ASICS automatise la gestion et la résolution des incidents grâce à l'analyse des logs en temps réel

Résumé

ASICS, une société multinationale japonaise issue de la fusion d'Onitsuka, de GTO et de Jelenk, propose une gamme complète de fournitures et de matériel de sport visant à créer un style de vie de qualité grâce à des technologies sportives intelligentes. Pour lutter contre les cybermenaces et traiter les incidents au moment même où ils surviennent, ASICS avait besoin d'une plateforme centrale pour gérer, corréler et analyser les logs générés à partir de plusieurs systèmes. Depuis le déploiement de Splunk® Enterprise, la société a constaté plusieurs avantages, notamment :

- Une visibilité en temps réel des incidents et des menaces grâce à l'analyse automatisée des logs ;
- Un renforcement de la responsabilité sociale grâce à l'amélioration de la sécurité et de la visibilité ;
- Une augmentation de l'efficacité et de la productivité grâce à des opérations simplifiées.

Pourquoi Splunk

Au fil des ans, ASICS a pris des mesures proactives pour protéger son entreprise. Parmi celles-ci, on peut citer la mise en œuvre du comité de sécurité de l'information et du bureau de la sécurité de l'information, ainsi que de l'équipe de réponse aux incidents de sécurité informatique (CSIRT) et du centre des opérations de sécurité (SOC). Cependant, après avoir mis en place ces ressources, la société ne parvenait toujours pas à gérer et à analyser de manière centralisée les logs générés à partir des systèmes internes dispersés sur différents sites, notamment les pare-feu, les serveurs proxy, et les systèmes de détection et de réponse des points de terminaison. Elle devait également préserver les traces de preuves aux fins de la responsabilité sociale. Toutes ces tâches étaient fastidieuses car elles nécessitaient de nombreuses procédures manuelles.

Une autre priorité consiste à détecter avec précision chaque menace de point de terminaison, que ce soit une fraude par e-mail, une cyberattaque ou tout autre problème, et à intervenir à temps grâce à une surveillance 24h/24, 7j/7. En ce qui concerne la prévention des crises, ASICS a également besoin d'un mécanisme fiable pour extraire les modèles anormaux et identifier les appareils suspects au moyen de la corrélation et de l'analyse historique des données de log. Splunk Enterprise répond non seulement à toutes ces exigences, mais impressionne également ASICS par sa flexibilité à travailler de manière transparente dans un environnement SOCl à petite échelle et sa capacité à être opérationnel dans un délai très court avec un petit investissement.

Secteur d'activité

- Fabrication

Scénarios d'utilisation Splunk

- Gestion des logs
- Sécurité et fraude

Défis

- Absence de réaction rapide face aux incidents et aux menaces
- Incapacité à centraliser la gestion et l'analyse des logs
- Réaction et résolution des incidents inefficaces demandant beaucoup d'efforts manuels
- Défis de responsabilité sociale en raison de possibles fuites de données et de risques de sécurité

Impact sur l'activité

- Sécurité de l'entreprise accrue grâce à une visibilité en temps réel des incidents et des menaces
- Efficacité opérationnelle améliorée grâce à la gestion automatisée et centralisée des logs, avec une intervention manuelle minimale
- Responsabilité sociale renforcée grâce aux opérations sécurisées et transparentes
- Croissance durable de l'entreprise avec le potentiel d'aller plus loin avec Splunk

Sources de données

- Pare-feu de nouvelle génération
- Proxys cloud
- Serveurs proxy
- Système de détection et de réponse des points de terminaison
- Logs d'événements du serveur cloud

Produits Splunk

- Splunk Enterprise

Automatisation de l'analyse des logs grâce à la visibilité en temps réel et aux informations opérationnelles

Fonctionnant sur un cloud privé virtuel dans le centre de données d'ASICS, le logiciel Splunk consolide les données de log de tous les systèmes et les analyse sur une plateforme centrale. Il génère ainsi des informations et donne une visibilité sur l'ensemble des opérations en temps réel. Ensuite, il calcule les scores de risque sur la base des recherches de corrélation et identifie les anomalies et les menaces en temps réel. Les opérateurs SOC peuvent désormais accéder au statut d'analyse partout et à tout moment via une console Web intuitive. Ils peuvent recevoir des alertes via leur smartphone en cas d'incidents urgents, tandis que le CSIRT d'ASICS peut facilement suivre les activités post-incidents.

Tous ces efforts sont automatisés, ce qui permet à ASICS de superviser en permanence son centre de données avec une intervention manuelle minimale. En automatisant la gestion des logs, ASICS économise une main d'œuvre précieuse et peut se concentrer sur d'autres activités commerciales à forte valeur ajoutée.

Responsabilité sociale assurée grâce au suivi rapide des incidents et au renforcement de la sécurité

En tant que société cotée en bourse, ASICS est tenue de fournir à ses parties prenantes une vision claire de l'entreprise. Par exemple, elle est responsable de la façon dont les données sont recueillies et dont chaque processus est mené, tel que la conception et la fabrication de chaussures. Grâce à Splunk Enterprise, ASICS peut rapidement anticiper et suivre les problèmes potentiels, ainsi qu'améliorer la sécurité. ASICS peut également extraire les informations opérationnelles des logs, identifier les événements et générer rapidement des rapports pour la direction et les parties prenantes via une interface intuitive. Le renforcement de la responsabilité sociale permet à ASICS de se forger une meilleure réputation auprès des parties prenantes internes et externes, tout en attirant des professionnels talentueux et en motivant les employés.

« En tant qu'outil d'analyse polyvalent, Splunk Enterprise soutient efficacement nos opérations et nous procure de nombreux avantages. Nous pensons que la solution Splunk pourrait dynamiser l'industrie du sport. »

— Shigekazu Tanimoto, Responsable en chef de la sécurité mondiale,
ASICS Corporation

Augmentation de l'efficacité et de la productivité grâce aux opérations simplifiées

Désormais au centre de l'infrastructure de sécurité d'ASICS, Splunk Enterprise fournit à l'entreprise un réseau de données corrélé et simplifie les opérations comme jamais auparavant. Entièrement compatible avec les applications existantes, le logiciel fonctionne bien avec toutes les parties de l'environnement commercial. Il permet une collaboration transparente entre les différents services, améliorant ainsi l'efficacité opérationnelle et la productivité.

Par ailleurs, ASICS explore des idées plus créatives grâce à Splunk Enterprise, telles que la détection des menaces internes malveillantes et des fuites de données, ce qui permet de protéger les actifs de l'entreprise et de préserver la confidentialité des employés. Pour cette raison, l'entreprise est en train d'évaluer Splunk User Behavior Analytics en vue d'une utilisation future. Elle prévoit également d'étendre l'utilisation de la solution Splunk à une zone géographique plus étendue en appliquant une stratégie régionale de Gestion de l'information et des événements de sécurité (SIEM) au profit d'autres pays.

En outre, ASICS tente d'exploiter le moteur d'analyse des big data du logiciel Splunk pour une gamme plus large d'applications commerciales. Par exemple, l'un de ses produits est une balle de baseball avec des capteurs intégrés qui mesurent les données du lancer. Les big data collectées à partir des capteurs peuvent fournir des informations qui aideront les athlètes à battre des records. Grâce à Splunk Enterprise, ASICS estime que le meilleur reste à venir et que l'avenir s'annonce durable.

AW_20-13538-Splunk-SEC-ASICS-A4-101-CS