Response to Pre-Bid Queries for SIEM & MDR RFI (SHCIL/RFI/NW/SIEM/2022-23/001)				Date : 22-JUNE-2022
Sr. No	**Section & Clause Ref. No./Annexure No**	**RFP text**	**Query**	**Response to query (to be left blank by Bidder)**
1	Annexure – II – Technical Solution Compliance	Vendor should have experience in THREAT ANTICIPATION to apply global threat intel to proactively fix gaps before threats reach us.	With the ability of threat anticipaition, do you expect a full fledged Threat Intelligence platform for threat enrichment using feeds and for finding IOCs in your environment OR do you expect threat hunting using intensive manual and automated techniqued to find unknown threats in the environment?	Yes, for Threat Anticipation Stockholding is expecting a full fledged threat Intelligence platform for threat enrichment using feeds and for finding IOCs.
2	Annexure – II – Technical Solution Compliance	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	Do you have a DLP solution and related policies in place for preventing data exfiltration?	No.
3	Annexure – II – Technical Solution Compliance	Vendor's solution should have the capability of alerting malware beckoning	We have usecases for known and reported C2 server IP addresses.	OK.
4	Annexure – II – Technical Solution Compliance	Vendor's solution should have the capability of alerting malware beckoning	Our SIEM-MDR technologies are hosted in very high availabiliy cloud in India. Do you expect DC and DR for the technologies to be hosted in 2 physically separate locations	Yes, Stockholding is expecting DC and DR for the technologies to be hosted in 2 physically separate locations.
5	Annexure – II – Technical Solution Compliance	Technical data/software are available or licensing model of the offer's capability	Please elaborate on this requirement for purpose of clarity. We own the licenses in our name as MSSP and offer those to customer onboarding with our SIEM-MDR.	OK.
6	Annexure – II – Technical Solution Compliance	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	Do you expect anti-phishing services for preventing social engineering attacks OR Do you expect usecases to detect password guessing , bruteforcing attempts, etc.?	Stockholding expect usecases to be integrated and additional services to be incorporated as per our requirement as bundle solution.
7	Solution Requirements	Vendor should have solution in RESPONSE ORCHESTRATION Evict attackers, eradicate threats, and advance our defenses	Is SOAR part of scope of Response Orchestration?	Stockholding has put up requirement. System Integrator may include SOAR as a part of scope of Response Orchestration if they feel so.
8	Solution Requirements		Is auto containment / playbook driven containmnet action part of scope?	Auto containment should be available with the solution but initially Stockholding will prefer to used manual containment.
9	Solution Requirements	Vendor should have experience THREAT HUNTING team with experienced threat hunters to discover evasive threats using Machine Learning	Is AI ML based threat hunting needed where the ML models first profile and then find the anamolies? or manual IOC hunting is only needed?	Stockholding is expecting both. Manual IOC hunting as well as AI ML based Threat Hunting.
10	Solution Requirements		Is Threat Hunting needed for Users? As in UBA (User behaviour analysis?	Yes
11	Solution Requirements		Is Threat Hunting needed for network flow (Netflow)? As in NTA (network Threat Analytics?	Yes, but do we need a tool with Netflow capabilities. Any additional licenses are required to integrate.
12	Solution Requirements	Vendor should have experience adding and configuring sensor feeds for implementation in customer SIEM	Which sensor feeds?	A threat intelligence feed (TI feed) is an ongoing stream of data related to potential or current threats to an organization's security
13	Solution Requirements	Vendor should have experience in accomplishing full system administration of Linux based network devices used to run a SIEM-MDR architecture.	Which network devices are anticipated to be part of SIEM architecture?	Firewall, WAF, IPS, Load Balancers, ESA Applainces, ISE Appliances, AIX OS, Solaris, Cent OS etc. Also if the logger is on Linux, MDR team must able to perform administrative task of Servers.
14	Solution Requirements	Vendor should have experience in INCIDENT ANALYSIS to get swift analysis on threats, impact on assets, blast radius.	Is the ticket analysis sent to customer capture this and include this?	Yes
15	Solution Requirements	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	Do ML model used for threat Hunting also need to be mapped to MITRE ATT&CK framework?	Yes, this is a mandatory requirement.
16	General Query	NA	Log collection methodology - IPSEC/MPLS/On-prem*	Log collection is On-prem at Stockholding end. Monitiring and Reporting should be at System Integrator's end for the complete solution.
17	General Query	NA	What is the total number of log generating devices to be monitored with the solution?	Stockholding needs to understand the type of solution (EPS based and/or Device based) available with System Integrators.
18	General Query	NA	What is the estimated consolidated log volume from all devices (events per second (eps) or Gigabytes per day)?	Minimum 2000 eps and Maximum 4000 eps
19	General Query	NA	If you answered the previous question, how many times per day does event load PEAK beyond the sustained average?	Is it device specific or event specific...???
20	General Query	NA	What is the number of monitored assets considered critical / high-priority for security or compliance reasons?	Critical and High priority Assets - 50, Medium Severity Assets - 75, Low Severity Assets - 100
21	General Query	NA	How is your data network distributed geographically? How many main data centers are there & how many remote sites connect back to each DC? A network drawing would assist.	3 Locations DC, DR and NDR. Network diagram understanding will be provided to successful System Integrator.
22	General Query	NA	Can we get the list of device, OS,Network Device, Security,Databases Device to Calculate the MPS	Yes, list of devices will be provided to successful system integrator.
23	General Query	NA	How long must the event logs be kept online(in days) & offline (days) for retentiona reasons?	Online 180 days, Offline - Stockholding need retnetion period of 7 Years.
24	General Query	NA	Do you required HA to Log Collector at all location	Yes, At DC and DR location.
25	Shortlisting Criteria	The Bidder should have minimum 3 years of experience with SIEM-MDR architecture	Will you also consider SOC refrences for BFSI customer. Also we request you to change it to 2 BFSI customer reference(SOC References) and also consider enterprise custoemr references.Also if possible pls change it to Bidder/OEM customer references.	The Bidder should have minimum 3 years of experience with SIEM-MDR architecture of which 2 BFSI Indian Customer reference can be provided.
26	Shortlisting Criteria	3 References where bidder has implemented and supporting SIEM-MDR solution for more than 500 devices in Public sector and BFSI.	Pls consider 2 BFSI and Enterprise customer also fro references. Also if you can also consider SOC customer references becz MDR is very new . Or you can also consider OEM references.	No change
28	Shortlisting Criteria	03 References where bidder has implemented and supporting SIEM-MDR solution for more than 500 devices in Public sector and BFSI	Can we provide global reference instead of India? We have global SOC running multiple customers outside India	No change
29	Shortlisting Criteria	03 References where bidder has implemented and supporting SIEM-MDR solution for more than 500 devices in Public sector and BFSI	1. Modify SIEM solution on the basis of 500 user or 5000 EPS 2.Modify experence of Govt. also with public sector and BFSI 3. Consider Client refrence detail for At Least 1 project	No change