INFOSECTRAIN
Educate. Excel. Empower.

wazuh.

Practical Training

Hands-on SIEM & XDR SOC Training

Course Highlights

24-Hour Instructor-Led Training

Hands-on SIEM & XDR SOC Training

Real-World Detection Engineering & Alert Tuning

Live Wazuh Environment with Attack Simulation

SOC Analyst Workflows & Investigation Techniques

Custom Decoder & Rule Development

Endpoint Telemetry, Active Response & Automation

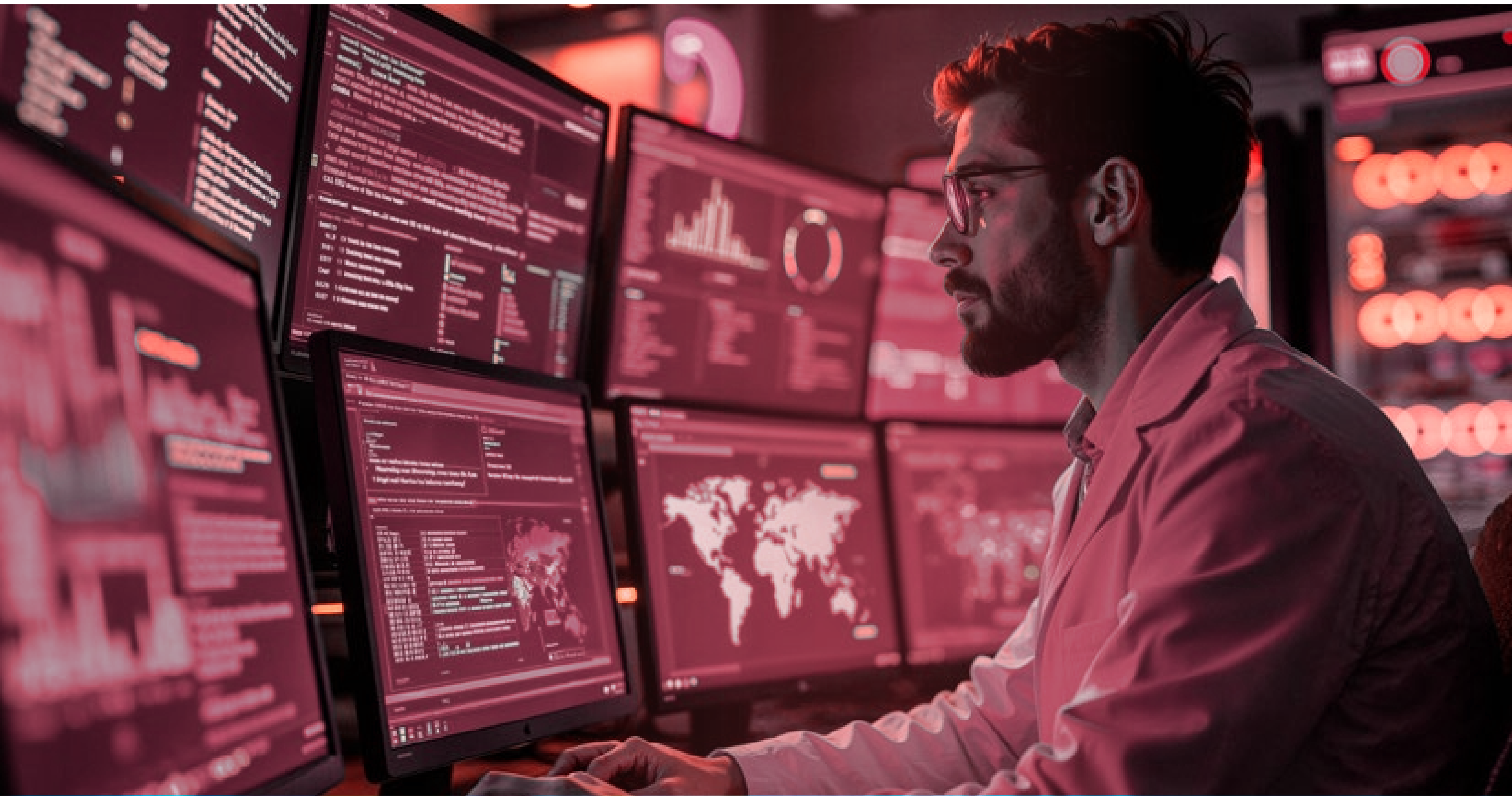
Vulnerability Detection & Compliance Monitoring

Recorded Sessions & Post-Training Support

About Course

InfosecTrain's Wazuh Hands-on Online Training is designed for professionals responsible for monitoring, detecting, and responding to security threats using SIEM and XDR technologies.

The course starts with Wazuh fundamentals and architecture, then progressively builds skills in log decoding, detection engineering, active response, vulnerability management, performance tuning, and SOC operations. Participants will gain hands-on experience across endpoint telemetry, rule tuning, dashboard creation, and alert investigation.



Course Objectives

You will be able to:

- Deploy and operate Wazuh as a SIEM & XDR platform
- Collect and analyze endpoint telemetry
- Build custom decoders and detection rules
- Tune alerts and reduce false positives
- Execute active response and automation
- Perform vulnerability detection and compliance checks
- Investigate alerts using SOC dashboards

Target Audience

- SOC Analysts (Tier 1/Tier 2/Tier 3)
- Detection Engineers
- Blue Team Professionals
- Security Monitoring Engineers
- SIEM Engineers
- Incident Response Analysts
- Cybersecurity Students and Practitioners

Pre-Requisites

- Basic understanding of cybersecurity concepts
- Familiarity with Linux and Windows environments
- Basic networking and log analysis knowledge
- Prior SOC or SIEM exposure is helpful but not mandatory

Course Content

Module 0 Orientation & Wazuh Mental Model

- What Wazuh is and What it is Not
- SIEM vs XDR vs EDR Clarification
- Core Wazuh Components: Agent, Manager, Indexer, Dashboard
- End-to-End Data Flow
- Navigating a Live Wazuh Environment
- Tracing an Alert from Raw Log to Dashboard

Module 1 Wazuh Architecture, Installation & Deployment

- Deployment Models: Single-Node vs. Distributed
- Manager, Indexer, and Dashboard Separation
- TLS, Certificates, and Secure Communication
- Agent Enrollment and Authentication
- Linux and Windows Agent Installation
- Agent Registration Troubleshooting
- Health Checks and Baseline Validation

Module 2 Wazuh Agent Internals & Endpoint Telemetry

- Agent Architecture and Internals
- Configuration Hierarchy and Agent Groups
- Windows Event Channels and Sysmon Integration
- Linux Log Collection and Auditing
- File Integrity Monitoring (FIM)
- Rootcheck Fundamentals
- Validating Agent-Generated Alerts

Module 3 Log Decoders: Parsing & Normalization

- Decoder Role and Structure
- Regex, Prematch, and Field Extraction
- JSON and Structured Logs
- Writing Custom Decoders (Linux & Windows)
- Decoder Ordering and Conflict Resolution
- Debugging with wazuh-logtest

Module 4 Detection Engineering with Wazuh Rules

- Rule Structure, Levels, and Hierarchy
- Correlation, Frequency, and Timeframe Rules
- Rule Chaining and Conditional Logic
- Custom Detection for Attack Scenarios
- False-Positive Reduction and Tuning
- MITRE ATT&CK Mapping
- Multi-stage Attack Detection

Module 5 Active Response & Automated Actions

- Active Response Architecture
- Built-in and Custom Responses
- Bash and PowerShell Automation
- Safety Controls and Validation
- Response Logging and Rollback

Module 6 Vulnerability Detection & Compliance Monitoring

- Vulnerability Detection Engine
- Software Inventory and CVE Correlation
- Vulnerability Alert Validation
- Compliance Monitoring Frameworks
- Configuration and Policy Compliance

Module 7 Indexer Internals, Performance & Scaling

- OpenSearch Indexer Architecture
- Shards, Replicas, and ILM
- Disk and Performance Monitoring
- High-Ingestion Tuning
- Query and Dashboard Troubleshooting

Module 8 Dashboarding, Queries & SOC Operations

- Navigating the Wazuh Dashboard
- Alert Querying and Filtering
- SOC-focused Dashboards
- Alert Triage and Investigations
- Analyst Productivity Optimization

Lab Environment Note

If a participant wishes to run the lab locally over VM (Virtual Machine) and does not have a credit card, below are the bare minimum specifications for their system or laptops.

LOCAL VM (No Credit Card Required)

- ✓ RAM: 16 GB
- ✓ Storage: 300 GB or more
- ✓ CPU: 8 Cores
- ✓ Supports Wazuh + Windows Lab Setup

CLOUD VM (Optional)

- ✓ Instructor-supported DigitalOcean setup
- ✓ $200 Free Credits (approx. 15–20 days)
- ✓ Credit card required
- ✓ Instructor assists with account and setup

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on