wazuh.

Wazuh for Security Engineers

- 4 days Course -

- 4 days 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. Special focus is given to the tuning of the Wazuh ruleset through the creation of custom rules and decoders. You will get direct experience with many of the Wazuh features, and learn many ways to bring these features together synergistically 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 along with procedures laid out in provided lab guides, to exercise the features in focus throughout the training. Throughout the duration of the course, you will have unrestricted access to your lab environment which will continue to be available for additional practice for 24 hours after the class ends. Comprehensive course materials containing theory and practical exercises will be provided during the course. Copies of the slide decks will also be provided 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 4.6.0

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 and 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…)
- Understand the variety of options available for pushing or pulling log content into Wazuh.

Table of Contents

Day 1

Day 2

Day 3

Day 4

- 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 little bit of background on the project itself.

Architecture and secure communication

This module describes the client-server Wazuh architecture and focuses on the two main components: the Wazuh manager cluster and the agents. Upon completing this module you will meet these objectives:

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

Deployment and agent registration methods

This module describes the Wazuh installation. It includes:

- 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 includes the following lab exercises:

- Install an agent on a Windows system. It is 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 meet these 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 exercises:

- Briefly tour the app in preparation for heavy use of the app during the rest of the training.

Agent push upgrades

This module describes how to use your Wazuh manager(s) to push Wazuh agent upgrades to your agents via the existing connection that agents hold open to their manager. Upon completing this module you will meet these objectives:

- Push agent upgrades via the Wazuh API.

Wazuh configuration

This module describes basic Wazuh configuration and shows how to push the configuration from manager to manager to agents. Upon completing this module you will meet these objectives:

- Identify the files where the configuration occurs, like ossec.conf and agent.conf, as well as which files and configuration categories can be centrally distributed vs individually maintained on a manager or agent.
- Know how to make configuration changes via the web app or command line.
- Understand the basic categories of configuration settings for managers and agents.
- Understand how configurations are propagated between managers and from managers to agents.
- Know how to use agent groups and profiles to organize the propagation of the right configuration elements to the right agents, even when huge numbers of agents are involved.

This module includes the following lab exercise:

- Manage your Wazuh manager primary configuration and internal options.
- Centralized agent configuration using agent groups and profiles.

- DAY 2 -

Day 2

Log Analysis

This module describes the log analysis component and how log messages flow agents to the manager. Upon completing this module you will meet these 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 following 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 helps with 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
- Looking up and tracing Wazuh rules for better understanding

Wazuh Indexer and dashboard

This module provides an introduction to Wazuh Indexer and shows the benefits of integrating the Wazuh manager with this open source log management tool. This module includes these topics:

- Indexing components, such as Filebeat, Wazuh Indexer and Wazuh Dashboard
- How does the Wazuh user benefit from this integration
- Using Wazuh Dashboard as the alert management console
- The Wazuh Dashboard app
- A detailed review of the Wazuh event/alert pipeline from event origination to the viewing of an alert about that event in the Wazuh web interface

Wazuh ruleset

This module describes the Wazuh ruleset. It includes these topics:

- Decoders and rules
- Diverse application coverage
- Regulatory compliance mapping
- Updating the ruleset
- Contributing to the ruleset

- Deep exploration of the Wazuh rule hierarchy and the flow of event analysis through the ruleset

Decoders and Rules

This module describes the different types of rules and decoders that Wazuh uses. You will learn to create rules for your own applications. Upon completing this module you will meet these objectives:

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

This module includes 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 the frequency and/or alert level
- Write a custom decoder for a specific log message
- Write custom rules that match a specific log message and assign an alert level
- Write an advanced custom rule based on an existing SSHD rule.
- Deploy Suricata on an agent and have Wazuh consume and alert on its JSON logs

CDB lists

This module includes the following topics:

- CDB list lookups from within rules
- Use cases for CDB lists
- File paths and line format for CDB lists
- Creation of new rules to use CDB lists

This module includes the following lab exercises:

- Escalate sshd alerts about known attackers' IPs
- Build 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 fits specific criteria.

Wazuh Ruleset Traversal

This module includes the following topic:

- Deep-dive into how the analysis engine hierarchically traverses through the ruleset while analyzing an event
- This is critical to understand well, to be able to successfully deploy custom escalation and whitelisting rules to tune the Wazuh ruleset to do what you need in your specific environment.

Indexer advanced pipeline configuration

This module includes the following topic:

- 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 exercises:

- Deploy an advanced ingest node pipeline and observe it at work in your live alert stream.

- DAY 3 -

Day 3

File Integrity Monitoring

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

- Understand how syscheck detects file changes
- List the different syscheck options
- Configure syscheck to do real-time detection
- Know how to set up syscheck for who-data collection and file change diff reporting
- Exclude files that change very often from syscheck monitoring

This module includes the following lab exercise:

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

Agent Inventory Collection and Vulnerability Detection

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

- How Wazuh agents can 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 of inventory data via the Wazuh API

This module includes the following lab exercise:

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

Rootkit Detection

This module describes how the rootcheck component can be used to detect rootkit and malware as well as application errors. Upon completing this module you will meet these objectives:

- Understand how Wazuh detects both user mode and kernel mode rootkits
- Understand how FIM helps 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 involves a walkthrough of the Wazuh integration system in which Wazuh managers can be configured to locally run Wazuh-provided and/or custom scripts in response to specific types of alerts being generated. It includes these topics:

- Configuration of the Wazuh manager to use various integrations
- Passing of full alert data plus static elements like API key or webhooks to integration scripts
- Review of the Wazuh-provided VirusTotal, Slack, and PagerDuty integration scripts, and how they can also be used as a template to build your own integration scripts.

Active response

This module describes how to configure Wazuh to trigger actions in response to certain alerts in order to automate remediation to security violations and threats. Upon completing this module you will meet these objectives:

- Define the active response component
- Know the active response scripts that come by default with a standard installation
- Differentiate between a stateful vs stateless command

This module includes the following lab exercise:

- Configure automatic firewall blocking in response to ssh brute force attacks and observe it works by brute force attacking your own agent.

Security Configuration Assessment

This module describes how Wazuh can be used for continuous self-auditing for security policy compliance.

- Choosing, customizing, and centrally SCA policies
- Types of checks that can be performed by SCA policies
- Pros and Cons of SCA vs CIS-CAT

- DAY 4 -

Day 4

Note that the many different integrations listed under day 4 are too numerous to address in a single day. Class participants will be polled during the training as to which integrations would be most relevant to their intended/desired use cases for Wazuh, and based on the findings, the best fit of topics for day 4 will be determined.

MITRE ATT&CK techniques

This module describes how Wazuh is mapping events against the MITRE ATT&CK framework.

- Enhancing alerts with MITRE
- Configuration example

Docker integration

This module describes how Wazuh can monitor Docker servers and container events.

This module includes the following lab exercise:

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

Tour of Amazon CloudTrail integration

In this module, the instructor gives a tour of AWS administrative events collected by the Wazuh aws-s3 module. This will include a review of the needed module configuration, plus observing such collected events via the Wazuh AWS dashboard.

Osquery integration

This module describes how Wazuh agents can use Osquery as a subagent for deeper audit insight. Wazuh enables management of Osquery agents, distribution of Osquery configs, scheduled execution of queries, and routing of the 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 one to track the appearance and disappearance of Linux user accounts. Simulate those events and observe Wazuh alerting about them.

Sysmon integration

This module shows how Windows Sysinternals Sysmon can be used with Wazuh for deeper monitoring of system activity. Wazuh can be used to manage Sysmon on agents.

This module includes the following lab exercise:

- Deploy Sysmon on the 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 moving 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 that must be addressed for environments using Wazuh manager clusters will also be addressed and discussed.