AMBIENT-IT

+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

Wazuh Security Engineer Training

3 days (21 hours)

Overview

Wazuh is an open-source SIEM and XDR platform that centralizes threat detection, monitoring, and response. With the Wazuh Manager, agents, dashboard, and indexer, Wazuh provides a comprehensive pipeline for analyzing events, enhancing visibility, and streamlining security operations.

Our Wazuh Security Engineer training will enable you to go beyond basic installation and master the essential aspects of a Wazuh platform ready for production environments.

You'll learn how to design a Wazuh architecture, deploy and manage agents, work with alerts, logs, and dashboards, and oversee the collection and analysis of security data.

The training also covers the creation of rules, decoders, and detection use cases, as well as managing the platform's functional caching, monitoring, access control, and best practices for operation.

Upon completion of the training, you will be able to configure a robust Wazuh platform, improve detection quality, streamline day-to-day administration, and prepare a production-ready foundation for your security teams.

Finally, this training covers hardening, observability, maintenance, and operational implementation to ensure the long-term security of your environments.

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.
- Deploy and manage the agents, the manager, the dashboard, and the indexer.
- Configure log collection, correlation, and operational visibility.
- Create and fine-tune rules and decoders to improve detection.
- Use dashboards, alerts, and metrics to manage security.
- Apply best practices for monitoring, security, and operational maintenance.

Target Audience

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

Prerequisites

- Basic knowledge of cybersecurity and technical monitoring.
- Proficiency in Linux fundamentals and system administration.
- Basic understanding of log management and event analysis.
- General understanding of network environments and exposed services.
- Experience with an administration or monitoring tool such as SIEM or XDR is a plus.

Technical Requirements

- A recent computer with at least 16 GB of RAM and a multi-core processor.
- A stable Wi-Fi or Ethernet connection for online activities.
- Access to a Linux lab environment, either local or virtual.
- An up-to-date web browser to use the Wazuh dashboard.
- A virtualization or remote access tool, depending on the environment provided by the instructor.

Curriculum for our Wazuh Security Engineer Training Course

[Day 1 - Morning]

Platform Fundamentals

- Understand Wazuh’s role within a detection and monitoring architecture.
- Identify the roles of the manager, agents, dashboard, and indexer.
- Explore the data flow from collection, analysis, indexing, to visualization.
- Review the main configuration objects and basic concepts of ossec.conf.
- Gain an understanding of operational use cases, from host monitoring to incident detection.

- Hands-on workshop: Map out a target Wazuh architecture and assign each component to its role.

[Day 1 - Afternoon]

Installation and

Commissioning

- Prepare a consistent deployment environment for an initial platform.
- Install and verify the prerequisites for the Wazuh Manager and the dashboard.
- Understand the dependencies of the indexer and the connection logic between services.
- Verify certificates, administrative accounts, and essential services.
- Diagnose common startup errors and connectivity issues.
- Hands-on workshop: Deploy a reference Wazuh instance and control access to the administration interface.

[Day 2 - Morning]

Agent Management and Data Collection

- Enroll an agent and track its lifecycle in the console.
- Configure log forwarding, file monitoring, and collection modules.
- Organize agents into groups to simplify large-scale operations.
- Monitor endpoint health, connectivity, and monitoring events.
- Customize collection settings based on business and technical requirements.
- Hands-on workshop: Register multiple agents, then check their status and initial alerts.

[Day 2 - Afternoon] Detection

and Normalization

- Understand the role of decoders in interpreting raw events.
- Build and test context-specific detection rules.
- Use the test engine to validate the correspondence between logs, decoders, and rules.
- Refine alerts with conditions, severity levels, and exceptions.
- Structure a step-by-step detection approach, from simple cases to business-specific scenarios.
- Hands-on workshop: Create a simple decoder and an associated rule based on an event log.

[Day 3 - Morning]

Analysis, Dashboards, and Operations

- Explore dashboards to monitor alerts, trends, and exposed assets.

- Review metrics useful for operational analysis and triage.
- Use the search, filtering, and contextualization features for incidents.
- Understand rights management and access control principles.
- Set up a monitoring routine for security teams.
- Hands-on workshop: Build a SOC-oriented dashboard to track a threat scenario.

[Day 3 - Afternoon] Standardization

and Best Practices

- Strengthen platform security by hardening components.
- Apply best practices for maintenance, backup, and operations.
- Prepare for scalability, monitoring, and service continuity.
- Organize recurring administration and monitoring tasks.
- Identify key considerations for a controlled transition to production.
- Hands-on workshop: Develop a Wazuh operations plan that includes monitoring, maintenance, and production deployment priorities.

Target Audience

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

Assessment at the Start of Training

The pre-training assessment 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 technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. 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.