Graylog Security

Stärken Sie Ihre Cybersicherheit mit hochentwickelter SIEM-Technologie

Graylog Security ist eine skalierbare Cybersecurity-Lösung, die Security Information and Event Management (SIEM), Threat Intelligence, Funktionen zur Erkennung von Anomalien und effizientes Datenmanagement kombiniert, um Ihren Sicherheitsexperten die Erkennung, Untersuchung und Reaktion auf Cyberbedrohungen zu erleichtern. Sie können Graylog Security entweder selbst im eigenen Unternehmen betreiben oder als Service nutzen (SaaS).

SIEM richtig gemacht

Unternehmen mit begrenzten Ressourcen benötigen eine kostengünstige und proaktive Lösung für die Erkennung von Bedrohungen, die Analyse von sicherheitsrelevanten Vorfällen, die Reaktionsmaßnahmen sowie Compliance-Berichte, um ihr Sicherheitsniveau zu erhöhen. Graylog Security basiert auf der Graylog-Plattform und kombiniert das Logdaten-Management, die Erkennung von Bedrohungen, Empfehlungen für Abhilfemaßnahmen sowie Reports, die einfach umzusetzen, zu verwalten und zu nutzen sind. Wir haben unsere Security-Plattform so konzipiert, dass sie alle Funktionalitäten bietet, die Sie benötigen – ohne die Komplexität und Kosten herkömmlicher SIEM-Lösungen.

Graylog Security im Überblick

Sicherheitsorientierte Workflows

Dank der einzigartigen, auf Sicherheit ausgerichteten Workflows von Graylog Security können Sie Ihre Produktivität und Effizienz steigern. Dabei profitieren Ihre Analysten von einem unmittelbaren Zugriff auf Untersuchungen, Alerts und Reporting-Funktionen.

Die wichtigsten Vorteile von Graylog Security

- Sie erkennen sofort, welche Assets (Maschinen/Benutzer) das größte Risiko darstellen, wenn Sie Ihre TDIR-Arbeiten priorisieren (TDIR: Threat Detection, Investigation and Response).
- Optimieren Sie die Nutzung von Logdaten von geringerem Wert, wobei diese für zukünftige Incident-Untersuchungen gespeichert werden.
- Erhalten Sie kontextbezogene Einblicke für Incident-Response-Berichte, die die wichtigsten Stakeholder informieren.
- Verstehen Sie im Rahmen der Incident-Untersuchungen schnell die zeitlichen Zusammenhänge bestimmter Events.
- Verschaffen Sie sich einen visuellen Überblick über Ihre aktuelle Bedrohungsabdeckung und schließen Sie schnell etwaige Lücken.

Risikobasierte Bewertung

Konzentrieren Sie sich mit einer automatisierten risikobasierten Bewertung auf die aktuellen Risiken. Graylog Security weist Warnmeldungen einen Risikowert zu, sodass Analysten sicherheitsrelevante Vorfälle sehr einfach priorisieren können.

Blitzschnelle Suche für forensische Analysen und Troubleshooting

Jede Sekunde zählt, wenn Sie Ihre IT-Umgebung vor Cyberbedrohungen schützen möchten. Graylog Security ist darauf ausgelegt, Terabytes an Daten in Sekundenschnelle zu analysieren, damit Sie wichtige Logdaten in Echtzeit finden können. Über ein einfaches Dropdown-Menü können Sie schnell auf bisherige Suchanfragen zugreifen.

Anomalie-Erkennung, die Sinn ergibt

Sichern Sie sich einen Vorsprung und wehren Sie Bedrohungsakteure und Cyberkriminelle ab. Die Funktionen zur Anomalie-Erkennung in Graylog Security basieren auf einer leistungsstarken Anomaly-Detection-Engine, die maschinelles Lernen (ML) nutzt, Ihre Umgebung automatisch versteht und Sie auf anomales Verhalten Ihrer Benutzer und Entitäten aufmerksam macht (UEBA: User and Entity Behavior Analytics).

Identifizieren Sie wichtige sicherheitsrelevante Events in einer Flut von Warnmeldungen

Es muss nicht schwierig sein, das Rauschen großer Datenmengen an bedeutungslosen Informationen zu durchdringen, um schnell an die benötigten Daten zu gelangen. Die Alert-Engine von Graylog Security erleichtert es Ihnen, das Rauschen herauszufiltern, damit Sie sich auf die wirklich wichtigen sicherheitsrelevanten Ereignisse konzentrieren können. Dies senkt die Alarmmüdigkeit (Alert Fatigue) und steigert die Produktivität.

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 Graylog diese verarbeitet. Sie können Ihre Standby-Daten selektiv wiederherstellen und in nützliche Informationen für zukünftige Untersuchungen verwandeln.

Folgen Sie den Breadcrumbs der Untersuchungen visuell

Graylog Security bietet einen Überblick über eine Untersuchung in einem kompakten Widget, das sich sehr einfach anpassen lässt. Analysten erhalten damit eine dynamische Echtzeit-Visualisierung des Untersuchungsverlaufs und eine umfassende Zeitleistenansicht der Security-Untersuchung – vom Beginn bis zur Lösung.

Verstehen Sie Ihre Bedrohungsabdeckung

Graylog Security bietet einen Echtzeit-Einblick in den Status Ihrer Bedrohungsabdeckung in Bezug auf die in der MITRE ATT&CK-Matrix beschriebenen Taktiken und Techniken. Sie sehen sofort, welche Sigma-Regeln derzeit in Ihrer Umgebung aktiviert sind. Indem Sie zusätzliche Regeln aktivieren können Sie Ihr Sicherheitsniveau erhöhen und Ihre Bedrohungsabdeckung auf Basis der Empfehlungen von Graylog verbessern.

Wie gut sind Sie aufgestellt, um Risiken zu minimieren?

Machen Sie sich mit Graylog Security ein Bild von Ihrer Cyberresilienz: Messen Sie kritische Sicherheits-KPIs, die aufzeigen, wie effektiv Sie Risiken mindern, damit Sie wissen, worauf Sie sich bei Ihren Optimierungsmaßnahmen konzentrieren müssen.

Senken Sie die TCO und stärken Sie gleichzeitig Ihre Sicherheit

Die cloudnativen Funktionen, die intuitive Benutzeroberfläche und die vordefinierten Inhalte von Graylog Security ermöglichen es, dass Sie – im Vergleich zu herkömmlichen SIEM-Lösungen – schneller wertvolle Informationen aus Ihren Logdaten gewinnen können. Senken Sie Ihren Arbeitsaufwand und Ihre Kosten mit Funktionen, die die Alarmmüdigkeit deutlich reduzieren, schnell Antworten liefern und Ihre Sicherheitsexperten optimal unterstützen. Nutzen Sie eine „warm Tier" (eine zusätzliche Zwischenebene), auf der die Daten abgelegt werden, um von kostengünstigeren Remote- oder On-Premises-Speicheroptionen zu profitieren und gleichzeitig dieselben blitzschnellen und robusten Suchfunktionen zu nutzen.

Leistungsstarke, blitzschnelle Funktionen

Anomalie-Erkennung/UEBA
Graylog Security bietet Funktionen, die schnell „normales" Verhalten erlernen und automatisch Abweichungen für Nutzer und Entitäten in jeder Größenordnung erkennen – mit kontinuierlicher Feinabstimmung und Verbesserung im Laufe der Zeit.

Compliance-Reports
Nutzen Sie die Dashboard-Funktionalitäten von Graylog, um Ihre planmäßigen Reports auf einfache Weise zu erstellen und zu konfigurieren.

Data-Routing
Lagern Sie Daten von geringerem Wert in ein Data Warehouse aus, bevor Sie diese nach einer selektiven Wiederherstellung zu einem späteren Zeitpunkt weiterverarbeiten.

Zusammenfassender Bericht zu Untersuchungen
Sie können GenAI nutzen, um Beweisstücke zusammenzufassen und so kontextbezogene Einblicke für IR-Berichte zu liefern, die zur Information wichtiger Stakeholder dienen.

Untersuchung von sicherheitsrelevanten Vorfällen
Der All-in-One-Workspace ermöglicht es, Datenbestände, Berichte, Beweise und andere kontextbezogene Informationen während der Untersuchung eines möglichen Vorfalls zu sammeln und zu organisieren.

Vordefinierte Dashboards und Warnmeldungen
Mit den vordefinierten Inhalten für spezifische Use Cases können Sie sofort durchstarten. Graylog bietet unter anderem Suchvorlagen, Dashboards, korrelierte Warnmeldungen sowie dynamische Nachschlagetabellen.

Risikobasierte Bewertungen
Konzentrieren Sie sich bei Ihrer Arbeit auf diejenigen Ereignisse und Probleme, die sich auf die Assets (Benutzer/Maschinen) mit dem höchsten Risiko beziehen.

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

SOAR-Integrationen
Stellen Sie Ihre Daten ganz einfach anderen geschäftskritischen Systemen zur Verfügung, um vollständige Transparenz zu schaffen und eine optimale Zusammenarbeit zu gewährleisten.

Widget für Einblicke in die Bedrohungsabdeckung
Visualisieren Sie die Bedrohungsabdeckung, die das MITRE ATT&CK-Framework nutzt und die darin beschriebenen Taktiken und Techniken abbildet.

Widget für Untersuchungen inklusive Zeitleiste
Graylog ermöglicht die leicht verständliche, zeitbasierte Visualisierung einer Untersuchung.

Einbindung von Schwachstellen-Scans
Nessus- und MS Defender-Scans werden zur Berechnung genauerer Risikobewertungen herangezogen.

graylog SECURITY

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

Überzeugen Sie sich selbst! Graylog möchte, dass Sie Antworten auf alle Ihre Fragen erhalten, bevor Sie sich für unsere Lösung entscheiden. Wir bieten Ihnen Produktdemos an, die die Funktionalitäten unserer Lösung aufzeigen und ausreichend Zeit für Fragen und Antworten bieten. Vereinbaren Sie noch heute einen Termin für eine Graylog Security-Demo und erleben Sie unsere leistungsstarke Cybersecurity-Plattform in Aktion.

Graylog Security ermöglicht Ihnen Einblick in Ereigniskorrelationen über Zehntausende von Netzwerkkomponenten hinweg hinsichtlich identifizierter Bedrohungen oder verdächtiger Aktivitäten.

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