📝 *Endpoint Security & Monitoring using Wazuh*

1️⃣ Introduction

Protecting end-user devices—such as laptops, desktop computers, and servers—from online attacks is known as endpoint security.
In order to obtain illegal access or disseminate malware, modern cyberattacks frequently target endpoints.
Organizations utilize monitoring and detection solutions that can spot suspicious activity in real time to deal with these dangers.
Wazuh, an open-source EDR and SIEM solution, is used in this work to integrate endpoint security and monitoring.

2️⃣ Objective of the Task

This task's primary goals are to:

- Protect systems against malware and unauthorized access
- Monitor system activity and file changes
- Create automated alerts for suspicious behavior
- Gain insight into how EDR tools function in practical settings.

This assignment is finished as part of Internee.pk's Cybersecurity Internship.

3️⃣ Endpoint Security & EDR Overview

A security system called Endpoint Detection and Response (EDR) keeps an eye on endpoint activity all the time.
EDR tools assist in:

- Monitoring user activity and records
- Identifying malware and suspicious activity
- Reacting swiftly to security problems.

Every device linked to the network is safeguarded and kept under observation thanks to endpoint security.

4️⃣ Wazuh Implementation

The primary endpoint security and monitoring tool for this assignment is Wazuh.
Log analysis, file integrity monitoring, intrusion detection, and automated alarm generating are just a few of its functions.
Centralized monitoring of all linked agents and security incidents is made possible by the Wazuh dashboard.

5️⃣ Agent Deployment & Status

On a Windows system, a Wazuh agent was set up to keep an eye on endpoint activity.
The agent showed up on the dashboard as Active after successfully connecting to the Wazuh manager.
This attests to the endpoint's correct connection and Wazuh server monitoring.

---

6 File Integrity Monitoring (FIM)

Important system files are monitored for modifications using File Integrity Monitoring (FIM).
Wazuh creates an alert whenever a file is added, changed, or removed.
In this assignment:

- Wazuh successfully identified the modification
- An alert was issued and shown on the dashboard
- A test file was created and changed

---

7 Sysmon Log Monitoring

A Windows utility called Sysmon (System Monitor) is used to create comprehensive system logs.
It logs system operations, file modifications, and process creation.
To find suspicious activity, Wazuh gathers and examines Sysmon logs.
This facilitates real-time system and user activity monitoring.

---

8 Automated Alerts

When questionable activity is identified, automated alerts are produced.
File change warnings, suspicious process execution, and security rule breaches are a few examples.
Wazuh shows notifications on the dashboard after classifying them according to severity.
This makes it possible to react quickly to possible security incidents.

---

9 MalwareBazaar (Threat Intelligence)

A platform for public threat intelligence is called MalwareBazaar.
It offers details on malware samples, malware hashes (MD5 and SHA256), and malware families.
In order to comprehend how threat intelligence aids security tools in identifying malware using hash-based detection, MalwareBazaar was investigated in this endeavor.
⚠️ No malicious software was downloaded or run.

🔟 Conclusion

This assignment gave me practical experience with endpoint monitoring and security. File integrity monitoring, log analysis, and automatic alarms were all effectively implemented with Wazuh.
Understanding how EDR technologies safeguard systems and identify risks in practical settings was made easier by the work.