

QUEL PRODUIT GRAYLOG EST FAIT POUR VOUS ?

Votre choix d'une solution de gestion des journaux devrait vous permettre d'en faire plus avec vos opérations informatiques et vos données de sécurité. Indépendamment de la taille de votre entreprise ou de votre équipe, de la pile d'événements et de données, des technologies et des configurations, Graylog dispose de la meilleure option pour satisfaire vos besoins.

QU'EST-CE QUE GRAYLOG SECURITY?

Graylog Security tient toutes les promesses du SIEM traditionnel sans la complexité, la fatigue des alertes et les coûts élevés. Construit sur la plateforme Graylog, Graylog Security réduit la pression sur le personnel chargé de la cybersécurité, renforce la posture générale de sécurité et réduit les risques.

POURQUOI C'EST IMPORTANT

Conçue selon des normes ouvertes, Graylog Open peut fournir les fonctionnalités de base d'une gestion centralisée des journaux dont vous avez besoin pour rassembler, valoriser, stocker et analyser les données. Graylog Security va encore plus loin en combinant les fonctionnalités SIEM, d'analyses de sécurité et de détection des anomalies pour fournir aux professionnels de la sécurité une plateforme de cybersécurité de pointe. Conçue pour relever les défis posés par les SIEM existants, Graylog Security facilite et accélère le travail des analystes en leur apportant la confiance, la productivité et l'expertise nécessaires, afin d'atténuer les risques causés par les menaces internes et les attaques basées sur les informations d'identification.

FONCTIONNALITÉ	GRAYLOG SECURITY
	Auto-géré, Hybride, Cloud
Détection des anomalies (AI/ML)	✓
Gestion des collecteurs	✓
Conformité et rapports réguliers	✓
Moteur de corrélation	✓
Enrichissement des données	✓
Visualisation des données	✓
Tables de recherche dynamiques	✓
Transporteur (Cluster-to-Cluster/Cluster-to-Cloud)	✓
Graylog Academy	✓
Graylog Illuminate (contenu de sécurité prêt à l'emploi)	✓
Journaux d'audit utilisateur Graylog	✓
Alertes d'incident et déclencheurs	✓
Renseignements intégrés sur les menaces, flux d'adresses IP géographiques, recherches.ups	✓
Archivage et restauration des journaux	✓
Pipelines	✓
API REST	✓
Contrôle d'accès basé sur les rôles	✓
Notifications de déclenchement de script	✓
Paramètres de recherche et de tableau de bord	✓
Analyse de sécurité	✓
Intégration S.O.A.R.	✓
Règles Sigma	✓
Assistance technique	✓
Chasse aux menaces	✓