Parcours introductif à la cybersécurité

Référence : **SECINTROB** Durée : **10 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaître le guide d'hygiène sécurité de l'ANSSI ou connaître les bonnes pratiques telles qu'elles sont décrites dans ce guide.. • Fondamentaux réseaux : Modèle OSI - Equipement réseaux - Fonctionnement TCP/UDP - Service applicatif commun (http, DNS, SMTP, SSL).. • Fondamentaux système : Compréhension de base Windows (Service, fonctionnement) - Compréhension de base Linux (CLI, Service, fonctionnement).. • La compréhension de l'anglais est un plus. .

PROFIL DES STAGIAIRES

• Tout salarié souhaitant se former aux fondamentaux de la Cybersécurité personnel informatique en montée de compétences, personnel en reconversion, chefs de projets, consultants, tous les acteurs de l'environnement digital de l'entreprise (administrateur réseaux, community manager, etc.) . • Toute personne en responsabilité d'un ou plusieurs process clefs de l'entreprise. .

OBJECTIFS

• A l'issue de la formation, le participant sera capable de mettre en œuvre de manière opérationnelle les principes fondamentaux, les normes et les outils de la sécurité informatique.. • Il sera en mesure de : . • Détenir une vision globale de la cybersécurité et son environnement (enjeux, écosystème…). • Connaître les différents référentiels, normes et outils de la cybersécurité. • Appréhender les métiers liés à la cybersécurité. • Connaître les obligations juridiques liées à la cybersécurité. • Comprendre les principaux risques et menaces ainsi que les mesures de protection. • Identifier les bonnes pratiques en matière de sécurité informatique.

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

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

Jour 1

- Les enjeux de la sécurité des S.I
- Profils et motivations des attaquants
- La cybercriminalité
- Panorama des menaces (APT, Phishing, fraude, …)
- Panorama des cyberattaques 2020/2021
- Les piliers de la cybersécurité : CIDT
- Exercice sur les besoins de sécurité CIDT
- Les mécanismes de sécurité
- Menaces risque et vulnérabilités
- Les CVE
- Démonstration exploitation d'une vulnérabilité
- Les acteurs de la cybersécurité
- L'organisation de la cybersécurité en France
- La CNIL : La protection des données à caractère personnel
- Quizz

Jour 2

- Connaître son S.I

- Types de réseau et interconnexion
- Sécuriser son réseau
- Les accès distant
- Les administrateurs
- WiFi
- Durcissement des terminaux
- Gestion des utilisateurs (privilèges, authentification,…)
- La sécurité physique
- Les contrats
- La surveillance et la supervision
- Gestion des incidents de sécurité
- Plan de secours
- Audit
- Quizz

Jour 3

- Les outils de l'attaquant
- Les types d'attaques (physique, système, réseau, web,…)
- Les APT
- Les pentest
- Les typologies de pentest
- Les méthodologies de pentest
- Le cycle de l'attaquant
- Unified Kill Chain
- Quizz sur la sécurité offensive

Jour 4

- La reconnaissance passive
- Les renseignements d'origine source ouverte
- TP Reconnaissance passive / OSINT
- La reconnaissance active
- Les scans réseau & de ports
- TP reconnaissance active (nmap, metasploit,…)

Jour 5

- Attaque Man In The Middle
- TP Man In The Middle
- Exploitation de CVE
- Trouver et utiliser des scripts d'exploitation de faille
- TP exploitation de failles
- Attaques Applicatives
- TP Attaques applicatives
- La Post-Exploitation
- TP Mise en place d'une Backdoor

Jour 6

- Sécurité du réseau
- Le pare-feu
- L'anti-virus
- IDS/IPS
- La segmentation
- Exemple pratique de sécurisation d'un réseau
- TP Mise en place d'une politique de filtrage

Jour 7

- La cryptographie
- Chiffrement symétrique
- Chiffrement asymétrique
- Les signatures numériques
- Les autorités de certification / IGC
- Quizz sur la cryptographie
- Les VPN
- Le protocole TLS
- Le protocole SSH
- TP Cryptographie

Jour 8

- Hardening Linux
- Hardening Windows
- Hardening équipements réseaux
- TP Hardening

Jour 9

- Introduction iso 27000
- La gouvernance de la sécurité
- La sécurité en mode projet
- Les chartes des utilisateurs
- Charte de l'administrateur système et réseau
- PSSI
- Présentation des métiers de la cybersécurité
- Etude de cas : Audit d'une entreprise

Jour 10

- L'avenir de la cybersécurité
- Mise en situation

Dates de formation

- 26 et 27 septembre + 06 - 07 - 17 - 18 - 27 et 28 octobre + 03 et 04 novembre