



trios College

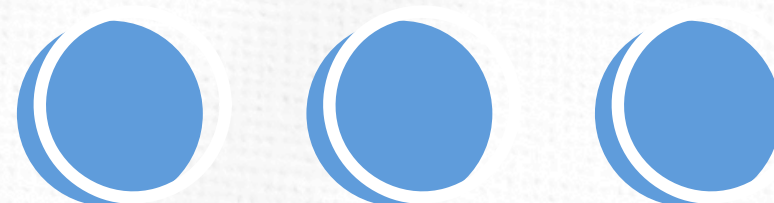
ASSIGNMENT 1

USING SIEM

*Security Information and Event
Management tools*

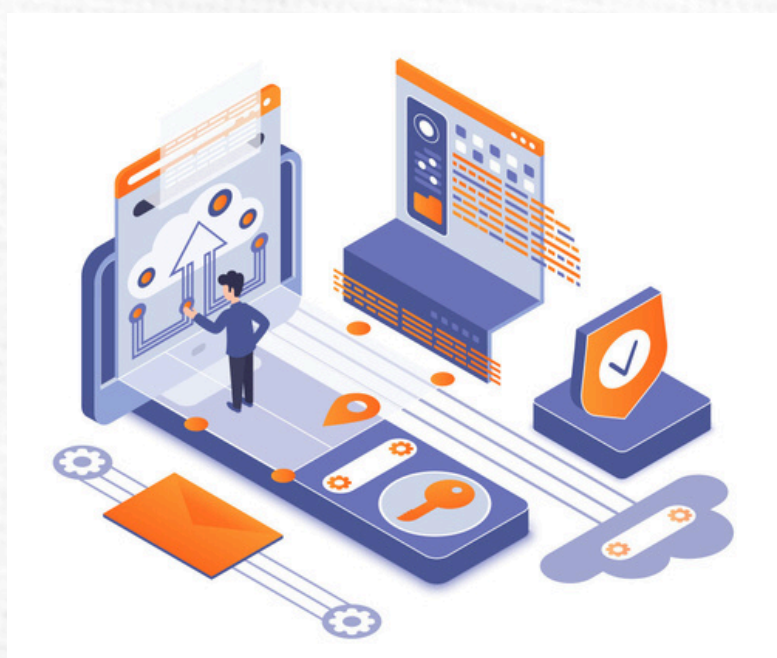
Prepared By : Rajeev Khoodeeram

Submitted To : Mr Abdul Choudhry



20
25

September 4



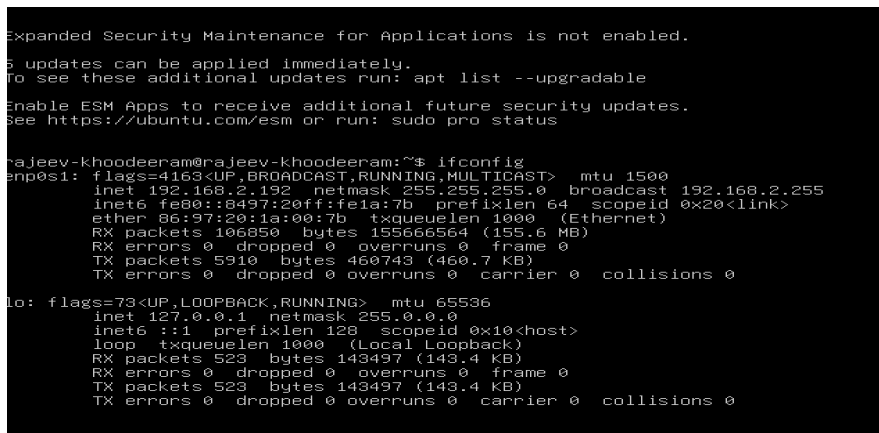
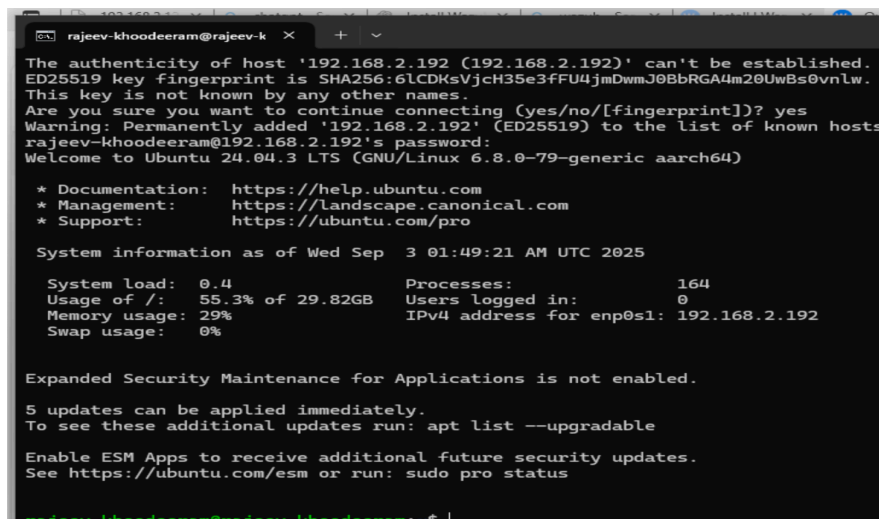
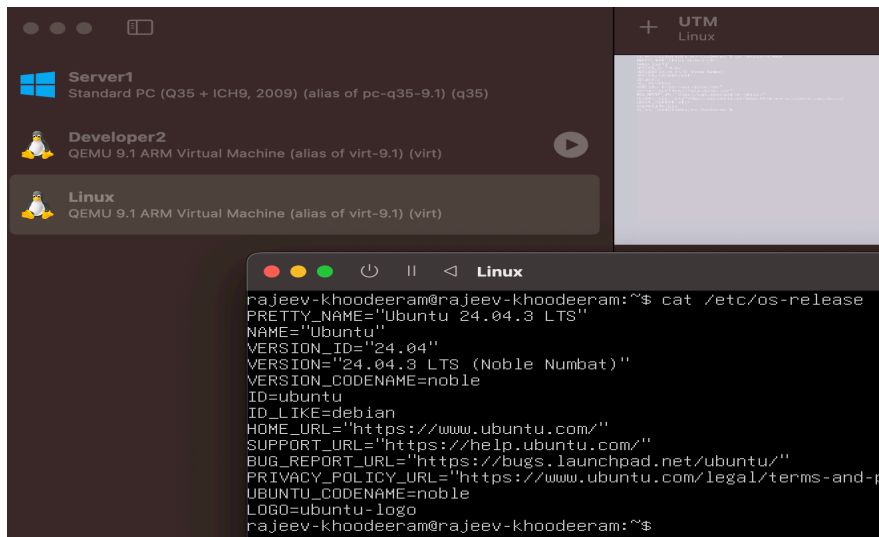
1. Overview	2
2. Installation of Ubuntu Server	3
3. Installation of Wazuh Manager	4
4. Wazuh Dashboard	5
5. Installation of Windows Agents / Endpoints (See Agent 005)	6
6. Configuration Assessment for your Windows 11 endpoint	7
7. File Integrity Monitoring of Windows 11 endpoint	8
8. Vulnerability Detection	9
9. What types of devices can Wazuh monitor?	10
10. Is it agent-based or agentless or both?	11
11. What are the differences between the free and paid version?	12
12. List 3 other SIEM products on the market that provide similar functionality to Wazuh.	14
12. Compare/contrast Security Onion with Wazuh.	15

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. Essentially, it's like having a security control center that watches over your digital assets 24/7.

2. Installation of Ubuntu Server

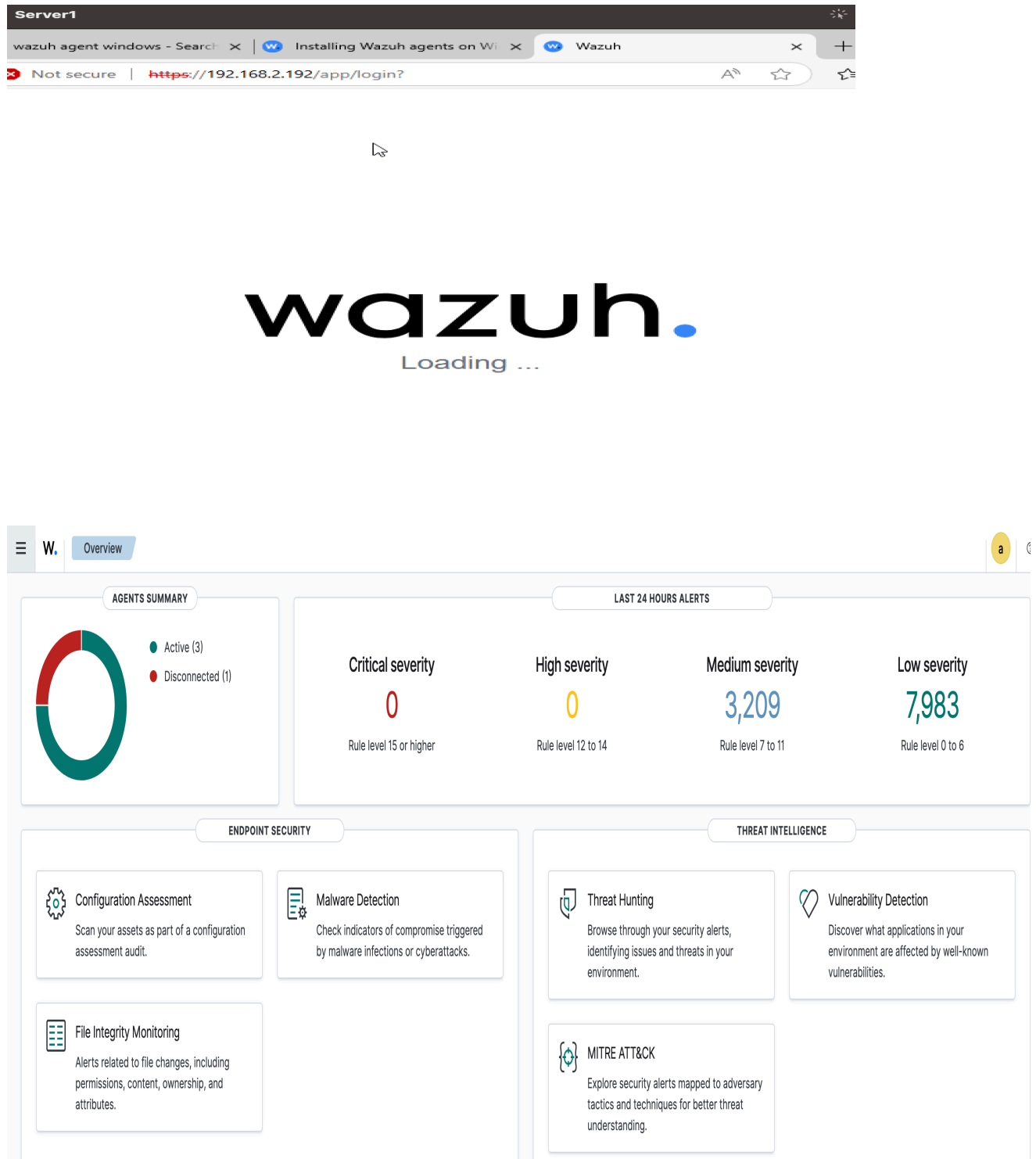


3. Installation of Wazuh Manager

```
Developer #1
Developer #1
rajeev-khoodeeram@rajeev-k x + v
rajeev-khoodeeram@rajeev-khoodeeram:~$ curl -sO https://packages.wazuh.com/4.12/wazuh-install...
./wazuh-install.sh -a
[sudo] password for rajeedv-khoodeeram:
02/09/2025 23:41:50 INFO: Starting Wazuh installation assistant. Wazuh version: 4.12.0
02/09/2025 23:41:50 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/09/2025 23:41:56 INFO: Verifying that your system meets the recommended minimum hardware re
02/09/2025 23:41:56 INFO: Wazuh web interface port will be 443.
02/09/2025 23:41:59 INFO: --- Dependencies ---
02/09/2025 23:41:59 INFO: Installing apt-transport-https.
02/09/2025 23:42:02 INFO: Installing debhelper.
02/09/2025 23:42:09 INFO: Wazuh repository added.
02/09/2025 23:42:09 INFO: --- Configuration files ---
02/09/2025 23:42:09 INFO: Generating configuration files.
02/09/2025 23:42:09 INFO: Generating the root certificate.
02/09/2025 23:42:09 INFO: Generating Admin certificates.
02/09/2025 23:42:09 INFO: Generating Wazuh indexer certificates.
02/09/2025 23:42:10 INFO: Generating Filebeat certificates.
02/09/2025 23:42:10 INFO: Generating Wazuh dashboard certificates.
02/09/2025 23:42:10 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key,
d passwords necessary for installation.
02/09/2025 23:42:10 INFO: --- Wazuh indexer ---
02/09/2025 23:42:10 INFO: Starting Wazuh indexer installation.
02/09/2025 23:42:30 INFO: Wazuh indexer installation finished.
02/09/2025 23:42:30 INFO: Wazuh indexer post-install configuration finished.
02/09/2025 23:42:30 INFO: Starting service wazuh-indexer.
02/09/2025 23:42:39 INFO: wazuh-indexer service started.
02/09/2025 23:42:39 INFO: Initializing Wazuh indexer cluster security settings.
02/09/2025 23:42:41 INFO: Wazuh indexer cluster security configuration initialized.
02/09/2025 23:42:41 INFO: Wazuh indexer cluster initialized.
02/09/2025 23:42:41 INFO: --- Wazuh server ---
02/09/2025 23:42:41 INFO: Starting the Wazuh manager installation.
02/09/2025 23:43:15 INFO: Wazuh manager installation finished.
02/09/2025 23:43:15 INFO: Wazuh manager vulnerability detection configuration finished.
02/09/2025 23:43:15 INFO: Starting service wazuh-manager.
```

```
03/09/2025 01:46:17 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: nn0AzQSR*w0JswY.+8eLT88F.PJ8YJgL
03/09/2025 01:46:17 INFO: Installation finished.
rajeev-khoodeeram@rajeev-khoodeeram:~$
```

4. Wazuh Dashboard



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

```
PS C:\Users\Administrator> Get-Service -name WazuhSvc

Status      Name      DisplayName
-----
Running     WazuhSvc  Wazuh
```

```
PS C:\Users\Administrator> C:\wazuh_rajeev2025.ps1

PS C:\Users\Administrator> net start wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Users\Administrator> NET START WazuhSvc
The Wazuh service was started successfully.

PS C:\Users\Administrator>
```

```
Microsoft Windows [Version 10.0.26100.4946]
(c) Microsoft Corporation. All rights reserved.

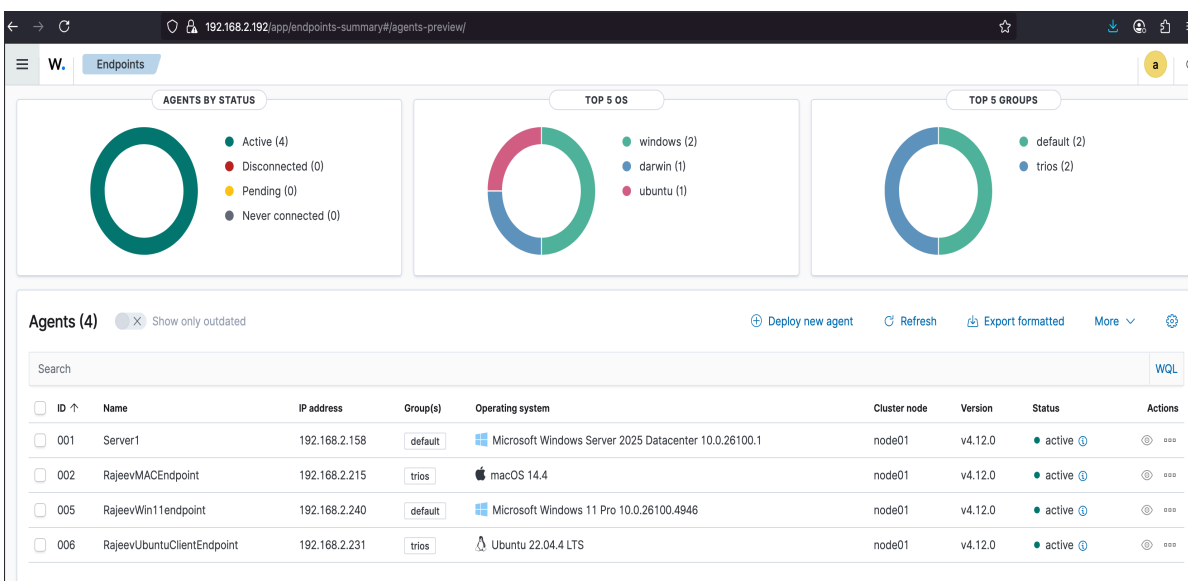
C:\Users\rajkh>ipconfig

Windows IP Configuration

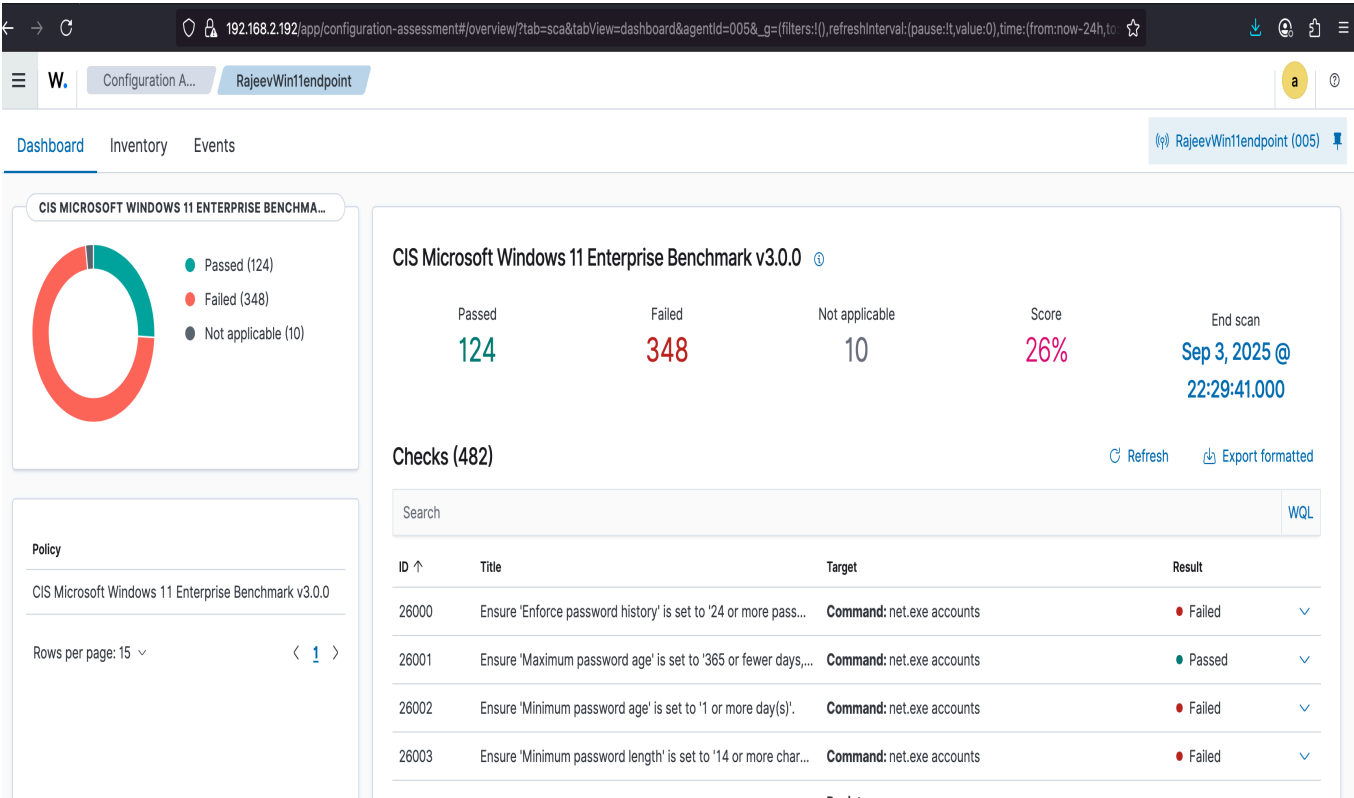
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : home.local
    Link-local IPv6 Address . . . . . : fe80::9a9b:7684:9161:66c%11
    IPv4 Address. . . . . : 192.168.2.240
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\Users\rajkh>
```



6. Configuration Assessment for your Windows 11 endpoint



7. File Integrity Monitoring of Windows 11 endpoint

W.

File Integrity M...

RajeevWin11endpoint

a

Dashboard

Inventory

Events

RajeevWin11endpoint (005)

Files (10)

Windows Registry (6563)

Files (10)

Refresh

Export formatted

Search

WQL

File	Last modified	User	User ID	Size
c:\windows\regedit.exe	Aug 17, 2025 @ 11:37:34.000	TrustedInstaller	S-1-5-80-956008885...	586752
c:\windows\system.ini	Apr 1, 2024 @ 04:44:46.000	SYSTEM	S-1-5-18	219
c:\windows\system32\drivers\etc\hosts	May 11, 2025 @ 18:23:22.000	SYSTEM	S-1-5-18	1060
c:\windows\system32\drivers\etc\lmhosts.sam	Apr 1, 2024 @ 04:44:47.000	SYSTEM	S-1-5-18	3683
c:\windows\system32\drivers\etc\networks	Apr 1, 2024 @ 04:44:47.000	SYSTEM	S-1-5-18	407
c:\windows\system32\drivers\etc\protocol	Apr 1, 2024 @ 04:44:47.000	SYSTEM	S-1-5-18	1358
c:\windows\system32\drivers\etc\services	Apr 1, 2024 @ 04:44:47.000	SYSTEM	S-1-5-18	17635
c:\windows\system32\windowpowershell\v1.0\powershell.exe	May 11, 2025 @ 17:49:59.000	TrustedInstaller	S-1-5-80-956008885...	504832
c:\windows\system32\winrm.vbs	Apr 1, 2024 @ 04:43:29.000	TrustedInstaller	S-1-5-80-956008885...	204072
c:\windows\win.ini	Apr 1, 2024 @ 04:44:46.000	SYSTEM	S-1-5-18	92

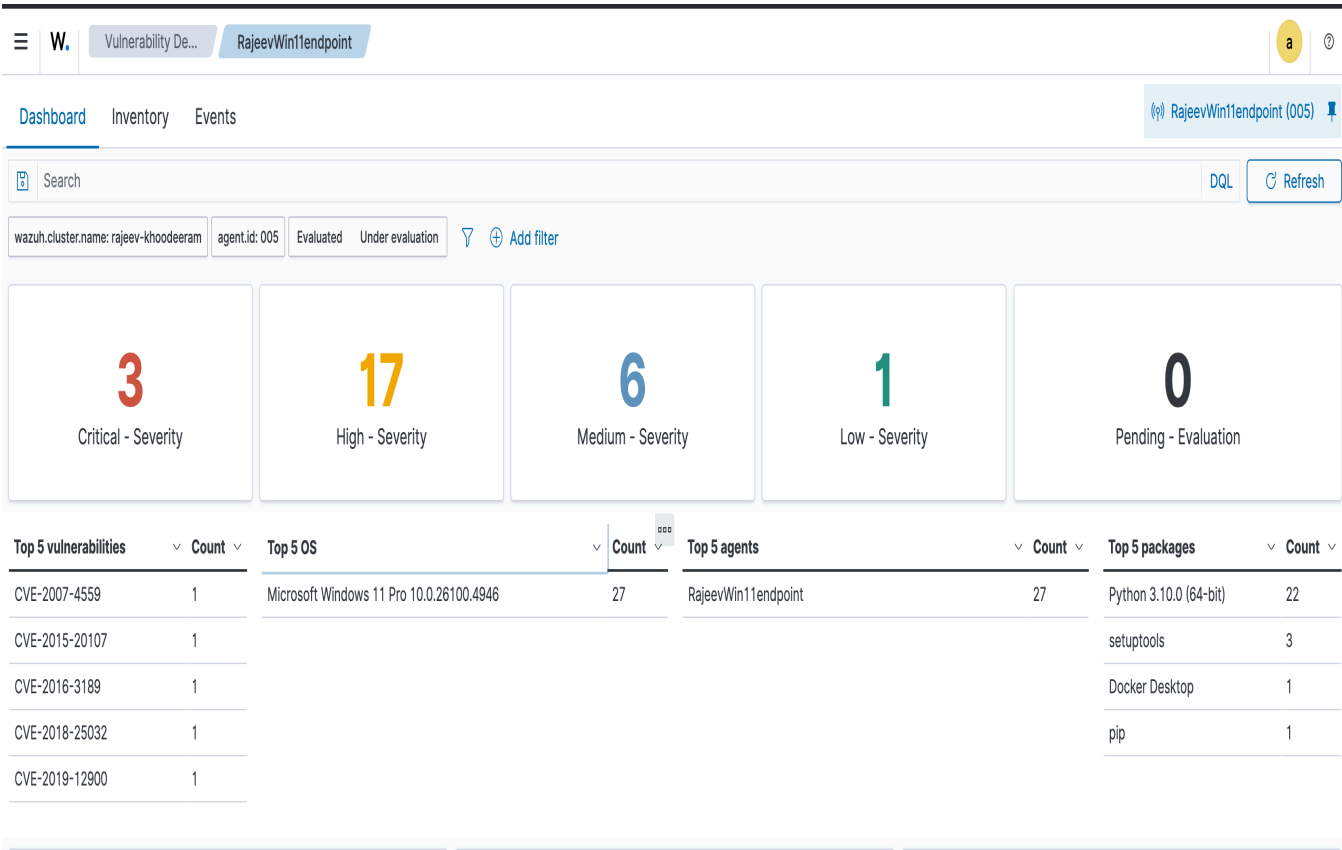
Rows per page: 15

<

1

>

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