

Sommaire

1. Introduction à la sécurité des logiciels

- Enjeux de la sécurité informatique
- Types de menaces et vulnérabilités
- Notions de sûreté et de sécurité

2. Concepts fondamentaux de la sécurité

- Confidentialité, intégrité, disponibilité CIA
- Authentification et contrôle d'accès
- Gestion des identités

3. Analyse des risques

- Méthodes d'analyse des risques EBIOS, MEHARI...
- Identification des actifs et des menaces
- Évaluation des impacts

4. Architecture sécurisée des applications

- Principes de conception sécurisée
- Cloisonnement et défense en profondeur
- Sécurité des architectures distribuées

5. Sécurisation du cycle de développement logiciel SDL

- Intégration de la sécurité dans le développement
- Bonnes pratiques de codage sécurisé
- Revue de code et audits

6. Vulnérabilités et attaques

- Types d'attaques injection SQL, XSS, buffer overflow...
- Exploitation des failles
- Études de cas

7. Tests et validation de la sécurité

- Tests d'intrusion (pentest)
- Outils d'analyse statique et dynamique
- Certification et validation

8. Gestion des incidents de sécurité

- Détection et réaction
- Plan de continuité et reprise

- Journalisation et traçabilité

9. Normes et réglementations

- Normes ISO
- Cadres réglementaires
- Bonnes pratiques internationales

10. Perspectives et évolutions

- Nouveaux défis cloud, IoT, IA
- Tendances en cybersécurité