

Sécurité des appareils et des applications mobiles

La sécurité de la mobilité informatique de bout en bout

 Présentiel ou en classe à distance



2 jours (14 h)

Prix inter : 1.850,00 € HT
Forfait intra : 4.050,00 € HT

Réf.: SR238



L'apparition des tablettes et des smartphones dont l'utilisation va toujours croissante, y compris en environnement professionnel, conduit les entreprises et organisations 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'accent 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.

A qui s'adresse cette formation ?



Pour qui

- 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-formes terminales et des applications mobiles



Prérequis

- Ce séminaire nécessite une connaissance sommaire de l'informatique
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

Programme

1 - 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)

2 - Panorama des fournisseurs majeurs de solutions de sécurité (MDM, MCM, MAM...)

- Airwatch, Good Technology, MobileIron
- Citrix XenMobile, IBM, Microsoft, SAP/Afria
- Vision et capacité opérationnelle des acteurs dans un marché en développement
- Commercialisation : appliance-serveur privé et Cloud SaaS des solutions de sécurité

3 - Sécurité par la gestion des appareils mobiles (MDM)

- Description des caractéristiques communes des solutions MDM (Mobile Device 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

4 - 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

5 - 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

6 - 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...)

7 - 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

8 - 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



Les objectifs de la formation

- 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
- Être en mesure de comprendre la sécurité des usages privés et professionnels dans le cadre du BYOD
- Connaître les métriques et critères de sélection des solutions



Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



Les points forts de la formation

- Une emphase particulière est mise sur les aspects à prendre en compte pour garantir la sécurité des données de l'entité.
- Les retours d'expérience d'un consultant spécialiste de la sécurité et de la mobilité.
- Le discours du séminaire est illustré de nombreux exemples concrets.
- 85% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.



Dates et villes 2026 - Référence SR238



Dernières places disponibles



Session garantie

Lille

du 12 mars au 13 mars

du 30 juil. au 31 juil.

du 29 oct. au 30 oct.

A distance

du 12 mars au 13 mars

du 30 juil. au 31 juil.

du 21 déc. au 22 déc.

du 28 mai au 29 mai

du 29 oct. au 30 oct.

Paris

du 12 mars au 13 mars

du 30 juil. au 31 juil.

du 21 déc. au 22 déc.

du 28 mai au 29 mai

du 29 oct. au 30 oct.

Marseille

du 12 mars au 13 mars

du 30 juil. au 31 juil.

du 29 oct. au 30 oct.

Rouen

du 12 mars au 13 mars

du 28 mai au 29 mai

du 29 oct. au 30 oct.

Sophia Antipolis

du 12 mars au 13 mars

du 28 mai au 29 mai

du 29 oct. au 30 oct.

Strasbourg

du 12 mars au 13 mars

du 28 mai au 29 mai

du 29 oct. au 30 oct.

Aix-en-Provence

du 12 mars au 13 mars

du 30 juil. au 31 juil.

du 29 oct. au 30 oct.

Toulouse

du 12 mars au 13 mars

du 30 juil. au 31 juil.

du 21 déc. au 22 déc.

Bordeaux

du 28 mai au 29 mai

du 29 oct. au 30 oct.

du 21 déc. au 22 déc.

Lyon

du 28 mai au 29 mai

du 29 oct. au 30 oct.

du 21 déc. au 22 déc.

Rennes

du 28 mai au 29 mai

du 30 juil. au 31 juil.

du 21 déc. au 22 déc.

Nantes

du 28 mai au 29 mai

du 30 juil. au 31 juil.

du 21 déc. au 22 déc.