Soluce Technologies

Initiation technique à la cybersécurité

Programme synthétique de formation

Connaissance basique de Linux recommandée

3 demi-journées Durée	**10 à 15** Participants	**Sur site** Présentiel obligatoire
Public visé : étudiants en école d'ingénieur (BAC+3 / BAC+4)		

Découverte pratique des principales menaces cyber : périphériques physiques, réseaux sans fil et protection des données. Une formation technique fondée sur des démonstrations et des exercices de sécurité offensive en environnement contrôlé.

Ce que vous saurez faire

Identifier les menaces physiques Reconnaître les périphériques externes à risque et les vecteurs d'intrusion physique.
Comprendre les attaques réseau Identifier les mécanismes d'attaques sur les réseaux Wi-Fi et les techniques d'ingénierie sociale
Expérimenter en environnement contrôlé Utiliser des outils de pentesting et analyser le fonctionnement de scénarios d'attaque.
Protéger les données Distinguer les différentes techniques de protection de l'information et leurs cas d'usages.
Adopter les mesures de protection Utiliser des mesures de prévention adaptées aux accès physiques, réseaux et données.

Résultats attendus

À l'issue de la formation, les participants sauront reconnaître plusieurs vecteurs d'attaque courants, expliquer leur fonctionnement à partir d'expérimentations encadrées et identifier les principales mesures pour sécuriser les équipements, les réseaux et les données.

Méthodes pédagogiques

- Démonstrations en direct de scénarios d'attaque
- Ateliers collaboratifs en petit groupe
- Manipulations sur des machines isolées
- Quiz interactif

Programme détaillé

SÉANCE 1 (½ JOURNÉE) – Sécurité physique et périphériques externes

- Introduction à la cybersécurité dans son ensemble
- Panorama des accès physiques non autorisés et des périphériques
- Démonstration d'une intrusion simulée sur un poste de laboratoire
- Découverte et adaptation d'un firmware simple de périphérique USB malveillant
- Identification des mesures protections

SÉANCE 2 (½ JOURNÉE) - Réseaux, Wi-Fi et ingénierie sociale

- Introduction aux fondamentaux réseau et présentation des menaces
- Démonstration d'un faux point d'accès Wi-Fi avec portail de connexion
- Prise en main d'outils professionnels de pentesting
- Attaque par déni de service sur un réseau de laboratoire isolé
- Identification des mesures protections

SÉANCE 3 (½ JOURNÉE) – Cryptographie et protection des données

- Introduction aux notions essentielles de cryptographie
- Attaque sur des machines volontairement vulnérables
- Identification des mesures protections