Stock Holding Corporation of India Limited

(StockHolding)

RFI Reference Number: SHCIL/RFI/NW/SIEM/2022-23/001

Date: 22. June. 2022

Request for Information (RFI)

For

Procurement of Security Information and Event Management (SIEM) with Managed Detection and Response (MDR) capabilities

DISCLAIMER

This **Request for Information (RFI)** is NOT a Request for Proposal, Invitation for Bid, or announcement of a solicitation. It is intended for information or planning purposes only. There is no bid package or solicitation document associated with this announcement. Response to this RFI is strictly voluntary and will not affect any potential offeror's ability to submit an offer if a solicitation is released. Any requests for a solicitation package will be disregarded. The Corporation does not intend to award a contract on the basis of this RFI or otherwise pay for the information solicited. No entitlement to payment of direct or indirect costs or charges by the Corporation will arise as a result of preparing submissions in response to this RFI and the Corporation use of such information. Respondents of this RFI may be requested to provide additional information/details based on their initial submittals.

This Request for Information (RFI) is being floated by the Stockholding on behalf of Information Technology Department, for the purpose of identifying organizations who are willing to participate in providing the "**Security Information and Event management (SIEM) with Managed Detection and Response (MDR) capabilities**" Services with robust, implementable, innovative, cost effective and scalable technology options.

RFI Document Details

Name of Organization	Stock Holding Corporation of India Limited
RFI Reference No.	**SHCIL/RFI/NW/SIEM/2022-23/001**
Requirement	**Security Information and Event management (SIEM) with Managed Detection and Response (MDR) capabilities**
Date of issue of RFI document	22-Jun-2022
Last date and time for submission of bidder queries (by email)	27-Jun-2022 @24:00 Hrs
Date, Time and place for online Pre-bid meeting	Pre-bid meeting (Online) at 01-Jul-2022@10:30 Hrs. To participate, please send your request to prit@stockholding.com on or before 30-Jun-2022, @ 14:00 Hrs
Last Date for Submission of Online RFI Response	08-Jul-2022
Date of Technical Presentation	12-Jul-2022 (To participate please send your request to prit@stockholding.com on or before 11-Jul-2022, @ 14:00 Hrs)

StockHolding reserves the right to modify/update activities/ dates as per requirements of the process.

Table of Contents

1. Background

The Stock Holding Corporation identified a principle operational need to enhance cyber Situational Awareness (SA) which aligns with the Stock Holding's critical information requirements. It must be informed by intelligence support to cyberspace operations, and leverage analytic capabilities applied to multiple Log sources of terabytes of data through a capable computing solution.

2. Objective

The primary objective of this Request for Information (RFI) is to identify and shortlist organizations who present the capability of providing effective and efficient solutions with a clear understanding of the scope, approach, methodology, functional and technical architecture, other technical requirements as per requirement of Stockholding, and reasonable time frame to complete the implementation of the system and Go-Live.
The Corporation is seeking comment from industry partners regarding Implementation of prototype and sustainment of Security Information and Event Management with Managed Detection and Response (SIEM-MDR) system.

The following are the key objectives of the RFI for Establishing.

1. Identify potential partners capable of providing SIEM-MDR services across multiple locations of Stockholding.
2. Obtain confirmation as to how the service providers would technologically and operationally provide services and support the SIEM-MDR Services.
3. Obtain confirmation from the respondents on how they propose to provide for scalability, upgradability and interoperability of the solution to be deployed.

3. Shortlisting Criteria

Below is the list of Eligibility criteria that would be followed to short list bidders.

Sl. No.	Criteria	Documents to be provided
1	The Bidder should be a company registered under the Indian Companies Act, 2013 and operational for the last five years.	Certificate of incorporation
2	The Bidder should have minimum 3 years of experience with SIEM-MDR architecture	a) Work Orders confirming year and area of activity
3	3 References where bidder has implemented and supporting SIEM-MDR solution for more than 500 devices in Public sector and BFSI.	1. Relevant Purchase Orders 2. Client reference details for at least 2 projects

Sl. No.	Criteria	Documents to be provided
4	Vendor should be storing logs only in India and same is not replicated outside India	Relevant document confirming the same is required

4. Solution Requirements

Capability statements (not more than ten (10) pages, Times New Roman, twelve (12) font) should address the following questions/statements not limited to below mentioned points:

1. Vendor should have experience with MicroFocus, Arc Sight, Qradar, Splunk and/or any other SIEM-MDR solutions
2. Vendor should have experience in integrating multiple OEM devices which seamlessly, process and distribute correlated and analysed network data, allowing for automated sharing of information to internal and external analysts and providing visualizations for immediate decision support.
3. Vendor should have experience in **THREAT ANTICIPATION** to apply global threat Intel to proactively fix gaps before threats reach us.
4. Vendor should have experience in **INCIDENT ANALYSIS** to get swift analysis on threats, impact on assets, blast radius.
5. Vendor should have experience in **SECURITY MONITORING** to Detect known threats in near real-time using sophisticated rules & correlations.
6. Vendor should have solution in RESPONSE **ORCHESTRATION** Evict attackers, eradicate threats, and advance our defenses.
7. Vendor should have experience **THREAT HUNTING** team with experienced threat hunters to discover evasive threats using Machine Learning.
8. Vendor should have experience being able to ingest threat awareness information and automate analysis of these threats against network data inputs to find anomalous behaviour like detecting and preventing **Data exfiltration**.
9. Vendor should have experience adding and configuring sensor feeds for implementation into a SIEM-MDR.
10. Vendor should have experience in accomplishing full system administration of Linux based network devices used to run a SIEM-MDR architecture.
11. Vendor's solution should have the capability of alerting malware beckoning.
12. Vendor need to be capable of operating SIEM-MDR instances in multiple locations.
13. Vendor should have a cloud storage for storing SIEM-MDR log's as a backup.
14. Specify technical data/software are available or licensing model of the offer's capability.
15. Vendor should have a solution on alert Policy violation, Network attacks, account misuse, application. attacks, malware and Ransomware, **Privilege escalations**, Data exfiltration and Social engineering.
16. Vendor should have Solution maps out the characteristics and specific tools used in an attack across the MITRE ATT&CK® framework as it will help SOC team assess the current effectiveness of Stockholding's existing security measures and the impact of the attack.

17. Vendor's Solution should supports MITRE ATT&CK framework as it documents common tactics, techniques, and procedures that can be used in advanced persistent threats against enterprise networks.
18. Whether vendor have any recommendations for the stockholding to consider regarding this effort.

Note: Bidder need to provide a Technical Solution document on the above mentioned capabilities.

Technical Presentation

A detail and in depth presentation of the solution proposed in RFI will be done after qualifying of general eligibility criteria and should provide an extensive solution understanding of the project. The presentation should contain all the points mentioned in the proposed solution. The presentations may be used in the RFI to select the best of breed solution.

5. Procedure for Submission of RFI

All interested, capable and responsible sources that wish to respond to this RFI are required to email their responses (.doc or .pdf format) to PRIT, (email: **prit@stockholding.com**) not later than 18:00 hrs IST**, 21st June 2022**."SIEM-MDR RFI RESPONSE" must be included in the subject line. Telephonic responses will not be accepted.

6. Instruction to Bidders

6.1 Language of RFI Preparation

The RFI response prepared by the RFI Participants and all correspondence and documents relating to the RFI responses exchanged by the RFI Participants and StockHolding, shall be written in the **English** language.

6.3 Clarification

If deemed necessary, StockHolding may seek clarifications on any aspect from the bidder. However, that would not entitle the RFI Participants to change or cause any change in the substance of the response submitted.

6.4 Right to Accept/Reject any or all RFI Responses

StockHolding reserves the right to accept or reject any RFI and to annul the tender process and reject all RFI responses at any time prior to award of the contract, without thereby incurring any liability to the affected RFI Participants or any obligation to inform the affected RFI Participants of the grounds for StockHolding's action.

StockHolding reserves the right to accept or reject any/all RFI solution if the solutions are not up to the mark.

7. Annexure – I – Shortlisting Criteria

Sl. No.	Criteria	Documents to be provided	Compliance (Yes/No)
1	The Bidder should be a company registered under the Indian Companies Act, 2013 and operational for the last five years.	Certificate of incorporation	
2	The Bidder should have minimum 3 years of experience with SIEM-MDR architecture	a) Work Orders confirming year and area of activity	
3	3 References where bidder has implemented and supporting SIEM-MDR solution for more than 500 devices in Public sector and BFSI.	a) Relevant Purchase Orders b) Client reference details for at least 2 projects	
4	Vendor should be storing logs only in India and same is not replicated outside India	Relevant document confirming the same is required	

Note: Document to be submitted along with RFI response

8. Annexure – II – Technical Solution Compliance

Sl. No.	Criteria	Compliance (Yes/No)
1	Vendor should have experience with MicroFocus, Arc Sight, Qradar, Splunk and/or any other SIEM-MDR solutions	
2	Vendor should have experience in integrating multiple OEM devices which seamlessly, process and distribute correlated and analysed network data, allowing for automated sharing of information to internal and external analysts and providing visualizations for immediate decision support.	
3	Vendor should have experience in **THREAT ANTICIPATION** to apply global threat intel to proactively fix gaps before threats reach us.	
4	Vendor should have experience in **INCIDENT ANALYSIS** to get swift analysis on threats, impact on assets, blast radius.	
5	Vendor should have experience in **SECURITY MONITORING** to Detect known threats in near real-time using sophisticated rules & correlations	
6	Vendor should have solution in RESPONSE **ORCHESTRATION** Evict attackers, eradicate threats, and advance our defenses.	
7	Vendor should have experience **THREAT HUNTING** team with experienced threat hunters to discover evasive threats using Machine Learning	
8	Vendor should have experience being able to ingest threat awareness information and automate analysis of these threats against network data inputs to find anomalous behaviour like detecting and preventing **Data exfiltration**	
9	Vendor should have experience adding and configuring sensor feeds for implementation into a SIEM-MDR	
10	Vendor should have experience in accomplishing full system administration of Linux based network devices used to run a SIEM-MDR architecture	
11	Vendor's solution should have the capability of alerting malware beckoning	
12	Vendor need to be capable of operating SIEM-MDR instances in multiple locations	
13	Vendor should have a cloud storage for storing SIEM-MDR log's as a backup	
14	Technical data/software are available or licensing model of the offer's capability	
15	Vendor should have a solution on alert Policy violation, Network attacks, account misuse, application. attacks, malware and Ransomware, **Privilege escalations**, Data exfiltration and Social engineering	
16	Vendor's Solution should supports MITRE ATT&CK framework as it documents common tactics, techniques, and procedures that can be used in advanced persistent threats against enterprise networks	