RSA NETWITNESS® LOGS

CONFORMITÉ ET CRÉATION DE RAPPORTS

- *Les rapports de conformité comprennent la création/suppression/modification de compte, les accès administrateur aux systèmes de conformité, les accès utilisateur aux systèmes de conformité, les privilèges d'escalade, les mises à jour du firmware, les modifications de configuration, la réussite de l'accès distant, etc.*

- *Les réglementations comportant des rapports spécifiques comprennent, pour plus de commodité :*
  - *Bâle II*
  - *Bill 198*
  - *FERPA (Family Educational Rights and Privacy Act)*
  - *FFIEC (Federal Financial Institutions Examination Council)*
  - *FISMA (Federal Information Security Management Act)*
  - *GLBA (Gramm-Leach-Bliley Act)*
  - *GPG13 (Good Practice Guide 13)*
  - *HIPAA (Health Insurance Portability and Accountability Act) de 1996*
  - *ISO 27002 (International Organization for Standardization 27002)*
  - *NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)*

- *NISPOM (National Industrial Security Program Operating Manual)*
  - *PCI (Payment Card Industry)*
  - *Loi Sarbanes-Oxley Act (SOX) de 2002*
  - *SSAE (Statement on Standards for Attestation Engagements 16)*

RSA NetWitness® Logs est un outil de surveillance de la sécurité et de recherche approfondie qui recueille, analyse, signale et stocke les données des fichiers log à partir de diverses sources afin de prendre en charge la conformité aux politiques de sécurité et les initiatives de conformité aux normes. La solution, modulaire et évolutive, peut être déployée dans n'importe quel type d'entreprise. Contrairement à d'autres approches SIEM basées sur les journaux, RSA NetWitness Logs analyse, enrichit et indexe les journaux au moment de la capture, créant ainsi des métadonnées de session qui permettent d'accélérer considérablement les alertes et les analyses.

RSA NetWitness Logs prend en charge la collecte sur un large éventail de protocoles, notamment Syslog, ODBC, SFTP, SCP, FTPS, SNMP, Check Point LEA, WinRM et bien plus encore. Il intègre les journaux de plus de 350 sources d'événements, notamment divers périphériques de sécurité et de réseau leaders sur le marché, des applications et des systèmes d'exploitation courants. En outre, il stocke des journaux bruts et extrait des métadonnées. La possibilité de surveiller les journaux de manière centralisée, quelle que soit leur source, et de déployer des composants de collecte sur site, virtuellement, sur des architectures hybrides ou dans des Clouds publics tels que Amazon Web Services (AWS) et Microsoft Azure, et des applications telles que Microsoft Office 365 et Salesforce, fait de RSA NetWitness Logs une solution polyvalente. La visibilité généralisée des journaux facilite l'administration et l'analyse des données dans les environnements distribués et virtuels, ce qui permet la détection, l'investigation, la création de rapports et la gestion de toutes les données des fichiers log en peu de temps.

CONFORMITÉ

La solution RSA NetWitness Logs inclut des cas d'utilisation de la conformité et des modèles préconçus pour SOX, PCI, HIPAA NERC et bien d'autres réglementations.

CRÉATION DE RAPPORTS

RSA NetWitness Logs vous offre la possibilité de personnaliser l'affichage et la mise en forme des rapports. Les rapports prédéfinis comprennent une ou plusieurs règles que vous pouvez également utiliser dans d'autres rapports personnalisés.

AUTOMATISATION DE LA DÉCOUVERTE DES JOURNAUX

Si vous êtes en sous-effectif ou surchargé de travail, avec des environnements hétérogènes en constante évolution, le flux de travail de découverte de RSA NetWitness Logs permet de relever ces défis. Contrairement aux autres collecteurs de journaux nécessitant une configuration manuelle, RSA NetWitness Logs dispose d'une analyse heuristique automatisée pour aider les équipes de sécurité à ingérer rapidement de nouvelles sources. La nouvelle technologie d'analyse dynamique restitue automatiquement les données brutes à partir de la plupart des sources de journaux et fournit un accès immédiat aux données de sécurité critiques sous la forme de métadonnées utiles. L'analyse automatique des nouvelles sources de journaux aide les organisations à s'adapter à la variété toujours plus grande de sources de journaux.

Les sources de journaux qui ne disposent pas d'un analyseur correspondant sont traitées automatiquement en fonction des règles. Les métadonnées sont extraites automatiquement en fonction des règles, et les métadonnées sont disponibles pour l'enrichissement, l'investigation, la création de rapports et les alertes provenant de nouvelles sources. L'automatisation de l'analyse des journaux permet une visibilité immédiate des journaux à partir de sources nouvelles, personnalisées ou non prises en charge.

Pour les journaux plus exigeants, l'outil RSA NetWitness Log Parser permet aux utilisateurs de créer facilement des analyseurs pour les nouvelles sources d'événements, non prises en charge ou personnalisées. Une prise en charge supplémentaire de l'analyse des journaux personnalisés est également disponible via la communauté RSA Link.

RAPIDITÉ ET POLYVALENCE

RSA NetWitness Logs permet de configurer et de gérer de manière sélective la conservation des données brutes et des métadonnées. La rétention à court terme offre un accès extrêmement rapide aux données. La rétention à plus long terme apporte un équilibre entre les besoins en stockage rentable et l'accès indexé à des fins de conformité.

ANALYTIQUE DU COMPORTEMENT DES UTILISATEURS ET DES ENTITÉS

RSA NetWitness UEBA Essentials prolonge l'étendue de l'analytique à l'identification des menaces avancées. RSA NetWitness UEBA Essentials est disponible via RSA Live à tous les clients RSA NetWitness Platform. La solution reflète une dimension des fonctionnalités analytiques qui permettent à nos clients d'identifier rapidement les menaces connues et inconnues d'aujourd'hui.

GESTION FLEXIBLE DE LA BANDE PASSANTE

Pour gérer les problèmes de bande passante, les administrateurs peuvent contrôler les éléments extraits et agrégés à partir de bureaux satellites vers les sites centralisés. RSA NetWitness Logs propose des options permettant de limiter les protocoles d'extraction avec des limites prédéfinies en termes de quantité et de types de journaux collectés. Cela comprend la compression et le chiffrement des données des fichiers log qui sont traitées et agrégées entre différents composants de l'architecture.

VISIBILITÉ SUR LES CLOUDS

Vous pouvez déployer RSA NetWitness Logs dans des architectures de cloud privé, public ou hybride. En outre, vous pouvez facilement surveiller les environnements Office 365 ou les applications Salesforce. Les composants modulaires peuvent être déployés virtuellement et au sein de clouds publics, notamment AWS et Amazon, pour permettre une meilleure visibilité sur les environnements Cloud complexes.

VISIBILITÉ SUR LES POINTS DE TERMINAISON

RSA NetWitness Endpoint Insights propose des analyses d'inventaire des points de terminaison essentiels, associées aux fonctionnalités de transfert et de filtrage des journaux Microsoft Windows, afin de réduire les coûts et la complexité liés à l'investigation des menaces. RSA NetWitness Endpoint Insights est un agent spécialement conçu pour apporter de la visibilité sur les configurations hôte, les détails du processus et le contexte de l'utilisateur, tout en simplifiant la surveillance des journaux Windows.

L'ÉVOLUTION PAR-DELÀ LES JOURNAUX

Étendez les fonctionnalités de détection des menaces au-delà des simples journaux avec RSA NetWitness Platform. RSA NetWitness Logs s'intègrent en toute transparence avec d'autres composants modulaires de RSA NetWitness Logs, notamment RSA NetWitness Network, RSA NetWitness Endpoint et RSA NetWitness Orchestrator. Cette intégration étroite et la plate-forme unifiée étendent votre visibilité et créent des métadonnées corrélées grâce à la puissance d'une approche SIEM avancée au sein de votre réseau. Vous bénéficiez d'une visibilité sur les journaux, les paquets, NetFlow et les points de terminaison pour une détection et une réponse plus rapides.

09/20 Fiche produit H16876-1 W386667.