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 needed for modern threat detection and response without compromise.Whether supporting a lean security team or a large enterprise SOC, Graylog empowers analysts to detect verified threats quickly, streamline investigations with guided AI workflows, and control data costs with selective ingestion.

## What Sets Graylog Security Apart

### Risk-Based Alerting

Prioritize threats using risk scoring, asset context, and adversary intelligence.

### Deploy Anywhere

Cloud, on-prem, or hybrid with the same powerful experience and API-driven design.

### Adversary Campaign Intelligence

Link detections to known attack campaigns for faster, more accurate triage.

### No-Compromise Data Retention

Preview, filter, and retrieve logs selectively to keep costs predictable without losing visibility.

### Threat Coverage Analyzer

Measure detection coverage against MITRE techniques and identify improvement opportunities instantly.

### Faster Investigations

AI-generated summaries, incident timelines, guided remediation steps, and shareable reports.

## Built for Analysts, Trusted by SOC Leaders, and Valued by CISOs

| Security Analysts | SIEM Architects/Admins | CISOs |
|---|---|---|
| • Cut alert fatigue with high-fidelity detections<br>• Get plain-language summaries of dashboards and alerts<br>• Investigate faster with guided workflows and AI timelines<br>• Share incident case summaries and AI-written reports | • Rapid setup with Input Wizard and prebuilt content packs<br>• Schema-aware data onboarding with minimal rework<br>• Route data by policy and cost using preview & selective retrieval<br>• API-ready, Sigma 2.0 compatible, extensible at scale | • Gain clarity with dashboards that highlight what matters<br>• Predictable pricing with license and storage controls<br>• Reduce investigation costs and time to respond<br>• Maintain control of AI with MCP guardrails and BYO models |

# Feature Highlights

graylog SECURITY

## Threat Detection & Prioritization Risk-Based Alerting

- Entity and asset-based risk scoring
- Adversary Campaign Intelligence
- Anomaly Detection and UEBA
- Vulnerability and asset ingest

## Faster Investigation & Response

- AI-generated summaries of dashboards & alerts
- Pivot-to-search & compact Timeline Widget
- Incident Investigation Workspace with replay and evidence tracking
- AI-written incident reports with prioritized steps
- Guided remediation instructions embedded in alerts

## Cost-Efficient Log Management

- Data Routing and Filtering for smart ingest
- Preview and Selective Retrieval from AWS Security Data Lake
- Lightning-fast search across hot, warm, and archive tiers
- Predictable, transparent licensing

## Security Coverage & Compliance

- Threat Coverage Widget mapped to MITRE ATT&CK
- Security and compliance dashboards with thresholds
- Automated and scheduled reports for audits
- Integrations with SOAR, ITSM, and third-party platforms

## Prebuilt Detection Content

- Continuously updated content packs with ready-to-use detections
- MITRE ATT&CK mapping for coverage tracking
- Source-aware recommendations for faster onboarding
- Out-of-the-box dashboards, alerts, and workflows

## Built for Scale & Simplicity

- Deploy in cloud, on-prem, or hybrid environments
- Manage departments and regions easily with flexible role-based access
- API-first design with Sigma 2.0 rule support
- MCP integration for bring-your-own AI models with Graylog guardrails

# See Graylog Security in Action

Schedule a live demo today to see how you can cut costs, speed investigations, and strengthen detection strategy — **without compromise**.

**graylog.com /see-demo**

## ABOUT GRAYLOG

Graylog delivers a SIEM designed around how security teams actually work: full visibility, explainable AI-driven insights, and faster investigations without unpredictable costs. Trusted by more than 50,000 organizations worldwide, Graylog helps analysts move from raw data to confident action with less effort. Automate the repetitive tasks. Keep focus 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