SOC LAB PROJECT REPORT – WAZUH SIEM Threat Detection and Monitoring

Author: Nezvi Hussain

Introduction
This project demonstrates the deployment of Wazuh SIEM in a SOC lab to monitor endpoints, detect threats, and perform incident response.

Objectives
Deploy SIEM, collect logs, detect attacks, analyze alerts, map MITRE ATT&CK;, and respond to incidents.

Lab Environment
Linux Wazuh Manager, Windows Endpoint with Agent, Virtualized environment, Sysmon, Nmap.

SIEM Deployment
Wazuh installed on Linux, dashboard accessed via web, Windows agent deployed and verified.

Log Monitoring
Authentication, system, and process logs collected and analyzed in real time.

Threat Scenarios
Brute force attacks, network reconnaissance, suspicious command execution.

Alert Analysis
Events analyzed by severity, frequency, source and impact.

Incident Response
Endpoint identification, log review, escalation and remediation recommendations.

Skills Applied
SIEM monitoring, log analysis, MITRE ATT&CK;, threat detection, incident response.

Conclusion
The lab provided real-world SOC analyst experience in monitoring and responding to cyber threats.