jamf

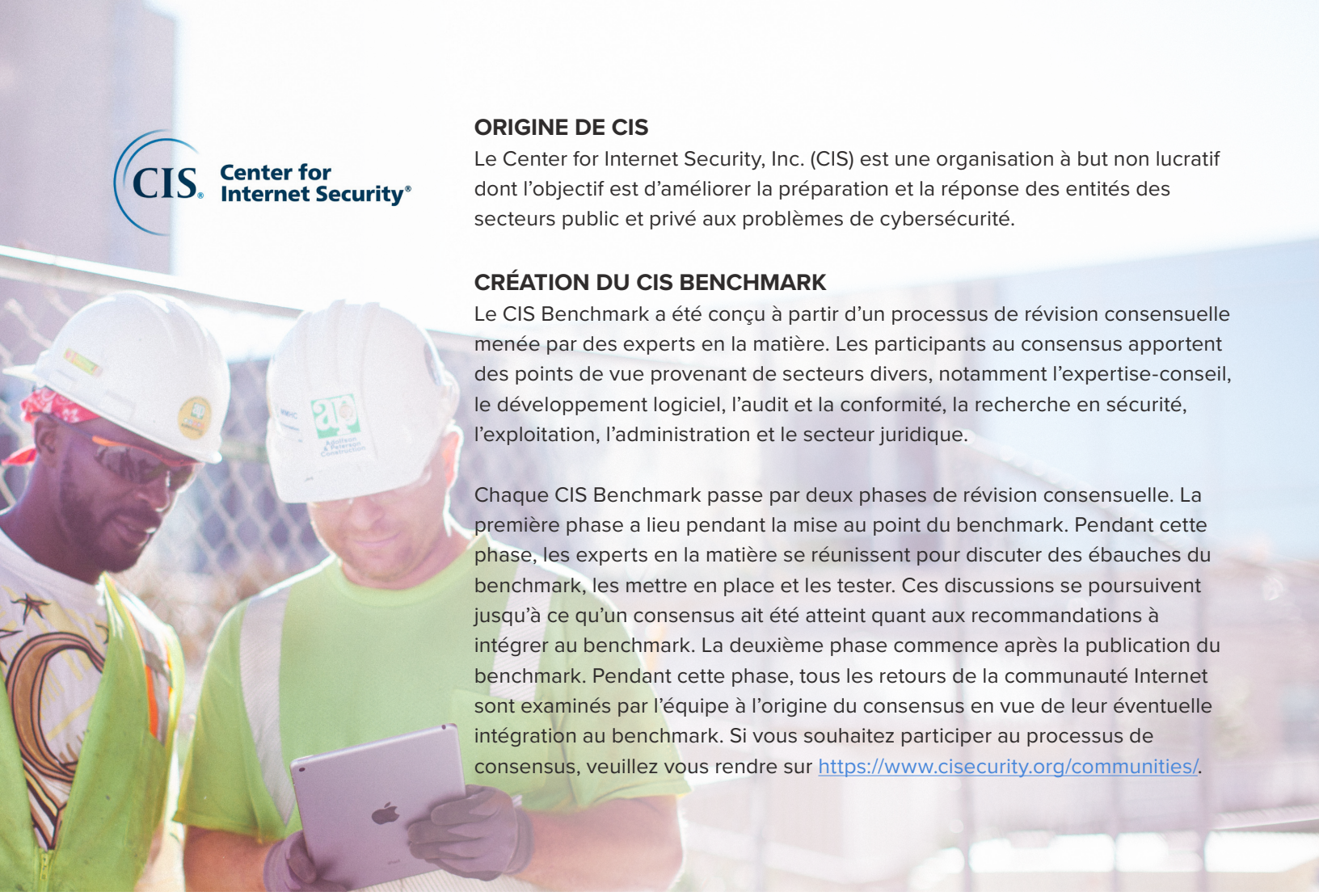
LIVRE BLANC

Check-list de sécurité iOS

Mettre en œuvre le Center for Internet Security (CIS) Benchmark pour iOS

Recommandations pour sécuriser iOS

L'outil CIS Benchmark pour iOS est une check-list de sécurité complète que les entreprises suivent pour sécuriser leurs iPad et leurs iPhone. Ce livre blanc explique comment mettre en œuvre les recommandations de cette organisation indépendante.



ORIGINE DE CIS

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.

CRÉATION DU CIS BENCHMARK

Le CIS Benchmark a été conçu à partir d'un processus de révision consensuelle menée par des experts en la matière. Les participants au consensus apportent des points de vue provenant de secteurs divers, notamment l'expertise-conseil, le développement logiciel, l'audit et la conformité, la recherche en sécurité, l'exploitation, l'administration et le secteur juridique.

Chaque CIS Benchmark passe par deux phases de révision consensuelle. La première phase a lieu pendant la mise au point du benchmark. Pendant cette phase, les experts en la matière se réunissent pour discuter des ébauches du benchmark, les mettre en place et les tester. Ces discussions se poursuivent jusqu'à ce qu'un consensus ait été atteint quant aux recommandations à intégrer au benchmark. La deuxième phase commence après la publication du benchmark. Pendant cette phase, tous les retours de la communauté Internet sont examinés par l'équipe à l'origine du consensus en vue de leur éventuelle intégration au benchmark. Si vous souhaitez participer au processus de consensus, veuillez vous rendre sur https://www.cisecurity.org/communities/.

CIS et la gestion d'iOS

QU'EST-CE QUE LE MDM ?

Le MDM (gestion des appareils mobiles) est le framework de gestion intégré d'Apple pour iOS, macOS et tvOS. Jamf Pro est la solution MDM standard pour les appareils Apple.

PROPRIÉTÉ DES APPAREILS

Les impératifs de sécurité varient selon le modèle technologique adopté par l'entreprise : appareils personnels avec une initiative BYOD (Bring Your Own Device) ou appareils appartenant à l'entreprise et distribués aux utilisateurs.

QUE SONT LES PROFILS DE CONFIGURATION ?

Les profils de configuration définissent les réglages des appareils iOS et sont distribués aux appareils par le biais de la solution MDM.

NIVEAU DE SÉCURITÉ

Le Niveau 1 (N1) et le Niveau 2 (N2) définissent les exigences de sécurité et les réglages devant être appliqués à un appareil personnel ou appartenant à l'entreprise. Le niveau N2 donne plus de contrôle sur l'appareil et va au-delà des exigences de sécurité de base.

QU'EST-CE QUE LA SUPERVISION ?

La supervision offre un niveau de gestion d'iOS supérieur pour les appareils enrôlés dans la gestion par le biais des programmes de déploiement Apple ou d'Apple Configurator.

QU'EST-CE QUE LE SERVICE APNS ?

Le service de notification push d'Apple (APNs) est nécessaire à la gestion iOS. Pour en savoir plus sur le service APNs, veuillez consulter l'article qui suit : https://www.jamf.com/blog/what-is-apple-push-notification-service-apns/ requirements.

Sécuriser les appareils appartenant à l'entreprise

Une étude récente a déterminé que 74 % des employés d'entreprise préfèreraient disposer d'un appareil appartenant à l'entreprise plutôt que d'utiliser un appareil personnel*. Jamf Pro aide les entreprises à mettre en œuvre leur programme d'appareils d'entreprise en toute sécurité, mais aussi à rationaliser la distribution et la gestion des iPad et iPhone appartenant à l'entreprise.

Recommandations CIS

Mise en place :

- Définissez un message de consentement et une description pour le profil d'inscription.
- Vérifiez qu'il est possible de supprimer le profil.

Fonctionnalités :

- N2 : Désactiver les captures d'écran et l'enregistrement d'écran.
- Désactiver la composition vocale lorsque l'appareil est verrouillé.
- Désactiver Siri lorsque l'appareil est verrouillé.
- Désactiver la sauvegarde iCloud.
- Désactiver les documents et les données iCloud.
- Désactiver le trousseau iCloud.
- Empêcher les apps gérées de stocker des données dans iCloud.
- Autoriser Forcer le chiffrement des sauvegardes.
- Désactiver Autoriser tous les contenus et réglages.
- N2 : Désactiver Autoriser les utilisateurs à accepter des certificats TLS non fiables.
- Désactiver Autoriser l'installation de profils de configuration.
- Désactiver Autoriser l'ajout de configurations VPN.
- Désactiver Autoriser la modification des réglages d'app des données cellulaires.
- N2 : Désactiver Autoriser le jumelage avec des hôtes non-Configurator.
- Désactiver Autoriser les documents de sources gérées dans les destinations non gérées.
- Désactiver Autoriser les documents de sources non gérées dans les destinations gérées.
- Autoriser Traiter AirDrop en tant que destination non gérée.
- Désactiver Autoriser Handoff.
- Autoriser Forcer la détection du poignet par l'Apple Watch.
- Désactiver Autoriser la configuration d'un nouvel appareil à proximité.
- Désactiver Afficher le Centre de contrôle sur l'écran de verrouillage.
- Désactiver Afficher le Centre de notifications sur l'écran de verrouillage.

Apps :

- Activer le forçage de l'alerte de fraude.
- Accepter les cookies défini sur « Des sites web que j'ai visités » ou « Du site web actuel uniquement ».

Domaines :
- Configurer les domaines web Safari gérés.

Codes d'accès :
- Interdire les valeurs simples.
- Longueur minimale du code d'accès définie sur « 6 » ou plus.
- Délai de verrouillage automatique défini sur « 2 minutes » ou moins.
- Délai de grâce maximum pour le verrouillage de l'appareil défini sur « Immédiat ».
- Nombre maximum de tentatives défini sur « 6 ».

VPN :
- Vérifier que le VPN est « Configuré ».
- Connexion VPN via l'app préférée.

E-mail :
- Définir le compte d'e-mail d'un utilisateur avec un profil d'e-mail.
- Empêcher l'utilisateur de déplacer des messages depuis ce compte.

Notifications :
- Configurer les réglages de notification pour toutes les apps gérées.

Message sur l'écran de verrouillage :
- Configurer un message « Si cet appareil est perdu, contactez… ».

Fonctionnalités de Jamf Pro

Jamf Pro vous permet de définir, d'activer et/ou de désactiver toutes les préférences système des niveaux N1 et N2 énumérées ci-dessus via des profils de configuration. L'application de certains de ces réglages nécessite que l'appareil iOS soit supervisé lors de son enrôlement.
Veuillez poursuivre la lecture pour en savoir plus sur la supervision iOS : https://support.apple.com/en-us/HT202837.

Jamf Pro donne aussi la possibilité aux entreprises de définir un message personnalisé à afficher sur l'écran de verrouillage pour que les appareils perdus soient récupérés et ne puissent pas être déverrouillés ou piratés.

*Source: https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/

Sécuriser les appareils personnels et BYOD

Recommandations CIS

Mise en place :

- Définissez un message de consentement et une description pour le profil d'inscription.
- Vérifiez qu'il est possible de supprimer le profil.

Fonctionnalités :

- Désactiver la composition vocale lorsque l'appareil est verrouillé.
- Désactiver Siri lorsque l'appareil est verrouillé.
- Empêcher les apps gérées de stocker des données dans iCloud.
- Autoriser Forcer le chiffrement des sauvegardes.
- N2 : Empêcher les utilisateurs d'accepter des certificats TLS non fiables.
- Interdire les documents de sources gérées dans les destinations non gérées.
- Autoriser Traiter AirDrop en tant que destination non gérée.
- N2 : Désactiver Autoriser Handoff.
- Désactiver Afficher le Centre de contrôle sur l'écran de verrouillage.
- Désactiver Afficher le Centre de notifications sur l'écran de verrouillage.

Apps:

- Activer le forçage de l'alerte de fraude dans Safari.
- Accepter les cookies défini sur « Des sites web que j'ai visités » ou « Du site web actuel uniquement».

Domaines:

- Configurer les domaines web Safari gérés.

Codes d'accès :

- Interdire les valeurs simples.
- Longueur minimale du code d'accès définie sur « 6 » ou plus.
- Délai de verrouillage automatique défini sur « 2 minutes » ou moins.
- Délai de grâce maximum pour le verrouillage de l'appareil défini sur « Immédiat ».
- Nombre maximum de tentatives défini sur « 6 ».

VPN:

- Vérifier que le VPN est « Configuré ».
- Connexion VPN via l'app préférée.

E-mail:

- Définir le compte d'e-mail d'un utilisateur avec un profil d'e-mail.
- Empêcher l'utilisateur de déplacer des messages depuis ce compte.

Notifications:

- Vérifier que le VPN est « Configuré ».
- Connexion VPN via l'app préférée.

Fonctionnalités de Jamf Pro

La solution BYOD de Jamf Pro vous permet de créer un message de consentement et une description personnalisés pour le profil d'inscription, et permet aux anciens employés de supprimer le profil BYOD par le biais d'un processus simple s'ils quittent l'entreprise ou le programme.

Si votre entreprise doit mettre en œuvre tous les réglages de sécurité N1 ou N2 recommandés par le CIS, vous devez utiliser la fonction de Jamf Pro permettant d'enrôler l'appareil iOS en tant qu'appareil non supervisé appartenant à l'entreprise. Nous vous recommandons également de désactiver le réglage d'enrôlement par l'utilisateur dans le cadre de l'enrôlement iOS d'appareils personnels. Créer et distribuer des profils de configuration dans Jamf Pro permet de configurer, désactiver et/ou activer tous les réglages de sécurité des niveaux N1 et N2 pour un appareil ou des groupes d'appareils.

Autres considérations

Jamf Pro permet aux entreprises d'aller au-delà de la simple gestion des appareils et des profils de configuration en garantissant que les appareils sont toujours équipés des logiciels les plus récents et ne laissent aucune possibilité d'accès aux attaques malveillantes.

Recommandations CIS :

• S'assurer que l'appareil iOS n'a pas été manifestement débloqué.
• Garder les logiciels à jour.
• Activer le téléchargement automatique des mises à jour d'apps.
• Sur les appareils des utilisateurs finaux seulement, activer Localiser mon iPad et/ou Localiser mon iPhone.
• S'assurer que les cibles de grande valeur exploitent la structure d'appareil iOS la plus récente.

Fonctionnalités de Jamf Pro

Jamf Pro assure une assistance le jour même pour les systèmes d'exploitation des iPad et iPhone, garantissant ainsi que les versions les plus récentes des logiciels sont toujours prises en charge. De plus, Self Service de Jamf Pro permet aux entreprises de mettre sur pied leur propre catalogue d'apps proposant toutes les ressources, les apps et les configurations dont pourraient avoir besoin les utilisateurs. L'accès à la demande est accordé à tous les utilisateurs, sans qu'ils aient à transmettre un ticket d'assistance au service informatique. Si un appareil est perdu ou volé, Jamf Pro peut le verrouiller, l'effacer et le réinitialiser en toute sécurité afin que les données personnelles et professionnelles ne soient jamais exposées.

L'amélioration de la sécurité de vos appareils commence ici

Avec Jamf Pro, il est plus facile de mettre en œuvre et de respecter les recommandations CIS Benchmark pour les appareils iOS d'Apple.

Demandez un essai gratuit pour mettre ce guide en pratique dans votre environnement.