Sécuriser un Mac avec les technologies Apple

Référence Agnosys	SE/SMTA
Durée	3 heures
Certification	Non
Support de cours	En français

Description

Dans un contexte où les ordinateurs sont de plus en plus utilisés en mobilité avec des données hébergées massivement dans des infrastructures en Cloud et des tentatives d'attaques toujours plus fréquentes, cette formation vous propose d'étudier les principales technologies Apple qui participent à la sécurisation d'un Mac et de son système d'exploitation macOS. Après en avoir compris les bénéfices et le fonctionnement, vous apprendrez à les mettre en œuvre à travers des démonstrations et des exercices pratiques.

Objectifs

Les participants découvriront et apprendront à mettre en œuvre les principaux mécanismes de sécurité intégrés dans le matériel Mac, dans le système d'exploitation macOS et dans les services Apple associés.

Qui peut s’inscrire ?

Tout utilisateur d'un Mac désireux de protéger son équipement contre des accès malveillants à ses données personnelles ou professionnelles et souhaitant pouvoir réagir efficacement en cas de destruction, de perte ou de vol de son équipement.

Pré-requis

Avant de s’inscrire à cette formation, les stagiaires doivent déjà avoir utilisé un Mac et posséder de bonnes notions sur le fonctionnement de macOS avec la version la plus récente disponible du système d'exploitation.ou bien avoir suivi la formation Premiers contacts avec mon Mac et macOS.

Participants et matériels

Cette formation est limitée à six participants maximum.

Les démonstrations seront réalisées avec un Mac avec la version la plus récente disponible du système d'exploitation.

Si vous souhaitez reproduire les démonstrations du formateur pendant le temps de la formation, vous devez disposer d'un Mac sous macOS avec la version la plus récente disponible du système d'exploitation. Cet appareil ne doit pas contenir de données sensibles non sauvegardées sous votre seule responsabilité.

Si cela s'avère utile, le formateur pourra observer l'écran de votre Mac et ainsi vous guider plus facilement dans la réalisation des manipulations nécessaires au bon déroulement de la formation.

Sujets traités

Principales technologies Apple de sécurisation Mac et macOS

– Mots de passe
– Processeur M1/M2 et puce de sécurité T2
– Verrouillage du stockage interne et chiffrement des données (FileVault 2)
– Sécurité des applications (Gatekeeper, AppStore)
– Confidentialité des données (Transparency Consent and Control)
– Déverrouillage et authentification biométrique (TouchID)
– Gestion centralisée avec MDM
– Volume système protégé par un sceau cryptographique (SSV)

Présentation des différents types de mot de passe

– Mot de passe de compte utilisateur
– Mot de passe de trousseau d'accès
– Mot de passe d'identifiant Apple et/ou de compte iCloud
– Mot de passe de programme interne (Firmware) sur Mac Intel

Partie pratique :
– Identification des différents mots de passe
– Utilisation de l'assistant mot de passe

Trousseau d'accès

– Rôle et paramétrage
– Utilisation du trousseau d'accès
– Gestion de la perte du mot de passe du trousseau

Partie pratique :
– Découverte et utilisation du trousseau d'accès
– Création d'une note sécurisée

Processeur M1/M2

– Identification de la présence d'un processeur M1/M2 sur un Mac
– Fonctions de sécurisation assurées par le processeur M1/M2
– Réglages de sécurité disponibles et implications

Partie pratique :
– Modification des réglages de sécurité liés au processeur M1/M2

Puce de sécurité T2

– Identification de la présence d'une puce de sécurité T2 sur un Mac
– Fonctions de sécurisation assurées par la puce de sécurité T2
– Réglages de sécurité disponibles et implications

Partie pratique :
– Modification des réglages de sécurité liés à la puce de sécurité T2

Identifiant Apple et compte iCloud

– Changement du mot de passe depuis le Mac ou depuis le site appleid.apple.com
– Localiser (Verrouiller, Effacer)
– Verrouillage d'activation (Mac M1/M2 / Intel T2)
– Génération d'un mot de passe d'application

Partie pratique :
– Visualisation de la position du Mac
– Gestion des paramètres de sécurité de l'identifiant Apple et du compte iCloud

FileVault 2

– Présentation de la technologie
– Verrouillage du stockage interne (Mac M1/M2 / Intel T2)
– Chiffrement des données (Mac Intel non T2)
– Affichage à l'écran ou séquestre dans iCloud de la clé de secours
– Séquence de démarrage d'un Mac M1/M2 avec FileVault 2 activé
– Séquence de démarrage d'un Mac Intel avec FileVault 2 activé
– Dépannage en cas d'oubli du mot de passe de compte utilisateur
– Chiffrement des données des volumes externes

Partie pratique :
– Activation de FileVault 2
– Utilisation de la clé de secours

Contrôles d'accès obligatoires

– La mise en bac à sable des applications
– Le Temps d'écran
– Les extensions du noyau (System Extensions et Kernel Extensions)
– La Protection de l'intégrité du système (SIP)
– Le Transparency Consent and Control (TCC)
– La technologie GateKeeper et la notarisation
– L'installation d'applications sûres depuis l'App Store
– Les préférences gérées via MDM

Partie pratique :
– Démonstration des contrôles d'accès obligatoires

Partition de secours macOS

– Démarrage sur la partition de secours
– Outils disponibles
– Instantanés locaux
– Réinstallation de macOS (le plus récent, d'origine, etc.)

Partie pratique :
– Démonstration de l'usage de la partition de secours

Autres technologies de protection du système

– Volume système protégé par un sceau cryptographique
  - meilleure protection contre les altérations malveillantes
  - lancement des mises à jour en arrière plan
– XProtect
– XD (Execute Disable)
– Address Space Layout Randomization (ASLR)
– Outils complémentaires de suppression de logiciels malveillants

Questions/Réponses sur les sujets abordés pendant la formation

Consultants Network

jamf SERVICES Partner

01 64 53 25 25 **www.agnosys.com** **contact@agnosys.fr**