GRAYLOG SECURITY

Gain Actionable Insight into Your Cybersecurity Posture

graylog SECURITY

Delivered to you in a self-managed or SaaS experience, Graylog Security is a scalable cybersecurity solution that combines Security Information and Event Management (SIEM), threat intelligence, incident investigation, and anomaly detection capabilities to help your security professionals simplify identifying, researching, and responding to cyber threats while continuously strengthening your security posture.

A Comprehensive, Powerful Cybersecurity Platform for the Mid-Enterprise

Resource-constrained organizations need affordable and proactive threat detection, incident analysis, and response, and compliance reporting to strengthen their security posture. Graylog Security combines centralized log management, threat detection, data normalization, correlation, and reporting that's easy to deploy, manage, and use. We've designed our security platform to provide the functionality you need without the complexity and cost of traditional SIEM solutions.

GRAYLOG SECURITY AT A GLANCE

Intuitive UI and User Workflows

Graylog Security comes pre-configured with robust point- and-click visualizations, search templates, investigation workflows, and an intuitive alert and correlation customi- zation wizard, all to help you increase visibility into your environment and quickly identify important or suspicious patterns in machine data as you hunt for cyberthreats.

GRAYLOG SECURITY BENEFITS

- Scour volumes of data in seconds with lightning-fast search capabilities
- Focus security efforts on what matters by filtering out alert noise
- Increase productivity with automation you can trust for repetitive and security-intensive tasks
- Leverage an anomaly detection ML engine that continuously learns your security behaviors over time

NO LOG LEFT BEHIND

Collecting logs from different sources can feel like herding cats if you don't have the right tool. Graylog Security can provide the context you need to make sense of large amounts of log data by automatically collecting, normalizing, and visualizing event log data from sources across your network.

LIGHTNING-FAST SEARCH FOR FORENSIC ANALYSIS AND TROUBLESHOOTING

Every second counts when trying to keep your environment secure and safe from cyber threats. Graylog Security is designed to parse terabytes of data in seconds, allowing you to find important log data in real-time quickly. Out-of-the-box search filters also provide fast data refinement.

ANOMALY DETECTION THAT MAKES SENSE

Stay ahead by keeping bad actors out. Graylog Security anomaly detection capabilities are designed with a powerful Machine Learning (ML) anomaly detection engine that can automatically understand your environment and alert you on what's not normal behavior for your users and entities (UEBA).

IDENTIFY PRIORITY SECURITY EVENTS IN A SEA OF ALERTS

Cutting through the noise to get to the data you need quickly doesn't have to be difficult. The Graylog Security alert engine makes it easy to filter out the noise so you can focus on the security events that really matter, reducing alert fatigue and maximizing productivity.

DEDICATED WORKSPACE FOR INCIDENT INVESTIGATIONS

Easily manage incident investigations from start to finish in Graylog Security with an all-in-one workspace to collect and organize datasets, reports, evidence, and other context while investigating a potential incident or issue, collaborate across teams throughout the entire investigation process, and quickly identify trends by using data saved from prior investigations.

S.O.A.R. WITH GRAYLOG SECURITY

Graylog Security can seamlessly integrate with your existing Security Orchestration, Automation, and Response (S.O.A.R.) platforms to collect log and security data and automatically initiate workflows from the correlation alerts that Graylog Security provides, helping you drastically reduce time to resolution (TTR) metrics.

NO TRAINING REQUIRED

Graylog Security's easy-to-learn interface is designed to facilitate collaboration and encourage the re-use of past work. There is no need to learn SQL or any proprietary query language or run multiple searches to find the data you need. Anyone on your team can quickly start using Graylog Security.

REDUCE TCO WHILE STRENGTHENING YOUR SECURITY

Graylog Security's cloud-native capabilities, intuitive UI, and out-of-the-box content means you can start getting valuable data from your logs quicker when compared to legacy SIEMs. Lower your labor costs with features designed to significantly reduce alert fatigue, get answers fast, and empower your security professionals.

POWERFUL, LIGHTNING-FAST FEATURES

ANOMALY DETECTION / UEBA

Capabilities that quickly learn "normal" behavior and automatically identify deviations for users and entities at scale, with continuous fine-tuning and improvement over time.

COMPLIANCE REPORTING

Leverage Graylog's dashboard functionality to easily build and configure scheduled reports.

CORRELATION AND ALERTING

Receive alerts via email, text, Slack, and more. Update alert criteria based on a dynamic list in a lookup table.

DATA NORMALIZATION AND ENRICHMENT

Perform faster research by adding WHOIS, IP Geolocation, threat intelligence, or other structured data.

GRAYLOG USER LOGS

Track who accessed what log data and what actions they took against it to ensure compliance and security.

INCIDENT INVESTIGATION

All-in-one workspace to collect and organize datasets, reports, evidence, and other context while investigating a potential incident.

PREBUILT DASHBOARDS, ALERTS

Start fast with prebuilt content — search templates, dashboards, correlated alerts, dynamic look-up tables, and more.

SEARCH QUERY BUILDER

Build and combine multiple searches for any type of analysis into one action and export results to a dashboard.

SECURITY ANALYTICS DASHBOARDS

Combine widgets to build customized data displays and automate the delivery of reports to your inbox.

SIGMA RULES

Easily import Sigma Rules to strengthen cyber incident detection and provide additional context for MTTR activities.

S.O.A.R. INTEGRATIONS

Easily share data with other business-critical systems for full transparency and collaboration.

THREAT INTELLIGENCE FEEDS

Add context to event log data with your existing threat intelligence feeds and pinpoint potential security issues.

graylog
SECURITY

ASK OUR EXPERTS AND SEE GRAYLOG SECURITY IN ACTION

Seeing is believing. At Graylog, we want you to get all your questions answered before you buy. We offer scheduled product demos that demonstrate product functionality and allow time for Q&A. **Schedule your Graylog Security demo today** and see our powerful cybersecurity platform in action.

Graylog Security allows you to gain insight into event correlations across tens of thousands of network components for identified threats or suspicious activity.

ABOUT GRAYLOG

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.