wazuh.

Essential Training for Security Engineers

› 4-Day Course ‹

Wazuh for Security Engineers › **4-Day Course** ‹

Overview

This four-day training course is designed for security engineers and consultants responsible for implementing, configuring, and operating Wazuh as an XDR and SIEM. It covers all the main components of Wazuh, and how to get the most out of them, with a special focus on tuning the Wazuh ruleset through the creation of custom rules and decoders. You will gain direct experience with many Wazuh features and learn various ways to integrate them synergistically for advanced use cases.

This course consists of lectures and hands-on exercises performed in a virtual lab environment provided to you by our team. The exercises teach you to perform configuration and operational tasks by following procedures outlined in the provided lab guides, allowing you to explore the features in focus throughout the training. During the course, you will have unrestricted access to your lab environment, which will remain available for additional practice for 24 hours after the class ends. Comprehensive course materials containing both theory and practical exercises will be provided. Copies of the slide decks will also be given at the end of the training.

4 days	Wazuh 4.14.4+
DURATION	SOFTWARE VERSIONS

Intended audience

- Security engineers
- Security analysts
- IT professionals who implement, operate, or support security systems

Prerequisites:

Familiarity with basic IT security concepts

Basic familiarity with Linux command line (enough to use a text editor)

*Networking should allow outgoing traffic for port **22 (SSH)**, **3389 (RDP)**, and **443 (UI)** to *.lab.wazuh.info*

Course Objectives

At the end of the course, you should be able to:

01 Describe key features and components of Wazuh.

02 Configure Wazuh managers and agents.

03 Create new rules and decoders.

04 Understand the Wazuh event/alert data pipeline, including the programs, data files, and network paths involved.

05 Navigate Wazuh alerts via various dashboards.

06 Use Wazuh modules for security configuration compliance checks and vulnerability assessment.

07 Monitor your Wazuh installation via the Wazuh web application.

08 Understand how Wazuh helps with regulatory compliance (such as PCI, SOC 2, HIPAA, GDPR, etc.)

Table of Contents

DAY 1

Day 1

Introduction to Wazuh

The course introduction provides students with a general overview. You will learn what Wazuh is and why companies use this tool. You will learn about Wazuh's principal capabilities and get a brief background on the project itself.

Architecture and Secure Communication

This module describes the Wazuh architecture and its fundamental components. Upon completing this module, you will achieve the following objectives:

- Understand the multi-platform Wazuh agent and its role in data collection.
- Describe the three central components: Wazuh server, Wazuh indexer, and Wazuh dashboard.
- List the different deployment options (all-in-one, single-node, and multi-node).
- Understand agentless monitoring capabilities for network devices and systems.
- Comprehend the data flow from agents through analysis to indexing and visualization.

Wazuh Server Cluster

This module describes the Wazuh server cluster architecture for environments requiring high availability and scalability. Upon completing this module, you will achieve the following objectives:

- Understand the master and worker node concepts in a Wazuh server cluster.
- Describe the responsibilities of master nodes in managing agents and configurations.
- Explain how worker nodes process events and synchronize with the master.
- Comprehend data synchronization between cluster nodes.
- Identify special considerations when managing clustered Wazuh deployments.

Wazuh Configuration

This module describes basic Wazuh configuration and demonstrates how to push configurations from manager to agents. Upon completing this module you will achieve the following objectives:

- Identify configuration files such as `ossec.conf` and `agent.conf`, as understand which files and configuration categories can be centrally distributed versus individually maintained on a manager or agent.
- Make configuration changes via the web app or command line.
- Understand the basic categories of configuration settings for managers and agents.
- Comprehend how configurations are propagated between managers and from managers to agents.
- Use agent groups and profiles to organize the propagation of the appropriate configuration elements to the right agents, even when large numbers of agents are involved.

This module includes the following lab exercise:

- Manage your Wazuh manager's primary configuration and internal options.
- Implement centralized agent configuration using agent groups and profiles.

Agent Registration and Connection to Wazuh Server

This module covers agent registration procedures for Linux and Windows systems. Upon completing this lab, you will achieve the following objectives:

- Install the Wazuh agent on Linux and Windows systems.
- Understand different agent registration methods.
- Register agents using self-enrollment with authentication passwords.
- Verify agent connectivity to the Wazuh manager.

Wazuh Dashboard

This module provides an initial introduction to the Wazuh dashboard and its key features. Upon completing this lab, you will achieve the following objectives:

- Understand the layout and navigation of the Wazuh dashboard.
- Know how to access and interpret key dashboards for alerts and agent status.
- Have a basic sense of the feature set of the Wazuh Dashboard.
- Prepare for extensive use of the dashboard throughout the rest of the training.

Remote agent upgrades

This module describes how to use the Wazuh manager to push upgrades to agents. Upon completing this lab, you will achieve the following objectives:

- Understand agent upgrade mechanisms via the manager.
- Push agent upgrades to connected agents using the Wazuh API.
- Verify successful agent upgrades.

Centralized Agent Configuration

This module covers centralized agent configuration management using agent groups. Upon completing this lab, you will achieve the following objectives:

- Understand the purpose and structure of agent.conf files.
- Create and organize agent groups for selective configuration management.
- Deploy centralized configurations to multiple agents using agent groups.
- Understand configuration propagation and validation procedures.
- Use the Wazuh API and dashboard to manage agent group assignments.

DAY 2

Day 2

Log Analysis

This module covers the log analysis component and how log messages flow from agents to the manager. Upon completing this module you will achieve the following objectives:

- Understand the capabilities of the log analysis engine.
- Differentiate between the collection process and the analysis process.
- Extract the content of a log message.
- Describe how log messages flow through the Wazuh pipeline.
- Understand the analysis phases: pre-decoding, decoding, and rule-based analysis.
- Locate the files where logs and alerts are stored.
- Monitor network devices via syslog.
- Understand how this component supports regulatory compliance.
- Benefit from the Wazuh ruleset and its regulatory compliance mapping.

This module includes two lab exercises:

- Generate a brute force attack.
- Analyze the log entries resulting from the previous exercises.
- Look up and trace Wazuh rules for better understanding.

Wazuh Ruleset

This module describes the Wazuh ruleset and rule structure. Upon completing this module you will achieve the following objectives:

- Understand atomic and composite rule concepts.
- Differentiate between rules that generate alerts and parent rules.
- Understand rule hierarchy and parent-child relationships.
- Explain alert levels and their security relevance.
- Understand frequency and timeframe concepts in composite rules.
- Identify the custom rule ID range to avoid conflicts.

This module covers the following topics:

- Atomic rules: simple rules analyzing individual events.
- Composite rules: rules correlating multiple events using frequency and timeframe.
- Rule structure and unique rule IDs.
- Alert level definitions (0-15) and security relevance.
- Parent rules and rule hierarchy for efficient matching.
- Rule-matched-sid and rule frequency-based escalation.
- Ignore timers to prevent alert floods from composite rules.
- Rule group tags and compliance mapping.
- MITRE ATT&CK technique mapping in rules.

Decoders and Rules

This module describes the various types of rules and decoders used by Wazuh. You will learn to create custom rules for your own applications. Upon completing this module you will achieve the following objectives:

- Understand rules, decoders, and pre-decoders.
- Familiarize yourself with different options.
- Create new rules and decoders for your own applications.
- Learn best practices for adapting the ruleset to your environment.

This module covers these topics:

- Definition of rules and decoders
- Atomic rules for single events
- Composite rules for multiple events
- Alert levels
- Pre-decoders vs decoders
- Regular expressions in Wazuh
- Testing your custom decoders and rules
- Wazuh dynamic decoding of incoming JSON log records

This module includes the following lab exercises:

- Modify an existing rule by altering its frequency and/or alert level.
- Write a custom decoder for a specific log message.
- Create custom rules that match a specific log message and assign an alert level.
- Develop an advanced custom rule based on an existing SSHD rule.
- Deploy Suricata on an agent and configure Wazuh to consume and alert on its JSON logs.

DAY 3

Day 3

CDB Lists

This module covers the following topics:

- CDB list lookups within rules
- Use cases for CDB lists
- File paths and line format for CDB lists
- Creating new rules to utilize CDB lists

This module includes the following lab exercises:

- Escalate SSHD alerts based on known attackers' IPs.
- Create a rule that looks up an extracted key in a CDB list and matches only if the value in the CDB associated with that key meets specific criteria.

Wazuh Ruleset Traversal

This module includes the following topics:

- In-depth exploration of how the analysis engine traverses the ruleset hierarchically while analyzing an event. Understanding this process is crucial for successfully deploying custom escalation and whitelisting rules to tailor the Wazuh ruleset to your specific environment.

Indexer Advanced Pipeline Configuration

This module covers the following topics:

- Advanced GeoIP and Autonomous System enrichment for your alerts
- Field normalization
- Split routing of different classes of alerts (and even non-alerting events) to separate index patterns
- Conditional textual transforms of field data.

This module includes the following lab exercise:

- Deploy an advanced ingest node pipeline and observe its operation in your live alert stream.
- Designing and Managing Index Lifecycle policies in Wazuh to optimize data storage and performance.

File Integrity Monitoring

This module covers the syscheck component used to detect changes in system binaries, configuration files, and files that contain critical content. Upon completing this module, you will achieve the following objectives:

- Understand how syscheck detects file changes on Windows and Linux systems.
- List the different syscheck options and monitoring modes.
- Configure syscheck for real-time detection.
- Set up syscheck for who-data collection and file change diff reporting.
- Exclude frequently changing files from syscheck monitoring.
- Apply syscheck configuration to specific agent groups.

Agent Inventory Collection and Vulnerability Detection

This module covers the syscollector and vulnerability-detection features in Wazuh, addressing:

- How Wazuh agents regularly collect and report inventory items to their manager
- How the inventory of installed software packages and their version levels can be automatically cross-referenced with public vulnerability databases to proactively alert about agents running vulnerable software
- Where collected inventory data can be reviewed in the Wazuh Dashboard
- Querying inventory data via the Wazuh API

Rootkit Detection

This module covers the rootcheck component used to detect rootkits and malware and application errors. Upon completing this module you will achieve the following objectives:

- Understand how Wazuh detects both user-mode and kernel-mode rootkits.
- Learn how FIM assists with rootkit detection.
- Generate alerts when there is a discrepancy in information regarding a file, process, port, or network interface.

DAY 4

Day 4

Active Response

This module describes how to configure Wazuh to trigger actions in response to certain alerts, automating remediation of security violations and threats. Upon completing this module, you will achieve the following objectives:

- Define the active response component.
- Know the active response scripts that come by default with a standard installation.
- Differentiate between stateful and stateless commands.
- Create custom active response commands and scripts.
- Deploy active response rules tied to specific alert conditions.

Wazuh Integration System

This module provides a walkthrough of the Wazuh integration system, where Wazuh managers can be configured to locally run Wazuh-provided and/or custom scripts in response to specific types of alerts being generated. It covers the following topics:

- Configuration of the Wazuh manager to use various integrations
- Passing full alert data plus static elements like API keys or webhooks to integration scripts
- Review of Wazuh-provided integration scripts for VirusTotal, Slack, and PagerDuty, and how these can be used as templates to build your own integration scripts

Security Configuration Assessment

This module explains how Wazuh can be used for continuous self-auditing for security policy compliance. It covers the following topics:

- Choosing, customizing, and centrally managing SCA policies
- Types of checks that can be performed by SCA policies
- Pros and cons of SCA versus CIS-CAT

Cloud Security

Wazuh helps increase the security of some of the most comprehensive and broadly adopted cloud platforms such as AWS, Microsoft Azure, and GCP. In this module, the instructor will provide an overview of Wazuh's cloud security capabilities, covering monitoring across AWS, Microsoft Azure, Google Cloud, GitHub, and Office 365, including instances, platform services, audit logs, and posture management.

Sysmon Integration

This module explains how Windows Sysinternals Sysmon can be used with Wazuh for more in-depth monitoring of system activity. Wazuh enables the management of Sysmon on agents.

This module includes the following lab exercise:

- Deploy Sysmon on a Windows agent system, fully integrated with Wazuh, and use it to detect the execution of a malicious command pattern.

Docker Integration

This module describes how Wazuh can monitor Docker servers and container events. It includes the following lab exercise:

- Install Docker on an agent system, enable the docker-listener Wazuh agent module, and observe how a series of container-related actions successfully generate Wazuh alerts.

Laboratory Exercises Summary

Hands-on lab exercises are integrated throughout the course, providing practical experience with real-world scenarios:

Session 1 – Setup & Agents

- [1a] **Prepare Wazuh Server Components**
  - *Skills:* Alert levels, authentication, API connectivity
- [1b] **Navigate the Dashboard**
  - *Skills:* Dashboard exploration, interface familiarity
- [1c] **Register linux-agent**
  - *Skills:* Agent installation, self-enrollment
- [1d] **Install Windows Agent**
  - *Skills:* Windows deployment variables
- [1e] **Register via Dashboard**
  - *Skills:* Dashboard agent registration
- [1f] **Agent Upgrades**
  - *Skills:* Manager-based agent updates
- [1g] **Centralized Configuration**
  - *Skills:* Agent groups, agent.conf deployment

Session 2 – Detection & Rules

- [2a] **Brute Force Attack**
  - *Skills:* Attack simulation, alert analysis
- [2b] **Assess Several Malicious Alerts**
  - *Skills:* Alert assessment, threat analysis
- [2c] **Looking Up Rules**
  - *Skills:* Rule lookup, rule identification
- [2d] **Write a Custom Decoder**
  - *Skills:* Custom decoder creation, log parsing
- [2e] **Write a Sibling Decoder**
  - *Skills:* Sibling decoder configuration, decoder chaining
- [2f] **Wazuh's Dynamic JSON Decoder**
  - *Skills:* JSON decoding, dynamic field extraction

Session 3 – Monitoring & Inventory

- [3a] **Modify Existing Rule**
  - *Skills:* Rule frequency, alert level tuning
- [3b] **Basic Custom Rules**
  - *Skills:* Custom rule creation, testing
- [3c] **Advanced Custom Rule**
  - *Skills:* Complex rules, parent-child relationships
- [3d] **CDB Lists - Escalation**
  - *Skills:* IP reputation lists
- [3e] **SSH Watch Lists**
  - *Skills:* Dynamic CDB list usage
- [3f] **Index Lifecycle**
  - *Skills:* Index management, retention
- [3g] **Extending Pipeline**
  - *Skills:* Custom ingest pipelines
- [3h] **Customize Syscheck**
  - *Skills:* File monitoring, who-data, diff reports
- [3i] **Inventory & Vulnerability**
  - *Skills:* Package vulnerability detection
- [3j] **Rootkit Detection**
  - *Skills:* Rootkit monitoring, process cloaking

Session 4 – Response & Integrations

- [4a] **Active Response**
  - *Skills:* Firewall blocking, automated remediation
- [4b] **Slack Integration**
  - *Skills:* External notifications
- [4c] **Custom SCA**
  - *Skills:* Policy compliance checking
- [4d] **Sysmon Integration**
  - *Skills:* Advanced Windows monitoring
- [4e] **Docker Integration**
  - *Skills:* Container monitoring

wazuh.