

Mis à jour le 18/08/2026

S'inscrire

Formation Certification Imperva Database Security Specialist

3 jours (21 heures)

Présentation

La formation Imperva Database Security Specialist vous prépare à valider une expertise reconnue sur la sécurisation des bases de données, la surveillance des activités et la protection des données sensibles. Vous consolidez les réflexes attendus pour réussir l'examen officiel et intervenir sur des environnements Imperva en contexte opérationnel.

Cette formation Certification Imperva Database Security Specialist vous permet d'aller au-delà des fondamentaux pour maîtriser les sujets clés évalués lors de la certification officielle IDSS. Vous y travaillez la logique de l'examen, les concepts de déploiement, de configuration et de supervision, ainsi que les mécanismes de contrôle indispensables en environnement réel.

Vous apprendrez à structurer une démarche de database security, à interpréter les scénarios de database activity monitoring, à comprendre les usages de politiques de sécurité et à relier les fonctions Imperva aux besoins de conformité et d'audit. L'objectif est de vous faire progresser avec une vision claire des attendus de certification.

À l'issue de la formation, vous serez en mesure d'aborder l'examen avec méthode, de reconnaître les cas d'usage typiques, de sécuriser les traitements sensibles et de justifier vos choix techniques. Vous disposerez aussi d'une base solide pour exploiter Imperva dans une logique de production, de contrôle et de gouvernance.

Cette préparation aborde également les bonnes pratiques de révision, les pièges fréquents de l'examen, les automatismes à acquérir et les mises en situation proches du format de certification. Vous consolidez ainsi vos compétences pour viser une réussite durable sur Imperva Database Security Specialist.

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 Database Security Specialist et les compétences validées.
- Maîtriser les principes de database activity monitoring, de contrôle et de protection des accès.
- Identifier les composants, les flux et les scénarios d'usage d'une architecture Imperva orientée base de données.
- Préparer efficacement l'examen officiel grâce à une révision structurée des thèmes de certification.
- S'entraîner sur des cas pratiques proches des situations rencontrées en production et en examen.

Public visé

- Administrateur bases de données
- Ingénieur sécurité
- Architecte sécurité
- Consultant cybersécurité
- Responsable conformité

Pré-requis

- Maîtrise des fondamentaux des bases de données et des environnements de production.
- Connaissances de base en cybersécurité, contrôle d'accès et journalisation.
- Expérience pratique avec des outils de supervision, d'audit ou de protection des données.
- Notions d'administration sur des environnements Imperva ou solutions équivalentes appréciées.
- Capacité à lire une documentation technique en anglais.

Pré-requis techniques

- Ordinateur récent avec processeur multicœur, mémoire suffisante et espace disque disponible pour les supports de cours.
- Connexion Wi-Fi ou Ethernet stable pour les éventuels ateliers à distance.
- Navigateur web à jour pour accéder aux supports, exercices et éventuelles interfaces de démonstration.
- Micro et casque recommandés pour les sessions en classe virtuelle.
- Accès à un environnement de travail standard avec autorisations suffisantes pour ouvrir les documents et manipuler les ressources de formation.

Programme de notre formation Imperva Database Security Specialist

[Jour 1 - Matin]

Fondamentaux de la certification

- Positionnement de la certification Imperva Database Security Specialist dans l'offre officielle Imperva.
- Lecture du périmètre d'examen, des attentes et des compétences évaluées.
- Rappels sur la sécurité des bases de données et les enjeux de conformité.
- Panorama des usages de database activity monitoring et de supervision.
- Organisation de la préparation, méthode de révision et gestion du temps d'apprentissage.
- Atelier pratique : cartographier les thèmes de l'examen et construire votre plan de révision sur 3 jours.

[Jour 1 - Après-midi]

Architecture et composants Imperva

- Présentation des briques fonctionnelles d'une architecture Imperva orientée bases de données.
- Rôle des composants de collecte, de contrôle et de remontée d'événements.
- Relations entre politiques, règles et mécanismes de détection.
- Notions de déploiement, de flux d'administration et de supervision.
- Points de vigilance sur les modes d'intégration en environnement de production.
- Atelier pratique : associer chaque composant Imperva à son rôle dans un scénario d'architecture type.

[Jour 2 - Matin]

Contrôle et surveillance des activités

- Principes de database activity monitoring et logique de traçabilité.
- Identification des événements pertinents pour l'audit et la détection.
- Compréhension des alertes, des exceptions et des comportements attendus.
- Gestion des accès, des rôles et des usages sensibles dans une base protégée.
- Lecture des scénarios d'exploitation courants et des questions fréquemment posées à l'examen.
- Atelier pratique : analyser un flux d'activité et distinguer événements normaux, alertes et anomalies.

[Jour 2 - Après-midi]

Politiques, conformité et protection des données

- Construction et lecture de politiques de sécurité adaptées aux bases de données.
- Notions de conformité, de séparation des rôles et de contrôle des accès.
- Protection des données sensibles et articulation avec les besoins d'audit.
- Gestion des exceptions, des seuils et des réponses attendues selon les cas d'usage.
- Approche orientée examen pour reconnaître rapidement les bonnes pratiques.
- Atelier pratique : choisir la politique la plus adaptée à un cas métier et justifier votre réponse comme en certification.

[Jour 3 - Matin]

Exploitation et cas de certification

- Revue des scénarios d'exploitation les plus probables dans l'examen IDSS.
- Lecture des indices techniques dans un énoncé et élimination des réponses distrayantes.
- Mise en relation entre besoins métier, contraintes de sécurité et choix de configuration.
- Bonnes pratiques de diagnostic, de contrôle et de validation des paramètres clés.
- Stratégies pour traiter les questions de niveau intermédiaire avec méthode et précision.
- Atelier pratique : résoudre une série de mini-cas d'examen en temps limité avec correction argumentée.

[Jour 3 - Après-midi]

Révision finale et préparation à l'examen

- Révision structurée des notions indispensables à retenir avant l'épreuve.
- Focus sur les pièges classiques, les confusions fréquentes et les points de vigilance.
- Stratégie de gestion du temps, de lecture rapide et de validation des réponses.
- Derniers rappels sur les thèmes Imperva à forte probabilité d'apparition.
- Conseils pour aborder sereinement le passage de la certification officielle.
- Atelier pratique : simulation finale de certification avec auto-évaluation et plan d'action personnalisé.

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.