+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 08/18/2026

Sign Up

Advanced Wazuh Training

2 days (14 hours)

Overview

Wazuh is an open-source XDR and SIEM platform that centralizes threat detection, correlation, and response across your endpoints, servers, and hybrid environments. With agents, rules, decoders, vulnerability scanning, FIM, and SCA, Wazuh enables you to build a robust and industrialized security monitoring system.

Our Advanced Wazuh training will take you beyond the basics to master the critical topics encountered when deploying and operating a Wazuh platform in production.

You'll learn how to structure a Wazuh server, Wazuh Indexer, and Wazuh Dashboard architecture; refine rules and decoders; and leverage File Integrity Monitoring, Security Configuration Assessment, and vulnerability detection.

By the end of the course, you will be able to optimize alert quality, reduce operational noise, better prioritize incidents, and set up a production-ready security monitoring system.

This training also covers active response, integration with the dashboard, agent administration, hardening best practices, and the essentials for ensuring reliable operation in a real-world environment.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the Wazuh architecture and the role of each component.

- Configure and manage agents and their centralized monitoring.
- Utilize the FIM, SCA, and vulnerability detection modules.
- Create and fine-tune rules and decoders to improve detection.
- Implement active response measures and relevant dashboards.
- Prepare a production-ready deployment using security best practices.

Target Audience

- Cybersecurity Analyst
- SOC Analyst
- Security Administrator
- Security Engineer
- Systems and Network Administrator

Requirements

- Basic knowledge of Linux and system administration.
- Practical experience with IT security and monitoring concepts.
- Understanding of logs, alerts, and event analysis.
- Experience with SIEM or log collection tools is preferred.
- Ability to read technical documentation in English.

Technical Requirements

- A recent computer with at least 16 GB of RAM is recommended for hands-on exercises.
- A stable Wi-Fi or Ethernet connection to access the test environments.
- A modern, up-to-date browser, such as Google Chrome or Mozilla Firefox.
- An SSH client and a terminal available on your workstation.
- A virtualization environment, such as VirtualBox or VMware Workstation, if the workshops are conducted locally.

Agenda for our Advanced Wazuh Training

[Day 1 - Morning]

Architecture and Data Flow

- Review of Wazuh’s key components and their roles in the detection chain.
- Understanding the data flow between the agent, server, indexer, and dashboard.
- Review of the ports, services, and data exchanges required for the platform to function.
- Differences between all-in-one, distributed, and clustered deployments.
- Managing initial checkpoints to validate an operational architecture.
- Hands-on workshop: mapping a target Wazuh architecture and identifying the data flows to secure.

[Day 1 - Afternoon]

Agents, Data Collection, and Monitoring

- Enrollment and administration of Wazuh agents.
- Configuring the collection of logs, system events, and security data.
- Monitoring agent status, versions, and connectivity.
- Managing agentless cases for certain network devices.
- Best practices for organizing monitoring by device fleet, role, or environment.
- Hands-on workshop: Registering an agent, verifying its reporting, and reviewing the collected data.

[Day 2 - Morning]

Advanced Detection and Compliance

- Using FIM and SCA modules to strengthen the security posture.
- Understanding vulnerability detection mechanisms and alert enrichment.
- Creating and customizing rules and filters to reduce alert noise.
- Interpreting alerts and prioritizing them based on business and technical context.
- A methodical approach to linking events to concrete threat scenarios.
- Hands-on workshop: adjusting an SCA rule and policy to produce more relevant detections.

[Day 2 - Afternoon]

Response, Dashboards, and Operations

- Building dashboards useful for operational monitoring and SOC management.
- Configuring Active Response to automate certain remediation actions.
- Exploring advanced dashboard features for analysis and diagnostics.
- Best practices for securing, hardening, and maintaining the platform.
- Organizing daily operations, controls, and monitoring points in production.
- Hands-on workshop: Design an automated response scenario and test it on a simple case.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in a new advanced IT technology or to acquire specific industry knowledge or modern methods.

Placement at the Start of Training

The assessment upon enrollment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technology, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also enables us to anticipate certain connection issues or

internal security issues within the company (in-house or virtual classroom) that could hinder the monitoring and smooth operation of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.