jamf

LIVRE BLANC

Checklist de sécurité macOS :

Mettre en œuvre les critères du Center for Internet Security (CIS) pour macOS

Recommandations pour sécuriser macOS

Les critères du Center for Internet Security (CIS) pour macOS offrent une liste de contrôle complète qui aide les entreprises à sécuriser leurs Mac. Jamf, la référence pour la gestion et la sécurité des appareils Apple au travail, a produit ce livre blanc pour vous accompagner dans la mise en œuvre des recommandations de cet organisme indépendant.

jamf PRO

QU'EST-CE QUE JAMF PRO ?

Jamf Pro est un ensemble d'outils administratifs destinés à vous aider à gérer vos appareils Apple.

jamf PROTECT

QU'EST-CE QUE JAMF PROTECT ?

Jamf Protect est une solution de sécurité des terminaux conçue spécifiquement pour Apple et les Mac dans le contexte professionnel.

jamf CONNECT

QU'EST-CE QUE JAMF CONNECT ?

Jamf Connect permet d'utiliser la même identité Cloud sur tous vos appareils Apple pour accéder aux ressources en toute transparence.

CIS Center for Internet Security®

QUI EST LE CENTER FOR INTERNET SECURITY ?

Le Center for Internet Security, Inc. (CIS) est une organisation à but non lucratif dont l'objectif est d'améliorer la préparation et la réponse des entités des secteurs public et privé aux problèmes de cybersécurité.

L'HISTOIRE DES CRITÈRES DU CIS

Les critères du CIS sont le fruit d'un processus de révision consensuelle menée par des experts en la matière. Les participants au consensus apportent les points de vue de différents secteurs : conseil, développement logiciel, audit et conformité, recherche en sécurité, opérations, administration et secteur juridique.

Chaque édition des critères CIS passe par deux phases de révision consensuelle. La première a lieu pendant la mise au point des critères. Pendant cette phase, les experts se réunissent pour discuter des projets de critères, les rédiger et les tester. Ces discussions se poursuivent jusqu'à ce qu'ils atteignent un consensus quant aux recommandations à intégrer aux critères. La deuxième phase commence après la publication des critères. Pendant cette phase, tous les retours de la communauté sont examinés par l'équipe du consensus en vue de leur éventuelle intégration aux critères. Si vous souhaitez participer au processus de consensus, veuillez consulter le site **https://community.cisecurity.org.**

JAMF PROTECT ET CIS

Jamf Protect a récemment reçu la certification CIS Benchmark du CIS. Les organisations qui ont choisi Jamf Protect peuvent aligner les configurations de leurs actifs critiques sur les normes et pratiques recommandées par les critères CIS pour macOS.

Les recommandations du CIS portent sur différents domaines de macOS où des contrôles doivent être mis en œuvre pour réduire la possibilité d'exfiltration de données.

Si Jamf Pro vous donne les outils pour suivre les recommandations du CIS, Jamf Protect automatise l'évaluation des paramètres de sécurité essentiels du CIS sur une base quotidienne. Vous pouvez ainsi valider la conformité de votre flotte macOS et superviser l'ensemble de vos priorités de sécurité selon tous les aspects des critères CIS.

Catégories de sécurité macOS

MISES À JOUR ET CORRECTIFS | PRÉFÉRENCES SYSTÈME | iCLOUD | JOURNALISATION ET AUDIT

CONFIGURATION RÉSEAU | COMPTES UTILISATEURS | ACCÈS ET AUTHENTIFICATION | AUTRES CONSIDÉRATIONS

Installation des mises à jour, des correctifs et des logiciels de sécurité

Jamf Pro vous permet de maintenir vos macOS et vos applications à jour en conditionnant et en déployant les mises à jour sur vos Mac clients à distance. Vous pouvez même créer un rapport pour surveiller l'état des mises à niveau de macOS en temps réel : vous saurez ainsi si toute votre flotte de Mac utilise sur le dernier OS disponible – autrement dit, le plus sécurisé.

Recommandations des critères du CIS

- Vérifier que tous les logiciels fournis par Apple sont à jour.
- Activer la mise à jour automatique.
- Autoriser l'installation des mises à jour des applications.
- Autoriser l'installation des mises à jour des fichiers de données du système et de sécurité.
- Autoriser l'installation des mises à jour de macOS.

Fonctionnalités de Jamf Pro :

- La gestion des correctifs vous aide à maintenir macOS et de nombreuses applications répandues à jour.
- Un serveur de mise à jour des logiciels personnalisé vous permet d'inscrire sur une liste d'autorisation les mises à jour approuvées pour vos Mac.
- Une règle permet d'activer les mises à jour automatique via l'App Store.
- Une règle permet de vérifier les mises à jour sur un Mac client.

Fonctionnalités de Jamf Connect :

- Nécessite un identifiant et un mot de passe cloud.
- Les comptes invités sont masqués.
- Pas d'indice de mot de passe pour les comptes locaux.

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages mentionnés ici pour valider la conformité en matière de mises à jour, de correctifs et de logiciels de sécurité.

Préférences système

Jamf Pro vous aide à configurer les Préférences Système pour répondre aux besoins de sécurité de votre organisation. Vous pouvez définir des réglages communs et avancés pour l'ensemble de votre flotte Mac pour renforcer ses défenses contre les attaques physiques et distantes.

Recommandations des critères du CIS :

Bluetooth :
- Désactiver le Bluetooth
- Désactiver le mode de découverte Bluetooth

Date et heure :
- Activer le réglage automatique de l'heure et de la date
- Vérifier la conformité de l'heure réglée

Bureau et économiseur d'écran :
- Définir un délai d'inactivité de 20 minutes ou moins pour l'activation de l'économiseur d'écran
- Sécuriser les coins de l'économiseur d'écran
- Familiariser les utilisateurs avec les outils de verrouillage et l'activation de l'économiseur d'écran dans l'angle du bureau

Partage :
- Désactiver les événements Apple à distance dans le cadre du partage
- Désactiver le partage Internet
- Désactiver le partage d'écran
- Désactiver le partage d'imprimante
- Désactiver la connexion à distance (SSH)
- Désactiver le partage de DVD ou de CD
- Désactiver le partage Bluetooth
- Désactiver le partage de fichiers
- Désactiver la gestion à distance (ARD)

Économiseur d'énergie :
- Désactiver la sortie de veille en cas d'accès au réseau

Sécurité et confidentialité :
- Activer FileVault
- Veiller à ce que tous les volumes de stockage APFS de l'utilisateur soient chiffrés
- Veiller à ce que tous les volumes de stockage CoreStorage de l'utilisateur soient chiffrés
- Activer Gatekeeper
- Activer le pare-feu
- Activer le mode furtif du pare-feu
- Examiner les règles de pare-feu des applications
- Activer les services de localisation
- Surveiller l'accès aux services de localisation
- Désactiver l'envoi de données de diagnostic et d'utilisation Apple

Autres aspects :
- iCloud (voir section ci-dessous)
- Sauvegarde automatique Time Machine
- Vérifier que les volumes Time Machine sont chiffrés
- Appairer le récepteur de télécommande infrarouge si la fonction est activée
- Activer la saisie sécurisée au clavier dans terminal.app
- Java 6 n'est pas le moteur d'exécution Java par défaut
- Supprimer les fichiers de façon sécurisée si nécessaire
- Vérifier que la version de l'EFI est valide et fait l'objet d'une vérification régulière

Fonctionnalités de Jamf Pro :

- Toutes les préférences système ci-dessus peuvent être définies via une règle du serveur Jamf Pro et/ou un profil de configuration
- Permet d'activer FileVault 2 et de déposer les clés dans l'inventaire de votre serveur Jamf Pro
- Permet de définir les réglages de l'économiseur d'écran et de mot de passe
- Permet de définir les réglages de partage
- Permet de définir les réglages de sécurité et de confidentialité
- Permet de déployer des règles qui désactivent Java

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité des préférences système

iCloud et autres services cloud

Jamf Pro soutient la stratégie iCloud de votre organisation en donnant aux administrateurs informatiques la possibilité de bloquer ou d'activer ce service cloud.

Recommandations des critères CIS

« Apple iCloud est un service grand public qui permet à un utilisateur de stocker des données, mais aussi de retrouver, contrôler et sauvegarder les appareils associés à son identifiant Apple. Dans le cas des appareils professionnels, l'utilisation d'iCloud doit respecter la politique d'utilisation acceptable de l'entreprise et les exigences de confidentialité des données. Quand iCloud est autorisé, les données copiées sur les serveurs d'Apple risquent d'être reproduites aussi bien sur les appareils personnels que professionnels. »

iCloud

- Configuration d'iCloud
- Trousseau iCloud
- iCloud Drive
- Synchronisation de documents avec iCloud Drive
- Synchronisation du bureau avec iCloud Drive

Fonctionnalités de Jamf Pro :

- Permet de désactiver iCloud à l'aide d'un profil de configuration
- Si iCloud n'est pas autorisé, iCloud Drive peut être supprimé de Finder

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité aux règles relatives à iCloud et aux autres services cloud

Journalisation et audit

Jamf Pro centralise les journaux produits par macOS pour faciliter leur exploitation par les administrateurs informatiques. Les administrateurs peuvent également utiliser ces journaux pour générer des rapports sophistiqués afin de détecter d'éventuels problèmes de sécurité.

Recommandations du CIS :

- Activer l'audit de technologie
- Configurer les marqueurs d'audit de sécurité
- Confirmer la conservation des audits de sécurité
- Contrôler l'accès aux dossiers d'audit
- Conserver le fichier install.log pendant 365 jours ou plus
- Vérifier que la journalisation du pare-feu est activée

Fonctionnalités de Jamf Pro :

- Les profils de configuration peuvent être modifiés par le biais d'un script
- Les fichiers journaux peuvent être transmis au serveur Jamf Pro et conservés aussi longtemps que nécessaire
- Le serveur Jamf Pro peut mettre en cache des journaux supplémentaires

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité aux règles de journalisation et d'audit

Configurations réseau

Jamf Pro facilite le déploiement des configurations réseau en assurant la distribution des paramètres Wi-Fi, VPN et même DNS. Jamf Pro se charge également de désactiver certains composants de serveur de macOS, hérités d'anciennes versions, afin que les utilisateurs n'ouvrent pas accidentellement des ports dont ils ignorent l'existence.

Recommandations du CIS :

- Désactiver le service de publicité Bonjour
- Activer l'option « Afficher l'état du Wi-Fi dans la barre de menu »
- Créer des emplacements spécifiques au réseau
- Vérifier que le serveur HTTP n'est pas en cours d'exécution
- Vérifier que le serveur nfs n'est pas en cours d'exécution

Fonctionnalités de Jamf Pro :

- Les réglages du réseau peuvent être intégrés dans un profil de configuration
- Apache, FTP et NFS peuvent tous être désactivés via une règle de serveur Jamf Pro

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité des configurations réseau

Comptes utilisateurs et environnement

Jamf Pro facilite la gestion des comptes locaux sur un Mac en permettant de créer des utilisateurs administrateurs ou ordinaires. Le binaire Jamf installé sur les machines clientes crée un compte de gestion caché qui dispose de droits d'administration pour exécuter des commandes et créer de nouveaux utilisateurs. Vous pouvez créer des règles pour sécuriser davantage l'écran de connexion et désactiver le compte invité.

Recommandations des critères du CIS :

- Afficher la fenêtre de connexion avec nom et mot de passe
- Désactiver l'option « Afficher les indices de mot de passe »
- Désactiver la connexion au compte invité
- Désactiver l'option « Autoriser les invités à se connecter aux dossiers partagés »
- Supprimer le dossier d'utilisateur invité
- Afficher les extensions de noms de fichiers
- Désactiver l'exécution automatique des fichiers sécurisés dans Safari
- Désactiver l'utilisation globale des plug-ins Safari
- Utiliser des contrôles parentaux pour les systèmes qui ne sont pas gérés de manière centralisée

Fonctionnalités de Jamf Pro :

- La fenêtre de connexion peut être modifiée via le profil de configuration
- Le compte invité peut être désactivé via une règle de serveur Jamf Pro
- Les comptes utilisateurs peuvent être créés via l'assistant d'inscription et Apple Business Manager
- Les comptes créés peuvent être standards ou administrateurs, selon les besoins.

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité aux règles relatives aux comptes utilisateurs et à l'environnement

Accès aux systèmes, authentification et autorisation

Jamf Pro permet de définir des autorisations de fichiers, d'appliquer des règles strictes en matière de mots de passe et de gérer l'accès au trousseau des utilisateurs. En créant un profil de configuration ou une règle de serveur Jamf Pro, vous pouvez activer à distance les réglages d'accès au systèmepour renforcer la sécurité des Mac.

Recommandations du CIS :

Permissions et contrôles d'accès au système de fichiers :

- Sécuriser les dossiers personnels
- Vérifier que les applications portant sur l'ensemble du système disposent d'autorisations appropriées.
- Vérifier que le dossier System ne contient pas de fichiers universellement accessibles en écriture
- Vérifier que le dossier Library ne contient pas de fichiers universellement accessibles en écriture

Gestion des mots de passe :

- Configurer le seuil de verrouillage des comptes
- Définir une longueur minimale pour le mot de passe
- Les mots de passe complexes doivent contenir un caractère alphabétique
- Les mots de passe complexes doivent contenir un caractère numérique
- Les mots de passe complexes doivent contenir un caractère spécial
- Les mots de passe complexes doivent comporter des majuscules et des minuscules
- Ancienneté du mot de passe
- Historique des mots de passe
- Réduire le délai d'attente de sudo
- Utiliser un horodatage distinct pour chaque combinaison utilisateur/tty
- Verrouiller automatiquement le trousseau de connexion en cas d'inactivité
- Vérifier que le trousseau de connexion est verrouillé lorsque l'ordinateur est en veille
- Activer la vérification des certificats OCSP et CRL
- Ne pas activer le compte « root »
- Désactiver l'ouverture de session automatique
- Exiger un mot de passe pour sortir l'ordinateur de veille ou de l'économiseur d'écran
- Vérifier que le mode hibernation est configuré sur le système
- Exiger un mot de passe administrateur pour accéder aux préférences du système
- Désactiver la possibilité de se connecter à la session active et verrouillée d'un autre utilisateur
- Créer une bannière de fenêtre de connexion
- Ne pas saisir d'indice de mot de passe
- Désactiver le changement rapide d'utilisateur
- Sécuriser les porte-clés et les éléments personnels
- Créer des porte-clés spécialisés pour différents usages
- État de la protection de l'intégrité du système

Fonctionnalités de Jamf Pro :

- La commande de réparation des autorisations peut être déclenchée via le Self Service ou exécutée automatiquement
- Vous pouvez créer des rapports pour rechercher les fichiers aux autorisations inappropriées dans les dossiers System et Library
- Activation des règles relatives aux mots de passe via le profil de configuration
- Possibilité d'ajouter une fenêtre et une bannière de connexion via des règles de serveur Jamf Pro
- Les droits d'accès aux dossiers peuvent être définis par un script dans une règle de serveur Jamf Pro

Fonctionnalités de Jamf Connect :

- Il est possible d'ajouter un message personnalisé sur l'écran de connexion pour exiger un mot de passe complexe, conformément aux règles d'identité cloud

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité aux règles d'accès au système, d'authentification et d'autorisation

Autres considérations

Jamf Pro permet aux administrateurs de personnaliser des paramètres de sécurité supplémentaires en définissant un mot de passe EFI, en désactivant le Wi-Fi dans les environnements hyper-sécurisés, etc. Vous pouvez également utiliser le serveur Jamf Pro pour renommer vos Mac pour simplifier l'inventaire. Jamf Pro vous permet également de dresser l'inventaire des logiciels dont dispose votre organisation et d'assurer le suivi des licences.

Recommandations des critères du CIS :

- Technologies sans-fil sur macOS
- Problématiques de confidentialité et de respect de la vie privée liées à la caméra iSight
- Considérations relatives au nom des ordinateurs
- Considérations relatives à l'inventaire des logiciels
- Considérations relatives au pare-feu
- Actions automatiques pour les supports optiques
- App Store – Considérations relatives au téléchargement automatique des applications achetées sur d'autres Mac
- Mot de passe de l'interface micrologicielle extensible (EFI)
- Réinitialisation du mot de passe de FileVault et du compte local à l'aide de l'AppleID
- La réparation des autorisations n'est plus nécessaire
- Paramètres de mot de passe de l'App Store
- Siri sur macOS
- Fonctionnalités Apple Watch sous macOS
- Sauvegarde des informations du système sur des ordinateurs distants
- Journalisation unifiée
- Considérations de sécurité au sujet d'AirDrop

Fonctionnalités de Jamf Pro :

- Le Wi-Fi peut être désactivé via le profil de configuration
- Le nommage des ordinateurs peut être automatisé sur le serveur Jamf Pro.
- Inventaire des logiciels et suivi des licences dans le serveur Jamf Pro
- Les mots de passe EFI peuvent être définis par le biais d'une règle

Fonctionnalités de Jamf Protect :

- Évalue tous les réglages énoncés ici pour vérifier la conformité des considérations supplémentaires

Conclusion

Jamf facilite la mise en œuvre et le suivi des critères du Center for Internet Security pour macOS.

jamf

www.jamf.com/fr

Testez les avantages de ces bonnes pratiques de sécurité en faisant un essai gratuit de Jamf. **Lancez-vous !**