Task 01

Wazuh Installation & FIM Monitoring

Duration: 10 Days

Goal: Set up Wazuh in your environment, start collecting real-time logs. This task will serve as the foundation for advanced monitoring and traffic analysis in the upcoming phases.

As part of this task, you will also configure **File Integrity Monitoring (FIM)** — a crucial security capability that detects changes to critical system files and directories in real-time. FIM helps identify unauthorized modifications, additions, or deletions, which can be early indicators of compromise or malicious activity. You will monitor specific paths, generate alerts based on file changes, and tune the system to reduce false positives while maintaining visibility.