Phase 1: Wazuh Threat Detection Lab Setup Documentation

Project Title:
Wazuh Threat Detection Lab - Phase 1: Core Setup & Windows & Linux Agent Integration

Objective

Establish a centralized security monitoring environment using **Wazuh**, focusing on core deployment and integrating Windows Server for log collection and endpoint monitoring.

Lab Environment Overview

Component	Details
Wazuh Manager	Installed on Ubuntu Server 22.04, static IP configured
Wazuh Dashboard	Version 4.12.0 (latest at time of deployment)
Windows Server	Domain Controller with Active Directory
Windows Agent	Installed and sending logs to Wazuh Manager
Network	Lab subnet `192.168.10.0/24`, private environment

Phase 1 Key Milestones

- ☑ Deployed Wazuh Manager & Dashboard on Ubuntu Server
- ☑ Configured Static IP for reliable agent connectivity
- ☑ Installed and activated Wazuh Agent on Windows Server
- ☑ Verified real-time event collection in Wazuh Dashboard

Technical Highlights

- **Wazuh Manager & Dashboard:** Installed via semi-assisted method on Ubuntu
- **Static IP:** Ensures consistent access to Wazuh Dashboard and Manager
- **Windows Agent:** Collecting Event Logs, Security Logs, and System events
- **Security Posture:** Initial hardening performed (password changes, restricted access)