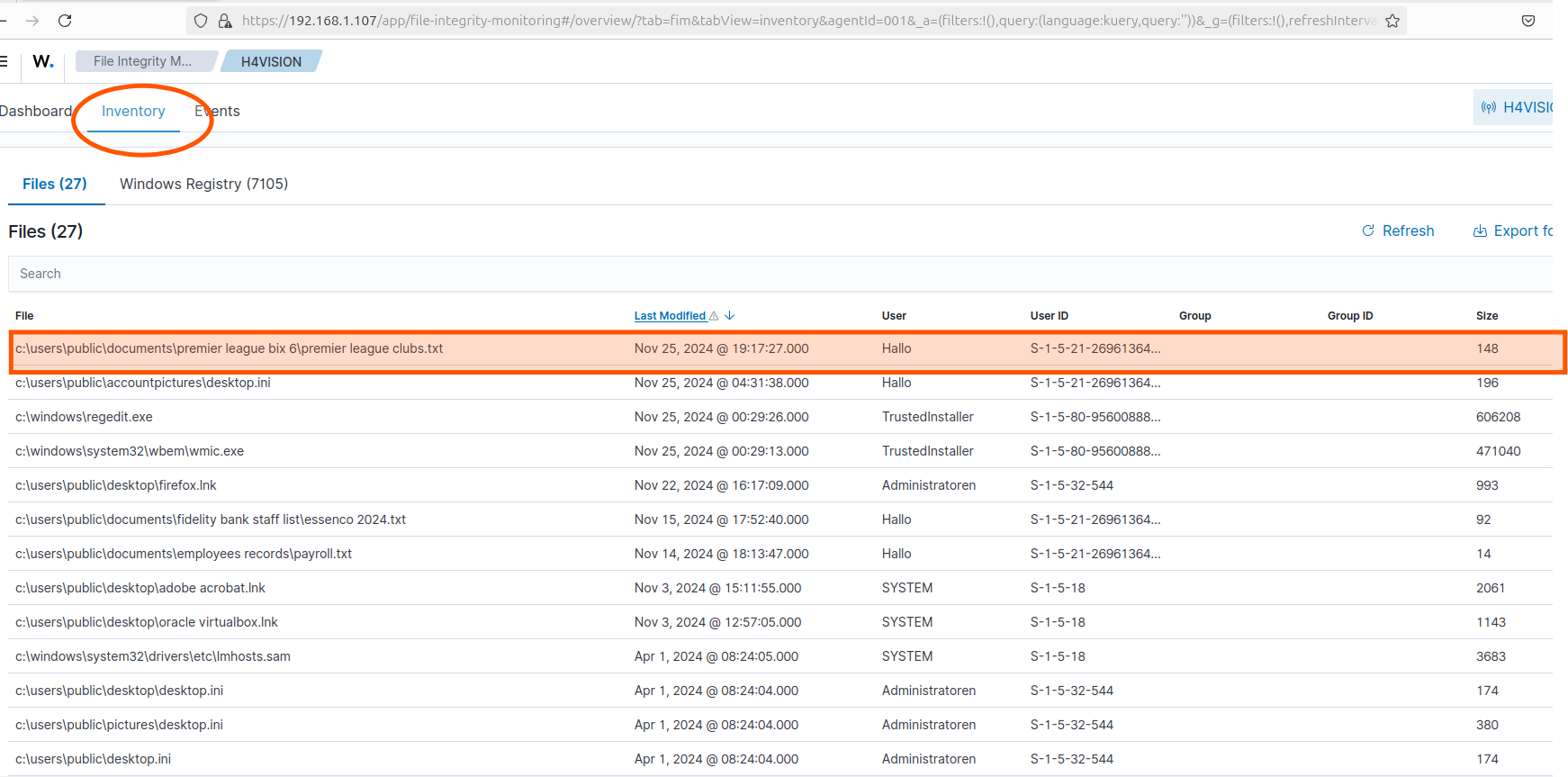
From the fig 6 above , This screenshot above showcases the **Wazuh Dashboard**, highlighting various security monitoring and alerting capabilities. #

We will explore some of the endpoint security features tool such as the file integrity monitoring (FIM) Monitors changes to files, including permissions and attributes.

* **Modifications**: Content changes, permission changes, or attribute modifications.
* **Additions or Deletions**: New files or removed files in monitored paths.

A file has been created in the public folder of the Agent and named ‘**premier league big six**’ an integrity test will be carried out on this file and we expect the Wazuh to pick this as log and trigger alert for the event of file modification.





**Re**viewing the FIM dashboard under the inventory log as highlighted ABOVE

* The file premier league clubs.txt located in c:\users\public\documents\premier league bix 6\ is highlighted.
* **Details**:
  + **Last Modified**: Indicates the date and time the file was last altered (Nov 25, 2024, at 19:17:27).
  + **User**: Shows the user who modified the file (Hallo).
  + **Size**: File size is 148 bytes.

Reviewing the FIM dashboard under the event log as highlighted above

