ENTERPRISE LOG MANAGEMENT MIT GRAYLOG & OPENSEARCH

Diese Lösung stellt eine skalierbare und leistungsfähige Enterprise Logging-Plattform bereit, die sowohl zentrale Log-Aufnahme als auch Analyse, Normalisierung, Alarmierung und Speicherung ermöglicht. Das System setzt auf bewährte Open-Source-Technologien:

- Graylog zur Verarbeitung und Analyse von Logdaten
- OpenSearch als hochperformante Such- und Speicherlösung
- Ingress Proxy zur sicheren und redundanten Log-Annahme

KERNEIGENSCHAFTEN

- Skalierbare 3-Tier-Architektur (Proxy, Graylog Core, OpenSearch Backend)
- Unterstützung strukturierter und unstrukturierter Logs
- Normalisierung & Anreicherung von Logs mit Metadaten
- Regelbasierte Alarmierung und Benachrichtigungen
- Volltextsuche & Dashboards (OpenSearch)
- TLS-geschützte Kommunikation
- Unterstützung von Syslog, GELF, Beats, REST u. v. m.
- Mandantenfähigkeit & rollenbasierte Benutzersteuerung
- Kompatibel mit SIEM-/SOC-Infrastrukturen

LEISTUNGSBESCHREIBUNG

- Planung und Architektur der Log-Management-Infrastruktur
- Bereitstellung des Ingress-Proxys (z. B. Nginx mit TLS und Reverse Proxy)
- Installation & Konfiguration von Graylog Nodes
- Einrichtung von Pipelines zur Anreicherung & Normalisierung
- Regeldefinition für Alarme (z. B. bei Login-Fehlern, kritischen Events)
- Integration von OpenSearch als Speicherbackend
- Anlage von Dashboards und Alerts
- Dokumentation & Schulung
- Rollout & Support

MH SERVICE
WORLD OF FORENSICS