Request for Proposal

Managed Security Service Provider (MSSP)

for

Security Information and Event Management – Security Operations Centre

(SIEM-SOC)

SBICAP Securities Limited (SSL)

Marathon Futurex, 12th Floor, A –Wing, N M Joshi Marg, Lower Parel, Mumbai - 400013

RFP NO. SSL/IT/RFP-003/2020-21

Request For Proposal (RFP)
For Hiring of SIEM-SOC Services from managed security service provider (MSSP).

ACTIVITY SCHEDULE

Sr No	Activity	Details
1.	RFP Number	SSL/IT/RFP-003/2020-21
2.	Bid Document Availability including changes/amendments, if any to be issued	RFP may be downloaded from Company's website https://www.sbismart.com/content/procurement-news
3.	Release of RFP	20th October, 2020
4.	Pre Bid	Queries on email
4.	Online Technical Bid submission	5th November, 2020 - 16:00 Hrs
5.	Technical Bid Opening	5th November, 2020 - 17:00 Hrs
6	Technical Bid Evaluation and Presentation of shortlisted Service Providers	6th November, 2020 to 10th November, 2020 (tentative schedule)
7.	Opening of Commercial Bids	11th November, 2020 - 11:30 Hrs (tentative)
8.	Method of Selection	The method of selection is Quality and Price Base Selection. The weights given to the Technical and Commercial Proposals are: Technical = 70% and Commercial= 30%
9.	Reverse Auction	12th November, 2020 - 11:30 Hrs (tentative)
10.	M/s. e-Procurement Technologies Ltd. – Contact Details	A-202, Wall Street - II, Opp. Orient Club, Ellisbridge, Ahmedabad – 380006. **Name**: Nandan / Fahad / Dharam Email: nandan.v@eptl.in / fahad@eptl.in / dharam@eptl.in Landline No. : 079 6813 6820, 6850, 6857, 6848 Official Mobile No. : 9081000427 / 9904406300
11	SSL - Contact Details	Mr. Sagar Kuperkar (Sr. Manager- IS) M - 9820098909 email – Sagar.Kuperkar@sbicapsec.com Mr. Rupesh Vedante (Dy. Manager - IS) M- 9967546663 email – Rupesh.Vedante@sbicapsec.com

Table of Contents

1. Introduction

1.1 Background

SBICAP Securities Ltd (SSL) is committed to improve its security posture and achieves this objective by updating its processes and technology periodically. Driven by this commitment, SSL is inviting bids from Service Providers (SP) to define, roll-out and support a comprehensive Security Operations Center (SOC) Framework which will provide assurance on the security posture and enhance SSL's capabilities to monitor, respond and mitigate threats against SSL.

SSL intends engaging with a Service Provider (SP) who has a sustainable and proven business model, recognized accreditation, established customer-base, distinguishable solution accelerators and enablers, high-performance personnel, while maintaining the ability to support SSL's evolving requirements.

SP's are advised to study the RFP document carefully. Submission of proposal shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

The RFP will be conducted online by M/s e-Procurement Technologies Ltd.. The response to this RFP should be full and complete in all respects. The SP must quote for all the items asked for in this RFP.

The SP shall bear all Prices associated with the preparation and submission of the proposal, including Price of presentation for the purposes of clarification of the proposal, if so desired by SSL. SSL will in no case be responsible or liable for those Prices, regardless of the conduct or outcome of the selection process.

1.2 Disclaimer:

1.2.1. The information contained in this RFP document or information provided subsequently to Bidder(s) whether verbally or in documentary form/email by or on behalf of SSL (Company), is subject to the terms and conditions set out in this RFP document.

1.2.2. This RFP is not an offer by SSL, but an invitation to receive responses from the eligible Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of SSL with the selected Bidder.

1.2.3. The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advices/clarifications. Company may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

1.2.4. SSL, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, Price or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.

1.2.5. SSL also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

1.2.6. The issue of this RFP does not imply that the SSL is bound to select a Bidder or to appoint the Selected Bidder or Concessionaire, as the case may be, for the Project and the Company reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

1.2.7. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respect will be at the Bidder's risk and may result in rejection of the Bid.

1.2.8. Proposed solution must be as per the detailed Technical Specifications and the Vendor should adhere to Scope of Work mentioned in this RFP.

1.2.9. The Purchase Order may be placed in part or full by SSL, the quantity or number of equipment to be purchased as mentioned in this RFP is only indicative. No guarantee or assurance is being provided hereby as to the exact quantity of equipment to be purchased or the minimum order quantity. SSL, however, reserves the right to procure extra quantity during the bid validity period of the offer and till 3 year from the date of project sign-off. The price of such procurement will be calculated on pro-rata basis of the balance period. The offer should be valid for SSL group companies.

1.3. Definitions

Throughout this RFP, unless inconsistent with the subject matter or context:

1.3.1. Vendor/ Service Provider/ System Integrator – MSSP / SIEM Vendors.

1.3.2. **Supplier/ Contractor/ Vendor** – Selected Vendor/System Integrator under this RFP.

1.3.3. **Company/ Purchaser/ SSL -** Reference to the "SSL", "Company" and "Purchaser" shall be determined in context and may mean without limitation "SSL Ltd.

1.3.4. **Proposal/ Bid** – the Vendor's written reply or submission in response to this RFP

1.3.5. **RFP/Tender** – the request for proposal (this document) in its entirety, inclusive of any Addenda that may be issued by SSL.

1.3.6. **Solution/ Services/ Work/ System** – "Solution" or "Services" or "Work" or "System" all services, scope of work and deliverable to be provided by a Vendor as described in the RFP and include services ancillary for Security information Event Management - Security Operations Center (SIEM-SOC) for continuous log monitoring and analysis, co-relation of all logs, threats and vulnerabilities. Etc. covered under the RFP.

1.3.7. **Product** – "Product" means SIEM and Security Tools implemented for SOC and log collector as mentioned in the tender.

1.3.8. **Server / Network / Website** – As specified within the technical requirement section of this RFP document.

2. RFP Process

- The technical and commercial proposal with the relevant information/documents/acceptance of all terms and conditions as described in this RFP document will be submitted online through M/s e-Procurement Technologies Ltd., Ahmedabad, the authorized agency approved by SSL for e-tendering on the website https://etender.sbi/SBI/.

- For any query related to e-tender and bid submission, the bidders may contact M/s e-Procurement Technologies Ltd., Ahmadabad as mentioned below:

  Nandan / Fahad / Dharam
  e-Procurement Technologies Limited
  Email: nandan.v@eptl.in / fahad@eptl.in / dharam@eptl.in
  Landline No. : 079 6813 6820, 6850, 6857, 6848
  Official Mobile No. : 9081000427 / 9904406300

- The Bidders will have to upload the duly signed and scanned tender documents and all Annexure Forms as part of technical bid have to be submitted online.
- The tender document is not required to be sent to us in hard copy.
- Please find below the RFP schedule for submissions and evaluations.

1.	Release of RFP	20th October, 2020
2.	Pre-Bid	Queries on email
3.	Online Technical Bid submission	5th November, 2020 - 16:00 Hrs
4.	Technical Bid Opening	5th November, 2020 - 17:00 Hrs
4.	Technical Bid Evaluation and Presentation of shortlisted Service Providers	6th November, 2020 to 10th November, 2020 (tentative schedule)
5.	Opening of Commercial Bids	11th November, 2020 - 11:30 Hrs (tentative)
7.	Reverse Auction	12th November, 2020 - 11:30 Hrs (tentative)

- The bidders are requested to note that:

  a) They cannot make their online submission after the time stipulated above and no extension of time will normally be permitted for submission of bids.
  b) It is mandatory to have a valid digital certificate issued by any of the valid Certifying Authority approved by Government of India to participate in the online bidding. The bidders are requested to ensure that they have the same, well in advance or if any assistance is required for the purpose, Bidders can contact our service provider (M/s e-Procurement Technologies Ltd.).

2.1 List of the Annexures to be submitted online as mentioned below :

S/N	Particulars	Annexure	To be submitted with
1	Technical Specification and Scope of Work	Annexure-A	Technical Bid
2	Inventory	Annexure-B	Technical Bid
3	Bidders Organization Profile & capability presentation to support the scope of work as per RFP and post implementation support.	Annexure-C	Technical Bid
4	Eligibility Criteria	Annexure-D	Technical Bid
5	Service Level Agreement	Annexure-E	Technical Bid
6	Pre-Bid Queries with SSL response to be submitted with Technical Bid.	Annexure-F	Technical Bid
7	Commercial Bid	Annexure-G	Commercial Bid
8	Tender Document duly signed		Technical Bid
9	Reverse Auction	Annexure-H	Online
10	Final Price Break-up by L1 vendor	Annexure-I	L1 Bidder
11	NDA	Annexure-J	L1 Bidder

2.2 Terms & Conditions :

2.2.1. Tender should strictly confirm to the specifications. Tenders not conforming to the specifications will be rejected summarily. Any incomplete or ambiguous terms/ conditions/ quotes will disqualify the offer.

2.2.2. SSL reserves the right to accept in part or in full or reject the entire quotation and cancel the entire tender, without assigning any reason there for at any stage.

2.2.3. Any terms and conditions from the Vendors are not acceptable to the SSL.

2.2.4. SSL reserves the right to impose and recover penalty from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.

2.2.5. Not with standing approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition**.** Payment shall be regulated on the actual work done at the accepted rates and payment schedule.

2.2.6. The L1 rates finalized discovered will be valid for 12 months and the L1 vendor is bound to execute the orders placed at L1 rates during the duration of the contract.

2.2.7. The validity period may be extended at the discretion of SSL which will be binding on the vendors.

2.2.8. The prices quoted for SIEM-SOC services should be for three year.

2.2.9. The prices should be **exclusive of all taxes**, the vendor should arrange for obtaining of permits wherever applicable.

2.2.10. During the validity period of tender quotes, any upward change in the exchange rate/ excise duty and customs duty are to be borne by the vendor. In the event of any downward revision of levies/duties etc., the same should be passed on to SSL, notwithstanding what has been stated in the quotation or in the Purchase Order.

2.2.11. The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports etc., pertaining to the SIEM-SOC for which the Vendor has quoted.

2.2.12. Vendor shall ensure that the SOC implemented have use cases with capabilities to detect both internal and external attacks/threats.

2.2.13. The tools used for SIEM-SOC by the vendor should be licensed one.
2.2.14. Cloud based solution / tools and the channel being used, should be clearly stated.
2.2.15. Vendor shall conduct monthly meeting with SSL and develop use cases to be integrated on the SIEM solution. Vendor shall ensure that use cases are updated regularly to keep it relevant to emerging threats.
2.2.16. It would be binding upon the vendor to maintain security of SSL systems at all times.
2.2.17. SSL may changes the bid evaluation criteria at its own discretion after receipt of bids from competent bidder. SSL also reserves the rights to remove components from Commercial bid for evaluation purpose and for releasing the work order for partial scope.
2.2.18. SSL will notify successful Bidder in writing by way of issuance of purchase order through letter or email that its Bid has been accepted. The selected Bidder has to acknowledge by return email/letter in token of acceptance.
2.2.19. Penalties for Delayed Implementation - The SIEM- SOC Implementation should be started immediately from the date of placing the letter of Intent / Purchase order whichever is earlier. If delayed, SSL will charge a penalty of 1% of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.
2.2.20. The Bidders will have to submit the Service Level Agreement as per Annexure - E and Non-disclosure Agreement as per Annexure – F together with acceptance of all terms and conditions of RFP, duly signed by the authorized signatory.
2.2.21. Copy of board resolution and power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

2.3 Payment Terms:

Sl. No.	Details
1.	Payment would be done on quarterly basis at the end of the quarter upon receipt of invoice from vendor.

3. Submission of Bids

A two-stage bidding process will be followed for evaluating the bids. The bidders should submit their responses to this RFP in two parts, i.e., first Technical Bid and Commercial Bid and second after techno-commercial evaluation the short-listed bidders will be called for Reverse Auction.

3.1 Technical Specification and Scope of Work (Requirements of SSL) is detailed at **Annexure-A.**
3.2 Inventory for the scope of work is detailed at **Annexure – B.**
3.3 Bidders Organisation Profile as per **Annexure – C**.
3.4 Eligibility criteria alongwith supporting documents as per **Annexure D.**
3.5 Service Level Agreement - as per **Annexure – E.**
3.6 Clarification to RFP - The Bidder should carefully examine and understand the specifications/ requirements/ conditions of the RFP and may seek clarifications, if required, before submitting the bids. The Bidders are required to direct all communications in writing through email to the designated SSL officials as per the time schedule defined above, in the Pre-bid Queries format as per **Annexure – F**.

4. Bid Evaluation Process

4.1 Bidder Eligibility Criteria

4.1.1. Bidder Profile and experience in the industry.
4.1.2. Bidders capability to support the RFP scope and based on the presentation.
4.1.3. Bidder support facilities / proactive support/Profile/ Previous experience.
4.1.4. OEM post sale support experience.
4.1.5. SSL will evaluate the technical and functional specification of all the equipment quoted by the Bidder.
4.1.6. During evaluation and comparison of bids, SSL may, at its discretion ask the bidders for clarification of its bid. The request for clarification shall be in writing and no change in prices or substance of the bid shall be sought, offered or permitted. No post bid clarification at the initiative of the bidder shall be entertained.
4.1.7. SSL reserves the right to evaluate the bids on technical & functional parameters including factory visit, client site visit and witness demos of the system and verify functionalities, response times, public documents, Market Share, OEM establishment blogs. Group Company experience with product etc.

4.2 Techno-Commercial evaluation

4.2.1. **Technical bids** will be examined by the Technical Committee of SSL which may call for clarifications/additional information from the Vendors which must be furnished to the Technical Committee in the time stipulated by the Technical Committee. E.g. Presentation, Demo or POC of the product.
4.2.2. Technical bids will be opened for eligibility criteria and technical evaluation.
4.2.3. Bids that are not substantially responsive are liable to be disqualified at the Co.'s discretion.
4.2.4. Technical evaluation will include technical information submitted as per technical Bid format, demonstration of proposed solution, reference calls and site visits, wherever required. The Bidder may highlight the noteworthy/superior features of their Services.
4.2.5. Proposed solution features, guaranteed uptime, integration, underlying components' etc.
4.2.6. Scalability / Capability of the proposed solution to meet future requirements not outlined in the RFP.
4.2.7. Support on open platforms and solution based on proposed technology (both software and hardware).
4.2.8. Management GUI for administration for proposed components
4.2.9. The Bidder will demonstrate/substantiate all claims made in the technical Bid to the satisfaction of the Company, the capability of the Services to support all the required functionalities at their Price in their lab or those at other organizations where similar Services is in use.
4.2.10. Vendor who have fulfilled the eligibility criteria will be evaluated as per the scoring parameters below : In this stage shortlisted Bidders will prepare technical proposal which shall comprise of (at a minimum)

i)	Eligibility criteria	–	10 marks
ii)	Architecture & SIEM solution	–	20 marks
iii)	Technical Evaluation of SOC	–	50 marks
iv)	Project Plan with Timelines	–	10 Marks
v)	Vendor presentations & SOC visits (if feasible)	–	10 Marks

4.2.11. The bidders who have attained minimum technical score & have complied with the points of Technical Bid shall qualify for Commercial Bid evaluation.

i. Technical Bid will be assigned a technical weightage. Only the bidders whose overall Technical score is 70 % or more will qualify for commercial bid evaluation.

ii. The Final technical score of the Bidder shall be calculated as follows -

Normalized Technical Score of a Bidder = {Technical Score of that Bidder / Score of the Bidder with the highest technical score} X 100 (adjusted to 2 decimals)

4.3 Commercial Bid evaluation

i. The Commercial bids for the technically qualified bidders will then be opened and reviewed by the Technical & Price Negotiation Committee (TPNC) of SSL to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at owner's discretion.

ii. The Commercial Bids of the technically qualified bidders shall be calculated as follows -

Normalized Commercial Score of a Bidder = {lowest discounted quote / Bidders discounted quote} X 100 (adjusted to 2 decimals)

iii. The final techno-commercial score will be Quality and Price based with the following weightage:

a) 70%: Final Technical Score
b) 30%: Final Commercial score

Final Score = (0.7*Final Technical Score) + (0.3*Final Commercial Score)

iv. The bidder will be given ranks in the descending order, i.e. the highest Final score shall be treated as Rank-1 bidder. Based on the rankings, the TPNC will shortlist the bidders for Reverse Auction round.

4.4 Reverse Auction :

4.1.1. All the Bidders who qualify in the techno-commercial evaluation process shall have to participate in the online reverse auction to be conducted by the Authorised service provider on behalf of SSL.

4.1.2. Shortlisted Bidders shall be willing to participate in the reverse auction process and must have a valid digital signature certificate. Bidders shall also be willing to abide by the e-business rules for reverse auction framed by the Authorised service provider. The details of e-business rules, processes and procedures will be provided by the Authorised service provider.

4.1.3. The Bidder will be selected as L1 on the basis of overall price package as quoted in the Reverse Auction.

4.1.4. Final Price Break-up details as per **Annexure – H**, should be submitted by the successful Bidder by next day of Reverse Auction.

4.1.5. Prices quoted must be "All Inclusive" except taxes as applicable.

4.1.6. SSL reserve the complete rights to issue a full or partial purchase order or to subtract any component from the proposed solution/ BILL OF MATERIAL at its own discretion.

5. General Terms & Conditions

5.1 Confidentiality

This document contains information confidential and proprietary to SSL. Additionally, the Bidder will be exposed by virtue of the contracted activities to internal business information of SSL, the Associates, Subsidiaries and/or business partners. The Bidders agree and undertakes that they shall keep confidential all matters relating to this RFP and will not make any disclosure to any person who is under the obligation under this document, any information, data, and know-how, documents, secrets, dealings, transactions or the terms or this RFP (the "Confidential Information"). Disclosure of receipt of this RFP or any part of the aforementioned information to parties not directly involved in providing the services requested could be treated as breach of confidentiality obligations and SSL would be free to initiate any action deemed appropriate.

The restrictions on disclosure of confidential information shall not apply to any matter which is already available in the public domain; or any disclosures made under law.

No news release, public announcement, or any other reference to this RFP or any program there under shall be made without written consent from SSL. Reproduction of this RFP, without prior written consent of SSL, by photographic, electronic, or other means is strictly prohibited.

5.2 Non-Disclosure Agreement

The shortlisted bidder will be required to sign a Non-Disclosure Agreement with SSL. The Bidder shall treat all documents, information, data and communication of and with SSL as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement.

5.3 Governing Law and Jurisdiction

All disputes and controversies arising out of this RFP and related bid documents shall be subject to the exclusive jurisdiction of the Courts in Mumbai and the parties agree to submit themselves to the jurisdiction of such court and the governing law shall be the laws of India.

5.4 Arbitration

All disputes and differences of any kind whatsoever shall be settled by Arbitration in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory amendment thereof. The dispute shall be referred to the sole arbitrator who shall be appointed by SSL. The venue of Arbitration proceedings shall be at Mumbai. The Arbitration proceedings shall be conducted in English Language. The award of the Arbitration shall be final and binding on both the Parties and shall be delivered in Mumbai in the English language. The fees of the Arbitrator and the cost of the Arbitration proceedings shall be equally borne by both the Parties.

5.5 Indemnification

The Bidder shall, at its own cost and expenses, defend and indemnify SSL against all losses, judgements, statutory and regulatory penalties, fines, damages, third-party claims on account of the any misrepresentation, infringement of intellectual property rights, fraud and breach of terms of this RFP/ violation by the Bidder of any or all national/international trade laws, norms, standards, procedures etc.

The Bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If SSL is required to pay compensation to a third party on account of the Bidder or association with the Bidder, then the Bidder shall be fully responsible for the same, including all expenses and court and legal fees.

5.6 Force Majeure

In case of delay in implementation of the Project on account of conditions which are beyond the control of the shortlisted bidder such as war, floods, earthquakes, strikes, lockouts, epidemics, pandemic, riots, fire or Governmental regulations superimposed after the date of order/ contract, the Parties shall be permitted to terminate the contract / bid document, if such delay extends for a period beyond 15 days. SSL shall not be liable to make any payments in this case.

5.7 Termination

SSL reserves the right to abandon the current tender process and restart the bidding process at any point of time without assigning any reason whatsoever. SSL can cancel the award granted to the elected Bidder at any point of time and restart the bid process completely or select another Bidder. The Elected Bidders understands and agrees that SSL shall not be obligated in any manner whatsoever and is free to stop / modify the bidding process at any stage without any liability.

5.8 Data Protection

The Bidders authorizes the release from time to time to SSL (and any of its Subsidiaries or Affiliates) all personal or professional data that is necessary or desirable for the administration of the RFP (the "Relevant Information"). Without limiting the above, the bidders permit SSL to collect, process, register and transfer to and aforementioned entities all Relevant Information. The Relevant Information will only be used in accordance with applicable law.

5.9 Intellectual Property

SSL shall have sole exclusive ownership to all its Intellectual property including and not limited to its trademarks, logos etc. This RFP shall in no way be considered as a transfer or assignment of the respective rights over any intellectual property owned, developed or being developed by SSL.

6. Annexure-A : Technical Specification and Scope of Work

Compliance: C – Fully compliant, P – Partially Compliant, N – Not compliant

The key requirements of SOC Transformation are as follows:

S.No	Requirements	Compliance	Remarks
1	**Security Monitoring Requirements**		
1.1	Vendor should monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach.		
1.2	Vendor should provide log baselines for all platforms under scope that are required to be monitored.		
1.3	Vendor platform should have capability to collect logs from most of the standard platforms like Windows, Linux, AIX, Solaris, Firewall, Network and other security devices or solution, etc.		
1.4	Vendor Platform should be able to collect logs from most of standard network, security devices, Data bases, Web servers and cloud services (Aws/Azure), SAAS Solutions, O365,etc.		
1.5	Vendor should detect both internal & external attacks. In addition to security attacks on IT infrastructure, vendors should also monitor for security events on databases and servers.		
1.6	Vendor should monitor, detect and manage incidents for the following minimum set of database security events. This is an indicative list and is not a comprehensive/complete set of events. Vendors should indicate their event list in proposal response. · Monitor Access to Sensitive Data (e.g. PII data) · Database access including logins, client IP, server IP and source program information. · Track and audit administrative commands		
1.7	Vendor should carry out correlations amongst the logs from multiple sources to detect multi-vector attacks.		
1.8	Vendor operations team should send alerts with details of mitigation steps to designated personnel as including any identified service provider of SSL.		
1.9	The Vendor should bring workflows and solutions that can automate majority of the incident response activities such as false positive management, managing white lists, escalation workflow, SLA management etc.		
1.10	Alerts should be notified to SSL only after proper triage process. Alerts from SIEM should be enriched with context data, environmental data, vulnerability data, historical data, threat intelligence etc.		
1.11	Historical parameters should include and not limited to attack volume, attacker volume, and destination volume for every alert.		
1.12	Vendor should give long term solution to prevent such threats in future		
1.13	Define, Develop and implement Use Cases based on standard methodologies such as Cyber Kill Chain		

1.14	Service provider should have capability to integrate log from nonstandard application and devices and service provider platform should be able to process them for generating alerts and reports		
1.15	Service Provider reports are in compliance with industry best practice and international standards like ISO 27001, PCI, SOC1, SOC2 etc. and regulatory requirement like SEBI.		
1.16	Service provider to assist the organization to ensure the log retention is as per local regulatory requirement like SEBI, NSE, and BSE, etc..		
1.17	Service Provider's solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples • Failed login attempts • Successful Login attempts from suspicious locations or unusual systems • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical & Horizontal port scans • Traffic from blacklisted IPs • Login attempts at unusual timings		
1.18	Service provider solution should be able to provide charts for top attacks & attackers, OWASP based threat analysis, Trending threats, attack demographics etc.		
1.19	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.		
1.20	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.		
1.21	Any failures of the event collection infrastructure must be detected and operations personnel must be notified.		
1.22	The solution should be able to support enrichment of data with contextual information like Geo Data, malicious IPs, Domains, URLs, Threat Intel and custom specified tags and annotations. The enrichment fields should be indexed along with the event in real-time at an individual event level and not done as a separate lookup process.		
1.23	Using the outbound plugins architecture the Vendor must provide integrations with services like ticketing systems, messaging platforms, vulnerability scanners etc. to facilitate automation of workflows.		
1.24	Vendor should detect both internal and external attacks. In addition to security attacks on IT infrastructure, Vendor should also monitor for security events on critical business applications, databases and also identify network behavior, user behavior anomalies.		
1.25	Vendor should monitor, detect and manage incidents for the following minimum set of IT infrastructure security events. This is indicative minimum list and is not a comprehensive/complete set of events. · Buffer Overflow attacks · Port and vulnerability Scans		

	· Password cracking · Worm/virus outbreak · File access failures · Unauthorized service restarts · Unauthorized service/process creation · Unauthorized changes to firewall rules · Unauthorized access to systems · SQL injection · Cross site scripting · All layer 7 web attacks via internet / intranet		
1.26	Vendor should monitor, detect and manage incidents for the following minimum set of business application security events. This is an indicative list and is not a comprehensive / complete set of events. · Attempted segregation of duties violations · Attempted access violations · Critical user additions, deletions · Creation, deletion and modification of critical application roles/groups · Changes to permissions or authorizations for critical application roles/groups · Changes to account and password policies in the application · Changes to critical application parameters · Changes to audit parameters		
2.	**Incident Analysis**		
2.1	Solution should support centralized incident management to prioritize and manage security incidents.		
2.2	Solution should support triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, ETDR.		
2.3	Solution should support machine driven triaging algorithms that considers contextual parameters, historical behavior and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same · Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert. · Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on. · Central Threat Intelligence feed should also be applied to identify threats through known bad actors		
2.4	Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters		
2.5	Solution should enable investigation of triaged alert/custom alerts deemed critical		
2.6	Investigation module should integrate with log sources (SIEM, ETDR, EPP, Data Lake) on demand to pull data related to the investigated alert. It should also include charting and graphs to analyse data		

2.7	Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise(IOCs), external network connections,		
2.8	Solution should support features to identify attacker attributes including threat intelligence score of attacker, who-is lookup information, geo-mapping in a single console.		
2.9	Solution should support models to build up the entire attack chain- from attack inception, progress of the attack and spread to attack in the network.		
2.10	Solution should provide run books for investigation steps corresponding to different types of attacks, derive attack inception and progress of the attack. i.e. Detect Patient Zero, Attack origin and Blast Radius.		
2.11	Solution should support integration with open source or commercial IOC sources. List the supported sources which can be integrated with Solution and brief on the integration approach. · Solution should support features to analyse and identify the impact of this attack on other assets.		
2.12	Solution should support models to derive attack inception and progress of the attack. List the details of investigation models used in the Solution.		
2.13	Solution should provide case management features to store raw and analyzed data for a specific alert or set of alerts. Provide details on the what artefacts can be stored related to an investigation		
2.14	Solution should support quick search across stored datasets in the Solution. Provide details of search features supported.		
2.15	Solution should provide run books for investigation steps corresponding to different types of attacks.		
2.16	Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.		
3.	**Incident Response**		
3.1	Solution should support quick response to an ongoing incident or serious threats with remote configuration of parameters in servers/desktops, Firewalls, AD (Active Directory), IPS, WAF, Network Switches & Routers · Automated Remediation for responding to commodity threats (e.g. recall malicious mails from inboxes, block bad IPs in Firewall, Disable bad users in Active Directory, etc.) · Solution should support multiple configuration parameters to servers/desktops including removal/changes to services, users, registry keys, software, and browser plugins.		
3.2	Solution should support the full workflow for incident classification, incident coordination such as assigning activities to different teams and tracking for closure, escalation of tasks, and exception approvals		
3.3	Solution should support the full workflow for incident coordination.		

3.4	Solution should support assigning activities to different teams and tracking for closure.		
3.5	Solution should support the workflow required to approve such auto mitigation action or have option to exempt certain auto mitigation from approval process.		
3.6	Solution should support escalation workflows. Provide details on the escalation matrix within Solution along with the levels and list the escalation medium (SMS/email)		
3.7	Solution should support tracking of security exception approvals for those threats and incidents for which remediation is not possible or compensating controls are available.		
3.8	Solution should integrate with external service desks such as e.g. BMC Remedy, Internal ticketing tool for leveraging existing service desk platform or SP to Provide Ticketing tool – SOC operations access to SSL.		
3.9	Solution should provide alert details and investigation outcomes linked and viewable for relevant remediation tickets.		
3.10	Incident Report with classification, chronology of events, RCA, IOC		
3.11	Track impacted assets related to an incident		
3.12	Tools for Response based on data and analytics		
3.13	Ability for quick Counter Response by integrating with devices such as firewall and AD for blocking traffic or quarantine system		
3.14	Usage of Ticketing and case management workflow		
3.15	Classification of incidents		
3.16	Maintain track of first response and subsequent measures taken for the incident		
3.17	Maintain chronological order of events related to incident response		
3.18	Maintain IOC and artifacts related to incident		
3.19	Incident response should include investigation of end points if required to conclude the investigation		
3.20	Centralized incident management to prioritize and manage security incidents.		
3.21	SP should bring a platform which facilitates collaboration between SOC and SSL with features comments on incidents, maintaining a history of conversation with time line, ability to add artifacts		
4	**Threat Hunting Requirements**		
4.1	Use algorithms and tools to actively hunt of attacks in large volume of data and create alerts that are passed on to analysts. Supports use of Big data platform for collection and analysis		
4.2	Define, develop, implement, update and maintain Hunting Framework which contains: · Create Strategic Hunt Missions which are objective based to identify malicious activity that has not triggered an alert · Search for Indicators of Compromise received from Threat Intelligence and Analytics		
4.3	Create knowledge base of IOCs		

4.4	Vendor should provide security analytics as a service to able to detect unknown attacks		
4.5	The analytics service should have models that are able to detect attacks in various stages of a cyber kill chain		
4.6	The analytics service should able to detect threats from various attacks vectors such as malware, web application attacks, network attacks, watering hole attacks, DNS attacks, insider threat, and data exfiltration. List the detection use cases which can detect above attacks using pre-built machine learning techniques and analytical models.		
4.7	Analytics using machine learning techniques should use multiple sources to identify malicious activity. A minimum the following sources should be used: · Netflow · IPS/IDS · Proxy · WAF · Windows logs · DNS · FW		
4.8	Solution should have pre-built AI models to detect targeted attacks (unknown attacks from unknown threat actors).		
4.9	Solution should have analytical models to detect different stages of Cyber Kill chain.		
4.10	Network Threat Hunting should leverage existing network sources for better detection of advanced attacks. Network sources should include Netflow, Proxy, DNS, IPS, VPN, Firewall, AD/Windows, Email logs		
4.11	Network threat hunting should use AI on network sources and enable hunting for attacks including but not limited to Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, Dynamic DNS attacks		
4.12	The service must be capable of identifying suspicious or hitherto undiscovered communication patterns. The service must support detection of newly discovered pattern in future		
4.13	The service should identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).		
5.	**Endpoint Detection & Response Service – It should support**		
5.1	Endpoint threat hunting should hunt for Process anomalies, Service anomalies, Hash values, Connection anomalies and indicators of compromises.		
5.2	EDR hunting should help to detect anomalies at the end point such as: · Detect Command and control activities · Detect Data stealing activities · Assess weakness by looking at vulnerabilities. · Searching for IOCs · Outlier detection of active system process, driver, services, network connections, etc.		

5.3	EDR should help perform the following : · Collection of forensic artifacts (Name, Hash code, Size, Loaded DLLs) of all binaries running in organization. · Matching of forensic artifacts against known indicator of compromise. · Segregating unknown forensic artifacts from known forensics artifacts. · Clustering of unknown forensic artifacts to find outlier binaries. · Analyzing outlier binaries using supervised neural network.		
5.4	EDR service should be able to take quick response actions such as: · Killing anomalous processes, deleting malicious binaries · Isolating end points		
5.5	Detect threats on endpoints by deploying EDR agents. The service should be able to take containment actions such as isolating infected endpoints		
5.6	Detect user anomalies using a combination of rules and machine learning model. Optionally provide sensors to capture network traffic to detect threats at the network level.		
6.	**User Behavior Analysis**		
6.1	Solution should provide UBA dashboard based on various UBA models outcome. · UBA Dashboard should highlight risky users based on objective scoring of users based on composite risk score comprising all behavior anomalies of the user · Organization should be able to define risk thresholds based on their risk appetite		
6.2	Detect malicious/illegal activities performed by users		
6.3	Solution to have capabilities to collect user data from variety of sources like Directory Services , IAM, VPN, Proxy,O365, etc.		
6.4	Service should be able to track user‘s activities locally and remote network sites and should be able to report usage behavior across the entire network.		
6.5	The service should incorporate multiple baseline behavioral models which cover behavioral risk categories like Data Exfiltration, Malicious Users, Illicit Behavior, compromised credentials, etc.		
6.6	Solution should support business application threat hunting for application to detect access and authorization anomalies using application logs, NetFlow.		
6.7	Solution should be able to search proactively and iteratively through a network or logs data to detect and isolate advanced threats that evade Signature based systems (SIEM, IDS, DLP etc.)		
6.8	Solution should support applying AI models on WAF events to detect targeted web application attacks		
6.9	Service provider should submit a daily threat hunting based on the threat hunting models deployed at the organization		
7.	**Threat Intelligence**		
7.1	Service should anticipate likely threats to the Organization based on global threat events and data and provide proactive measures to prevent such happenings in the Organization.		

7.2	Service should support integration of machine readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise & false positives in threat intelligence feeds		
7.3	Service should provide strategic threat intelligence about incidents and breaches happening across the global and provide actionable intelligence such as · Can SSL be susceptible to such an attack? · If yes, which assets in the organization are susceptible? · Provide IoC's where relevant · Provide mitigation steps for each advisory		
7.4	Service should apply the threat intelligence to Organization assets, network traffic, security event and users to provide actionable report on likely impact on each entity and recommend pre-emptive measures.		
7.5	Solution should track status of assets against IoCs, CVEs and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities. Service provider should track closure and corresponding risk reduction		
7.6	Service should have machine algorithms to auto-evaluate an asset and assign a business value to the asset		
7.7	Solution should support STIX/TAXII for automated integration of actionable intelligence with security technologies.		
7.8	Service should support 3rd party / external threat intelligence to aid incident response by bringing in organizational context and internal information available in SIEM and other sources of security information		
8	Vulnerability Management		
8.1	Reports Should be provided on vulnerability status along with mitigation recommendations.		
8.2	Integration of vulnerability information with the Threat management system to get 360 degree view of the asset.		
9	**General Requirements**		
9.1	Service provider team should have the following skills: · Security analysts · Incident investigator · Threat hunter · Data scientists · Threat intelligence analytics · Incident responders · Specialized security team for IOC collection, deeper analysis, forensic investigation		
9.2	Solution should provision reconstructing common file formats including word document, image, Web page.		
9.3	The platform should have machine learning capabilities and other advanced analytics of structured as well as unstructured security & network data.		

9.4	The Log management solution (Centralized) is required at SSL for collection of logs from different log sources. VMs and Storage for Log collector will provide by SSL. Vendor to provide required specification document for log collector.		
9.5	Vendor shall build the capacity of the SIEM solution that can handle the log retention as mentioned below: · Three months – Online · Two Years – Offline		
9.6	24x7x365 real time logs monitoring, analysis and correlation using security analytics, Threat hunting, Threat Intelligence consisting of Indicators of Compromise (IOC) and other threat intel (vulnerabilities report, incident reports etc.).		
9.7	The proposed solution should provide end-to end capability to setup an SIEM, Big Data Security Analytics Platform and SOAR for storage, indexing, searching, analysis, correlation, reporting, visualization, orchestration of different types of structured / semi-structured data generated within the organization.		
9.8	The proposed system should support SAN, NAS and DAS for adding external storage as and when required. The bidder is expected to size the storage as per the requirements mentioned in this RFP. The bidder‘s response should include the calculations/ logic used to arrive at the sizing. It is to be noted that proposed hardware should be based on RAID 5. The solution should have adequate redundancy for handling disk failures.		
9.9	Vendor will be responsible to store logs in industry standard solution and format.		
9.1	If connectivity between log collection agents and logger is down then the Log collector agents should store the logs of at least 3 days and send them once connectivity is established.		
9.10	Alerting events/incidents and recommending remedial actions.		
9.11	Incident analysis (Triage) to remove false positives, incident notification.		
9.12	Daily report of events/incidents, correlation, analysis and recommendations. The daily report shall cover the correlation analysis of all the devices included as part of scope.		
9.13	Monthly report summarizing the list of events/incidents reported, correlation analysis, recommendations, status of actions by SSL and other security advisories. It should include the trend analysis comparing the present month’s data with the previous month data.		
9.14	Detect known as well as unknown threats by using machine learning and security analytics		
9.15	Consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies		
9.16	Proactive threat hunting on daily basis, which otherwise gets undetected via signature based systems.		
9.17	Be Cyber-Ready to respond to attacks swiftly.		

9.18	Complete analysis and correlation of logs from all the devices/solutions under scope		
9.19	Provide and/or develop parsing rules for standard/ non-standard logs respectively. Pre-defined / custom parsers should be available for parsing logs for the following applications but not limited to: Oracle E-Business Suite, Opentext Documentum platform etc.		
9.20	The proposed solution should have available connectors to support the standard devices / applications, wherever required the vendor should develop customized connectors for all standard/custom devices/applications at no extra Price		
9.21	24x7x365 uninterrupted security monitoring operations. Submit a report in case of service non availability of the devices along with the status.		
9.22	Automate security processes to reduce resource drain and threat response times		
9.23	Skilled and capable staff with expertise in at least the following domains: · Event monitoring and analysis · Incident detection and response · Threat Intelligence · Use Case engineering and new integrations to increase visibility · Threat Hunting · Security Analytics		
9.24	Correlation of low priority alerts with subsequent alerts to detect multi-stage attacks.		
9.25	Reduction of remediation time · Automated real time prioritization of alerts · Automated data collection for investigation followed by quick analysis on a single window. · Assisted remediation steps (integration with security devices to push policy/configuration remotely) for faster mitigation of threats		
9.26	Provide central dashboard to capture risk posture and maturity levels of organization at any given point of time.		
9.27	Comprehensive security dashboard (web based dashboard) for viewing real-time incidents/events, alerts, status of actions taken, tracking of key security metrics and provide security threat scorecards. Vendor shall also provide customized dashboard to suit as per SSL requirements.		
9.28	Vendor shall provide different dashboard and screens for different roles as mentioned below for viewing real-time incidents / events, alerts, status of actions taken etc.: • Top Management (Company View) • IS Team (complete and detailed dashboard of security posture of the organization setup being monitored through this SOC) • Auditors (Internal auditor, External auditors etc.)		
9.29	The offered cyber security product shall be complying with the Indian government regulations.		

9.30	Vendor needs to ensure that SOC solution can integrate with the IT system using standard methods/ protocols/ message formats without affecting the existing functionality of SSL.		
9.31	SOC setup/infrastructure may be subjected to audit from SSL and/or third party and/or regulatory body. It shall be responsibility of the Vendor to co-operate and provide necessary information and support to the auditors. The Vendor must ensure that the audit observations are closed on top priority and to the satisfaction of SSL and its appointed auditors. Extreme care should be taken by the Vendor to ensure that the observations do not get repeated in subsequent Audits. Such non-compliance by Vendor shall attract penalty as defined in SLA.		
9.32	The solution should consist of security monitoring, incident response, security analytics, proactive threat hunting, threat Intelligence consisting of Indicators of Compromise (IOC) and other threat intel (vulnerabilities, strategic, tactical etc.), SIEM engineering, Endpoint Detection & Response, User Behavioral Anomaly detection, vulnerability scanning and network threat detection.		
9.33	Service Providers should propose monitoring platforms, to best suit the requirements stated in the RFP.		
9.34	To Develop & recommend improvement plans for the SOC as needed to maintain an effective and secure computing environment		
9.35	For improvement of SOC Monitoring at SSL. SP should done the Firewall rules review half yearly basis and Network aritecture review annually.		
9.36	Effective and Efficient Governance Model with fortnightly, monthly, quarterly and annual reviews		
9.37	SLA's and implementation timelines for the various activities would be mutually agreed while signing a contract with the selected SP. However, SP is expected to give an overall implementation and roll out plan as part of this proposal with templates of SLA, Project Plan, Governance meeting templates etc.		
9.38	NBAD and UEBA shall be considered as part of MSSP services, monitoring devices which provides insight of anomalies and potential risk to the network.		
9.39	The applications and databases logs shall be considered for the correlation.		
9.40	Standard Operating Procedure (SOP) shall be developed for all the products /solutions /services provided including alert management, incident management, forensics, report management, log storage and archiving, SOC business continuity, operational documents, escalation matrix, change management, use cases, knowledge documents, playbook etc.		
9.41	Analytical reports on Daily, weekly and Monthly basis and Ad-hoc reports as and when to be provide by service provider		
9.42	IT Forensic services for root cause of incident and investigations as and when required		

9.43	During the exit of the contract or services vendor should provide logs as per retention period from their end to SSL without any Price		
10	**Security Incident and Crisis Management services**		
10.1	Alignment of Security Incident management plan in line with SSL Cyber Crisis Management Plan (CCMP) and Cyber Security Policy		
10.2	The Incident and Cyber crisis management support shall be (preferred offsite and, in case of emergency, onsite support is mandatory) provided by MSSP		
10.3	MSSP will provide a detailed process for managing cyber incidents - describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents		
10.4	Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact		
10.5	The incident management solution should be able to register any security event and generate alerts		
10.6	Establishing process for identifying, preventing, detecting, analysing & reporting all Information Security incidents as per the best practices, this may revise time to time as per the requirements		
10.7	Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement		
10.8	Describe the incident response process including the roles and responsibilities and scope of action in line with CCMP		
10.9	MSSP should do root cause analysis for security incidents and recommend implementation of controls to prevent reoccurrence		
10.10	MSSP must provide on demand timely support by performing investigation and forensic analysis on the logs by doing the necessary analysis on the logs by doing the necessary analysis and log review and providing required data on a timely fashion		
10.11	Faster incident response by replacing purely ad-hoc activities with Advanced playbooks, analytical tools, incident management tools and reporting, which liberates security analysts to spend less time doing research and more time doing analysis		
10.12	MSSP shall provide backend professional incident management team support in case of severe incident occurs		
11	**Packet Capture Analysis – Optional**		
11.1	Solution should enable network visibility with high speed packet capture. Solution should provision reconstruction of network traffic using packet capture and make it available in formats including PCAP		
11.2	Solution should support Deep Packet Inspection (DPI) to classify protocols & applications by capturing packet.		
11.3	Solution should have capabilities for packet capture analysis for zero-day threat detection, retrospection & metadata extraction feed into analytics engine for contextual enrichment & forensic analysis.		

7. Annexure-B : Inventory

List of devices / servers (Total 50 device list Approximate)

Sr. No.	Model	IOS / OS Version	Qty
1.	Network Devices	Firewall, Proxy (UTM), Routers, Switches, Load Balancer, VPN, etc..	20
2.	Systems	AD, AV, DLP, Email, Application, etc.	10
3.	Servers	OS & DB	20

8. Annexure – C : Bidder's Organization Profile

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)
Date: _____
To:
The Head, Information Security
Marathon Futurex, 12th Floor,
A –Wing, N M Joshi Marg,
Lower Parel, Mumbai 400013

Dear Sir,
Ref: **SSL/IT/RFP/003** dated: 20/10/2020
Details of the Bidder:

S/N	Particulars	Bidders Comment
1	Name of Bidders Company	
2	Registered Office Address	
3	Date of Incorporation	
4	Contact Person Phone and Email	
5	Director, MD & CEO Name and contacts	
6	Total Employee count PAN India	
7	Brief description of the Bidder including details of its main line of Business	
8	Company /firms website URL	
9	Of the Authorized Signatory of the Bidder (i.e. Name, Designation, address, contact no., email)	
10	Income Tax. No. (GST/PAN/GIR). Please enclosed photocopy of latest income tax clearance certificate	
11	Bidders support office presence at Mumbai, Hyderabad, Chennai, New Delhi, Kolkata)	If not available, how bidder will support remote locations
12	Total No. of clients in India for the bidder for similar implementation SIEM-SOC	
13	Total number of clients in for similar implementations (active engagements) SIEM -SOC	
14	No. of Years of experience, Bidder has in System Integration and providing managed services	
15	Number of technicians available in for proposed solution and its components	
16	The Organisation certificated with process ISO 9001/20000,27001/ITIL etc. (Certificate to be provided)	
17	Capability to support 24/7	

9. Annexure – D : Compliance For Eligibility Criteria

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

#	Eligibility Criteria	Compliance (Compliant/ Not Compliant)	Supporting Evidence
1.	The MSSP should be a current legal entity with a minimum 5 years of experience in India.	Y/N	Certificate of Incorporation or Appropriate Supporting Document
2.	The vendor should have the experience of owning and managing a well-established Security Operations Centre (SOC) for at least five years. Vendor shall provide the details of the SOC including the location, infrastructure, tools used, companies served, process and methodology, staff employed	Y/N	Self-Declaration
3.	The MSSP should have performed managed SOC services for at least two clients during the last 3 financial years, with at least one of which should preferably be in the BFSI. Kindly furnish details of the same in the Technical Proposal. Size of SOC services must be similar or larger than SSL	Y/N	Customer references to be provided & Copies of Purchase Orders
4.	The service provider shall not assign or sub-contract the assignment or any part there of to any other person/firm.	Y/N	Self-Declaration
5.	The bidder should be a company registered in India as per Company ACT 1956. The bidder should have experience of minimum five years in Supply of SIEM-SOC solution in India.	Y/N	Incorporation Certificate
6.	The Bidder's Account should not have been declared as a Non-Performing Asset (NPA) in the Books of any bank or financial institution as on 31.03.2020.	Y/N	Certificate from Bank/ Auditor
7.	The bidder must submit an undertaking that no Government / undertaking organizations have blacklisted the bidder for any reason. Past/present litigations, disputes, if any (Adverse litigations could result in disqualification, at the sole discretion of the SSL)	Y/N	Undertaking by Bidder.
8	Minimum Annual Turnover should be INR 50 Crores in each of the Preceding three financial years.	Y/N	Auditors Certificate or CA certificate
9	Financial statements i.e. Audited Balance sheet and Profit & Loss accounts for last three years (FY2017-18, FY2018-19 and FY2019- 20)	Y/N	Auditors Certificate or CA certificate

10	The participant should be a profit-making entity for minimum of Preceding Three years. It should not have incurred / reported losses during any of the last Three financial years.	Y/N	Appropriate Supporting Document
11	An undertaking that, no penalties/fines have been imposed on their entities by any Regulator or Govt Agency or any Authority for breach of any Regulations or Laws.	Y/N	Supporting Document
12	MSSP to have a functioning Disaster Recovery site and approved Business Continuity Plan to support SSL for continuity of SOC Operations	Y/N	Supporting Document
13	The MSSP should have permanent office in India	Y/N	Appropriate Supporting Document

10. Annexure – E : Service Level Agreement (SLA)

1.1. SLAs for 24 x 7 Threat Detection & Response Services will be applied as below:

Sr No	Alerts Priority Type	Time to Notify (TTN)	Time to Investigate & Recommend remedial action	Uptime (measured monthly)
1	Critical (P0)	1 hour	2 hours	95%
2	High (P1)	4 hours	4 hours	95%
3	Others (P2)	24 hours	Next Business Day (NBD)	95%

1.2. For every breach of Service levels as stated above, SSL may claim a penalty of 1 % of agreement value (calculated on daily basis) for every hour of breach of time. However, the aggregate of all such penalties shall not exceed 25 % of the overall charges paid by SSL for the said quarter.

1.3. Daily report of events/incidents, correlation, analysis, recommendations and closure status by next business day.

1.4. Monthly report by 7th day of every month (including excel based reports).

1.5. Information must be shared as stated above of getting validated information about the potential security threats/vulnerabilities new global security threats/zero day attacks in circulation to the designated SSL official and suggest suitable countermeasures to safeguard against such evolving threats/attacks along with the analysis. The advisories should be customized to SSL Infrastructure. Report pertaining to the same should be part of the monthly report.

1.6. Report on recommendations regarding enhancement of security of SSL should be part of the monthly report.

1.7. 24*7*365 dashboard availability to be ensured.

1.8. **VALIDITY OF AGREEMENT:** The Agreement/ SLA will be valid for the period of three years. The SSL reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.

1.9. For purpose of calculating penalty, uptime is calculated as under:

$$\text{Uptime (\%)} = \frac{\text{Sum of total hours during quarter - Sum of downtime hours during quarter}}{\text{Sum of total hours during the quarter}} * 100$$

Total hours during the quarter = No. of working days i.e. 90 * 24 hours = 2160 hours

$$\text{Uptime (\%)} = \frac{2160 - \text{Sum of downtime hours during quarter}}{2160} * 100$$

11. Annexure-F : Pre-Bid Queries

S. No.	Page No	Section (Name & No.)	Statement as per tender document	Query by bidder	Reason for Query
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

12. Annexure G : Commercial Bid

PART-1

1. SIEM Software Price

S.N.	Item	Type – In house / cloud	EPS or equivalent GB units (A)	Price Capex / Opex per Unit (B)	Total price (A*B)
A	License Price				
B	3 years Support Price				
	Total SOC Monitoring & Management Price/ annum				

2. SOC Monitoring & Management Services

S.N.	Item	EPS or equivalent GB	No. of devices approx.. (a)	Unit Price per quarter (in INR) (b)	Yearly Price (excl Tax) (in INR) c=a*b*4
A	Offsite - Monitoring & Management Services (24*7)				
	Total SOC Monitoring & Management Price/ annum				

3. SIEM Hardware Price

S.N.	Item	Config	OS License Price	HW Price	Total Price
A	Hardware - In house / cloud				
B	3 years Support Price				
	Total SOC Monitoring & Management Price / annum				

PART-2
Overall package price as shown below:

Total Price (in INR)		
S. No.	**Description**	**Amount (in INR) (excl. taxes)**
1-a	SIEM Software licenses Events per Second (EPS) or equivalent Mb indexed per day	
1-b	3 years Support Price	
2	Total SOC Monitoring & Management Price for 50 devices for 3 years	
3-a	SIEM hardware	
3-b	3 years Support Price	
4	Total Implementation, Integration and Training cost (One Time)	
5	Any Other cost	
Overall package price (Sum of S.No. 1+2+3+4+5)		

13. Annexure H : Reverse Auction – Overall Package Price

To arrive at L-1 bidder, Revers Auction will be conducted for the overall package price as shown below:

Total Price (in INR) excluding taxes		
S. No.	**Description**	**Amount (in INR) (excl. taxes)**
Overall package price		

14. Annexure I : Final Price Break-up : To be submitted by the L1 Vendor

1. SIEM Software Price

S.N.	Item	Type – In house / cloud	EPS or equivalent GB units (A)	Price Capex / Opex per Unit (B)	Total price (A*B)
A	License Price				
B	3 years Support Price				
	Total SOC Monitoring & Management Price/ annum				

2. SOC Monitoring & Management Services

S.N.	Item	EPS or equivalent GB	No. of devices approx.. (a)	Unit Price per quarter (in INR) (b)	Yearly Price (excl Tax) (in INR) c=a*b*4
A	Offsite - Monitoring & Management Services (24*7)				
	Total SOC Monitoring & Management Price/ annum				

3. SIEM Hardware Price

S.N.	Item	Config	OS License Price	HW Price	Total Price
A	Hardware - In house / cloud				
B	3 years Support Price				
	Total SOC Monitoring & Management Price / annum				

4	Total Implementation, Integration and Training cost (One Time)	
5	Any Other cost	

*This Price shall remain valid during the entire contract period of three years.

15. Annexure – J : Non-Disclosure Agreement (NDA)

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

THIS AGREEMENT ("**the Agreement**") is made on this _____day of _____, 2020.

BETWEEN

SBICAP Securities Limited, an Indian company duly incorporated under the Companies Act, 1956, having its registered office at Marathon Futurex, 12th Floor, A & B Wing, Mafatlal Mill Compound, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013 (hereinafter for the purposes of this agreement, referred to as **"SSL"/ "Disclosing Party"**), which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and permitted assigns;

AND

_____LIMITED, a company incorporated Registered under the Companies Act, 1956 and having its registered office at _____ _____ in (hereinafter referred to as the "Receiving Party"), which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns)

WHEREAS:

1. SSL is registered with SEBI as a Stock Broker and a Depository Participant and distributing third party financial products including mutual funds/Tax Free bonds and is registered with Association of Mutual Funds in India (AMFI).

2. **The Receiving Party** is engaged in the business of _____.

3. **SSL** and **the Receiving Party** are in the process of discussion and negotiation wherein **SSL** will provide its Information related to Systems, Device, Applications, logs, etc. ("Information") to the **Receiving Party** and may in the course of discussion, negotiation and/or performance of the said Services, disclose, provide or make available to **the Receiving Party** certain Confidential Information as defined herein below; and

4. **SSL** desires to restrict use and disclosure of such Confidential Information as set out herein below.

NOW THEREFORE in consideration of the mutual promises and covenants contained in this Agreement, and the mutual disclosure of Confidential Information to each other, the Parties hereto agree as follows:

1. Confidential Information and Confidential Materials

(a) "Confidential Information" means non-public information that **SSL** designates as being confidential or which under the Confidential Information circumstances surrounding disclosure ought to be treated as

confidential. "Confidential Information" includes, without limitation, information relating to released or unreleased SSL's services or products, the marketing or promotion of any **SSL** Product, SSL's business policy, Confidential Information or practices, and information received from others that **SSL** is obligated to treat as confidential. Confidential Information disclosed to the Receiving Party by any parent or agent of **SSL**, or by any subsidiary of parent of **SSL,** is covered by this Agreement.

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without the Receiving Party's breach of any obligation owed to **SSL**; (ii) became known to the Receiving Party prior to **SSL**'s disclosure of such information to the Receiving Party; (iii) became known to the Receiving Party from a source other than the breach of an obligation of confidentiality owed to SSL; (iv) is independently developed by the Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation, written or printed documents and computer disks or tapes, whether machine or user readable, the Software being licensed including any manual and documents relating to the Software, its Source Code, etc.

2. Restrictions

(a) Except as provided below, the Receiving Party shall not disclose any Confidential Information to third parties. However, the Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order, provided the Receiving Party shall give SSL reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. This restriction on disclosure of Confidential Information shall apply to all the Confidential Information disclosed before entering the service agreement and shall continue to have effect during the subsistence of the Service Agreement. It shall also survive the termination of such agreement for provision of the services, as set out in the recitals hereinabove.

(b) The Receiving Party shall take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, to keep confidential the Confidential Information. The Receiving Party may disclose Confidential Information or Confidential Material only to the Receiving Party's employees or consultants on a need-to-know basis. The Receiving Party will have executed or shall execute appropriate written agreements with its employees and consultants sufficient to enable it to comply with all the provisions of this Agreement

(c) Confidential Information and Confidential Materials may be disclosed, reproduced, summarized or distributed only in pursuance of the Receiving Party's business relationship with SSL, and only as otherwise provided hereunder. The Receiving Party agrees to segregate all such Confidential Materials from the confidential materials of others in order to prevent commingling.

(d) Publications: the Receiving Party shall not make any news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the SSL.

3. Rights and Remedies

(a) The Receiving Party shall notify SSL immediately upon discovery of any unauthorized use or disclosure of Confidential Information and/or Confidential materials, or any other breach of this Agreement by the Receiving Party, and will co-operate with SSL in every reasonable way to help SSL to regain possession of the Confidential Information and/or Confidential Materials and prevent its further unauthorized use.

(b) The Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at SSL's request, or at SSL's option, certify destruction of the same.

(c) The Receiving Party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information or Confidential Materials and that SSL shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

4. Miscellaneous

(a) All Confidential Information and Confidential Materials are and shall remain the property of SSL or any affiliate thereof. By disclosing information to the Receiving Party, SSL and/or its affiliate(s) do not grant any express or implied right to the Receiving Party to or under any patents, copyrights, trademarks, or trade secret information.

(b) Any software, product, service and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.

(c) Terms of confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire products without use of other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by persons who have had access to the Confidential Information, including the ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(d) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both Parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of SSL, its agents, or employees, but only by an instrument in writing signed by an authorized officer of SSL. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(e) This Agreement shall be governed by and construed in accordance with the laws of India and shall be subject to the exclusive jurisdiction of the courts of Mumbai.

(f) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and assigns.

(g) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(h) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.

(i) In the event this Agreement (including any schedules, exhibits or attachments hereto) is signed in both the English language and in any another language, any conflict or inconsistency between the different language versions shall be resolved solely by reference to the English language version.

5. Arbitration

All the disputes in connection with this Agreement, the construction of any provision of this agreement or the rights, duties or liabilities of the parties hereto under this Agreement shall be amicably settled. However, in the event of any such disputes are not settled amicably between the Parties, reference shall be to three arbitrators. Each party shall appoint its Arbitrator and the two respective Arbitrators appointed by each party shall appoint a presiding Arbitrator to adjudicate the dispute, difference, claim, etc. between the parties. A Party wishing to refer a dispute to arbitration shall appoint its arbitrator and send notice of such appointment in writing to the other party requiring the other party to appoint its own arbitrator within 30 calendar days of that notice and stating that it will appoint its arbitrator as sole arbitrator unless the other party appoints its own arbitrator and gives notice that it has done so within the 30 days specified above. If the other party does not appoint its own arbitrator and give notice that it has done so within the 30 days specified, the Party referring a dispute to the arbitration may, without the requirement of any further prior notice to the other party, appoint its arbitrator as sole arbitrator and shall advise the other party accordingly. The award of such sole arbitrator shall be binding on both parties as if he had been appointed by agreement.

The arbitration will be held **in Mumbai, India** and will be conducted in the English language.

IN WITNESS WHEREOF, THE PARTIES HERETO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED AS OF THE DAY AND YEAR FIRST ABOVE WRITTEN

SIGNED AND DELIVERED)
For SBICAP Securities Limited)

)
in the presence of:)
)
1.
2.)
SIGNED AND DELIVERED)
For _____Limited)
in the presence of:)

1.)
2.)