Agent VitalSigns SIEM ™ pour z/OS VSA

Événements de sécurité mainframe en temps réel transmis à n'importe quel SIEM d'entreprise

Lorsque la sécurité des données est en jeu, il est impératif d'identifier rapidement les problèmes et les menaces afin d'atténuer les risques. VitalSigns SIEM Agent pour z/OS (VSA) place le mainframe au centre de l'infrastructure de sécurité de votre entreprise afin de filtrer le bruit et de détecter les événements critiques en temps réel.

VSA s'intègre aux fonctionnalités de sécurité z/OS standard (RACF, ACF2 et Top Secret) afin de recueillir des informations détaillées sur les événements de sécurité du mainframe à partir de tous les systèmes z/OS et LPAR de votre réseau.

Des filtres avancés et granulaires séparent rapidement et facilement les incidents critiques des problèmes quotidiens, et les envoient dans le format approprié à votre SIEM d'entreprise.

Le traitement des événements est entièrement compatible zIIP sans configuration supplémentaire. Lors de tests de référence, l'agent VSA a atteint une compatibilité zIIP globale supérieure à 99 % lors du traitement des enregistrements SMF seuls, et jusqu'à 60 % lors du traitement des messages de console seuls.

Améliorations significatives en matière de sécurité

VSA acquiert les messages en temps réel à partir de la console système z/OS, du système de gestion SMF (System Management Facility) et du système de gestion de l'information IMS (Information Management System). Un dictionnaire de données complet vous offre un contrôle sans précédent pour définir les données significatives et créer des filtres.

L'agent utilise les filtres définis pour détecter les événements importants, puis reformate les données sous forme d'événements syslog, CEF ou LEEF et les transmet à un ou deux SIEM d'entreprise. Le SIEM interprète les données, puis les transmet aux personnes et aux systèmes responsables de la sécurité de l'entreprise. L'équipe de sécurité dispose d'une vue centrale de tous les événements qu'elle doit reconnaître.

Conformité et audit simplifiés

La surveillance des événements de sécurité à l'échelle de l'entreprise est essentielle, non seulement pour suivre les activités malveillantes, mais aussi pour respecter les normes de conformité exigeantes d'aujourd'hui. Les administrateurs peuvent définir des éléments spécifiques pour des niveaux supplémentaires de surveillance ou d'audit : les fichiers contenant des informations de crédit, par exemple, ou des détails sur les soins de santé. Les équipes mainframe peuvent compter sur VSA pour filtrer et formater les données appropriées afin de se conformer à des politiques d'audit strictes.

Grâce à une surveillance continue, des alertes en temps réel et des processus d'audit simplifiés, VSA aide à respecter les réglementations en matière de sécurité des données, notamment le RGPD, la loi SOX, la loi FISMA, la norme 23 NYCRR 500, la norme PCI DSS, la loi HIPAA, la loi GLBA et la publication 1075 de l'IRS.

VSA comble une lacune importante dans votre infrastructure de sécurité en transmettant en temps réel les enregistrements d'événements z/OS à votre solution SIEM.

À l'aide de filtres puissants et granulaires pour les enregistrements SMF et IMS, VSA détecte les événements critiques, puis envoie des alertes en temps réel à n'importe quel SIEM distribué, tel que :

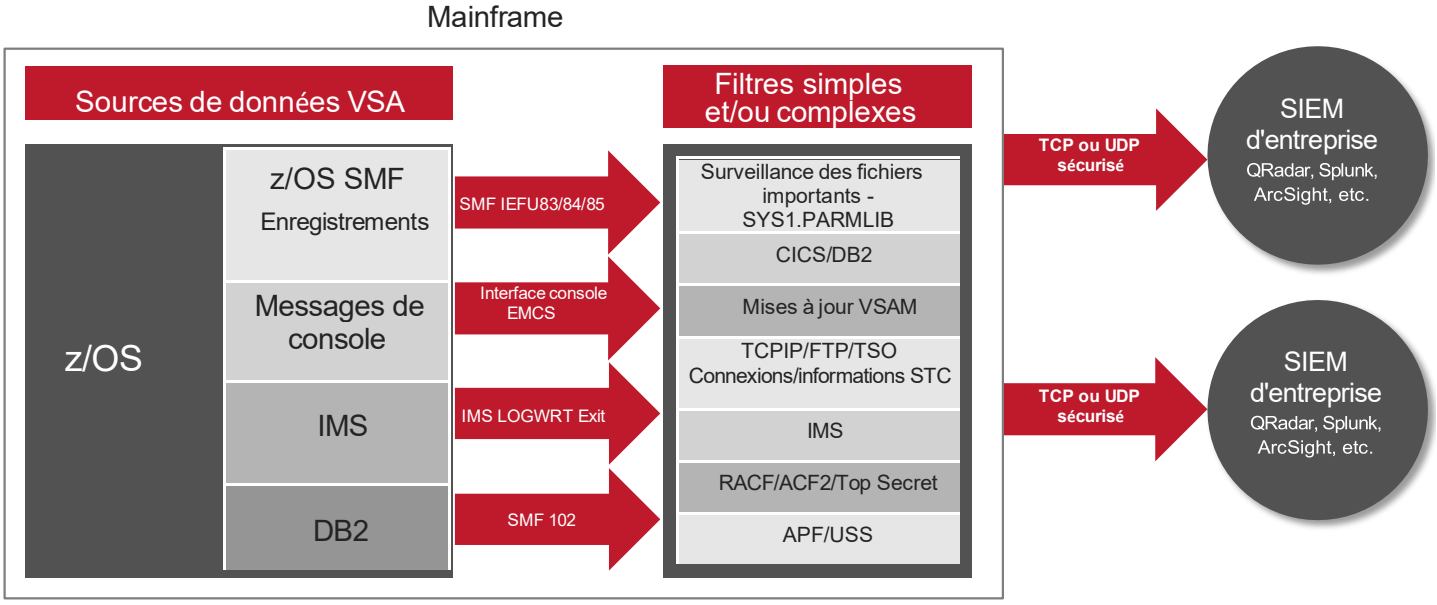
- Splunk
- LogRhythm
- QRadar
- AlienVault
- ArcSight
- et bien d'autres

Des exemples de tableaux de bord peuvent être importés dans Splunk pour afficher les événements de sécurité, l'activité LPAR et les échecs d'accès à partir de l'agent VSA sur z/OS.

Avec VSA, vous bénéficiez d'une visibilité qui vous permet de rechercher et de suivre des événements de sécurité ciblés et définis sur le mainframe.

VitalSigns SIEM Agent™ pour z/OS a été désigné comme un **produit novateur** pour la gestion des données et des informations par le magazine Database Trends and Applications.

Découvrez comment VSA peut améliorer la sécurité de votre entreprise.



La sécurité implique de surveiller toutes les portes

Les agents logiciels VSA convertissent les données du mainframe en événements syslog, CEF ou LEEF afin de les transmettre aux technologies SIEM ou à tout autre logiciel utilisant le protocole TCP/IP.

Les SIEM d'entreprise consolident les informations VSA avec les renseignements de sécurité provenant d'autres systèmes tels que UNIX, Windows et Cisco. Les SIEM peuvent ensuite analyser et visualiser les données sur l'ensemble du spectre.

Vous n'avez plus besoin de plusieurs équipes de sécurité pour protéger plusieurs plateformes. Vous bénéficiez d'une visibilité totale sur l'environnement z/OS, ainsi que sur les environnements de systèmes distribués et ouverts.

Pour plus d'informations sur VitalSigns SIEM Agent for z/OS, rendez-vous sur www.sdsusa.com/siem/

Laissez VSA travailler pour vous

- Interfaces avec les produits de sécurité z/OS standard : RACF, ACF2, Top Secret.
- Surveille z/OS, UNIX System Services (USS) et DB2.
- Collecte et surveille les enregistrements SMF, les enregistrements de journaux IMS et les enregistrements de données de performances CICS.
- Les API permettent de définir et de filtrer les événements TSO, CICS et batch.
- Formate les données du mainframe au format syslog, CEF ou LEEF.
- S'installe facilement et rapidement avec un minimum de ressources et sans IPL z/OS.
- Les règles de surveillance simples ou complexes sont facilement définies à l'aide d'ISPF Edit.
- Utilise à la fois la détection d'attaques basée sur les signatures et celle basée sur les anomalies.
- La configuration peut être partagée par les agents VSA s'exécutant sur différents LPAR.
- Faible encombrement dans chaque LPAR et faible charge CPU.

Logiciels mainframe de qualité depuis 1982

Software Diversified Services fournit des logiciels mainframe et distribués complets et abordables, axés sur la cybersécurité et la conformité. Des centaines d'organisations à travers le monde, dont de nombreuses entreprises du classement Fortune 500, font confiance aux logiciels SDS. Nos équipes d'experts en développement et notre assistance technique primée sont basées à Minneapolis, dans le Minnesota. Pour en savoir plus, rendez-vous sur notre site Web.