



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Mobile Device Management (MDM)

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

La mobilité informatique est aujourd'hui au coeur de l'organisation du travail des entreprises, avec une intégration de plus en 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 coeur 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

- | Maîtriser le vocabulaire et les concepts MDM, MAM et MCM
- | 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
- | Approfondir les concepts, les technologies MDM/MAM/MCM et les outils existants.

Public

| décideurs, architectes, administrateurs réseaux et systèmes concernés par les problèmes de sécurité, responsables de l'audit informatique, chefs de projets informatiques, correspondants informatiques.

Prérequis

- | 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" (TEMM), constitue une base de connaissances complète.

Programme de la formation

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 réglementation

Référence	MDMA
Durée	3 jours (21h)
Tarif	2 090 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

- du 21 au 23 décembre 2026
- du 12 au 14 avril 2027
- du 27 au 29 octobre 2027

PARIS

- du 21 au 23 décembre 2026
- du 12 au 14 avril 2027
- du 27 au 29 octobre 2027

[VOIR TOUTES LES DATES](#)

- | 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

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.