

WAZUH SIEM & XDR

OPEN-SOURCE SECURITY PLATFORM



Wazuh SIEM Training

(Hands-On Open-Source SIEM & XDR Operations)

The Wazuh SIEM Training at Zoom Technologies is a complete, hands-on program that takes you from SIEM fundamentals to confident operation of Wazuh — the open-source SIEM and XDR platform used by SOC teams worldwide. You'll deploy the full Wazuh stack (agent, server, indexer, dashboard and Filebeat), onboard a lab of Windows 11, Windows Server, Ubuntu Desktop and Ubuntu Server machines, and configure every major capability live: Windows Advanced Audit Policy and Linux auditing, File Integrity and Registry Monitoring, malware detection with Sysmon, Defender logs, CDB lists and VirusTotal, custom decoders and log archives, MITRE ATT&CK attack simulation with Invoke-AtomicRedTeam, SSH brute-force detection with AbuseIPDB and Active Response, vulnerability detection, SCA and Suricata network intrusion detection. By the end, you'll be able to deploy, monitor, detect, respond and report with Wazuh in a real enterprise environment — finishing with email alerting and custom SOC dashboards.

Key Topics:

- SIEM Fundamentals
- Wazuh Architecture & Installation
- Lab Setup & Agent Deployment
- Windows & Linux Endpoint Monitoring
- Malware Detection & FIM
- Sysmon & Threat Intelligence
- Threat Hunting & Decoders
- MITRE ATT&CK Attack Simulation
- Active Response
- Vulnerability Management & SCA
- Suricata Intrusion Detection
- Alerting & Dashboards

Wazuh SIEM Training

Module 1: SIEM Fundamentals

- What is SIEM (Security Information and Event Management)
- Key features: log management, event correlation, threat detection, centralised monitoring, incident response
- SIEM functions: log collection, log processing and analysis, log archival

Module 2: Introduction to Wazuh

- What is Wazuh: open-source SIEM with XDR capabilities
- Core capabilities: log analysis, FIM, SCA, vulnerability detection, threat intelligence, malware and rootkit detection, Active Response
- Regulatory compliance monitoring, system inventory and cloud security monitoring
- Endpoint, command and script monitoring

Module 3: Wazuh Architecture & Installation

- Wazuh agent, server, indexer and dashboard
- Role of Filebeat in the data pipeline
- Preparing the Wazuh environment and installation
- Accessing and navigating the Wazuh dashboard

Module 4: Lab Setup & Agent Deployment

- Installing Windows 11, Windows Server, Ubuntu Desktop and Ubuntu Server VMs
- Deploying Wazuh agents on Windows and Linux endpoints
- Verifying agent connectivity and log flow

Module 5: Windows Endpoint Monitoring

- Local security policy and Advanced Audit Policy configuration
- Default Windows logs
- USB (PnP) device monitoring
- Logon/logoff and object-access auditing
- Command monitoring through process creation events

Module 6: Linux Endpoint Monitoring

- Default Ubuntu logs
- Enabling audit policies
- Command monitoring in Ubuntu
- Generating login and logoff alerts

Module 7: Malware Fundamentals & Detection

- Malware types: virus, worm, Trojan horse, ransomware, RAT, rootkit
- How Wazuh detects malware
- Collecting and analysing Windows Defender logs

Module 8: File Integrity & Registry Monitoring

- File Integrity Monitoring (FIM) on Windows and Ubuntu
- Windows Registry monitoring
- FIM on Ubuntu Server

Module 9: Threat Intelligence Integrations

- Working with CDB lists
- VirusTotal integration for file reputation
- AbuseIPDB integration for IP reputation

Module 10: Sysmon Integration

- What Sysmon is and why it matters
- Integrating Sysmon with Wazuh to detect malware

Module 11: Threat Hunting Foundations

- Introduction to threat hunting
- Wazuh decoders
- Log data collection and archives

Module 12: MITRE ATT&CK & Attack Simulation

- Introduction to the MITRE ATT&CK framework
- Simulating attacks with Invoke-AtomicRedTeam
- Command monitoring for attack detection

Module 13: Active Response

- Detecting SSH brute-force attacks
- Active Response: automatically blocking the attacker

Module 14: Vulnerability Management & SCA

- Vulnerability management in the SOC
- Detecting vulnerabilities across endpoints
- Security Configuration Assessment (SCA)

Module 15: Intrusion Detection

- NIDS vs HIDS
- Suricata IDS integration
- Detecting malicious command execution

Module 16: Alerting, Dashboards & Visualization

- Configuring email notifications
- Anatomy of a dashboard
- Creating custom dashboards and visualizations