

# Wazuh

## What is Wazuh?

- **Open-Source Security Platform:** Free and open-source solution for security monitoring, threat detection, incident response, and compliance.
- **Unified Capabilities:** Combines aspects of **XDR** (Extended Detection and Response) and **SIEM** (Security Information and Event Management).
- **Agent-Based:** Uses lightweight agents deployed on endpoints to collect data.

## Core Capabilities / What it Does:

- **Endpoint Detection & Response (EDR):**
  - **File Integrity Monitoring (FIM):** Detects changes to critical files and configurations.
  - **Intrusion Detection (HIDS):** Identifies suspicious activities, rootkits, and unauthorized access on hosts.
  - **Vulnerability Detection:** Scans for known software vulnerabilities (CVEs) on endpoints.
  - **Security Configuration Assessment (SCA):** Checks for deviations from security baselines (e.g., CIS Benchmarks).
  - **Active Response:** Can automate actions to contain threats (e.g., block IP, kill process).
- **Log Management & SIEM:**
  - Collects, parses, and normalizes logs from virtually any source (OS, apps, network devices, cloud).
  - Performs real-time **event correlation** to identify attack patterns.
  - Generates **alerts** for suspicious activities.
- **Cloud Security:** Integrates with AWS, Azure, GCP for cloud infrastructure monitoring.
- **Compliance Monitoring:** Helps meet regulatory requirements like **SOC 2**, PCI DSS, GDPR, HIPAA by providing audit trails and continuous monitoring.

## **Key Components (How it Works):**

### **1. Wazuh Agent:**

- Lightweight software installed on monitored systems (servers, laptops, VMs, containers, cloud instances).
- Collects data, performs FIM, HIDS, SCA, vulnerability scans.
- Communicates securely with the Wazuh Manager.

### **2. Wazuh Server (Manager):**

- The central brain of Wazuh.
- Processes, analyzes, and correlates data received from agents.
- Applies detection rules and generates security alerts.
- Can be deployed in a cluster for high availability and load balancing in larger environments.

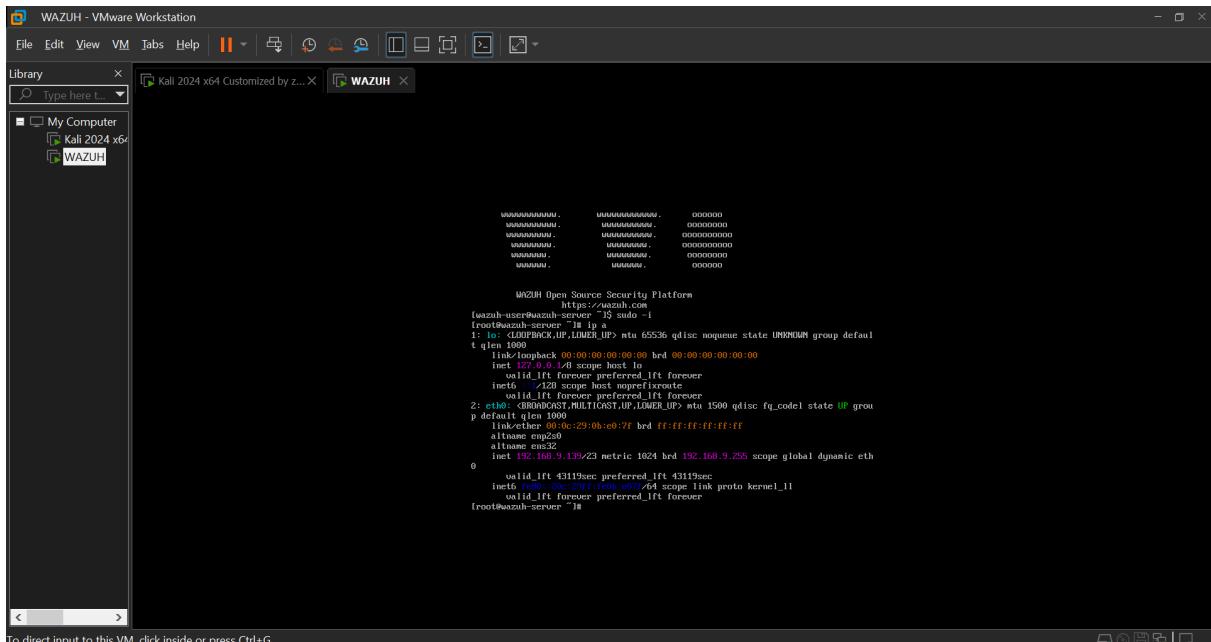
### **3. Wazuh Indexer:**

- (Typically OpenSearch or Elasticsearch).
- Stores and indexes all collected security events and alerts.
- Enables fast and powerful searching and historical analysis of data.
- Can be deployed in a cluster for scalability.

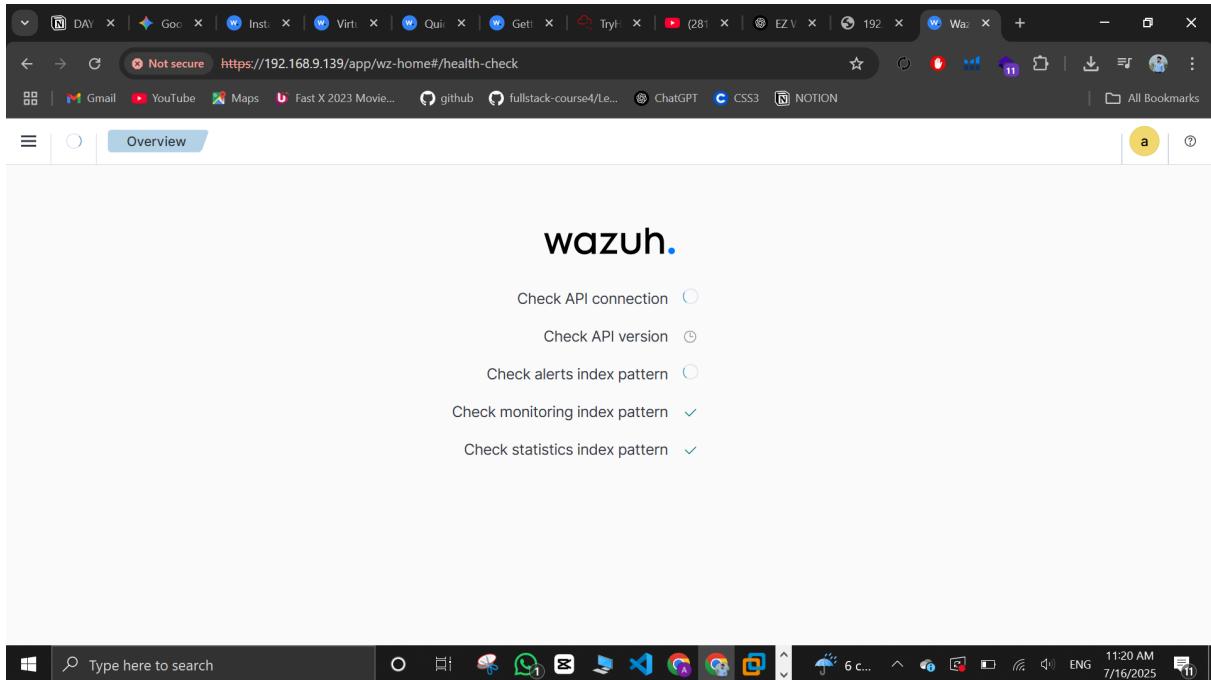
### **4. Wazuh Dashboard:**

- (Built on OpenSearch Dashboards/Kibana).
- The web-based user interface for managing Wazuh.
- Provides visualizations, dashboards, real-time alerts, and a search console for security data

installed wazuh server through and ova file that was imported in vmware



accessed the dashboard through web browser



This screenshot shows the Wazuh dashboard interface. At the top, there's a summary section for 'AGENTS SUMMARY' stating 'This instance has no agents registered. Please deploy agents to begin monitoring your endpoints.' Below this is a section for 'LAST 24 HOURS ALERTS' with four categories: Critical severity (0), High severity (0), Medium severity (2), and Low severity (8). The dashboard also includes sections for 'ENDPOINT SECURITY' (Configuration Assessment, Malware Detection) and 'THREAT INTELLIGENCE' (Threat Hunting, Vulnerability Detection). A search bar and taskbar are at the bottom.

## deployed agent

This screenshot shows the 'Vulnerability Detection' dashboard for the agent 'DESKTOP-0QVFAMH'. The top navigation bar shows the URL as https://192.168.9.139/app/vulnerability-detection#/overview?tab=vuls&tabView=dashboard&agentId=002&... The main area displays five summary cards: Critical - Severity (1), High - Severity (0), Medium - Severity (0), Low - Severity (0), and Pending - Evaluation (0). Below these are five detailed sections: Top 5 vulnerabilities (CVE-2023-21554, Count 1), Top 5 OS (Microsoft Windows 10 Pro 10.0.19044.1288, Count 1), Top 5 agents (DESKTOP-0QVFAMH, Count 1), Top 5 packages (Microsoft Windows, Count 1), and a search bar. The taskbar at the bottom shows various application icons and system status.