RADICL™
THE FUTURE OF CYBERSECURITY

MANAGED LOG ANALYTICS (MLA)

Enterprise SIEM power without the SIEM burden, featuring centralized log collection, AI-assisted search, and an automated 1 year compliance archive, managed 24/7 by the RADICL vSOC.

OVERVIEW

RADICL MLA ingests logs from every corner of your environment — endpoints, servers, cloud, identity, and security tools — and normalizes them into one consistent, searchable schema. Whether you're answering an assessor's question or investigating an active incident, MLA puts your data at your fingertips while RADICL carries the operational load.

KEY CAPABILITIES

COLLECT

Unlimited log sources via API and Syslog, agentless in most environments with no per-connector fees or source limits.

ESCALATE

Spot something suspicious? Escalate in-platform to the RADICL vSOC for expert investigation and incident response.

SEARCH

14 or 90 days of Velocity data, searchable via ES|QL or AI-assisted natural language — no query training required.

MANAGED OPS

All technology, tuning, and ingestion-health monitoring is handled by RADICL 24/7.

WHY TEAMS CHOOSE RADICL MLA

- **Replace an expensive, noisy SIEM** (like Splunk or Sentinel) that drains your budget with hidden ingestion and connector fees.
- **Investigate threats without SIEM training** using AI-enabled natural language search built for IT generalists.
- **Meet log retention mandates** across compliance frameworks, such as NIST 800-171 and NIST CSF, with an automated 1-year archive.
- **Stop silent log failures** with 24/7 vSOC ingestion-health monitoring that catches gaps before attackers or assessors do.
- **Consolidate your security stack** by pairing MLA with RADICL MDR for a complete security operations SIEM.
- **Maintain continuous compliance** with always-on log collection and audit-ready, on-demand evidence.

UNLIMITED
log sources,
no connector fees

90 DAYS
hot velocity search data

1 YEAR
automated
compliance archive

24/7 VSOC
managed operations

WWW.RADICL.COM · (720) 738-7529 · BOULDER, COLORADO

IS MLA A SIEM?

Yes, by most definitions. MLA collects logs from every source, normalizes them, retains them for compliance, and lets you search them in plain English. But SIEMs are typically built for teams with time, tooling, and deep expertise, and require constant tuning that most teams can't sustain.

RADICL simplifies this by separating responsibilities. **Detection and response live in RADICL MDR**, where dedicated operators and purpose-built analytics act in real time. **MLA is built for what SIEMs do best**: search, investigate, and prove compliance. Together, MDR and MLA deliver full visibility without forcing you to staff a security engineering team.

MLA	+	MDR	=	FULL SIEM OUTCOMES, ZERO SIEM OVERHEAD
Search • Investigation • Compliance Evidence		24/7 Threat Detection • Expert Response		

YOUR VISIBILITY

If it generates a log, MLA can collect it. Gain visibility across your **cloud and productivity platforms, identity and access providers**, and **network and infrastructure stack** — including:

Azure, aws, cisco, cisco Meraki, paloalto, FORTINET, SONICWALL, Google Workspace, ATLASSIAN, box, vmware, DELL, okta, cisco DUO

These are a representative sample; MLA supports unlimited sources via API and Syslog.

WE MANAGE THE INFRASTRUCTURE. YOU GET THE ANSWERS.

✔ FRICTIONLESS ONBOARDING

Point your log sources at our cloud collectors — agentless in most environments. Our team guides setup so critical data flows correctly from day one.

✔ AUTOMATED NORMALIZATION

We map messy, disparate data into one consistent schema for a unified search experience without custom parsing rules to write.

✔ 24/7 HEALTH MONITORING

Silent log failures lead to audit failures. If a source stops reporting, our vSOC catches it and drives remediation without visibility gaps.

✔ ARCHIVING & RECOVERY

We manage your 1-year cold storage. When assessors request history, we handle recovery and make it searchable on demand.

COMPLIANCE-READY BY DESIGN

Assessors don't take your word for it — they want a central log store, verifiable records, and on-demand pulls. MLA delivers **tamper-evident, searchable evidence** that maps to audit-logging, retention, and incident-response requirements across frameworks — including **NIST 800-171** (Audit & Accountability, Incident Response) and the **NIST Cybersecurity Framework** (Detect & Respond functions).

Schedule a demo and watch AI-assisted search answer your first question in seconds.
radicl.com/lets-talk-now