

THE PUNE DISTRICT CENTRAL CO-OPERATIVE BANK LTD.



**INFORMATION TECHNOLOGY DEPARTMENT
HEAD OFFICE: Pune District Central Co-op. Bank Ltd.,
4 B , B. J. Road, Pune.
Pin – 411001**

RFP No.: PDCC/IT-Tender/2024-25/002

Date: 19.08.2024

**Corrigendum – 1
For
REQUEST FOR PROPOSAL (RFP) FOR
Selection of Service Provider for Cyber Security Operation Center
on
Hybrid Model**



Table of Contents

1. Extension of Dates for Submission and Opening of Bids3

2. Modification in RFP Clause.....3



Corrigendum –1.0 For Request for Proposal (RFP) For Selection of Service Provider for Cyber Security Operation Center on Hybrid Model

In reference to the Request for Proposal (RFP) For Selection of Service Provider for Cyber Security Operation Center on Hybrid Model, reference no RFP No.: PDCC/IT-Tender/2024-25/002 dated 19/08/2024, all are advised to note following:

1. Extension of Dates for Submission and Opening of Bids

| Activity | Existing Dates | Revised Dates |
|--|------------------------------|------------------------------|
| Last Date, Time and Place for submission of Bid | 02.09.2024, upto 15:00 hours | 10.09.2024, upto 15:00 hours |
| Date and Time of Eligibility cum Technical Bid opening | 02.09.2024, 16:30 hours | 10.09.2024, 16:30 hours |

2. Modification in RFP Clause

| Sr. No | Section Number | Page Number | Point Number | Original Clause | PDCC Bank Response |
|--------|--|-------------|--|---|---|
| 1 | 3.1 Eligibility Criteria | 20 | C. EXPERIENCE & SERVICE CAPABILITY | Service Model: The bidder should provide the CSOC services from MeitY empaneled Government community cloud infrastructure i.e., SIEM/SOAR/ DLP/PIM etc., Solution should be hosted with MeitY empaneled government community cloud. | Revised Clause: Service Model: The bidder should provide the CSOC services from MeitY empaneled cloud infrastructure i.e., SIEM/SOAR/ DLP/PIM etc., Solution should be hosted with MeitY empaneled cloud. |
| 2 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for SOAR - Sl. No. 2 | SOAR must be integrated platform with SIEM on same user interface | Revised Clause: SOAR must be integrated platform with SIEM to comply with minimum requirement mentioned in RFP. |
| 3 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for SOAR - Sl. No. 3 | SOAR solution should collect real time global threat intel data, dedupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner | Revised Clause: SOAR solution should collect real time global threat intel data, dedupe and process threat intelligence in a holistic and actionable manner. |
| 4 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NAC- Sl. No. 23 | The solution should support Microsoft NAP and Trusted Computing Group. | Please consider the clause as deleted |
| 5 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NBAD- Sl. No. 3.13 | The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL. | Revised Clause: The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd. |

| Sr. No | Section Number | Page Number | Point Number | Original Clause | PDCC Bank Response |
|--------|--|-------------|--|--|--|
| 6 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NBAD- Sl. No. 4.37 | The solution must be able to provide visibility of user endpoint workstations and support & service options to collect telemetry from these endpoints including username, process names and process hashes involved in the network traffic. | Revised Clause: The solution must be able to provide visibility of user endpoint workstations network traffic. |
| 7 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NBAD- Sl. No. 7.7 | The solution should have an automated scanner to identify assets and should also be able to schedule the scans | Please consider the clause as deleted |
| 8 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NBAD- Sl. No. 8.1 | The solution should have detailed ASN traffic visibility | Please consider the clause as deleted |
| 9 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NBAD- Sl. No. 8.4 | The solution should have native integration with CERT CMTX & NCIPC Threat Feeds | Please consider the clause as deleted |
| 10 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for NBAD- Sl. No. 8.2 | The solution should have native integration with any PDNS service to obtain unlimited DNS resolution and domains hosted information along with WHOIS directly from the portal | Please consider the clause as deleted |
| 11 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- Sl. No. 1 | Solution should strengthen end point security solution with improved visibility and new technical controls to detect and prevent from advanced sophisticated attack against users including Anti Phishing, Web form protection, account takeover protection, Browser based attacks and corporate credential theft. | Revised clause: Solution should strengthen end point security solution with improved visibility and new technical controls to detect and prevent from advanced sophisticated attacks, Browser based attacks and corporate credential theft. |
| 12 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- Sl. No. 2 | Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on URL reputation-based Techniques to identify phishing URL's | Revised clause: Solution must detect and block access to phishing sites. Solution should not be only dependent on URL reputation-based Techniques to identify phishing URL's |
| 13 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- Sl. No. 3 | Solution should have protection for account takeover attacks and also solution should alert users on the reuse of corporate password use on external sites | Revised clause: Solution should alert users on the reuse of corporate password use on external sites |

| Sr. No | Section Number | Page Number | Point Number | Original Clause | PDCC Bank Response |
|--------|--|-------------|---------------------------------------|--|--|
| 14 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 6 | Solution should have capability to detect and prevent different exploit techniques including ROP chaining, ASLR Bypass, VBScript God Mode, Stack Pivoting and Blue Keep without having signature database. | Revised Clause: Solution should have capability to detect and prevent different exploit techniques. |
| 15 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 7 | Solution should not have dependency on 3rd party ssl interceptor and also does not require any additional client certificate to inspect ssl traffic at browser level. The solution must have inbuilt ransomware detection mechanism. The solution must be able to identify 0-day attacks, emulate the threat while eliminating the threat on a real-time basis and deliver the file to the user by reconstructing the content. | Revised Clause: The solution must have inbuilt ransomware detection mechanism. The solution must be able to identify 0-day attacks. |
| 16 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 16 | The Solution should have interface to search for IOCs provided through the endpoint management UI, CLI and an API. The search will return a list of all endpoints which match the IOCs | Revised clause: The Solution should have interface to search for IOCs provided through the endpoint management UI. The search will return a list of all endpoints which match the IOCs |
| 17 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 23 | The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on both monitored and non-monitored systems. | Revised Clause: The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on monitored systems. |
| 18 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 38 | The solution should collect Browser History information including URL visited, last visit time, visit count and browser used. | Revised Clause: The solution should collect Browser History information including URL visited, last visit time and browser used. |
| 19 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 39 | The solution should collect file information including file name, directory path, File size, md5, DES-3 and sha1 hash, time of creation and deletion and user executing the process. | Revised Clause: The solution should collect file information including file name, directory path, File size, md5, DES-3, AES, sha256 and sha1 hash and user executing the process. |



Corrigendum – 1.0 For Request for Proposal (RFP) For Selection of Service Provider for Cyber Security Operation Center on Hybrid Model

| Sr. No | Section Number | Page Number | Point Number | Original Clause | PDCC Bank Response |
|--------|--|-------------|---------------------------------------|--|--|
| 20 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 40 | The solution should show the IP addresses and host names from hosts file on Windows, Linux, and macOS devices. | Revised Clause: The solution should show the IP addresses and host names from hosts file on Windows & RedHat Linux. |
| 21 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 44 | The solution should support Windows, Linux and MacOS | Revised Clause: The solution should support Windows & RedHat Linux. |
| 22 | 8.10 Annexure 10: Functional and Technical Specification | 64 | Excel Spreadsheet for EDR- SI. No. 50 | The solution should be able to run a vulnerability scan on a particular endpoint if under investigation. | Please consider the clause as deleted |
| 23 | Section 2: Detailed Scope of Work | 11 | Point No. 5 | The Bank intends to have various modules of SIEM placed in DC to be in HA (High Availability) mode, also the Bank intends to have SIEM modules in DR and NDR for redundancy. | The Bidder shall consider implementation of bank-end CSOC components at Bank's DC (in HA mode) & DR (In Standalone mode) only. CSOC should monitor entire Bank's infrastructure including the NDR. |