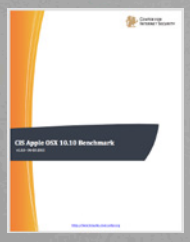


Checklist de la sécurité de Mac OS X :

Mise en œuvre du benchmark pour OS X du Center for Internet Security (CIS)

Recommandations concernant la sécurité de Mac OS X

Le benchmark pour OS X du Center for Internet Security est souvent vu comme une Checklist complète destinée aux organisations qui souhaitent assurer la sécurité de leurs Mac. Ce livre blanc de JAMF Software « Les experts de la gestion Apple » vous expliquera comment mettre en œuvre les recommandations de cette organisation indépendante.

Qu'est-ce que Casper Suite ?

Casper Suite est un ensemble d'outils de gestion des appareils Apple.

Qu'est-ce que le JSS ?

Compatible avec les serveurs Mac, Windows et Linux, le JAMF Software Server (JSS) est le serveur de gestion de la suite.

Qu'est-ce qu'une règle ?

Les règles sont les principaux outils utilisés pour mettre en œuvre des changements sur un Mac client. Le JSS envoie des commandes à un agent sur le Mac.

Center for Internet Security®

Qu'est-ce que le CIS ?

Le Center for Internet Security, Inc (CIS) est une organisation à but non lucratif dont l'objectif est d'aider les structures publiques et privées à améliorer leur réactivité et leurs actions en matière de cybersécurité.

Comment le benchmark du CIS a-t-il été créé ?

Le benchmark du CIS est né d'un consensus élaboré par un groupe d'experts. Ces experts proposent des points de vue issus de différents milieux (conseil, développement de logiciels, audit et conformité, recherche en sécurité, opérations, gouvernement, juridique).

Chaque benchmark du CIS connaît deux phases d'examen. La première phase concerne le développement initial du benchmark. Au cours de cette phase, les experts débattent, créent et testent des ébauches du benchmark. La discussion se prolonge jusqu'à ce qu'un consensus soit trouvé pour proposer des recommandations. La seconde phase commence une fois que le benchmark est publié. Pendant cette phase, tous les avis fournis par la communauté Internet sons examinés par l'équipe du consensus afin d'être pris en compte dans le benchmark. Si vous souhaitez participer au processus de consensus, visitez le site https://community.cisecurity.org.

- Benchmark CIS Apple OS X 10.10

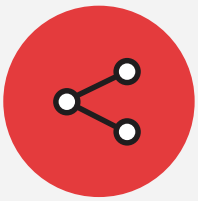
Catégories de sécurité pour OS X

Mises à jour et correctifs

Préférences système

iCloud

Journalisation et audit



Configuration réseau

Comptes utilisateurs

Accès et authentification

Autres éléments

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

Casper Suite vous permet de garder vos applications et votre système d'exploitation à jour en regroupant et en déployant à distance des mises à jour vers vos Mac clients. Vous pouvez même créer des rapports vous indiquant quelles machines ont été mises à jour et lesquelles sont toujours en attente.

Recommandations du CIS :

- Vérifier que le système d'exploitation et les applications sont à jour à l'aide d'un outil de mise à jour de logiciels
- Activer la mise à jour automatique dans l'App Store
- Activer les mises à jour de sécurité automatiques

Fonctionnalités de Casper Suite :

- Mise à jour de vos systèmes Mac OS X grâce à la gestion des correctifs
- Création d'une liste blanche des mises à jour autorisées pour vos Mac grâce à un serveur de mise à jour de logiciels personnalisé
- Exécution d'une règle pour activer les mises à jour automatiques via l'App Store
- Exécution d'une règle pour rechercher des mises à jour pour un Mac client

Préférences système

Casper Suite vous aide à configurer vos Préférences système afin de répondre aux besoins de votre organisation en matière de sécurité. Vous pouvez facilement activer à distance et en masse des réglages tels que des mots de passe et des écrans de veille afin de restreindre l'accès physique aux Mac. Vous pouvez également configurer des réglages avancés tels que la désactivation de SSH ou du partage de fichiers afin de protéger votre Mac contre les attaques à distance.

Recommandations du CIS :

Bluetooth:

- Désactiver le Bluetooth
- Désactiver le mode Détection du Bluetooth

Date et heure :

- Activer le réglage automatique de la date et de l'heure

Bureau et écran de veille :

- Définir le délai d'activation de l'écran de veille sur 20 minutes ou moins
- Activer les coins actifs pour lancer l'écran de veille
- Définir un délai plus élevé pour l'arrêt de l'écran que pour l'écran de veille

Partage :

- Désactiver les Événements Apple distants dans le 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 par Bluetooth
- Désactiver le partage de fichiers
- Désactiver la gestion à distance (ARD)

Économies d'énergie :

- Désactiver la recherche d'accès réseau
- Désactiver la mise en veille de l'ordinateur lorsque celui-ci est alimenté

Sécurité et confidentialité :

- Activer FileVault 2
- Activer Gatekeeper
- Activer le pare-feu
- Activer le mode furtif du pare-feu
- Examiner les règles du pare-feu des applications (https://support.apple.com/fr-fr/HT201642)

Autres :

- iCloud (voir la section ci-dessous)
- Activer la saisie clavier sécurisée dans terminal.app
- Ne pas définir Java 6 comme version de Java par défaut
- Vider la Corbeille en mode sécurisé

Fonctionnalités de Casper Suite :

- Possibilité de définir toutes les Préférences système ci-dessus via une règle du JSS et/ou un profil de configuration
- Activation de FileVault 2 et dépôt de clés dans l'inventaire du JSS
- Configuration de l'écran de veille et des réglages des mots de passe
- Configuration des réglages de partage
- Configuration des réglages de sécurité et de confidentialité
- Déploiement d'une règle de désactivation de Java

iCloud et autres services cloud

Casper Suite vous aide à mettre en œuvre la stratégie iCloud de votre organisation en offrant aux administrateurs la possibilité de bloquer ou d'activer le service basé sur le cloud.

Recommandations du CIS :

"Le service iCloud d'Apple fait partie des nombreuses solutions sur le cloud utilisées pour synchroniser des données sur plusieurs plateformes. Il doit donc être contrôlé de manière cohérente avec les autres services cloud de votre environnement. Parlez-en avec vos employés et configurez l'accès de manière à protéger au mieux les données en fonction de vos activités.

Fonctionnalités de Casper Suite :

- Désactivation d'iCloud via un profil de configuration et/ou une règle du JSS
- Suppression d'iCloud Drive du Finder, si iCloud n'est pas autorisé

Journalisation et audit

Casper Suite peut aider les administrateurs informatiques à garder une trace des journaux générés par OS X et centralisés dans un même endroit. Les administrateurs peuvent également exécuter des rapports avancés sur ces journaux afin de rechercher d'éventuels problèmes de sécurité.

Recommandations du CIS :

- Configurer le fichier asl.conf
- Conserver le fichier system.log pendant au moins 90 jours
- Conserver le fichier appfirewall.log pendant au moins 90 jours
- Conserver le fichier auth.log pendant au moins 90 jours
- Activer les audits de sécurité
- Configurer les indicateurs d'audit de sécurité
- Activer la journalisation à distance pour les Mac sur les réseaux de confiance
- Conserver le fichier install.log pendant au moins un an

Fonctionnalités de Casper Suite :

- Modification des fichiers de configuration via un script
- Envoi des fichiers journaux au JSS et stockage aussi longtemps que nécessaire
- Mise en cache de journaux supplémentaires par le JSS

Configuration réseau

Casper Suite simplifie la configuration des réseaux pour les administrateurs informatiques en leur permettant d'effectuer des réglages par Wi-Fi, VPN et même DNS. La solution permet également de désactiver certains composants serveurs OS X, afin d'empêcher les utilisateurs d'ouvrir accidentellement des ports qu'ils ne connaissent pas.

Recommandations du CIS :

- Vérifier le statut du Wi-Fi dans la barre de menu
- Créer des emplacements spécifiques pour le réseau
- Vérifier que le serveur HTTP n'est pas en cours d'exécution (Apache)
- Vérifier que le serveur FTP n'est pas en cours d'exécution
- Vérifier que le serveur NFS n'est pas en cours d'exécution

Fonctionnalités de Casper Suite :

- Intégration de paramètres réseau dans un profil de configuration
- Désactivation d'Apache, du FTP et de NFS via un script dans une règle du JSS

Comptes utilisateurs et environnement

Casper Suite aide les organisations à gérer les comptes locaux sur Mac, en leur permettant par exemple de créer des utilisateurs standard ou administrateurs. L'application jamf binary présente sur les machines client crée un compte de gestion masqué disposant des droits administrateurs nécessaires pour exécuter des commandes et créer de nouveaux utilisateurs. Vous pouvez également créer des règles pour sécuriser l'écran de connexion et désactiver le compte invité.

Recommandations du CIS :

- Afficher uniquement les champs du nom d'utilisateur et du mot de passe sur la fenêtre de connexion
- Désactiver l'affichage d'indices du mot de passe
- Désactiver le compte invité
- Interdire aux invités de se connecter aux dossiers partagés
- Afficher les extensions des noms de fichier
- Désactiver l'exécution automatique des fichiers fiables dans Safari à des fins multiples

Fonctionnalités de Casper Suite :

- Configuration de la fenêtre de connexion via un profil de configuration
- Désactivation du compte invité via une règle du JSS
- Création de comptes utilisateurs via l'Assistant réglages et le DEP ou lors de l'imaging
- Création de comptes standard ou administrateurs, selon les besoins

Accès système, authentification et autorisations

Casper Suite vous aide à configurer des autorisations d'accès aux fichiers, à gérer les accès aux trousseaux et à définir des règles de mot de passe sécurisées pour vos utilisateurs. En créant un profil de configuration ou une règle du JSS, vous pouvez activer à distance des réglages d'accès au système pour sécuriser davantage votre Mac.

Recommandations du CIS :

- Sécuriser le dossier de départ (interdire la lecture des autres dossiers de départ)
- Réparer les autorisations régulièrement
- Rechercher des autorisations dans les applications à l'échelle du système
- Rechercher des fichiers en écriture non restreinte dans le dossier Système
- Rechercher des fichiers en écriture non restreinte dans le dossier Bibliothèque
- Réduire le délai d'expiration de Sudo
- Verrouiller automatiquement le trousseau de connexion en cas d'inactivité
- Vérifier que le trousseau de connexion est verrouillé lorsque l'ordinateur est en veille
- Vérifier les certificats OCSP et CRL
- Ne pas activer le compte « root »
- Désactiver la connexion automatique
- Demander un mot de passe pour quitter le mode veille de l'ordinateur
- Demander un mot de passe administrateur pour accéder aux préférences à l'échelle du système
- Désactiver la connexion à une autre session active et verrouillée de l'utilisateur
- Définir des mots de passe complexes (contenant des chiffres, des lettres et des symboles)
- Définir une longueur minimale pour les mots de passe
- Configurer un seuil de verrouillage de compte
- Créer un message personnalisé pour l'écran de connexion
- Créer une bannière pour la fenêtre de connexion
- Désactiver les indices de mot de passe
- Désactiver la permutation rapide d'utilisateur
- Sécuriser les trousseaux individuels
- Créer des trousseaux spécialisés à des fins multiples

Fonctionnalités de Casper Suite :

- Configuration d'autorisations d'accès à un dossier via un script dans une règle du JSS
- Exécution automatique ou déclenchement de la réparation des autorisations via Self Service
- Création de rapports pour rechercher de mauvaises autorisations dans les fichiers des dossiers Système ou Bibliothèque
- Activation de règles de mot de passe via un profil de configuration
- Ajout d'une fenêtre et d'une bannière de connexion via une règle du JSS

Autres points importants

Casper Suite aide les administrateurs informatiques à personnaliser des réglages de sécurité supplémentaires en configurant un mot de passe EFI, en désactivant le Wi-Fi dans les environnements hyper-sécurisés, etc. Vous pouvez également utiliser le JSS pour renommer vos Mac afin de simplifier l'inventaire. Enfin, Casper Suite vous permet d'inventorier les ressources logicielles et de garder une trace des licences de votre organisation.

Recommandations du CIS :

- Désactiver le Wi-Fi et utiliser uniquement le réseau Ethernet
- Couvrir les caméras iSight
- Nommer les ordinateurs selon un modèle pertinent
- **Inventorier les logiciels**
- Mettre en place un pare-feu
- Mettre en place des actions automatiques pour le média optique
- Définir un mot de passe EFI
- Réinitialiser le mot de passe de l'identifiant Apple

Fonctionnalités de Casper Suite :

- Désactivation du Wi-Fi via un profil
- Automatisation de l'attribution de noms aux ordinateurs via des réglages dans le JSS
- Inventaire des logiciels et suivi des licences dans le JSS
- Configuration des mots de passe EFI via une règle et/or i'imaging

Conclusion

Casper Suite vous permet de suivre et de facilement mettre en œuvre les benchmarks de l'organisation indépendante Center for Internet Security pour OS X.

Pour en savoir plus sur la manière de sécuriser vos Mac à l'aide Casper Suite, visitez la page **www.jamfsoftware.com/fr/securiser-apple-grace-a-casper-suite**

JAMF software

france@jamfsoftware.com | +33 186 263 005 | www.jamfsoftware.com/fr