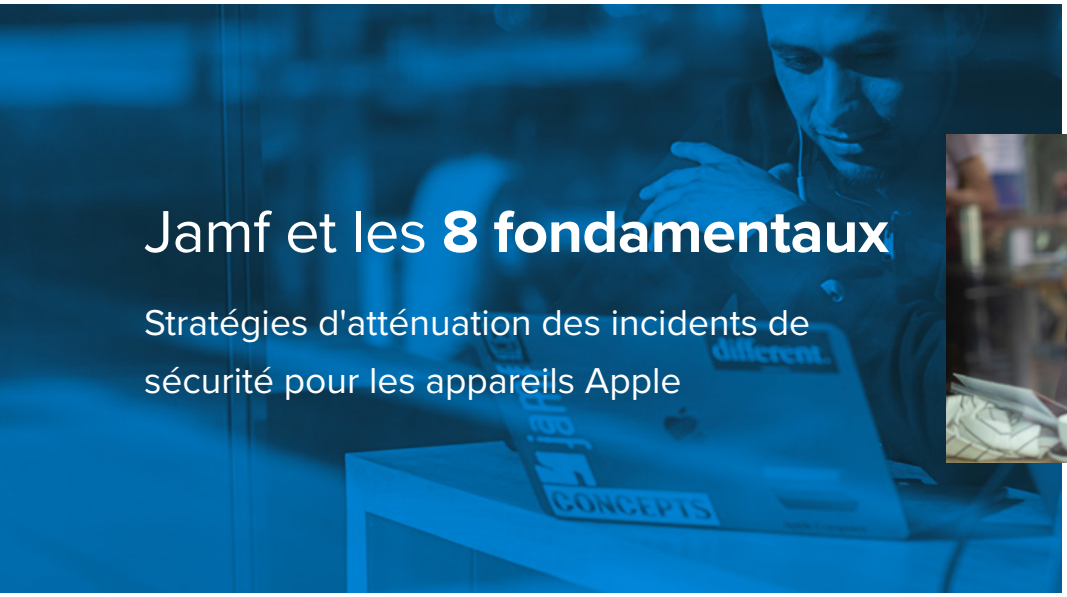
jamf



Jamf et les **8 fondamentaux**

Stratégies d'atténuation des incidents de sécurité pour les appareils Apple

Les organisations sont continuellement exposées à un paysage de risques de cybersécurité qui évolue sans cesse. Le Centre australien de cybersécurité (ACSC) a établi huit stratégies d'atténuation clés comme base de référence essentielle : les 8 fondamentaux. Ces principes ont pour but de prévenir les incidents de sécurité informatique. En tant que référence pour gérer et sécuriser Apple, Jamf propose un guide détaillant le modèle de maturité des 8 fondamentaux et l'intérêt des solutions Jamf pour le mettre en œuvre.

Que sont les 8 fondamentaux ?

Le Centre australien de cybersécurité (ACSC) de la Direction australienne des signaux a mis au point une série de stratégies d'atténuation de base pour aider les organisations à réduire l'impact des incidents de cybersécurité. Publiés pour la première fois en 2017, ces 8 fondamentaux sont associés à quatre niveaux de maturité qui accompagnent les entreprises dans leur implémentation. Chaque étape atténue un niveau supérieur de sophistication et de ciblage adverse.

Les 8 fondamentaux sont conçus pour protéger les terminaux Windows, mais de nombreuses organisations ont besoin des mêmes contrôles pour leurs appareils Apple. Les 8 fondamentaux n'empêcheront pas un adversaire déterminé et bien financé de compromettre la posture de sécurité globale d'une organisation. Ces principes doivent donc être pris en compte dans le cadre d'une stratégie d'atténuation holistique plus vaste.

Si vous êtes novice en matière de sécurité Apple et que vous souhaitez acquérir les notions de base, consultez notre e-book **Introduction à la sécurité des appareils Apple**.

Protection contre les logiciels malveillants

1 Contrôlez les applications pour empêcher l'exécution d'exécutables, de bibliothèques, de scripts, d'installateurs ou d'applets de panneaux de contrôle sur les postes de travail à partir de profils d'utilisateurs standards.

Les capacités de Jamf :

- Surveillance, alertes, blocage en temps réel des logiciels malveillants et mise en quarantaine des applications et processus suspects, avec prise en charge des listes de blocage personnalisées
- Gestion des applications : applications approuvées par Apple via l'App Store ou par des développeurs identifiés
- Profils de configuration et règles permettant de configurer les listes de blocage ou de sécurité définissant les applications approuvées
- Les détections de communications malveillantes de commande et contrôle (C2), de même que les alertes correspondantes, peuvent être exportées et centralisées dans un SIEM ou un SOAR.

2 Corrigez les applications. Appliquez les correctifs, les mises à jour et les mesures d'atténuation recommandées par les fournisseurs pour combler les vulnérabilités de sécurité dans les applications.

Les capacités de Jamf :

- Évaluation des risques liés aux applications avec vérification continue des versions afin de détecter et de signaler les logiciels obsolètes ou vulnérables.
- Déploiement et gestion des applications, mise à jour automatique vers la version la plus récente disponible sur l'App Store d'Apple
- « App Installers », qui automatisent le packaging, l'hébergement, le déploiement et la mise à jour des applications tierces
- Identification des sites malveillants pour bloquer les téléchargements d'applications à risque sur les appareils protégés

3 Configurez les paramètres de macro de Microsoft Office pour bloquer les macros provenant d'Internet et autoriser uniquement l'exécution des macros approuvées – que ce soit dans un « emplacement de confiance » avec un accès limité en écriture, ou sur la base d'une signature numérique associée à un certicat.

Les capacités de Jamf :

- Renforcement de la gestion des macros Microsoft Office grâce à un large éventail de préférences
- Surveillance et alerte en cas de téléchargement de fichiers malveillants ou d'exécutables contenant des macros Microsoft Office.
- Rapports détaillés pouvant être envoyés à des outils tiers de gestion des informations et des événements de sécurité (SIEM).

4 Durcissez les applications utilisateurs. Bloquez l'accès aux sites à risque. Désactivez les fonctionnalités inutiles de Microsoft Office (à commencer par OLE), des navigateurs web et des lecteurs de PDF.

Les capacités de Jamf :

- Une liste riche de profils de configuration pour gérer les appareils et les réglages des applications
- Filtrage du contenu web pour bloquer les publicités et les sites non approuvés
- Surveillance, détection, blocage et mise en quarantaine des processus malveillants
- Moteur de règles permettant d'appliquer les critères de sécurité tels que CIS et NIST
- Attributs d'extension personnalisés offrant des fonctionnalités de rapport et de notification enrichies

Limiter l'ampleur des incidents de cybersécurité

5 Limitez les privilèges administratifs sur les systèmes d'exploitation et les applications en fonction des tâches de l'utilisateur. Vérifiez régulièrement la nécessité des privilèges.

Les capacités de Jamf :

- Application par Self Service des règles qui ne nécessitent pas de privilèges d'utilisateur élevés
- Rapports sur les privilèges des comptes locaux, les élévations de privilèges et les saisies de mots de passe erronées, et regroupement des journaux unifiés.
- Accès réseau zero-trust (ZTNA) pour limiter l'accès aux applications via les assertions d'identité
- L'évaluation des risques liés aux appareils est prise en compte dans les règles d'accès afin d'appliquer le principe du moindre privilège.

6. Corrigez les systèmes d'exploitation. Corrigez ou atténuez vulnérabilités « à risque extrême » touchant les appareils fixes et mobiles dans les 48 heures. Utilisez la version la plus récente des systèmes d'exploitation. N'utilisez pas de versions non prises en charge.

Les capacités de Jamf :

- Gestion des correctifs imposant la mise à jour de l'OS sur les appareils Apple
- Vérifications de l'hygiène des appareils – OS vulnérables, profils à risque, jailbreak/root, etc.
- Rapports sur les versions d'OS et les outils de sécurité intégrés, pour une visibilité totale sur l'activité malveillante et l'état des appareils
- Règles d'accès aux applications basées sur les risques pour les appareils présentant des vulnérabilités « extrêmes » au niveau de l'OS

7. Adoptez l'authentification multifacteur y compris pour les VPN, RDP, SSH et autres accès à distance, et ce pour tous les utilisateurs effectuant des opérations privilégiées ou accédant à des dépôts de données importants (sensibles).

Les capacités de Jamf :

- Authentification multifacteur basée sur IP auprès de tous les services en contact avec Internet
- Authentification par identité cloud, synchronisation des mots de passe et utilisation de l'AMF avec mots de passe à usage unique.
- ZTNA pour les apps SaaS ou d'entreprise, application du principe de moindre privilège par le biais d'assertions d'identité AMF.
- Intégration de l'accès conditionnel de Microsoft
- Intégration SAML : Self Service, inscription initiée par l'utilisateur

Récupération des données et disponibilité des systèmes

> **8. Sauvegardez quotidiennement** les données importantes, les logiciels et les paramètres de configuration, et conservez-les pendant au moins trois mois. Testez la procédure de restauration au départ, une fois par an et à chaque modification de l'infrastructure informatique.
>
> **Les capacités de Jamf :**
>
> - Connexions aux réseaux de sauvegarde protégées par des règles d'accès zero-trust et utilisation exclusive de services de sauvegarde approuvés
> - Filtrage de contenu basé sur des catégories qui permet aux organisations de limiter l'accès aux services Shadow IT, et en particulier aux services cloud et de stockage de fichiers non approuvés.

Conclusion

Jamf facilite la mise en œuvre et le suivi des 8 stratégies fondamentales recommandées par le Centre australien de cybersécurité pour atténuer les incidents de cybersécurité.

Découvrez ces fonctionnalités de sécurité par vous-même en profitant d'un essai gratuit.