PRÉSENTATION DU PRODUIT

File Integrity Monitoring

L'utilisation d'une surveillance constante pour garantir l'intégrité des fichiers sensibles est bien plus qu'une des meilleures pratiques de sécurité. Pour de nombreuses organisations, il s'agit également d'un mandat réglementaire. En combinant la surveillance de l'intégrité des fichiers (File Integrity Monitoring) avec une solution SIEM, la gestion des journaux (Log Management), l'analyse des machines (Machine Analytics) et l'investigation des hôtes et des réseaux (Host Forensics et Network Forensics), LogRhythm permet aux clients de simplifier et de renforcer leur sécurité, leur vérification et leur conformité à l'aide d'une solution unique totalement intégrée.

Surveillance de l'intégrité des fichiers (File Integrity Monitoring) centrée utilisateur

L'approche holistique de LogRhythm permet au personnel de sécurité d'être notifié lorsque des fichiers sont créés ou que des fichiers clés sont visualisés, supprimés ou modifiés, et lorsque la propriété collective de fichiers est changée. Pour une surveillance sélective, LogRhythm fournit des contrôles et des filtres granulaires qui peuvent identifier des fichiers spécifiques et réaliser des balayages aux intervalles souhaités ou fonctionner en temps réel pour une protection continue. Le comportement au niveau du fichier peut alors être corrélé avec des activités de sécurité et de vérification supplémentaires pour construire une fenêtre complète sur l'activité réseau potentiellement dangereuse.

PCI DSS 11.5 exige de :

Déployer une surveillance de l'intégrité des fichiers pour alerter le personnel de modifications non autorisées de fichiers du système ou de contenus critiques, et réaliser des comparaisons de fichiers au moins une fois par semaine, ou plus fréquemment si le processus peut être automatisé.

« La conformité PCI n'est qu'un instantané. Assumer que vous êtes en sécurité parce que vous avez adopté des mesures préventives vous rend plus vulnérable. Vous devez intervenir pour avoir un temps d'avance sur ceux qui cherchent constamment à exploiter des failles dans votre réseau. »

Bernie Rominski
Responsable de sécurité informatique
Regis Corporation

Grâce à l'ajout de la surveillance de l'intégrité des fichiers (File Integrity Monitoring), LogRhythm peut être utilisé pour surveiller un large éventail de comportements malveillants et générer les alertes correspondantes, de l'accès irrégulier d'un utilisateur à des fichiers confidentiels aux violations liées à un réseau zombie, en passant par la transmission de données sensibles. La solution combinée permet aux organisations de satisfaire à des exigences spécifiques de conformité à la réglementation, comme la Payment Card Industry Data Security Standard (PCI DSS) 11.5 et 12.9, sans avoir besoin d'acheter un autre produit.

Intégration totale avec la gestion des journaux et des événements (Log Management et Event Management) et avec la surveillance et le contrôle des points d'accès (Endpoint Monitoring & Control)

- Répond à 80 exigences différentes en matière de contrôle de PCI DSS.
- Envoie des alertes contextualisées lorsque des données confidentielles sont visualisées, modifiées ou supprimées.
- Fournit un jeu complet de données d'investigation pour identifier rapidement la source des atteintes à la sécurité.
- Configuration et administration centralisées, fondées sur des politiques.

Surveillance de tous les types de fichiers

- Surveille les fichiers exécutables, les fichiers de configuration, les fichiers de contenu, les fichiers de journal et de vérification, les fichiers Internet, et bien d'autres encore.
- Les contrôles granulaires garantissent que chaque fichier surveillé est analysé selon la fréquence souhaitée.
- La surveillance de l'intégrité des fichiers (FIM) en temps réel fournit des informations spécifiques : quel utilisateur a visualisé, modifié ou supprimé quels fichiers.

Des politiques prêtes à être utilisées sont fournies pour les applications courantes.

La surveillance de l'intégrité des fichiers (File Integrity Monitoring) de LogRhythm est prise en charge sur les systèmes Windows, Unix et Linux.