Lebanese Red Cross

Managed SOC RFP

Contents

A. Project goals

LRC is seeking a Security Operations Center Managed Service as part of its strategic initiative to build strong proactive measures to detect and respond to security incidents and cyber threats and risks. Vendors were called to present their service offerings to monitor, analyze logs to proactively report anomalies and detect security incidents and work on continual improvement of the log correlation and alerting capabilities.

B. Company requirements

The below are the minimum requirements for the company that will be selected for the implementation of LRC software solution

- The company should have than 5 years or more in the security field especially in SOC.
- The company should have offices in Beirut Lebanon
- The partner should be a partner with the Vendor (if exists)
- ISO 27001: Information Security Management
- ISO 27017: Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO 27018: Information technology — Security techniques — Code of practice for
- protection of Personally Identifiable Information (PII) in public clouds acting as PII
- processors
- ISO 20000: Information technology -- Service management -- Part 1: Service management system requirements
- ISO 22301: Societal security -- Business continuity management systems -- Requirements.
- ISO 27035: Information security incident management
- NIST 800-61: Computer Security Incident Handling Guide
- The company should have at least 30 employees, the company should submit a statement of the number of its employees form the Social Security or CNSS

- For queries on this, please contact the Procurement, on the following email: **Hoda.fakih@redcross.org.lb**

C. Project Overview

A security operation center (SOC) is a facility that houses a team of IT and IT security experts responsible for monitoring and analyzing an organization's IT health and security posture on an ongoing basis. The team's goal is to detect, analyze, and respond to any health alert, and cyber security incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with IT Experts, Security Analysts and Engineers as well as managers who oversee the overall operations.

Security operation centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

LRC is releasing the Managed Security Operation Centers for the below reasons:

- Real Time health Visibility:
- Higher Visibility of the Threat Landscape:
- Cost Effective with monitoring 24/7
- Zero maintenance headaches

D. Exiting environment

1. Generic data:

- Number of users: 150
- Number of IP addresses: 250
- Security Solution: Kaspersky Management console
- Virtual Machines: 9
- Physical Servers: 4
- Endpoints (Desktops & Laptops): 150
- Number of Data Centres: 1

2. List of Operating Systems used:

- Windows 2016
- Ubuntu

3. List of applications:

- Microsoft Dynamic
- ESRI ArcGIS Enterprise

4. Current Internet Connection

- Number of Public IPs:15
- Locally Published Services:
- Other: GIS Application
- Other: Dynamic

5. Current Network Structure

- Details related to the network infrastructure:
- Segmented Network : 9 VLAN
- Network access control: 1
- Wireless endpoint: 36

6. Current Security Structure

- Security solution, Installed:

Type	QTY	Brand
Firewall	1	PaloAlto
Server Protection	10	Kaspersky
EDR	300	Kaspersky
Endpoint Protection	300	Kaspersky

E. Solution Main Aspects

The solution should be 24/7 operational teams dealing with different type of IT task all around the clock.

The main objective of the managed security operation center is to provide a proactive and reactive approach to different type of IT and IT security alerts, by providing adequate and timely responses.

F. The scope of work

The primary goal of the Incident Response is to restore contain any security breach as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

The Bidder will support the customer with the development of the needed incident response playbooks, such as:

- Malware Outbreak
- Phishing
- Data Theft
- Denial of Service
- Unauthorized Access
- …etc

1. Incident Response Time

Impact is the effect on the business due to the loss or security breach of the service. Impact is assessed as follows:

Urgent	These incidents will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security, affect mission-critical equipment or services or damage public confidence in the organization
High	Less serious events are likely to impact a smaller group of users, disrupt non-essential services and breaches of network security policy.
Medium	Many minor types of incident can be capably handled by internal IT support and security. All events should be reported back to the information security team who will track occurrences of similar events. This will improve understanding of the IT security challenges and may raise awareness of new attacks.
Low	It is not necessary to report on incidents with little or no impact or those affecting only a few users, such as isolated spam or antivirus alerts; minor computer hardware failure; and loss of network connectivity to a peripheral device, such as a printer.

Once impact and urgency are assessed, priority is calculated according to the following table:

Priority Code	Description	Response Time	Resolution Time
1	Urgent	1 hour	4 hours
2	High	4 business hours	2 business days
3	Medium	8 business hours	5 business days
4	Low	24 business hours	8 business days

The response time is validated as soon as the ticket of the incident is assigned to the analyst.

The resolution time should have the following output, either full resolution or a work around is in place to contain and restore the operation to its normal state.
The priority table can be redefined based on specific services and the customer need.

N.B: The incident response is part of the offering and is not bound by any additional cost.

2. Escalation

Primary and backup contacts will be assigned at the project initiation for escalation and exceptions.

3. Security Automation & Orchestration

The incident analysis is integrated with SOAR platform, providing fast automated response allowing the SOC team to focus on actual threats and reducing the false positive alerts. The team is dedicated on developing advanced use case for orchestration, automation and response.

4. SOC Tasks

The main tasks of the SOC Team are as follow:

- 24/7 Monitoring for the infrastructure security health status
- Monthly Vulnerability Scanning
- Security consultancy support
- Playbook development
- **SOC Analyst:**
- Log Collection
- Log Analysis
- Incident Identification
- Incident Classification
- Incident Notification
- Security Monitoring 24/7
- Building new SIEM Use-Cases
- Incident Response (Remotely & On site)
- Incident Analysis and Forensics
- Security Intelligence Dissemination
- Active Threat Hunting

G. Target deliverable schedule

Project Timeline: 12 Months

H. Project Milestones

A Project Manager from the bidding team should work with the LRC team and guide the entire process from kick-off to go-live. This ensures a smooth deploying of the project

Main functions of the implementation handled by the project manager include:

- Reviewing project goals and objectives to ensure a proper implementation
- Developing a detailed implementation plan that is customized to the unique needs of the business
- Assisting with developing and managing project schedules and completion deadlines
- Coordinating and conducting training
- Providing progress reports throughout your implementation process

I. Training Plan

As part of the service offering, an awareness session should be offered by the Bidder team covering the follow:

- Information and Data security: This topic will tackle the sources of information, and how many 'normal' actions can reveal too much information about us and that leads to enterprise breach. It also breaks down the different attacks and techniques used for each scenario, and how the human ring is the weakest in the chain of security.

- Password Security: We are living in a post-password era, where an easily predictable chain of characters defines our identity and how this simple chain can put organizations out of business. This topic will emphasize on how, where and when passwords are disclosed to cyber criminals and how to avoid it.

- Phishing, Social Engineering and Physical Security: Social Engineering is the art of exploiting human vulnerabilities, where phishing has been one of the most successful attacks for a long time. This topic will bring all the classical attacks to the table, along with advanced techniques that are believed to be applicable nowadays and the near future.

1. Training Objectives

- The training courses allow the users to discover the solution, operate, and manage its various functions. The training covers the utilization as well as parameterization and administration of the application to optimize and streamline the operations. The main objectives are:
- Enable users and administrators to gain an overall understanding of the scope and purpose of the overall solution.
- Provide each user with hands-on experience around the system's functions.
- Share knowledge and functional use of the solution while ensuring that LRC's team has the total ownership to carry out all duties and operations by himself.

2. Training Documentation

- Training materials in English (Admin/Technical and end-users/Functional).
- Any other related documentation (electronic format)

J. Communication Tools

1. Types of Communication

- The below details shall be applicable for the above stated intervention types:
- Dedicated contact persons to handle calls, emails, and tickets from LRC.
- Immediate on-site presence when necessary.
- Support hot line for an unlimited number of service requests during the business time interval.
- Email tickets support.
- Portal tickets support.
- Email notification on proactive product change.
- Onsite Software bug fixes when needed.
- Fault incident report to be kept up to date.

2. Response Mechanism

Bidder Team incident response time is divided according to the following criteria:

- Level 1 severity: Serious Incidents; these incidents happen due to a system crash. They are of highest priority, thus having a response time of four (4) working hours. The objective is to have a workaround within the eight (8) working hour's timeframe else if it is impossible will be escalated within Bidder Team and LRC with the appropriate action plan.

- Level 2 severity: Average Incidents; these incidents are not as serious, thus having less priority. They can be system configuration problem. The response time is eight (8) working hours. The objective is to have a workaround within the twenty-four (24) working hour's timeframe.

- Level 3 severity: Minor Incidents and Improvements; these incidents include adding new functionalities to the system. These are minor changes, hence not being urgent. The response time is two (2) working days and implementation action plan is provided to the client's approval

K. The services cover the following

- SOC as a Service:
- SIEM Customization
- 24*7 Cyber Security Monitoring
- Covering up to 500 EPS
- Rules and Report Development
- Threat Intelligence News Alert
- Security Support
- SOAR Integration Backend
- Cyber Threat Intelligence Service
- Managed Vulnerability Scanning
- 25 Device with 10 EPS
- Premium Threat Intelligence (IOC)
- User Entity Behavior Anomaly
- Automated best practice reports
- System & Application Monitoring
- Network Monitoring
- Online Availability Monitoring
- Built-in Ticketing System
- 24/7 Support

L. Bidder Evaluation Matrix

Matrix tool that can be used to evaluate submitted bids and identify the one that provides the best value for money and allows LRC to score and weight Bidder.

Quality	
Quality Criteria	Section Weighting %
Functionality & Methodology	**15%**
Technical Write up	
Design of the solution	
Training	
Mitigation Plan	
Prices	**65%**
Innovation	**5%**
Additional features	
Integrations with different platforms	

Bidder	
Company Size References Geographical Existence Certifications Experiences	**15%**

M. Tender Submission Requirements

1. Bidder Company Profile
2. Products Portfolio
3. Project References
4. Full technical description
6. Technical Team Resumes
7. Technical Proposal includes Project Pricing breakdown and Pricing for Future Expansion