AGENT CONFIGURATION REPORT

What is Wazuh?

Wazuh is a free and open source security platform used for threat detection , complaince monitoring, and incident response. It helps organizations tomonitor their infrastructure in real-time by collecting and analyzing data from end points (like servers, desktops or cloud instances).

Wazuh works as a **SIEM (Security Information and Event Management**) and **XDR (Extended Detection and Response)** solution.

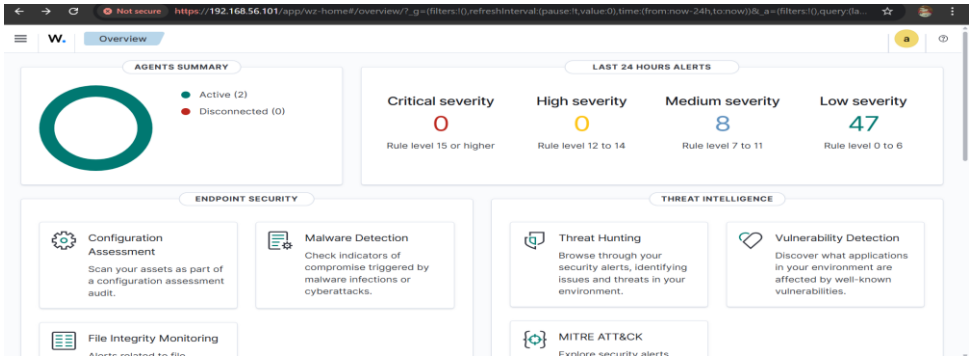
What is Wazuh agent?

The **wazuh agent** is lightweight piece of software installed on endpoints (such as Linux, Windows, or macOS machines). Its primarily job to:

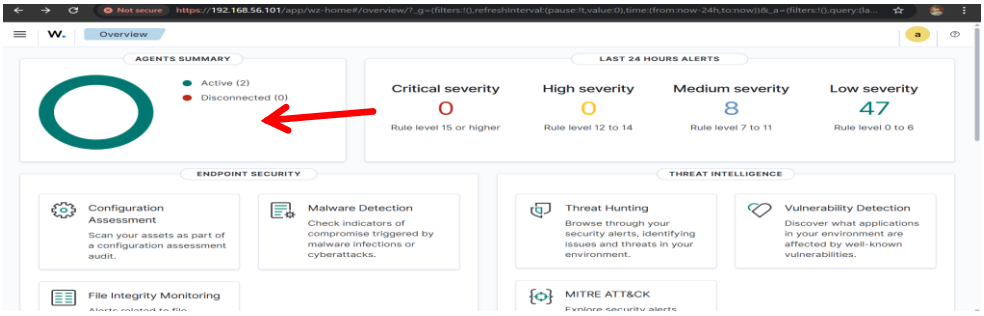
- **Collect system data** (logs, events, file changes etc)
- **Send that data** securely to the Wazuh Manager
- **Enforce active response rules** (like blocking malicious IPs or restarting services)

Each endpoint you want to monitor needs to have the wazuh agent installed and configured.

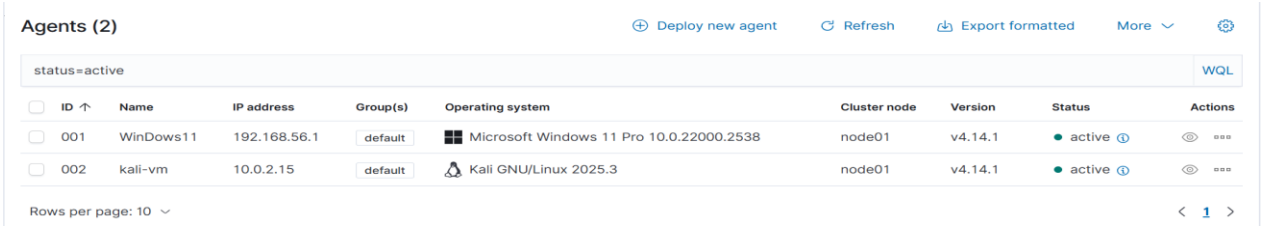
Wazuh Dashboard:



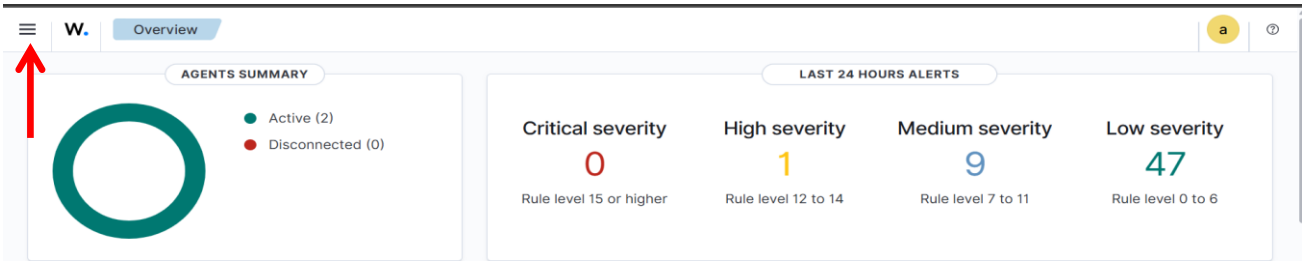
Click On the Active:

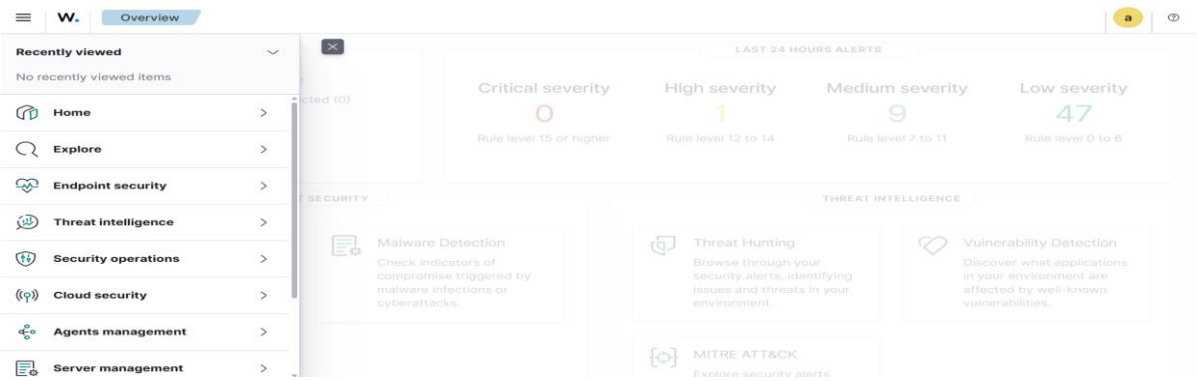


It’s Showing 2 Active Agent:

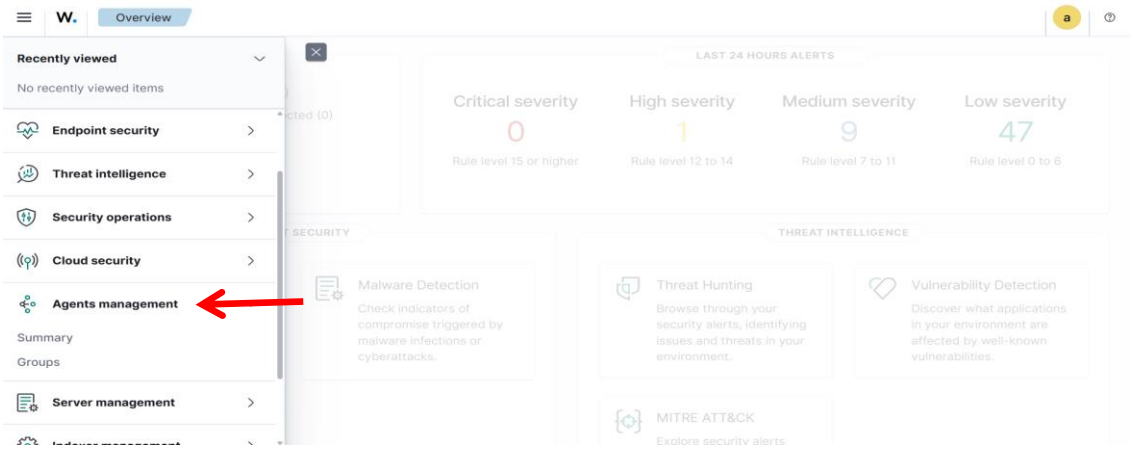


Click On the Menu:

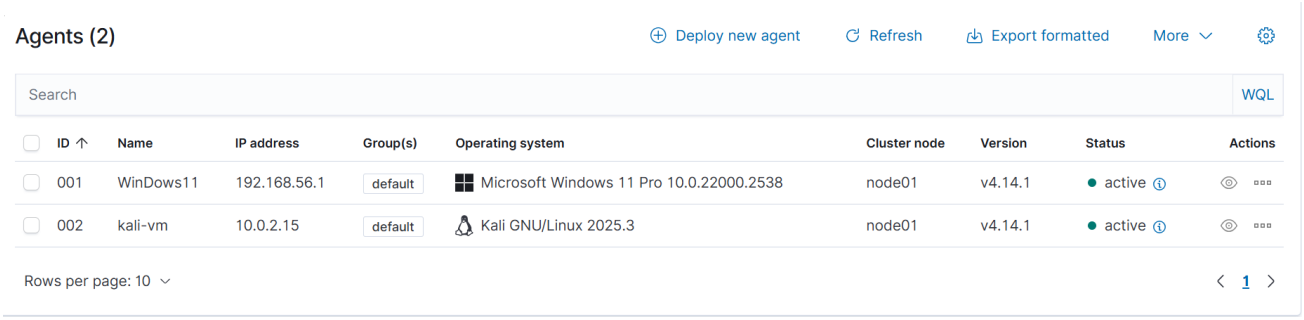




Click on Agents Management:

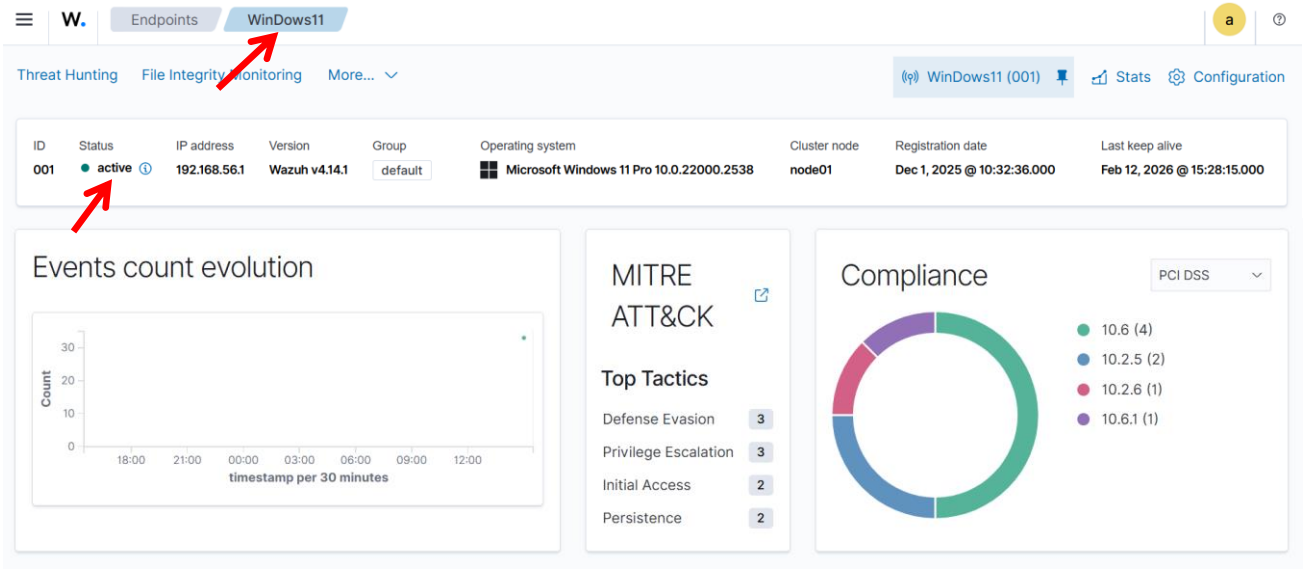


Click on the Summary It will redirect to page showing all the agents:

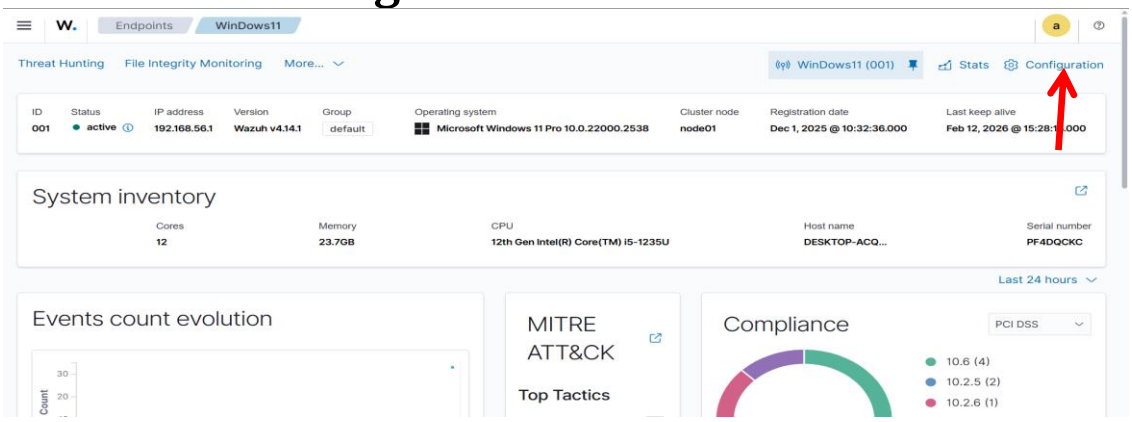


Click on any agent you want to generate report I am selecting active agent (WinDows11)

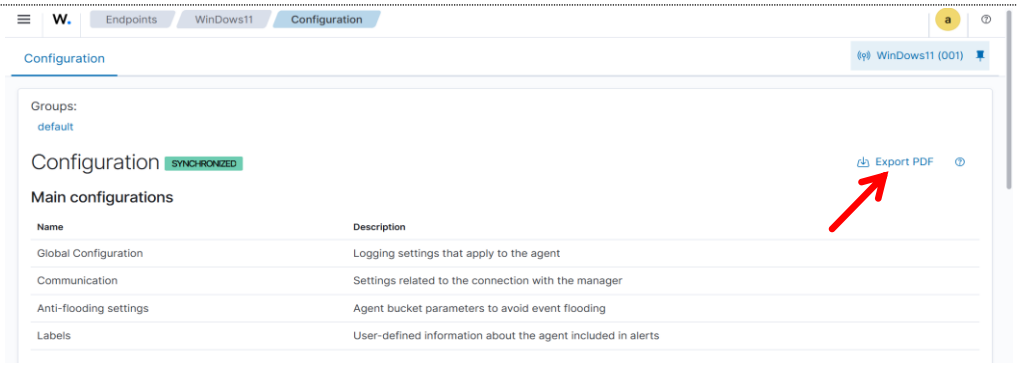
After selecting It will show you:



Now click the Configuration icon:

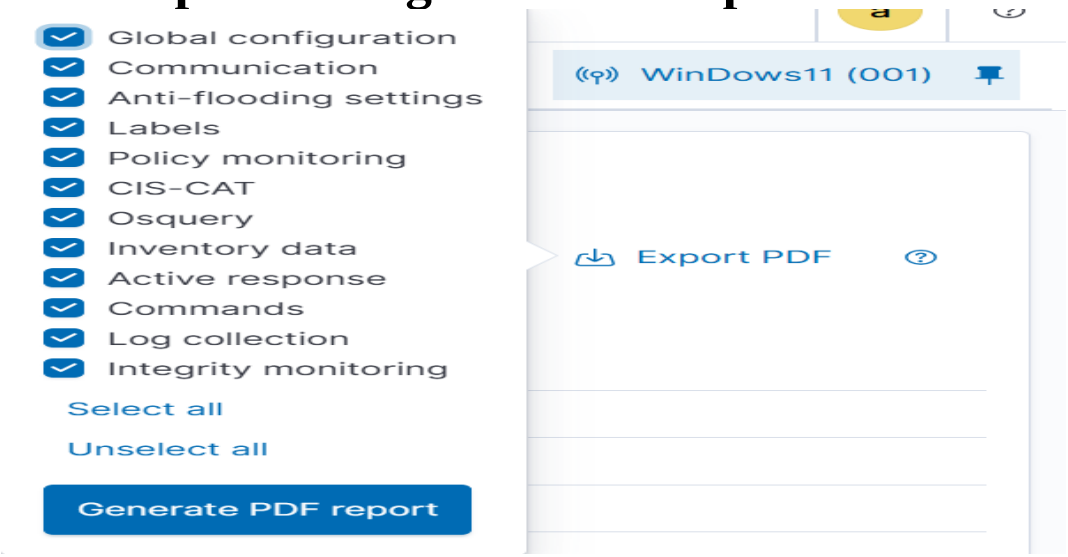


There you can see the option to generate the report:

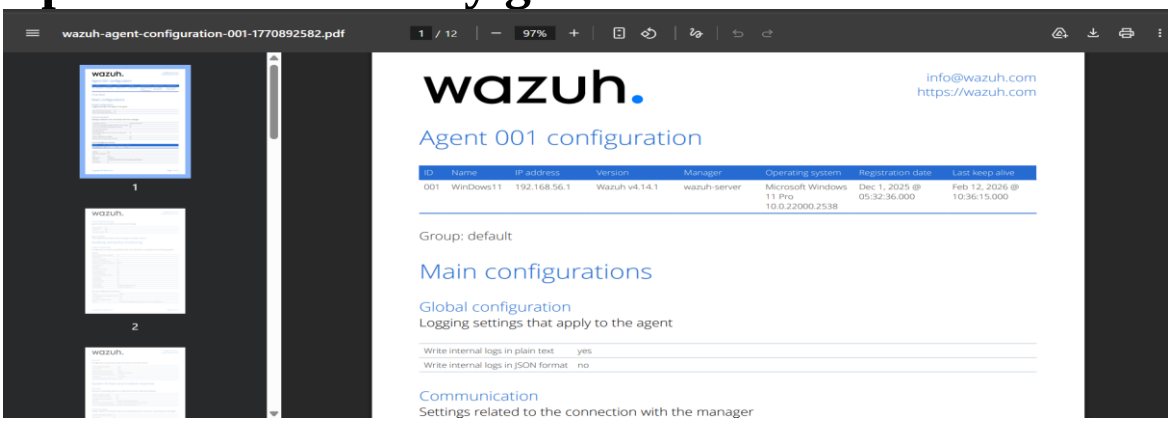


Click the export PDF

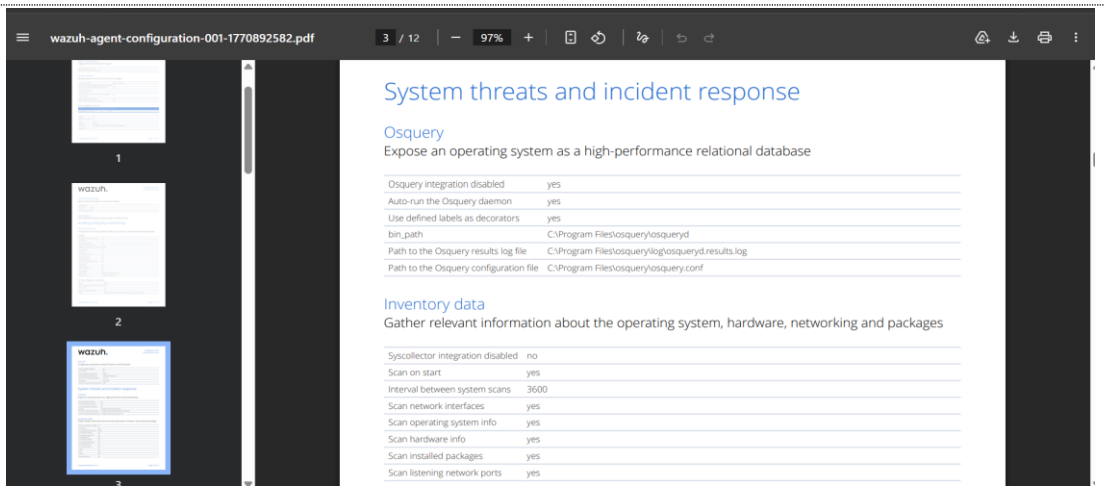
Check the option and genrate the report:



Report is scuccessfully generated:



Showing all the configuation details



Summary:

Viewing or generating a Wazuh agent configuartion report povides critical visibility into the security posture of an endpoint. It ensures the agent is properly connected to the Wazuh manager, verifies that essential modules like file integrity monitoring, vulnerability detection and system inventory are enabled, and confirms that the setup complice with organization or regulatory standards. This information is valuable for auditing, documentation, and troubleshooting, allowing security teams to quickly indentify misconfiguration, coverage gaps or, disabled features. Overall, it strengths endpoint monitoring and support proactive threat detection and response.

Other SIEM:

Splunk

IBM Qradar

Azure Sential