+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 08/18/2026

Sign Up

# Imperva Web Security Associate Certification Training

3 days (21 hours)

## Overview

The Imperva Web Security Associate certification validates your ability to master the fundamentals of web application protection, WAFs, and Imperva defense mechanisms. This training course provides targeted preparation for the official exam, with a focus on understanding, configuration, and validation of your knowledge.

Our Imperva Web Security Associate Certification training allows you to go beyond the essentials to solidify the skills required for working in Imperva environments and securing applications exposed to the Internet.

You will learn to understand the solution’s architecture, identify the main web attack vectors, configure basic protections, and interpret detection, logging, and alert handling mechanisms.

Upon completion of the training, you will be able to approach the IWSA exam systematically, connect application security concepts to real-world uses of the platform, and answer certification questions with greater confidence.

This preparation also covers practical scenarios, analytical skills, and best practices required to pass an intermediate-level certification in an operational context.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

## Objectives

- Understand where the Imperva Web Security Associate certification fits into the certification path.
- Master the principles of web application security and WAF protection.
- Identify the key features of the Imperva platform for securing applications.
- Effectively prepare for the official IWSA exam with a certification-focused approach.
- Apply best practices for configuration, monitoring, and troubleshooting to real-world scenarios.

# Target Audience

- Cybersecurity Engineer
- Security administrator
- Application security consultant
- SOC Analyst
- Security Architect

# Prerequisites

- Basic knowledge of networks, HTTP, and web architecture.
- Understanding of application security challenges and common web attacks.
- Prior experience with an Imperva environment or a WAF solution is preferred.
- Basic knowledge of system administration and monitoring a security platform.

# Technical Prerequisites

- A recent computer with an up-to-date browser and a comfortable workspace for the hands-on sessions.
- A stable Wi-Fi or Ethernet connection for remote sessions and demonstrations.
- A browsing environment compatible with training materials, PDFs, and guided exercises.
- A microphone and headset if the session is attended in a virtual classroom.
- Access to an Imperva demo or lab environment, if applicable, depending on the course format.

# Curriculum for our Imperva Web Security Associate Training

## [Day 1 - Morning]

### Certification Fundamentals

- Understand the scope of the Imperva Web Security Associate certification.
- Identify the requirements of the official exam and the expected level of proficiency.
- Review the basics of web security, WAFs, and common threats.
- Position the Imperva solution within an application protection strategy.
- Link key concepts to recurring topics on the exam.
- Hands-on workshop: mapping out the knowledge areas to review for the IWSA exam.

[Day 1 - Afternoon]

## Architecture and Components

- Describe the general architecture of an Imperva solution for web protection.
- Understand the role of the collection, analysis, and decision-making components.
- Distinguish between legitimate traffic flows and suspicious behavior.
- Understand the operating principles of a protection policy.
- Connect the concepts of authentication, logging, and operational visibility.
- Hands-on workshop: Analyze an architectural diagram and identify security control points.

[Day 2 - Morning]

## Application Protection

- Examine the main categories of attacks on web applications.
- Understand how a WAF detects and blocks attacks.
- Examine rules, exceptions, and profiling mechanisms.
- Understand how to manage false positives in a production environment.
- Link protection use cases to business needs and technical constraints.
- Hands-on workshop: assess multiple attack scenarios and select the appropriate protection response.

[Day 2 - Afternoon]

## Configuration and Monitoring

- Discover the essential settings of an Imperva security policy.
- Understand logging, alerting, and event monitoring options.
- Analyze key metrics for day-to-day management.
- Learn how to interpret alerts and prioritize actions.
- Reinforce the diagnostic skills required for the exam.
- Hands-on workshop: Read activity logs and identify relevant security events.

[Day 3 - Morning]

## Targeted review and practice

- Review the most important concepts in the form of a structured summary.
- Reinforce the technical vocabulary related to the IWSA certification.
- Explore the connections between theory, configuration, and use cases.
- Identify common exam pitfalls and reading errors.
- Put into perspective the topics most likely to be tested.
- Hands-on workshop: Take a practice quiz with answers on the key chapters of the certification.

## [Day 3 – Afternoon] Final

### exam preparation

- Organize a final review session before taking the certification exam.
- Adopt a method for quickly scanning questions and distractors.
- Manage time, prioritize questions, and double-check answers.
- Review key considerations related to web security and monitoring concepts.
- Finalize your personal strategy for taking the Imperva Web Security Associate exam.
- Hands-on workshop: Simulate an exam session and review answers with explanations.

# Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

# Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

# Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

# Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

# Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

# Certification

A certificate will be issued to each trainee who has completed the entire training program.