Formation « Essentiels techniques de la cybersécurité »

Réf : ESSCYBER

La sécurité des systèmes d'information (SSI), aujourd'hui appelée cybersécurité, semble un jargon lointain pour certains. Il est important de démystifier en expliquant concrètement comment ça marche, et la meilleure des sensibilisations à la cybersécurité est la formation qui explicite. Grâce à sa vision pragmatique de la sécurité : connaitre l'attaque pour mieux se défendre, et aux différentes mises en application proposées, cette formation permet aux stagiaires de comprendre la nécessité de la SSI, d'en aborder les concepts théoriques (cryptographie, contrôle d'accès...) et d'identifier tous les domaines auxquels elle s'applique (système, réseau, applications...).

Objectifs

- Acquérir la connaissance des concepts fondamentaux de la SSI.
- Identifier les besoins en sécurité à tous les niveaux (système, réseau, applications...)
- Comprendre les différents types d'attaques
- Connaitre les mesures de sécurité permettant de les contrer

Durée & horaires

- 2 jours soit 14 heures
- De 09h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Toute personne souhaitant acquérir la compréhension de la cybersécurité
- Responsable de la sécurité (RSSI) de formation non technique
- Chef de projet et acteur d'un projet sécurité

Cette formation est accessible à un public plus large que la formation SECUCYBER en permettant aux personnes au profil non informaticien ou non technique d'obtenir une vision opérationnelle de la cybersécurité

Pré-requis

- Cette formation ne nécessite pas de prérequis particuliers, elle est accessible à un large public.

Méthode pédagogique

- Cours magistral avec de nombreux exemples pratiques

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Sécurité : concepts fondamentaux

- Concepts de base
- Gestion du risque : vulnérabilité, menace, impacts métiers
- Dans la peau d'un attaquant
- Principes de base : connaître son SI, moindre privilège, défense en profondeur

Cryptographie

- Chiffrement
- Hachage
- Signature
- TLS
- PKI/IGC

Sécurité des réseaux

- Principes de base
- Attaques
- Contrôle d'accès
- Filtrage et relayage
- Architecture sécurisée
- WiFi

Sécurité des applications

- Vulnérabilités web : le TOP 10 de l'OWASP
- Vulnérabilités mémoire
- Attaques et défenses
- Processus de développement

Sécurité des systèmes

- Contrôle d'accès
- Minimisation et durcissement
- Veille sécurité
- Mise à jour
- Sauvegarde
- Journalisation
- Protection du poste de travail
- Equipements mobiles