Fondamentaux techniques de la cybersécurité

Référence : **SECFONDX** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Bonnes connaissances en informatique.

PROFIL DES STAGIAIRES

• . • Administrateurs système ou réseau.

OBJECTIFS

• Maîtriser le vocabulaire et les concepts principaux du domaine. • Connaître différentes techniques d'attaque. • Choisir et appliquer les bonnes mesures de sécurité.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

SSI – principes de bases

- Pourquoi la SSI ?
- Notion de risque
- Les règles de base
- Contrôle d'accès : AAA ; Gestion des utilisateurs ; Authentification ; Gestion des privilèges

Cryptographie

- Concepts fondamentaux
- Fonctions de base : Chiffrement ; Hachage ; Signature
- Protocoles : TLS ; IPSec ; SSH
- PKI / IGC

Réseau

- Modèles théoriques : OSI, TCP/IP
- Attaques classiques : Découverte de ports ; Man-in-the-Middle
- Contrôle d'accès réseau
- Segmentation : Qu'est qu'une bonne architecture ? ; Comment segmenter son réseau ; VLAN ; Parefeu ; Proxy
- Réseaux sans fil
- Sécuriser le Cloud

Applications

- Architecture n-tiers
- Protocoles
- Authentification et sessions
- Top 10 de l'OWASP
- Buffer Overflow
- Processus de développement

Windows

- Installation
- Bitlocker
- Mesures Windows 10 : Device Guard ; Application Guard ; Exploit Guard
- Gestion des administrateurs

- Éviter le Pass-The-Hash

Linux

- Système de fichiers
- Minimisation
- Comptes utilisateurs
- Authentification
- SELinux
- AppArmor
- SSH
- Netfilter
- Journalisation

Gestion d'incidents

- SOC et CSIRT
- Gestion d'incidents
- La base : sauvegarde et journalisation
- Analyse inforensique