# WAZUH - THE OPEN-SOURCE SECURITY PLATFORM

**NIKHIL R**

**202202278**

**SYMBIOSIS CENTRE FOR DISTANCE LEARNING (SCDL)**

**ACADEMIC YEAR 2025-2026**

# DECLARATION BY THE LEARNER

This is to declare that I have carried out this project work myself in part fulfilment of the Post Graduate Diploma in Information Technology Program of SCDL. The work is original, has not been copied from anywhere else and has not been submitted to any other University/Institute for an award of any degree/diploma.

Name: NIKHIL R

Signature:

Place: Muvattupuzha

Date: 10th July 2025

# INDEX

# CHAPTER 1 – INTRODUCTION

## OBJECTIVE

In today's rapidly evolving digital landscape, cybersecurity has become a critical area of focus for organizations of all sizes. As threats grow in sophistication, the demand for robust, open-source security solutions has increased significantly. Wazuh stands out as a comprehensive, free, and open-source security monitoring platform designed to provide threat detection, integrity monitoring, incident response, and compliance capabilities. It is widely used by security professionals and organizations to build scalable and efficient Security Information and Event Management (SIEM) environments.

This project serves as a hands-on initiative to gain a foundational understanding of Wazuh by deploying it in a controlled virtual environment. The goal is to simulate real-world use cases and security challenges, enabling a practical understanding of how Wazuh collects, processes, analyses, and visualizes security data.

The project aims at detailed study of Wazuh's core components—Wazuh Agent, Wazuh Manager, Wazuh Indexer, and Wazuh Dashboard—each of which plays a critical role in the end-to-end functioning of the platform. Through the process of installation, configuration, and testing, the project provides experiential learning in managing security events, monitoring endpoints, and interpreting alerts using Wazuh's powerful dashboard.

Furthermore, the creation of a home lab setup allows for a safe and flexible environment where experimental configurations and troubleshooting can be performed freely. This trial-and-error approach reinforces learning by encouraging exploration and problem-solving without the risk of impacting live systems.

By the end of the project, the user will have developed a solid working knowledge of Wazuh's architecture, its practical applications in security operations, and a strong foundation to build on for more advanced cybersecurity practices in the future.

## SCOPE AND BACKGROUND

The aim of this project is to explore and understand the Wazuh security platform in a controlled, self-hosted virtual environment. Wazuh is a powerful open-source solution for threat detection, integrity monitoring, incident response, and compliance. Given the complexity and range of features Wazuh offers, this project focuses on key foundational aspects, limiting the scope to essential components and basic functionalities suitable for learning and experimentation in a home lab setup.

### Scope of the Project

This project is limited to the following areas:

- **Understanding Core Components:**
  A detailed study of the main components of Wazuh, including:
  - **Wazuh Manager:** Responsible for processing collected data, triggering alerts, and enforcing rules.
  - **Wazuh Agent:** Installed on monitored endpoints to collect log data and send it to the manager.
  - **Wazuh Indexer:** Used to store and search security data.
  - **Wazuh Dashboard:** A user-friendly web interface for visualizing and analyzing security data.
- **Installation and Configuration in a Virtual Lab:**
  The project involves setting up Wazuh in a home lab environment using Oracle VirtualBox. It includes step-by-step installation, configuration, and validation of each component in a virtual network to simulate real-world conditions.
- **Log Monitoring and Threat Detection:**
  Using the Wazuh Dashboard to monitor logs from endpoints, analyze events, and detect suspicious activity. This helps develop a practical understanding of how Wazuh identifies and reports threats in real time.
- **Basic Endpoint Integration:**
  Installing and configuring Wazuh agents on virtual machines, such as Kali Linux, to simulate

monitored endpoints. The project covers basic agent-manager communication and event generation from these endpoints.

**Out of Scope**

While the project covers essential functionalities, it intentionally excludes advanced or enterprise-level features that require more complex infrastructure and extended time. These include:

- **Advanced Rule Tuning and Custom Decoders:**
  The project does not delve into creating custom detection rules, decoders, or configuring advanced log parsing.
- **Large-Scale or Production Deployment:**
  Implementation in a high-availability or enterprise environment, including clustering and scaling, is not considered.
- **Third-Party SIEM Integrations:**
  Integration with other SIEM tools (such as Splunk or Elastic Stack beyond Wazuh's native components) is not covered.

**USER REQUIREMENT**

| Component | Minimum Requirement | Suggested Requirement |
|---|---|---|
| **CPU** | Dual-core (Intel i5 4th gen / Ryzen 3) | Quad-core or higher (Intel i7 / Ryzen 5+) |
| **RAM** | 8 GB | 16 GB |
| **Storage** | 256 GB SSD | 512 GB+ SSD |
| **OS** | Windows 10/Linux (Kali VM or dual boot) | Windows 10/Linux (Kali VM or dual boot) |
| **Graphics** | Integrated graphics | Integrated or basic GPU |
| **Networking** | Wi-Fi support | Wi-Fi + Ethernet |

# CHAPTER 2 - ANALYSIS OF WORK DONE AND DESIGN

## TOOLS USED

- MS Windows 11 Home Single
- Oracle Virtual Box Version 7.1.6
- Kali Linux 2025
- Wazuh Central Components
- Wazuh Universal agent

## Test Procedures and Implementation

Wazuh is a security platform that provides unified XDR and SIEM protection for endpoints and cloud workloads. The solution is composed of a single universal agent and three central components: the Wazuh server, the Wazuh indexer, and the Wazuh dashboard. Wazuh is free and open source. Its components abide by the GNU General Public License, version 2, and the Apache License, Version 2.0 (ALv2).

As per official Wazuh website (https://wazuh.com/), for a setup of 1 to 25 agents, 4 vCPU, 8 GB RAM and 50 GB storage is recommended. The Wazuh central components require a 64-bit Intel, AMD, or ARM Linux processor (x86_64/AMD64 or AARCH64/ARM64 architecture) to run.

The Wazuh indexer and Wazuh server can be installed on a single host or be distributed in cluster configurations. User can choose between installation methods for each Wazuh central component. Both options provide instructions to install the central components on a single host or on separate hosts. For more deployment flexibility and customization, install the Wazuh central components by starting with the Wazuh indexer deployment. This deployment method allows the all-in-one installation, and the installation of the components on separate servers. Wazuh provides other installation alternatives. This includes Ready to use machines using virtual machine (OVA) or Amazon Machine Image (AMI), Containers such as Docker and Kubernetes, offline installation by downloading Wazuh components or from source, by compiling source code and copy binaries to user's computer. For the scope of this project, we are using Ready to use machine using virtual machine (OVA). This project shows step by step installation of components starting from Oracle Virtual Box.

Downloaded and installed Oracle Virtual box for Windows Hosts. VirtualBox. 2025. "Downloads." Accessed July 10, 2025. https://www.virtualbox.org/wiki/Downloads

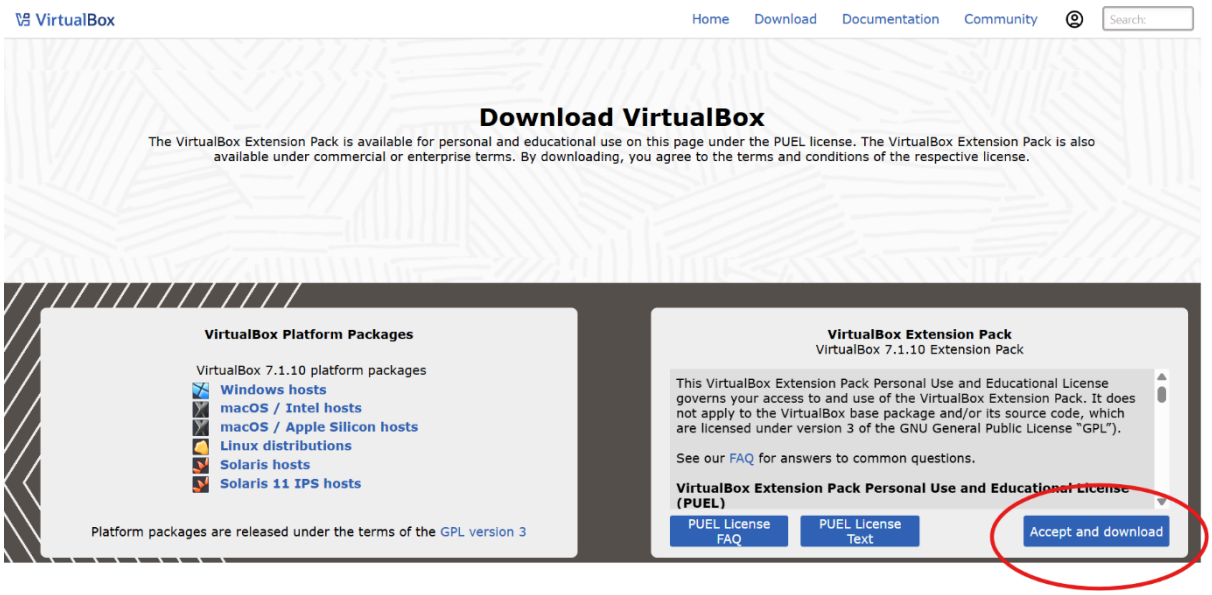



*Figure 1*

Downloaded and added Kali Linux prebuilt Virtual machine for Oracle virtual box. Kali Linux. 2025. "Get Kali – Kali Virtual Machines." Accessed July 10, 2025. https://www.kali.org/get-kali/#kali-virtual-machines .

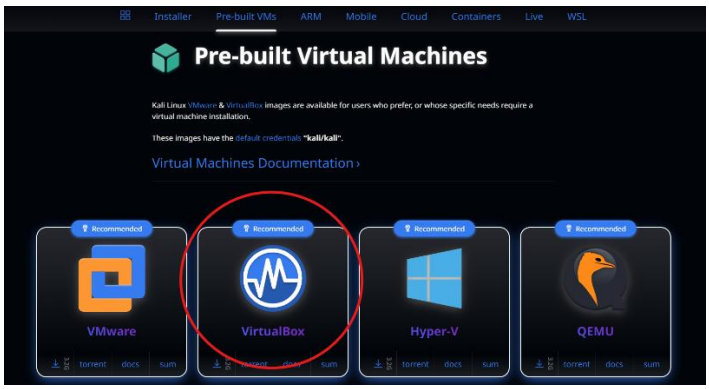



*Figure 2*

Ran Kali Linux in Oracle Virtual Box.


*Figure 3*


*Figure 4*

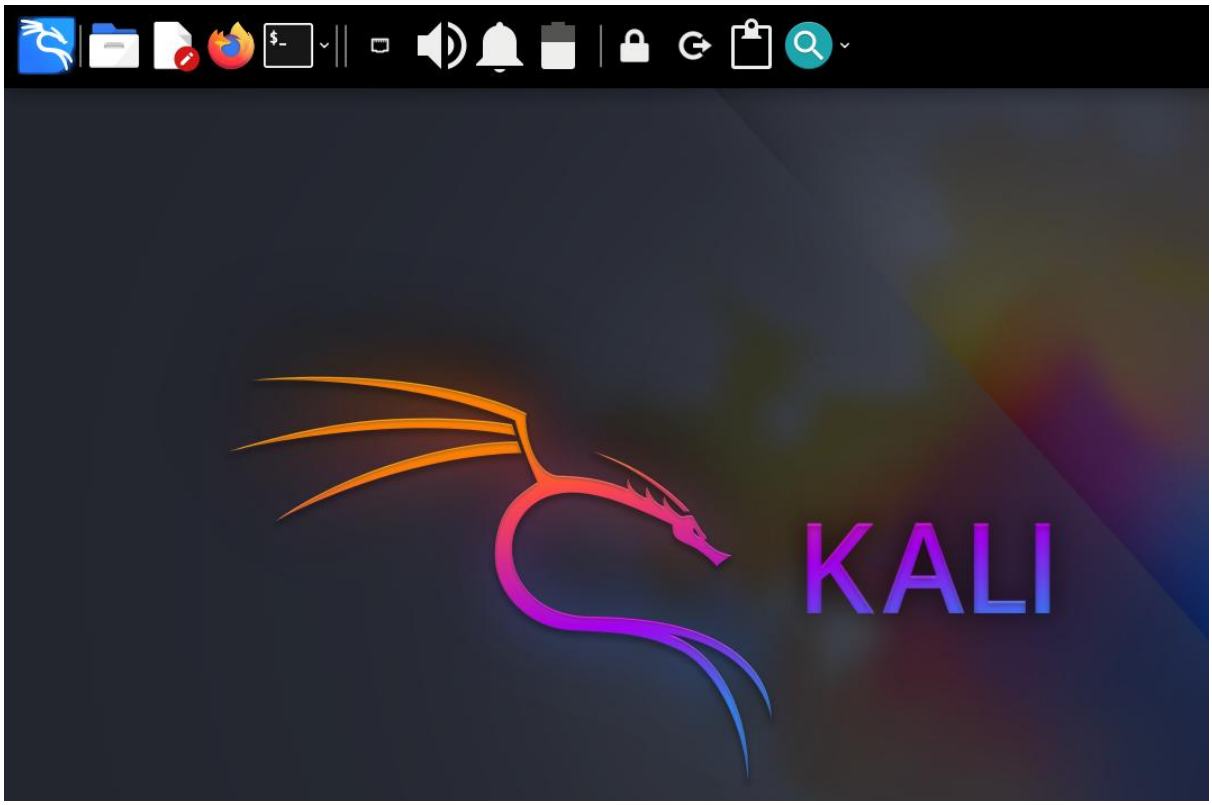



*Figure 5*

Visited https://wazuh.com/ for downloading Wazuh central components (Wazuh. 2025. "Wazuh: The Open-Source Security Platform." Accessed July 10, 2025. https://wazuh.com/).

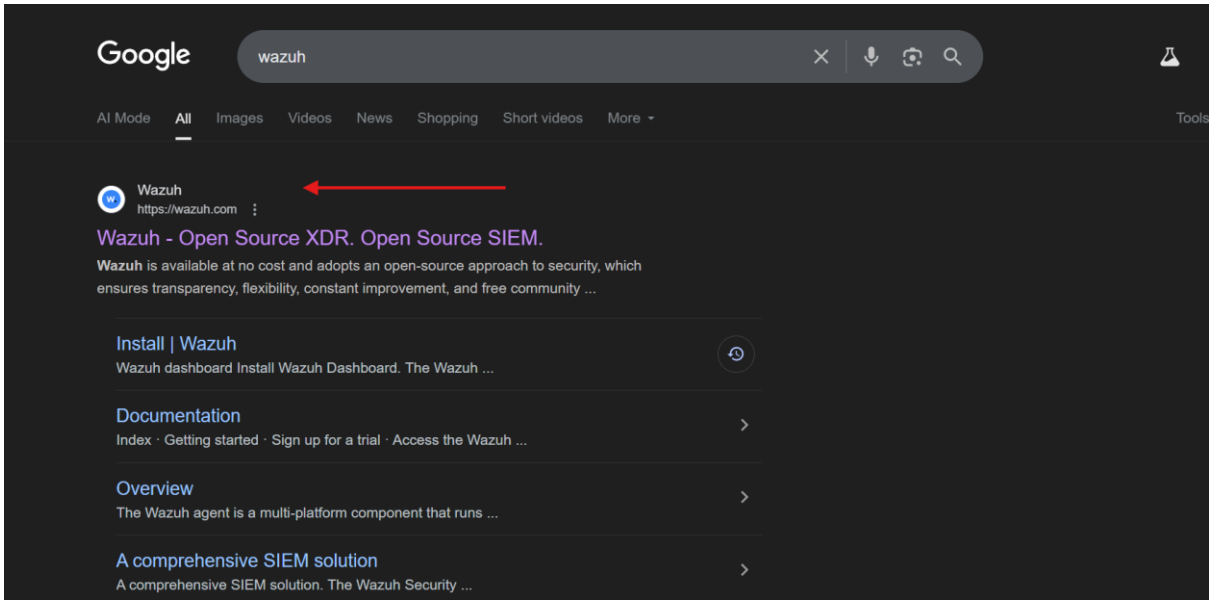



*Figure 6*

This was the home page of Wazuh.

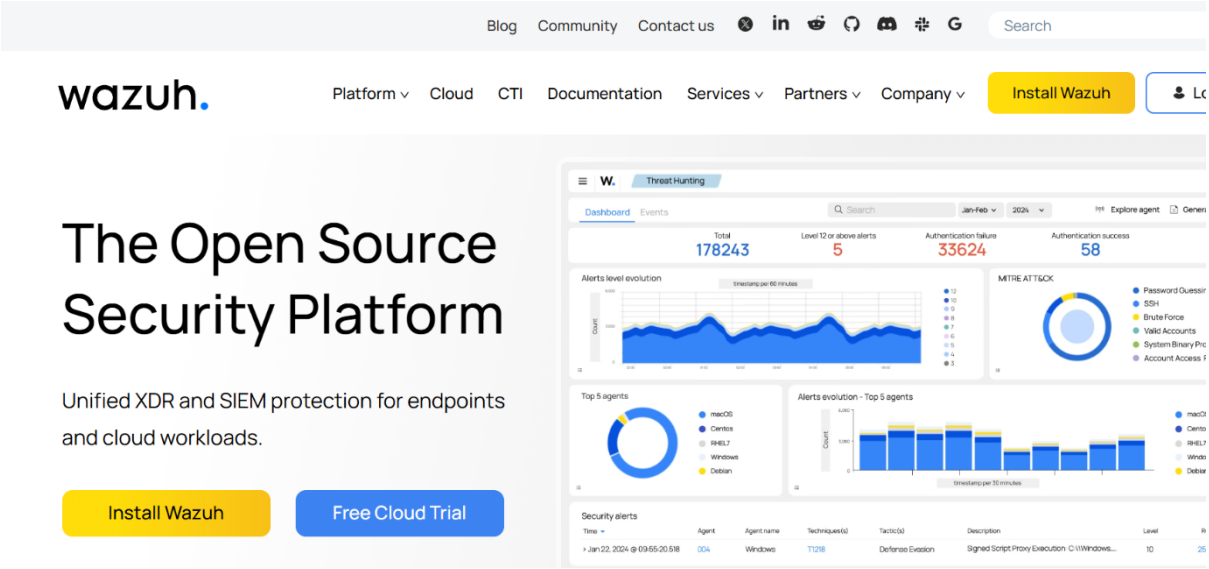



*Figure 7*

Visited documentation section for detailed guide.

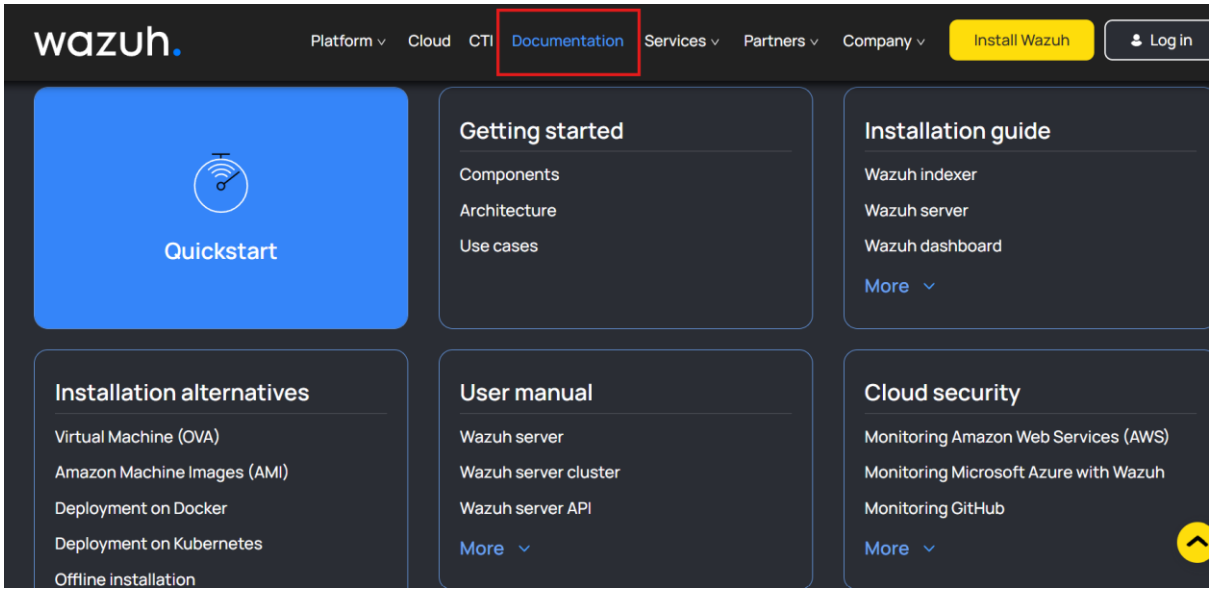



*Figure 8*

For the scope of this project, ready to use machine are used, which can be added and ran using Oracle Virtual Box.

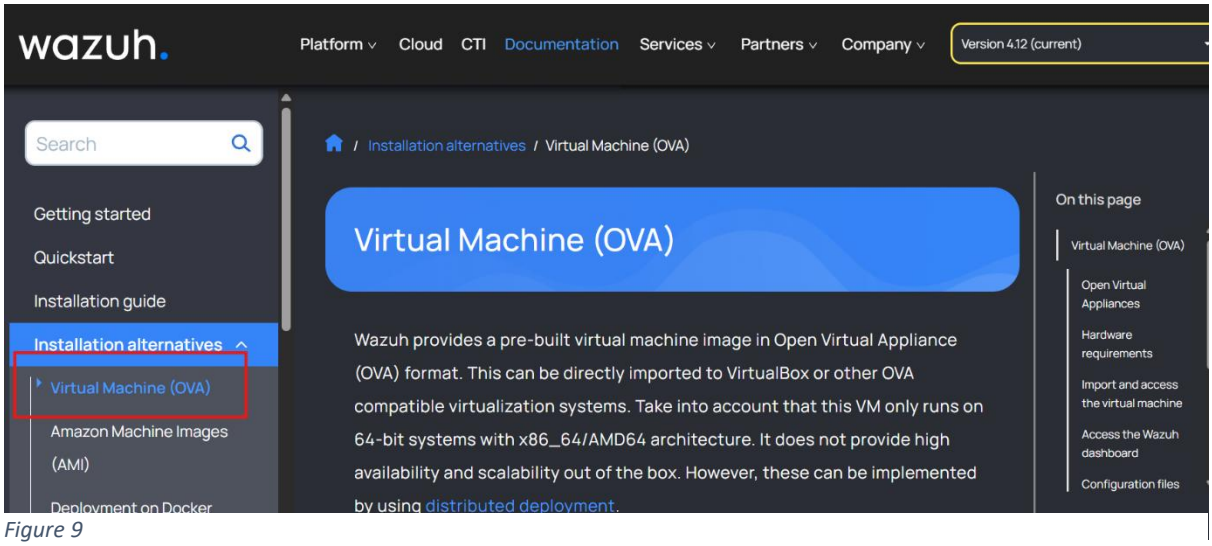



*Figure 9*

The .OVA file was downloaded from link - https://packages.wazuh.com/4.x/vm/wazuh-4.12.0.ova, as shown in the image (Wazuh. 2025. "Wazuh 4.12.0 OVA Virtual Machine." Accessed July 10, 2025. https://packages.wazuh.com/4.x/vm/wazuh-4.12.0.ova).

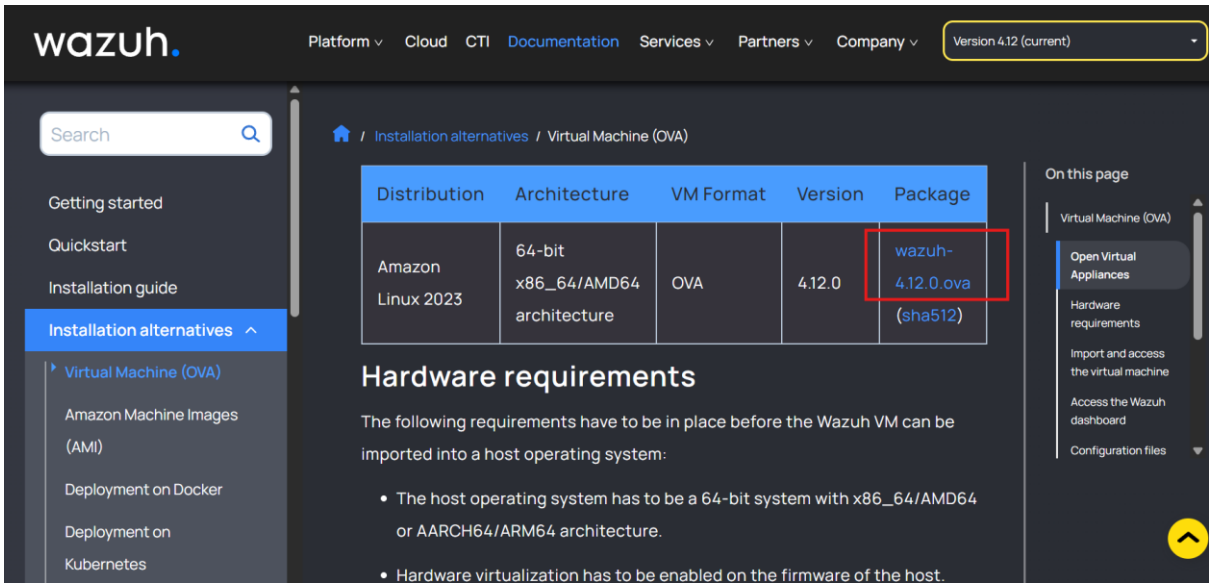



*Figure 10*

The file had an approximate size of 3.25 GB

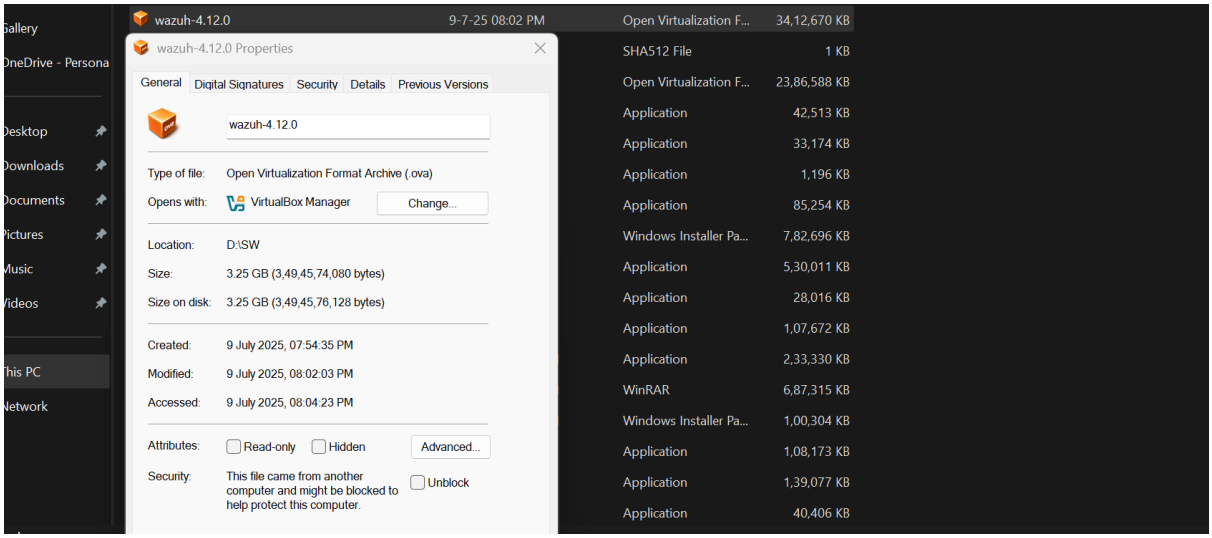



*Figure 11*

Opened Oracle Virtual box and imported .OVA file of Wazuh. The settings were tweaked to match system configuration.

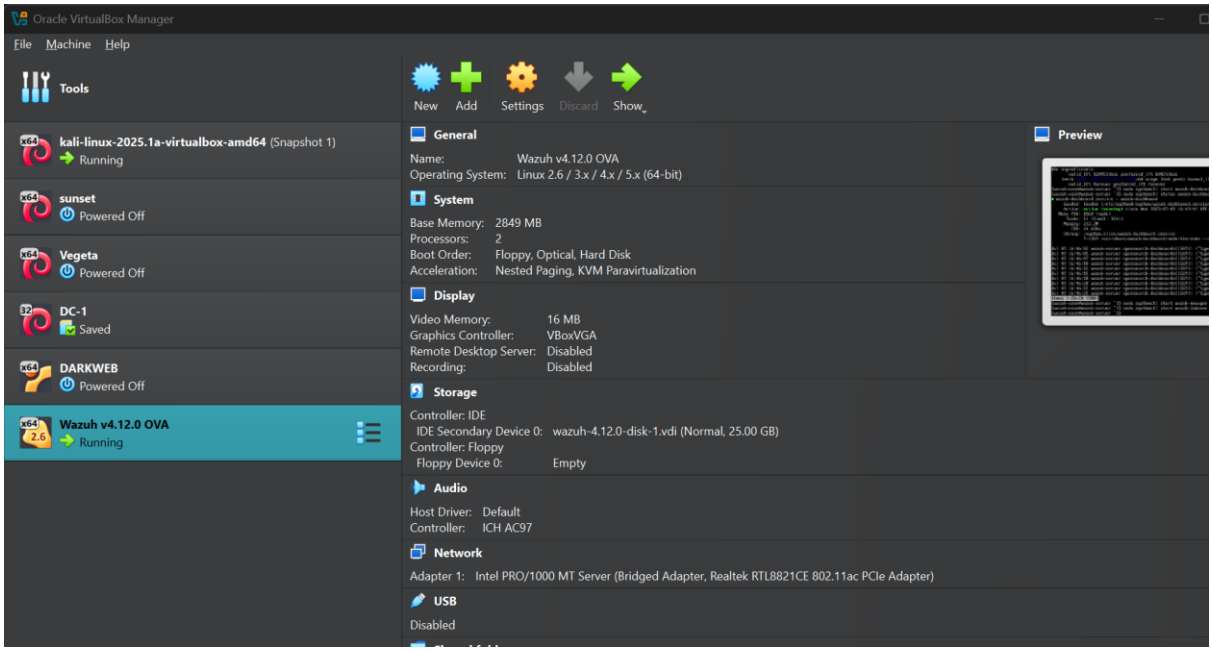



*Figure 12*

Ran the imported virtual machine.


*Figure 13*

Login credentials were provided in the website.

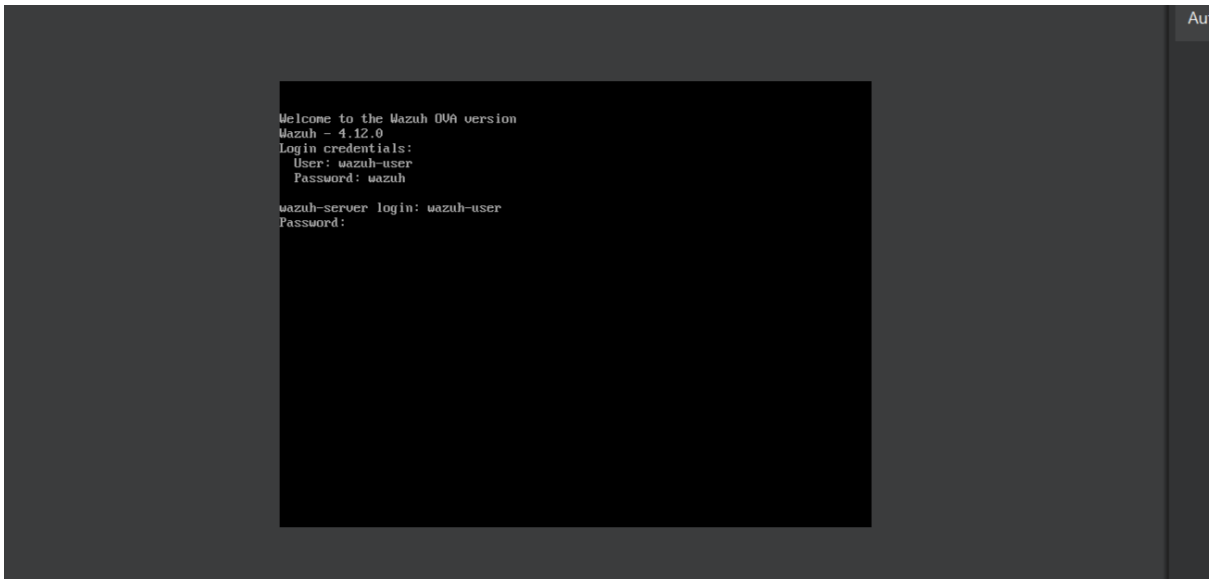



*Figure 14*

Once logged in, a command line interface came visible.


*Figure 15*

Following commands were used to start Wazuh dashboard, manager and indexer.

- sudo systemctl start wazuh-dashboard
- sudo systemctl start wazuh-manager
- sudo systemctl start wazuh-indexer

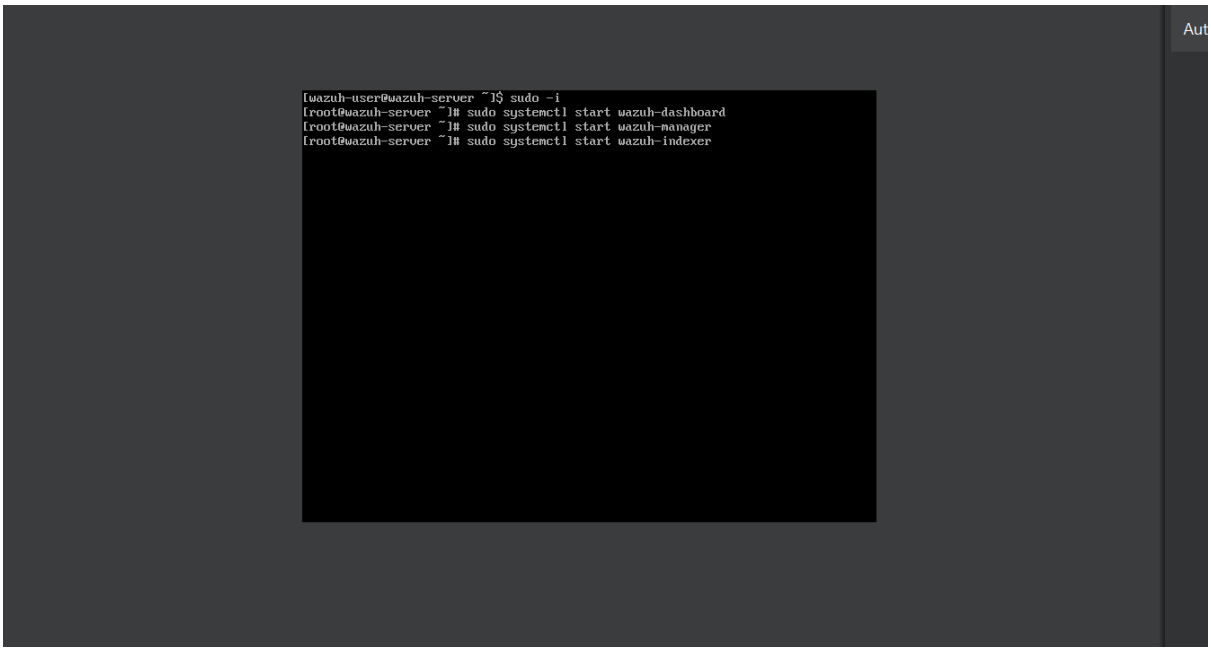



*Figure 16*

Accessed the IP address from CLI using command ‘ip a’.

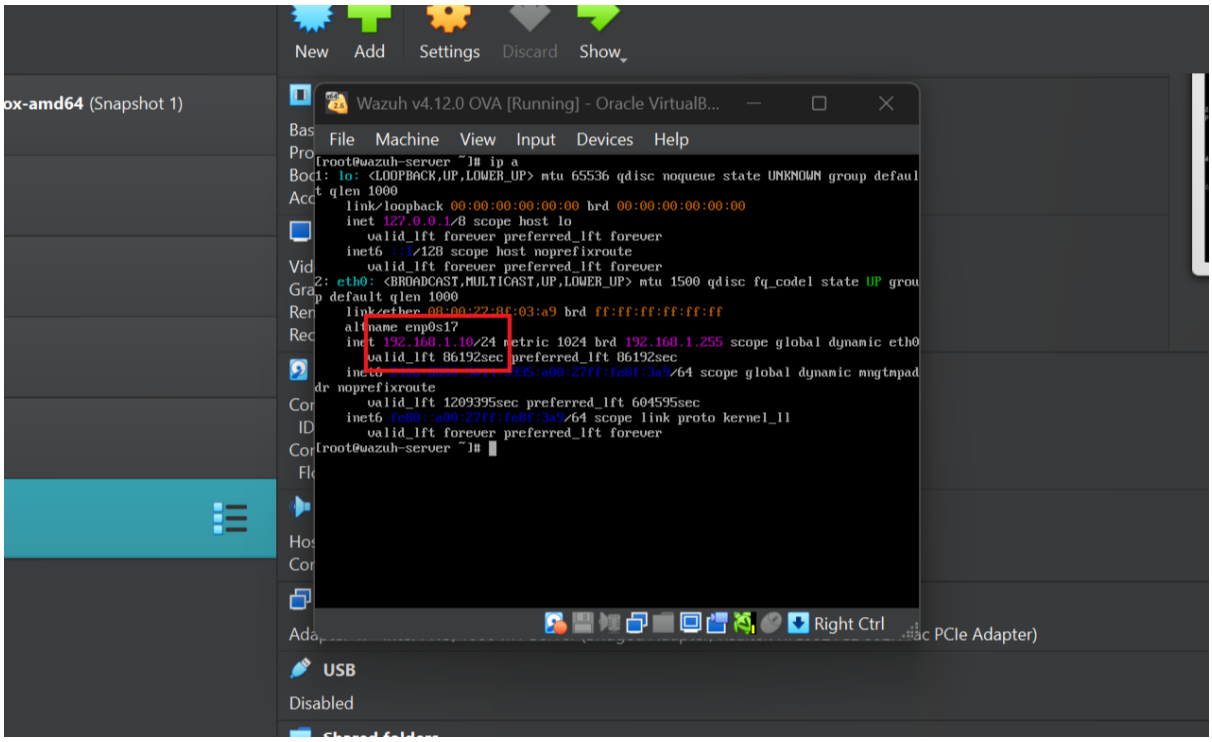



*Figure 17*

Used this IP address to access wazuh dashboard in user’s host OS. Here the IP of Wazuh machine was 192.168.1.10. Here the host OS was Windows 11 and Brave browser was used for accessing Wazuh dashboard.

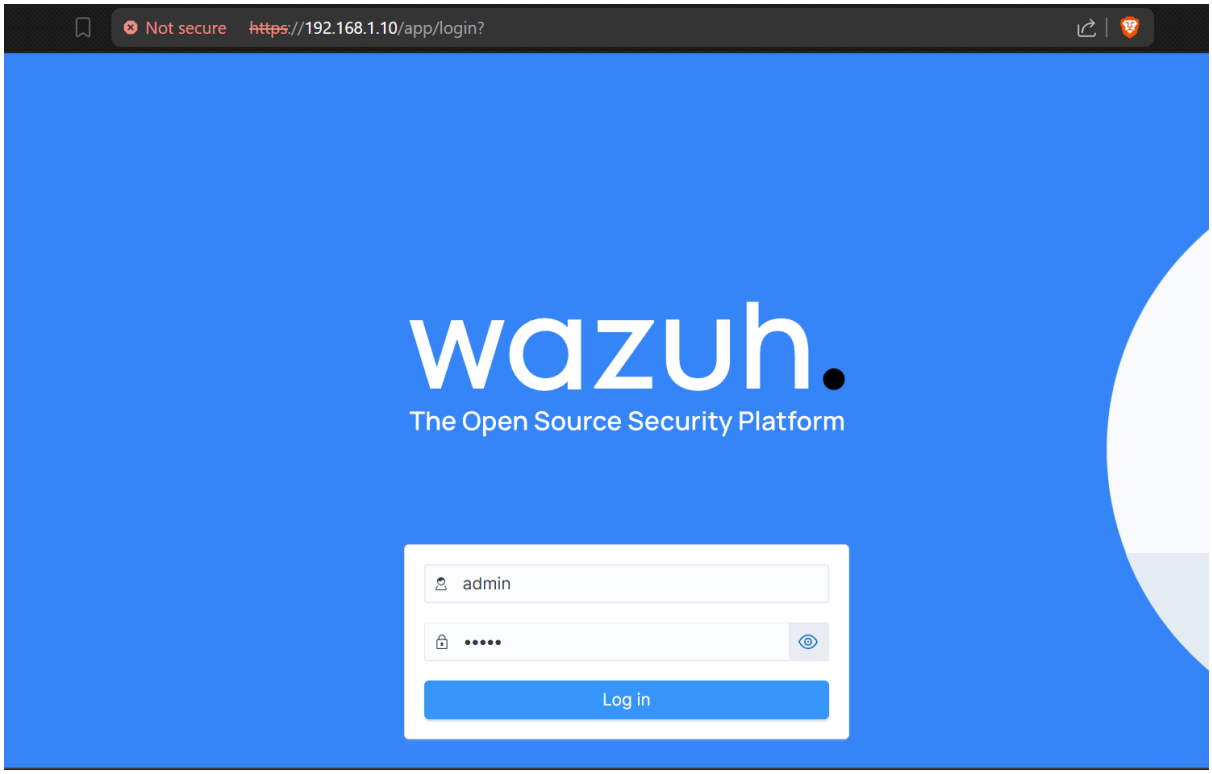



*Figure 18*

This was the dashboard of Wazuh. Agents were added from here.

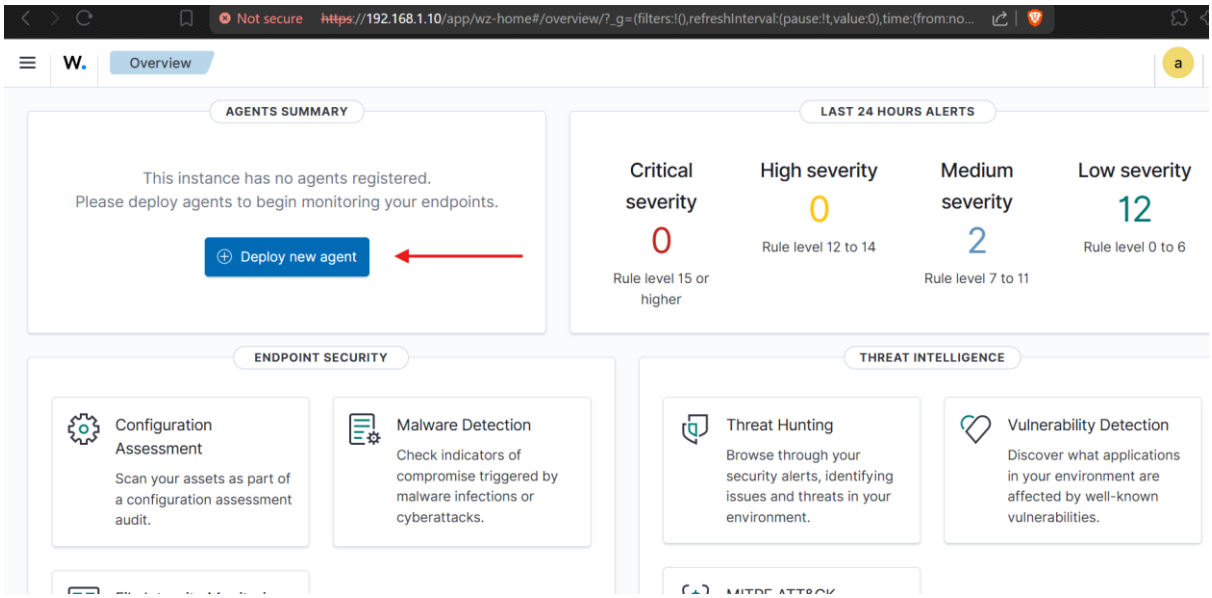
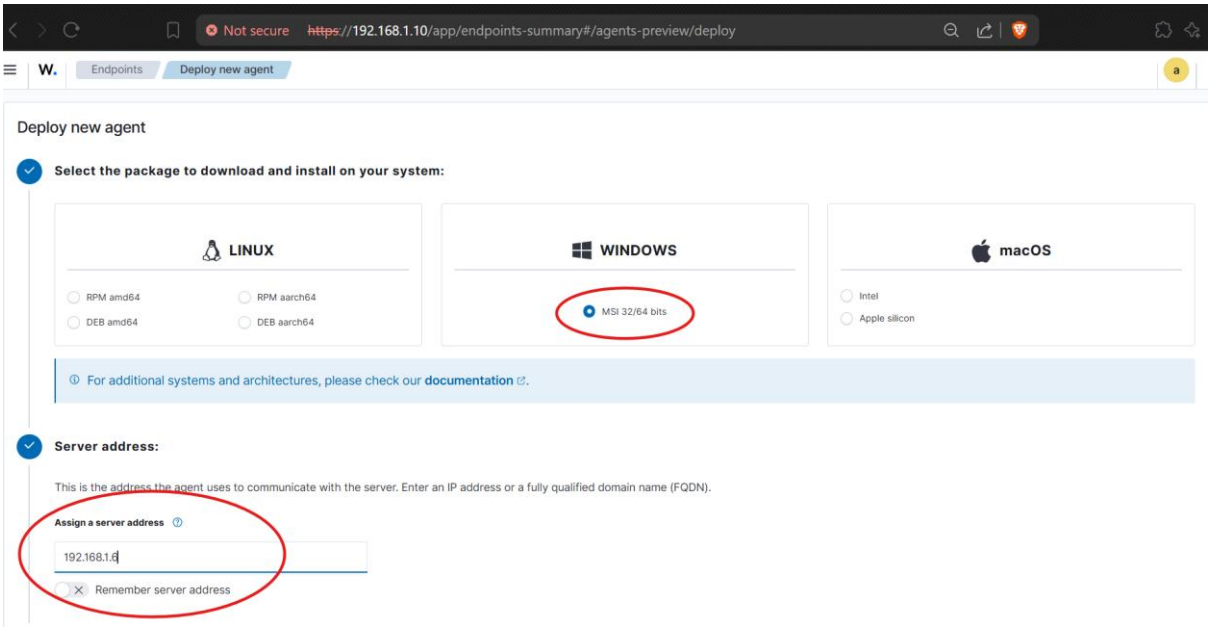



*Figure 19*

Selected deploy agent option. Selected which agent was to be deployed (OS), added address and name.

*Figure 20*



Wazuh provided a command that can be copied and executed in agent terminal with administrator privilage, which will download and install wazuh agent in system. Windows agent was added.

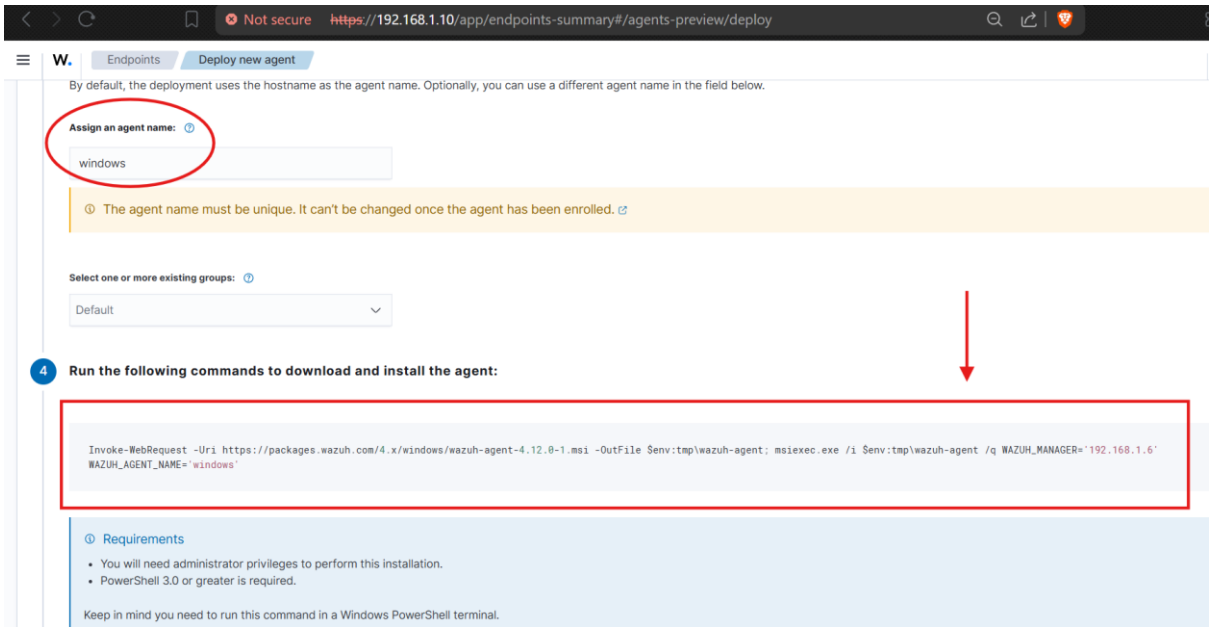



*Figure 21*

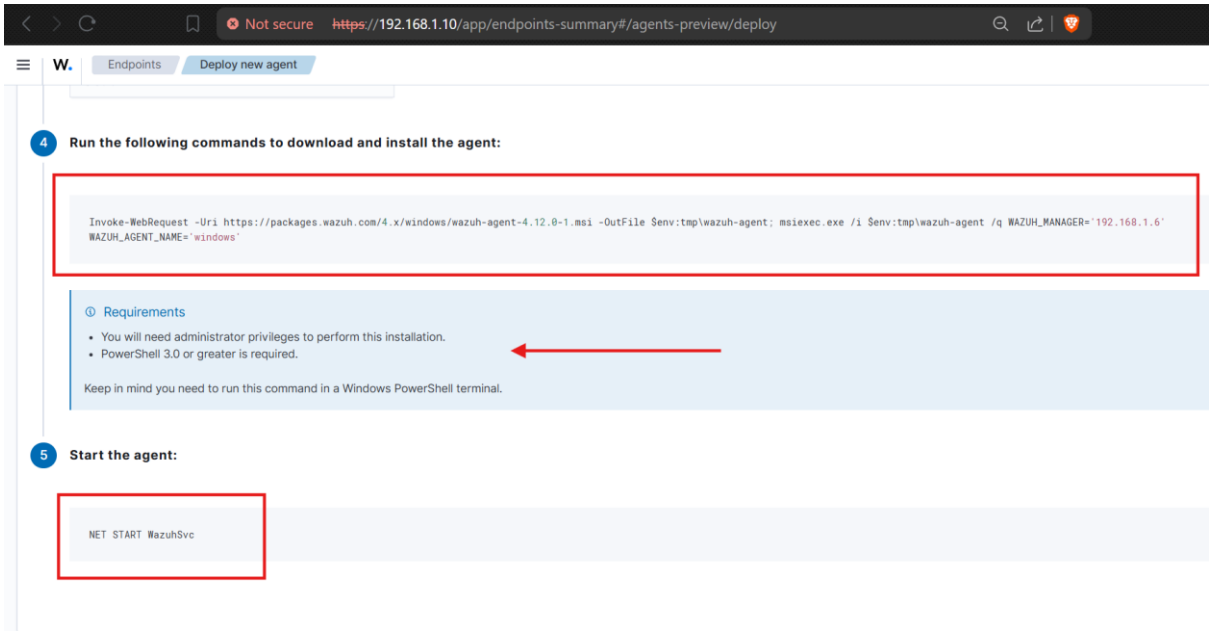



*Figure 22*

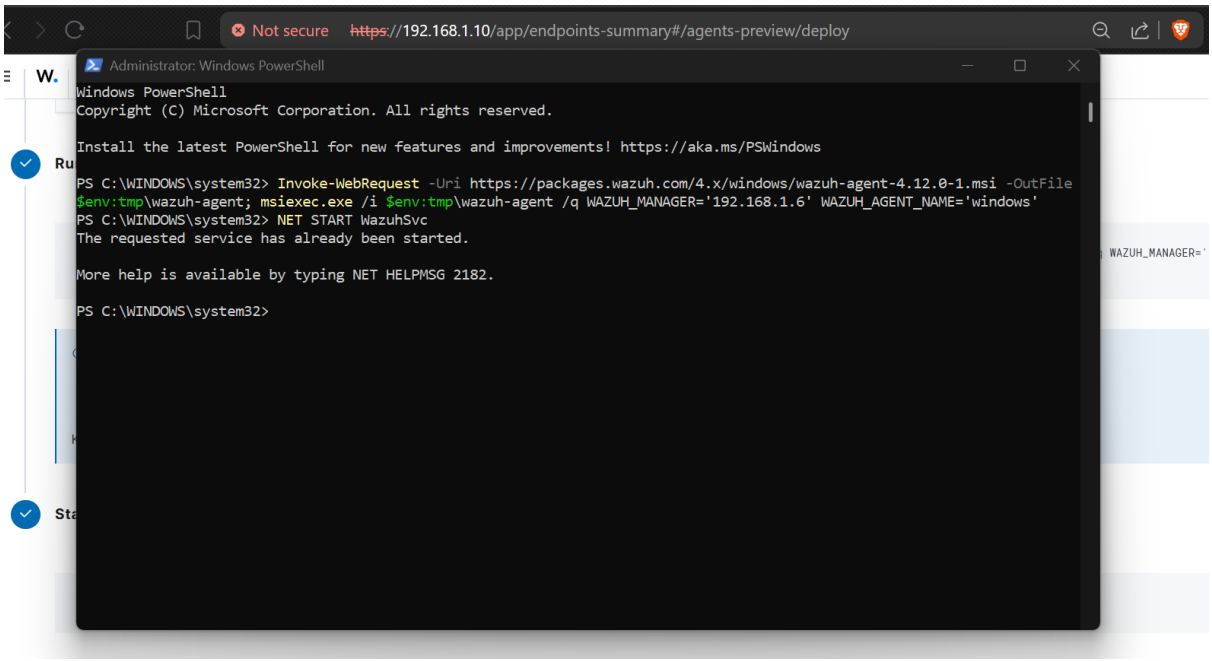



*Figure 23*

Repeated same steps to add linux agent.

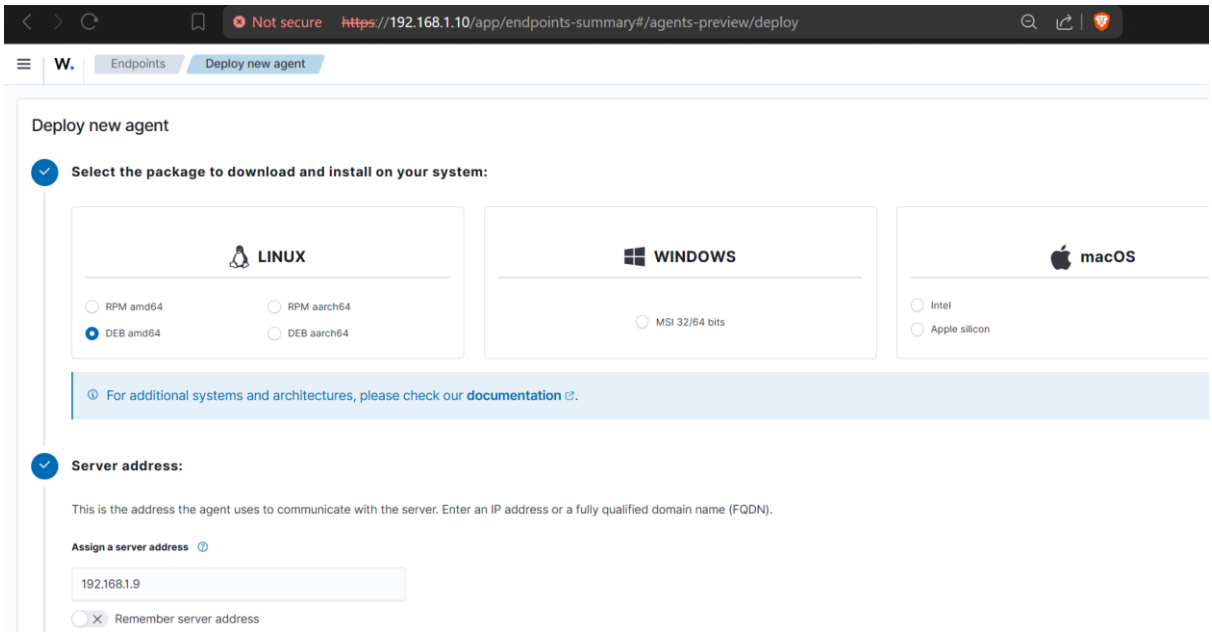



*Figure 24*

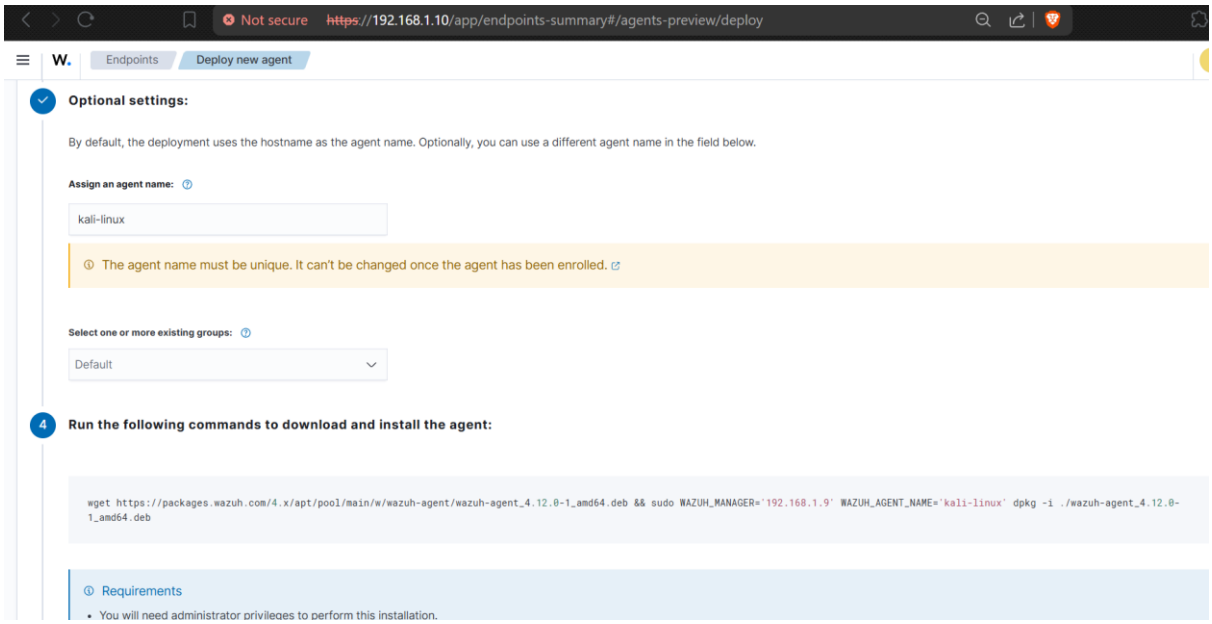



*Figure 25*

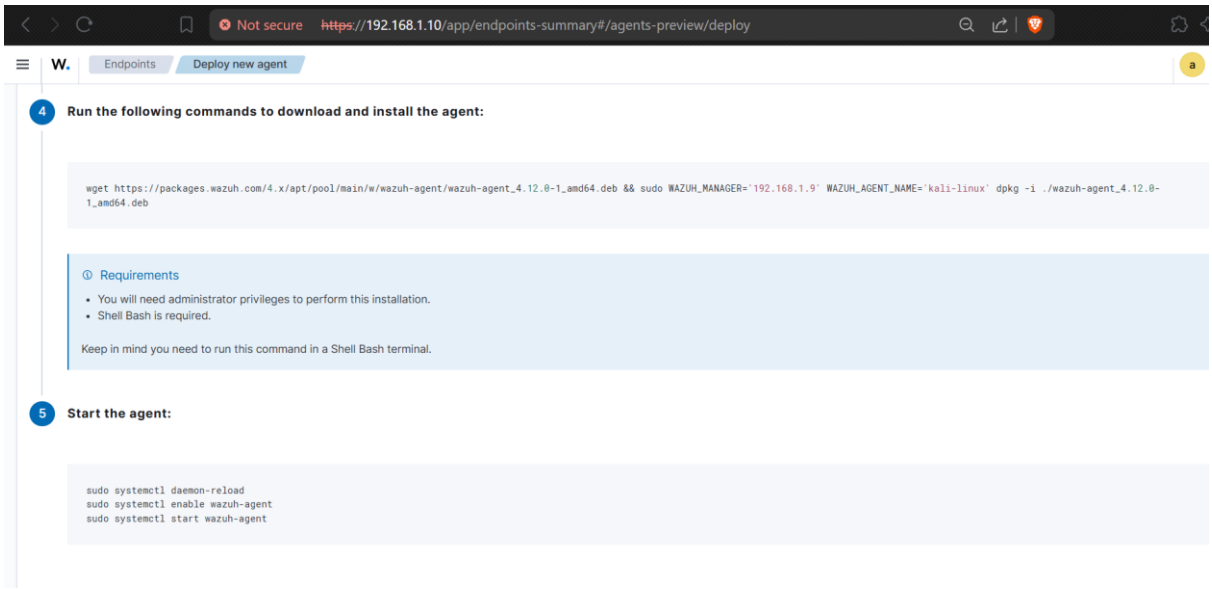



*Figure 26*

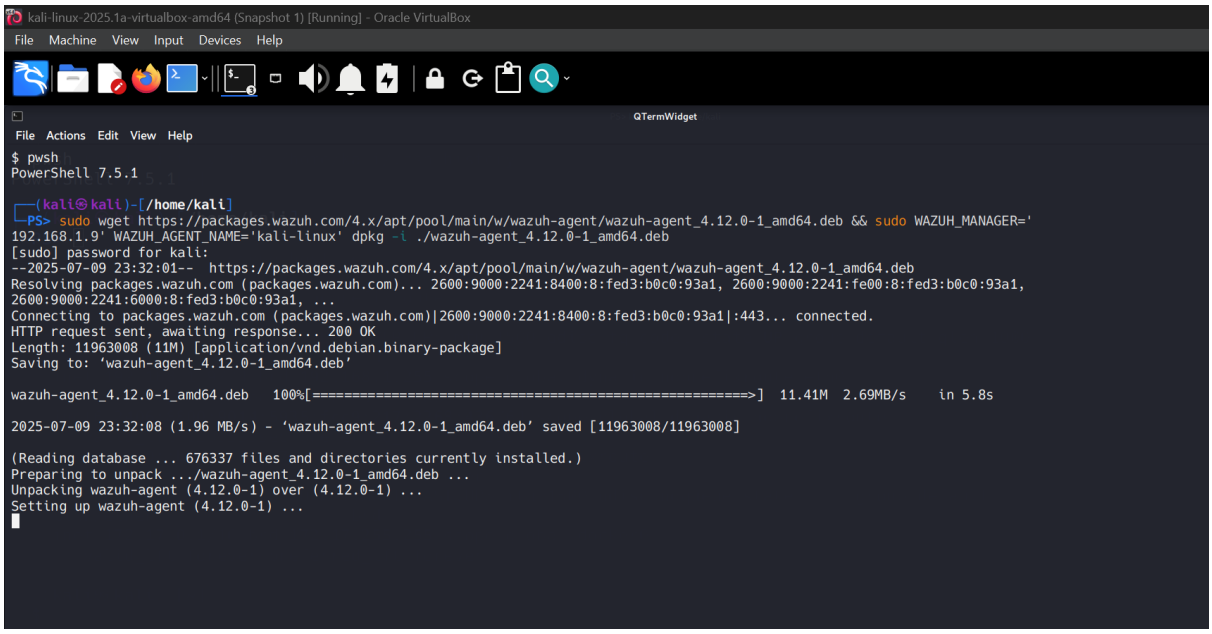



*Figure 27*

The agent summary screen showed 2 active agents.

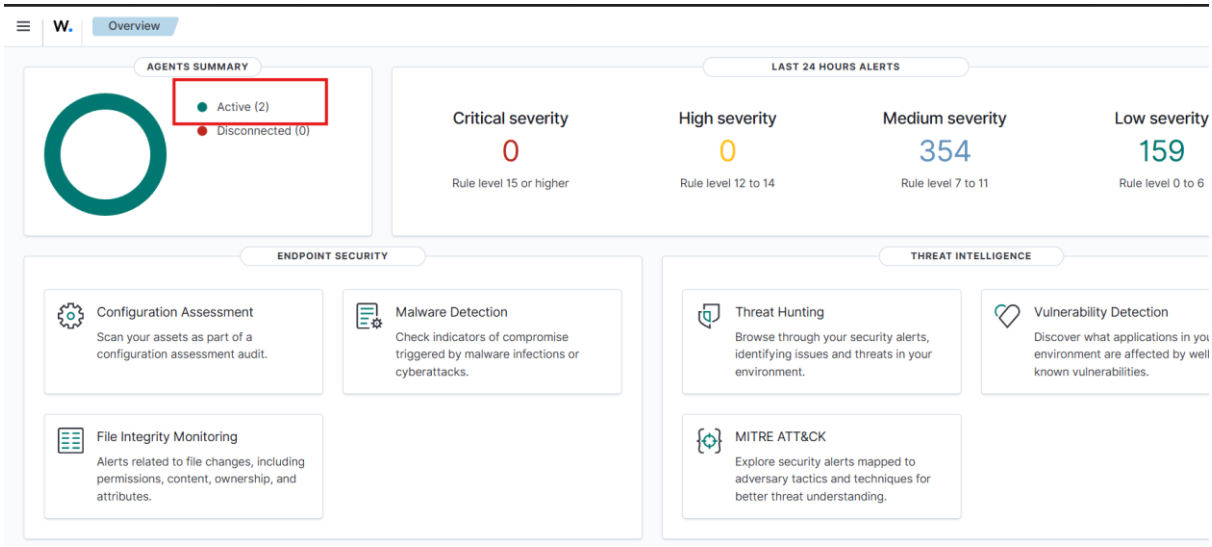



*Figure 28*

Two agents are showed in dashboard, Windows and Kali.

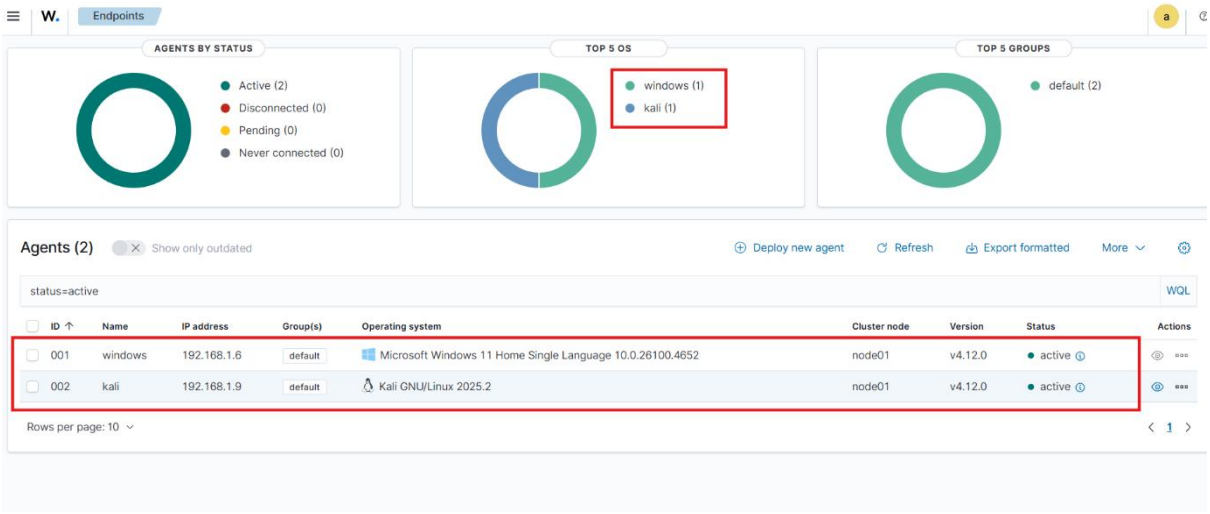



*Figure 29*

Selected Windows to see detailed dashboard of Windows endpoint.

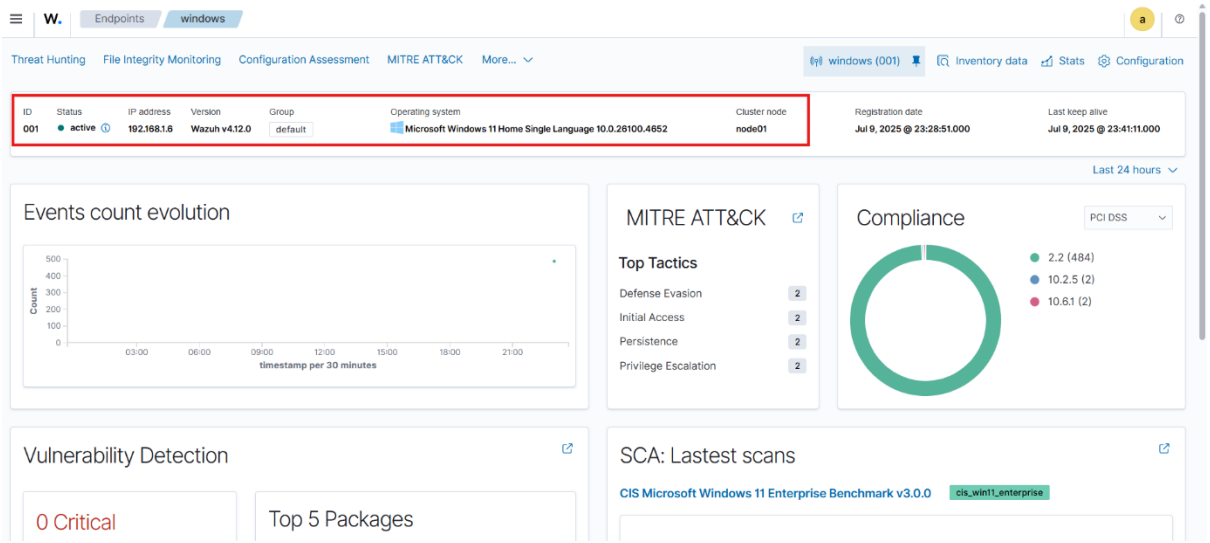



*Figure 30*

Under Threat hunting, events of the endpoints are listed.

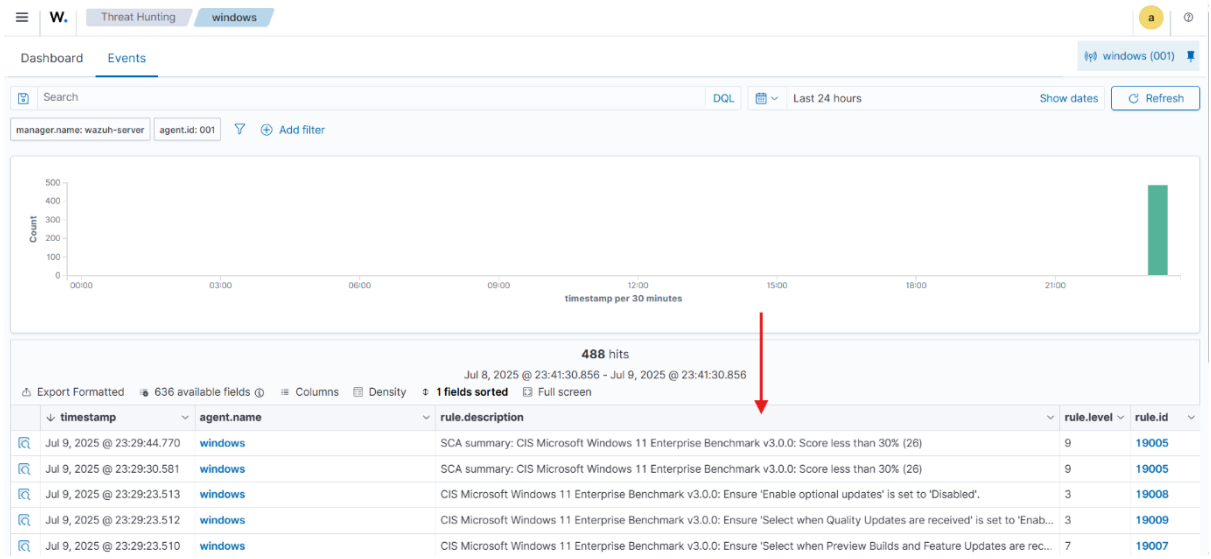



*Figure 31*

Events such as Logon failure, Logon Success etc are captured using pre built rules.

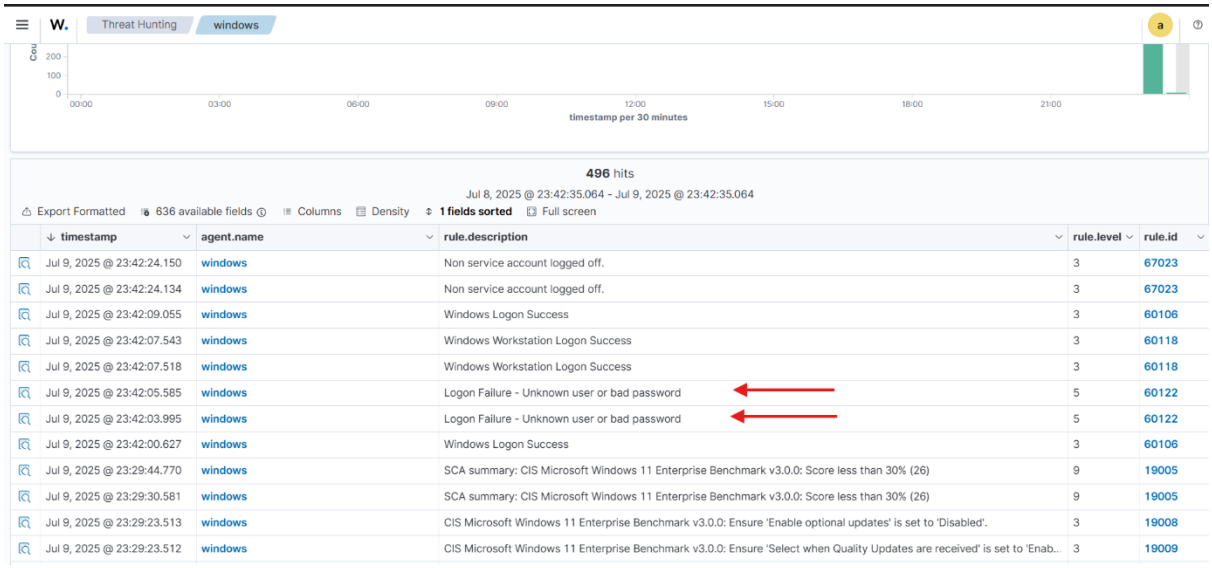



*Figure 32*

Windows Event ID 4625 was used in search bar to filter Logon Failure events during a specific period.

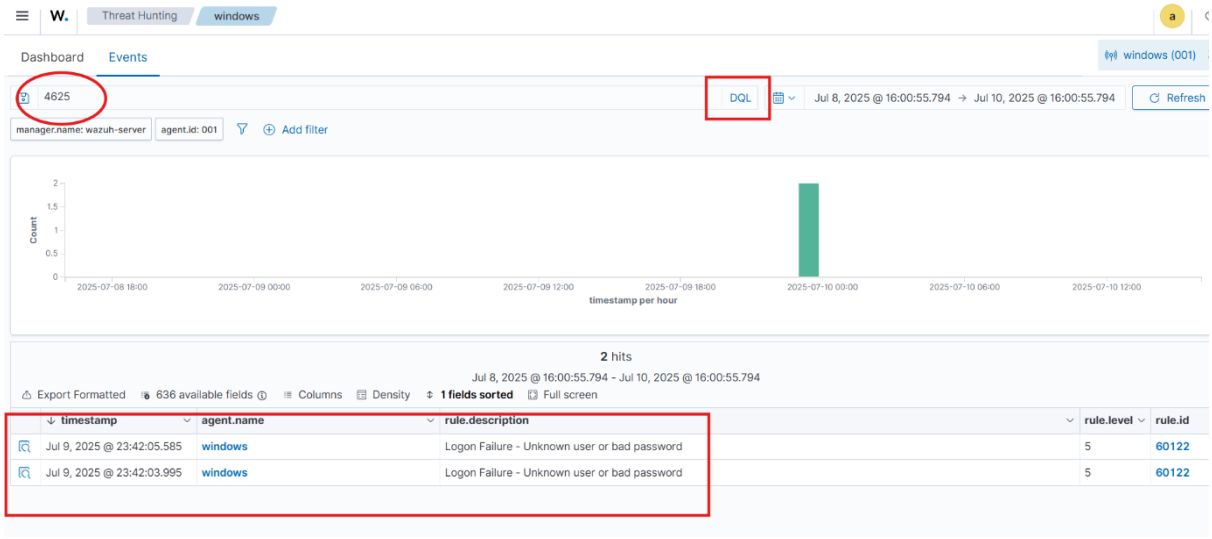



*Figure 33*

Each event expanded to see document details.

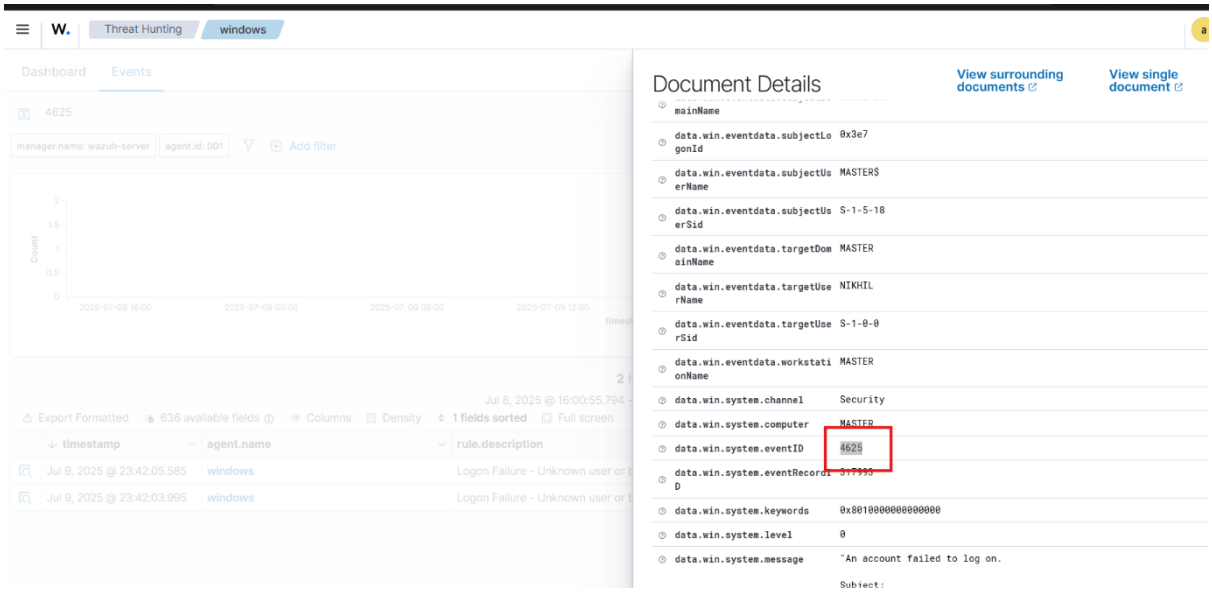



*Figure 34*

Wazuh also has Vulnerability detection capabilities. It showed top 5 vulnerabilities along with CVE number and count.

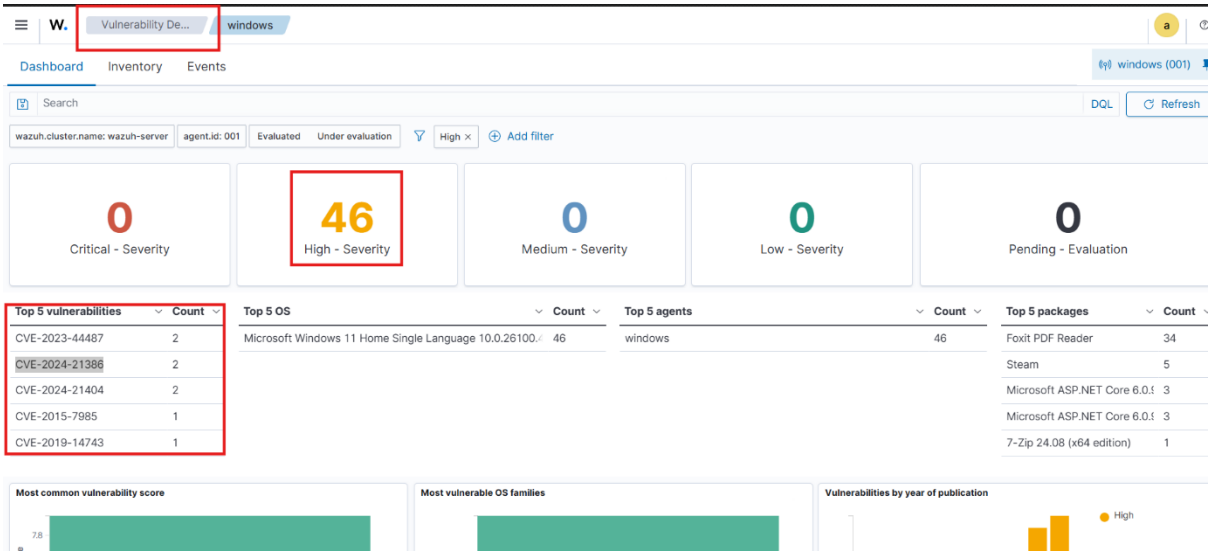



*Figure 35*

Wazuh also included a compliance monitoring platform for endpoints.

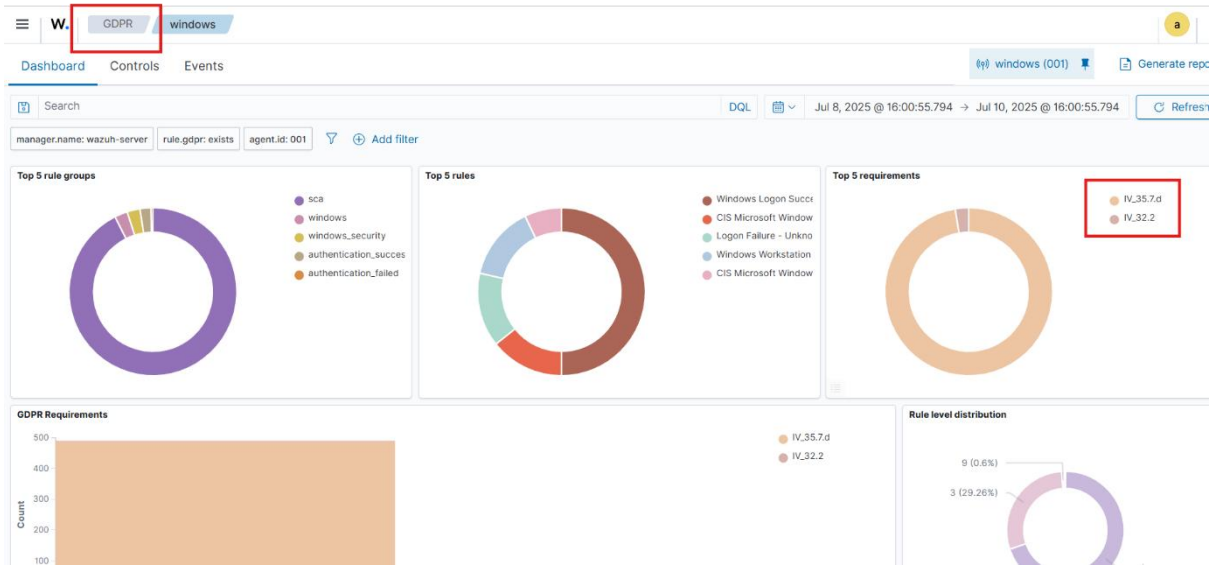



*Figure 36*

Reports related to a specific compliance such as GDPR was generated by Wazuh.

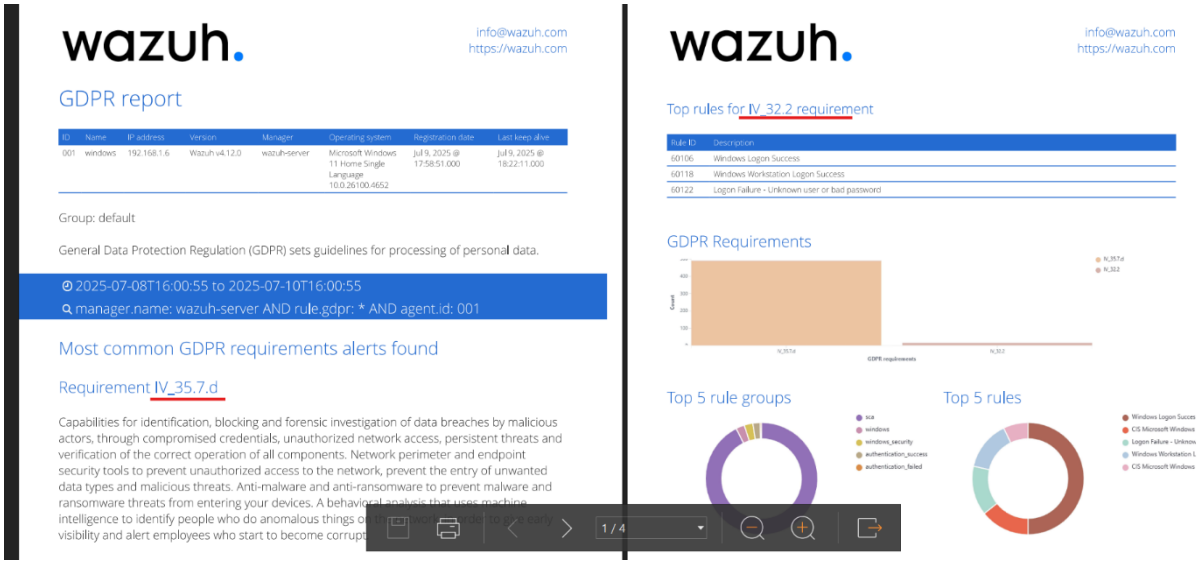



*Figure 37*

# CHAPTER 3 - LEARNING EXPERIENCES

## Application of Knowledge in the Project

This project was designed as a practical learning journey to understand the working of Wazuh, an open-source security platform used for endpoint monitoring, log analysis, threat detection, and compliance enforcement. By building and experimenting with a personal home lab, User was able to simulate real-world scenarios, test configurations, and reinforce theoretical knowledge with hands-on experience.

To facilitate this, user set up a virtualized home lab using VirtualBox, where the official Wazuh all-in-one OVA was deployed on an Ubuntu server. The lab environment included integration with a Windows host system as an endpoint with the Wazuh agent installed. This setup allowed user to freely experiment, troubleshoot issues, and repeat configurations in a risk-free environment. It also helped user to gain familiarity with the installation process, basic networking, firewall settings, remote management, and the practical application of security monitoring tools in a controlled setting.

During this project, theoretical knowledge about SIEM systems, endpoint monitoring, and log analysis was applied in a practical scenario by deploying and configuring Wazuh. The objective was to build a home lab environment where user could safely experiment, perform trial and error, and gain hands-on experience with real-world cybersecurity tools.

To implement Wazuh effectively, it was essential to understand the function and interaction of its main components: the Wazuh Agent, Wazuh Server, Wazuh Indexer, and Wazuh Dashboard. These components collectively support the collection, analysis, storage, and visualization of security data.

The main components of Wazuh Central components and Wazuh agent are depicted in the image.

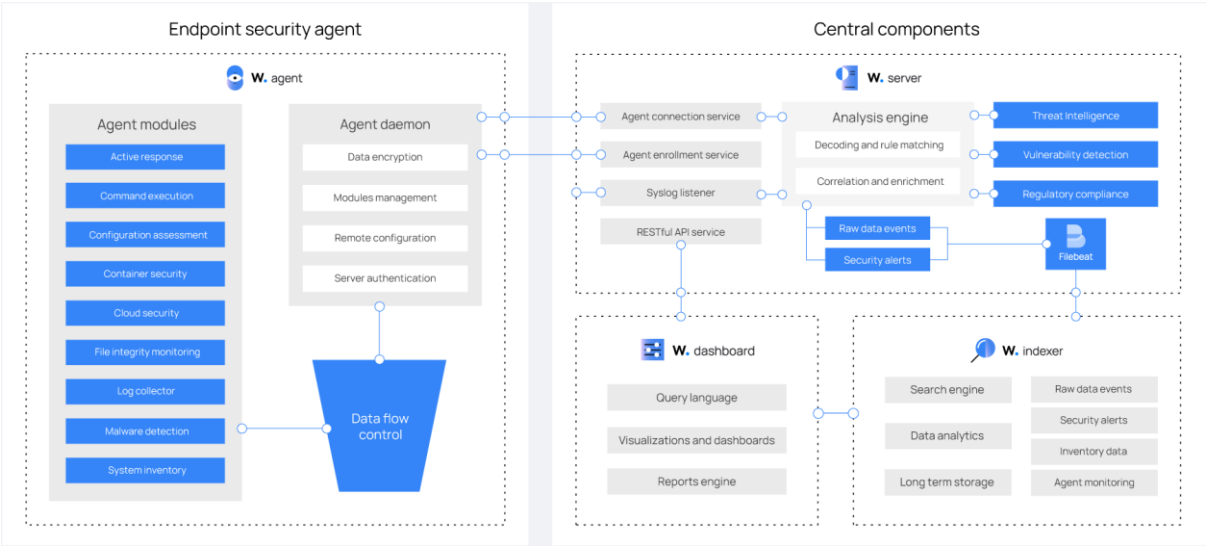



*Figure 38*

**Wazuh Agent** was Installed on endpoint systems (such as Windows/Linux machines or containers), the Wazuh Agent acts as the data collector. Through its various modules, it performs:

- File Integrity Monitoring (FIM): Tracks changes to critical files and directories.
- Log Collection: Gathers system, application, and security logs.
- Malware Detection: Scans for malicious behavior or patterns.
- Cloud and Container Security: Monitors Docker containers or cloud workloads.

The agent runs a daemon that manages module operations and securely transmits data to the server after authentication and encryption. User learned how to configure the agent manually and remotely, and how to troubleshoot connectivity and log forwarding issues.

**Wazuh Server** was the core processing unit in the architecture. In lab:

- It handled incoming connections from agents, managed agent registration, and accepted syslog input.
- It decoded, correlated, and enriched security data using rules and threat intelligence feeds.

- It provided mechanisms for real-time alerting, vulnerability assessment, and compliance reporting (e.g., PCI-DSS, GDPR).

Through server-side configuration files and rulesets, user learned to tune alerts, reduce noise, and focus on relevant security events. This hands-on experience helped solidify concepts like log normalization, correlation, and rule tuning.

**Wazuh Indexer** stored all incoming security data. It enables:

- Real-time search and filtering of events and alerts.
- Historical data storage for forensic analysis and compliance auditing.
- Efficient indexing of event logs, FIM data, alerts, and inventory.

Learning to query the indexer using Wazuh's custom language helped user understand how structured data was stored and accessed. User also configured index rotation to manage storage effectively.

**Wazuh Dashboard** served as the graphical interface for analysts and administrators. It enabled user to:

- Visualize alerts and events using dashboards and charts.
- Run custom searches and filter logs for incident investigation.
- Generate automated reports for auditing and compliance.

By navigating and customizing the dashboard, User gained confidence in identifying threat trends, viewing agent status, and correlating alerts with system actives.

# CHAPTER 4 – CONCLUSION

Through this project, a foundational understanding of Wazuh as an open-source security monitoring platform was achieved. The study covered the installation process, core components (Agent, Server, Indexer, and Dashboard), and their interconnections. It also explored how Wazuh collects, analyzes, and visualizes security data for effective threat detection and response.

## Findings

Wazuh is a powerful and flexible open-source solution that provides enterprise-grade security monitoring capabilities. It supports multiple features such as file integrity monitoring, vulnerability detection, malware detection, and compliance reporting. Its modular structure and scalability make it suitable for both small environments and large, distributed infrastructures.

## Recommendations

To enhance the capabilities of Wazuh, it is recommended to integrate it with other security and analytics platforms. For example, integrating Wazuh with third-party SIEM tools like Splunk or cloud platforms such as AWS and Azure can extend visibility and improve threat intelligence. Additionally, coupling Wazuh with ticketing systems (like Jira or ServiceNow) and SOAR tools can automate incident response and streamline workflows, making the overall security posture more proactive and efficient.

## CHAPTER 5 – BIBLIOGRAPHY


- [1] Wazuh, "Wazuh: The Open Source Security Platform." [Online]. Available: https://wazuh.com/. [Accessed: Jul. 10, 2025].
- [2] Wazuh, "Wazuh 4.12.0 OVA Virtual Machine." [Online]. Available: https://packages.wazuh.com/4.x/vm/wazuh-4.12.0.ova. [Accessed: Jul. 10, 2025].
- [3] VirtualBox, "Downloads." Oracle, 2025. [Online]. Available: https://www.virtualbox.org/wiki/Downloads. [Accessed: Jul. 10, 2025].
- [4] VirtualBox, "Oracle VM VirtualBox." [Online]. Available: https://www.virtualbox.org/. [Accessed: Jul. 10, 2025].
- [5] Kali Linux, "Get Kali – Kali Virtual Machines." [Online]. Available: https://www.kali.org/get-kali/#kali-virtual-machines. [Accessed: Jul. 10, 2025].
- [6] Kali Linux, "Kali Linux." [Online]. Available: https://www.kali.org/. [Accessed: Jul. 10, 2025].
- [7] NetworkChuck, YouTube channel. [Online]. Available: https://www.youtube.com/@NetworkChuck. [Accessed: Jul. 10, 2025].
- [8] Rajneesh Cyber, YouTube channel. [Online]. Available: https://www.youtube.com/@RajneeshCyber. [Accessed: Jul. 10, 2025].
- [9] John Hammond, YouTube channel. [Online]. Available: https://www.youtube.com/@_JohnHammond. [Accessed: Jul. 10, 2025].