+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 Specialist (IWSS) Certification Training

3 days (21 hours)

Overview

The Imperva Web Security Specialist certification validates your ability to secure web applications with Imperva, master WAF protection mechanisms, bot management, and API security, and prepare for an exam focused on operational expertise.

Our Imperva Web Security Specialist (IWSS) Certification Training course helps you prepare for the official certification, with a focus on the skills required in a production environment.

You will learn to understand the solution’s architecture, analyze web attack vectors, configure protection policies, and leverage key detection and mitigation features.

The training also emphasizes exam preparation, analyzing security scenarios, best practices for configuration, and the mindset required to accurately answer certification questions.

Upon completion of the course, you will be able to strengthen the security of an application perimeter, better manage Imperva protections, and approach the exam with a structured and operational mindset.

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

Objectives

- Understand the functional scope of Imperva Web Security and its use cases.
- Identify major web threats, including OWASP attacks, bots, and API abuse.
- Configure the main protection, detection, and response mechanisms.
- Utilize WAF, logging, and monitoring features to secure an application.
- Effectively prepare for the format and requirements of the IWSS certification.
- Apply best practices for hardening and validation in the context of certification.

Target Audience

- Application Security Engineer
- Security administrator
- SOC Analyst
- Cybersecurity Consultant
- Application Security Manager

Prerequisites

- Basic knowledge of web security and application protection.
- Understanding of HTTP attacks, OWASP, and application filtering mechanisms.
- Previous experience with a WAF or application security solution.
- Understanding of network principles, proxies, DNS, and application traffic.
- Experience administering production or pre-production environments.

Technical Requirements

- A recent computer with at least 8 GB of RAM and an up-to-date browser.
- A stable Wi-Fi or Ethernet internet connection for demonstrations and exercises.
- Access to a work environment compatible with the web consoles used during the training.
- A microphone and headset if the session is held remotely.
- A local environment capable of viewing security captures, exports, and logs.

Curriculum for our Imperva Web Security Specialist (IWSS) Training

[Day 1 - Morning]

Fundamentals of the Solution

- The role of Imperva Web Security in an application protection strategy.
- Review of key concepts: WAF, web protection, traffic inspection, and security policies.
- Overview of the platform’s components and their role in the overall architecture.
- Review of the main threat scenarios covered by the solution.
- Preparation for the vocabulary and recurring concepts of the IWSS exam.

- Hands-on workshop: getting started with the interface, locating essential menus, and reviewing an initial dashboard.

[Day 1 - Afternoon] Web

Threats and Protections

- Analysis of the most common application attacks, including injections and control bypasses.
- Understanding the different types of security signatures, rules, and exceptions.
- Managing false positives and balancing protection with service continuity.
- Introduction to behavioral and contextual detection mechanisms.
- Review of typical scenarios encountered in a web security-focused certification exam.
- Hands-on workshop: identifying multiple malicious requests and selecting the appropriate protective response.

[Day 2 - Morning] Policy

Configuration

- Developing a security policy based on business requirements.
- Configuring filtering rules, exceptions, and alert thresholds.
- Managing application profiles and trust zones.
- Analyzing logs, events, and alerts to refine the security posture.
- Best practices for validation before going live.
- Hands-on workshop: Create a simple policy, adapt it to real-world scenarios, and verify its impact.

[Day 2 - Afternoon]

Bot Management and API Security

- Understanding automated attacks and misuse of web applications.
- Distinguishing between human traffic, simple bots, and advanced bots.
- Principles of API protection and monitoring suspicious calls.
- Interpreting signals to detect abnormal behavior.
- Mitigation use cases based on the observed risk level.
- Hands-on workshop: Analyzing a set of requests and prioritizing behaviors to address.

[Day 3 - Morning]

Operations and Monitoring

- Monitoring security activity and interpreting metrics useful for operations.

- Interpreting events, traces, and alerts to classify an incident.
- Using reports to manage security and document decisions.
- Managing changes and monitoring the impact of policy adjustments.
- Review of key points frequently assessed on the exam.
- Hands-on workshop: analyzing an incident scenario and producing a well-reasoned security analysis.

[Day 3 - Afternoon]

Intensive exam preparation

- Structured review of key IWSS concepts and common areas of weakness.
- Putting certification questions into context with operational use cases.
- Strategies for speed reading, eliminating distractors, and time management.
- Review of vocabulary, configuration, and diagnostic points.
- Methodological tips for ensuring accurate answers during the exam.
- Hands-on workshop: mock exam with annotated grading and reinforcement of learned material.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technology or to acquire specific professional knowledge or modern methods.

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.