LCM security

LIFE CYCLE MANAGEMENT

Security Excellence. Business Value.

SERVICE CATALOG

MSSP OFFERINGS

ABOUT LCM SECURITY INC.

For almost 20 years, LCM (Life Cycle Management) Security Inc. has built our security practice on a Life Cycle approach to Security. The Life Cycle approach has been guiding organizations of all sizes to help define their processes, people and technology requirements to meet acceptable levels of risk tolerance.

LCM aligns our Assessment, Remediation, Monitoring and Managed services against industry standards and best practice to customer requirements such as NIST, PCI, CIS or HIPAA. This allows an organization to focus its resources against specific measurable controls and build budgets that directly support the goals and compliance requirements of the organization.

ABOUT LCM'S MSSP OFFERING

Implementing the final component of the Life Cycle Approach is critical to a customer's ability to maintain the required Security, Compliance, and Risk Tolerance goals. LCM Security's proven methodologies are the ideal MSSP offerings to assist you with creating ongoing processes to maintain your goals. LCM's MSSP offering includes:

- Log Management
- Incident Response
- Vulnerability Management
- Quarterly Management Review
- Patch Management
- Scheduled Pen Test
- Reporting
- PCI ASV Scans
- End Point Management

BUNDLED MSSP OFFERINGS

Number of Devices Monitored by FortiSIEM	Level of Service for Cloud-Based FortiSIEM MSSP	Monthly Total Cost Including Infrastructure
10	Monitoring, incident response and reporting, monthly ticketing,	**$2,500**
50	Monitoring, incident response and reporting, monthly ticketing,	**$6,000**
100	Monitoring, incident response and reporting, monthly ticketing,	**$7,000**
200	Monitoring, incident response and reporting, monthly ticketing,	**$9,000**

1	Additional Devices to any 50 and 100 and 200 devices Add	**$30 each**
1	Add quarterly reporting process	**$1,000**
1	Add monthly and on demand Qualys vulnerability scans and analysis	**$2,000**

Notes:

1. Includes Hosting and data retention for 1 year and backup
2. Includes all FortiSIEM, Qualys, and Vendor support
3. On boarding process TBD per customer engagement

OVERALL SERVICE DESCRIPTION

- Daily reviewing of logs for devices that are in-scope and supported by the **SIEM**.
- 24x7x365 monitoring of the **SIEM** Log Monitoring software, including any system health issues and alerts of any attempt to modify or tamper with the logs stored on the **SIEM** data collector.
- Development of a security baseline of normal activity for Customer after reviewing the logs for a period of three to six months.
- Respond to any anomalies or deviations from the baseline that may indicate malicious activity.

- Correlation of critical events based on agreed upon parameters and then alerting on receipt of those triggers.
- Integration of LCM Security team into Customer's Incident Response Process where required.
- Device Maintenance and Support for the **SIEM** Log Monitoring platform.
- Perform problem identification, rectification and escalation between the manufacturer and Customer on the log monitoring platform
- Provide a central Help Desk and ticketing system as a single point of contact for Customer. Integrate (cross reference) tickets with any Customer in-house tickets.
- Regular updates to the software such that Customer is never more than (n-1) from the currently supported manufacturer's recommended release.
- Quarterly Management Meeting to provide updates on the service and support and provide a management overview.
- Monthly technical conference calls to review open trouble tickets and escalations if any.
- Monthly Summary Reports of trouble tickets and escalations.
- Access to the **SIEM** standard web portal dashboard**s,** reports and score cards.