


Replies to Prebid Queries of Gem bid ref. no. GEM/2022/B/2885701 dated 27/12/2022 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach and Attack Simulation Solution in Canara Bank for 3 years

| Sl. No. | Gem Bid Clause | Gem Bid Clause/Technical Specification | Bidder's Query | Bank's Reply |
|---------|--|---|---|--|
| 1 | Annexure-5 Pre-Qualification Criteria | <p>Criteria</p> <p>The bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020.</p> <p>Documents to be submitted for Compliance</p> <p>Certificate of local content to be submitted as per Annexure-6 and Annexure-7 as applicable.</p> | <p>We request to remove this clause</p> | <p>Bidder has to comply with RFP terms and condition.</p> <p>Bidder to refer https://dptl.gov.in/public-procurements for complete details on Public Procurement (Preference to Make in India).</p> |
| 2 | 20. Payment terms | <p>Escrow Payment</p> <p>10% of the payment will be released after signing Escrow Agreement and depositing of source code.</p> | <p>This clause needs to be removed as this is not a custom made software especially for CANARA Bank</p> | <p>Kindly refer to Corrigendum-2.</p> |
| 3 | Annexure-1 Scope of Work | <p>The solution must have the capability to simulate inside-out and outside-in attack. The solution should have the capability to instrument attacks on each of the below vectors:</p> <ul style="list-style-type: none"> Endpoint based attacks Network based attacks Email based attacks Proxy Attacks on cloud infrastructure <p>The list is illustrative, not exhaustive</p> | <p>You have mentioned cloud infrastructure. Kindly clarify what type of cloud? AWS, AZURE, Or just a VM on cloud. Kindly mention what kind of attacks you expect on respective cloud environment.</p> | <p>The details will be shared to selected bidder.</p> |
| 4 | Annexure-2 Technical and Functional Requirements | <p>47. The solution should have the capability to integrate and consume threat feeds such as IOCs, IPs etc. from third party intelligence/regulators like CSITE, CERT-IN, etc.</p> | <p>In what form these feeds will be received? If third party refuse to directly integrate then what?</p> | <p>Bidder has to comply with RFP terms and condition.</p> |
| 5 | Annexure-2 Technical and Functional Requirements | <p>54. The solution should have the capability of Auto discovering the security technologies deployed in the infrastructure including but not limited</p> | <p>This is not a job of BAS tool. This is job of defensive tool - Hence remove</p> | <p>Kindly refer to Corrigendum-2.</p> |



| | | | | |
|---|---|---|---|--|
| | | to SIEM, Proxy, IDS, Firewall, DLP, Endpoint Protection and malware analysis tools. | | |
| 6 | Annexure-2 Technical and Functional Requirements | 58. The solution should have the capability of providing Detect, alerting analysis including SIEM Correlation rule analysis. | This is not job of BAS tool. This is a job of defensive tool and not offensive tool - Hence remove | Bidder has to comply with RFP terms and condition. Bidder has to suggest SIEM rules for detecting such attacks. |
| 7 | Annexure-2 Technical and Functional Requirements | 65. The bidder should propose an on - premise solutions and no information should be sent outside the organization, unless it has got dependency for testing any external testing component, with specific consent of the bank. Additionally, the solution should have no dependency on the cloud for the on-prem deployment except for carrying out the intended activity, the updates, upgrades for the solution and security contents. | In this scenario how can one do Outside in Attack? Infiltration attacks? You need a component outside to outside-In attack. How can one do inside-out attack like exfiltration? Kindly change the clause to Hybrid deployment | Kindly refer to Corrigendum-2 for the amended clause. |

Date: 20/01/2023
Place: Bangalore


 Deputy General Manager
