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

Updated on 27/05/2024

Sign up

Wazuh training: Detect threats in real time

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.

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 in 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 4.3).

Objectives

- Describe the main features and components of Wazuh
- Configuring Wazuh managers and agents
- Create new rules and decoders
- Understand the Wazuh event/alert data pipeline and the programs, data files and network paths involved.

- Browse Wazuh alerts for security, configuration, compliance checks and vulnerability assessment
- Monitor your Wazuh installation via the web application
- Understand how Wazuh helps with regulatory compliance (PCI, SOCKS, HIPAA, RGPD...)
- Understand the variety of options available for pushing or extracting log content in Wazuh

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

Wazuh training program

Day 1: Presentation

- Introduction to Wazuh
- Architecture and secure communication
- Agent deployment and registration methods
- Wazuh dashboard
- Agent push upgrade
- Wazuh configuration

Day 2: Analysis

- Log analysis
- Wazuh Indexer and dashboard
- Wazuh rule set
- Decoders and rulers
- CDB lists
- Crossing the Wazuh set of rules
- Advanced indexer pipeline configuration

Day 3: Monitoring

- File integrity monitoring

- Agent inventory and vulnerability detection
- Rootkit detection
- Wazuh integration system
- Active response
- Security configuration assessment

Day 4: Integration

- Techniques MITRE ATT&CK
- Docker integration
- Amazon CloudTrail integration overview
- Osquery integration
- Sysmon integration
- Visit the Wazuh Manager cluster
- Automated alert processing
- Evaluation

Companies concerned

This 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 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 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, with 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.