wazuh.

Suggested Background

Wazuh Essential Training

Reference guide for prospective participants

Classification: Course participants

1. Introduction

The Wazuh Essential Training is designed to teach the Wazuh platform from the ground up. Therefore, no prior experience with Wazuh or any of its specific modules, processes, or components is required.

However, the course involves working with real environments: operating systems, networks, services, and security event analysis. For participants to get the most out of the training, it is important to have a solid foundation in general technology before starting.

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 or student considering starting the Wazuh Essential Training. Typical profiles include:

- IT professionals with an interest in cybersecurity and monitoring.
- Students or recent graduates in systems, networking, or information security programs.
- SOC analysts in the early stages of their careers.
- System administrators looking to add detection and response capabilities to their skill set.

Regardless of the profile, what defines readiness is not the job title or years of experience, but mastery of a set of fundamental technical skills.

3. Required Knowledge for the Course

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

3.1 Operating Systems (Linux and Windows)

Wazuh is deployed primarily in Linux environments, but also monitors Windows agents. Because the labs touch both systems, you should be able to operate each one with basic proficiency. The two subsections below list the specific skills for Windows and Linux.

What you should be able to do on Windows

The participant must be able to:

- ✓ Connect via RDP and navigate the system interface.
- ✓ Open PowerShell and run basic administration commands.
- ✓ Review the Event Viewer and find relevant entries.

What you should be able to do on Linux

The participant must be able to:

- ✓ Navigate the file system and manage relative and absolute paths.
- ✓ Edit plain text configuration files (vi, nano, or another editor).
- ✓ Start, stop, and verify the status of services (systemctl, service).
- ✓ Install packages using your distribution's package manager (apt, yum, dnf).
- ✓ Review file permissions and adjust them when necessary.
- ✓ Connect to a remote server via SSH and run basic commands.
- ✓ Identify error messages in system logs (/var/log).

3.2 Networks and Communications

Wazuh involves communication between the server and deployed agents. Understanding networking fundamentals is key to diagnosing issues during installation and configuration.

What you should be able to do

The participant must be able to:

- ✓ Distinguish among IP address, port, and protocol, and understand how each affects connectivity.
- ✓ Validate the DNS resolution and verify that a hostname resolves correctly.

- ✓ Use basic diagnostic tools: ping, nslookup, traceroute, netstat, ss.
- ✓ Access a remote system via SSH or RDP for basic checks.
- ✓ Differentiate whether a failure is a network or application issue.

3.3 Data, Logs, and Formats

A large part of the practical work in Wazuh involves ingesting, interpreting, and analyzing events. Logs are the raw material of the SIEM. Those who cannot read them fluently will have difficulty in the course labs.

What you should be able to do

The participant must be able to:

- ✓ Recognize the minimum structure of a log: timestamp, source, event type, and content.
- ✓ Read and interpret JSON and syslog events, identifying their key fields.
- ✓ Use search and filtering commands in the console: grep, awk, cat, and less.
- ✓ Identify which fields of an event are useful for an investigation.
- ✓ Detect inconsistencies or missing data in a set of events.

3.4 Information Security Fundamentals

Wazuh is a security platform. To get the most out of it, participants need a basic vocabulary and a risk perspective from which to interpret what is happening in monitored systems.

What you should be able to do

The participant must be able to:

- ✓ Differentiate between normal, suspicious, and critical activity in an IT environment.
- ✓ Understand concepts such as vulnerability, severity, attack vector, and exposure surface.
- ✓ Recognize basic threat patterns: brute force, privilege escalation, and exfiltration.
- ✓ Justify why an event deserves attention and what the next step would be.
- ✓ Classify incidents by response priority.

3.5 Technical Work Methodology

The Essential Training includes lab exercises that require following precise procedures and validating results at each step. The ability to work in an organized manner is as important as technical knowledge.

What you should be able to do

The participant must be able to:

- ✓ Follow a multi-step technical guide without losing order or skipping stages.
- ✓ Record the changes made and how you validated each result.
- ✓ Resume work from a known point if something fails (conceptual rollback).

4. Recommended Knowledge

The items listed below are not requirements to start the course. However, those who master them will progress faster in the more advanced training labs.

Basic regular expressions (regex) — useful for creating custom decoders and rules in Wazuh.
Editing XML, YAML, or JSON files — many Wazuh configurations are expressed in these formats.
Reading technical documentation in English — Wazuh documentation, rules, and decoders are primarily in English; the ability to read basic-to-intermediate technical English makes the labs easier to follow.
Basic familiarity with web browsers — navigating dashboards, using filters and search, and working with web-based interfaces such as the Wazuh Dashboard, where much of the lab work takes place.

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 can connect via SSH to a Linux system and run basic commands.	☐
2	I can connect via RDP to a Windows system and open PowerShell.	☐
3	I understand what a port is and how it affects connectivity between services.	☐
4	I can verify whether a service is active and restart it safely.	☐
5	I can edit a configuration text file in Linux without breaking its structure, using a terminal text editor such as nano or vi.	☐
6	I can use log search commands to locate errors (grep, less, tail).	☐
7	I can interpret a simple JSON event and identify its main fields.	☐
8	I can identify source and destination in a network event.	☐
9	I understand the difference between an informational event and one that indicates risk.	☐
10	I know the concept of repeated access attempts (brute force) and its indicators.	☐
11	I can install basic packages on Linux using my distribution's package manager.	☐
12	I can review and adjust file permissions when necessary.	☐
13	I can run basic PowerShell commands to manage files and processes.	☐
14	I can diagnose whether a failure is a network or application issue and formulate hypotheses.	☐
15	I can follow a multi-step technical guide without losing order.	☐
16	I can record what I changed and how I validated the result.	☐
17	I can read basic technical documentation in English.	☐
18	I know basic concepts of vulnerability and severity in cybersecurity.	☐
19	I can work in a lab environment while following good operational practices.	☐
20	I am willing to solve problems through testing, analysis, and iterative validation.	☐

Interpreting the Results

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

Result	Interpretation
17–20 Yes answers	Ready profile. Starting the course is recommended without the need for prior reinforcement.
13–16 Yes answers	Functional profile. Reinforcing specific areas before or during the first sessions is recommended.
0–12 Yes answers	Building profile. Some targeted preparation in the weaker areas - a few of the linked resources in this guide, alongside the course itself - will help you get the most out of the training. Because the Essential Training teaches Wazuh from the ground up, these gaps are a starting point, not a barrier.

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 Essential Training teaches Wazuh from the ground up.

No prior experience with the platform, its modules, its architecture, or its internal configuration processes is required. All of that content is an objective of the course, not a prerequisite.

What does matter is arriving with a solid technical foundation in systems, networks, logs, and general security. The stronger the 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