Gérer et sécuriser des Mac et des appareils iOS avec Mosyle Fuse

Référence Agnosys	SS/GSMF
Durée	3 jours
Certification	Non
Support de cours	En français

Description

Dans un contexte où la cybersécurité est un enjeu majeur, Mosyle Fuse propose une solution tout-en-un pour assurer la gestion et la sécurisation des appareils Apple dans les petites et moyennes entreprises. Depuis une interface unique, les administrateurs peuvent déployer, configurer et mettre à jour les appareils inscrits, appliquer des stratégies de sécurité contre les menaces et bloquer l'accès aux sites malveillants et aux contenus inappropriés. Cette formation vous guidera dans la mise en œuvre de Mosyle Fuse, en vous permettant d'exploiter ses fonctionnalités essentielles pour contribuer à un environnement informatique robuste et contrôlé, tout en respectant un budget maîtrisé.

Objectifs

• Savoir déployer et configurer des Mac, des iPhone et des iPad avec Mosyle Fuse
• Savoir gérer les appareils avec des profils de configuration et des commandes MDM
• Savoir mettre à jour les appareils de manière centralisée
• Savoir appliquer des stratégies de sécurité pour une protection contre les menaces
• Savoir bloquer l'accès aux sites malveillants et aux contenus inappropriés

Qui peut s'inscrire ?

Cette formation s'adresse aux administrateurs système des petites et moyennes entreprises, ainsi qu'aux consultants Apple responsables de mettre en place une solution à la fois accessible et efficace pour la gestion et la sécurisation d'une flotte de Mac et d'appareils iOS.

Pré-requis

Pour suivre cette formation, vous devez disposer des connaissances attendues pour un technicien assurant le support au quotidien des Mac et des appareils iOS équipés de versions de macOS et d'iOS sorties voici moins de trois ans.

Pour vous assurer de disposer de ces connaissances, nous vous invitons à consulter les contenus des deux formations suivantes et au besoin, à vous y inscrire :
- Support macOS : les clés d'une assistance aux utilisateurs réussie (SE/SUPMOS)
- Support iOS : prise en main et assistance aux utilisateurs (IPD/SUPIOS).

Veuillez noter que si vous disposez des certifications Apple Certified Support Professional ou Apple Certified IT Professional obtenues voici moins de trois ans, vous pourrez également suivre cette formation dans les meilleures conditions.

Nous insistons sur le fait que cette formation est centrée sur la gestion et la sécurisation des Mac et des appareils iOS avec Mosyle Fuse et qu'elle n'inclut pas la découverte des systèmes d'exploitation macOS et iOS.

Participants et matériels sous la responsabilité d'Agnosys

Cette formation est limitée à six participants maximum.

La classe sera équipée d'une instance Mosyle Fuse, ainsi que des Mac et des appareils iOS nécessaires pour les démonstrations réalisées par le formateur.

Matériels sous la responsabilité exclusive des participants

Chacun des participants devra être équipé sous sa responsabilité :
- d'un Mac de test équipé de la version la plus récente disponible du système d'exploitation macOS, sur l'assistant de configuration initiale
- d'un iPad de test équipé de la version la plus récente disponible du système d'exploitation iPadOS, sur l'assistant de configuration initiale
- d'un réseau Wi-Fi basique avec authentification WPA/WPA2/WPA3
- d'un compte Apple personnel fonctionnel (authentification à deux facteurs activée).

Les processus d'inscription automatisée des appareils Apple (Automated Device Enrollment) seront traités par le formateur sous la forme de démonstrations.

Attention — Le Mac et l'iPad seront effacés pendant la formation et ne doivent donc pas contenir de données. Ils ne doivent pas être inscrits dans une solution MDM. Ils peuvent appartenir à un programme de déploiement Apple mais ne doivent pas être associés à un profil d'inscription automatisée des appareils. Le Mac de test ne doit pas être une machine virtuelle (le formateur ne gèrera pas cette spécificité).

Recommandation — Pour fluidifier la réalisation des travaux pratiques, notamment lors des tâches requérant un changement de compte utilisateur, nous recommandons aux participants de suivre la formation depuis un autre ordinateur Mac ou PC ou une tablette, équipé d'une caméra et d'un micro, qui servira uniquement à l'utilisation du logiciel Zoom et à l'affichage des ressources du cours.

Sujets traités

Infrastructure

– Modèle de déploiement moderne
– Composants rendant possible un déploiement moderne
– Présentation de Mosyle Fuse
– Présentation du programme de déploiement Apple Business Manager
– Présentation du cadre de gestion des Mac et des appareils iOS
– Flux requis
– Fonctionnement du Push via APNs
– Configuration initiale et renouvellement du certificat Push
– Configuration d'une identité de supervision dans Apple Configurator 2

Travaux pratiques :
– Préparation du Mac et de l'appareil iOS pour les exercices
– Connexion à Mosyle Fuse
– Supervision manuelle d’un appareil iOS avec Apple Configurator 2

Inscription des appareils

– Modèle de déploiement One to One (1 appareil, 1 utilisateur régulier)
– Inscription des appareils et inscription automatisée des appareils
– Configuration de Mosyle Fuse pour l'inscription automatisée des appareils
– Ajout d'un appareil à Apple Business Manager avec Apple Configurator pour iPhone
– Synchronisation des appareils entre Apple Business Manager et Mosyle Fuse
– Gestion des profils d'inscription automatisée des appareils
– Inscription d’un Mac et d'un appareil iOS en inscription automatisée des appareils

Travaux pratiques :
– Inscription d’un Mac et d'un appareil iOS depuis un navigateur Web
– Association des appareils inscrits à des groupes d’appareils
– Association des appareils inscrits à des utilisateurs

Distribution d'applications

– Acquisition en masse de licences d’apps
– Sites et jetons par site
– Transfert de licences entre sites
– Délégation
– Moyens de paiement et crédit VPP
– Distribution multinationale
– Configuration de Mosyle Fuse pour la distribution gérée

Travaux pratiques :
– Assignation des apps pour un déploiement requis ou à la demande
– Distribution d’une app de l’App Store
– Distribution d’une app du catalogue Mosyle
– Distribution d'une app encapsulée dans un paquet (PKG)
– Configuration des apps iOS déployées (AppConfig)

Gestion des appareils

– Inventaire des appareils
– Bénéfices de la supervision
– Profils de configuration
– Gestion déclarative des appareils (Declarative Device Management)
– Configuration des mises à jour
– Commandes MDM

Travaux pratiques :
– Distribution d’une configuration Wi-Fi
– Application de restrictions et de réglages
– Configuration des mises à jour macOS et iOS via la gestion déclarative des appareils

Sécurité et confidentialité avec les technologies Apple

– Puce Apple silicon, Secure Boot
– Sécurité du matériel, du système, des données et des apps
– Verrouillage d’activation
– Règles de mot de passe et de code de verrouillage
– FileVault, SecureToken et Bootstrap Token
– Firewall applicatif

– Gatekeeper
– Approbation des System Extensions
– Réglages de confidentialité et Privacy Preferences Policy Control (TCC)
– Séparation transparente des données professionnelles et personnelles
– Gestion de l'ouverture des sources gérées dans des destinations non gérées
– Gestion de l'ouverture des sources non gérées dans des destinations gérées
– Domaines gérés
– Mode perdu

Travaux pratiques :
– Activation de FileVault et du Firewall applicatif
– Configuration de Gatekeeper
– Configuration d'un code de verrouillage
– Gestion des flux de données (sources gérées vers destinations non gérées)
– Mode perdu et géolocalisation

Sécurité et conformité avec les technologies Mosyle Fuse

– Présentation du module Sécurité
– Activation des règles d'un référentiel de sécurité et des remédiations automatisées
– Utilisation des groupes de sécurité comme périmètres d'autres réglages
– Configuration de l'outil de détection et de suppression des logiciels malveillants
– Configuration de la fonction "Administrateur à la demande"
– Configuration de la fonction "Confiance zéro automatisée"

Travaux pratiques :
– Activation des règles d'un référentiel de sécurité et des remédiations associées
– Configuration de l'outil de détection et de suppression des logiciels malveillants
– Vérification du fonctionnement de l'outil avec un exemple de logiciel malveillant
– Utilisation de la fonction "Administrateur à la demande"
– Observation des journaux d'activité

Filtrage de contenu

– Présentation du filtrage DNS
– Configuration des réglages de confidentialité et de journalisation
– Configuration de la page de blocage
– Limitation des risques de contournement
– Sélection des catégories filtrées
– Blocage des domaines malveillants, récents, par pays hôte
– Gestion des listes sûres et d'exclusions
– Configuration des alertes

Travaux pratiques :
– Activation du filtrage DNS
– Visualisation des configurations réseau déployées sur les appareils
– Vérification du fonctionnement du filtrage de contenu
– Observation des journaux d'activité

Réinitialisation locale et à distance

– Réinitialisation locale d’un Mac et d’un appareil iOS
– Réinitialisation à distance d’un Mac et d’un appareil iOS

Travaux pratiques :
– Réinitialisation à distance d’un appareil iOS
– Réinitialisation locale d’un Mac

AGNOSYS Conseil - Audit - Formation
Consultants Network
jamf SERVICES Partner
01 64 53 25 25 www.agnosys.com contact@agnosys.fr