Request for proposal for procurement of Next Generation Security information and event management (SIEM) Solution

RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022

National Payments Corporation of India
Unit no. 202, 2nd floor,
Raheja Titanium, CTS No. 201,
Western Express Highway,
Goregaon East, Mumbai 400 063
Email- itprocurement@npci.org.in
Website: www.npci.org.in

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to Bidder or applicants whether verbally or in documentary form by or on behalf of National Payments Corporation of India (NPCI), is provided to the Bidder on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by NPCI to any parties other than the Bidders/ applicants who are qualified to submit the Bids ("Bidders"). The purpose of this RFP document is to provide Bidder with information to assist the formulation of their Proposals. This RFP document does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP document and where necessary obtain independent advice. NPCI makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP document. NPCI may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP document.

Checklist

The following items must be checked before the Bid is submitted:

1. Online transfer of Rs 17,700/- (Rs. Seventeen thousand seven hundred only inclusive of GST@18%) towards cost of Bid document in Folder – 'A'
2. Online transfer / Bank Guarantee of Rs. 5,00,000/- (Rupee Five lakhs only) towards Bid Security in Folder 'A'- Earnest Money Deposit (EMD)

   On account of the COVID-19 pandemic conditions, the bidders shall pay the Bid Cost & EMD through the above mentioned mode and the remittance proof shall be submitted to NPCI for the same, failing which the bid is liable to be rejected.

   Remittance proof in favor of "National Payments Corporation of India" payable at Mumbai" amounting to Rs. 17,700/- (Rs. 15,000/- plus GST @18 %) towards bid purchase cost and Rs. 5,00,000/- towards Bid Security.

   The electronic / wire transfer can be done to designated NPCI bank account as detailed below:
   Account Name: National Payments Corporation of India
   Bank Name: HDFC Bank
   Account No: 00600530001133
   IFSC Code: HDFC0000060
   Address: Maneckji Wadia Bldg., Ground Floor, Naik Motwani Marg, Fort, Mumbai - 400023
   BSR Code: 0510062
   SWIFT Code: HDFCINBBXXX

3. Eligibility Criteria, Technical and Commercial Bids are to be prepared in accordance with the RFP document.
4. Folder 'A'- Eligibility Criteria Response
5. Folder 'B'- Technical Response
6. RFP document duly sealed and signed by the authorized signatory on each page is to be enclosed in Folder – 'A'.
7. Prices are quoted in Indian Rupees (INR).
8. All relevant Certifications, audit reports, etc. are to be enclosed to support claims made in the bid in relevant Folders.
9. All the pages of documents submitted as part of Bid are duly sealed and signed by the authorized signatory.

Abbreviations and Acronyms

The following abbreviations and acronyms defined in this RFP are as under

BG	Bank Guarantee
DC	Data Centre
EMD	Earnest Money Deposit
IPR	Intellectual Property Rights
LAN	Local Area Network
NPCI	National Payments Corporation of India
OEM	Original Equipment Manufacturer
RFP	Request for Proposal
PBG	Performance Bank Guarantee
SAN	Storage Area Network
SLA	Service Level Agreement
WAN	Wide Area Network
SI	System Integrator
OEM	Original Equipment Manufacturer
SIEM	Security Information and Event Management

Section 1 - Bid Schedule and Address

Sr. No.	Description	
1	Name of Project	Request for proposal for procurement Next Generation Security information and event management (SIEM) Solution
2	Tender Reference Number	NPCI/RFP/2021-22/IT/17
3	Date of release of RFP	**24.02.2022**
4	Last date of receiving pre-bid clarifications in writing from vendors	**04.03.2022 6.30 pm** (Please note that any pre-bid queries beyond the date and time mentioned will be not be considered)
5	Date and Time for Pre-bid Meeting	Not applicable
6	Last date and time for Bid Submission	**16.03.2022 5.30 pm**
7	Details of Bid Submission and opening of Bids	Electronic bid response submission should be made to the following email address: • **siddhesh.chalke@npci.org.in** • **benny.joseph@npci.org.in** **Folder A (Eligibility), Folder B (Technical) and Folder C(Commercial):** **Commercial bid (Folder C) should be password protected.** The password to Commercial bid needs to be shared only upon request after successful technical qualification.
8	Date and Time of Eligibility & Technical bid Opening	**16.03.2022 6.00 pm**
9	Date and Time of Commercial Bid Opening	Commercial Bid to be submitted in the password protected PDF document along with Technical Bids. The password to be shared only after request from NPCI's designated authority. NPCI reserves the right to discover the lowest price through Reverse auction OR Price discussion mechanism or both if opted by NPCI. NPCI will inform the method of price negotiation to technically qualified bidders.
10	Name and Address for communication	Head – Strategic IT Procurement National Payments Corporation of India, Unit no. 202, 2nd floor, Raheja Titanium, CTS No. 201, Western Express Highway, Goregaon East, Mumbai 400063
11	Bid Related Queries	Sandeep Tiwari | Contact: +91 9999983500 Email id: sandeep.tiwari@npci.org.in Arvind Patil | Contact: +91 8082044772 Email id: arvind.patil@npci.org.in Benny Joseph| Contact: +91 02240508500 Email id: benny.joseph@npci.org.in Siddhesh Chalke | Contact: +91 8657995380 Email id: siddhesh.chalke@npci.org.in
12	Bid cost	Rs. 17,700/- (Rs. 15,000/- plus GST @18 %)
13	Bid Security	Rs. 5,00,000/- (Rupees Five lakhs only)

Section 2 – Introduction

2.1 About NPCI

NPCI is a Company registered under Section 25 of the Companies Act, 1956 (corresponding to Section 8 of The Companies Act, 2013) with its Registered Office in Mumbai, India. NPCI was promoted by 10 (Ten) banks in India under the aegis of the Indian Bank's Association with majority shareholding by Public Sector Banks. Presently, 54 (Fifty-Four) banks are shareholders of NPCI. Out of which 17 (Seventeen) are Public Sector Banks (PSB), 17 (Seventeen) Private Sector Banks, 3 (Three) Foreign Banks, 10 (Ten) Multi State Cooperative Banks and 7 (Seven) Regional Rural Banks.

The vision, mission and values of NPCI are: Vision - To be the best payments network globally, Mission – Touching every Indian with one or other payment services and to make our mission possible, we live and work by six core values: Passion for Excellence, Collaboration, Customer Centricity, Agility, Security and Innovation.

NPCI, during its journey, has made a significant impact on the retail payment systems in the country. Dedicated to the nation by our former President, Shri Pranab Mukherjee, endorsed by the Hon'ble Prime Minister, Shri Narendra Modi and later made the card of choice for the ambitious Pradhan Mantri Jan Dhan Yojana, RuPay is now a known name. RuPay is an indigenously developed Payment System – designed to meet the expectation and needs of the Indian consumer, banks and merchant eco-system. The alliances with international network partners (Discover Financial Services, Japan Credit Bureau and China Union Pay) provides valuable access to global acceptance footprint and offer world class payment solutions to RuPay cardholders.

NPCI aim is to transform India into a 'less-cash' society by touching every Indian with one or other payment services. With each passing year we are moving towards our vision to be the best payments network globally.

2.2 Objective of this RFP

The objective of the RFP is to procure s Next Generation Security information and event management (SIEM) Solution.

2.3 Cost of the RFP

The Bidder shall bear all costs associated with the preparation and submission of its bid and NPCI will, in no case, be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

2.4 Due Diligence

The Bidders are expected to examine all instructions, terms and specifications stated in this RFP. The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. Also the decision of NPCI on rejection of bid shall be final and binding on the bidder and grounds of rejection of Bid should not be questioned after the final declaration of the successful Bidder.

The Bidder is requested to carefully examine the RFP documents and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, Bidder should seek necessary clarifications by e-mail as mentioned in Section-1. Any query received after the last date for submission of pre-bid queries as given in Section-1 will not be considered.

2.5 Ownership of this RFP

Section 3 – Scope of Work

3.1 Scope of work:

The scope of work will broadly include supply, installation and subsequent maintenance and support for the proposed Next Generation Security information and event management (SIEM) Solution. NPCI intends to procure following solution and the broad scope of work will include but not limited to the following:

- To install and configure Next Generation Security information and event management (SIEM) solution at NPCI DC and DR as per the proposed Bill of material.
- Instances – 04 Nos. as active-active for two DC's.
- To configure Next Generation Security information and event management (SIEM) solution at Primary DC and Disaster Recovery site.
- Bidder shall also undertake to carry out implementation / operationalization including but not limited to move, add, and delete changes / customization of such software updates, releases, version upgrades.
- Bidder should update and maintain all supplied equipment to correctly reflect actual state of the setup at any point in time during the warranty period.
- Bidder should ensure availability of on-site resource if required for troubleshooting and resolution of technical issues back-to-back support from OEM.
- Bidder should support the migration of the Current SIEM Correlation Rulesets, policies, operations, Integrations and features and building new New Correlation Rulesets, policies, operations, Integrations and features required by organization for the proposed solution during the implementation phase & during the entire product lifecycle thereafter for 3 years.
- The solution quoted by bidder should not be declared as EOL or EOS (End of Support) by the OEM before the last date of submission of RFP. Bidder to provide the details of the EOL or EOS (End of Support) timelines for the proposed components.
- Bidder to factor and propose hardware/software based solution entirely as per their architecture which includes but not limited to associated monitoring and management software(s) and database license if any.
- Appliances/ Hardware proposed by the bidder should have dual/ redundant power supply for each server/ components at DC and DR and fiber gigabit NIC adapter connectivity for each hardware component proposed.
- Bidder should demonstrate compliance to Technical requirements documented in this document for the solution implemented.
- The bidder / OEM shall provide 24*7*365 basis post implementation technical support for the components supplied. Support center must be based in INDIA.
- Implementation of the solution and migration of policies from existing solution to be done by Bidder/OEM directly. Resumes & Certifications of the team members/SME's to be shared as part of RFP response.
- Bidders are expected to provide the onsite support if the technical issues are not remotely resolved by them.
- Prior to configuration and integration, the bidder needs to understand the requirement of NPCI and prepare detailed implementation plan. On approval of the same by NPCI, integration of the Next Generation Security information and event management (SIEM)
- solution needs to be carried out. Detailed solution architecture, design, traffic flow and policies, integrations, rulesets (existing & proposed) should be documented. Deployment of the solution will start only after acceptance by NPCI.
- The Bidder shall develop a Project Management Plan & should be reviewed by OEM. The plan shall also detail all milestones and indicate when the required deliverable will be available to NPCI.
- The progress of the implementation shall be monitored on regular basis and the deviations, exceptions shall be analysed and corrective actions to be recommended / suggested / executed.
- The first monitoring report would be submitted on completion of 1 month from the date of acceptance of the Next Generation Security information and event management (SIEM) Solution and thereafter every fortnight with suggested/required remediation.
- The Bidder assess existing solution architecture & must prepare architecture design, optimize network to increase performance, documentation, project plan, SOP Documents and training document as part of the proposed solution & implementation services.

- Technical Training should be arranged by OEM directly.
- 3 days of Extensive SIEM OEM Administration & troubleshooting Training (SME Level) for NPCI officials & NPCI's service Providers for 15 People on the first year after implementation & for 15 People on second & third consecutive year.
- Post Implementation: Twice annually, OEM is required to review the Implementation, deployment, Health, Configuration check and suggest fine tuning according to industry best practices, a minimum 5-7 days per review & fine tuning effort of the OEM needs to be factored for implemented solution.
- Qualified resources as SIEM SME's with L2 - L3 Level Onsite Support for 3 years 16/7*365, basis with defined SLA in RFP. At least 1 Onsite engineer should present in Hyderabad 16/7*365 Days. Rest support will be on-call basis.

Technical specifications as per Annexure J

3.2 Single Point of Contact

The selected Bidder shall appoint a single point of contact, with whom NPCI will deal with, for any activity pertaining to the requirements of this RFP.

4.1 Eligibility Criteria

The Eligibility Criteria are furnished below:

A] Start-ups:

Sr. No	Eligibility Criteria
1	The bidder should be incorporated or registered in India under Companies Act/Partnership Act / Indian Trust Act (Annual filling with ROC) and should have the Certificate issued by Department for Promotion of Industry and Internal Trade (DPIIT) or in the process of applying the same and shall be submitted before a formal engagement with NPCI.
2	The bidder's annual turnover should be less than Rs. 100 crores as per audited financial statements in each of the financial years from the date of registration/ incorporation subject to compliance to Sr. No. 3
3	The date of incorporation of the bidder should be anywhere between 1 to 10 financial years.
4	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad.
5	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.
6	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission
7	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.
8	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.

B] Other than start-ups:

Sr. No	Eligibility Criteria	MSME	Other than MSME
1	Registration and incorporation	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act at least since **last 3 years**. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for **at least 2 years** as on date of submission of the bid. b. In case the bidder is the result of a demerger or hiving off, at least one of the demerged company or resulting company should have been in operation for **at least 2 years** as on the date of submission of bid.	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act **at least since last 5 years**. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for **at least 5 years** as on date of submission of the bid. b. In case the bidder is the result of a demerger or hiving off, at least one of the demerged company or resulting company should have been in operation for **at**

			least 5 years as on the date of submission of bid.
2	Turnover & profitability	The bidder should have reported minimum annual turnover of **Rs. 8 crore** and should have reported profits (profit after tax) as per audited financial statements in at least 2 out of last 3 financial years (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.	The bidder should have reported minimum annual turnover of **Rs. 20 crores** in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.
3	Governance – Statutory obligations	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.
4	Blacklisting	Neither the OEM nor the bidder should have been currently blacklisted by any Bank or institution in India or abroad	Neither the OEM nor the bidder should have been currently blacklisted by any Bank or institution in India or abroad
5	Manufacturer authorization (MAF)	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the

		once he is eligible for price discussion.	distribution channel once in any other capacity once he is eligible for price discussion.
6	Bid cost	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission.	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission.
7	Bid earnest money (EMD)	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.
8	Bid participation	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEM's product.	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEM's product.

Section 5 - Instruction to Bidders

5.1 RFP

RFP shall mean Request for Proposal. Bid, Tender and RFP are used to mean the same. The Bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding document. Submission of a bid not responsive to the bidding document in every respect will be at the Bidders risk and may result in the rejection of its bid without any further reference to the bidder.

5.2 Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its bid, and NPCI will in no case be responsible or liable for those costs.

5.3 Content of Bidding Document

The Bid shall be in 3 separate Folder A, B and C.

5.4 Clarifications of Bidding Documents

A prospective Bidder requiring any clarification of the bidding Documents may notify NPCI in writing through email any time prior to the deadline for receiving such queries as mentioned in Section 1. The subject of the email for pre-bid queries should be titled **"Pre-bid queries – RFP for procurement of Next Generation Security information and event management (SIEM) Solution - RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022."**

Bidders should submit the queries only in the format given below, in an **excel sheet**:

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)

Replies to all the clarifications, modifications will be received will be uploaded on NPCI website. Any modification to the bidding documents which may become necessary shall be made by NPCI by issuing an Addendum.

Please note that the responses to the pre-bid queries would become part of this RFP document.

5.5 Amendment of Bidding Documents

1. At any time prior to the deadline for submission of bids, NPCI may for any reason, whether at its own initiative or in response to a clarification requested by a Bidder, amend the Bidding Documents.
2. Amendments will be provided in the form of Addenda to the bidding documents, which will be posted in NPCI's website. Addenda will be binding on Bidders. It will be assumed that the amendments contained in such Addenda had been taken into account by the Bidder in its bid.
3. In order to afford Bidders reasonable time to take the amendment into account in preparing their bids, NPCI may, at its sole and absolute discretion, extend the deadline for the submission of bids, in which case, the extended deadline will be posted on NPCI's website.
4. From the date of issue, the Addenda to the tender shall be deemed to form an integral part of the RFP.

5.6 Earnest Money Deposit (EMD)

The Bidder is required to deposit Rs. 5,00,000/- (Rupees Five lakhs only) in the form of electronic fund transfer/Bank Guarantee in favor of "National Payments Corporation of India" payable at Mumbai or Bank Guarantee issued by a scheduled commercial bank valid for six (6) months, with a claim period of 12 months after the expiry of validity of the Bank Guarantee as per the statutory provisions in this regard, as per format in Annexure A1 or A2. No interest will be paid on the EMD.

The electronic / wire transfer can be done to designated NPCI bank account as detailed below:
Account Name: National Payments Corporation of India

Bank Name: HDFC Bank
Account No: 00600530001133
IFSC Code: HDFC0000060
Address: Maneckji Wadia Bldg., Ground Floor, Naik Motwani Marg, Fort, Mumbai – 400023
BSR Code: 0510062 SWIFT Code: HDFCINBBXXX

5.7 Return of EMD

The EMDs of successful Bidder/s shall be returned / refunded after furnishing Performance Bank Guarantee as required in this RFP. EMDs furnished by all unsuccessful Bidders will be returned on the expiration of the bid validity / finalization of successful Bidder, whichever is earlier.

5.8 Forfeiture of EMD

The EMD made by the bidder will be forfeited if:

1. Bidder withdraws its bid before opening of the bids.
2. Bidder withdraws its bid after opening of the bids but before Notification of Award.
3. Selected Bidder withdraws its bid / Proposal before furnishing Performance Bank Guarantee.
4. Bidder violates any of the provisions of the RFP up to submission of Performance Bank Guarantee.
5. Selected Bidder fails to accept the order within five days from the date of receipt of the order. However, NPCI reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.
6. Bidder fails to submit the Performance Bank Guarantee within stipulated period from the date of acceptance of the Purchase Order. In such instance, NPCI at its discretion may cancel the order placed on the selected Bidder without giving any notice.

5.9 Period of Validity of Bids

Bids shall remain valid for a period of 180 days after the date of bid opening as mentioned in Section 1 or as may be extended from time to time. NPCI reserves the right to reject a bid valid for a period shorter than 180 days as non-responsive, without any correspondence.

5.10 Extension of Period of Validity

In exceptional circumstances, prior to expiry of the bid validity period, NPCI may request the Bidders consent to an extension of the validity period. The request and response shall be made in writing. Extension of validity period by the Bidder should be unconditional and irrevocable. The EMD provided shall also be suitably extended. A Bidder may refuse the request without forfeiting the bid Security.

5.11 Format of Bid

The bidder shall prepare one copy (one PDF copy marked as ORIGINAL) of the Eligibility and Technical Bid only. **The commercial bid will be submitted as password protected PDF file.**

5.12 Signing of Bid

The Bid shall be signed by a person or persons duly authorized to sign on behalf of the Bidder. All pages of the bid, except for printed instruction manuals and specification sheets shall be initialed by the person or persons signing the bid.

The bid shall contain no interlineations, erasures, or overwriting, except to correct errors made by the Bidder, in which case such corrections shall be initialed by the person or persons signing the Bid.

The bid shall be signed by a person or persons duly authorized to bind the bidder to the contract. Such authority shall be either in the form of a written and duly stamped Power of Attorney (Annexure G) or a Board Resolution duly certified by the Company Secretary, which should accompany the Bid.

5.13 Bidding process

The Bid shall be prepared in 3 different folders i.e Folder A, Folder B and Folder C.
Each of the 3 folders shall be put into Folder marked as **"Request for Proposal for procurement of Next Generation Security information and event management (SIEM) Solution".**

In light of the lock imposed due to the COVID-19 pandemic, bids should be submitted through **email.** Folder A (Eligibility) & Folder B (Technical) and Folder C (Commercial) to the following email ids:
siddhesh.chalke@npci.org.in
benny.joseph@npci.org.in

5.14 Contents of the 3 Folders

Folder A - Eligibility Bid

The following documents as per the sequence listed shall be inserted inside Folder A:

1 Bid Earnest Money in the form of RTGS **OR** Bid Earnest Money in the form of Bank Guarantee – format provided in **Annexure A2**
2 Bid Offer form (without price) – **Annexure B**
3 Bidder Information – **Annexure C**
4 Declaration of Clean Track Record by Bidder – **Annexure D**
5 Declaration of Acceptance of Terms and Conditions – **Annexure E**
6 Declaration of Acceptance of Scope of Work – **Annexure F**
7 Power of Attorney for signing of bid – **Annexure G**
8 Eligibility Criteria Matrix – **Annexure H**
9 OEM/Manufacturer Authorization Letter – **Annexure I**
10 Audited Balance Sheet and Profit and Loss Statements, Auditors Reports & Notes to accounts for last 3 years
11 CA Certificate that the total turnover has never crossed Rs. 100 Cr since incorporation / registration (if more than 3 years) (only in case of Start-ups)
12 RFP document duly sealed and signed
13 All necessary supporting documents as per Annexures
14 RFP document duly sealed and signed by the authorized signatory on each page
15 All necessary supporting documents

Folder B - Technical Bid

The following documents shall be inserted inside Folder B:

1 Section 11 – Compliance to Technical Requirements duly completed - **Annexure J**
2 Client Details for **Annexure K**
3 Masked Price Bid (**Annexure M & N**)
4 Detailed Bill of Material for Software with line item details, giving quantity and functions - **Masked Annexure L**

Technical Bid Folder shall not include any financial information. If the Technical Bid contains any financial information the entire bid will be rejected**.**

Folder C - Commercial Bid (should be password encrypted)

1 Commercial Bid Form – **Annexure M**
2 Commercial Bid – **Annexure N**
3 Detailed Bill of Material – **Annexure L**

5.15 Bid Submission

The Bidder should bear all the costs associated with the preparation and submission of their bid and NPCI will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process. Bids sealed in accordance with the instructions to Bidders should be delivered at the address as mentioned in the Section 1.

The offers should be made strictly as per the formats enclosed. No columns of the tender should be left blank. Offers with insufficient/inaccurate information and offers which do not strictly comply with the stipulations given in this RFP, are liable for rejection.

5.16 Bid Currency

All prices shall be expressed in Indian Rupees only.

5.17 Bid Language

The bid shall be in English Language.

5.18 Rejection of Bid

The bid is liable to be rejected if the bid document:

a) Does not bear signature of authorized person.
b) Is received through Fax.
c) Is received after expiry of the due date and time stipulated for Bid submission.
d) Is incomplete / incorrect.
e) Does not include requisite documents.
f) Is Conditional.
g) Does not conform to the terms and conditions stipulated in this Request for Proposal.
h) No bid shall be rejected at the time of bid opening, except for late bids and those that do not conform to bidding terms.

5.19 Deadline for Submission

The last date of submission of bids is given in Section 1. However, the last date of submission may be amended by NPCI and shall be notified through its website.

5.20 Extension of Deadline for submission of Bid

NPCI may, at its discretion, extend this deadline for submission of bids by amending the bidding documents which will be informed through NPCI website, in which case all rights and obligations of NPCI and Bidders will thereafter be subject to the deadline as extended.

5.21 Late Bid

Bids received after the scheduled time will not be accepted by the NPCI under any circumstances. NPCI will not be responsible for any delay.

5.22 Modifications and Withdrawal of Bids

Bids once submitted will be treated, as final and no further correspondence will be entertained on this.

No bid will be modified after the deadline for submission of bids.

5.23 Right to Reject, Accept/Cancel the bid

NPCI reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever.

NPCI does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender without assigning any reason whatsoever. NPCI also reserves the right to re-issue the Tender without the Bidders having the right to object to such re-issue.

5.24 RFP Abandonment

NPCI may at its discretion abandon the process of the selection of bidder at any time before notification of award.

5.25 Bid Evaluation Process

The Bid Evaluation will be carried out in 2 stages:

Stage 1 -Folder 'A' i.e. Eligibility bid and **Folder 'B'** i.e. Technical bid will be evaluated. Only those Bidders who have submitted all the required forms comply with the eligibility and technical criteria will be considered for further evaluation.

Stage 2 -Folder 'C' of those Bidders who qualify the eligibility and technical criteria will be evaluated.

5.26 Single bid

In the event of only one responsive bidder or only one bidder emerging after the evaluation process, NPCI may continue with the RFP process.

5.27 Price discovery method:

Bidder to submit their best price. NPCI reserves right to discover the lowest price through the Reverse Auction and/or may be deliberated through Price Discussion Committee if so opted by NPCI management. If first Reverse Auction does not result successful, NPCI reserves the right to call technical qualified bidders for price discussion and declare the successful bidder through Price discussion method instead of conducting 2nd Reverse Auction. The decision with respect to conduct of 2nd Reverse Auction or otherwise shall be communicated to technically qualified bidders.

5.28 Contacting NPCI

From the time of bid opening to the time of Contract award, if any Bidder wishes to contact NPCI for seeking any clarification in any matter related to the bid, they should do so in writing by seeking such clarification/s from an authorized person. Any attempt to contact NPCI with a view to canvas for a bid or put any pressure on any official of the NPCI may entail disqualification of the concerned Bidder and/or its Bid.

Section 6 - Bid Opening

6.1 Opening of Bids

Bids will be opened in 2 stages:

Stage 1 – Opening of Eligibility and Technical Bids: In the first stage the Eligibility bid i.e. Folder 'A' and Technical Bid i.e. Folder 'B' will be opened. NPCI will open Eligibility bids (Folder 'A') and Technical bid (Folder 'B') on the date, time and address mentioned in Section 1 or as amended by NPCI from time to time.

Stage 2 – Opening of Folder C - Commercial Bids i.e. Folder 'C' will be opened for technically qualified bidders.

Bidder to submit their best price. Commercial bids will be opened for Reverse Auction **or** Price discussion(PDC) method with technically qualified bidders if so opted by NPCI management. In case, Commercial evaluation will be done through Reverse Auction, Business Rules and Terms & Conditions and Procedures of Reverse Auction have been published on NPCI's website i.e. www.npci.org.in

Section 7 - Bid Evaluation

7.1 Preliminary Examination of Eligibility Bids

NPCI will examine the bids to determine whether they are complete; whether the required information have been provided as underlined in the bid document; whether the documents have been properly signed and whether the bids are generally in order. Eligibility and compliance to all the forms and Annexure would be the first level of evaluation. Only those Bids which comply to the eligibility criteria will be taken up for further technical evaluation. NPCI may waive any minor informality, non-conformity or irregularity in a bid that does not constitute a material deviation provided such waiver does not prejudice or affect the relative ranking of any Bidder. If a Bid is not substantially responsive, it will be rejected by NPCI and may not subsequently be made responsive by the Bidder by correction of the nonconformity. NPCI's determination of bid responsiveness will be based on the content of the bid itself. NPCI may interact with the Customer references submitted by Bidder, if required.

7.2 Examination of Technical Bids

The Technical Evaluation will be based on the following broad parameters:

a. Compliance to Technical Specifications as specified in the RFP.
b. NPCI reserves the right to call for presentation and discussions on the approach of execution of project etc., from the short-listed Bidders based on the technical bids submitted by them to make an evaluation. Such presentations and minutes of meetings will become part of the technical bid.
c. Review of written reply, if any, submitted in response to the clarification sought by NPCI, if any.
d. Submission of duly signed compliance statement as stipulated in Annexures. Details / Brochures containing details about the proposed hardware are to be enclosed.
e. To assist in the examination, evaluation and comparison of bids, NPCI may, at its discretion, ask any or all the Bidders for clarification and response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.
f. NPCI may interact with the Customer references submitted by bidder, if required.
g. NPCI reserves the right to shortlist bidders based on technical evaluation criteria.
h. Bidder should re-submit 2 detailed Bill of material, BOM (one with commercial to IT procurement team and another without commercial to user team) within 3 days if there are any shortfall in BOM found during technical presentation.

7.3 Technical Scoring Matrix:

TECHNICAL SCORING MATRIX		
Sr. No.	**Description**	**Score**
Technical Evaluation Part - A		30
1	Technical Requirements compliance	
2	Clarity of requirements specified in RFP	
Part - B Vendor Evaluation Matrix		25
1	Customer BFSI reference in India Please provide at least 3 India References (Combination of Bidder + OEM reference would be an added advantage) including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	
2	Work experience in past (similar project)	
Proposed Solution Part - C		25
1	Approach /Methodology /Quality of Sample reports and RFP documentation	
2	Comprehensiveness of the documents & Project Management Plan	
3	Clarity thought of delivery & Support	
RFP Presentation Part - D		20
1	RFP presentation	

2	Q and A	
	Total Score of Part - A, B, C and D	100

Scoring Matrix: Bidders scoring a minimum of **75%** marks would be eligible for the commercial bid opening.

Basis technical presentation if there are any changes in the BOM, bidders are expected to share the updated BOM with commercials to IT procurement and BOM without commercials to business user team within 3 days. Bidders who do not share the BOM within 3 days will be disqualified.

In the event of only one responsive bidder or only one bidder emerging after the evaluation process, NPCI may continue with the RFP process.

7.4 Evaluation of Commercial Bids:

NPCI reserves the right to discover the lowest price through the Reverse Auction OR Price discussion mechanism or both if so opted by NPCI management. NPCI will inform the method of price negotiation to technically qualified bidders.

If first Reverse Auction does not result successful, NPCI reserves the right to call technical qualified bidders for price discussion and declare the successful bidder through Price discussion method instead of conducting 2nd Reverse Auction. The decision with respect to conduct of 2nd Reverse Auction or otherwise shall be communicated to technically qualified bidders. In case, Commercial evaluation will be done through Reverse Auction, Business Rules and Terms & Conditions and Procedures of Reverse Auction have been published on NPCI's website i.e. **www.npci.org.in**

7.5 Successful Evaluated bidder:
The bidder with lowest commercial bid as per Clause 7.4 will be declared as the successful bidder.

In case such Successful Bidder fails to start performing the work required under the Purchase order/Contract, NPCI reserves the right to cancel the Purchase Order/ Contract and de-bar such bidder from participating in future RFPs/ enquiries, if though fit so to do by NPCI. NPCI decision in this respect shall be final and binding on the bidders.

NPCI reserves the right to place the order with the L2 bidder, in case the L1 bidder refuses to accept the order or otherwise gets disqualified as per the terms of the RFP, provided the L2 bidder matches the price quoted by the L1 bidder. In case the 2nd lowest bidder is unable to match the L1 price, NPCI reserves the right to place order with the shortlisted L3 bidder and so on.

8.1 Notification of Award / Purchase Order

After selection of the L1 bidder, as given in Clause # 7.5, and after obtaining internal approvals and prior to expiration of the period of Bid validity, NPCI will send Notification of Award / Purchase Order to the selected Bidder. Once the selected Bidder accepts the Notification of Award the selected Bidder shall furnish the Performance Bank Guarantee to NPCI.

8.2 Term of the Order

The term of the Notification of Award/Purchase Order shall be for a period of 3 years wherein the price of the deliverables as specified in the RFP would be at a fixed rate.

8.3 Acceptance Procedure

- Within 5 days of receipt of Notification of Award/Purchase Order the successful Bidder shall send the acceptance.
- Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award.

8.4 Performance Bank Guarantee

The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.

8.5 Taxes and Duties

- All taxes deductible at source, if any, shall be deducted at as per then prevailing rates at the time of release of payments.
- Prices shall be exclusive of all taxes.
- The bidder shall meet the requirements of applicable Goods & Services Tax (GST).
- If the invoice raised in any financial year is not settled on or before 30th September of the next financial year, the bidder would be liable to provide a fresh invoice or will accept payment without reimbursement of the GST portion related to such invoice.
- All taxes, if any, shall be deducted at source as per the prevailing rate at the time of release of payments. In case the successful bidder is eligible for "No deduction" or "Lower rate for deduction" of applicable tax at source than the rate prescribed by the Income Tax Act then, the successful bidder shall submit the necessary certificate issued be competent Income Tax authority valid for the period pertaining to the payment. The successful bidder shall meet the requirements of the extant GST legislations.
- If NPCI requests, the successful bidder shall confirm to NPCI in writing that the GST amount charged in invoice is declared in its GSTR-1 and GSTR-3B and payment of GST and other requisite taxes in relation to the invoice has been made. NPCI, in its sole discretion, may decide in consultation with the successful bidder that the invoice will be paid in two batches (i) Base Amount (ii) Tax Amount. NPCI, in its sole discretion, may decide that tax Amount will be paid only after the successful bidder provides sufficient proof that the GST amount charged in invoice is declared in its GSTR-1 and GSTR-3B and payment of requisite taxes has been made.
- The successful bidder agrees to ensure proper discharge of tax liability within statutory time periods with respect to all payments made or to be made to the successful bidder by NPCI. In the event of failure, non-compliance by the successful bidder with the extant GST legislations/Rules and the terms of this clause (including non-compliance that leads to input tax credit not being available to NPCI), NPCI shall be entitled to not release payment and payment shall be kept on hold till such discrepancy is resolved by the successful bidder. Such holding of payments by NPCI

shall not be a breach of its obligations under this Purchase Order. In case of any disputes due to non-matching of GST credit, same shall be resolved by the successful bidder within 30 days of intimation by NPCI, failing which NPCI shall not remit the invoice amount.

- NPCI reserves the right to impose penalty of such amount as may be determined by it up to the value of GST amount involved and any corresponding damages as it may feel appropriate resulting from the successful bidder's breach of any condition or Rule/Regulation of the extant GST legislations or any other applicable tax laws/regulations.

8.6 Invoicing Requirements:

- Invoice/debit note/credit note needs to be issued within 30 days from the date of provision of Deliverables or completion of Services. Further, the invoices/debit note/credit note must cover all the particulars prescribed under GST Invoice Rules. The Successful bidder agrees to comply with invoicing requirements as per GST Invoice Rules and the terms of this clause (including e-invoicing requirements) and/or any other requirement as may be notified by the tax authorities from time to time.
- The Successful bidder invoices/debit note/credit note should be received by NPCI within 2 weeks from the date of issue of invoice.
- The Successful bidder has the obligation to raise invoices/debit note/credit note basis the correct addresses and registration number of the relevant NPCI branch as listed in the Purchase Order

8.7 Timely Provision of Invoices/ Debit Note/ Credit Note:

All necessary invoices and/or adjustment entries to an invoice (Credit Note, Purchase Returns, and Debit Notes) shall be submitted to NPCI by the Successful bidder before September of the succeeding financial year

8.8 Key Deliverables

The bidder shall provide following deliverables:

1. Supply, installation, maintenance and post implementation support for the entire Next Generation SIEM solution (Software, Hardware, License for OS core based, license for DB core based with unliFmited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials(BOM).
2. Compliance for Software/Instance supplied by bidder/OEM. Readiness/Compatibility - Virtualization-Compatible, Server Should be OS Agnostic. Virtualization Environments Should support Open source Virtualization Platforms/ environments such as Open stack, LinuxKVM etc.
3. Implementation of the complete solution
4. Integrate SIEM with all existing applications, infra tools such as AD, PIM, SIEM, SOAR, etc.
5. Detailed Implementation reports, detailed HLD's & detailed LLD's.
6. Detailed SOP's for all standard & advanced SIEM procedures including but not limited to Daily Operations, Monitoring, Failovers, integrations, addition of new Correlation rules, improving correlation rules etc.
7. 3 days of extensive SIET-7 days per review & fine tuning effort of the OEM needs to be factored for implemented solution.

8.9 Delivery Address:

Data Center – Hyderabad
NPCI, - C/o Reliance Communications Ltd.,
Plot No 20, Survey No 64,
Opp. Mahindra Satyam,
Hitec City Layout,
Madhapur, R.R. Dist.- Hyderabad - 500019.

Data Center – Chennai
NPCI, C/o STT Global Centers India Pvt Ltd,
Tiruvalluvar Satellite Earth Solution,
No. 226, Red Hills Road, Kallikuppam,
Ambattur, Chennai.

8.10 Delivery schedule

Delivery, installation & commissioning of the Next Generation Security information and event management (SIEM) solution should be completed within 16 weeks from the date of receipt of purchase order.

- Delivery of hardware, software, and license should be within 6 weeks.
- Installation & commissioning should be completed in next 10 weeks.
- Installation Certificate for each installation should be signed by NPCI and the bidder

8.11 Penalty for default in delivery

If the successful bidder does not deliver & implement the solution as per the above delivery schedule, or such authorized extension of delivery period as may be permitted in writing by NPCI, NPCI shall impose a penalty as given below:

- Non Delivery of above at NPCI - at the rate of 0.5% of the total Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5% of the PO value.
- In case the delay exceeds 10 days beyond the stipulated delivery period of RFP, NPCI reserves the right to cancel the order without prejudice to other remedies available to NPCI
- Without any prejudice to NPCI's other rights under the Applicable Law, NPCI may recover the liquidated damages, if any, accruing to NPCI, as above, from any amount payable to the supplier, as per the Agreement.

8.12 End of Sale

The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.

8.13 Warranties

The successful bidder(s) shall provide comprehensive on-site warranty for 3 years for complete Solution with back to back arrangements with the respective OEM from the date of acceptance of hardware / software.

- ✓ The deliverable(s) should not have been declared End of Sale as on the date of submission of the bid and on the date of delivery.
- ✓ The successful bidder(s) should ensure that the equipment proposed in this RFP, should not be declared as End of Life (EOL) or End of Support (EOS) by the OEM within the 3 years contract period.
- ✓ If the deliverable(s) is declared End of Life (EOL) or End of Support anytime during the contract period, the successful bidder shall forthwith replace the equipment at no additional cost to NPCI.
- ✓ Bidder shall also update necessary OS, Patches and should support the hardware and the software for the period of three years from the date of acceptance of the entire system.
- ✓ The upgrades, new releases (Minor/major) versions, bug fixes etc. for the hardware and system software will be supplied to NPCI at no extra cost, with the necessary documentation during contract period.
- ✓ Bidder shall implement all software updates, new releases & version upgrades on the supplied components during the warranty period. Bidder should update and maintain all supplied components to correctly reflect actual state of the setup at any point in time during the warranty period.
- ✓ Bidder guarantees the whole of the Goods against any defects or failure, which arise due to faulty materials, workmanship or design (except materials or design furnished by NPCI).If during the Warranty Period any Goods/software are found to be damaged or defective or not acceptable, they shall promptly be replaced or rectified /re-furnished or rendered by Bidder at its own cost (including the cost of dismantling and reinstallation) on the request of NPCI and if removed from the Site for such purpose, Bidder has to provide standby Goods till the original

Goods are repaired or replaced / re-furnished, rendered. All goods shall be removed and redelivered to NPCI by Bidder at its own cost. Bidder shall have to submit Performance

8.14 Support

The successful bidder shall provide comprehensive on-site support of the solution for a period of 3 years with back to back support with the OEM.

- All the terms and conditions of the Purchase Order will be applicable during such support period.
- 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.
- Bidder shall provide and install patches/ updates/ version upgrades of all software provided under this contract at no extra cost to NPCI during Warranty period.
- Bidder guarantees the whole of the Goods against any defects or failure, which arise due to faulty materials, workmanship or design (except materials or design furnished by NPCI).If during the Warranty Period any Goods/software are found to be damaged or defective or not acceptable, they shall promptly be replaced or rectified /re-furnished or rendered by Bidder at its own cost (including the cost of dismantling and reinstallation) on the request of NPCI and if removed from the Site for such purpose, Bidder has to provide standby Goods till the original Goods are repaired or replaced / re-furnished, rendered. All goods shall be removed and redelivered to NPCI by Bidder at its own cost

8.15 Service Level Requirements (SLA)

The SLA specifies the expected levels of service to be provided by the Bidder to NPCI. This expected level is also called the baseline. Any degradation in the performance of the solution and services is subject to levying penalties.

Payments to the Bidder are linked to the compliance with the SLA metrics. During the contract period, it is envisaged that there could be changes to the SLAs, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e. NPCI and Bidder.

The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to NPCI or its designated personnel to the tools used for SLA monitoring.

Definitions

1. "Availability" means the time for which the services and facilities are available for conducting operations on the AIC system including application and associated infrastructure.
   Availability is defined as (%) = (Operation Hours –Downtime) * 100%
   (Operation Hours)
2. The business hours are 24*7*365 on any calendar day the NPCI is operational.
3. All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.
4. The "Operation Hours" for a given time frame are calculated after deducting the planned downtime from "Operation Hours". The Operation Hours will be taken on 24x7 basis, for the purpose of meeting the Service Level requirements i.e. availability and performance measurements both.
5. "Downtime" is the actual duration for which the system was not able to service NPCI or the Clients of NPCI, due to System or Infrastructure failure as defined by NPCI and agreed by the Bidder.
6. "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during business hours. Further, scheduled maintenance time is planned downtime with the prior permission of NPCI.

7. "Incident" refers to any event / abnormalities in the functioning of any of IT Equipment / Services that may lead to disruption in normal operations of the Data Centre, System or Application services.

Interpretation & General Instructions

1. Typical Resolution time will be applicable if systems are not available to the NPCI's users.
2. The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. The Bidder is expected to provide the following service levels. In case the service levels defined in the tables below cannot be achieved, it shall result in a breach of contract and invoke the penalty clause.
3. A Service Level violation will occur if the Bidder fails to meet Minimum Service Levels on a monthly basis for a particular Service Level.
4. Quarterly SLAs would be analyzed. However, there would be month wise SLAs and all SLA targets have to be met on a monthly basis.
5. Overall Availability and Performance Measurements will be on a quarterly basis for the purpose of Service Level reporting. Month wise "Availability and Performance Report" will be provided by the Bidder for every quarter in the NPCI suggested format and a review shall be conducted based on this report. Availability and Performance Report provided to NPCI shall contain the summary of all incidents reported and associated performance measurement for that period.
6. The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for cutting fees.

Severity Levels

Severity Definition during Live operations due to Infrastructure/Functional issues of the proposed solution, the SLA's will be applicable post go-live of Compliance Solution at DC, DRS and other NPCI Offices.

Description: Time taken to resolve the reported problem Severity is defined as:

Level	Function/Technologies
Severity 1	i Such class of errors will include problems, which prevent users from making operational use of solution. ii Security Incidents iii No work-around or manual process available iv Financial impact on NPCI v Infrastructure related to providing solution to the NPCI users comprising of but not limited to the following: a. Proposed Solution Tools / Application Servers b. Proposed Solution Database Servers / Appliance c. Proposed Solution servers/appliances d. Network components, if any proposed by the bidder
Severity 2	i Any incident which is not classified as "Severity 1" for which an acceptable workaround has been provided by the Bidder or; ii Any problem due to which the Severity 2 infrastructure of the proposed solution is not available to the NPCI users or does not perform according to the defined performance and query processing parameters required as per the RFP or; iii Users face severe functional restrictions in the application irrespective of the cause. iv Key business infrastructure, systems and support services comprising of but not limited to the following: a The Solution Test & Development and Training Infrastructure and Application b Infrastructure for providing access of dashboards, scorecards, etc.

Severity 3	i	Any incident which is not classified as "Severity 2" for which an acceptable workaround has been provided by the Bidder;
	ii	Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround.
	iii	No impact on processing of normal business activities
	iv	Equipment/system/Applications issues and has no impact on the normal operations/day-today working.
	v	All other residuary proposed solution Infrastructure not defined in "Severity 1" & "Severity 2"

During the term of the contract, the bidder will maintain the solution in perfect working order and condition and for this purpose will provide the following repairs and maintenance services

Onsite Resource SLAs:

Defined Severity Levels -

Severity 1 – (Incidents mentioned but not limited to)

- Unable to capture events from End devices due to non-availability of the solution.
- Unable to detect critical & High security events on SIEM dashboard
- Non-availability of the SIEM solution for more than 15 Minutes

Severity 2 - (Incidents mentioned but not limited to)

- No Proper Parsing of the all log resources
- Timely update of the Content on SIEM
- Unrelieved Configuration change on SIEM resulting into Outage

Severity 3 - (Incidents mentioned but not limited to)

- Incidents which doesn't fall under Severity 1 & Severity 2 Category will be considered as Severity 3.
- NPCI will impose a maximum penalty of 20% of the overall quarterly SIEM operations charges per quarter.
- Severity of incident will be validated by the NPCI, NPCI reserves the right to define incident severity which falls/doesn't falls under mentioned category
- Fraction of a week beyond 3 days including holidays of that week of delay will be considered as a complete week of delay.
- The maximum penalty due to non-adherence of SLA will not exceed 10% of the total cost of the project calculated up to and as on the date when such penalty is required to be charged. However, in addition to the above penalty, the NPCI may invoke Bank Guarantee submitted by the bidder if the bidder fails to adhere to SLA or any of the terms & conditions in the RFP.
- For any delay for which the reasons are not solely and directly attributable to NPCI, the timelines for deliverables (like Agreement Validity, BG Validity, Warranty etc) shall be suitably extended.
- Bidder should provide professional support for the entire SIEM solution & its components, to remediate, bug fixes, upgradation and other maintenance activities throughout the Contract without any additional cost to NPCI.

8.15 Penalty on non-adherence to SLAs:

The following Resolution Service Level Agreement (SLA) would be applicable during Warranty are applicable for critical and non-critical incidents. The reported issue would be classified as Critical or Non-Critical by NPCI only.

a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand

only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total value.

b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR 5,000/- (Indian Rupees Five Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 10,000 for each hour with a max cap of 5% of total value.

c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of INR 2,000/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total value.

d) The penalty amount would be calculated and deducted from the performance bank guarantee during warranty period.

e) Further if the number of downtime instances during a month exceeds 3 times, an additional 0.50% downtime will be reduced from uptime and the penalty will be calculated accordingly.

f) If a breach occurs & goes undetected even after a proper rule/policy in SIEM solution is in place, a penalty of Rs. 10,000/- per event will be deducted or the loss due to the breach whichever is higher. The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the NPCI such as termination of contract, invoking performance guarantee and recovery of amount paid etc.

Penalty for default of SLA by Bidders Onsite Resources:

Service Level Category	SLA Measurement & Failure Indicator	Penalty Calculation
Onsite personnel resources	• <70% of required strength • <50% of required strength • <25% of required strength	• Rs. 10000/- per resource per week • Rs. 15000/- per resource per week • Rs. 20000/- per resource per week Penalty Calculation starts from the day of breach of SLA until the required strength is achieved.
Non-detection of security incidents by SIEM	• From the date of Production Go-Live	• Rs. 10000/- per incident Rs. 1 Lakh per Critical / High incident Rs. 25,000 per Medium incident
Services Offered by Onsite Personnel Resources	• Severity 1 – Response time – 15 Minutes Resolution time – 30 Minutes • Severity 2 – Response time – 30 Minutes Resolution time – 60 Minutes • Severity 3 – Response time – 180 Minutes Resolution time – 24 Hours	Penalty In case of SLA breach for Sev 1,2,3 Issues - • Rs. 20000/- per Severity 1 incident • Rs. 10000/- per Severity 2 incident • Rs.5000/- per Severity 3 incident

Non-Compliance of Terms & conditions (T& C) mentioned in this RFP	- Major T&C Non-compliance - Minor T&C Non-compliance	• Rs. 20,000 per week per Terms & Conditions • Rs. 10,000 per week per Terms& Conditions

8.16 Prices

Price shall remain fixed for a period of 3 years from the date of issuance of 1st Purchase Order. There shall be no increase in price for any reason whatsoever and therefore no request for any escalation of the cost / price shall be entertained.

8.17 Repeat Order:

NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the deliverables included in the Solution at the agreed unit rate for individual categories of purchase order during the period of 3 years from the date of award / 1st Purchase Order.

8.18 Product Upgrades

Notwithstanding what is contained and provided in Clause 8.9 herein above, at any time during term of the purchase order / performance of the Contract, should technological advances be introduced by the OEM/ Bidder for information technologies originally offered by the supplier in its bid and still to be delivered, the bidder shall be obliged to offer to NPCI the latest version of the available technologies having equal or better performance or functionality throughout the contract period without any extra cost to NPCI.

During performance of the Contract, the bidder shall offer to NPCI all new versions, releases and updates of standard software, as well as related technical support within 30 days of their availability from the OEM.

8.19 Payment Terms:

- **Hardware**: Payment shall be released within 30 days after submission of correct invoice along with necessary supporting documents along with hardware delivery report duly signed by NPCI officials
- **Software/Licenses**: Payment shall be released within 30 days after delivery of the software /licenses along submission of correct invoice with necessary supporting documents and delivery/installation report duly signed by NPCI officials
- **Installation/Implementation Charges**: Payment shall be released within 30 days after successful implementation upon submission of correct invoice along with necessary supporting documents i.e. implementation/installation report duly signed by NPCI officials.
- **AMC**: Payment shall be made quarterly in arrears within 30 days from the date of receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.
- If the invoice raised in any financial year is not settled on or before 30th September of the next financial year, the vendor would be liable to provide a fresh invoice or will accept payment without reimbursement of the GST portion related to such invoice.
- The vendor shall comply with all the applicable Goods & Services Tax (GST) legislations as decided by the Government from time to time.
- Payment will be released within 30 days of receipt of correct invoices along with necessary documents / certificates duly signed by authorized NPCI official.
- For the purpose of payment, the end of the quarter will be June, Sept, Dec and March.
  Invoice shall contain all details regarding PAN & registration number for GST

8.20 Migration activities for change of location:

In case NPCI wishes to shift the devices from one place to another anywhere in the country e.g. Data centre Migration, adequate support will be made available by the bidder by arranging field engineer for the purpose of dismantling of devices/software/service supplied by Service provider/bidder & 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/bidder. 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 reinstallation 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 - bidder provided resource to integrate devices delivered at required location or Data Center & coordinate with NPCI NOC to extend the reachability.

8.21 Confidentiality

The Successful bidder shall treat the details of this PO and other contract documents executed between NPCI and the successful bidder as secret and confidential. The Successful bidder shall execute separate NDA on the lines of the format provided in the Annexure Z hereof.

In the event of disclosure of Confidential Information to a third party in violation of the provisions of this Clause, the Successful bidder shall use all reasonable endeavors to assist NPCI in recovering and preventing such third party from using, selling or otherwise disseminating of such information. The Parties' obligations under this Section shall extend to the non-publicizing of any dispute arising out of PO.

The terms of this clause shall continue in full force and effect for a period of five (5) years from the date of disclosure of such Confidential Information.

In the event of termination of this PO, upon written request of the NPCI, The Successful bidder shall immediately return the Confidential Information of NPCI, or at the NPCI's option destroy any remaining Confidential Information and certify that such destruction has taken place.

8.22 Indemnity

The bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting from any act or omission or negligence or misconduct of the bidder and its employees and representatives, breach of the terms and conditions of the agreement or purchase order, false statement by the bidder, employment claims of employees of the bidder, third party claims arising due to infringement of intellectual property rights, death or personal injury attributable to acts or omission of bidder, violation of statutory and regulatory provisions including labour laws, laws related to information technology and intellectual property rights, breach of confidentiality obligations, breach of warranty, etc.

Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect, consequential and incidental damages and compensation. Bidder shall indemnify NPCI, provided NPCI promptly notifies the Bidder in writing of such claims and the Bidder shall have the right to undertake the sole defense and control of any such claim.

8.23 Bidder's Liability

The selected Bidder will be liable for all the deliverables.

The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract/purchase order.

The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.

8.24 Obligations of the Bidder

Standard of Performance: The Bidder shall perform the services and carry out their obligations with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment materials and methods. The Bidder shall always act in respect of any matter relating to this Contract or to the services as faithful advisor to NPCI and shall at all times support and safeguard NPCI's legitimate interests in any dealings with third parties.

Prohibition of Conflicting Activities: The Bidder shall not engage and shall cause their personnel not to engage in any business or professional activities that would come in conflict with the activities assigned to them under this RFP.

8.25 Exit option and contract re-negotiation

a) NPCI reserves its right to cancel the order in the event of happening of one or more of the situations as mentioned in the "Order Cancellation" herein under.
b) Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder should continue to provide the facilities to NPCI at NPCI's locations.
c) Reverse transition mechanism would be activated in the event of cancellation of the contract or exit by the bidders prior to expiry of time for awarding the final bid / the contract. The Bidder should perform a reverse transition mechanism to NPCI or its selected vendor. The reverse transition mechanism would facilitate an orderly transfer of services to NPCI or to an alternative 3rd party / vendor nominated by NPCI. Where NPCI elects to transfer the responsibility for service delivery to a number of vendors, NPCI will nominate a vendor who will be responsible for all dealings with the Bidder regarding the delivery of the reverse transition services.
d) The reverse transition services to be provided by the Bidder shall include the following:
    i. The Bidder shall suitably and adequately train NPCI or its designated team for fully and effectively manning, operating the Devices.
    ii. Bidder shall provide adequate documentation thereof.
    iii. The Bidder shall jointly manage the Devices with NPCI or designated team for a reasonable period of time
e) Knowledge Transfer: The Bidder shall provide such necessary information, documentation to NPCI or its designee, for the effective management and maintenance of the Deliverables under this RFP/Purchase Order/contract. Bidder shall provide documentation (in English) in electronic form where available or otherwise a single hardcopy of all existing procedures, policies and programs required for supporting the Services.
f) Warranties:
    1. All the warranties held by or in the name of the bidder shall be assigned or transferred as-is, in the name of NPCI. The bidder shall execute any and all such documents as may be necessary in this regard.
    2. The bidder shall return confidential information and will sign off and acknowledge the return of such confidential information.
    3. The bidder shall provide all other services as may be agreed by the parties in connection with the reverse transition services. However, in case any other services, in addition to the above are needed, the same shall be scoped and priced.
    4. The bidder recognizes that considering the enormity of the assignment, the transition services listed herein are only indicative in nature and the bidder agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the bidder under the scope, upon termination or expiration thereof, for any reason whatsoever.
g) The rates for availing services during reverse transition period would be the same as payable during the contract period for the respective services as contained and provided in this RFP.
h) During which the existing Bidder would transfer all knowledge, know-how and other things necessary for NPCI or new bidder to take over and continue to manage the services. The Bidder

agrees that the reverse transition mechanism and support during reverse transition will not be compromised or affected for reasons whatsoever is for cancellation.

i) NPCI shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.
j) NPCI and the successful bidder shall together prepare the Reverse Transition Plan. However, NPCI shall have the sole decision to ascertain whether such Plan has been complied with.
k) The Bidder agrees that in the event of cancellation or exit or expiry of the RFP/Purchase Order/contract it would extend all necessary support to NPCI or its selected vendors as would be required

8.26 Extension of Contract

The bidder shall be required to consistently execute, in a successful and professional manner, the jobs assigned under this RFP or subsequent Purchase Order / Contract, as shall be entered by NPCI with the Bidder, to the satisfaction of and as decided by the NPCI up to a period of three (3) years (completion period) reckoned from the date of commencement of the services and may be extended for further period on satisfactory performance by bidder. However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 6 months' period on the same rates and terms & conditions of the Contract. NPCI has right to alter (increase or decrease) the number of resources. NPCI has right to place repeat order to the bidder for any resources mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by NPCI.

8.27 Order Cancellation

NPCI reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to NPCI alone;

i. Delay in delivery is beyond the specified period as set out in the Purchase Order before acceptance of the product; or,
ii. Serious discrepancy in the quality of service expected.
iii. If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the bidder turns out to be incorrect and/or bidder conceals or suppresses material information.

In case of order cancellation, any payments made by NPCI to the Bidder for the particular service would necessarily have to be returned to NPCI with interest @ 15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the Purchase Order and any additional expenditure to be incurred by NPCI to appoint any other Bidder. This is after repaying the original amount paid.

8.28 Termination of Purchase Order/Contract

For Convenience: NPCI, by written notice sent to Bidder, may terminate the Purchase Order/ contract in whole or in part at any time for its convenience giving three months' prior notice. The notice of termination may specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective. NPCI shall consider request of the bidder for pro-rata payment till the date of termination.

For Insolvency: NPCI at any time may terminate the contract by giving written notice to Bidder, if Bidder becomes bankrupt or insolvent. In this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to NPCI.

For Non-Performance: NPCI reserves its right to terminate the contract in the event of Bidder's repeated failures (say more than 3 occasions in a calendar year to maintain the service level prescribed by NPCI).

8.29 Effect of Termination

- The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment.

- Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services
- The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by NPCI, continue to provide facility to NPCI at no less favorable terms than those contained in this RFP. In case NPCI wants to continue with the Bidder's facility after the completion of this contract then the Bidder shall offer the same terms to NPCI.
- NPCI shall make such prorated payment for services rendered by the Bidder and accepted by NPCI at the sole discretion of NPCI in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to the Bidder.
- NPCI may make payments of undisputed amounts to the Bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies NPCI may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.
- Upon cancellation of contract/completion of period of service, the Bidder should peacefully handover the legal possession of all the assets provided and obtains discharge from NPCI. NPCI also reserves the right to assign or allot or award the contract to any third party upon cancellation of the availed services.

8.30 Force Majeure

For purpose of this clause, "Force Majeure" means an unforeseeable event beyond the control of the successful and not involving NPCI or the successful 's fault or negligence.

If either party is prevented, restricted, delayed or interfered by reason of: a) Fire, explosion, cyclone, floods, droughts, earthquakes, epidemics; b) War, revolution, acts of public enemies, blockage or embargo, riots and civil commotion; c) Any law, order, proclamation, ordinance or requirements of any Government or authority or representative of any such Government, including restrictive trade practices or regulations; d) Strikes, shutdowns or labour disputes which are not instigated for the purpose of avoiding obligations herein; or e) Any other circumstances beyond the control of the party affected; then notwithstanding anything here before contained, the party affected shall not be liable for non-performance of delay in performance of its obligations contained herein provided the party so affected uses its best efforts to remove such cause of non-performance, and when such cause is removed the party shall continue performance in accordance with the terms of the Purchase Order.

Each of the parties agrees to give written notice forthwith to the other upon becoming aware of an event of Force Majeure, the said notice to contain details of the circumstances giving rise to the event of Force Majeure. If the event of Force Majeure continues for more than twenty (20) days, either party shall be entitled to terminate the Purchase Order at any time thereafter by giving written notice to the other party

8.31 Resolution of Disputes

All disputes or differences between NPCI and the bidder shall be settled amicably. If, however, the parties are not able to resolve them, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

NPCI and the successful Bidder shall make every effort to resolve amicably by direct informal negotiation; any disagreement or dispute arising between them under or in connection with this RFP.

If, however, NPCI and successful Bidder are not able to resolve them, following dispute resolution mechanism shall be applied:

1. In case of Dispute or difference arising between NPCI and the successful Bidder relating to any matter arising out of or connected with this RFP, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators, one each to be appointed by NPCI and the successful Bidder. The third Arbitrator shall be chosen by mutual discussion between NPCI and the successful Bidder.

2. Arbitration proceedings shall be held at Mumbai, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English;
3. The decision of the majority of Arbitrators shall be final and binding upon NPCI and Successful Bidder. The cost and expenses of Arbitration proceedings will be paid as determined by mutual chosen third Arbitrator. However, the expenses incurred by each party in connection with the preparation, presentation, etc., of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself; and
4. Where the value of the contract is Rs.1.00 Crore and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator should be appointed by mutual consent between the parties.
5. Any appeal will be subject to the exclusive jurisdiction of courts at Mumbai.

8.32 Compliance with Applicable Laws of India

The Bidder confirms to NPCI that it complies with all Central , State, Municipal laws and local laws and rules and regulations and shall undertake to observe, adhere to, abide by, comply with and notify NPCI about compliance with all laws in force including Information Technology Act 2000, or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and for all purposes of this RFP, and shall indemnify, keep indemnified, hold harmless, defend and protect NPCI and its officers/staff/personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this RFP or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the RFP, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NPCI and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate NPCI and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and NPCI will give notice of any such claim or demand of liability within reasonable time to the Bidder.

8.33 Legal Compliances:

The Bidder confirms to NPCI that its personnel/ employees/staff are covered under the provision of various Acts enacted for the protection and benefits of workmen /employees /staff or otherwise such as Employees State Insurance Act and Employees Provident Fund Miscellaneous Provision Act etc. and such other Acts like Profession Tax Act etc. as applicable and that Bidder is duly registered under the provisions of the said Acts and is complying with the provisions of the Acts.

The Bidder shall allow NPCI as well as regulatory authorities to verify books in so far as they relate to compliance with the provisions of these Acts and shall provide on demand by NPCI & regulatory authorities such documentary proof as may be necessary to confirm compliance in this regard. NPCI shall not be responsible in any event to the employees of Bidder for any of their outstanding claims or liability in that regard. NPCI shall not be responsible for any claim or demand made by such personnel for their dues outstanding against Bidder. Bidder indemnifies and shall keep NPCI

indemnified from any of such claims/ losses/ damages and demands by any of its personnel, if any, raised on NPCI.

8.34 Intellectual Property Rights:

All rights, title and interest of NPCI in and to the trade names, trademark, service marks, logos, products, copy rights and other intellectual property rights shall remain the exclusive property of NPCI and Bidder shall not be entitled to use the same without the express prior written consent of NPCI. Nothing in this RFP including any discoveries, improvements or inventions made upon with/by the use of the Bidder or its respectively employed resources pursuant to contract shall either vest or shall be construed so that to vest any proprietary rights to the Bidder.

Notwithstanding, anything contained in this RFP, this clause shall survive indefinitely, even after termination of this Purchase Order.

8.35 Applicable Law and Jurisdiction

Applicable Law**:** The Agreement shall be governed by and interpreted in accordance with the Indian Law. The jurisdiction and venue of any action with respect to the subject-matter of this Agreement shall be the Courts of Mumbai in India and each of the parties hereto submits itself to the exclusive jurisdiction and venue of such courts for the purpose of any such action.

8.36 Solicitation of Employees

Both NPCI & successful Bidder the Parties should agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties should agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge to directly or indirectly solicit of this contract for employing the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

8.37 Facilities provided by NPCI:

NPCI shall provide seats, with required facilities like internet, intranet & LAN Connectivity free of cost for official work. These facilities shall not be used for any personal use. In case of any misuse of the facilities, penalty as deemed fit shall be imposed and recovered from the pending bills of Bidder.

8.38 No Damage of NPCI Property

Bidder shall ensure that there is no loss or damage to the property of NPCI while executing the Contract. In case, it is found that there is any such loss/damage due to direct negligence/non-performance of duty by any personnel, the amount of loss/damage so fixed by NPCI shall be recovered from Bidder.

8.39 Fraudulent and Corrupt Practice

"Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of the project and includes collusive practice among Bidder's (prior to or after Bid submission) designed to establish Bid prices at artificial non-competitive levels and to deprive the NPCI of the benefits of free and open competition.

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official or a NPCI official in the process of project execution. NPCI will reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing the project.

8.40 Governing Language

All correspondences and other documents pertaining to this Agreement shall be in English only.

8.41 Addresses for Notices

Following shall be address of NPCI and Bidder

NPCI address for notice purpose:
Managing Director& CEO

National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051
Supplier's address for notice purpose: (To be filled by supplier)

Category	Specification	Requirement
General features		
A1	The bidder should have back to back arrangement with the OEM so that NPCI will be able to log a call with the OEM directly	Must have
A2	The vendor/bidder must be Gold/Tier-1 or Silver/Tier-2 of the OEM for the proposed product	Must have
A3	The bidder should have support offices in Mumbai, Hyderabad and Chennai.(Also DC in India)	Must have
A4	The bidder should have minimum 2 skilled OEM certified staff for the product proposed.(Bidder to share certification details of Skilled OEM certified staff)	Must have
A5	The Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).	Must have
A6	Solution/appliance to provide High Availability (HA) and Load Balancing functionality and must have RAID redundancy (for hard drives), Network redundancy (for management network interfaces) and Power-Supply module redundancy and 4x1G/10G network interfaces per server. (Bidder to explain architecture)	Must have
A7	The solution must ensure all the system components continue to operate in case of any other part of the system fails or loses connectivity.	Must have
A8	The Proposed solution should be on standard platform. In case of Software platform, bidder should factor hardware, OS, Database and storage any other license to support the SIEM solution including scalability with no additional cost to be borne by the customer	Must have
A9	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR (Active-Active). DR should be active all the time to ensure continuous security monitoring. Solution should have capability to create connector between Data centres & send the logs across for high availabilty across DC's. (Logs from DC1 should be available at DC2 & viceversa i.e. Site level redundancy for SIEM mgmt + logs)	Must have
A10	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peers nodes and across multiple sites with near zero RTO & RPO.	Must have
A11	The solution must have an automated backup and recovery process.	Must have
A12	The solution must automate internal health checks and notify the user in case of problems.	Must have
A13	The solution should be able to continue to collect data during database backup, de-fragmentation and other management scenarios, without any disruption to service.	Must have
SIEM Platform specifications		
B1	The proposed solution should be sized for 30,000 sustained EPS at correlation layer per Data centre but should be able to handle 60,000 peak EPS at correlation layer without dropping events or queuing events (for SIEM) per Data Centre.	Must have
B2	The Proposed solution should have capability to collect logs from most of the standard platforms like Microsoft Windows, Linux(All flavours),MAC OS,AIX, Solaris, Firewalls, Network, other security devices or solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls ,Active Directory servers,Web servers, Private cloud (VMware,	Must have

	Openstack) & cloud services (Aws/Azure/GCP), SAAS Solutions, O365, etc.	
B3	Proposed SIEM solution should act as common data lake for Correlation, SOAR,NDR,UEBA and threat hunting.	Must have
B4	The Proposed solution should have inbuilt security mechanism for protecting itself from security attacks	Must have
B5	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc (High avaliability)	
B6	The proposed solution must support caching mode of transfer for data collection, so as to ensure data is being logged in the event loss of network connectivity, and resume sending of data upon network connection.	Must have
B7	The SIEM platform should have capability to provide automatic Notification to SOC teams as defined in playbooks based on Conditional decision & Trigger Functions.	Must have
B8	The proposed solution must be able to collect data from new devices added into the environment, without disruption to the ongoing data collection.	Must have
B9	The proposed solution must provide for secure user access via HTTPS,ssh.	Must have
B10	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click.	Must have
B11	Solution should able to integrate with any 3rd party / Open source SIEM.	Must have
B12	The proposed solution must be able to monitor and report user and privileged users access activities.	Must have
B13	The Proposed solution must offer all of the below built-in threat detection techniques out of the box: 1.Detect Web Application Threats. 2.Detect APT Threats. 3.Integrate with leading HoneyPot solutions. 4.Integrate with leading NBAD,NDR tools. 5.Give visibility of endpoints also by integrating with EDR,DLP,HIPS,Antivirus etc for endpoint analytics. 6.Integrate with SOAR tools for automation. 7.Integrate with leading Threat intellegance Platform(TIP).	Must have
B14	The proposed solution must provide a query interface that allows users to search for data stored within the solution.	Must have
B15	The solution shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	Must have
B16	The solution should be able to part and filter logs on the basis of type of logs, date etc.	Must have
B17	In addition to the advanced analytics capabilities like MDR, solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples but not limited though : • Failed login attempts • Login attempts from suspicious locations • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical & Horizontal port scans • Traffic from blacklisted Ips • Login attempts at unusual timings	Good to have

B18	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data.	Must have
B19	The solution must have an incident review framework for incident management. Incident review framework to facilitate incident tracking, investigation, pivoting and closure	Must have
B20	Risk scoring framework to apply risk scores to any asset or user based on relative importance or value to the business	Must have
B21	The proposed solution must be able to read data input from the following static log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. Windows Events Logs c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.	Good to have
B22	The solution must be able to provide the capability to fully customise alerts, reports and dashboards to the business requirements.	Must have
B23	The solution must allow tracking of incidents from correlation rule through investigation of that event to closure.	Good to have
B24	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc to provides rapid insights and operational visibility into large-scale Unix and Linux environments machine data : syslog, metrics and configuration files.	Good to have
B25	Integration with corporate directories (AD, LDAP, etc) to extract employee information including: -- Employee user names, first, last, phone, manager, department, location, if privileged, if on watchlist, start and end dates, etc.Enables ability to correlate multiple user names back to a single employee	Must have
B26	The solution must be able to provide the capability to annotate events, modify status, build a chronological timeline for the incident before and after a triggered event.	Good to have
B27	The solution must be able to assign any arbitrary risk score to any data point or fields, example,user name, host name, location etc.	Good to have
B28	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.	Must have
B29	The solution must be able to support multiple transport mechanisms such as TCP,STIX and Trusted Automated exchange of Indicator Information (TAXII).	Must have
B30	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built.	Good to have

B31	The solution must be able to support the following indicators: 1.Network,IP - HTTP Referrer, User Agent, Cookie, Header, Data, URL - Domain - Endpoint - File Hash, Name, Extension, Path and Size - Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data - Process Name, Arguments, Handle Name, Handle Type - Service Name, Description - Certificate - Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm - Email - Email Address, Subject Body	Must have
B32	Solution should support triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, AV, EDR,Firewall (all with Well Known OEM's as well as Open source platforms) .	Must have
B33	Solution should support machine driven triaging algorithms that considers contextual parameters, historical behavior and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same · Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert. · Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on. · Central Threat Intelligence feed should also be applied to identify threats through known bad actors	Good to have
B34	Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters	Good to have
B35	Investigation module should integrate with log sources (ETDR, EPP, Data Lake) on demand to pull data related to the investigated alert. It should also include charting and graphs to analyse data	Good to have
B36	Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise(IOCs), external network connections.	Must have
B37	Solution should support models to build up the entire attack chain-from attack inception, progress of the attack and spread to attack in the network.	Must have
B38	Solution should support features to identify attacker attributes including threat intelligence score of attacker, who-is lookup information, geomapping in a single console.	Must have
B39	Solution should provide run books for investigation steps corresponding to different types of attacks, derive attack inception and progress of the attack. i.e. Detect Patient Zero, Attack origin and Blast Radius.	Must have
B40	Solution should support integration with open source or commercial IOC sources. List the supported sources which can be integrated with Solution and brief on the integration approach. Solution should support features to analyse and identify the impact of this attack on other assets.	Must have

B41	Solution should provide case management features to store raw and analyzed data for a specific alert or set of alerts. Provide details on the what artefacts can be stored related to an investigation	Must have
B42	Solution should support quick search across stored datasets in the Solution. Provide details of search features supported.	Must have
B43	Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.	Must have
B44	The proposed solution must come with pre-packaged alerting capability,flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.	Must have
B45	The proposed solution machine learning capabilities must includes API access, role-based access controls for machine learning models.	Good to have
B46	The proposed solutions machine learning capabilities must allow adidition of custom machine learning algorithms from popular open source Python libraries.	Must have
B47	The update in log format for a given OEM in its OS upgrade or other patch should be accordingly parsed on the solution provider side.	Must have
Log Analysis		
C1	The solution should support log collection, flow collection and other standard method for integrating devices and applications. Logs obtained from devices should be copied and stored in vendor SoC within 3 minutes from the actual log event at the integrated device.	Must have
C2	The solution should have connectors or similar integrators to support the devices/applications, wherever required the bidder should develop customized connectors/integrators at no extra cost	Must have
C3	The proposed solution should support collection of events through customization of connectors or similar integration for the assets that are not natively supported. Solution should adhere to industry standards for event collection: syslog, OPSEC, WMI, SDEE, ODBC, JDBC, FTP, SCP, HTTP, text file, CSV, XML file etc.	Must have
C4	All log data to be authenticated (time-stamped across multiple time zone) encrypted and compressed before transmission to manager console.	Must have
C5	The solution should have high availability feature built in for automated switch over to secondary collector/integrator in the event of primary collector failing. No performance degradation is permissible even in case of failure	Must have
C6	The solution should provide time based, criticality based, store and forward feature at each data collection point	Good to have
C7	Solution should capability to filter undesired, non-security logs at collection, processing and visualization layer.	Must have
C8	The proposed solution must be able to read data input from the following static log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. The solution must be able to accept the following live data streams from cloud server less functions like raw or JSON formatted data over HTTP/HTTPS.	Must have
C9	The proposed solution should be able to consume logs from any log source without writing parser beforehand or while integration. Parsers should be built once log is ingested	Must have

C10	provide capability to search raw and indexed logs as full text, natural language, time range values, IPs, IP subnet mathematical & statistical functions, logical operators, occurrences count, regex, similar events, first & last seen, predictive & prescriptive search suggestions etc.	Must have
C11	solution should capable of retrieving the archived logs for reporting, analysis, correlation, investigation and forensics.	Must have
C12	Solution should have ability to restore / replay older logs for incident investigation	Must have
C13	Solution should have capability to filter, blacklist or white list single or group of IP, user, URL, etc. in rules, reports, dashboard etc.	Must have
C14	The solution should provide detection/correlation of logs with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open Source TI feeds)	Must have
Management Center and administration		
D1	The solution should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules	Must have
D2	The solution should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics based, Behavioral based, etc., across different devices and applications	Must have
D3	The solution should be able to parse and correlate multi-line logs and flow data.	Must have
D4	The solution should have the ability to correlate all the field present in a log/flow data.	Must have
D5	The solution should have the ability to gather information on real time threats and zero day attacks from anti-virus, IPS and IDS and analyses data against the information for any threats	Must have
D6	The solution should provide a web-based, user friendly console or a wizard based console to create rule.	Must have
D7	The solution should support logical operation and nested rules for creation of complex rules.	Must have
D8	The solution should allow applying filters and sorting of query results.	Must have
D9	The solution should be able to accept or integrate with asset details to provide asset level events, incidents, vulnerabilities and issues.	Must have
D10	The proposed solution should have the ability to perform free text search on events, incidents, rules and other parameters	Must have
D11	The solution should support integration with big data platforms.	Must have
D12	The solution should be able to integrate with incident management and ticketing tools	Must have
Threat Intelligence		
E1	The proposed solution should detect threats using graph-based threat anomalies, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threat anomalies are public-facing website attack or fraudulent website activity.	Must have
E2	The Proposed solution TI Service should anticipate likely threats to the Organization based on global threat events and data and provide proactive measures to prevent such happenings in the Organization.	Good to have
E3	The Proposed solution should support integration of machine readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise & false positives in threat intelligence feeds	Must have

E5	The Proposed Solution should track status of assets against IoCs, CVEs and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities. Service provider should track closure and corresponding risk reduction	Good to have
E6	The Solution should support STIX/TAXII for automated integration of actionable intelligence with security technologies.	Must have
E7	The solution should support 3rd party / external threat intelligence to aid incident response by bringing in organizational context and internal information available in SIEM and other sources of security information	Must have
E8	The proposed solution should detect threats like Lateral Movement and Data Exfilteration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.	Must have
E9	The Proposed solution should Automatically enrich all incoming events with minimum following information. These fields should be customizable to add/modify/delete as desired by administrator): - Asset Owner, BIA & CIA - Geo-location of IP - Reputation of IP, URL, File etc. - Hash of files - Historical security incidents on same IP/same host/same user/same vulnerability/same location etc. - Threat Intelligence: (IoAs), (IoCs), and adversary's TTPs - Vulnerability information of asset. - Application Security review data. - Zone classification - Risk score of assets Bidder to Provide details on what additional enrichment options can be provided by the solution.	Must have
E10	The Proposed solution should be capable to correlate events, network activity data, alerts, and vulnerability data to provide complete view of security threats and generate real-time security alerts	Must have
E11	The Proposed solution should be capable to detect Slow attacks, advance persistent threats, file less attacks, advance malwares, zero-day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI / ML. Also, capable to prevent & predict known-known, known-unknown and unknown-unknown threats by monitoring entire IT infrastructure and leveraging real-time threat intelligence.	Must have
E12	The solution must be able to integrate with real time threat intelligence feeds for the purpose of correlating events. These feeds should be updated automatically.	Must have
E13	The correlations engine should be updated with real time security intelligence updates from the OEM	Must have
Network Detection and response (NDR)		
F1	The solution should support On-premise deployment	Must have
F2	The Proposed solution must be PCI-DSS or ISO 27001 Compliant	Good to have
F3	Scalability of the proposed solution should be such as to cover critical network segments/verticals with abillty to ingest up to 30,000 FPS / 30 Gbps Per Data Centre (DC & DR)	Must have
F4	The Proposed solution should have separate component for packet/flow sensor, telemetry processing and management functions for ideal performance.	Must have

F5	The Proposed solution should support installation of all components manually e.g. Threat intelligence database, Geo-IP database, IP reputation, Upgrade firmware/ upgrade patches etc. (offline download & install). This is to avoid any limitations to the solution inside an air-gapped environment (absence of internet connectivity)	Good to have
F6	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts.	Must have
F7	The solution must support application definition beyond protocol and port. The system must support the identification of applications using ports other than the well-known, and applications tunnelling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP).	Must have
F8	The solution must Identify & profile traffic by TCP and UDP ports.	Must have
F9	Solution must support Netflow collection and correlation.	Good to have
F10	The Solution should capture flow information from multiple network points like Network traffic collected via TAP, SPAN, and/or Mirror OR must support JFlow, SFLow, IPFIX collection and correlation.	Must have
F11	The solution must support traffic profiling associated with logical network design (e.g., Subnet/CIDR).	Must have
F12	The solution must identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).	Must have
F13	The solution must create clearly independent and differentiated profiles from local traffic vs. traffic originating or destined for the internet.	Must have
F14	The solution must support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc	Must have
F15	The solution must be able to adjust itself in DHCP environment and yet uniquely identify machines with high accuracy despite change of IP Address	Must have
F16	Solution shall have a feature capable of enabling retrospective analysis of the incident's logs, returning the connection in seconds, minutes, hours or days before a certain anomaly had been identified	Must have
F17	Solution shall create unique profiling for each user and device, as well as for the relations between them.	Must have
F18	The Proposed Solution must be able to scale up and down based on changes in scope	Must have
F19	The Proposed solution must able to monitor all network traffic in real time	Must have
F20	The Proposed solution able to query at least 1 months' worth of meta historic data	Must have
F21	The solution should Integrate with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provide full historical mapping of User Name to IP address logins in a searchable format	Must have
F22	The Proposed solution should be able to Obtain/receive logs from Various critical infrastructure log sources such as SIEM, DNS logs, DHCP logs, AD logs etc. for additional correlation if required.	Good to have

F23	The solution should provide the capability to respond quickly and effectively with complete knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing security controls.	Must have
F24	The solution should be capable of providing visibility of east-west traffic in an encapsulated network of ACI / SDA fabric, Natively or with a Use of VM based Telemetry sensor or should be feasible in a way. (Bidder to mention feasibility)	Good to have
F25	The Solution should be intelligent and should automatically tweak itself through automated learning	Must have
F26	Support creation of custom models for anomaly detection	Must have
F27	The solution must detect "zero-day" events by leveraging anomaly based detection.	Must have
F28	The solution must dynamically learn behavioural norms and expose changes as they occur.	Must have
F29	The solution must detect and present views of traffic pertaining to observed threats in the network.	Must have
F30	The solution must display traffic profiles in terms of packet rate. This capability must be available for simple TCP analysis (TCP Flags, etc.) but rate-based information may be presented for other profiles (e.g., applications).	Must have
F31	The solution must be able to profile communication originating from or destined to the internet by Geographic regions in real-time.	Good to have
F32	The solution should Analyse access and its abuse with identity-centric behaviour analytics	Good to have
F33	The solution should Model good behaviour to expose unknown bad through peer groups, clustering and outliers	Must have
F34	The solution should Leverage predictive security analytics to risk-score incidents.	Must have
F35	The Solution should Optimize resources and time with use machine learning algorithms efficiently, unsupervised & shall be able to predict/detect anomalies.	Must have
F36	Solution must be able to identify/alert new and unknown attack behaviours without making use of signatures or rules.	Must have
F37	Solution should support a rule engine for users to define custom rules to leverage NDR capability. Rule engine should support all possible fields & parameters from a Packet header.	Must have
F38	Solution must be able to identify any anomalous behaviour in the environment and alert/highlight these behaviours in real time. (Real time alerts)	Must have
F39	The solution must detect internal denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc., identify the presence of botnets in the network, identify DNS spoofing attack etc. and detect long-lived connections that may be associated with data-exfiltration.	Must have
F40	The solution must be able to detect suspicious communication channels Services or applications not running over its standard ports. (i.e. HTTP not over port 80)	Must have
F41	The solution must be able to Detect and predict any data exfiltration by identifying abnormal behaviour as a part of cyber kill chain stages / MITRE / a well known attack framework.	Good to have
F42	The solution must be able to Identify abnormal communication for protocol, commands, non-standard ports anomalies	Must have
F43	The solution must be able to identify IP / Port scanning reconnaissance attacks	Must have

F44	The solution must be able to identify Malware / malicious bots detection through C2 (command and control) communication	Must have
F45	The solution should provide Detection of data exfiltration based on abnormal packet size (such as exfiltration in ICMP,DNS packets)	Must have
F46	The solution should provide Detection of lateral movement based on suspicious connections with machines in the network	Must have
F47	The solution should provide Detection of network crawling based on anomalous pattern detection	Must have
F48	The solution should provide detection/correlation of Communication/Flows with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open Source TI feeds)	Must have
F49	The solution should be able to store PCAP & Meta data of Communication/Flows if matched with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open Source TI feeds)	Must have
F50	The solution must be able to identify Attack & Reconnaissance Tools - Check for commonly used penetration testing tool and malware user agents	Must have
F51	The solution must be able to identify Possible Masqueraded file transfer - Look for files transferred with an incorrect file extension. Ignore common external domains.	Must have
F52	The solution must be able to identify BitCoin Activity - Any communications using the BitCoin mining protocol	Must have
F53	New User Agent communication - Any new/suspicious user agent communication seen on from/to device which is rare on the device/in the whole environment	Must have
F54	Identifying traffic of Privacy VPN's - Personal VPN solutions which enable the user to avoid network monitoring solutions.	Must have
F55	The proposed Solution should have inbuilt Models to detect use of various cloud storage services. (eg. Amazon S3, Dropbox etc)	Must have
F56	The proposed solution should be capable of identifying APT Activity - Detection of known Advanced Persistent Threat indicators.	Must have
F57	The proposed solution should be able to identify TCP/UDP malformed packets, TCP/IP stack fingerprinting methodologies e.g. Christmas Tree packet.	Must have
F58	Non-standard DNS server used - Devices using uncommon DNS servers which were previously idle/were not DNS servers	Must have
F59	The solution must be able to identify RST storm- A large number of packets with the reset flag set. This may disrupt normal communications	Must have
F60	The solution must be able to identify Vulnerable Protocols - Use of out-of-date/Known Vulnerable Protocols e.g. SMB, Kerberos,NetBios, old versions for TLS/SSL.	Must have
F61	The solution must be able to identify Unusual Connectivity- New or unusual connections, either an external connection to/from domains/sources that are Unusual/Suspicious/rare.	Must have
F62	The solution must be able to identify Address Scan - Scanning for single/multiple devices listening on a specific port	Must have
F63	The solution must be able to identify Port Scan - Scanning single/multiple devices to see which ports are open on it.	Must have
F64	The solution must be able to identify Bruteforcing - Repeated failed logins (KERBEROS, SSH or FTP). This could be indicative of malicious password guessing.	Must have

F65	Solution must identify a ransomware attack basis the network traffic and alert the respective team..	Must have
F66	Solution must identify and investigate suspicious volumes of data transferred internally.	Must have
F67	Solution must identify and investigate anomalies in patterns of DNS requests.	Must have
F68	Solution must check for any Active sessions for longer than accepted time period	Must have
F69	The solution should detect and alert on anomalies in DNS communications so as to pre-emptively help detect security risks.	Must have
F70	The solution shall be able to identify crypto compliance for endpoints (TLS, SSL versions)	Must have
F71	The solution must do Identification of Malicious behaviour in encrypted traffic without decryption.	Good to have

Support Official requirement -

- Personnel resources should be provided for the Contract period. L2 & L3 onsite personnel resources of the bidder to be designated as **Sr. Security Analyst** & **Sr. Technology Specialist** with clear demarcation of their roles.
- The bidder is required to provide onsite human resource for L2 & L3 resources from the date of SIEM solutions installation.
- Bidder shall provide resources, being deployed at NPCI's Hyderabad Location.
- In Future, NPCI may require to increase onsite personnel resources of the bidder and / or OEMs from time to time. The same need to be provided within one month from the date of such communication.
- The onsite resources must be provided adequate guidance, assistance and support by competent offsite subject matter experts (SME) of the bidder & OEMs.
- Bidder shall provide SOD & EOD report with respect to SIEM health regularly.
- Bidder shall provide Managed Security Services for SIEM Management, SIEM Monitoring, SIEM Operations, SIEM Automation, Content Development to fine-tune existing rules & develop new content based on latest threat vectors. Bidder should keep improving SIEM platform for better Return on investment. As detailed in Annexure-A hereto, through its following resources.

Sr. No.	Role	Level	Minimum No of resources to be deployed to achieve 16x7x365
1	SIEM	L2 Resources	3
2	SIEM	L3 Resource	1 (9x5x365)

Support Official Qualification:

The staff's skills, educational qualification, experience, certification and competence in Hardware, OS, and all other components involved in the solution and software product specialists will impact on quality of delivery for the services. It is desirable that suitable persons are deployed for NPCI's requirements. Minimum qualifications criteria for all the professionals to be deployed in the project are as follows (but not limited to):

Educational Qualification: The staff deployed on the project should have a good academic record and a professional degree in IT / Computer Science from any recognized university / Institute in India.

***Certifications and Experience:** The staff deployed on the project should have be an OEM certified SIEM Specialist (Mandatory). L2 Should have a Minimum 3 years of SIEM & SOC Experience. L3 Should have a Minimum 5 years of Experience in SIEM, SOC & Content Development.

* NPCI Reserves the right to relax above criteria on merit & case to case basis.

General Guidelines:

a. The NPCI SOC team will be 24x7x365 environment and personal resources should be able to work in shifts and flexible working hours to support the operations.
b. NPCI reserves the right to interview all the personnel resources to be deployed on the project and reject if not found suitable for the project.
c. At a later stage also if any of the personnel resources are found unsuitable to perform duties or any of the personnel resources violates any of the NPCI guidelines, NPCI may seek removal of all such personnel resources.
d. NPCI expects to build a strong team and there should be no single point of dependency on any one individual. NPCI's services should always remain immune to any such dependencies.
e. Bidder is required to obtain permission from NPCI in writing before removing any of the personnel resources from the project.
f. NPCI expects deployed resource / personnel resources to constantly keep upgrading their product / domain knowledge & skills.
g. As soon as NPCI adopts a newer version of an existing technology, NPCI expects the existing staff working in the project to get certified on the same or the Bidder should arrange for the additional resources with requisite qualifications/certifications.
h. Proper on boarding and off boarding processes are required to be followed.
i. All the staff are required to abide by the NPCI's applicable policies and NDA.
j. The team should be adequate to ensure the unhindered 24x7x365 operations and support. 16x7x365 support to be provided onsite, Rest of 8x7x365 support to be provided on-call basis (Remote support) who could be a senior member from amongst the team.
k. L3 Engineer /Team Lead would be the single point of contact for NPCI.
l. NPCI should be provided with a dedicated and exclusive team.
m. A detailed shift roster has to be published at the start of the month in consultation with NPCI
n. The bidder should factor in an increase of 15% on personnel resources on YoY basis at the agreed cost and Terms & Conditions in this RFP. However, NPCI will take a final call on this at its own discretion.
o. The onsite resources must work as per NPCI's working days and hours or as decided by NPCI for smooth functioning of NPCI SOC.
p. Bidder will be responsible for police verification & background checks of all resources before on boarding.

Role and Responsibilities of onsite Team:

Indicative roles and responsibilities of onsite resources is given below. However, NPCI reserves the right to use onsite resources as per the project requirements, criticality etc. from time to time.

Resource Level	Roles & Responsibilities
L2(Sr. Security Analyst)	• Monitor SIEM Console & Dashboards and provide response to the reported incidents Filtered by L1. • Monitor and review the L1 activities • Support the day to day operation of a highly available distributed multi-clusteried multi-tenant SIEM deployment.

	• Perform initial analysis for known issues and provide the appropriate recommendations for closure. • Monitor & Reporting of system components health and take necessary action in case of any observed issue. • Provide noce ltification and communication with Incident management and respective application team upon threat detection. • Perform analysis on the reported incidents, determine the root cause, recommend the appropriate solution. • Should provide real time situational awareness to the NPCI's stakeholders. • Use and apply learnings from incident and provide recommendation for standardizing the SIEM Solution. • Develop and implement processes for interfacing with operational teams and other supporting teams. • Ensure the SIEM integration is intact among the NPCI SOC solutions, other assets • Design, create and customize the dashboards as per the NPCI's requirements. • ensure the necessary NPCI SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas. • Automating Day to Day Tasks related with SIEM Operations (but not limited to) • Above is illustrative list of general activities. All Technology specific activities Related to SIEM to be carried out. • SIEM Management, SIEM Monitoring, SIEM Operations, SIEM Automation, Content Development to fine-tune existing rules & develop new content based on latest threat vectors. Ensure & keep improving SIEM platform for better Return on investment. • Should have good understanding on MITRE att&ck framework.
L3(Sr. Technology Specialist)	• Monitor and review the L2 activities • Should provide real time situational awareness to the NPCI's stakeholders. • Use and apply learnings from incident and provide recommendation for standardizing the SIEM Solution. • Ensure the SIEM integration is intact among the NPCI SOC solutions, other assets • Design, create and customize the dashboards as per the NPCI's requirements. • ensure the necessary NPCI SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas. • Support on boarding and maintenance of a wide variety of data sources to include various OS, appliance, and application logs. • Create Custom queries, custom dashboards, and visualizations to support NPCI's requirements and monitoring of the SIEM deployment • Create and manage SIEM knowledge objects to include apps, dashboards, saved and scheduled searches and alerts • Support access requests and modifications and permissions • Support troubleshooting and remediation of issues as they arise with data ingestion and SIEM infrastructure • Work on Improvement of overall posture of SIEM deployment to achieve Best return on investment. • Monitor & report on cyber threats and Suggest any changes needed to protect the organization in SIEM, Leading End-to-End Implementation of the suggested changes along with L2. • SIEM Management, SIEM Monitoring, SIEM Operations, SIEM Automation, Content Development to fine-tune existing rules & develop new content based on latest threat vectors. Ensure & keep improving SIEM platform for better Return on investment. • Should have a very good understanding on MITRE att&ck framework.

In case any of the above requirements are not generic in nature, it may be brought to the notice of NPCI through pre-bid mechanism.

Dated this…… Day of……2022

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Section 10 - Documents forms to be put in Folder A

Annexure A1 - Bidder's Letter for EMD

To

The Chief Executive Officer
National Payments Corporation of India,
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Subject: RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022

We have enclosed an EMD in the form of a RTGS - UTR No/BG No. ____ issued by the branch of the _____Bank, for the sum of Rs. _____ (Rupees _____). This EMD is as required by clause 5.6 of the Instructions to Bidders of the above referred RFP.

Thanking you,

Yours faithfully,

(Signature of the Bidder)
Printed Name:
Designation:
Seal:
Date:
Business Address:

Annexure A2 - Bid Security (Bank Guarantee)

_____
[Bank's Name, and Address of Issuing Branch or Office]

National Payments Corporation of India: _____

Date: _____

BID GUARANTEE No.: _____

We have been informed that_____ (hereinafter called "the Bidder") has submitted to you its bid dated (hereinafter called "the Bid") for the execution of _____under RFP No.

Furthermore, we understand that, according to your conditions, bids must be supported by a bank guarantee.

At the request of the Bidder, we _____ hereby irrevocably undertake to pay you without any demur or protest, any sum or sums not exceeding in total an amount of Rs._____/-(Rupees _____ only) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

(a) Has withdrawn its Bid during the period of bid validity specified by the Bidder in the Form of Bid; or

(b) having been notified of the acceptance of its Bid by NPCI during the period of bid validity, (i) fails or refuses to execute the Contract document; or (ii) fails or refuses to furnish the performance security, if required, in accordance with the Instructions to Bidders.

This guarantee will expire:

(a) If the Bidder is the successful bidder, upon our receipt of copies of the contract signed by the Bidder and the performance security issued to you upon the instruction of the Bidder; or

(b) if the Bidder is not the successful bidder, upon the earlier of (i) our receipt of a copy of your notification to the Bidder of the name of the successful bidder; or (ii) twelve months after the expiration of the Bidder's Bid.

Consequently, any demand for payment under this guarantee must be received by us at the Office on or before that date.

_____
[Signature]

Annexure A3 - Bid Security

(PERFORMANCE BANK GUARANTEE FORMAT)

Date:

Beneficiary: NATIONAL PAYMENTS CORPORATION OF INDIA
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Performance Bank Guarantee No:
We have been informed that---------- (hereinafter called "the Supplier") has received the purchase order no. "----------" dated ---------- issued by National Payments Corporation of India (NPCI), for ---------- (hereinafter called "the Purchase Order").

Furthermore, we understand that, according to the conditions of the Purchase order, a Performance Bank Guarantee is required to be submitted by the Supplier to NPCI.
At the request of the Supplier, We ----------(name of the Bank , the details of its incorporation) having its registered office at ---------- and, for the purposes of this Guarantee and place where claims are payable, acting through its ---- branch presently situated at ---------- (hereinafter referred to as "Bank" which term shall mean and include, unless repugnant to the context or meaning thereof, its successors and permitted assigns),hereby irrevocably undertake to pay you without any demur or objection any sum(s) not exceeding in total an amount of Rs.---------- (in figures) (Rupees---------(in words)------- only) upon receipt by us of your first demand in writing declaring the Supplier to be in default under the purchase order, without caveat or argument, or your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

Please note that you may, if you so require, independently seek confirmation with –(Bank Name & Issuing branch address)----------, that this Bank Guarantee has been duly and validly issued.

Notwithstanding anything contained in the foregoing:
The liability of ---------- (Bank), under this Bank Guarantee is restricted to a maximum total amount of Rs. ---------- (Amount in figures and words).
This bank guarantee is valid upto ----------.
The liability of ---------- (Bank), under this Bank Guarantee is finally discharged if no claim is made on behalf of NPCI within twelve months from the date of the expiry of the validity period of this Bank Guarantee.
Our liability pursuant to this Bank Guarantee is conditional upon the receipt of a valid and duly executed written claim or demand, by ---------- (Bank)---------- -------- (Address), delivered by hand, courier or registered post, or by fax prior to close of banking business hours on ---------- (date should be one year from the date of expiry of guarantee) failing which all rights under this Bank Guarantee shall be forfeited and ---------- (Bank), shall stand absolutely and unequivocally discharged of all of its obligations hereunder.

This Bank Guarantee shall be governed by and construed in accordance with the laws of India and competent courts in the city of Mumbai shall have exclusive jurisdiction.

Kindly return the original of this Bank Guarantee to ---------- --------- (Bank & Its Address), upon (a) its discharge by payment of claims aggregating to Rs. -------- (Amount in figures & words); (b) Fulfillment of the purpose for which this Bank Guarantee was issued; or (c) Claim Expiry Date (date should be one year from the date of expiry of this Bank Guarantee).
All claims under this Bank Guarantee will be payable at ---------- ---------- (Bank & Its Address).

{Signature of the Authorized representatives of the Bank}

Annexure B - Bid Offer Form (without Price)

(Bidder's Letter Head)

OFFER LETTER

Date:

To
The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Dear Sir,

Subject: RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022

We have examined the above referred RFP document. As per the terms and conditions specified in the RFP document, responses to the pre-bid queries and in accordance with the schedule of prices indicated in the commercial bid and made part of this offer.
We acknowledge having received the following addenda / corrigenda/ pre-bid responses to the RFP document.

Addendum No. / Corrigendum No/Pre-bid responses	Dated

While submitting this bid, we certify that:

1. Prices have been quoted in INR.

2. The prices in the bid have not been disclosed and will not be disclosed to any other bidder of this RFP.

3. We have not induced nor attempted to induce any other bidder to submit or not submit a bid for restricting competition.

4. We agree that the rates / quotes, terms and conditions furnished in this RFP are for NPCI and its Associates.

If our offer is accepted, we undertake, to start the assignment under the scope immediately after receipt of your order. We have taken note of Penalty clauses in the RFP and agree to abide by the same. We also note that NPCI reserves the right to cancel the order and order cancellation clause as per terms and condition would be applicable. We understand that for delays not attributable to us or on account of uncontrollable circumstances, penalties will not be levied and that the decision of NPCI will be final and binding on us.

We agree to abide by this offer till 180 days from the last date stipulated by NPCI for submission of bid, and our offer shall remain binding upon us and may be accepted by NPCI any time before the expiry of that period.

Until a formal contract is prepared and executed with the selected bidder, this offer will be binding on us. We also certify that the information/data/particulars furnished in our bid are factually correct. We also accept that in the event of any information / data / particulars are found to be incorrect, NPCI will have the right to disqualify /blacklist us and forfeit bid security.

We undertake to comply with the terms and conditions of the bid document. We understand that NPCI may reject any or all of the offers without assigning any reason whatsoever.

As security (EMD) for the due performance and observance of the undertaking and obligation of the bid we submit herewith RTGS/BG bearing no. _____ dated _____ drawn in favor of "National Payments Corporation of India" or Bank Guarantee valid for ____ days for an amount of Rs._____ (Rs. _____ only) payable at Mumbai.

Yours sincerely,

Authorized Signature [In full and initials]:
Name and Title of Signatory:
Name of Company/Firm:
Address

Annexure C - Bidder Information

(Bidder's Letter Head)

Details of the Bidder				
1	Name of the Bidder			
2	Address of the Bidder			
3	Constitution of the Company (Public Ltd/ Pvt Ltd)			
4	Details of Incorporation of the Company.	Date:		
		Ref #		
5	Permanent Account Number (PAN)			
6	Valid Goods & Services Tax (GST) Registration Numbers			
7	City			
8	State			
9	Pin Code / State Code			
10	GSTIN Number			
11	HSN Number			
12	Name & Designation of the contact person to whom all references shall be made regarding this tender			
13	Telephone No. (Cell # and Landline # with STD Code)			
14	E-Mail of the contact person:			
15	Website			
Financial Details (as per audited Balance Sheets) (in Cr)				
19	Year	**2018-19**	**2019-20**	**2020-21**
20	Net worth			
21	Turn Over			
22	PAT			

Dated this…… Day of……..2022

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure D - Declaration for Clean Track Record

(Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Sir,

I have carefully gone through the Terms & Conditions contained in the **RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022**. I hereby declare that my company has not currently been debarred/black listed by any Government / Semi Government / Private organizations in India / abroad. I further certify that I am competent officer and duly authorized by my company to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure E - Declaration for Acceptance of RFP Terms and Conditions

(Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Dear Sir,

I have carefully gone through the terms & conditions contained in the **RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022**. I declare that all the provisions of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure F - Declaration for Acceptance of Scope of Work

(Bidder's Letter Head)

To

The Chief Executive Officer
National Payments Corporation of India
1001A, B wing 10th Floor,
'The Capital', Bandra-Kurla Complex,
Bandra (East), Mumbai - 400 051

Sir,

I have carefully gone through the scope of work (including the scope of work mentioned in responses to pre-bid queries/Corrigendum/Corrigenda) contained in the RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022. I declare that all the provisions of this RFP / Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:

Annexure G - Format Power of Attorney

(On Stamp paper of relevant value)

Know all men by the present, we _____ (name of the company and address of the registered office) do hereby appoint and authorize _____ (full name and residential address) who is presently employed with us holding the position of _____ as our attorney, to do in our name and on our behalf, deed and things necessary in connection with or incidental to our proposal for _____ in response to the **RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022** by NPCI, including signing and submission of all the documents and providing information/responses to NPCI in all the matter in connection with our bid. We hereby agree to ratify all deeds and things lawfully done by our said attorney pursuant to this Power of Attorney and that all deeds and things done by our aforesaid attorney shall always be deemed to have been done by us.

Dated this _____ day of _____ 2022.
For _____.

(Signature)

(Name Designation and Address)

Accepted

(Signature)
(Name Designation)
Date:
Business Address:

Annexure H - Eligibility Criteria Compliance
(Bidder's Letter Head)

A] Start-ups:

Sr. No	Eligibility Criteria	Compliance (Yes/No)	Documentary proof to be attached
1	The bidder should be incorporated or registered in India under Companies Act/Partnership Act / Indian Trust Act (Annual filling with ROC) and should have the Certificate issued by Department for Promotion of Industry and Internal Trade (DPIIT) or in the process of applying the same and shall be submitted before a formal engagement with NPCI.		1.Certificate of incorporation 2.MSME registration certificate (if applicable) 3. DPIIT Certificate
2	The bidder's annual turnover should be less than Rs. 100 crores as per audited financial statements in each of the financial years from the date of registration/ incorporation subject to compliance to Sr. No. 3		1. Standalone **audited** financial statements for last 3 years a. Balance sheets b. Profit /loss statement c. Signed Statutory Auditor's Report d. Notes to Accounts and Schedules forming part of accounts to be submitted. • *Complete financial statements duly signed/ approved by Auditor.* 2. CA certificate in case more than 3 years for previous years
3	The date of incorporation of the bidder should be anywhere between 1 to 10 financial years		Certificate of incorporation/ registration
4	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad.		Declaration letter from the **Bidder** and **OEM** as per **Annexure D**
5	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.		Authorization from OEM as per **Annexure I** Self-declaration of not being part of distribution channel
6	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission		Remittance proof of RTGS in favor of NPCI
7	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.		Remittance proof of RTGS/ BG in favor of NPCI

8	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.		OEM Authorization letter to be provided

B] Other than Start-ups:

Sr. No.	MSME	Other than MSME	Compliance Yes/No	Documentary proof to be attached
1.	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last three (3) years. a) In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least two (2) years as on date of submission of the bid. b) In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least two (2) years as on the date of submission of bid.	The bidder is a Company registered under the Companies Act/ Partnership / LLP at least since last five (5) years. a) In case the bidder is the result of a merger / acquisition, at least one of the merging companies should have been in operation for at least five (5) years as on date of submission of the bid. b) In case the bidder is the result of a demerger / hiving off, at least one of the demerged company or resulting company should have been in operation for at least five (5) years as on the date of submission of bid.		1. Certificate of incorporation 2. MSME registration certificate (if applicable)

2.	The bidder should have reported minimum annual turnover of Rs. **8 crores** and should have **reported profits (profit after tax**) as per audited financial statements in at least **2 out of last 3 financial years** (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.	The bidder should have reported minimum annual turnover of Rs. **20 crores** in each of the last **3** financial years and should have reported profits (profit after tax) as per audited financial statements **in last 3 financial years** (FY 2018-19, 2019-20, 2020-21). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.		Standalone financial **audited** financial statements 1. Balance sheets 2. Profit/ loss statement 3. Signed Statutory Auditor's Report 4. Notes to Accounts and Schedules forming part of accounts to be submitted.

3	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary self-declaration along with extract of auditors' report.		Self-declaration to be provided by Bidder
4	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad	Neither the OEM nor the Bidder should have been currently blacklisted by any Bank or institution in India or abroad		Declaration from OEM as per Annexure D on company letter head Declaration from Bidder as per Annexure D on company letter head
5.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.	The bidder should be authorized to quote and support for OEM products and services. The bidder shall not get associated with the distribution channel once in any other capacity once he is eligible for price discussion.		Declaration from OEM (as per Annexure-I) Self-declaration by bidder of not being part of distribution channel
6.	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission	The bidder has paid the bid cost as given in the RFP at the time of purchasing the bid document or has paid or submitted along with the bid submission		Remittance proof of Electronic Transfer in favor of NPCI
7.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.	The Bidder has paid or submitted along with the bid submission required EMD as mentioned in the RFP.		Remittance proof of Electronic Transfer/ BG in favor of NPCI
8.	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.	The OEM can authorize multiple bidders to participate on the OEMs behalf, however, in such a case, the OEM will not be allowed to participate on itself. The bidder is authorized to participate on behalf of only a single OEMs product.		Self-declaration to be provided along with customer references

Dated this…… Day of……2022

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure I - OEM / Manufacturer's Authorization Letter

[The Bidder shall require the Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be on the letterhead of the Manufacturer and should be signed by a person with the proper authority to sign documents that are binding on the Manufacturer. The Bidder shall include it in its bid]

Date:

To:

WHEREAS

We_____, are official manufacturers/OEM vendors of_____. We_____ do hereby authorize M/S_____ to submit a bid the purpose of which is to provide the following Goods, manufactured by us _____, and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty, with respect to the Goods offered by the above firm.

Signed by the Manufacturer/OEM Vendor:

Name:

Title:

Seal:

Dated on _____ day of _____, _____

Section 11 - Documents to be put in Folder 'B'

(Bidder's Letter Head)

Annexure J - Technical Compliance

Category	Specification	Requirement	Compliance (Yes/No)
	General features		
A1	The bidder should have back to back arrangement with the OEM so that NPCI will be able to log a call with the OEM directly	Must have	
A2	The vendor/bidder must be Gold/Tier-1 or Silver/Tier-2 of the OEM for the proposed product	Must have	
A3	The bidder should have support offices in Mumbai, Hyderabad and Chennai.(Also DC in India)	Must have	
A4	The bidder should have minimum 2 skilled OEM certified staff for the product proposed.(Bidder to share certification details of Skilled OEM certified staff)	Must have	
A5	The Solution quoted by the bidder should be in Gartner Leader or Challenger Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).	Must have	
A6	Solution/appliance to provide High Availability (HA) and Load Balancing functionality and must have RAID redundancy (for hard drives), Network redundancy (for management network interfaces) and Power-Supply module redundancy and 4x1G/10G network interfaces per server. (Bidder to explain architecture)	Must have	
A7	The solution must ensure all the system components continue to operate in case of any other part of the system fails or loses connectivity.	Must have	
A8	The Proposed solution should be on standard platform. In case of Software platform, bidder should factor hardware, OS, Database and storage any other license to support the SIEM solution including scalability with no additional cost to be borne by the customer	Must have	
A9	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR (Active-Active). DR should be active all the time to ensure continuous security monitoring. Solution should have capability to create connector between Data centres & send the logs across for high availabilty across DC's. (Logs from DC1 should be available at DC2 & viceversa i.e. Site level redundancy for SIEM mgmt + logs)	Must have	
A10	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peers nodes and across multiple sites with near zero RTO & RPO.	Must have	
A11	The solution must have an automated backup and recovery process.	Must have	
A12	The solution must automate internal health checks and notify the user in case of problems.	Must have	
A13	The solution should be able to continue to collect data during database backup, de-fragmentation and other management scenarios, without any disruption to service.	Must have	
SIEM Platform specifications			
B1	The proposed solution should be sized for 30,000 sustained EPS at correlation layer per Data centre but should be able to handle 60,000 peak EPS at correlation layer without dropping events or queuing events (for SIEM) per Data Centre.	Must have	

B2	The Proposed solution should have capability to collect logs from most of the standard platforms like Microsoft Windows, Linux(All flavours),MAC OS,AIX, Solaris, Firewalls, Network, other security devices or solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls ,Active Directory servers,Web servers, Private cloud (VMware, Openstack) & cloud services (Aws/Azure/GCP), SAAS Solutions, O365, etc.	Must have	
B3	Proposed SIEM solution should act as common data lake for Correlation, SOAR,NDR,UEBA and threat hunting.	Must have	
B4	The Proposed solution should have inbuilt security mechanism for protecting itself from security attacks	Must have	
B5	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc (High avaliability)		
B6	The proposed solution must support caching mode of transfer for data collection, so as to ensure data is being logged in the event loss of network connectivity, and resume sending of data upon network connection.	Must have	
B7	The SIEM platform should have capability to provide automatic Notification to SOC teams as defined in playbooks based on Conditional decision & Trigger Functions.	Must have	
B8	The proposed solution must be able to collect data from new devices added into the environment, without disruption to the ongoing data collection.	Must have	
B9	The proposed solution must provide for secure user access via HTTPS,ssh.	Must have	
B10	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click.	Must have	
B11	Solution should able to integrate with any 3rd party / Open source SIEM.	Must have	
B12	The proposed solution must be able to monitor and report user and privileged users access activities.	Must have	
B13	The Proposed solution must offer all of the below built-in threat detection techniques out of the box: 1.Detect Web Application Threats. 2.Detect APT Threats. 3.Integrate with leading HoneyPot solutions. 4.Integrate with leading NBAD,NDR tools. 5.Give visibility of endpoints also by integrating with EDR, DLP, HIPS, Antivirus etc for endpoint analytics. 6.Integrate with SOAR tools for automation. 7.Integrate with leading Threat Intelligence Platform(TIP).	Must have	
B14	The proposed solution must provide a query interface that allows users to search for data stored within the solution.	Must have	
B15	The solution shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.	Must have	
B16	The solution should be able to part and filter logs on the basis of type of logs, date etc.	Must have	

B17	In addition to the advanced analytics capabilities like MDR, solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples but not limited though : • Failed login attempts • Login attempts from suspicious locations • Authorization attempts outside of approved list • Vendor logins from unauthorized subnets • Vertical & Horizontal port scans • Traffic from blacklisted Ips • Login attempts at unusual timings	Good to have	
B18	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data.	Must have	
B19	The solution must have an incident review framework for incident management. Incident review framework to facilitate incident tracking, investigation, pivoting and closure	Must have	
B20	Risk scoring framework to apply risk scores to any asset or user based on relative importance or value to the business	Must have	
B21	The proposed solution must be able to read data input from the following static log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. Windows Events Logs c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.	Good to have	
B22	The solution must be able to provide the capability to fully customise alerts, reports and dashboards to the business requirements.	Must have	
B23	The solution must allow tracking of incidents from correlation rule through investigation of that event to closure.	Good to have	
B24	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc to provides rapid insights and operational visibility into large-scale Unix and Linux environments machine data : syslog, metrics and configuration files.	Good to have	
B25	Integration with corporate directories (AD, LDAP, etc) to extract employee information including: -- Employee user names, first, last, phone, manager, department, location, if privileged, if on watchlist, start and end dates, etc.Enables ability to correlate multiple user names back to a single employee	Must have	
B26	The solution must be able to provide the capability to annotate events, modify status, build a chronological timeline for the incident before and after a triggered event.	Good to have	
B27	The solution must be able to assign any arbitrary risk score to any data point or fields, example,user name, host name, location etc.	Good to have	
B28	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.	Must have	
B29	The solution must be able to support multiple transport mechanisms such as TCP,STIX and Trusted Automated exchange of Indicator Information (TAXII).	Must have	
B30	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built.	Good to have	

B31	The solution must be able to support the following indicators: 1.Network,IP - HTTP Referrer, User Agent, Cookie, Header, Data, URL - Domain - Endpoint - File Hash, Name, Extension, Path and Size - Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data - Process Name, Arguments, Handle Name, Handle Type - Service Name, Description - Certificate - Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm - Email - Email Address, Subject Body	Must have	
B32	Solution should support triaging of alerts from number of security products including SIEM, DLP, IPS, WAF, Anti-APT, AV, EDR, Firewall (all with Well Known OEM's as well as Open source platforms) .	Must have	
B33	Solution should support machine driven triaging algorithms that considers contextual parameters, historical behaviour and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same · Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert. · Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on. · Central Threat Intelligence feed should also be applied to identify threats through known bad actors	Good to have	
B34	Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters	Good to have	
B35	Investigation module should integrate with log sources (ETDR, EPP, Data Lake) on demand to pull data related to the investigated alert. It should also include charting and graphs to analyse data	Good to have	
B36	Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise(IOCs), external network connections.	Must have	
B37	Solution should support models to build up the entire attack chain-from attack inception, progress of the attack and spread to attack in the network.	Must have	
B38	Solution should support features to identify attacker attributes including threat intelligence score of attacker, who-is lookup information, geomapping in a single console.	Must have	
B39	Solution should provide run books for investigation steps corresponding to different types of attacks, derive attack inception and progress of the attack. i.e. Detect Patient Zero, Attack origin and Blast Radius.	Must have	
B40	Solution should support integration with open source or commercial IOC sources. List the supported sources which can be integrated with Solution and brief on the integration approach. Solution should support features to analyse and identify the impact of this attack on other assets.	Must have	
B41	Solution should provide case management features to store raw and analyzed data for a specific alert or set of alerts. Provide details on the what artefacts can be stored related to an investigation	Must have	

B42	Solution should support quick search across stored datasets in the Solution. Provide details of search features supported.	Must have	
B43	Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.	Must have	
B44	The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment.	Must have	
B45	The proposed solution machine learning capabilities must includes API access, role-based access controls for machine learning models.	Good to have	
B46	The proposed solutions machine learning capabilities must allow addition of custom machine learning algorithms from popular open source Python libraries.	Must have	
B47	The update in log format for a given OEM in its OS upgrade or other patch should be accordingly parsed on the solution provider side.	Must have	
Log Analysis			
C1	The solution should support log collection, flow collection and other standard method for integrating devices and applications. Logs obtained from devices should be copied and stored in vendor SoC within 3 minutes from the actual log event at the integrated device.	Must have	
C2	The solution should have connectors or similar integrators to support the devices/applications, wherever required the bidder should develop customized connectors/integrators at no extra cost	Must have	
C3	The proposed solution should support collection of events through customization of connectors or similar integration for the assets that are not natively supported. Solution should adhere to industry standards for event collection: syslog, OPSEC, WMI, SDEE, ODBC, JDBC, FTP, SCP, HTTP, text file, CSV, XML file etc.	Must have	
C4	All log data to be authenticated (time-stamped across multiple timezone) encrypted and compressed before transmission to manager console.	Must have	
C5	The solution should have high availability feature built in for automated switch over to secondary collector/integrator in the event of primary collector failing. No performance degradation is permissible even in case of failure	Must have	
C6	The solution should provide time based, criticality based, store and forward feature at each data collection point	Good to have	
C7	Solution should capability to filter undesired, non-security logs at collection, processing and visualization layer.	Must have	
C8	The proposed solution must be able to read data input from the following static log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. The solution must be able to accept the following live data streams from cloud server less functions like raw or JSON formatted data over HTTP/HTTPS.	Must have	
C9	The proposed solution should be able to consume logs from any log source without writing parser before hand or while integration. Parsers should be built once log is ingested	Must have	
C10	provide capability to search raw and indexed logs as full text, natural language, time range values, IPs, IP subnet mathematical & statistical functions, logical operators, occurrences count, regex, similar events, first & last seen, predictive & prescriptive search suggestions etc.	Must have	

C11	solution should capable of retrieving the archived logs for reporting, analysis, correlation, investigation and forensics.	Must have	
C12	Solution should have ability to restore / replay older logs for incident investigation	Must have	
C13	Solution should have capability to filter, blacklist or white list single or group of IP, user, URL, etc. in rules, reports, dashboard etc.	Must have	
C14	The solution should provide detection/correlation of logs with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open Source TI feeds)	Must have	
Management Center and administration			
D1	The solution should have a centralized correlation engine and a management center/console which allows creation of an unlimited number of correlation rules	Must have	
D2	The solution should be able to perform different correlations (but not limited to): Rule based, Historical based, Heuristics based, Behavioral based, etc., across different devices and applications	Must have	
D3	The solution should be able to parse and correlate multi-line logs and flow data.	Must have	
D4	The solution should have the ability to correlate all the field present in a log/flow data.	Must have	
D5	The solution should have the ability to gather information on real time threats and zero day attacks from anti-virus, IPS and IDS and analyses data against the information for any threats	Must have	
D6	The solution should provide a web-based, user friendly console or a wizard based console to create rule.	Must have	
D7	The solution should support logical operation and nested rules for creation of complex rules.	Must have	
D8	The solution should allow applying filters and sorting of query results.	Must have	
D9	The solution should be able to accept or integrate with asset details to provide asset level events, incidents, vulnerabilities and issues.	Must have	
D10	The proposed solution should have the ability to perform free text search on events, incidents, rules and other parameters	Must have	
D11	The solution should support integration with big data platforms.	Must have	
D12	The solution should be able to integrate with incident management and ticketing tools	Must have	
Threat Intelligence			
E1	The proposed solution should detect threats using graph-based threat anomalies, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threat anomalies are public-facing website attack or fraudulent website activity.	Must have	
E2	The Proposed solution TI Service should anticipate likely threats to the Organization based on global threat events and data and provide proactive measures to prevent such happenings in the Organization.	Good to have	
E3	The Proposed solution should support integration of machine readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise & false positives in threat intelligence feeds	Must have	

E5	The Proposed Solution should track status of assets against IoCs, CVEs and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities. Service provider should track closure and corresponding risk reduction	Good to have	
E6	The Solution should support STIX/TAXII for automated integration of actionable intelligence with security technologies.	Must have	
E7	The solution should support 3rd party / external threat intelligence to aid incident response by bringing in organizational context and internal information available in SIEM and other sources of security information	Must have	
E8	The proposed solution should detect threats like Lateral Movement and Data Exfiltration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.	Must have	
E9	The Proposed solution should Automatically enrich all incoming events with minimum following information. These fields should be customizable to add/modify/delete as desired by administrator): - Asset Owner, BIA & CIA - Geo-location of IP - Reputation of IP, URL, File etc. - Hash of files - Historical security incidents on same IP/same host/same user/same vulnerability/same location etc. - Threat Intelligence: (IoAs), (IoCs), and adversary's TTPs - Vulnerability information of asset. - Application Security review data. - Zone classification - Risk score of assets Bidder to Provide details on what additional enrichment options can be provided by the solution.	Must have	
E10	The Proposed solution should be capable to correlate events, network activity data, alerts, and vulnerability data to provide complete view of security threats and generate real-time security alerts	Must have	
E11	The Proposed solution should be capable to detect Slow attacks, advance persistent threats, file less attacks, advance malwares, zero-day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI / ML. Also, capable to prevent & predict known-known, known-unknown and unknown-unknown threats by monitoring entire IT infrastructure and leveraging real-time threat intelligence.	Must have	
E12	The solution must be able to integrate with real time threat intelligence feeds for the purpose of correlating events. These feeds should be updated automatically.	Must have	
E13	The correlations engine should be updated with real time security intelligence updates from the OEM	Must have	
Network Detection and response (NDR)			
F1	The solution should support On-premise deployment	Must have	
F2	The Proposed solution must be PCI-DSS or ISO 27001 Compliant	Good to have	
F3	Scalability of the proposed solution should be such as to cover critical network segments/verticals with abillty to ingest up to 30,000 FPS / 30 Gbps Per Data Centre (DC & DR)	Must have	
F4	The Proposed solution should have separate component for packet/flow sensor, telemetry processing and management functions for ideal performance.	Must have	

F5	The Proposed solution should support installation of all components manually e.g. Threat intelligence database, Geo-IP database, IP reputation, Upgrade firmware/ upgrade patches etc. (offline download & install). This is to avoid any limitations to the solution inside an air-gapped environment (absence of internet connectivity)	Good to have	
F6	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts.	Must have	
F7	The solution must support application definition beyond protocol and port. The system must support the identification of applications using ports other than the well-known, and applications tunnelling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP).	Must have	
F8	The solution must Identify & profile traffic by TCP and UDP ports.	Must have	
F9	Solution must support Netflow collection and correlation.	Good to have	
F10	The Solution should capture flow information from multiple network points like Network traffic collected via TAP, SPAN, and/or Mirror OR must support JFlow, SFLow, IPFIX collection and correlation.	Must have	
F11	The solution must support traffic profiling associated with logical network design (e.g., Subnet/CIDR).	Must have	
F12	The solution must identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.).	Must have	
F13	The solution must create clearly independent and differentiated profiles from local traffic vs. traffic originating or destined for the internet.	Must have	
F14	The solution must support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc	Must have	
F15	The solution must be able to adjust itself in DHCP environment and yet uniquely identify machines with high accuracy despite change of IP Address	Must have	
F16	Solution shall have a feature capable of enabling retrospective analysis of the incident's logs, returning the connection in seconds, minutes, hours or days before a certain anomaly had been identified	Must have	
F17	Solution shall create unique profiling for each user and device, as well as for the relations between them.	Must have	
F18	The Proposed Solution must be able to scale up and down based on changes in scope	Must have	
F19	The Proposed solution must able to monitor all network traffic in real time	Must have	
F20	The Proposed solution able to query at least 1 months' worth of meta historic data	Must have	
F21	The solution should Integrate with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provide full historical mapping of User Name to IP address logins in a searchable format	Must have	
F22	The Proposed solution should be able to Obtain/receive logs from Various critical infrastructure log sources such as SIEM, DNS logs, DHCP logs, AD logs etc. for additional correlation if required.	Good to have	

F23	The solution should provide the capability to respond quickly and effectively with complete knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing security controls.	Must have	
F24	The solution should be capable of providing visibility of east-west traffic in an encapsulated network of ACI / SDA fabric, Natively or with a Use of VM based Telemetry sensor or should be feasible in a way. (Bidder to mention feasibility)	Goot to have	
F25	The Solution should be intelligent and should automatically tweak itself through automated learning	Must have	
F26	Support creation of custom models for anomaly detection	Must have	
F27	The solution must detect “zero-day” events by leveraging anomaly based detection.	Must have	
F28	The solution must dynamically learn behavioural norms and expose changes as they occur.	Must have	
F29	The solution must detect and present views of traffic pertaining to observed threats in the network.	Must have	
F30	The solution must display traffic profiles in terms of packet rate. This capability must be available for simple TCP analysis (TCP Flags, etc.) but rate-based information may be presented for other profiles (e.g., applications).	Must have	
F31	The solution must be able to profile communication originating from or destined to the internet by Geographic regions in real-time.	Good to have	
F32	The solution should Analyse access and its abuse with identity-centric behaviour analytics	Good to have	
F33	The solution should Model good behaviour to expose unknown bad through peer groups, clustering and outliers	Must have	
F34	The solution should Leverage predictive security analytics to risk-score incidents.	Must have	
F35	The Solution should Optimize resources and time with use machine learning algorithms efficiently, unsupervised & shall be able to predict/detect anomalies.	Must have	
F36	Solution must be able to identify/alert new and unknown attack behaviours without making use of signatures or rules.	Must have	
F37	Solution should support a rule engine for users to define custom rules to leverage NDR capability. Rule engine should support all possible fields & parameters from a Packet header.	Must have	
F38	Solution must be able to identify any anomalous behaviour in the environment and alert/highlight these behaviours in real time. (Real time alerts)	Must have	
F39	The solution must detect internal denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc., identify the presence of botnets in the network, identify DNS spoofing attack etc. and detect long-lived connections that may be associated with data-exfiltration.	Must have	
F40	The solution must be able to detect suspicious communication channels Services or applications not running over its standard ports. (i.e. HTTP not over port 80)	Must have	
F41	The solution must be able to Detect and predict any data exfiltration by identifying abnormal behaviour as a part of cyber kill chain stages / MITRE / a well known attack framework.	Good to have	
F42	The solution must be able to Identify abnormal communication for protocol, commands, non-standard ports anomalies	Must have	
F43	The solution must be able to identify IP / Port scanning reconnaissance attacks	Must have	

F44	The solution must be able to identify Malware / malicious bots detection through C2 (command and control) communication	Must have	
F45	The solution should provide Detection of data exfiltration based on abnormal packet size (such as exfiltration in ICMP,DNS packets)	Must have	
F46	The solution should provide Detection of lateral movement based on suspicious connections with machines in the network	Must have	
F47	The solution should provide Detection of network crawling based on anomalous pattern detection	Must have	
F48	The solution should provide detection/correlation of Communication/Flows with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open Source TI feeds)	Must have	
F49	The solution should be able to store PCAP & Meta data of Communication/Flows if matched with malicious IP's / hosts / Domains / sites /IOC's (leveraging external/Third Party/Open Source TI feeds)	Must have	
F50	The solution must be able to identify Attack & Reconnaissance Tools - Check for commonly used penetration testing tool and malware user agents	Must have	
F51	The solution must be able to identify Possible Masqueraded file transfer - Look for files transferred with an incorrect file extension. Ignore common external domains.	Must have	
F52	The solution must be able to identify BitCoin Activity - Any communications using the BitCoin mining protocol	Must have	
F53	New User Agent communication - Any new/suspicious user agent communication seen on from/to device which is rare on the device/in the whole environment	Must have	
F54	Identifying traffic of Privacy VPN's - Personal VPN solutions which enable the user to avoid network monitoring solutions.	Must have	
F55	The proposed Solution should have inbuilt Models to detect use of various cloud storage services. (eg. Amazon S3, Dropbox etc)	Must have	
F56	The proposed solution should be capable of identifying APT Activity - Detection of known Advanced Persistent Threat indicators.	Must have	
F57	The proposed solution should be able to identify TCP/UDP malformed packets, TCP/IP stack fingerprinting methodologies e.g. Christmas Tree packet.	Must have	
F58	Non-standard DNS server used - Devices using uncommon DNS servers which were previously idle/were not DNS servers	Must have	
F59	The solution must be able to identify RST storm- A large number of packets with the reset flag set. This may disrupt normal communications	Must have	
F60	The solution must be able to identify Vulnerable Protocols - Use of out-of-date/Known Vulnerable Protocols e.g. SMB, Kerberos,NetBios, old versions for TLS/SSL.	Must have	
F61	The solution must be able to identify Unusual Connectivity- New or unusual connections, either an external connection to/from domains/sources that are Unusual/Suspicious/rare.	Must have	
F62	The solution must be able to identify Address Scan - Scanning for single/multiple devices listening on a specific port	Must have	
F63	The solution must be able to identify Port Scan - Scanning single/multiple devices to see which ports are open on it.	Must have	
F64	The solution must be able to identify Bruteforcing - Repeated failed logins (KERBEROS, SSH or FTP). This could be indicative of malicious password guessing.	Must have	

F65	Solution must identify a ransomware attack basis the network traffic and alert the respective team..	Must have	
F66	Solution must identify and investigate suspicious volumes of data transferred internally.	Must have	
F67	Solution must identify and investigate anomalies in patterns of DNS requests.	Must have	
F68	Solution must check for any Active sessions for longer than accepted time period	Must have	
F69	The solution should detect and alert on anomalies in DNS communications so as to pre-emptively help detect security risks.	Must have	
F70	The solution shall be able to identify crypto compliance for endpoints (TLS, SSL versions)	Must have	
F71	The solution must do Identification of Malicious behaviour in encrypted traffic without decryption.	Good to have	

The bidder is required to provide exhaustive list of the hardware, software, etc. to implement the project.
Dated this…… Day of……2022

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure K - Client Reference

(Bidder's Letter Head)

RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022

Sr.No	Particulars	Details
1	Name of the Organization	
2	Contact Person Name and Designation	
3	Phone Number of the Contact person	
4	Email Address of the Contact person	

(Signature)

(Name) (In the capacity of)
Duly authorized to sign Bid for and on behalf of

Annexure M - Commercial Bid Form
(Bidder's Letter Head)

(To be included in Commercial Bid Folder)

To

NPCI

Dear Sirs,

Re: RFP for procurement of Next Generation Security information and event management (SIEM) Solution- RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022.

Having examined the Bidding Documents placed along with RFP, we, the undersigned, offer to provide the required infrastructure in conformity with the said Bidding documents for the sum of Rs.……..(Rupees_____) (exclusive of taxes) or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to provide External Cyber Threat Intelligence Solutions within the stipulated time schedule. We agree to abide by the Bid and the rates quoted therein for the orders awarded by NPCI up to the period prescribed in the Bid which shall remain binding upon us. Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We have complied with all the terms and conditions of the RFP. We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this…… Day of……..2022

(Signature)

(Name) (In the capacity of)

Duly authorized to sign Bid for and on behalf of

Request for proposal for procurement of Next Generation Security information and event management (SIEM) Solution

Annexure N - Commercial Bid

RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022
RFP for procurement of SIEM Solution
(Bidder's Letter Head)

Table 1:

Sr. No.	Description	Qty	Equipment cost with 1 year onsite OEM warranty		AMC/Support for 2nd Year		AMC/Support for 3rd Year		Grand total (GT) (INR)
			Unit Price (INR)	Total Unit Price (INR)	Unit Price (INR)	Total Unit Price (INR)	Unit Price (INR)	Total Unit Price (INR)	
		A	B	C=A*B	D	E=A*D	F	G = A*F	T= (C+E+G)
1	Software cost								
2	Hardware cost								
3	Implementation cost (if any)								
4	Support cost								
5	Others (if any, please specify)								
Total (GT)									

- The bidder shall meet the requirements of Goods & Services Tax (GST)

(Amount in Rs)

All prices are exclusive of taxes.

Dated this…… Day of……..2022

(Signature)
(Name)
(In the capacity of)
Duly authorized to sign Bid for and on behalf of

Request for proposal for procurement of Next Generation Security information and event management (SIEM) Solution
Annexure L - Bill of Material

RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022
(Bidder's Letter head)

Line Item Wise Prices
(Details of all line items of the Commercial Bid)

Line Item	Item Name / Part No	Description	Unit Price incl 1 year warranty and support	2nd Year- AMC with support	3rd Year- AMC with support	Sub Total	Quantity	Total Price
1								
2								
3								
4								
5								
5								
6								
Total (Exclusive of taxes)								

- Delivery locations would be as per clause 8.8 of the RFP

NON-DISCLOSURE AGREEMENT (NDA)

This Non-Disclosure Agreement ("**Agreement**") is made and entered on this -------- day of ----------, 2022 ("**Effective Date**") between

NATIONAL PAYMENTS CORPORATION OF INDIA, a company incorporated in India under Section 25 of the Companies Act, 1956 (corresponding to Section 8 of the Companies Act, 2013) and having its registered office at **1001A, B Wing, 10th Floor, The Capital, Plot 70, Block G, Bandra-Kurla Complex, Bandra (East), Mumbai - 400 051, Maharashtra**, CIN: U74990MH2008NPL189067 (Hereinafter referred to as "**Disclosing Party**", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns);

AND

_____, a company/Partnership/Sole Proprietor/Association of People/ and having its registered office at _____ CIN;_____ (Hereinafter referred to as "**Receiving Party**", which expression shall mean and include unless repugnant to the context, its successors and permitted assigns).

Disclosing Party and Receiving Party shall hereinafter be jointly referred to as the "Parties" and individually as a "Party".

NOW THEREFORE

In consideration of the mutual protection of information herein by the parties hereto and such additional promises and understandings as are hereinafter set forth, the parties agree as follows:

Article 1: PURPOSE

The purpose of this Agreement is to maintain in confidence the various Confidential Information, which is provided between Disclosing Party and Receiving Party to perform the considerations (hereinafter called "Purpose") set forth in below:

Purposes:

1.
2.
3.
4.
5.

Article 2: DEFINITION

For purposes of this Agreement, "**Confidential Information**" means the terms and conditions, and with respect to Disclosing Party, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to the Purpose (including, but not limited to, information identified as being proprietary and/or confidential or pertaining to, pricing, marketing plans or strategy, volumes, services rendered, customers and suppliers lists, financial or technical or service matters or data, employee/agent/ consultant/officer/director related personal or sensitive data and any information which might reasonably be presumed to be proprietary or confidential in nature) excluding any such information which (i) is known to the public (through no act or omission of the Receiving Party in violation of this Agreement); (ii) is lawfully acquired by the Receiving Party from an independent source having no obligation to maintain the confidentiality of such information; (iii) was known to the Receiving Party prior to its disclosure under this Agreement; (iv) was or is independently developed by the Receiving Party without breach of this Agreement; or (v) is required to be disclosed by governmental or judicial order, in which case Receiving Party shall give the Disclosing Party prompt written notice, where possible, and use reasonable efforts to ensure that such disclosure is accorded confidential treatment and also to enable the Disclosing Party to seek a protective order or other appropriate remedy at Disclosing Party's sole costs.

Article 3: NO LICENSES

This Agreement does not obligate the Disclosing Party to disclose any particular proprietary information; to purchase, sell, license, transfer, or otherwise dispose of any technology, services, or products; or to enter into any other form of business, contract or arrangement. Furthermore, nothing contained hereunder shall be construed as creating, conveying, transferring, granting or conferring to the Receiving Party any rights, license or authority in or to the Confidential Information disclosed to the Receiving Party under this Agreement or to any information, discovery or improvement made, conceived, or acquired before or after the date of this Agreement. No disclosure of any Confidential Information hereunder shall be construed to be a public disclosure of such Confidential Information by the Receiving Party for any purpose whatsoever. This Agreement does not create a joint venture or partnership between the parties.

Article 4: DISCLOSURE

1. Receiving Party agrees not to use the Disclosing Party's Confidential Information for any purpose other than for the specific purpose as mentioned in Article 1. Receiving Party agrees and undertakes that it shall not, without first obtaining the written consent of the Disclosing Party, disclose or make available to any person, reproduce or transmit in any manner, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except both parties may disclose any Confidential Information to their Affiliates, directors, officers, representatives, agents, employees or advisors of their own or of Affiliates on a "need to know" basis to enable them to evaluate such Confidential Information in connection with the negotiation of the possible business relationship; provided that such persons have been informed of, and agree to be bound by obligations which are at least as strict as the recipient's obligations hereunder. For the purpose of this Agreement, Affiliates shall mean, with respect to any party, any other person directly or indirectly Controlling, Controlled by, or under direct or indirect common Control with, such party. "Control", "Controlled" or "Controlling" shall mean, with respect to any person, any circumstance in which such person is controlled by another person by virtue of the latter person controlling the composition of the Board of Directors or owning the largest or controlling percentage of the voting securities of such person or by way of contractual relationship or otherwise.
2. The Receiving Party shall use the same degree of care and protection to protect the Confidential Information received by it from the Disclosing Party as it uses to protect its own Confidential Information of a like nature, and in no event such degree of care and protection shall be of less than a reasonable degree of care.
3. The Disclosing Party does not make any representation or warranty as to the accuracy or completeness of Confidential Information. The Disclosing Party shall not be in any way responsible for any decisions or commitments made by Receiving Party in relying on the Disclosing Party's Confidential Information.

Article 5: RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

The Receiving party agree that upon termination of this Agreement or at any time during its currency, at the request of the Disclosing Party, the Receiving Party shall promptly deliver to the Disclosing Party the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Receiving Party or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

Article 6: INJUNCTIVE RELIEF

The Receiving Party hereto acknowledge and agree that it would be impossible or inadequate to measure and calculate the Disclosing Party's damages from any breach of the covenants set forth herein. Accordingly, the Receiving Party agrees that in the event of a breach or threatened breach by the Receiving Party of the provisions of this Agreement, the Disclosing Party will have no adequate remedy in money or damages and accordingly the Disclosing Party, in addition to any other right or remedy available, shall be entitled to injunctive relief against such breach or threatened breach by the Receiving Party and to specific performance of any such provisions of this Agreement. Disclosing Party shall be entitled to recover its costs and fees, including reasonable attorneys' fees, incurred in obtaining any such relief. If the Receiving Party is aware of a suspected or actual breach of this Agreement from Receiving Party's side, it shall (i) promptly notify the Disclosing Party in writing

immediately; and (ii) take all reasonable and essential steps to prevent or stop any suspect or actual breach of this Agreement; (iii) Receiving Party shall cooperate with any and all efforts of the Disclosing Party to help the Disclosing Party regain possession of Confidential Information and prevent its further unauthorized use.

Article 7: NON-WAIVER

No failure or delay by either party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement thereof or the exercise of enforcement of any other right, remedy or power.

Article 8: DISPUTE RESOLUTION

Notwithstanding anything contained in Article 6 and the express rights of the Disclosing party contained and provided thereto, If any dispute arises between the parties hereto during the subsistence or thereafter, in connection with or arising out of this Agreement, the dispute shall be referred to arbitration under the Indian Arbitration and Conciliation Act, 1996 (or any statutory modification or re-enactment thereof and rules framed thereunder from time to time) by a sole arbitrator appointed by Disclosing Party Arbitration shall be held in Mumbai, India. The proceedings of arbitration shall be in the English language. The arbitrator's award shall be final and binding on the parties.

Article 9: GOVERNING LAW AND JURISDICTION

This Agreement shall be governed exclusively by the laws of India and jurisdiction shall be vested exclusively in the courts at Mumbai in India.

Article 10: NON-ASSIGNMENT

This Agreement shall not be amended, modified, assigned or transferred by Receiving Party without the prior written consent of Disclosing Party.

Article 11: TERM

This Agreement shall remain valid from the effective date till the time the Receiving Party is receiving Confidential Information or until the termination of this Agreement, whichever is later. This Agreement may be terminated by either Party by giving prior written notice of sixty (60) days to the other Party. However, the Receiving Party shall not be entitled to terminate this Agreement if there is subsisting business engagement between the Parties. Irrespective of the termination, the obligation of the Receiving Party to protect Confidential Information disclosed under this Agreement shall survive termination of this Agreement and shall remain in effect indefinitely.

Article 12: INTELLECTUAL PROPERTY RIGHTS, Media Disclosure, Publicity and Public Interaction

12.1 Receiving Party shall not use or permit the use of Disclosing Party's names, logos, trademarks or other identifying data, or infringe Patent, Copyrights or interact with media for any disclosure of findings or otherwise discuss or make reference to Disclosing Party in any notices to third Parties, any promotional or marketing material or in any press release or other public announcement or advertisement, however characterized, without Disclosing Party's prior written consent.

12.2 Any interaction by the Receiving Party with media for any disclosure of findings, publicity, public interactions for undue advantage and/or any association whatsoever of Disclosing Party, without express consent/approval from Disclosing Party, shall result in breach, and for every incident of breach the Receiving Party shall be liable to pay the Disclosing Party, an amount which Disclosing Party, in its sole and absolute discretion, deems fit. This shall be without prejudice to the right of Disclosing Party to peruse any other right or remedy available to it under law.

Article 13: INDEMNITY

In the event the Receiving Party discloses, disseminates or releases any Confidential Information received from the Disclosing Party, except as provided in this agreement, such disclosure, dissemination or release will be deemed a material breach of this Agreement and the Receiving Party shall stop its breach of this agreement immediately and indemnify Disclosing party against losses resulting from its default, including the reasonable legal costs, which have been incurred by Disclosing party to investigate the default.

Article 14: GENERAL

1. Nothing in this Agreement is intended to confer any rights/remedies under or by reason of this Agreement on any third party.
2. Any notices or communications required or permitted to be given hereunder may be delivered by hand, deposited with a nationally recognized overnight carrier, electronic-mail, or mailed by certified mail, return receipt requested, postage prepaid, in each case, to the address of the other party first indicated above (or such other addressee as may be furnished by a party in accordance with this paragraph). All such notices or communications shall be deemed to have been given and received (a) In the case of personal delivery or electronic-mail, on the date of such delivery, (b) In the case of delivery by a nationally recognized overnight carrier, on the third business day following dispatch and (c) In the case of mailing, on the seventh working business day following such mailing.
3. This Agreement and the confidentiality obligations of the Parties under this Agreement supersedes all prior discussions and writings with respect to the Confidential Information and constitutes the entire Agreement between the parties with respect to the subject matter hereof and any additional agreement, if any, shall be binding along with that relevant Agreement in addition to this Non-Disclosure Agreement without affecting the provisions of this agreement. In the event where only this agreement is existing than the provisions of this Agreement shall prevail. If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provisions or part(s) thereof shall be stricken from this Agreement or modified, rewritten or interpreted to include as much of its nature and scope as will render it enforceable. The remaining provisions will continue in full force and effect.
4. Any breach of any provision of this Agreement by Receiving Party hereto shall not affect the Disclosing party's non-disclosure and non-use obligations under this Agreement.
5. The Parties agree that all Confidential Information shall remain the exclusive property of the Disclosing Party and its affiliates, successors and assigns.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement by their duly authorized representatives as of the Effective Date written above.

NATIONAL PAYMENTS CORPORATION OF INDIA	**TYPE COMPANY NAME**
By: Name:	By: Name:
Designation:	Designation: