trios College

ASSIGNMENT 1

USING SIEM

Security Information and Event Management tools

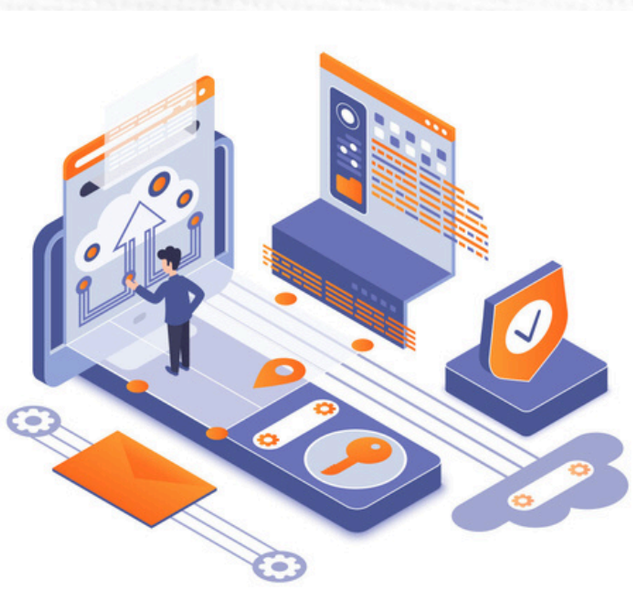
Prepared By : Rajeev Khoodeeram

Submitted To : Mr Abdul Choudhry

Course : Security Fundamentals

2025

September 4

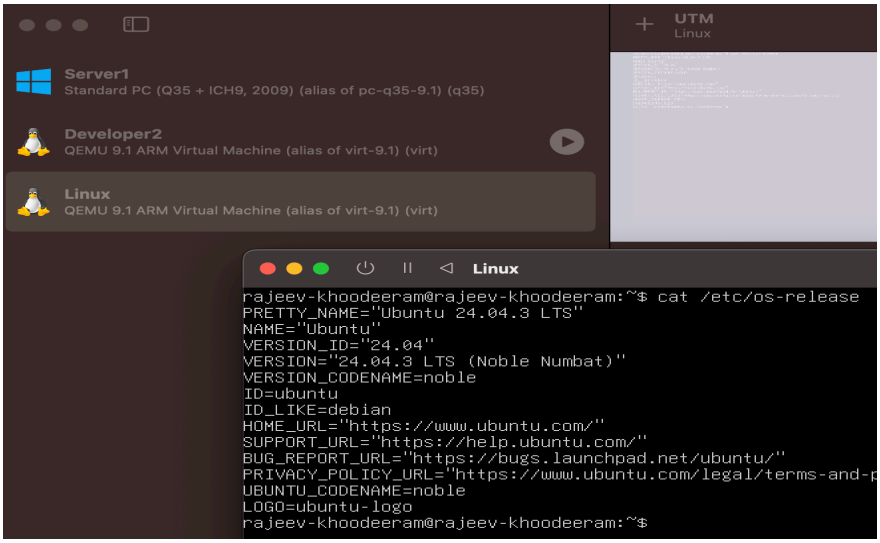


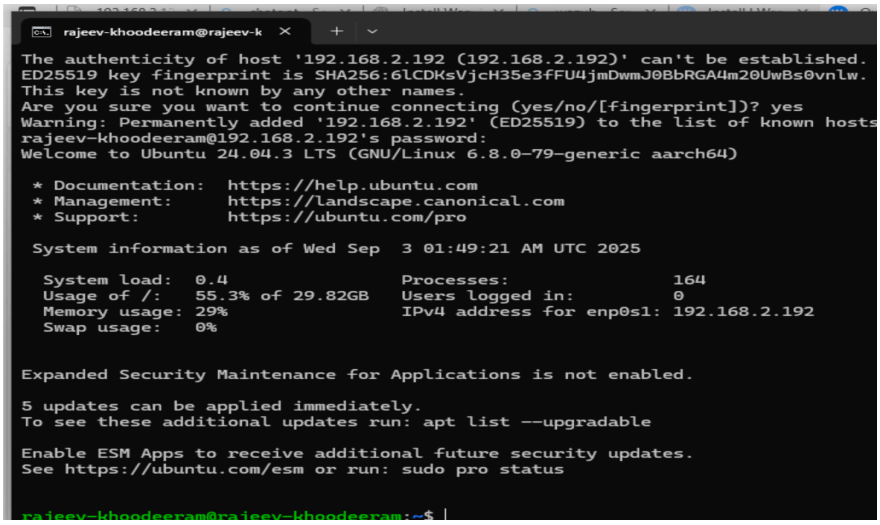
1. Overview

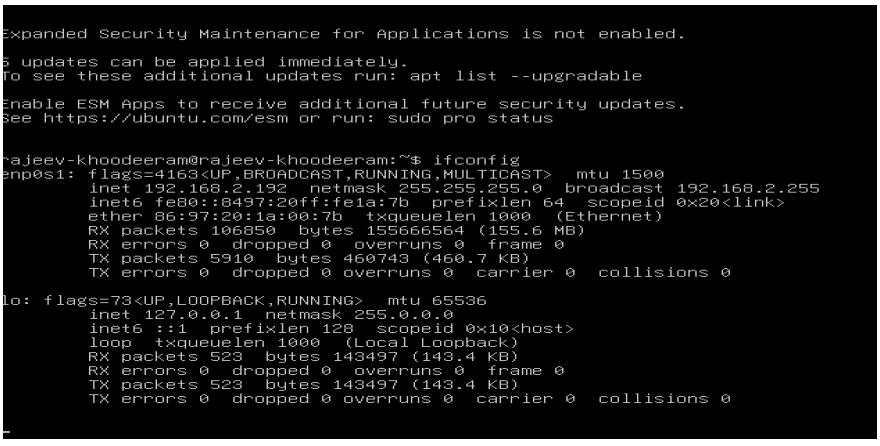
SIEM (Security Information and Event Management) is a tool that helps organizations keep an eye on their IT environment. It collects logs and security events from different systems—like servers, network devices, and applications—then analyzes them to spot unusual activity or potential threats.

In today's world, cyberattacks are constant and often sophisticated. SIEM helps detect breaches quickly, investigate incidents efficiently, and ensure compliance with security regulations. Essen- tially, it's like having a security control center that watches over your digital assets 24/7.

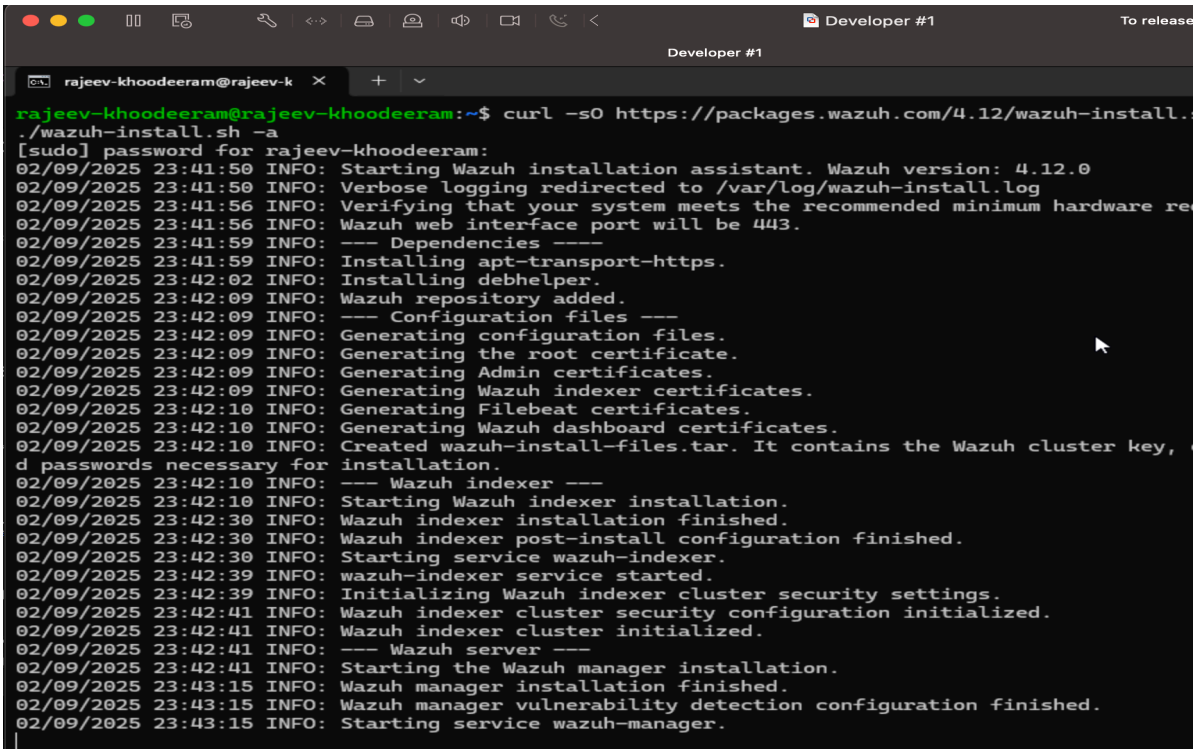
2. Installation of Ubuntu Server



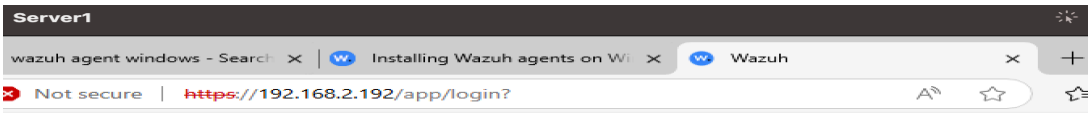


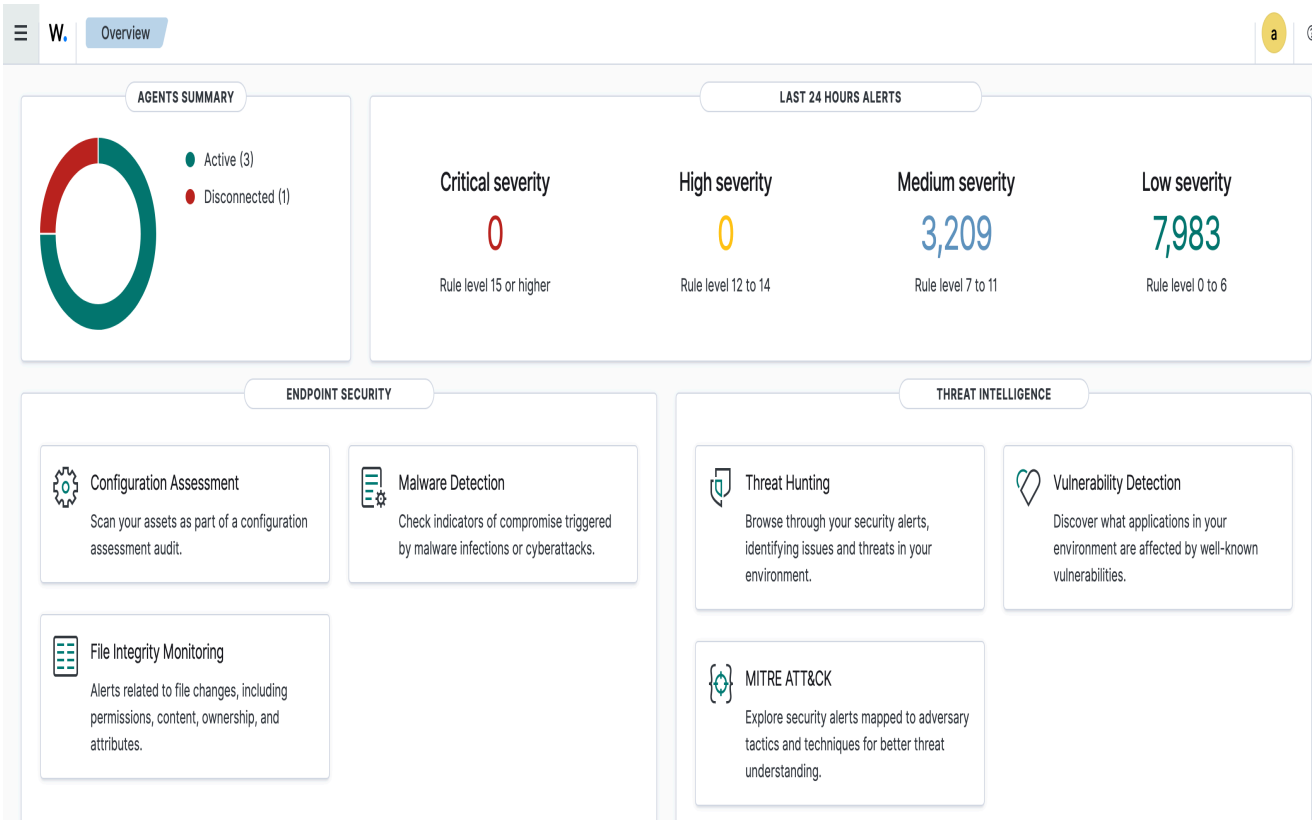


3. Installation of Wazuh Manager

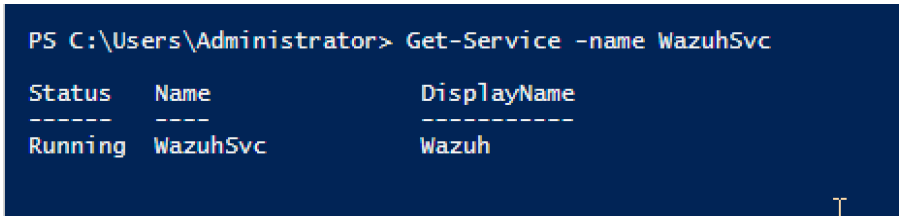


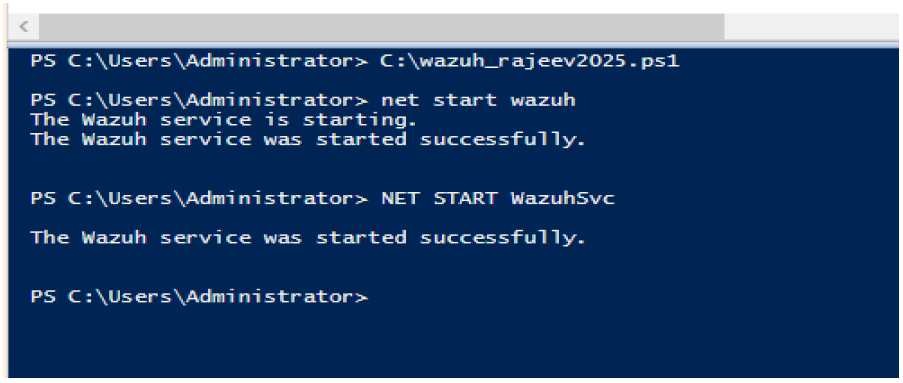
4. Wazuh Dashboard

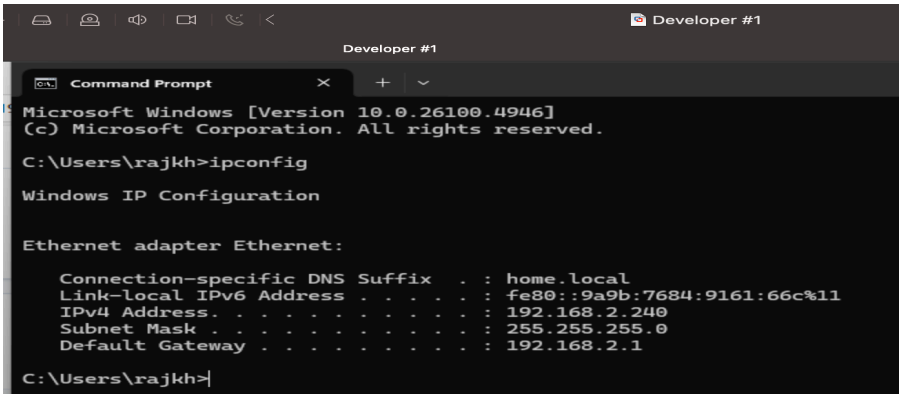


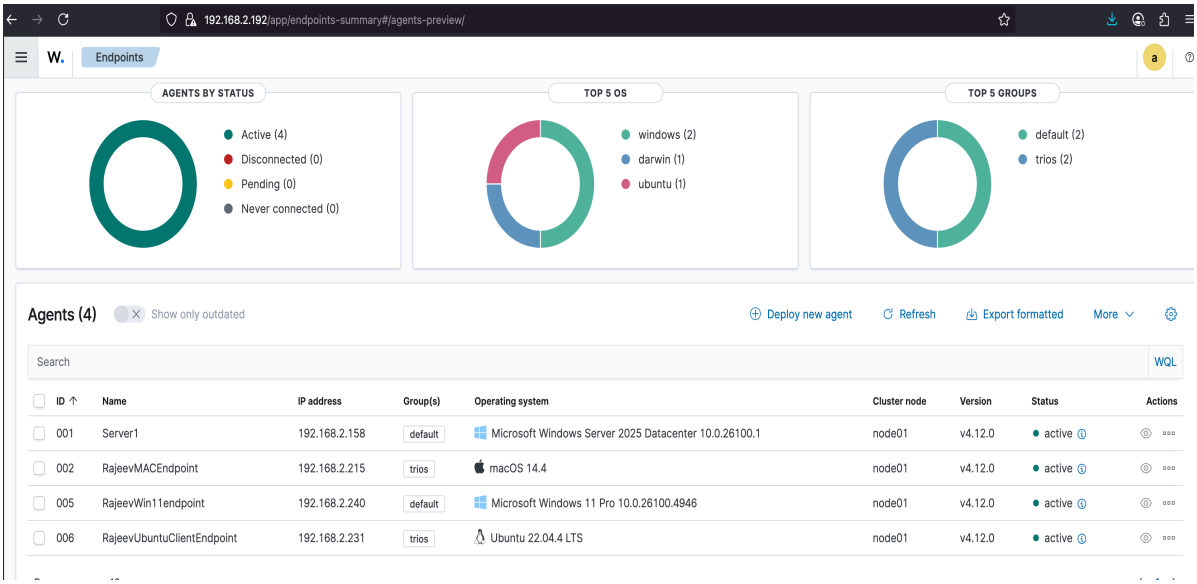


5. Installation of Windows Agents / Endpoints (See Agent 005)

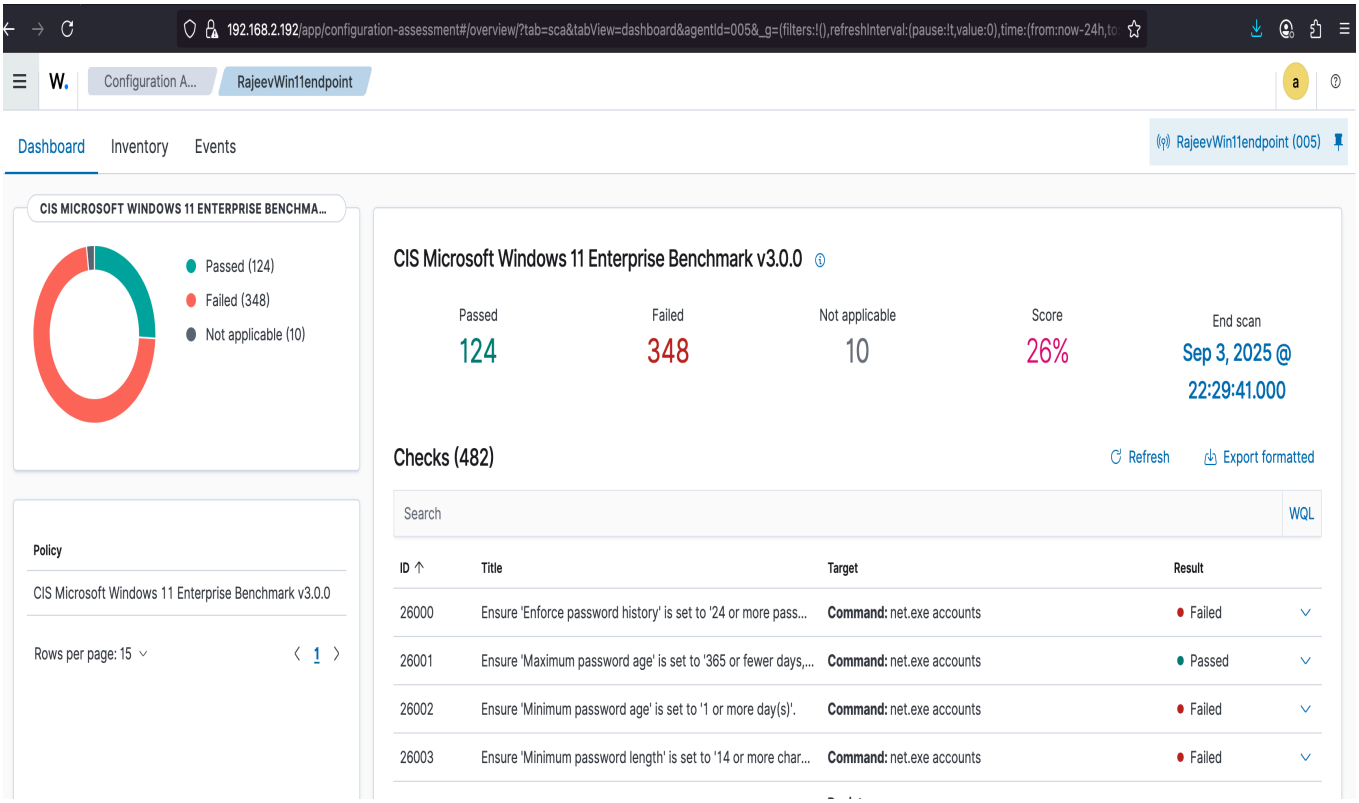




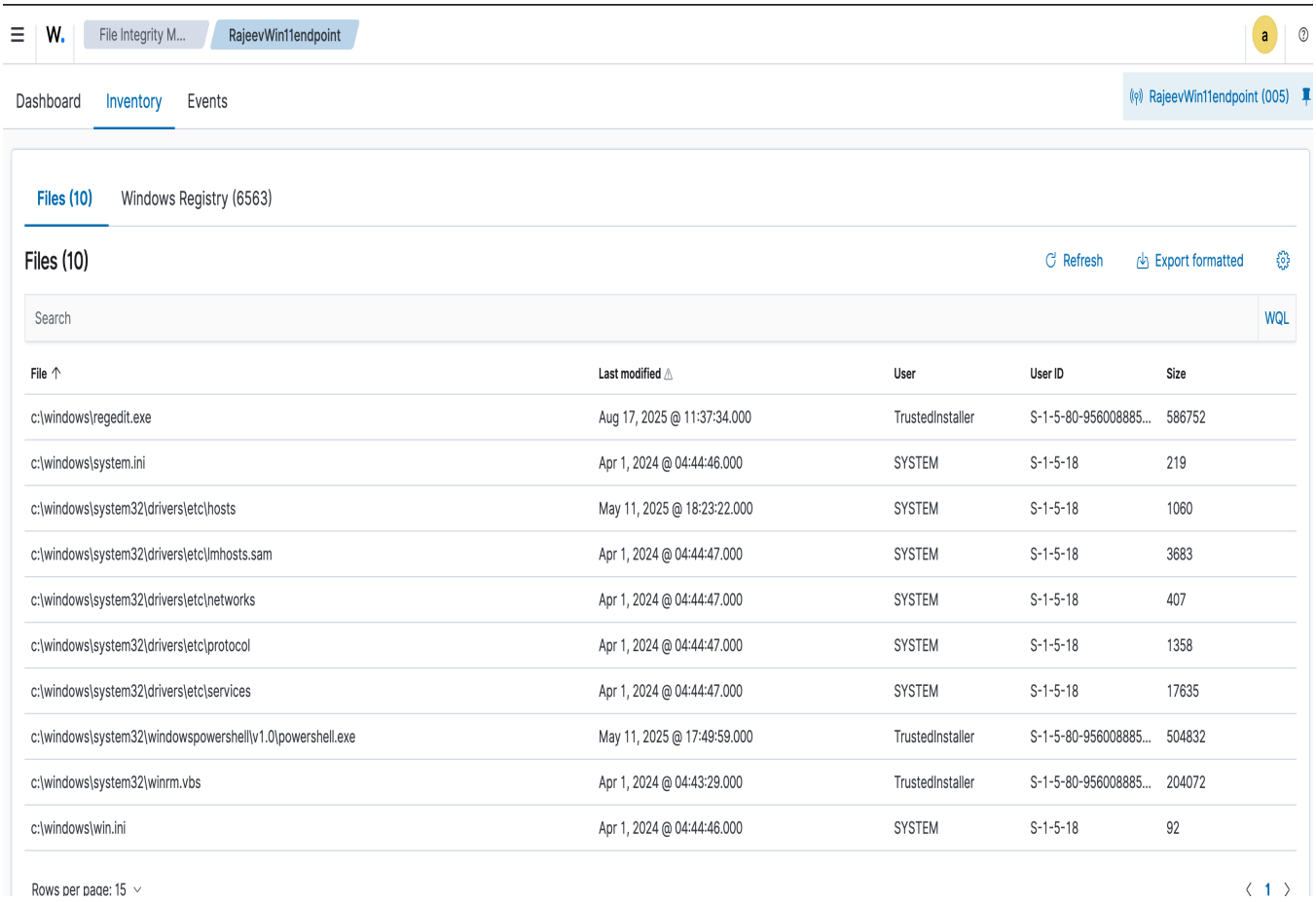




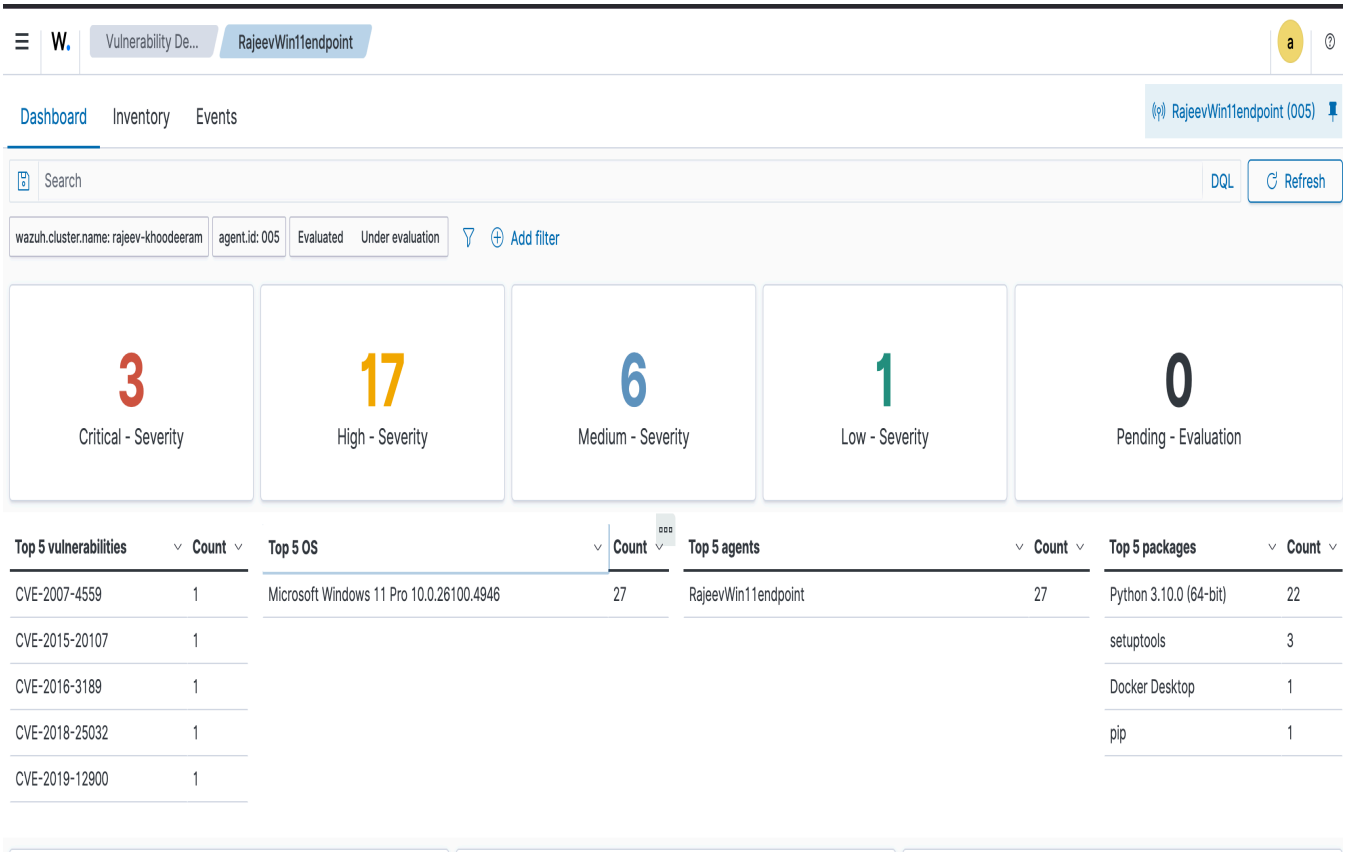
6. Configuration Assessment for your Windows 11 endpoint



7. File Integrity Monitoring of Windows 11 endpoint



8. Vulnerability Detection



9. What types of devices can Wazuh monitor?

1. **Operating systems supported by Wazuh agents**:

- **Linux/Unix**: Ubuntu, Debian, CentOS, RHEL, SUSE, Amazon Linux, Solaris, AIX, HP-UX
- **Windows**: Windows 7/10/11, Windows Server 2012/2016/2019/2022
- **macOS**: Intel and Apple Silicon versions

2. **Cloud Services**

- **AWS** (CloudTrail, CloudWatch, GuardDuty)
- **Microsoft Azure** (Activity Logs, Security Center)
- **Google Cloud (GCP)** (Stackdriver, Security Command Center)

3. Network Devices & Security Appliances

- Firewalls (Cisco ASA, Fortinet, Palo Alto, pfSense, etc.)
- Routers & Switches (Cisco, Juniper, HP, etc.)

10. Is it agent-based or agentless or both?

Wazuh is **primarily agent-based**, but it also supports **agentless monitoring** in certain cases. Here's a detailed breakdown:

1. Agent-Based

- ✦Wazuh agents are installed on endpoints (Windows, Linux, macOS, cloud instances, containers).
- ✦Agents collect **logs, events, file integrity changes, vulnerability data, configuration audits, and security alerts**.
- ✦They communicate securely with the Wazuh manager for analysis and reporting.
- ✦Agent-based monitoring is the **full-featured approach**, offering real-time detection and active response capabilities.

2. Agentless

- ✦Wazuh can also monitor systems **without installing an agent** using protocols like **SSH (Linux/macOS), WMI (Windows), or API integrations**.
- ✦Typically used for **network devices, routers, switches, or systems where installing an agent is not possible**.
- ✦Some features may be limited compared to agent-based monitoring (e.g., file integrity monitoring may not work fully).

11. What are the differences between the free and paid version?

Wazuh Open Source (Free)

- **Cost**: $0
- **Deployment**: On-premises (self-hosted)
- **Core Features**:
  - ✦ Real-time log analysis and alerting
  - ✦ File integrity monitoring
  - ✦ Intrusion detection
  - ✦ Vulnerability detection
  - ✦ Cloud workload protection
  - ✦ Compliance reporting
- **Support**: Community-driven support via forums and documentation
- **Scalability**: Suitable for small to medium-sized environments; requires manual setup and maintenance

Wazuh Cloud (Paid)

- **Cost**: Starts at **$571/month** for the Small profile; pricing increases with scale and features
- **Deployment**: Managed cloud environment on AWS
- **Core Features**:
  - ✦ Fully managed Wazuh infrastructure

- ✦ Pre-configured environments (Small, Medium, Large profiles)
- ✦ Automatic scaling and updates
- ✦ Integrated dashboards and analytics
- ✦ PCI DSS Level 1 and SOC 2 compliance

- **Support**: 24/7 professional support included
- **Scalability**: Designed for enterprises and organizations requiring high availability and minimal maintenance

12. List 3 other SIEM products on the market that provide similar functionality to Wazuh.

1. **Security Onion**

Security Onion is a free and open-source Linux distribution for intrusion detection, network security monitoring, and log management

2. **Graylog**
Graylog is an open-source log management platform that enables organizations to collect, index, and analyze log data. It offers a powerful search and analysis interface, alerting capabilities, and supports various data sources.

3. **Elastic SIEM**
Elastic SIEM is a part of the Elastic Stack (formerly known as the ELK Stack) and provides real-time security analytics and insights.

12. Compare/contrast Security Onion with Wazuh.

Security Onion

- A Linux distribution built for **network security monitoring (NSM)**, **intrusion detection (IDS/IPS)**, and **log management**.
- Bundles multiple open-source security tools (Suricata, Zeek, Elastic Stack, OSSEC/ Wazuh, TheHive, CyberChef, etc.) into a ready-to-use platform.
- Primarily **network-centric** but can also monitor endpoints.
- Complain features are limited
- It is a dedicated OS available as .iso file

Wazuh

- A **Security Information and Event Management (SIEM) + XDR (Extended Detection and Response)** platform.
- Focused on **endpoint security**, log collection, vulnerability detection, compliance, and threat detection.
- Uses an **agent-based architecture** (though it supports some agentless monitoring).
- Strong support for various compliance (GDPR, NIST, HIPAA, etc)
- It is a platform installed on Linux servers