Fiche du cours

60 h

Titre :

SEC200 - Introduction à la Cybersécurité

Description :

Ce cours initie les étudiants aux bases essentielles de la cybersécurité moderne. Il présente les concepts clés de protection des systèmes, les menaces les plus courantes et les principaux modèles de défense comme la triade CIA et le Zero Trust. Les participants découvrent les types d'attaques (phishing, ransomware, DDoS), les bases de la cryptographie, la gestion des accès et l'importance de la sécurité organisationnelle.
Ils se familiarisent également avec les outils de protection utilisés dans les environnements professionnels, notamment les pare-feu, les antivirus, les SIEM et les EDR, à travers une étude de cas pratique.

Objectifs :

- Comprendre les fondamentaux de la cybersécurité et les modèles de défense.*
- Identifier les menaces et vecteurs d'attaque courants.*
- Assimiler les bases de la cryptographie et de la gestion des accès.*
- Se familiariser avec les outils et pratiques utilisés dans les SOC.

Chapitres :

1. Panorama de la cybersécurité et état des menaces*
2. Principes fondamentaux : CIA triad, Zero Trust, AAA*
3. Types d'attaques : phishing, ransomware, DDoS, malware, insiders*
4. Introduction à la cryptographie*
5. Gestion des identités et accès : MFA, IAM*
6. Sensibilisation et sécurité organisationnelle*
7. Outils de défense : firewall, antivirus, SIEM, EDR*
8. Étude de cas pratique : attaque simulée et réponse étape par étape

À la fin :

Vous comprendrez les bases stratégiques et techniques de la cybersécurité et serez capable d'identifier les menaces, de reconnaître les vulnérabilités et d'appliquer les bonnes pratiques de sécurité de premier

niveau. Vous serez également en mesure de collaborer avec des équipes de sécurité et de vous préparer à des modules plus avancés comme la sécurité réseau, applicative ou cloud.