Formation **Sécurité des réseaux**

Donnez à votre équipe les compétences essentielles pour fortifier le réseau de votre organisation contre les cyber-menaces les plus sophistiquées grâce à notre formation intensive sur la sécurité des réseaux. Couvrant tous les aspects, des principes de sécurité fondamentaux aux techniques de protection avancées, ce cours permettra aux professionnels de l'informatique de sécuriser les accès, de protéger les données, d'assurer des échanges sécurisés et de renforcer les systèmes et les applications contre les failles. Grâce à des activités pratiques basées sur des scénarios réels, votre équipe ne se contentera pas d'apprendre, mais appliquera également ses connaissances pour gérer et améliorer votre infrastructure de sécurité. Donnez à vos collaborateurs les connaissances nécessaires pour protéger vos actifs vitaux et garantir la conformité avec les normes de l'industrie IT.

Durée
5 jours

Objectifs pédagogiques

- Identifier et analyser les menaces et les vulnérabilités du réseau
- Mettre en œuvre des mesures de sécurité adaptées
- Gérer les contrôles d'accès et l'authentification
- Concevoir et appliquer des stratégies de protection des données
- Sécuriser les canaux de communication
- Renforcer les systèmes et sécuriser les applications

Public
Administrateurs systèmes et réseaux, ingénieurs télécoms, techniciens support...

Prérequis
Les participants doivent avoir bonne compréhension des concepts réseau ainsi qu'une familiarité avec les systèmes d'exploitation.

Programme de formation

Phase d'inclusion

Introduction à la formation Sécurité des réseaux

Concepts fondamentaux de la sécurité des réseaux, risques et vulnérabilités
Le périmètre et les acteurs de la sécurité des réseaux
L'évolution des menaces pesant sur les réseaux, panorama des risques actuels
Implications juridiques et réglementaires de la sécurité des réseaux
Exemples d'activités pratiques : analyse d'attaques récentes sur les réseaux et de leur impact sur les entreprises, identification des vulnérabilités potentielles dans un scénario de réseau donné.

Comprendre les menaces réseau et les méthodes d'attaque

Types de menaces réseau : intrusions, DDoS, logiciels malveillants, phishing
Analyse détaillée des vecteurs d'attaque et de leurs mécanismes
Vulnérabilités courantes dans les systèmes et applications
Exemples d'activités pratiques : simulation d'une attaque de phishing dans un environnement contrôlé.

Sécurité des accès

Principes fondamentaux du contrôle d'accès et de la gestion des identités
Techniques pour des systèmes d'authentification et d'autorisation robustes
Mise en œuvre du contrôle d'accès au réseau (NAC)
Aspects pratiques de la gestion des accès dans un réseau d'entreprise
Exemples d'activités pratiques : mise en place d'un contrôle d'accès basé sur les rôles sur un réseau.

Sécurité des données

Importance du cryptage et du stockage sécurisé des données
Mise en œuvre et gestion du cryptage à travers différentes couches
Meilleures pratiques pour la sauvegarde des données et la reprise après sinistre
Exemples d'activités pratiques : cryptage et transmission sécurisée des données sur les réseaux.

Sécurité des échanges

Sécuriser des canaux de communication (courrier électronique, VoIP, transfert de données)
Mise en œuvre de protocoles de sécurité tels que SSL/TLS, HTTPS
Sécurisation des API et autres interfaces d'échange de données
Exemples d'activités pratiques : configuration de SSL sur un serveur web.

Sécurité des systèmes (hardening)

Techniques de hardening pour Windows et Linux
Configurations de sécurité et meilleures pratiques pour les systèmes d'exploitation
Mises à jour régulières des systèmes et gestion des correctifs
Exemples d'activités pratiques : analyse des vulnérabilités du système et application de correctifs.

Sécurité des applications

Sécurité dans le développement et le déploiement d'applications
Utilisation de pare-feu pour applications web (WAF)
Effectuer des tests de sécurité et des audits sur les applications
Exemples d'activités pratiques : configuration d'un WAF et test des vulnérabilités web courantes.

Tendances futures et amélioration continue

Technologies émergentes dans le domaine de la sécurité des réseaux (IA, sécurité de l'IoT).
Apprentissage et amélioration continus des pratiques de sécurité des réseaux
Création d'une culture de sensibilisation à la sécurité au sein des organisations.

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.