Parcours introductif à la Cybersécurité

Référence : **SECINTRO** Durée : **8 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Connaître le guide d'hygiène sécurité de l'ANSSI ou connaître les bonnes pratiques telles qu'elles sont décrites dans ce guide. • 2-Fondamentaux réseaux : Modèle OSI - Equipement réseaux - Fonctionnement TCP/UDP - Service applicatif commun (http, DNS, SMTP, SSL). • 3-Fondamentaux système : Compréhension de base Windows (Service, fonctionnement) - Compréhension de base Linux (CLI, Service, fonctionnement). • 4-La compréhension de l'anglais est un plus. • 5-**Les journées de formation seront** : 09 10 22 et 23 Novembre et 06 07 13 et 14 D2cembre 2021.

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

• Acquérir la vision globale de la sécurité. • Connaître les référentiels de normes de la sécurité. • Connaître les obligations juridiques liées à la Cybersécurité. • Comprendre les nouveaux métiers liés à la Cybersécurité. • Comprendre les enjeux de la Cybersécurité. • Comprendre le cycle et la réflexion d'un attaquant. • Appréhender l'implémentation d'une 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

Jour 1

- Notions de sécurité
- Enjeux
- Appréhender les termes spécifiques à la sécurité
- Panorama 2017 de la sécurité
- Dimension géostratégique
- Les acteurs
- Les types de métiers
- Organisation de la sécurité
- Menaces risque et vulnérabilités
- Volets techniques de la sécurité
- Volets organisationnels de la sécurité
- Volets physiques de la sécurité
- Mener une veille pro active
- Manager la sécurité
- Aspects juridiques
- Aspects normatifs
- Quizz, bilan
- Travail personnel sur les notions de sécurité (à rendre sous deux semaines)

Jour 2

- Les volets de protection du SI
- Comprendre et agir avec le CID
- Le chiffrement
- Les droits
- L'authentification
- L'IAM
- Intégrer la mobilité
- Architecture et composants
- SIEM et SOC
- L'esprit du forensique
- Les incidents de sécurités : études et comportements
- Tds sur droits et authentification
- Bilan, question réponses, travaux personnels

Jour 3

- Revue des menaces
- Les types de logiciels malveillants
- Les phases d'une attaque
- Point sur les APT
- La force du Social engineering
- Les attaques physiques
- Les attaques sur les données
- Les attaques sur le web
- Les attaques sur les mails
- Autres vecteurs d'attaques
- Risques encourus
- Réponse à incident : adopter les réflexes et comportements
- Principes de reversing
- TDs, bilan, travaux personnels sur la mise en place des attaques et analyses. Quizz sur le juridique et risques encourus

Jour 4

- Sécurité des systèmes
- Vulnérabilités du micro processeur
- Etude des architectures systèmes
- Analyse de la mémoire
- Le BoF
- Le fuzzing
- La séparation des privilèges

Jour 5

- Hardening linux
- Hardening windows
- Hardening serveurs
- La sécurité dans le cloud
- Droits et devoirs au regard de la règlementation
- TDs, tp sur hardening systèmes, bof et fuzzing. Quizz sur droits et devoirs

Jour 6

- Sécurité du réseau
- Tcp-ip : forces et vulnérabilités
- Les composants
- Les équipements de sécurité
- Fw et ids : comprendre, implémenter et agir sur les règles
- Les VPN
- Protocole TLS
- Protocole SSH
- HTTPS

Jour 7

- Les communications unifiées
- Sécurité et IPV6
- Sécurité des systèmes mobiles
- Sécurité et IoT
- Les IGC
- Méthode pour appréhender la sécurisation du réseau
- Exemple d'architectures sécurisées
- TDs ips, fw. Etudes de cas architectures sécurisées. Tps fw ids, ssh, tls, ipv6, igc et vpn

Jour 8

- Introduction NIS
- Introduction iso 27000
- Introduction RGPD
- La gouvernance de la sécurité
- La sécurité en mode projet
- Les chartes des utilisateurs
- Charte de l'administrateur système et réseau
- PSSI
- Quizz sur normes et directives.
- Tps : suivant scénario rédaction chartes utilisateur, administrateur réseau et pssi