Updated on 24/06/2025

Sign up

Wazuh Training

4 days (28 hours)

PRESENTATION

Our Wazuh training course will enable you to effectively secure your IT infrastructures and monitor potential threats in real time. Unlike other security tools, Wazuh offers a unified platform for different environments such as data centers, cloud infratructures and applications.

In this training course, aimed at security engineers and consultants responsible for implementing, configuring and operating a Wazuh HIDS/SIEM system. It covers all the main Wazuh components and how to get the most out of them.

You'll get first-hand experience with many of Wazuh's features and learn many ways to bring these features together in synergy for advanced purposes.

The course is made up of lectures and practical exercises designed to help you understand how the technology works. These exercises teach you how to carry out configuration and operation tasks to exercise the features developed throughout the course.

As with all our training courses, this one will introduce you to the latest stable version of Wazuh (at the time of writing: Wazuh 4.11).

Objectives

- Explain Wazuh's architecture and operation in detail
- Install, configure and administer a Wazuh infrastructure
- Customize the ruleset (decoders, rules, personalized scenarios)
- Monitor system integrity and detect vulnerabilities
- Automate incident detection and response (Active Response)
- Implement advanced integrations
- Administer a Wazuh environment in HA cluster mode

Target audience

- IT professionals
- System administrators
- Network administrators
- DevOps engineers
- Cloud solution architects

Prerequisites

- Experience with basic IT security concepts
- Basic knowledge of the Linux command line
- Test My Knowledge

Technical requirements

- A PC capable of running Docker containers (minimum 16 GB RAM required) for labs

Our Wazuh training program

Day 1: Introduction, Architecture, Deployment and Configuration

Introduction to Wazuh

- Introduction to Wazuh
- Architecture and secure communication
- Agent deployment and registration
- Discovering the Wazuh Dashboard
- Configuring Wazuh

Architecture and secure communication

- Wazuh client-server architecture
- Communication between components
- Securing exchanges Deploying and

registering agents

- Wazuh server deployment options
- Installation requirements

- Agent registration methods
- Agent upgrades
- TP/Lab 1: Deploying and registering an agent

Discovering the Wazuh Dashboard

- Connecting to the Wazuh Dashboard
- Introduction to the interface
- Exploring key sections
- Lab 2: Exploring the Wazuh Dashboard

Configuring Wazuh

- Main configuration files
- Centralized agent configuration
- Basic configuration options
- Lab 3: Centralized agent configuration

Day 2: Log analysis, rules and decoders

Log analysis

- Wazuh log analysis engine
- Log flow in the Wazuh pipeline
- Analysis phases
- Locating logs and alerts
- Network device monitoring via Syslog
- Regulatory compliance support
- TP/Lab 4: Log analysis and monitoring of

Wazuh rules Indexer and Dashboard

- Integration with OpenSearch indexer
- Using the Wazuh Dashboard as an alert management console
- Detailed Wazuh Ruleset

event/alert pipeline

- Wazuh Ruleset structure
- Various application coverage
- Updating the Ruleset
- Ruleset contribution (brief mention if relevant to audience)
- In-depth exploration of rules hierarchy Decoders

and rules

- Definition of rules, decoders and pre-decoders
- Types of rules
- Decoders in detail
- Creating custom rules and decoders
- Best practices for adapting Ruleset
- Testing custom decoders and rules
- Dynamic decoding of incoming JSON logs
- TP/Lab 5 : Creating a custom decoder and rule CDB lists

- How CDB lists work
- CDB list use cases
- File format and paths
- Creating rules using CDB lists
- TP/Lab 6: Using CDB lists

Day 3: Monitoring, detection and response

File integrity monitoring (FIM)

- How the FIM module (Syscheck) works
- Syscheck configuration options
- FIM exclusions
- FIM alerts
- FIM use cases
- Lab 7: Configuring and analyzing FIM results Inventory

collection & vulnerability detection

- Inventory collection (Syscollector)
- Vulnerability detection module
- Vulnerability scanner configuration
- Viewing vulnerabilities
- Using inventory via the Wazuh API (brief mention)
- TP/Lab 8: Vulnerability detection

Rootkit detection

- How the Rootcheck module works
- Detection methods
- Rootcheck alerts
- Lab 9: Rootkit simulation

Wazuh integration system

- Integration system overview
- Integration configuration
- Examples of integrations provided by

Wazuh Active response

- Active response concept
- Default active response scripts
- Command types
- Active response configuration
- Active response examples
- TP/Lab 10: Configuring an automatic active response Safety

Configuration Assessment (SCA)

- How the SCA module works
- SCA policies
- Centralized management of SCA policies
- Types of SCA checks
- SCA evaluation results
- Lab 11: SCA policy execution

Day 4: Threat Intelligence, advanced integrations and HA administration

MITRE ATT&CK techniques

- Introduction to the MITRE ATT&CK framework
- Mapping Wazuh alerts with MITRE ATT&CK
- Navigating the MITRE ATT&CK Dashboard module
- Using ATT&CK Navigator
- TP/Lab 12: Exploring MITRE ATT&CK mapping in Wazuh

Advanced integrations

- Docker, Trivy and SCA integration
- Osquery integration
- TP/Lab 13: Execute an Osquery query via Wazuh and analyze the results in the Dashboard
- Sysmon integration (Windows)
- Lab 14: Simulate a Sysmon event
- Azure integration
- Office 365 integration
- Integration with IT platforms (VirusTotal, MISP)
- Lab 15: EICAR testing and VirusTotal integration
- ClamAV and YARA Rules

integration HA cluster management

- Deploying a Wazuh in an HA cluster (multi-VMs using Docker on nodes)
- Certificate rotation
- Adding new nodes
- HA cluster upgrades (Docker and installed source versions)
- Snapshots

Conclusion & next steps

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.