CINQ DIFFICULTÉS RENCONTRÉES DANS L'ANALYSE DE LA SÉCURITÉ

ET COMMENT LES ÉVITER

VARONIS

TABLE DES MATIÈRES

> “Les organisations ne parviennent pas à détecter les piratages dans des délais rapides, avec moins de 20 % des vols de données détectés en interne.[1]

Gartner

VARONIS

INTRODUCTION

De nombreuses organisations ont commencé à envisager de mettre en place une analyse de la sécurité pour renforcer leurs capacités de détection.

Les entreprises qui se lancent dans l'exploration des technologies d'analyse de la sécurité et de collecte des journaux (logs) pensent souvent pouvoir détecter les piratages en envoyant simplement des journaux à un serveur central pour analyse. S'il est vrai que l'on a besoin de journaux, leur donner du sens est bien plus difficile que ce que l'on pourrait penser.

Voici cinq problèmes que les organisations rencontrent lorsqu'elles tentent d'explorer leurs journaux de manière proactive et d'enquêter sur les incidents de sécurité :

1. Les journaux sont nombreux – la plupart des organisations devront conserver des centaines de millions d'événements par jour. Appareils réseau, terminaux, systèmes de sécurité, applications, appareils de stockage, proxies – tous écrivent une multitude d'événements, et chaque type d'appareil et de fournisseur rédige ses journaux à sa façon.

2. Ils ne sont pas utilisables dans leur forme brute.

Pour utiliser les journaux, il faut d'abord analyser leur syntaxe ou reconnaître les objets qu'ils décrivent : Il s'agit d'un utilisateur, il s'agit d'un appareil, il s'agit d'un événement de connexion, etc. Sans analyse syntaxique des journaux, il est impossible d'établir des relations entre les objets d'un journal et ceux d'un autre, ce qui est impératif pour mettre en place une analyse proactive et minutieuse des données. C'est d'autant plus difficile que les journaux n'ont pas de format standard – chacun des différents formats doit donc faire l'objet d'une analyse syntaxique. En outre, dans certains journaux, un simple « événement » est décrit en plusieurs lignes qui apparaissent parfois dans le désordre. Ces journaux sont plus utiles lorsqu'ils sont combinés, aussi bien pour les humains que pour les technologies d'analyse.

3. Même au terme d'une analyse adéquate, ces journaux manquent de contexte. Les analystes en sécurité doivent définir des priorités et examiner les journaux qui débouchent sur l'émission d'une alerte. Qui est l'utilisateur et que fait-il ? Est-ce sa machine ? Où travaille-t-il ? Les analystes en sécurité consacrent beaucoup de temps à la recherche de ce type d'informations pour déterminer la nature de l'événement de sécurité, ou savoir si c'en est vraiment un.

4. Les événements individuels sont dépourvus de contexte. Ils n'ont pas de liens évidents avec des événements qui se sont produits avant ou sur d'autres systèmes, et les incidents de sécurité peuvent s'étaler sur plusieurs semaines, mois, voire plus. Ils ne précisent pas le rôle de l'utilisateur, s'il s'agit de son poste de travail habituel, de son emplacement normal, si les données auxquelles il accède sont sensibles, ou s'il y a quelque chose d'inhabituel dans l'événement. Les analystes doivent souvent passer en revue des milliers d'événements pour répondre à ces questions et obtenir suffisamment de contexte pour comprendre et répondre à un incident unique.

5. La piste est souvent froide lorsque l'on en vient à se poser la question la plus importante : nos données sont-elles en sécurité ? Ceci est dû au fait que, bien souvent, les activités d'accès aux données ne sont pas capturées, conservées ou analysées.

Par exemple, de nombreuses organisations ne capturent ou ne conservent aucune information sur la façon dont les utilisateurs interagissent avec les fichiers ou e-mails – qui sont visés par de nombreuses fuites de données.

Ces difficultés aident à expliquer pourquoi les journaux bruts produisent relativement peu d'alertes significatives et pourquoi leur analyse demande des compétences et du temps. Ce document explique comment l'analyse de la sécurité peut surmonter ces obstacles pour réduire les faux positifs, accélérer les enquêtes et bloquer les attaques plus rapidement.

> La Gestion des événements et informations de sécurité (SIEM) n’est pas une collecte de journaux consistant à capturer et conserver tous les journaux de tous les appareils et applications, sans discrimination. Pourtant, elle est souvent abordée de cette façon parce que l’on s’imagine qu’il sera facile de donner du sens à toutes ces données une fois qu’elles seront dans le système SIEM. Comme on pouvait le prévoir, ce qui devait contribuer à réduire les parasites ne fait que les amplifier et en générer encore davantage. Lorsque l’on recherche une aiguille dans une botte de foin, mieux vaut ne pas augmenter le volume de la botte.[1]

Gartner

VARONIS

COLLECTE INTELLIGENTE

Collecter des journaux n'a pas l'air plus compliqué que de configurer les appareils pour qu'ils écrivent sur un serveur syslog. Mais les journaux des appareils sont très bavards et écrivent un grand nombre de lignes pour décrire un seul « événement ».

Les lignes en sont pas toujours dans le bon ordre, et ne présentent pas toutes un intérêt pour la sécurité. Parfois, les appareils écrivent dans plusieurs fichiers journaux qu'il faut alors combiner. Pour ne rien arranger, les appareils sont différents, leurs journaux sont dissemblables, et ils changent d'une version à l'autre. Chaque fournisseur consigne des informations différentes dans les journaux et utilise des formats différents pour des éléments tels que les noms d'utilisateur, noms d'hôte et domaines.

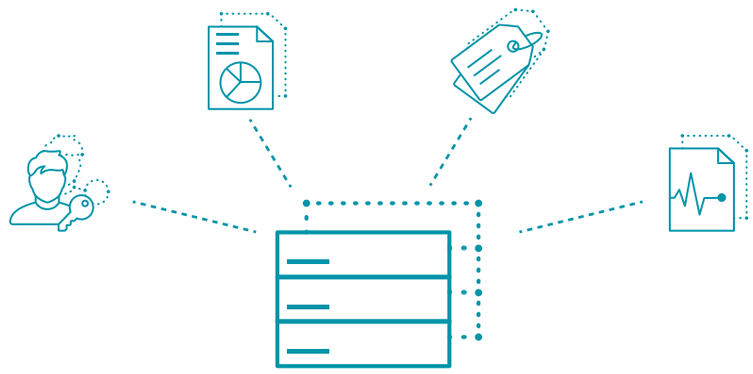
À titre d'exemple, le démarrage d'une session VPN distante sera dispersé sur 10 à 20 événements différents du journal, souvent rangés dans le désordre puisque de nombreux utilisateurs interagissent avec le système simultanément.

Voici à quoi ressemble le journal brut d'une seule connexion VPN émise par un fournisseur VPN :

```
Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Key Exchange number 1 occurred for user with NCIP 172.16.248.93

Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with ESP tran
sport mode.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Starting dsagentd session.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with SSL tran
sport mode.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: Session started for user with IPv4 address 172.16.
248.93, hostname OSHEZAF-LT

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Agent login succeeded for oshezaf/VaronisCertificate from 84.229.
120.164 with Pulse-Secure/8.3.3.1021 (Windows 10) Pulse/5.3.3.1021.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[] - Host Checker realm restrictions successfully passed for oshezaf/VaronisCertificat
e , with certificate 'CN=Ofer Shezaf, OU=Herzliya, OU=IL, OU=Users, OU=Varonis, DC=varonis, DC=com'

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[] - Primary authentication successful for oshezaf/CertificateServer from 84.229.120.1
64

Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.12
0.164] oshezaf()[] - Host Checker policy 'Varonis' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user
 'oshezaf'.

Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.12
0.164] oshezaf()[] - Host Checker policy 'Domain' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user
 'oshezaf'.
```

Si un serveur syslog se charge volontiers de collecter tous vos journaux bruts, il prend en contrepartie beaucoup de place sur le disque et exige une grande puissance de traitement pour effectuer la moindre opération, pour un résultat d'une utilité très relative. Les journaux de VPN prennent de la place, les journaux DNS et proxy encore plus.

Il est plus pertinent et efficace de mettre en place en amont quelques opérations de traitement, suppression et analyse syntaxique, en particulier si vous envoyez ces journaux à un système facturé au mégaoctet. Les solutions d'analyse de sécurité peuvent faire le tri dans les journaux bruts pour réduire la quantité de données de 70 à 80 %. Grâce à l'analyse et à la résolution de quelques journaux en amont (c'est un utilisateur qui se connecte, c'est un hôte, etc.), ces journaux sont préparés à une analyse centrale rapide. Un système de collecte intelligent qui analyse, supprime et rassemble les événements bruts de manière pertinente peut même offrir un certain niveau d'analyse et d'alerte au point de collecte. Par exemple, un système de collecte intelligent peut émettre une alerte en quasi temps-réel lorsqu'un certain utilisateur tente de se connecter à un VPN (au lieu d'attendre que les journaux bruts soient transportés et analysés par un serveur central).



> “Dans le cadre d’une étude menée par Gartner, la majorité des fournisseurs de SIEM ont déclaré que la quasi-totalité de leur base installée (environ 85 %) n’utilise pas actuellement de fonctionnalités avancées de détection ou d’analyse des menaces.[2]

Gartner

VARONIS

ENRICHISSEMENT ET ANALYSE

Imaginons que vous ayez mis en place un système intelligent de collecte, suppression et analyse pour rendre vos journaux assez exploitables. À ce stade, si vous souhaitez procéder à une analyse minutieuse, vous disposez d'une solution bien plus efficace que de simplement passer des journaux bruts au peigne fin, mais vous avez quand même du travail avant de pouvoir obtenir des connaissances proactives et significatives et de disposer d'une capacité d'analyse. Procéder à une analyse efficace exige de disposer de contexte sur les utilisateurs, les systèmes et les données.

Un utilisateur peut être un cadre disposant d'un accès aux données sensibles, un administrateur doté d'un accès à l'infrastructure principale ou une personne qui vient de démissionner. Un système peut être un serveur critique, une poste de travail ou un système de test. Les fichiers peuvent contenir des informations personnelles ou de la propriété intellectuelle. Ou il peut s'agir de photos de chats.

Sans ce contexte, il est très difficile de faire la différence entre quelque chose d'important et quelque chose de futile. L'exécution d'un outil d'administration tel qu'un analyseur réseau, ou sniffer (et générant une multitude de requêtes DNS) par un utilisateur non administrateur déclenchera probablement le verrouillage immédiat de son compte et de son poste de travail ; le même logiciel exécuté par un administrateur connu (et générant une multitude de requêtes

DNS) entraînera l'envoi d'un e-mail ou un coup de fil. Un téléchargement important vers un emplacement inhabituel doit retenir l'attention si l'utilisateur ou le poste de travail a récemment accédé à des données personnelles ou de la propriété intellectuelle critique. L'accès à des photos de ses enfants, n'est probablement pas grand-chose.

Non seulement les événements doivent être enrichis avec du contexte pour permettre un traitement efficace, mais le contexte doit être rassemblé et affiné au fil du temps. Les utilisateurs accèdent à des ensembles de données différents situés sur des systèmes différents, depuis des postes de travail différents, à des moments différents et depuis des lieux différents. C'est là que l'apprentissage automatique (machine learning) peut s'avérer réellement efficace – établir et maintenir des comportements de référence pour les interactions entre tous les utilisateurs, systèmes et données.

Un dernier point sur l'analyse de la sécurité – elle n'est performante que si elle possède une quantité suffisante de données ou métadonnées pertinentes à analyser. Si les données sont la ressource que vous souhaitez protéger le plus activement, vous devez savoir si quelqu'un a réellement pu y accéder. Si certaines de vos données critiques sont conservées dans des systèmes de fichiers ou de messagerie, c'est l'activité de ces systèmes qui est au cœur du problème – sans informations la concernant,

vous ne pouvez pas répondre à la question la plus importante de toutes concernant la sécurité : « nos données sont-elles en sécurité ? »

Malheureusement, on ne dispose bien souvent pas de journaux bruts sur l'activité des fichiers et des e-mails. Lorsque ces journaux sont disponibles, ils sont à l'état brut et volumineux, comme c'est le cas des données de télémétrie du périmètre. Si vous attachez de l'importance à la sécurité de vos données, vous aurez un important atout en main si vous disposez d'une technologie centrée sur les données apportant du contexte sur l'utilisation et la sensibilité des données (sur le plus grand nombre possible de dépôts de données clés).

RÉPONSE

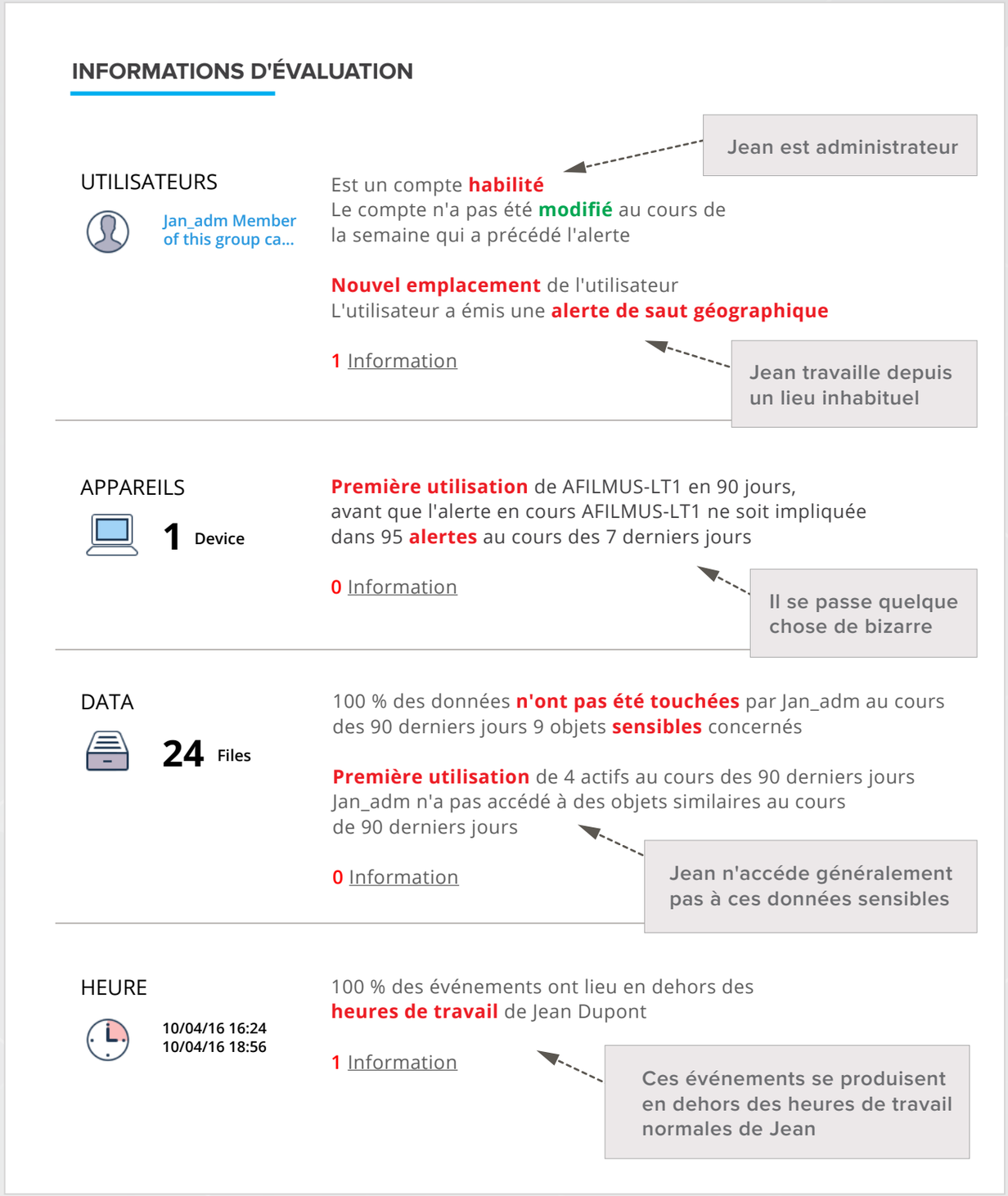
Les analystes en sécurité reçoivent une multitude d'alertes – malware détecté sur un poste de travail, compte verrouillé, échec de connexion depuis le Pôle Sud. Non seulement les événements bruts non analysés génèrent davantage d'alertes, mais chacune d'elles est bien plus longue à examiner.

Pour savoir s'il convient de répondre, ou comment, l'analyste doit établir des liens entre les événements manuellement, une tâche longue et fastidieuse.

Imaginons qu'un analyste reçoive une alerte émise par un système de détection de programmes malveillants : « fichier malveillant détecté sur 10.10.150.12. » La première étape peut consister à identifier le poste de travail, appeler son propriétaire et vérifier s'il a réellement été infecté par un malware. Si c'est le cas, il convient alors d'interroger les journaux du proxy pour identifier d'où vient le malware, si des connexions ont été établies avec des lieux inhabituels, et/ou si d'importantes quantités de données ont été envoyées. Si c'est le cas, la crainte d'un accès à des données sensibles commence à provoquer des crampes d'estomac chez l'analyste, et l'enquête se poursuit.

L’analyse de sécurité accélère considérablement ce processus. Les analystes reçoivent moins d’alertes, celles-ci ont plus de sens et sont plus faciles à analyser – en particulier si les relations et le contexte sont fournis avec l’alerte.

Pour établir une chronologie et déterminer l’ampleur de l’incident, les analystes doivent posséder des informations sur le compte de l’utilisateur, l’appareil, les données et le moment où la (ou les) alertes ont eu lieu. L’analyse de la sécurité indique si l’utilisateur accède au réseau depuis un emplacement normal (pour lui), si le compte possède des droits d’accès, si un accès à des données sensibles a eu lieu, et si l’événement s’est produit durant les horaires habituels de l’utilisateur. Ce contexte l’aide à déterminer si une alerte signale une menace réelle ou une anomalie sans importance.



Event Time	Event Type	SAM Accou	Event Statu	Blacklisted.	Country	Connection Type	Upload Siz.	Download .	Session Du	IP Address	External IP Addr.
12/05/2017 4:15 PM	VPN login request		✔			Unkonwn					192.168.200.89
12/05/2017 4:15 PM	VPN login request		✔			Tunneling				172.16.212.150	192.168.200.89
12/05/2017 4:18 PM	VPN logout request		✔			Tunneling	265349	41638	158	172.16.212.150	192.168.200.89
12/07/2017 9:48 AM	VPN login request	dpnini	✔	–	Israel	AccessApplica...					89.139.198.93
12/07/2017 10:02 AM	VPN logout request	dpnini	✔	–	Israel	Unkonwn					89.139.198.93

Si, sur la base des informations apportées par ce contexte, l'analyste décide d'agir, il disposera d'événements propres liés à l'incident.

CONCLUSION

Une analyse de la sécurité combinant collecte intelligente de métadonnées pertinentes, analyse syntaxique et enrichissement basé sur l'apprentissage automatique réduit le nombre d'alertes reçues ainsi que le temps nécessaire pour percer leur mystère. Des alertes moins nombreuses et plus riches de sens multiplient les chances d'identifier les incidents de sécurité réels, et l'on sait combien chaque seconde compte en matière de cyber sécurité.

Un utilisateur figurant sur une liste de surveillance et envoyant des données sensibles sur un site Web immédiatement après y avoir accédé en dehors de ses heures de travail sera en tête des cas suspects à traiter, tout comme l'administrateur qui lit les e-mails du PDG et les marque comme « non lus » sur le VPN depuis un pays chaud et ensoleillé. Un compte censé exécuter votre base de données déclenchera une alerte s'il commence soudainement à accéder aux données de patients, contrairement à un utilisateur qui actualise des douzaines de fichiers à la fin du mois durant ses horaires de travail habituels, depuis son poste de travail normal, pour la bonne raison que cela fait partie de son travail.

Que vous envisagiez de consolider vos journaux ou de mettre en place un projet de SIEM, ou si vous avez le sentiment que votre solution est trop lente ou pas suffisamment intelligente, essayez d'utiliser une solution d'analyse de la sécurité. Outre le fait qu'elle augmentera vos chances d'isoler les événements de sécurité importants, une solution efficace d'analyse de la sécurité vous aidera à passer moins de temps à enquêter, à réduire vos dépenses de traitement et l'espace de stockage consommé (et les coûts associés), et à satisfaire plus facilement vos besoins de conformité.

À PROPOS DE VARONIS

Varonis est un pionnier de la sécurité et de l'analyse des données, et mène un autre combat que les entreprises de cybersécurité classiques. Varonis protège les données d'entreprise conservées sur site et dans le cloud : fichiers sensibles et e-mails ; données confidentielles sur les clients, patients et employés ; dossiers financiers ; plans stratégiques et produit ; et autre propriété intellectuelle.

La plate-forme de sécurité des données Varonis détecte les menaces internes et les cyberattaques en analysant les données, l'activité des comptes et le comportement des utilisateurs. Il prévient et limite les catastrophes en verrouillant les données sensibles et obsolètes et maintient un état sécurisé grâce à l'automatisation.

Axé sur la sécurité des données, Varonis répond aux besoins de différents cas d'utilisation tels que gouvernance, conformité, classification et analyse des menaces. Fondé en 2005, Varonis comptait déjà quelque 6 250 clients dans le monde au 31 décembre 2017 — parmi eux figurent des leaders de nombreux secteurs : technologie, grande consommation, vente au détail, services financiers, santé, fabrication, énergie, médias et éducation.

Démo en direct

Installez Varonis dans votre propre environnement. Rapide et simple

info.varonis.com/trial-fr

Évaluation des risques des données

Obtenez un instantané de la sécurité de vos données, réduisez votre profil de risque et corrigez vos véritables problèmes de sécurité.

info.varonis.com/express-assessment-fr

[1] Gartner, Using SIEM for Targeted Attack Detection, Oliver Rochford & Kelly M. Kavanagh, 12 March 2014
[2] Gartner, Summer of SIEM 2017 Coming..., Anton Chuvakin, 11 July 2017

À PROPOS DE DATALERT

DatAlert analyse automatiquement les informations recueillies par notre Plate-forme de sécurité des données afin de détecter, signaler et remédier en quasi temps réel aux menaces qui visent vos données.

Avec DatAlert, vous êtes averti lorsqu'un événement exige une intervention urgente – comme lorsque quelqu'un accède à, ou chiffre plusieurs fichiers sensibles, lit les e-mails d'un dirigeant ou apporte des modifications à la politique de groupe en dehors des heures normales de contrôle des modifications.

EN SAVOIR PLUS

> "Varonis est une solution fantastique

Gartner peerinsights™

★★★★★

VARONIS

À PROPOS DE VARONIS EDGE

Varonis Edge analyse les appareils situés sur le périmètre, notamment le DNS, le VPN et les proxies Web, pour établir des liens entre les événements en périphérie et détecter les programmes malveillants, intrusions APT et exfiltrations.

DatAlert et Edge détectent toute activité suspecte et empêchent les fuites de données sur les plates-formes, visualisent les risques et définissent des priorités dans les enquêtes.

EN SAVOIR PLUS

Des milliers de grandes entreprises mondiales font confiance à Varonis pour gérer et protéger leurs données

NASA ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL

VARONIS