Formation **Cybersécurité : solutions techniques**

Explorez les technologies pour sécuriser votre système d'information

Cette formation Cybersécurité est conçue pour fournir une compréhension approfondie des différents aspects de la cybersécurité et des solutions techniques associées. Les participants apprendront les fonctions, les utilisations courantes et les étapes de configuration des protocoles de sécurité, des systèmes d'authentification et d'autorisation, des technologies de chiffrement et des systèmes IDS/IPS. Ils auront l'occasion de mettre en pratique leurs connaissances avec des exemples concrets. Cette formation est donc idéale pour les professionnels souhaitant se perfectionner dans le domaine de la cybersécurité et découvrir les meilleures pratiques pour protéger les systèmes informatiques.

Durée

4 jours

Objectifs pédagogiques

- Définir les concepts clés de la cybersécurité et de la sécurité des systèmes d'information
- Expliquer les fonctions et les utilisations courantes des différents protocoles de sécurité réseau
- Comprendre les systèmes d'authentification et d'autorisation et les utiliser pour protéger les ressources informatiques
- Mettre en œuvre les technologies de chiffrement pour protéger les données
- Utiliser les systèmes de détection et de prévention (IDS/IPS) pour protéger les réseaux informatiques
- Identifier et adresser les principaux risques liés au cloud computing
- Connaître les meilleures pratiques pour sécuriser des applications
- Estimer les futurs défis à relever en matière de sécurité des systèmes d'information

Public

Administrateurs systèmes et réseaux, ingénieurs sécurité, RSSI, DSI, chefs de projet, architectes...

Prérequis

Bonnes connaissances sur les systèmes d'information et les technologies réseaux.

Programme de formation

Introduction à la formation Cybersécurité : solutions techniques

Présentation générale de cette formation Cybersécurité

Cybersécurité et sécurité des systèmes d'information

Les principaux protocoles de sécurité réseau

Définition des protocoles de sécurité réseau
Les différents types de protocoles (VPN, SSH, SSL/TLS, etc.)
Les fonctions des protocoles de sécurité (authentification, chiffrement, intégrité des données, etc.)
Présentation des protocoles les plus couramment utilisés (IPsec, SSL/TLS, SSH, etc.)
Les utilisations courantes de ces protocoles (VPN, chiffrement des communications, etc.)
Exemples concrets d'utilisation des protocoles
Les étapes de configuration des protocoles de sécurité (installation, paramétrage, etc.)
Les outils de gestion et de surveillance des protocoles
Les bonnes pratiques de gestion des protocoles de sécurité

Les systèmes d'authentification et d'autorisation

Définition des systèmes d'authentification et d'autorisation
Les différents types de systèmes d'authentification (basés sur des mots de passe, des jetons, des certificats, etc.)
Les fonctions des systèmes d'authentification et d'autorisation (vérification de l'identité, attribution des droits d'accès, etc.)
Présentation des systèmes d'authentification les plus couramment utilisés (Active Directory, LDAP, RADIUS, etc.)
Les utilisations courantes de ces systèmes d'authentification (authentification pour les réseaux, les systèmes d'exploitation, les applications, etc.)
Exemples concrets d'utilisation des systèmes d'authentification
Les étapes de configuration des systèmes d'authentification et d'autorisation
La gestion des utilisateurs et des rôles dans les systèmes d'authentification et d'autorisation
Les meilleures pratiques de sécurité pour la gestion des systèmes d'authentification et d'autorisation

Les technologies de chiffrement

Définition de chiffrement et de déchiffrement
Les différents types de chiffrement (symétrique, asymétrique, à clé secrète, à clé publique)
Les algorithmes de chiffrement couramment utilisés (AES, RSA, DES, etc.)
Les protocoles de chiffrement utilisés pour protéger les données en transit (SSL, TLS)
Les technologies utilisées pour chiffrer les données en repos (disques durs chiffrés, bases de données chiffrées, etc.)
Mise en pratique: Configuration d'un chiffrement de disque dur
Les certificats X.509 et leur utilisation pour l'authentification et la signature numérique
Les protocoles de gestion de clés (PKCS, KMIP)
Exemple de mise en pratique: génération d'un certificat auto-signé et utilisation pour chiffrer un fichier
Les différentes méthodes de stockage de clés (matériel, logiciel, à chaud, à froid)
Les politiques de rotation des clés et de gestion des accès
Les normes et réglementations relatives à la sécurité des clés (FIPS, Common Criteria)
Les attaques courantes contre les systèmes de chiffrement (man-in-the-middle, déchiffrement par force brute, etc.)
Les contre-mesures à mettre en place pour protéger les systèmes de chiffrement (authentification forte, mise à jour régulière des logiciels, etc.)
Exemple de mise en pratique : analyse de vulnérabilités sur un système de chiffrement et mise en place de contre-mesures

Les systèmes de détection et de prévention des intrusions (IDS/IPS)

IDS : système qui détecte les intrusions en analysant les données de trafic réseau
IPS : système qui prévient les intrusions en bloquant les paquets malveillants
Les avantages et les limites de chacun de ces systèmes
Les différents types de firewalls (matériel, logiciel, réseau)
Les règles de filtrage des paquets et de contrôle d'accès
Exemple de cas pratique : Configuration d'un firewall pour bloquer les connexions entrantes non autorisées
Attaques réseau : DoS, DDoS, spoofing, sniffing, etc.

Attaques applicatives : injection SQL, cross-site scripting, etc.
Méthodes de détection : signatures, comportements, anomalies
Installation et configuration d'un système IDS/IPS
Mise en place des règles de filtrage et des alertes
Exemple de cas pratique : Configuration d'un système Snort en mode IDS
Analyse des alertes et des journaux d'événements
Identification des sources d'intrusion et des cibles
Prise de décisions en matière de réponse à une intrusion

Technologies de sécurité pour le cloud computing

Les risques liés à la confidentialité et à l'intégrité des données
Les risques liés à la disponibilité des données
Les risques liés à la conformité réglementaire
Les risques liés à la sécurité physique des centres de données
Les différents types de cloud (public, privé, hybride)
Les avantages et inconvénients de chaque type de cloud en termes de sécurité
Les meilleures pratiques pour la gestion des identités et des accès
La mise en place de contrôles de sécurité pour protéger les données stockées dans le cloud
Les outils et technologies disponibles pour la surveillance et la protection des données dans le cloud
Exemple de cas pratique : Déploiement d'un système de surveillance des données dans un environnement de cloud public
Les normes et réglementations applicables au cloud computing
Les exigences de conformité pour les données stockées dans le cloud
Les outils et technologies pour assurer la conformité dans le cloud

Sécurité des applications Web et des bases de données

Présentation des risques OWASP les plus courants (injection SQL, failles XSS, etc.)
Définition et explication du principe de défense en profondeur
Les meilleures pratiques pour la sécurisation des applications web, en utilisant les différentes couches de défense (authentification, autorisation, cryptographie, ...)
Les outils et technologies disponibles pour protéger les applications web contre les risques OWASP
Exemple de cas pratique : Mise en place d'une politique de sécurité pour une application web en utilisant les principes de défense en profondeur
Les différents types d'attaques contre les bases de données
Les meilleures pratiques pour la sécurisation des bases de données
Les outils et technologies disponibles pour protéger les bases de données

Sécurité des smartphones

Présentation des risques liés à l'utilisation d'un smartphone : vol, piratage, espionnage, perte de données, etc.
Présentation des principales menaces pour un smartphone : malware, phishing, réseaux WiFi publics, etc.
Mise à jour du système d'exploitation et des applications
Utilisation d'un mot de passe ou d'une empreinte digitale pour déverrouiller le smartphone
Utilisation d'une application de sécurité pour protéger le smartphone contre les menaces
Utilisation d'un VPN pour se protéger sur les réseaux WiFi publics

Les tendances et défis futurs de la sécurité des systèmes d'information

Les tendances en matière de cybersécurité, telles que l'IA et l'apprentissage automatique, la sécurité des clouds hybrides, la sécurité de l'IoT, la sécurité des applications mobiles, la sécurité des données
Les menaces émergentes telles que les attaques de ransomware, les attaques de phishing, les attaques à la sécurité des réseaux 5G, les attaques de rançonnage de données, les attaques de cryptojacking
Les enjeux de la sécurité des données dans un monde de plus en plus connecté

Conclusion et synthèse de la formation

Récapitulatif des principaux enseignements de la formation
Mise en place d'un plan d'action pour mettre en pratique les enseignements de la formation
Questions/Réponses selon les besoins des apprenants
Questionnaires de satisfaction

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques.
- 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 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.