LIC-CO/IT-BPR/NW/RFP/2023-2024/TDIR dated 18 December 2023 - Corrigendum-III

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Bidder Query	Response
1	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
2	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
3	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
4	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
5	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"
6	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
7	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
8	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
9	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
10	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
11	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
12	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"
13	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 "Revised Annexure C - Minimum Eligibility Criteria"
14	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"
15	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"
16	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"
17	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"
18	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"
19	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"

20	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"
21	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 continity 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"
22	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"
23	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"
24	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"
25	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"
26	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"
27	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"
28	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"
29	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"
30	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"
31	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"
32	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"
33	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"
34	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"
35	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"
36	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"
37	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"
38	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"
39	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"
40	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.
41	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" .
42	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"
43	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"
44	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
45	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" .
46	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
47	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
48	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
49	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
50	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
51	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
52	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

53	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
54	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
55	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 revise "Annexure F"
56	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 algorightms 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 revise "Annexure F"
57	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"
58	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"
59	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"
60	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"
61	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"
62	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"
63	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"
64	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" .
65	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"
66	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"
67	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"
68	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 "Revised Annexure D - Technical Scoring"
69	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"
70	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
71	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"
72	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"
73	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"
74	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"
75	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"
76	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" .
77	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" .
78	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" .

79	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" .
80	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
81	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"
82	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" .
83	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"
84	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"
85	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"
86	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"
87	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"
88	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"
89	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
90	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"
91	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"
92	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"
93	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"
94	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" .
95	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" .
96	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" .
97	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" .
98	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"
99	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" .
100	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" .
101	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"
102	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"

103	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"
104	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"
105	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"
106	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"
107	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"
108	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"
109	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"
110	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"
111	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"
112	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"
113	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"
114	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"
115	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"
116	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" .
117	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" .
118	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" .Clause Deleted
119	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" .
120	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"
121	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 "Revised Annexure C - Minimum Eligibility Criteria"
122	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"
123	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"
124	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" .
125	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"
126	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"
127	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"

128	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"
129	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"
130	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"
131	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"
132	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"
133		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".
134	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"
135	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" .
136	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" .
137	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" .
138	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" .
139	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" .
140	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" .
141	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"
142	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"
143		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"
144		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"
145	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"
146	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"
147	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 "Revised Annexure C - Minimum Eligibility Criteria"
148	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"
149	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"
150				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 "
151	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" .
152	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" .
153	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" .

154	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"
155	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" .
156	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" .
157	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" .
158	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" .
159	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"
160	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"
161	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
162	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
163	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" .
164	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" .
165	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" .
166	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" .
167	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" .
168	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" .
169	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" .
170	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" .
171	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" .
172	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" .
173	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" .
174	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"
175	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" .
176	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"
177	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"
178	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"

179	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"
180	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"
181	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"
182	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"
183	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"
184	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"
185	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"
186	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"
187	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 "Revised Annexure C - Minimum Eligibility Criteria"
188	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"
189	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"
190	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"
191	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"
192	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"
193	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"
194	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"
195	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"
196	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"
197	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"
198	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"
199	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"
200	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"
201	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 "Revised Annexure C - Minimum Eligibility Criteria"

202	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"
203	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"
204	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"
205	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"
206	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"
207	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"
208	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"
209	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"
210	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 "Revised Annexure D - Technical Scoring"
211	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 "Revised Annexure D - Technical Scoring"
212	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"
213	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"
214	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"
215	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"
216	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"
217	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"

218	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"
219	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"
220	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"
221	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"
222	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"
223	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
224	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"
225	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"
226	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"
227	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)"
228	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)"
229	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"
230	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"
231	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"
232	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"
233	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"
234	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"
235	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"
236	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"
237	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"
238	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"
239	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"
240	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"
241	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"
242	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"

243	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"
244	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"
245	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
246	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
247	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
248	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
249	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
250	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"
251	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"
252	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"
253	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"
254	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"
255	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"
256	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"
257	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"
258	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"
259	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"
260	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"
261	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" .
262	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"
263	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"
264	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"
265	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"

266	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"
267	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"
268	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"
269	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"
270	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"
271	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"
272	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"
273	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"
274	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"
275	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"
276	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"
277	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"
278	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"
279	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
280	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 • 1 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"
281	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"
282	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" .
283	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" .
284	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" .
285	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" .
286				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"
287	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"
288	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"
289				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"
290				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

291	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 "Revised Annexure C - Minimum Eligibility Criteria"
292	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"
293	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"
294	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"
295	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 "Revised Annexure C - Minimum Eligibility Criteria"
296	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"
297	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"
298	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"
299	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"
300	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"
301	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"
302	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"
303	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"
304	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 Lld. 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"
305	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" .
306	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" .
307	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)"
308	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"
309	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"
310	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

311	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"
312	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"
313	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"
314	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"
315	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" .
316	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.
317	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" .
318	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" .
319	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
320	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"
321	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"
322	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."
323	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
324			97	Audit and access	we would request that this clause be deleted as audit rights are not a surviving clause.	"Audit and access" deleted
325	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"
326	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
327	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"
328	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"
329	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"

330	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"
331	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.
332	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
333	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
334	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
335	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
336	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
337	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
338	General query			General query	Please specify the existing ticketing tool used by LIC	The RFP for ticketing tool is under progress
339	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
340	General query			General query	Current strenght of resources/perations team managing SIEM, SOAR, UEBA & EDR	The information shall be shared with the succesful bidder
341	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
342	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
343	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
344	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
345	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
346	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
347	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
348	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
349	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
350	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
351	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
352	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
353	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 .
354	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
355	5. Resource Deployment	SOC Manager	73	Certifications- CISSP/CISM/CISA/GCIH	The interpretation of "/" is or ? Kindly validate	Yes
356	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
357	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
358	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
359	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
360	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
361	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
362				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
363	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

364	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"
365	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"
366	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"
367	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
368	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"
369	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"
370	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"
371	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"
372	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"
373	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"
374	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"
375	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"
376	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"
377	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"
378		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"
379		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"
380		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"
381		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"
382		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"
383		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"
384		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"
385	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"
386	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"
387	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"
388	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"
389	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"
390	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"
391	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"
392	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"
393	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"

394	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"
395	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"
396	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"
397	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"
398	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"
399	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"
400	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"
401	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"
402	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"
403	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"
404	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"
405	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"
406	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"
407	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"
408	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"
409	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"

410	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"
411	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"
412	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"
413	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"
414	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"
415	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"
416	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 patache s, this feature can achieve through patach management tool, request to remove this point from RFP	Please refer to revised "Section E: Scope of Services"
417	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"
418	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"
419	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"
420	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"
421	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
422	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"
423	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
424				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"
425	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"
426	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"
427	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 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"
428	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"
429	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"
430	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"
431	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"
432	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"

433	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"
434	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"
435	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"
436	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"
437	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"
438	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"
439	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"
440	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"
441	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"
442	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"
443	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"
444	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"
445	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"
446	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"
447	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"
448	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"
449	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"
450	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"
451	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"
452	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"

453	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"
454	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"
455	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"
456	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"
457	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"
458	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"
459	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"
460	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"
461	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"
462	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"
463	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"
464	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"
465	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"
466	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"
467	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"
468	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"
469	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"
470	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"
471	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"
472	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"
473	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"
474	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"
475	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"
476	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"
477	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"
478	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"
479	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"
480	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"

481	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"
482	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"
483	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"
484	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"
485	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"
486	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"
487	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
488	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"
489	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"
490	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"
491	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"
492	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"
493	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"
494	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"
495	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"
496	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"
497	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"
498	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"
499	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"
500	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"
501	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
502	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
503	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"
504	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"