

Résumé de la Formation en Cybersécurité

Présentation Générale

Cette formation en cybersécurité vise à fournir aux participants une compréhension solide des enjeux, des techniques de défense, et des outils essentiels à la protection des systèmes d'information. Elle s'adresse à des étudiants ou professionnels souhaitant acquérir ou renforcer leurs compétences en sécurité informatique.

Objectifs de la Formation

- Comprendre les enjeux stratégiques de la cybersécurité
- Identifier les menaces et les schémas d'attaque
- Apprendre les techniques de protection des systèmes et réseaux
- Utiliser les outils de détection, d'analyse et de défense
- Simuler des tests d'intrusion en environnement contrôlé

Contenus Clés

- Enjeux, lois et organisation de la cybersécurité
- Cryptographie, gestion des identités et des accès (MFA, PAM)
- Sécurisation des systèmes (Windows/Linux) et des réseaux (VPN, VLAN, pare-feu)
- Étude des menaces : ransomwares, phishing, malwares, APT
- Tests d'intrusion : méthodologies, outils (Nmap, Wireshark, Metasploit)
- Analyse de logs et détection avec SIEM
- Ateliers pratiques : campagne de phishing, détection de portes dérobées, simulation d'attaques, architecture sécurisée

Résultats Attendus

- Maîtriser les bases de la sécurité informatique
- Identifier et contrer les menaces courantes
- Manipuler des outils de sécurité et d'analyse
- Élaborer une architecture sécurisée adaptée
- Réaliser des simulations de tests d'intrusion
- Être préparé à des certifications de niveau débutant