rebit.org.in

RFP – Static Application Security Testing (SAST) solution

Pre-bid meeting – Q & A

Venue: Reserve Bank Information Technology Pvt Ltd (ReBIT)
502, Building No 1, Mind Space Juinagar,
Nerul, Navi Mumbai – 400706

Date & Time: 28-Feb-2020 (4pm to 6pm)

Meeting Organizer: Prajakta Sharma

Minutes Taker: Prajakta Sharma

Published Date: March 6, 2020

Sr No	RFP Section Number	RFP Page Number	RFP Point Number	Query Description	Response
1	4.2	10	6	Please provide the list of file servers (including the format) that you want the SAST solution to be integrated with it.	We are considering standard file servers. File server is only used for storing source code of different applications on which SAST tool should perform the scans.
2	4.2	10	10	Our understanding is that ReBIT will be provisioning the required Hardware for the rollout of the SAST Solution. Please confirm.	Yes, the understanding is correct. However, bidder is required to share the hardware specifications.

3	4.2	11	1	Do the project manager and associated support personnel be at onsite during the testing and acceptance phase?	No change in this criteria. The condition mentioned in the RFP remains the same. The project manager may not be required on-site during the complete testing and acceptance phase however a support personnel will be required.
4	4.9	17	2, 3	Do the project manager and associated support personnel must be at onsite during the hand holding phase?	No change in this criteria. The condition mentioned in the RFP remains the same. The project manager may not be required on-site during the complete testing and acceptance phase however a support personnel will be required.
5	7.3	29	3, 4	Please let us know the timeline for the PoC. Also, please let us know if the sample code mentioned in the RFP will be provisioned by ReBIT during POC phase. If Yes, please share the details of the same.	Timelines will be shared later with the bidders who have qualified the technical round.

6	11.18	71	1	What programming languages should be considered for Mobile platform? Is there a specific language support required for mobile?	Standard programming languages available in the market. Bidders are required to specify the programming languages supported by their tool as part of the technical bid.
7	11.18	72	18	HP/UX is not supported. Can this be removed from the requirements or can we have separate clause for each platform mentioned in clause 18 (Linux, MacOS, HP/UX, Solaris)?	No change in this criteria. The condition mentioned in the RFP remains the same. This is good-to-have expectation from the solution.
8	11.18	73	26	Are you referring to Makefile, ANT, Maven, Gradle, CMAKE, etc. like Automatic build tools and Bamboo, TeamCity, Ansible, etc., like Deployment tools?	Yes, the understanding is correct.
9	11.18	74	Support - 4	Is eLearning referred for SAST tool learning or Security Practices?	It is "SAST tool learning"
10	11.18	74	Reports - 2	Wizard based custom reports creation is not supported. Can we deliver the custom reports through our professional services?	No change in this criteria. The condition mentioned in the RFP remains the same. This is good-to-have expectation from the solution. If bidders feel this would be covered through professional services then that will add to their total TCO.

11	11.18	74	Reports - 3	Can XLS format mentioned in “csv, pdf, xls, text, HTML, XML = 7” – can “xls” be removed if CSV is supported? “pdf, xls, HTML, XML = 4” – can be replaced with CSV format?	xls can be removed only if csv is supported. However other formats like pdf, txt, HTML and XML are required.
12	6.1 In conjunction with 11.16	23, 68	6 & 7 4	Our One Year subscription cost includes standard 8 x 5 support by phone, email and WebEx. Since SAST tool comes after the source code is written but before the commit, it probably would not require 365 x 24 x 7 support as SAST tool will not be mission critical. RFP has mentioned 8.30 AM to 7.30 PM as Operational Working Hours. Typically, Level 3 and Level 4 SLA is found adequate by other users globally. Our Technical Support adequately covers the 24 x 5 support requirements thru Email, Phone, WebEx and “follow-the-sun” support model.	No change in this criteria. The condition mentioned in the RFP remains the same.

13	6.1 In conjunction with 11.16	23 68	6 & 7 4	Is 365 x 24 x 7 support is mandatory, and are support persons required to be present onsite at ReBIT, or offsite availability is okay?	Fulltime onsite support is not required. Only when there are issues, an on-site support will be required
14	6.5	25		If ReBIT wish to charge penalty for delay in Implementation and Go Live, ReBIT to ensure the required Hardware, Tools with which SAST is to be integrated as well as facilities including ReBIT personnel are ready and made available whenever they are requested. Any delay due to non-availability of the above should not be considered towards bidder delay.	The understanding is correct.
15	6.4	25		For penalties charged against SLAs the downtime should be counted from the time it was reported and not from the time the issue occurred.	The understanding is correct.
16	8.7 3.1	35 7	Bid Submission Schedule	With respect to EMD, Technical and Commercial Bid Submission Schedule, is the submission to be Physical or Electronic? The RFP mentions 3 envelopes in one place and e-procurement in another place.	Both the options are available.

17	5.1	21	7	GST revision (upward or downward) if any to be considered from the date of announcement of change in the rate. Invoice for the period during which the change in announced will contain two parts – one till the date of announcement at old rate and other from the date of announcement at new rate.	The understanding is correct
18	4.2	11	1	Project Manager will NOT be a full-time resource. A SPOC (Single Point of Contact) will be deployed full time to co-ordinate between vendor and customer teams. Other resources will be full time till the Go Live.	The understanding is correct.
19	7.2	27	3	Past experience of SI is only in Product License to 3 or more organizations. Implementation and integration support experience only by OEM.	The complete responsibility for delivering the scope of work mentioned in the RFP should be with the bidder.
20	Eligibility Criteria	27	3	*Request Support Cost to be paid annually in advance* Support Cost will be paid on Quarterly basis, equally divided in 12 quarters. Support Cost will be paid at the beginning of each quarter for the support provided for previous quarter.	No change in this criteria. The condition mentioned in the RFP remains the same.
21	11.18 Technical Specifications	73	31	*Request ReBIT to consider changing this to leaders+ challengers' quadrant in Gartner's. Also request this to be part of the eligibility criteria.* - "Product must be listed in the latest magic quadrant published by Gartner"	No change in this criteria. The condition mentioned in the RFP remains the same.

22	Partnering with the OEM	40	9.6	"It will be the sole responsibility of the Bidder to get the proposed technical solution vetted by the OEM as part of the response, if he is not the OEM; and submit a copy of the same to the ReBIT confirming their partnership regarding the implementation of the project." - *is there a ReBIT format for the same?*	There is no ReBIT format for the same however bidders should ensure that the OEM letter shared by them covers all the points mentioned in section 9.6.
23	Support	74	2	"The solution should provide multiple concurrent scanning of minimum 4 application." - *Concurrency for 4 applications can be provided. However, this will impact ReBIT's cost in terms of underlying hardware/processing resources and licensing required to complete the scans in a reasonable scan time. ReBIT might kindly consider having this changed to 2 which should suffice their needs*	We will agree with this.
24	Solution should have e-Learning and other such developer coaching module	74	4	*The same is available but would need additional licensing. Would ReBIT be agreeable to the OEM factoring in e-Learning costs in their proposal?*	No change in this criteria. The condition mentioned in the RFP remains the same. This is good-to-have expectation from the solution. If bidders feel this would be additional licensing then that will add to their total TCO.
25	Milestone: Go Live	19		100% of subscription cost. *Request ReBIT to consider 100% on award of contract.*	No change in this criteria. The condition mentioned in the RFP remains the same.

26	Support Period of 3 Years	19		Support Cost will be paid on Quarterly basis, equally divided in 12 quarters. Support Cost will be paid at the beginning of each quarter for the support provided for previous quarter. *(Request ReBIT's consideration for support costs paid annually in advance).*	No change in this criteria. The condition mentioned in the RFP remains the same.
27	False positive %	29	3	"It is to be noted that the number of false positive reported by the Tool should not exceed 20% of the total number of vulnerabilities observed and also, number of true positive should not be less than 80% of the total number of vulnerabilities reported by the Tool.10 Marks grade scoring (Actual POC Score) will be awarded for this activity." - *False positive ratio for the tool is dependent on the code sample provided and cannot be pre-determined. All tools will have a tendency to report a higher number of false positives in the initial scans.*	No change in this criteria. The condition mentioned in the RFP remains the same.
28	Backup and Archiving	13	4.3.1 point 3 and 4	Every OEM will have a different approach to backup, archival and restoration. We would want to know ReBIT's Backup and Archival strategy so we can address the same along with the partner.	We will share the Backup, archival and restoration policy with the successful bidder. It is standard process which aims for zero data loss during failure.

29	Technical Specification	73	20	Solution integrated with developer environments should provide security tips while developers are coding This is a feature specific to a single OEM. Could ReBIT elaborate on why this functionality is required?	No change in this criteria. The condition mentioned in the RFP remains the same. This is good-to-have expectation from the solution.
30	Technical Specification	73	28	The solution must offer the feature to scan the source code locally developed by the developer in run-time environment without requiring connection to a centralized server *This is a feature specific to a single OEM. Could ReBIT elaborate on why this functionality is required?*	No change in this criteria. The condition mentioned in the RFP remains the same. This is good-to-have expectation from the solution.
31	Technical Specification	73	30	The solution must be inclusive of any database required for its functioning. While the tool includes a basic Database version for out of the box functionality, it is recommended that ReBIT move to a full-featured version of the Database for use in its production environment. Would ReBIT procure the Database separately or would it want us to include the same as part of our commercial response? The ReBIT team may also use any existing compatible Database license for the same at its discretion.	No change in this criteria. The condition mentioned in the RFP remains the same. If there is separate cost, bidders can add it in Sr. No 5 - Other Items.

32	System Requirement Specification Document (Test Cases)	15	5	(Test Cases) – "Could the ReBIT team elaborate on test cases would be considered?"	Testcases will be broadly covered to assess the features of the tool defined as part of Technical Specifications.
33	4.4 Process & System Study 11.1 Annexure A: Submission Checklist	14 47	4.4 11.1	Section 4.4 states that, "The successful Bidder will be required to create a detailed System Requirement Specification document ..." whereas, in section 11.1 submission checklist for technical bid includes Technical Solutions (System Requirement Specifications Document) Please confirm if we have to give at the time of bid submission or need to be provided by the successful bidder.	This needs to be given at the time of bid submission as part of Technical bid.
34	11.18 Technical Specifications	74	11.18	"The solution should have the capability to schedule scanning activity." This feature is enabled and made available in conjunction with code repositories and build servers or OS scheduled jobs. Hence, request to mark this point as Good-to-Have or modify requirement accordingly please.	No change in this criteria.
35	4.5 Deployment and Testing	16	4.5	Should the vendor provide onsite support for the subscription years	Fulltime onsite support is not required. Only when there are issues, an on-site support will be required
36	7.2 Minimum Eligibility Criteria	27	7.2	We request you to consider the PO copy. The clause in the RFP is not spelling the same very clearly.	Ok. PO copy can also be considered in place of contract copy.

37	4.3.5 Guidelines for Maintenance and Support	14	4.3.5	*ReBIT will conduct dynamic application security testing of SAST tool for major/moderate critical changes before production implementation* --> Will DAST tool scan the application for vulnerabilities	No, ReBIT will carry out a VAPT to identify any vulnerabilities in the underlying infrastructure and the tool. Bidders will be required to fix all the vulnerabilities which are identified as part of this activity.
38	NA	NA	NA	Can Jenkins be used to schedule the scan?	Yes, however security patch update of this tool and if any vulnerabilities observed in this tool should be fixed by the bidder.
39	Indemnification	39	9.3	It may so happen that the tool may not be able to identify a vulnerability which may lead to breach due to its exploit. No tool can give 100% assurance to cover all true positives.	This clause is standard ReBIT clause.
40	NA	NA	NA	When SRS is required to be submitted and what it should contain?	The SRS should be submitted as part of the Technical Bid document containing details mentioned in the RFP such as Tool integrations with Source code repository, IDE (Integrated Developer Environment), File server, Build tool etc.
41	NA	NA	NA	Will there be scoring for SRS?	No, there will be no separate scoring for SRS.

42	4.3.4 Security Requirements	14	4	Standards Benchmark - Is it necessary to get the VAPT reports from the independent organization	ReBIT will carry out a VAPT to identify any vulnerabilities in the underlying infrastructure and assign the Severity to identified vulnerabilities. Bidders will be required to honour the vulnerability rating given by VAPT team and fix all the vulnerabilities which are identified as part of this activity.
43	4.11.2 Change Management	20	4.11.2	Can all the changes be tracked in an excel?	Yes
44	4.11.1 Incident Management and Response Management	19	4.11.1	Can the incidents be logged in a portal?	Yes
45	4.3.1 Backup and Archiving	13	4.3.1	What is expected in the DR process?	Standard DR process which can be initiated when the tool fails ensuring there is zero data loss. Further, it should be able to restore all the backups such as Database backup, Configuration backup etc.
46	4.2 Scope of Work	12	5	Termination: *5. On termination of the project, the Bidder commits to provide all necessary support in handing over the project to new incumbent identified by ReBIT* --> In this case only ReBIT specific documents will be handed over.	Yes, all the documents created for ReBIT use for this RFP (except any IPR related information of the Tool proposed by the Bidder) will be handed over to the new incumbent identified by ReBIT.

47	NA	NA	NA	Can OEM bid through multiple bidders?	Each OEM should bid through only one bidder. OEM represented by more than one bidder shall be disqualified.

Note: This document shall form part and parcel of the RFP and therefore bidders are advised to take the clarifications/responses into account, as applicable, while submitting the bids.