wazuh.

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 a Wazuh HIDS/SIEM system. 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 get direct experience with many Wazuh features, and learn various ways to synergistically integrate them for advanced purposes.

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.

Intended audience

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

Duration: 4 days

Software versions:

- Wazuh 4.8.0

Prerequisites:

- Familiarity with basic IT security concepts
- Basic familiarity with Linux command line (enough to use a text editor)

Course Objectives

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

- Describe key features and components of Wazuh.
- Configure Wazuh managers and agents.
- Create new rules and decoders.
- Understand the Wazuh event/alert data pipeline including the programs, data files, and network paths involved.
- Navigate Wazuh alerts via various dashboards.
- Use Wazuh modules for security configuration compliance checks and vulnerability assessment.
- Monitor your Wazuh installation via the Wazuh web application.
- Understand how Wazuh helps with regulatory compliance (such as PCI, SOCKS, HIPAA, GDPR, etc.).
- Explore the variety of options available for pushing or pulling log content into Wazuh.

Table of Contents

Day 1
- Introduction to Wazuh
- Architecture and Secure Communication
- Deployment and Agent Registration Methods
- Wazuh Dashboard
- Agent Push Upgrades
- Wazuh Configuration

Day 2
- Log Analysis
- Wazuh Indexer and Dashboard
- Wazuh Ruleset
- Decoders and Rules
- CDB Lists
- Wazuh Ruleset Traversal
- Indexer Advanced Pipeline Configuration

Day 3
- File Integrity Monitoring
- Agent Inventory Collection and Vulnerability Detection
- Rootkit Detection
- Wazuh Integration System
- Active Response
- Security Configuration Assessment

Day 4
- MITRE ATT&CK Techniques
- Docker Integration
- Tour of Amazon CloudTrail Integration
- Osquery Integration
- Sysmon Integration
- Touring the Wazuh Manager Cluster

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 client-server Wazuh architecture, focusing on its two main components: the Wazuh manager cluster and the agents. Upon completing this module, you will achieve the following objectives:

- List and describe the basic Wazuh components on both the manager and agent sides.
- Understand how the data flows.
- Describe the communication between Wazuh components, including encryption and authentication.

Deployment and Agent Registration Methods

This module covers Wazuh installation and registration methods, including:

- Installation via packages (Windows MSI, plus yum and apt repository)

This module also describes different ways to register agents, such as:

- Self-enrollment
- Deployment variables during package installation
- Agent_auth CLI tool

This module also includes the following lab exercises:

- Install an agent on a Windows system. (Preinstalled on Linux systems).
- Register all agents using different methods.

Considerations for mass deployment and auto-registration of agents will also be addressed, as well as for upgrading agents.

Wazuh Dashboard

This module provides an initial introduction to the Wazuh dashboard. Upon completing this module you will achieve the following objectives:

- Know how to connect the Wazuh Dashboard to the Wazuh API.
- Have a basic sense of the feature set of the Wazuh Dashboard.

This module includes the following lab exercise:

- Briefly tour the app to prepare for extensive use throughout the rest of the training.

Agent Push Upgrades

This module describes how to use your Wazuh manager(s) to push upgrades to your Wazuh agent via the existing connection that agents maintain with their manager. Upon completing this module you will achieve the following objective:

- Push agent upgrades via the Wazuh API.

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.

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 Indexer and Dashboard

This module introduces the Wazuh Indexer and demonstrates the benefits of integrating the Wazuh manager with this open-source log management tool. This module covers the following topics:

- Indexing components, such as Filebeat, Wazuh Indexer and Wazuh Dashboard
- How the Wazuh user benefits from this integration
- Using the Wazuh Dashboard as the alert management console
- Overview of The Wazuh Dashboard application
- A detailed review of the Wazuh event/alert pipeline from event origination to viewing the alert in the Wazuh web interface

Wazuh Ruleset

This module describes the Wazuh ruleset and includes the following topics:

- Decoders and rules
- Diverse application coverage
- Regulatory compliance mapping

- Updating the ruleset
- Contributing to the ruleset
- In-depth exploration of the Wazuh rule hierarchy and the flow of event analysis through the ruleset

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.

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 topic:

- 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.

DAY 3

Day 3

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.
- List the different syscheck options.
- 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.

This module includes the following lab exercise:

- Set up comprehensive FIM monitoring on an agent, make changes, and observe the resulting FIM alerts.

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

The module includes the following lab exercises:

- Install an intentionally outdated and vulnerable version of a software package and observe Wazuh's alert about it.
- Explore the Wazuh Dashboard and the Wazuh API's ability to query agent inventory data.

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.

This module includes the following lab exercise:

- Install a rootkit on an agent that cloaks a process, and observe Wazuh detect and alert on it.

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

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.

The module includes the following lab exercise:

- Configure automatic firewall blocking in response to SSH brute force attacks and observe its effectiveness by brute force attacking your own agent.

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

DAY 4

Day 4

Please note that the numerous integrations listed under Day 4 are too extensive to cover in a single day. During the training, class participants will be polled to determine which integrations are most relevant to their intended or desired use cases for Wazuh. Based on the results, the most suitable topics for Day 4 will be selected.

MITRE ATT&CK Techniques

This module explains how Wazuh is mapping events against the MITRE ATT&CK framework. It covers the following topics:

- Enhancing alerts with MITRE
- Configuration example

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.

Tour of Amazon CloudTrail Integration

In this module, the instructor will give a tour of AWS administrative events collected by the Wazuh aws-s3 module. This will include a review of the necessary module configuration, and an observation of the collected events via the Wazuh AWS dashboard.

Osquery Integration

This module describes how Wazuh agents can use Osquery as a subagent for deeper audit insights. Wazuh facilitates the management of Osquery agents, distribution of Osquery configurations, scheduled execution of queries, and routing of results to the manager.

This module includes the following lab exercise:

- Set up an Osquery scenario to track the appearance of new Chrome extensions on Windows systems and another to monitor the appearance and disappearance of Linux user accounts. Simulate these events and observe how Wazuh alerts on them.

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.

Touring the Wazuh Manager Cluster

In this module, the instructor will demonstrate the transition from a single-manager setup to a multi-node Wazuh manager cluster. Then state and configuration changes will be traced live as agent state information makes its way up to the master node manager and config changes on the master node manager make their way down the worker node managers and then to individual agents. Special considerations for environments using Wazuh manager clusters will also be addressed and discussed.