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

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	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"
3		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"
4		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"
5		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"
6	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"
7	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"
8	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"
9	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).
10	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).
11	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"
12	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"
13	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"
14	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"
15	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 behavour 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"
16	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"
17	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"
18	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"

19	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"
20	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
21	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
22	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
23	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.
24	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
25	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"
26	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.
27	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"
28	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
29	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
30	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"
31	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"
32	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
33	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"
34	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"
35	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"
36	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"

37	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"
38	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"
39	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"
40	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"