Request for Proposal for procurement of Enterprise Security Service Bus (ESSB)
Solution - NPCI/RFP/2019-20/IT/06 dated 05.07.2019

Consolidated list of Replies to Pre-bid Queries

S.No	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)	NPCI Response
1	8.12 Support (AMC)	22	8.12	After expiration of warranty period of one (1) year,NPCI at its discretion may enter into Annual Maintenance Contract (AMC) at the rate mentioned in Purchase Order for period of 2nd and 3rd year. All the terms and conditions of the Purchase Order will be applicable during such AMC period	Request bank to confirm if the AMC is part of TCO for the commercial evaluation, since as per this clause bank may or may not enter into AMC.		Yes
2	8.16 Repeat Order:	24	8.16	NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and/or services at the agreed unit rate for individual categories of purchase order during the period of 1 year from the date of award / 1st Purchase Order.	Request NPCI to change the price validity for the repeat order to a maximum of 180 days from the price discovery date.		No change in RFP
3	3.1 Scope of work:	10	3.1	Implementation of the solution to be done by OEM directly. Resumes of the team members to be shared as part of RFP response.	Request Bank to ask for resume post L1 decleration.		Bidders can hide details like actual name,address,contacts etc and can share actual resumes.
4	8.19 Migration activities for change of location:	25	8.19	In case NPCI wishes to shift the devices from one place to another anywhere in the country, adequate support will be made available by the bidder by arranging field engineer for the purpose of dismantling of devices supplied by Service provider & hand-over to the concerned Officials or Data Center, pre-shifting inspection, post-shifting inspection, re-installation etc. of all devices supplied by Service provider. All migration related activities to be done after Business / session hours /according to business convenience & the engineer has to be deployed as per the requirements. NPCI will bear all expenses for packing, shifting, insurance and other incidentals at actual. NPCI will not be responsible or liable for any losses, damages to the items of equipment's, tools and machinery while such dismantling, pre-shifting inspection, post-shifting inspection, and re-installation etc. is being carried out. Bidder shall make available adequate alternative arrangement to ensure that the system functioning is neither affected nor dislocated during the shifting process. It is the responsibility of field engineer to integrate devices delivered at required location or Data Center & coordinate with NPCI NOC to extend the reachability.	As per this RFP clause , NPCI can do this shifting multiple time and bidder to provide necessory services for this . Request NPCI to modify the commercial sheet to quote the commercial rate per migration. Since the quantity (No of time's shifting or migration requirement) is not specified, this cost will not be able to add to the product cost.		No change in RFP
5	Section 9 - Technical Specifications, Investigation Capabilities	34	C.7	The solution must provide periodic updates of threat intelligence for incident artifacts, E.g.: A file has been captured now after 3 days some vendor threat feeds has confirmed it belongs to an APT Group	Is this required for open incidents or closed incients and whether NPCI will be giving any source to lookup TI information?		Required for both open and close .Yes NPCI will provide TI for direct integration with SOAR.
6	Section 9 - Technical Specifications, Integration Capabilities	36	E.13	Ability to easily write a new integration without having to contact the OEM	Whether NPCI will develop custom integration and want to add into orchestraion? or while writing playbook few of the tasks NPCI wants to automate by writing custom code then in playbooks itself?		Direct integration will be done by NPCI ,rest has to be developed//customized/integarte by OEM with the help of bidders.
7	Section 9 - Technical Specifications, Reporting Capabilities	37	F.15	The tool should document all IOCs from integrated threat feeds	does this clause imply that NPCI wants this IOCs documented related to incidents they are investigating or any other IOC they want to ingest into tool from feed provider ?		Both
8	Section 9 - Technical Specifications, Dashboards	37	G.6	Clear situational awareness of the SOC alert handling status via dashboard	Can we get more detail about the situational awareness here?		Example like currents status,open incidents,where it is pending,management reports,analyst reports and status etc.
9	7.3 Technical Scoring Matrix:	18		Customer BFSI reference in India	Since SOAR is relatively new technology,we request NPCI to consider reference globally and not just BFSI segment for India market for scoring		More weightage will be given to India BFSI reference while scoring
10	Additional Queries				What is the current/expected EPS in NPCI environment ?		45000 +
11	Additional Queries				What is the expected number of alerts handled per day in current SOC and how much needs to be factored		300 per day
12	Additional Queries				What is the alert retention period for NPCI which needs to be factored ?? Do we need to consider as 180 days		Solution should have the ability to store 180 days .Also restore mechanism for serching alerts from archieve should be available .
13	Additional Queries				Does NPCI have IOCs in .csv or any format .What are the Threat Intel platforms NPCI have deployed for ESSB integration ?		Yes.TI details will be shared with qualify bidders
14	Additional Queries				What are the concurrent analyst NPCI would need on SOAR platform across shifts ?		Oncall support whenever nessery post implementaion
15	Additional Queries				What is the existing Ticketing Tool deployed in NPCI ?		Bidders to specify the list of ticketing tool their solution supports.
16	Additional Queries				Can NPCI provide list of Security tools & Applications deployed in their environment which is considered as part of ESSB solution for automation,enrichment and response.		Bidders to specify the list of security tools their solution supports.
17	7.3 Technical Scoring Matrix:	18		Customer BFSI reference in India	Since SOAR is relatively new technology,we request NPCI to consider reference globally and not just BFSI segment for India market for scoring		More weightage will be given to India BFSI reference while scoring
18	General Queries				What is the current/expected EPS in NPCI environment ?		45000 +
19	General Queries				What is the expected number of alerts handled per day in current SOC and how much needs to be factored		300
20	General Queries				What is the alert retention period for NPCI which needs to be factored ?? Do we need to consider as 180 days		Solution should have the ability to store 180 days .Also restore mechanism for serching alerts from archieve should be available .
21	General Queries				Does NPCI have IOCs in .csv or any format .What are the Threat Intel platforms NPCI have deployed for ESSB integration ?		Yes.TI details will be shared with qualified bidders
22	General Queries				What are the concurrent analyst NPCI would need on SOAR platform across shifts ?		Oncall support whenever nessery post implementaion
23	General Queries				What is the existing Ticketing Tool deployed in NPCI ?		Bidders to specify the list of ticketing tool their solution supports.
24	General Queries				Can NPCI provide list of Security tools & Applications deployed in their environment which is considered as part of ESSB solution for automation,enrichment and response.		Bidders to specify the list of security tools their solution supports.

25	Section 3 – Scope of Work	10	3.1	To enable SOC/IR team to provide automatic remediation of raised alerts through playbooks provided and placed inside the ESSB solution	Please define what is a playbook and do you want semi-automation or complete automation? Also please mention the types of Playbooks or automated playbooks would you need to be quoted for the tender. For example automated playbook for Malicious file download, Potential Phishing etc.		Play book is automated action defined for specific type of incident which has to be triggered when an incident occures.It can complete/semi automation depending on the type of action defined in the play book.Play books counts can not be fixed .
26	Section 7 - Bid Evaluation	18	7.3	Technical Scoring Matrix:- RFP Presentation Part – B OEM Evaluation Matrix-Customer BFSI reference in India-	Would a global large BFSI suffice?		More weightage will be given to India BFSI reference while scoring
27	Section 8 - Terms and Conditions	20	8.6	Point 3- Network connectors for integration and collection of data	Please provide the details the products for data collection.		Details will be shared with qualified bidders.
28	Section 8 - Terms and Conditions	20	8.6	Point 5- Additional User License	We would need to know how many SOC agents /users woud be using the solution/ manning the service?		Initially NPCI will use the base user license ,aditiuonal licenses can be procured as part of repeat order on basis of unit price mentioned in the commercial.
29	8.13 Service Level Requirements (SLA)	22	8.13	Bidder shall help NPCI team to integrate all security and network solutions available in NPCI environment with the said Solution	Provide the technology / product names/ software and hardware versions for all integrations required	Please mention the product names etc. so that we can validate integration with them	Details will be shared with qualified bidders.
30	8.13 Service Level Requirements (SLA)	22	8.13	Hands-on training for minimum 6 days to different stakeholders in NPCI needs to be provided with relevant technical documents / workbooks/ guides.	Would online technical documents suffice or you would need hard copies? Please clarify?	Please mention to include online documentation	Both online and offline and hard copies are required.
31	Section 9 - Technical Specifications	32	A.8	The solution must support user authentication via SAML	Please share the solution you are using for this?		Details will be shared with qualified bidders.Bidders to elaborated the solution/authentication supported.
32	Section 9 - Technical Specifications	32	A.20	The Solution should support 2 factor Authentication and support for the tool	Please clarify which 2 FA solution you would be using.		Details will be shared with qualified bidders.Bidders to elaborated the solution/authentication supported.
33	Section 9 - Technical Specifications	32	A.24	The company should have own support facilities in India.	Being local partners we have dedicated support people. Would this qualify?	If so please ammend point to imply the same	RFP is self explaonatory
34	Section 9 - Technical Specifications	33	B.16	The solution must be able to automatically extract email attachments from emails and store that for the related incidents as attachments.	We need details of quantum of data to size the storage. Please let us know how much data would be stored in GB.		It depends upon incident to incident .However roughly 15 incidents triggered per day.
35	Section 9 - Technical Specifications	32	C.4	Integration of Threat intelligence data feeds, along with data provided through STIX TAXII format for data enrichment	Please list out how many threat intelligence data feeds and their names and also clarify if the same are available with NPCI		Details will be shared with qualified bidders.Bidders shuld supports STIX TAXII format for data enrichment.
36	Section 9 - Technical Specifications	34	C.7	The solution must provide periodic updates of threat intelligence for incident artifacts, E.g.: A file has been captured now after 3 days some vendor threat feeds has confirmed it belongs to an APT Group	The solution can ingest threat intell feeds and uses them for enrichment and to reduce number of false positives. As per the use case mentioned- once an artefact is created, the use can use the correlation engine to conduct enrichment. If the user can check back in time for a particular artefact created in the past, he can find out if a threat feed has picked it up. This means the user has to query back into historic data and retrieve the artefact data". Please confirm if this is your use case.		Understing is correct.
37	Section 9 - Technical Specifications	36	E.13	Ability to easily write a new integration without having to contact the OEM	Please explain if you mean bi-directional integration or not ? Also it would be upto NPCI to provide access/support ane API's for the said products. Please confirm.		Yes both should be there. Access to API will be provided by NPCI.However support to integradte the solution via API should be with OEM.
38	Technical Specification	32	A.9	The solution must not be licensed based on the number of actions that can performed per day.	Every OEM has there own methodology for licensing , to promote equal playing field it is thus requested to remove this clause	Clause removal	No change in RFP
39	Technical Specification	32	A.14	Automation of threat hunting and threat intel monitoring including malware analysis and identification, raising tickets and blocking of IoCs	We understand the malaware analysis and identification is expected out of the integration between the tool and other OEM product , we hope our understanding is inline with your expectation. In case of any deviation of expectation please explain the following point.	Clarification	Understing is correct.
40	Technical Specification	32	A.23	Preferably the solution should be in use by a customer in a similar industry (BFSI)	SOAR is a upcoming technology with limited amount customer in the country , it is thus requested to relax the particular specification and rephrase the same as: The solution should be deployed in atleast 1 Govt/BFSI customer.	Modification	More weightage will be given to India BFSI reference while scoring
41	Technical Specification	33	B.7	Existing playbooks with major endpoint, DLP, Firewall and other security vendors provide rapid integration capabilities	Roles of playbooks are to align the business logic and SOP with the SOC operation. Integration with solution such as DLP, firewall and other device are the core functionality of SOAr platform. Hence it is requested to re-phrase the same as: The solution should support integration with leading DLP , Firewall , Siem solution to anme a few.	Modification	No change in RFP
42	Technical Specification	33	B.28	Visual/Form way of interacting with orchestration platform API (instead of REST/SOAP API) in the playbooks.	Please explain the expectation from the following, is the expectation here is to have a workflow editior which can help in designing the playbook using drag and drop functionality	Clarification	Understing is correct and by visual we mean drag and drop or form based interaction to define actions/parameters
43	Technical Specification	35	D.20	The system will support Event logging	Event logging is a funstionality of SIEM solution , it is thus requested to remove the following point.	Clause removal	Event related to an alert will be logged by the SOAR soulution not the direct/all events
44	Technical Specification	35	D.24	Track all forensic data related to an incident in one location (support large files, pcaps, system images, snapshots etc) (data > 20GB)	File size with such large volume are not used for forensics investigation as they span over a large portion of time, to narrow down on investigation smaller pcaps are utilized it is thus requested to remove the file size restriction and rephrase the same as : Track all forensic data related to an incident in one location (support large files, pcaps, system images, snapshots etc)	Modification	Incident data can vary in size, which is not limited to said artifacts. An analyst will only attach relevant data to it, however to maintain integrity of evidences, larger file size might be attached to incident thus, large file support is required
45	Technical Specification	36	D.43	The tool should support SOAP and REST APIs within the platform for additional ingestion and export capabilities.	Every OEM support different form of integration with third party product , it is thus requested to rephrase the following specs to promote participation for all. The tool should support SOAP or REST API or Python withing the platform for additional ingestion and export capability	Modification	No change in RFP as SOAP and REST APIs should be supported for any future integration, however python support can be provided by OEM to create customization in integration
46	Technical Specification	36	D.45	The tool should have feature of allowing Incoming alerts to be grouped or created as individual incidents. Likewise created incidents that share an associational link can be grouped together for simplified correlation and response activities.	Grouping and corelation is a feature of SIEM , it is thus requested to rephrase the following spec as: Tool should provide information on incident with similar artifacts/IOC.	Modification	Incoming alerts generated from SIEM or other tools should be grouped together by the SOAR solution for analyst to understand the incidents and situation better
47	Technical Specification	36	F.1	Exporting (csv, xml, pdf, docx, email) and report generation capabilities	Every solution has there own method of exporting data pertaining to the incident , it is thus requested to re-phrase the same as. Exporting (CSV/XML/PDF/dpcx/email) & report generation.	Modification	No change in RFP. Please mention the report formats supported by your solution

48	Support	22	8.12	Bidder shall maintain all the spares required for maintenance of equipment supplied to NPCI for the period of three (3) years. In case Bidder is not able to repair the equipment due to unavailability of spares, Bidder shall replace the entire equipment with the latest model available in the market with same functionality.	If the OEM has stopped the production, partner shall not be able to supply required spares if needed to be changed.	Modification	No change in RFP
49	Payment Terms	24	8.18	Installation Payment	Milestone payment terms	Modification	No change in RFP
50	Scope of Work	10	3.1	Implementation of the solution to be done by OEM directly. Resumes of the team members to be shared as part of RFP response.	Implementation to be done by OEM/Bidder	Modification	Bidders can hide details like actual name,address,contacts etc and can share actual resumes.
51	Scope of Work	10	3.1	Supply of Hardware	Consortium for Supply/installation of hardware	Modification	No change in RFP. Bidder/OEMs to specify the detail BOM along with license for the solution to provided.
52	MAF	49	Annexure 1	Guarantee and warranty	MAF, Will be as per IBM T&C	Modification	MAF from the OEM should be provided as per the format mentioned in Annexure-I
53	Eligibility Criteria	10	4.1	Eligibility Criteria	The bidder should have reported minimum annual turnover of Rs. 15 Crores as per audited financial statements in each of the last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019) and should have reported profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019). **We are profitiable for 2017-18 and last year book are yet to audited, request if you can consider ONE Year as profiable clause and request for provisional balance sheet for 2018-19**	Change in Clause	No change in RFP. The eligibility criteria is self explanatory. As mentioned in the RFP, In case audited financial statements for 2018-2019 are not ready, then management certified financial statement shall be considered for 2018-2019, however, this exception is not available in case of previous financial years.