CYBER LION

Log Security Monitoring

AI Powered Log Collection

CyberLion Log Security Monitoring is a managed security product that collects, aggregates, and normalizes log data from hundreds of sources for AI enabled analysis using CyberLion's analytics platform, SIEM, threat intelligence, and 24/7 365 Security Operations Center. Identify threat-like behavior in your systems such as impossible logins, multi-factor bypass, coordinated attacks, and rogue agents.

CLOUD INFRASTRUCTURE ATTACKS

Alerts on threat-like behavior in AWS services

UNAUTHORIZED ACCESS

Monitoring who is accessing devices and where they connect to, and alert when source or target is unknown or suspicious

COMPROMISED USER CREDENTIALS

Uses behavioral analysis to detect anomalous behavior by users, indicating a compromise. For example, logins at unusual hours or at unusual frequency

ANOMALOUS PRIVILEGE ESCALATION

Detects users changing or escalating privileges for critical systems

THIRD-PARTY VIOLATIONS

Monitors activity by external vendors and partners who have access to organizational systems, to identify anomalous behavior or escalation of privileges

MULTI-VECTOR ATTACKS

Correlates data from multiple sources to get consolidated visibility of multiple attacks

KEY FEATURES

Hundreds of Supported Integrations

SIEM Analysis

AI Analytics Engine

Multi-tenancy dashboard

Self-service Reporting

Deployment of physical or virtual appliance for on-prem logs (like syslog)

Supports key industry and regulatory compliance standards such as continuous monitoring and log retention

ROI on existing investments - Merge data from your existing security tools with multiple sources to provide greater visibility and re-use existing investment

www.cyberlion.cloud

info@cyberlion.cloud

704-800-5470