

Formation Sécurité des bases de données

Présentation

Cette formation permet aux professionnels IT de comprendre et de mettre en œuvre les meilleures pratiques de sécurisation des bases de données. Elle aborde les menaces courantes, les mécanismes de contrôle d'accès, le chiffrement, l'audit, la gestion des vulnérabilités et la conformité réglementaire. À travers des ateliers pratiques, les participants apprendront à protéger efficacement les données sensibles dans des environnements Oracle, SQL Server, MySQL ou PostgreSQL.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Identifier les menaces et vulnérabilités spécifiques aux bases de données.
- Mettre en œuvre des politiques de contrôle d'accès et de gestion des privilèges.
- Appliquer des techniques de chiffrement des données au repos et en transit.
- Configurer l'audit, la journalisation et la détection d'activités suspectes.
- Intégrer la sécurité des bases de données dans une démarche de conformité (RGPD, ISO 27001...).

Prérequis

- Connaissances de base en administration de bases de données (Oracle, SQL Server, MySQL, PostgreSQL).
- Notions en sécurité informatique et en réseau.
- Expérience en exploitation ou développement d'applications connectées à une base de données.

Public

- Administrateurs de bases de données (DBA)
- Ingénieurs sécurité ou DevSecOps
- Développeurs d'applications manipulant des données sensibles
- Responsables IT ou RSSI
- Auditeurs techniques ou consultants en conformité



Programme de la formation

Jour 1 : Menaces, vulnérabilités et contrôle d'accès

Module 1 : Panorama des menaces sur les bases de données

- Attaques courantes : injection SQL, élévation de privilèges, exfiltration
- Vulnérabilités logicielles et erreurs de configuration
- Risques internes et erreurs humaines

Module 2 : Contrôle d'accès et gestion des privilèges

- Modèles de sécurité : RBAC, ABAC, principe du moindre privilège
- Comptes utilisateurs, rôles, groupes
- Sécurisation des comptes administrateurs

Atelier

- Analyse de vulnérabilités sur une base de test + mise en place de rôles et permissions

Jour 2 : Chiffrement, audit et surveillance

Module 3 : Chiffrement des données

- Chiffrement au repos (TDE, tablespaces, fichiers)
- Chiffrement en transit (SSL/TLS)
- Gestion des clés (KMS, HSM)

Module 4 : Audit et journalisation

- Audit natif (Oracle Audit, SQL Server Audit, MySQL Audit Plugin)
- Suivi des connexions, des requêtes sensibles, des modifications
- Intégration avec un SIEM

Atelier

- Activation du chiffrement et configuration d'un audit de requêtes sensibles

Jour 3 : Sécurité avancée et conformité**Module 5 : Sécurité applicative et bonnes pratiques**

- Sécurisation des connexions applicatives
- Prévention des injections SQL
- Séparation des environnements (dev, test, prod)

Module 6 : Conformité et gouvernance

- Exigences RGPD, ISO 27001, PCI-DSS
- Masquage des données (data masking, redaction)
- Plan de remédiation et documentation de sécurité

Atelier

- Mise en œuvre d'un scénario de conformité RGPD avec masquage de données personnelles

Organisation**Formateur**

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Équilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.

- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Évaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.