



ASSIGNMENT 1

USING SIEM

Security Information and Event Management tools

Prepared By : Rajeev Khoodeeram

Submitted To : Mr Abdul Choudhry

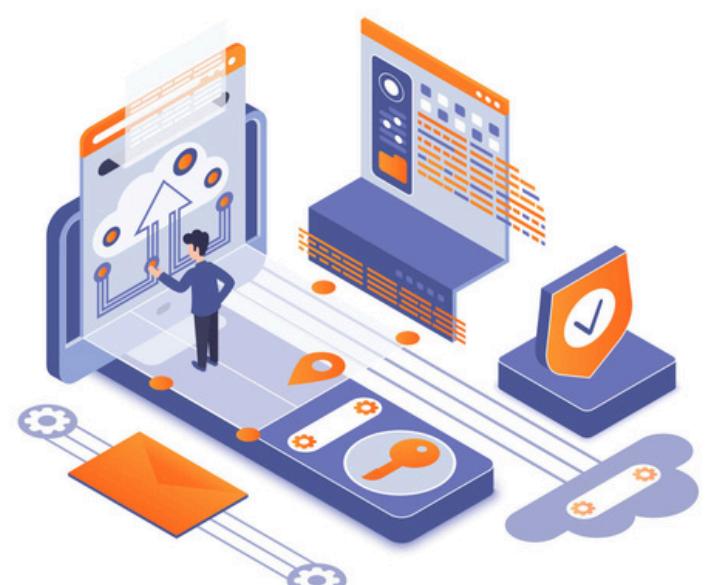


20
25

September 4



Course : Security Fundamentals



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



```
rajeev-khoodeeram@rajeev-khoodeeram:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-p
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
rajeev-khoodeeram@rajeev-khoodeeram:~$
```

```
rajeev-khoodeeram@rajeev-k: ~ + | 
The authenticity of host '192.168.2.192 (192.168.2.192)' can't be established.
ED25519 key fingerprint is SHA256:6lCDKsVjCH3Se3ffU4jmDwmJ0BbRGA4m20UwBs0vnLw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.192' (ED25519) to the list of known hosts.
rajeev-khoodeeram@192.168.2.192's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-79-generic aarch64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Sep  3 01:49:21 AM UTC 2025

System load:  0.4          Processes:           164
Usage of /:   55.3% of 29.82GB   Users logged in:  0
Memory usage: 29%          IPv4 address for enp0s1: 192.168.2.192
Swap usage:   0%          

Expanded Security Maintenance for Applications is not enabled.

5 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

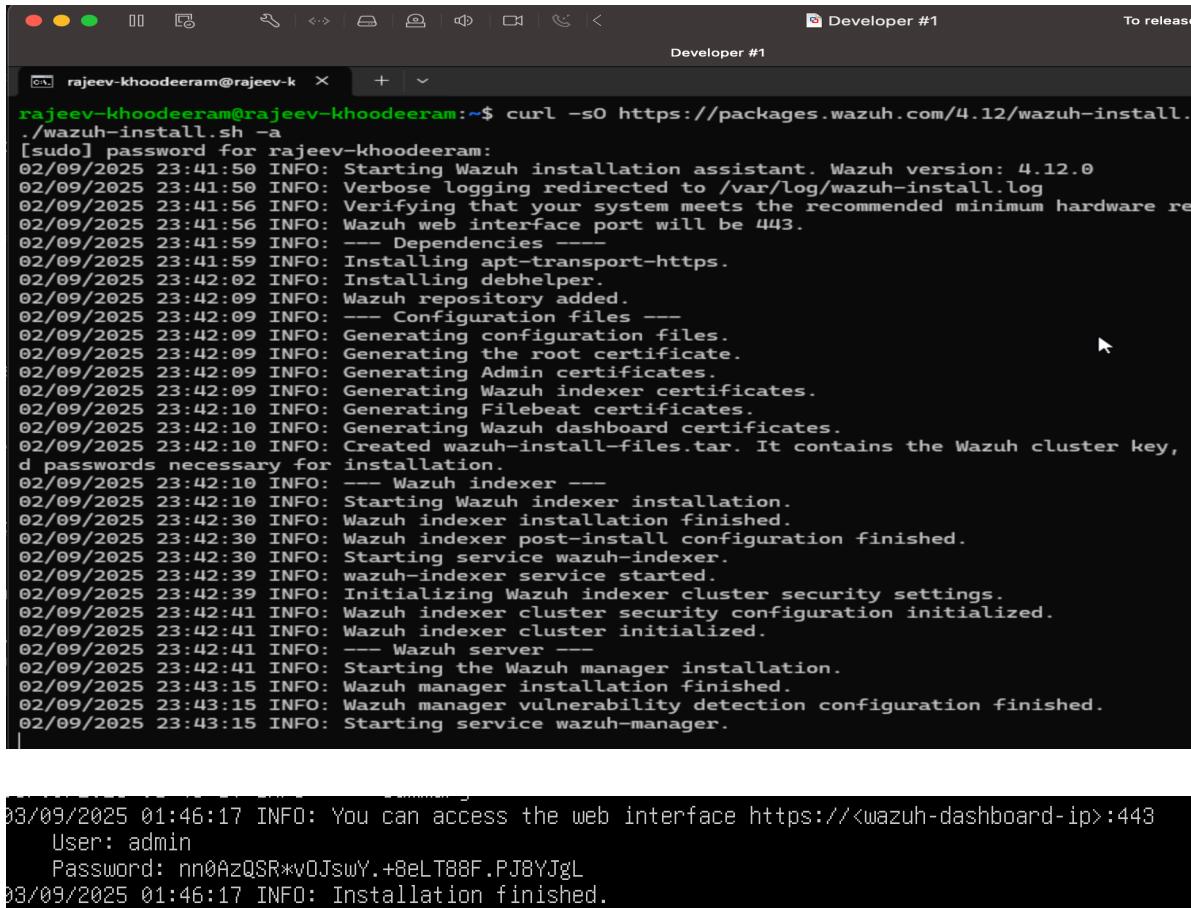
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

rajeev-khoodeeram@rajeev-khoodeeram:~$ |
```

```
rajeev-khoodeeram@rajeev-khoodeeram:~$ ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.192  netmask 255.255.255.0  broadcast 192.168.2.255
                inet6 fe80::8497:20ff:fe1a:007b  prefixlen 64  scopeid 0x20<link>
                    ether 86:97:20:1a:00:7b  txqueuelen 1000  (Ethernet)
                    RX packets 166850  bytes 155666564 (155.6 MB)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 5910  bytes 460743 (460.7 KB)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopeid 0x10<host>
                    loop  txqueuelen 1000  (Local Loopback)
                    RX packets 523  bytes 143497 (143.4 KB)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 523  bytes 143497 (143.4 KB)
                    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

3. Installation of Wazuh Manager

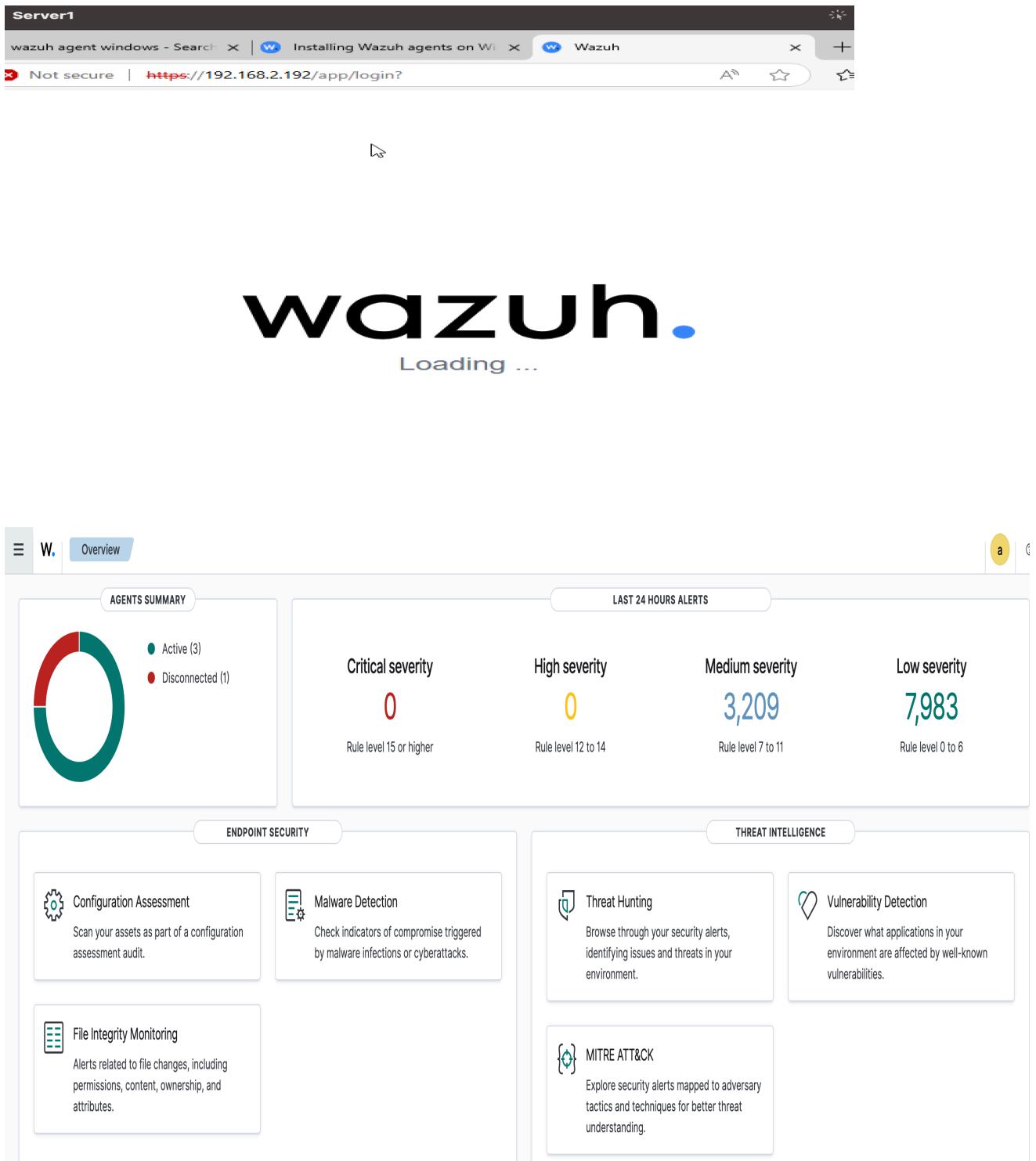


The terminal window shows the execution of the Wazuh Manager installation script. The user runs `curl -s0 https://packages.wazuh.com/4.12/wazuh-install.sh -a` to download and execute the script. The script performs various tasks including dependency checks, configuration file generation, certificate creation for Wazuh indexer and Filebeat, and the creation of a cluster key. It also installs the Wazuh indexer service and starts it. Finally, it installs the Wazuh manager service and starts it, providing the admin user and password for access.

```
rajeev-khoodeeram@rajeev-khoodeeram:~$ curl -s0 https://packages.wazuh.com/4.12/wazuh-install.sh -a
[sudo] password for rajeev-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 requirements.
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
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*v0JswY.+8eLT88F.PJ8YJgL
03/09/2025 01:46:17 INFO: Installation finished.
rajeev-khoodeeram@rajeev-khoodeeram:~$
```

4. Wazuh Dashboard



The screenshot shows the Wazuh Dashboard interface. At the top, a browser window displays the URL <https://192.168.2.192/app/login?>. The dashboard itself has a large "wazuh." logo with "Loading ..." below it. The main content area is divided into several sections:

- AGENTS SUMMARY**: A donut chart showing 3 Active agents and 1 Disconnected agent.
- LAST 24 HOURS ALERTS**: A summary of alerts by severity:
 - Critical severity: 0 (Rule level 15 or higher)
 - High severity: 0 (Rule level 12 to 14)
 - Medium severity: 3,209 (Rule level 7 to 11)
 - Low severity: 7,983 (Rule level 0 to 6)
- ENDPOINT SECURITY**:
 - Configuration Assessment**: Scan your assets as part of a configuration assessment audit.
 - Malware Detection**: Check indicators of compromise triggered by malware infections or cyberattacks.
 - File Integrity Monitoring**: Alerts related to file changes, including permissions, content, ownership, and attributes.
- THREAT INTELLIGENCE**:
 - Threat Hunting**: Browse through your security alerts, identifying issues and threats in your environment.
 - Vulnerability Detection**: Discover what applications in your environment are affected by well-known vulnerabilities.
 - MITRE ATT&CK**: Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

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>
```

```
Developer #1
Command Prompt
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>
```

The screenshot shows the Wazuh web interface with the following sections:

- Endpoints** tab selected.
- AGENTS BY STATUS**: A donut chart showing the status of agents. Legend: Active (4), Disconnected (0), Pending (0), Never connected (0).
- TOP 5 OS**: A donut chart showing the top 5 operating systems. Legend: windows (2), darwin (1), ubuntu (1).
- TOP 5 GROUPS**: A donut chart showing the top 5 groups. Legend: default (2), trios (1).
- Agents (4)**: A table listing the agents:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Server1	192.168.2.158	default	Microsoft Windows Server 2025 Datacenter 10.0.26100.1	node01	v4.12.0	● active ⓘ	...
002	RajeevMACEndpoint	192.168.2.215	trios	macOS 14.4	node01	v4.12.0	● active ⓘ	...
005	RajeevWin11endpoint	192.168.2.240	default	Microsoft Windows 11 Pro 10.0.26100.4946	node01	v4.12.0	● active ⓘ	...
006	RajeevUbuntuClientEndpoint	192.168.2.231	trios	Ubuntu 22.04.4 LTS	node01	v4.12.0	● active ⓘ	...
- Buttons: Deploy new agent, Refresh, Export formatted, More, and a search bar.

6. Configuration Assessment for your Windows 11 endpoint

The screenshot shows a web-based configuration assessment tool for a Windows 11 endpoint. The top navigation bar includes a back arrow, forward arrow, a refresh icon, and the URL 192.168.2.192/app/configuration-assessment#/overview?tab=sca&tabView=dashboard&agentId=005&_g=filters:(),refreshInterval:(pause:0,value:0),time:(from:now-24h,to:now). The title bar shows 'W. Configuration A...' and 'RajeevWin11endpoint'. The top right corner has a yellow badge with the letter 'a' and a refresh icon.

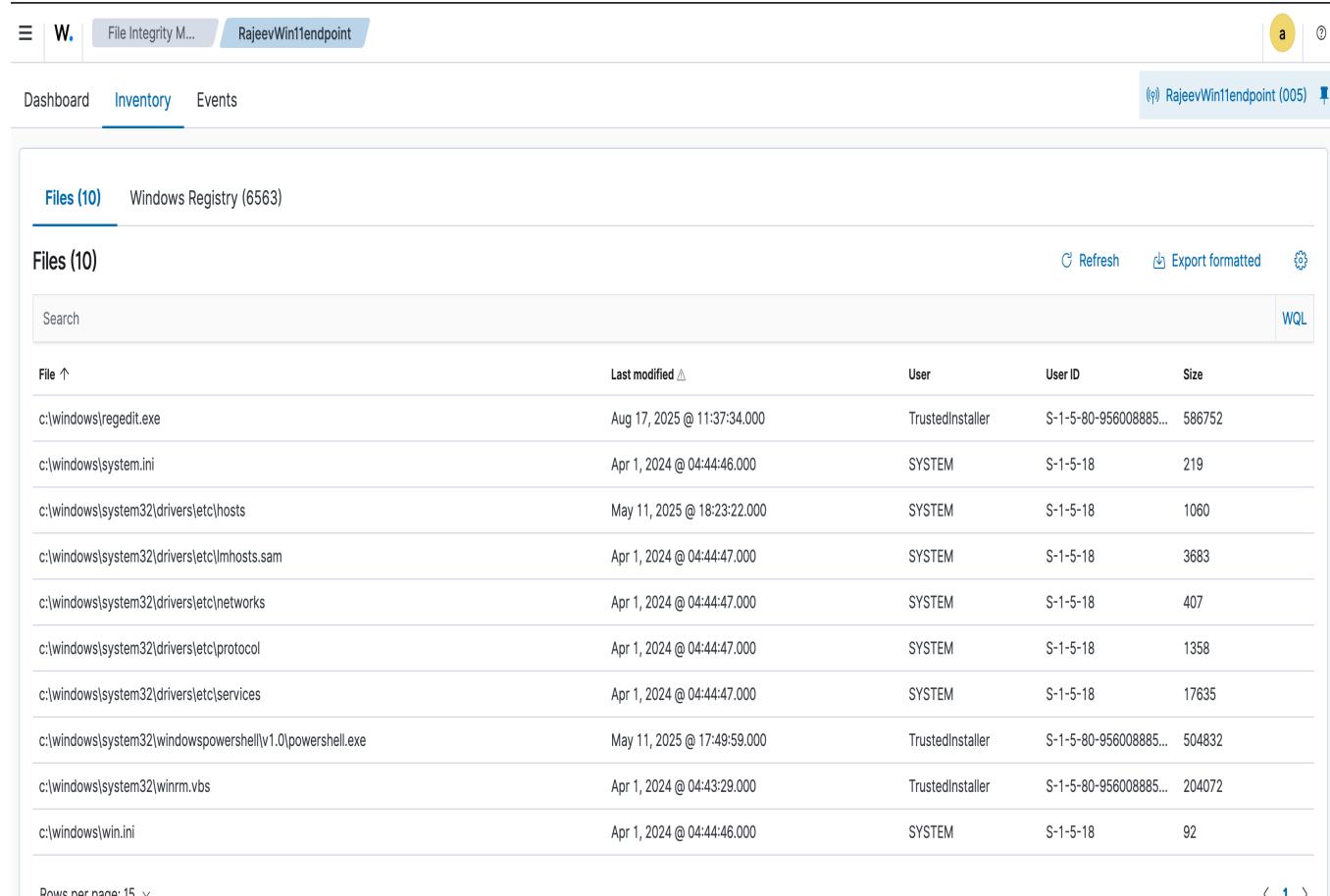
The main content area is divided into sections:

- CIS MICROSOFT WINDOWS 11 ENTERPRISE BENCHMARK**: A donut chart showing the status of checks. The legend indicates:
 - Passed (124)
 - Failed (348)
 - Not applicable (10)
- CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0**: Summary statistics:

Passed	Failed	Not applicable	Score	End scan
124	348	10	26%	Sep 3, 2025 @ 22:29:41.000
- Checks (482)**: A table listing 482 configuration checks. The columns are: ID, Title, Target, and Result. The table includes rows for password policies, such as:

ID	Title	Target	Result
26000	Ensure 'Enforce password history' is set to '24 or more pass...' Command: net.exe accounts		Failed
26001	Ensure 'Maximum password age' is set to '365 or fewer days...' Command: net.exe accounts		Passed
26002	Ensure 'Minimum password age' is set to '1 or more day(s)'. Command: net.exe accounts		Failed
26003	Ensure 'Minimum password length' is set to '14 or more char...' Command: net.exe accounts		Failed

7. File Integrity Monitoring of Windows 11 endpoint



The screenshot shows a web-based interface for monitoring file integrity. At the top, there are navigation tabs: 'Dashboard', 'Inventory' (which is selected and highlighted in blue), and 'Events'. The main content area is titled 'Files (10)' and shows a list of 10 files. Each file entry includes the file path, last modified date, user, user ID, and size. The files listed are: 'c:\windows\regedit.exe', 'c:\windows\system.ini', 'c:\windows\system32\drivers\etc\hosts', 'c:\windows\system32\drivers\etc\lmhosts.sam', 'c:\windows\system32\drivers\etc\networks', 'c:\windows\system32\drivers\etc\protocol', 'c:\windows\system32\drivers\etc\services', 'c:\windows\system32\windowspowershell\v1.0\powershell.exe', 'c:\windows\system32\winrm.vbs', and 'c:\windows\win.ini'. The interface also includes a search bar, a refresh button, an 'Export formatted' button, and a 'WQL' link. The top right corner shows a user profile with the letter 'a' and a help icon.

File	Last modified	User	User ID	Size
c:\windows\regedit.exe	Aug 17, 2025 @ 11:37:34.000	TrustedInstaller	S-1-5-80-95600885...	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\windowspowershell\v1.0\powershell.exe	May 11, 2025 @ 17:49:59.000	TrustedInstaller	S-1-5-80-95600885...	504832
c:\windows\system32\winrm.vbs	Apr 1, 2024 @ 04:43:29.000	TrustedInstaller	S-1-5-80-95600885...	204072
c:\windows\win.ini	Apr 1, 2024 @ 04:44:46.000	SYSTEM	S-1-5-18	92

8. Vulnerability Detection

The screenshot shows the Wazuh Vulnerability Detection interface. At the top, there is a navigation bar with a menu icon, a search bar containing 'W.', and a tab labeled 'Vulnerability De... RajeevWin11endpoint'. On the far right are a user icon and a refresh button.

Below the navigation bar, there is a breadcrumb navigation with 'Dashboard', 'Inventory', and 'Events'. To the right of the breadcrumb is a status bar showing '(p) RajeevWin11endpoint (005)' with a refresh icon.

The main content area features a search bar with a magnifying glass icon and a 'Search' button, along with 'DQL' and 'Refresh' buttons. Below the search bar are several filters: 'wazuh.cluster.name: rajeev-khoodeeram', 'agent.id: 005', 'Evaluated', 'Under evaluation', and 'Add filter'.

The dashboard displays five summary cards with large numbers and severity labels:

- Critical - Severity:** 3
- High - Severity:** 17
- Medium - Severity:** 6
- Low - Severity:** 1
- Pending - Evaluation:** 0

Below the dashboard, there are five tables with dropdown menus for sorting and filtering:

- Top 5 vulnerabilities:** Count (dropdown menu). Data:

CVE-2007-4559	1
CVE-2015-20107	1
CVE-2016-3189	1
CVE-2018-25032	1
CVE-2019-12900	1
- Top 5 OS:** Count (dropdown menu). Data:

Microsoft Windows 11 Pro	10.0.26100.4946	27
--------------------------	-----------------	----
- Top 5 agents:** Count (dropdown menu). Data:

RajeevWin11endpoint	27
---------------------	----
- Top 5 packages:** Count (dropdown menu). Data:

Python 3.10.0 (64-bit)	22
setuptools	3
Docker Desktop	1
pip	1

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)

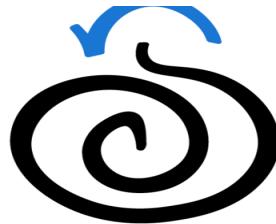
- **Cost:** Starts at **\$571/month** for the Small profile; pricing increases with scale and features
- **Deployment:** Managed cloud environment on AWS
- **Core Features:**
 - ◆ Fully managed Wazuh infrastructure

- ◆ 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.
- Complaint 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