Formation Mobile Device Management (MDM) - Avancé

Description de la formation Mobile Device Management

La mobilité informatique est aujourd'hui au cœur de l'organisation du travail des entreprises, avec une intégration de plus importante de la dématérialisation des services et des infrastructures. Les entreprises, quel que soit leur taille ou leur domaine d'activité, intègrent les usages des terminaux mobiles, smartphones, PC et tablettes au cœur de leur stratégie de sécurité.

Cette **formation pratique Mobile Device Management (MDM)** a pour vocation d'approfondir les concepts, les technologies MDM/MAM/MCM et les outils existants afin de comprendre et de se protéger efficacement contre les menaces intrinsèques à ces nouveaux usages.

Objectifs

À l'issue de cette **formation Mobile Device Management**, vous serez en mesure de:

- Maîtriser le vocabulaire et les concepts MDM, MAM et MCM
- Comprendre et définir une politique de sécurité mobile pour votre entreprise
- Choisir la meilleure solution MDM pour votre entreprise
- Enrôler et piloter la sécurité sur une flotte de terminaux mobiles

À qui s'adresse cette formation ?

Public :

Cette formation Mobile Device Management s'adresse principalement aux décideurs, architectes, administrateurs réseaux et systèmes concernés par les problèmes de sécurité, responsables de l'audit informatique, chefs de projets informatiques, correspondants informatiques.

Prérequis :

Pour suivre ce cours Mobile Device Management dans de bonnes conditions, il est nécessaire d'avoir des bases sur les OS mobiles en tant qu'utilisateur et de disposer d'une culture de base sur la sécurité informatique. La formation Comment gérer efficacement la mobilité d'entreprise (Réf. TEMM), constitue une base de connaissances complète.

Contenu du cours Mobile Device Management

Mobile Device Management : vocabulaire et concepts

Origines et historique : Nouveaux comportements et usages
Les enjeux du BYOD : entre sécurité et mobilité
BYOD, CYOD, COPE, BYOA : Les contraintes de sécurité à prendre en compte
Problématique des données privées / données professionnelles : Les apports de la Conteneurisation et du Sandboxing

Les terminaux

Présentation et spécificités des smartphones et tablettes.
Agent MDM résident, MDM Protocol et API MDM
Les systèmes (iOS, Android, BlackBerry) : architectures, configuration, sécurité données, réseau, applicative.
Navigateurs, application client
Récupération de données, accès SSH. Limites et risques.

Les risques et menaces en mobilité

Intrusion sur le SI depuis un terminal compromis
Propagation de code malicieux sur un smartphone

Non-respect des lois et de la règlementation

Publication d'applications malveillantes

Vol par usurpation d'identité, par attaque MITM (man in the middle)

Pertes de données, effacement du terminal

Déni de service (blocage des fonctions du terminal)

Fuite d'information (mail, fishing et autres)

Récupérations de données stockées

Travaux pratiques

Démonstrations d'attaques

Exemples de dégâts selon la force d'un virus

Stratégie de sécurité Mobile

Risques, usages, besoins : comment bien définir sa stratégie mobile

Les bonnes pratiques du déploiement

MDM, MAM, MCM : quelles solutions pour gérer sa flotte mobile ?

Présentation des solutions du marché

Les fonctionnalités disponibles

Critères de sélection d'une solution MDM (logiciel, sécurité)

Travaux pratiques

Mise en place d'une instance MDM de gestion d'une flotte mobile

Prise en main des fonctionnalités de configuration des terminaux (règle de déverrouillage, restrictions des fonctions des smartphones enrôlés, etc)

Politique de sécurité mobile : Création de règles de conformités des terminaux et procédures de contrôle des non conformités

Implémentation de mécanismes de défense en cas de menace

MDM : Exploitation et Maintien en condition de sécurité

Principes d'exploitation d'une flotte

Inventaire, gestion de parc et suivi de déploiement (politique de sécurité, applications, mise à jour d'OS)

Travaux pratiques

Gestion des politiques de configuration des terminaux

Création de profils utilisateurs et administrateurs

Enrôlement des terminaux

Déploiement d'une politique de sécurité

Inventaire des terminaux et suivi d'activation

MAM/MCM : pour se protéger des applications et des sites web malveillants

Comparaison MDM/MAM

Les cas d'usage

Gestion du cycle de vie (versioning) des applications ALM

Travaux pratiques

Création d'un catalogue d'applications d'entreprise

Mise en place de whitelist / blacklist d'applications

Suivi de déploiement d'une application d'entreprise sur un groupe de terminaux

Révocation, ré-enrôlement, remplacement de terminal d'un utilisateur

Maquette complète de synthèse

Mise en place d'un système MDM/MAM

Enrôlement, pilotage d'une flotte de terminaux par chaque stagiaire

Tests depuis des équipements mobiles en couverture 3G/4G et wifi

Travaux Pratiques

Cette formation est ponctuée de nombreux travaux pratiques et démonstrations.

Remarque : l'ensemble des travaux pratiques est également réalisable à distance si vous optez pour cette formule.