info@wazuh.com
https://wazuh.com

Wazuh for Security Engineers – 3-day course

Overview

This three-day training course is designed for security engineers and consultants responsible for implementing, configuring and operating the Wazuh security platform. The course focuses on the different components and the best practices to get the most out of them. It also equips participants with the right set of tools to modify and create their own rules and decoders in order to customize detection capabilities. Additionally, we will demonstrate and teach the different capabilities, new features and usability.

This course is a combination of lectures and hands-on exercises for which an online environment will be provided. The online exercises teach you to perform tasks by viewing a demonstration and then completing the tasks in the provided lab environment. This environment will be made available for 24 hours after the class for additional practice. Comprehensive course materials containing theory and practical exercises will be provided during the course as well.

Intended audience

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

Duration 3 days

Software version

- Wazuh 3.11.2

Prerequisites

- Familiarity with Linux commands
- Basic familiarity with IT security content

Course Objectives

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

- Describe the key features and components of Wazuh
- Describe the architecture of Wazuh
- Deploy and configure Wazuh
- Create or customize rules and decoders
- Manage Wazuh alerts
- Perform administrative tasks
- Use Elastic Stack to monitor Wazuh alerts
- Analyze Kibana dashboards and create your own
- Use the Wazuh app for Kibana to manage your Wazuh installation
- Understand how Wazuh helps with PCI DSS compliance and other regulations
- Monitor AWS infrastructure

Table of Contents

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 Wazuh client-server 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 different processes taking place on both the agent side and the manager side
- Understand how the data flows
- Describe the communication among Wazuh's components. 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:

- Manual method
- Using authd for automated registration
- Using the Wazuh RESTful API
- Using deployment variables to install, register and configure agents

This module includes the following lab exercises:

- Install an agent on both a Windows and a Linux machine
- 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 app for Kibana

This module provides an initial introduction to the Wazuh Kibana app. Upon completing this module you will meet these objectives:

- Know how to connect the Wazuh Kibana app to the Wazuh API
- Have a basic sense of the feature set of the Wazuh Kibana app

This module includes the following lab exercises:

- Connect the preinstalled Wazuh Kibana app to the Wazuh API on your manager
- Briefly tour the app in preparation for heavy use of the app during the rest of the training

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:

- Centralized agent configuration using agent groups and profiles

Log Analysis

This module describes the log analysis component and how log messages flow from 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 the log message flows
- Understand the following analysis phases: pre-decoding, decoding and rules
- 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 the following 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

Elastic Stack integration

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

- Elastic Stack components, such as: Filebeat, Elasticsearch, and Kibana
- How the Wazuh user benefits from this integration
- Using Kibana as the alert management console
- The Wazuh Kibana app

Day 2

Rules and Decoders

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

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

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 for 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 Kibana app
- 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 the alert generated by Wazuh in response
- Explore the Wazuh Kibana app's 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

Day 3

Note that the many different integrations listed under day 3 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 3 will be determined.

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.

Active response

This module describes how to configure Wazuh to trigger actions in response to certain alerts in order to automate remediation of 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 how it works by brute force attacking your own agent.

Hacking Wazuh

This module describes how to troubleshoot and debug Wazuh. It includes the following topics:

- Monitoring network communications between the manager and the agents using tcpdump
- Monitoring files that are in-use by Wazuh processes using lsof
- Monitoring process communication between the agent and manager using strace
- Monitoring open sockets of Wazuh processes using netstat

VirusTotal FIM integration

This module describes Wazuh's module that queries VirusTotal about new or changed files that are subject to FIM monitoring.

This module includes the following lab exercise:

- Configure your manager to perform VirusTotal FIM lookups, and then test it by installing simulated malware into an agent in a FIM-monitored directory.

Slack integration

This module describes how Wazuh can generate Slack messages in response to specific Wazuh alerts.

This module includes the following lab exercise:

- Join the Wazuh training Slack channel and then configure your manager to forward ssh brute force alerts to Slack, observing the messages in the Slack channel after triggering such an alert.

Extending the Wazuh Integration System

This module describes how the Wazuh manager can run any custom script you like, in response to specific Wazuh alerts, passing along the entire event to the script to be acted upon. It includes these topics:

- How to configure the manager(s) to use your custom integration script
- How to use the existing VirusTotal, Slack, or PagerDuty integration script as a template to build your own integration script.

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.

OpenSCAP integration

This module describes the OpenSCAP integration done at an agent level. Upon completion of this module you will meet these objectives:

- Understand how integration, configuration and files location work
- Use OpenSCAP to ensure the system is configured according to certain standards, such as CIS benchmarks
- Use OpenSCAP to detect vulnerabilities in a system
- Use OpenSCAP to meet PCI requirements

This module includes the following lab exercises:

- Deploy OpenSCAP on a Linux agent and peruse the scan results
- Build a Wazuh exclusion rule to silence a specific OpenSCAP finding

Tour of Amazon CloudTrail Integration

In this module, the instructor gives a live demonstration of collecting AWS administrative events via the aws-s3 module on Wazuh manager. This will include review of the needed module configuration, generating some events, and then observing the alerts generated about them in the Wazuh Kibana app.

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 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.