graylog SECURITY

# The SIEM FOR LEAN TEAMS

Security teams need full detection and response capability without the complexity, cost, or tuning overhead that makes enterprise SIEM impractical. Graylog Security delivers the coverage, automation, and analyst experience that lean teams require to stay ahead of real threats.

## What Sets Graylog Security Apart

### Smarter Detection, Less Noise

Correlates entity behavior, asset risk, and live threat campaigns to surface only the alerts that demand attention. Analysts investigate. They do not filter.

### Fast Time to Value

68 alerts, 42 reports, and 7 dashboards ship ready at deployment. Measurable threat coverage from day one, with no custom rules required.

### Deploy Anywhere, Without Trade-Offs

Cloud, on-prem, or hybrid with identical capabilities across every model. Built-in MCP server access included at no extra cost across all tiers.

### Predictable Retention Costs

A built-in data lake stores years of logs outside your active license. Preview and retrieve only what an investigation requires.

## Built for Analysts, Trusted by Security Leaders

| Security Analysts | SIEM Architects/Admins | CISOs |
|---|---|---|
| • High-fidelity detections surface only the alerts that require attention<br>• Open an investigation and find every related event already pre-loaded<br>• Move from alert to action faster with consolidated remediation procedures<br>• Share AI-written case summaries without leaving the platform | • Go live with coverage across 7 attack surfaces for coverage of top 10 threats on day one<br>• Onboard new data sources with schema-aware parsing and minimal rework<br>• Route data by policy and cost to eliminate over-ingestion<br>• Eliminate manual tuning with dynamic shard sizing and parallel restore jobs | • Surface the risks that matter most without wading through noise<br>• Control licensing and storage costs with no surprise invoices<br>• Reclaim analyst shift time lost to manual triage and case assembly<br>• Audit-ready incident reports generated automatically at case closure |

# Feature Highlights

graylog SECURITY

## Threat Detection & Prioritization

- Native Impossible Travel and Log Volume detectors surface behavioral threats that rule-based detection misses
- Tunable anomaly detection with debug output showing exactly why each detector fired
- Entity-based risk scoring with configurable thresholds by asset group, including separate scoring for privileged accounts
- Sigma rule import from private GitHub, GitLab, and Bitbucket repositories with full version control

## Faster Investigation & Response

- Risk score threshold breach automatically creates an Investigation with related events and logs pre-loaded
- Consolidated remediation steps from every alert surfaced in one procedure list, no SOAR required
- AI-written incident reports generated at case closure, including timelines, evidence lists, and audit-ready documentation
- Event status syncs across all attached evidence when Investigation status changes

## Cost-Efficient Log Management

- Built-in data lake stores standby logs outside the active license with data preview and selective retrieval included
- Parallel archive restore jobs run simultaneously, cutting recovery from weeks to hours
- Azure Blob Storage fully supported for archives, warm tier, and Data Lake
- Transparent, analysis-based pricing with no per-GB ingest fees

## Security Coverage & Compliance

- 68 prebuilt alerts, 42 reports, and 7 dashboards covering the top 10 security threats ship ready at deployment
- Entity table Slice-By filters alerts and events by type, priority, owner, status, and risk score in one click
- Bulk add multiple log messages to an Investigation in a single action from any log view
- MCP server access included at no extra cost across all tiers, with bring-your-own-LLM support

# 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 is the AI-powered SIEM and centralized log management platform trusted by 60,000+ organizations worldwide. By combining scalable log management, real-time correlation, and explainable AI, Graylog turns overwhelming data into clear insight and confident action. **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