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

Mise à jour nov. 2023

Durée 3 jours (21 heures)

« Délai d'accès maximum 1 mois »

Infrastructure

OBJECTIFS PROFESSIONNELS

- - 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

PARTICIPANTS

-

PRE-REQUIS

- PUBLIC : Administrateurs systèmes et réseaux, responsables informatique et/ou sécurité
- PRÉ-REQUIS : Une réelle connaissance informatique est nécessaire

MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de
- 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.
- Remise d'un support de cours.

MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise 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. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

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.

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Programme de formation

1. Concepts de base des réseaux (02h15)

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

2. Sécurité physique (00h45)

- Services généraux
- Contrôles techniques
- Menaces sur la sécurité physique

3. Principes de base de la SSI (01h30)

- Modèle de risque
- Défense en profondeur
- Identification, authentification et autorisation
- Classification des données
- Vulnérabilités

4. Politiques de sécurité informatique (00h30)

- Principe
- Rôles et responsabilités

5. Plan de continuité d'activité (00h30)

- Exigences légales et réglementaires
- Stratégie et plan de reprise après sinistre

6. Analyse des conséquences (00h45)

- Évaluation de crise
- Facteurs de succès
- Fonctions business critiques

7. Gestion des mots de passe (01h00)

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

8. Sécurité Web (01h00)

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

9. Détection d'intrusion en local (00h30)

- Détection d'intrusion
- A quoi s'attendre

10. Détection d'intrusion en réseau (01h00)

- Outils
- Déni de service
- Réaction automatisée
- Pots de miel

11. Gestion des incidents de sécurité (01h00)

- 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 (01h30)

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

13. Pare-feu et zones de périmètres (DMZ) (00h30)

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

14. Audit et appréciation des risques (00h45)

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

15. Cryptographie (03h00)

- 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 (01h00)

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

17. Stéganographie (00h45)

- Types
- Applications
- Détection

18. Sécurité opérationnelle (01h45)

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