Sécurité des systèmes mobiles

Androïd / Ios

LE PUBLIC

Toute personne concernée par un projet mobile.

LES OBJECTIFS

Maîtriser les risques associés aux plateformes mobiles

Mettre en place les mesures de sécurité nécessaires pour faire face à ces risques

VOTRE FORMATION

DURÉE : 5 JOURS

35 heures

PROCHAINE SESSION :

6, 7, 8, 15, et 16 juillet 2020

LIEU : En distanciel

PRIX : 1 495 €

net de taxes

PRÉ-REQUIS

Bases en informatique et télécom (comprendre des termes comme serveur, firewall, Wifi, 5G, etc.).

Cette formation ne cherche pas mettre en œuvre la solution de tél ou tel éditeur mais à en dresser un inventaire objectif.

MODALITES

Formation 100 % à distance

De 4 à 16 participants

9h –17h30

Financement éligible au FNE Formation pour tout salarié d'entreprise en activité partielle

Matériel requis : Smartphone sous Androïd et Apple iOS. A défaut, prévoir un coût supplémentaire pour des logiiciels de simulation en ligne.

VOTRE CONTACT :

Andrea FALLOURD
Conseillère en formation
06 74 51 44 97
afallourd@itescia.fr

ITESCIA - Campus de Pontoise
8 rue Pierre de Coubertin
95300 PONTOISE

www.itescia.fr

VOTRE PROGRAMME

La plupart de nos vies numériques tournent autour de l'utilisation de smartphones et de tablettes, la sécurité mobile est devenue une préoccupation majeure en matière de sécurité. Ce cours examinera en profondeur tous les aspects de la sécurité mobile. A partir de l'évaluation des risques des applications mobiles, nous examinerons les différents dangers et menaces qui mettent en danger notre protection des consommateurs et des données. Nous couvrons des exemples de sécurité réelle soit dans le cadre de sécurité des smartphones, soit par des applications tierces.

Introduction sur les enjeux de la sécurité sur Mobile

PME, startups, grands comptes : des risques propres à chacun

Définir sa stratégie selon ses besoins

Identification de vulnérabilités des plates-formes mobiles

Menace et vulnérabilités sur Smartphones

Escalade de privilège (Jailbreak et Rooting)

Attaques sur les OS (iOS, Android, Windows Phone)

Sécurité par la gestion des appareils mobiles (MDM)

Définition et fonctionnement d'un MDM

Limite d'usage dans la zone (exemple de solution)

Renforcement logiciels (SE Android) et Trust Zone (étanchéité)

Contrôle de l'accès utilisateur au terminal

Sécurité par la gestion des applications (MAM)

Définition et fonctionnement d'un MAM

Isolation par les containers

Apps Stores privés et autorisés : API et connecteurs

Séparation des applications du terminal et du serveur

Sécurité par la gestion des contenus et données (MCM)

Définition du MCM (Mobile Content Management)

DLP, SIEM et stockage sécurisé cloud

Chiffrement (On Device Encryption FIPS 140-2 (AES))

Les différentes attaques possibles sur un téléphone volé

Récupérer les données d'une application mobile non sécurisée

Sécuriser les stockages de données en local

Le choix des algorithmes de chiffrement

Focus iOS : le Keychain

Focus Android : Keychain - Keystore Provider - AccountManager

Attaques « man in the middle »

Intercepter des appels réseaux non sécurisés (démonstration)

Livecode : mise en place du TLS pinning

Focus Android : utilisations de l'API Safety-Net

Attaques sur le binaire / le code de l'application

Décompiler une application Android récupérée sur le store

Obfusquer le code de son application Android avec Proguard et R8

Android attaques par l'exemple

Comprendre Android avec Termux

Reverse engineering des APK

Introduction à Drozer

Attaque MiTM pour Android et l'art du re-packaging

Introduction à Exposed et JDWP

iOS attaques par l'exemple

Introduction à iOS

C'est quoi le SCA

Le reverse engineering des IPA

Attaque MiTM pour iOS et l'art du repackaging