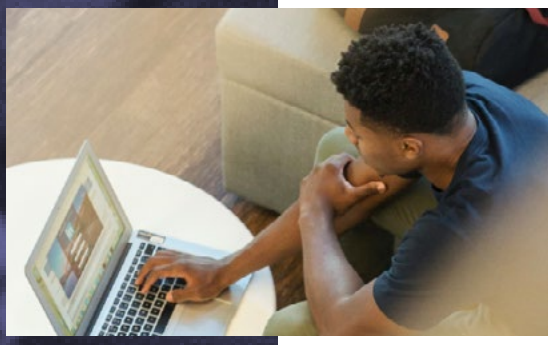
jamf

LIVRE BLANC

Guide sur le processus de réponse aux incidents de sécurité sur macOS



Lorsqu'une entreprise fait l'objet d'une cyberattaque ou d'une brèche de sécurité, l'efficacité et l'efficience de sa capacité de réaction sont directement liées à la quantité des dommages subis, au temps de reprise nécessaire et aux frais engendrés. C'est ce que l'on appelle une intervention en cas d'incident informatique. Il s'agit d'un élément essentiel d'un programme de sécurité probant utilisé par les équipes chargées du service informatique ou de la sécurité de l'information.

Même si la plupart des entreprises disposent d'une solide expérience dans la défense contre les menaces informatiques, votre organisation peut utiliser certains outils, workflows et bonnes pratiques afin de s'y préparer et d'être prête à faire face à une éventuelle cyberattaque ou brèche de sécurité. Et, avec le nombre croissant de Mac dans l'entreprise, il est maintenant temps d'optimiser vos pratiques de sécurité Mac et de garantir la protection de votre entreprise.

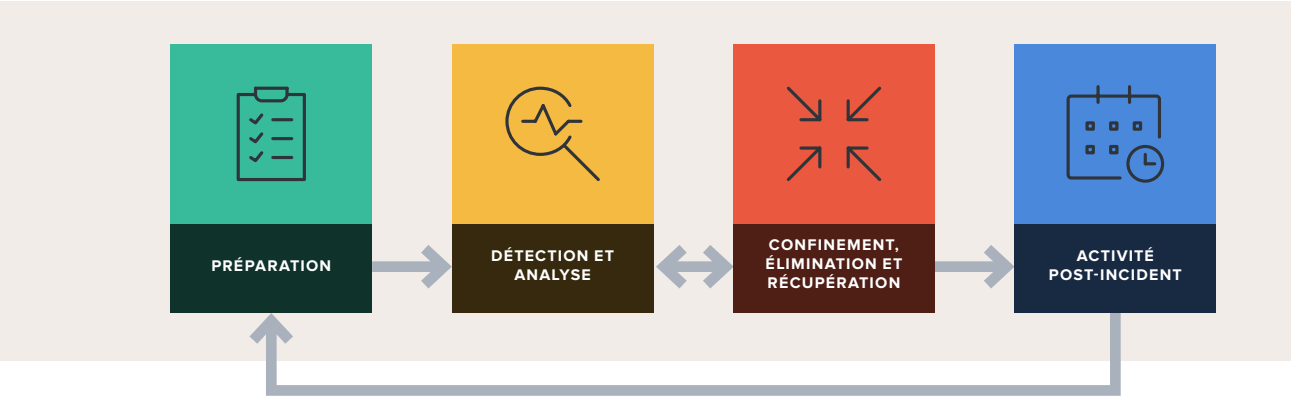
Dans notre livre blanc, vous apprendrez à réaliser les étapes suivantes :

1. Se préparer aux incidents
2. Détecter et analyser les incidents
3. Contenir, éradiquer et récupérer suite à des incidents
4. Surveiller l'activité post-incident

Les attaques uniques exigent une défense unique

Le Mac étant de plus en plus utilisé, les organisations doivent redoubler d'attention afin de pouvoir protéger et sécuriser leurs Mac au-delà des solutions de sécurité proposées par Windows. Les Mac ont toujours intégré des outils de sécurité. Cependant, en prenant en considération les nouveaux processus d'attaque et la part de marché croissante, de meilleures méthodes doivent être adoptées pour protéger le système d'exploitation et les données de votre entreprise. Mais, peu importe la façon dont vous exploitez vos solutions de sécurité Mac, la réponse aux incidents doit être méthodique et cohérente.

Comme le prévoit le National Institute of Standards and Technology (NIST), les quatre composantes d'une intervention en cas d'incident de sécurité sont les suivantes :



Étape 1 : Se préparer aux incidents

La sécurité est une priorité de premier plan pour toutes les organisations, ou presque, et deviendra encore plus importante avec le nombre croissant d'entreprises qui adoptent le travail à distance. Les administrateurs informatiques ont besoin d'avoir une sécurité aussi élevée que possible. La sécurité des terminaux doit être gérée, contrôlée, corrigée et configurée. Pour ce faire, une variété d'outils entrent en jeu.

Avec Jamf Pro, des tableaux de bord vous tiendront informés de l'état des appareils Mac et baliseront le matériel qui a besoin de votre attention. Grâce à la fonctionnalité brevetée du groupe intelligent, les administrateurs informatiques peuvent cibler les appareils qui doivent être mis à jour, reconfigurés ou corrigés et améliorer ainsi leur posture de sécurité. Tout cela se fait à distance et peut être automatisé sans que le service informatique n'ait à toucher physiquement l'appareil.

Afin d'avoir une visibilité sur ce qui se passe sur un appareil, Jamf Protect, une solution professionnelle de protection des terminaux conçue pour Mac, rassemble des informations sur les processus et les fichiers tout en procédant à d'autres analyses comportementales. Toutes ces informations vous seront très utiles pour procéder à une analyse en temps réel et post-événement, identifier ainsi les activités malveillantes et envoyer des avertissements. Choses importantes à prendre en considération :

- La prévention des menaces de Jamf Protect bloquera et mettra automatiquement en quarantaine les logiciels malveillants et publicitaires. Les entreprises souhaitant limiter l'accès à certains logiciels indésirables peuvent également le configurer au sein de Jamf Protect via des signatures, des identifiants d'équipe pour les développeurs, etc.
- Des procédures d'analyse intégrées à Jamf Protect permettent de détecter les formes communes d'attaque contre macOS. Afin que les mécanismes de détection puissent correctement atténuer les risques, l'analyse est cartographiée dans le cadre MITRE ATT&CK® et fournit une couverture fiable contre les vecteurs d'attaque.
- Jamf Protect recueille un niveau fiable de données associées à toute attaque identifiée. Vous pouvez donc consulter toutes les informations concernant les processus, les utilisateurs, les groupes et les binaires au moment où une menace est détectée.
- Vous pouvez transmettre les données et les avertissements de Jamf Protect à votre SIEM. Vous pouvez également directement envoyer les données journalisées provenant de macOS Unified Logging à votre SIEM ou à tout autre système d'enregistrement.
- Grâce à Jamf Pro, de nombreuses attaques peuvent être contrées par le biais de réponses communes pour lesquelles vous pouvez configurer et automatiser les réponses et actions de restauration.
- Pour répondre à un incident, des workflows additionnels peuvent être automatiquement ou manuellement déclenchés dans Jamf Pro en utilisant la portée des groupes intelligents qui lanceront les politiques et les profils de configuration.

Les politiques et les profils de configuration permettent les solutions suivantes :

ISOLATION DU RÉSEAU	Isoler les appareils qui peuvent faire l'objet d'une attaque active là où les dommages doivent être contenus.
PÉNALITÉ	Restreindre l'accès aux ressources de l'entreprise à un utilisateur douteux.
VERROUILLER LES APPAREILS	Verrouiller l'accès à l'appareil aux utilisateurs pendant l'enquête sur une activité suspecte.
SUPPRIMER LES OBJETS	Supprimer à distance les applications, les plugins ou les fichiers indésirables de l'appareil.
MISE EN QUARANTAINE DE L'APPAREIL	Si un incident nécessite d'accéder physiquement à un appareil et ne peut être réparé à distance, le mettre en quarantaine et l'isoler jusqu'à que le service informatique puisse le contrôler physiquement.
EXÉCUTER DES SCRIPTS/DES COMMANDES PERSONNALISÉS	Exploiter les scripts et les commandes qui permettent de récupérer les données ou les informations à distance de l'appareil sans y toucher physiquement.
ENVOYER DES MESSAGES PERSONNALISÉS À L'UTILISATEUR FINAL	Communiquer directement les informations concernant les tentatives d'attaque ou les politiques et les bonnes pratiques de l'organisation aux utilisateurs finaux.
RÉCUPÉRER LES APPAREILS	Redéployer à distance macOS et les applications sur un appareil qui doit être remis en état.

Étape 2 : Détecter et analyser

Même si l'équipe chargée de la sécurité est alertée en cas d'attaque, elle ne doit jamais se reposer sur ses lauriers. Quels que soient le degré de préparation et les mécanismes de prévention mis en place, les équipes de sécurité doivent supposer que les attaques arriveront à passer au travers de leurs meilleures défenses et être prêtes à intervenir.

Imaginez qu'un utilisateur final télécharge accidentellement une application compromise… C'est à ce moment là que votre solution de sécurité de terminaux doit fonctionner efficacement. Au moment où l'incident de sécurité se produit, et si vous n'avez aucune idée de l'impact qu'il pourrait avoir, vous devez recueillir les informations pertinentes, analyser la menace et avoir la capacité d'isoler cet appareil pour éviter toute nouvelle contamination.

Pour mener leur enquête sur l'incident, les équipes de sécurité ont toujours besoin d'une plus grande visibilité. Pour cela, il est courant qu'elles recueillent des journaux de divers systèmes et appareils dans leur SIEM ou d'autres systèmes d'agrégation de journaux. Une organisation peut alors avoir une vision complète et personnalisable de ce qui se passe dans sa flotte de Mac et mener à bien son enquête ou son audit.

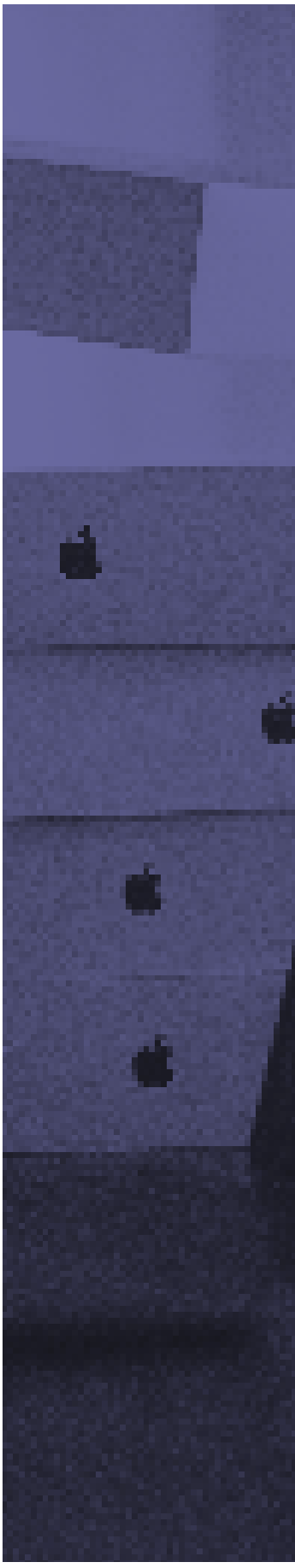
Étape 3 : Contenir, éradiquer et restaurer

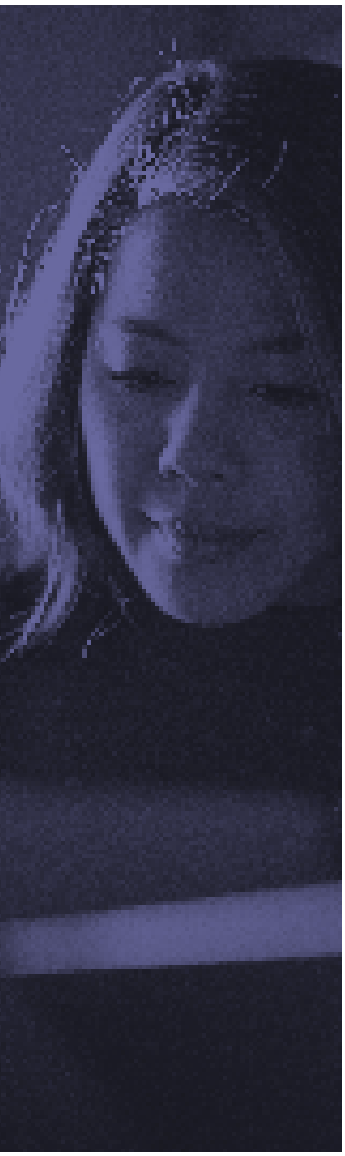
Lorsque votre réseau fait l'objet d'une attaque active, le temps est primordial. Dans un premier lieu, il faut stopper l'attaque et empêcher son expansion à d'autres systèmes. Étant donné que vous vous êtes préalablement préparé, Jamf Protect pourra probablement bloquer les processus concernés. Cependant, cela ne signifie aucunement que les autres tentatives d'attaque, celles qui ne sont pas si évidentes, seront éradiquées. Pour réduire les risques de dommages au minimum lors d'une intervention sur un avertissement lié à l'activité, Jamf Protect repose sur la technologie du groupe intelligent ainsi que sur toutes les commandes de gestion des appareils mobiles (MDM) et Jamf Pro. Voici quelques exemples de réponses automatisées :

- Isoler la machine sur le réseau pour qu'elle ne puisse communiquer qu'avec l'infrastructure de gestion.
- Réduire l'accès au cloud ou aux ressources de l'entreprise.
- Fournir des indications à l'utilisateur final pour l'informer de la présence d'une activité malveillante sur son appareil et lui conseiller de s'abstenir de toute autre action.

Une fois l'appareil sécurisé et l'attaque arrêtée, les équipes chargées du service informatique et de la sécurité devront analyser plus en détail ce qui s'est passé sur l'appareil et si d'autres scripts, binaires, portes dérobées, nouveaux identifiants et risques supplémentaires persistent. Avec Jamf, les équipes peuvent :

- Récupérer les binaires bloqués de la quarantaine et les inspecter.
- Supprimer les binaires identifiés ou autres fichiers.
- Identifier les applications nouvellement installées.
- Identifier de nouveaux comptes d'utilisateurs locaux.





Une fois que Jamf aura atténué l'attaque, il faudra également sécuriser les appareils. Grâce à la puissance des règles de Jamf Pro et des groupes intelligents, vous pouvez nettoyer votre environnement sans frais supplémentaires :

- En exécutant des scripts et des commandes personnalisées et en réinitialisant ainsi les paramètres de sécurité.
- En envoyant des messages personnalisés aux utilisateurs finaux pour les rediriger vers des ressources d'aide supplémentaires.
- En redéployant macOS sur l'appareil et en réinstallant des applications.

Étape 4 : Activité post-incident

Avec Jamf Protect, les équipes chargées du service informatique et de la sécurité peuvent recevoir des notifications opportunes en cas d'incident et disposent des outils dont elles ont besoin pour analyser ce qui s'est exactement passé. Dans un environnement Windows, les processus de confinement, d'éradication et de récupération sont souvent construits sur mesure. Jamf permet d'avoir accès à cette fonctionnalité sur Mac. Les équipes pourront ainsi réagir et remédier au prochain incident de sécurité de la meilleure façon qui soit pour Apple.

Après un incident :

- Jamf Protect continue de surveiller et de faire état de toutes les menaces et activités supplémentaires.
- Vous pouvez personnaliser Jamf Protect et élargir ses fonctionnalités pour couvrir les autres menaces ciblées que votre équipe informatique ou InfoSec identifie.
- Ajouter des informations binaires sur les menace identifiées dans une liste de prévention personnalisée pour assurer la protection de l'ensemble de la flotte de Mac.
- S'assurer que les utilisateurs finaux ciblés par une attaque repassent leur certification en suivant la formation opérationnelle InfoSec.

Optimisez la sécurité de vos Mac dès aujourd'hui

Pour évaluer efficacement un incident de sécurité et déterminer la vulnérabilité potentielle d'une brèche, Jamf Pro, associé à Jamf Protect, vous permet de surveiller, d'éviter, de détecter et de contrer la myriade d'attaques qui peuvent s'en prendre à votre flotte de Mac et d'intervenir en conséquence.

Que vos utilisateurs finaux téléchargent des applications compromises ou que vous fassiez l'objet de tentatives de phishing ou d'attaques de ransomware, la restauration vous permet de prendre les mesures nécessaires pour sécuriser votre matériel, vos logiciels et les données de votre entreprise.

Testez les fonctionnalités de notre réponse aux incidents de sécurité avec un essai gratuit.

Demandez un essai

Ou contactez votre revendeur Apple.