Management SI

Les essentiels de la cybersécurité

5 jours (35 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

- Présentation des Cyber-menaces actuelles et sites de référence sur la cybersécurité
- Directives et exigences de conformité
- Cyber rôles nécessaires à la conception de systèmes sûrs
- Cycle des attaques processus de gestion des risques
- Stratégies optimales pour sécuriser le réseau d'entreprise
- Zones de sécurité et solutions standards de protection

Pré-requis

- Connaissances en réseaux TCP/IP

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

- Professionnels de la sécurité informatique, personnels d'exploitation, administrateurs réseau et consultants en 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. Le champ de bataille

- La croissance d'Internet dans le monde entier
- Principes et objectifs de sécurité
- Terminologie des menaces et de l'exposition
- Documents et procédures de gestion des risques

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

2. Structure de l'Internet et TCP/IP
- Normes de conformité juridique
- Internet Leadership IANA
- Modèle TCP/IP

3. Évaluation de la vulnérabilité et outils
- Vulnérabilités et exploits
- Outils d'évaluation de la vulnérabilité
- Techniques d'attaques avancées, outils et préventions

4. Sensibilisation à la cyber sécurité
- Ingénierie sociale : Objectifs de l'ingénierie sociale, cibles, attaque, hameçonnage
- Sensibilisation à la cyber sécurité : Politiques et procédures

5. Cyber-attaques : Footprinting et scannage
- Footprinting
- Identification du réseau cible et sa portée
- Techniques de scannage de port

6. Cyberattaques : Effraction
- Attaque des mots de passe, escalade des privilèges
- Authentification et décodage du mot de passe

7. Cyberattaques : Porte dérobée et cheval de Troie (Backdoor and Trojans)
- Logiciels malveillants, Cheval de Troie, Backdoor et contre-mesures
- Communications secrètes
- Logiciel anti-espion
- Pratiques de lutte contre les logiciels malveillants

8. Évaluation et gestion des risques cybernétiques
- Actifs protégés : CIA Triad
- Processus de détermination de la menace
- Catégories de vulnérabilités
- Actifs de l'entreprise vs risques

9. Gestion des politiques de sécurité
- Politique de sécurité
- Références de politiques

10. Sécurisation des serveurs et des hôtes
- Types d'hôtes
- Directives de configuration générale et correctifs de sécurité
- Renforcement des serveurs et périphériques réseau
- Renforcement de l'accès sans fil et sécurité des VLAN

11. Sécurisation des communications
- Application de la cryptographie au modèle OSI
- Tunnels et sécurisation des services

12. Authentification et solutions de chiffrement
- Authentification par mot de passe de systèmes de chiffrage
- Fonctions de hachage
- Avantages cryptographiques de Kerberos
- Composants PKI du chiffrement à clef symétrique, du chiffrement asymétrique, des signatures numériques

13. Pare-feu et dispositifs de pointe
- Intégration de la sécurité générale
- Prévention et détection d'intrusion et défense en profondeur

- Journalisation

14. Analyse criminalistique
- Gestion des incidents
- Réaction à l'incident de sécurité

15. Reprise et continuité d'activité
- Types de catastrophes et Plan de reprise d'activité (PRA)
- Haute disponibilité
- Documentation de collecte de données
- Plan de Reprise d'Activité et Plan de Continuité d'Activité

16. Cyber-révolution
- Cyberforces, Cyberterrorisme et Cybersécurité : crime, guerre ou campagne de peur ?

17. LABS
- Lab1: Installation du lab
- Lab 2 : Comprendre TCP/IP
- Lab 3 : Evaluation de la vulnérabilité
- Lab 4 : Sensibilisation à la cybersécurité
- Lab 5 : Scannage
- Lab 6 : Cyber-attaques et mots de passe
- Lab 7 : Cyber-attaques et portes dérobées
- Lab 8 : Évaluation des risques
- Lab 9 : Stratégies de sécurité
- Lab 10 : Sécurité hôte
- Lab 11 : Communications secrètes
- Lab 12 : Authentification et cryptographie
- Lab 13 : Snort IDS
- Lab 14 : Analyse criminalistique
- Lab 15 : Plan de continuité des affaires