RFP for procurement of Next Generation Security information and event management (SIEM) Solution - RFP # NPCI/RFP/2021-22/IT/17 dated 24.02.2022."							
Consolidated list of Replies to Pre-bid Queries							
S.No	**Document Reference**	**Page No**	**Clause No**	**Description in RFP**	**Clarification Sought**	**Additional Remarks (if any)**	**NPCI Response**
1	A5. Section 9 - Technical Specifications	38	A5. Section 9 - Technical Specifications	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).	Request you to please consider this The Solution quoted by the bidder should be in Gartner Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).		No Change in RFP Terms.
2	7.3 Technical Scoring Matrix	21	7.3 Technical Scoring Matrix	Customer BFSI reference in India Please provide at least 3 India References	Request you to lease consider reference in BFSI/ PSU/ Govt vertical.		No Change in RFP Terms.
3	A9. Section 9 - Technical Specifications	38	A9. Section 9 - Technical Specifications	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)	We do have DC/DR and DR will be active, but the data and log processing will be done only by primary. However you can use the analytics and see incidents in DR. hence for a wider participation request you to modify this clause as "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."		Our Understanding is Servers at DC1 will forward logs to SIEM solution at DC1, Servers at DC2 will forward logs to SIEM solution at DC2, a copy of all logs from DC1 SIEM solution should be available at DC2 SIEM Solution & vice-versa. No change in RFP Terms.
4	A10. Section 9 - Technical Specifications	38	A10. Section 9 - Technical Specifications	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.	We do have DC/DR and DR will be active, but the data and log processing will be done only by primary. However you can use the analytics and see incidents in DR. hence for a wider participation request you to modify this clause as "The proposed solution must support single site or multiple site clustering."		Devices at each Datacentre will be forwarding logs to local collector/broker, a copy of Collector/broker logs will be forwarded to Correlation engines of both DC1 & DC2 (DC & DR). We should have Log retension at both Data Cantre to achieve Compliance. We have dedicated Link for replication, Latency is within the limits. No change in RFP Terms.
5	B11. Section 9 - Technical Specifications	39	B11. Section 9 - Technical Specifications	Solution should able to integrate with any 3rd party / Open source SIEM.	please let us know the use case of this clause		We want to have centralised dashboard of other Open source SIEM's which we are currently operating.
6	B45. Section 9 - Technical Specifications	42	B45. Section 9 - Technical Specifications	The proposed solution machine learning capabilities must includes API access, role-based access controls for machine learning models.	Kindly modify this clause as "The proposed solution machine learning/Augumented Intelligent for UEBA capabilities must includes API access, role-based access controls for machine learning models. ."		No Change in RFP Terms.
7	B46. Section 9 - Technical Specifications	42	B46. Section 9 - Technical Specifications	The proposed solutions machine learning capabilities must allow adidition of custom machine learning algorithms from popular open source Python libraries.	Kindly modify this clause as "The proposed solutions machine learning capabilities/Augumented Intelligent for user and entity behavior Analytics must allow adidition of custom machine learning algorithms from popular open source Python libraries."		No Change in RFP Terms.
8	C5. Section 9 - Technical Specifications	42	C5. Section 9 - Technical Specifications	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	Pleae clarify -Are you referring to this requirement for DC and DR or only at the same site.		This will be only at the same site. No change in RFP Terms.
9	D11. Section 9 - Technical Specifications	43	D11. Section 9 - Technical Specifications	The solution should support integration with big data platforms.	for Big data integration we need more details the use cases, hence please share the same		Big Data Integration refers to Integration with platforms to perform analytics. If Product has inherent capability, no external integration is required.

10	F10. Section 9 - Technical Specifications	45	F10. Section 9 - Technical Specifications	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.	Please suggest - Is NPCI having a mechanism to send the flow information to SIEM solution ?		This requirement is for NDR module in NextGen SIEM - NPCI will leverage existing Network Devices to send flow information directly wherever possible. NPCI is not having a mechanism to convert TAP/SPAN/Mirrored traffic to Flow data & send to NBAD module. Such Mechanism to be factored by the Bidder in the solution.
11	F71. Section 9 - Technical Specifications	48	F71. Section 9 - Technical Specifications	The solution must do Identification of Malicious behaviour in encrypted traffic without decryption.	Can you please elaborate this requirement in details.		Encrypted Traffic Analysis is a method of malware detection and cryptographic assessment of secured network sessions, which does not rely on decryption. No Change in RFP Terms.
12	Section 9 - Technical Specifications	38	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).	Need to rephrase as - The Solution quoted by the bidder should be in Gartner Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).	Referring Gartner MQ itself narrow down vendors for evaluation and give broader coverage to SIEM vendors for participation in RFP.	No Change in RFP Terms.
13	Section 9 - Technical Specifications	41	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	Need to rephrase as - The solution must be able to support the following indicators: 1. Network,IP - Domain - File Hash - Email	IOC are not limited to given indicators only and vary from intelligence feed available with TI communities. For the broader participation, listed indicators (1. Network,IP, Domain, File Hash, Email) are good to consider and standard for all solution vendors to comply.	No Change in RFP Terms.
14	4.1 Eligibility Criteria	12	2.1	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).	We request to amend the caluse as " Should we have **Positive NETWORTH** instead of profit after tax in last 3 financial years (FY 2018-19, 2019-20, 2020-21). Or should be Profit **After Tax in any two FY.**	We request you to amend the caluse as Due to Pandemic our **Profit after Tax is not there in FY-20-21 however we have postive networth. In lockdown the profit after tax affected due to many reason**. All other PSU BFSI considering this caluse and giving relaxation for FY20-21. PLease help to amend so that we can submit our BID.	Kindly refer Corrigendum 1
15	Payment Terms:	30	8.19	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.	We request to amend the payment term as Yearly Advance as it is software and need to bill on Year basis		No Change in RFP Terms.
16	Delivery schedule	25	8.1	Delivery of hardware, software, and license should be within 6 weeks	Please help to amend this as delivery in 8-10 weeks as now deliveies are getting affected.		Refer Corrigendum.
17	3.1	10	3.1	Scope of Work	Can you please provide the geographical location of DC and DR		Refer page 24 of Next-Gen SIEM RFP NPCI/RFP/2021-22/IT/17 dated 24.02.2022 on NPCI's official Website.
18	3.1	10	3.1	Scope of Work	What is the Connectivity between DC and DR		We have L3 Connectivity between NPCI DC Chennai & NPCI DC Hyderabad. (Both DC's are active-active)
19	3.1	10	3.1	Scope of Work	Do you prefer a Hardware Appliance or a Virtual Appliance for the SIEM ?		We Prefer Hardware Appliance. Entire Solution to be factored by Bidder.
20		68	B.2	Technical Compliance	Total Number of Servers to be added under the Scope of this Project .		Total Around ~5000 Devices per Data Centre
21					What is the retention period required for storing Logs		4 months online retension (Hot). 18 Months Cold Retension (NPCI's Backup solution). Solution should support restore & replay of logs as per RFP ask.
22		68	B.3	Technical Compliance	Are you also looking at SOAR from this Project .		We are not looking for SOAR. No change in RFP Terms.

23		68	B.3	Technical Compliance	If SOAR is needed , How many Playbooks are to be created as part of the Project .		We are not looking for SOAR. No change in RFP Terms.
24		67	A.6	Technical Compliance	Is HA needed for all Components of SIEM ?		Yes.
25		68	B.2	Technical Compliance	Do you have any legacy / Home Grown Applications to be integrated with SIEM , Please provide Details .		We do have some XML, Java based homegrown applications.
26		48		Support Official Requirement	Where do you want the support Engineers to be Based at.		Support Engineers to be based at Hyderabad.
27	RFP-for-procurement-of-SIEM-Solution	11	3.1- Scope of work	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		Please change- Qualified resources as SIEM SME's with L2 - L3 Level Onsite Support for 3 years 16/5*365, basis with defined SLA in RFP. At least 1 Onsite engineer should present in Hyderabad 16/5*365 Days. Rest support will be on-call basis	No Change in RFP Terms. Bidder to factor resources & deliverables accordingly.
28	RFP-for-procurement-of-SIEM-Solution	12	4.1 - Eligibility criteria			Please relax this clause and change as per- **Other than MSME-** 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 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.	No Change in RFP
29	RFP-for-procurement-of-SIEM-Solution	21	7.3 Technical Scoring Matrix	Customer BFSI reference in India Please provide at least 3 India References (Combination of Bidder + OEM reference would be an added advantage)		Please relax this clause and consider- any 3 SIEM reference from OEM/ Bidder	No Change in RFP Terms.
30	RFP-for-procurement-of-SIEM-Solution	23	8.4 Performance Bank Gurantee	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		Please change - The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 3% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 3 months	No Change in RFP
31	RFP-for-procurement-of-SIEM-Solution	28	8.5 SLA	Severity- Non-availability of the SIEM solution for more than 15 Minute		Please change- Non-availability of the SIEM solution for more than 45 Minute	No Change in RFP Terms.
32	RFP-for-procurement-of-SIEM-Solution	29	8.5 SLA	SLA Measurement & Failure Indicator - **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		Please change- SLA Measurement & Failure Indicator - Severity 1 – Response time – 30 Minutes Resolution time – 45 Minutes Severity 2 – Response time – 60 Minutes Resolution time – 90 Minutes Severity 3 – Response time – 24 Minutes Resolution time – 1.5 Day	No Change in RFP Terms. As Bidder will be deploying resources at NPCI, response times are in-line with respect to criticality of SIEM infrastructure.
33	RFP-for-procurement-of-SIEM-Solution	30	8.19 Payment terms	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.		Please change - Payment shall be made Yearly in advance 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.	No Change in RFP Terms.

34	RFP-for-procurement-of-SIEM-Solution	38	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).	Need to rephrase as - The Solution quoted by the bidder should be in Gartner Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).	Referring Gartner MQ itself narrow down vendors for evaluation and give broader coverage to SIEM vendors for participation in RFP.	No Change in RFP Terms.
35	RFP-for-procurement-of-SIEM-Solution	41	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	Need to rephrase as - The solution must be able to support the following indicators: 1. Network,IP - Domain - File Hash - Email	IOC are not limited to given indicators only and vary from intelligence feed available with TI communities. For the broader participation, listed indicators (1. Network,IP, Domain, File Hash, Email) are good to consider and standard for all solution vendors to comply.	No Change in RFP Terms.
36	RFP-for-procurement-of-SIEM-Solution	67	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.		It is recommended to keep the EPS number with a peak buffer of 5-10%. To handle 60K EPS, irrespective of the OEM NPCI would require almost double the compute & storage compared to the compute & storage of 30K EPS. Hence would request to reconsider Peak and sustained numbers. We recommend to keep a single EPS number.	Hardware Sizing should be mapped to handle peak EPS (60K) as per RFP ask.
37	RFP-for-procurement-of-SIEM-Solution	68	B11	Solution should able to integrate with any 3rd party / Open source SIEM.	Which SIEM is currently in use ?		We are currently using HP Arcsight 7.4. We want to forward Open source Logs e.g. ELK, Logstash or Fluentd to Proposed SIEM solution.
38	RFP-for-procurement-of-SIEM-Solution	73	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)	Please clarify if 30K FPS / 30 Gbps is per location / DC. or is it combined traffic of 30 Gbps of DC & DR put together. If so, please clarify the split of the traffic between DC & DR.		Requirement is to have 30,000 FPS / 30 Gbps Per Data Centre to be ingested to NDR module of Next generation SIEM solution. (We are looking for a combined SIEM + NDR solution)
39	RFP-for-procurement-of-SIEM-Solution.pdf	73	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)	Please clarify the following: 1. Bandwidth utilization to monitor? (i.e traffic – how many links and how much Gbps per link and what is the current average utilization per link today) per DC, please describe in detail for sizing of each of the above sections and scenarios 2. What network switches are in use and do they have available TAP or SPAN ports ? How many ports are available and what network interfaces? (1G copper or fiber, 10G fiber , 40G fiber) please describe in detail for sizing. 3. Are any packet broker currently used ? 4. How many segments to be monitored at each location. 5. Please explain the connectivity at each segment (is it 1 G/10G copper, Fiber, LX, SX or LC)		For each Data Centre (DC1 & DC2) - A. Netflow , jflow & Sflow will account to 10% of Data (out of 30Gbps / 30,000FPS). Rest of the data will be captured using Tap/Mirror/Span. Bidder shall consider 4 Physically Distinct Network segments within each Data Centre to collect the Flows/Span/tap/mirror data. B. Retension period for flow data is as per RFP Ask. C.Network interfaces for FLow/SPAN/TAP collection to be considered - Min. 4x1G Copper Ports, 4x1G Fiber Ports, 4x10G Fiber Ports (Bidder to factor Transreceivers/SFP's) D. No Packet Brokers / No Network TAP's currently in Use. E.Network switches are of Cisco & Juniper & can be used for SPAN wherever necessary.
40	RFP-for-procurement-of-SIEM-Solution.pdf	76	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)	Please clarify if PCAP needs to be done only for flows which match a malicious IP / host etc and not for all events / flows.		Understanding meets the expectations. No change in RFP Terms.

41	RFP-for-procurement-of-SIEM-Solution.pdf	67	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.		It is recommended to keep the EPS number with a peak buffer of 5-10%. To handle 60K EPS, irrespective of the OEM NPCI would require almost double the compute & storage compared to the compute & storage of 30K EPS. Hence would request to reconsider Peak and sustained numbers. We recommend to keep a single EPS number.	Bidder should factor requirements as per the RFP Ask. No Change in RFP Terms.
42	RFP-for-procurement-of-SIEM-Solution.pdf	68	B11	Solution should able to integrate with any 3rd party / Open source SIEM.	Which SIEM is currently in use ?		We are currently using HP Arcsight 7.4. We want to forward Open source Logs e.g. ELK, Logstash or Fluentd to Proposed SIEM solution.
43	RFP-for-procurement-of-SIEM-Solution.pdf	73	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)	Please clarify the following: 1. Bandwidth utilization to monitor? (i.e traffic – how many links and how much Gbps per link and what is the current average utilization per link today) per DC, please describe in detail for sizing of each of the above sections and scenarios 2. What network switches are in use and do they have available TAP or SPAN ports ? How many ports are available and what network interfaces? (1G copper or fiber, 10G fiber , 40G fiber) please describe in detail for sizing. 3. Are any packet broker currently used ? 4. How many segments to be monitored at each location. 5. Please explain the connectivity at each segment (is it 1 G/10G copper, Fiber, LX, SX or LC)		For each Data Centre (DC1 & DC2) - A. Netflow , jflow & Sflow will account to 10% of Data (out of 30Gbps / 30,000FPS). Rest of the data will be captured using Tap/Mirror/Span. Bidder shall consider 4 Physically Distinct Network segments within each Data Centre to collect the Flows/Span/tap/mirror data. B. Retension period for flow data is as per RFP Ask. C.Network interfaces for FLow/SPAN/TAP collection to be considered - Min. 4x1G Copper Ports, 4x1G Fiber Ports, 4x10G Fiber Ports (Bidder to factor Transreceivers/SFP's) D. No Packet Brokers / No Network TAP's currently in Use. E.Network switches are of Cisco & Juniper & can be used for SPAN wherever necessary.
44	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	39	B7	The SIEM platform should have capability to provide automatic Notification to SOC teams as defined in playbooks based on Conditional decision & Trigger Functions	Kindly clarify the requirement of Playbooks in the SIEM solution. Playbooks are ideally a part of SOAR solutions	Kindly remove the word Playbooks	Refer Corrigendum.
45	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	40	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	Kindly clarify the need to assign an aribitary risk score to any field. Risk scores are usually assigned to Idendities and assets	Kindly modify to remove the clause arbitary risk score to any field or data point.	No Change in RFP Terms.
46	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	41	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	This feature is specific to a single OEM	Request to kindly remove this clause	No Change in RFP Terms.
47	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	41	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	This feature is specific to a single OEM	Request to kindly remove this clause	No Change in RFP Terms.

48	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	41	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	Kindly clarify the need for run books in the SIEM solution. Run books are usually a part of SOAR solutions.	Kindly remove the word run book	Refer Corrigendum.
49	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	42	C6	The solution should provide time based, criticality based, store and forward feature at each data collection point	Store and forward feature is not an NG SIEM functionality as it duplicates storage at multiple levels. Kindly clarify if the requirement	Kindly remove this clause	Refer Corrigendum.
50	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	42	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	This clause contradicts clause C2 where it has been mentioned to use connectors. We assume that collection of logs from any log source without writing parser should be okay	Kindly clarify our assumption in the clarification	For any unparsed log, the bidder should be able to develop parsers as per agreed SLA's.
51	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	49	Section 9 - Technical Specifications	Role and Responsibilities of onsite Team: Resource Level-L2(Sr. Security Analyst): Roles & Responsibilities: - Monitor SIEM Console & Dashboards and provide response to the reported incidents Filtered by L1. - Monitor and review the L1 activities - Provide notification and communication with Incident management and respective application team upon threat detection.	The alert and incident monitoring and management is relevent in SOC threat management/Incidenemt management. In this resources are expected to SIEM management so pls clarify	Kindly remove monitoring and analysis related Roles and responsibilities	No Change in RFP Terms.
52	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	49	Section 9 - Technical Specifications	Role and Responsibilities of onsite Team:			No Change in RFP Terms.
53	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	10	3.1	Bidder should support the migration of the Current SIEM Correlation Rulesets, policies, operations, Integrations and features	The content migration from one OEM may not be applicable so need to create the content manually taking exising content as input. Is this approach ok?	Kindly modify the wordings accordingly	Approach is OK. OEM/Bidder has to migrate all Rules,Policies and active lists from existing solution. Bidder should factor efforts to achieve as per RFP ask.
54	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	10	3.1	Implementation of the solution and migration of policies from existing solution to be done by Bidder/OEM directly.	The content migration from one OEM may not be applicable so need to create the content manually taking exising content as input. Is this approach ok?	Kindly modify the wordings accordingly	Approach is OK. OEM/Bidder has to migrate all Rules,Policies and active lists from existing solution. Bidder should factor efforts to achieve as per RFP ask.
55	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	26	8.15, Definitions 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.	The IT equipment and IT services related incident record maintenance should be under IT team and its downtime and SIEM un-availability due to that will be excluded from SLA	Kindly modify the wordings accordingly	No Change in RFP Terms.
56	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	28	8.15	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	Is this also included few logs not reporting dur to unavailability of Log collector/Agent ?	Kindly clarify , If yes need to factor resources to deliver this SLA	Yes. Resources needed to be factored accordingly. No change in RFP Terms.

57	RFP Reference No: NPCI/RFP/2021-22/IT/17 dated 24.02.2022	29	8.15	Service Level Category: Non-detection of security incidents by SIEM	This clause should be modified to cover non-detection of security incident by SIEM limited to the use cases defined in the solution	Kindly clarify or modify the wordings accordingly	Refer Corrigendum.
58	Section-4 Eligibility Criteria B] Other than start-ups	13	Sr. No. 3	There shall be no continuing statutory default as on date of submitting the response to the tender. Necessary selfdeclaration along with extract of auditors' report.	As books of accounts are closed financial year wise and latest accounts audited are of FY 2020-21. Hence necessary documents i.e. Statutory Audit Report or Tax Audit Report can be produced for FY 2020-21 only. Kindly confirm for which period self declaration to be provided and what documents would required in its supporting.		Last Audited Financial Year i.e. 2020-21
59	Section-8 8.4 Performance Bank Guarantee	23	8.4	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.	As per RFP clasue no. 8.2 "The term of the Notification of A**ward/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." So, we request you to kindly give clarity on exact period of validity of PBG.		Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 3 years, 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.
60	TECHNICAL SCORING MATRIX	21	7.3	Customer BFSI reference in India Please provide at least 3 India References (Combination of Bidder + OEM reference would be an added advantage)	Request you to change as "Customer BFSI/Govt. reference in India Please provide at least 3 India References (Combination of Bidder + OEM reference would be an added advantage)" for better participation		No Change in RFP Terms.
61					Kindly clarify Implementation is expected to be done by OEM or Bidder ?		It can be any of the two. Ownership will be with the Bidder.
62					Network switch to connect hardware in NPCI environment will be provided by NPCI or need to factor as a part of solution		Bidder to factor the entire solution & all its components according to the RFP ask. Network switch will be provided by NPCI. No Change in RFP Terms.
63	Scope of work:	10	3.1	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.	Request you to provide details on what is the make of existing SIEM tool		HP Arcsight 7.4
64	Annexure J Technical Compliance	39	B.13	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).	Request you to clarify which Make respective tools are used by NPCI		All leading Players & open source technologies in this space.
65	Section 9 - Technical Specifications	38	A11	The solution must have an automated backup and recovery process.	Plesae clarify if backup infrastructure needs to be provided by the bidder or will NPCI use own backup solution currently deployed		NPCI will provide Backup infrastructure. Backup script & path, process should be facilitated by the proposed solution or bidder.

66	Section 9 - Technical Specifications	38	A11	The solution must have an automated backup and recovery process.	If NPCI is to provide backup software and infrastructure, will it suffice to make the data to be backedup available as files ?		NPCI will provide Backup infrastructure. Backup script & path, process should be facilitated by the proposed solution or bidder.
67	Section 9 - Technical Specifications	38	A11	The solution must have an automated backup and recovery process.	If the bidder is required to provision backup setup, please provide details such as backup architecture (D2D or D2T or D2D2T) and the backup policy to be considered while sizing and designing backup solution,		NPCI will provide Backup infrastructure. Backup script & path, process should be facilitated by the proposed solution or bidder.
68	Section 9 - Technical Specifications	38	A11	The solution must have an automated backup and recovery process.	We understand the backup at DC and DR shall run independent with no replication across sites. Kindly confirm or clarify.		NPCI will provide Backup infrastructure. Backup script & path, process should be facilitated by the proposed solution or bidder.
69	3.1 Scope of work:	10		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.	We understand the NIC shall be 10G with SR optics populated. Kindly confirm or clarify		We required dual power and 4*1/10G FC NIC (with Transceiver) along with dedicated hardware management interface.
70	3.1 Scope of work:	10		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.	We understand the data at DC and DR will be independent with no replication across sites. Kindly confirm or clarify.		We required dual power and 4*1/10G FC NIC (with Transceiver) along with dedicated hardware management interface.
71	3	13	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.	Submission of statutory defalut is in relation to finance or blacklisting.			This is in relation to Finance. For blacklisting there is seprate format in i.e. Annexure D
72	Checklist	3	1.Online transfer of Rs 17,700/- Tender Fees	Can we submit DD also.			Yes
73	Generic		Hardware Requirment	Are you Ok for Make in India Products specifically for hardwre.	As per Govt gudelines on make in india.		Hardware should meet the technical specifications of RFP requirement agnostic to build & make. Hardware Support should strictly meet SLA requirements as per RFP ask.
74	3.1. Scope of Work.	11	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.	How many Onsite engineers are required and which of these like L1/L2/L3 and in how many locations. This sentence is little confusing hence asking for clarifications.			Refer Corrigendum.
75	8.10--Delivery schedule	25	Delivery of hardware, software, and license should be within 6 weeks.	Delivery timelines should be 10-12 weeks.	Due to shortage of Chip globally, Oem is taking 2 month buffer for hardware delivery.		Refer Corrigendum.
76	8.10--Delivery schedule	25	Installation & commissioning should be completed in next 10 weeks.	Installation & comissioning should be should be 12-16 weeks post hardware/software delivery.	It is SIEM, SOAR, UEBA etc which needs time and also maturity of the solutions are required.		Refer Corrigendum.
77	Section 9 - Technical Specifications; A3	38	The bidder should have support offices in Mumbai, Hyderabad and Chennai. (Also DC in India)	Pls remove this clause . Since you have asked onsite engineers then there is no point to have support offices.	Since you have already asked onsite engineers, then why support offcies are required in these locations.		No Change in RFP Terms.

78	Support Official requirement -	48	•The bidder is required to provide onsite human resource for L2 & L3 resources from the date of SIEM solutions installation.	How many resources do you require and in which all locations. Pls clarifiy in numbers			Please ref page 48 of Next Generation SIEM RFP, NPCI/RFP/2021-22/IT/17 dated 24.02.2022.
79	Support Official requirement -	48	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.	Are you asking to provide these additional resouce required at no charges(FOC).Or you will pay for the same.			For Any additional onsite personnel resources required apart from the RFP Ask, additional charges will be bourne by NPCI.
80	Additional Quarry			Should we propose SIEM for DR as well apart from HA?			Bidder to propose SIEM for NPCI DC1 & DC2 (Active-Active)
81	Additional Quarry			Should we propose a siem in DR?if yes Should we propose DR also with the same EPS?			Yes. Bidder to propose same SIEM with same size EPS (for SIEM) & FPS (For NDR Module)
82	Additional Quarry			We feel, for the scale and size of the requirement 30k to 50k EPS, for such a setup it is imperative that customer shall need automated remediation such as SOAR. Also, the intent is quite clear from the RFP, but we notice the customer has not asked for it. Another RFP process just for the soar leading to separate implementation effort, related integrations challenges and separate cost is not an efficient way to go about it.			No Change in RFP Terms.
83	Additional Quarry			Is there QCBS RFP, Will there be any commercial advantages for being technically superior			This is a standard RFP.
84	Section 3 – Scope of Work	10	Section 3.1 : Scope of Work: Point 2	Instances – 04 Nos. as active-active for two DC's	Sizing may require more than 4 instance		Bidder to factor the entire solution & all its components according to the RFP ask & should cater the technical requirement. No Change in RFP Terms.
85	Section 3 – Scope of Work	10	Section 3.1: Scope of Work	16/7*365 support mentioned	Which two shifts the resources are expected.		Shift Schedules can be managed between 7AM to 11PM.
86	Section 3 – Scope of Work	10	Section 3.1: Scope of Work	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.	Total 2 DC sites we are considering, kindly calrify more on HA requirements for both DC & DR		Each component of the solution should have Data centre Level HA. (e.g. Collectors, Loggers & ESM/correlation engine)
87	Section 3 – Scope of Work	10	Section 3.1: Scope of Work	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.	Kindly share the existing platform name, data sources list with count & correlation rules enabled by existing platform to consider migration activity		Existing platform is HP Arcsight 7.4. Data source includes 30+ odd technologies, 400 Rulesets & around 6000 assets. Around 400 Ruleset needed to be migrated from existing SIEM solution to proposed Next Gen SIEM solution.
88	Section 3 – Scope of Work	10	Section 3.1: Scope of Work	Additional Cluse	Whats the retention period for data storage		4 months online retension (Hot). 18 Months Cold Retension (NPCI's Backup solution).

89	Section 3 – Scope of Work	11	3.1 Scope of work:	▯ 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.	Request NPCI to consider the Training and Post Implementation review by OEM or OEM Authorized service partners.		NPCI follows a Maker-checker process. As implementation would be done by SI, review should be done by OEM. Training should be delivered strictly by OEM. No change in RFP terms.
90	Section 3 – Scope of Work	11	3.1 Scope of work:	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.	RFP Page No: 48 1. SIEM L2 Resources 3 Number for 16x7x365 Support 2. SIEM L3 Resource 1 (9x5 ~~x365~~) Support please confirm the number of L2 & L3 engineers required per location per Shift as 1 Onsite engineer should present in Hyderabad 16/7*365 Days.		Our expectation is to support needed to for 16 Hours per day being handled by 2 nos of L2 resources, & 9 Hours per day being Supported by 1 Nos of L3 Resource at out Hyderabad office.
91	Section 5 - Instruction to Bidders	16	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.	Request NPCI to accept the degitally signed documents using as valid "Digital signing Certificate".		Digitally signed documents are accepted
92	Section 7 - Bid Evaluation	21	7.3 Technical Scoring Matrix: Part – B Vendor Evaluation Matrix	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 Score - 25 Marks	Reqeust NPCI to Specify the Score for Each Reference with same OEM and Defferent OEM as well.		No Change in RFP Terms.
93	Section 8 - Terms and Conditions	23	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.	Request NPCI to limit the Value of PBG to 3 % of Contract value as per guidelines of Ministry of Finance, Department of Expenditure Procurement Policy Division (No. F.9/4/2020-PPD) dated 30th December 2021 which are applicable to all tenders/ contracts issued/ concluded till 31st March 2022.		No Change in RFP
94	Section 8 - Terms and Conditions	25	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	As there global chip shortage all OEM in this space have major delivery issues. Reqeust NPCI move delivery of hardware to 16 weeks without any LD and modify the project schedule accordingly. Also request npci to change this to "Delivery, installation & commissioning of the proxy solution should be completed within 30 weeks from the date of receipt of purchase order."		Refer Corrigendum.

95	Section 8 - Terms and Conditions	25	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.	Reqeust NPCI to consider the End of Sale (EOSL) period as maximum 1 year only as there will be revision and updage on products every year. Request NPCI to consider the clause as :- "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 reached ~~declared~~ **End of Support** ~~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."		No Change in RFP Terms.
96	Section 8 - Terms and Conditions	28	8.15 Penalty on non-adherence to SLAs:	8.15 Penalty on non-adherence to SLAs: as per RFP	Request NPCI to confirm the The maximum penalty due to non-adherence of SLA will not exceed 10% of the total cost of the project.		No Change in RFP Terms.
97	Section 8 - Terms and Conditions	29	8.15 Penalty on non-adherence to SLAs:	Onsite Resource SLAs: Defined Severity Levels – 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.** 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 only) for each hour of delay up to 12 hours, beyond 12 hours**	SLA Penalty is contradicting for for each Severity Level as mentioned. Please clarify.		As severity can differ from case to case basis, NPCI reserves the right to define incident severity for each incident. No Change in RFP Terms.
98	Section 8 - Terms and Conditions	30	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.	Request NPCI to consider the repeat order validity as maximum 6 months from the price discovery date.		No Change in RFP

99	Section 8 - Terms and Conditions	32	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 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.Neither Party shall be liable to the other Party for loss of profit, loss of any contract or for any indirect or consequential loss or damage which may be suffered by the other Party regarding this Tender		No Change in RFP
100	Section 9 - Technical Specifications	38	General features	The bidder should have support offices in Mumbai, Hyderabad and Chennai.(Also DC in India)	Request NPCI to consider this clause as " The bidder should have support offices in Maharashtra , Telengala & Tamilnadu."		No Change in RFP Terms.
101	Section 9 - Technical Specifications	39	Sectrion 9 : Technical Specification : B7	The SIEM platform should have capability to provide automatic Notification to SOC teams as defined in playbooks based on Conditional decision & Trigger Functions	Request NPCI to "Kindly remove the word Playbooks and clarify the requirement of Playbooks in the SIEM solution. Playbooks are ideally a part of SOAR solutions"		Refer Corrigendum.
102	Section 9 - Technical Specifications	40	Sectrion 9 :Technical Specification :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	Kindly remove the clause arbitary risk score to any field or data point.		No Change in RFP Terms.
103	Section 9 - Technical Specifications	41	Sectrion 9 :Technical Specification :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	Request to NPCI "kindly remove this clause feature is specific to a single OEM"		No Change in RFP Terms.
104	Section 9 - Technical Specifications	41	Sectrion 9 :Technical Specification :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	Request to NPCI " Kindly remove this clause as this feature is specific to a single OEM"		No Change in RFP Terms.
105	Section 9 - Technical Specifications	41	Sectrion 9 : Technical Specification :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	Kindly remove this clause as Run books are usually a part of SOAR solutions.		Refer Corrigendum.
106	Section 9 - Technical Specifications	42	Sectrion 9 : Technical Specification :C6	The solution should provide time based, criticality based, store and forward feature at each data collection point	Store and forward feature is not an NG SIEM functionality as it duplicates storage at multiple levels. Kindly remove this clase		No Change in RFP Terms.
107	Section 9 - Technical Specifications	42	Sectrion 9 :Technical Specification : 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	This clause contradicts clause C2 where it has been mentioned to use connectors. We assume that collection of logs from any log source without writing parser should be okay		Refer Corrigendum.

108	Section 9 - Technical Specifications	42	Sectrion 9 :Technical Specification :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.	Kindly clarify for Performance and capacity monitoring required in SIEM?		No Change in RFP Terms.
109	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :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 airgapped environment (absence of internet connectivity)	Not all the components can be supported through NexgenSIEM Platform		No Change in RFP Terms.
110	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :F9	Solution must support Netflow collection and correlation.	SIEM platform may lack correlation capabilites for flow data		No Change in RFP Terms.
111	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :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.	SIEM platform may lack correlation capabilites for flow data		This requirement is for NDR module in NextGen SIEM - NPCI will leverage existing Network Devices to send flow information directly wherever possible. NPCI is not having a mechanism to convert TAP/SPAN/Mirrored traffic to Flow data & send to NBAD module. Such Mechanism to be factored by the Bidder in the solution.
112	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :F13	The solution must create clearly independent and differentiated profiles from local traffic vs. traffic originating or destined for the internet.	Need clarity on expectations		Expectation is to identify traffic originated/Destined to or frome Intranet/Internet network using Next Gen SIEM's NDR capability.
113	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :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	Need clarity on expectations		This expectation is based on Behaviour based / ML based analysis to be done on Packet/flow data provided to Next gen SIEM NDR solution.
114	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :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.	Need clarity on integration efforts with SIEM , DNS logs, DHCP Logs, AD Logs etc		NPCI's all internal infrastructure logs, DNS logs, DHCP Logs, AD Log to be received by Next Gen SIEM with NDR capability for additional correlation with Packet/flow data.
115	Section 9 - Technical Specifications	45	Sectrion 9 :Technical Specification :F22	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)	Need clarity on expectations		This expectation is from Next Generation SIEM's NDR capability.
116	Section 9 - Technical Specifications	46	Sectrion 9 :Technical Specification :F24	The Solution should be intelligent and should automatically tweak itself through automated learning	Tweaking & Triage activity is manual done by analyst		No Change in RFP Terms.
117	Section 9 - Technical Specifications	46	Sectrion 9 :Technical Specification :F34	The solution should Leverage predictive security analytics to risk-score incidents.	This feature is specific to a single OEM		No Change in RFP Terms.
118	Section 9 - Technical Specifications	46	Sectrion 9 :Technical Specification :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.	Single OEM platform may not have rule engine out of box available for flow data		No Change in RFP Terms.
119	Section 9 - Technical Specifications	46	Sectrion 9 :Technical Specification :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 dataexfiltration.	Single OEM platform may not have out of box detection capabilities available for flow data		No Change in RFP Terms.

120	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :F45	The solution should provide Detection of data exfiltration based on abnormal packet size (such as exfiltration in ICMP,DNS packets)	Need to create custom machine learning models for this use case		Bidder to factor all the efforts to cover mentioned technical specifications in this RFP. No change in RFP Terms.
121	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :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)	This would need separate packet capture solution, single OEM will not able to provide		No Change in RFP Terms.
122	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :F50	The solution must be able to identify Attack & Reconnaissance Tools - Check for commonly used penetration testing tool and malware user agents	Need more clarity on expectations		Expectation - Next Gen SIEM should be able to identify traffic patterns for such attacks with its NDR capability
123	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :F54	Identifying traffic of Privacy VPN's - Personal VPN solutions which enable the user to avoid network monitoring solutions.	Need more clarity on expectations		Expectation - Next Gen SIEM should be able to identify traffic patterns for such communication with its NDR capability
124	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :F55	The proposed Solution should have inbuilt Models to detect use of various cloud storage services. (eg. Amazon S3, Dropbox etc)	whats the montoring expectation for storage Buckets		Expectation - Next Gen SIEM should be able to identify traffic patterns for such communication to various cloud storage services with its NDR capability
125	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :F57	The proposed solution should be able to identify TCP/UDP malformed packets, TCP/IP stack fingerprinting methodologies e.g. Christmas Tree packet.	Functionality may not be available with Single OEM		No Change in RFP Terms.
126	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :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	Functionality is not available with Single OEM		No Change in RFP Terms.
127	Section 9 - Technical Specifications	47	Sectrion 9 :Technical Specification :F62	The solution must be able to identify Address Scan - Scanning for single/multiple devices listening on a specific port	Solution can Integrate with Scanners to share results		Expectation - Next Gen SIEM should be able to identify traffic patterns for such communication with its NDR capability within the network with Packet capture/flow data ingested to it.
128	Section 9 - Technical Specifications	48	Sectrion 9 :Technical Specification :F63	The solution must be able to identify Port Scan - Scanning single/multiple devices to see which ports are open on it.	Solution can Integrate with Scanners to share results		Expectation - Next Gen SIEM should be able to identify traffic patterns for such communication with its NDR capability within the network with Packet capture/flow data ingested to it.
129	Section 9 - Technical Specifications	48	Sectrion 9 :Technical Specification :F69	The solution should detect and alert on anomalies in DNS communications so as to pre-emptively help detect security risks.	Functionality is not available with Single OEM		No Change in RFP Terms.
130	Section 9 - Technical Specifications	48	Sectrion 9 :Technical Specification :F70	The solution shall be able to identify crypto compliance for endpoints (TLS, SSL versions)	Functionality is not available with Single OEM		No Change in RFP Terms.
131	Section 9 - Technical Specifications	48	Sectrion 9 :Technical Specification :F71	The solution must do Identification of Malicious behaviour in encrypted traffic without decryption	Functionality is not available with Single OEM		Encrypted Traffic Analysis is a method of malware detection and cryptographic assessment of secured network sessions, which does not rely on decryption. No Change in RFP Terms.
132	Section 10 - Documents forms to be put in Folder A	65	Annexure H :Eligibility Criteria: Point 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 OEM's product.	Can we dilute this clause as threat intelligence with specs shared in RFP can only be achieved with Threat Intel Platform which can be easily integrated with SIEM solution		No Change in RFP Terms.
133	Section 11 - Documents to be put in Folder 'B'	74	Sectrion 11 :Technical Specification :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	Functionality is not available with Single OEM		No Change in RFP Terms.
134	Section 11 - Documents to be put in Folder 'B'	74	Sectrion 11 :Technical Specification :F07	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).	Functionality is not available with Single OEM		No Change in RFP Terms.

135	Section 11 - Documents to be put in Folder 'B'	74	Sectrion 11 :Technical Specification :F18	The Proposed Solution must be able to scale up and down based on changes in scope	Tricky point in terms of NDR, solution may not be auto scalable need to define it prior before adding anything in scope		Bidder to factor solution as per RFP ask. No changes in RFP Terms.
136	Section 11 - Documents to be put in Folder 'B'	75	Sectrion 11 :Technical Specification :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).	Functionality is not available with Single OEM		No Change in RFP Terms.
137	Section 9 - Technical Specifications	38	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).	Need to rephrase as - The Solution quoted by the bidder should be in Gartner Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).	Referring Gartner MQ itself narrow down vendors for evaluation and give broader coverage to SIEM vendors for participation in RFP.	No Change in RFP Terms.
138	Section 9 - Technical Specifications	41	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	Need to rephrase as - The solution must be able to support the following indicators: 1. Network,IP - Domain - File Hash - Email	IOC are not limited to given indicators only and vary from intelligence feed available with TI communities. For the broader participation, listed indicators (1. Network,IP, Domain, File Hash, Email) are good to consider and standard for all solution vendors to comply.	No Change in RFP Terms.
139	Section 9 - Technical Specifications	38	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).	Need to rephrase as - The Solution quoted by the bidder should be in Gartner Magic Quadrant for SIEM solution, consecutively for last Two years (Two of last 3 years).	Referring Gartner MQ itself narrow down vendors for evaluation and give broader coverage to SIEM vendors for participation in RFP.	No Change in RFP Terms.
140	Section 9 - Technical Specifications	41	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	Need to rephrase as - The solution must be able to support the following indicators: 1. Network,IP - Domain - File Hash - Email	IOC are not limited to given indicators only and vary from intelligence feed available with TI communities. For the broader participation, listed indicators (1. Network,IP, Domain, File Hash, Email) are good to consider and standard for all solution vendors to comply.	No Change in RFP Terms.
141	RFP	10	3.1 Scope of work	Instances – 04 Nos. as active-active for two DC's.	Does NPCI want to go for dedicated instances or is Cloud SOC platform okay to be proposed?		Our expectation is to have On-premise solution. No Change in RFP terms.
142	RFP	10	3.1 Scope of work	Bidder should support the migration of the Current SIEM Correlation Rulesets, policies, operations, Integrations and features	How many rulesets, policies, use cases are currently configured which need to be migrated?		Existing platform is HP Arcsight 7.4. Data source includes 30+ odd technologies, 400 Rulesets & around 6000 assets. Around 400 Ruleset needed to be migrated from existing SIEM solution to proposed Next Gen SIEM solution.

143	RFP	10	3.1 Scope of work	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.	If the proposed solution is software based, will NPCI provide the required hardware? If yes, NPCI will have to manage the hardware upto OS layer. Please confirm		Entire Solution to be factored by the Bidder.
144	RFP	38	Section 9 - Technical Specifications	The solution must have an automated backup and recovery process.	NPCI will provide storage for backup. Please confirm		4 months online retension (Hot). 18 Months Cold Retension (NPCI's Backup solution).
145	RFP	38	Section 9 - Technical Specifications	The solution must automate internal health checks and notify the user in case of problems.	NPCI will provide the health monitoring tool. Please confirm		Understanding should be as - Solution itself should be able to cover internal health checks & notify user in case of problems. External health Checks would be performed by Monitoring tool facilitated by NPCI.
146	RFP	39	Section 9 - Technical Specifications	Solution should able to integrate with any 3rd party / Open source SIEM.	Kindly elaborate this statement. Next Gen SIEM cannot integrate with another SIEM platform		Expectation - Proposed solution should be able to integrate with 3rd Party/Open source OEM platforms. Should be able to share Logs/alerts etc via API or any other possible way of communication.
147	RFP	49	General Guidelines:	NPCI. l. NPCI should be provided with a dedicated and exclusive team.	If bidder proposes 16x7x365 dedicated resource (L2/L3) as per RFP and 24x7x365 shared support team, will that be okay. Please confirm.		No Change in RFP Terms.
148	RFP		General		IS there any migration to be done from the existing platform? Use cases, tickets etc?		Yes.
149	RFP		General		What is the current ITSM used? The proposed SOC platform will be integrated with this ITSM. Please confirm		NPCI is using ITSM tool of BMC
150	RFP	31	8.21 Confidentiality		The clause should be made mutually applicable. The provisions of confidentiality should be made applicable to NPCI as well as the rates and other sensitive information should be preserved.		No Change in RFP Terms.
151	RFP	31	8.22 Indemnity		The clause should be made mutually applicable. Edits in the clause as follows: ~~The bidder~~ Each Party shall indemnify, protect and save ~~NPCI~~ the other and hold ~~NPCI~~ the other harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating toor resulting from any act or omission or negligence or misconduct of the ~~bidder~~ other party and its employees and representatives, ~~breach of the terms and conditions of the agreement or purchase order~~, false statement by the ~~bidder~~ other party, employment claims of employees of the ~~bidder~~ other party, ~~third party claims arising due to infringement of intellectual property rights~~, death or personal injury attributable to acts or omission of ~~bidder~~ other party, 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 Suggested change: Indemnity to be limited to twelve(12) months of amount paid by NPCIL to Bidder under the Purchase Order		No Change in RFP Terms.
152	RFP	31	8.23 Bidder's Liability		Limit of Liability for Deliverables suggested to be twelve(12) months of amount paid by NPCIL to Bidder under the Purchase Order		No Change in RFP Terms.

153	RFP	34	8.30 Force Majeure		Please include Pandemic and add the following in the last para: Except for Bidder's payment obligations accruing under this Purchase Order up to the date of a bona fide Force Majeure event, Neither party shall have any liability to the other in respect of the termination of this Purchase Order as a result of an event of Force Majeure.		No Change in RFP Terms.
154	RFP	35	8.32 Compliance with Applicable Laws of India		Suggest deletion of the red part below, as Indemnification is agreed in 8.18 earlier: 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~~		No Change in RFP
155	RFP	36	8.34 Intellectual Property Rights:		Clause suggested to be made mutually applicable. "NPCIL may have the right to IPR which is developed by Bidder subject to the payment by NPCI for such development and in furtherance of the Contract pursuant to this RFP"		No Change in RFP
156	RFP	36	8.39 Fraudulent and Corrupt Practice	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.	Clause revised as follows: NPCI will reject a proposal for award if it ~~determines~~ is proven beyond doubt that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing the project.		No Change in RFP
157	RFP	10	3.1 Scope of work	Security incident management	As part of TCL's standard service is to do security incident monitoring and reporting. Please confirm whether incident response and remediation is also there in this deal		Entire Solution to be factored by the Bidder according to the RFP ask.
158	RFP	10	3.1 Scope of work	Security incident management	Please share us the past 3 months SIEM ticket counts like IR, CR and SR and how many use cases are deployed on Arcsight?		Not applicable.
159	RFP	10	3.1 Scope of work	SLA	TCL provides response and update SLAs for security incident but not resolution SLA		No Change in RFP Terms.
160	RFP	10	3.1 Scope of work	Security incident management	Are forensic and threat hunting services required?		Not applicable.

161	RFP	10	3.1 Scope of work	To configure Next Generation Security information and event management (SIEM) solution at Primary DC and Disaster Recovery site.	Should the bidder propose SIEM for DR as well, apart from HA? Or only the collectors who will collect the data and send it to the primary data center siem?		Our Data Centres are Active-Active. Bidder should propose SIEM for Both DC & DR. Logs will be collected locally at each DC. Copy of logs will be sent across DC's for Log Availability & Replication. The EPS support should be same for both DC & DR
162	RFP	10	3.1 Scope of work	To configure Next Generation Security information and event management (SIEM) solution at Primary DC and Disaster Recovery site.	Should thebidder propose a siem in DR? if yes, Should we propose DR also with the same EPS?		Our Data Centres are Active-Active. Bidder should propose SIEM for Both DC & DR. Logs will be collected locally at each DC. Copy of logs will be sent across DC's for Log Availability & Replication. The EPS support should be same for both DC & DR
163	RFP	11	3.1 Scope of work	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.	Does NPCI expect bidder to provide resources to perform 24*7*365 Security Event moniting on the Security Events?		Please ref page 48, 49 & 50 of Next Generation SIEM RFP, NPCI/RFP/2021-22/IT/17 dated 24.02.2022.
164	RFP	11	3.1 Scope of work	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.	The onsite resources are expected to Monitor, Manage and Maintain only the SIEM platform, Platform Uptime and its configurations. Kindly confirm		Please ref page 48, 49 & 50 of Next Generation SIEM RFP, NPCI/RFP/2021-22/IT/17 dated 24.02.2022.
165	RFP		General		Does NPCI has availability monitoring solution in place and integrated with NPCI's ticketing system?		Yes
166	RFP	25	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.	1. We understand all NPCI IT Assets and Apps are actively sending logs to the existing SIEM with connectivity and firewall rules set. Kindly Confirm? 2. Kindly share the percentage of Assets and Apps integrated with the existing SIEM solution. 3. We understand all configurational level changes on the IT assets and Apps would be done by NPCI team. Kindly Confirm?		Refer Corrigendum.
167	RFP	13	4.1 - Eligibility Criteria B] - Other than start-ups; Other than MSMEs Clause 2 - Turnover & profitability	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).	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 2 of 3 financial years** (FY 2018-19, 2019-20, 2020-21).		Kindly refer Corrigendum 1
168	RFP		Miscellaneous		Kindly clarify if remote access to the SIEM platform in DC and DR will be extended to bidders operation team for monitoring and management		As Bidders operations team will be located at Hyderabad DC, Necessary access to SIEM platform will be extended on-premise
169	RFP		Miscellaneous		In case remote access to SIEM platform is allowed , Bidder will recommend the Internet bandwith required for establishing the connecvitivity towards NPCI DC and DR , NPCI to factor and make provision for bandwidth and associated infrastructure at DC/DR		Acknowledged
170	RFP	26	8.15 Service Level Requirements (SLA)	All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.	Kindly elaborate on the support required for Office/Branches.		Support is required for Next-Gen SIEM solution including all its components.
171	RFP	38	A.10 (General Features)	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	Any Connectivity between DC and DR for required replication to be provided by NPCI. PLease confirm.		Connectivity Required for Replication will be Provided by NPCI. No change in RFP Terms.
172	RFP		General		Please provide Current SIEM Correlation Rulesets, policies, operations, Integrations and features informaiton		Existing platform is HP Arcsight 7.4. Data source includes 30+ odd technologies, 400 Rulesets & around 6000 assets. Around 400 Ruleset needed to be migrated from existing SIEM solution to proposed Next Gen SIEM solution.

173	RFP		General		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		No Change in RFP Terms.
174	RFP		General		SLA based on Severity 1,2, 3, assumed related to platofrm avaibality and not log based alerting		No Change in RFP Terms.
175	RFP	25	8.11 Penalty for default in delivery	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	Both these points are contradicting. Second points needs to be deleted as cap of 5% i.e. additional 10 weeks beyond stipulated period is provided, then penalising for delay beyond 10 days will be covered in point 1. Post those additional 10 weeks customer may think to cancel the contract		No Change in RFP Terms.
176	RFP	25	8.11 Penalty for default in delivery	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.	Request to NPCI to kindly cap the penalty to 0.5% of the value of undelivered cost of the project.		No Change in RFP Terms.
177	RFP	30	8.19 Payment Terms:	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.	Request AMC to be paid quarterly in advance		No Change in RFP Terms.
178	RFP	80	Annexure N - Commercial Bid	Line Item Wise Prices	What is expected in this table? Request NPCI to get the breakup of the commercial bid from successful bidder		Detailed Breakup of Solution /No Change in RFP
179	RFP	34	14.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.	Request NPCI to pay successful bidder 100% of the unexpired value of the contract in case of termination for convenience		No Change in RFP
180	RFP				Kindly extend the last date and time of submission of bid by atleast 2 weeks		Acknowledged
181	RFP	25	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	Owing to global semiconductor crisis, delivery schedule of all OEMs has been collasped. OEMs are not committing any confirm delivery timelines and hence request you to atleast make it minimum 30 weeks from the date of PO		Refer Corrigendum.
182	RFP	28	8.15 Service Level Requirements (SLA)	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	Request NPCI to cap the SLA penalty to 5% of the Total Annual recurring cost		No Change in RFP Terms.
183	RFP		General		Kindly confirm the overall capping on the Penalty in case of non adherance of SLAs		Refer Page 26,27,28,29,30 of Next-Gen SIEM RFP NPCI/RFP/2021-22/IT/17 dated 24.02.2022 on NPCI's official Website.

184	RFP		General		Please provdie informaiton on Backup requirement, exisitng solution if any, Data retention, Online, offline. Offsite		4 months online retension (Hot). 18 Months Cold Retension (NPCI's Backup solution).
185	RFP		General		Please confirm if NPCI is using backup management for SIEM solution.		Yes, NPCI is using backup management solution.
186	RFP		General		Please confirm the number of log sources currently integrated with the existing solution?		Existing platform is HP Arcsight 7.4. Data source includes 30+ odd technologies, 400 Rulesets & around 6000 assets. Around 400 Ruleset needed to be migrated from existing SIEM solution to proposed Next Gen SIEM solution.
187	RFP		General		Cloud log sources integration is also in scope? Please confirm the number of cloud assets and vendors in scope for the integration?		Yes. We have SAAS Products, AWS, Azure & GCP. Bidder to factor efforts required as per RFP Ask.
188	RFP		General		Is there any direct connectivity between the NCPI other location and cloud infrastructure to forward the logs to DC & DR?		Connectivity Required for to forward logs across DC, DR & Cloud, Replication will be Provided by NPCI. No change in RFP Terms.
189	RFP		General		Do you want collectors to be hosted in DC & DR only or any regional branch locations and cloud?		Collectors to be hosted in DC & DR.
190	RFP		General		Any existing Threat inteligence customer platform that needs to be integrated with the proposed SIEM?		Yes
191	RFP		General		Is there any threat hunting resource requirement? -		Yes
192	RFP		General		Who will be responsible for the log forwarding on the respective log sources?		Integration of the device will be with Bidder & Respective support team in NPCI will support to implement log forwarding on the respective log sources. end-to-end ownership of operations, maintainence & compliance for SIEM will be with Bidder.
193	RFP		General		Dual forwarding of the logs will be done till the new platform is live?		Bidder shall consider this usecase.
194	RFP		General		IS there any compliance modules in scope?		ISO 27001, PCI-DSS
195	RFP		General		Current log retention and archival policy and expected from the proposed platform?		4 months online retension (Hot). 18 Months Cold Retension (NPCI's Backup solution).
196	RFP	82	Annexure Z		Bidder recommendes to make the NDA mutual.		No Change in RFP
197	RFP	83	Annexure Z- Clause 6		we can agree to injunctive relief however the cost implication to be deleted. We can suggest the below:- REMEDIES. The Parties acknowledge that money damages would not be a sufficient remedy for any breach of this Agreement by a Party and that a Party will be entitled to seek injunctive relief and specific performance as remedies. Such remedies will be in addition to any other remedies available		No Change in RFP
198	RFP	84	Annexure Z- Clause 11		Both parties need to agree to a definite term. Bidder can agree to a term not exceeding 7 years		No Change in RFP
199	RFP	84	Annexure Z- Clause 12/13		Article 12 and 13 may be deleted. IP related can be built in the main agreement and not as part of NDA. Indemnity clause to be deleted		No Change in RFP

200	RFP	85	Annexure Z- Clause 14.3		14(3) to be replaced with ENTIRE AGREEMENT. This Agreement represents the entire agreement between the Parties and supersedes and cancels all previous negotiations, agreements or commitments (whether written or oral) with respect to the subject matter hereof. This Agreement shall not be amended or modified in any manner, except by an instrument in writing signed by a duly authorized representative of each of the Parties hereto. This Agreement may be executed in as many counterparts as may be required, each of which when delivered is an original but all of which taken together constitute one and the same instrument		No Change in RFP
201	RFP		General		Please provide the current SOAR platform details that NPCI is currently using.		HP Arcsight 7.4
202	RFP		General		If SOAR is already available, is NPCI going to continue with the same.		Yes.
203	RFP		General		The Bidder recommends that native SOAR is provided as part of this RFP scope.		No Change in RFP Terms.
204	RFP		General		Is Big Data Security, Data Lake part of the Deliverable against this RFP?		No.
205	RFP		General		Will independent SOAR management be with SIEM platform management? Please confirm.		No Change in RFP Terms.
206	Section 9 - Technical Specifications - General Features	38	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)	We understand that the expectation from load balancing is to have the capability to forward logs collected at one site to the other site for storage purposes. i.e Data collected at DC to be forwarded to DR site also, please confirm if our understanding is inline with your expectation.		Understanding meets the expectations. No change in RFP Terms.
207	Section 9 - Technical Specifications - General Features	38	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)	We understand the expecation from the following clause is to have Both console active and working at all times & the data collected at respective sites should also be forwarded to other site for storage perspective. Please suggest if the data forward from DC to DR also need to be correlated at DR site. This would require double the capcity at correlation layer i.e 60K each at both sites.		Our Understanding is Servers at DC1 will forward logs to SIEM solution at DC1, Servers at DC2 will forward logs to SIEM solution at DC2, a copy of all logs from DC1 SIEM solution should be available at DC2 SIEM Solution & vice-versa. No change in RFP Terms.
208	Section 9 - Technical Specifications - General Features	38	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.	Please elaborate on the network connectivity between both DC & DR and the network latency on this network.		Devices at each Datacentre will be forwarding logs to local collector/broker, a copy of Collector/broker logs will be forwarded to Correlation engines of both DC1 & DC2 (DC & DR). We should have Log retension at both Data Cantre to achieve Compliance. We have dedicated Link for replication, Latency is within the limits. No change in RFP Terms.
209	Section 9 - Technical Specifications - General Features	38	A11	The solution must have an automated backup and recovery process.	Our understanding is that Bakup is expected to be automated while the recovery process shall be performed manually on need basis , please confirm if our understanding is inline with your expectation.		NPCI will provide Backup infrastructure. Backup script & path, process should be facilitated by the proposed solution or bidder.

210	Section 9 - Technical Specifications - SIEM Platform Specifications	38	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	1. Industry standard for spike/ sudden burst is around 10-15%, genrally an increase by 100% in the EPS is not observed moverover any peak beyond 30 second is considered as sustained EPS. It is thus requested to re-phrase the same as : The proposed solution should be sized for 30,000 sustained EPS at correlation layer per Data centre but should be able to handle sudden spike/burst by additonal 10% of sustained EPS capacity at collection layer. Also, please clarify if the expectation is to have logs collected at each site to be forwarded to other needs to be correlated or just stored. As correlation of logs from both sites will result in 60K EPS each at both sites.		Understanding partially meets the expectations. In case of Failure of SIEM solution at site A, Site B should be able to handle EPS mentioned as per RFP ask. Bidder should factor requirements as per the RFP Ask. No Change in RFP Terms.
211	Section 9 - Technical Specifications - SIEM Platform Specifications	39	B3	Proposed SIEM solution should act as common data lake for Correlation, SOAR,NDR,UEBA and threat hunting.	From this point we understand the expectation is to have a platform which collect data from solution such as SOAR , NDR , UBA and other solution while providing a single platform to perform correlation , investigation		Understanding meets the expectations. No change in RFP Terms.
212	Section 9 - Technical Specifications - SIEM Platform Specifications	39	B7	The SIEM platform should have capability to provide automatic Notification to SOC teams as defined in playbooks based on Conditional decision & Trigger Functions.	Playbook are functionality offered by SOAR platforms , we understand the expectation is to have ability to configure who should be alerted for a particular offense. For example a phishing offense should be alerted to Mail Admin / Security Team. please confirm if our understanding is inline with your expectation. It is thus requested to re-phrase the same as The SIEM platform should have capability to provide automatic Notification to SOC teams.		Refer Corrigendum.
213	Section 9 - Technical Specifications - SIEM Platform Specifications	40	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.	Please elaborate on what falls under the unstructured Data .		Unstructured logs are massive text files made up of strings, which are ordered sequences of characters that are meant to be read by humans.
214	Section 9 - Technical Specifications - SIEM Platform Specifications	40	B20	Risk scoring framework to apply risk scores to any asset or user based on relative importance or value to the business	We understand the expectation is to have capability to manually/Automatically allocate risk score/weight to users & assests. Please confirm if our understanding is inline with your expectation.		Understanding meets the expectations. No change in RFP Terms.
215	Section 9 - Technical Specifications - SIEM Platform Specifications	40	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.	We understand the expectation isto assgin weight to data point such as assests , users etc. Please confirm if the understanding is in line to the expectation.		Understanding meets the expectations. No change in RFP Terms.
216	Section 9 - Technical Specifications - SIEM Platform Specifications	41	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	We understand the expectation is to add log sources on the go and being able to correlate the data collected. The data shall also be avialable for graphical representation. Please confirm if the understanding is inline with the expectation		Understanding is in-line with expectations.
217	Section 9 - Technical Specifications - SIEM Platform Specifications	41	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.	The following functionality is a SOAR Feature it is thus requested to remove the same.		Refer Corrigendum.

218	Section 9 - Technical Specifications - SIEM Platform Specifications	42	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.	Please clarify the enviornment in consideration ? Are we looking at the visibility in terms of the deployment of the SIEM and its components.		Understanding is to identify & alert Performance, capacity bottlenecks, service interruptions/deteriorations etc. No change in RFP Terms.
219	Section 9 - Technical Specifications - SIEM Platform Specifications	42	B46	The proposed solutions machine learning capabilities must allow adidition of custom machine learning algorithms from popular open source Python libraries.	The SIEM platfrom are desgined considering high performance looking at the speed and volume at which the data is ingested. Addin custom ML algorithm on the fly will result in higher utilization and slowness in the platform. It is thus requested to keep customization of ML algorithm on seperate platform and remove the following clause from the specification.		No Change in RFP Terms.
220	Section 9 - Technical Specifications - Log Analysis	42	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.	The Platform support ingestion of logs in near real time, ingestion to parsing depends on multiple factors and thus it is not possible to confirm on a finite duration of tie required for the same. It is thus requested to re-phrase the same as: 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 in near real time from the actual log event at the integrated device.		No Change in RFP Terms.
221	Section 9 - Technical Specifications - Log Analysis	42	C4	All log data to be authenticated (time-stamped across multiple time zone) encrypted and compressed before transmission to manager console.	Encryption of log data require additional time in processing the data at time of storage and retrival. Since commanly SIEM platform uses their proprietary database it difficult for any outsider of thirs party to gain access of data through unauthrozed means. The platforms use hashing to ensure the integrity check , it is thus request to re-phrase the same as : All log data to be authenticated (time-stamped across multiple time zone) compressed before transmission to manager console. The solution should also have the provison of hashing to ensure integrity of collected data.		Refer Corrigendum.
222	Section 9 - Technical Specifications - Management Center and administration - Threat Intelligence	43	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	We undertand the expectation is to ingest intelligence from multiple threat intelligence feed. Additionally the same can be used in various rules to help organization gain visibility into threat overall security posture. Please confirm if our understanding is inline with you expectation.		Understanding is in-line with expectations.
223	Section 9 - Technical Specifications - Management Center and administration - Network Detection and response (NDR)	44	F2	The Proposed solution must be PCI-DSS or ISO 27001 Compliant	Is the expectation here to have compliance Reports aroud the PCI & ISO or the solution is expected to be PCI or ISO compliant		The solution is expected to be PCI or ISO compliant. No Change in RFP Terms.

224	Section 9 - Technical Specifications - Management Center and administration - Network Detection and response (NDR)	44	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)	Please share the segmented view of the 30 GB infrastructure for each DC's A. Please provide segregation of how much of this traffic will be over Netflow , jflow or Sflow & how much needs to be tapped/Mirrored/Spanned. B. Is the flow data collected need to be stored on the local site or a copy is required on the secondary site also for correlation activities.		For each Data Centre (DC1 & DC2) - A. Netflow , jflow & Sflow will account to 10% of Data (out of 30Gbps / 30,000FPS). Rest of the data will be captured using Tap/Mirror/Span. Bidder shall consider 4 Physically Distinct Network segments within each Data Centre to collect the Flows/Span/tap/mirror data. B. Retension period for flow data is as per RFP Ask. C.Network interfaces for FLow/SPAN/TAP collection to be considered - Min. 4x1G Copper Ports, 4x1G Fiber Ports, 4x10G Fiber Ports (Bidder to factor Transreceivers/SFP's) D. No Packet Brokers / No Network TAP's currently in Use. E.Network switches are of Cisco & Juniper & can be used for SPAN wherever necessary.
225	Section 9 - Technical Specifications - Management Center and administration - Network Detection and response (NDR)	46	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).	We understand the the expectation here is to have total amount of data transferred by a certain application during communication. Please explain if our understanding is inline with your expectation.		Understanding should be to display tcp traffic profiles based on TCP flags, eg. TCP Syn Packets, TCP Resets, Chrismas tree packets etc. No change in RFP Terms.
226	Section 9 - Technical Specifications - Management Center and administration - Network Detection and response (NDR)	46	F34	The solution should Leverage predictive security analytics to risk-score incidents.	We understand the expectation from the following clause is to understand the importance of a particular incident/offense in a particular enviornment by means of metric that is comparable and calculated using algorith to understand the risk rating. Please confirm if our understsanding meeting your expectation. It is thus requested to re-phrase the same as : The solution should Leverage Algorithm to asses to risk-score/ratings for incidents.		Understanding meets the expectations. No change in RFP Terms.
227	Section 9 - Technical Specifications - Management Center and administration - Network Detection and response (NDR)	47	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)	Collection of PCAP required specific network appliance , please confirm if the scope of RFP require's to capture the packets (header + payload) in the enviornment. IF yes , please share 1. Total Throughput of the network required to be captured 2. Utilization of the required network 3. Duration for which the raw packet need to be captured.		Scope of RFP expected is to have a Next generation SIEM solution with built-in features of NDR (Network Detection & Response) capabilities. Refer Points F4 on Page no 44, F20 on Page no 45 of Next Generation SIEM RFP NPCI/RFP/2021-22/IT/17 dated 24.02.2022
228	Section 9 - Technical Specifications - Management Center and administration - Network Detection and response (NDR)	47	F52	The solution must be able to identify BitCoin Activity - Any communications using the BitCoin mining protocol	Please elaborate on protocols in reference.		Our Requirement to be understood as to identify any Bitcoin/ Crypto currency websites/ Any Bitcoin mining related communication to be identified by NDR module in SIEM. No Change in RFP Terms.
229							
230					The RFP scope ask for Instances – 04 Nos. as active-active for two DC's., please confirm if the expectation is to have 2 Active setup with HA or we are looking at two set of active passive setup ? i.e Active Setup at DC and its backup in DR another active setup in DR and its backup in DC.		Understanding should be - Active-Active Setup in DC, Active-Active Setup in DR.
231					In terms of High Availability do we need to factor HA for each and every components.		Yes. HA components needed to be factored accordingly. No change in RFP Terms.
232					Please share log retention duration for the setup A. Online & offline log retention for Events & Flows		4 months online retension (Hot). 18 Months Cold Retension (NPCI's Backup solution).

233					Our understanding for sizing from the RFP A. EPS required at each site is sustained 30,000 with capability to store the logs forward from other site for search purpose only. B. 30,000 FPS from a 30 GB network need to be collected for each data center and unlike events the flows will remain in the local datacenter only.		Understanding should be - A. EPS required at each site is sustained 30,000 with capability to store & co-relate also the logs forward from other site for search & co-relate in case of failure at one site. Understanding is correct - B. 30,000 FPS from a 30 GB network need to be collected for each data center and unlike events the flows will remain in the local datacenter only.
234					Please share distribution of flow data that will be forwarded by Netflow , jflow & Sflow and the flows that will be captured using tapping/mirroring/spanning. Also elaborate on the network segment which support capturing and which can only forward flows.		For each Data Centre (DC1 & DC2) - A. Netflow , jflow & Sflow will account to 10% of Data (out of 30Gbps / 30,000FPS). Rest of the data will be captured using Tap/Mirror/Span. Bidder shall consider 4 Physically Distinct Network segments within each Data Centre to collect the Flows/Span/tap/mirror data. B. Retension period for flow data is as per RFP Ask. C.Network interfaces for FLow/SPAN/TAP collection to be considered - Min. 4x1G Copper Ports, 4x1G Fiber Ports, 4x10G Fiber Ports (Bidder to factor Transreceivers/SFP's) D. No Packet Brokers / No Network TAP's currently in Use. E.Network switches are of Cisco & Juniper & can be used for SPAN wherever necessary.
235					Also please share the total count of server that shall be integrated to the SIEM platform Directly or indirectly.		Existing platform is HP Arcsight 7.4. Data source includes 30+ odd technologies, 400 Rulesets & around 6000 assets. Around 400 Ruleset needed to be migrated from existing SIEM solution to proposed Next Gen SIEM solution.
236	RFP-for-procurement-of-SIEM-Solution	10	Section 3 – Scope of Work 3.1 Scope of work:	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.	Bidder will create new policies based on existing usecase/correlation rule/policies configured. Migration of Current SIEM Correlation Rulesets, policies, operations, is only supported in case of same OEM. Kindly confirm and more details on the understanding.		Bidder should create & implement new rules/policies based on MITRE att&ck framework on the newly deployed solution along with Existing rules. Content Development. Refer Corrigendum
237	RFP-for-procurement-of-SIEM-Solution	21	7.3 Technical Scoring Matrix:	Part – B Vendor Evaluation Matrix Customer BFSI reference in India Please provide at least 3 India References	Request NPCI to consider following clause Part – B Vendor Evaluation Matrix Customer BFSI/PSU/Government/Enterprise reference in India		No Change in RFP Terms.
238	RFP-for-procurement-of-SIEM-Solution	25	8.10 Delivery schedule	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	As Hardware delivery are delayed from OEM , we request NPCI to increase delivery time to 20 weeks. 8.10 Delivery schedule Delivery, installation & commissioning of the Next Generation Security information and event management (SIEM) solution should be completed within 22 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 12 weeks. • Installation & commissioning should be completed in next 10 weeks. • Installation Certificate for each installation should be signed by NPCI and the bidder		Refer Corrigendum.