

GRAYLOG SECURITY

Obtenez des informations exploitables de votre posture en matière de cybersécurité

Proposé dans le cadre d'un environnement personnel ou dans le cloud, Graylog Security est une solution de cybersécurité évolutive qui combine des fonctionnalités de gestion des informations et des événements de sécurité (SIEM), de renseignement sur les menaces et de détection des anomalies, pour permettre à vos professionnels de la sécurité de simplifier l'identification, la recherche et la réponse aux cybermenaces tout en renforçant continuellement votre posture de sécurité.

Une plateforme de cybersécurité complète et puissante pour les entreprises de toute taille

Les entreprises aux ressources limitées ont besoin d'une détection des menaces abordable et proactive, d'une analyse et d'une réponse aux incidents, ainsi que de rapports de conformité pour renforcer leur sécurité. Graylog Security combine la gestion centralisée des journaux, la détection des menaces, la normalisation et la corrélation des données, et des rapports faciles à déployer, à gérer et à utiliser. Nous avons conçu notre plateforme de sécurité pour vous fournir les fonctionnalités dont vous avez besoin, sans la complexité et le coût des solutions SIEM traditionnelles.

GRAYLOG SECURITY D'UN SEUL COUP D'ŒIL

Flux de travail de l'utilisateur et d'une interface utilisateur intuitive

Graylog Security est préconfiguré avec des visualisations pointer-cliquer robustes, des modèles de recherche, des flux de travail d'enquête et un assistant intuitif de personnalisation des alertes et des corrélations, le tout pour vous aider à augmenter la visibilité dans votre environnement et à identifier rapidement les modèles importants ou suspects dans les données machine lorsque vous traquez des cybermenaces.

graylog
SECURITY

AVANTAGES DE GRAYLOG SECURITY

- Examine des volumes de données en quelques secondes avec des capacités de recherche ultra-rapides
- Concentre les efforts de sécurité sur l'essentiel en filtrant le bruit des alertes
- Augmente la productivité grâce à l'automatisation à laquelle vous pouvez faire confiance pour des tâches répétitives et exigeantes en matière de sécurité
- Tire parti d'un moteur ML de détection d'anomalies qui étudie constamment vos comportements sécuritaires au fil du temps



Aucun oubli de journal

Rassembler des journaux de différentes sources peut paraître une tâche compliquée si vous n'avez pas le bon outil. Graylog Security peut vous fournir le contexte dont vous avez besoin pour donner un sens à de grandes quantités de données de journaux, en recueillant, normalisant et visualisant automatiquement les données de journaux d'événements à partir de sources sur votre réseau.

Recherche instantanée pour l'analyse et la résolution de pannes

Chaque seconde compte lorsque vous essayez de protéger votre environnement contre les cybermenaces. Graylog Security est conçu pour analyser des téraoctets de données en quelques secondes, ce qui vous permet de trouver rapidement des données de journaux importantes en temps réel. Des filtres de recherche prêts à l'emploi permettent également d'affiner rapidement les données.

Détection d'anomalies pertinente

Gardez une longueur d'avance sur les mauvais garçons. Les capacités de détection d'anomalies de Graylog Security reposent sur un puissant moteur de détection d'anomalies de machine learning (ML), qui peut comprendre automatiquement votre environnement et vous alerter sur un comportement anormal de vos utilisateurs et entités (UEBA).

Identifiez les événements de sécurité prioritaires dans un océan d'alertes

Filtrer le bruit pour obtenir les données dont vous avez besoin rapidement ne doit pas être compliqué. Le moteur d'alerte de Graylog Security facilite le filtrage du bruit afin que vous puissiez vous concentrer sur des événements de sécurité vraiment importants, réduisant la fatigue due aux alertes et maximisant la productivité.

Suivez le rythme de la réglementation et de la conformité

Rester au courant des dernières réglementations et normes en constante évolution peut être un travail à temps plein en soi. Les capacités de collecte et d'archivage des journaux avec un tableau de bord intégré et des rapports automatisés permettent à Graylog Security de vous aider à rester en conformité.

S.O.A.R. avec Graylog Security

Graylog Security peut s'intégrer de manière transparente à vos plateformes existantes d'orchestration, d'automatisation et de réponse de sécurité (S.O.A.R.) pour collecter des données de journal et de sécurité, et lancer automatiquement des flux de travail à partir des alertes de corrélation fournies par Graylog Security, vous aidant ainsi à réduire considérablement les métriques de temps de résolution (TTR).

Aucune formation nécessaire

L'interface très accessible de Graylog Security est conçue pour faciliter la collaboration et encourager la réutilisation des travaux antérieurs. Il n'est pas nécessaire d'apprendre SQL ou un langage de requête propriétaire, ou d'exécuter plusieurs recherches pour trouver les données dont vous avez besoin. N'importe qui dans votre équipe peut rapidement commencer à utiliser Graylog Security.

FONCTIONNALITÉS PUISSANTES ET ULTRA-RAPIDES



DÉTECTION D'ANOMALIES / UEBA

Apprentissage rapide du comportement « normal » et identification automatique des écarts des utilisateurs et des entités à grande échelle, avec un ajustement et une amélioration permanents au fil du temps.



ARCHIVAGE

Stockez des données plus anciennes sur un support lent et réimportez-les facilement dans Graylog lorsque vous en avez besoin.



RAPPORTS DE CONFORMITÉ

Tirez parti de la fonctionnalité du tableau de bord de Graylog pour élaborer et configurer facilement les plannings des rapports.



CORRÉLATION ET ALERTE

Recevez des alertes par e-mail, SMS, Slack et davantage. Mettez à jour les critères d'alerte en fonction d'une liste dynamique dans une table de consultation.



NORMALISATION ET ENRICHISSEMENT DES DONNÉES

Effectuez des recherches plus rapides en ajoutant le WHOIS, la géolocalisation IP, les renseignements sur les menaces ou d'autres données structurées.



JOURNAUX UTILISATEURS DE GRAYLOG

Surveillez qui a accédé à quelles données de journal, et quelles mesures ils ont prises pour s'assurer de la conformité et de la sécurité.



ENQUÊTES SUR LES INCIDENTS

Créez et combinez plusieurs recherches pour tout type d'analyse en une seule fois et exportez les résultats vers un tableau de bord.



TABLEAUX DE BORD PRÉDÉFINIS, ALERTES

Commencez rapidement avec du contenu prédéfini – modèles de recherche, tableaux de bord, alertes corrélées, tables de consultation dynamiques, et plus encore.



GÉNÉRATEUR DE REQUÊTES DE RECHERCHE

Créez et combinez plusieurs recherches pour tout type d'analyse en une seule fois et exportez les résultats vers un tableau de bord.



TABLEAUX DE BORD D'ANALYSES DE SÉCURITÉ

Combinez des widgets pour créer des affichages de données personnalisés et automatiser la livraison des rapports sur votre messagerie.



INTÉGRATIONS S.O.A.R.

Partagez facilement les données avec d'autres systèmes essentiels d'entreprise pour une collaboration et une transparence totales.



FLUX DE RENSEIGNEMENTS SUR LES MENACES

Apportez du contexte aux données des journaux d'événements avec vos flux de renseignements sur les menaces existants et repérez des problèmes de sécurité potentiels.

CONSULTEZ NOS EXPERTS ET OBSERVEZ GRAYLOG SECURITY EN ACTION

Voir c'est croire. Chez Graylog, nous voulons que vous obteniez toutes les réponses à vos questions avant d'acheter. Nous proposons des démonstrations sur rendez-vous, qui expliquent la fonctionnalité de nos produits et accordent du temps aux questions. **Planifiez votre démo avec Graylog Security aujourd'hui** et observez notre puissante plateforme de cybersécurité en action.



Graylog Security vous permet de mieux comprendre des corrélations d'événements parmi des dizaines de milliers de composants de réseau afin d'identifier des menaces ou des activités suspectes.

À PROPOS DE GRAYLOG

La gestion des journaux comme il se doit. Déployée dans plus de 50 000 installations à travers le monde, Graylog est une solution de gestion des journaux centralisée et primée, conçue pour la vitesse et l'évolutivité de la capture, du stockage et de l'analyse en temps réel de téraoctets de données machine. Graylog permet à des centaines de milliers d'utilisateurs d'explorer leurs données chaque jour pour résoudre des problèmes de sécurité, de conformité, d'exploitation et de développement d'applications.

www.graylog.org
info@graylog.com
1301 Fannin Street, Suite 2140
Houston, TX 77002

©2022 Graylog, Inc. All rights reserved.