

Vous allez apprendre à

Cette formation vous permettra de passer en revue les techniques nécessaires pour auditer une application mobile iOS, ainsi que les vulnérabilités les plus courantes sur ce type d'applications.

Que vous soyez auditeur technique ou bien développeur, la connaissance des mauvaises pratiques de sécurité ainsi que les techniques d'exploitation est nécessaire. Venez approfondir vos connaissances sur les vulnérabilités liées à cette plateforme à travers cette formation !

Cette formation vous permettra de voir des méthodes d'audit avancées pour les application mobiles Android.

L'objectif de la formation est d'aller au-delà de la formation « Introduction ». Cette formation est entièrement axée sur la pratique.

Public visé

- RSSI, responsables sécurité, DSI, consultants SSI.
- Administrateurs système, cloud, réseau.
- Intégrateurs, architectes IT et toute personne impliquée dans la protection des données sensibles.

Les objectifs de la formation

À la fin de la journée, les participants seront capables de :

- Expliquer les mécanismes de base du chiffrement des données.
- Identifier les solutions adaptées selon l'environnement (cloud, datacenter, endpoint...).
- Gérer le cycle de vie des clés, certificats, tokens et secrets.
- Choisir des solutions de chiffrement adaptées à leur SI (on-prem et SaaS).
- Évaluer les exigences réglementaires et normatives associées au chiffrement.

Les prérequis de la formation

- Connaissances de base en systèmes d'information et sécurité.
- Aucune compétence mathématique en cryptographie requise.

Programme de la formation

Module 1 : Principes fondamentaux du chiffrement

- Chiffrement symétrique vs asymétrique
- Notions de clés, IV, algorithmes courants (AES, RSA, ECC)
- Hachage, signature, chiffrement de flux vs de blocs
- Risques liés à une mauvaise implémentation

Module 2 : Gestion des secrets et des clés

- Qu'est-ce qu'un secret ? Quelles sont les menaces ?
- Gestion du cycle de vie : création, stockage, rotation, révocation
- Vaults, HSM, TPM, KMIP, KMS
- Intégration avec CI/CD, DevOps, containers

Module 3 : Solutions de chiffrement selon l'environnement

- Sur le poste de travail / endpoint : BitLocker, FileVault, EFS
- Dans le datacenter : LUN chiffrés, bases de données, HSM
- Dans le cloud : BYOK / HYOK, KMS natifs, chiffrement S3/EBS, Azure Disk Encryption
- Sur IaaS : chiffrement des VM, disques, volumes, snapshots

Module 4 : Chiffrement & certificats : enjeux et pratiques

- Certificats, PKI, TLS, S/MIME, certificat machine vs utilisateur
- Cycle de vie des certificats : génération, déploiement, renouvellement
- Gestion multi-environnement : Cloudflare, Let's Encrypt, Microsoft CA...
- Risques liés aux certificats expirés ou mal gérés

Module 5 : Gouvernance, audit et conformité

- Recommandations ISO 27001 / 27018 / 27701
- Alignement avec le RGPD : chiffrement comme mesure technique
- Journalisation, preuve de conformité, auditabilité
- Bonnes pratiques d'effacement sécurisé

QCM final + échange sur l'intégration dans une politique SSI existante



2 Jours
14 Heures



Sur demande



+33 1 89 62 34 30



formation@acgcybersecurity.fr



Campus Cyber, Tour
Eria, 5 Rue Bellini 92800
Puteaux, FRANCE

Toutes nos formations sont
accessibles aux personnes en
situation de handicap.

ACG CyberAcademy 2025