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

Mis à jour le 18/08/2026

S'inscrire

Formation Certification Imperva Web Security Specialist (IWSS)

3 jours (21 heures)

Présentation

La certification Imperva Web Security Specialist valide votre capacité à sécuriser des applications web avec Imperva, à maîtriser les mécanismes de protection WAF, bot management et API security, et à préparer un examen orienté expertise opérationnelle.

Notre formation Certification Imperva Web Security Specialist (IWSS) vous accompagne dans la préparation de la certification officielle, avec une approche centrée sur les compétences attendues en environnement de production.

Vous apprendrez à comprendre l'architecture de la solution, à analyser les vecteurs d'attaque web, à configurer les politiques de protection et à exploiter les fonctions clés de détection et de mitigation.

La formation met également l'accent sur la préparation à l'examen, la lecture des scénarios de sécurité, les bonnes pratiques de paramétrage et les réflexes attendus pour répondre avec précision aux questions de certification.

À l'issue du parcours, vous serez en mesure de renforcer la sécurité d'un périmètre applicatif, de mieux piloter les protections Imperva et d'aborder l'examen avec une vision structurée et opérationnelle.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le périmètre fonctionnel de Imperva Web Security et ses cas d'usage.
- Identifier les menaces web majeures, dont les attaques OWASP, les bots et les abus d'API.
- Configurer les principaux mécanismes de protection, de détection et de réponse.
- Exploiter les fonctions de WAF, de journalisation et de supervision pour sécuriser une application.
- Se préparer efficacement au format et aux attendus de la certification IWSS.
- Appliquer les bonnes pratiques de durcissement et de validation en contexte de certification.

Public visé

- Ingénieur sécurité applicative
- Administrateur sécurité
- Analyste SOC
- Consultant cybersécurité
- Responsable sécurité des applications

Pré-requis

- Connaissances de base en sécurité web et en protection des applications.
- Notions sur les attaques HTTP, OWASP et les mécanismes de filtrage applicatif.
- Expérience préalable avec une solution WAF ou de sécurité applicative.
- Compréhension des principes réseau, proxy, DNS et flux applicatifs.
- Pratique de l'administration d'environnements de production ou de préproduction.

Pré-requis techniques

- Un ordinateur récent avec au moins 8 Go de mémoire vive et un navigateur à jour.
- Une connexion Internet stable en Wi-Fi ou Ethernet pour les démonstrations et exercices.
- Un accès à un environnement de travail compatible avec les consoles web utilisées pendant la formation.
- Un micro et un casque si la session se déroule à distance.
- Un environnement local permettant de consulter des captures, exports et journaux de sécurité.

Programme de notre formation Imperva Web Security Specialist (IWSS)

[Jour 1 - Matin]

Fondamentaux de la solution

- Positionnement de Imperva Web Security dans une stratégie de protection applicative.
- Rappel des concepts clés : WAF, protection web, inspection du trafic et politiques de sécurité.
- Présentation des composants de la plateforme et de leur rôle dans l’architecture globale.
- Lecture des principaux scénarios de menace couverts par la solution.
- Préparation au vocabulaire et aux notions récurrentes de l’examen IWSS.

- Atelier pratique : prise en main de l’interface, repérage des menus essentiels et lecture d’un premier tableau de bord.

[Jour 1 - Après-midi]

Menaces et protections web

- Analyse des attaques applicatives les plus courantes, dont les injections et les contournements de contrôle.
- Compréhension des familles de signatures, règles et exceptions de sécurité.
- Gestion des faux positifs et arbitrage entre protection et continuité de service.
- Introduction aux mécanismes de détection comportementale et contextuelle.
- Lecture des cas typiques rencontrés dans un examen de certification orienté sécurité web.
- Atelier pratique : qualifier plusieurs requêtes malveillantes et choisir la réponse de protection adaptée.

[Jour 2 - Matin]

Configuration des politiques

- Construction d’une politique de sécurité à partir d’un besoin métier.
- Paramétrage des règles de filtrage, des exceptions et des seuils d’alerte.
- Gestion des profils d’application et des zones de confiance.
- Exploitation des journaux, événements et alertes pour affiner la posture de sécurité.
- Bonnes pratiques de validation avant mise en production.
- Atelier pratique : créer une politique simple, l’ajuster sur des cas réels et vérifier son impact.

[Jour 2 - Après-midi]

Bot management et API security

- Compréhension des attaques automatisées et des usages abusifs des applications web.
- Différenciation entre trafic humain, bots simples et bots avancés.
- Principes de protection des API et de contrôle des appels suspects.
- Lecture des signaux utiles pour détecter un comportement anormal.
- Cas d’usage de mitigation selon le niveau de risque observé.
- Atelier pratique : analyser un jeu de requêtes et classer les comportements à traiter en priorité.

[Jour 3 - Matin]

Exploitation et supervision

- Suivi de l’activité de sécurité et lecture des indicateurs utiles à l’exploitation.

- Interprétation des événements, traces et alertes pour qualifier un incident.
- Utilisation des rapports pour piloter la protection et documenter les choix.
- Gestion des changements et contrôle de l’effet des ajustements de politique.
- Révision des points de vigilance fréquemment évalués à l’examen.
- Atelier pratique : exploiter un scénario d’incident et produire une analyse de sécurité argumentée.

[Jour 3 - Après-midi]

Préparation intensive à l’examen

- Révision structurée des notions clés de IWSS et des zones de fragilité fréquentes.
- Mise en perspective des questions de certification avec les cas d’usage opérationnels.
- Stratégies de lecture rapide, d’élimination des distracteurs et de gestion du temps.
- Vérification des points de vocabulaire, de configuration et de diagnostic.
- Conseils méthodologiques pour sécuriser les réponses lors de l’épreuve.
- Atelier pratique : simulation d’examen avec correction commentée et consolidation des acquis.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.