VARONIS + FIREEYE TAP

Les organisations stockent d'énormes quantités de données non structurées, des fichiers et des e-mails, qui comprennent certaines de leurs informations les plus précieuses. Malheureusement, ces ressources sont fréquemment dérobées à l'occasion d'atteintes graves à la sécurité, soit par des employés qui abusent de leur accès (comme pour Snowden) ou par des personnes extérieures qui utilisent les données d'authentification des employés (comme pour Sony).

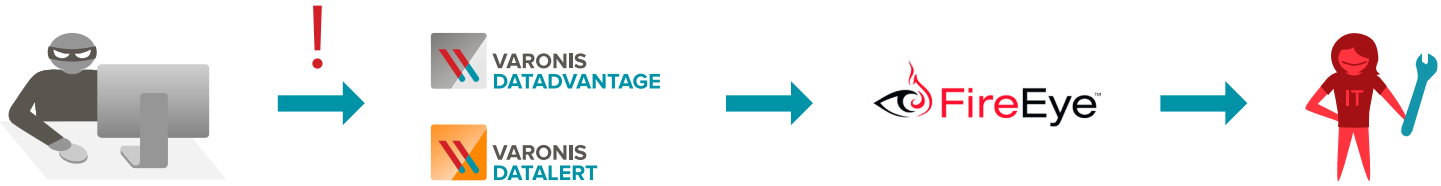
Les organisations, confrontées à une technologie en constante évolution et à un environnement de menaces, ont compris qu'il n'était plus réaliste de ne protéger que leur périmètre pour se prémunir des assaillants. Aggravant le risque, les utilisateurs qui sont déjà à l'intérieur des murs ont accès à beaucoup plus d'informations que nécessaire pour accomplir leur travail. Pire encore, les organisations sont rarement informées de l'atteinte à leur sécurité avant des mois, si toutefois elles le savent un jour, car sur la plupart des systèmes internes, le comportement des utilisateurs n'est pas surveillé ni analysé pour repérer les abus.

Varonis a aidé des milliers de clients à protéger leurs données non structurées en analysant l'activité des utilisateurs à travers les fichiers et les e-mails, les permissions et les métadonnées du système de fichiers, ainsi que le contenu des fichiers.

Dans une récente enquête informelle réalisée par e-mail, sur 141 clients de Varonis, 31 % ont répondu qu'ils avaient déjà détecté des activités d'employés suspectes ou des logiciels malveillants grâce à nos solutions.

Les clients de FireEye rapportent des renseignements relatifs aux menaces depuis de nombreuses sources et notamment IDS/IPS, DLP, les applications professionnelles et les journaux des pare-feu.

Avec l'intégration de Varonis et FireEye TAP, les clients de FireEye et Varonis bénéficient d'un système de renseignements sans précédent dans l'univers des données non structurées ; celles dont elles disposent en plus grand nombre et qu'elles connaissent le moins. De la reconnaissance initiale à l'exfiltration des données et la dissimulation de l'attaque, Varonis et FireEye TAP vous aident à repérer les signes annonciateurs avant que vous ne fassiez la une des journaux.



DES CAPACITÉS DE DÉTECTION IMMÉDIATES

Intégrez aisément Varonis DatAdvantage et DatAlert avec FireEye TAP et identifiez :

- Les comportements utilisateur statistiquement inhabituels
- Les suppressions et les modifications massives
- Les infections par des logiciels malveillants et des rançongiciels comme Cryptolocker et Cryptowall
- Les escalades de privilèges
- L'accès administratif aux données utilisateur
- Les accès inhabituels ou administratifs aux informations d'identification personnelle
- Les échecs de connexion répétés
- Les modifications effectuées hors des fenêtres de contrôle
- Et bien plus encore

L'installation de Varonis DatAdvantage et DatAlert peut prendre une heure seulement et l'intégration avec FireEye TAP est aussi simple que de configurer une adresse IP.

À PROPOS DE DATADVANTAGE

Varonis DatAdvantage s'assure à tout moment que seules les bonnes personnes ont accès aux bonnes données, contrôle toute l'activité et alerte en cas d'abus.

Varonis sécurise vos données depuis l'intérieur, en utilisant l'apprentissage machine pour modéliser et détecter les activités anormales, de manière à stopper les atteintes à la sécurité des données avant même qu'elles ne se produisent.

À PROPOS DE DATALERT

Varonis DatAlert déclenche des alertes en temps réel sur plusieurs plates-formes en se basant sur l'activité liée aux fichiers et aux e-mails, aux modifications de permissions et à d'autres événements critiques, pour vous aider à détecter en temps réel les éventuelles atteintes à la sécurité, les mauvaises configurations et d'autres problèmes.

À PROPOS DE VARONIS

Varonis est le principal fournisseur de solutions logicielles pour les données d'entreprise non structurées d'origine humaine.

Varonis offre une plateforme logicielle innovante permettant aux entreprises de cartographier, d'analyser, de gérer et de faire migrer leurs données non structurées. En savoir plus sur www.varonis.fr.

Évaluation gratuite de 30 jours:

DANS LES HEURES SUIVANT L'INSTALLATION:

Vous pouvez instantanément effectuer une vérification des autorisations : Fichier et autorisations d'accès aux dossiers et comment cartographier les utilisateurs et groupes spécifiques. Vous pouvez même générer des rapports.

UN JOUR APRÈS L'INSTALLATION:

Varonis DatAdvantage commencera par vous montrer quels utilisateurs accèdent aux données, et de quelle manière.

3 SEMAINES APRÈS L'INSTALLATION:

Varonis DatAdvantage fournira des recommandations très fiables sur la façon de limiter l'accès aux fichiers et aux dossiers aux seuls utilisateurs en ayant besoin pour leur travail.

À PROPOS DE FIREEYE

FireEye est un leader des solutions de cybersécurité, qui protège les ressources les plus précieuses au monde contre ceux qui les menacent. Notre cocktail de technologie, de renseignement et d'expertise, servi par l'équipe de réponse aux incidents la plus réactive, nous permet d'éliminer les conséquences des atteintes à la sécurité.

DEMARREZ VOTRE ESSAI GRATUIT