

Sommaire

1. **Introduction à la sécurité informatique**
 - Définitions et enjeux
 - Évolution des menaces numériques
 - Concepts fondamentaux de cybersécurité
2. **Sécurité des systèmes d'information**
 - Politique de sécurité
 - Gestion des risques
 - Analyse des vulnérabilités
3. **Cryptographie et mécanismes de protection**
 - Chiffrement symétrique et asymétrique
 - Fonctions de hachage
 - Signatures électroniques
 - Infrastructure à clé publique (PKI)
4. **Sécurité des réseaux**
 - Architecture réseau sécurisée
 - Protocoles sécurisés
 - Pare-feu et filtrage
 - Réseaux privés virtuels (VPN)
5. **Authentification et contrôle d'accès**
 - Gestion des identités
 - Authentification forte
 - Autorisations et privilèges
6. **Cybercriminalité et cyberattaques**
 - Types d'attaques informatiques
 - Malware, phishing, spyware
 - Techniques des cybercriminels
 - Études de cas réels
7. **Sécurité des applications et des services Internet**
 - Sécurité Web
 - Protection des bases de données
 - Sécurité des échanges électroniques
8. **Gestion des incidents et continuité**
 - Détection des intrusions
 - Réponse aux incidents
 - Sauvegarde et reprise après sinistre
9. **Gouvernance et audit de sécurité**
 - Normes ISO 27001
 - Audit et conformité
 - Gestion organisationnelle de la sécurité
10. **Cybersécurité moderne**
 - Nouvelles menaces
 - Cloud computing et sécurité
 - Sécurité mobile
 - Tendances futures
11. **Exercices corrigés**

- Études de cas
- QCM
- Exercices pratiques
- Corrigés détaillés