

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

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)

- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

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

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

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