ManageEngine
Log360

La base de l'audit et de la **sécurisation de votre périmètre réseau** avec un outil de **SIEM**

www.manageengine.fr/log-management

Introduction

Pour déjouer les attaques de réseau, vous devez d'abord être au courant des événements de sécurité critiques qui se produisent sur votre réseau. Si la surveillance des performances du réseau est importante pour le diagnostic et pour garantir le bon fonctionnement, l'audit des données des logs générés par vos périphériques réseau est crucial pour identifier les événements de sécurité qui vous intéressent. Mais en raison du volume élevé d'événements générés par les périphériques de votre réseau, l'audit de ces événements en temps réel peut être difficile, voire impossible.

Dans ce guide, vous apprendrez les bases de l'audit et de la sécurisation du périmètre de votre réseau en utilisant une solution de gestion des informations et des événements de sécurité (SIEM).

Extraire de précieuses indications sur la sécurité à partir des logs des périphériques réseau

Toute activité se produisant dans le périmètre de votre réseau est enregistrée dans un journal. Les pare-feu, les systèmes de détection d'intrusion (IDS), les systèmes de prévention des intrusions (IPS), les routeurs et les switchs génèrent tous de gros volumes de données syslog qui contiennent des informations précieuses sur chaque événement survenant sur votre réseau. Ce sont ces journaux que les administrateurs sécurité doivent vérifier pour s'assurer que leur réseau est sain et sûr. La collecte et l'analyse des journaux de vos périphériques réseau se résument à trois étapes :

- **Activer la journalisation :** Connectez-vous à l'interface graphique de périphérique réseau en tant qu'administrateur et activez la connexion au système. L'appareil génère alors des entrées de log pour un ensemble d'événements spécifiés et transmet les données au serveur distant spécifié.
- **Centraliser la collecte des logs :** Centralisez la collecte des logs : Déployez une solution SIEM pour centraliser les données des journaux de tous vos périphériques réseau. Le stockage centralisé des données de journalisation est essentiel car il vous aide à relier les points et à découvrir les schémas d'attaque en corrélant les événements provenant de différentes sources.
- **Analyser les logs pour détecter les attaques :** Configurez des profils de rapport et d'alerte sur votre solution SIEM pour les incidents de sécurité critiques. Ces rapports vous aideront à surveiller en permanence les incidents de sécurité survenant sur votre réseau afin de vous assurer qu'aucune menace potentielle ne passe inaperçue.

Obtenir une visibilité complète du réseau grâce aux rapports d'audit

Les équipes de sécurité peuvent examiner périodiquement l'activité du réseau en établissant des rapports à l'aide d'une solution SIEM. Les rapports d'audit fournissent une visualisation claire des événements de sécurité importants qui se sont produits au cours d'une période donnée. Cela vous donnera une visibilité totale du périmètre de votre réseau et vous aidera à fournir des rapports tant pour les audits internes que pour les audits de conformité.

Détecter les menaces à la sécurité grâce aux alertes

Pour détecter les menaces en temps réel, configurez des alertes pour les événements qui posent un problème de sécurité. En fonction de vos besoins, sélectionnez les événements pour lesquels vous avez besoin d'alertes et ceux que vous pouvez examiner périodiquement dans des rapports. Lorsqu'une alerte est déclenchée, vous pouvez rapidement enquêter sur les événements connexes qui se sont produits en exploitant la fonctionnalité de recherche de votre solution SIEM. Allez plus loin et automatisez la réponse aux menaces en configurant un script personnalisé qui sera exécuté lorsqu'une alerte est déclenchée.

Comment la corrélation des événements peut améliorer la détection des menaces

Les événements individuels en eux-mêmes peuvent ne pas donner un contexte suffisant pour vous aider à identifier une menace potentielle de sécurité, et l'identification manuelle de modèles anormaux est presque impossible étant donné le volume de données d'événements. C'est là qu'intervient le moteur de corrélation d'événements de votre solution SIEM, qui associe différents événements survenant sur votre réseau et identifie tout modèle d'événement susceptible de constituer une menace pour la sécurité de votre réseau. Cela permettra non seulement de réduire le bruit de l'alerte, mais aussi de découvrir des menaces qui pourraient autrement passer inaperçues.

Détecter instantanément le trafic malveillant grâce à Threat Intelligence

Dans le domaine de la détection et de la réponse aux menaces, la Threat Intelligence (TI) permet d'atténuer les attaques provenant de sources malveillantes connues. L'intégration de votre solution SIEM à un processeur de flux de TI renforcera la capacité de détection et d'atténuation des menaces de votre équipe de sécurité. Avec un flux TI augmenté, une solution SIEM peut corréler les données des logs réseau avec le flux pour identifier instantanément le trafic provenant de sources malveillantes connues.

Comment ManageEngine Log360 aide à vérifier les journaux des périphériques réseau

Log360 est une solution SIEM complète qui permet de sécuriser le périmètre de votre réseau. Log360 collecte et analyse en temps réel les syslogs des périphériques réseau pour aider à détecter les menaces de sécurité le plus tôt possible.

Rapports et alertes prêts à l'emploi

Log360 est livré avec des rapports et des profils d'alerte prêts à l'emploi pour un large éventail de constructeurs d'équipements réseaux. Ainsi, les équipes de sécurité peuvent commencer à exécuter des rapports et à déclencher des alertes dès le premier jour. Programmez des rapports pour examiner périodiquement les événements de sécurité importants qui se produisent sur le réseau. Les grandes entreprises peuvent facilement créer des rapports personnalisés et des conditions d'alerte spécifiques à l'environnement pour répondre à leurs diverses exigences en matière d'audit.

Le moteur de corrélation avancé de Log360 peut associer les logs des périphériques réseau aux informations d'événements provenant d'autres machines pour détecter les attaques avancées. Par exemple, il peut corréler l'activité du client VPN avec l'activité de connexion et d'autres serveurs pour détecter l'installation de logiciels et de services suspects.

CAS D'USAGE

Audit du trafic firewall

Avec Log360, vous pouvez vérifier le trafic du pare-feu en temps réel, y compris les connexions acceptées et refusées. Auditer le trafic en fonction de la source, de la destination, du protocole et du port pour analyser en profondeur les tendances du trafic firewall.

Détection des attaques de réseau

Log360 traite les journaux IDS et IPS et vous avertit en temps réel des attaques sur votre réseau. Vous pouvez surveiller les éventuelles activités d'attaque du réseau en fonction de la source, de la destination et de la gravité afin de détecter et d'atténuer les attaques le plus tôt possible.

Suivi des changements de configuration

Autoriser des modifications de la configuration des périphériques réseau sans les vérifier peut mettre en péril la sécurité de votre réseau. Avec Log360, vous pouvez vérifier les changements de configuration des routeurs et les modifications des règles de pare-feu. Assurez la sécurité et la conformité en surveillant en permanence toutes les règles de pare-feu qui ont été ajoutées, supprimées et modifiées, ainsi que les changements exécutés sur votre routeur.

Détection des trafics malveillants avec la Threat Intelligence

Le processeur d'alimentation STIX/TAXII intégré de Log360 et la base de données mondiale des menaces IP augmentée vous garantissent une mise à jour dynamique avec les dernières données sur les menaces. Cela vous aidera à détecter et à bloquer immédiatement le trafic malveillant qui interagit avec votre réseau.

Fabricants d'équipements réseau pris en charge par Log360

Log360 prend en charge immédiatement les constructeurs de périphériques réseau suivants :

Pour plus de détails, veuillez contacter le service d'assistance à l'adresse suivante :

log360-support@manageengine.com