Graylog Security

Renforcez votre cybersécurité avec une technologie SIEM avancée

Disponible en mode hébergée ou SaaS, Graylog Security est une solution de cybersécurité évolutive qui combine des fonctionnalités de gestion des informations et événements de sécurité (SIEM), de détection des menaces et réponse aux incidents (TDIR), de renseignement sur les menaces, d'investigation des incidents et de détection des anomalies. Elle aide ainsi les professionnels de la sécurité à faciliter l'identification, la recherche et la réponse aux cybermenaces.

Les avantages du SIEM

Les organisations ayant souvent des ressources limitées ont besoin d'un système abordable et proactif de détection des menaces, d'analyse et de réponse aux incidents et de rapports de conformité pour renforcer leur position en matière de sécurité. Conçu sur la plateforme Graylog, Graylog Security intègre la gestion des journaux d'entreprise, la détection des menaces, les étapes de remédiation suggérées et les rapports faciles à déployer, à gérer et à utiliser. Nous avons conçu notre plateforme de sécurité de sorte qu'elle offre les fonctionnalités dont vous avez besoin sans la complexité et le coût prohibitif des solutions traditionnelles de SIEM.

Aperçu de Graylog Security

Interface utilisateur axée sur la sécurité

Augmentez votre productivité et votre efficacité grâce à l'interface utilisateur unique de Graylog Security, axée sur la sécurité et conçue pour permettre aux analystes d'accéder rapidement aux enquêtes, alertes et rapports de de flux de travail.

Avantages de Graylog Security

- Parcourir un grand nombre de données en quelques secondes grâce à des fonctions de recherche ultra rapides.
- Suivre efficacement des actifs et identifier rapidement l'origine d'un problème ou d'un journal.
- Focalisez les efforts de sécurité sur ce qui compte en filtrant le bruit des alertes
- Augmenter la productivité grâce à une automatisation fiable pour les tâches répétitives et exigeantes en matière de sécurité
- Tirer parti d'un moteur ML de détection d'anomalies qui s'adapte continuellement à vos pratiques en matière de sécurité.

Notation basée sur les risques

Se concentrer sur les risques “immédiats” grâce à l’évaluation automatisée basée sur les risques. Graylog Security attribue une note de risque à chaque alertes afin que les analystes puissent facilement classer les incidents de sécurité par ordre de priorité.

Recherche ultra-rapide pour l’analyse détaillée et la résolution des problèmes

Chaque seconde compte lorsqu’il s’agit de protéger votre environnement contre les cybermenaces. Graylog Security est conçu pour analyser des téraoctets de données en quelques secondes, vous permettant de trouver des données importantes en temps réel. Accédez à l’historique des requêtes précédentes à partir d’un menu déroulant facile à utiliser.

Une détection efficace des anomalies

Gardez une longueur d’avance écartant toute intrusion. Les capacités de Graylog Security en matière de détection d’anomalies sont conçues avec un puissant moteur de détection d’anomalies par apprentissage automatique (ML) qui peut comprendre automatiquement votre environnement et vous alerter sur ce qui constitue un comportement suspect des utilisateurs ou entités (UEBA).

Identifiez les événements de sécurité prioritaires dans une multitude d’alertes

Il n’est pas toujours facile d’occulter le bruit pour se focaliser rapidement sur les données dont on a besoin. Le moteur d’alerte de Graylog Security facilite le filtrage du bruit afin que vous puissiez vous concentrer sur les événements de sécurité qui comptent vraiment, réduisant ainsi la fatigue des alertes et maximisant la productivité.

Espace de travail dédié aux enquêtes sur les incidents

Graylog Security permet de gérer facilement les enquêtes sur les incidents, du début à la fin, et ce grâce à un espace de travail tout-en-un qui permet de collecter et d’organiser des ensembles de données, des rapports, des preuves et d’autres éléments contextuels pendant l’enquête sur un incident ou un problème potentiel, de collaborer entre les équipes tout au long du processus d’enquête et d’identifier rapidement les tendances en utilisant les données sauvegardées lors d’enquêtes précédentes.

Trouvez rapidement les actifs défaillants

Le module d’Actifs de Graylog Security vous permet de suivre différents types d’actifs dans l’environnement et d’enrichir les messages de journal avec leurs informations. Les informations relatives à vos actifs peuvent être facilement ajoutées via l’interface utilisateur de Graylog ou synchronisées via LDAP ou AD.

Couverture contre les menaces organisées

Graylog Security vous aide à détecter les menaces dans votre environnement en s’appuyant sur des techniques cybernétiques avancées telles que la détection d’anomalies, les règles Sigma, les renseignements sur les menaces et le cadre MITRE ATT&CK®.

Comment mitigezvous les risques ?

Évaluez votre cyber-résilience avec Graylog Security en mesurant les ICP de sécurité critiques qui déterminent l’efficacité avec laquelle vous réduisez les risques. Ainsi vous saurez comment concentrer vos initiatives d’amélioration.

Réduisez le coût total d'acquisition tout en renforçant votre sécurité

Les capacités de Graylog Security basées sur le cloud, l'interface utilisateur intuitive et le contenu prêt à l'emploi signifient que vous pouvez commencer à obtenir des données précieuses à partir de vos journaux plus rapidement que les SIEM traditionnels. Optimisez la charge de travail grâce à des fonctionnalités conçues pour réduire considérablement la fatigue liée aux alertes, obtenir des réponses rapides et responsabiliser vos équipes sécurité. Utilisez un niveau de stockage « intermédiaire » pour conserver les données, ce qui permet des options de stockage à distance ou sur site moins coûteuses, tout en offrant la même expérience de recherche rapide et robuste.

Fonctionnalités puissantes et ultra-rapides

Détection d'anomalies / UEBA
Des fonctionnalités qui apprennent rapidement les comportements « normaux » et identifient automatiquement les écarts pour les utilisateurs et les entités à grande échelle, avec un réglage et une amélioration continus au fil du temps.

Enrichissement des actifs
Obtenez un aperçu de votre environnement grâce à la possibilité de suivre différents actifs et d'enrichir les messages de journal avec des informations supplémentaires.

Rapports de conformité
Tirez parti de la fonctionnalité du tableau de bord de Graylog pour créer et configurer facilement des rapports planifiés.

Corrélation et alerte
Recevez des alertes par e-mail, SMS, Slack et bien plus encore. 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 des utilisateurs de Graylog
Consultez qui a accédé à quelles données de journal et quelles mesures ont été prises pour garantir la conformité et la sécurité.

Enquête d'incident
Espace de travail tout-en-un pour collecter et organiser des ensembles de données, des rapports, des preuves et d'autres contextes tout en enquêtant sur un incident potentiel.

Tableaux de bord prédéfinis, alertes
Démarrez rapidement avec du contenu prédéfini pour les cas d'utilisation de la sécurité : modèles de recherche, tableaux de bord, alertes corrélées, tables de consultation dynamiques, etc.

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

Tableaux de bord d'analyse de sécurité
Combinez des widgets pour créer des affichages de données personnalisés et automatisez la livraison de rapports dans votre boîte de réception.

Intégrations SOAR
Partagez facilement des données avec d'autres systèmes critiques pour une transparence et une collaboration totale.

Flux de renseignements sur les menaces
Ajoutez du contexte aux données des journaux d'événements avec vos flux de renseignements sur les menaces existantes et identifiez les problèmes potentiels de sécurité.

graylog
SECURITY

Consultez nos experts et voyez Graylog Security à l'œuvre

Voir, c'est croire. Chez Graylog, obtenez réponse à toutes vos questions avant de vous engager. Nous proposons des démos produits sur mesure au cours desquels nous présentons les fonctionnalités des produits et répondons à toutes vos questions. **Planifiez votre démo Graylog Security dès aujourd'hui** et découvrez notre puissante plateforme de cybersécurité à l'œuvre.

Graylog Security vous permet de mieux comprendre les corrélations d'événements à travers des dizaines de milliers de composants du réseau afin de détecter les menaces identifiées ou les activités suspectes.

À PROPOS DE GRAYLOG

Graylog est un leader de la gestion des journaux et des informations de sécurité (SIEM), rendant le monde et ses données plus efficaces et sécurisés. Conçu par des praticiens pour les praticiens, Graylog permet à des milliers de professionnels de l'informatique et de la sécurité de trouver des réponses à partir de données et de résoudre chaque jour des problèmes de sécurité, de conformité, d'exploitation et de DevOps. Avec plus de 50 000 installations dans le monde, Graylog est une plate-forme conçue pour être rapide et évolutive dans la capture, le stockage et l'analyse en temps réel de téraoctets de données machine. Graylog élimine le bruit et offre une expérience utilisateur exceptionnelle en rendant l'analyse des données, la recherche des menaces, la détection et l'enquête sur les incidents rapides et efficaces grâce à une architecture plus rentable et plus flexible.

www.graylog.org
info@graylog.com | 1301 Fannin Street, Suite 2000, Houston, TX 77002

graylog