Formation Sécurité des appareils et des applications mobiles

La sécurité de la mobilité informatique de bout en bout

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

L'apparition des tablettes et des smartphones dont l'utilisation va toujours croissante, y compris en environnement professionnel, conduit les entreprises à s'adapter à de nouveaux besoins mais aussi à de nouvelles contraintes. Et effectivement, si les déploiements de solutions mobiles sont souvent relativement indolores, donc finalement assez rapides, il ne faut pas pour autant, dans la précipitation, négliger l'étape vitale de la sécurité dont dépendra le bon fonctionnement des appareils et des applications. Après avoir mis l'emphase sur les vulnérabilités des plates-formes et des applications mobiles, ce séminaire proposera un état des lieux des technologies et solutions de sécurité disponibles sur le marché.

Référence	RES238
Durée	2 jours (14h)
Tarif	1 790 €HT

Objectifs

| Identifier les points de vulnérabilité des solutions de mobilité, de bout en bout
| Disposer d'une vision d'ensemble des technologies et des solutions déployées pour protéger les plates-formes et les applications mobiles
| Expliquer la sécurité des usages privés et professionnels dans le cadre du BYOD
| Identifier les métriques et critères de sélection des solutions

Public

| Responsables informatiques, consultants généralistes
| Directeurs et managers du SI souhaitant découvrir les nouvelles possibilités sur le champ de la mobilité
| Toute personne amenée à réaliser des choix techniques de solutions de sécurité des plates-forme

Prérequis

| Ce séminaire nécessite une connaissance sommaire de l'informatique

Programme de la formation

Identification de vulnérabilités des plates-formes mobiles
| Caractéristiques techniques et vulnérabilités des tablettes et Smartphones
| Risques d'escalade de privilège (Jailbreak et Rooting)
| Attaques d'Operating System (iOS, Android, Windows Phone)
| Niveaux d'attaque d'une solution de mobilité : plate-forme terminale, applications, réseaux mobiles, donnée (contenu)

Panorama des fournisseurs majeurs de solutions de sécurité (MDM, MCM, MAM...)
| Airwatch, Good Technology, MobileIron
| Citrix XenMobile, IBM, Microsoft, SAP/Afiria
| Vision et capacité opérationnelle des acteurs dans un marché en développement
| Commercialisation : appliance-serveur privé et Cloud SaaS des solutions de sécurité

Sécurité par la gestion des appareils mobiles (MDM)
| Description des caractéristiques communes des solutions MDM (Mobile Device

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 15 au 16 mai 2025
du 26 au 27 juin 2025

PARIS
du 15 au 16 mai 2025
du 26 au 27 juin 2025

AIX-EN-PROVENCE
du 15 au 16 mai 2025
du 26 au 27 juin 2025

BORDEAUX
du 26 au 27 juin 2025
du 28 au 29 août 2025

GRENOBLE
du 26 au 27 juin 2025
du 28 au 29 août 2025

LILLE
du 15 au 16 mai 2025
du 28 au 29 août 2025

LYON
du 26 au 27 juin 2025
du 28 au 29 août 2025

NANTES
du 15 au 16 mai 2025
du 26 au 27 juin 2025

VOIR TOUTES LES DATES

Management) : prise en main à distance, géolocalisation des terminaux, vérification de conformité....
| Utilisation limitée aux zones géographiques (exemple de solution)
| Renforcement des couches logicielles (SE Android) et création de la Trust Zone (étanchéité)
| Suivi de consommation
| Accès de l'utilisateur au terminal
| Métriques et critères essentiels de sélection des solutions

Sécurité par la gestion des applications (MAM)
| Description des caractéristiques communes des solutions MAM (Mobile Application Management) : mise à jour automatique des applications, installation interdite des Apps....
| Isolation par les containers
| Apps Stores privés et autorisés : intégration des applications de l'écosystème par des API et connecteurs
| Séparation des interactions entre les applications du terminal et du serveur
| Métriques de qualité et critères principaux de choix

Sécurité par la gestion des contenus et données (MCM)
| Définition du MCM (Mobile Content Management)
| Sécurité contre les fuites des données (DLP)
| Sécurité par la surveillance des activités (SIEM)
| Encryptions gérées des données (On Device Encryption FIPS 140-2 (AES))
| Cloud de stockage sécurisé et partagé pour les mobiles

Sécurité des terminaux mobiles personnels utilisés dans le cadre professionnel (BYOD)
| Définition du concept BYOD (Bring Your Own Device)
| Isolation par la virtualisation du terminal associée aux MDM et MAM
| Sécurité par la responsabilisation : fixation d'un cadre légal d'utilisation (chartre d'utilisation, confidentialité CNIL...)

Sécurité de la connectivité des terminaux aux serveurs d'applications
| Solutions existantes : VPN SSL, Firewall
| Authentification d'accès aux réseaux : NAC et RBAC
| Sécurité selon les types de réseaux GSM/4G et WiFi et les lieux de connexion

Impacts et grandes tendances
| Banalisation et abstraction des plates-formes terminales mobiles
| Convergence des solutions mobiles et traditionnelles fixes
| Refonte des dispositifs de sécurité actuels

Méthode pédagogique

Une emphase particulière est mise sur les aspects à prendre en compte pour garantir la sécurité des données de l'entreprise.Les retours d'expérience d'un consultant spécialiste de la sécurité et de la mobilité.Le discours est illustré de nombreux exemples concrets.

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.