Suggested Background

Wazuh Advanced Training

Reference guide for prospective participants

Classification: Course participants

1. Introduction

The Wazuh Advanced Training builds directly on the Wazuh Essential Training. It assumes participants already operate Wazuh in a real or lab environment and focuses on advanced configuration: authentication and access control, platform modules, threat intelligence integrations, cloud and API administration, and AI-assisted operations.

The course involves programmatic interaction with the platform, external identity providers, cloud services, and third-party security tools. For participants to get the most out of the training, it is important to arrive with hands-on Wazuh experience and a working knowledge of the surrounding technologies covered below.

This document describes those prerequisites. It does not set a formal admission level or propose a leveling program: its purpose is transparent and practical.

2. Who Is This Document For?

This guide is intended for any professional considering starting the Wazuh Advanced Training. Typical profiles include:

- Security engineers and SOC analysts who completed the Wazuh Essential Training and now operate Wazuh in production.
- Wazuh administrators who manage a live deployment and want to extend it with authentication, integrations, and API-driven automation.
- SOC team leads designing multi-tenant dashboards, reporting, and threat intelligence workflows on top of Wazuh.
- Engineers evaluating AI-assisted security operations who already have hands-on Wazuh experience.

Regardless of the profile, what defines readiness is not the job title or years of experience, but hands-on familiarity with the Wazuh platform and working knowledge of the technologies it integrates with.

3. Required Knowledge for the Course

The following describes the five knowledge areas we consider fundamental for following the Advanced Training without difficulty. Each area includes a description of what the participant should be able to do independently.

3.1 Wazuh Platform Experience

The Advanced Training does not reintroduce Wazuh basics. Participants are expected to already operate a Wazuh deployment, ideally gained through the Essential Training or equivalent hands-on experience. The two subsections below list the specific skills expected in the Dashboard and at the manager and agent level.

What you should be able to do in the Wazuh Dashboard

The participant must be able to:

- ✓ Navigate the Wazuh Dashboard and locate alerts from at least three different modules, such as FIM, vulnerability detection, and SCA.
- ✓ Use Dashboard search, filters, and saved views to narrow down a set of alerts.
- ✓ Explain the role of the Wazuh indexer, Wazuh server, and Wazuh Dashboard within the platform architecture.

What you should be able to do with the Wazuh server and agents

The participant must be able to:

- ✓ Edit ossec.conf on the Wazuh server or an agent and restart the corresponding service after a change.
- ✓ Create a local user account and assign it a role through the Security plugin.
- ✓ Locate the Wazuh server logs (ossec.log) and identify a startup or connection error.
- ✓ Differentiate between a decoder and a rule when reading an existing ruleset entry.

3.2 Identity, Access, and Authentication Concepts

The Advanced Training configures role-based access control and connects external identity providers to the Wazuh platform. A working vocabulary of access-control concepts makes this module easier to follow.

What you should be able to do

The participant must understand:

- ✓ What role-based access control (RBAC) means and how it differs from per-user permissions.
- ✓ What a directory service such as LDAP or Active Directory is used for.
- ✓ What single sign-on (SSO) means and the role of an external identity provider (IdP) in a SAML flow.
- ✓ What multi-factor authentication (MFA) is and why it reduces credential risk.
- ✓ What a TLS certificate does when it secures a login page.

3.3 APIs, Automation, and Data Formats

Several Advanced modules operate the platform programmatically through the Manager API, the Wazuh-indexer API, and custom integration scripts. Comfort with REST APIs and structured data formats is expected going in.

What you should be able to do

The participant must understand:

- ✓ What an API is, and specifically what makes an API "RESTful."
- ✓ What a tool such as curl or Postman is used for when testing an API.
- ✓ What JSON is and how data is structured as key-value pairs.
- ✓ What a JWT or API token is used for.
- ✓ What YAML is and how it differs from JSON.
- ✓ What a Bash or Python script is and why scripting helps automate a repetitive task.

3.4 Cloud, Containers, and Kubernetes Fundamentals

Wazuh ingests logs from cloud providers and monitors containerized and Kubernetes workloads. Participants should already be comfortable navigating these environments, even without deep administration experience.

What you should be able to do

The participant must understand:

- ✓ What IAM (Identity and Access Management) means in a public cloud account.
- ✓ What a cloud audit log — such as AWS CloudTrail or Azure Log Analytics — records.
- ✓ What a container is and how it differs from a virtual machine.
- ✓ What Kubernetes is, and what a pod, node, and API server are.

3.5 Threat Intelligence and Security Analysis Concepts

The course integrates Wazuh with external threat intelligence sources. Familiarity with the underlying concepts lets participants focus on the Wazuh-specific configuration rather than the terminology.

What you should be able to do
The participant must understand: ✓ What an Indicator of Compromise (IoC) is. ✓ What the MITRE ATT&CK framework is used for. ✓ What YARA is and what a "rule" means in that context. ✓ What MISP is and what a threat intelligence feed does. ✓ What VirusTotal is and what a file-reputation lookup means.

4. Recommended Knowledge (Non-Exclusive)

The items listed below are not requirements to start the course. However, those who master them will move faster through the Advanced labs.

Helpful, but not required
✓ Scripting beyond the basics in Python or Bash — useful for building and modifying custom Wazuh integrations and wodles. ✓ OpenSearch or Elasticsearch query syntax — helps when building custom visualizations and troubleshooting the Wazuh indexer. ✓ Hands-on exposure to a public cloud console (AWS, Azure, or GCP) beyond IAM — speeds up the cloud ingestion labs. ✓ Familiarity with generative AI APIs, such as OpenAI or a similar provider — relevant for the AI-assisted operations module. ✓ Prior SOC or incident response experience — helps contextualize the threat intelligence and detection labs.

5. Readiness Self-Assessment

The following questionnaire will help you objectively identify which areas you are solid in and where you might need to strengthen before starting. Mark **Yes** only when you can perform the action without direct assistance.

#	Action or knowledge	Yes / No
1	I have deployed or operated a Wazuh manager and at least one agent in a real or lab environment.	☐
2	I can navigate the Wazuh Dashboard and locate alerts from at least three different modules.	☐
3	I can edit ossec.conf and restart the corresponding Wazuh service after a configuration change.	☐
4	I can differentiate between a decoder and a rule when reading a Wazuh ruleset entry.	☐
5	I am comfortable administering a Linux server from the command line (services, permissions, package management).	☐
6	I understand what role-based access control (RBAC) is and how permissions map to roles.	☐
7	I know the basic difference between LDAP/Active Directory authentication and SAML single sign-on.	☐
8	I can make an authenticated REST API call and interpret a JSON response.	☐
9	I understand what a JWT or API token is and how it is used to authenticate a request.	☐
10	I can read and edit a JSON or YAML file without breaking its structure.	☐
11	I can write a short Bash or Python script to automate a repetitive task.	☐
12	I have basic familiarity with a public cloud console, including its IAM and logging services.	☐
13	I understand what a Docker container is and can view logs from a running container.	☐
14	I know the basic building blocks of Kubernetes, such as pods, nodes, and the API server.	☐
15	I can explain what an Indicator of Compromise (IoC) is and give concrete examples.	☐

#	Action or knowledge	Yes / No
16	I am familiar with the MITRE ATT&CK framework and how it classifies adversary techniques.	☐
17	I understand, at a conceptual level, how a signature-based tool like YARA scans for malware patterns.	☐
18	I understand what a threat intelligence feed is and how it enriches security alerts.	☐
19	I can follow a multi-step technical lab involving several interconnected systems without losing track of state.	☐
20	I am comfortable working with English-language technical documentation and command-line tools.	☐

Interpreting the Results

Add up the total affirmative answers and consult the following table:

Result	Interpretation
17–20 Yes answers	Ready profile. Starting the Advanced Training is recommended without the need for prior reinforcement.
13–16 Yes answers	Functional profile. Reinforcing specific areas — most likely identity and access, APIs, or cloud concepts — before or during the first sessions is recommended.
0–12 Yes answers	Building profile. Consolidating hands-on Wazuh experience is advisable before starting the Advanced Training. Revisiting the Wazuh Essential Training, or the linked resources in this guide, will help you get the most out of the course.

Remember: this questionnaire is a self-diagnosis tool, not an admission filter. Its value lies in helping you arrive at the course in the best possible condition.

6. Final Note

The Wazuh Advanced Training builds on hands-on Wazuh experience to teach advanced configuration: authentication and access control, platform modules, integrations, threat intelligence, cloud and API administration, and AI-assisted operations.

No prior experience with these advanced capabilities is required - that is the objective of the course, not a prerequisite.

What does matter is arriving with a working Wazuh deployment already under your belt and a working knowledge of the surrounding technologies it integrates with. The stronger that foundation, the more you will get out of each session.

If you have questions about your readiness or want to consult prior study resources, you can contact the training team at:
wazuh.com/services/training-courses