+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 Associate

3 jours (21 heures)

Présentation

La certification Imperva Web Security Associate valide votre capacité à maîtriser les fondamentaux de la protection des applications web, du WAF et des mécanismes de défense Imperva. Cette formation vous prépare de manière ciblée à l'examen officiel, avec une approche orientée compréhension, configuration et validation des acquis.

Notre formation Certification Imperva Web Security Associate vous permet d'aller au-delà des notions essentielles pour consolider les compétences attendues sur les environnements Imperva et sécuriser les applications exposées sur Internet.

Vous apprendrez à comprendre l'architecture de la solution, à identifier les principaux vecteurs d'attaque web, à paramétrer les protections de base et à interpréter les mécanismes de détection, de journalisation et de traitement des alertes.

À l'issue de la formation, vous serez en mesure d'aborder l'examen IWSA avec méthode, de relier les concepts de sécurité applicative aux usages concrets de la plateforme et de répondre plus sereinement aux questions de certification.

Cette préparation couvre également les cas pratiques, les réflexes d'analyse et les bonnes pratiques attendues pour réussir une certification de niveau intermédiaire dans un contexte opérationnel.

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

Objectifs

- Comprendre le positionnement de Imperva Web Security Associate dans le parcours de certification.
- Maîtriser les principes de sécurité applicative web et de protection par WAF.
- Identifier les fonctions clés de la plateforme Imperva pour sécuriser les applications.
- Préparer efficacement l'examen officiel IWSA avec une logique orientée certification.
- Appliquer les bonnes pratiques de configuration, de supervision et de diagnostic sur des cas concrets.

Public visé

- Ingénieur cybersécurité
- Administrateur sécurité
- Consultant sécurité applicative
- Analyste SOC
- Architecte sécurité

Pré-requis

- Connaissances de base en réseaux, en HTTP et en architecture web.
- Compréhension des enjeux de sécurité applicative et des attaques courantes sur le web.
- Pratique préalable d'un environnement Imperva ou d'une solution WAF appréciée.
- Notions sur l'administration système et la supervision d'une plateforme de sécurité.

Pré-requis techniques

- Un ordinateur récent avec navigateur à jour et espace de travail confortable pour les ateliers.
- Une connexion Wi-Fi ou Ethernet stable pour les séquences à distance et les démonstrations.
- Un environnement de consultation compatible avec les supports de formation, PDF et exercices guidés.
- Un micro et un casque si la session est suivie en classe virtuelle.
- Un accès éventuel à un environnement Imperva de démonstration ou de laboratoire, selon le dispositif pédagogique.

Programme de notre formation Imperva Web Security Associate

[Jour 1 - Matin]

Fondamentaux de la certification

- Comprendre le périmètre de la certification Imperva Web Security Associate.
- Identifier les attentes de l’examen officiel et le niveau de maîtrise attendu.
- Revoir les bases de la sécurité web, du WAF et des menaces courantes.
- Positionner la solution Imperva dans une stratégie de protection applicative.
- Associer les concepts clés aux thèmes récurrents de l’évaluation.
- Atelier pratique : cartographier les domaines de connaissances à réviser pour l’examen IWSA.

[Jour 1 - Après-midi]

Architecture et composants

- Décrire l’architecture générale d’une solution Imperva pour la protection web.
- Comprendre le rôle des composants de collecte, d’analyse et de décision.
- Différencier les flux de trafic légitimes des comportements suspects.
- Lire les principes de fonctionnement d’une politique de protection.
- Relier les notions d’authentification, de journalisation et de visibilité opérationnelle.
- Atelier pratique : analyser un schéma d’architecture et repérer les points de contrôle de sécurité.

[Jour 2 - Matin]

Protection des applications

- Étudier les principales catégories d’attaques sur les applications web.
- Comprendre la logique de détection et de blocage d’un WAF.
- Examiner les règles, exceptions et mécanismes de profilage.
- Appréhender la gestion des faux positifs dans un contexte de production.
- Relier les cas d’usage de protection aux besoins métier et aux contraintes techniques.
- Atelier pratique : qualifier plusieurs scénarios d’attaque et choisir la réponse de protection appropriée.

[Jour 2 - Après-midi]

Configuration et supervision

- Découvrir les paramètres essentiels d’une politique de sécurité Imperva.
- Comprendre les options de journalisation, d’alerting et de suivi des événements.
- Analyser les indicateurs utiles pour le pilotage quotidien.
- Apprendre à interpréter les alertes et à prioriser les actions.
- Consolider les réflexes de diagnostic attendus dans l’examen.
- Atelier pratique : lire des journaux d’activité et identifier les événements de sécurité pertinents.

[Jour 3 - Matin]

Révision ciblée et entraînement

- Revoir les notions les plus importantes sous forme de synthèse structurée.
- Consolider le vocabulaire technique lié à la certification IWSA.
- Travailler les liens entre théorie, configuration et cas d’usage.
- Identifier les pièges fréquents de l’examen et les erreurs de lecture.
- Mettre en perspective les thèmes à forte probabilité de questionnement.
- Atelier pratique : réaliser un quiz blanc corrigé sur les chapitres clés de la certification.

[Jour 3 - Après-midi]

Préparation finale à l’examen

- Organiser la dernière révision avant le passage de la certification.
- Adopter une méthode de lecture rapide des questions et des distracteurs.
- Gérer le temps, la priorisation et la vérification des réponses.
- Revoir les points de vigilance liés aux notions de protection web et de supervision.
- Valider la stratégie personnelle de passage de l’examen Imperva Web Security Associate.
- Atelier pratique : simuler une session d’examen et corriger les réponses avec justification.

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.