Life Insurance Corporation of India – RFP/Tender for onboarding System Integrator (SI) to Implement Threat Detection and Incident Response Tools - Response to Pre-Bid queries-2 (LIC-CO/IT-BPR/NW/RFP/2023-2024/TDIR dated 18 December 2023)

S.No.	RFP Section	Sub-Section	Pg No	RFP Clause	Bidder Query	LIC Response
1	Annexure C - Minimum Eligibility Criteria Clause Number 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. The proposed OEM-product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization or in one organization for 1 lakh users 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 with at least 4000 endpoints. The proposed OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization or in one organization for 1 lakh users during the last 3 years preceding to the date of the RFP OR The Bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported ~~proposed EDR OEM~~ to at least 01 (one) client in PSU/Government/Private/BFSI Sector in India with at least 5000 endpoints. The OEM product for EDR should have been successfully running in minimum three organizations for minimum 30000 users in each organization or in one organization for 1 lakh users during the last 3 years preceding to the date of the RFP	Please refer to "Revised Annexure C and Eligibility Criteria-3"
2	EDR Clause Number 1 and 2			The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints should be an On-prem solution for EPP component: -should be On-prem for anti APT or sandboxing solution -should be Hybrid/On-prem solution for EDR component with a broker server.The Hybrid EDR componnet of solution should be hosted on Cloud based in India at DC and DR. Solutions at DC and DR to be 100% bidirectional replica. The following points should be ensured by the bidder w.r.t. the cloud components of the proposed solution: No endpoint, server or network component of LICs intranet should connect to the CSP cloud directly. They should be connected with LIC's on-premise server which in-turn will connect to CSP cloud through LIC's proxy. The proposed solution should be deployed in hybrid model with components, features and functionalities through LIC On-premise DC / DR and MeitY compliant Cloud Data Center hosted in India.	The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints should be an On-prem solution for EPP component: -should be **Hybrid/**On-prem for anti APT or sandboxing solution -should be Hybrid/On-prem solution for EDR component with a broker server.The Hybrid EDR componnet of solution should be hosted on Cloud based in India at DC and DR. Solutions at DC and DR to be 100% bidirectional replica. The following points should be ensured by the bidder w.r.t. the cloud components of the proposed solution: No endpoint, server or network component of LICs intranet should connect to the CSP cloud directly. They should be connected with LIC's on-premise server which in-turn will connect to CSP cloud through LIC's proxy. The proposed solution should be deployed in hybrid model with components, features and functionalities through LIC On-premise DC / DR and MeitY compliant Cloud Data Center hosted in India.	Please refer to "Revised Annexure F – Technical Compliance-3"
3	EDR Clause Number 70			The solution must block the user from browsing to a known malicious URLs or domain	The ~~solution must block the user from browsing to a known malicious URLs or domain~~ **proposed solution shall be able to prevent all the malicious activities when a user clicks on any bad URLs**	Please refer to "Revised Annexure F – Technical Compliance-3"
4	Annexure-F			The solution must support up to 30000 Windows OS endpoints/clients and 45000 RHEL OS endpoints should be an On-prem solution for EPP component: -should be On-prem for anti APT or sandboxing solution -should be Hybrid/On-prem solution for EDR component with a broker server. The Hybrid EDR component of solution should be hosted on Cloud based in India at DC and DR. Solutions at DC and DR to be 100% bidirectional replica. The following points should be ensured by the bidder w.r.t. the cloud components of the proposed solution: No endpoint, server or network component of LICs intranet should connect to the CSP cloud directly. They should be connected with LIC's on-premise server which in-turn will connect to CSP cloud through LIC's proxy. The proposed solution should be deployed in hybrid model with components, features and functionalities through LIC On-premise DC / DR and MeitY compliant Cloud Data Centre hosted in India	We seek your clarification on the below: 1. as per the RFP, EPP has to be on-prem 2. Existing EPP solution Trend Micro Apex One for 30000 Windows and Trend Micro Deep security for 65000 valid till December 2025 and 1433 Deep security licenses valid till June'26 3. RFP also mentions that co-exist of EDR with current EPP solution. considering all the above points together, OEM/bidder is not getting enough clarity whether EPP licenses to be quoted along with EDR for current RFP tenure Requesting you to specifically callout bidder has to propose on-prem EPP solution in this RFP along with EDR. Please do mention it in the commercial format G	Please refer to "Revised Annexure F – Technical Compliance-3"
5	EDR Section			The solution must support additionally up to 4000+ Servers and should be an On-prem solution for EPP component -should be On-prem for anti APT or sandboxing solution -should be Hybrid/On-prem solution for EDR component with a broker server, The Hybrid EDR component of solution should be hosted on Cloud based in India at DC and DR. Solutions at DC and DR to be 100% bidirectional replica . The following points should be ensured by the bidder w.r.t. the cloud components of the proposed solution: No endpoint, server or network component of LICs intranet should connect to the CSP cloud directly. They should be connected with LIC's on-premise server which in-turn will connect to CSP cloud through LIC's proxy. The proposed solution should be deployed in hybrid model with components, features and functionalities through LIC On-premise DC / DR and MeitY compliant Cloud Data Centre hosted in India	We seek your clarification on the below: 1. as per the RFP, EPP has to be on-prem 2. Existing EPP solution Trend Micro Apex One for 30000 Windows and Trend Micro Deep security for 65000 valid till December 2025 and 1433 Deep security licenses valid till June'26 3. RFP also mentions that co-exist of EDR with current EPP solution. considering all the above points together, OEM/bidder is not getting enough clarity whether EPP licenses to be quoted along with EDR for current RFP tenure Requesting you to specifically callout bidder has to propose on-prem EPP solution in this RFP along with EDR. Please do mention it in the commercial format G	Please refer to "Revised Annexure F – Technical Compliance-3"
6	Point no 1 Annexure-F EDR Section			current commercial format EDR Solution inclusive of all components (software, licenses, other equipment's, etc. and its implementation) as per technical specifications	proposed commercial format : On-Prem EPP Solution inclusive of all running components (software, licenses, other equipment's, etc. and its implementation) as per LIC requirement EDR Solution inclusive of all components (software, licenses, other equipment's, etc. and its implementation) as per technical specifications	The Commercial bid line item for EDR should be inclusive of all components EPP, Sandboxing, EDR and their software, licenses, hardware,other equipment's, etc. and its implementation).Detailed breakup to be given separately
7	Revised Section E – Scope of Work Services - 2	C. Security Information and Event Management (SIEM) – point vi		The provision for creation of custom parsers (300 nos.) will be carried out by the OEM and they should transfer the logic of making it to the successful bidder. The unit price of the custom parsers will be derived from the commercial sheets on a pro-rata basis and this rate will be frozen for 5 years. However, the payment for custom parsers will be based on the actual parsers deployed by LIC. LIC also reserves the right to increase the requirement of custom parsers as per the actual requirement.	The provision for creation of custom parsers (300 nos.) will be carried out by the OEM / partners and they should transfer the logic of making it to the successful bidder. The unit price of the custom parsers will be derived from the commercial sheets on a pro-rata basis and this rate will be frozen for 5 years. However, the payment for custom parsers will be based on the actual parsers deployed by LIC. LIC also reserves the right to increase the requirement of custom parsers as per the actual requirement.	Please refer to "Revised Section E - Scope of Services-3"

8	Revised Annexure F – Technical Compliance-2	14		The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be available on the connectors/log collectors. It should be configurable as per requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.	Point 14 - The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time for running the searches. The dual forwarding or synchronisation feature should be available on the connectors/log collectors/log processors. It should be configurable as per requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.	Please be guided by the RFP
9	Revised Annexure F – Technical Compliance-2	15		The proposed solution must support single site or multiple site clustering allowing data to be replicated across ~~the peer's nodes and across multiple sites with near zero RTO & RPO.~~ ~~Use Case: In future if it is decided to run both DC & DR Active-Active, then the entire cluster should work as single cluster which is deployed in DC & DR.~~	The proposed solution must support single-site or multiple-site clustering allowing data to be replicated across the DC & DR site.	Please be guided by the RFP
10	Revised Annexure F – Technical Compliance-2	16		The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level ~~with near zero RPO and RTO~~. Like big data platforms, the solution should also allow admin to decide on the replication factor within DC and replication factor for DR. DR should always be active ~~and should be updated with artifacts for any incident analyst is working on~~.	The proposed solution must support the data replication natively without relying on other third-party replication technologies on the operating system or storage level. Like big data platforms, the solution should also allow the admin to decide on the replication factor within DC and the replication factor for DR. DR should always be active for running searches and should be updated with artifacts for any incident analyst is working on the centralized case management system.	Please be guided by the RFP
11	Revised Annexure F – Technical Compliance-2	50		The proposed solution should act as common data lake for correlation between (but not limited to) SOAR, NBAD, UEBA and threat hunting, etc.	The proposed solution should act as common data lake OR A PLATFORM for correlation OR SEARCHING between (but not limited to) DATA RESIDING IN SOAR, NBAD, UEBA and threat hunting, etc.	Please refer to "Revised Annexure F – Technical Compliance-3"
12	Revised Eligibility Criteria-2 and Annexure C-2	Revised Annexure C and Eligibility Criteria,Point No.5	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. During the last 5 years preceding to the date of the RFP, the proposed OEM product for SIEM should have been successfully running in minimum two organizations with minimum 500 branches and 60,000 EPS / 2897 GB per day, in each of the organization.	We request you to amend the clause As "During the last 5 years preceding to the date of the RFP, the proposed OEM product for SIEM should have been successfully running in minimum two organizations with 60,000 EPS / 2897 GB per day, in each of the organization" Sir, By keeping the branch numbers as 500 branches,It is restricting major MII Indian companies from participating.We have deployed our solutions in Multi-locations and Multi-sites which includes deployment of more than 1,00,000 EPS in critical organisations.So we kindly request you to remove the statement "500 branches".Please help us address this query to inolve a healthy participation which will help more Technically Qualified Indian Make in India Starups such as ours to participate in this opportunity	Please refer to "Revised Annexure C and Eligibility Criteria-3"