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

Mise à jour janv. 2023

Durée : 3 jours - 21 heures

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

PRÉREQUIS

- Une réelle connaissance informatique est nécessaire

PARTICIPANTS

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

MOYENS PÉDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
- Remise d'un support de cours.

MODALITÉS D'ÉVALUATION

- Feuille de présence signée en demi-journée
- Évaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Évaluation formative tout au long de la formation
- Évaluation sommative faite par le formateur ou à l'aide des certifications disponibles

MOYENS TECHNIQUES EN PRÉSENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

MOYENS TECHNIQUES DES CLASSES À DISTANCE

- A l'aide d'un logiciel comme Teams, Zoom... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants recevront une convocation avec lien de connexion
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

ACCESSIBILITÉ

- Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages sur l'ensemble de nos formations. Aussi, si vous rencontrez une quelconque difficulté, nous vous invitons à nous contacter directement afin d'étudier ensemble les possibilités de suivre la formation

Programme de formation

1. Concepts de base des réseaux

- Paquets et adresses
- Ports de services IP
- Protocoles sur IP
- TCP / UDP / ICMP
- DHCP / DNS
- VoIP (SIP)
- 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 responsabilités

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
- Pots de miel

11. Gestion des incidents de sécurité

- Préparation, identification et confinement
- Éradication, recouvrement et retour d'expérience
- Techniques d'enquête et criminalistique informatique
- Guerre de l'information offensive et défensive

12. Méthodes d'attaques

- Débordement de tampon
- Comptes par défaut
- Envoi de messages en masse
- Navigation web
- Accès concurrents

13. Pare-feu et zones de périmètres (DMZ)

- Types de pare-feu
- Architectures possibles : avantages et inconvénients

14. Audit et appréciation des risques

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

15. 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

16. PGP

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

17. Stéganographie

- Types
- Applications
- Détection

18. Sécurité opérationnelle

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