+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 17/05/2024

S'inscrire

Formation Préparation à la Certification GIAC GMOB®

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

La certification GIAC GMOB® est bien plus qu'une simple accréditation, c'est une validation de vos compétences en sécurité des appareils mobiles. En obtenant cette certification, vous prouvez votre expertise dans un domaine crucial de la cybersécurité, renforçant ainsi votre crédibilité professionnelle.

L'examen GIAC GMOB® est conçu pour évaluer vos connaissances approfondies sur divers aspects de la sécurité des appareils mobiles. Avec des modules couvrants tout, de l'analyse des applications mobiles à la manipulation du trafic réseau, l'examen GIAC GMOB teste votre compréhension et votre capacité à relever les défis de sécurité actuels.

Notre formation GIAC GMOB® offre un parcours complet pour vous préparer à réussir l'examen avec succès. Vous acquérez les compétences nécessaires pour détecter les vulnérabilités, sécuriser les applications et protéger les données sur les appareils mobiles.

La formation est constamment mise à jour pour refléter les dernières avancées et les meilleures pratiques dans le domaine de la sécurité mobile.

Objectifs

- Maîtriser les techniques d'évaluation des applications mobiles
- Comprendre les faiblesses potentielles des canaux chiffrés et développer des techniques de protection du trafic réseau mobile
- Acquérir une compréhension approfondie des modèles de sécurité Android et iOS
- Apprendre à détecter, prévenir et atténuer les attaques de type Man-in-the-Middle (MitM) sur les communications mobiles

- Pratiquer la rétro-ingénierie des applications mobiles et mettre en place des mesures de protection contre le tampering

Public visé

- **Administrateurs réseaux**
- Consultants en sécurité
- Pentesters
- Ingénieurs en sécurité informatique
- Analystes en sécurité

Pré-requis

Aucun prérequis spécifique, mais avoir une expérience professionnelle dans la sécurité est un plus.

Note : Ambient IT n'est pas propriétaire de GIAC GMOB®, cette certification appartient à GIAC®, Inc.

PROGRAMME DE NOTRE FORMATION GIAC GMOB

INTRODUCTION À LA SÉCURITÉ DES APPAREILS MOBILES

- Vue d'ensemble de la sécurité des appareils mobiles
- Les menaces courantes sur les plateformes mobiles
- Cadre légal et normes de conformité
- Présentation des outils d'analyse de sécurité mobile
- Importance de la politique de sécurité mobile en entreprise

ANALYSE DES APPLICATIONS MOBILES

- Techniques d'évaluation des binaires d'applications mobiles
- Comprendre et analyser les permissions des applications
- Détecter les comportements potentiellement nuisibles
- Utilisation d'outils d'analyse statique et dynamique
- Études de cas sur les vulnérabilités courantes

ÉVALUATION DE LA SÉCURITÉ DES APPLICATIONS MOBILES

- Introduction au Mobile Application Security Verification Standard (MASVS)
- Auditer la sécurité d'une application mobile avec MASVS
- Bonnes pratiques de codage et de développement sécurisé
- Étude de la sécurité des sessions et du stockage des données

- Tests d'intrusion pour applications mobiles

ATTAQUE DU TRAFIC CHIFFRÉ

- Comprendre le SSL/TLS et les faiblesses potentielles
- Outils et techniques pour exploiter les canaux chiffrés
- Mise en place d'un environnement de test pour l'interception de trafic
- Analyse des données interceptées et détection de fuites d'informations
- Techniques de protection et de renforcement du chiffrement

GESTION DES APPAREILS ET APPLICATIONS ANDROID

- Configuration et structure des données sous Android
- Sécurité et gestion des applications Android
- Modèles de sécurité Android et implications pour la posture de sécurité
- Rooting, déverrouillage du bootloader et leurs implications sécuritaires
- Outils de gestion d'entreprise pour appareils Android

GESTION DES APPAREILS ET APPLICATIONS IOS

- Configuration et structure des données sous iOS
- Sécurité et gestion des applications iOS
- Modèles de sécurité iOS et implications pour la posture de sécurité
- Jailbreaking et ses implications sécuritaires
- Outils de gestion d'entreprise pour appareils iOS

MANIPULATION DU COMPORTEMENT DES APPLICATIONS MOBILES

- Techniques d'évasion de la sécurité pour tester les applications
- Modification des fichiers de configuration et des paramètres de l'application
- Utilisation de frameworks de test pour simuler des comportements d'application
- Détournement de la logique d'application pour révéler des vulnérabilités
- Automatisation des tests de sécurité des applications mobiles

MANIPULATION DU TRAFIC RÉSEAU

- Techniques pour capturer et manipuler le trafic réseau mobile
- Utilisation de proxies et analyseurs de réseau pour les tests de pénétration
- Simulation d'attaques sur réseaux sans fil et cellulaires
- Détection et prévention des attaques Man-in-the-Middle (MitM)
- Sécurisation des communications entre l'application et le serveur

ATTÉNUATION CONTRE LES LOGICIELS MALVEILLANTS ET LE VOL D'APPAREILS MOBILES

- Stratégies de protection contre les logiciels malveillants mobiles
- Solutions de sauvegarde et de restauration des données mobiles
- Technologies de chiffrement et de protection des données en repos et en transit
- Gestion des risques liés au vol ou à la perte d'appareils mobiles
- Utilisation des fonctionnalités de sécurité intégrées et des solutions MDM/EMM

RÉTRO-INGÉNIERIE ET SÉCURISATION DES APPLICATIONS MOBILES

- Concepts de base de la rétro-ingénierie des applications mobiles
- Outils et environnements pour la rétro-ingénierie
- Protection des applications contre la rétro-ingénierie
- Techniques de détection et de défense contre le tampering
- Évaluation des risques et mesures de sécurité pour les applications distribuées

SYNTHÈSE ET MISE EN PRATIQUE

- Révision des concepts clés et préparation à l'examen GIAC GMOB
- Ateliers pratiques et études de cas
- Simulation d'audit de sécurité d'une application mobile
- Stratégies pour maintenir la compétence en sécurité mobile
- Discussion sur les tendances émergentes et l'avenir de la sécurité mobile

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.