CYBER BANGLA

Assignment as Project

On

WAZUH

Submission Date: 12th December, 2023

Submitted By	Submitted To
MD YEASIN ARAFAT ID: 2023368 Batch: 08	FAYSAL HOSSAIN Cyber Security Researcher, Cyber Bangla

Wazuh

Wazuh is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats and behavioral anomalies.

Features:

- Security Analytics
- Intrusion/Malicious activities Detection
- Log data analysis
- Vulnerability detection
- Incident response
- Cloud security
- Regularity compliance

Components:

1. **Wazuh Agent**: It helps to protect your system by providing threat prevention, detection, and response capabilities.

2. **Wazuh Server**: It analyzes the data received from the agents, triggering alerts when threats or anomalies are detected. It is also used to manage the agent configuration remotely and monitor their status.

Wazuh as EDR

Endpoint Detection and Response is an endpoint (**any device of a company/org which connects with a network**) security **solution**.

Simply, detect incidents of end-point and response for solution.

Purpose of EDR:

- Enhancing an organization's cybersecurity posture by providing advanced capabilities for detecting, responding to, and mitigating security threats at the endpoint level.
- Record and store endpoint-system-level behaviors

3 primary duties:

1. Data Gathering
2. Data Recording
3. Detection

Wazuh can be strengthened by integrating it with Endpoint Detection and Response (EDR) capabilities.

Here, some steps for EDR solution in Wazuh-

1. **Pick EDR Solution**: Choose a suitable EDR solution like CrowdStrike or Carbon Black.
2. **Integrate with Wazuh**: Establish communication channels for seamless event sharing.
3. **Centralized Monitoring**: Configure Wazuh to monitor and analyze data from the EDR solution.
4. **Incident Response**: Create coordinated incident response procedures with Wazuh and EDR.

Wazuh as SIEM

Security Information and Event Management (SIEM) is a **heart** of SOC; without SIEM we can't think about SOC.

It is used in cybersecurity to provide real-time analysis of security alerts generated by various **hardware** and **software** systems within an organization.

Purpose: Suppose, we have 100 servers, 1000 users, 2000- routers, switches and firewalls. If we want to check the security of these, we have to check single by singe which is time and cost expenses. So, SIEM solves this problem by connecting all tools in centrally.

Functionality of SIEM:

- **Log User Access**: SIEM gets unauthorize access notification.
- **Track System Changes**: When any changes happen in system, SIEM track this change.
- **Monitor Adherence to Corporate Policies**: Monitoring the corporate's policies.

Here are some steps for SIEM-

1. **Data Collection**: Collects logs from various IT sources, like servers and endpoints.
2. **Log Parsing and Normalization**: Standardizes and parses diverse log formats for analysis.
3. **Detection Rules**: Utilizes predefined and customizable rules to identify security threats.

Install an Agent of Wazuh

1. Open dashboard of Wazuh by your IP
2. Click on “Add Agent”
3. **Deploy a new agent**:
    a. Choose OS as Windows
    b. Give fully-qualified domain name-FQDN (such as-www.wordpress.org) or Ip address of your network server.
    c. Assign the agent to a group: Leave it
    d. Copy commands from 4 no steps
4. Open powershell as admin
5. Paste this command your device’s powershell (3.0+) for agent installation
6. After installing wazuh agent, you’ll get a command like “NET STARTWazuhSyc” from step 5
7. Copy this command and run again on powershell
8. **To confirm it whether it is running or not**:
    a. Win + S: Services
    b. Click on “W”
    c. Wazuh service is found
    d. Status- Running
9. Go back into dashboard > 3 dots > Wazuh
10. You can see the number of agents

All written details are shown the given video.