LIC-CO/IT-BPR/NW/RFP/2023-2024/TDIR dated 18 December 2023 - Prebid Query Responses

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Bidder Query	Response
1	6. Eligibility Criteria	Point No.02	14	The Bidder must have an annual turnover of minimum Rs. 600 Crores per annum during the last 03 (three) years preceding the date of this RFP.	**We kindly request you to modify the clause as follows:** **"The Bidder must demonstrate an annual turnover of at least Rs. 250 Crores per annum for the three years preceding the date of this RFP.** **Please refer to the GFR guidelines for turnover criteria."**	Please be guided by the RFP
2	6	6.5	14	The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	We request LIC to keep this mandatory so that LIC can get a proven best of the breed solutions in the SIEM space.	Please be guided by the RFP
3	6	6.6	15	The proposed OEM for the SIEM Solution should figure in the Leaders or Challengers Quadrant of Gartner in the last published report. This clause will not be applicable for the OEMs proposed or quoting of product under the regulations of Make In India.	We request LIC to only consider Gartner Leaders Quadrant as leaders consistantly innovate and address critical SOC requirements and help detect complex threats.	Please be guided by the RFP
4	Annexure F - SIEM	2		The peak EPS that the proposed solution can address without any additional license, server, storage or appliance should be minimum twice than the sustained EPS proposed.	This is very critical as no functionality in the SIEM should be stopped or no events should be dropped even after crossing the license limit. Hence we request LIC to make this mandatory.	Please be guided by the RFP
5	Brief Scope of Work	Functional NGSOC Architecture (Indicative)	56	TIP to be integrated for all solutions	Please let us know the TIP being used and which needs to be integrated for this solution	Please be guided by the RFP
6	Brief Scope of Work	Security Dashboards	58	The bidder should implement an integrated online security dashboard for services provided to LIC	Please let us know how is the bidder expected to create these dashboards	Please be guided by the RFP
7	Detailed Scope of Work	Security Information and Event Management (SIEM)	67	Setting up basic system health monitoring and log analysis through Management and Reporting appliance.	Please confirm the current health monitoring tool will be extended for this project	Please be guided by the RFP
8	Brief Scope of Work	Security Dashboards	58	Anti-phishing services Security Analysis, Mitigation and reporting	Please confirm which tool is used for Anti Phishing security services	Please be guided by the RFP
9	Brief Scope of Work	Security Dashboards	58	As part of deliverables, bidder must provide integrated dashboard along with Display Panel / TV set covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc	Please confirm dashboard is not limited to only SIEM tool	Please be guided by the RFP
10	Support Process Requirement:		58	The on-site L1 and L2 support may also be required to work on Sunday/LIC holidays or beyond office hours on working days, for which an advance notice will be given.	What is the scope of service post working hours?	Please be guided by the RFP
11	Section 19. Right to terminate the Process	19 (a)	31	a.LIC may terminate the RFP process at any time without assigning any reasons whatsoever. LIC makes no commitments, express or implied, that this process will result in a business transaction with anyone.	Any termination/cancellation without any reason shall not be post award of the RFP.	Please be guided by the RFP
12	Section 22. Patent Rights and other Litigation costs:	Section 22	33	In the event of any claim asserted by a third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the systems or any parts thereof with relation to the Hardware deliverables, in LIC's country, the Bidder will act expeditiously to extinguish such claim. If the Bidder fails to comply and LIC is required to pay compensation to a third party resulting from such infringement, the Bidder will be responsible for the compensation including all expenses (court costs and lawyer fees). LIC will give notice to the Bidder of such claim, if it is made, without delay as when received. In no event shall LIC be liable for any indirect, incidental or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered. For this purpose, it would be immaterial how such liability may arise, provided that the claims against customers, users and service providers of LIC are considered as a direct claim.	With respect to all indemnity Claims including intellectual property claims, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent twelve (12) months of charges collected by Bidder pursuant to the applicable PO giving rise to the liability. In no event shall either Party be liable for any indirect, incidental or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered.	Please be guided by the RFP
13	Section 33. Limitation of Liability	Section 33	36	33. Limitation of Liability Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	Please remove the requirement of Liquidated Damages. We request the Limitation liability clause to mentioned in RFP capping Bidder liability under the contract. Limitation of liability clause. "Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence (including gross negligence or wilful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. For any liability not excluded by the foregoing, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent twelve (12) months of charges collected by Bidder pursuant to the applicable order giving rise to the liability. Such limited liability is applicable for all claims including those for liquidated damages, confidentiality, infringement of Intellectual Property and any indemnification under the Agreement.	Please be guided by the RFP
14	Rights reserved by LIC	Section 42 (k)	40	LIC may terminate the agreement if it determines at any time that Vendors or their representatives were engaged in corrupt, fraudulent, collusive or coercive practices during the selection process or the execution of that agreement, without the concerned Vendors having taken timely and appropriate action satisfactory to the LIC to remedy the situation	Any such termination shall be basis mutual discussion and suggested not to be discredtionary.	Please be guided by the RFP
15	Cancellation of Contract and Compensation	Section 47	42	The entire clause - please refer to the verbiage on page 42	The termination rights are unilateral in nature. The termination rights should be mutual.	Please be guided by the RFP
16	Cancellation of Contract and Compensation			LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and / or reduce the scope of the Services.	Minimum 90 days notice period should given with cure period of additional 90 days	Please be guided by the RFP

17	Cancellation of Contract and Compensation			LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and / or reduce the scope of the Services.	In case of pre mature termination or downgrade of Contract, ETC (Early Termination Charges) to be paid by Customer equivalent to the remainder of the total contract value, notice period will be 90 days in case of termination	Please be guided by the RFP
18	27. Period of Validity of Bids	Point a	35	Bids shall remain valid for 12 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule. LIC shall reject a bid as non-responsive if the bid is submitted with a shorter validity period.	There are various commercial factors like currency variations, supply chain issues, etc., that have impact on quoted price. So we request LIC to consider changing this as follows: "Bids shall remain valid for 6 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule. LIC shall reject a bid as non-responsive if the bid is submitted with a shorter validity period."	Please be guided by the RFP
19	3. Sizing Requirements	Point 6 - Network Behavior Anomaly Detection	71	30 Gbps or its equivalent Flows Per Second or Packets per Second	In "Annexure F – Technical Compliance.xlsx", NBAD Technical Specifications - Point 1, you have provided Per site traffic volume and in Point 2 you have mentioned retention requirement of 5 days packet level data. But in this point you have mentioned NBAD Sizing requirement of 30 Gbps traffic. As per our understanding, we need to use the Per Site Traffic Specifications and Retention Period mentioned under "Annexure F – Technical Compliance.xlsx" to meet LIC Requirements, please confirm.	Please be guided by the RFP
20	3. Sizing Requirements	Point 5 - Packet Capture	71	Packet Capture 30 Gbps or its equivalent Packets per Second	In "Annexure F – Technical Compliance.xlsx", PCAP Technical Specifications - Point 1, you have provided Per site traffic volume and in Point 3 you have mentioned retention requirement of 5 days packet level data. But in this point you have mentioned Packet Capture Sizing requirement of 30 Gbps traffic. As per our understanding, we need to use the Per Site Traffic Specifications and Retention Period mentioned under "Annexure F – Technical Compliance.xlsx" to meet LIC Requirements, please confirm.	Please be guided by the RFP
21	6. Eligibility Criteria	Eligibility Criteria, Point 6	15	The proposed OEM for the SIEM Solution should figure in the Leaders or Challengers Quadrant of Gartner in the last published report. This clause will not be applicable for the OEMs proposed or quoting of product under the regulations of Make In India. Latest published Report of Gartner or appropriate documents supporting Make In India Claim.	Requesting LIC to get the Gartner criteria removed from the eligibility criteria since it violates Ministry of Commerce and Industry issued restrictive eligibility criteria for OEM selection document released as on 20th Dec 2022 The link to the above referred document is : https://www.meity.gov.in/writereaddata/files/OM%20to%20All%20Ministries%20Depts%20wrt%20common%20eg%20of%20restrictive%20and%20discriminatory%20conditions%20against%20local%20suppliers%2012202022.pdf	Please be guided by the RFP
22	Technical Compliance for SIEM	Point 16	Sheet SIEM Technical Specifications	The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms, the solution should also allow admin to decide on the replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	!- Solution is asking for Active-Active stacks in DC and DR where technically replication is not required. OR Please change the clause and allow third party replication. "Proposed platform must support the data replication natively or through third party replication technologies on the operating system or storage level with near zero RPO and RTO. Platform should also allow admin to decide on replication factor with in DC and replication factor forDR. DR should always be active and should be updated with artifacts for any incident analyst is working on. "	Please be guided by the RFP
23	Technical Compliance for SIEM	Point 65	Sheet SIEM Technical Specifications	Machine learning should be embedded across the platform (such as but not limited to SIEM, SBDL, UEBA, etc.). It should empower every user in the SOC with ML. Security analyst should be able to build ML Models from UI i.e. using predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Machine learning models are delivered through ML Model which are pre-configured and managed by OEM only as they are complex in nature and requires high skill set. Custom data models is supported by limited OEM's only. Requesting LIC to please delete this point to allow more reputated OEM's to participate. OR Please change this to: "Machine learning should be embedded across the platform (such as but not limited to SIEM, SBDL, UEBA, etc.). It should empower every user in the SOC with ML. Security analyst should be able to build ML Models/Detection Rules from UI i.e. using predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models/Detection Rules with steps to build, train and implement model/Rules and There should not be any limitation in writting detection rules. An Analyst can write unlimited detection rules without any restriction on the license to detect threat anomalies. " ."	Please be guided by the RFP
24	Technical Compliance for SIEM	Point 69	Sheet SIEM Technical Specifications	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools such as (but not limited to) TensorFlow, PyTorch, R, Python, Scala, etc.	Machine learning models are delivered through ML Model which are pre-configured and managed by OEM only as they are complex in nature and requires high skill set. Custom data models can be a security concern as it exposes the Data Models to be manipulated.Requesting LIC Please Delete this point to allow more reputated OEM's to participate. OR Please change clause to: (Allow inbuilt non customised, self learning, inbuilt data model for ML) "The proposed solution must provide GUI that can easily help to build, built-in or custom/Self learning machine learning models/detection rules using the guided experience and should be able to augement the detection done using pre-built machine learning with alert rules. Proposed platform should natively have inbuilt ML capabilities and should not have separate engine / compute requirements for running ML models"	Please be guided by the RFP

25	Technical Compliance for SIEM	Point 72	Sheet SIEM Technical Specifications	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.	Request LIC to please delete the Clause as it is restricted. Justification : Each OEM has different approach to implement Use Cases, this is Specific and restricted clause we request to change the clause or delete the clause for wider participation	Please be guided by the RFP
26	Technical Compliance for SIEM	Point 73	Sheet SIEM Technical Specifications	The proposed solution should not have separate compute requirements to run the ML models. It should be embedded in the SIEM solution.	Request LIC to please delete the Clause as it is restricted. Justification : Each OEM has different approach to implement Use Cases, this is Specific and restricted clause we request to change the clause or delete the clause for wider participation	Please be guided by the RFP
27	Technical Compliance for UEBA	Point 17	Sheet UEBA Technical Specifications	The proposed solution should have the capability to employ models on Web Application Firewall (WAF) events for the purpose of identifying targeted web application attacks.	Request LIC to please delete the Clause as it is restricted. Justification : Employing or Deploying Models on third Party device is not the native functionality and capability of UEBA solutions, this is requested Clause hence we request LIC to remove the clause.	Please be guided by the RFP
28	Technical Compliance for PCAP	Additional Points	Sheet PCAP Technical Specifications	We request LIC to Include certain important Specifications as a Part of Packet Capture SOW and its core functionality to enchance the threat hunting and IOC detection and malware extraction, these are missing from the current specification.	!- Solution should be capable of performing Deep Packet Inspection (DPI) in all layers of the OSI stack (Layer 2-7) including application payload data and not just relying on header information like host, IP addresses etc.. !-The soluion must should be capable of doing full session reconstruction at the point of capture from raw packets to meaningful artefacts like email, FTP data files, VoIP conversations including PHP, JavaScript and .Net files should be able to do object extractions from sessions like pcaps, zip files, office documents, media, embedded malicious attachments etc. The system should provide a feature to extract various types of files from network traffic (.exe, .pdf, .doc, .gif, .jpeg, .wav, .mp3, etc.). !-For malware detection and analysis solution should extract the malicious embedded object for further analysis in a zip format with a password (to prevent the analyst from accidentally executing an illegal file, or to prevent automatic deletion by the AV software on the PC used for the investigation). !-Proposed platform should adopt technics to provide visibility into channels that are trying to blend in with other traffic, but do not follow normal protocol behaviour. Proposed solution should understand the behaviour of the protocol and highlight in case of any discrepancy !-It should be able to search more than 100 metadata items such as IP address, hostname, user account, command, email, filename, server name, client name, etc. based on the index, also provide an option for collection of raw packets	Please be guided by the RFP
29	Technical Compliance for PCAP	Additional Points	Sheet PCAP Technical Specifications	Additional Points for Packet Capture	We request LIC to include the following SOW points that should help the analysis in various Network Threat Detection use cases as listed below, but not limited to a) Continuous Monitoring: Ability to capture network traffic, index and play back all network data, and to provide Analyst with timely, targeted and prioritized information b) Remote Access / Web Shells: Full session reconstruction gives visibility into a common artifact left by attackers communicating with Web Shells (HTTP POST, no GET, no Referrer). After initial detection of suspicious activity, Proposed Solution should allow an analyst to see what the threat actor was doing on the compromised host, reconstruct exfiltrated data, and track lateral movement. c) Spear Phishing: Proposed Solution should reconstruct network protocols on the wire and can extract and analyze files being transferred. Combining this with deep file inspection, file anomalies signifying potentially malicious executable delivery can be alerted on and investigated. Spear phishing is a common delivery mechanism employed by attackers, often carrying malicious files (e.g. Encrypted executables, weaponized PDFs). d) Malicious Protocols - Gh0st RAT: Many commonly used remote access tools (RATs) have been programmed with custom network protocols to evade detection by traditional tools. Proposed solution should support through full session reconstruction and deep inspection into network traffic, is able to detect the Gh0st RAT protocol in real-time	Please be guided by the RFP
30	Technical Compliance for PCAP	Additional Points	Sheet PCAP Technical Specifications	Additional Points for Packet Capture	We request LIC include folloiwng Eligibility CRITERIA for Packet Capture OEM as this is missing to qualify quality OEM. 1. OEM should have provided similar solution for at least 2 BFSI customers in India during last 5 years. OEM to provide undertaking for same. 2. OEM to have ability to provide product support 24x7x365 from India 3. The proposed OEM should have presence in India for last 10 years. OEM Undertaking to be provided. 4. OEM should have centre of excellence in India with presence of core engineering, support, professional services functions and minimum employee strength of 300 people.	Please be guided by the RFP
31	Annexure F – Technical Compliance	SIEM- Technical specification		The proposed solution must be disaster recovery (DR) ready and should also provide a high availability (HA) feature at the log collection layer, logger layer, correlation layer and search layer. The bidder may choose to provide HA either natively (in case of appliance) or through OS based clustering (in case of software).	Kindly clarify whether the SIEM solutions should be in High Availability on DC as well as in DR.	Please be guided by the RFP

32	Section D: Current Environment	1. Current Environment	48	LIC is currently having the following structure and geographical spread: Corporate Office (also called as Central Office): Mumbai Zonal Offices: 8 (Bhopal, Kolkata, Chennai, Hyderabad, Kanpur, Delhi, Mumbai, Patna) Zonal training Centers: 8 (Bhopal, Kolkata, Chennai, Hyderabad, Agra, Delhi, Pune and Jamshedpur) Management Development Centre: 1 (Mumbai) Divisional Offices: 113 Pension & Group Superannuation Units: 74 BOs/ SOs/ MOs etc.: 4800 (approx.)	Considering the deployment with the Geographical spread shared on this point , it will be worthwhile for LIC to consider below points in the RFP for smooth operations. 1. The solution deployed should enable LIC to gain visibility across all network conversations, including east-west and north-south traffic, to detect both internal and external threats. 2. The solution deployed should ensure visibility with in the branch traffic as well as of end users for the lateral movements (within the branch and between Branch to branch) uptill the DO Offices minimally so as to ensure the security policy framework is well administered 3. The deployed solution for NBAD with visibility for end users til branches should be in such a way that the WAN utilization across MPLS links is minimally impacted to the order of 5-10%.	Please be guided by the RFP
33	Section E: Scope of Services	3. Implementing	53	Validation of deployment of the solutions/services to be performed based on industry best practices by respective OEM of the deployed solution/service. In case OEM is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a separate report to LIC accordingly. Bidder shall perform necessary changes as recommended by the OEM.	Request this be changed as below to accomodate OEM certified Partners. Validation of deployment of the solutions/services to be performed based on industry best practices by respective OEM of the deployed solution/service. In case OEM/OEM certified partner is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a separate report to LIC accordingly. Bidder shall perform necessary changes as recommended by the OEM/OEM certified partner.	Please be guided by the RFP
34	Section E: Scope of Services	3. Implementing	53	The OEM is required to conduct the audit, at the end of implementation and once in end of every year during the contract period. The recommendations/ remediation changes required after each audit should be completed within 3 months.	Request to limit OEM Vadidation for one time activity post deployment.	Please be guided by the RFP
35	Section E: Scope of Services	2. Detailed Scope of Work	62	The bidder shall also engage the services of the respective OEMs for post implementation audit, validation and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Request this be changed as below to accomodate OEM certified Partners. The bidder shall also engage the services of the respective **OEMs/OEM Certified Partner** for post implementation audit, validation and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Please be guided by the RFP
36	Section E: Scope of Services	2. Detailed Scope of Work	62	Bidder has to quote for highest/ premium support available from the OEM along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features, etc. for all the OEMs.	Request this be changed as below to accomodate OEM certified Partners. Bidder has to quote for highest/ premium support available from the OEM/OEM Cetified Partner along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features, etc. for all the OEMs/OEM certified Partners	Please be guided by the RFP
37	Section E: Scope of Services	3. Sizing Requirements	71	6. Network Behavior Anomaly Detection Proposed Sizing: 30 Gbps or its equivalent Flows Per Second or Packets per Second	LIC has evloved to SDN architecture on the DC depoying Cisco ACI which has distributed Gateway for the servers carrying the workloads in the DC , so becomes extremely important and critical for LIC to consider the East West traffic visibility apart from the North-South Traffic visibility traditionally done. Request this point be rephrased as below considering the East West Traffic (lateral movement) visibility asks inline to #34 of the NBAD Tech compliance ; Assuming similar traffic on East:West we ve arrived at double the number asked in RFP , LIC may guide us if this is otherwise. 6. Network Behavior Anomaly Detection Proposed Sizing: 60 Gbps or its equivalent Flows Per Second or Packets per Second	Please be guided by the RFP
38	Additional Inputs/Suggestions for the RFP				It will be worthwhile for LIC to consider below points in the RFP to ensure right design is in place for operations considering the DC/DR locations. 1. The deployed solution should ensure the Netflow is forwarded to NBI on LIC which consumes the Netflow without a need for the individual routers/swtches/FW to send dulicate flows to remote far ends consuming NW bandwidth unnecesarliy and also causing CPU utilisation on the Switches/Firewalls etc due to multiple flows enablement. 2. Creating a seaprate network for monitoring , observability , telemetry collection and troubleshoting will help LIC with operations ease in DC. With SDN being adopted with DC for LIC , we can place Network elements in each DC which will receive SPAN, telemetry, visibility, observability data from the ACI leaf switches and then send this info to the flow collectors/far end devices for visibility/observabliity as aproporate keeping this traffic separated from the Data Traffic.	Please be guided by the RFP
39	6. Eligibility Criteria		14	The Bidder must have an annual turnover of minimum Rs. 600 Crores per annum during the last 03 (three) years preceding the date of this RFP.	We request you to revise this clause as "The Bidder must have an Average annual turnover of minimum Rs. 600 Crores for the last 03 (three) years preceding the date of this RFP.	Please be guided by the RFP
40	6. Eligibility Criteria		14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	Please be guided by the RFP

41	Technical Bid		22	3	We undserstood that SI needs to provide security tools and licenses along with Hardware and Software i.e server/VMs, OS and Database as described in RFP and Rack, Power, ground support will be provided by LIC. Please confirm.	Please be guided by the RFP
42					Can we propose SaaS/hybrid tools also for all in-scope services for better resilliency and scalability?	Please be guided by the RFP
43	Annexture F			Techinical Specificition	We understood that initially we need to roll out 80,000 EPS from day 1? Please clarify.	Please be guided by the RFP
44				High Availability	Please help to share if any preference on Backup solution. What is the frequncy of backup (Daily, Weekly and monthly). Is there any retention policy available. Please confirm the type of backup requirment. Is there any compliance policy in place for backup.	Please be guided by the RFP
45	Point # 6	Eligibility Criteria	15	The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP.	The proposed OEM product for SIEM should have been successfully running in minimum three organizations with distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP.	Please be guided by the RFP
46	Point # 6	Eligibility Criteria	15	The proposed OEM for the SIEM Solution should figure in the Leaders or Challengers Quadrant of Gartner in the last published report. This clause will not be applicable for the OEMs proposed or quoting of product under the regulations of Make In India.	The proposed OEM for the SIEM Solution should figure in the Leaders or Challengers Quadrant of Gartner / IDC / Forrester in any of the last 3 years published report.	Please be guided by the RFP
47	Annexure F	Technical Compliance for SIEM	50	The proposed solution should act as common data lake for correlation between (but not limited to) SOAR, NBAD, UEBA and threat hunting, etc.	The proposed solution should have a data lake for correlation between (but not limited to) SOAR, NBAD, UEBA and threat hunting, etc.	Please be guided by the RFP
48	Annexure F	Technical Compliance for SIEM	56	The proposed solution must be designed to provide a query response within 30 seconds or less.	Response time of a query depends upon several factors like, the complexity of the query conditions, the size of the data on which the query is run, the mentioned period of the query, the fieldset type (indexed, unindexed) etc. Request to please elaborate and provide more details on the exact requirements of the use case.	Please be guided by the RFP
49	Annexure F	Technical Compliance for SIEM	108	The proposed solution must offer support for an automated health check mechanism that continuously monitors the operational status and performance of all system components. These health checks should encompass critical aspects of system functionality, including hardware, software, network connectivity, and service availability such as but not limited to, CPU usage spikes, RAM usage spikes, etc.	Request to delete the clause The specification mentioned in the clause is for a NMS solution and request to be deleted from the section.	Please be guided by the RFP
50	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	we request LIC to modify the clause as the Bidder or its OEM should have a minimum of 1 year of experience in supplying, implementing, and supporting a minimum 2 out of the 9 in-scope solutions in the multiple purchase order related to this RFP to organizations in PSU/Government/Private/BFSI Sector Firms with more than 500 endpoint licences across different locations in India"	Please be guided by the RFP
51	Section E: Scope of Services	1. Brief Scope of Work -> Asset Inventory (Indicative)	55	6. OS Servers - Linux	Here you have mentioned Linux, can you please elaborate exact OS name for Linux?	Please be guided by the RFP
52	Section E: Scope of Services		55	32. Linux Endpoints	Here you have mentioned Linux endpoints, can you please elaborate exact OS name for Linux?	Please be guided by the RFP
53	Section E: Scope of Services	1. Brief Scope of Work -> Security Dashboards:	58	As part of deliverables, bidder must provide integrated dashboard along with Display Panel / TV set covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc. The dashboard should be an easy-to-use web user interface with search function, create reports, as well as access cases and applications, with just a few clicks. The bidder should implement an integrated online security dashboard for services provided to LIC.	As a Bidder do we need to provide a Display Panel/TV set appliances with the proposed solutions? If this is the case it may require extra cost for the same.	Please be guided by the RFP
54	Section E: Scope of Services	2. Detailed Scope of Work -> I. General Requirements	61	The bidder needs to make sure that the solution deployed in DR has real time replication of data of DC. DR should be used for reporting, threat hunting, searching, etc.	The solution is required for only DC or both DC & DR locations.	Please be guided by the RFP
55	Section E: Scope of Services		63	All the solutions should be seamlessly integrated with the LIC's NTP solution and must be compatible with any provided NTP version.	Kindly help us with the name/OEM of the existing NTP solution.	Please be guided by the RFP
56	Section E: Scope of Services	2. Detailed Scope of Work -> II. Next-Generation Security Operations Center (NGSOC)	64	The vendor and OEM should develop out of the box use cases to identify and detect security incidents.	Kindly elaborate on what out-of-the-box use cases need to be developed.	Please be guided by the RFP
57	Section E: Scope of Services		65	The OEM should perform audits once after the implementation and once in every year and report the overall efficiency of the NGSOC. The remediations after the audit should be given. Additionally, should present an efficiency improvement plan to ensure continuous progress in detection.	Instead of OEM, can the bidder do the audits every year or it is compulsory to do by OEM only?	Please be guided by the RFP
58	Section E: Scope of Services	2. Detailed Scope of Work -> III. Security Information and Event Management (SIEM)	66	The vendor should ensure to provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non-standard logs and with all the solutions without any extra cost for LIC. These parsers should be implemented by the OEM.	Kindly help us with the name and code of the custom applications used by the LIC.	Please be guided by the RFP
59	Section E: Scope of Services		66	The vendor should have out of the box capability to create and customize dashboards.	We can create a custom dashlet or dashboard if that feature is available or else integrate with any 3rd party captive portal solution if required.	Please be guided by the RFP
60	Section E: Scope of Services	2. Detailed Scope of Work -> IV. Security Orchestration, Automation and Response (SOAR)	67	The bidder should guarantee that the solution allows for the inclusion of manual changes within automated workflows within 4 hours.	This needs to be checked by OEM if a provided solution can automate workflows within 4 hours.	Please be guided by the RFP
61	3. Sizing Requirements	3. Sizing Requirements	71	Sizing requirement	We request LIC to provide exact sizing for BoQ and future growth percentages	Please be guided by the RFP
62					Kindly clarify the hardware, OS, resources & database will be provided from LIC end?	Please be guided by the RFP
63					Suggestion to LIC- It is recommended to consolidate all nine solutions into a single agent and console, supplemented by the integration of an additional ITSM tool for efficient ticket management.	Please be guided by the RFP

64					Point to be added: "The proposed solution should store all the telemetry data collected from the LIC at MeitY compliant Data Centre in India and analytics should happen in India only." Justification: LIC is a nation critical infrastructure and to ensure data privacy and compliance requirement, the vendor shall ensure all the data collected and processed is within India region and CSP where vendor is hosted is MeitY empanalled. There are pub sector FSI institutions who has requested for the same when selecting a cloud delivered EDR soltion. pls refer GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please be guided by the RFP
65	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "The proposed CTI vendor to have their solution implemented in atleast 5 Bank/BFSI/National Critical Infrastructure Environment within India in last 3 years." Justification: We request this point to be added as it would make sure that a solution adopted & already deployed in LIC like environment in terms of size & complexity.	Please be guided by the RFP
66	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "The proposed solution should not enforce the license nor restrict the usage of the system incase of an incidental increase of the platform users." Justification: The reason to add this point is in case if increase of users which is unplanned, the solution should not restrict the user until LIC decides to go for additional licenses.	Please be guided by the RFP
67	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "Proposed CTI solution should have convergence of Investigation data and Threat Intel data in a single platform where IOCs are auto-correlated with existing incident data to provide real-time context to LIC for incident response." Justifiation: We request this point to be added as it would provide critical additional context to the existing incidents.	Please be guided by the RFP
68	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "Poposed CTI solution should support out of the box playbook mapped to all the MITRE Tactics for swift automated actions on the ingested threat intel." Justification: We request to add this as this point as it would have the playbooks mapped to the worldwide adopted MITRE framework.	Please be guided by the RFP
69	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "Solution should have a 5+ year history of scanning the internet. Documentation to be provided to substantiate the claim". Justification: This point is recommended to be added as it would make sure that the solution being proposed has been well adopted & has been in the domain for a reasonable time.	Please be guided by the RFP
70	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "Solution should rescan daily or faster to discover the newly propagated assets/services and same can be mitigated quickly if any issues associated with it." Justification: It is strongly recommeded to add this point as more frequent scans would provide visibility to LIC quicker than the potential time available to the attackers to discover it.	Please be guided by the RFP
71	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Points to be added: "Proposed EASM solution should have the ability to automatically remediate exposures natively as part of built-in workflow. This should include full resolution of the incident by reaching back via API and blocking the service at the port level." Justification: It is strongly recommeded to add this point as it is very important to remediate the exposures discovered by the EASM. This would make sure, that the vulnerability is taken care of giving the least amount of time to be exploited.	Please be guided by the RFP
72	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: Out of the box(OOTB) Case management functionality & integration to case management tools." Request to add this point as it would it having the context of threat intel to cases being worked upon by analysts/soc engineers would provide them with additional information & help them respond.	Please be guided by the RFP
73	Annexure F	Technical Compliance for Threat Intelligence		Request this new point to be added	Point to be added: "Out of the Box integration to communication/notification". For the solution to be adopted & have ease of use, it is important that it has out of the box integration with communications/notifications systems.	Please be guided by the RFP
74	Annexure F	Technical Complinace for SOAR		Request this new point to be added	Point to be added: "The integrations/playbooks should run in their individual container." It is strongly recommened to add this point as it would make sure the playbook executions are secured & once integration configured does not interfere with another at runtime.	Please be guided by the RFP
75	Annexure F	Technical Complinace for SOAR		Request this new point to be added	Point to be added: "The SOAR solution should be dedicated & not part of the SIEM." It is recommded to add this point so that a dedicated SOAR solution with comprehensive feature/functionality is proposed. This would ensure the SIEM & SOAR are isolated & once does not affect the other in terms of functioning/resources etc..	Please be guided by the RFP
76	SIEM Compliance	Technical Specification	Point no. 1	The proposed solution must be able to handle 60000 EPS sustained with scalability without any additional hardware/ licence sustained up to 80000 EPS from day one.	Please share the break-up of each site with its EPS & FPM distribution/consumption.	Please be guided by the RFP
77	SIEM Compliance	Technical Specification	Point. 12	If the primary analysis/ correlation engine is not functional all correlation activity should be possible from secondary sites as well.	Please confirm if the correlation engine failure can failover to the secondary available node as high availability failover. Also if both the correlation engine fails then we can perform the site level failover - Please confirm if this is acceptable	Please be guided by the RFP

78	SIEM Compliance	Technical Specification	Point. 14	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be available on the connectors/log collectors. It should be configurable as per requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.	Most of the SIEM tools supports DC DR replication by many different ways. The design with dual log forwarding is one of the method which is a manual make shift arrangement to move logs between the sites. This approach has some down sides like a connectivity issue can cause data loss leading to data inconsistency. To avoid such problem new gen SOC adopted tool driven approach to write the logs between DC & DR sites-In this one site is active and other site is passively receiving the replicated data. The DR site will be made active only when the primary site fails - please confirm if this is acceptable.	Please be guided by the RFP
79	SIEM Compliance	Technical Specification	Point. 15	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO. Use Case: In future if it is decided to run both DC & DR Active-Active, then the entire cluster should work as single cluster which is deployed in DC & DR.	This point indicates a different architecture as single cluster compared to the dual log forwarding mentioned in point no. 14. The site peering can be done in multiple ways and we suggest this to be done by proposing active-passive architecture using SIEM native capabilities - please confirm if the peering done by active-passive with minimum of 5 mins of RPO/RTO as the lowest.	Please be guided by the RFP
80	SIEM Compliance	Technical Specification	Point. 16	The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms, the solution should also allow admin to decide on the replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	The required data is already taken care as a native replication that includes the artifacts. However the same is only available from DR site once the DR site is promoted as active site and failover is performed from DC to DR. please confirm if this is acceptable	Please be guided by the RFP
81	SIEM Compliance	Technical Specification	Point. 41	The proposed solution should support SAN, NAS and DAS for adding external storage as and when required.	Please confirm if it is fair to assume NAS & DAS storage requirement is for storing the archived data & not for the online log & flow data - please help in clarifying this.	Please be guided by the RFP
82	SIEM Compliance	Technical Specification	Point. 50	The proposed solution should act as common data lake for correlation between (but not limited to) SOAR, NBAD, UEBA and threat hunting, etc.	Is it fair to assume that it could be a common repository and not necessarily be a Data lake only?	Please be guided by the RFP
83	SIEM Compliance	Technical Specification	Point. 61	The proposed solution must have the ability to create correlation rules by weighing the TIP feeds based on priority/confidence score.	Is it fair to assume that TIP feed with weightage will be provided by LIC?	Please be guided by the RFP
84	SIEM Compliance	Technical Specification	Point. 68	The proposed solution must possess built-in function for Predictive Analysis: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customize the results Indicative Use Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console weather this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.	Please confirm if this can be achieved via Anomaly & behavioural rules within the SIEM	Please be guided by the RFP
85	SIEM Compliance	Technical Specification	Point. 90	The proposed solution should have end user and admin access with required licenses for unlimited users.	The tool doesn't have any license on the users, however it may run out of resource capacity incase kept unlimited.	Please be guided by the RFP
86	SIEM Compliance	Technical Specification	Point. 106	The vendor needs to be responsible for ensuring that the implemented solution complies with the specifications detailed in ISO 27001, ISO 27002, PCI DSS,IRDAI, CERT-IN, IT ACT 2000,SEBI, DPDP 2023, etc and other laws of the land applicable to LIC.	You are requested to share the applicable compliance for the OEM providing the tool and share the relevant applicable control for the tool provider.	Please be guided by the RFP
87	SOAR Compliance	Technical Specification	Point. 9	The solution should have source code available for review for automations, playbooks and integrations.	The required source code will be available for the custom content created for the SOAR platform. Please confirm if this is acceptable.	Please be guided by the RFP
88	SOAR Compliance	Technical Specification	Point. 40	The solution should have version control capability for playbooks, allowing for viewing version history for all or selected playbook and provide option for restoring to an older version.	Our SOAR solution has ability to create a duplicate playbook with a specific version naming of the playbook itself. The same can be downloaded for modification and then uploaded as a different/new version - please confirm if this is acceptable.	Please be guided by the RFP
89	SOAR Compliance	Technical Specification	Point. 41	The solution should allow addition of ad hoc tasks during live execution within a playbook.	The platform generates the required task within a case based on the dynamic progression of the incident. Please confirm if this is acceptable	Please be guided by the RFP
90	SOAR Compliance	Technical Specification	Point. 64	The solution should have bi-directional capability to mirror investigation in Slack, MS Teams or any other LIC's communication channels for external collaboration in real-time.	The SOAR tool can integrate with MS Teams for posting the information about the incident or task directly to MS Channel - please confirm if this is acceptable	Please be guided by the RFP
91	SOAR Compliance	Technical Specification	Point. 69	The solution should have the capability to conduct analytics and investigations and also provide recommendations in accordance with any globally recognized frameworks, such as the MITRE ATT&CK framework, Cyber Kill Chain Model, NIST, etc.	Our solution supports the larger framework as MITRE Framework which covers the techniques (total 18) against the 7 tactics specified in Cyber Kill Chain - please confirm if this is acceptable.	Please be guided by the RFP
92	SOAR Compliance	Technical Specification	Point. 71	The solution's collaboration capability should be extended to external users (such as but not limited to internal or external council, HR, PR, etc.).	Is it fair to assume that external users can collaborate via Teams & Slack integration with SOAR - please confirm	Please be guided by the RFP
93	SOAR Compliance	Technical Specification	Point. 103	The vendor needs to be responsible for ensuring that the implemented solution complies with the specifications detailed in ISO 27001, ISO 27002, SEBI, IRDAI, PCI DSS, CERT-IN, IT ACT 2000, DPDP 2023, etc. and any other law of the land applicable for LIC.	You are requested to share the applicable compliance for the OEM providing the tool and share the relevant applicable control for the tool provider.	Please be guided by the RFP
94	UEBA Compliance	Technical Specification	Point. 9	The proposed solution should support standard methodologies such as Cyber Kill Chain, MITRE ATT&CK framework, NIST, etc. and other leading frameworks and provide suggestions for remediation.	Our solution supports the larger framework as MITRE Framework which covers the techniques (total 18) against the 7 tactics specified in Cyber Kill Chain - please confirm if this is acceptable.	Please be guided by the RFP
95	UEBA Compliance	Technical Specification	Point. 14	The proposed solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time.	The identity/entity related use cases can be achieved via NBAD components as a work around - please confirm if this is acceptable	Please be guided by the RFP
96	UEBA Compliance	Technical Specification	Point. 15	The proposed solution should not send data to any cloud for processing of UEBA models. All ML models in UEBA should run on-premise only.	The following points require both flows and network details along with information of entity, this usecase is more inclined toward a dedicated UEBA solution instead of UBA solution. It is thus requested to make this point optional to help promote higher participation.	Please be guided by the RFP
97	UEBA Compliance	Technical Specification	Point. 17	The proposed solution should have the capability to employ models on Web Application Firewall (WAF) events for the purpose of identifying targeted web application attacks.	This point appears to be OEM specific and we request you to make it optional to help promote higher participation	Please be guided by the RFP
98	UEBA Compliance	Technical Specification	Point. 18	The proposed solution should have flexibility to configure rolling window for a period of minimum 30 days for behaviour profiling.	Please confirm if the rolling period is between 7-15 days instead of 30 days	Please be guided by the RFP

99	UEBA Compliance	Technical Specification	Point. 23	The proposed solution should have the capability to store anomalies identified from log sources such as (but not limited to) Firewall, IDS, IPS, Active Directory , Office365, etc.	This point can be achieved via SIEM deliverables - please confirm if this is acceptable	Please be guided by the RFP
100	UEBA Compliance	Technical Specification	Point. 31	The proposed solution should have capability for identity threat analytics for IDPs such as but not limited to Azure AD, Okta, Google identity, etc.	Integrating the mentioned IDP's would be possible provided the availability of LDAP integration from it - please confirm	Please be guided by the RFP
101	UEBA Compliance	Technical Specification	Point. 40	The proposed solution should offer dashboards and reports that deliver daily, weekly, and monthly insights regarding high-risk users and entities based on their risk score ratings.	The following points require both flows and network details along with information of entity, this usecase is more inclined toward a dedicated UEBA solution instead of UBA solution. It is thus requested to make this point optional to help promote higher participation.	Please be guided by the RFP
102	UEBA Compliance	Technical Specification	Point. 42	The proposed solution should have exporting and report generation capabilities such as but not limited to Excel, PDF, XML, etc.	The tool has capability for reporting CSV, PDF & XML is used for exporting the rules, log source parsing etc. Please confirm if this is acceptable	Please be guided by the RFP
103	UEBA Compliance	Technical Specification	Point. 43	The proposed solution should have low-latency and not affect the performance of data lake. Results from the queries should be available within 5-minutes from execution.	The Query response time largely depends on multiple factors like query syntax, HW resources, load on the system etc. Most of the OEM providing the 5 mins commitment will limit the number of results/capping first 1000 logs. Please consider this point as optional or also add the point to ensure that query result shouldnt terminate or truncate any number of results queried by the analyst.	Please be guided by the RFP
104	UEBA Compliance	Technical Specification	Point. 48	The vendor needs to be responsible for ensuring that the implemented solution complies with the specifications detailed in ISO 27001, ISO 27002, SEBI, IRDAI, PCI DSS, CERT-IN, IT ACT 2000, DPDP 2023, etc. and any other law of the land applicable for LIC.	You are requested to share the applicable compliance for the OEM providing the tool and share the relevant applicable control for the tool provider.	Please be guided by the RFP
105	PCAP Compliance	Technical Specification	Point. 7	The solution should support for capturing and storing data from (but not limited to) multiple network segments, VLANs, network locations, etc. The solution must be capable of supporting Public or Private Cloud infrastructure deployment using industry standard ecosystems. The solution should support deployment into Public Cloud platforms like Amazon Web Services (AWS), Microsoft Azure environments, Google Cloud, etc. The solution should be capable of capturing traffic on Private Cloud, Containers, Dockers & other virtual Infrastructure without the need of third party components. > Microsoft Hyper-V > VMware's ESX, NSX-V & NSX-T > OpenStack > Ubuntu/KVM	Capturing NW data/meta-data can be done from the mentioned sources via NBAD solution. As there are provisions available like VTAP, VPC Flows etc for gaining the NW visibility from the cloud/virtual environment. - Please move this point to NBAD complaince. The PCAP solution will need raw port mirroring and the same can be deployed to on-prem form factor as it requires TAP/Mirror ports that capture the RAW packets.	Please be guided by the RFP
106	PCAP Compliance	Technical Specification	Point. 16	The solution should provide real-time analysis capabilities for immediate insights into network behaviour and potential security incidents.	This is taken care in NBAD tool - please remove this from PCAP compliance	Please be guided by the RFP
107	PCAP Compliance	Technical Specification	Point. 29	The solution should analyse packet data using integration with 3rd party intelligence (IOC) , for threat detection and highly contextual investigation.	The packet data and tool is tieing back to the SIEM tool where this is taken care - please confirm if this is acceptable.	Please be guided by the RFP
108	PCAP Compliance	Technical Specification	Point. 32	The solution should use cases to detect the following incident categories (but not limited to): -DDOS attack -Suspicious communication over non standard port -Data exfiltration -Command and Control communication -The Onion Router usage -SSH with watched country -Privacy VPN usage -Reconnaissance attack -Detection of unknown DGA (domain generation algorithm) attack	This is taken care in NBAD tool - please move this from PCAP to NBAD compliance	Please be guided by the RFP
109	PCAP Compliance	Technical Specification	Point. 37	The solution should have risk assessment analysis and attack surface analysis to focus on the risk rather than focusing solely on the threats.	This can be achieved by NBAD tool - please confirm if this is acceptable	Please be guided by the RFP
110	PCAP Compliance	Technical Specification	Point. 38	The solution should look for potential risks in the LIC environment such as (but not limited to) known insecure application such as Rlogin, telnet, expired or self-signed certificates, etc.	This can be achieved by NBAD tool - please confirm if this is acceptable	Please be guided by the RFP
111	PCAP Compliance	Technical Specification	Point. 40	The solution should have the out of the box capability to generate and schedule custom reports based on specific criteria, timeframes, or data fields as and when required.	This can be achieved by NBAD tool - please confirm if this is acceptable	Please be guided by the RFP
112	PCAP Compliance	Technical Specification	Point. 41	The solution should have predefined report templates for common use cases, such as (but not limited to) traffic analysis, security incidents, or compliance reporting.	This can be achieved by NBAD tool - please confirm if this is acceptable	Please be guided by the RFP
113	PCAP Compliance	Technical Specification	Point. 43	The solution should have capability to automate and visualize traffic patterns.	This can be achieved by NBAD tool - please confirm if this is acceptable	Please be guided by the RFP
114	PCAP Compliance	Technical Specification	Point. 46	The vendor needs to be responsible for ensuring that the implemented solution complies with the specifications detailed in SEBI, IRDAI, PCI DSS, CERT-IN, IT ACT 2000, DPDP 2023, RBI etc. and any other law of the land applicable for LIC.	You are requested to share the applicable compliance for the OEM providing the tool and share the relevant applicable control for the tool provider.	Please be guided by the RFP
115	NBAD Compliance	Technical Specification	Point. 3	The solution should comply with industry standards, such as IRDAI, RBI, DPDP, SEBI, CERT-IN, IT ACT 2000, etc. and any law of the land applicable for LIC.	You are requested to share the applicable compliance for the OEM providing the tool and share the relevant applicable control for the tool provider.	Please be guided by the RFP
116	NBAD Compliance	Technical Specification	Point. 9	The solution should have the capability to integrate with external threat intelligence feeds which has a confidence level more than 70 % to enhance anomaly detection with up-to-date threat information.	This point can be achieved via SIEM deliverables - please confirm if this is acceptable	Please be guided by the RFP
117	NBAD Compliance	Technical Specification	Point. 10	The solution should have the ability to state fully reassemble unidirectional flows into bi-directional conversations; handling deduplication of data and asymmetry and eliminate redundant packets or telemetry to improve system performance.	The mentioned action is performed by the Traffic/TAP aggregators which sends these inputs to NBAD solution - Please confirm if this is acceptable	Please be guided by the RFP
118	NBAD Compliance	Technical Specification	Point. 13	The solution should integrate with existing cyber security solutions such as (but not limited to) SIEM, SOAR, EDR, NAC,UEBA etc. to alert the admin, provide mitigation actions like quarantine / block / apply custom policies both automatically on the endpoint to block further spread of the malware/worm across the network without affecting legitimate traffic on the network.	The solution will integrate SIEM SOAR for monitoring and orchestrating the response action. Also will leverage the existing tools/technology for performing the actions like blocking/quarantine etc.. - Please confirm if this is acceptable	Please be guided by the RFP
119	NBAD Compliance	Technical Specification	Point. 16	The solution must store processed telemetry or packet metadata in a redundant fashion such that data is accessible for querying and reporting even in the case of a failure of the telemetry or packet metadata processing component.	It is understood that the component holding data is made available from alternate node while local device failure and from the alternate site incase of a site level disaster - please confirm	Please be guided by the RFP
120	NBAD Compliance	Technical Specification	Point. 17	The solution should be a dedicated behaviour analytics solution delivering advanced Network Detection & Response (NDR) use cases and not a subset capability of SIEM or PCAP solution.	The NBAD solution having its own ML algorithm mapped under SIEM console ensuring no performance or capability is lost. At the same time, analyst gets a unified console to manage the UBA & SIEM - please confirm if this can be acceptable.	Please be guided by the RFP

121	NBAD Compliance	Technical Specification	Point. 39	The solution should be capable to classify, extract and reconstruct network activity along with session reconstruction and packet analysis. No data should be sent to any 3rd party or open source components and cloud for any type of analysis.	This is taken care in PCAP tool - please move this from NBAD to PCAP compliance	Please be guided by the RFP
122	Section E: Scope of Services	3. Sizing Requirements	71	6. Network Behavior Anomaly Detection Proposed Sizing: 30 Gbps or its equivalent Flows Per Second or Packets per Second	Request this be rephrased as below considering the East West Traffic(lateral movement) visibility asks inline to #34 of the NBAD Tech compliance ; Assuming similar traffic on East:West we ve arrived at double the number asked in RFP , LIC may guide us if this is otherwise. 6. Network Behavior Anomaly Detection Proposed Sizing: 60 Gbps or its equivalent Flows Per Second or Packets per Second	Please be guided by the RFP
123	General query			General query	LIC will provide the underlying hardware/VMs/Storage required for new solutions. Will LIC team install the provided infrastructure or bidder to supposed to install it?	Please be guided by the RFP
124	Section E: Scope of Services	Support Process Requirement:	58	The on-site L1 and L2 support may also be required to work on Sunday/LIC holidays or beyond office hours on working days, for which an advance notice will be given.	Is this or operations team or project implementation team also?	Please be guided by the RFP
125	Section C: Instructions to Bidders (ITB)	Rights reserved by LIC	41	Ascertain the effectiveness and efficiency of the resources deployed for this project through interview, performance review etc. and insist for proper substitute.	We suggest that LIC conduct interviews for L2 and above grade only & L1 candidates can be selected by Bidder itself	Please be guided by the RFP
126	Section E: Scope of Services	Transition from existing SOC to NGSOC:	60	Manage day to day operations of currently running SOC setup from two months from date of issuance of PO.	Please specify the timeline upto which the current setup is to be mnaged by new partner	Please be guided by the RFP
127	Section E: Scope of Services	Transition from existing SOC to NGSOC:	60	Bidder must ensure that the existing data remain usable for necessary searching, link analytics, hunting, regulatory requirements, forensic investigation etc.	Please specify the current data retention policy in place	Please be guided by the RFP
128	Eligibility Criteria	Eligibility Criteria	15	The Bidder must have an annual turnover of minimum Rs. 600 Crores per annum during the last 03 (three) years preceding the date of this RFP	Request to amend the clause as below The Bidder must have an annual turnover of minimum Rs. 500 Crores per annum during the last 03 (three) years preceding the date of this RFP	Please be guided by the RFP
129					Kindly clarify Hardware, OS, Resources, and database that will be provided from the LIC end.	Please be guided by the RFP
130	6 - Eligibility Criteria	S. No - 1	14	The bidder must be a registered legal entity in India	Please confirm if Limited Liability Partnership form of organization is eligible	Please be guided by the RFP
131	6. Eligibility Criteria	6.6	15	The proposed OEM for the SIEM Solution should figure in the Leaders or Challengers Quadrant of Gartner in the last published report. This clause will not be applicable for the OEMs proposed or quoting of product under the regulations of Make In India.	We request LIC to only consider Gartner Leaders Quadrant as leaders consistantly innovate and address critical SOC requirements and help detect complex threats.	Please be guided by the RFP
132	3. Technical Bid	3. Technical Bid	22	LIC will be responsible to provide all the hardware required for in-scope solutions' implementation, i.e server/VMs and will provide RHEL OS and Database – MySQL, if required as part of the solution. All other software and hardware if any should be provided by bidder, included in BoQ and prices quoted for in the Commercial Bid Document.	We assume that LIC will supply the server, storage, operating system, database, network, and backup needed to implement the NGSOC components. This should not be restrictive to specific & named solution as this may indicate that LIC is providing an unfair advantage to specific OEMs whoes solutions are based on the above basline solutions. Also, provide clairty on the Top of the Rack switiches and integration with existing LIC's network and security ecosystem. As this service elements are provided by LIC and LIC's Partners, it will be advantageous for seamless integration that LIC provides these elements for NGSOC to ensure uniformity in its systems and services	Please be guided by the RFP
133	25. Placing of Orders and Making Payments	Point a	35	The Central Office of LIC at Mumbai will place orders (either in full or in phases) with successful bidder for deliverables under this RFP at any time during the validity period of this tender.	All the pricing submitted to LIC is based on the assumption that the full scope of the RFP. Request LIC to either declare the phases in the RFP. Also, this may impact the project payout & signoff criteria. Hence, Request LIC to remove this clause & provide to place order in full as price may be linked to the size/quanity of the products.	Please be guided by the RFP
134	43. Right to Verification		41	LIC reserves the right to verify any or all the statements made by the Bidder in the tender document and to inspect the Bidder's facility related to scope of work, if necessary, to establish to its satisfaction the Bidder's capacity/ capabilities to perform the job .	Request to modify as the entire work is being delivered out of LIC office.	Please be guided by the RFP
135	55. Varying the Services	Point I	46	LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, etc. cost to be quoted in the commercial bid. Any change in the scope beyond this 25% will be informed to the vendor in writing. If LIC wants to vary the Services:	These prices will be indicative and will need to be appropriatly substanciated by factoring- curreny fluctuation, inflation and the impact of additional scope on the existing SOC management team. It may also neccessitate in adding adddtional resouces for support the current services.	Please be guided by the RFP
136	point 1 : Brief Scope of Work	Phase 3: Implementing	52	Bidder shall recommend ways for secure communication and assist LIC in defining the use cases as applicable for the solutions. All such configurations/ changes shall be documented as part of the policy/process documentation. The use cases created should be undergoing the full use case lifecycle such as creation, testing, finetuning of false positive, automation, notification to the LIC specified personnel, etc.	This is scope of on-site to provide continous improvement in reference to LIC's enviornment. As a bidder, we require clear-cut goals for implementation team to ensure the solutions are implemented and operationalized. Hence only limited scope of implementatoin of such use cases will be undertaken to ensure sufficent implemenation is achieved in specified number of weeks. Rest of the improvements, new use cases, etc will be undertaken during steady state operations. Kindly change and move this point to sustainance phase.	Please be guided by the RFP
137	point 1 : Brief Scope of Work	Compliance with IS Security Policy:	54	The SI shall have to comply with LIC's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder.	LIC will be responsible for providing standards applicable for the services mentioned in the RFP. Appropriate communication, workshop and trainings should be provided for the same.	Please be guided by the RFP
138	Compliance with IS Security Policy:		54	Physical and logical separation from other customers of the Vendor	Services are being delivered out of LIC offices.	Please be guided by the RFP
139	point 1 : Brief Scope of Work	Asset Inventory (Indicative)	55	Please find below the indicative asset inventory list of LIC:	It will be helpful if LIC indicates the minimum assets list be mandatory for operationalizing the NG-SOC and to achive sign-off criteria. This will help in achieving meaning full transistion and measurable objectives to move into sustainance phase.	Please be guided by the RFP
140	point 1 : Brief Scope of Work	Documentation	56	All the documents shall be supplied in properly bound volumes of A4 size sheets. Three sets of hardcopies as applicable and one softcopy on USB shall be supplied as final document.	Looking at the sustainability and enviornmental goals. Request LIC to consider technical deliverables in e-format. Printing and submitting these documentation on papers may impact the sustainability initiatives undertaken by Government of India and also violate our commitments to the same.	Please be guided by the RFP

141	point 1 : Brief Scope of Work	Documentation	56	Vendor shall also submit Delivery and Installation Report, Warranty certificates, License Copies for all the items supplied along with the supplies.	Please indicate what are the specific documents , solution-wise accepted by your procurement team to ensure smooth process of acceptance of the document. All warranty. Service inititations and license validations are delivered directly to identified SPOC of LIC. It is LIC's SPOC's duty to ensure that procurement is apprised of all the relevant deliverables to their procurement teams. Bidders team faces un-neccessary troubles in fulfilling these criterias shared are the last moment.	Please be guided by the RFP
142	point 1 : Brief Scope of Work	Documentation	56	Vendor shall ensure to guarantee that the documentation of all the process related to the NGSOC such as (but not limited to) tenant provisioning, implementation, onboarding of data sources, 24/7 monitoring, threat hunting, incident management, threat intelligence, forensic investigation, forensic investigation, severity SLA, incident response plan, regulatory guidelines (CERT-In, RBI, IRDAI, SEBI, etc.) should be documented and submitted as part of the process documentation	Request you to remove the word - guarantee, as the bidder will be supporting LIC in all the relevant 3rd party assessments for the NG-SOC. Also, updation of document is a periodic process. Hence the usage of the word is conflicting	Please be guided by the RFP
143	Section E: Scope of Services	Section E: Scope of Services	58	No telephone connection will be provided by LIC to the onsite support persons.	Could you please clarify which communication channel (LIC email, their own mobile) the SOC team will use to coordinate and communicate with LIC officials and other team members? In such large RFP & LIC being such a prestigous organization, restricting such communication channels, will impact LIC and lossen LICs' controls.	Please be guided by the RFP
144	Security Dashboards		58	The dashboard should be secure web based with multi factor authentication enabled online portal available over desktop, Mobile, Tablet and iPad.	LIC should ensure that the existing authentication platform to enable achivement of this particular ask is available and LIC will extend all the support necessary to the bidder to intergrate and achieve the functionality.	Please be guided by the RFP
145	Security Dashboards		59	The dashboard should be provided as integrated view by integrating with the following tools	Specifying a specific view of dashboard is limiting the deliverables. Request LIC to ensure addition of the " Where ever feasiable ". Before the start of such work, bidder will work on mutual agreed deliverables in phases to ensure dashboard is delivered.	Please be guided by the RFP
146	2. Detailed Scope of Work	I. General Requirements	62	Bidder has to quote for highest/ premium support available from the OEM along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features, etc. for all the OEMs.	Request LIC to add this point as part of the MAF to be shared by the OEMs	Please be guided by the RFP
147	Section E: Scope of Services	2. Detailed Scope of Work	63	The successful bidder shall co-ordinate and co-operate with the other vendors appointed by the LIC so that the work shall proceed smoothly without any delay and to the satisfaction of LIC.	LIC has to enforce appropriate structure and governance model to ensure smooth coordinantion. Based on the past experience, there have been many governance issues, where the coordination is left in the hands of vendors.	Please be guided by the RFP
148	Section E: Scope of Services	2. Detailed Scope of Work	63	Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.	This is an open statement. Request you to modify " Successful bidder will conduct a site survey to ensure that all the relevant components to be provided by LIC is mentioned. Post confirmation of site-survey and submission of the BoM to LIC, if any components, are missing, then this clause shall be applicable.	Please be guided by the RFP
149	SLA & Penalty	Project Phase level SLA:	84	Ensure that any technical issues escalated, but not resolved by the on-site Personnel/vendor, should be closed/ resolved within 1 day.	Request LIC to specify an example on what conditions trigger this SLA and how this will be calculated and applied. ? This may end up being a simple tool of red-tapism and dispute.	Please be guided by the RFP
150	SLA & Penalty	Project Phase level SLA:	84	Failure to ensure collection of all logs for which the solutions have been procured.	Request LIC to specify an example on what conditions trigger this SLA and how this will be calculated and applied. ? This may end up being a simple tool of red-tapism and dispute.	Please be guided by the RFP
151	SLA & Penalty	Project Phase level SLA:	85	Point no 17,18 The on-site Personnel or his designated substitute should be present in LIC's premises as per the RFP conditions. If the on-site Personnel leaves before expiry of 1 year for reasons other than death and hospitalisation.	After such rigourous process and such stringnent compliance, it is preposterous on part of LIC to apply such SLAs on the bidder. No bidder has control on the resource and such contracual terms with the employees for the project may be unsustainable in court of law. Kindly request you to remove this SLA penalties as they embed a great seed of distrust with the bidder.	Please be guided by the RFP
152	SLA & Penalty	Penalties on Non-Performance of SLA during contract period:	86	Updates should be provided over email at intervals :- Critical, High, Medium and Low	LIC's ITSM tool should be configured to automatically support sending such updates and workflows. Without such provision, it will add tremendous impact on the onsite resource as they will lose the focus with respect to SOC operations and focus more on providing the updates. Request if LIC mandates its ticketing vendor to support the bidder's objective accordingly	Please be guided by the RFP
153	SLA & Penalty	Threat intelligence accuracy	89	Threat intel feeds should have confidence more than 90% and should be incorporated into all possible alerts/alert flow/ incident response.	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis.	Please be guided by the RFP
154	SLA & Penalty	Security Intelligence Services	89	Advisories within 12 hours of any new major global threats & vulnerabilities disclosures.	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis.	Please be guided by the RFP
155	SLA & Penalty	SLA & Penalty	89	Open OEM Support tickets/cases: Unable to close the OEM support tickets within 2 weeks without any workaround	Penalty should not imposed on SI if OEM doesn't have workaround. Please remove this clause	Please be guided by the RFP
156	SLA & Penalty	Security Intelligence Services	91	All solutions must guarantee the capability to retrieve data within 48 hours from their offline storage mechanism.	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis. Beyound SIEM, why is this necessary or required ?	Please be guided by the RFP
157	Section G: Payment Terms & Conditions	N/A	99	Delivery of software and appliances : Certificate by the bidder indemnifying the Corporation against Violation of Copyright and Patents.	This is already part of the RFP terms and conditions. Adding this additonal requirement is not necessary and creates more complexity	Please be guided by the RFP
158	Section G: Payment Terms & Conditions	N/A	99	Installation and integration, initial OEM audit and acceptance testing as per scope of work. o Certificate by the bidder indemnifying the Corporation against Violation of Copyright and Patents etc. o OEMs certification of the deployment being in accordance with the scope of work. o Receipt of Installation certificate & sign-off duly signed and stamped by the Bidder, and counter-signed by the officials of IT dept., LIC Central Office.	This is already part of the RFP terms and conditions. Adding this additonal requirement is not necessary and creates more complexity Please remove " o Certificate by the bidder indemnifying the Corporation against Violation of Copyright and Patents etc. o OEMs certification of the deployment being in accordance with the scope of work. " and Also LIC central office is verifying everything. KIndly do the needful	Please be guided by the RFP

159			113		Point to be added: "The proposed solution should store all the telemetry data collected from the LIC at MeitY compliant Data Centre in India and analytics should happen in India only." Justification: LIC is a nation critical infrastructure and to ensure data privacy and compliance requirement, the vendor shall ensure all the data collected and processed is within India region and CSP where vendor is hosted is MeitY empanalled. There are pub sector FSI institutions who has requested for the same when selecting a cloud delivered EDR soltion. pls refer GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please be guided by the RFP
160	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point no. 1The proposed solution must be able to handle 60000 EPS sustained with scalability without any additional hardware/ licence sustained up to 80000 EPS from day one.	Please share the break-up of each site with its EPS & FPM distribution/consumption.	Please be guided by the RFP
161	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point no. 2The peak EPS that the proposed solution can address without any additional license, server, storage or appliance should be minimum twice than the sustained EPS proposed.	Please confirm the HW sizing to be done for 80k EPS or 1.6L EPS (twice as stated in point no. 2)	Please be guided by the RFP
162	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 14The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be available on the connectors/log collectors. It should be configurable as per requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.	Most of the SIEM tools supports DC DR replication by many different ways. The design with dual log forwarding is one of the method which is a manual make shift arrangement to move logs between the sites. This approach has some down sides like a connectivity issue can cause data loss leading to data inconsistency. To avoid such problem new gen SOC adopted tool driven approach to write the logs between DC & DR sites-In this one site is active and other site is passively receiving the replicated data. The DR site will be made active only when the primary site fails - please confirm if this is acceptable. Focus should be on achiving the SLA & availability rather the method is which it is to be achieved. Specifying methods may seem to be aligning with particular OEM solution.	Please be guided by the RFP
163	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 15The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO. Use Case: In future if it is decided to run both DC & DR Active-Active, then the entire cluster should work as single cluster which is deployed in DC & DR.	This point indicates a different architecture as single cluster compared to the dual log forwarding mentioned in point no. 14. The site peering can be done in multiple ways and we suggest this to be done by proposing active-passive architecture using SIEM native capabilities - please confirm if the peering done by active-passive with minimum of 5 mins of RPO/RTO as the lowest. Focus should be on achiving the SLA & availability rather the method is which it is to be achieved. Specifying methods may seem to be aligning with particular OEM solution. Also, this is not a business application where near zero RTO & RPO is needed, expecially for an on-prem solution. Please review	Please be guided by the RFP
164	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 16The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms, the solution should also allow admin to decide on the replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	The required data is already taken care as a native replication that includes the artifacts. However the same is only available from DR site once the DR site is promoted as active site and failover is performed from DC to DR. please confirm if this is acceptable. Focus should be on achiving the SLA & availability rather the method is which it is to be achieved. Specifying methods may seem to be aligning with particular OEM solution. Also, this is not a business application where near zero RTO & RPO is needed, expecially for an on-prem solution. Please review	Please be guided by the RFP
165	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 41The proposed solution should support SAN, NAS and DAS for adding external storage as and when required.	Please confirm if it is fair to assume NAS & DAS storage requirement is for storing the archived data & not for the online log & flow data - please help in clarifying this.	Please be guided by the RFP
166	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 50The proposed solution should act as common data lake for correlation between (but not limited to) SOAR, NBAD, UEBA and threat hunting, etc.	Is it fair to assume that it could be a common repository and not necessarily be a Data lake only?	Please be guided by the RFP
167	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 61The proposed solution must have the ability to create correlation rules by weighing the TIP feeds based on priority/confidence score.	Is it fair to assume that TIP feed with weightage will be provided by LIC?	Please be guided by the RFP
168	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 68The proposed solution must possess built-in function for Predictive Analysis: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customize the results Indicative Use Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console weather this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.	Please confirm if this can be achieved via Anomaly & behavioural rules within the SIEM	Please be guided by the RFP
169	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 72The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.	Machine learning engine is a resource intensive action and hence it is better to keep it away from the core platform - this ensures the stability of the core SIEM platform kept untouched. The output is better achieved with two separate engine - please confirm if this point can be made optional as not all SIEM tool has common engine for ML & SIEM.	Please be guided by the RFP
170	Annexure F: Technical Compliance	UEBA Technical Specification	113	Point. 40The proposed solution should offer dashboards and reports that deliver daily, weekly, and monthly insights regarding high-risk users and entities based on their risk score ratings.	The following points require both flows and network details along with information of entity, this usecase is more inclined toward a dedicated UEBA solution instead of UBA solution. It is thus requested to make this point optional to help promote higher participation.	Please be guided by the RFP
171	Annexure F: Technical Compliance	PCAP Technical Specification	113	Point. 4The solution should support full line-rate packet capture, real-time conversion to layer 3-7 metadata and have retention of 6 months historical meta-data for trend analysis, long-term reporting and back in time investigation. This back in time feature should be able to enable a user to quickly perform historical security event analysis.	For retaining metadata the same PCAP tool wont be possible. This will need NBAD component - please eliminate the need of meta data as it is overlapping point from NBAD compliance	Please be guided by the RFP
172	Cyber Theat Intelligence (CTI)			The vendor needs to be responsible for ensuring that the implemented platform complies with the specifications detailed in ISO 27001, ISO 27002, SEBI, IRDAI, PCI DSS, IT Act 2000, DPDP 2023, etc. and any other law of the land applicable for LIC.	Request to please consider SOC2 as well.	Please be guided by the RFP

173	Section E: Scope of Services	1. Brief Scope of Work - Point 3 - Implementing	52	Other existing security solutions and any security solutions procured in future as applicable	Kindly confirm which are the security solutions that LIC plan to procure in furture. This will help us in understanding the feasibility and efforts required for integration with the proposed solutions	Please be guided by the RFP
174	Section E: Scope of Services	Asset Inventory (Indicative)	55	Application Inventory - 255	Kindly share the application details (name, version, type of log generated etc). This will help us in understanding the feasibility and efforts requiredfor integration with the proposed solution	Please be guided by the RFP
175	Section E: Scope of Services	Security Dashboards:	59	Anti-phishing services Security Analysis, Mitigation and reporting	As part of the RFP, there is no ASK for anti-phishing services. Hence request LIC to confirm if they have already procured this service and would like to integrate the same with the proposed SIEM solution. Kindly confirm	Please be guided by the RFP
176	Section E: Scope of Services	Security Dashboards:	59	Other security solutions, Technologies and devices as required by LIC	Which are the other solution that LIC plan to integrate with the proposed SIEM solution? Kindly share the details for the same to understand the feasibility and efforts	Please be guided by the RFP
177	Section E: Scope of Services	2. Detailed Scope of Work - I. General Requirements	63	The vendor is required to plan and execute red team and purple team exercises at end of every six months. The red team activities should be performed only from external parties/ vendors/ resources and should not be related with blue team and purple team. Bidder shall provide and implement patches/ upgrades/ updates for hardware/software/ operating system / middleware, etc. as and when released by service provider/ OEM or as per requirements of LIC. Bidder should bring to notice of LIC all releases/ version changes.	To have a maker/checker request LIC to remove this point from bidder scope and appoint a 3rd party vendor by LIC to do the same	Please be guided by the RFP
178	Section E: Scope of Services	VIII. Packet Capture (PCAP)	69	Packet Capture	Kindly confirm if LIC has a SSL decryptor solution that can be leveraged to decrypt the traffic and sent it to Pcap or is Bidder expected to propose the same	Please be guided by the RFP
179	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	86	System Availability (Each solution)- Uptime percentage is calculated on a monthly basis for the solutions. In the event of any hardware issues, the Bidder must guarantee the availability of replacement devices to meet the SLAs.	Our understanding is the ASK is for solution SLA and not for individial component solutions like PCAP, NBAD solutions. Kindly clarify	Please be guided by the RFP
180	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	88	Ongoing Operational Enhancement and Reporting Requirements	Continuous improvement may or may not lead to reduction in the event response time. Hence requesting LIC to remove this point or make it as mutually acceptable metric after implementation and baseline for six months	Please be guided by the RFP
181	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	89	SOAR Playbook - Achieve a playbook success rate of no less than 95%.	Since it ia new solution being implemented and it does not have any baseline, request you to exempt bidder from penalty or make it mutually acceptable metric after implementation and baseline for six months	Please be guided by the RFP
182	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	89	SOAR Automation Automate at least 90% of eligible incident response actions	Since it ia new solution being implemented and it does not have any baseline, request you to exempt bidder from penalty or make it mutually acceptable metric after implementation and baseline for six months	Please be guided by the RFP
183	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	89	UEBA Accuracy Detect anomalies with 95% accuracy while maintaining a false positive rate of no more than 5%.	Since it ia new solution being implemented and it does not have any baseline, request you to exempt bidder from penalty or make it mutually acceptable metric after implementation and baseline for six months	Please be guided by the RFP
184	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	89	Threat intelligence accuracy Threat intel feeds should have confidence more than 90% and should be incorporated into all possible alerts/alert flow/ incident response.	Since it ia new solution being implemented and it does not have any baseline, request you to exempt bidder from penalty or make it mutually acceptable metric after implementation and baseline for six months	Please be guided by the RFP
185	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	89	Ensure data integrity with no more than 1% packet loss. Retain captured PCAP data for a minimum of 90 days and 365 days in cold storage for incident response in near real time or within 1 hour for archived date.	Since it ia new solution being implemented and it does not have any baseline, request you to exempt bidder from penalty or make it mutually acceptable metric after implementation and baseline for six months	Please be guided by the RFP
186				Additional Query	Kindly clarify whether LIC will provide the underlying infrastructure (hardware & software) for the solution proposed	Please be guided by the RFP
187				Additional Query	Kindly clarify whether LIC will provide enterprise edition for Database (MS Sql etc) which are needed for real time replication or bidder has to be provide the same	Please be guided by the RFP
188	Annexure F - NGSOC Technical Specifications	point 16		The SOC shall implement the following security controls to ensure the confidentiality, integrity, and availability of LIC's information systems and networks(but not limited to): -Multi-factor authentication (MFA) to ensure that only authorized personnel have access to the SOC and its systems. -Role-based access control (RBAC) to limit access to sensitive information and systems based on user roles and responsibilities. -Encryption to protect sensitive data both in transit and at rest. -The security controls should comply with IS audit and IRDAI audit requirements.	Kindly confirm which MFA solution is currently used by LIC and with which proposed solution needs to be integrated. Is the usecase only for admins accessing the console?	Please be guided by the RFP
189	Annexure F - PCAP Technical Specifications	Point 8		The solution should support analysis of both encrypted and non-encrypted traffic. Vendor to specify if any other components are used natively or by third party for achieving this	Request LIC to clarify the port requirement for decrypting SSL traffic as SSL decryption has to be placed inline for decryption traffic. Also clarify the no of concurrent connections/sec to be handled for both encrypted and non-encrypted traffic to be handled	Please be guided by the RFP
190	Annexure F - NBAD Technical Specifications	Point 7		The solution should offer seamless integration with existing security infrastructure such as but not limited to SIEM, IDS/IPS, firewalls, and threat intelligence feeds across all platforms at LIC for enhanced visibility and correlation.	Kindly confirm the usecase for integration with IDS/IPS and Firewall to understand the feasibility of integration as OEMs may not have have any specific use case for the same. If there is no specific use case that can be identified, request you to delete the clause. Also integrat	Please be guided by the RFP
191	Annexure F - NBAD Technical Specifications	Point 9		The solution should have the capability to integrate with external threat intelligence feeds which has a confidence level more than 70 % to enhance anomaly detection with up-to-date threat information.	Our understand is integration is expected and LIC already has threat feeds needed.Kindly clarify	Please be guided by the RFP
192	SIEM Compliance	Technical Specification	Point no. 2	The peak EPS that the proposed solution can address without any additional license, server, storage or appliance should be minimum twice than the sustained EPS proposed.	Many OEMs license on Average EPS, Peak EPS. Since the license requirement is 2x, we suggest to allow the server based licensing as well. It can help you consume the EPS spikes better as the spike can also go beyond 80k EPS as well. - please confirm	Please be guided by the RFP

193				Eligibility Criteria Query	We would like to change the clause which mentions references of three customers were 60,000+ EPS is in operation. We would like to change it from 3 to 2 references.	Please be guided by the RFP
194				Additional Query	What is the current EPS/MPS?	Please be guided by the RFP
195	3. Activity Schedule	7 - Earnest Money deposit (EMD)	11	EMD to be submitted of Rs. 6 Crores	Rs. 6 Crores is a very high value of EMD. Kindly request LIC to keep EMD in range of 2% of estimated budget of RFP.	Please be guided by the RFP
196	12. Evaluation process for selection of bidder	p), q), r)	28	p) Computation Methodology for rating bidders on 'Technical plus Commercial basis': q) There would be a weightage of 70% to the technical score and 30% for the final Commercial price quoted by the bidder at the end of online reverse auction. r) It would be normalized as under for each bidder: - Total Score (up to 3 decimals) = {(T x 0.7) / Thigh} + {(LLow x 0.3) / L}	Since LIC is evaluating the bids on basis of Technical & Commercial with 70:30 weightage, then kindly request LIC to request for a final price submission alongwith technical proposal to shorten the timeline for evaluation. This similar evaluation methodology is used by RBI & SEBI in their bids.	Please be guided by the RFP
197	55. Varying the Services	I.	46	I. Variations proposed by LIC – LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, etc. cost to be quoted in the commercial bid. Any change in the scope beyond this 25% will be informed to the vendor in writing.	25% is a very high percentage for scope change to be factored for Services, Appliances and Licenses. Kindly request LIC to provide Change Requests for additional requirement so that the bidder can provide a best possible price during evaluation.	Please be guided by the RFP
198	7. Service Level Agreements (SLAs) & Penalties	Penalty caps	91	The total penalty for onsite support shall not exceed 100% of the quarterly charges payable for onsite support for reasons other than absence.	Kindly request LIC to cap the penalty at 10% of quarterly payable for onsite support.	Please be guided by the RFP
199	Technical Bid	Point No 4	22	LIC will be responsible to provide all the hardware required for in-scope solutions' implementation, i.e server/VMs and will provide RHEL OS and Database – MySQL, if required as part of the solution. All other software and hardware if any should be provided by bidder, included in BoQ and prices quoted for in the Commercial Bid Document.	We request LIC to clarify what kind of hardware, VM and Hypervisor that LIC will provide, it is understood that for non-RHEL OS, non-MySQL DB should be proposed by bidder as part of the respective solution in commercial template.	Please be guided by the RFP
200	Section E	1	60	Once all the log sources integrated with existing SOC are migrated to NGSOC, ensure the existing SOC is up & running in steady state with security patches by obtaining same from respective OEMs, settings etc. for two years.	Will LIC renew the contract with the existing SIEM and other SOC tools? If bidder need to renew the contract for next 2 years, then we need the exact details of the existing solutions with serial numbers and contract dates.	Please be guided by the RFP
201	Section E	2	63	The vendor is required to plan and execute red team and purple team exercises at end of every six months. The red team activities should be performed only from external parties/ vendors/ resources and should not be related with blue team and purple team. Bidder shall provide and implement patches/ upgrades/ updates for hardware/software/ operating system / middleware,etc. as and when released by service provider/ OEM or as per requirements of LIC. Bidder should bring to notice of LIC all releases/ version changes.	Please provide the scope details and coverage of the Red team activities. i.e., No of IPs, No of applications, kduration of the activities, etc.	Please be guided by the RFP
202	Section E	6	84	Delay in implementation of devices which could not be integrated in the initial phase beyond three weeks.	Integration of all the assets as mentioned in the RFP within 3 weeks is practically difficult. Kindly relook at the clause and consider deletion. This would largely impact of the overall delivery of the project. Anyways as part of Operations, the team is responsible for integrating the devices, hence request LIC to remove this clause.	Please be guided by the RFP
203	Annexure F Technical Compliance	4		The proposed solution must be disaster recovery (DR) ready and should also provide a high availability (HA) feature at the log collection layer, logger layer, correlation layer and search layer. The bidder may choose to provide HA either natively (in case of appliance) or through OS based clustering (in case of software).	We assume that the HA is required at DC and the standalone setup is required at DR site to fulfill the SLA requrements. Please confirm.	Please be guided by the RFP
204	Section C:	9.b	24	Vendor will be entirely responsible for upfront payment of all applicable taxes like GST, License fees, road permits etc. GST shall be mentioned in the Invoices and payments will be made as per invoices submitted. GST wherever applicable, shall be mentioned in the Invoices submitted and shall be reimbursed as per actuals on production of the original receipt in proof of having paid the said taxes on behalf of LIC. In case concrete evidence of having paid the appropriate taxes is not submitted within a maximum period of two months from the date of payment of the taxes, the vendor will not be eligible for any reimbursement on this count.	Bidder understands that as per the GST law, there is no requirement to pay GST upfront and hence no proof of upfront payment of GST can be provided by the bidder. Request LIC to pay GST amount along with payment for invoices raised by bidder	Please be guided by the RFP
205	Section C:	27.a	35	Bids shall remain valid for 12 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule. LIC shall reject a bid as non-responsive if the bid is submitted with a shorter validity period.	Bidder requests to limit the price Validity to 120 days	Please be guided by the RFP
206	Section C:	47.e	43	LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and / or reduce the scope of the Services.	Bidder requests for a notice period of 90 days. Also, in the event of reduction in scope, the price for remaining scope shall be mutually agreed between the parties	Please be guided by the RFP
207	Section C:	47.j	43	In the event of LIC terminating the Contract in whole or in part, LIC may procure, upon such terms and in such manner as it deems appropriate, Systems or Services similar to those undelivered, and the Successful bidder shall be liable to LIC for any excess costs for such similar systems or Services. However, the Successful bidder shall continue the performance of the Contract to the extent not terminated.	We request that Bidders liability for such excess cost shall be capped to 10% of TCV	Please be guided by the RFP
208	Section E:	1	54	Service Provider further agrees that whenever required by LIC, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the LIC/ IRDAI and or any regulatory authority required for conducting the audit. LIC reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the Service Provider (e.g., financial, internal control and security reviews) & findings made on the Service Provider in conjunction with the services provided to LIC.	Bidder understand that any information internal/intrinsic to Bidder's course of operations will be excluded from ay such audit/review.	Please be guided by the RFP
209	Section E:	7.22	85	In case of cancellation of orders due to delay in deliveries/installations or deficiency in services etc., besides the penalty being charged, the vendor may also be blacklisted by Life Insurance Corporation of India & may not be allowed to participate in any tenders for a period to be decided by LIC. Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements to a maximum of 10% of the cost of that item(s).	Bidder request to remove the below as the clause is subjective and LIC already has protection of risk purchase clause "Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements to a maximum of 10% of the cost of that item(s)."	Please be guided by the RFP

210	Section E:	7.Penalty caps:	91	The total penalty for delivery and installation shall not exceed 10% of the PO value. The total penalty for onsite support shall not exceed 100% of the quarterly charges payable for onsite support for reasons other than absence.	We request modification of clause to as below: The total penalty for onsite and offsite support per quarter shall not exceed 10% of the quarterly charges payable for onsite and offsite support for reasons other than absence. In case of absence of onsite support, actual amount shall be deducted up to 100% of the quarterly charges payable for the absent resource	Please be guided by the RFP
211	Section F	1.e	92	In case of cancellation of orders due to delay in deliveries/installations or deficiency in services etc., besides the penalty being charged, the vendor may also be blacklisted by Life Insurance Corporation of India & may not be allowed to participate in any tenders for a period to be decided by LIC. Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements.	Bidder request to remove the below as the clause is subjective and LIC already has protection of risk purchase clause "Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements to a maximum of 10% of the cost of that item(s)."	Please be guided by the RFP
212	Section F	4	93	In case if required, the vendor must provide necessary support at no additional cost to LIC for one time transportation/shipping during the entire contract period from current place of installation to another data center of LIC. Such requirement and applicable details will be communicated by LIC to the vendor. Vendor shall provide a detailed plan of action for the same.	We request LIC to confirm on number of instances of such shifting expected during the contract term.Additionally since there are costs associated with delivery/re-installation we request LIC to consider such requests via a change request process.	Please be guided by the RFP
213	Section F	6	93	In the event of termination of the selected Bidder due to any cause whatsoever, [whether consequent to the stipulated terms of the RFP or otherwise], LIC shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the terminated Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Bidder to take over the obligations of the terminated Bidder in relation to the execution/continued execution of the scope of the work defined in RFP. This period of transition shall not exceed six months from the effective date of termination.	Bidder understand that such transition will be provided on chargeable basis	Please be guided by the RFP
214	Section F	8.a	95	LIC may, at any time, by a prior written notice of 30 days, terminate the contract or reduce the scope of the Services	Bidder requests for a notice period of 90 days. Also, in the event of reduction in scope, the price for remaining scope shall be mutually agreed between the parties	Please be guided by the RFP
215	Section F	8.a	95	the scope of the Services is reduced, LIC's liability to pay the Service Charges or to provide LIC Material abates in accordance with the reduction in the Services.	In the event of reduction in scope, the price for remaining scope shall be mutually agreed between the parties	Please be guided by the RFP
216	Section F	8	95	In the event of LIC terminating the Contract in whole or in part, LIC may procure, upon such terms and in such manner as it deems appropriate, Systems or Services similar to those undelivered, and the Vendor shall be liable to LIC for any excess costs for such similar systems or Services. However, the Vendor shall continue the performance of the Contract to the extent not terminated.	Bidders requests that liability for such excess cost shall be capped to 10% of TCV	Please be guided by the RFP
217	Section F	8	96	Termination and reduction for convenience	1.Bidder request for 90 days notice for termination for convenience. 2.We understan that LIC shall Pay for services rendered till effective date of termination 3.We understand that LIC shall pay the bidder for any advance payment already made by the bidder to OEMs/third parties for providing warranty, AMCs etc for the period beyond the effective termination date	Please be guided by the RFP
218	Section G	10	100	Following documents will be required to be submitted for release of payment: i) Invoice printed on Vendor's own letterhead (with reference to Purchase order, description of goods/ services delivered, quantity, unit price, total amount) Life Insurance Corporation of India – RFP/Tender for onboarding System Integrator (SI) to Implement Threat Detection and Incident Response Tools LIC-CO/IT-BPR/NW/RFP/2023-2024/TDIR dated 18 December 2023 Page 101 of 142 ii) Proof of payment of GST/Octroi / Entry Tax (wherever applicable) iii) UV Certificate (wherever applicable) duly signed and stamped by the Vendor, and countersigned by the LIC officials from the concerned project/department of LIC.	Bidder understands that as per the GST law, there is no requirement to pay GST upfront and hence no proof of upfront payment of GST can be provided by the bidder. Request LIC to pay GST amount along with payment for invoices raised by bidder	Please be guided by the RFP
219	Section G	12.d	101	LIC reserves the right to terminate the contract earlier, with two months' notice for reasons of non-performance and unsatisfactory services. In any case LIC's decision in this case will be final and binding. In case of vendor being discontinued for deficiency in service, the contract may be terminated, and the vendor may be blacklisted by LIC and may not be allowed to participate in the future tenders for a period to be decided by LIC. Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements	Bidder request to remove the below as the clause is subjective and LIC already has protection of risk purchase clause "Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements to a maximum of 10% of the cost of that item(s)."	Please be guided by the RFP
220	22		33	In no event shall LIC be liable for any indirect, incidental or consequential damage or liability, under or in connection with or arising out of this RFP, or out of any subsequent agreement relating to any hardware, software and services delivered. For this purpose, it would be immaterial how such liability may arise, provided that the claims against customers, users and service providers of LIC are considered as a direct claim.	We request that this clause be made mutual to be equitable.	Please be guided by the RFP
221	24	b	34	PBG period of 63 months	We request that the PBG period be the same as the contract period, i.e. of 60 months.	Please be guided by the RFP

222	24	j	34	The PBG will be invoked in full or part (to be decided by LIC) if the bidder fails to honour expected deliverables or part as per this RFP after issuance of PO during the period of contract. i. The bidder fails to honour expected deliverables or part as per this RFP after issuance of PO. ii. Any legal action is taken against the bidder restricting its operations. iii. Any action taken by statutory, legal or regulatory authorities for any breach or lapses which are directly attributable to the bidder iv. LIC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.	We request that the clause be amended as below: "The PBG will be invoked in full or part (to be decided by LIC) in the eventuality of a material breach if the bidder fails to honour expected deliverables or part as per this RFP after issuance of PO during the period of contract and the selected vendor will be provided notice and a cure period of not less than 30 days to rectify such material breaches. i. The bidder fails to honour expected deliverables or part as per this RFP after issuance of PO. ii. Any legal action is taken against the bidder restricting its operations. iii. Any action taken by statutory, legal or regulatory authorities for any breach or lapses which are directly attributable to the bidder iv. LIC incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions. We would kindly submit that the PBG must be invoked only for material breaches and the bidder must be provided a cure period to rectify breaches before PBG is invoked.	Please be guided by the RFP
223	33		36	Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	We would request that the clause be amended accordingly: "Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor neither party shall not be liable to the other LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or business, interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of both the parties the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment." We request LIC to remove indirect and consequential damages for IPR infringement. The exclusion of indirect and consequential damages must also apply to LDs. Limitation of Liability must also apply to costs of repairs and replacements of defective equipment.	Please be guided by the RFP
224	34	a	37	The vendor shall be liable for any delay in execution or failure of their respective obligations under this agreement except for delay caused by occurrence of events beyond control of the vendor, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action, or regulations of government, local or other public authorities.	We would kindly request that this clause be edited as below: "The vendor shall be liable for any delay in execution or failure of their previously agreed upon respective obligations, beyond the cure period granted, under this agreement except for delay caused by occurrence of events beyond control of the vendor, including but not limited to natural calamities, fire, explosions, floods, power shortages, acts of God, hostility, acts of public enemy, wars, riots, strikes, sabotage, order/action, or regulations of government, local or other public authorities. For clarity - such an event will not preclude LIC from its payment obligations to the vendor." Please accept new insertion excusing performance in case of Force Majeure situation. LIC's payment obligations not to be covered under such excusing of performance.	Please be guided by the RFP
225	35	c	37	c) The Vendor shall not be entitled to suspend the Service(s) or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service(s) in accordance with the provisions of the RFP notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.	We request LIC to accept the below modification. "c) Unless the nature of the dispute is such that it would be impractical for the Service(s) to be continued, tThe Vendor shall not be entitled to suspend the Service(s) or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service(s) in accordance with the provisions of the RFP notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings."	Please be guided by the RFP
226	35	d	38	The work under contract shall continue during the Arbitration proceedings and no payment due or payable to the Contractor shall be withheld on account of such proceedings.	We request the clause be amended as below: "The work under contract shall continue during the Arbitration proceedings and no payment due or payable to the bidder or Contractor shall be withheld on account of such proceedings."	Please be guided by the RFP
227	36	A(a)	38	Against all actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC.	We request that the clause be amended as below to only include direct claims: "Against all direct actions, proceedings, claims, demands, costs and expenses which may be made against LIC by a third party arising out of the sale of vendor's services to LIC."	Please be guided by the RFP
228	42	f	41	Recover any dues payable by the selected Vendor from any amount outstanding to the credit of the selected Vendor, including the pending bills and/or invoking PBG or other payment pending from the vendor, if any, under this contract.	We request that the bidder also have a say in this and it is not a unilateral decision.	Please be guided by the RFP
229	47	e	43	LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and /or reduce the scope of the Services.	We would kindly request for this time frame to be 30 days as opposed to one week in order to be able to adjust the requirements accordingly.	Please be guided by the RFP
230	Section F:1	e	92	In case of cancellation of orders due to delay in deliveries/installations or deficiency in services etc., besides the penalty being charged, the vendor may also be blacklisted by Life Insurance Corporation of India & may not be allowed to participate in any tenders for a period to be decided by LIC.	We request that blacklisting be restricted to only matters relating to fraud and corrupt practices.	Please be guided by the RFP

231	6		93	Consequences of termination	We request that the termination clause on page 43 be replicated here to maintain consistency (and on page 97)	Please be guided by the RFP
232	7		94	The liability of the bidder, regardless of the nature of the action giving rise to such liability and in case of claims against the LIC arising out of misconduct or gross negligence of the bidder, its employees and subcontractors or through infringement of rights, patents, trademarks, copyrights, Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.	We request that the clause be amended as below: "The liability of the bidder, regardless of the nature of the action giving rise to such liability and in case of claims against the LIC arising solely out of wilful misconduct or gross negligence of the bidder, its employees and subcontractors or through infringement of rights, patents, trademarks, copyrights, Intellectual Property Rights or breach of confidentiality obligations (excluding liability for personally identifiable information and sensitive personal data and/or information) shall be unlimited." Please accept modified language as above to limit liability solely for wilful misconduct. We cannot agree to uncapped liability for confidentiality breaches without excluding liability for personally identifiable information and sensitive personal data and/or information.	Please be guided by the RFP
233	47		95	The Vendor will indemnify LIC against all third-party claims of infringement of patent, Intellectual Property Rights, trademark, copy right or industrial design rights arising from use of the Vendor's Solution or any part thereof throughout the Offices of LIC, including but not limited to the legal actions by any third party against LIC.	Kindly accept the below modifications to keep in line with the edits in the clause above: "The Vendor will indemnify LIC against all direct third-party claims of infringement of patent, Intellectual Property Rights, trademark, copy right or industrial design rights arising from use of the Vendor's Solution or any part thereof throughout the Offices of LIC, including but not limited to the legal actions by any third party against LIC, if used in the authorized manner."	Please be guided by the RFP
234	12	d	101	LIC reserves the right to terminate the contract earlier, with two months' notice for reasons of non-performance and unsatisfactory services. In any case LIC's decision in this case will be final and binding. In case of vendor being discontinued for deficiency in service, the contract may be terminated, and the vendor may be blacklisted by LIC and may not be allowed to participate in the future tenders for a period to be decided by LIC. Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements. Spares and support for the appliances should be available for a minimum period of six years from the date of installation of the appliances irrespective of whether the equipment is manufactured by the Vendor or procured from any other OEM. The entire responsibility will rest on the Vendor for servicing and proper functioning of the equipment. During this specified period if it is found that spares or support is not available, the appliances will have to be replaced by equivalent or higher model subject to evaluation if required by LIC, by the vendor at no extra cost to LIC.	We kindly request that the clause be amended as below: "LIC reserves the right to terminate the contract earlier, with two months' notice for material breach and subsequent cure period of not less than 30 days to rectify the breachfor reasons of non-performance and unsatisfactory services. In any case LIC's decision in this case will be final and binding. In case of vendor being discontinued for deficiency in service, the contract may be terminated, and the vendor may be blacklisted by LIC and may not be allowed to participate in the future tenders for a period to be decided by LIC. Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements. Spares and support for the appliances should be available for a minimum period of six years from the date of installation of the appliances irrespective of whether the equipment is manufactured by the Vendor or procured from any other OEM. The entire responsibility will rest on the Vendor for servicing and proper functioning of the equipment. During this specified period if it is found that spares or support is not available, the appliances will have to be replaced by equivalent or higher model subject to evaluation if required by LIC, by the vendor at no extra cost to LIC." Please accept the modifications proposed.	Please be guided by the RFP
235			104	If our Bid for this RFP/tender is accepted, we undertake to enter into and execute at our cost, when called upon by LIC to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.	If our Bid for this RFP/tender is accepted, we undertake to enter into and execute at our cost, when called upon by LIC to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us. [It is submitted that certain terms of the RFP need modification and all such terms may not be discussed during the pre-bid stage. It is hence requested to permit bidders to submit their revisions, suggestions, additions etc. to the terms of the RFP as part of the bid submission.]	Please be guided by the RFP
236	Annexure Q		134	The Respondent herein agrees and undertakes to indemnify and hold LIC harmless from any loss, damage, claims, liabilities, charges, costs, or expense (including attorneys' fees), that may arise or be caused or result from or be paid/incurred/suffered or caused to be paid/incurred/ suffered by reason of any breach, failure, delay, impropriety or irregularity on its part to honors, observe, adhere to, abide by or comply with any of the terms and conditions of this Agreement. In the event that the Respondent shall be liable to LIC in connection with this Agreement, the Respondent's liability shall be limited to the value of the Contract.	The Respondent herein agree and undertake to indemnify and hold LIC harmless from any loss, damage, claims, liabilities, charges, costs, or expense (including reasonable attorneys? fees), that may arise or be caused or result from or be paid/incurred/suffered or caused to be paid/incurred/ suffered by reason of any breach, failure, delay, impropriety or irregularity on its part to honour, observe, adhere to, abide by or comply with any of the terms and conditions of this Agreement. In the event that the Respondent shall be liable to LIC in connection with this Agreement, the Respondent?s liability shall be limited to the value of the Contract. To the extent the Respondent shares any Confidential Information with LIC, the obligaitons of this Agreement and any subsequent agreements entered into, shall apply mutatis mutandis to LIC. Please agree to have this NDA mutual also covering any confidential information shared by the bidder.]	Please be guided by the RFP
237	Annexure N	Pre-Integrity Pact	5	Sanctions for Violations	We request that this be restricted to wilful actions and with the bidder's knowledge.	Please be guided by the RFP
238	Annexure F: Technical Compliance	NBAD Technical Specifications/ 34	113	The solution should be capable of providing visibility of east-west traffic in an encapsulated network of data center fabrics by decapsulating the overlay VxLAN headers to track endpoints.	Kindly remove this clause as this is an OEM specific clause.	Please be guided by the RFP

239	Section C:	55.1	46	LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, etc. cost to be quoted in the commercial bid. Any change in the scope beyond this 25% will be informed to the vendor in writing. If LIC wants to vary the Services	Kindly confirm do the bidder need to mandatorily factor 25% buffer from day-1 for all the solutions as mentioned in below table or the proposed product should have capability to scale up by 25%?	Please be guided by the RFP
240	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	2.The Bidder must have an annual turnover of minimum Rs.600 Crores per annum during the last 03 (three) years preceding the date of this RFP	We hereby declare that we comply the public procurement guidelines issued by the Ministry of Commerce & Industry, Department of Promotion & Internal Trade (Public Procurement Section) in which it is directed and regulated through sub clause of B of main clause no.10.: Specification in Tender and other procurement solicitations is as follow. "Procuring entities shall endeavour to see that eligibility conditions, including on matters like turnover, Expereience criteria, production capability, and financial strength do not result in the unreasonable exclusion of Class-I supplier/ Class-II Local Supplier who would otherwise be eligible, beyond what is essential for ensuring quality, technical compliance or creditworthiness of the supplier." Hence, We request LIC to exempt the Turnover criteria clause for Make in India and Class I local suppliers.	Please be guided by the RFP
241	6. Eligibility Criteria	Point No.04	14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	**We kindly request you to modify the clause as follows:** **The** Bidder/OEM should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Minimum Eligiblity Criteria"
242	6. Eligibility Criteria	Point No.05	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	We kindly request you to modify the clause as follows: The bidder/ OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	Please refer to the revised "Minimum Eligiblity Criteria"
243	6. Eligibility Criteria	Point No.07	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
244	6. Eligibility Criteria	Point No.10	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	We kindly request you to modify the clause as follows: The bidder must have a minimum of 25 IT Security permanent professionals on their payroll with certifications such as OEM Level Certification. Minimum 10 resources must have OEM Level Certification.	Please refer to the revised "Minimum Eligiblity Criteria"
245	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to consider **3 year's of experience** from multiple PO's on day of submission as below: **The Bidder should have minimum of 3 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions** in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. I. Security information and event management (SIEM) (with common security data lake for SOAR, UEBA, CTH) II. Next Generation Security Operations Center (NGSOC) III. Security Orchestration, Automation and Response (SOAR) IV. User and Entity Behavior Analysis (UEBA) V. Cyber Threat Hunting (CTH) VI. Cyber Threat Intelligence (CTI) VII. Packet Capture (PCAP) VIII. Network Behavior Anomaly Detection (NBAD)/ Network Detection and Response (NDR) IX. Endpoint Detection and Response (EDR)	Please refer to the revised "Minimum Eligiblity Criteria"
246	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	Request LIC to consider below clause for qualification. The bidder during the last 3 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM/Managed SIEM/SOC Service (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	Please refer to the revised "Minimum Eligiblity Criteria"
247	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request LIC to consider as below for the given RFP. The bidder during the last 2 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users/SOAR/NBAD for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"

248	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	10 The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	Request LIC to consider below clause: 10 The bidder must have a minimum of 50 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/CEH/CISA/CISM/Security Certification/OEM Level Certification. Minimum 10 resources must have OEM Level Certification (preferably of the proposed OEM).	Please refer to the revised "Minimum Eligiblity Criteria"
249	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	2 The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request LIC to consider below clause including MSSP (Single Customer) for technical evaluation 2 The bidder should have relevant and similar security operation center / security solutions implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 3 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
250	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	5 The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India:	Request LIC to consider below clause for technical evaluation 5 The Bidder during the last 2 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India:	Please refer to the revised "Minimum Eligiblity Criteria"
251	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	7 The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ Professional OEM Level Certification. • Every Additional 10 Resources -> 2 Marks subject to maximum of 10 marks • 100 Resources -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Request LIC to consider below clause for technical evaluation 7 The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/OSCP/CEH/CISA/CISM/Security Certification/OEM Level Certification. • Every Additional 10 Resources -> 2 Marks subject to maximum of 10 marks • 100 Resources -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Please refer to the revised Annexure D
252	6	6.7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	UEBA is still not adopted by many large organizations, hence we request LIC to change it to below: The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 20,000 users for minimum 01 organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
253	Annexure D		109	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India: • More than 2 references -> 10 marks • 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	UEBA is still not adopted by many large organizations, hence we request LIC to change it to below: The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India: • More than or equal to 2 references -> 10 marks • 1 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Minimum Eligiblity Criteria"
254	6	6.10.	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	Does this mean overall 25 across all OEMs asked in the RFP? we request LIC to make this as 10 OEM level certification(preferably of the proposed OEM)	Please refer to the revised "Minimum Eligiblity Criteria"
255	Section E	1.1	51	Use case workshop to be conducted to discuss on existing use cases to be migrated, new use cases as per MITRE ATT&CK, CIS, compliance requirements of LIC, etc.	It is always better to have usecase workshop to be conducted by the OEM, hence requesting LIC to change this to below: Use case workshop to be conducted by OEM to discuss on existing use cases to be migrated, new use cases as per MITRE ATT&CK, CIS, compliance requirements of LIC, as per the lates threat trends, usecases priority also should be captured so that the bidder can implement the usecases accordingly etc.	Please refer to revised "Section E: Scope of Services"
256	Section E	1	62	The bidder shall ensure that the configuration, implementation and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Bidders are officially trained and certified partners of the OEM, hence we request implementation needs to be done by the bidder, however validation of implementation which is asked in the RFP needs to be done by the OEM. We request you to please change this to below: The bidder shall ensure that the configuration, implementation and testing of the solution components to be carried out by resources from the bidder as decided by LIC at the time of implementation.The overall responsibility of the implementation shall be with bidder.	Please refer to revised "Section E: Scope of Services"

257	Section E	1	64	The OEM services team shall devise the implementation plan with clear and objective timeline. The implementation may be tracked using a standard IT Project Management Template like Gantt chart or timeline chart.	Project Manager will be from the bidder. Hence we request LIC to change it to below: The bidder services team shall devise the implementation plan with clear and objective timeline. The implementation may be tracked using a standard IT Project Management Template like Gantt chart or timeline chart.	Please refer to revised "Section E: Scope of Services"
258	Section E	2	66	The vendor should ensure to provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non-standard logs and with all the solutions without any extra cost for LIC. These parsers should be implemented by the OEM.	Building custom parsers for integration is key part of operations and data on boarding and bidder will have more detailed insights of the LIC environment. Proposed solution should support build of custom parsers should be a key requirement in the RFP. Hence we request LIC to have the parsers built during the contract from the bidder as OEM can help in supporting the OOTB parsers. Hence we request you to change it to below: The vendor should ensure to provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non-standard logs and with all the solutions without any extra cost for LIC. These parsers should be implemented by the bidder. All supported devices parsers should be supported by OEM as and when required.	Please refer to the revised "Section E: Scope of Services"
259	Section E	3.3	71	SOAR (Security Orchestration, Automation and response) 30 authorized user licenses	Looking at the size of LIC and similar large deployments like LIC, based on our expeience we have seen that 10 to 12 user license for SOAR is sufficient. Hence we request LIC to reduce the SOAR licenses to 12.	Please refer to the revised "Section E: Scope of Services"
260	Section E	4.1	71	SLA Performance - OEM R,A in RACI	Bidders are managing the SOC for LIC and hence its difficult for OEM to take commit on the SLA's hence we request LIC to have OEM only informed in RACI and not responsibile and accountable for SLA performance for SIEM, SOAR and UEBA as these solutions will be deployed on-prem at LIC.	Please refer to revised "Section E: Scope of Services"
261	Section E	4.1	71	Business Continuity Management - OEM R,A in RACI	Bidders are managing the SOC for LIC and hence its difficult for OEM to take commit on the business continuity management hence we request LIC to have OEM only informed in RACI and not responsibile and accountable for business contინity management for SIEM, SOAR and UEBA as these solutions will be deployed on-prem at LIC.	Please refer to revised "Section E: Scope of Services"
262	Section E	4.3	72	Use Case Content Creation/Review/Modification OEM - R,I	Use case creation, review, modification is part of daily operations and bidder will be doing the daily operations hence we request LIC to have OEM only informed and not responsible for usecase content creation/review/modification.	Please refer to revised "Section E: Scope of Services"
263	Section E	4.3	72	Custom Parser - OEM R,A	Custom parser creation is part of daily operations as new devices will be onboarded as per LIC environment. Custom parsers are for data sources which are not supported by OEM OOTB. Hence custom parsers OEM should only be informed and not responsible and accountable. We request LIC to have OEM only informed.	Please refer to revised "Section E: Scope of Services"
264	Section E	4.3	72	SIEM Platform administration - OEM R	Bidder is managing the operations for LIC hence we request LIC to have OEM only informed for SIEM Platform administration and not responsible.	Please refer to revised "Section E: Scope of Services"
265	Section E	4.3	72	Dashboard Development - OEM A	Dashboard developement is part of SOC operations hence we request LIC to have OEM only informed and not accountable for dashboard development.	Please refer to revised "Section E: Scope of Services"
266	Section E	4.3	72	Performance Optimization - OEM A	Bidder will be managing the entire SOC operations hence any performance optimization OEM cannot be accountable hence we request LIC to have OEM only informed. OEM can provide best practices so that the performance is optimized.	Please refer to revised "Section E: Scope of Services"
267	Section E	4.4	72	Incident investigation - OEM A,I	Bidder is managing the SOC operations hence OEM cannot be accountable for incident investigation, we request LIC to have OEM only informed.	Please refer to revised "Section E: Scope of Services"
268	Section E	4.4	72	Incident remediation - OEM A,I	Bidder is managing the SOC operations hence OEM cannot be accountable for incident remediation , we request LIC to have OEM only informed.	Please refer to revised "Section E: Scope of Services"
269	Section E	4.5	72	Threat modelling - OEM A,I	Threat modeling is a key service in SOC and bidder will be providing the service hence we request LIC to have OEM informed and not accountable for threat modeling.	Please refer to revised "Section E: Scope of Services"
270	Section E	4.7	72	Periodic Threat Hunting Scenarios - OEM A	Threat hunting is a service which is offered by the bidder and hence we request LIC to have threat hunting scenarios only informed for the OEM.	Please refer to revised "Section E: Scope of Services"
271	Section E	4.7	72	Threat Hunting Reporting - OEM A	Threat hunting is a service which is offered by the bidder and hence we request LIC to have threat hunting reporting only informed for the OEM.	Please refer to revised "Section E: Scope of Services"
272	Section E	4.8	72	Profiling - OEM A	Bidder will be integrating the data sources and doing baseline profiling of the users or entities with UEBA solution. Hence we request LIC to have OEM only informed.	Please refer to revised "Section E: Scope of Services"
273	Section E	4.8	72	Report Incidents - OEM A	Bidder is managing the SOC operations hence OEM will have little to no visibility and cannot be accountable for reporting of incidents , we request LIC to have OEM only informed.	Please refer to revised "Section E: Scope of Services"
274	Section E	4.8	72	Rules and policy creation - OEM A	Rules and policy creation is part of daily operations and bidder will be doing the daily operations hence we request LIC to have OEM only informed and not accountable for policy creation.	Please refer to revised "Section E: Scope of Services"
275	Section E	4.8	72	Incident Analysis - OEM A	Bidder is managing the SOC operations hence OEM cannot do incident analysis, we request LIC to have OEM only informed.	Please refer to revised "Section E: Scope of Services"
276	Section E	4.8	72	UEBA Platform administration - OEM R	Bidder will be managing and administring the entire SOC platform and all the solutions hence OEM cannot take responsibility for UEBA administration. Hence we request LIC to have OEM informed for UEBA platform administration.	Please refer to revised "Section E: Scope of Services"
277	Section E	4.9	72	Integration with other solutions - OEM A,C	Most of the leading solutions integration will be available OOTB. Bidder will be implementing and integrating these solutions. OEM can be consulted and informed in this case. We request LIC to have OEM only informed or consulted for integration with other solutions.	Please refer to revised "Section E: Scope of Services"
278	Section E	4.9	72	Automation Configuration - OEM A,C	All configurations including automation will be done by the bidder, hence we request LIC to have OEM informed and consulted for automation configuration.	Please refer to revised "Section E: Scope of Services"

279	Section E	4.9	72	SOAR Platform administration - OEM R	Bidder will be managing and administring the entire SOC platform and all the solutions hence OEM cannot take responsibility for SOAR administration. Hence we request LIC to have OEM informed for UEBA platform administration.	Please refer to revised "Section E: Scope of Services"
280	Section F	7	94	LIC ownership of Intellectual Property Rights in Contract Material e. All Intellectual Property Rights in the Contract Material shall vest in LIC; f. to the extent that LIC needs to use any of the Auxiliary Material provided by the Vendor to receive the full benefit of the Services (including the Contract Material), the Vendor grants to, or must obtain for, a world-wide, royalty free, perpetual, non-exclusive license to use, reproduce, adapt, modify and communicate that Auxiliary Material.	With the advent of new technologies and changing business models, software companies are embracing alternative licensing methods that are more flexible, scalable, and cost-effective. hence most of the leading software companies do not offer perpetual licenses. We request LIC to change the licensing model from perptual to subscription based.	LIC ownership of Intellectual Property Rights in Contract Material e. All Intellectual Property Rights in the Contract Material shall vest in LIC; f. to the extent that LIC needs to use any of the Auxiliary Material provided by the Vendor to receive the full benefit of the Services (including the Contract Material), the Vendor grants to, or must obtain for, a world-wide, royalty free, perpetual/subscription based, non-exclusive license to use, reproduce, adapt, modify and communicate that Auxiliary Material.
281	Annexure F - SIEM	3		The proposed solution and the supporting infrastructure (server, storage and any other equipment) should adequately support current event volume and further projected growth which could be 20% YoY.	LIC has asked for 60000 EPS scalable up to 80000 EPS, is LIC looking for 60k EPS + 20% YOY or 80k+20%YOY? Should the solution be sized for 80k EPS or 80k EPS + 20% YOY ? i.e end of 5th year 165k EPS is expected and should the solution be sized for 165k EPS? Please let us know what is the license LIC is expecting in Year 1 , Year 2 through year 5.	Please refer to the revised "Annexure F"
282	Annexure F - SIEM	20		The solution should provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non standard logs without any extra cost for LIC. These parsers should be part of the solution and implemented by the OEM.	Custom parser creation is part of daily operations as new devices will be onboarded as per LIC environment. Custom parsers are for data sources which are not supported by OEM OOTB. Hence we request LIC to change this specification to below: The solution should provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non standard logs without any extra cost for LIC. These parsers should be part of the solution and implemented by the bidder with the help from OEM if required.	Please refer to revised Annexure-F SIEM and revised "Section E: Scope of Services"
283	Annexure F - SIEM	59		The proposed solution should have the ability to model incoming event data into logical groups such as domains, networks, applications, criticality of target devices, etc and make this data modelling to assist for aiding in data filtering and logical segregation.	Logs which are filtered should not be counted in license. We request LIC to change it to below: The proposed solution should have the ability to model incoming event data into logical groups such as domains, networks, applications, criticality of target devices, etc and make this data modelling to assist for aiding in data filtering and logical segregation. Logs which are filtered should be counted in license.	Please refer to the revised "Annexure F"
284	Annexure F - SIEM	64		The proposed solution should have a minimum of 15 behavioural anomalies models and provide AI/ML capabilities for detecting threats in LIC infrastructure with the integrated log sources	Behavioral based anomalies are primary the functionality for UEBA. SIEM should have ML natively available to build custom ML models, OOTB machine learning algorithms which can be called as functions etc. We request LIC to have this specification in UEBA.	Please refer to revised Annexure-F SIEM . Clause Deleted
285	Annexure F - SIEM	105		The proposed solution should provide perpetual licensing option, including a description of what is included in the maintenance and support agreement.	With the advent of new technologies and changing business models, software companies are embracing alternative licensing methods that are more flexible, scalable, and cost-effective. hence most of the leading software companies do not offer perpetual licenses. We request LIC to change the perptual / subscription based.	Please refer to the revised "Annexure F"
286	Annexure F - SOAR	11		The solution should support 800+ integrations out of the box. Integration packs should include pre-built use cases consisting of playbooks, automation actions, scripts that can be customised for LIC's SOC. The solution should have an integration store that is continuously updated with both OEM and vendor provided integration.	800+ number is too high as there are not so many different security tools or source types. We request LIC to make it 250 to 300 OOTB integrations and can have 2500 actions OOTB.	Please refer to revised Annexure-F SOAR
287	Annexure F - SOAR	21		The solution should encrypt (such as but not limited to SHA 256, TLS v1.3, etc.) all incident data and reports and have audit logging on changes to the platform configuration.	Is LIC looking for encryption during transit or during communication across components in the solution? as the data at rest encryption is taken at the hardware level. We request LIC to change it to below: The solution should have encrypted communication within the components all incident data and reports and have audit logging on changes to the platform configuration.	Please refer to revised Annexure-F SOAR
288	Annexure F - SOAR	22		The solution should manage dependencies automatically required for automation processes.	Dependencies can be identified in the playbooks or configuration during the automation process, but resolving the dependencies like permission to kill the process at the endpoint is a dependency but it cannot be resolved by SOAR automatically it needs to be done at the admin level by LIC. Hence we request to change it to below: The solution should show dependencies automatically required for automation processes.	Please refer to revised Annexure-F SOAR
289	Annexure F - SOAR	23		The solution should be architected to support minimum 60000 EPS and to effectively handle an unlimited volume of cases generated within the solution.	SOAR solutions are architected based on the alerts and number of users. As all SIEM EPS are not forwarded to SOAR we request LIC to please help to provide the alerts which will be handeled by SOAR and total number of users logging in to platform. Based on our past experience we have seen that ~100 alerts are expected to reach SOAR from SIEM to take actions. Hence we request you to change it to below: The solution should be architected to support ~100 alerts per minute or 15 users and to effectively handle the cases generated within the solution.	Please refer to revised Annexure-F SOAR

290	Annexure F - SOAR	26		The solution should support standard languages like but not limited to Python, JS, PowerShell, BASH, etc. to create and customize scripts.	Most of the leading SOAR platforms support drag and drop options to create playbooks and have Python to create edit the code. JS is not used by majority of SOAR vendors and as part of actions BASH scripts can be used. We request LIC to have python as the coding language. Hence request to change it to below: The solution should support standard languages like but not limited to Python, PowerShell in actions, BASH in actions, etc. to create and customize scripts.	Please refer to revised Annexure-F SOAR
291	Annexure F - SOAR	27		The solution should support 250+ out of the box playbooks. The playbooks should support: - nested playbooks to deploy multiple automations as part of a single use case - conditional decision trees - user surveys for input from various stake holders in the use case/reviews - time based actions - escalation actions	Most of the leading SOAR platforms has OOTB 100+ playbooks and 2000+ actions. We request LIC to change it to below: The solution should support 100+ out of the box playbooks. The playbooks should support: - nested playbooks to deploy multiple automations as part of a single use case - conditional decision trees - user surveys for input from various stake holders in the use case/reviews - time based actions - escalation actions	Please refer to revised Annexure-F SOAR
292	Annexure F - SOAR	61		The solution should use machine learning for analyst assignment and auto-calculate incident severity.	Most of the leading SOAR solutions dont need machine learning for ticket assignment and incident severity creation. ML is used to suggest which analyst can help in solving similar incidents. Hence we request LIC to change it to below: The solution should use machine learning to recommend analyst assignment and playbook based on past incidents.	Please refer to revised Annexure-F SOAR
293	Annexure F - SOAR	99		The licensing model should distinguish between different user roles, such as administrators, analysts, and responders, offering appropriate pricing for each role based on their access and usage requirements.	Every OEM has different licensing models. Some OEM's dont have licenses for built-in user accounts for the automation and the admin users do not count against a license. Hence we request to simplify this to below so that it becomes generic specification for all OEM's.: The licensing model should be based on number users independent to any user role and licenses should factored based on the ask in this RFP.	Please refer to revised Annexure-F SOAR
294	Annexure F - SOAR	115		The vendor must have previously deployed the proposed solution of equal size and configuration or more in at least three PSU/Banks/Private Banks/BFSI institutions, each with a minimum of 60000 EPS in the last 3 financial year preceding to the date of this RFP.	SOAR licensing, sizing is purely on number of users and alerts to be handled by the SOAR. Hence we request to please ask for references only without actual EPS it can handle. We request to change it to below: The vendor must have previously deployed the proposed solution/any SOAR solution of equal size and configuration or more in at least two PSU/Banks/Private Banks/BFSI institutions in the last 3 financial year preceding to the date of this RFP.	Please refer to the revised "Annexure F"
295	Annexure F - UEBA	5		The proposed solution must have the scalability to handle the volume of data generated up to 80000 EPS , all assets/entities in LIC and should be capable to handle increase in volume of data / number of assets/entities as per LIC's growth (20% YoY).	UEBA doesnt not need entire data of SIEM, only 30 to 40% of SIEM data ingested is relevant for UEBA. Hence we request LIC to ask for total number of users and ~40k EPS for UEBA.	Please refer to the revised "Annexure F"
296	Annexure F - UEBA	21		The proposed solution should have the capacity to utilize both unsupervised and supervised machine learning algorithms, artificial intelligence and deep learning.	Most of the leading UEBA solutions use built on unsupervised machine learning algorighthms to profile normal behavior for each identity and asset, and then looks for unusual behavior patterns across those identities and assets. This has been proven to be more accurate to detect threats. We request LIC to change it to below: The proposed solution should be built on unsupervised machine learning algorithms to build the profile of normal behavior for each user and entity and further ML should be used to detect unusual behavior patterns across those identities and assets.	Please refer to the revised "Annexure F"
297	Detailed Scope of Work	General Requirements	62	The Bidder should provide backup solution for proposed setup. The backup taken should be SHA-256 encrypted.	Please specify the backup duration for the contract period	Please refer to the revised "Section E: Scope of Services"
298	Project Timelines	The Phase Wise Project Timelines for SIEM	82	Phase 1 : Implementation of SIEM, SOC, SOAR and UEBA	Considering the complexity and integration of a large number of log sources, kindly change the timelines from T + 32 to T + 45	Please refer to the revised "Section E: Scope of Services"
299	Project Timelines	The Phase Wise Project Timelines for SIEM	82	Phase 3 : Implementation of PCAP and NBAD	Considering the complexity and integration of a large number of log sources, kindly change the timelines from T + 8 to T + 16	Please refer to the revised "Section E: Scope of Services"
300	Brief Scope of Work	Transition from existing SOC to NGSOC	60	Manage day to day operations of currently running SOC setup from two months from date of issuance of PO	Kindly change time line of 2 months to be inline with new SIEM delivery timeline	Please refer to revised "Section E: Scope of Services"
301	Brief Scope of Work	Transition from existing SOC to NGSOC	60	Manage day to day operations of currently running SOC setup from two months from date of issuance of PO	Kindly confirm the SIEM tool for Existing solution	Please refer to revised "Section E: Scope of Services"
302	Detailed Scope of Work	Next-Generation Security Operations Center (NGSOC)	64	The vendor should ensure the reduction of remediation time as per defined SLA	remediation time cannot the part of SOC SLA as this is depending on other solutions Need to change accordingly	Please refer to revised "Section E: Scope of Services"
303	Detailed Scope of Work	Next-Generation Security Operations Center (NGSOC)	66	The vendor should conduct root cause analysis (RCA) and provide RCA reports for security incidents as outlined by LIC's requirements.	Kindly change the RCA limit only for P1 , for other P2 , P3 and P4 will have investgration details in ITSM	Please refer to revised "Section E: Scope of Services"
304	3. Technical Bid		22	LIC will be responsible to provide all the hardware required for in-scope solutions' implementation, i.e server/VMs and will provide RHEL OS and Database – MySQL, if required as part of the solution.	Whether LIC will provide the online storage and offline storage (tape library) both at DC and DR?	Please refer to the revised "Annexure F"
305	Eligibility Criteria	Point no 4	14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Request you to please revised the clause as per below: The Bidder should have minimum of 5 years of experience in supplying, implementing/supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Minimum Eligiblity Criteria"

306	Eligibility Criteria	Point no 5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Request you to please revised the clause as per below: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented/supported the SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum two organizations of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
307	Eligibility Criteria	point no 7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request you to please revised the clause as per below: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented /supported the proposed UEBA OEM for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Minimum Eligiblity Criteria"
308	Annexure D: Technical Scoring	Point no 2	109	The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to change the clause as per below: The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
309	Annexure D: Technical Scoring	point no 3	109	The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Minimum Eligiblity Criteria"
310	Annexure D: Technical Scoring	point no 4	109	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. 2 references of 60,000 EPS and above -> 15 Marks • 2 references of 50,000 EPS and above -> 12 Marks • 2 references of 30,000 EPS and above -> 8 Marks • 2 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D
311	Commercial Bid		23	The Bidder should have the capability to implement and maintain the project during the contract period of 5 years. The vendor should also be able to carry out any changes, if necessitated by LIC during the contract period of 5 years. The contract period may be further extended by a period of two years at the sole discretion of LIC of India on the same terms & conditions including the price component.	Request LIC to kindly modify the clause as "The contract period may be further extended by a period of two years after mutual discussion and agreement on terms & conditions including the price component."	Please refer to the revised "Commercial Bid"
312	Payment Terms		99	Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC (30%)	Request to make this milestone at 60% of cost	Please refer to the revised "Payment Terms & Conditions"
313	Payment Terms		99	Installation and integration, initial OEM audit and acceptance testing as per scope of work. (40%)	Request to make this milestone at 30% of cost	Please refer to the revised "Payment Terms & Conditions"
314	Payment Terms		99	After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/ (25%)	Request to make this milestone at 5% of cost	Please refer to the revised "Payment Terms & Conditions"
315	Payment Terms		99	Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work (5%)	Request to make this milestone at 5% of cost	Please refer to the revised "Payment Terms & Conditions"
316	Annexure F – Technical Compliance.xlsx	NBAD Technical Specifications - Point 2	1	The packet captured at line rate for all sensors shall be stored for 7 days and metadata to be stored for 1 year. The storage required for such retention shall be planned by the bidder and included. The selected vendor shall store 5 days packet level data / raw data at any point of time, which must include contents required for network forensic purpose like packet analysis, session analysis, host analysis, error analysis, TCP analysis etc. Accordingly, bidder shall provision the required storage capacity in the proposed solution.	There is typo error in the first line which need to be corrected as per the requirement. So, we request to change the clause mention as: "The packet captured at line rate for all sensors shall be stored for 5 days and metadata to be stored for 1 year. The storage required for such retention shall be planned by the bidder and included. The selected vendor shall store 5 days packet level data / raw data at any point of time, which must include contents required for network forensic purpose like packet analysis, session analysis, host analysis, error analysis, TCP analysis etc. Accordingly, bidder shall provision the required storage capacity in the proposed solution."	Please refer to the revised "Annexure F"
317	Annexure F – Technical Compliance.xlsx	NBAD Technical Specifications - Point 32	1	The solution should support the enrichment of a packet or flow to provide information about source/destination such as MAC/IP/Port numbers and country, application name, Bytes, Packets, URLs, TLS versions Client Side, TLS version and cipher in use from server side, Username, Proxy IP address, NAT device, action taken-allowed/denied, etc. are available.	1. We request to change the clause mention as: "The solution should support the enrichment of a packet or flow to provide information about source/destination such as MAC/IP/Port numbers and country, application name, Bytes, Packets, URLs, TLS versions Client Side, TLS version and cipher in use from server side, Proxy IP address, NAT device, etc. are available". 2. We request on the clarification for the action taken - allowed / denied etc.	Please refer to the revised "Annexure F"

318	Annexure F – Technical Compliance.xlsx	NBAD Technical Specifications - Point 52	1	The solution shall reconstruct full session from packet data, including web, email, and chat sessions, along with associated files so as to easily investigate security incidents without the need for packet expertise.	Since capturing Email and Chat files will be associated with Privacy issues, we request to change the clause mention as: "The solution shall reconstruct full session from packet data, including web, ftp, and remote sessions, along with associated files so as to easily investigate security incidents without the need for packet expertise."	Please refer to the revised "Annexure F"
319	Annexure F – Technical Compliance.xlsx	PCAP Technical Specifications - Point 25	1	The solution should capture the network traffic and support forwarding the captured packets to other network-based security tools/technologies.	Packets can be stored and forwarded to security devices manually. PCAP should be always on Packet capture with on device packet decode capability . So, we request to change the clause as mention: "The solution should capture the network traffic and support manual export or download of packets or forwarding the captured packets to other network-based security tools/technologies."	Please refer to the revised "Annexure F"
320	Annexure F – Technical Compliance.xlsx	PCAP Technical Specifications - Point 35		The solution should allow import of PCAP data, making it easy to analyse historical data and compare captured data to a "known-good" baseline.	PCAP should be always on Packet Capture tool ingesting packets from all the vantage points and on device packet decode capability. So, we request to remove this clause.	Please refer to the revised "Annexure F" . Clause Deleted
321	2. Detailed Scope of Work	IX. Network Behavior Anomaly Detection (NBAD)	69	The vendor should calculate precise flows per second to determine the level of network traffic.	Flows per second is specific to a technology and we utilize packets for NBAD, we request to change the clause to: "The vendor should calculate precise flows per second or traffic throughput (bps)to determine the level of network traffic."	Please refer to revised "Section E: Scope of Services"
322	7. Service Level Agreements (SLAs) & Penalties	Penalties on Non-Performance of SLA during contract period - Point 18	89	PCAP data accuracy Ensure data integrity with no more than 1% packet loss. Retain captured PCAP data for a minimum of 90 days and 365 days in cold storage for incident response in near real time or within 1 hour for archived date.	As mentioned in "Annexure F – Technical Compliance.xlsx", PCAP Technical Specifications, Point # 3, we need to store 5 days packet level data. So, we request you to modify this clause as follows: "PCAP data accuracy Ensure data integrity with no more than 1% packet loss. Retain captured PCAP data for up to 5 days for incident response in near real time and metadata for 365 days for trend analysis."	Please refer to the revised "Annexure F"
323	6. Project Timelines	The Phase Wise Project Timelines as below - Point 2	82	Delivery of all the equipment as quoted in the bill of materials for each solution/ service in-scope. Date of delivery of last item shall be taken as date of delivery for all items. T + 8 Weeks	Considering the additional time required for PO process from Bidder to OEM, we request to change the delivery time in this clause from "T + 8 Weeks" to "T + 12 Weeks"	Please refer to the revised "Section E: Scope of Services"
324	6. Project Timelines	The Phase Wise Project Timelines as below - Point 3	82	Phase 3 : Implementation of PCAP and NBAD T + 8 Weeks	First, Implementation will happen after Hardware Delivery, so both cannot be "T + 8 Weeks", we request you to increase the schedule for Implementation Time based on Delivery Time. Secondly, as mentioned in separate point, considering the additional time required for PO process from Bidder to OEM, we have requested to change the delivery time in that clause from "T + 8 Weeks" to "T + 12 Weeks". Accordingly, we request to change the Implementation of PCAP and NBAD in this clause from "T + 8 Weeks" to "T + 24 Weeks".	Please refer to the revised "Section E: Scope of Services"
325	4. RACI Matrix	PCAP	73	PCAP Platform administration SI: A OEM: R	Since SI is going to manage the PCAP Solution for LIC, we request you to change add Responsible - R for SI: PCAP Platform administration SI: RA OEM: R	Please refer to revised "Section E: Scope of Services"
326	27. Period of Validity of Bids	Point e	35	The prices under this RFP will be valid for a period of five years from the date of issue of first Purchase Order.	There are various commercial factors like currency variations, supply chain issues, etc., that have impact on quoted price. So we request LIC to consider changing this as follows: "The prices under this RFP will be valid for a period of 6 months from the date of issue of first Purchase Order."	Please refer to the revised "Period of Validity of Bids"
327	27. Period of Validity of Bids	Point f	36	The commercial offer shall be on a fixed price basis for the contact period. No upward revision in the price would be considered on account of subsequent increases during the offer validity period except for GST and any other applicable taxes.	There are various commercial factors like currency variations, supply chain issues, etc., that have impact on quoted price. So we request LIC to consider changing this as follows: "The commercial offer shall be on a fixed price basis for 6 months from the date of Purchase Order of items in Original Bid BoQ. No upward revision in the price would be considered on account of subsequent increases during the offer validity period except for GST and any other applicable taxes."	Please refer to the revised "Period of Validity of Bids"
328	Section E: Scope of Services 1. Brief Scope of Work	Training & Certification	56	#NAME?	1. Both these points seem to be contradictory as in first point its mentioned that Training to be provided at no cost and in second point its mentioned Training cost shall include Certification level Training. For Certification OEM needs to factor Training Cost. So, please confirm whether or not OEM is required to factor Training and Certification Cost. 2. If we need to include Training and Certification Cost, then, we request you to include Training and Certification Cost Item in "Annexure G - Commercial Bid (Indicative Pricing) (2).xlsx".	Please refer to the revised "Section E: Scope of Services"
329	7. Service Level Agreements (SLAs) & Penalties	Penalties on Non-Performance of SLA during contract period - 19 NBAD Accuracy	90	Achieve an alert accuracy rate of at least 95% while maintaining a false positive rate of no more than 5%.	NBAD's fundamental concept is to alert on Suspicious behavior. Suspicous may or may not be malicious, that can be determined only through forensic investigation. Therefore, the an alert accuracy rate of atleast 95% with false positive rate of no more than 5% is not expected from NBAD Solution. So, we request to delete this clause.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
330	Annexure F – Technical Compliance.xlsx	NBAD Technical Specifications - Point 1	1		Please clarify the number, speed (1G/10G) and type (Copper/Fiber-Short Range/Long Range) of ports required on NBAD Probe at each site	Please refer to the revised "Annexure F"
331	Annexure F – Technical Compliance.xlsx	PCAP Technical Specifications - Point 1	1		Please clarify the number, speed (1G/10G) and type (Copper/Fiber - Short Range/Long Range) of ports required on PCAP Appliance at each site	Please refer to the revised "Annexure F"
332	6. Eligibility Criteria	Eligibility Criteria, Point 5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/ Government/ Private/BFSI Sector.	The asked requirement as eligibility criteria is restrictive for Major reputed Bidders hence we request LIC Team to change the clause and also include bidder or OEM experience in the same clause as below. "The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported SIEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/ Government/ Private/BFSI Sector. "	Please refer to the revised "Minimum Eligiblity Criteria"

333	6. Eligibility Criteria	Eligibility Criteria, Point 7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/ Private/ BFSI Sector Firms with more than 500 branches across different locations in India. Letter of acceptance (LoA)/ purchase order/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/ Particulars confirming relevant experience.	UEBA being an advanced technology has been implemented only in recent time for Indian customers hence, the asked requirement as eligibility criteria is restrictive for Major reputed Bidders and OEMs . We request LIC team to please change the clause as below. "The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the UEBA for minimum 02 (two) organisations in PSU/Government/ Private/ BFSI Sector Firms." Letter of acceptance (LoA)/ purchase order/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/ Particulars confirming relevant experience.	Please refer to the revised "Minimum Eligiblity Criteria"
334	Technical Compliance for SIEM	Point 71	Sheet SIEM Technical Specifications	The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries such as (but not limited to) NLP, Python, etc.	Please change this to : The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms/alert detection rules from popular open source libraries by supporting writing similar logic in the solution.	Please refer to the revised "Annexure F"
335	Technical Compliance for SOAR	Point 11	Sheet SOAR Technical Specifications	The solution should support 800+ integrations out of the box. Integration packs should include pre-built use cases consisting of playbooks, automation actions, scripts that can be customised for LIC's SOC. The solution should have an integration store that is continuously updated with both OEM and vendor provided integration.	Out Of the Box Integration asked is OEM specific its too high for any typical SOAR solution we request LIC to change the clause as The solution should support 100+ integrations out of the box. Integration packs should include pre-built use cases consisting of playbooks, automation actions, scripts that can be customised for LIC's SOC. The solution should have an integration store that is continuously updated with both OEM and vendor provided integration.	Please refer to the revised "Annexure F"
336	Technical Compliance for SOAR	Point 12	Sheet SOAR Technical Specifications	The solution must have out-of-the-box use cases ecosystem with 800+ integrations including but not limited to the following technologies: -Forensic tools (e.g. FTK, EnCase, Autopsy..) -IT (e.g. AD, SAML...) -Communication tools (e.g. email, Slack, HipChat...) -SIEM tools -Endpoint Security -Network Security -Active Directory -Threat Intelligence -Dynamic malware analysis	Out Of the Box Integration asked is OEM specific its too high for any typical SOAR solution we request LIC to change the clause as The solution must have out-of-the-box use cases ecosystem with 100+ integrations including but not limited to the following technologies:	Please refer to the revised "Annexure F"
337	Technical Compliance for SOAR	Point 27	Sheet SOAR Technical Specifications	The solution should support 250+ out of the box playbooks. The playbooks should support: - nested playbooks to deploy multiple automations as part of a single use case - conditional decision trees - user surveys for input from various stake holders in the use case/reviews - time based actions - escalation actions	Out Of the Box Playbook asked is OEM specific its too high for any typical SOAR solution we request LIC to change the clause as The solution should support 100+ out of the box playbooks. The playbooks should support:	Please refer to the revised "Annexure F"
338	3. Sizing Requirements	Point 3	Page 71	SOAR (Security Orchestration, Automation and response), 30 authorized user licenses	We recommend LIC to change the clause and asked the licenses on Role basis. SOAR (Security Orchestration, Automation and response), Solution should include min 5 Admin level access licenses out of 30 Analyst and rest should be read only analyst licenses.	Please refer to the revised "Section E: Scope of Services"
339	Technical Compliance for UEBA	Point 21	Sheet UEBA Technical Specifications	The proposed solution should have the capacity to utilize both unsupervised and supervised machine learning algorithms, artificial intelligence and deep learning.	Requesting LIC to please change the Clause as " The solution should have advanced unsupervised machine learning analytics models,algorithms, artificial intelligence and deep learning." Unsupervised machine learning is more advance method to detect Unknown threats using Unlabeled data, supervised Machine learning is resource intensive and simply a rule based detection and practically any machine learning concept is not applicable for supervised ML here hence we request to please change the clause.	Please refer to the revised "Annexure F"
340	Technical Compliance for UEBA	Point 27	Sheet UEBA Technical Specifications	The proposed solution should have the capability to support a model that enables interconnection or chaining of Machine Learning models, allowing the output from one ML model to serve as input to another ML model. This is necessary for correlating multiple user-based attacks.	Request to please delete the Clause as it is restricted for multiple UEBA vendors. Justification : Each OEM has different approach to implement Use Cases, like correlating of multiple user-based attacks, Chaining ML Models is Specific and restricted clause we request to change the clause or delete the clause for wider participation	Please refer to the revised "Annexure F"
341	6. Eligibility Criteria	Eligibility Criteria,Point No.5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	This clause might unintentionally exclude technically qualified SIEM OEMs without direct experience with the vendor for the specified duration. To expand the pool of qualified SIEM options without compromising cybersecurity standards, we kindly ask for a reconsideration. Our suggestion is to limit the clause to "The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed /Similar SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector".This adjustment would allow us to consider a broader range of SIEM solutions while maintaining the expertise of established SOC vendors. Also Kindly requesting to provide Exception or Relaxation for Technically qualifed Make In India Starups for the clause "The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP", as this will help more Make In India Startup OEMs to come forward and particpate in this opportunity.	Please refer to the revised "Minimum Eligiblity Criteria"

342	6. Eligibility Criteria	Eligibility Criteria,Point No.7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Kindly requesting to provide Exception or Relaxation for Technically qualifed Make In India Starups,this will help more Make In India Startup OEMs to come forward and particpate in this opportunity.	Please refer to the revised "Minimum Eligiblity Criteria"
343	Section E: Scope of Services	4. RACI Matrix Table : Section Service SIEM	72		The responsibility and accountability of "SIEM Platform Administration" in the table mentioned under the service SIEM occurs two times which are contradictory to each other. Kindly requesting to confirm whether responsibility is that of bidder or OEM.	Please refer to revised "Section E: Scope of Services"
344	Section E: Scope of Services	1. Brief Scope of Work	51	2. Designing - o OEM should design the overall implementation architecture (high-level diagram and low-level diagram) for each in-scope solution. o Architecture workshop to be conducted by OEM to design the architecture as per industry best practices.	Request this be changed as below to accomodate OEM certified Partners. 2. Designing - o OEM/OEM certified partner should design the overall implementation architecture (high-level diagram and low-level diagram) for each in-scope solution. o Architecture workshop to be conducted by OEM/OEM certified partner to design the architecture as per industry best practices.	Please refer to revised "Section E: Scope of Services"
345	Section E: Scope of Services	2. Detailed Scope of Work	62	The bidder / System Integrator shall engage the services of respective OEMs for plan, design and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be changed as below to accomodate OEM certified Partners. The bidder / System Integrator shall engage the services of respective OEMs/OEM Certified partner for plan, design and implementation of the solution. The OEM(s)/OEM Certified Partner must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to revised "Section E: Scope of Services"
346	Section E: Scope of Services	2. Detailed Scope of Work	62	The bidder is responsible for integrating all assets within the LIC environment and this responsibility shall rest exclusively with the bidder. The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance and adoption of the total solution leveraging the behaviour modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Request this be changed as below to accomodate OEM certified Partners. The bidder is responsible for integrating all assets within the LIC environment and this responsibility shall rest exclusively with the bidder. The bidder shall ensure that the **OEM(s)/OEM Certified partner** has end to end responsibility for plan, design, implementation, maintenance and adoption of the total solution leveraging the behaviour modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Please refer to revised "Section E: Scope of Services"
347	Section E: Scope of Services	2. Detailed Scope of Work	62	The bidder shall ensure that the configuration, implementation and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be changed as below to accomodate OEM certified Partners. The bidder shall ensure that the configuration, implementation and testing of the solution components to be carried out by resources from the **OEM/OEM certified partner** as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM/OEM Certified Parnter	Please refer to revised "Section E: Scope of Services"
348	Section E: Scope of Services	2. Detailed Scope of Work	62	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be changed as below to accomodate OEM certified Partners. The **bidder and OEM/OEM certified partner's** services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below	Please refer to revised "Section E: Scope of Services"
349	Section E: Scope of Services	2. Detailed Scope of Work	70	under IX. Network Behavior Anomaly Detection (NBAD) The vendor has to implement use cases in consultation with LIC, after conducting appropriate workshops along with the OEM.	Request this be changed as below to accomodate OEM certified Partners. The vendor has to implement use cases in consultation with LIC, after conducting appropriate workshops along with the **OEM/OEM Certified partner**	Please refer to "Revised Section E: Scope of Services"
350	Section E: Scope of Services	4. RACI Matrix	71	The Tabular Colum mention OEM	Request the tablular column to say OEM/OEM Certified parter	Please refer to revised "Section E: Scope of Services"
351	Section E: Scope of Services	4. RACI Matrix	72	10. NBAD Anomaly and Threat Detection ; OEM scope is 'R'	Request the scope of OEM/OEM certified partner to be 'C'	Please refer to revised "Section E: Scope of Services"
352	Section E: Scope of Services	4. RACI Matrix	72	10. NBAD Dashboard and Reporting ; OEM scope is 'R'	Request the scope of OEM/OEM certified partner to be 'C'	Please refer to revised "Section E: Scope of Services"
353	Section E: Scope of Services	4. RACI Matrix	72	10. NBAD Incident Analysis ;OEM scope is 'A'	Request the scope of OEM/OEM certified partner to be 'C'	Please refer to revised "Section E: Scope of Services"
354	Section E: Scope of Services	4. RACI Matrix	73	10. NBAD NBAD Platform administration ;OEM scope is 'R'	Request the scope of OEM/OEM certified partner to be 'C'	Please refer to revised "Section E: Scope of Services"
355	Annexure F: Technical Compliance	NBAD Technical Specifications	113	The solution should have the scalability to cover the entire enterprise network with ability to support traffic rate as per following site requirements or its equivalent Flows Per Second or Packets Per Second from day one. Sampling rate to be 1:1 only. Internet Facing Sites: - Site A: 3 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Considering the deployment with the Geographical spread shared on this point , it will be worthwhile for LIC to consider below points in the RFP for smooth operations. 1. The solution deployed should enable LIC to gain visibility across all network conversations, including east-west and north-south traffic, to detect both internal and external threats. 2. The solution deployed should ensure visibility with in the branch traffic as well as of end users for the lateral movements (within the branch and between Branch to branch) uptill the DO Offices minimally so as to ensure the security policy framework is well administered 3. The deployed solution for NBAD with visibility for end users til branches should be in such a way that the WAN utilization across MPLS links is minimally impacted to the order of 5-10%.	Please refer to the revised "Annexure F"

356	Annexure F: Technical Compliance	NBAD Technical Specifications	113	2. The packet captured at line rate for all sensors shall be stored for 7 days and metadata to be stored for 1 year. The storage required for such retention shall be planned by the bidder and included. The selected vendor shall store 5 days packet level data / raw data at any point of time, which must include contents required for network forensic purpose like packet analysis, session analysis, host analysis, error analysis, TCP analysis etc. Accordingly, bidder shall provision the required storage capacity in the proposed solution.	Request this point be removed from NBAD section and moved to PCAP Section since this is specific to PCAP solution asks of the RFP	Please refer to the revised "Annexure F"
357	Annexure F: Technical Compliance	Nbad Technical Specification	113	39. The solution should be capable to classify, extract and reconstruct network activity along with session reconstruction and packet analysis. No data should be sent to any 3rd party or open source components and cloud for any type of analysis.	Request this point be removed from NBAD section and moved to PCAP Section since this is specific to PCAP solution asks of the RFP	Please refer to the revised "Annexure F"
358	Annexure F: Technical Compliance	Nbad Technical Specification	113	52. The solution shall reconstruct full session from packet data, including web, email, and chat sessions, along with associated files so as to easily investigate security incidents without the need for packet expertise.	Request this point be removed from NBAD section and moved to PCAP Section since this is specific to PCAP solution asks of the RFP	Please refer to the revised "Annexure F"
359	Annexure F: Technical Compliance	Nbad Technical Specification	113	51. The solution should have the capability to detect zero-day events, multi-stage, fileless and other evasive advanced attacks using behaviour analytics and signature-less analysis.	Request this point to be rephrased as below since **Filesless inspection** is not native NBAD solution functionality: The solution should have the capability to detect zero-day events, multi-stage threats and other evasive advanced attacks using behaviour analytics and signature-less analysis	Please refer to the revised "Annexure F"
360	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	115	_ (OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _ (OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to revised "Annexure H"
361	6. Eligibility Criteria		14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	We request you to revise this clause as "The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting any of the 9 in-scope solutions related to this RFP to organisations in PSU/Government/ Private/BFSI Sector Firms in India."	Please refer to the revised "Minimum Eligiblity Criteria"
362	6. Eligibility Criteria		15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
363	6. Eligibility Criteria		15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	The bidder must have a minimum of 100 IT permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification / CCNA / MCSE, etc. HR undertaking to be provided by organization authorized signatory.	Please refer to the revised "Minimum Eligiblity Criteria"
364	Technical Compliance for UEBA	Point 21	Sheet UEBA Technical Specifications	The proposed solution should have the capacity to utilize both unsupervised and supervised machine learning algorithms, artificial intelligence and deep learning.	Requesting LIC to please change the Clause as " The solution should have advanced unsupervised machine learning analytics models,algorithms, artificial intelligence and deep learning." Unsupervised machine learning is more advance method to detect Unknown threats using Unlabeled data, supervised Machine learning is resource intensive and simply a rule based detection and practically any machine learning concept is not applicable for supervised ML here hence we request to please change the clause.	Please refer to the revised "Annexure F"
365	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	We request LIC to consider the amendment of this clause as this is an advanced solution and it has been deployed by a few organizations and the number count will not be available as per the eligibility criteria requirement so we request LIC to modify the clause as: "The Bidder or its OEM should have a minimum of 1 year of experience in supplying, implementing, and supporting minimum 3 out of the 9 in-scope solutions in the multiple purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 1000 licences across different locations in India"	Please refer to the revised "Minimum Eligiblity Criteria"
366	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	We request LIC to consider the amendment of this clause as this is an advanced solution and it has been deployed by a few organizations and the number count will not be available as per the eligibility criteria requirement so we request LIC to modify the clause as: "The bidder or its OEM during the last 3 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 2500 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with combined 2800 EPS distributed across India in the last 3 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company"	Please refer to the revised "Minimum Eligiblity Criteria"
367	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request LIC to amend this clause because UEBA is the new solution and there is not much deployment in any of the organizations. Instead of asking for the deployment numbers, we request LIC to modify the clause as: "The Bidder or its OEM should have the capability for demonstrating the UEBA Solution and also ready to do the Proof of Concept (POC) as per the LIC requirements "	Please refer to the revised "Minimum Eligiblity Criteria"

368	Eligibility Criteria	4	14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India or Globally.	Please refer to the revised "Minimum Eligiblity Criteria"
369	Eligibility Criteria	4	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of maximum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India/Globally of maximum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	Please refer to the revised "Minimum Eligiblity Criteria"
370	Eligibility Criteria	7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India or Globally.	Please refer to the revised "Minimum Eligiblity Criteria"
371	Annexure-D Technical scoring	2	109	The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in Indiaor Globally from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Minimum Eligiblity Criteria"
372	Annexure-D Technical scoring	4	109	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India or globally for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work	Please refer to the revised "Annexure - D"
373		4	13 and 60	Objective and Transition from existing SOC to NGSOC	Is our understanding correct that LIC is enhancing its information security posture for implementing Threat Detection and Incident Response Solutions.Will this require a migration from current platform? What is the current platform? What is current EPS count	Please refer to revised "Section E: Scope of Services".
374	Resource Deployment		73		Please confirm on support model expectation. Is it via dedicated or shared model? Please help in sharing no. of locations where in onsite resources deployed?	Please refer to the revised "Section E: Scope of Services"
375	Annexure F	Technical Compliance for SIEM	6	The proposed solution must have the ability to retain logs and data. Raw logs and associated normalised events must be stored on online media for a duration of 6 months from the date of the event, and this data should be queryable and reportable. Offline availability of logs to be planned for 5 Years for all log sources. This could be stored in low cost storage for 2 years and rest can be saved in Tape library.	Our understanding from clause is that online retention is for 6 months and the overall retention is for 5 years. Do let us know if the understanding is correct.	Please refer to the revised "Annexure F"
376	Annexure F	Technical Compliance for SOAR	8	The solution should support CI/CD pipeline for faster development.	This is not a SOC solution specification but of an application development framework. Kindly delete the clause	Please refer to the revised "Annexure F"
377	Annexure F	Technical Compliance for SOAR	11	The solution should support 800+ integrations out of the box. Integration packs should include pre-built use cases consisting of playbooks, automation actions, scripts that can be customized for LIC's SOC. The solution should have an integration store that is continuously updated with both OEM and vendor provided integration.	Request to modify the clause - The solution should not have license limitation for integration and integration pack should include pre-built use cases consisting of playbooks, automation actions, scripts that can be customized for LIC's SOC. The solution should have an integration store that is continuously updated with both OEM and vendor provided integration.	Please refer to the revised "Annexure F"
378	Annexure F	Technical Compliance for SOAR	27	The solution should support 250+ out of the box playbooks. The playbooks should support: -nested playbooks to deploy multiple automations as part of a single use case. -conditional decision trees -user surveys for input from various stake holders in the use case/reviews- time based actions -escalation actions	Leading SOAR vendors provide playbook template to drive specific playbooks based on required use cases and one playbook template can drive more than 10-20 playbooks which will address LIC requirements for the clause. Hence attaching a specific number is not the right metric. Please confirm.	Please refer to the revised "Annexure F"
379	Annexure F	Technical Compliance for SOAR	39	The solution should support sending out authenticated surveys to drive the investigation workflow.	Request clarity on the specific requirement of 'sending out authenticated surveys to drive the investigation workflow'.	Please refer to the revised "Annexure F"
380	Annexure F	Technical Compliance for SOAR	61	The solution should use machine learning for analyst assignment and auto-calculate incident severity.	Request clarity on using machine learning for analyst assignment.	Please refer to the revised "Annexure F"

381	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	We request LIC to modify the clause as "The bidder & its OEM during the last 3 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM for a minimum of 01 (one) organizations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum one organizations with minimum 2000 EPS distributed across India in the last 3 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company"	Please refer to the revised "Minimum Eligiblity Criteria"
382	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	We request LIC to modify this clause as the bidder or Its OEM must have a minimum of 40 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as OEM Level Certification.	Please refer to the revised "Minimum Eligiblity Criteria"
383		4	14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Can the bidder submit 2-3 different purchase orders of a minimum of 5 out of 9 solutions or it is necessary to submit a single PO for all 5 solutions?	Please refer to the revised "Minimum Eligiblity Criteria"
384		10	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	The count of 25 resources is fixed or can be changed and reduced as per the request by the bidder.	Please refer to the revised "Minimum Eligiblity Criteria"
385	13. Online Reverse Auction	j	29	Online reverse auction subject to Guidelines on Public Procurement Preference to Make in India)	Is this a mandate clause or just a preference? Can the bidder submit a solution that does not belong to India?	Please refer to the revised "Online Reverse Auction"
386	Section E: Scope of Services	1. Brief Scope of Work -> Transition from existing SOC to NGSOC:	60	Transition from existing SOC to NGSOC	If LIC has SOC in place, may we know the OEM/Model of the existing solution currently used?	Please refer to the revised "Section E: Scope of Services"
387	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	We request LIC to amend the clause as the Bidder or its OEM should have an experience in supplying, implementing, and supporting in-scope solutions in the purchase order related to this RFP to organizations in PSU/Government/Private/BFSI Sector Firms with more than 8 years of experience in Cyber Security domain"	Please refer to the revised "Minimum Eligiblity Criteria"
388	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	We request LIC to modify the clause as "The bidder & its OEM during the last 3 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM for a minimum of 01 (one) organizations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum one organizations with minimum 1500 EPS distributed across India in the last 3 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company"	Please refer to the revised "Minimum Eligiblity Criteria"
389	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	We request LIC to modify this clause as t Its OEM must have a minimum of 50 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as OEM Level Certification.	Please refer to the revised "Minimum Eligiblity Criteria"
390				Request this point to be added	For all the solutions being proposed & the critical features, we would recommend LIC do a demonstration of them so that they are validated. We request LIC to score the demosntrations & include them in the final score calculation.	Please refer to the revised "Technical Bid "
391	SIEM Compliance	Technical Specification	Point. 8	The proposed solution should have the capability to effectively manage peak EPS (80000 EPS) and handle burst periods which could be 3 times more than the peak EPS without dropping logs.	This point is contradicting to point no. 3 above. As the earlier point was mentioning twice the sustained capacity (i.e. 1,60,000 EPS) but here it is mentioned as 3 times. Also the server based licensing protects you from any such EPS license capping. please allow server based licensing as well as suggested - please confirm the exact spike capacity to be considered.	Please refer to the revised "Annexure F"
392	SIEM Compliance	Technical Specification	Point. 33	The proposed solution's search performance should be capable of searching through millions of unstructured (raw) logs within 5 minutes.	The Query response time largely depends on multiple factors like query syntax, HW resources, load on the system etc. Most of the OEM providing the 30 seconds commitment will limit the number of results/capping first 1000 logs. Please consider this point as optional or also add the point to ensure that query result shouldnt terminate or truncate any number of results queried by the analyst	Please refer to the revised "Annexure F"
393	SIEM Compliance	Technical Specification	Point. 35	The proposed solution should have capability to collect, normalize and store configuration data from various devices and use it for analysis.	Most of the SIEM tools typically ingests the log, flows and raw packets data for anaylsis - using device configuration data falls out side of SIEM pureview and hence this point should be made optional	Please refer to the revised "Annexure F"
394	SIEM Compliance	Technical Specification	Point. 56	The proposed solution must be designed to provide a query response within 30 seconds or less.	The Query response time largely depends on multiple factors like query syntax, HW resources, load on the system etc. Most of the OEM providing the 30 seconds commitment will limit the number of results/capping first 1000 logs. Please consider this point as optional or also add the point to ensure that query result shouldnt terminate or truncate any number of results queried by the analyst.	Please refer to the revised "Annexure F"
395	SIEM Compliance	Technical Specification	Point. 70	The proposed solution machine learning capabilities must include API access and role-based access controls for machine learning models.	Our interpretation is LIC needs API access to manage and control the ML model - if so, we don't have any such provision specifically for this requirement.	Please refer to the revised "Annexure F"
396	SIEM Compliance	Technical Specification	Point. 72	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.	Machine learning engine is a resource intensive action and hence it is better to keep it away from the core platform - this ensures the stability of the core SIEM platform kept untouched. The output is better achieved with two separate engine - please confirm if this point can be made optional as not all SIEM tool has common engine for ML & SIEM.	Please refer to the revised "Annexure F"

397	SIEM Compliance	Technical Specification	Point. 73	The proposed solution should not have separate compute requirements to run the ML models. It should be embedded in the SIEM solution.	Same as point 72 (Query point 18)	Please refer to the revised "Annexure F"
398	SIEM Compliance	Technical Specification	Point. 86	The proposed solution should be able to provide inbuilt charts for top attacks & attackers, OWASP & MITRE ATT&CK based threat analysis, trending threats, attack demographics etc. These charts and reports to be in details addressing attack vectors, channels, and methods.	All the mentioned reports are achieveable except OWASP which will ned custom configuration - please confirm if this is acceptable	Please refer to the revised "Annexure F"
399	SIEM Compliance	Technical Specification	Point. 87	The proposed solution should natively provide ability to add custom content to the report such as (but not limited to) header, footer, table of contents, notes, etc.	The tool has capability of whitelabeling the reports with client's log and layout can be customised. However TOC, header/footer and notes needs to be managed manually by the bidder - please confirm if this is OK. Or bidder can use the 3rd part reporting mechanism to fulfill this requirement	Please refer to the revised "Annexure F"
400	SIEM Compliance	Technical Specification	Point. 89	The reports should have the option to be exported in PDF, Word, CSV, and HTML formats.	The tool has capability of exporting in all the mentioned format except word doc - please let us know if this is acceptable	Please refer to the revised "Annexure F"
401	SOAR Compliance	Technical Specification	Point. 8	The solution should support CI/CD pipeline for faster development.	Our app exchange and app used by the platform uses dockerised instance and CI-CD delivery mechanism. Please confirm if this is acceptable	Please refer to the revised "Annexure F"
402	SOAR Compliance	Technical Specification	Point. 39	The solution should support sending out authenticated surveys to drive the investigation workflow.	Raising a surveys could be important however it may not be available with all the OEM as mandatory feature. You are requested to make this as an optional requirement.	Please refer to the revised "Annexure F"
403	SOAR Compliance	Technical Specification	Point. 62	The solution should support creation of customizable forms for change/request management.	Form creation may be leveraged by the 3rd party integrations line slack/teams or customised workflow tool via API integration as a workaround to this - we believe that form management isnt SOAR core deliverables - please make this as an optional point or let us know if the custom 3rd party integration can be acceptable.	Please refer to the revised "Annexure F"
404	SOAR Compliance	Technical Specification	Point. 66	The solution must provide for a virtual War Room and evidence dashboard on a per incident basis for comprehensive collection of all investigation actions, artifacts, and collaboration at one place.	Having a WAR room within SOAR platform may not be necessary and it could be a specific to an OEM. Having such collaboration may be leveraged by the 3rd party integrations line slack/teams - please make this as an optional point or let us know if the point can be addressed by the mentioned integration is can be acceptable.	Please refer to the revised "Annexure F"
405	SOAR Compliance	Technical Specification	Point. 84	The solution should support creation of customized reports in formats such as (but not limited to) CSV, Doc and PDF with custom logo of LIC.	We support all the mentioned formats except .DOC. Please confirm if this is acceptable	Please refer to the revised "Annexure F"
406	UEBA Compliance	Technical Specification	Point. 6	The proposed solution should support data encryption at rest and in transit such as (but not limited to) FDE, TLS v1.3, SSL, etc. to ensure data privacy.	The tool has the capability of doing the encryption at rest, however it can have heavy overheads on the performance - we strongly suggest to make this point optional.	Please refer to the revised "Annexure F"
407	UEBA Compliance	Technical Specification	Point. 25	The proposed solution should offer case management, incident investigation, and comprehensive reporting capabilities, enhancing investigation and response by integrating embedded security orchestration and automation features for accelerated processes.	This point can be achieved via SIEM & SOAR deliverables - please confirm if this is acceptable	Please refer to the revised "Annexure F"
408	UEBA Compliance	Technical Specification	Point. 27	The proposed solution should have the capability to support a model that enables interconnection or chaining of Machine Learning models, allowing the output from one ML model to serve as input to another ML model. This is necessary for correlating multiple user-based attacks.	Multiple user based attacks can also be achieved via search based correlation and independent ML models. Please confirm the exception on the nesting ML models requirement.	Please refer to the revised "Annexure F"
409	PCAP Compliance	Technical Specification	Point. 1	The solution should have the scalability to cover the entire enterprise network (North / South and East / West) with ability to perform high speed lossless packet capture & analysis functions for a network traffic capture as per following site requirements from day one. Internet Facing Sites: - Site A: 3.0 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Is it assumed that Site A, B, C & D are equivalent to North Site A, West Site B, East Site C & South Site D?	Please refer to the revised "Annexure F"
410	PCAP Compliance	Technical Specification	Point. 1	The solution should have the scalability to cover the entire enterprise network (North / South and East / West) with ability to perform high speed lossless packet capture & analysis functions for a network traffic capture as per following site requirements from day one. Internet Facing Sites: - Site A: 3.0 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Confirm the average utilisation of each BW capacity mentioned	Please refer to the revised "Annexure F"
411	PCAP Compliance	Technical Specification	Point. 4	The solution should support full line-rate packet capture, real-time conversion to layer 3-7 metadata and have retention of 6 months historical meta-data for trend analysis, long-term reporting and back in time investigation. This back in time feature should be able to enable a user to quickly perform historical security event analysis.	For retaining metadata the same PCAP tool wont be possible. This will need NBAD component - please eliminate the need of meta data as it is overlapping point from NBAD compliance	Please refer to the revised "Annexure F"

412	PCAP Compliance	Technical Specification	Point. 26	The solution should capture and record all network packets in full (both header and payload). In addition, Solution should be capable of selectively saving packet data based on specific application, protocol and time duration or in combination of them for any interested event or incident with in the dashboard/console system in a standard PCAP format. The saved PCAP file can be made accessible on a file share for other tools. Solution should support acquiring/capturing real-time packet with following options per Application Traffic: • Capture the entire packet. • Intelligent slicing of packet based on protocol. • Packet Truncation. • Exclude specific packets • Capture only headers	As per the industry practice the configurations like selectively choosing headers, packet truncation etc taken care by Traffic/TAP aggregators which sends these inputs to PCAP - Please confirm if this is acceptable	Please refer to the revised "Annexure F"
413	PCAP Compliance	Technical Specification	Point. 35	The solution should allow import of PCAP data, making it easy to analyze historical data and compare captured data to a “known-good” baseline.	This can be achieved by NBAD tool - please confirm if this is acceptable	Please refer to the revised "Annexure F"
414	NBAD Compliance	Technical Specification	Point. 1	The solution should have the scalability to cover the entire enterprise network with ability to support traffic rate as per following site requirements or its equivalent Flows Per Second or Packets Per Second from day one. Sampling rate to be 1:1 only. Internet Facing Sites: - Site A: 3 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Please confirm if the mapping and the total BW interpretation per site is correct:- 1. North Zone- Delhi - 7 Gbps - [SITE A] 2. West Zone - Mumbai (DC) - 4.5 Gbps - [SITE B] 3. East Zone - Kolkatta - 5 Gbps - [SITE C] 4. South Zone - Chennai - 7 Gbps - [SITE D] 5. South Central - Hyderabad (BLR - DR) - 8 Gbps - [SITE E] 6. Central Zone - Bhopal - 4 Gbps - [SITE F] 7. East Central Zone - Patna - 1 Gbps - [SITE G] 8. North Central Zone - Kanpur - 1 Gbps - [SITE H]	Please refer to the revised "Annexure F"
415	NBAD Compliance	Technical Specification	Point. 52	The solution shall reconstruct full session from packet data, including web, email, and chat sessions, along with associated files so as to easily investigate security incidents without the need for packet expertise.	This is taken care in PCAP tool - please move this from NBAD to PCAP compliance	Please refer to the revised "Annexure F"
416	Section E: Scope of Services	Transition from existing SOC to NGSOC:	60	Once all the log sources integrated with existing SOC are migrated to NGSOC, ensure the existing SOC is up & running in steady state with security patches by obtaining same from respective OEMs, settings etc. for two years. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, is required to extract old logs for forensic investigation, in case required.	Backup Logs of old SIEM solution can be restored only in the same solution & cannot be restored in the new solution	Please refer to the revised "Section E: Scope of Services"
417	Section E: Scope of Services	Resource Deployment	73	General query	For certification requirement, kindly accept the relevant industry standard certifications instead of specific certifications like GCFA & SANS	Please refer to the revised "Section E: Scope of Services"
418	Eligibility Criteria	Eligibility Criteria	15	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to amend the clause as below The Bidder should have minimum of 3 years of experience in supplying, implementing and supporting minimum 4 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
419	Eligibility Criteria	Eligibility Criteria	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP.	We request to remove the word "Proposed" and enable us to submit the references as per the eligibility. Request to amend the clause as below The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the any SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
420	Eligibility Criteria	Eligibility Criteria	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM)	Request to amend the clause as below The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ CEH/CISA/CISM OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM)	Please refer to the revised "Minimum Eligiblity Criteria"
421	Annexure D -Technical Scoring	Annexure D - Technical Scoring	109	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	We request to remove the word "Proposed" and revised the EPS count references numbers. Request to amend the clause as below The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the any SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 1 reference of 3,00,000 EPS and above -> 15 Marks • 2 references of 2,00,000 EPS and above -> 12 Marks • 3 references of 1,50,000 EPS and above -> 8 Marks • 4 references of 80,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"

422	Annexure D -Technical Scoring	Annexure D - Technical Scoring	109	The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to amend as below The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 4 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
423	Section-G Payment Terms & Conditiona	Section-G Payment Terms & Conditiona	99	30% of cost - Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC (30% of cost)	We request to change the payment terms to 70% Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC	Please refer to the revised "Payment Terms & Conditions"
424	Section-G Payment Terms & Conditiona	Section-G Payment Terms & Conditiona	99	40% - Installation and integration, initial OEM audit and acceptance testing as per scope of work.(40% of the cost)	We request to change the payment 20 % on Installation and integration, initial OEM audit and acceptance testing as per scope of work.	Please refer to the revised "Payment Terms & Conditions"
425	Section-G Payment Terms & Conditiona	Section-G Payment Terms & Conditiona	99	25% - After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s	We request to change 10% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s	Please refer to the revised "Payment Terms & Conditions"
426	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	2.The Bidder must have an annual turnover of minimum Rs.600 Crores per annum during the last 03 (three) years preceding the date of this RFP	We request LIC to exempt this annual turnover clause for MSE & and startup companies as per the GFR rule its is been mentioned that annual turnover & experience criteria should be exempted for Startup & MSE bidder	Please refer to the revised "Minimum Eligiblity Criteria"
427	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	We request LIC to amend the clause as the Bidder or its OEM should have an experience in supplying, implementing, and supporting in-scope solutions in the purchase order related to this RFP to organizations in PSU/Government/Private/BFSI Sector Firms with more than 3 years of experience in IT Infrastructure & Cyber Security business line"	Please refer to the revised "Minimum Eligiblity Criteria"
428	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	We request LIC to modify the clause as "The bidder & its OEM during the last 3 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM for a minimum of 01 (one) organizations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum one organizations with minimum 750 EPS distributed across India in the last 1 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company"	Please refer to the revised "Minimum Eligiblity Criteria"
429	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	We request LIC to modify this clause as t Its OEM must have a minimum of 30 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as OEM Level Certification.	Please refer to the revised "Minimum Eligiblity Criteria"
430	1. Brief Scope of Work	Training & Certification	57	Pre-Implementation: Provide training to the LIC personnel/ Onsite support team on the product architecture, functionality and the design for each solution under the scope of this RFP.	Please share the number of batches and batch size for the training	Please refer to the revised "Section E: Scope of Services"
431	1. Brief Scope of Work	Training & Certification	57	Post Implementation: Provide hands-on training to the LIC personnel/ Onsite support team on day to day operations, alert monitoring, policy configuration, rule creation, report generation for all solutions etc.	Please share the number of batches and batch size for the training	Please refer to the revised "Section E: Scope of Services"
432	1. Brief Scope of Work	Training & Certification	57	Training cost shall be inclusive of Certification level training for three participants.	Please clarify the certification level	Please refer to the revised "Section E: Scope of Services"
433	5. Resource Deployment	SIEM SME	75	SIEM Integration SME	Kindly define the onsite resource requirement and resources per shift	Please refer to the revised "Section E: Scope of Services"
434	5. Resource Deployment	SIEM SME	75	SIEM Engineering Team	Kindly define the onsite resource requirement and resources per shift	Please refer to the revised "Section E: Scope of Services"
435	5. Resource Deployment	SIEM SME	75	Dashboard Experts	Kindly define the onsite resource requirement and resources per shift	Please refer to the revised "Section E: Scope of Services"
436	5. Resource Deployment	SOAR SME	78	SOAR Architect	Kindly define the onsite resource requirement and resources per shift	Please refer to the revised "Section E: Scope of Services"
437	5. Resource Deployment	SOAR SME	78	SOAR API Integrator	Kindly define the onsite resource requirement and resources per shift	Please refer to the revised "Section E: Scope of Services"
438	Annexure C: Eligibility Criteria	Eligibility Criteria	107	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 4. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) should have minimum of 5 years of experience in supplying, implementing and supporting minimum 4 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms in India.	Please refer to the revised "Minimum Eligiblity Criteria"

439	Annexure C: Eligibility Criteria	Eligibility Criteria	107	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 4. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) should have minimum of 7 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single/Multiple purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms in India.	Please refer to the revised "Minimum Eligiblity Criteria"
440	Annexure C: Eligibility Criteria	Eligibility Criteria	107	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 5. a. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) during the last 7 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 30,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. b. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Please refer to the revised "Minimum Eligiblity Criteria"
441	Annexure C: Eligibility Criteria	Eligibility Criteria	107	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Since this is OEM dominated RFP, we request the bank to consider modification of the clause as: 5. The bidder /OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Please refer to the revised "Minimum Eligiblity Criteria"
442	Annexure C: Eligibility Criteria	Eligibility Criteria	107	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 7. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) during the last 7 years preceding to the date of this RFP should have supplied, implemented and supported UEBA OEM for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms in India.	Please refer to the revised "Minimum Eligiblity Criteria"
443	Annexure C: Eligibility Criteria	Eligibility Criteria	107	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Since this is OEM dominated RFP, we request the bank to consider modification of the clause as: 7. The bidder /OEM during thelast 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
444	Annexure C: Eligibility Criteria	Eligibility Criteria	108	10. The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	10. The bidder must have a minimum of 30 IT Security permanent professionals with experience in-scope solutions on their payroll with atleast 10 resources with certifications in security domain such as CISSP/ OSCP/ OEM Level Certification / Equivalent etc.. Minimum 5 resources must have OEM Level Certification (preferably any combination of the proposed OEM).	Please refer to the revised "Minimum Eligiblity Criteria"
445	Annexure C: Eligibility Criteria	Eligibility Criteria	107	2. The Bidder must have an annual turnover of minimum Rs. 600 Crores per annum during the last 03 (three) years preceding the date of this RFP.	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 2. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) must have an annual turnover of minimum Rs. 500 Crores per annum during the last 03 (three) years preceding the date of this RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
446	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	Annual turnover during the last 03 (three) years preceding the date of this RFP. • Greater than INR 900 Crore -> 10 Marks • Greater than INR 700 Crore up to INR 900 Crores -> 7 Marks • Greater than INR 500 Crore up to INR 700 Crores -> 5 Marks	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP . Hence we request the bank to consider credentials of the bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) .	Please refer to the revised "Annexure - D"

447	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	2. The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 2. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
448	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	3. The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	3. The Bidder/OEM during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
449	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	3. The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	3. The Bidder / or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) during the last 7 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 4 out of 9 in single/Multiple Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms in India. • Every Additional reference -> 5 Marks subject to maximum of 10 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
450	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	4. The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to consider modification of the clause as under: 4. The Bidder/OEM during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
451	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	5.The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India: • More than 2 references -> 10 marks • 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to consider modification of the clause as under: 5.The Bidder /OEM during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India: • More than 2 references -> 10 marks • 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
452	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	110	7. The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ Professional OEM Level Certification. • Every Additional 10 Resources -> 2 Marks subject to maximum of 10 marks • 100 Resources -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	7. The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with Security certifications such as CISSP/ OSCP/ Professional OEM Level Certification/ Equivalent etc. • Every Additional 2 Resources -> 2 Marks subject to maximum of 10 marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Please refer to the revised "Annexure - D"
453	Section G: Payment Terms & Conditions	Milestones--Payments	99	1. Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC.------30% 2. Installation and integration, initial OEM audit and acceptance testing as per scope of work.-------40% 3. After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s--------25% 4. Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work.-----5%	Request to modify the Clause as: 1. Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC.------60% 2. Installation and integration, initial OEM audit and acceptance testing as per scope of work.-------25% 3. After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s--------10% 4. Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work.-----5%	Please refer to the revised "Payment Terms & Conditions"

454	6 - Eligibility Criteria	S. No - 5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector.	Already, LIC has defined the selection criteria for the bidder using the eligibility criteria w.r.t. bidders experience in executing such similar projects. By adding this clause, LIC is futher limiting the options available to the bidder. Ideally, this should be OEM's crtieria. Hence request you to remove this clause atleast for the bidder. or allow reference where the bidder may be providing such managed SOC services dedicatedly. Also request to add the following as 60,000 EPS or 2TB per day ?	Please refer to the revised "Minimum Eligiblity Criteria"
455	6 - Eligibility Criteria	S. No - 7	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Already, LIC has defined the selection criteria for the bidder using the eligibility criteria w.r.t. bidders experience in executing such similar projects. The expectation of Entity analystics made more sense, when there was absence of Network Behaviour Analytics. Many SIEM platforms didnt have Network Behaviour Analytics as an add-on component & hence they have come out with UEBA offering. With a strong combination of UBA, NBA and EDR, LIC will achieve much more than independently limiting the selection criteria to UEBA. UEBA is still not adopted by many large organizations. Hence request you to remove this clause atleast for the bidder.	Please refer to the revised "Minimum Eligiblity Criteria"
456	6. Eligibility Criteria	6. Eligibility Criteria	14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to modify this clause as, The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 50 branches across different locations in India. Reason: Few enterprise-wide major customers are large in terms of volume and criticality but do not have more than 50 branch offices.	Please refer to the revised "Minimum Eligiblity Criteria"
457	6. Eligibility Criteria	6. Eligibility Criteria	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Request LIC to modify this clause as, The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The bidder should have been successfully implemented SIEM technology and running in minimum three organizations with minimum 50 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company. Reason: 1. Few enterprise-wide major customers are large in terms of volume and criticality but do not have more than 50 branch offices. 2. Bidder should have technology skill set & strength to manage such large volume SOC operations.	Please refer to the revised "Minimum Eligiblity Criteria"
458	6 - Eligibility Criteria	S. No - 4	15	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the same across multiple purchase orders. It may be limited to the same client but not every client purchases all these technologies across 1 RFP / Purchase Order	Please refer to the revised "Minimum Eligiblity Criteria"
459	6. Eligibility Criteria	6. Eligibility Criteria	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to modify this clause as, The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the UEBA Technology of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 50 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
460	6. Eligibility Criteria	6.7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	UEBA is still not adopted by many large organizations, hence we request LIC to change it to below: The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 20,000 users for minimum 01 organisations in PSU/Government/Private/BFSI Sector Firms with more than 50 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
461	6. Eligibility Criteria	6.10.	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	Does this mean overall 25 across all OEMs asked in the RFP? we request LIC to make this as 10 OEM level certification(preferably of the proposed OEM)	Please refer to the revised "Minimum Eligiblity Criteria"
462	4. Commercial Bid	Point viii	23	The Bidder should have the capability to implement and maintain the project during the contract period of 5 years. The vendor should also be able to carry out any changes, if necessitated by LIC during the contract period of 5 years. The contract period may be further extended by a period of two years at the sole discretion of LIC of India on the same terms & conditions including the price component.	Based on the previous experience of 5 years. Predictibilty of pricing is available for 3 years (As per current industry practice). Any extension on the same terms and conditions and pricing is not available beyound 5 years as the bidder is also supplying lot of 3rd party components. Request to restrict pricing validation to term of contract	Please refer to the revised "Period of Validity of Bids"
463	27. Period of Validity of Bids	Point d	35	The contract is for a period of five years .	Based on general legal terms, the period of contract is from the date of issuance of the purchase order. Also the same, has been mentioned in LIC's RFP. Kindly clarify the understanding.	It should be from the day of sign- off
464	55. Varying the Services	55. Varying the Services	46	LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, etc. cost to be quoted in the commercial bid. Any change in the scope beyond this 25% will be informed to the vendor in writing.	How the rate will be determined if new licenses or applications are needed.	Please refer to the revised "Period of Validity of Bids", revised ""Pricing, Billing, Duties and Taxes" and revised "Varying the Services"

465	point 1 : Brief Scope of Work	Phase 2 : Designing	51	o SOP for operations of the solution. o Detailed roles and responsibilities defined in RACI matrix. o Minimum Baselines Standard Document (MBSS)/Secure Configuration Document (SCD). o Access controls and security measures implemented document.	This is scope of on-site to provide continous improvement in reference to LIC's enviornment. As a bidder, we require clear-cut goals for implementation team to ensure the solutions are implemented and operationalized. Hence only limited scope of implementatoin of such use cases will be undertaken to ensure sufficent implemenation is achieved in specified number of weeks. Rest of the improvements, new use cases, etc will be undertaken during steady state operations. Kindly change and move this point to sustainance phase.	Please refer to the revised "Section E: Scope of Services"
466	Section E	1	57	The bidder and OEM are required to provide training jointly table for people nominated by the LIC for each solution specified in the scope of work.	Most of the bidders are certified hence we request you to please change it to below: The bidder are required to provide training for people nominated by the LIC for each solution specified in the scope of work. The scope will be relevant to only 10 personnel for a period of 1-day.	Please refer to the revised "Section E: Scope of Services"
467	Security Dashboards		58	As part of deliverables, bidder must provide integrated dashboard along with Display Panel / TV set covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc.	Please confirm if the display panels needs to be included	Please refer to the revised "Annexure G - Commercial Bid (Indicative Pricing)"
468	Security Dashboards		58	As part of deliverables, bidder must provide integrated dashboard along with Display Panel / TV set covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc. The dashboard should be an easy-to-use web user interface with search function, create reports, as well as access cases and applications, with just a few clicks.	LIC should ensure that the and development and a production platform with relevant tools like powerBI or Tabuelu is available to the bidder to deliver such and outcome. Also, no opertaional SLA may be applicable for such functionality as this may not critical security function but a good to have feature.	Please refer to the revised "Annexure G - Commercial Bid (Indicative Pricing)"
469	Transition from existing SOC to NGSOC:		60	b. Bidder must ensure that the existing data remain usable for necessary searching, link analytics, hunting, regulatory requirements, forensic investigation etc.	These components are not supplied by the bidder and have a separate contract. Bidder cannot own this responsibility and will provide services on best effort basis. Bidder will not be penalized for any of the issue arising out of the existing platfrom and data.	Please refer to the revised "Section E: Scope of Services"
470	2. Detailed Scope of Work	I. General Requirements	62	The bidder is responsible for integrating all assets within the LIC environment and this responsibility shall rest exclusively with the bidder.	This statement is misleading and the bidder does not yeild any ownership or authority to execute this responsibility. LIC will provide a dedicated SPOC to ensure that all the requirements of the bidder are fulfilled in a timely manner to execute the scope in specified time.	Please refer to the revised "Section E: Scope of Services"
471	Section E: Scope of Services	2. Detailed Scope of Work	63	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	Request LIC to be practical and clear on the expectations. Apart from the annual growth on scale, there is also impact on the implemenation, integration, steady state monitoring, no of alerts to be handled and incident response guidance. A 20% increase in annual scope will be avail addtional efforts and addtional to monitoring team. This needs to be discussed	Clause Deleted . Please refer to the revised "Section E: Scope of Services"
472	5. Resource Deployment	SOC Analyst	73	Certification - CEH & any one SANS certificate	Request up have only one certification. i.e. CEH. SANS certification is a costly affair for any individual and this will need great investment and time. Such resources are not available in the market easily. Request you to kindly consider the experiece of 4 years as sufficient enough.	SANS deleted . Please refer to the revised "Section E: Scope of Services"
473	5. Resource Deployment	Forensic Analyst	73	Forensic Analyst - 5 Years of experience Certifications- GCFE/ GCFE & CHFI	5 years of forensic analyst is sufficient enough to operate dedicatedly. This is very stringent requirement. SANS certification is a costly affair for any individual and this will need great investment and time. Such resources are not available in the market easily. Request you to kindly consider the experiece of 4 years as sufficient enough and only have CHFI as minimum certification.	GCFE deleted. Please refer to the revised "Section E: Scope of Services"
474	5. Resource Deployment	SIEM SME	75	Dashboard Experts – 3 Years of experience	This is basically software development experts and work on generic requirements. They may have similar experience for inegrating and creating a dashboard and may not be Cyber Security Expert.	Please refer to the revised "Section E: Scope of Services"
475	5. Resource Deployment	Threat Intelligence platform Analyst	77	5 Years of experience Certifications- GCTI/CTIA	5 years of integrated SOC Analyst and Threat hunting experience is sufficient enough to operate. This role can be combined with threat hunting. Also the certification requirement is very stringent requirement. SANS certification is a costly affair for any individual and this will need great investment and time. Such resources are not available in the market easily. Request you to kindly merge the scope of work and consider the experiece as sufficient enough	GCTI deleted . Please refer to the revised "Section E: Scope of Services"
476	5. Resource Deployment	Threat Hunter	78	5 Years of experience Certifications- GCFA	5 years of integrated SOC Analyst and Threat hunting experience is sufficient enough to operate. This role can be combined with threat hunting. Also the certification requirement is very stringent requirement. SANS certification is a costly affair for any individual and this will need great investment and time. Such resources are not available in the market easily. Request you to kindly consider the experiece as sufficient enough	GCFA deleted . Please refer to the revised "Section E: Scope of Services"
477	6. Project Timelines	6. Project Timelines	82	The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to modify this clause as, The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 50 branches across different locations in India.	Please refer to the revised "Minimum Eligiblity Criteria"
478	6. Project Timelines	6. Project Timelines	82	Implementation of in-scope solutions/ services. Phase 1 : Implementation of SIEM, SOC, SOAR and UEBA T + 32 Weeks Phase 2 : Implementation of CTI and CTH T + 12 Weeks Phase 3 : Implementation of PCAP and NBAD T + 8 Weeks	Request LIC to extend the Implementation timelines as below for the in-scope solutions/ services. Phase 1 : Implementation of SIEM, SOC, SOAR and UEBA T + 40 Weeks Phase 2 : Implementation of CTI and CTH T + 16 Weeks Phase 3 : Implementation of PCAP and NBAD T + 24 Weeks. Also specify the specific information : Starting of Managed Security Services & sign-off Critieria (When 75% of crown jewels of LIC are integrated. Also mention that if 75% of servers and 10,000 endpoints assets are implemented, that can be used as solution for sign-ff & go-live criteria. Achiving a specific minimum number is very important)	Please refer to the revised "Section E: Scope of Services"

479	6. Project Timelines	6. Project Timelines	82	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go-Live Certificate from LIC. T + 33 Weeks	Request LIC to extend the timeline for Successful Final Acceptance Test of all in-scope solutions as below, T + 33 Weeks	Please refer to the revised "Section E: Scope of Services"
480	6. Project Timelines	6. Project Timelines	83	Implementation of EDR and roll out of agents in the endpoints. Date of implementation of last device shall be taken as date of installation of all devices. T + 24 Weeks	Request LIC to extend the Implementation timelines as below for EDR and roll out of agents in the endpoints. T + 40 Weeks	Please refer to the revised "Section E: Scope of Services"
481	SLA & Penalty	Project Phase level SLA:	83, 84, 85	Points 1,2,3,12,14,15,16,19,20,21 Kick-off meeting with LIC within 1 week of PO. Request for the details of hardware to LIC within 1 week of PO. Request for details of information from LIC within 4 weeks from the date of purchase. The details of Project Coordinator are not communicated to LIC within 3 weeks of receipt of PO If the first (introductory) meeting is not held within 2 weeks If structured weekly meetings are not held (by the Service Delivery Manager) with ED(IT)/Secy(IT)/Dy.Secy(IT)/ Asst.Secy.(IT), Network Section, CO, Mumbai. If CV and certified documents of the proposed candidates as per Resource Deployment section are not submitted within 5 weeks from date of Purchase Order (PO) In case vendor wants to change the onsite support person, minimum of one-and-half month (45 days) advance notice shall be given by the vendor to LIC. If not done, penalty will be imposed. In case vendor wants to change the onsite person, an overlapping period of at least 21 days has to be there between the new and old onsite support person. If not done, penalty will be imposed. In case LIC wishes to get the onsite person changed if replacement from the identified pool is not provided within 45 days.	Without adequate information and site-survey, it will be difficult to order the requisite items. After such rigourous process and such stringnent compliance, it is preposterous on part of LIC to start the project with such distrust. Every bidder has a set target of progressing and executing the project. Kindly request you to remove this SLA penalties as the embed a great seed of distrust with the bidder.	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
482	SLA & Penalty	Project Phase level SLA:	84	Delay in implementation of devices which could not be integrated in the initial phase beyond three weeks. Delay in submission of implementation Plan, HLD and LLD beyond 6 weeks from the date of issue of purchase order	Every bidder has a set target of progressing and executing the project. Kindly request you to remove this SLA penalties as they embed a great seed of distrust with the bidder. Bidder has already submitted a gurantee to LIC for the execution of the project. As mentioned in the RFP, LIC is not taking any ownership of ensuring the responsibility for supporting the mentioned goals in the RFP. The bidder is exposing themselves to tremendous financial and project execution risk	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
483	SLA & Penalty	Project Phase level SLA:	84	In case of a malfunctioning of appliances, hardware, hardware components accessories, systems software, or any products, the relevant defect should be attended immediately and rectified within 4 hours of the receipt/notice of the complaint. In case any of the system is completely down the defect should be attended and rectified within 8 hours of receipt of notice.	Please apply this SLA only if the availability of the operations is impacted. The onsite team will be lost in management of SLA rather than ensuring the appropriate rectification of the project.	Please refer to "Revised Service Level Agreements (SLAs) & Penalties"
484	SLA & Penalty	Project Phase level SLA:	84	Delay in posting of on-site support Personnel as per Resource Deployment section beyond 6 weeks from the date of issue of purchase order for security products.	The Bidder's complete investment is at stake for execution of this project. Unnecessary conditions during the implementation may end up being a simple tool of red-tapism and dispute. Kindly remove this clause.	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
485	SLA & Penalty	Downtime of standby / HA components:	87	1% hourly increment after resolution period has lapsed within the overall cap	Till the time the SLAs and availability factor is maintained. LIC should not be unnessary penalizing the bidder on the standby components. This may end up being a simple tool of red-tapism and dispute. Please remove this clause	Please refer to the revised Service Level Agreements (SLAs) & Penalties
486	SLA & Penalty	SOC solution management- Version/ Release/Upgrades / Patches	87	If the patches/signature files are not deployed within a period of 7 working days of LIC from the release of latest version/update by OEM, it will attract a penalty of 0.5% of the charges from yearly on-site & remote monitoring services for each week of delay or part thereof.	The measurement of the SLA violates the N-1 approach of LIC. This may end up being a simple tool of red-tapism and dispute. Please remove this clause	Please refer to the revised Service Level Agreements (SLAs) & Penalties
487	SLA & Penalty	Audit of Next gen SOC solutions Unable to close Health Check-up observations within 2 weeks Security Bug/ vulnerability / enhancements etc. – Rectification of security and operational bug/ Vulnerability/ enhancements	87,89	Audit findings and the remediation actions after each audit should be completed within 3 months. A 5% penalty will be imposed for each week of delay in addressing critical and important findings. Unable to close Health Check-up observations within 2 weeks	Remedial actions will be limited to configuration changes and some technical upgradation of the solution (on best effort basis). No OEM Vendor provides a timeline, if there significant changes needed to meet a new complaince requirement or patch levels. Request you to please remove the penalty or limit the penalty to only configuration changes only.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
488	SLA & Penalty	Ongoing Operational Enhancement and Reporting Requirements	87	Achieve a 2% reduction in event response time on a quarterly basis. Achieve a 5% reduction in the reporting timeline for critical and high-priority events on a quarterly basis. A 2% penalty will be imposed for failure to reduce false positives and for not fine-tuning policies, rules, and correlation rules.	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
489	SLA & Penalty	UEBA Accuracy	89	Detect anomalies with 95% accuracy while maintaining a false positive rate of no more than 5%.	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
490	SLA & Penalty	PCAP data accuracy	89	Ensure data integrity with no more than 1% packet loss. Retain captured PCAP data for a minimum of 90 days and 365 days in cold storage	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis. A 30days of PCAP raw data will be 2.5+ peta byte. Kindly confirm whether it is raw data or event data which needs to be stored.	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
491	SLA & Penalty	Security Intelligence Services	90	Achieve an alert accuracy rate of at least 95% while maintaining a false positive rate of no more than 5%.	Request LIC to publish a framework on how this will be measured. Without adequate framework, measurement and applicability will be on adhoc basis.	Clause Deleted . Please refer to the revised "Section E: Scope of Services"

492	Section G: Payment Terms & Conditions	N/A	99	Delivery of software and appliances : 30 % of cost Installation and integration, initial OEM audit and acceptance testing as per scope of work.-40% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s-25% Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work.- 5%	Request you to revise this payment schedule Delivery of software and appliances : 70 % of cost Installation and integration, initial OEM audit and acceptance testing as per scope of work.-20% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s-5% Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work.- 5%	Please refer to the revised "Payment Terms & Conditions"
493	Section G: Payment Terms & Conditions	N/A	99	Payment for the Onsite Services will be done on quarterly basis at the end of each quarter. o Verification of 'Service level agreements' defined in this RFP o OEM Quarterly Audit Report	Verification of SLA is LIC's internal process, which should the bidder bear the brunt of submittion the verification. Also, no OEM Provides an Audit report, they provide feedback of assessment over an email. Kindly LIC should accept the same for release of payments	Please refer to the revised "Payment Terms & Conditions"
494	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point no. 1The proposed solution must be able to handle 60000 EPS sustained with scalability without any additional hardware/ licence sustained up to 80000 EPS from day one.	Since the required capacity is 80k as peak, please confirm if the propopsal	Please refer to the revised "Annexure F"
495	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 8The proposed solution should have the capability to effectively manage peak EPS (80000 EPS) and handle burst periods which could be 3 times more than the peak EPS without dropping logs.	This point is contradicting to point no. 3 above. As the earlier point was mentioning twice the sustained capacity (i.e. 1,60,000 EPS) but here it is mentioned as 3 times. Also the server based licensing protects you from any such EPS license capping. please allow server based licensing as well as suggested - please confirm the exact spike capacity to be considered.	Please refer to the revised "Annexure F"
496	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 20The solution should provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non standard logs withut any extra cost for LIC. These parsers should be part of the solution and implemented by the OEM.	Please clarify is this is related to ability of the proposed solution to provide custom connectors. Kindly let us know if this can be performed by the OEM Business Partners. If not then please help us with the approximate count of the custom connectors needed.	Please refer to the revised "Section E: Scope of Services"
497	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 33The proposed solution's search performance should be capable of searching through millions of unstructured (raw) logs within 5 minutes.	The Query response time largely depends on multiple factors like query syntax, HW resources, load on the system etc. Most of the OEM providing the 30 seconds commitment will limit the number of results/capping first 1000 logs. Please consider this point as optional or also add the point to ensure that query result shouldnt terminate or truncate any number of results queried by the analyst	Please refer to the revised "Annexure F"
498	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 35The proposed solution should have capability to collect, normalize and store configuration data from various devices and use it for analysis.	Most of the SIEM tools typically ingests the log, flows and raw packets data for anaylsis - using device configuration data falls out side of SIEM pureview and hence this point should be made optional	Please refer to the revised "Annexure F"
499	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 56The proposed solution must be designed to provide a query response within 30 seconds or less.	The Query response time largely depends on multiple factors like query syntax, HW resources, load on the system etc. Most of the OEM providing the 30 seconds commitment will limit the number of results/capping first 1000 logs. Please consider this point as optional or also add the point to ensure that query result shouldnt terminate or truncate any number of results queried by the analyst.	Please refer to the revised "Annexure F"
500	Annexure F: Technical Compliance	SOAR Technical Specification	113	Point. 12The solution must have out-of-the-box use cases ecosystem with 800+ integrations including but not limited to the following technologies: -Forensic tools (e.g. FTK, EnCase, Autopsy..) -IT (e.g. AD, SAML...) -Communication tools (e.g. email, Slack, HipChat...) -SIEM tools -Endpoint Security -Network Security -Active Directory -Threat Intelligence -Dynamic malware analysis	Tasks specific to forensic tool & dynamic malware analysis will need custom integration, remaining can be achieved - please confirm if this is acceptable.	Please refer to the revised "Annexure F"
501	Annexure F: Technical Compliance	UEBA Technical Specification	113	Point. 21The proposed solution should have the capacity to utilize both unsupervised and supervised machine learning algorithms, artificial intelligence and deep learning.	Our solution ensure the quality output by utilising the supervised learning without Deep learning and unsupervised learning -please confirm if this is acceptable	Please refer to the revised "Annexure F"
502	Annexure F: Technical Compliance	PCAP Technical Specification	113	Point. 1The solution should have the scalability to cover the entire enterprise network (North / South and East / West) with ability to perform high speed lossless packet capture & analysis functions for a network traffic capture as per following site requirements from day one. Internet Facing Sites: - Site A: 3.0 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Is it assumed that Site A, B, C & D are equivalent to North Site A, West Site B, East Site C & South Site D?	Please refer to the revised "Annexure F"
503	Annexure F: Technical Compliance	PCAP Technical Specification	113	Point. 1The solution should have the scalability to cover the entire enterprise network (North / South and East / West) with ability to perform high speed lossless packet capture & analysis functions for a network traffic capture as per following site requirements from day one. Internet Facing Sites: - Site A: 3.0 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Confirm the average utilisation of each BW capacity mentioned	Please refer to the revised "Annexure F"

504	6. Eligibility Criteria	4	14	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request lic to change to "The Bidder during the last 6 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order or multiple po's from same organization related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. "	Please refer to the revised "Minimum Eligiblity Criteria"
505	6. Eligibility Criteria	point 5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector	Since Lic has mentioned the SIEM OEM should be from Gartner leader/challengers quadrant request lic to change as below for larger participation "The bidder during the last 6 years preceding to the submission date of this RFP should have supplied, implemented and supported the SIEM OEM (of minimum 30,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. Further bidder must have experience of deploying SIEM solution with combined capacity of 60000 EPS or more(across multiple organization) in last 5 years as on date of submission of bids in PSU/ Government Organizations."	Please refer to the revised "Minimum Eligiblity Criteria"
506	6. Eligibility Criteria	7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	For larger participation request Lic to change "The bidder during the last 6 years preceding to the submission date of this RFP should have supplied, implemented and supported UEBA solution for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India" or " The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. "	Please refer to the revised "Minimum Eligiblity Criteria"
507	Section E: Scope of Services	Training & Certification	57	Pre-Implementation: Provide training to the LIC personnel/ Onsite support team on the product architecture, functionality and the design for each solution under the scope of this RFP	Request LIC to clarify the number of participants. Also confirm if the training is to be conducted onsite at LIC premises or it can be an online training	Please refer to the revised "Section E: Scope of Services"
508	Section E: Scope of Services	Training & Certification	57	Post Implementation: Provide hands-on training to the LIC personnel/ Onsite support team on day to day operations, alert monitoring, policy configuration, rule creation, report generation for all solutions etc.	Request LIC to clarify the number of participants Also confirm if the training is to be conducted onsite at LIC premises or it can be an online training	Please refer to the revised "Section E: Scope of Services"
509	Section E: Scope of Services	Training & Certification	57	Training cost shall be inclusive of Certification level training for three participants.	Our understanding is this is one time training and certification to be done for 3 participants. Training can be conducted online. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
510	Section E: Scope of Services	Transition from existing SOC to NGSOC:	60	Once all the log sources integrated with existing SOC are migrated to NGSOC, ensure the existing SOC is up & running in steady state with security patches by obtaining same from respective OEMs, settings etc. for two years. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, is required to extract old logs for forensic investigation, in case required	For the existing SOC to be manged the same should be under the active support with the existing OEM. Also depending on the complexity in retriving of logs existing OEM professional services will be needed. Request LIC to confirm the existing OEM suport and PS services availability.	Please refer to the revised "Section E: Scope of Services"
511	Section E: Scope of Services	2. Detailed Scope of Work - I. General Requirements	62	The bidder / System Integrator shall engage the services of respective OEMs for plan, design and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Kindly confirm if LIC needs OEM resources to do the end to end deployment along with bidder	Please refer to the revised "Section E: Scope of Services"
512	Section E: Scope of Services	2. Detailed Scope of Work - I. General Requirements	62	The bidder shall ensure that the configuration, implementation and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Kindly clarify whether LIC needs the OEM for onsite implementation or bidder can do the implementation	Please refer to the revised "Section E: Scope of Services"
513	Section E: Scope of Services	2. Detailed Scope of Work - I. General Requirements	62	The Bidder should provide backup solution for proposed setup. The backup taken should be SHA256 encrypted.	Since backup solution can be common request lic to clarify whether existing backup solution has to be used or bidder needs to provide the solution	Please refer to the revised "Section E: Scope of Services"
514	Section E: Scope of Services	III. Security Information and Event Management (SIEM)	66	The vendor should ensure to provide any number of custom connectors and parsers required for integration of proprietary or custom applications or non-standard logs and with all the solutions without any extra cost for LIC. These parsers should be implemented by the OEM.	Please share the details of the inventory (make, model, version, type). This will help us to understand the feasibility, efforts and out of the box integration availability	Please refer to the revised "Section E: Scope of Services"
515	Section E: Scope of Services	III. Security Information and Event Management (SIEM)	66	Migrate the existing logs to the new setup after reviewing the same in consultation with LIC.	Kindly clarify whether the existing logs from SIEM will be provided in raw log format. It is not possible to process and migrate normalized logs. Kindly clarify the expectation	Please refer to the revised "Section E: Scope of Services"
516	Section E: Scope of Services	6. Project Timelines	82	Phase 2 : Implementation of CTI and CTH T + 12 Weeks	Request you to consider the clause as below - Phase 2 : Implementation of CTI and CTH T + 16 Weeks	Please refer to the revised "Section E: Scope of Services"
517	Section E: Scope of Services	6. Project Timelines	82	Phase 3 : Implementation of PCAP and NBAD T + 8 Weeks	Considering delivery of appliance will take 8 weeks request you to consider the clause as below - Phase 3 : Implementation of PCAP and NBAD T + 16 Weeks	Please refer to the revised "Section E: Scope of Services"
518	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	90	Achieve an alert accuracy rate of at least 95% while maintaining a false positive rate of no more than 5%.	Since it ia new solution being implemented and it does not have any baseline, request you to exempt bidder from penalty or make it mutually acceptable metric after implementation and baseline for six months	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
519	Annexure D: Technical Scoring	Point 3	109	The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Request lIC to change to The Bidder during the last 6 years preceding to the submision date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order or multiple orders from same client) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised Annexure -D

520	Annexure D: Technical Scoring	Point 4	109	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. •3 references of 60,000 EPS and above -> 15 Marks •3 references of 50,000 EPS and above -> 12 Marks •3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	For larger participation request lic to change as below - The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. •Combined capacity of 100,000 EPS and above -> 15 Marks •Combined capacity of 70,000 EPS and above -> 12 Marks •Combined capacity of 50,000 EPS and above -> 8 Marks • [illegible] references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
521	Annexure D: Technical Scoring	Point 7	110	The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ Professional OEM Level Certification. • Every Additional 10 Resources -> 2 Marks subject to maximum of 10 marks • 100 Resources -> 5 Marks	Request you to reconsider the clause as below - The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ Professional OEM Level Certification. • Every Additional 5 Resources -> 2 Marks subject to maximum of 10 marks • 50 Resources -> 5 Marks	Please refer to the revised "Annexure - D"
522	Annexure F - PCAP Technical Specifications	Point 6		The solution should seamlessly integrate with tools such as (but not limited to) SIEM, IDS/IPS, network devices, TIP, NBAD, etc. and any other tools deployed at LIC.	Kindly confirm the usecase for integration with IDS/IPS, TIP, NBAD as PCAP ideally will be connected to the span port of the switch to collect traffic from identified segments. If there is no specific use case that can be identified, request you to delete the clause. Also integration depends on the existing capabilities of the tools in LIC. Request LIC to provide the list of all tools for which integration is needed	Please refer to the revised "Annexure F"
523	Annexure F - NBAD Technical Specifications	Point 13		The solution should integrate with existing cyber security solutions such as (but not limited to) SIEM, SOAR, EDR, NAC,UEBA etc. to alert the admin, provide mitigation actions like quarantine / block / apply custom policies both automatically on the endpoint to block further spread of the malware/worm across the network without affecting legitimate traffic on the network	Kindly confirm the usecase for integration with EDR and UEBA to understand the feasibility of integration as OEMs may not have have any specific use case for the same. If there is no specific use case that can be identified, request you to delete the clause	Please refer to the revised "Annexure F"
524	SOAR Compliance	Technical Specification	Point. 12	The solution must have out-of-the-box use cases ecosystem with 800+ integrations including but not limited to the following technologies: -Forensic tools (e.g. FTK, EnCase, Autopsy..) -IT (e.g. AD, SAML...) -Communication tools (e.g. email, Slack, HipChat…) -SIEM tools -Endpoint Security -Network Security -Active Directory -Threat Intelligence -Dynamic malware analysis	Tasks specific to forensic tool & dynamic malware analysis will need custom integration, remaining can be achieved - please confirm if this is acceptable.	Please refer to the revised "Annexure F"
525	SOAR Compliance	Technical Specification	Point. 99	The licensing model should distinguish between different user roles, such as administrators, analysts, and responders, offering appropriate pricing for each role based on their access and usage requirements.	The SOAR tool licenses are based on the named license and have a flat licensing across any type of user - please allow us to quote the same. Alternatively it is up to SI to convert The role based pricing at their level.	Please refer to the revised "Annexure F"
526				Request this new point to be added	For all the solutions being proposed & the critical features, we would recommend LIC do a demonstration of them so that they are validated. We request LIC to score the demosntrations & include them in the final score calculation.	Please refer to the revised "Annexure - D"
527	Annexure F: Technical Compliance	PCAP Technical Specifications/ 15	113	The solution should have efficient indexing and searching capabilities to quickly locate and retrieve specific packets based on various criteria. The solution should provide support for search functionality not just on Layer 3, Layer 4 but also on Layer 7 for HTTP, DNS, DB, LDAP and others such as time, links, IP address, port applications, protocols, unstructured hex or binary data, etc.	Pleqse note that Hex and Binary data is not a part of indexed metadata. Request you to please remove this from the clause	Please refer to the revised "Annexure F"
528	Annexure F: Technical Compliance	PCAP Technical Specifications/ 26	113	The solution should capture and record all network packets in full (both header and payload). In addition, Solution should be capable of selectively saving packet data based on specific application, protocol and time duration or in combination of them for any interested event or incident with in the dashboard/console system in a standard PCAP format. The saved PCAP file can be made accessible on a file share for other tools. Solution should support acquiring/capturing real-time packet with following options per Application Traffic: • Capture the entire packet. • Intelligent slicing of packet based on protocol. • Packet Truncation. • Exclude specific packets • Capture only headers	The functionality of the PCAP solution is to capture complete packet for Forensic investigation, Intelligent slicing or packet truncation will defeat the purpose of it. We would suggest to rephrase it to "The solution should capture and record all network packets in full (both header and payload). In addition, Solution should be capable of selectively saving packet data based on specific application, protocol and time duration or in combination of them for any interested event or incident with in the dashboard/console system in a standard PCAP format. The saved PCAP file can be made accessible on a file share for other tools. Solution should support acquiring/capturing real-time packet with following options per Application Traffic: • Capture the entire packet. • Exclude specific packets • Capture only headers"	Please refer to the revised "Annexure F"
529				Eligibility Criteria Query	We would like to change the clause which mentions to references of 75,000 On UEBA. As this is a recent technology technology and while every customer of LogRhythm has access to UVA functionality, The number of enterprises in India who have deployed Send has that number of users are not so many. so we would like the number to be reduced to 5000 or the number of references to be reduced from 2 to 1	Please refer to the revised "Minimum Eligiblity Criteria"
530				Additional Query	Lastly On the licensing model, since we notice Since we notice the payment terms are annual, even when we Have a perpetual licensing model option. We cannot propose the same since the perpetual model requires hundred percent upfront license payment. model, Thus, we left with proposing subscription license for this RFP.	Please refer to this corrigendum regarding this aspects

531	6. Eligibility Criteria	Eligibility Criteria,Point No.5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Kindly request to provide Exception or Relaxation for Technically qualifed Make In India Starups for the clause "The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP", as this will help more Make In India Startup OEMs to come forward and particpate in this opportunity.	Please refer to the revised "Minimum Eligiblity Criteria"
532	9. Pricing, Billing, Duties and Taxes	c)	24	c) Prices once fixed will be valid throughout the entire contract period. The Vendor should not, under any circumstances, request for an increase in the prices once prices are approved by LIC. No price variation relating to increases in Government levies/ taxes/ cess/ customs duty & excise duty including any newly introduced taxes shall be permitted.	Taxes, Duties (including Custom Duty), Levies etc are not within bidder's control. Hence the bidder requests LIC to allow for price revision to the extent of revision in any of these factors by Honourable Government.	Please refer to the "Revised Period of Validity of Bids"
533	Section G: Payment Terms & Conditions		99	The payment terms defined in RFP are as below: o Delivery – 30% o Installation & Integration – 40% o After Go-Live – 25% o Training – 5%	Kindly request LIC to revise the payment terms as below as per industry standards: o Delivery – 70% o Installation & Integration – 20% o After Go-Live – 5% o Training – 5%	Please refer to the revised "Payment Terms & Conditions"
534	Annexure C: Eligibility Criteria		3	The bidder should be in operating-profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP.	The bidder should be in operating-profit (EBITDA i.e. Earnings before Interest, Tax, Depreciation & Amortization) during any of the 02 (two) years out of the last 03(three) financial year(s) i.e., FY2022-2023, FY2021-2022 and FY2020-2021	Please refer to the revised "Minimum Eligiblity Criteria"
535	Annexure C	Point No 3	107	The bidder should be in operating-profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP.	Profitability is a better factor to consider Bidder's capability to manage the long term sustainability and financial health and manage the Critical SOC deployment hence we request LIC to modify clause as below : Bider should have made profit (before tax) in all the last three financial years preceding the date of this RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
536	Annexure C	Point no 4	107	The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We understand that the experience asked is during the last 5years preceding the date of the RFP	Please refer to the revised "Minimum Eligiblity Criteria"
537	Annexure C	Point No 5	107	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	SIEM is horizontal solution deployment in an enterprise's Cyber Security ecosystem. Since the Solution is decided basis the holistic stack we request LIC not to tie the bidder experience to under specific/proposed OEM. Bidder requests the clause to be modified as below : The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported SIEM Solution (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector with minimum 500 branches distributed across India. The proposed OEM product for SIEM should have been successfully running in minimum two organizations in PSU/Government/Private/BFSI Sector with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company.	Please refer to the revised "Minimum Eligiblity Criteria"
538	Annexure C	Point No 7	107	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	UEBA is a relatively nascent technology in terms of its deployment scale. It will be more appropriate if OEM implementation for the scale is evaluated . Alternately we request LIC to consider bidder experience for other technology solutions being deployed in the SOC. Hence request LIC to modify the clause to as below: The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the UEBA for 1000 users / NBAD with Minimum 10 Gbps throughput for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM should have been successfully running in minimum two organizations in PSU/Government/Private/BFSI Sector with minimum 500 branches distributed across India of minimum 50000 users	Please refer to the revised "Minimum Eligiblity Criteria"
539	Annexure C	Point no 10	108	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	In the current collaborative scheme of things where resources are spread across locations and support customers , there are data privacy guidelines that need to be maintained by HR. Taking these into account some of the personal data credentials Bidders do not publish the Certification Number and Copy of Certificates as supporting documentation .A declaration from the Head of HR confirming the number of certified resources and their skill area/years of certification is widely accepted document in Public Sector bids. Hence request LIC to remove the ask for Certification Number & Certification Copies under supporting documents.	Please refer to the revised "Minimum Eligiblity Criteria"

540	Annexure D	Point no 3	109	The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	There have been limited large scale implementations considering the nature and scale of work as outlined in the current RFP,additionally some of the technologies are fairly nascent . Hence request LIC to modify the clause as below : The Bidder during the last 5 years preceding to the date of this RFP, should have supplied, implemented and supported in-scope solutions (minimum 5 out of 9 in single Purchase Order) related to this RFP to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. • Every Additional reference -> 5 Marks subject to maximum of 20 marks • 1 reference -> 10 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
541	Annexure D	Point no 4	109	The Bidder during the last 5 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the proposed SIEM OEM (excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	There have been limited large scale implementations considering the nature and scale of work as outlined in the current RFP, Hence request LIC to modify the clause as below The Bidder during the last 7 years preceding to the date of this RFP, must have experience in PSU/Government/Private/BFSI Sector Firms in India for setting up the SIEM Solution(excluding MSSP / Shared SOC Center delivery model) and successful running the operations for minimum 3 years In India. • 3 references of 60,000 EPS and above -> 15 Marks • 3 references of 50,000 EPS and above -> 12 Marks • 3 references of 30,000 EPS and above -> 8 Marks • 3 references of 20,000 EPS and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
542	Annexure D	Point no 5	110	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India: • More than 2 references -> 10 marks • 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	There have been limited large scale implementations considering the nature and scale of work as outlined in the current RFP,additionally some of the technologies are fairly nascent . Hence request LIC to modify the clause as below :The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported UEBA/NDR/NBAD/PCAP solutions to clients in the PSU/Government/Private/BFSI Sector Firms in India: • Each additional reference -> 2.5 marks • 1 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/ Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure - D"
543	Scope of Services	Phase 2 Designing	55	Policy & Procedure Documents: o SOP for solution implementation. o SOP for operations of the solution.	Typically, SOP is prepared for operational activities, SOP for implementation can be rephrased as implementation documentation, LLD should cover solution implementation and design.	Please refer to the revised "Section E: Scope of Services"
544	Scope of Services	Transition from existing SOC to NGSOC	60	Running existing SOC in parallel with NGSOC until all existing log sources are integrated with NGSOC c. LIC has currently deployed SIEM, SOAR and UEBA. Vendor shall plan for the complete transition of the existing LId. Bidder must submit the project plan & transition timelines from current SOC to NGSOC as a part of the RFP responsC's SOC architecture, network, applications, processes etc.	Request LIC to share the exact make, model version details of existing SIEM, SOAR and UEBA to plan for transition and takeover activities. LIC to support with Handover and Knowledge transfer sessions from existing vendor upto the satisfaction of the bidder for seamless transition.	Please refer to the revised "Section E: Scope of Services"
545	Annexure F	Technical Compliance SIEM		The proposed solution must have the ability to retain logs and data. Raw logs and associated normalised events must be stored on online media for a duration of 6 months from the date of the event, and this data should be queryable and reportable. Offline availability of logs to be planned for 5 Years for all log sources. This could be stored in low cost storage for 2 years and rest can be saved in Tape library.	Request LIC to confirm if the Low cost storage and tape library will be provided by LIC or by bidder?	Please refer to the revised "Annexure F"
546	Annexure F	Technical Compliance SIEM		The proposed solution should natively cache logs locally on the collection layer for at least 3 days.	Request for clarification as This point contradicts with point 25 for caching duration, 2 or 3 days?	Please refer to the revised "Annexure F"
547	Section E	1	58	As part of deliverables, bidder must provide integrated dashboard along with Display Panel / TV set covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc.	Kindly confirm do bidder need to propose the Display panel / TV set for SOC? If yes, kindly share the specifications and quantities for the same.	Please refer to the revised "Annexure G - Commercial Bid (Indicative Pricing)"
548	Section E	1	60	a. Manage day to day operations of currently running SOC setup from two months from date of issuance of PO.	Kindly confirm how many months the bidder need to manage existing SOC? What will be the SLA for the existing SOC? Will LIC ensure the hand over training to be provided to bidder from the existing SOC services vendor?	Please refer to the revised "Section E: Scope of Services"
549	Section E	1	60	The vendor needs to provide all those services which are being provided by existing vendor as per SLA in force.	Kindly share the SLA details the current vendor is providing to factor required resources.	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
550	Section E	2	63	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth	Please confirm the license and hardware requirement for 20% YoY growth to be proposed in commercials. The commercial template doesn't have provision to put this values.	Please refer to the revised "Section E: Scope of Services". Clause Deleted
551	Section E	6	82	Delivery of all the equipment as quoted in the bill of materials for each solution/ service in-scope. Date of delivery of last item shall be taken as date of delivery for all items. => T+8 weeks	Since the hardware/appliance delivery schedule from OEM is minimum 8 to 14 weeks, We request LIC to extend the supply of equipments to T+14 weeks.	Please refer to the revised "Section E: Scope of Services"
552	Section E	6	82	Phase 3 : Implementation of PCAP and NBAD --> T + 8 Weeks	The delivery of items is mentioned as T+8 weeks in Line no 2 but in Line no 3, Phase 3 is mentioned as Implementation also happen in T+8 weeks. We assume it is a Typo error, Please confirm.	Please refer to the revised "Section E: Scope of Services"
553	Section E	6	84	Delivery of all hardware and software solution needed as *The delivery of the last hardware/ software solution will be deemed as the date of delivery of all equipment and penalty will be applicable accordingly. per the expected deliverables*within the defined timeline.	We request LIC to relax the clause and apply the penalty for undelivered portion instead of the total PO value.	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"

554	Section E	6	84	Delay in implementation of all devices beyond the expected deliverables** within the defined timeline. **The implementation of the last hardware/software solution will be deemed as the date of delivery of all equipment and penalty will be applicable accordingly.	We request LIC to relax the clause and apply the penalty for undelivered portion instead of the total PO value.	Please refer to the revised "Service Level Agreements (SLAs) & Penalties"
555	Section C:	2.xvi	20	The quantities mentioned in the Technical/ Commercial Bid are indicative only and will be used to determine a successful bidder. However, the actual quantities may differ at the time of issuing Purchase Order/s, depending on the circumstances prevailing at that time.	Bidder requests that the price submitted shall be valid only for the given quantity in RFP. Price for any variation in quantity shall be mutually agreed between the parties	Please refer to the revised "Pricing, Billing, Duties and Taxes" .
556	Section C:	4.Viii	23	The Bidder should have the capability to implement and maintain the project during the contract period of 5 years. The vendor should also be able to carry out any changes, if necessitated by LIC during the contract period of 5 years. The contract period may be further extended by a period of two years at the sole discretion of LIC of India on the same terms & conditions including the price component.	Since there is an impact on costs due to inflationary, forex and other factors bidders requests that Price for such change /extension shall be mutually agreed between the parties	The contract period may be further extended by a period of two years at the sole discretion of LIC of India on the same terms & conditions . However the prices will be decided mutually based on negotiations.
557	Section C:	9.c	24	Prices once fixed will be valid throughout the entire contract period. The Vendor should not, under any circumstances, request for an increase in the prices once prices are approved by LIC. No price variation relating to increases in Government levies/ taxes/ cess/ customs duty & excise duty including any newly introduced taxes shall be permitted.	Bidder requests clarifications inline with provision of clause 27f of the RFP, Price shall be adjusted for variation in GST or similar indirect taxes	Please refer to the revised "Pricing, Billing, Duties and Taxes" .
558	Section C:	25 a) and b)	35	a) The Central Office of LIC at Mumbai will place orders (either in full or in phases) with successful bidder for deliverables under this RFP at any time during the validity period of this tender. b) LIC reserves the right to place repeat orders for additional services/ reassessment on the same terms & conditions during the validity of the contract.	Bidder request for the following consideration 1. The price submitted by the bidder shall be valid only for the given quantity in RFP. Price shall be mutually agreed in the event of any variation in quantity 2. Price for additional orders placed beyond the initial implementation period shall be agreed mutually	Please refer to the revised "Pricing, Billing, Duties and Taxes" .
559	Section E:	7	83	Service Level Agreements (SLAs) & Penalties	Bidder Requests the Following Considerations- 1. Item no.7,8 and 9 in the Implementation SLA table is in the nature of SLAs, hence penalty should be calculated as a percentage of warranty/AMC prices and not on the total PO value. 2. Resignation by employee shall also be excused from the purview of penalty under the following clause "If the on-site Personnel leaves before expiry of 1 year for reasons other than death and hospitalization". 3. Bidder requests to remove the below as the clause is subjective and LIC already has protection of risk purchase clause "Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements to a maximum of 10% of the cost of that item(s)." 4. Quarterly SLAs shall be capped to 10% quarterly charges 5.The total penalty for onsite and offsite support per quarter shall not exceed 10% of the quarterly charges payable for onsite and offsite support for reasons other than absence. In case of absence of onsite support, actual amount shall be deducted up to 100% of the quarterly charges payable for the absent resource	Please refer to the revised Service Level Agreements (SLAs) & Penalties
560	Section G	3	99	Payments will be made as per below table, subject to bidder completing in-scope activities for the agreed project plan. LIC reserves the right to temporarily withhold payment and impose penalty, if it is not satisfied with progress made during that period or if there is delay in activity timelines	Payment milestones mentioned in RFP do not provide any support in terms of commercials for the delivered assets and the work done. We would requestpayments to be made Relevant to work executed. request to modify the payment term as below, which is in line with cost incurred at each stage. 1. Delivery of software and appliances - 80% of cost 2. Installation and integration, initial OEM audit and acceptance testing as per scope of work - 10% of cost 3. After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 5% of the cost 4. Training/knowledge transfer, documentation of entire solution - 5% of the cost 5. Payment for the Onsite Services - Monthly in arrears Additionally there is no separate line item as per commercial template for implementation services however there is a penalty attached to delay in implenmentation. Request LIC to include Implementation charges as a seprate line item since this will also ease out any calculation required under incremental capacity required during the contract period.	Please refer to the revised "Payment Terms & Conditions"
561	Section G	3	99	New	We understand that payments will be made within 30 days from submission of invoice for all undisputed invoices.	Please refer to the revised "Payment Terms & Conditions"
562	15	b	30	Violation of NDA may lead to legal action and blacklisting.	We reuest LIC to review blacklisting for breach of NDA. Kindly accept the below modification: "Violation of NDA may lead to legal action and blacklisting." We request for the same amendment to be made for clause 21(1) on page 32.	Clause 15b modified as "Violation of NDA will lead to forfeiture of performance Bank guarantee and additionally will lead to legal action and blacklisting."
563	24	g	34	The PBG may be invoked for entire amount if the vendor backs-out of his obligations as per this tender or if the fresh PBG is not received by LIC one month prior to the expiry of the earlier PBG; apart from other actions that may be decided by LIC.	We request that the clause be deleted and replaced as below: "Subject to a notice and cure period of not less than 30 days, the PBG may be invoked solely for material breaches of the Contract." PBG must be invoked only for material breaches and the bidder must be provided a cure period to rectify breaches before PBG is invoked.	The PBG may be invoked for entire amount if the vendor backs-out of his obligations as per this tender or if the fresh PBG is not received by LIC one month prior to the expiry of the earlier PBG; apart from other actions that may be decided by LIC . This condition is subject to providing the vendor a thirty days cure period in writing
564			97	Audit and access	we would request that this clause be deleted as audit rights are not a surviving clause.	"Audit and access" deleted

565	Annexure F: Technical Compliance	PCAP Technical Specifications/ 1	113	The solution should have the scalability to cover the entire enterprise network (North / South and East / West) with ability to perform high speed lossless packet capture & analysis functions for a network traffic capture as per following site requirements from day one. Internet Facing Sites: - Site A: 3.0 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site A - 4 Gbps - West: Site B - 4 Gbps - East: Site C - 4 Gbps - South: Site D - 4 Gbps - DR: Site E - 8Gbps - Site F - 4 Gbps - Site G - 1 Gbps - Site H - 1 Gbps	Request you to please provide the bifurcation based on DC & DR, it will help us in placement of devices. Also, please note that the throughput mentioned as requirement in the RFP is 30Gbps. However, if we add up the site wise throughput it turns out to be 37.5Gbps. Request you to please let us know the throughput for which we have to design the solution. We assume that the probe for NBAD & PCAP will be deployed in high Availability mode in each site and Centralized management at DC and DR, kindly confirm.	Please refer to the revised "Annexure F"
566	Annexure K	Performance Bank Guarantee		After finalization of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having Branches in Mumbai) equal to 10% of the Total Contract Value	As per revised GFR recommendation released in 2020, most public sector organizations have started accepting PBG equal to 3% of Total Contract Value. Request LIC's views and considerations for the same.	After finalization of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having Branches in Mumbai) equal to 5% of the Total Contract Value
567	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	4. The Bidder should have minimum of 5 years of experience in supplying, implementing and supporting minimum 5 out of the 9 in-scope solutions in a single purchase order related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India	We hereby declare that we comply the public procurement guidelines issued by the Ministry of Commerce & Industry, Department of Promotion & Internal Trade (Public Procurement Section) in which it is directed and regulated through sub clause of B of main clause no.10.: Specification in Tender and other procurement solicitations is as follow. “Procuring entities shall endeavour to see that eligibility conditions, including on matters like turnover, Expereience criteria, production capability, and financial strength do not result in the unreasonable exclusion of Class-I supplier/ Class-II Local Supplier who would otherwise be eligible, beyond what is essential for ensuring quality, technical compliance or creditworthiness of the supplier.” Hence, We request LIC to exempt the Experience criteria clause for Make in India and Class I local suppliers.	Please refer to the revised "Minimum Eligiblity Criteria"
568	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed SIEM OEM (of minimum 60,000 EPS) for a minimum of 01 (one) organisations in PSU/Government/Private/BFSI Sector. The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed across India of minimum 60,000 EPS in the last 5 years preceding to the date of the RFP. It should be a full-fledged captive SOC shall not have outsourced the SOC activities to any other company	We hereby declare that we comply the public procurement guidelines issued by the Ministry of Commerce & Industry, Department of Promotion & Internal Trade (Public Procurement Section) in which it is directed and regulated through sub clause of B of main clause no.10.: Specification in Tender and other procurement solicitations is as follow. “Procuring entities shall endeavour to see that eligibility conditions, including on matters like turnover, Expereience criteria, production capability, and financial strength do not result in the unreasonable exclusion of Class-I supplier/ Class-II Local Supplier who would otherwise be eligible, beyond what is essential for ensuring quality, technical compliance or creditworthiness of the supplier.” Hence, We request LIC to exempt the Experience criteria clause for Make in India and Class I local suppliers.	Please refer to the revised "Minimum Eligiblity Criteria"
569	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed UEBA OEM of minimum 75,000 users for minimum 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We hereby declare that we comply the public procurement guidelines issued by the Ministry of Commerce & Industry, Department of Promotion & Internal Trade (Public Procurement Section) in which it is directed and regulated through sub clause of B of main clause no.10.: Specification in Tender and other procurement solicitations is as follow. “Procuring entities shall endeavour to see that eligibility conditions, including on matters like turnover, Expereience criteria, production capability, and financial strength do not result in the unreasonable exclusion of Class-I supplier/ Class-II Local Supplier who would otherwise be eligible, beyond what is essential for ensuring quality, technical compliance or creditworthiness of the supplier.” Hence, We request LIC to exempt the Experience criteria clause for Make in India and Class I local suppliers.	Please refer to the revised "Minimum Eligiblity Criteria"
570	Section B:Invitation for Request for Proposal	6. Eligibility Criteria	15	The bidder must have a minimum of 100 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP/ OSCP/ OEM Level Certification. Minimum 25 resources must have OEM Level Certification (preferably of the proposed OEM).	We hereby declare that we comply the public procurement guidelines issued by the Ministry of Commerce & Industry, Department of Promotion & Internal Trade (Public Procurement Section) in which it is directed and regulated through sub clause of B of main clause no.10.: Specification in Tender and other procurement solicitations is as follow. “Procuring entities shall endeavour to see that eligibility conditions, including on matters like turnover, Expereience criteria, production capability, and financial strength do not result in the unreasonable exclusion of Class-I supplier/ Class-II Local Supplier who would otherwise be eligible, beyond what is essential for ensuring quality, technical compliance or creditworthiness of the supplier.” Hence, We request LIC to exempt the Experience criteria clause for Make in India and Class I local suppliers.	Please refer to the revised "Minimum Eligiblity Criteria"

571	Additional Point	PBG		a) After finalization of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having Branches in Mumbai) equal to 10% of the Total Contract Value.		a) After finalization of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having Branches in Mumbai) equal to 5% of the Total Contract Value.
572	Section D	1	48	1. Current Environment LIC is currently having the following structure and geographical spread: Corporate Office (also called as Central Office): Mumbai Zonal Offices: 8 (Bhopal, Kolkata, Chennai, Hyderabad, Kanpur, Delhi, Mumbai, Patna) Zonal training Centers: 8 (Bhopal, Kolkata, Chennai, Hyderabad, Agra, Delhi, Pune and Jamshedpur) Management Development Centre: 1 (Mumbai) Divisional Offices: 113 Pension & Group Superannuation Units: 74 BOs/ SOs/ MOs etc.: 4800 (approx.)	Do all these locations have data sources which will need to be integrated with the SIEM? Please help us with the data size location wise so that we can size the log collectors for each of these locations.	The details shall be shared with the succesful bidder
573	Brief Scope of Work	Functional NGSOC Architecture (Indicative)	56	Ticketing tool to be used for effective incident handling	Please let us know the ITSM tool to be used for this solution	The RFP for ticketing tool is under progress
574	Detailed Scope of Work	General Requirements	62	The Bidder should provide backup solution for proposed setup. The backup taken should be SHA-256 encrypted.	Does LIC also need a backup of all the logs?	No , For logs the retention period has been specified in the RFP
575	Section E: Scope of Services	Asset Inventory (Indicative)	55	Asset inventory	While LIC has shared the asset inventory. Request if the count of public facing assests can be shared as well. This would be required to license the EASM hence.	The information shall be shared with the succesful bidder
576	SOAR Compliance	Technical Specification	Point. 32	The solution should have out of the box playbooks available to cover cloud security use-cases such as but not limited to unauthorized resource access, suspicious API activity, cloud infrastructure misconfigurations, isolating endpoints, etc.	The mentioned playbooks are available as a part of our integrations available from our app exchange - please confirm if this is acceptable	Yes
577	SOAR Compliance	Technical Specification	Point. 51	The solution should normalize data coming from various sources such as network devices, applications, active directory, etc.	Data normalisation would typically be part of SIEM and the same can be taken care with the Bi-directional integration between SIEM & SOAR - hope this is acceptable	Yes , the understanding is correct
578	General query			General query	Please specify the existing ticketing tool used by LIC	The RFP for ticketing tool is under progress
579	General query			General query	Please specify the existing SIEM, SOAR, UEBA & EDR tool used by LIC	The information shall be shared with the succesful bidder
580	General query			General query	Current strenght of resources/perations team managing SIEM, SOAR, UEBA & EDR	The information shall be shared with the succesful bidder
581	General query			General query	Please specify volumetrics of existing SIEM, SOAR, UEBA & EDR which are to be managed by the bidder	The information shall be shared with the succesful bidder
582	Submission of Bids	Submission of Bids	19	Hard copy of the bids in sealed envelopes are to be submitted in the following manner within three working days of eligibility and technical bid opening:	Please confirm whether the hardcopy submission is mandatory as we shall be submitting in the Online. However, we shall submit the original Integrity Pact in stamp paper.	Yes
583	Password Protection	Password Protection	24	The copies of the item specifications (eligibility, technical and commercial) should be submitted in soft copy format by all participating Bidders. The specifications in the spreadsheets will be password protected. The bids are to be submitted in the format (soft copy) as per the Annexures in this RFP. The password used will be validated by LIC for checking the authenticity.	Does the online submitted documents to be protected by Password. Please clarify	Yes
584	1. Brief Scope of Work	Ticketing Tool	58	The bidder shall integrate all solutions with the ticketing tool of LIC for effective reporting and logging of information security incidents.	Please provide the ticketing tool details	The RFP for ticketing tool is under progress
585	1. Brief Scope of Work	Security Dashboards	58	The dashboard should be secure web based with multi factor authentication enabled online portal available over desktop, Mobile, Tablet and iPad. This should have the automated facility of sending e-mails and SMSs. Dashboard should be available through mobile app if feasible.	Kindly confirm email gateway and SMS gateway will be provided by LIC	Yes
586	1. Brief Scope of Work	Transition from existing SOC to NGSOC	60	Manage day to day operations of currently running SOC setup from two months from date of issuance of PO.	Kindly provide the details of existing SOC tools which need to be managed	The details shall be shared with the succesful bidder
587	1. Brief Scope of Work	Transition from existing SOC to NGSOC	60	Once all the log sources integrated with existing SOC are migrated to NGSOC, ensure the existing SOC is up & running in steady state with security patches by obtaining same from respective OEMs, settings etc. for two years. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, is required to extract old logs for forensic investigation, in case required.	We assume that all existing SOC tools are under warrenty for next two years. Kindly confirm	No
588	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	2. The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation and operational experience of in PSU/Government/Private/BFSI Sector in India from the date of issuance of RFP. • Greater than 9 Years -> 10 Marks • Greater than 7 Years up to 9 Years -> 7 Marks • Greater than 5 Years up to 7 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly clarify that Onsite Implementation of SIEM shall be considered as Similar SOC /Security Solutions experience?	Yes
589	29. Duration of the Engagement		35	The duration of the engagement would be 5 years from the issuance of the first Purchase Order (or deployment of resources).	Please confirm if the term of 5 years is inclusive of implementation	It should be from the day of sign- off
590	27. Period of Validity of Bids	27. Period of Validity of Bids	35	The contract is for a period of five years	Could you please specify whether the term of the contract will begin on the day that we manage the day-to-day operations of the SOC setup that is currently in place OR Contract will begin following the approval of the new NGSOC and the start of operations?	It should be from the day of sign- off
591	Compliance with IS Security Policy:		54	Responsibilities in carrying out background verification of personnel deployed from vendor side regularly and submit the report as and when needed by LIC	Background verification is done on resource on-boarding. If it needs to be done periodically for existing resources, please mention schedule of the same as there is associated cost in fulfulling this request. Or LIC should pay for the same at actuals.	This is to be done at the time of on-boarding of the onsite resource . If the onsite resouce is changed or a new onsite resouce is onboarded subsequently this has to be done again
592	Section E	1	55	Asset Inventory	We request if you can please provide the list and exptected EPS/GB per day location wise. It will be helpful if LIC indicates the minimum assets list be mandatory for operationalizing the NG-SOC and to achive sign-off criteria. This will help in achieving meaning full transistion and measurable objectives to move into sustainance phase. While LIC has shared the asset inventory. Request if the count of public facing assests can be shared as well. This would be required to license the EASM hence.	The details shall be shared with the succesful bidder

593	Section E: Scope of Services	Section E: Scope of Services	58	The bidder shall ensure that for all incident management, change management and problem management of IT infrastructure included in RFP is done through ticketing tool which shall be implemented by LIC.	Kindly provide additional information on the status of the tool. Whether procures, under-implementation or currently operatinal ?	The RFP for ticketing tool is under progress .
594	Transition from existing SOC to NGSOC:	Transition from existing SOC to NGSOC:	60	LIC has currently deployed SIEM, SOAR and UEBA. Vendor shall plan for the complete transition of the existing LIC's SOC architecture, network, applications, processes etc.	Please provide the information below for the current SOC. 1.SIEM : make / model, current EPS count, ~Use cases, Architecture 2. SOAR :make/model and no. of user/Analyst licenses, ~no. of playbooks created 3. UEBA : Make/model, no. of user licenses and use cases/models created on existing UEBA Also share the existing available integration with SIEM, SOAR and UEBA	The details shall be shared with the succesful bidder
595	5. Resource Deployment	SOC Manager	73	Certifications- CISSP/CISM/CISA/GCIH	The interpretation of "/" is or ? Kindly validate	Yes
596	Annexure F: Technical Compliance	SIEM Technical Specification	113	Point. 12If the primary analysis/ correlation engine is not functional all correlation activity should be possible from secondary sites as well.	Please confirm if the correlation engine failure can failover to the secondary available node as high availability failover. Also if both the correlation engine fails then we can perform the site level failover - Please confirm if this is acceptable	Yes
597	Section E: Scope of Services	1. Brief Scope of Work - Point 3 - Implementing	52	As per LIC's requirement, the successful bidder of the project shall be ready to shift, occasionally, the equipment from one place to other, uninstall and reinstall all the equipment without any additional cost to LIC.	Our understanding is this activity of shiftwill be done only once in the entire contract period. Kindly clarify	Yes
598	Section E: Scope of Services	Ticketing Tool	58	The bidder shall ensure that for all incident management, change management and problem management of IT infrastructure included in RFP is done through ticketing tool which shall be implemented by LIC.	Kindly confirm which ticketing tool is being used by LIC.	The RFP for ticketing tool is under progress
599	Section E: Scope of Services	2. Detailed Scope of Work - I. General Requirements	62	The bidder needs to make sure that the solution deployed in DR has real time replication of data of DC. DR should be used for reporting, threat hunting, searching, etc.	Kindly clarify if SIEM solution is needed in active/active in DC & DR or in active/passive	Active - Active
600	Section E: Scope of Services	III. Security Information and Event Management (SIEM)	67	Bidder has to provide an integrated case management workflow in the SIEM as well as integrate with the service desk solution for incident management workflow and create process as per best practices in consultation with LIC.	Kindly confirm which service desk solution is being used by LIC. This will help us in understanding the feasibility and efforts required for integration	The RFP for ticketing tool/service desk solution is under progress
601	Section E: Scope of Services	Penalties on Non-Performance of SLA during contract period:	87	Downtime of standby / HA components	Some solution like Pcap do not support HA. Hence for such solutions and any solution component that do not support HA, request LIC to excempt bidder from penalties	Applicable only for components supporting HA
602				Additional Query	What is the Ticketing tool currently used? if yes please specify and does it need to integrate?	The RFP for ticketing tool is under progress
603	Section G	12.g	102	In case of shifting of any appliance supplied by the vendor at any location of LIC, wherever the appliance has to be shifted from one LIC location to another, the vendor is required to uninstall / reinstall and maintain the system/s at the new location, without any extra cost to LIC of India on account of reinstallation. LIC will pay transportation charges, GST or any other government taxes.	We request LIC to confirm on number of instances of such shifting expected during the contract term.Additionally since there are costs associated with delivery/re-installation we request LIC to consider such requests via a change request process.	The bidder can factor one shifting during the contract period
604	6. Eligibility Criteria	Point No.08	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We kindly request you to modify the clause as follows: The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
605	6. Eligibility Criteria	Point No.08	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We kindly request you to modify the clause as follows: The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
606	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	As multiple clause over another is restricting the competitive participation. We request to consider below clause. 8. The Bidder during the last 2 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 5000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 5000 users in each organization during the last 2 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"

607	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	109	6. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 60000 endpoints -> 15 Marks • Greater than 40000 endpoints -> 10 Marks • Greater than 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request LIC to consider below clause for technical evaluation 6. The Bidder during the last 2 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 40000 to 60000 endpoints -> 15 Marks • Greater than 30000 to 40000 endpoints -> 10 Marks • Greater than 5000 to 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
608	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	As multiple clause over another is restricting the competitive participation. We request to consider below clause. 8. The Bidder during the last 2 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 5000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 5000 users in each organization during the last 2 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
609	Annexure-F	EDR Section	NA	The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem/Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
610	Annexure-F	EDR Section	NA	The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support additionally up to 4000+ Servers and should be an On-prem/ Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
611	Annexure-F	EDR Section	NA	The solution must use an “Authentication Token” for securely registering a new client installation to the Solution.	This is a vendor-specific point. Every EDR solution has a different mechanism to register the new EDR client installation. Hence, we request the LIC team modify the point as **"The solution must have a secure mechanism to communicate the new client installer with the management server."**	Please refer to the revised "Annexure F"
612	Annexure-F	EDR Section	NA	The solution must allow to manage the agent version and components from the management interface ability to run on hypervisor - VMware, Nutanix etc.	The management interface of most of the on-premise EDR solutions runs on the top of the Windows Server OS, which can be hosted on hypervisors like VMWare, Nutanix etc. We are requesting to change the clause to "The solution must allow to manage the agent version and components from the management interface hosted on the Windows Server & the underline platform can be hypervisor - VMware, Nutanix etc. "	Please be guided by the RFP
613	Annexure-F	EDR Section	NA	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	This is not EDR functionality. The Application Control feature of Endpoint Security can allow or block access to the applications based on the policies. However, we need more clarification for restricting network access for specified applications function.	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
614	Annexure-F	EDR Section	NA	The solution will Automatically learn and authorize logged in users	This is not EDR functionality. This functionality belongs to the IAM solution. We are requesting the LIC team to give more clarity on this functionality w.r.t EDR functionality	Please refer to the revised "Annexure F"
615	Annexure-F	EDR Section	NA	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	This is a vendor-specific point. We are requesting the LIC team to modify this point as **" The solution must have scrubbing/sandboxing capabilities. Incoming files will be extracted of all potential malicious content such as scripts, macros, and active content."**	Please refer to the revised "Annexure F"
616	Annexure-F	EDR Section	NA	Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data	To search data, including File, Process, Network, Registry, Injection, and user data, it is required to be recorded. Hence, we are requesting the LIC team to remove the word "Undetected Sensor" data from the clause	Please refer to the revised "Annexure F"
617	Annexure-F	EDR Section	NA	Solution must be GDPR , DPDPB compliant, HIPPA, PCI-DSS	DRDP law is yet to be effective, hence, requesting the LIC team to remove the DPDPB compliant point	Please refer to the revised "Annexure F"
618	Annexure-F	EDR Section	NA	The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report	We seek more clarification on this use w.r.t the EDR functionality.	As most of the EDR solution are being built on top of AI ML so the solution can enhance itself and be effective. We want the EDR to have that capabilities. This can include details about when the threat was first detected, what actions it has taken on the system, how it propagates, which other systems in the network it has affected, and other relevant information. This rich contextual information allows for better understanding and quicker incident response.
619	Suggestion	EDR Section	NA	EDR telemetrty to be used for doing attack surface risk management - user risk, device risk, App risk level with companywide risk score followed by mitigation	Requesting you to add this functionality	Please be guided by the RFP
620	Suggestion	EDR Section	NA	Forensics and IR to be part of the platform	Requesting you to add this functionality	Please be guided by the RFP
621	Suggestion	EDR Section	NA	Dark Web Monitoring for leaked credentials of LIC	Requesting you to add this functionalitiy	Please be guided by the RFP
622	Suggestion	EDR Section	NA	Generative AI to be included as part of Platform for accelerating the Detection and Response for LIC	Requesting you to add this functionality	Please be guided by the RFP
623	Suggestion	EDR Section	NA	Solution to have Vulnerability assessment and prioritization	Requesting you to add this functionality	Please be guided by the RFP

624	Eligibility Criteria		15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Request to change the OEM clause as " The proposed OEM product for EDR should have been successfully running in minimum 5 organizations for minimum 5000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
625	Endpoint Detection and Response (EDR)		70	Bidder to ensure the proposed EDR solution is capable of coexisting with the currently implemented Antivirus solution in LIC until its end of validity	Please clarify if LIC already has an existing EDR/EPS solution & wants EDR for some unprotected systems or want 2 EDR solutions to coexist together or already has EPS solution & wants to buy EDR solution.	Please refer to revised "Section E: Scope of Services"
626	Annexure F	EDR		11. The solution should be able to provide remote collection of troubleshooting logs	Request to change the Point as " The solution should be able to provide collection of logs from Systems for troubleshooting"	Please be guided by the RFP. The expectation here is that the Logs from any remote system should be available on the management server for troubleshooting
627		EDR		12. The solution should only enable Admins to remotely run the PowerShell script on the client	Request to change the point as "The solution should only enable Admins to remotely run Live OS Query"	Please refer to the revised "Annexure F"
628		EDR		13. Solution must be GDPR , DPDPB compliant	GDPR is not applicable in India, so request to change the Point as " Solution must be taking high regulations for DPDP compliance"	Please refer to the revised "Annexure F"
629		EDR		17. The solution must use an "Authentication Token" for securely registering a new client installation to the Solution.	Request to change the point as "The solution must use a secure mechanism for securely registering a new client installation to the solution."	Please refer to the revised "Annexure F"
630		EDR		22. This solution allows running under device guard features enabled: HVCI, Credentials Guard and Windows Defender App Control	Request to change this point as "The solution allows protection for Devices & provides App Control"	Please refer to the revised "Annexure F"
631		EDR		26. The solution allows upgrade to newer versions without performing a reboot	Request to change this point as "The solution allows database updates to newer updates without performing a reboot."	Please be guided by the RFP. The expectation here is that, the major and minor upgrades or updates need to happen without rebooting device or servers so it would not impact business.
632		EDR		34. The solution should have the ability to re-brand user notifications	Request to change this point as "The solution should have the ability to Email notifications"	Please refer to the revised "Annexure F"
633		EDR		58. The solution should protect against the "Pass the Hash" technique for credential theft.	Request to change this point as "The solution should protect against Malwares that can do credential theft"	Please refer to the revised "Annexure F"
634		EDR		69. Incoming files will be emulated by sandboxing for potentially malicious content.	Request to change this point as "Files can be emulated by sandboxing for checking potentially malicious content"	Please be guided by the RFP. The expectation here is that the incoming files shall be analysed by the sandbox for any malicious threat, before being delivered to the enduser system.
635		EDR		77. The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report	Request to change this point as "The solution will provide anti-malware & security detections by automatically using behavior & AI Technologies"	PLease be guided by the RFP. As most of the EDR solution are being built on top of AI ML so the solution can enhance itself and be effective. We want the EDR to have that capabilities. This can include details about when the threat was first detected, what actions it has taken on the system, how it propagates, which other systems in the network it has affected, and other relevant information. This rich contextual information allows for better understanding and quicker incident response.
636		EDR		95. The vendor is responsible for documenting log retention details, which is subject to approval by LIC. Log storage - 2 years as per LIC policy	Request to change this point as "The vendor is responsible for log retention details which is provided by EDR solution & subject to approval by LIC & the SIEM solution can store logs for longer duration."	Please refer to the revised "Annexure F"
637	Annexure-F	EDR Section		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem/Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
638	Annexure-F	EDR Section		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support additionally up to 4000+ Servers and should be an On-prem/ Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
639	Annexure-F	EDR Section		The solution must use an "Authentication Token" for securely registering a new client installation to the Solution.	This is a vendor-specific point. Every EDR solution has a different mechanism to register the new EDR client installation. Hence, we request the LIC team modify the point as **"The solution must have a secure mechanism to communicate the new client installer with the management server."**	Please refer to the revised "Annexure F"
640	Annexure-F	EDR Section		The solution must allow to manage the agent version and components from the management interface ability to run on hypervisor - VMware, Nutanix etc.	The management interface of most of the on-premise EDR solutions runs on the top of the Windows Server OS, which can be hosted on hypervisors like VMWare, Nutanix etc. We are requesting to change the clause to "The solution must allow to manage the agent version and components from the management interface hosted on the Windows Server & the underline platform can be hypervisor - VMware, Nutanix etc. "	Please be guided by the RFP
641	Annexure-F	EDR Section		The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	This is not EDR functionality. The Application Control feature of Endpoint Security can allow or block access to the applications based on the policies. However, we need more clarification for restricting network access for specified applications function.	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
642	Annexure-F	EDR Section		The solution will Automatically learn and authorize logged in users	This is not EDR functionality. This functionality belongs to the IAM solution. We are requesting the LIC team to give more clarity on this functionality w.r.t EDR functionality	Please refer to the revised "Annexure F"

643	Annexure-F	EDR Section		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	This is a vendor-specific point. We are requesting the LIC team to modify this point as **" The solution must have scrubbing/sandboxing capabilities. Incoming files will be extracted of all potential malicious content such as scripts, macros, and active content."**	Please refer to the revised "Annexure F"
644	Annexure-F	EDR Section		Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data	To search data, including File, Process, Network, Registry, Injection, and user data, it is required to be recorded. Hence, we are requesting the LIC team to remove the word "Undetected Sensor" data from the clause	Please refer to the revised "Annexure F"
645	Annexure-F	EDR Section		Solution must be GDPR , DPDPB compliant	DRDP law is yet to be effective,hence, requesting the LIC team to remove the DPDPB compliant point	Please refer to the revised "Annexure F"
646	Annexure-F	EDR Section		The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report	We seek more clarification on this use w.r.t the EDR functionality.	As most of the EDR solution are being built on top of AI ML so the solution can enhance itself and be effective. We want the EDR to have that capabilities. This can include details about when the threat was first detected, what actions it has taken on the system, how it propagates, which other systems in the network it has affected, and other relevant information. This rich contextual information allows for better understanding and quicker incident response.
647	Suggestion	EDR Section		EDR telemetrty to be used for doing attack surface risk management - user risk, device risk, App risk level with companywide risk score followed by mitigation	Requesting you to add this functionality	Please be guided by the RFP
648	Suggestion	EDR Section		Forensics and IR to be part of the platform	Requesting you to add this functionality	Please be guided by the RFP
649	Suggestion	EDR Section		Dark Web Monitoring for leaked credentials of LIC	Requesting you to add this functionality	Please be guided by the RFP
650	Suggestion	EDR Section		Generative AI to be included as part of Platform for accelerating the Detection and Response for LIC	Requesting you to add this functionality	Please be guided by the RFP
651	Suggestion	EDR Section		Solution to have Vulnerability assessment and prioritization	Requesting you to add this functionality	Please be guided by the RFP
652	Annexure C: Eligibility Criteria	N/A	107	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Request this be changed as below 8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported EDR solution to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users Or One Organization with minimum 1 Lakh users during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
653	Annexure F: Technical Compliance	EDR Technical Specifications	113	34. The solution should have the ability to re-brand user notifications	Please clarify the expectation of 're-brand'. Does it refer to changing the default text inside the user notification?	Please refer to the revised "Annexure F"
654	Annexure F: Technical Compliance	EDR Technical Specifications	113	35. The solution should have the ability to control the level of messages to show to users	Please clarify what are the different levels of messages to be shown to users. Kindly provide an example if possible	EDR should have capabilities to control user notification to show detection and prevention notification.
655	Annexure F: Technical Compliance	EDR Technical Specifications	113	59. The solution should be integrated with the existing monitoring Solution	Please provide information on the existing monitoring solution used.	Please be guided by the RFP
656	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We request LIC to **modify the clause as**: "The **Bidder or its OEM** during the **last 1 year preceding** to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at **least 1000 endpoints**. The proposed OEM product for EDR should have been successfully running in **minimum two organizations** for **average 1500 endpoints** during the **last 1 year preceding** to the date of the RFP"	Please refer to the revised "Minimum Eligiblity Criteria"
657	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We request LIC to modify the clause as: "The Bidder & its OEM should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 900 endpoints. The proposed OEM product for EDR should have been successfully running in organizations for average of 900 endpoints during the last 1 year preceding the date of the RFP"	Please refer to the revised "Minimum Eligiblity Criteria"
658	Eligibility Criteria	8	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India **or Globally** with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP	Please refer to the revised "Minimum Eligiblity Criteria"

659	Section B: Invitation for Request for Proposal	6. Eligibility Criteria	15	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We request LIC to modify the clause as: "The Bidder & its OEM during the last 1 year preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 500 endpoints. The proposed OEM product for EDR should have been successfully running in minimum one organizations for average of 500 endpoints during the last 1 year preceding the date of the RFP"	Please refer to the revised "Minimum Eligiblity Criteria"
660	Annexure F	Technical Compliance for EDR		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	The request if to modify this point to allow cloud solutions we well. The modified point is: "The solution must support up to 30,000 Windows OS endpoints/clients and 45,000 RHEL OS endpoints and should be an On-prem solution/Cloud based in India" Justification: Considering advancement in technology, attackers are able to create highly sophisticated attacks. They leverage technologies such as Cloud, AI & ML. In order to detect & prevent from such attacks, Security vendors needs to bring advancement in the product at a very fast pace. Also they need to leverage AI & ML as well. Such things are only possible if the security solution is delivered from the cloud as it is easy to leverage resources from the cloud. In an On-Prem deployment, the security solution will be binded by the compute available on prem only. It cannot scale or keep up the pace of advancement required to detect & prevent against modern day threats. LIC must prioritize security efficacy of the solution as the top most criteria, which is superior in case of cloud-based solutions compared to on-premise solutions. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please refer to the revised "Annexure F"
661	Annexure F	Technical Compliance for EDR		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We request to modify this point. The modified point is: "The solution must support additionally up to 4,000+ Servers and should be an On-prem solution/Cloud based in India" Justification: As per the MITRE testing's done over the last few years for EDR solutions, all the solutions offered by the OEMs were cloud based solutions & not on prem versions. The primary reason for doing the same was to make sure that the best platform with the required resources to detect & protect is evaluated in these advanced cyber-attack tests. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.	Please refer to the revised "Annexure F"
662	Annexure F	Technical Compliance for EDR		Solution must be GDPR , DPDPB compliant	We request to remove this point or make it optional, the revised point recommended is as: "Solution must be GDPR /DPDPB compliant" Justification: DPDPB is fairly a new compliance and just recently launched, it will ideally need some time to get the framework matured and acceptable across the industry. Also, OEM's need some time to ensure they have thoroughly worked on the principles of this compliance before they publish compliance for it.	Please refer to the revised "Annexure F"
663	Annexure F	Technical Compliance for EDR		The solution must use an “Authentication Token” for securely registering a new client installation to the Solution.	Request to modify this point as: "The solution must have a mechanism to securely register a new client installation to the LIC EDR Solution." Justification: This feature is available with a limited set of OEMs & hence would restrict participation. Solutions have capability to identify endpoints not belonging to LIC by putting in various filter conditions, LIC can use it to identify these endpoint & remove them from the console periodically. Also pls note that the endpoint package distribution is to be controlled as process, either providing it to the endpoint imaging team or hosting it on an internal software portal where users are identified first before allowing them to deploy. Also regular desktop/laptop users normally do not have user permissions to do package installations on their own.	Please refer to the revised "Annexure F"
664	Annexure F	Technical Compliance for EDR		The solution should have the ability to re-brand user notifications	**Request is to modify this point as: "The solution should have the ability to send user notifications when flagged for malicious activity". Justification:** Getting user notifications in real-time shall be topmost priority of LIC, rather than the format and outlook of notification. Also having a custom rebranding is a good to have & not a core functionality of an EDR solution.	Please refer to the revised "Annexure F"
665	Annexure F	Technical Compliance for EDR		The solution will identify and block out-going communication to malicious C&C sites	Request to modify this point & not limit only to C&C communication, the revised point recommended is: "The solution will identify and block out-going malicious communication as a result of file-based or file-less attacks". Justification: Any communications which are executed out of malicious file-based / fileless attacks shall be blocked and it should not just be limited to C&C sites. Blocking C&C sites (URLs) in particular is a URL filtering solution feature & not a core EDR functionality. This will limit more solutions from being proposed to LIC. URL filtering is a proxy solution functionality for which LIC has a proxy already deployed.	Please refer to the revised "Annexure F"
666	Annexure F	Technical Compliance for EDR		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	**Request is to modify the point as: "The solution must have capability to look at contents of the file such as scripts, macros and block it if found malicious". Justification:** This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Even after scrubbing there can be residual malware which might harm the endpoint & hence as a practice it is always recommended to block content which is malicious in nature.	Please refer to the revised "Annexure F"

667	Annexure F	Technical Compliance for EDR		When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Request is to modify the point as: "The original file must be accessible to end user if is found to be benign by the sandbox". Justification: This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Also scrubbing does not ensure 100% malware removal. If there is residual malware left, the file would still pose a security danger on the endpoint & within the LIC network. As a practice it is always recommended to fully block any malicious content.	Please refer to the revised "Annexure F"
668	Annexure F	Technical Compliance for EDR		The solution must block the user from browsing to a known malicious URLs or domains.	Request to remove this point as it is a proxy functionality. This is not a core functionality of an EDR solution & will severely limit participation as it would allow only a limited set of solution to qualify. LIC already has this functionality with their existing AV solution.	Please be guided by the RFP.
669	Annexure F	Technical Compliance for EDR		All files written on the filesystem will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious	Request to modify the point to include execution of files as a stage for analysis, the modified point is as: "All files written/executed on the filesystem will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious". Justification: Malware activities are initiated when files or process are executed. This is applicable for general file OR file less attacks. LIC must focus on malicious activity & ability of the solution to detect & prevent such malicious activities. Submitting all unknown files for sandboxing at the time of being writing is not ideal. Only the ones which are when executed should be ideally analyzed & if the local endpoint analysis is not able to give a conviction should be submitted for sandboxing.	Please refer to the revised "Annexure F"
670	Annexure F	Technical Compliance for EDR		The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information	**Request to change the point as: "The solution will list reputation analysis on files whether Benign or malicious and accordingly take action on it."**. **Justification:** URL and IP reputation along with geolocation is core functionality of a proxy solution & not EDR. If not changed, it will allow a limited set of solutions to be eligible to bid here.	Please be guided by the RFP. It should be inbuilt fuctionality of EDR. As per IOC management whether an IP or URL is blacklisted or not can be identified and appropriate action can be taken.
671	Annexure F	Technical Compliance for EDR		The solution should be able to log the C&C communication from the emulated BOT file	**Request the point to be modified as: "The solution should be able to log all the communications from the emulated BOT file". Justification:** Logging should not just be limited to C&C communications, all the communication logs from emulated BOT shall be available in the solution. Loggin only c&c will provide limited visibility. There can be destinations which are not yet classified as C&C and not logging them will create a visibility gap.	Please refer to the revised "Annexure F"
672	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution must be deployed in a similar size FSI environment in India (100,000 end points or higher) & must be operational for last 2 years & more. This should not be AV but EDR deployment" Justification: We recommend to add this point as it would Ensure that Vendor has expertise and capability of successfully executing and managing large organization such as LIC for optimal ROI of the investment of solution	Please be guided by the RFP
673	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "In order to secure LIC environment against sophisticated attacks, the proposed solution must have higher degree of security efficacy. It must be tested & secured top 3 position in last 2 MITRE ATT&CK evaluations results (Wizard Spider + Sandstrom & Turla) for the highest Technique based Analytics detection with not more than 5 configuration changes collectively." Justification: It is strongly recommended to add this point as LIC is a National Critical Infrastructure and security of its environment is paramount to both LIC and Nation. It is therefore very important for LIC to select the solution which has established and demonstrated its security effectiveness in Industry standard evaluation tests and the vendor which has produced best results in order to guard LIC from sophisticated cyber threats.	Please refer to the revised "Annexure F"
674	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "Proposed solution should have a mechanism to install dissolvable agent after analyzing anomalous traffic in network logs." Justification: While prevention and detection of threats on managed endpoints is important, it is also critical to know if there's malicious/suspicious traffic seen on an unmanaged endpoints in the environment. Detection of threats on the unmanaged assets can help LIC take swift actions to curtail the attack chain early in the stage. Dissolvable agent would help install agents on such endpoints. LIC has many third party vendors which work for then & this use case can also extend to 3rd party assists where LIC wants to collect endpoint telemetry for a short duration.	Please be guided by the RFP
675	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "Proposed solution should have identity analytics to detect user/identity based threats such as lateral movement, and it should have supervised and unsupervised learning capabilities." Justification: With almost every attack leveraging compromised user access to spread laterally in the environment and execute the attacks, it is very important for LIc to have real-time view of user activities where the solution can clearly call out the anomalies in user behavior comprising of suspicious actions associated with the user	Please be guided by the RFP

676	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution should provide automatic aggregation functionality so that related alerts are displayed in a unified Incident view for easier investigations with a casuality chain view." Justification: Major challenge for security team is to understand the larger picture of a multi-stage attack, given that pieces of same attack are seen as alerts on different tools and often this information is seen in isolation. It is very important for LIC security team to get a consolidated & unified visibility of entire attack chain automatically stitched together to quickly understand such multi-stage attacks and take coordianted response to it.This can drastically help LIC team to reduce MMTD and MMTR for cyber threats. This feature will enhance & provide a larger picture to the SOC of multi stage attacks with respect to endpoint. This will will ease of investigation & response capabilities. Also this is a core feature of EDR.	Please refer to the revised "Annexure F"
677	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution shall provide comprehensive protection against exploits including MacOS, Linux (RHEL, Ubuntu & Centos Flavours) and processes running in Linux Containers.** **Solution shall leverage extensive techniques for exploit prevention on RHEL servers icluding but not limited to Brute Force Protection, Java Deserialization, Kernel Integrity Monitoring, Local Privilege Escalation Protection, Reverse Shell Protection, ROP, Shellcode Protection, SO Hijacking Protection etc.. and shall not simply rely on IPS signatures and CVSS scores for protection" Justification:** LIC having larger stack of RHEL (Linux), it is very important that the vendor provides extensive technique based exploit prevention for RHEL servers to safeguard LIC holistically. It is very important for LIC to include this as they have a large adoption of the Linux OS.	Please refer to the revised "Annexure F"
678	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below: File hash Information collection, Termination of the service, Download of binary,Addition of hash value to block list, Delete the file, Send the hash to get the verdict (TI integration), Execute a python script, Execute a powershell script." Justification:** - Quick response of victim systems in a situation where some suspicious/malicious events are seen needs to be invetigated quickly with granular controls needed on the endpoints. - At such critical times actions such as Task manager view, File manager view, python script execution plays very important role in detailed investigation of the victim endpoint. - IT admin shall have remote parallell access to the endpoint under investigation in a way it shall not affect the enduser routine work & is non intrusive.	Please refer to the revised "Annexure F"
679	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file" Justification:** The solution shall deploy pro-active ransomware protection capability such as honeypot via decoy file creation. Such a pro-active approach will help LIC to prevent an ransomware attack before even the files are encrypted and moved to the attacker server.	Please refer to the revised "Annexure F"
680	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution should support collection of logs from third party security solutions like Active Directory, Firewall (Palo Alto, Fortigate, Cisco, Checkpoint), Proxy, DNS, DHCP, O365 etc from day 1 with licenses included as part of solution offered" **Justification:** - Major challenge for security team is to understand the larger picture of a multi-stage attack, given that pieces of same attack are seen as alerts on different tools and often this information is seen in isolation. - It is very important for LIC security team to get a consolidated & unified visibility of entire attack chain automatically stitched together to quickly understand such multi-stage attacks and take coordianted response to it. - This can drastically help LIC team to reduce MMTD and MMTR for cyber threats	Please be guided by the RFP
681	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The Solution should perform Network Traffic Analytics capability for:** **-Malicious Encrypted Traffic (Header Analysis)** **-North & South Malicious Traffic Monitoring Using AI (Data Exfiltration, C2C, DNS Tunneling etc.)** **-East & West Malicious Traffic Monitoring using AI (Lateral Movement)** **-Protocol Monitoring (DNS, NTLM, MSRPC, Kerberos, SSL/TLS, LDAP, IMAP etc.)** **-Identify Data Exfiltration Via Legitimate Protocols (DNS Tunneling, ICMP Tunneling).** **-Identify And Block Usage Of Common Attack Tools (Metasploit, Empire, Cobalt Etc.)" Justification:** Asides endpoint visbility, it is equally important to have insights of network traffic and anomalies in network to correlate it with enduser/endpoint activity and have better understanding of complete incident lifecycle	Please be guided by the RFP

682	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution should have single console for below features : - NGAV & EDR, Threat Hunting, Forensic, Network Traffic Analytics, Historical Queries, Identity Analytics, Cloud Workloads & Container Security" Justification:** An integrated and unified solution will help LIC security team get holistic visibility of their environment which can improve the secuirty effectuveness and efficacy of the solution. Consolidated visibility with cross-data analytics will yield better detections and reduce the MTTD and MTTR for LIC team. This also helps LIC team to ease the operations of the solution and management is simplified.	Please be guided by the RFP
683	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution should have asset management functionality to maintain a central repository of all assets for correlation and identification of rogue devices. " Justification:** Idenitifcation of rogues devices within LIC environment can help security team keep a track of legitimate organistaion devices and ensure that no devices are running without EDR agent which can pose a severe threat to LIC if that device is breached. This is very important fucntionality & we request LIC to include the same. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.	Please be guided by the RFP
684	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: ""The proposed solution is capable of Detection & Prevention Capabilities Against Identity Theft Attacks Such Below: SSO & AD Session Hijacking, Data Exfiltration, Compromised Credentials, Compromised Devices, Privileged User Monitoring, Unconstrained Delegation, Enumeration (User, SMB, NetBIOS, DNS etc.),The Printer Bug, Protection against Mimikatz to Extract the TGT, Pass the Ticket, Pass the Token, Pass the Hash, DCSync to Domain Compromise, Impossible traveler" Justification:** With almost every attack leveraging Identity theft and compromised identity to spread laterally in the environment and execute the attacks, it is very important for LIC to have real-time view of user activities where the solution can clearly call out the anomalies in user behaviour comprising of suspicious actions associated with the user. This will help to prevent Identity based attacks on LIC environment and provide contextual awareness to LIC team on early suspicions of malicious insiders to take mitigation actions before they turn rogue.	Please be guided by the RFP
685	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution should support demonstration Of Impersonation, Risky User Activities, Credential Misuse, Impossible Travel etc. and should have timeline view & 360 degree identity view with its user risk score. " Justification:** This will help to identify suspicious user activites and track it back with user risk scoring to take appropriate actions	Please be guided by the RFP
686					**Point to be added: "The proposed solution should store all the telemetry data collected from the LIC at MeitY compliant Data Centre in India and analytics should happen in India only." Justification:** LIC is a nation critical infrastructure and to ensure data privacy and compliance requirement, the vendor shall ensure all the data collected and processed is within India region and CSP where vendor is hosted is MeitY empanalled. There are pub sector FSI institutions who has requested for the same when selecting a cloud delivered EDR soltion. pls refer GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please be guided by the RFP
687	Annexure F: Technical Compliance	EDR Technical Specifications	113	Solution must be GDPR , DPDPB compliant	**Requets LIC to amend this clause as:** Solution must be Comply with regulations such as PCI-DSS and HIPAA.	Please refer to the revised "Annexure F"
688	Annexure F: Technical Compliance	EDR Technical Specifications	113	LIC has asked on-premise EDR solution as per the RFP, however there are many technical points which are indicating to NGAV/Endpoint Security features.	Request LIC to confirm, does vendor has to provide NGAV solutions along with on-premise EDR, need your inputs on this point for better understanding which will help vendor to design the technical architecture and solutions accordingly. In case LIC does not want NGAV solutions at this point, can you please make those NGAV points as not-mandatory , so that accordingly vendor can design the architecture and solution where new on-premise EDR can co-exist with existing AV solutions in LIC environment, please help us with your inputs on this point.	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
689	Annexure F: Technical Compliance	EDR Technical Specifications	113	Console access should support using 3rd party systems authentication (Two Factor Authentication)	**Request LIC to amend this clause as** "Console access should support using own native authentication or integrating with third party server AAA system like (AD,LDAP,etc)"	Please refer to the revised "Annexure F"
690	Annexure F: Technical Compliance	EDR Technical Specifications	113	Solution must use provide modern and easy remote deployment/installation/uninstallation methods (Including script support)	**Request to amend this clause as :** Solution must use provide modern and easy remote deployment/installation/uninstallation methods (Including script support) & 3rd party solutions like (sccm/IT management tool)	Please be guided by the RFP
691	Annexure F: Technical Compliance	EDR Technical Specifications	113	This solution allows running under device guard features enabled: HVCI, Credentials Guard and Windows Defender App Control	**Vendor specific Point: Request to amend this clause as** : This solution allows running under device guard features and Credentials Guard. App control feature can be achieve through NGAV / Endpoint Security solutions	Please be guided by the RFP
692	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution should have the ability to control the level of messages to show to users	**Request to amend this clause as :** The solution should have the ability to provide the level of messages to show to users or soc team.	Please be guided by the RFP

693	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution will enforce Firewall rules to allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols	**Request to remove this clause from RFP,** as this feature is part of host based firewall , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
694	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution will be used to restrict or allow IPV4/6 network traffic	**Request to remove this clause from RFP,** as this feature is part of host based firewall , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
695	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution's client Firewall should remain active during a client upgrade.	**Request to remove this clause from RFP,** as this feature is part of host based firewall , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
696	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	**Request to remove this clause from RFP,** as this feature is part of application white-listing/contol , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
697	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution will be able to Whitelist\Blacklist applications.	**Request to remove this clause from RFP,** as this feature is part of application white-listing/contol , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
698	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution will protect against existing and zero-day ransomware without requiring signature updates	**Request LIC to amend this clause as** "The solution will protect against existing and zero-day ransomware with or without requiring signature updates."	Please be guided by the RFP. LIC expects the EDR solution to act on protecting against existing and Zero-day ransomware even if the signatures are not updated by using behaviour analytics or other strategies. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
699	Annexure F: Technical Compliance	EDR Technical Specifications	113	The solution will remediate and restore files that were encrypted during a ransomware attack.	**Request to remove this point,** this feature can be achieve via Endpoint Security / NGAV solutions, EDR can only detect and provide response for any threat on endpoint environment.	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
700	Annexure F: Technical Compliance	EDR Technical Specifications	113	deploy antivirus and EDR agents, manage updates and patches, and monitor antivirus and EDR events to identify potential security incidents	**Request to amend this clause as :** The vendor is responsible for documenting log retention details with help of integrating with SIEM solutions provided / approved by LIC	Please be guided by the RFP
701	Annexure F: Technical Compliance	EDR Technical Specifications	113	The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as IRDAI, DPDP Act etc.)	Request to amend this clause as: The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as PCI-DSS & HIPAA, etc.)	Please refer to the revised "Annexure F"
702	Detailed Scope of Work	General Requirements	70	The vendor should monitor and manage software patching and updates on endpoints to mitigate vulnerabilities.	Request to clarify this point, hope LIC is not expecting the EDR solution will provide and manage Microsoft Windows OS and application pataches, this feature can achieve through patach management tool, request to remove this point from RFP	Please refer to revised "Section E: Scope of Services"
703	Endpoint Detection and Response	General Requirements		LIC has asked on-premise EDR solution as per the RFP, however there are many technical points which are indicating to NGAV/Endpoint Security features.	Request LIC to confirm, does vendor has to provide NGAV solutions along with on-premise EDR, need your inputs on this point for better understanding which will help vendor to design the technical architecture and solutions accordingly. In case LIC does not want NGAV solutions at this point, can you please make those NGAV points as not-mandatory , so that accordingly vendor can design the architecture and solution where new on-premise EDR can co-exist with existing AV solutions in LIC environment, please help us with your inputs on this point.	Please be guided by the RFP. Present AV solution will expire in Dec 2025. Along with EDR, the AV solution is to be proposed as solution is being procured for 5 years
704	Endpoint Detection and Response	Sizing Requirements	71	Endpoint Detection and Response : 30000 Windows OS desktops /laptops and 45000 RHEL OS desktops 4000 Servers	Request to LIC for confirming on the total EDR licenses for their requirement , does vendor has to consider total 79000 EDR licenses which is mix of windows & Linux platform.	Please refer to the revised "Annexure F"
705	Endpoint Detection and Response	General Requirements		Windows OS & Linux OS	Request LIC to provide details on existing OS platform like version details, this will help vendor to check the OS compitability with EDR agent	Please be guided by the RFP
706	Endpoint Detection and Response	General Requirements		The vendor should integrate the tool with vulnerability management systems to assess the endpoint's security posture.	Request LOC to amend this clause as : The vendor should share relevant threat information with vulnerability management systems which help to assess the endpoint's security posture.	Please be guided by the RFP

707	Eligibility Criteria	Eligibility Criteria		The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We request to remove the word "Proposed" and enable us to submit the references as per the eligibility. Request to amend the clause as below The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the any EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users Or One Organization with minimum 1 Lakh usersduring the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
708	Section E: Scope of Services	2. Detailed Scope of Work -> X. Endpoint Detection and Response (EDR)	70	The vendor should assess the existing endpoint security infrastructure and identify any gaps or vulnerabilities.	Kindly help us with the name/OEM of the existing EDR solution.	Please be guided by the RFP
709	Section E: Scope of Services	2. Detailed Scope of Work -> X. Endpoint Detection and Response (EDR)	70	The vendor should integrate the tool with vulnerability management systems to assess the endpoint's security posture.	Kindly help us with the name/OEM of the existing vulnerability management systems solution.	Please be guided by the RFP
710	1. Brief Scope of Work	On-Site Support Services for EDR	60	Deploy antivirus and EDR agents, manage updates and patches, and monitor antivirus and EDR events to identify potential security incidents	Kindly provide the details of central management software for end points/users.	Please be guided by the RFP
711	5. Resource Deployment	EDR	81	EDR Solution Architect	Kindly define the onsite resource requirement and resources per shift	Please be guided by the RFP
712	Annexure C: Eligibility Criteria	Eligibility Criteria	107	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints.	Since this is OEM dominated RFP, we request the bank to consider modification of the clause as: 8. The Bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints.	Please refer to the revised "Minimum Eligiblity Criteria"
713	Annexure C: Eligibility Criteria	Eligibility Criteria	107	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints.	We have gone through restructuring of the company business focusing digital business as seperate entity operating from February 2021. Since the new entity will have to depend on it parent company to comply with experiance and financial eligibility parameters of the RFP we request the bank to consider modification of the clause as: 8. The bidder or bidder's parent company (incase bidder is wholly owned subsidary of the parent company) during the last 7 years preceding to the date of this RFP should have supplied, implemented and supported the EDR to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India.	Please refer to the revised "Minimum Eligiblity Criteria"
714	Annexure D: Technical Scoring	Technical Evaluation Criteria – Parameters	110	6.The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 60000 endpoints -> 15 Marks • Greater than 40000 endpoints -> 10 Marks • Greater than 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to consider modification of the clause as under: 6.The Bidder /OEM during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 60000 endpoints -> 15 Marks • Greater than 40000 endpoints -> 10 Marks • Greater than 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
715	6. Eligibility Criteria	8	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Request you to consider the revised clause as below - **The Bidder during the last 5 years preceding to the submission date of this RFP should have supplied, implemented and supported EDR solution to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 15000 endpoints.** The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
716	Section E: Scope of Services	6. Project Timelines	83	Implementation of EDR and roll out of agents in the endpoints. Date of implementation of last device shall be taken as date of installation of all devices - T + 24 Weeks	Kindly confirm if LIC is using any patch management tool which can help in rolling out the agents to all endpoints and servers.	Please be guided by the RFP
717	Section E: Scope of Services	6. Project Timelines	83	Implementation of EDR and roll out of agents in the endpoints. Date of implementation of last device shall be taken as date of installation of all devices - T + 24 Weeks	If there is no patch management tool, kindly confirm if LIC will provide onsite support at zonal offices, RO, BO and other locations for deployment of agents on endpoints and servers	Please be guided by the RFP
718	Annexure D: Technical Scoring	Point 6	110	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: •Greater than 60000 endpoints -> 15 Marks •Greater than 40000 endpoints -> 10 Marks •Greater than 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	For larger participation request lic to change as below - **The Bidder during the last 5 years preceding to the submision date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of:** **•Greater than 30000 endpoints -> 15 Marks** **•Greater than 15000 endpoints -> 10 Marks** **•Greater than 5000 endpoints -> 5 Marks** (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
719				The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	Request LIC to relax this clause and allow cloud vendors as long the solution is based on the ministry of electronics and information technology (Meity) empanelled CSP	Please refer to the revised "Annexure F"
720	Annexure F - EDR Technical Specifications	Point 15		Console access should support using 3rd party systems authentication (Two Factor Authentication)	Kindly confirm the MFA solution used by LIC to understand the feasibility and effort for integration	Please refer to the revised "Annexure F"
721	Annexure F - EDR Technical Specifications	Point 68		When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Kindly confirm if bidder needs to propose on-premise sandbox or cloud based sandbox is fine	Please refer to the revised "Annexure F"

722	Annexure F	Technical Compliance for EDR		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	**The request if to modify this point to allow cloud solutions we well. The modified point is: "The solution must support up to 30,000 Windows OS endpoints/clients and 45,000 RHEL OS endpoints and should be an On-prem solution/Cloud based in India" Justification:** Considering advancement in technology, attackers are able to create highly sophoticated attacks. They leverage technologies such as Cloud, AI & ML. In order to detect & prevent from such attacks, Security vendors needs to bring advancement in the product at a very fast pace. Also they need to leverage AI & ML as well. Such things are only possible if the security solution is delivered from the cloud as it is easy to leverage resources from the cloud. In an On-Prem deployment, the security solution will be binded by the compute available on prem only. It cannot scale or keep up tha pace of advancement required to detect & prevent against modern day threats. LIC must prioritize security efficacy of the solution as the top most criteria, which is superior in case of cloud-based solutions compared to on-premise solutions. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please refer to the revised "Annexure F"
723	Annexure F	Technical Compliance for EDR		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	**We request to modify this point. The modified point is: "The solution must support additionally up to 4,000+ Servers and should be an On-prem solution/Cloud based in India" Justifiction**: As per the MITRE testings done over the last few years for EDR solutions, all the solutions offered by the OEMs were cloud based solutions & not on prem versions. The primary reason for doing the same was to make sure that the best platform with the required resources to detect & protect is evaluated in these advanced cyber attack tests. There are equally sized public sector banks who have opted for cloud based EDR solution, **refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.**	Please refer to the revised "Annexure F"
724	Annexure F	Technical Compliance for EDR		Solution must be GDPR , DPDPB compliant	**We request to remove this point or make it optional, the revised point recommende is as: "Solution must be GDPR /DPDPB compliant" Justification:** DPDPB is fairly a new compliance and just recently launched, it will ideally need some time to get the framework matured and acceptable across the industry. Also, OEM's need sometime to ensure they have thorughly worked on the principles of this compliance before they publish compliance for it	Please refer to the revised "Annexure F"
725	Annexure F	Technical Compliance for EDR		The solution must use an "Authentication Token" for securely registering a new client installation to the Solution.	**Request to modify this point as: "The solution must have a mechanism to securely register a new client installation to the LIC EDR Solution." Justification:** This feature is available with a limited set of OEMs & hence would restrict participation. Solutions have capability to identify endpoints not beloging to LIC by putting in various filter conditions, LIC can use it to identify these endpoint & remove them from the console periodically. Also pls note that the endpoint package distribution is to be controlled as process, either providing it to the endpoint imaging team or hosting it on an internal software portal where users are identified first before allowing them to deploy. Also regular desktop/laptop users normally do not have user permissions to do package installations on their own.	Please refer to the revised "Annexure F"
726	Annexure F	Technical Compliance for EDR		The solution should have the ability to re-brand user notifications	**Request is to modify this point as: "The solution should have the ability to send user notifications when flagged for malicious activity". Justification:** Getting user notifications in real-time shall be topmost priority of LIC, rather than the format and outlook of notification. Also having a custom rebranding is a good to have & not a core functionality of an EDR solution.	Please refer to the revised "Annexure F"
727	Annexure F	Technical Compliance for EDR		The solution will identify and block out-going communication to malicious C&C sites	**Request to modify this point & not limit only to C&C communication, the revised point recommended is: "The solution will identify and block out-going malicious communication as a result of file-based or file-less attacks". Justification:** Any communications which are executed out of malicious file-based / fileless attacks shall be blocked and it should not just be limited to C&C sites. Blocking C&C sites (URLs) in particular is a URL filtering solution feautre & not a core EDR functionality. This will limit more solutions from being propsosed to LIC. URL filtering is a proxy solution functionality for which LIC has a proxy already deployed.	Please refer to the revised "Annexure F"
728	Annexure F	Technical Compliance for EDR		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	**Request is to modify the point as: "The solution must have capability to look at contents of the file such as scripts, macros and block it if found malicious". Justification:** This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Even after scrubbing there can be residual malware which might harm the endpoint & hence as a practice it is always recommended to block content which is malicious in nature.	Please refer to the revised "Annexure F"
729	Annexure F	Technical Compliance for EDR		When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	**Request is to modify the point as: "The original file must be accessible to end user if is found to be benign by the sandbox". Justification:** This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Also scrubbing does not ensure 100% malware reomoval. If there is residual malware left, the file would still pose a security danger on the endpoint & within the LIC network. As a practice it is always recommended to fully block any malicious content.	Please refer to the revised "Annexure F"
730	Annexure F	Technical Compliance for EDR		The solution must block the user from browsing to a known malicious URLs or domains.	Request to remove this point as it is a proxy functionality. This is not a core functionality of an EDR solution & will severly limit participation as it would allow only a limited set of solution to qualify. LIC already has this functionality with their existing AV solution.	Please be guided by the RFP.
731	Annexure F	Technical Compliance for EDR		All files written on the filesystem will monitored and statically analysed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious	**Request to modify the point to include execution of files as a stage for analysis, the modified point is as: "All files written/executed on the filesystem will monitored and statically analysed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious". Justification:** Malware activities are initiated when files or process are executed. This is aplicable for general file OR file less attacks. LIC must focus on malicious activity & ability of the solution to detect & prevent such malicious activities. Submitting all unknown files for sandboxing at the time of being writing is not ideal. Only the ones which are when executed should be ideally analysed & if the local endpoint analysis is not able to give a conviction should be submitted for sandboxing.	Please refer to the revised "Annexure F"
732	Annexure F	Technical Compliance for EDR		The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information	**Request to change the point as: "The solution will list reputation analysis on files whether Benign or malicious and accordingly take action on it.". Justification:** URL and IP reputation along with geolocation is core functionality of a proxy solution & not EDR. If not changed, it will allow a limited set of solutions to be eligible to bid here.	Please be guided by the RFP. It should be inbuilt fuctionality of EDR. As per IOC management whether an IP or URL is blacklisted or not can be identified and appropriate action can be taken.

733	Annexure F	Technical Compliance for EDR		The solution should be able to log the C&C communication from the emulated BOT file	**Request the point to be modified as: "The solution should be able to log all the communications from the emulated BOT file". Justification:** Logging should not just be limited to C&C communications, all the communication logs from emulated BOT shall be available in the solution. Loggin only c&c will provide limited visibility. There can be destinations which are not yet classified as C&C and not logging them will create a visibility gap.	Please refer to the revised "Annexure F"
734	Annexure F	Technical Compliance for EDR		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	**The request if to modify this point to allow cloud solutions we well. The modified point is: "The solution must support up to 30,000 Windows OS endpoints/clients and 45,000 RHEL OS endpoints and should be an On-prem solution/Cloud based in India" Justification:** Considering advancement in technology, attackers are able to create highly sophoticated attacks. They leverage technologies such as Cloud, AI & ML. In order to detect & prevent from such attacks, Security vendors needs to bring advancement in the product at a very fast pace. Also they need to leverage AI & ML as well. Such things are only possible if the security solution is delivered from the cloud as it is easy to leverage resources from the cloud. In an On-Prem deployment, the security solution will be binded by the compute available on prem only. It cannot scale or keep up tha pace of advancement required to detect & prevent against modern day threats. LIC must prioritize security efficacy of the solution as the top most criteria, which is superior in case of cloud-based solutions compared to on-premise solutions. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please refer to the revised "Annexure F"
735	Annexure F	Technical Compliance for EDR		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	**We request to modify this point. The modified point is: "The solution must support additionally up to 4,000+ Servers and should be an On-prem solution/Cloud based in India" Justifiction**: As per the MITRE testings done over the last few years for EDR solutions, all the solutions offered by the OEMs were cloud based solutions & not on prem versions. The primary reason for doing the same was to make sure that the best platform with the required resources to detect & protect is evaluated in these advanced cyber attack tests. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.	Please refer to the revised "Annexure F"
736	Annexure F	Technical Compliance for EDR		Solution must be GDPR , DPDPB compliant	**We request to remove this point or make it optional, the revised point recommende is as: "Solution must be GDPR /DPDPB compliant" Justification:** DPDPB is fairly a new compliance and just recently launched, it will ideally need some time to get the framework matured and acceptable across the industry. Also, OEM's need sometime to ensure they have thorughly worked on the principles of this compliance before they publish compliance for it	Please refer to the revised "Annexure F"
737	Annexure F	Technical Compliance for EDR		The solution must use an “Authentication Token” for securely registering a new client installation to the Solution.	Request to modify this point as: "The solution must have a mechanism to securely register a new client installation to the LIC EDR Solution." Justification: This feature is available with a limited set of OEMs & hence would restrict participation. Solutions have capability to identify endpoints not belonging to LIC by putting in various filter conditions, LIC can use it to identify these endpoint & remove them from the console periodically. Also pls note that the endpoint package distribution is to be controlled as process, either providing it to the endpoint imaging team or hosting it on an internal software portal where users are identified first before allowing them to deploy. Also regular desktop/laptop users normally do not have user permissions to do package installations on their own.	Please refer to the revised "Annexure F"
738	Annexure F	Technical Compliance for EDR		The solution should have the ability to re-brand user notifications	**Request is to modify this point as: "The solution should have the ability to send user notifications when flagged for malicious activity". Justification:** Getting user notifications in real-time shall be topmost priority of LIC, rather than the format and outlook of notification. Also having a custom rebranding is a good to have & not a core functionality of an EDR solution.	Please refer to the revised "Annexure F"
739	Annexure F	Technical Compliance for EDR		The solution will identify and block out-going communication to malicious C&C sites	Request to modify this point & not limit only to C&C communication, the revised point recommended is: "The solution will identify and block out-going malicious communication as a result of file-based or file-less attacks". Justification: Any communications which are executed out of malicious file-based / fileless attacks shall be blocked and it should not just be limited to C&C sites. Blocking C&C sites (URLs) in particular is a URL filtering solution feature & not a core EDR functionality. This will limit more solutions from being proposed to LIC. URL filtering is a proxy solution functionality for which LIC has a proxy already deployed.	Please refer to the revised "Annexure F"
740	Annexure F	Technical Compliance for EDR		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	**Request is to modify the point as: "The solution must have capability to look at contents of the file such as scripts, macros and block it if found malicious". Justification:** This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Even after scrubbing there can be residual malware which might harm the endpoint & hence as a practice it is always recommended to block content which is malicious in nature.	Please refer to the revised "Annexure F"
741	Annexure F	Technical Compliance for EDR		When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Request is to modify the point as: "The original file must be accessible to end user if is found to be benign by the sandbox". Justification: This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Also scrubbing does not ensure 100% malware removal. If there is residual malware left, the file would still pose a security danger on the endpoint & within the LIC network. As a practice it is always recommended to fully block any malicious content.	Please refer to the revised "Annexure F"
742	Annexure F	Technical Compliance for EDR		The solution must block the user from browsing to a known malicious URLs or domains.	Request to remove this point as it is a proxy functionality. This is not a core functionality of an EDR solution & will severely limit participation as it would allow only a limited set of solution to qualify. LIC already has this functionality with their existing AV solution.	Please be guided by the RFP.

743	Annexure F	Technical Compliance for EDR		All files written on the filesystem will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious	Request to modify the point to include execution of files as a stage for analysis, the modified point is as: "All files written/executed on the filesystem will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious". Justification: Malware activities are initiated when files or process are executed. This is applicable for general file OR file less attacks. LIC must focus on malicious activity & ability of the solution to detect & prevent such malicious activities. Submitting all unknown files for sandboxing at the time of being writing is not ideal. Only the ones which are when executed should be ideally analyzed & if the local endpoint analysis is not able to give a conviction should be submitted for sandboxing.	Please refer to the revised "Annexure F"
744	Annexure F	Technical Compliance for EDR		The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information	**Request to change the point as: "The solution will list reputation analysis on files whether Benign or malicious and accordingly take action on it."**. **Justification:** URL and IP reputation along with geolocation is core functionality of a proxy solution & not EDR. If not changed, it will allow a limited set of solutions to be eligible to bid here.	Please be guided by the RFP. It should be inbuilt fuctionality of EDR. As per IOC management whether an IP or URL is blacklisted or not can be identified and appropriate action can be taken.
745	Annexure F	Technical Compliance for EDR		The solution should be able to log the C&C communication from the emulated BOT file	**Request the point to be modified as: "The solution should be able to log all the communications from the emulated BOT file". Justification:** Logging should not just be limited to C&C communications, all the communication logs from emulated BOT shall be available in the solution. Loggin only c&c will provide limited visibility. There can be destinations which are not yet classified as C&C and not logging them will create a visibility gap.	Please refer to the revised "Annexure F"
746	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution must be deployed in a similar size FSI environment in India (100,000 end points or higher) & must be operational for last 2 years & more. This should not be AV but EDR deployment" Justification: We recommend to add this point as it would Ensure that Vendor has expertise and capability of successfully executing and managing large organization such as LIC for optimal ROI of the investment of solution	Please be guided by the RFP
747	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "In order to secure LIC environment against sophisticated attacks, the proposed solution must have higher degree of security efficacy. It must be tested & secured top 3 position in last 2 MITRE ATT&CK evaluations results (Wizard Spider + Sandstrom & Turla) for the highest Technique based Analytics detection with not more than 5 configuration changes collectively." Justification: It is strongly recommended to add this point as LIC is a National Critical Infrastructure and security of its environment is paramount to both LIC and Nation. It is therefore very important for LIC to select the solution which has established and demonstrated its security effectiveness in Industry standard evaluation tests and the vendor which has produced best results in order to guard LIC from sophisticated cyber threats.	Please refer to the revised "Annexure F"
748	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "Proposed solution should have a mechanism to install dissolvable agent after analyzing anomalous traffic in network logs." Justification: While prevention and detection of threats on managed endpoints is important, it is also critical to know if there's malicious/suspicious traffic seen on an unmanaged endpoints in the environment. Detection of threats on the unmanaged assets can help LIC take swift actions to curtail the attack chain early in the stage. Dissolvable agent would help install agents on such endpoints. LIC has many third party vendors which work for then & this use case can also extend to 3rd party assets where LIC wants to collect endpoint telemetry for a short duration.	Please be guided by the RFP
749	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "Proposed solution should have identity analytics to detect user/identity based threats such as lateral movement, and it should have supervised and unsupervised learning capabilities." Justification: With almost every attack leveraging compromised user access to spread laterally in the environment and execute the attacks, it is very important for LIc to have real-time view of user activities where the solution can clearly call out the anomalies in user behavior comprising of suspicious actions associated with the user	Please be guided by the RFP
750	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution should provide automatic aggregation functionality so that related alerts are displayed in a unified Incident view for easier investigations with a causality chain view." Justification: Major challenge for security team is to understand the larger picture of a multi-stage attack, given that pieces of same attack are seen as alerts on different tools and often this information is seen in isolation. It is very important for LIC security team to get a consolidated & unified visibility of entire attack chain automatically stitched together to quickly understand such multi-stage attacks and take coordinated response to it.This can drastically help LIC team to reduce MMTD and MMTR for cyber threats. This feature will enhance & provide a larger picture to the SOC of multi stage attacks with respect to endpoint. This will will ease of investigation & response capabilities. Also this is a core feature of EDR.	Please refer to the revised "Annexure F"

751	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution shall provide comprehensive protection against exploits including MacOS, Linux (RHEL, Ubuntu & Centos Flavors) and processes running in Linux Containers. Solution shall leverage extensive techniques for exploit prevention on RHEL servers including but not limited to Brute Force Protection, Java Deserialization, Kernel Integrity Monitoring, Local Privilege Escalation Protection, Reverse Shell Protection, ROP, Shellcode Protection, SO Hijacking Protection etc.. and shall not simply rely on IPS signatures and CVSS scores for protection" Justification: LIC having larger stack of RHEL (Linux), it is very important that the vendor provides extensive technique based exploit prevention for RHEL servers to safeguard LIC holistically. It is very important for LIC to include this as they have a large adoption of the Linux OS.	Please refer to the revised "Annexure F"
752	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below: File hash Information collection, Termination of the service, Download of binary,Addition of hash value to block list, Delete the file, Send the hash to get the verdict (TI integration), Execute a python script, Execute a powershell script." Justification:** - Quick response of victim systems in a situation where some suspicious/malicious events are seen needs to be invetigated quickly with granular controls needed on the endpoints. - At such critical times actions such as Task manager view, File manager view, python script execution plays very important role in detailed investigation of the victim endpoint. - IT admin shall have remote parallell access to the endpoint under investigation in a way it shall not affect the enduser routine work & is non intrusive.	Please refer to the revised "Annexure F"
753	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file" Justification:** The solution shall deploy pro-active ransomware protection capability such as honeypot via decoy file creation. Such a pro-active approach will help LIC to prevent an ransomware attack before even the files are encrypted and moved to the attacker server.	Please refer to the revised "Annexure F"
754	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution should support collection of logs from third party security solutions like Active Directory, Firewall (Palo Alto, FortiGate, Cisco, Checkpoint), Proxy, DNS, DHCP, O365 etc. from day 1 with licenses included as part of solution offered" Justification: - Major challenge for security team is to understand the larger picture of a multi-stage attack, given that pieces of same attack are seen as alerts on different tools and often this information is seen in isolation. - It is very important for LIC security team to get a consolidated & unified visibility of entire attack chain automatically stitched together to quickly understand such multi-stage attacks and take coordinated response to it. - This can drastically help LIC team to reduce MMTD and MMTR for cyber threats	Please be guided by the RFP
755	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The Solution should perform Network Traffic Analytics capability for: -Malicious Encrypted Traffic (Header Analysis) -North & South Malicious Traffic Monitoring Using AI (Data Exfiltration, C2C, DNS Tunneling etc.) -East & West Malicious Traffic Monitoring using AI (Lateral Movement) -Protocol Monitoring (DNS, NTLM, MSRPC, Kerberos, SSL/TLS, LDAP, IMAP etc.) -Identify Data Exfiltration Via Legitimate Protocols (DNS Tunneling, ICMP Tunneling). -Identify And Block Usage Of Common Attack Tools (Metasploit, Empire, Cobalt Etc.)" Justification: Asides endpoint visibility, it is equally important to have insights of network traffic and anomalies in network to correlate it with end-user/endpoint activity and have better understanding of complete incident lifecycle	Please be guided by the RFP
756	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution should have single console for below features : - NGAV & EDR, Threat Hunting, Forensic, Network Traffic Analytics, Historical Queries, Identity Analytics, Cloud Workloads & Container Security" Justification: An integrated and unified solution will help LIC security team get holistic visibility of their environment which can improve the security effectiveness and efficacy of the solution. Consolidated visibility with cross-data analytics will yield better detections and reduce the MTTD and MTTR for LIC team. This also helps LIC team to ease the operations of the solution and management is simplified.	Please be guided by the RFP
757	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: "The proposed solution should have asset management functionality to maintain a central repository of all assets for correlation and identification of rogue devices. " Justification: Identification of rogues devices within LIC environment can help security team keep a track of legitimate organization devices and ensure that no devices are running without EDR agent which can pose a severe threat to LIC if that device is breached. This is very important functionality & we request LIC to include the same. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.	Please be guided by the RFP

758	Annexure F	Technical Compliance for EDR		Request this new point to be added	Point to be added: ""The proposed solution is capable of Detection & Prevention Capabilities Against Identity Theft Attacks Such Below: SSO & AD Session Hijacking, Data Exfiltration, Compromised Credentials, Compromised Devices, Privileged User Monitoring, Unconstrained Delegation, Enumeration (User, SMB, NetBIOS, DNS etc.),The Printer Bug, Protection against Mimikatz to Extract the TGT, Pass the Ticket, Pass the Token, Pass the Hash, DCSync to Domain Compromise, Impossible traveler" Justification: With almost every attack leveraging Identity theft and compromised identity to spread laterally in the environment and execute the attacks, it is very important for LIC to have real-time view of user activities where the solution can clearly call out the anomalies in user behavior comprising of suspicious actions associated with the user. This will help to prevent Identity based attacks on LIC environment and provide contextual awareness to LIC team on early suspicions of malicious insiders to take mitigation actions before they turn rogue.	Please be guided by the RFP
759	Annexure F	Technical Compliance for EDR		Request this new point to be added	**Point to be added: "The proposed solution should support demonstration Of Impersonation, Risky User Activities, Credential Misuse, Impossible Travel etc. and should have timeline view & 360 degree identity view with its user risk score. " Justification:** This will help to identify suspicious user activites and track it back with user risk scoring to take appropriate actions	Please be guided by the RFP
760				Request this new point to be added	Point to be added: "The proposed solution should store all the telemetry data collected from the LIC at MeitY compliant Data Centre in India and analytics should happen in India only." Justification: LIC is a nation critical infrastructure and to ensure data privacy and compliance requirement, the vendor shall ensure all the data collected and processed is within India region and CSP where vendor is hosted is MeitY empaneled. There are pub sector FSI institutions who has requested for the same when selecting a cloud delivered EDR solution. pls refer GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please be guided by the RFP
761	Annexure-F	EDR Section		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem/Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
762	Annexure-F	EDR Section		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support additionally up to 4000+ Servers and should be an On-prem/ Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
763	Annexure-F	EDR Section		The solution must use an "Authentication Token" for securely registering a new client installation to the Solution.	This is a vendor-specific point. Every EDR solution has a different mechanism to register the new EDR client installation. Hence, we request the LIC team modify the point as **"The solution must have a secure mechanism to communicate the new client installer with the management server."**	Please refer to the revised "Annexure F"
764	Annexure-F	EDR Section		The solution must allow to manage the agent version and components from the management interface ability to run on hypervisor - VMware, Nutanix etc.	The management interface of most of the on-premise EDR solutions runs on the top of the Windows Server OS, which can be hosted on hypervisors like VMWare, Nutanix etc. We are requesting to change the clause to "The solution must allow to manage the agent version and components from the management interface hosted on the Windows Server & the underline platform can be hypervisor - VMware, Nutanix etc. "	Please be guided by the RFP
765	Annexure-F	EDR Section		The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	This is not EDR functionality. The Application Control feature of Endpoint Security can allow or block access to the applications based on the policies. However, we need more clarification for restricting network access for specified applications function.	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
766	Annexure-F	EDR Section		The solution will Automatically learn and authorize logged in users	This is not EDR functionality. This functionality belongs to the IAM solution. We are requesting the LIC team to give more clarity on this functionality w.r.t EDR functionality	Please refer to the revised "Annexure F"
767	Annexure-F	EDR Section		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	This is a vendor-specific point. We are requesting the LIC team to modify this point as **" The solution must have scrubbing/sandboxing capabilities. Incoming files will be extracted of all potential malicious content such as scripts, macros, and active content."**	Please refer to the revised "Annexure F"
768	Annexure-F	EDR Section		Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data	To search data, including File, Process, Network, Registry, Injection, and user data, it is required to be recorded. Hence, we are requesting the LIC team to remove the word "Undetected Sensor" data from the clause	Please refer to the revised "Annexure F"
769	Annexure-F	EDR Section		Solution must be GDPR , DPDPB compliant	DRDP law is yet to be effective, hence, requesting the LIC team to remove the DPDPB compliant point	Please refer to the revised "Annexure F"
770	Annexure-F	EDR Section		The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report	We seek more clarification on this use w.r.t the EDR functionality.	As most of the EDR solution are being built on top of AI ML so the solution can enhance itself and be effective. We want the EDR to have that capabilities. This can include details about when the threat was first detected, what actions it has taken on the system, how it propagates, which other systems in the network it has affected, and other relevant information. This rich contextual information allows for better understanding and quicker incident response.
771	Annexure F: Technical Compliance	EDR Technical Specifications - point 13	113	Solution must be GDPR , DPDPB compliant	Request LIC to amend this clause as: Solution must be Comply with regulations such as PCI-DSS and HIPAA.	Please refer to the revised "Annexure F"

772	Annexure F: Technical Compliance	EDR Technical Specifications	113	LIC has asked on-premise EDR solution as per the RFP, however there are many technical points which are indicating to NGAV/Endpoint Security features.	Request LIC to confirm, does vendor has to provide NGAV solutions along with on-premise EDR, need your inputs on this point for better understanding which will help vendor to design the technical architecture and solutions accordingly. In case LIC does not want NGAV solutions at this point, can you please make those NGAV points as not-mandatory , so that accordingly vendor can design the architecture and solution where new on-premise EDR can co-exist with existing AV solutions in LIC environment, please help us with your inputs on this point.	Please be guided by the RFP. Present AV solution will expire in Dec 2025. Along with EDR, the AV solution is to be proposed as solution is being procured for 5 years
773	Annexure F: Technical Compliance	EDR Technical Specifications point 15	113	Console access should support using 3rd party systems authentication (Two Factor Authentication)	**Request LIC to amend this clause as** "Console access should support using own native authentication or integrating with third party server AAA system like (AD,LDAP,etc)"	Please refer to the revised "Annexure F"
774	Annexure F: Technical Compliance	EDR Technical Specifications - point 16	113	Solution must use provide modern and easy remote deployment/installation/uninstallation methods (Including script support)	**Request to amend this clause as :** Solution must use provide modern and easy remote deployment/installation/uninstallation methods (Including script support) & 3rd party solutions like (sccm/IT management tool)	Please be guided by the RFP
775	Annexure F: Technical Compliance	EDR Technical Specifications - point 22	113	This solution allows running under device guard features enabled: HVCI, Credentials Guard and Windows Defender App Control	**Vendor specific Point: Request to amend this clause as** : This solution allows running under device guard features and Credentials Guard. App control feature can be achieve through NGAV / Endpoint Security solutions	Please be guided by the RFP
776	Annexure F: Technical Compliance	EDR Technical Specifications - point 34	113	The solution should have the ability to re-brand user notifications	Request LIC to amend this clause as : The solution should have the ability to provide user notifications	Please refer to the revised "Annexure F"
777	Annexure F: Technical Compliance	EDR Technical Specifications - point 35	113	The solution should have the ability to control the level of messages to show to users	**Request to amend this clause as :** The solution should have the ability to provide the level of messages to show to users or soc team.	Please be guided by the RFP
778	Annexure F: Technical Compliance	EDR Technical Specifications - point 42	113	The solution will enforce Firewall rules to allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols	**Request to remove this clause from RFP,** as this feature is part of host based firewall , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. Present AV solution will expire in Dec 2025. Along with EDR, the AV solution is to be proposed as solution is being procured for 5 years
779	Annexure F: Technical Compliance	EDR Technical Specifications - point 43	113	The solution will be used to restrict or allow IPV4/6 network traffic	**Request to remove this clause from RFP,** as this feature is part of host based firewall , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
780	Annexure F: Technical Compliance	EDR Technical Specifications - point 44	113	The solution's client Firewall should remain active during a client upgrade.	**Request to remove this clause from RFP,** as this feature is part of host based firewall , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
781	Annexure F: Technical Compliance	EDR Technical Specifications - point 46	113	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	Request to remove this clause from RFP, as this feature is part of application white-listing/control , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
782	Annexure F: Technical Compliance	EDR Technical Specifications - point 47	113	The solution will be able to Whitelist\Blacklist applications.	**Request to remove this clause from RFP,** as this feature is part of application white-listing/contol , the same can be available on endpoint security / NGAV solutions	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
783	Annexure F: Technical Compliance	EDR Technical Specifications - point 52	113	The solution will protect against existing and zero-day ransomware without requiring signature updates	**Request LIC to amend this clause as** "The solution will protect against existing and zero-day ransomware with or without requiring signature updates."	Please be guided by the RFP. LIC expects the EDR solution to act on protecting against existing and Zero-day ransomware even if the signatures are not updated by using behaviour analytics or other strategies. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
784	Annexure F: Technical Compliance	EDR Technical Specifications - point 53	113	The solution will remediate and restore files that were encrypted during a ransomware attack.	**Request to remove this point,** this feature can be achieve via Endpoint Security / NGAV solutions, EDR can only detect and provide response for any threat on endpoint environment.	Please be guided by the RFP. LIC wants to use enhanced features of EDR solution and not the traditional AV, as there is already a AV solution existing at LIC. Present AV solution will expire in Dec 2025 .Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
785	Annexure F: Technical Compliance	EDR Technical Specifications - point 68	113	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Please elaborate on this point regarding scrubbing capabilities, wanted to understand LIC's expectations on this point, also request to amend this clause as : When scrubbing, the original file must be accessible by SOC admin if is found to be benign by the sandbox	Please refer to the revised "Annexure F"
786	Annexure F: Technical Compliance	EDR Technical Specifications - point 70	113	The solution must block the user from browsing to a known malicious URLs or domains.	**Request LIC to remove this clause:** The same feature can be achieve via Web Gateway/proxy or Endpoint Security/NGAV solutions	Please be guided by the RFP.

787	Annexure F: Technical Compliance	EDR Technical Specifications - point 79	113	The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information	Request LIC to amend this clause as : The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show as part of the reputation information.	Please be guided by the RFP. It should be inbuilt fuctionality of EDR. As per IOC management whether an IP or URL is blacklisted or not can be identified and appropriate action can be taken.
788	Annexure F: Technical Compliance	EDR Technical Specifications - point 95	113	The vendor is responsible for documenting log retention details, which is subject to approval by LIC. Log storage - 2 years as per LIC policy	**Request to amend this clause as :** The vendor is responsible for documenting log retention details with help of integrating with SIEM solutions provided / approved by LIC	Please refer to the revised "Annexure F"
789	Annexure F: Technical Compliance	EDR Technical Specifications - point 96	113	The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as IRDAI, DPDP Act etc.)	Request to amend this clause as: The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as PCI-DSS & HIPAA, etc.)	Please refer to the revised "Annexure F"
790	Endpoint Detection and Response	General Requirements		LIC has asked on-premise EDR solution as per the RFP, however there are many technical points which are indicating to NGAV/Endpoint Security features.	Request LIC to confirm, does vendor has to provide NGAV solutions along with on-premise EDR, need your inputs on this point for better understanding which will help vendor to design the technical architecture and solutions accordingly. In case LIC does not want NGAV solutions at this point, can you please make those NGAV points as not-mandatory , so that accordingly vendor can design the architecture and solution where new on-premise EDR can co-exist with existing AV solutions in LIC environment, please help us with your inputs on this point.	Please be guided by the RFP
791	Endpoint Detection and Response	Sizing Requirements	71	Endpoint Detection and Response : 30000 Windows OS desktops /laptops and 45000 RHEL OS desktops 4000 Servers	Request to LIC for confirming on the total EDR licenses for their requirement , does vendor has to consider total 79000 EDR licenses which is mix of windows & Linux platform.	Please refer to the revised "Annexure F"
792	Endpoint Detection and Response	General Requirements		Windows OS & Linux OS	Request LIC to provide details on existing OS platform like version details, this will help vendor to check the OS compatibility with EDR agent	Please be guided by the RFP
793	Endpoint Detection and Response	General Requirements		The vendor should integrate the tool with vulnerability management systems to assess the endpoint's security posture.	Request LOC to amend this clause as : The vendor should share relevant threat information with vulnerability management systems which help to assess the endpoint's security posture.	Please be guided by the RFP
794	Annexure F: Technical Compliance	EDR Technical Specifications	113	34. The solution should have the ability to re-brand user notifications	Please clarify the expectation of 're-brand'. Does it refer to changing the default text inside the user notification?	Please refer to the revised "Annexure F"
795	Annexure F: Technical Compliance	EDR Technical Specifications	113	35. The solution should have the ability to control the level of messages to show to users	Please clarify what are the different levels of messages to be shown to users. Kindly provide an example if possible	EDR should have capabilities to control user notification to show detection and prevention notification.
796	Annexure F: Technical Compliance	EDR Technical Specifications	113	59. The solution should be integrated with the existing monitoring Solution	Please provide information on the existing monitoring solution used.	Please be guided by the RFP
797	6 - Eligibility Criteria	S. No - 8	14	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints.	Already, LIC has defined the selection criteria for the bidder using the eligibility criteria w.r.t. bidders experience in executing such similar projects. By adding this clause, LIC is further limiting the options available to the bidder. Ideally, this should be OEM's criteria. Hence request you to remove this clause at least for the bidder.	Please refer to the revised "Minimum Eligiblity Criteria"
798	6. Eligibility Criteria	6. Eligibility Criteria	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Request LIC to modify this clause as, The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the EDR solution to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
799	On-Site Support Services for EDR	On-Site Support Services for EDR	60	EDR : onsite support for Branch offices	We assume that LIC's existing end point support team will provide hand and feet support for end point related troubleshooting.	Please be guided by the RFP
800	X.Endpoint Detection and Response (EDR)		70	Bidder to ensure the proposed EDR solution is capable of coexisting with the currently implemented Antivirus solution in LIC until its end of validity.	Request to share details of the current solutions and there should be a mention that the EDR should be an independent OEM to fulfill the need for comprehensive defense in depth requirements and to nullify any unreasonable advantage the existing OEM and OEM's partner may have. If LIC wishes to utilize the same OEM, then LIC can negotiate the upgrade with the existing OEM directly and the bidders can only focus on providing the managed EDR services to ensure appropriate fairness.	Please be guided by the RFP
801	6. Project Timelines	6. Project Timelines	83	Implementation of EDR and roll out of agents in the endpoints. Date of implementation of last device shall be taken as date of installation of all devices. T + 24 Weeks	Request LIC to extend the Implementation timelines as below for EDR and roll out of agents in the endpoints. T + 40 Weeks	Please be guided by the RFP
802	EDR Implementation SLA	Implementation Time	90	The period within which the EDR solution will be fully implemented and operational post-contract signing	This can never be achieved as the number of endpoints is an indicative number. Kindly reqiest if this can be modified to 100% of crown jewels and 30% of Endpoints of windows and linux respectively. Else, LIC should clarify on what is the signoff critieria ?	Please be guided by the RFP
803	EDR Implementation SLA	Uptime	90	The percentage of time the EDR system is expected to be operational and available. 99.99%	IS this uptime for the central management console of EDR ? Please specify accordingly	Please be guided by the RFP
804	EDR Implementation SLA	Incident Resource Time	90	Resolution Time Severity 1 - 30Mins Severity 2 - 2 Hrs. Severity 3 - 8Hrs	Response time should be in line with the SOC services response time. There should not be any SLA on resolution. IN many cases, Bidder will await action response from LIC. Please modify accordingly	Please be guided by the RFP
805	EDR Implementation SLA	Change Management	90	Successful implementation of change within 24 hrs. post approval	LIC has to ensure the availability of the asset on which the change is to be implemented. Any impact, post change, no SLA will be applicable on the specific action	Please be guided by the RFP
806	EDR Implementation SLA	Data Retention Period Backup Frequency Backup Restoration Drills	90	The duration of logs and data are retained within the SIEM system before rotation or archiving. How often data should be backed up to ensure recoverability. To Check the backup restoration effectiveness	LIC has to clarify on the overall expectations and applicability of the same currently in reference to existing AV system	Please be guided by the RFP

807	EDR Implementation SLA	Reinstallation/ Repair	90	Process for reinstallation or repairing in the event of system failure	If there is a need to re-install or repair of the existing deployment, the respective asset owner has to update. Also this SLA should only be applicable for crown jewels. For endpoints, LIC's FM team can do the needful and seek help only if there is failure. This is important as the onsite team is limited and they cannot be overwhelmed for small repeatable task.	Please be guided by the RFP
808	Annexure C: Eligibility Criteria	N/A	107	8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Request this be changed as below 8. The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported EDR solution to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users Or One Organization with minimum 1 Lakh users during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
809	Annexure F	Technical Compliance for EDR	113	The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	**The request if to modify this point to allow cloud solutions we well. The modified point is: "The solution must support up to 30,000 Windows OS endpoints/clients and 45,000 RHEL OS endpoints and should be an On-prem solution/Cloud based in India" Justification:** Considering advancement in technology, attackers are able to create highly sophoticated attacks. They leverage technologies such as Cloud, AI & ML. In order to detect & prevent from such attacks, Security vendors needs to bring advancement in the product at a very fast pace. Also they need to leverage AI & ML as well. Such things are only possible if the security solution is delivered from the cloud as it is easy to leverage resources from the cloud. In an On-Prem deployment, the security solution will be binded by the compute available on prem only. It cannot scale or keep up tha pace of advancement required to detect & prevent against modern day threats. LIC must prioritize security efficacy of the solution as the top most criteria, which is superior in case of cloud-based solutions compared to on-premise solutions. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please refer to the revised "Annexure F"
810	Annexure F	Technical Compliance for EDR	113	The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We request to modify this point. The modified point is: "The solution must support additionally up to 4,000+ Servers and should be an On-prem solution/Cloud based in India" Justification: As per the MITRE testing's done over the last few years for EDR solutions, all the solutions offered by the OEMs were cloud based solutions & not on prem versions. The primary reason for doing the same was to make sure that the best platform with the required resources to detect & protect is evaluated in these advanced cyber-attack tests. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.	Please refer to the revised "Annexure F"
811	Annexure F	Technical Compliance for EDR	113	Solution must be GDPR , DPDPB compliant	We request to remove this point or make it optional, the revised point recommended is as: "Solution must be GDPR /DPDPB compliant" Justification: DPDPB is fairly a new compliance and just recently launched, it will ideally need some time to get the framework matured and acceptable across the industry. Also, OEM's need some time to ensure they have thoroughly worked on the principles of this compliance before they publish compliance for it.	Please refer to the revised "Annexure F"
812	Annexure F	Technical Compliance for EDR	113	The solution must use an “Authentication Token” for securely registering a new client installation to the Solution.	Request to modify this point as: "The solution must have a mechanism to securely register a new client installation to the LIC EDR Solution." Justification: This feature is available with a limited set of OEMs & hence would restrict participation. Solutions have capability to identify endpoints not belonging to LIC by putting in various filter conditions, LIC can use it to identify these endpoint & remove them from the console periodically. Also pls note that the endpoint package distribution is to be controlled as process, either providing it to the endpoint imaging team or hosting it on an internal software portal where users are identified first before allowing them to deploy. Also regular desktop/laptop users normally do not have user permissions to do package installations on their own.	Please refer to the revised "Annexure F"
813	Annexure F	Technical Compliance for EDR	113	The solution should have the ability to re-brand user notifications	**Request is to modify this point as: "The solution should have the ability to send user notifications when flagged for malicious activity". Justification:** Getting user notifications in real-time shall be topmost priority of LIC, rather than the format and outlook of notification. Also having a custom rebranding is a good to have & not a core functionality of an EDR solution.	Please refer to the revised "Annexure F"
814	Annexure F	Technical Compliance for EDR	113	The solution will identify and block out-going communication to malicious C&C sites	Request to modify this point & not limit only to C&C communication, the revised point recommended is: "The solution will identify and block out-going malicious communication as a result of file-based or file-less attacks". Justification: Any communications which are executed out of malicious file-based / fileless attacks shall be blocked and it should not just be limited to C&C sites. Blocking C&C sites (URLs) in particular is a URL filtering solution feature & not a core EDR functionality. This will limit more solutions from being proposed to LIC. URL filtering is a proxy solution functionality for which LIC has a proxy already deployed.	Please refer to the revised "Annexure F"
815	Annexure F	Technical Compliance for EDR	113	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	**Request is to modify the point as: "The solution must have capability to look at contents of the file such as scripts, macros and block it if found malicious". Justification:** This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Even after scrubbing there can be residual malware which might harm the endpoint & hence as a practice it is always recommended to block content which is malicious in nature.	Please refer to the revised "Annexure F"

816	Annexure F	Technical Compliance for EDR	113	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	**Request is to modify the point as: "The original file must be accessible to end user if is found to be benign by the sandbox". Justification:** This point is specific to a few OEM and not all the vendors will be able to qualify, hence needs to be changed to as recommended. This will ensure more OEM will able to bid & LIC will get price advantage. Also scrubbing does not ensure 100% malware reomoval. If there is residual malware left, the file would still pose a security danger on the endpoint & within the LIC network. As a practice it is always recommended to fully block any malicious content.	Please refer to the revised "Annexure F"
817	Annexure F	Technical Compliance for EDR	113	The solution must block the user from browsing to a known malicious URLs or domains.	Request to remove this point as it is a proxy functionality. This is not a core functionality of an EDR solution & will severely limit participation as it would allow only a limited set of solution to qualify. LIC already has this functionality with their existing AV solution.	Please be guided by the RFP.
818	Annexure F	Technical Compliance for EDR	113	All files written on the filesystem will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious	Request to modify the point to include execution of files as a stage for analysis, the modified point is as: "All files written/executed on the filesystem will monitored and statically analyzed. If found as potentially malicious the files will be emulated by sandboxing and quarantined if found as malicious". Justification: Malware activities are initiated when files or process are executed. This is applicable for general file OR file less attacks. LIC must focus on malicious activity & ability of the solution to detect & prevent such malicious activities. Submitting all unknown files for sandboxing at the time of being writing is not ideal. Only the ones which are when executed should be ideally analyzed & if the local endpoint analysis is not able to give a conviction should be submitted for sandboxing.	Please refer to the revised "Annexure F"
819	Annexure F	Technical Compliance for EDR	113	The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information	**Request to change the point as: "The solution will list reputation analysis on files whether Benign or malicious and accordingly take action on it.". Justification:** URL and IP reputation along with geolocation is core functionality of a proxy solution & not EDR. If not changed, it will allow a limited set of solutions to be eligible to bid here.	Please be guided by the RFP. It should be inbuilt fuctionality of EDR. As per IOC management whether an IP or URL is blacklisted or not can be identified and appropriate action can be taken.
820	Annexure F	Technical Compliance for EDR	113	The solution should be able to log the C&C communication from the emulated BOT file	**Request the point to be modified as: "The solution should be able to log all the communications from the emulated BOT file". Justification:** Logging should not just be limited to C&C communications, all the communication logs from emulated BOT shall be available in the solution. Loggin only c&c will provide limited visibility. There can be destinations which are not yet classified as C&C and not logging them will create a visibility gap.	Please refer to the revised "Annexure F"
821	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution must be deployed in a similar size FSI environment in India (100,000 end points or higher) & must be operational for last 2 years & more. This should not be AV but EDR deployment" Justification: We recommend to add this point as it would Ensure that Vendor has expertise and capability of successfully executing and managing large organization such as LIC for optimal ROI of the investment of solution	Please be guided by the RFP
822	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "In order to secure LIC environment against sophisticated attacks, the proposed solution must have higher degree of security efficacy. It must be tested & secured top 3 position in last 2 MITRE ATT&CK evaluations results (Wizard Spider + Sandstrom & Turla) for the highest Technique based Analytics detection with not more than 5 configuration changes collectively." Justification: It is strongly recommended to add this point as LIC is a National Critical Infrastructure and security of its environment is paramount to both LIC and Nation. It is therefore very important for LIC to select the solution which has established and demonstrated its security effectiveness in Industry standard evaluation tests and the vendor which has produced best results in order to guard LIC from sophisticated cyber threats.	Please refer to the revised "Annexure F"
823	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	**Point to be added: "Proposed solution should have a mechanism to install dissolvable agent after analyzing anomalous traffic in network logs." Justification:** While prevention and detection of threats on managed endpoints is important, it is also critical to know if there's malicious/suspicious traffic seen on an unmanaged endpoints in the environment. Detection of threats on the unmanaged assets can help LIC take swift actions to curtail the attack chain early in the stage. Dissolvable agent would help install agents on such endpoints. LIC has many third party vendors which work for then & this use case can also extend to 3rd party assests where LIC wants to collect endpoint telemetry for a short duration.	Please be guided by the RFP
824	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	**Point to be added: "Proposed solution should have identity analytics to detect user/identity based threats such as lateral movement, and it should have supervised and unsupervised learning capabilities." Justification:** With almost every attack leveraging compromised user access to spread laterally in the environment and execute the attacks, it is very important for LIc to have real-time view of user activities where the solution can clearly call out the anomalies in user behaviour comprising of suspicious actions associated with the user	Please be guided by the RFP
825	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution should provide automatic aggregation functionality so that related alerts are displayed in a unified Incident view for easier investigations with a causality chain view." Justification: Major challenge for security team is to understand the larger picture of a multi-stage attack, given that pieces of same attack are seen as alerts on different tools and often this information is seen in isolation. It is very important for LIC security team to get a consolidated & unified visibility of entire attack chain automatically stitched together to quickly understand such multi-stage attacks and take coordinated response to it.This can drastically help LIC team to reduce MMTD and MMTR for cyber threats. This feature will enhance & provide a larger picture to the SOC of multi stage attacks with respect to endpoint. This will ease of investigation & response capabilities. Also this is a core feature of EDR.	Please refer to the revised "Annexure F"

826	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution shall provide comprehensive protection against exploits including MacOS, Linux (RHEL, Ubuntu & Centos Flavors) and processes running in Linux Containers. Solution shall leverage extensive techniques for exploit prevention on RHEL servers including but not limited to Brute Force Protection, Java Deserialization, Kernel Integrity Monitoring, Local Privilege Escalation Protection, Reverse Shell Protection, ROP, Shellcode Protection, SO Hijacking Protection etc.. and shall not simply rely on IPS signatures and CVSS scores for protection" Justification: LIC having larger stack of RHEL (Linux), it is very important that the vendor provides extensive technique based exploit prevention for RHEL servers to safeguard LIC holistically. It is very important for LIC to include this as they have a large adoption of the Linux OS.	Please refer to the revised "Annexure F"
827	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below: File hash Information collection, Termination of the service, Download of binary, Addition of hash value to block list, Delete the file, Send the hash to get the verdict (TI integration), Execute a python script, Execute a PowerShell script." Justification: - Quick response of victim systems in a situation where some suspicious/malicious events are seen needs to be investigated quickly with granular controls needed on the endpoints. - At such critical times actions such as Task manager view, File manager view, python script execution plays very important role in detailed investigation of the victim endpoint. - IT admin shall have remote parallel access to the endpoint under investigation in a way it shall not affect the end-user routine work & is non-intrusive.	Please refer to the revised "Annexure F"
828	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	**Point to be added: "The proposed solution shall provide anti-ransomware capability through creation of decoy file and not using customer live file" Justification:** The solution shall deploy pro-active ransomware protection capability such as honeypot via decoy file creation. Such a pro-active approach will help LIC to prevent an ransomware attack before even the files are encrypted and moved to the attacker server.	Please refer to the revised "Annexure F"
829	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution should support collection of logs from third party security solutions like Active Directory, Firewall (Palo Alto, FortiGate, Cisco, Checkpoint), Proxy, DNS, DHCP, O365 etc. from day 1 with licenses included as part of solution offered" Justification: - Major challenge for security team is to understand the larger picture of a multi-stage attack, given that pieces of same attack are seen as alerts on different tools and often this information is seen in isolation. - It is very important for LIC security team to get a consolidated & unified visibility of entire attack chain automatically stitched together to quickly understand such multi-stage attacks and take coordinated response to it. - This can drastically help LIC team to reduce MMTD and MMTR for cyber threats	Please be guided by the RFP
830	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	**Point to be added: "The Solution should perform Network Traffic Analytics capability for:** **-Malicious Encrypted Traffic (Header Analysis)** **-North & South Malicious Traffic Monitoring Using AI (Data Exfiltration, C2C, DNS Tunneling etc.)** **-East & West Malicious Traffic Monitoring using AI (Lateral Movement)** **-Protocol Monitoring (DNS, NTLM, MSRPC, Kerberos, SSL/TLS, LDAP, IMAP etc.)** **-Identify Data Exfiltration Via Legitimate Protocols (DNS Tunneling, ICMP Tunneling).** **-Identify And Block Usage Of Common Attack Tools (Metasploit, Empire, Cobalt Etc.)" Justification:** Asides endpoint visbility, it is equally important to have insights of network traffic and anomalies in network to correlate it with enduser/endpoint activity and have better understanding of complete incident	Please be guided by the RFP
831	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution should have single console for below features : - NGAV & EDR, Threat Hunting, Forensic, Network Traffic Analytics, Historical Queries, Identity Analytics, Cloud Workloads & Container Security" Justification: An integrated and unified solution will help LIC security team get holistic visibility of their environment which can improve the security effectiveness and efficacy of the solution. Consolidated visibility with cross-data analytics will yield better detections and reduce the MTTD and MTTR for LIC team. This also helps LIC team to ease the operations of the solution and management is simplified.	Please be guided by the RFP
832	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution should have asset management functionality to maintain a central repository of all assets for correlation and identification of rogue devices. " Justification: Identification of rogues devices within LIC environment can help security team keep a track of legitimate organization devices and ensure that no devices are running without EDR agent which can pose a severe threat to LIC if that device is breached. This is very important functionality & we request LIC to include the same. There are equally sized public sector banks who have opted for cloud based EDR solution, refer bid: GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80k users.	Please be guided by the RFP

833	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: ""The proposed solution is capable of Detection & Prevention Capabilities Against Identity Theft Attacks Such Below: SSO & AD Session Hijacking, Data Exfiltration, Compromised Credentials, Compromised Devices, Privileged User Monitoring, Unconstrained Delegation, Enumeration (User, SMB, NetBIOS, DNS etc.),The Printer Bug, Protection against Mimikatz to Extract the TGT, Pass the Ticket, Pass the Token, Pass the Hash, DCSync to Domain Compromise, Impossible traveler" Justification: With almost every attack leveraging Identity theft and compromised identity to spread laterally in the environment and execute the attacks, it is very important for LIC to have real-time view of user activities where the solution can clearly call out the anomalies in user behavior comprising of suspicious actions associated with the user. This will help to prevent Identity based attacks on LIC environment and provide contextual awareness to LIC team on early suspicions of malicious insiders to take mitigation actions before they turn rogue.	Please be guided by the RFP
834	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	Point to be added: "The proposed solution should support demonstration Of Impersonation, Risky User Activities, Credential Misuse, Impossible Travel etc. and should have timeline view & 360 degree identity view with its user risk score. " Justification: This will help to identify suspicious user activates and track it back with user risk scoring to take appropriate actions	Please be guided by the RFP
835			113		Point to be added: "The proposed solution should store all the telemetry data collected from the LIC at MeitY compliant Data Centre in India and analytics should happen in India only." Justification: LIC is a nation critical infrastructure and to ensure data privacy and compliance requirement, the vendor shall ensure all the data collected and processed is within India region and CSP where vendor is hosted is MeitY empaneled. There are pub sector FSI institutions who has requested for the same when selecting a cloud delivered EDR solution. pls refer GEM/2023/B/3460972. This RFP was released by Bank Of Baroda for 80K users.	Please be guided by the RFP
836	Annexure F: Technical Compliance	EDR Technical Specifications	113	34. The solution should have the ability to re-brand user notifications	Please clarify the expectation of 're-brand'. Does it refer to changing the default text inside the user notification?	Please refer to the revised "Annexure F"
837	Annexure F: Technical Compliance	EDR Technical Specifications	113	35. The solution should have the ability to control the level of messages to show to users	Please clarify what are the different levels of messages to be shown to users. Kindly provide an example if possible	EDR should have capabilities to control user notification to show detection and prevention notification.
838	Annexure F: Technical Compliance	EDR Technical Specifications	113	59. The solution should be integrated with the existing monitoring Solution	Please provide information on the existing monitoring solution used.	Please be guided by the RFP
839	Annexure C	Point No 8	107	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	EDR covering enterprise wide deployment is a relatively newer technology in terms of its deployment scale. It will be more appropriate if OEM implementation for the scale is evaluated . Hence request LIC to modify the clause to as below: The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the EDR to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 15000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised "Minimum Eligiblity Criteria"
840	Annexure D	Point no 6	110	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 60000 endpoints -> 15 Marks • Greater than 40000 endpoints -> 10 Marks • Greater than 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	While LIC may seek EDR reference projects from Bidder , since there are have been limited deployments of this scale we request LIC to consider the following clause. The bidder must have experience during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Equal to or Greater than 15000 endpoints -> 10 Marks • Equal to or Greater than 10000 endpoints -> 7 Marks • Equal to or Greater than 5000 endpoints -> 5 Marks The OEM must have experience during lthe last 5 years preceding to to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • 3 references of Greater than 30000 endpoints -> 5 Marks • 2 references of Greater than 30000 endpoints -> 3 Marks • 1 references of 30000 endpoints -> 2 Marks (Supporting Document: Bidder (SI)/OEM should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
841	Annexure-F	EDR Section		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem/Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
842	Annexure-F	EDR Section		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support additionally up to 4000+ Servers and should be an On-prem/ Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"

843	Annexure-F	EDR Section		The solution must use an "Authentication Token" for securely registering a new client installation to the Solution.	This is a vendor-specific point. Every EDR solution has a different mechanism to register the new EDR client installation. Hence, we request the LIC team modify the point as **"The solution must have a secure mechanism to communicate the new client installer with the management server."**	Please refer to the revised "Annexure F"
844	Annexure-F	EDR Section		The solution must allow to manage the agent version and components from the management interface ability to run on hypervisor - Vmware, Nutanix etc.	The management interface of most of the on-premise EDR solutions runs on the top of the Windows Server OS, which can be hosted on hypervisors like VMWare, Nutanix etc. We are requesting to change the clause to **"The solution must allow to manage the agent version and components from the management interface hosted on the Windows Server & the underline platform can be hypervisor - Vmware, Nutanix etc. "**	Please be guided by the RFP
845	Annexure-F	EDR Section		The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	This is not EDR functionality. The Application Control feature of Endpoint Security can allow or block access to the applications based on the policies. However, we need more clarification for restricting network access for specified applications function.	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
846	Annexure-F	EDR Section		The solution will Automatically learn and authorize logged in users	This is not EDR functionality. This functionality belongs to the IAM solution. We are requesting the LIC team to give more clarity on this functionality w.r.t EDR functionality	Please refer to the revised "Annexure F"
847	Annexure-F	EDR Section		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	This is a vendor-specific point. We are requesting the LIC team to modify this point as **" The solution must have scrubbing/sandboxing capabilities. Incoming files will be extracted of all potential malicious content such as scripts, macros, and active content."**	Please refer to the revised "Annexure F"
848	Annexure-F	EDR Section		Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data	To search data, including File, Process, Network, Registry, Injection, and user data, it is required to be recorded. Hence, we are requesting the LIC team to remove the word "Undetected Sensor" data from the clause	Please refer to the revised "Annexure F"
849	Annexure-F	EDR Section		Solution must be GDPR , DPDPB compliant	DRDP law is yet to be effective, hence, requesting the LIC team to remove the DPDPB compliant point	Please refer to the revised "Annexure F"
850	Annexure-F	EDR Section		The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report	We seek more clarification on this use w.r.t the EDR functionality.	As most of the EDR solution are being built on top of AI ML so the solution can enhance itself and be effective. We want the EDR to have that capabilities. This can include details about when the threat was first detected, what actions it has taken on the system, how it propagates, which other systems in the network it has affected, and other relevant information. This rich contextual information allows for better understanding and quicker incident response.
851	Suggestion	EDR Section		EDR telemetrty to be used for doing attack surface risk management - user risk, device risk, App risk level with companywide risk score followed by mitigation	Requesting you to add this functionality	Please be guided by the RFP
852	Suggestion	EDR Section		Forensics and IR to be part of the platform	Requesting you to add this functionalitiy	Please be guided by the RFP
853	Suggestion	EDR Section		EDR OEM's own Generative AI to be included as part of Platform for accelerating the Detection and Response for LIC	Requesting you to add this functionality	Please be guided by the RFP
854	Brief Scope of Work	On-Site Support Services for EDR	60	8x5 real-time monitoring uptime, availability, health performance of EDR devices with mitigation support.	What is the scope of service post 8x5? How will the incidents be managed?	Please be guided by the RFP
855	Project Timelines	The Phase Wise Project Timelines of EDR as below	83	Implementation of EDR and roll out of agents in the endpoints	Please confirm which tool can be used for central agent rollout for EDR for the endpoints	Please be guided by the RFP
856	Annexure-F	EDR Section		The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints and should be an On-prem/Cloud-based/Hybrid solution"**	Please refer to the revised "Annexure F"
857	Annexure-F	EDR Section		The solution must support additionally up to 4000+ Servers and should be an On-prem solution	We are requesting the LIC team to change the clause to **"The solution must support additionally up to 4000+ Servers and should be an On-prem/ Cloud-based/Hybrid solution"**	Please be guided by the RFP
858	Annexure-F	EDR Section		The solution must use an "Authentication Token" for securely registering a new client installation to the Solution.	This is a vendor-specific point. Every EDR solution has a different mechanism to register the new EDR client installation. Hence, we request the LIC team modify the point as **"The solution must have a secure mechanism to communicate the new client installer with the management server."**	Please refer to the revised "Annexure F"
859	Annexure-F	EDR Section		The solution must allow to manage the agent version and components from the management interface ability to run on hypervisor - Vmware, Nutanix etc.	The management interface of most of the on-premise EDR solutions runs on the top of the Windows Server OS, which can be hosted on hypervisors like VMWare, Nutanix etc. We are requesting to change the clause to **"The solution must allow to manage the agent version and components from the management interface hosted on the Windows Server & the underline platform can be hypervisor - Vmware, Nutanix etc. "**	Please be guided by the RFP
860	Annexure-F	EDR Section		The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes.	This is not EDR functionality. The Application Control feature of Endpoint Security can allow or block access to the applications based on the policies. However, we need more clarification for restricting network access for specified applications function.	Please be guided by the RFP. In all the modern EDR solutions application whitelisting is one of the key feature and most of the solution are supporting it. Present AV solution will expire in Dec 2025. Along with EDR the AV solution is to be proposed as solution is being procured for 5 years
861	Annexure-F	EDR Section		The solution will Automatically learn and authorize logged in users	This is not EDR functionality. This functionality belongs to the IAM solution. We are requesting the LIC team to give more clarity on this functionality w.r.t EDR functionality	Please refer to the revised "Annexure F"

862	Annexure-F	EDR Section		The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content	This is a vendor-specific point. We are requesting the LIC team to modify this point as **" The solution must have scrubbing/sandboxing capabilities. Incoming files will be extracted of all potential malicious content such as scripts, macros, and active content."**	Please refer to the revised "Annexure F"
863	Annexure-F	EDR Section		Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data	To search data, including File, Process, Network, Registry, Injection, and user data, it is required to be recorded. Hence, we are requesting the LIC team to remove the word "Undetected Sensor" data from the clause	Please refer to the revised "Annexure F"
864	Annexure-F	EDR Section		Solution must be GDPR , DPDPB compliant	DRDP law is yet to be effective, hence, requesting the LIC team to remove the DPDPB compliant point	Please refer to the revised "Annexure F"
865	Annexure-F	EDR Section		The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report	We seek more clarification on this use w.r.t the EDR functionality.	As most of the EDR solution are being built on top of AI ML so the solution can enhance itself and be effective. We want the EDR to have that capabilities. This can include details about when the threat was first detected, what actions it has taken on the system, how it propagates, which other systems in the network it has affected, and other relevant information. This rich contextual information allows for better understanding and quicker incident response.
866	Suggestion	EDR Section		EDR telemetrty to be used for doing attack surface risk management - user risk,device risk,App risk level with company wide risk score followed by mitigation	Requesting you to add this functionalitiy	Please be guided by the RFP
867	Suggestion	EDR Section		Forensics and IR to be part of the platform	Requesting you to add this functionality	Please be guided by the RFP
868	Suggestion	EDR Section		Dark Web Monitoring for leaked credentials of LIC	Requesting you to add this functionality	Please be guided by the RFP
869	Suggestion	EDR Section		Generative AI to be included as part of Platform for accelerating the Detection and Response for LIC	Requesting you to add this functionality	Please be guided by the RFP
870	Suggestion	EDR Section		Solution to have Vulnerability assessment and prioritization	Requesting you to add this functionality	Please be guided by the RFP
871	Eligibility Criteria	point no 8	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	The Bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented/supported the EDR solution for at least 01 (one) client in PSU/Government/Private/BFSI Sector in India The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	Please refer to the revised Annexure D
872	Annexure D: Technical Scoring	point no 6	110	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 60000 endpoints -> 15 Marks • Greater than 40000 endpoints -> 10 Marks • Greater than 30000 endpoints -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to please change the clause as per below: The Bidder/OEM during the last 5 years preceding to the date of this RFP, must have supplied, implemented /supported EDR solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for a minimum endpoint count of: • Greater than 5 customers-> 15 Marks • Greater than 4 customer -> 10 Marks • Greater than 3 customers -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised Annexure D
873	Suggestion	EDR Section			Why EDR for LIC should be in Hybrid model (a combination of on-premise & cloud) ? a. Considering advancement in technology, attackers are utilizing cloud based AI, ML, microservices kind of environment which can scale up, scale down in an instant. To keep up with that pace or rather be ahead of them the traditional on prem deployment approach for EDR will not work. b. Moreover will LIC be ready to take this risk for next 5 years? c. If you still have apprehension with cloud mandate both DC & DR of the proposed solution should be in India.	Please be guided by the RFP
874	Annexure F	Technical Compliance for EDR	113	Request this new point to be added	As MITRE ATT&CK is a reputed, independent, nonprofit organization and is evident with its reference for other technologies in the SoC RFP, the same reference of MITRE ATT&CK evaluations should be considered for EDR as well? To onboard the OEM's with the high security efficacy as defined by some independent, nonprofit organizations like MITRE you have to have EDR on cloud. When MITRE performs "Real World Attack Simulations" that characterizes advanced attacker groups, every OEM sends the cloud version of their solution for those tests to secure the highest score and showcase the highest efficacy which is possible only with AI/ML analysis performed on the cloud.	Please refer to the revised "Annexure F"
875	6.Eligibility Criteria	SN.8	15	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 30000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP.	We recommend the following alterations to the criteria: "The Bidder during the last 5 years preceding to the date of this RFP should have implemented and supported the proposed EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least **3000 endpoints**. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization during the last 3 years preceding to the date of the RFP."	Please refer to the revised "Minimum Eligiblity Criteria"
876	Section E: Scope of Services	1. Brief Scope of Work (On-Site Support Services for EDR)	60	8x5 real-time monitoring uptime, availability, health performance of EDR devices with mitigation support.	We assume that all EDR scope includes AV management.	Understanding is correct
877	Section E: Scope of Services	5. Resource Deployment	81	_	In EDR operation there is mention of EDR & Onsite EDR . Does it mean even branch level support we have to provide for EDR by being available onsite	Understanding is correct