G-Cloud 15 Service Description

Graylog Security Cloud

Cloud21
A Tegria Company

Table of Contents

1. Proposed Services Delivered

12 month to 3 year options available for:

- Cloud Software – **Graylog Security Cloud** (alternative Self-Hosted option available)
- Cloud21 Monthly Health Checks – 1 day per month
- Cloud21 Graylog Managed Alerts service – Lite package 1 day per week, standard 5 day per week (and any options in between)

One off options:

- Cloud21 Self Hosted update support package (2 day)

2. Overview

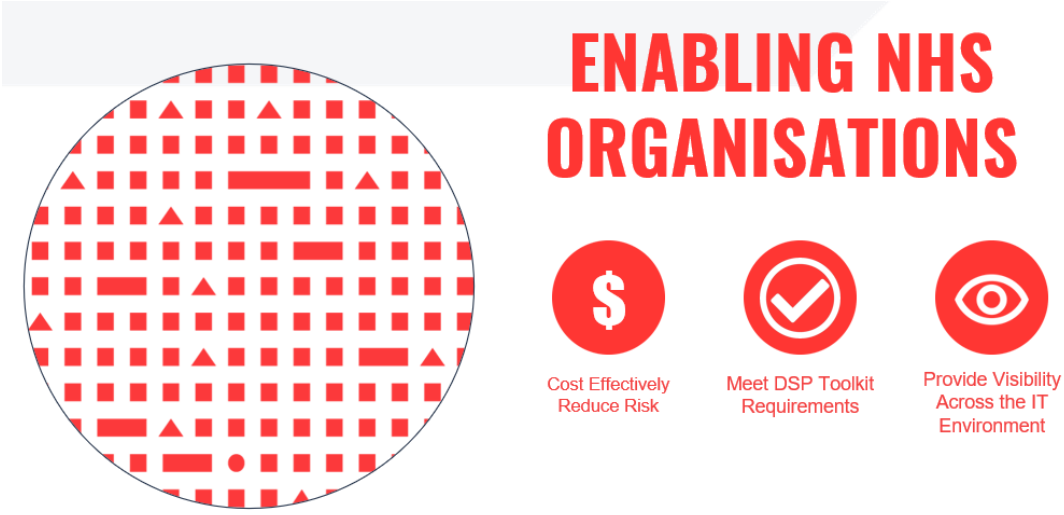
Data. Insights. Answers.

Deployed in more than 60,000 installations worldwide, Graylog is an award-winning solution built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog enables hundreds of thousands of users to explore their data every day to solve security, compliance, operational, and application development issues.

Graylog elevates cybersecurity through its comprehensive SIEM, Centralized Log Management, and API Security solutions, providing the edge in Threat Detection & Incident Response (TDIR) across diverse attack surfaces. The company's unique blend of AI/ML, advanced analytics, intuitive design, and providing the best Analyst Experience (AX) makes cybersecurity smarter, not harder.

What You Can Do with Graylog Security:

• Collect log data from across your entire environment
• Scour volumes of log data in seconds with lightning-fast search
• Easily create dashboards from search queries for regular review
• Reduce alert fatigue to focus security efforts on what matters
• Increase productivity with automation for repetitive and security-intensive tasks
• Leverage AI capabilities that continuously learn your behaviours
• Seamlessly integrate with the rest of your SOC tech stack
• Demonstrate your cybersecurity resilience to audit & regulatory compliance bodies



Why Graylog for the NHS?

- Centralised logging requirement for DSPT met
- Cloud21 managed alerts service to triage / escalate / monthly reporting
- Cloud21 support in developing Security and Operational dashboards
- Commercially competitive product
- Available as a Cloud solution (Cloud First) or On-Premise
- Reduce risk of breaches
- Aids forensic analysis in the event of a breach
- Fast to set up and simple to enable

Common NHS use cases:

- Brute Force Attack
- Lateral Movement
- Malware Outbreak
- Insider Threat Detection
- Network Monitoring
- Sensitive Data Exfiltration
- Medical Device Monitoring
- Top 10 Support Desk Queries
- DSPT Compliance
- Exploitation of Legacy Equipment

graylog

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.

ASSET ENRICHMENT
Gain insight across your environment with the ability to track different assets and enrich log messages with additional information.

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.