EduGroupe
Accompagner pour réussir

Les bases de la cybersécurité

Référence : **SECCYBERB** Durée : **3 jours (21 heures)** Certification : **Aucune**

Connaissances préalables

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

Profil des stagiaires

- Toute personne désireuse de découvrir les bases de la cybersécurité (sécurité informatique).

Objectifs

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

Certification préparée

- Aucune

Méthodes pédagogiques

- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire

Formateur

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

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

Contenu du cours

1. Introduction pour se former à la cybersécurité (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

2. 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

3. 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

4. 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

5. 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 fil. La sécurité des dispositifs mobiles
- La sécurité des logiciels. Les concepts de Security by Design et Privacy by Design
- La supervision de la sécurité

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.