Updated 03/31/2025

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 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.

This course consists of lectures and practical exercises to understand how the technology works. These exercises teach you how to carry out configuration and operating tasks order to exercise the functionalities 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

- Install, configure and manage the Wazuh infrastructure (Manager, Agents, Indexer, Dashboard).
- Customize rulesets by developing advanced decoding, rules and scenarios adapted to their specific environment.
- Automate incident detection and response (via Active Response scripts) and compliance with security policies.
- Monitor system integrity (FIM) and detect vulnerabilities and rootkits.

- Implement advanced integrations with third-party solutions (Docker, AWS, Osquery, Sysmon, MITRE ATT&CK).
- Administer a clustered Wazuh environment to ensure high availability and resilience.
- Explain Wazuh's architecture and operation in detail.

Target audience

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

Prerequisites

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

Technical requirements

- A PC capable of running Docker containers (minimum 8 GB RAM required) for the labs

Wazuh training program

DISCOVERY & INSTALLATION

- Introduction to Wazuh and use cases
- Architecture and secure communication
- Installing a Wazuh cluster (Manager, Indexer, Dashboard)
- Agent deployment and registration methods
- Wazuh dashboard: discover the features
- Agent push upgrade
- Wazuh basic configuration
- Workshop 1: Deploying a complete environment
- Workshop 2: Agent registration and supervision

ANALYSIS & DETECTION

- Security log analysis
- How the Wazuh Indexer and Dashboard work
- Wazuh rule set
- Decoders, rules and CDB lists

- Wazuh pipeline: understanding and optimization
- Workshop 3: Creating custom rules
- Workshop 4: Alert analysis and advanced filtering

MONITORING & RESPONSE

- File integrity monitoring
- Agent inventory collection
- Vulnerability detection
- Rootkit detection
- Active response and remediation
- Security configuration assessment (CIS, PCI, GDPR...)
- Workshop 5: Attack simulation and detection
- Workshop 6: Setting up an active response

INTEGRATION & CASE STUDIES

- MITRE ATT&CK techniques applied to Wazuh
- Osquery integration for advanced inventory
- Sysmon integration for Windows Events
- Amazon CloudTrail integration overview
- Automated alert processing
- Visit the Wazuh Manager cluster & best practices
- Optimization and troubleshooting
- Workshop 7: Integrating an external tool (Osquery or Sysmon)
- Workshop 8: Incident detection & remediation case study

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer 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 enabling 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 with regard to the training to come, 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 course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

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

Validation

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

Sanction

A certificate will be issued to each trainee who completes the course.