graylog SECURITY

SIEM Without Compromise

No More Trade-Offs. Just Results.

Security teams shouldn't have to choose between visibility, speed, and cost. Graylog Security delivers everything you need for modern threat detection and response—without compromise. Whether you're a lean security team or a large enterprise SOC, Graylog empowers you to detect real threats faster, streamline investigations, and eliminate data tax fatigue.

What Sets Graylog Security Apart

Risk-Based Alerting
Prioritize real threats based on context like asset criticality and adversary intel.

Deploy Anywhere
Cloud, on-prem, or hybrid—with the same powerful experience.

Adversary Campaign Intelligence
Tie alerts to known campaigns for deeper insight and better triage.

No-Compromise Data Retention
Preview, store, and restore logs without surprise costs.

Threat Coverage Analyzer
See what you're protected against and where to improve—instantly.

Faster Investigations
Pivot-to-search, automated workflows, and compact timeline widgets.

Designed for Security Analysts, Built for CISOs, and Loved by Admins

Security Analysts	SIEM Architects/Admins	CISOs
• Cut through the noise with high-fidelity alerts • Investigate faster with guided workflows • See the full attack story, not just the blips	• Easy setup for fast time-to-value with input wizard and pre-built content onboarding • API-ready, extensible, Sigma 2.0 compatible • Route data smartly, not expensively	• Complete visibility, no guesswork • Predictable pricing and strategic insights • Reduce risk, not just respond to it

Feature Highlights

graylog SECURITY

Threat Detection & Prioritization Risk-Based Alerting

- Asset-based Risk Scoring Model
- Adversary Campaign Intelligence
- Anomaly Detection / UEBA
- Vulnerability Scan Ingest

Faster Investigation & Response

- Pivot-to-Search Timeline Widget
- Investigation Summary Reports (GenAI-enhanced)
- Prebuilt Dashboards & Alerts
- Incident Investigation Workspace

Security Coverage & Compliance

- Threat Coverage Widget (MITRE-mapped)
- Security Analytics Dashboards
- Compliance Reporting & Scheduled Reports
- Native SOAR & 3rd Party Integrations

Cost-Efficient Log Management

- Data Routing to Data Warehouse
- Selective Retrieval from Cold Storage
- Lightning-Fast Search at Scale
- Transparent, Flexible Licensing

Built for Scale & Simplicity

- Cloud-native or On-Prem Deployment
- Sigma 2.0 Rule Support
- API-First Architecture
- MSSP-Ready Multi-Tenancy

Prebuilt Detection Content (Illuminate)

- Content Hub with Illuminate Packs
- MITRE ATT&CK Mapping
- Source-Aware Recommendations
- Continuously Updated Rule Library

See Graylog Security in Action

Schedule a live demo today to explore how you can reduce costs, time to insight, and future-proof your log strategy — **without compromise**.

graylog.com /see-demo

ABOUT GRAYLOG

Graylog delivers a SIEM that works the way teams actually need: full visibility, real detection, and faster investigations—without blowing the budget. Trusted by 50,000+ organizations worldwide, Graylog helps analysts skip the noise and get to what matters. Automate the heavy lifting. Stay focused on real threats. Learn more at graylog.com or connect with us on Bluesky and LinkedIn.

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

graylog