LIVRE BLANC

Protection optimisée des informations et visibilité maximale grâce à la fonction Security Intelligence en temps réel

Simplifiez-vous la gestion des logs et obtenez les informations exploitables dont vous avez besoin pour renforcer la sécurité de votre entreprise

Les nouvelles technologies d'infrastructure informatique (virtualisation, informatique en nuage [cloud computing] et mobilité, notamment) bouleversent la façon dont les utilisateurs interagissent entre eux et avec les informations, ce qui amène les entreprises à adopter de nouvelles méthodes de travail. De plus en plus interconnectée et distribuée, l'entreprise gagne en agilité. Cependant, les spécialistes de la sécurité des informations font face à de nouvelles difficultés, tant en matière de garantie de la sécurité qu'en ce qui concerne la surveillance des contrôles de stratégie.

Face aux exigences de conformité qui lui sont imposées, votre entreprise a très certainement déployé un outil permettant de recueillir et de gérer les journaux. Mais êtes-vous sûr qu'il vous informe sur les événements de sécurité et qu'il les analyse en temps réel ? Existe-t-il un moyen d'y voir plus clair dans la masse de données de sécurité ainsi générée afin d'être en mesure de contrôler vos stratégies en permanence et de lutter contre des menaces sans cesse plus élaborées ?

Il se peut même que votre outil de gestion des logs ne réponde plus tout à fait aux besoins de votre entreprise en termes de conformité : les directives évoluent et, dans bien des cas, le recueil des journaux ne suffit pas. Pour réduire vos risques d'échouer aux audits, vous devez pouvoir présenter des rapports qui vous aident non seulement à passer en revue les anomalies, mais aussi à prouver votre démarche à des auditeurs toujours plus soupçonneux.

NetIQ

NetIQ | LIVRE BLANC

Table des matières

Surveillance de l’activité des utilisateurs

Dans son Rapport d’enquête 2011 sur les violations de données, Verizon indique que 86 % des organisations qui ont été victimes d’une violation de données en ont été informées par un tiers (une agence fédérale chargée de l’application de la loi, en général). Dans 70 % des cas, il existait des indices, dans les fichiers journaux de l’entreprise, qui auraient pu signaler la violation, mais qui sont passés inaperçus. Cela montre bien que les entreprises peinent à analyser correctement les informations recueillies dans un délai suffisant, et ce, bien que les données collectées soient adéquates.

En matière de gestion des événements et de création de rapports de sécurité, les personnes représentent souvent un risque, surtout si les processus sont majoritairement manuels. Lorsque l’identification des événements liés à la sécurité s’appuie sur une inspection manuelle des journaux, l’opération prend beaucoup de temps et, souvent, elle ne permet pas d’obtenir le niveau de Security Intelligence (gestion intelligente des données de sécurité) pour réagir adéquatement.

Plus il faut de temps pour trouver une violation, plus les pirates ont de temps pour exploiter une brèche. Même quand vous trouvez des drapeaux rouges, êtes-vous en mesure de localiser leur origine ou d’identifier les personnes qui compromettent ainsi la sécurité de votre entreprise ? Et parvenez-vous à opérer assez rapidement pour identifier les problèmes en temps réel, dès qu’ils se produisent ?

Dans un contexte où les équipes sont surexploitées, tandis que les budgets stagnent ou même diminuent, votre organisation doit optimiser ses ressources en travaillant plus efficacement. L’automatisation de la gestion des événements et de la création de rapports de sécurité doit englober un maximum d’aspects (surveillance, corrélation et même traitement des anomalies, par exemple), afin d’assurer une détection et une résolution plus rapides des anomalies, et de libérer les membres de votre équipe qui pourront ainsi consacrer plus de temps et d’efforts à l’étude de questions vraiment importantes.

De plus, si vous pouvez lier la gestion des événements et les informations de sécurité aux fonctionnalités de surveillance des activités des utilisateurs, vous serez en mesure d’associer les utilisateurs à des actions spécifiques sur l’ensemble de vos systèmes, ce qui simplifiera la mise en conformité. Par ailleurs, les informations seront fournies sous une forme aussi visuelle que possible afin de permettre à tous (spécialistes et non-spécialistes) de les interpréter.

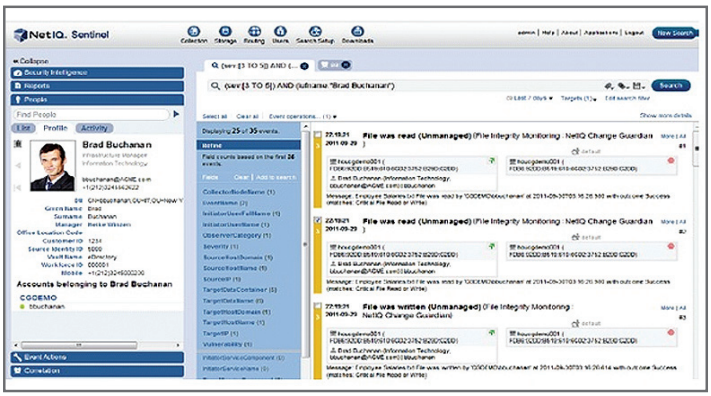

Figure 1. *La surveillance de l’activité des utilisateurs permet d’associer les utilisateurs à des activités spécifiques sur l’ensemble des systèmes.*

Une solution facile à déployer, flexible et évolutive

Aujourd’hui, vous avez le choix entre de multiples outils de gestion des logs, un certain nombre d’entre eux étant même téléchargeables gratuitement. Toutefois, si votre outil ne fait que gérer les journaux et que vous cherchez à protéger votre entreprise, vous devez installer d’autres outils ou logiciels assurant les fonctionnalités de sécurité qui vous manquent. Malheureusement, la mise en oeuvre et l’intégration peuvent s’avérer complexes, et les activités de l’entreprise peuvent être interrompues au cours du processus.

Si l’outil utilisé est statique ou peu flexible, il risque de ne pas s’adapter à vos nouveaux besoins, en cas de changement au niveau des technologies exploitées ou du modèle de fonctionnement. De même, il peut être incapable de traiter les nouveaux types de violations et menaces potentielles, ou les difficultés liées à la gestion et aux accès des utilisateurs privilégiés.

L’idéal serait de mettre en oeuvre une solution qui assurerait la gestion des logs d’une part, et proposerait également des fonctionnalités SIEM (Security Information and Event Management - gestion des événements et informations de sécurité), qui assureraient la visibilité des systèmes de votre entreprise et fourniraient des renseignements en temps réel sur ces systèmes, afin de minimiser les menaces de sécurité, d’améliorer les opérations et d’appliquer les contrôles de stratégies.

Création de rapports pour tous les publics

Il est essentiel de créer différents rapports adaptés aux diverses parties de l’entreprise, afin de garantir une parfaite compréhension des risques et menaces, et pour répondre aux critères d’audit et de conformité. Avec un simple outil de gestion des logs, la création de rapports peut s’avérer complexe. Le processus consistant à recueillir les données, les exporter vers une application telle que Microsoft Excel pour les exploiter, puis présenter les informations dans un format de visualisation via une application telle que Microsoft PowerPoint, prend beaucoup de temps et comporte d’importants risques d’erreurs.

Avec un outil plus sophistiqué, en revanche, les rapports sont créés rapidement (en quelques secondes dans certains cas) grâce à des modèles prédéfinis qui assurent un format graphique riche. Vous pouvez inclure la hiérarchie d’informations de votre choix, en fonction du public, par exemple : informations de synthèse de haut niveau pour les CRO (responsables des

risques) et les CSO (responsables de la sécurité), avec la possibilité d'explorer la hiérarchie afin d'obtenir plus de détails et de preuves concernant des événements identifiés, ainsi que des données historiques et comparatives si nécessaire.

Ainsi, vous gagnerez du temps, les risques d'erreur diminueront et vous serez en mesure de présenter les informations dans un format accessible à votre public. De plus, en signalant le temps gagné et les économies réalisées grâce aux puissantes fonctionnalités de création de rapports et de recherche dynamique de l'outil, vous pourrez rapidement démontrer le retour sur investissement réalisé en passant des déploiements de gestion manuelle ou tactique des logs à la nouvelle méthode.

Détection efficace des anomalies

Il s'avère souvent difficile d'identifier les événements signalant des problèmes réels ou potentiels, et qui doivent être étudiés de plus près. Certaines anomalies ne correspondent pas à une menace ou violation de sécurité potentielle. Par exemple, si un pic de logins dépasse largement le nombre normal de logins pendant une après-midi spécifique, il est possible que cette anomalie s'explique facilement à l'aide des cycles d'opérations connus et des autres systèmes. Par exemple, le pic peut s'expliquer par le fait que des partenaires accèdent à une application de suivi des ventes pour réaliser des opérations qu'ils n'effectuent que le dernier jour de chaque trimestre.

Une vue à une dimension affichant l'écart par rapport à une ligne de base ne garantirait pas la gestion intelligente des données de sécurité ni l'identification des vrais problèmes. Il vous faut un outil qui rassemble les événements et détecte automatiquement les anomalies de l'environnement, sans que vous ayez à créer des règles de corrélation présupposant que vous savez déjà exactement ce que vous cherchez.

L'outil choisi doit permettre d'analyser les anomalies depuis à peu près toutes les perspectives possibles, et vous offrir la possibilité d'étudier une anomalie spécifique en fonction de toute combinaison d'attributs et de fenêtres de temps. Ainsi, vous disposerez de la flexibilité et du contrôle dont vous avez besoin pour rechercher les tendances d'événements et les relations de cause à effet qui pourraient signaler une anomalie, et vous déterminerez facilement la nature exacte de la menace.

Par exemple, vous pourriez repérer la séquence suivante : un administrateur crée un compte d'utilisateur privilégié qui est utilisé immédiatement pour accéder à un serveur particulier et y récupérer des informations pour les copier sur un périphérique de stockage externe. Une fois l'utilisateur délogué, le compte est rapidement supprimé et les journaux pertinents sont supprimés du serveur de fichiers. Avec une telle gestion intelligente des données de sécurité, vous êtes mieux informé : il vous suffit de regarder la tendance pour voir qu'elle pointe vers une anomalie. Vous détectez donc celle-ci plus rapidement et plus facilement, sans avoir à corréler manuellement des séries d'événements, et vous pouvez vous mettre à enquêter sans attendre.

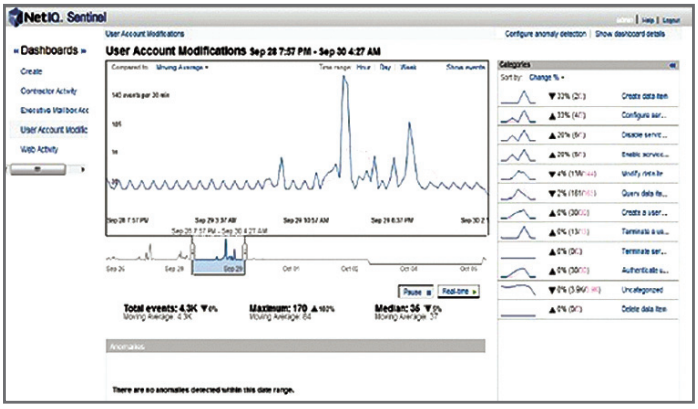

Figure 2. *Des renseignements exploitables à portée de main en temps réel grâce à un tableau de bord de sécurité.*

L'idéal serait que l'outil propose les deux méthodes d'analyse des anomalies (visuelle et automatique). Une méthode visuelle, telle qu'un tableau de bord, vous aide à analyser les lignes de base et les tendances en surveillant les pics et les creux d'activité et en les comparant au modèle de comportement normal. Si vous pouvez afficher à la fois des données historiques et en temps réel, vous serez en mesure de bénéficier d'une gestion intelligente des données encore plus poussée, qu'il s'agisse de recréer l'état historique du système au moment de l'anomalie, ou de connaître l'évolution de vos niveaux de sécurité et de conformité.

Si l'analyse visuelle est déjà efficace en soi, une fonctionnalité supplémentaire de détection automatique des anomalies la renforce en permettant d'identifier les écarts par le biais d'une analyse à la fois plus souple, plus étendue et plus détaillée.

En cas de détection d'un événement qui s'écarte des activités normales, l'outil génère une alerte en temps réel pour inviter un spécialiste de la sécurité à s'en charger immédiatement. Selon l'outil, vous pourrez peut-être configurer le lancement automatique d'un processus de traitement aligné sur vos processus internes (désactivation d'un compte utilisateur, par exemple).

Comment NetIQ peut-il vous aider ?

NetIQ comprend que les entreprises ont besoin de bénéficier d'une gestion intelligente des données de sécurité en temps réel afin de renforcer leur sécurité globale et de prendre des décisions avisées, ainsi que les problèmes que cela pose.

Les solutions SIEM traditionnelles proposant des fonctions avancées s'avèrent souvent très complexes. Pour que les clients tirent pleinement profit des technologies SIEM, il leur faut des solutions simples à utiliser et à déployer, qui s'adaptent rapidement à leurs environnements en changement perpétuel et qui fournissent des renseignements corrects et exploitables (les informations appropriées fournies aux parties prenantes qui en ont besoin, en temps voulu) pour faciliter l'identification et la diminution des menaces de sécurité.

NetIQ® Sentinel™ 7 est doté de fonctionnalités SIEM complètes qui simplifient les processus par rapport aux autres outils SIEM et maximisent la capacité de l'équipe de sécurité informatique à adapter la solution SIEM aux besoins de l'entreprise.

NetIQ Sentinel 7 est un produit unifié qui regroupe des fonctionnalités SIEM et de gestion des logs. Vous bénéficiez d'une visibilité en temps réel sur l'intégralité de vos activités informatiques, ce qui vous permet de réduire les menaces de sécurité, d'améliorer les opérations de sécurité et d'appliquer automatiquement des contrôles de stratégie à travers les environnements physiques, virtuels et en nuage.

Grâce à sa combinaison de renseignements en temps réel, de détection d'anomalies et de fonctionnalités de surveillance de l'activité des utilisateurs qui permettent de mettre en place un mécanisme d'avertissement prédictif et d'évaluer précisément les activités informatiques, NetIQ Sentinel est un outil SIEM d'une efficacité sans précédent. Comme le système est moins complexe à déployer et à utiliser que la plupart des systèmes SIEM traditionnels, toutes les entreprises peuvent désormais bénéficier de la gestion intelligente des données de sécurité.

De plus, NetIQ Sentinel assure une intégration transparente avec la gestion des identités, de manière à associer les utilisateurs à des activités spécifiques sur l'ensemble des environnements. Cela facilite l'identification des risques critiques, écourte sensiblement les temps de réaction et permet de traiter rapidement les menaces et violations de sécurité, avant qu'elles n'affectent les activités de l'entreprise.

Conclusion

Avec NetIQ Sentinel, solution SIEM et de gestion des logs à la fois simple et puissante, vous disposerez de la gestion intelligente des données de sécurité dont vous avez besoin pour respecter les exigences de conformité et renforcer la protection de vos activités. Vous serez en mesure d'optimiser le temps et les ressources à votre disposition, grâce à des processus automatisés qui libèreront le personnel des tâches manuelles pour lui permettre de se concentrer sur des points réellement importants. Vous proposerez également des rapports graphiques qui aideront le personnel interne à se faire une idée claire de la sécurité de l'organisation et à se fier aux activités de l'équipe.

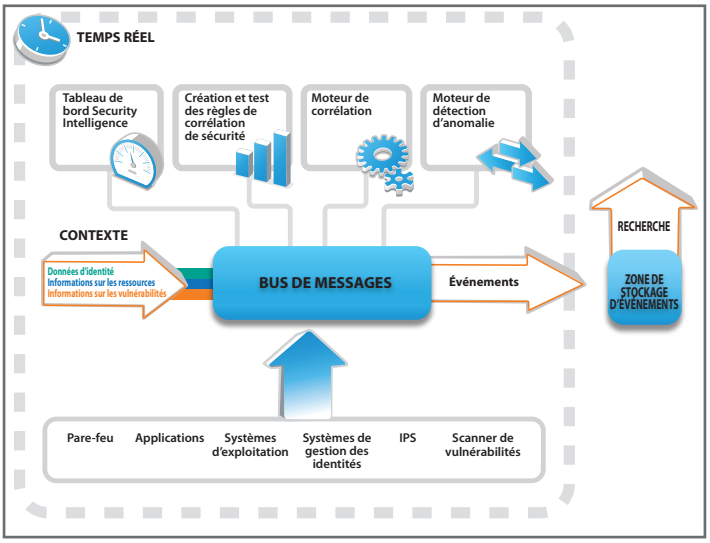

Figure 3. *Grâce aux composants d'architecture de NetIQ Sentinel, les entreprises disposent des renseignements et de la visibilité en temps réel dont elles ont besoin quant aux événements informatiques.*

À propos de NetIQ

NetIQ est un fournisseur international de logiciels informatiques d'entreprise dont les efforts sont constamment axés sur la réussite de ses clients. NetIQ comble, à moindres frais, les besoins de ses clients et partenaires en matière de protection des informations. De plus, notre société gère les aspects complexes des environnements d'applications dynamiques hautement distribués.

Notre portefeuille comprend des solutions automatisées et évolutives, spécialisées dans la gestion des identités, de la sécurité et de la gouvernance, ainsi que des opérations informatiques. Les entreprises sont ainsi en mesure de fournir, mesurer et gérer en toute sécurité des services informatiques à l'échelle de leurs environnements physiques, virtuels et en nuage (cloud computing). Associées à notre approche pratique et orientée client de la résolution des problèmes informatiques récurrents, ces solutions aident les entreprises à réduire les coûts, la complexité et les risques.

Pour en savoir plus sur nos solutions logicielles reconnues par les professionnels du secteur, visitez le site **www.netiq.com**.

562-FR1009-001 DS 07/12

France

Tour Franklin
100/101, Quartier Boieldieu
92042 Paris la Défense Cedex
France
Tel: +01 55 62 50 00
Fax: +01 55 62 51 99

Email : contact-fr@netiq.com
info@netiq.com
www.netiq.com
http://community.netiq.com

Pour obtenir la liste complète de nos bureaux d'Amérique du Nord, d'Europe, du Moyen-Orient, d'Afrique, d'Asie-Pacifique et d'Amérique latine, visitez la page : **www.netiq.com/contacts**.

Suivez-nous :