Graylog Enterprise

Ihre Logdaten sprechen mit Ihnen. Können Sie es hören?

Da moderne IT-Umgebungen immer umfassender und komplexer werden, wird es auch immer schwieriger, Einblicke in Cybersecurity-Probleme zu erhalten, da Anwendungen, Systeme und Geräte im gesamten Netzwerk immer größere Mengen an Logdaten generieren. Manuelle Ansätze für die Erfassung, Normalisierung und Analyse von Logdaten lassen sich nur schlecht skalieren. Daher benötigen Unternehmen bessere Möglichkeiten, große Mengen an Logdaten zu erfassen und zu analysieren – ohne die Experten für SecOps, IT und DevSecOps zu überlasten.

Die wichtigsten Vorteile von Graylog

- Konsolidieren Sie die Logdaten aus Ihrer gesamten IT-Umgebung in einem zentralen Repository zur Analyse.
- Konzentrieren Sie sich auf das Wesentliche, indem Sie unbedeutende Warnmeldungen herausfiltern.
- Steigern Sie Ihre Produktivität mit einer zuverlässigen Automatisierung für wiederkehrende Aufgaben.

Logdaten-Management und -Analyse für maximale Transparenz

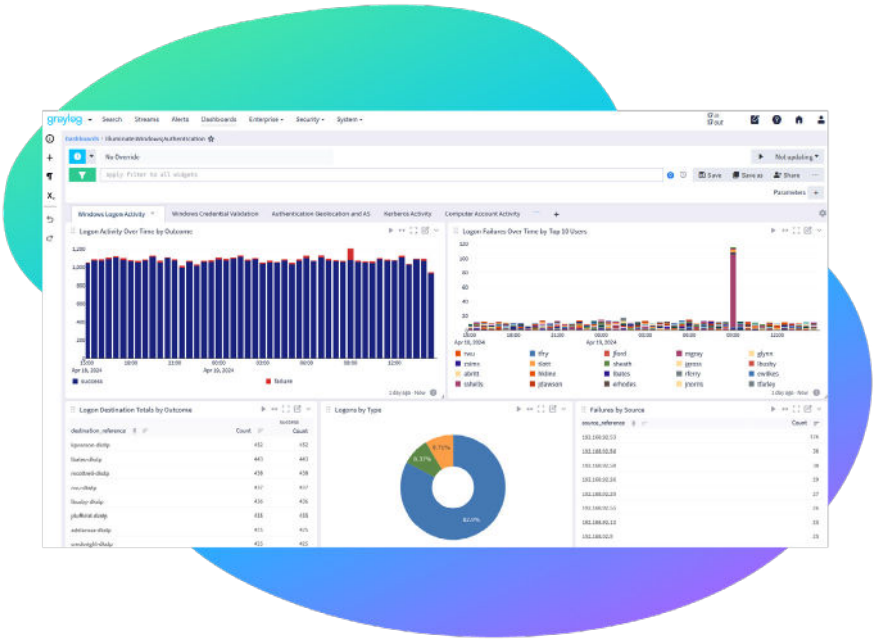
Graylog Enterprise ist eine umfassende Lösung für die Management und die Analyse von Logdaten, die Sie dabei unterstützt, Event-Logdaten zu zentralisieren, zu durchsuchen und zu analysieren. Sie können Graylog Enterprise entweder im eigenen Unternehmen betreiben oder als cloudnativen Service nutzen. Auch Unternehmen mit begrenzten Ressourcen können mit dieser Lösung Sicherheits- und Leistungsprobleme schneller erkennen, Ausfallzeiten minimieren und den Betrieb optimieren.

Graylog Enterprise im Überblick

Die Sammlung und Analyse von Event-Logdaten für maximale Transparenz

Ihre Infrastruktur, Geräte und Anwendungen generieren große Mengen an Logdaten, die Ihnen einen Einblick in den Zustand Ihrer IT-Umgebung geben können. Alle Logdaten, einschließlich der Syslog-, Windows®- oder VMware®-Events, sind wichtige Komponenten des Gesamtbildes Ihrer Umgebung und können bei der Fehlerbehebung und der Erkennung von Bedrohungen helfen. Graylog Enterprise sammelt, normalisiert und analysiert die Logdaten, damit Sie die Ursachen von Sicherheits- und Leistungsproblemen schneller erkennen und finden können.

Leistungsstarke Such- und Filterfunktionen für eine einfachere Fehlersuche und schnellere Fehlerbehebung



Kontinuierlich entstehen große Mengen an Logdaten. Die wichtigen Informationen zu finden kann wie die Suche nach der Nadel im Heuhaufen sein. Graylog Enterprise ist darauf ausgelegt, Petabyte an Daten in Sekundenschnelle zu analysieren. Mit dieser Lösung können Sie relevante Daten in Echtzeit finden und Ihre Logdaten ganz einfach farblich kennzeichnen, um sie zu filtern und Probleme zu identifizieren.

Verleihen Sie Ihren Logdaten Leben – mit Funktionen für die Visualisierung

Mit Graylog Enterprise können Sie Ihre Logdaten ganz einfach über einen interaktiven Stream visualisieren, um potenzielle Probleme in Echtzeit zu erkennen.

Für eine niedrigere TCO: nützliche Informationen vs Standby-Daten mit Graylog – Cribl ist nicht erforderlich

Graylogs Data-Routing-Funktion ermöglicht es Ihnen, Logdaten von geringerem Wert einfach in ein weniger kostspieliges Data Warehouse (Standby-Daten) auszulagern, bevor diese von Graylog verarbeitet werden. Sie können Ihre Standby-Daten selektiv wiederherstellen und in verwertbare Daten für zukünftige Untersuchungen umwandeln.

Werden Sie schneller aktiv – mit anpassbaren Alerts und Benachrichtigungen

Ihre Anwender sollten Probleme nicht vor Ihnen erkennen. Dank der intelligenten Alert-Engine von Graylog Enterprise können Sie Warnmeldungen und Zustelloptionen anpassen, einschließlich E-Mail- und Slack®-Benachrichtigungen, und ein externes Skript auslösen, damit Sie Probleme beheben können, bevor diese den laufenden Betrieb beeinträchtigen.

Out-of-the-Box-Inhalte bieten schnell einen Mehrwert

Graylog Enterprise bietet vordefinierte Inhalte, die Sie dabei unterstützen, die Analyse von Logdaten zu optimieren. Sie können sofort Inhalte wie vorkonfigurierte Suchvorlagen, Dashboards, korrelierte Warnmeldungen und vieles mehr nutzen, um den Ursachen von Sicherheitsproblemen schneller auf den Grund zu gehen.

Leistungsstarke, blitzschnelle Funktionen

Alerts und Benachrichtigungen
Passen Sie Warnmeldungen an Ihre Anforderungen an und erhalten Sie diese per E-Mail, SMS, Slack® und mehr.

Archivierung
Archivieren Sie Event-Logdaten für die Analyse und erkennen Sie Trends im Zeitverlauf.

Data Routing
Lagern Sie Daten von geringerem Wert in ein Data Warehouse aus, bevor sie diese selektiv wiederherstellen und zu einem späteren Zeitpunkt weiterverarbeiten.

Forwarder
Senden Sie Daten ganz einfach an die Graylog Cloud oder an eine Graylog Server-Installation On-Premises.

Inhalte beleuchten
Mit den integrierten Parsern und vordefinierten Dashboards, die das Graylog-Schema nutzen, können Sie sofort durchstarten.

Integrationsmöglichkeiten dank REST-API
Leiten Sie Daten ganz einfach an andere geschäftskritische Systeme weiter, um vollständige Transparenz zu schaffen und eine optimale Zusammenarbeit zu gewährleisten.

Interaktive Dashboards
Kombinieren Sie verschiedene Widgets, um individuelle Datenansichten zu erstellen und die Zustellung von Reports an Ihren Posteingang zu automatisieren.

Darstellung der Logdaten
Visualisieren Sie Ihre Daten in Echtzeit – noch während Events auftreten. Stellen Sie die kontinuierliche Verfügbarkeit sicher und optimieren Sie die Untersuchungen.

Zeitgesteuerte Berichte
Nutzen Sie die Dashboard-Funktionalitäten von Graylog, um auf einfache Weise planmäßige Reports zu erstellen und zu konfigurieren.

Suchvorlagen
Speichern und teilen Sie parametrisierte Suchvorgänge und Dashboards.

Workflows für Suchvorgänge
Erstellen und kombinieren Sie mehrere Abfragen in einer Aktion.

Management der Teams
Überwachen Sie den Zugriff auf Entitäten und Funktionalitäten. Dies umfasst auch die LDAP-/Active Directory-Integration.

Sprechen Sie mit unseren Experten und erleben Sie Graylog Enterprise in Aktion

Verlassen Sie sich nicht nur auf unser Wort! Graylog ist der Meinung, dass Sie die Möglichkeit haben sollten, Antworten auf alle Ihre Fragen zu erhalten – noch bevor Sie sich zu einem Kauf entschließen. Deshalb bieten wir Produktdemos an, die Ihnen einen umfassenden Einblick in den Leistungsumfang unserer Lösung geben und ausreichend Zeit für Fragen und Antworten lassen. Überzeugen Sie sich selbst, wie einfach es ist, Logdaten nahtlos zu erfassen, zu normalisieren und zu überwachen, um Leistungsprobleme zu identifizieren.

graylog
ENTERPRISE

Graylog Enterprise ist nicht nur eine CLM-Lösung, sondern der beste Freund Ihres IT-Ökosystems. Werden Sie noch heute Teil der Revolution im Logdaten-Management.

ÜBER GRAYLOG

Graylog unterstützt Security-Teams mit hochmodernen, skalierbaren Lösungen, die die Erkennung von Bedrohungen, deren Untersuchung sowie die Reaktion darauf (TDIR) schneller, intelligenter und effizienter gestalten. Damit sind Unternehmen den sich ständig weiterentwickelnden Cyberbedrohungen immer einen Schritt voraus. Graylogs Algorithmen für maschinelles Lernen verbessern die Erkennung von Anomalien, während KI-gestützte Reports zu den Untersuchungen sowie Empfehlungen für Abhilfemaßnahmen es Security-Teams ermöglichen, schnell und präzise auf sicherheitsrelevante Vorfälle zu reagieren. Die skalierbaren und kostengünstigen Lösungen von Graylog werden von großen Unternehmen wie auch kleineren Teams gleichermaßen geschätzt und ermöglichen ein effizientes Logdaten-Management und optimierte Sicherheitsprozesse. Mit seinen Open-Source-Wurzeln und über 50.000 Installationen weltweit sorgt die Produktsuite von Graylog – Graylog Enterprise, Graylog Security, Graylog API Security und Graylog Open – dafür, dass sich Security-Teams auf das Wesentliche konzentrieren können: den Schutz ihrer Systeme. Weitere Informationen finden Sie auf unserer Website graylog.com. Gerne können Sie uns auch über X (Twitter) und LinkedIn kontaktieren.

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

graylog