GRAYLOG ILLUMINATE

OUR EXPERTISE. YOUR SUCCESS.

Graylog provides a powerful, flexible, and seamless centralized log management experience. IT, Security, and DevOps teams can manage operations, explore data, trace errors, detect threats, quickly and easily find meaning in the data, and take actions faster. As a result, our customers enjoy increased productivity, improved performance, secure systems, and an empowered team.

Paired with Graylog Enterprise or Graylog Cloud, customers can start fast with pre-built content that normalizes all data, regardless of source, giving you consistency in reporting, alerting, and analysis, plus the power to easily correlate data across different types of data sources.

START FAST WITH PREBUILT CONTENT FOR GRAYLOG ENTERPRISE AND GRAYLOG CLOUD.

AUTHENTICATION

- Easily correlate authentication data across different types of data sources.
- Gain visibility into who is trying to log into what throughout your IT environment.

NETWORKS

- Monitor and analyze the data, identify any malicious activity occurring within your network.
- Isolate the source of the activity and quickly respond to the threats.

APPLICATIONS

- Eliminate the manual setup necessary to detect, monitor, and analyze application issues across your IT infrastructure.
- Visualize your application data in pre-built dashboards and drill down for details and deeper insights.

HELP ME SEE MY DATA

Graylog Schema is a blueprint for how we map data fields to a standardized field name in the product, allowing for pieces of Graylog to be developed more generically and across many technologies.

CORRELATED ALERTS

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

DYNAMIC LOOKUP TABLES

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

INTERACTIVE DASHBOARDS

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

SCHEDULE REPORTS

Enter one or more criteria for a more comprehensive search. Easily save and share regularly run searches.

SEARCH TEMPLATES

Enter one or more criteria for a more comprehensive search. Easily save and share regularly run searches.

STREAMS & PIPELINES

Route log messages into categories in real time and control data processing by tying streams to your pipelines.

GRAYLOG ILLUMINATE CONTENT

Gain insights about cybersecurity and compliance.

ILLUMINATE CORE

Dashboards

- Device Investigation Drill Down
- Enterprise Authentication
- Account Investigation Drill Down

Processing

- 12 x Pipelines
- 81 x Pipeline Rules
- 11 x Lookup Tables

O365 SPOTLIGHT

- Illuminate O365

PALO ALTO 9

Dashboards

- Palo Alto Summary — Threat Activity
- URL Filtering
- Network Activity
- Global Protect Activity

Processing

- 1 x Pipeline
- 18 x Pipeline Rules
- 1 x Lookup Table

OKTA

Dashboards

- Okta

Processing

- 1 x Pipeline
- 11 x Pipeline Rules
- 3 x Lookup Tables

WINDOWS

Dashboards

- Authentication
- Identity and Access Management
- Processing

Processing

- 1 x Pipeline
- 11 x Pipeline Rules
- 13 x Lookup Tables

SYSMON

Dashboards

- Overview
- User Investigation Drill Down
- Process Investigation Drill Down — Host Investigation Drill Down

Processing

- 5 x Pipelines
- 87 x Pipeline Rules — 1 x Saved Search
- 1 x Lookup Tables

EVENTS

Core

- Logins from different countries in time window
- Potential Brute Force Attack
- Potential Password Spraying Detection

Windows

- Multiple accounts Locked Out
- Login failed due to accessing an unauthorized host
- Security log cleared
- Multiple Accounts Locked Out
- Detect built-in administrator attempting network login
- Windows: Detect weak Kerberos ticket requests

GRAYLOG ENTERPRISE AND GRAYLOG CLOUD

POWERFUL, LIGHTNING-FAST FEATURES

ARCHIVING

Store older data on slow storage and easily re-import it into Graylog when you need it.

CONTENT PACKS

Share configurations of extractors, inputs, pipelines, dashboards and more. Move easily from Test to Production.

CORRELATED ALERTS

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

DYNAMIC LOOKUP TABLES

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

FORWARDER

Easily send data to Graylog Cloud or to an on-premise Graylog Server installation.

INTERACTIVE DASHBOARDS

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

LOG VIEW

View data in real-time, ensure continued availability, streamline investigations.

PARAMETERIZATION

Enter one or more criteria for a more comprehensive search. Easily save and share as templates.

PIPELINES

Set rules for data processing to ensure the right parser, data enrichment and lookup table(s) are applied.

REST API

Easily integrate your data into 3rd party systems to automate reporting, workflow and research.

SCALABLE SEARCH

Build complex queries in minutes with Graylog's web console—no proprietary query language needed.

SCHEDULE REPORTS

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

SEARCH WORKFLOW

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

STREAMS

Categorize log messages in real-time to easily target queries, reports and dashboards for faster results.

TEAMS MANAGEMENT

Control entity access and capabilities. Includes LDAP/Active Directory integration.

USER AUDIT LOGS

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

ABOUT GRAYLOG

Graylog is a leading log management solution that hundreds of thousands of IT professionals across the globe rely on every day. With a focus on security, compliance, operations, and DevOps, Graylog delivers a better user experience by making analysis ridiculously fast and efficient using a more cost-effective and flexible architecture. Purpose-built for modern log analytics, Graylog removes complexity from data exploration, compliance audits, and threat hunting so users can quickly and easily find meaning in data and act faster.