Sumo Logic Professional Services

sumo logic

Cloud SIEM Implementation Services

Accelerated Time to Value

Professional Services Cloud SIEM Implementation Services enable customers to rapidly deploy, operationalize, and realize value from your Sumo Logic SIEM investment. Our structured, tiered approach is designed to move customers from initial data ingestion to advanced threat detection and response while building internal capability and long-term self-sufficiency.

These services are grounded in security operations best practices enabling faster time-to-value, and improved detection coverage.

Customer Outcomes

Tier 1 Outcomes — Foundational Deployment

Establish a fully functional Sumo Logic Cloud SIEM environment with core data ingestion and baseline detection capabilities.

- Accelerated onboarding with initial data sources connected
- Foundational visibility into security events and logs
- Baseline detection rules and dashboards operational
- Initial SOC workflows established
- Early life-cycle detection rule tuning

Tier 2 Outcomes — Operational Maturity

Expand Sumo Logic SIEM capabilities to support broader use cases, improved detection fidelity, and operational efficiency.

- Expanded data ingestion across priority systems and environments
- Custom parser development and normalization mappings
- Initial set of custom rules
- Tuned detection rules to reduce noise and improve signal quality
- Establish incident response workflows

Tier 3 Outcomes — Advanced Security Operations

Enable advanced threat detection, automation, and optimization for mature and complex environments.

- Expanded set of custom rules
- Advanced detection engineering (custom rules, correlation, threat modeling)
- MITRE ATT&CK alignment assessment
- Automated containment response workflow
- Mature SOC operating model with continuous improvement framework

Deliverables	Tier 1	Tier 2	Tier 3
Supported Log Sources - Collection into Cloud SIEM	up to 3	up to 5	up to 10
Configure pre-built roles for Cloud SIEM Admins and Analysts	✓	✓	✓
Install built-in applications for Log Sources and administrators	✓	✓	✓
Deploy pre-built SOC dashboards	✓	✓	✓
Built-in detection rules enabled	✓	✓	✓
Configure partitions	✓	✓	✓
Configure domain normalizations	✓	✓	✓
Configure network blocks	✓	✓	✓
Add standard match lists and values	✓	✓	✓
Configure Cloud SIEM action for email notification on insight creation and rule disablement	✓	✓	✓
Security Insights session - enablement for SOC analysts	✓	✓	✓
Rule Tuning Recommendations	✓	✓	✓
Perform early life-cycle Rule Tuning	✓	✓	✓
Rule Tuning session - best practices for administrators	✓	✓	✓
Post-deployment Hypercare Support (2 weeks)	✓	✓	✓
Practitioner Best Practices		✓	✓
Metadata and Partition design recommendations		✓	✓
Configures entity lookups for user or host normalizations		✓	✓
Custom Log Sources - Collection, Parsers and Normalization		up to 1	up to 3
Configure customer threat intelligence feeds		✓	✓
Custom Rules discovery and development session		up to 3	up to 10
Refined Tuning of Detection Rules to reduce noise		✓	✓

Deliverables	Tier 1	Tier 2	Tier 3
Playbook templates for incident response: notifications, enrichment, ticket creation		✓	✓
Midpoint Value Realization Review		✓	✓
MITRE ATT&CK assessment and recommendations			✓
Automation playbook discovery and development for containment			✓
Final Value Realization & Maturity Assessment Report			✓
Post-deployment Expert Services (3 months, 5 hours/month)			✓
Knowledge Transfer			
Provided knowledge transfer for daily maintenance of the system	✓	✓	✓
Best practices for detection engineering and tuning	✓	✓	✓
Implementation Closure			
Final implementation report with outcomes	✓	✓	✓
KPI Baseline Review (time-to-value, MTTD, MTTR, etc)	✓	✓	✓

Key Value Metrics

- **Time to Value:** Initial detections live within weeks
- **MTTD:** Improved time to detect threats
- **MTTR:** Improved incident response time
- **Detection Coverage:** % of critical assets monitored
- **Signal-to-Noise Ratio:** Reduction in false positives
- **Alert Volume per Analyst:** Ensuring manageable workloads

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
855 Main Street, Redwood City, CA 94603

www.sumologic.com