Graylog Enterprise

Vos logs parlent. Les écoutez-vous?

Alors que les parcs informatiques modernes ne cessent de croître en taille et en complexité, la visibilité des problèmes de cybersécurité devient de plus en plus difficile, car les applications, systèmes et appareils du réseau produisent considérablement plus de données de logs. Les approches manuelles de collecte, de normalisation et d'analyse des logs sont peu évolutives. Les organisations ont donc besoin d'un meilleur moyen de collecter et d'analyser de gros volumes de données sans créer une lourde charge pour les professionnels SecOps, IT et DevSecOps.

Gestion et analyse des logs d'entreprise pour une meilleure visibilité

Mise à votre disposition en mode autogéré ou cloud native, Graylog Enterprise est une solution complète de gestion et d'analyse des journaux qui vous aide à centraliser, rechercher et analyser les données des logs d'événements afin que les organisations disposant de ressources limitées puissent identifier plus rapidement les problèmes de sécurité et de performance, réduire les temps d'arrêt et rationaliser les opérations.

Avantages de Graylog

- Consolide les données des journaux de l'ensemble de votre entreprise dans un référentiel centralisé à des fins d'analyse
- Parcours un grand nombre de données en quelques secondes grâce à des fonctions de recherche ultra rapides.
- Concentre les efforts de performance sur l'essentiel en filtrant le bruit des alertes
- Augmente la productivité grâce à une automatisation fiable des tâches courantes

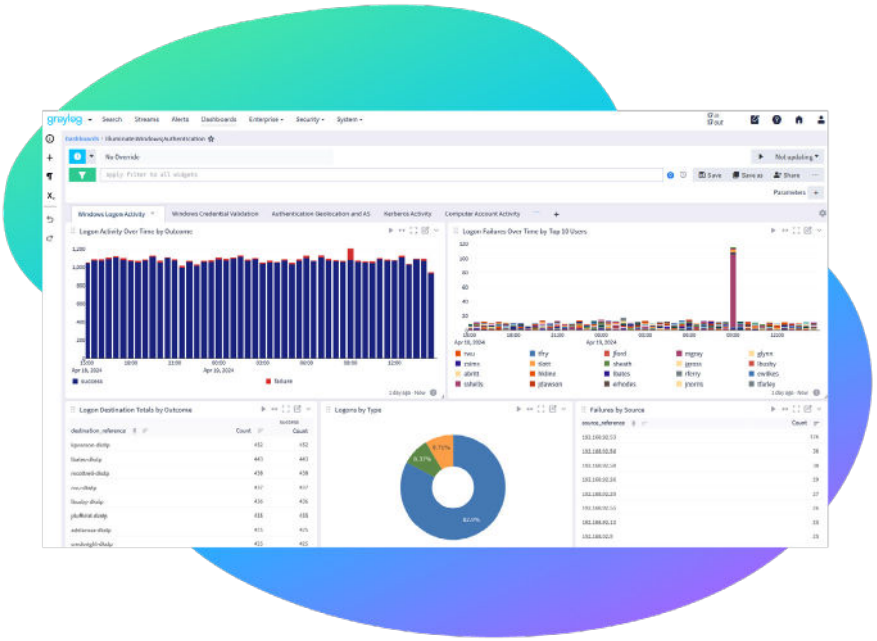
Aperçu de Graylog Enterprise

Collecte et analyse des journaux d'événements pour une meilleure visibilité

Votre infrastructure, vos appareils et vos applications génèrent des quantités de données de log qui peuvent vous donner une idée de l'état de votre parc. Toutes les données de log, y compris les événements syslog, Windows® ou VMware®, sont des éléments essentiels de votre environnement dans son ensemble et peuvent contribuer à la résolution des problèmes et à la détection des menaces. Graylog Enterprise collecte, normalise et analyse les données de log afin que vous puissiez détecter et trouver plus rapidement la cause principale des problèmes de sécurité et de performance.

Puissantes capacités de recherche et de filtrage pour faciliter la résolution des problèmes

Les données de journal vous sont transmises rapidement et trouver la bonne information peut être aussi difficile que de chercher une aiguille dans une botte de foin. Graylog Enterprise est conçu pour analyser des pétaoctets de données en quelques secondes, vous permettant de trouver rapidement des données en temps réel et d'appliquer facilement un code couleur à vos données de journal pour faciliter le filtrage et l'identification des problèmes.



Améliorez la qualité de vos journaux grâce aux fonctions de visualisation

Grâce à Graylog Enterprise, visualisez facilement vos journaux via un flux interactif afin d'identifier les problèmes en temps réel.

Identifiez les événements prioritaires parmi une multitude d'alertes

Accéder facilement aux données dont vous avez besoin ne devrait pas être compliqué. Graylog Enterprise facilite le filtrage du bruit afin que vous puissiez vous concentrer sur les événements prioritaires, réduisant ainsi la fatigue des alertes et éliminant le besoin de sortir de la plateforme pour une analyse supplémentaire.

Passez rapidement à l'action grâce aux alertes et notifications personnalisées

Vos utilisateurs ne devraient pas détecter les problèmes avant vous. Le moteur d'alerte intelligent de Graylog Enterprise vous permet de personnaliser les alertes et les options de livraison, y compris les notifications par e-mail et Slack®, ainsi que la possibilité de déclencher un script externe afin que vous puissiez commencer à résoudre les problèmes avant qu'ils n'affectent la continuité des activités.

Un contenu prêt à l'emploi qui génère rapidement de la valeur ajoutée

Graylog Enterprise est doté d'un contenu prêt à l'emploi pour vous aider à rationaliser l'analyse des données de journaux. Démarrez rapidement avec du contenu tel que des modèles de recherche préconfigurés, des tableaux de bord, des alertes corrélées, etc., et détectez plus rapidement la cause première des problèmes de sécurité.

Fonctionnalités puissantes et ultra-rapides

Alertes et notifications
Personnalisez les alertes et recevez-les par e-mail, SMS, Slack®, etc.

Archivage
Archivez les journaux d'événements à des fins d'analyse et identifiez les tendances au fil du temps.

Moteur de corrélation
Collectez automatiquement des informations provenant de différents journaux afin d'identifier les problèmes potentiels.

Transfert
Envoyez facilement des données à Graylog Cloud ou à une installation de serveur Graylog sur site.

Contenu pré-installé Illuminate
Démarrez rapidement avec des analyseurs et des tableaux de bord prédéfinis exploitant le schéma Graylog.

Intégrez à l'aide de l'API Rest
Partagez facilement des données avec d'autres systèmes critiques pour une transparence et une collaboration totales.

Tableaux de bord interactifs
Combinez des widgets pour créer des affichages de données personnalisés et automatiser la livraison de rapports par email.

Aperçu du journal
Visualisez les données en temps réel au fur et à mesure que les événements se produisent, garantissez une disponibilité continue et rationalisez les enquêtes.

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

Modèle de recherche
Sauvegardez et partagez des recherches et des tableaux de bord paramétrés.

Flux de travail de recherche
Créez et combinez plusieurs requêtes en une seule action.

Gestion des équipes
Contrôlez l'accès et les capacités des unités. Intégration du LDAP/Active Directory.

Consultez Nos Experts et Voyez Graylog Enterprise à l'œuvre

Ne vous contentez pas de nous croire sur parole. Chez Graylog, nous pensons que vous devriez avoir la possibilité d'obtenir des réponses à toutes vos questions avant de vous engager. C'est pourquoi nous proposons des démos produits sur mesure au cours desquels nous présentons les fonctionnalités des produits et répondons à toutes vos questions. Découvrez comme il est facile de collecter, de normaliser et de contrôler vos données de journal de manière transparente afin d'identifier les problèmes de performance.

graylog
ENTERPRISE

Graylog Enterprise n'est pas seulement une solution de gestion centralisée des journaux, c'est le meilleur allié de votre écosystème informatique. Rejoignez dès aujourd'hui la révolution de la gestion des journaux.

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