ENTERPRISE LOG MANAGEMENT MIT GRAYLOG & OPENSEARCH

This solution provides a scalable and powerful enterprise logging platform that enables centralised log collection, analysis, normalisation, alerting and storage. The system relies on proven open source technologies:

- Graylog for processing and analysing log data
- OpenSearch as a high-performance search and storage solution
- Ingress proxy for secure and redundant log acceptance

KEY FEATURES

- Scalable 3-tier architecture (proxy, Graylog Core, OpenSearch backend)
- Support for structured and unstructured logs
- Normalisation & enrichment of logs with metadata
- Rule-based alerts and notifications
- Full-text search & dashboards (OpenSearch)
- TLS-protected communication
- Support for Syslog, GELF, Beats, REST and much more.
- Multi-client capability & role-based user control
- Compatible with SIEM/SOC infrastructures

SERVICE DESCRIPTION

- Planning and architecture of the log management infrastructure
- Provisioning the Ingress proxy (e.g. Nginx with TLS and reverse proxy)
- Installation & Konfiguration von Graylog Nodes
- Setting up pipelines for enrichment & normalisation
- Rule definition for alarms (e.g. for login errors, critical events)
- Integration of OpenSearch as storage backend
- Creation of dashboards and alerts
- Documentation & Training
- Rollout & Support

SERVICE
WORLD OF FORENSICS