jamf



Jamf Mobile Forensics

Protégez les appareils mobiles contre les cyberattaques avancées.

Qu'ils soient fonctionnaires, cadres d'entreprise, personnalités politiques ou autres**, les utilisateurs à haut risque sont confrontés à des menaces qui exigent des stratégies de défense concrètes**. Pour lutter contre les menaces persistantes avancées (APT), les logiciels espions mercenaires, les attaques chapeautées par des États voyous et les exploitations zéro-clic, les équipes de sécurité doivent analyser en permanence l'intégrité des appareils et détecter tous les indicateurs de compromission (IOC), sans perturber les utilisateurs, déployer des agents invasifs ni exposer d'informations personnelles identifiables (PII).

Jamf Mobile Forensics ajoute une couche de sophistication à la défense contre les menaces mobiles : cet outil aide les équipes de sécurité à détecter et à explorer les menaces qui échappent aux outils traditionnels.

Avantages clés :

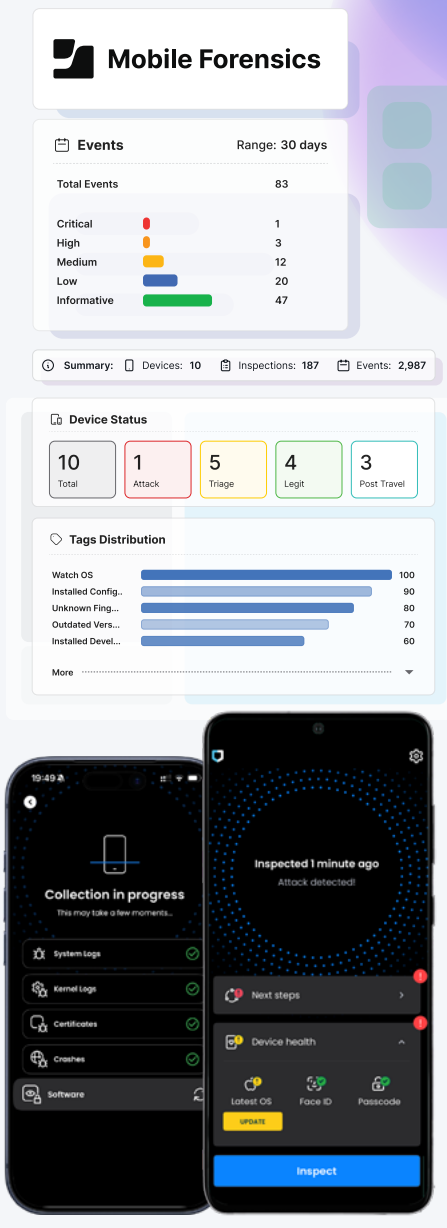
- Détectez les attaques ciblées et « zero day » avant qu'elles ne pénètrent dans le réseau
- Analysez en profondeur tous les types de journaux (système, crash, noyau et applications) sans rooter ni jailbreaker l'appareil
- Simplifiez les enquêtes criminalistiques et réduisez la part de recherche manuelle
- Protégez la confidentialité des utilisateurs et garantissez la fiabilité des appareils des utilisateurs à haut risque

Chaîne d'exploitation mobile

Progression de la chaîne d'exploitation mobile, de l'accès initial à la post-exploitation :

Pièce jointe malveillante / Exploitation WebKit → Accès initial → Exécution de code (compromission de processus WebContent) → Escalade de privilèges → Furtivité/évasion → Activité post-exploitation (collecte de données, accès au micro ou à la caméra, etc.) → Communication C2 → Nettoyage / mesures anti-analyse criminalistique

L'analyse des menaces et la chaîne d'exploitation aident les équipes de sécurité à comprendre le déroulement des événements et à déterminer les mesures à prendre. Jamf Mobile Forensics vous apporte cette visibilité.



Réduisez de plusieurs semaines à quelques minutes le temps consacré à l'analyse criminalistique des mobiles

Analyses de criminalistique numérique à distance et réponse aux incidents

Réduisez les temps d'arrêt et assurez la productivité des utilisateurs stratégiques

- L'analyse comportementale exclusive détecte les comportements anormaux, les attaques « zero day » et les IOC propres à Pegasus, à Predator et à d'autres logiciels espions.
- Évitez les expositions prolongées en explorant la télémétrie au niveau de l'appareil
- Grâce à l'analyse instantanée, les équipes de sécurité comprennent la marche à suivre et répondent immédiatement aux attaques avancées.

Recherche proactive des menaces

Traduisez des données de sécurité complexes en informations exploitables

- Simplifiez les workflows d'enquête en regroupant les chronologies, les types et les degrés de gravité des événements en incidents unifiés
- Automatisez les chronologies d'événements pour examiner directement de quelle façon et à quel moment un appareil a été compromis
- Détecter les IOC inconnus en analysant les fichiers, les applications, les processus, les journaux de collisions, etc.

Analyse pilotée par l'homme et renforcée par l'IA

L'analyse IA fait office d'assistant de recherche en criminalistique

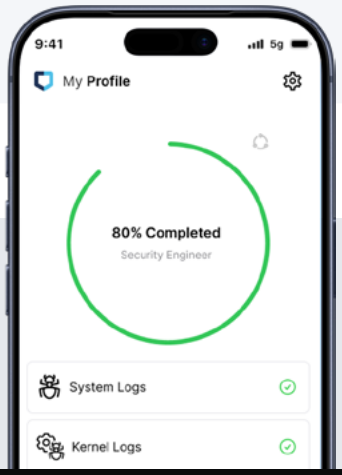
- Elle allège les recherches manuelles nécessaires à l'analyse des pannes d'appareils et des anomalies.
- Elle résume les incidents et recommande les étapes à suivre pour les corriger
- L'analyse IA est désactivée par défaut pour laisser aux entreprises un contrôle total sur l'utilisation de l'IA

** L'analyse IA est une fonctionnalité réservée au cloud.*

Criminalistique et confidentialité par conception

Protégez les utilisateurs contre toutes les menaces pesant sur leur confidentialité et sur l'intégrité de leur appareil

- Aucune IPI n'est prélevée. L'analyse ne nécessite aucun accès aux mots de passe, photos, vidéos, messages, contacts, historique des appels, historique du navigateur, jetons d'authentification à deux facteurs, ni données d'applications
- L'application DFIR à distance réalise des analyses silencieuses à des intervalles définis par l'organisation et délivre aux utilisateurs des informations sur la sécurité de l'appareil.



Jamf Mobile Forensics bénéficie du soutien de **Jamf Threat Labs**, notre équipe de chercheurs en sécurité, d'analystes et d'ingénieurs. Ces experts publient des recherches sur les logiciels malveillants et les logiciels espions mobiles, et apportent constamment des améliorations aux moteurs de Jamf Mobile Forensics

jamf

www.jamf.com/fr/

© 2026 Jamf, LLC. Tous droits réservés.

Pour en savoir plus, contactez votre représentant Jamf.
Ou demandez une version d'essai.