

Évaluer et renforcer la conformité et la sécurité de macOS



Référence Agnosys	SE/CSMOS
Durée	1 jour
Certification	Non
Support de cours	En français

Description

Dans un monde où les cybermenaces évoluent constamment, il est essentiel de garantir que vos systèmes macOS répondent aux normes de sécurité les plus strictes et respectent les réglementations en vigueur. Cette formation est conçue pour vous fournir les connaissances et les outils nécessaires afin d'évaluer de manière approfondie l'état actuel de la conformité et de la sécurité de vos Mac, et pour mettre en œuvre des stratégies efficaces pour renforcer ces aspects.

Afin de pouvoir mettre en œuvre dans leur organisation les connaissances acquises dès leur retour de formation, les participants se verront remettre une licence macOS Compliance Spotter Essential d'une durée de 2 mois (support sans engagement via le canal dédié #compliancespotter sur le Mac Admins Slack).

Objectifs

- Comprendre les menaces et les vulnérabilités spécifiques à macOS
- Identifier les différents mécanismes de sécurité intégrés au niveau logiciel et matériel
- Évaluer la conformité d'un Mac par rapport à un référentiel de sécurité
- Configurer macOS pour une conformité et une sécurité optimales
- Mettre en œuvre des outils tiers pour améliorer ces aspects

Qui peut s'inscrire ?

Cette formation est destinée aux responsables de la conformité et aux administrateurs système qui ont pour mission de garantir la sécurité des données, le respect de la vie privée des utilisateurs, ainsi que la protection des équipements informatiques au sein de leur organisation.

Pré-requis

Pour profiter pleinement de cette formation, il est recommandé de disposer au préalable d'une expérience pratique d'administration et de gestion au quotidien du système d'exploitation macOS, ou bien d'avoir suivi la formation Administration et support de macOS (SE/ASMOS).

Participants et matériels mis à disposition

Cette formation est limitée à huit participants maximum.

La classe sera dotée d'une solution MDM Mosyle Business et des Mac requis 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
- configuré avec un compte administrateur local connu
- non inscrit dans une solution MDM
- non équipé d'une solution de sécurité interdisant un accès complet à Internet.

Sujets traités

Chapitre 1 : Introduction à la conformité et à la sécurité sur macOS

- Les concepts liés de conformité et de sécurité
- État actuel des menaces
 - Aperçu des principales menaces de sécurité pour macOS
 - Exemples de cas de cyberattaques sur macOS
- Vulnérabilités courantes
 - Les faiblesses exploitables dans macOS
 - Importance de l'installation des mises à jour de sécurité

Travaux pratiques :

- Préparation du Mac pour les exercices
- Accès à la console d'administration de Mosyle Business
- Inscription du Mac dans Mosyle Business

Chapitre 2 : Évaluation de la conformité d'un Mac

- Présentation de macOS Security Compliance Project
 - Projet Open source pour développer et maintenir des directives de sécurité
 - Application d'un référentiel de sécurité
 - Évaluation de la posture d'un Mac tout au long de son exploitation
- Présentation de Jamf Compliance Editor
 - Génération des ressources depuis l'outil
 - Identification des profils de configuration pour le durcissement
 - Identification du script de remédiation et d'analyse
 - Identification du fichier de configuration pour l'application des règles
- Exécution manuelle d'une analyse pour obtenir un score initial de conformité

Travaux pratiques :

- Installation de Jamf Compliance Editor
- Génération des ressources pour le référentiel de sécurité "CIS Benchmark - Level 1"
- Identification des ressources générées
- Exécution manuelle d'une analyse pour obtenir le score initial de conformité

Chapitre 3 : Optimisation de la sécurité d'un Mac

- Présentation des mécanismes de sécurité intégrés
 - Secure Enclave
 - Démarrage sécurisé et démarrage depuis un volume externe
 - Propriété du volume
- Paramètres de sécurité de base
 - Configuration du pare-feu
 - Activation de FileVault pour le verrouillage du volume de démarrage
- Paramètres de sécurité avancés
 - Contrôle de l'intégrité du système (SIP)
 - Utilisation de Gatekeeper pour contrôler les applications autorisées
 - Verrouillage d'activation et verrouillage à distance
 - Volume système en lecture seule et volume SSV
 - Recovery password (fonctionnalité MDM)
- Bonnes pratiques de gestion des comptes utilisateurs
 - Limitation des comptes administrateurs
 - Implémentation d'une solution de rotation de mot de passe (EasyLAPS)
 - Utilisation des comptes standards et gestion des privilèges
 - Le mode isolement
 - Le cas du compte invité et de FileVault
 - Authentification à deux facteurs (2FA) pour l'accès aux services
- Politiques de mot de passe
 - Configuration des exigences de mot de passe fort

- Gestion des expirations et des réinitialisations de mot de passe

Travaux pratiques :

- Configuration locale du pare-feu (blocage du service de partage d'écran)
- Configuration de FileVault 2 par profil de configuration
- Configuration de Gatekeeper par profil de configuration
- Configuration d'une règle de mots de passe par profil de configuration

Chapitre 4 : Sécurisation des données et des applications

- Configuration des paramètres de confidentialité et de sécurité (TCC)
- Protection des données
 - Stratégies de sauvegarde et de restauration
 - Utilisation de Time Machine de manière sécurisée
- Protection des applications
 - Sandboxing des applications
 - Saisie sécurisée dans le Terminal

Travaux pratiques :

- Configuration d'une sauvegarde chiffrée
- Chiffrement de volumes externes
- Gestion du TCC par profil de configuration
- Vérification qu'une application est sandboxée

Chapitre 5 : Sécurisation des accès réseaux et des services

- Configuration sécurisée des services réseau
 - Sécurisation des partages de fichiers et de l'accès à distance (SSH)
 - Connexion automatique à des réseaux Wi-Fi
- VPN et accès sécurisé à distance

Travaux pratiques :

- Configuration d'une connexion VPN par profil de configuration

Chapitre 6 : Utilisation des outils de sécurité intégrés

- XProtect et MRT (Malware Removal Tool)
- Rapid Security Responses
- Utilisation de la Console
- Surveillance et analyse des logs

Travaux pratiques :

- Vérification des versions de XProtect via SilentKnight

Chapitre 7 : Utilisation d'outils de conformité et de sécurité tiers

- Antivirus et logiciels anti-malware
 - Présentation des solutions populaires pour macOS
 - Suppression des extensions indésirables de Safari
- Surveillance et gestion centralisée de la sécurité
 - Solutions MDM (Mobile Device Management) pour macOS (Jamf, Mosyle, etc.)
 - Solutions EDR (SentinelOne, Microsoft Defender, Jamf Protect, etc.)
 - Automatisation de l'analyse de conformité (macOS Compliance Spotter)
 - Gestion des appareils perdus
 - Gestion du verrouillage d'activation (depuis le MDM, ABM ou ASM)

Travaux pratiques :

- Surveillance de macOS via le MDM
- Vérification des extensions dans Safari
- Déclenchement manuel d'une remédiation suivie d'une analyse de conformité mSCP
- Inscription au canal dédié #compliancespotter sur le Mac Admins Slack



Consultants Network

01 64 53 25 25

www.agnosys.com



SERVICES
Partner

contact@agnosys.fr

© 2024 Agnosys. Tous droits réservés. R.C.S. EVRY B 422 568 121.

Enregistré sous le numéro 11910439891. Cet enregistrement ne vaut pas agrément de l'État.