Sécurité des bases de données

Référence : BAOS Niveau : Intermédiaire Durée : 2 jours (14h.)

Tarif: Nous Contacter Date: Juin, Juillet, Aout Contact: +225 22469017 / 74622582

Objectifs

La sécurité des données est devenue un sujet crucial face aux risques de piratage, d'exploitation des vulnérabilités ou au vol des supports physiques de sauvegarde. Les administrateurs de bases de données sont par conséquent particulièrement impliqués dans la sécurité, et ce, à différents niveaux :
· Lors de l'installation et de la configuration de la base de données (y inclus le téléchargement et l'installation des correctifs de sécurité)
· Dans la gestion des comptes utilisateurs (Identification et Authentification)
· Pour protéger les connexions réseaux
· Afin de sécuriser les données sensibles (chiffrement).
Ils se doivent également d'auditer régulièrement les composants base de données au niveau approprié.
Ce cours vous enseigne une méthode de travail, véritable feuille de route technique et documentaire, pour renforcer la sécurité de vos bases de données.
À l'issue de cette formation, vous vous aurez acquis les connaissances et les compétences nécessaires pour :
· Utiliser une méthodologie de travail, étape par étape
· Comprendre la complémentarité entre les différentes actions
· Identifier des axes d'amélioration et d'optimisation.

Public

Cette formation Sécurité des bases de données s'adresse aux responsables sécurité, administrateurs de bases de données, développeurs SQL, les chefs de projets, et à toute personne souhaitant obtenir une vision d'ensemble, exhaustive, sur les outils de sécurité proposés par les bases de données.

Pré-requis

Il est recommandé d'avoir quelques connaissances sur les bases de données.

Contenu du cours

Étape 1 : Sécuriser l'accès aux bases de données à l'aide des paramètres d'initialisation et des

protections réseau

Étape 2 : Créer des rôles et des privilèges pour l'Identification et l'Authentification

Créer un rôle de sécurité
Les comptes Utilisateur prédéfini
Les privilèges
L'authentification forte

Étape 3 : Chiffrer les données qui se déplacent à travers le réseau

Le chiffrement

Étape 4 : Protéger l'accès aux données sensibles

Réduire la surface
Les contextes d'application

Étape 5 : Restreindre l'affichage des données sensibles

Étape 6 : Limiter l'accès aux données sensibles

Étape 7 : Partager les données en toute sécurité

Étape 8 : Renforcer la sécurité avec des outils intégrés ou externe

Étape 9 : Configurer l'audit pour tracer l'activité sur la base de données

Les stratégies d'audit prédéfinies