LIC-CO/IT-BPR/NW/RFP/2023-2024/TDIR dated 18 December 2023-Response to Pre-Bid Queries

S. No.	RFP Section	Sub-Section	Pg No.	RFP Clause	Bidder Query	LIC Response
1	Revised Annexure C - Minimum Eligibility Criteria	Annexure C: Eligibility Criteria,Point No.7	1	The Bidder during the last 07 (seven) years preceding to the date of this RFP should have supplied implemented and supported/ maintained the SIEM solution (of minimum 30,000 EPS / 1448 GB per day) 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 / 2897 GB per day in the last 5 years preceding to the date of the RFP.	Kindly request to remove 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 / 2897 GB per day in the last 5 years preceding to the date of the RFP" or provide exemption or waive off for Technically Qualified Make In India Startup OEMs. This will help more Make In India startups to come forward and participate in this opportunity.	Please refer to the " revised Eligiblity Criteria-2 and Annexure C-2"
2	Annexure Q:	Non-Disclosure Agreement (NDA)	131	Respondent agrees to receive the Proprietary Information or other information from LIC and treat all such information as confidential information and to safeguard LIC's confidential information, property, information systems, network, databases and other data.	We propose to make it mutual	Please be guided by the RFP and the Corrigendum III
3	Annexure Q:	Non-Disclosure Agreement (NDA)	134	The Respondent herein agrees and undertakes to indemnify and hold LIC harmless from any loss, damage, claims, liabilities, charges, costs, or expense (including attorneys' fees), that may arise or be caused or result from or be paid/incurred/suffered or caused to be paid/incurred/ suffered by reason of any breach, failure, delay, impropriety or irregularity on its part to honors, observe, adhere to, abide by or comply with any of the terms and conditions of this Agreement. In the event that the Respondent shall be liable to LIC in connection with this Agreement, the Respondent's liability shall be limited to the value of the Contract.	We cannot agree to indemnity at NDA level and of such wide import and propose to remove the same.	Please be guided by the RFP and the Corrigendum III
4	Annexture F	SIEM Compliance 58		The proposed solution should natively provide an out of the box mechanism to discover and classify assets by system type (mail servers, database servers, etc) to minimize false positives associated with poor asset classification.	Directly asset discovery wont possible from Solution. We can integrate with Asset discovery Tool	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
5		SIEM		Machine learning should be embedded across the platform (such as but not limited to SIEM, SBDL, UEBA, etc.). It should empower every user in the SOC with ML. Security analyst should be able to build ML Models from UI i.e. using predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Need relaxation on this clause due to Machine Learning	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
6		SIEM		The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries .	Need relaxation on this clause for ML	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
7		SIEM		The proposed solution should natively have ML capabilities .	Need relaxation on this clause for ML	Please be guided by the RFP and the Corrigendum III
8		SOAR		The solution should have source code available for review for automations, playbooks and integrations.	Need relaxation on this clause for ML	Please be guided by the RFP and the Corrigendum III
9		SOAR		The solution should support 150+ 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	This looks like specific to vendor, please relax this. No. of playbooks, Automations will be ok.	Please be guided by the RFP and the Corrigendum III
10		SOAR		The solution should be able to handle creation of complex playbook which involves nested playbooks to achieve reusability and modularity without additional license requirements.	This looks like specific to vendor, please relaxthis clause. creation of playbooks, without any licence requirements will be good	Please be guided by the RFP and the Corrigendum III
11		UEBA		The proposed solution should not send data to any cloud for processing of UEBA models. All ML models in UEBA should run on-premise only.	Need to relaxation on this clause	Please be guided by the RFP and the Corrigendum III
12		UEBA		The proposed solution should have the capability to support a model that allows the output of one ML model to serve as an input for another ML model .	Need to relax this clause due to Machine Learning	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
13		CTH		The vendor should have the capability to perform(but not limited to) Network Traffic Analysis, UEBA, Machine Learning and advanced Behavioural analytics.	Need relaxation on Machine Learning Prtion	Please be guided by the RFP and the Corrigendum III
14		CTH		Vendor should detect user anomalies using a combination of rules, machine learning model using Artificial Intelligence and Deep learning	Need to relaxation on this clause	Please be guided by the RFP and the Corrigendum III
15		CTH		The vendor should be Leveraging machine learning(AI & ML & Deep Learning) and also utilize various sources to identify malicious activities, including but not limited to NetFlow, IPS/IDS, proxy, WAF, Windows logs, Sysmon, Linux, DNS, and EDR and all devices that are available with LIC	Need to relaxation on this clause	Please be guided by the RFP and the Corrigendum III
16	Section E	Dashbaord		Dashboards	For Dashbords need saperate tool or should be provided from SIEM Platform ?	Please be guided by the RFP and the Corrigendum III
17	Annexture F	UEBA		UEBA should not have saperate data lake, data lake should be same for both platform	Can we get relaxation for this clause ?	Please be guided by the RFP and the Corrigendum III
18	Revised Annexure C	Eligibility Criteria		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 / 2897 GB per day in the last 5 years preceding to the date of the RFP.	Request relaxation on this clasue. Request below changes: The proposed OEM product of SIEM should have been succesfully running in minimum two organizations of minimum 60,000 EPS/2897 GB per day in the last 5 year preceding to the date of the RFP out of which one customer must have minimum 500 branches distributed across India Or The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches distributed globally of minimum 60,000 EPS / 2897 GB per day in the last 5 years preceding to the date of the RFP.	Please refer to the " revised Eligiblity Criteria-2 and Annexure C-2"
19	Revised Annexure F: Technical Compliance	NBAD Technical Specifications	Additional point as per PreBid Query Point #71	71. it should be a dedicated solution delivering all PCAP specifications and use cases mentioned above and should not be subset capability of SIEM or any other solution	Request this to be removed from NBAD section since its applicable to PCAP solution; also #17 of NBAD specs conveys the same point;	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
20	Annexture F	PCAP		The solution should support for capturing and storing data from (but not limited to) multiple network segments, VLANs, network locations, etc. The solution must be capable of supporting Public or Private Cloud infrastructure deployment using industry standard ecosystems. The solution should support deployment into Public Cloud platforms like Amazon Web Services (AWS), Microsoft Azure environments, Google Cloud, etc. The solution should be capable of capturing traffic on Private Cloud, Containers, Dockers & other virtual Infrastructure without the need of third party components. > Microsoft Hyper-V > VMware's ESX, NSX-V & NSX-T > OpenStack > Ubuntu/KVM	Need to be removed	Please be guided by the RFP and the Corrigendum III
21	Annexture F	NBAD		The solution should be a dedicated behaviour analytics solution delivering advanced Network Detection & Response (NDR) use cases and not a subset capability of SIEM or PCAP solution.	Need to be removed	Please be guided by the RFP and the Corrigendum III
22	Annexture F	NBAD		The solution should support monitoring the LIC's public/private cloud infrastructure by collecting, transforming and analysing packet data or network data or telemetry from Cloud service providers.	Need to be removed	Please be guided by the RFP and the Corrigendum III
23	Revised Minimum Eligibility Criteria Annexure C	Annexure C Point No 5	NA	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 /2897 GB per day in the last 5 years preceding to the date of the RFP.	LogRhythm is a robust SIEM (Security Information and Event Management) solution that offers comprehensive capabilities for detecting, analysing, and responding to cyber threats and have multiple deployments across organizations in India including large/marquee enterprises .They are also recognised by Gartner as leaders for 8 years. Considering the above credentials, we request you to revise the OEM Eligibility criteria to as below: The proposed OEM product for SIEM should have been successfully running in minimum three organizations with minimum 500 branches /sites in the last 5 years preceding to the date of the RFP; Out of which atleast one customer reference should be of minimum 60,000 EPS /2897 GB per day.	Please refer to the " revised Eligiblity Criteria-2 and Annexure C-2"
24	Revised Annexure F Technical Compliance	PCAP Technical Specifications	NA	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 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site P - 4 Gbps - West: Site Q - 4 Gbps - East: Site R - 4 Gbps - South: Site S - 4 Gbps - Site A - 4 Gbps - Site B - 1 Gbps - Site C - 1 Gbps - Site D - 8Gbps The cumulative bandwidth at the sites A , B , C and D can be arrived at by adding the bandwidth at Internet facing sites and MPLS colo sites The deployed solution for PCAP with visibility for end users should be in such a way that the WAN utilization across MPLS links is minimally impacted to the order of 5-10%.	Request LIC to clarify as per below understanding of the bidder : There are 12 sites as mentioned along with the Bandwidth throughput. We understand that bidder need to deploy the PCAP Probe/Analytics solution in each of the 12 locations locally. Also the bidder needs to deploy Central management solution in DC (Vile Parle Mumbai) and DR (Bangalore).	There are 8 sites mentioned along with the Bandwidth throughput. The bidder need to deploy the PCAP Probe/Analytics solution in each of the locations locally. Also the bidder needs to deploy Central management solution in DC (Vile Parle Mumbai) and DR (Bangalore).

25	Revised Annexure F Technical Compliance	NBAD Technical Specifications	NA	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 P - 4 Gbps - West: Site Q - 4 Gbps - East: Site R - 4 Gbps - South: Site S - 4 Gbps - Site A - 4 Gbps - Site B - 1 Gbps - Site C - 1 Gbps - Site D - 8Gbps The cumulative bandwidth at the sites A , B , C and D can be arrived at by adding the bandwidth at Internet facing sites and MPLS colo sites The deployed solution for NBAD with visibility for end users should be in such a way that the WAN utilization across MPLS links is minimally impacted to the order of 5-10%.	Request LIC to clarify as per below understanding of the bidder : There are 12 sites as mentioned along with the Bandwidth throughput. We understand that bidder need to deploy the NBAD Probe/Analytics solution in each of the 12 locations locally. Also the bidder needs to deploy Central management solution in DC (Vile Parle Mumbai) and DR (Bangalore).	There are 8 sites mentioned along with the Bandwidth throughput. The bidder need to deploy the NBAD Probe/Analytics solution in each of the locations locally. Also the bidder needs to deploy Central management solution in DC (Vile Parle Mumbai) and DR (Bangalore).
26	Revised Scope of Services -Section E	Sizing Requirements	22	PCAP- 30 Gbps or its equivalent Packets per Second	As per specificatons given in the Technical Compliance (Annexure F), the combined throughput for all sites is adding upto 37.5 Gbps. Hence request LIC to change the minimum sizing in the document "Revised Scope of Services"	Please be guided by the RFP and the Corrigendum III
27	Revised Scope of Services -Section E	Sizing Requirements	22	NBAD- 30 Gbps or its equivalent Flows Per Second or Packets per Second	As per specificatons given in the Technical Compliance (Annexure F), the combined throughput for all sites is adding upto 37.5 Gbps. Hence request LIC to change the minimum sizing in the document "Revised Scope of Services"	Please be guided by the RFP and the Corrigendum III
28	Technical Bid	Point no v	1	This bill of Quantity (BoQ) as per Annexure R should be itemized separately for all the environments, including DC, UAT and Disaster Recovery (DR)	Request LIC to define the Scope/sizing to be considered for UAT . Can bidder consider 5% of the Production Sizing as UAT sizing (including Hardware, Software, OS,DB)	Please be guided by the RFP and the Corrigendum III
29	Annexure F	NBAD Technical Specifications Point No 71		It should be a dedicated solution delivering all PCAP specifications and use cases mentioned above and should not be a subset capablity of SIEM or any other solution	We understand PCAP as mentioned in the technical compliance here is a typo. This needs to be NBAD.	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
30	Annexure F	SIEM Technical Specifications Point no 65		Machine learning should be embedded across the platform (such as but not limited to SIEM, SBDL, UEBA, etc.). It should empower every user in the SOC with ML. Security analyst should be able to build ML Models from UI i.e. using predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Custom build of ML Model use cases are specific for Business Analytics Platform and may not be applicable for Security Analytics Solution as asked in the RFP clause. Hence request LIC to remove the below specifications from the current clause "It should empower every user in the SOC with ML. Security analyst should be able to build ML Models from UI i.e. using predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks."	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
31	Annexure F	SIEM Technical Specifications Point no 69		The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools such as (but not limited to) TensorFlow, PyTorch, R, Python, Scala, etc.	Custom build of ML Model use case and integration with NLP are specific for Business Analytics Platform and may not be applicable for Security Analytics Solution as asked in the RFP clause. Hence kindly request LIC to remove this point.	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
32	Annexure F	SIEM Technical Specifications Point no 71		The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries .	Custom build of ML Model/Algorithm use cases are specific for Business Analytics Platform and may not be applicable for Security Analytics Solution as asked in the RFP clause. . Hence request LIC to remove this clause	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
33	Annexure F	UEBA Technical Specifications Point no 21		The proposed solution should have the capacity to utilize *unsupervised* machine learning algorithms, artificial intelligence and deep learning .	Every UEBA OEM has their own method of idelifying the susupicious/ abnormal user behaviour using their own method (Supervised/Un Supervised/ Other algorithm) ; hence request LIC to modify clause as below. The proposed solution should have the capacity to utilize machine learning algorithms, artificial intelligence and deep learning	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
34	Annexure F	UEBA Technical Specifications Point no 27		The proposed solution should have the capability to support a model that allows the output of one ML model to serve as an input for another ML model .	Custom build of ML Model/Algorithm use cases are specific for Business Analytics Platform and may not be applicable for Security Analytics Solution as asked in the RFP clause. . Hence request LIC to remove this clause	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
35	Annexure F	UEBA Technical Specifications Point no 41		The proposed solution should have the capability to support fine-tuning of various meta-data attributes of behaviour models, AI and ML models.	Fine tuning of ML models are not recommended in production environment because this may impact largely the ML algorithms in representating false/incorrect corelation outputs.Hence request LIC to remove this clause.	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
36	Section C:	47.e	43	LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and / or reduce the scope of the Services.	The RFP has different clauses for notice period for termination. Request LIC to confirm the notice period.	Please be guided by the RFP and the Corrigendum III
37	Section C:	55.I	46	LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, etc. cost to be quoted in the commercial bid. Any change in the scope beyond this 25% will be informed to the vendor in writing. If LIC wants to vary the Services:	Bidder understands that for all the line items (Sr no 1 to Sr no 8) as mentioned in the Annexure G - Commercial Template, bidder needs to factor additional 25% of buffer capacity for appliance/ License/ services	Please refer to the revised "Varying the Services-2"
38	Section F	1.e	92	In case of cancellation of orders due to delay in deliveries/installations or deficiency in services etc., besides the penalty being charged, the vendor may also be blacklisted by Life Insurance Corporation of India & may not be allowed to participate in any tenders for a period to be decided by LIC. Also, a lump sum amount as deemed fit by LIC (within the limits of PBG) will be imposed as penalty on the vendor to make good of losses suffered by LIC in terms of business loss and for making alternate arrangements.	Since there is a provision of Risk Purchase clause as part RFP we request LIC to define the limit for the Lump Sum charge being refffered/ mentioned here .	Please be guided by the RFP and the Corrigendum III
39	Section G	12	101	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.	Since there is a provision of Risk Purchase clause as part RFP we request LIC to define the limit for the Lump Sum charge being refffered/ mentioned here .	Please be guided by the RFP and the Corrigendum III
40				A) RFP Page 43- POint no 47e LIC may, at any time, by a prior written notice of one week, terminate the successful bidder and /or reduce the scope of the Services b) Page no 96 Point 8b : LIC may, at any time, by a prior written notice of 30 days, terminate the contract or reduce the scope of the Services	The termination criteria mentioned in the main RFP document under various sections is different. Considering the scope and sclae of project we sincerely request LIC to confirm the notice period of 90 days towards any such notice of termination.	Please be guided by the RFP and the Corrigendum III
41	Section 33	3 Limitation of Liability	36	Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	We sincerely LIC to consider an overall capping towards The cost of replacing or repairing defective equipment.	Please be guided by the RFP and the Corrigendum III
42	Section 33	3 Limitation of Liability	36	Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Conditions of Contract Clause, the vendor shall not be liable to LIC, whether in contract or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the bidder to pay liquidated damages to LIC; and the aggregate liability of the bidder to LIC, whether under the Contract, in tort or otherwise, shall not exceed the total value of purchase order(s) issued to the bidder provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.	We request clarity under the **"Conditions of Contract clause"** as defined here	Please be guided by the RFP and the Corrigendum III
43	Revised Section G Payment Terms			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	Request LIC to confirm on billing milestones & payment terms for the following line items of the Commercial Bid Sr. 9 - Direct Premium Support Sr. no 10- Custom Parser Sr. no 12- OEM Audit	Please refer to the revised "Payment Terms & Conditions-2"
44	Technocal Bid & Revised Technical Bid			Components provided by LIC	Technical bid as per RFP dated 18th Dec 2023 mentions that LIC will provide RHEL & MySQL licenses whereever necessary however Revised Technical Bid published on 17th March 2024 does not specify any details on OS & DB Provisioning. Request LIC to clarify	Please be guided by the RFP and the Corrigendum III
45	Revised Varying in the Services			Variations proposed by LIC – LIC reserves the right to initiate any change in the scope of contract. Vendors must factor in a maximum of 25% scope changes within the services, appliances, licenses, on-site support 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.	We request LIC to clarify if this variation of upto 25% is to be factored by bidder from day 1for all the solution components including Hardware,Software/Licenses,OS,Network.	Please be guided by the RFP and the Corrigendum III
46	Revised Annexure F			Should be on-premise for anti-APT or sandbox solutions :	Request LIC to clarify whether you need sandbox solutions in this RFP, this would be additional costing for all bidder, want to confirm the need of Sandbox at LIC	Please be guided by the RFP and the Corrigendum III
47	Revised Annexure F			This solution will allow deploying the client and protecting machines running on terminal servers	Request to share the OS type and versions of Terminal Server	Servers may be on Windows Server, RHEL , RHEL servers , SUSE Linux servers , IBM Linux servers , Orcale Linux servers

48	Revised Annexure F			The proposed solution shall provide comprehensive protection against exploits including MacOS,Linux (RHEL,Ubuntu & Cenos Flavours) and processes running Linux Container. 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.	These exploit techniques can be leverage by Endpoint Security & EDR for Windows OS Platform. Protection for linux & MacOS will be challenge for all the OEM vendors, we would request to modify this point and mention that these features are relevant to Windows OS not for Linux & MacOS or else request LIC to keep this point as Non-Mandatory clause	The point is mandatory as Linux OS is implemented in LIC in the following versions RHEL desktops and RHEL servers , SUSE Linux servers , IBM Linux servers , Orcale Linux servers
49	Revised Annexure F			Does **additional points which are added as new points from 98 to 102** are mandatory to comply for bidders or these are Good to have points from the solutions.	Request to LIC to provide clarifications on the points from 98 to 102, these additional points/features which are added newly are mandatory or good to have features in this RFP	The additionals points from 98 to 102 are mandatory
50	Revised Annexure F	NBAD - #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 P - 4 Gbps - West: Site Q - 4 Gbps - East: Site R - 4 Gbps - South: Site S - 4 Gbps - Site A - 4 Gbps - Site B - 1 Gbps - Site C - 1 Gbps - Site D - 8Gbps The cumulative bandwidth at the sites A , B , C and D can be arrived at by adding the bandwidth at Internet facing sites and MPLS colo sites The deployed solution for NBAD with visibility for end users should be in such a way that the WAN utilization across MPLS links is minimally impacted to the order of 5-10%.	As per earlier understanding there were 12 sites (Internet – 4 and MPLS – 8), accordingly we had prepared BOM with 12 Probes. With above addition after Corrigendum-3, we need to get a clarification about the number of sites and total throughput per site for optimized BoQ sizing. Our understanding is that LIC have 8 sites with following breakup, please confirm: - Sites A,B,C,D have both Internet and MPLS link - Sites P,Q,R,S have only MPLS link	Yes, the understanding of eight sites is correct.
51	Revised Annexure F	NBAD - #32		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 etc. are available	We perform enrichment via metadata, Username is not supported. So, request to either remove Username. Our understanding is that flow or packet enrichment is required with one OR more of the stated parameters, not necessarily all, please confirm.	Please be guided by the RFP and the Corrigendum III
52	Revised Annexure F	NBAD - #70		The ports of the proposed solution should support port speeds of 1G,10G,25G or 40G for both Copper and Fiber . Both SR and LR types must be supported . The number of ports should be factored as per the requirements of the RFP	Since this directly affects BOQ sizing and commercials, we request to provide exact number and type (Copper/Fiber) of ports required of each speed (1G/10G/25G/40G) so that all Bidders factor necessary hardware in their proposal. Our understanding is that packet or flow needs to be collected from more than four points at each site, so bidder is required to factor atleast one network packet broker at each site populated with 16 x 1G/10G Multimode Fiber Transceivers, please confirm.	Please factor Network Packet Broker , as per the number of ingestion points
53	Revised Annexure F	NBAD - #3		The solution should comply with industry standards, such as IRDAI, RBI, DPDP, SEBI, CERT-IN, IT ACT 2000, etc. and any law of the land applicable for LIC.	Our understanding is that we are referring to guidelines about data security and integrity. For example, our solution has features and functionality to provide Role based access, data masking, storing data locally, data encryption. Hope this will suffice LIC requirement, please confirm. Our understanding is that LIC is referring to guidelines about data security and integrity and to comply with this point LIC expects that the NBAD solution should have features and functionalities that provides Role based access, data masking, storing data locally, data encryption, please confirm.	Please be guided by the RFP and the Corrigendum III
54	Revised Annexure F	NBAD - #72		The OEM must have previously deployed the proposed solution of 10Gbps or its equivalent flows per second or packets per second in at least three PSU/Banks/Private Banks/BFSI institutions, in the last 3 financial year preceding to the date of this RFP.	We request a change in the language as follows: "The OEM must provide references for the proposed solution of 10Gbps or its equivalent flows per second or packets per second in at least three PSU Banks/Private Banks/BFSI institutions, in the last 3 financial year."	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
55	Revised Annexure F	PCAP - #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 Gbps - Site B: 500 Mbps - Site C : 1 Gbps - Site D: 3 Gbps MPLS Colo Sites: - North: Site P - 4 Gbps - West: Site Q - 4 Gbps - East: Site R - 4 Gbps - South: Site S - 4 Gbps - Site A - 4 Gbps - Site B - 1 Gbps - Site C - 1 Gbps - Site D - 8Gbps The cumulative bandwidth at the sites A , B , C and D can be arrived at by adding the bandwidth at Internet facing sites and MPLS colo sites The deployed solution for PCAP with visibility for end users should be in such a way that the WAN utilization across MPLS links is minimally impacted to the order of 5-10%.	As per earlier understanding there were 12 sites (Internet – 4 and MPLS – 8), accordingly we had prepared BOM with 12 Probes. With above addition after Corrigendum-3, we need to get a clarification about the number of sites and total throughput per site for optimized BoQ sizing. Our understanding is that LIC have 8 sites with following breakup, please confirm: - Sites A,B,C,D have both Internet and MPLS link - Sites P,Q,R,S have only MPLS link	Yes, the understanding of eight sites is correct.
56	Revised Annexure F	PCAP - #28		The solution should have the ability to selectively store packets captured in an external storage or store in cloud by following industry best practice and any other applicable law of the land for data security.	Request to change this as follows: "The solution should have the ability to selectively store packets captured in an internal/external storage or store in cloud by following industry best practice and any other applicable law of the land for data security." Our solution includes internal storage that can be used to store packet level data as per LIC's packet like data retention requirement. Our extended storage unit (ESU) is an optional component that can be provided if packet like data retention increases in future. With current packet like data retention requirements we can meet the requirements with internal storage, hope this is acceptable to LIC, please confirm.	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
57	Revised Annexure F	PCAP - #36		The solution should allow playback of captures to verify the effectiveness of remediation measures and security enforcement tools.	Need clarification about requirement Our understanding of this point is that PCAP solution should have features like HTTP Session Reconstruction, Replay HTTP sessions on packets at capture points before and after security enforcement tools (example before and after firewall) that helps to verify effectiveness of remediation measures, please confirm.	Please be guided by the RFP and the Corrigendum III
58	Revised Annexure F	PCAP - #46		The vendor needs to be responsible for ensuring that the implemented solution complies with the specifications detailed in SEBI, IRDAI, PCI DSS, CERT-IN, IT ACT 2000, DPDP 2023, RBI etc. and any other law of the land applicable for LIC.	Our understanding is that we are referring to guidelines about data security and integrity. For example, our solution has features and functionality to provide Role based access, data masking, storing data locally, data encryption. Hope this will suffice LIC requirement, please confirm. Our understanding is that LIC is referring to guidelines about data security and integrity and to comply with this point LIC expects that the PCAP solution should have features and functionalities that provides Role based access, data masking, storing data locally, data encryption, please confirm.	Please be guided by the RFP and the Corrigendum III
59	Revised Annexure F	PCAP - #56		The ports of the proposed solution should support port speeds of 1G,10G,25G or 40G for both Copper and Fiber . Both SR and LR types must be supported . The number of ports should be factored as per the requirements of the RFP	Since this directly affects BOQ sizing and commercials, we request to provide exact number and type (Copper/Fiber) of ports required of each speed (1G/10G/25G/40G) so that all Bidders factor necessary hardware in their proposal. Our undertsand is that packet or flow needs to be collected from more than four points at each site, so bidder is required to factor atleast one network packet broker at each site populated with 16 x 1G/10G Multimode Fiber Transceivers, please confirm.	Please factor Network Packet Broker , as per the number of ingestion points

60	Revised Annexure F	PCAP - #3		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 to change this as follows: "The packet/flow (no sampling) captured at line rate for all sensors shall be stored for 5 days and metadata to be stored for 180 days . 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 netflow/packet analysis, host analysis, TCP analysis etc. Accordingly, bidder shall provision the required storage capacity built within the proposed PCAP appliance." Our understanding for 5 days packet level data storage is considering that every day there will be about 12 hours of busy traffic and 12 hours of non-busy/idle traffic, please confirm.	Please factor for 15 busy hours and nine normal hours
61	Revised Section G - Payment Terms & Conditions	Revised Section G - Payment Terms & Conditions	1	45% of cost - Delivery of all in-scope software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC.	We request to change the payment terms 70% of cost - Delivery of all in-scope software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC.	Please be guided by the RFP and the Corrigendum III
62	Revised Section G - Payment Terms & Conditions	Revised Section G - Payment Terms & Conditions	1	40 % of cost of items listedb under SN 2 and 25% of the cost of items under SN1 in this table - Installation and integration, initial OEM audit and acceptance testing as per scope of work.	We request to change the payment terms 20 % of cost of items listed in SN 2 and SN1 in this table. - After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s	Please be guided by the RFP and the Corrigendum III
63	Revised Section G - Payment Terms & Conditions	Revised Section G - Payment Terms & Conditions	1	10 % of cost of items listed in SN 2 and 5% of the cost items under SN1 in this table - 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 be guided by the RFP and the Corrigendum III
64	Eligibility Criteria Clause 8 -			**Eligibility Criteria Clause 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 5000 endpoints.	**Change requested -** Instead of proposed, requesting you to make it The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported ANY EDR OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 5000 endpoints. **Justification** 1. EDR being a component of large SoC RFP, bidder's having extensive experience in implementing and managing SoC would not necessarily have too much experince on EDR. 2. EDR as a technology is almost similar across all the OEM's so experince of having implemented one EDR would not limit bidder's to only that EDR but as the technology is almost similar they can technically implement other soluitions as well 3. Hence the request to remove 'proposed OEM' word to 'any OEM', so that bidder's would have the choice to suggest and implement out of all the good EDR solutions available in the market.	Please be guided by the RFP and the Corrigendum III
65	Query for EDR against the clause of on-prem sandboxing				As to combat ever evolving threats you have ensured that EDR should be hybrid, requesting you to allow the same for sandboxing as well. As in on-prem you can evaluate the file only in static and dynamic stage but in cloud an unknown potential malicious file can be detonated in using multiple analysis including static,dynamic, recursive, memory fingerprinting & leverage additional compute for detailed AI/ML analysis for a more accurate & comprehensive outcome.	Please be guided by the RFP and the Corrigendum III
66	Revised Annexure F: Technical Compliance	NBAD Technical Specifications	Additional point as per PreBid Query Point #71	71. it should be a dedicated solution **delivering all PCAP** specifications and use cases mentioned above and should not be subset capability of SIEM or any other solution	Request this to be removed from NBAD section since its applicable to PCAP solution; also #17 of NBAD specs conveys the same point	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
67	Revised Annexure F _ Technical Specifications	SIEM Technical Specifications Sr No 111	NA	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 3000 logs in the last 3 financial year preceding to the date of this RFP.	We understand that in line with the Technical Specifications for SOAR, NBAD as mentioned in Annexure F; the clause is applicable for OEM and not the vendor/ bidder. We request LIC to revise the clause as below. The OEM must have previously deployed the SIEM solution in at least three PSU/Banks/Private Banks/BFSI institutions, each with a minimum 3000 logs in the last 3 financial year preceding to the date of this RFP.	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
68	Revised Annexure F _ Technical Specifications	EDR Technical Specifications Sr No 100	NA	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..	The above point refers to protecting processes running in Linux Containers. We would like to know if any Linux containers are running in the LIC environment and, if so, how many. Also, please note that "Container Security" is a separate solution and not part of the EDR functionality. Please advise if we should quote Container Security licenses or not. Awaiting for your clarifications at the earliest	At present there are no Linux Containers in the LIC environment and 'Container Security' as a separate feature is not required now and Container Security licenses are not to be quoted. The bidder can provide information on whether the proposed OEM products support this feature
69	Additional Point	NA	NA	Resources to manage the underlying infra	Since the bidder has to provide infra for the proposed solution, request LIC to consider dedicated resources to manage the underlying Infra and incorporate as a separate line item in the commercial sheet	Please refer to the revised "Section E: Scope of Services-2"
70	Additional Point	NA	NA	Ticketing and Monitoring Tool	As per the pre-bid response, LIC mentioned that LIC is in the process of procuring ticketing tool. Considering the timegap which may arise between RFP closures, request LIC to confirm whether bidder has to provide monitoring and ticketing tool for availability and SLA tracking for a year or two	Please refer to the revised "Section E: Scope of Services-2"
71	Penalties on Non-Performance of SLA during contract period:	SIEM		Critical events should be notified within 30 minutes of the event identification and resolution within 1 hour. High priority events should be notified within 1 hour of the event identification and resolution within 4 hours.Medium priority events should be notified within 4 hours of the event identification and resolution within 2 business days.Low priority events should be notified within 12 hours of the event identification and resolution within 5 business days.	Need to remove Resolution SLA for Monitoring	Please be guided by the RFP and the Corrigendum III
72	Project Timelines	SIEM		Phase 1 : Implementation of SIEM, SOC, SOAR and UEBA T + 32 Weeks	Need To change in timelines from for T+45 weeks	Please be guided by the RFP and the Corrigendum III
73	Project Timelines	NBAD and PCAP		Phase 3 : Implementation of PCAP and NBAD T + 8 Weeks	Need To change in timelines from for T+16 weeks	Please be guided by the RFP and the Corrigendum III
74	Eligibility Criteria Clause 8 -			Eligibility Criteria Clause 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 5000 endpoints.	We hope this message finds you well. I am writing to request a change to a specific clause in the Request for Proposal (RFP) document Life Insurance of India - RFP/ Tender for onboarding System Integration (SI)to implement Threat Detection and Incident Response Tool (Annexure -C). The clause in question states that "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 5000 endpoints." Request to amend this clause as : We would like to propose an amendment to this clause to read as follows: "The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported EDR(Technologies) by any OEM to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 5000 endpoints." We believe that this change will provide more	Please be guided by the RFP and the Corrigendum III
75					1.Point 1 - The mentioned capacity of 3862 GB per day = 80000 EPS calculates to ~600 event byte size which is significantly low. 2.Considering the environment it would need a higher license than factored. Typically for such workload types we consider 1000 event bytes. The cloud-heavy environment would go up to 1500+ bytes per event. 3.Request LIC to revisit this and consider adding the byte size for better estimations & allow us to quote. Also, our solution neither blocks the search ability nor stops the detection when the license limitation is applied.	Please be guided by the RFP and the Corrigendum III
76	Revised Annexure F _ Technical Specifications	SIEM Technical Specifications Sr No 14, 15, 16	NA		The mentioned architecture in point no. 14 with dual log forwarding (active-active setup) is supported & will be configured using our tool. Request to make points 15 & 16 optional as long as the SIEM data is available at both main sites and it can sustain a site/component level failure & also ensure the data availability at the alternate site.	Please be guided by the RFP and the Corrigendum III

77	Revised Annexure F _ Technical Specifications	SIEM Technical Specifications Sr No 50	NA		The correlation & threat hunting purpose can be met with the event and flow data collected by SIEM from NBAD, UBA. However, the SOAR will log the required offense & findings consuming the correlated data from the SIEM alert. Hope this is acceptable	Please be guided by the RFP and the Corrigendum III
78	Revised Annexure F _ Technical Specifications	SIEM Technical Specifications Sr No 56	NA		This point should be made optional (30 seconds with 1000 results at least).	Please be guided by the RFP and the Corrigendum III
79	Revised Annexure F _ Technical Specifications	SIEM Technical Specifications Sr No 61	NA		TIP - It is understood that LIC will provide the TIP for necessary correlation	Please be guided by the RFP and the Corrigendum III
80	Revised Annexure F _ Technical Specifications	SOAR Technical Specifications Sr No 12	NA		Need an exception specifically for the out of box integration of "Forensic tools"	Please be guided by the RFP and the Corrigendum III
81	Annexure F	CTI		The vendor needs to be responsible for ensuring that the implemented platform complies with the specifications detailed in ISO 27001, ISO 27002, SEBI, IRDAI, PCI DSS, IT Ac 2000, DPDP 2023, etc. and any other law of the land applicable for LIC.	Kindly remove this clause as the Cyber Threat Intell will be provided as a feed and these feeds would be directly ingested into the SIEM platform.	Please be guided by the RFP and the Corrigendum III
82	Annexure F	CTI		The vendor must provide adequate support, including regular updates and patches for security vulnerabilities. The vendor shall apply upgrades and patches to the platform and its related components as needed to maintain their effectiveness and security. Patches could be N-1 however if major vulnerabilities are identified with exploit and severity as high or critical, immediate patching is necessary.	Kindly remove this clause as the Cyber Threat Intell will be provided as a feed and these feeds would be directly ingested into the SIEM platform.	Please be guided by the RFP and the Corrigendum III
83	Annexure F	CTI		The solution should support (but not limited to) RADIUS, Active Directory, LDAP, PAM or SSO for authentication.	Kindly remove this clause as the Cyber Threat Intell will be provided as a feed and these feeds would be directly ingested into the SIEM platform.	Please be guided by the RFP and the Corrigendum III
84	Annexure F	CTI		The platform should allow to retrieve system logs for diagnostic purposes or for troubleshooting.	Kindly remove this clause as the Cyber Threat Feeds would be directly ingested into the SIEM platform. Also the Cyber Threat Feeds do not retrieve any logs for any troubleshooting. These are just feeds integrated via STIX/TAXII mode	Please be guided by the RFP and the Corrigendum III
85	Annexure F	CTI		The platform should have native capability for automated backup or recovery process.	Kindly remove this clause as the Cyber Threat Feeds would be directly ingested into the SIEM platform. Also the Cyber Threat Feeds do not have any bakcup/restore process. These are just feeds integrated via STIX/TAXII mode	Please be guided by the RFP and the Corrigendum III
86	Annexure F	CTI		The platform should possess the capability to promptly notify designated personnel or teams of LIC in the event of any component failure. This notification mechanism shoul be real-time and capable of delivering alerts via multiple channels, such as email, SMS, or integration with incident management platforms	Kindly remove this clause as the Cyber Threat Feeds would be directly ingested into the SIEM platform. There is no failure of the palatform as such. These are just feeds integrated via STIX/TAXII mode	Please be guided by the RFP and the Corrigendum III
87	Annexure F	CTI		The platform must offer support for an automated health check mechanism that continuously monitors the operational status and performance of all system components. These health checks should encompass critical aspects of system functionality, including hardware, software, network connectivity, and service availability such as but not limited to, CPU usage spikes, RAM usage spikes, etc.	Kindly remove this clause as the Cyber Threat Feeds would be directly ingested into the SIEM platform. This is via direct integration into the SIEM platform. These are just feeds integrated via STIX/JSON mode	Please be guided by the RFP and the Corrigendum III
88	Annexure F	CTI		The health check mechanism should be configurable and adaptable to specific monitoring requirements and thresholds, allowing for proactive issue identification.	Kindly remove this clause as the Cyber Threat Feeds would be directly ingested into the SIEM platform. This is via direct integration into the SIEM platform. These are just feeds integrated via STIX/JSON mode	Please be guided by the RFP and the Corrigendum III
89	Annexure F	CTI		The vendor should monitor and analyze CPU usage to ensure efficient resource utilization and detect anomalies that might indicate performance issues or potential security threats.	Kindly remove this clause as the Cyber Threat Feeds would be directly ingested into the SIEM platform. This is via direct integration into the SIEM platform. These are just feeds integrated via STIX/JSON mode	Please be guided by the RFP and the Corrigendum III
90	Annexure F	CTI		The platform should support custom indicators such as (but not limited to) Credit cards, Mobile numbers, Aadhar card ID numbers, etc.	Cyber Threat Feeds do not PII data. They contain majorly IOC, IPs, Hash, URL, Domains. Kindly remove this clause	Please be guided by the RFP and the Corrigendum III
91	Annexure F	CTI		The platform should be able to support reliable, actionable feeds for such as (but not limited to): a. IP Addresses b. Domain Names c. Hashes d. E-Mails e. File Names f. Blacklists g. Malware Indicators h. Autonomous System Numbers i. Mutex j. Win Registry Key k. Port i. HTTP Session Object m. User-Agent	They contain majorly IOC, IPs, Hash, URL, Domains. Kindly modify this clause	Please be guided by the RFP and the Corrigendum III
92	Annexure F	CTI		The platform should have custom indicator attributes which can be shared with subsidiaries.	The threat feeds are of global nature. They cannot be custom driven for LIC	Please be guided by the RFP and the Corrigendum III
93	Annexure F	CTI		The platform should be capable of mapping the TTP to APT Groups to zero down the APT groups targeting LIC.	This is a manual activity and not part of CTI	Please be guided by the RFP and the Corrigendum III
94	Annexure F	CTI		The platform should support ML-based automated correlation between various objects of the received threat intel.	This is part of SIEM. Please remove this clause	Please be guided by the RFP and the Corrigendum III
95	Annexure F	CTI		The platform should have capabilities to automatically harness the critical IOC and map it back to MITRE ATT&CK navigator relevant TTP.	This is part of SOC management. Kindly remove this clause	Please be guided by the RFP and the Corrigendum III
96	Annexure F	CTI		The platform should support interactive analysis to mark the severity and risk, track and add notes/ comments for the indicators which can be shared with other analysts.	This is part of SOC management. Kindly remove this clause	Please be guided by the RFP and the Corrigendum III
97	Annexure F	CTI		The platform should have a feature to auto generate executive reports for higher management.	Reports will be generated via SIEM console. Kindly remove this clause	Please be guided by the RFP and the Corrigendum III
98	Annexure F	CTI		The reports generated in the platform should provide technical intelligence such as (but not limited to) vulnerabilities, network, security risk/ malware files, etc.	The technical intelligence is presented in the form of Threat Advisory, not reports. Kindly modify the clause	Please be guided by the RFP and the Corrigendum III
99	Annexure F	CTI		The platform should have advanced auditable logs which show each and every individual's log such as users, subscriber, polled sources with the data received etc., and a tab of all the input and output data flow.	Kindly remove this clause as the Cyber Threat Intell will be provided as a feed and these feeds would be directly ingested into the SIEM platform.	Please be guided by the RFP and the Corrigendum III
100	Annexure F	CTI		The platform should provide features to measure ROI of threat intel operations such as the amount of data ingested, acted upon, and disseminated. It should make it possibl for the executives to measure the entire ROI of the procedure.	There is no way to calculate the ROI. Kindly remove this clasue	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
101	Annexure F	CTI		The platform should have capabilities to automatically harness the critical IOC and map it back to MITRE ATT&CK navigator relevant TTP.	The IOC is only an indicator. This is not a action against which we can map it to the MITRE ATT&CK framework. Kindly remove this clause	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
102	Annexure F	CTI		The platform should be capable of integrating with existing internal security/network devices such as (but not limited to) SIEM, IDS, IPS, Anti-APT solution, Firewall, UEBA, etc.	Ideally the Threat Feeds should be integrated only with SIEM to avoid duplication at the log sources level. Kindly modify the clause " The platform should be capable of integrating with SIEM and its relevant components"	Please be guided by the RFP and the Corrigendum III
103	Annexure F	NBAD		The solution should be a dedicated behaviour analytics solution delivering advanced Network Detection & Response (NDR) use cases and not a subset capability of SIEM or PCAP solution.	We request to delete PCAP from this spec and change as follows: "The solution should be a dedicated behaviour analytics solution delivering advanced Network Detection & Response (NDR) use cases and not a subset capability of SIEM Solution. For PCAP and NBAD solution, Application and Sensor / Probe may store and process packet / flow on same device. If it does not have these capabilities on the same device, the bidder shall propose two separate dedicated devices."	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
104	Annexure F	NBAD		The OEM must have previously deployed the proposed solution of 10Gbps or its equivalent flows per second or packets per second in at least three PSU/Banks/Private Banks/BFSI institutions, in the last 3 financial year preceding to the date of this RFP.	We request to change this as follows: "The OEM must have previously deployed the proposed solution of 10Gbps or its equivalent flows per second or packets per second in at least two Government/PSU/Banks/Private Banks/BFSI institutions, in the last 3 financial year preceding to the date of this RFP."	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
105	Annexure F	PCAP		It should be a dedicated solution delivering all PCAP specificationsand use cases mentioned above and should not be a subset capablity of SIEM or any other solution.	We request to change this as follows: "It should be a dedicated solution delivering all PCAP specificationsand use cases mentioned above and should not be a subset capablity of SIEM or any other solution. For PCAP and NBAD solution, Application and Sensor / Probe may store and process packet / flow on same device. If it does not have these capabilities on the same device, the bidder shall propose two separate dedicated devices."	Please refer to the revised "Revised Annexure F – Technical Compliance-2"
106	Annexure F /SoW	PCAP/SoW		The vendor must address secure storage options and should have data storage duration and capacity to ensure that packet captured at line rate by sensors at each site shall be stored for 7 days and metadata to be stored for 1 year.	As per Revised Technical Specifications, we request you to change this as follows: "The vendor must address secure storage options and should have data storage duration and capacity to ensure that packet captured at line rate by sensors at each site shall be stored for 5 days and metadata to be stored for 180 days."	Please refer to the revised "Section E: Scope of Services-2"