



Varonis et LogRhythm

Avec l'intégration de Varonis et de LogRhythm, nos clients communs bénéficient de moyens de veille inégalés sur le royaume des données non structurées, données qu'ils ont généralement le plus et pourtant connaissent le moins. De la reconnaissance initiale à l'exfiltration des données, Varonis et LogRhythm vous aident à repérer les signes avant-coureurs avant qu'un incident ne se transforme en atteinte à la sécurité des données de grande ampleur.

Les solutions de Varonis détectent les cyberattaques et identifient les menaces internes grâce à une analyse approfondie des métadonnées, à l'apprentissage machine et à l'analyse avancée du comportement des utilisateurs. Varonis enregistre davantage de métadonnées relatives aux données non structurées et aux systèmes de fichiers que n'importe quelle autre solution : DatAdvantage surveille de manière non intrusive l'activité menée sur un vaste éventail de plates-formes, incluant Windows, NAS, SharePoint, Exchange, Active Directory, UNIX/Linux et Office365.

DatAdvantage et DatAlert de Varonis analysent et suivent les données, l'activité des comptes et le comportement des utilisateurs tout en surveillant tout comportement suspect et toute activité inhabituelle afin de sécuriser les données de l'intérieur.

L'intelligence de sécurité et l'analyse de LogRhythm permettent une gestion de bout en bout sur l'ensemble du cycle de vie de la menace. LogRhythm fournit également des solutions ciblées pour la SIEM, la surveillance et l'infoperspective du réseau et du point de terminaison ainsi que l'analyse de la sécurité.

LogRhythm collecte et analyse en permanence les données utilisateurs dynamiques capturées par Varonis. Ces données sont exploitées en combinaison avec des pétaoctets d'autres données machine collectées sur l'ensemble des systèmes composant l'environnement d'une organisation. Le but étant de rapidement détecter les menaces et événements à haut risque et de leur donner un degré de priorité. Ces actions permettent aux équipes de sécurité de neutraliser rapidement les menaces avant qu'elles ne se transforment en incidents ou atteintes à la sécurité des données à fort impact.



CAPACITÉS DE DÉTECTION IMMÉDIATE

DatAdvantage et DatAlert de Varonis s'intègrent facilement avec la plate-forme d'intelligence de sécurité de LogRhythm pour identifier :

- Un comportement utilisateur statistiquement inhabituel
- Des modèles suspects de tentatives infructueuses de connexion et d'activité utilisateur anormale
- Les suppressions et les modifications massives
- Les modifications effectuées hors des fenêtres de contrôle
- Les infections de programmes malveillants et de rançongiciels comme CryptoLocker et CryptoWall
- Les anomalies d'authentification géographiques et temporelles indiquant des comptes compromis
- Les escalades de privilèges non autorisées
- Et bien plus encore
- L'accès administratif aux données utilisateur
- Un accès inhabituel ou administratif à des informations personnelles identifiables

L'installation de DatAdvantage et de DatAlert de Varonis ne prend pas plus d'une heure et l'intégration avec LogRhythm est aussi simple que la configuration d'une adresse IP.

Grâce aux modules d'extension SmartResponse™ de LogRhythm, les analystes peuvent prendre immédiatement des mesures de protection en cas de menaces utilisateur, notamment verrouiller un point de terminaison associé à un compte utilisateur compromis et désactiver un utilisateur dans Active Directory.

À propos de VARONIS

Varonis est le principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques. Grâce au lancement d'une plateforme logicielle innovante, Varonis permet aux entreprises d'analyser, de protéger, de gérer et de faire migrer leurs données non structurées. Varonis est spécialisé dans les systèmes de fichiers et de messagerie contenant de précieux documents de traitement de texte, feuilles de calcul, présentations, séquences audio et vidéo, e-mails et textes.

À propos de LOGRHYTHM

LogRhythm est un grand fournisseur de renseignements et d'analyses de sécurité qui aide les entreprises du monde entier à détecter, contrer et neutraliser rapidement les cybermenaces. Sa plateforme primée réunit une gestion des informations et événements de sécurité de pointe, la gestion des journaux, l'analyse technique des réseaux et des terminaux, et des analyses de sécurité évoluées. En plus de protéger ses clients des risques associés aux cybermenaces, LogRhythm leur fournit une automatisation et une garantie de conformité innovantes ainsi que des renseignements informatiques détaillés.