logrok

AI-Driven Secure Log Intelligence Platform

Log intelligence built for classified, air-gapped, and mission-critical networks.
FIPS 140-3 validated. DISA STIG hardened. Zero telemetry. Full operational sovereignty.

What is logrok?

logrok is a self-hosted log intelligence platform purpose-built for security operations. It collects, enriches, indexes, and analyzes log data from your entire infrastructure — servers, network devices, cloud services, and industrial control systems. Deploy as a hardened VM appliance or on Kubernetes. No vendor lock-in. No telemetry. Your data stays yours.

Key Capabilities

1. **Unified Log Collection**
   Ingest from syslog TCP/UDP/TLS, webhooks, cloud APIs, and files. 200K+ EPS on a single node — fewer appliances, lower cost.
2. **Four Search Modes**
   Plain text, regex, Lucene query syntax, and natural-language AI search across billions of events.
3. **Visual Pipeline Editor**
   Drag-and-drop topology builder for log collection pipelines. Generate, deploy, and version configs visually.
4. **Dashboards & Alerting**
   Custom dashboards with live widgets. Alert rules on patterns, thresholds, or anomalies.
5. **AI Noise Filtering**
   Automatically detect repetitive log patterns. Classify, route, or suppress noise to surface actionable events.
6. **Detection Engine**
   25 built-in SQL detection rules with MITRE ATT&CK mapping. Correlation logic and custom rule DSL.
7. **Encrypted Storage & 20+ Destinations**
   AES-256-GCM at rest with per-tenant keys. Route to file, S3, Kafka, Splunk, Elasticsearch, Azure, GCP, Datadog, Loki, and more.
8. **Tamper-Evident Audit Trail**
   Append-only audit log of every platform action. Non-repudiation for compliance and forensic review.
9. **Zero Trust Access Control**
   MFA-ready SSO with FIDO2, YubiKey, CAC/PIV support. Defense-in-depth tenant isolation.
10. **OCSF Classification**
    Events classified to OCSF v1.3 for vendor-neutral detection rules and data lake federation.

200K+	25+	AES-256	FIPS	100%
Events/sec sustained	Detection rules	Encrypted at rest	140-3 compliant	Air-gap capable

Architecture

- **Control Plane**
  REST API + Web UI + AI agent interface. Pipelines, search, alerts, and automation.
- **Ingest Plane**
  High-performance log collector with config agents. Zero-touch pipeline deployment.
- **Data Plane**
  SQL analytics engine, config store with row-level security, SSO, and encrypted local storage.

Deployment

- **VM Appliance**
  FIPS-hardened Linux appliance. Runs on any major hypervisor or bare metal.
- **Kubernetes / k3s**
  Helm charts. Each plane scales independently.
- **Air-Gapped**
  Offline container images. No call-home license activation.
- **Docker Compose**
  Single-host eval in under 5 minutes.

Who It's For

- **Defense & Intelligence**
  FIPS 140-3 (OS-level CMVP certs), DISA STIG, CMMC L2. Full compliance evidence.
- **Critical Infrastructure**
  Air-gapped OT/ICS/SCADA. No cloud dependency. Offline operation.
- **Government / NATO**
  On-prem sovereign data. MFA-ready SSO. LDAP/AD federation support.
- **Enterprise SOC / MSSP**
  Multi-tenant isolation, OCSF detection, 200K+ EPS.

Security Posture

- ✓ FIPS 140-3 validated crypto (NIST CMVP #4823, #4750)
- ✓ DISA STIG + CIS Level 1 hardened OS baseline
- ✓ Zero telemetry — no data exfiltration risk
- ✓ MFA: TOTP, FIDO2/YubiKey, Passkeys, CAC/PIV smart cards
- ✓ Full audit trail — every action logged and attributable
- ✓ No cloud dependency — sovereign on-premises operation

Compliance & Standards

- ✓ NIST SP 800-53 — security controls for federal systems
- ✓ CMMC Level 2 — controlled unclassified information (CUI)
- ✓ DISA STIG — Defense Information Systems Agency benchmarks
- ✓ CIS Level 1 — Center for Internet Security baseline
- ✓ OCSF v1.3 — Open Cybersecurity Schema for allied interop
- ✓ SSO federation — LDAP/AD, SAML 2.0, OpenID Connect

Get Started

- **Evaluation**
  Docker Compose in under 5 minutes. Full feature access.
- **Pilot**
  VM appliance image for on-site evaluation with your data.
- **Production**
  Hardened appliance or Kubernetes with full support.

Contact

Logiqum Kft.
+36 70 731 1133
contact@logiqum.com
logrok.com • logiqum.com

Available for classified environments