Sécurité des appareils et des applications mobiles, synthèse

Cours Synthèse de 1 jour - 7h
Réf : SPM - Prix 2024 : 950€ HT

Les terminaux mobiles s'intègrent de plus en plus dans notre environnement de travail et dans nos projets, et engendrent de nouveaux défis en termes de sécurité. Ce séminaire propose une synthèse des problématiques de sécurité posées par ces appareils : communication, stockage de données, publication d'applications...

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Identifier les services de sécurité des systèmes d'exploitation mobiles

Définir les règles de sécurité dans une conduite de projet mobile

Différencier les solutions de sécurité selon le terminal

Définir les critères de choix d'une solution MDM

Identifier les impacts du BYOD sur la sécurité

LE PROGRAMME

dernière mise à jour : 12/2019

1) Les terminaux

- Présentation et spécificités des mobiles, tablettes.
- Les systèmes (iOS, Android, BlackBerry) : architectures, configuration, sécurité données, réseau, applicative.
- Signature du Code. Protection Mémoire.
- Navigateurs, application client (user-agent) et son sandbox.
- Applications sandbox.
- Raccordement USB. Récupération de données, accès SSH. Limites et risques.

2) Bring Your Own Device - BYOD et Mobile Device Management

- Problématiques du BYOD, CYOD, COPE, BYOA.
- Enjeux du BYOD (sécurité, productivité, financier...). Premiers retours d'expérience.
- Problématique de nos données privées professionnelles.
- Solutions de virtualisation (vmWare, Citrix, Client Hyper-V), Desktops as a Service.
- Mobile Device Management : Présentation des solutions du marché (AirWatch, MobileIron...). Apple Configuration iPhone.
- Critères de sélection d'une solution MDM (logiciel, sécurité, gestion de parc matériel).
- MDM : présentation des solutions de Microsoft, Samsung Knox, Blackberry.

3) Critères de sécurité

- Présentation des risques selon l'OWASP (GoatDroid, IOS Project).
- Stockage de données métier, sessions, authentification (mémoire, SD, FS, keychain, etc.).
- Comprendre le Root Android, Jailbreaking.
- Protocoles d'échanges serveur.
- Impact des injections SQL et XSS dans les applications in-App, SMS.
- Solutions d'authentification, autorisation, biométrie.

PARTICIPANTS

Chefs de projet, développeurs, décideurs, marketeurs et toute personne souhaitant avoir une vue synthétique et précise sur la sécurité des appareils et des applications mobiles.

PRÉREQUIS

Aucune connaissance particulière.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Solutions de cryptographie (données, filesystem), backup restauration du terminal.
- Antivirus, antiphishing.

4) Développer une application dans un store

- Règles de publication AppStore, Google Play. Stores alternatifs, Store d'entreprise.
- Certificats de publication Apple, fichiers de provision, certificats.
- Google Licence LVL.
- Application IPA, APK, désassemblage.
- Impact des librairies, framework sur la sécurité de l'application.
- Gestion et contrôle distant du contenu.
- Comment tester une application ?
- Notification : externalisation, risque de spam, mécanismes.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 04 juil., 15 oct., 10 déc.	2024 : 27 juin, 08 oct., 03 déc.