Formation Sécurité des appareils et des applications mobiles, synthèse

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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...

Référence	SPM
Durée	1 jour (7h)
Tarif	970 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

le 16 octobre 2025

PARIS

le 9 octobre 2025

VOIR TOUTES LES DATES

Objectifs

| 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

Public

| Chefs de projet
| Développeurs
| Décideurs
| Marketeurs
| Toute personne souhaitant avoir une vue synthétique et précise sur la sécurité des appareils et des applications mobiles.

Prérequis

| Aucune

Programme de la formation

Les terminaux
| Présentation et spécificités des mobiles, tablettes.
| Les systèmes (IOS, Androïd, BlackBerry Windows) : 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.

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.

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 de Authentification, autorisation, émergence biométrie.
| Solutions de cryptographie (données, filesystem), backup restauration du terminal.
| Antivirus, antiphishing.

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.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.