Les bases de la cybersécurité

Référence : **SECCYBERB** Durée : **3 jours** Certification : **Non**

CONNAISSANCES PREALABLES

• Connaître et comprendre le guide d'hygiène sécurité de l'ANSSI..

PROFIL DES STAGIAIRES

• Toute personne désireuse de découvrir les bases de la sécurité informatique..

OBJECTIFS

• Comprendre les fondamentaux de la sécurité informatique. • Connaître les conséquences possibles d'une attaque 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 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

Introduction à la sécurité informatique

- Les menaces et les risques
- La sécurité du poste de travail
- Le processus d'authentification
- Le cadre réglementaire et juridique
- Les bons réflexes

Les menaces et les risques

- Qu'est-ce que la sécurité informatique ?
- Comment une négligence peut-elle créer une catastrophe ?
- Les responsabilités de chacun
- L'architecture d'un SI et leurs vulnérabilités potentielles
- La sociologie des pirates. Réseaux souterrains. Motivations

Les fondamentaux de la sécurité des SI

- La gestion des risques et les objectifs de sécurité
- Le métier du RSSI. Les normes et les réglementations
- L'analyse des risques informatiques
- Le processus d'un audit de sécurité
- Le plan de secours et le coût de la sécurité
- Les solutions et les architectures de sécurité
- La supervision de la sécurité
- Les aspects juridiques. Les bonnes pratiques

La gestion des risques et les objectifs de sécurité

- La définition du risque et ses caractéristiques : potentialité, impact, gravité
- Les différents types de risques : accident, erreur, malveillance
- Les contre-mesures en gestion des risques : prévention, protection, report de risque, externalisation

La sécurité dans le cyberespace

- Le cyberespace et la sécurité de l'information

- Le pare-feu, la virtualisation et le Cloud Computing
- La sécurité des postes clients
- Les bases de la cryptographie
- Le processus d'authentification des utilisateurs
- La sécurité des réseaux sans fils. La sécurité des dispositifs mobiles
- La sécurité des logiciels. Les concepts de Security by Design et Privacy by Design
- La supervision de la sécurité