Management SI

Principes et notions fondamentales de la sécurité des systèmes d'information

3 jours (21 heures)

Délai maximum : 2 mois.

Parcours concourant au développement des compétences. Action de formation réalisée en application des articles L 6313-1 et L 6313-2 du Code du travail.

Si vous êtes en situation de handicap, contactez-nous avant le début de votre formation pour que nous puissions vous orienter efficacement et vous accueillir dans les meilleures conditions.

Objectifs pédagogiques

- Connaître le vocabulaire et les principes théoriques de la sécurité des systèmes d'information, mais de manière très pratique, donc très concrète, pour des praticiens
- Connaître toutes les base de la sécurité opérationnelle, à la fois en sécurité réseau, en sécurité des systèmes Windows et Linux et en sécurité applicative

Pré-requis

- Une réelle connaissance informatique est nécessaire

Modalités pédagogiques

Modalités de formation:

- Formation réalisée en présentiel, à distance ou mixte,
- Toutes nos formations peuvent être organisées dans nos locaux ou sur site
- Feuille de présence signée en demi-journée, questionnaires d'évaluation de la satisfaction en fin de stage et 60 jours après, attestation de stage et certificat de réalisation.
- Horaires de la formation: 9h - 12h30 et 13h30 - 17h.
- Les horaires de la formation sont adaptables sur demande.

Moyens pédagogiques

- Formateur expert dans le domaine,
- Mise à disposition d'un ordinateur, d'un support de cours remis à chaque participant,
- Vidéo projecteur, tableau blanc et paperboard,
- Formation basée sur une alternance d'apports théoriques et de mises en pratique
- Formation à distance à l'aide du logiciel Teams pour assurer les interactions avec le formateur et les autres stagiaires, accès aux supports et aux évaluations. Assistance pédagogique afin de permettre à l'apprenant de s'approprier son parcours. Assistance technique pour la prise en main des équipements et la résolution des problèmes de connexion ou d'accès. Méthodes pédagogiques : méthode expositive 50%, méthode active 50%.

Public visé

- Administrateurs systèmes et réseaux, responsables informatique et/ou sécurité

Modalités d'évaluation et de suivi

- Evaluation des acquis tout au long de la formation : QCM, mises en situation, TP, évaluations orales…

Programme de formation

1. Concepts de base des réseaux

- Paquets et adresses
- Ports de services IP
- Protocoles sur IP

Contacts

Notre centre à **Mérignac**
14 rue Euler
33700 MERIGNAC
05 57 92 22 00
contact@afib.fr

Notre centre à **Périgueux**
371 Boulevard des Saveurs,
24660 COULOUNIEIX CHAMIERS
05 64 31 02 15
contact@afib.fr

Principes et notions fondamentales de la sécurité des systèmes d'information

- TCP / UDP / ICMP
- DHCP / DNS
- VoIP (SI P)
- Réseaux sans fil

2. Sécurité physique
- Services généraux
- Contrôles techniques
- Menaces sur la sécurité physique

3. Principes de base de la SSI
- Modèle de risque
- Défense en profondeur
- Identification, authentification et autorisation
- Classification des données
- Vulnérabilités

4. Politiques de sécurité informatique
- Principe
- Rôles et responsabilité

5. Plan de continuité d'activité
- Exigences légales et réglementaires
- Stratégie et plan de reprise après sinistre

6. Analyse des conséquences
- Évaluation de crise
- Facteurs de succès
- Fonctions business critiques

7. Gestion des mots de passe
- Stockage, transmission et attaque des mots de passe
- Windows
- Authentification forte (Tokens, biométrie)
- Single Sign On
- RADIUS

8. Sécurité Web
- Protocoles de sécurité du Web
- Contenus dynamiques
- Attaques des applications Web
- Durcissement des applications Web

9. Détection d'intrusion en local
- Détection d'intrusion
- A quoi s'attendre

10. Détection d'intrusion en réseau
- Outils
- Déni de service
- Réaction automatisée

11. Pots de miel

Principes et notions fondamentales de la sécurité des systèmes d'information

12. Gestion des incidents de sécurité
- Préparation, identification et confinement
- Eradication, recouvrement et retour d'expérience
- Techniques d'enquête et criminalistique informatique

13. Guerre de l'information offensive et défensive

14. Méthodes d'attaques
- Débordement de tampon
- Comptes par défaut
- Envoi de messages en masse
- Navigation web
- Accès concurrents

15. Pare-feu et zones de périmètres
- Types de pare-feu
- Architectures possibles : avantages et inconvénients

16. Audit et appréciation des risques
- Méthodologies d'appréciation des risques
- Approches de la gestion du risque
- Calcul du risque / SLE / ALE

17. Cryptographie
- Besoin de cryptographie
- Types de chiffrement
- Symétrique / Asymétrique
- Empreinte ou condensat
- Chiffrement
- Algorithmes
- Attaques cryptographiques
- Types d'accès à distance (VPN, DirectAccess)
- Infrastructures de Gestion de Clés
- Certificats numériques
- Séquestre de clés

18. PGP
- Installation et utilisation de PGP
- Signature de données
- Gestion des clés
- Serveurs de clés

19. Stéganographie
- Types
- Applications
- Détection

20. Exigences légales
- Gestion administrative
- Responsabilité individuelle
- Opérations privilégiées
- Types de mesures de sécurité
- Reporting