Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
1	Page No: 09	**1.7 Qualification Criteria**	F. The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer	Please Rephase this: F. The bidder/OEM should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.		The bidder should have executed similar/relevant works related to DC Network/Network-Security architecture planning/designing for cumulative 6 Crore INR during last 3 years & **atleast 1 project of SIEM & SOAR implementation in DC distributed environment should be present in previous similar work experience.** Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.
2	Page No: 09	**1.7 Qualification Criteria:**	The Bidder should be a CMMI Level - 3 or CMMI Level - 5 company. An undertaking to be submitted in this regard.	The Bidder/OEM should be a CMMI Level - 3 or CMMI Level - 5 company. An undertaking to be submitted in this regard. Request you to kindly add ISO 27001 :2014 which will have some relevant since it is a security Bid	CMMI is more relevant to Software engineering/devel opment, while bidder's role is to supply and implement the solution, hence, request you to kindly amend the clause for larger participation and fair competition.	No Change.Tender Clause remain same.
3	Page No: 09	**1.7 Qualification Criteria:**	The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNOD/ TPSODL /TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.	The bidder should have executed the Cyber Security Project for cumulative 6 Crore INR during last 5 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL /TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.	Request you to kindly amend the clause for larger participation and fair competition.	The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years & **similar work experience should atleast 1 project of SIEM & SOAR**. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.
4	Page No: 08	**1.7 Qualification Criteria:**	B. The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report of 2021 for last three years. The Bidder should furnish documentary evidence regarding this.	The proposed SIEM/SOAR vendor must be in magic quadrant of Gartner SIEM report for last three years. The Bidder should furnish documentary evidence regarding this.	This seems to be a printing mistake as it is a SIEMSOAR tender not Firewall. So in the interest of larger participation and healthy competition, we request to kindly amend the clause as per recommendation:	The proposed SIEM/SOAR vendor must be in magic quadrant of Gartner SIEM report for last three years. The Bidder should furnish documentary evidence regarding this.
5	Page No: 08-09	**1.7 Qualification Criteria:**	C. The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM personnel only. All the compliances should be submitted in the Bidder's letter head.	C. The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM authorized partner under the supervision of OEM. All the compliances should be submitted in the Bidder's letter head.	This clause asks that installation shall be carried out by OEM personnel only. We would like to bring this to notice of Tata Power that OEM Professional Services are very costly and can disbalance the overall budget of the RFP, so it would be better if instead of OEM, installation is carried out by OEM authorized partner under the guidance of OEM (same is asked in RFP techincal specification as well - refer point 74). And morevoer SIEM SOAR is not a niche technology anymore, so mostly all the SI/Bidders have the capabilities to install this. In this regard, we request to amend the clause as	Tha clause stands as follows- 1. The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. 2. The bidder must have at least 1 or more of the same OEM certified engineers. 3. Installation will be carried out by OEM certified resources & HLD/LLD should be validated by OEM as per standards and best practices. OEM need to provide confirmation against the same on their Letter head. 4.All the Technical Compliances & Unpriced BoQ needs to be submitted in the OEM's letter head only by the Bidder.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
6		**Scope of Work & Service Level Agreement**	3. Scope of Work j) OEM Team/Engineer should do the implementation services at site (TPSODL/TPCODL/TPWODL/TPNODL)	j) OEM / OEM authorized partner should do the implementation services at site (TPSODL/TPCODL/TPWODL/ TPNODL)	This clause asks that installation shall be carried out by OEM personnel only. We would like to bring this to notice of Tata Power that OEM Professional Services are very costly and can disbalance the overall budget of the RFP, so it would be better if instead of OEM, installation is carried out by OEM authorized partner under the guidance of OEM (same is asked in RFP techincal specification as well - refer point 74). And morevoer SIEM SOAR is not a niche technology anymore, so mostly all the SI/Bidders have the capabilities to install this. In this regard, we request to amend the clause as	Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
7	8 of 48	**Qualification**	B. The proposed firewall vendor must be in Leader's quadrant of Gartner Enterprise Firewall report of 2021 for last three years. The Bidder should furnish documentary evidence regarding this.	The proposed SIEM/SOAR vendor must be in Magic Quadrant of Gartner SIEM report for last three years. The Bidder should furnish documentary evidence regarding this.		This clause is deleted
8	8-9 of 48	**Qualification**	C. The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM personnel only. All the compliances should be submitted in the Bidder's letter head.	C. The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM authorized partner under the supervision of OEM. All the compliances should be submitted in the Bidder letter head alongwith OEM Confirmation on Letter Head Confirming the Complainces.		Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
9	9 of 48	**Qualification**	F. The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.	We understand that by similar works, Tata Power means atleast 1 SIEM and SOAR order copy, out of Total Cumulative 6 Cr INR Similar Works . Kindly confirm to avoid any confusion. It is to be Requested to have Bidders who has atleast One SIEM SOAR Order Copy. This will give more Autheticity of the Bidder on similar Works.		The bidder should have executed similar/relevant works related to DC Network/Network-Security architecture planning/designing for cumulative 6 Crore INR during last 3 years & **atleast 1 project of SIEM & SOAR implementation in DC distributed environment should be present in previous similar work experience.** Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.
10	16 of 48	**Payment Terms**	On delivery of the software complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. The payment a payment of 60% of the Invoice basic value along with 100% tax as applicable, shall be made within 90 days of the submission of the invoices along with all the requisite documents However, for MSME Bidders, the payment shall be released within 45 days of the submission of the bills/invoice.	Kindly amend as " 80% Payment shall be release within 45days against delivery and rest 20% will be released after complete installation, being MSME		Remains as per the original Tender terms.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
11	28 of 48	**Scope of Work & Service Level Agreement**	3. Scope of Work j) OEM Team/Engineer should do the implementation services at site (TPSODL/TPCODL/TPWODL/TPNODL)	Please Amend this as " OEM / OEM authorized partner should do the implementation services at site (TPSODL/TPCODL/TPWODL/TPNODL). Although the Responsibility of Complete Implentation will only be with OEM. OEM Confirmation on Letter Head to be kept Mandatory.		Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
12	Page No 8	**1.3. Calendar of Events**	Last date and time of receipt of Bids: 22.10.2023, 17:00 Hours	In view of the upcoming Dussehra holidays and the size & complexity of the requirement we would request TPCODL to kindly extend the bid submission date to 6th November 2023.		Extension shall be done suitably.
13	8	**1.7 Qualification Criteria**	B. The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM personnel only. All the compliances should be submitted in the Bidder's letter head.	The OEM would be finalized basis the requirement specified in the RFP and it is not always possible to have resources certified on a solution from a particular OEM. We have a team of technical resources certified on a variety of security solutions including SIEM and SOAR. Hence, to promote wider participation we would request TPCODL to kindly amend the clause as suggested herewith: *The bidder should either be an OEM or an authorized channel partner of OEM. In case the Bidder is a channel partner of the OEM, the Bidder shall submit an Authorization Letter certified from OEM in this regard. The bidder must have at least 1 or more certified engineers. Installation will be carried out by OEM personnel only. All the compliances should be submitted in the Bidder's letter head.*		Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
14	9	**1.7 Qualification Criteria**	E. The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company created as a wholly owned subsidiary of the main Parent Company. In view of the above we would request TPCODL to kindly consider the relevant project experience of both the Parent Company and the Subsidiary Company (Bidder) for Qualification Criteria compliance. Please confirm the acceptance of our requests.		The bidder should have executed similar/relevant works related to DC Network/Network-Security architecture planning/designing for cumulative 6 Crore INR during last 3 years & **atleast 1 project of SIEM & SOAR implementation in DC distributed environment should be present in previous similar work experience.** Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.
15	9	**1.7 Qualification Criteria**	E. The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.	For promoting wider participation we would request TPCODL to kindly amend the clause as suggested below: *The bidder or any member of the Group Company should have executed similar works for cumulative 5 Crore INR during last 3 years (1st April 2020 onwards). Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.* Please confirm the acceptance of our request.		The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years **(atleast 1 project should be of SIEM & SOAR)**. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
16	9	**1.7 Qualification Criteria**	E. The bidder should have executed similar works for cumulative 6 Crore INR during last 3 years. Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.	Our understanding of "similar works" is supply & implementation of security solutions which includes SIEM and / or SOAR solution. Please confirm our understanding.		The bidder should have executed similar/relevant works related to DC Network/Network-Security architecture planning/designing for cumulative 6 Crore INR during last 3 years & **atleast 1 project of SIEM & SOAR implementation in DC distributed environment should be present in previous similar work experience.** Copy of work orders / completion certificate to be submitted in this regard. In case the Bidder have previous association with Tata Power or TPDDL/TPCODL / TPNODL / TPSODL / TPWODL/Discoms/Utilities/Industries/PSU for supply of similar product, performance feedback of the same will be solely considered irrespective of the performance certificate issued by bidder's other customer.
17	16	**7.1.** **Special Conditions of Contract**	f) Delivery period shall be 60 days from date of receipt of Release Order / CAT-A GTP approval, whichever is later.	Currently the IT industry is facing multiple challenges such as shortage of IC chips, international conflicts, disruption of supply chain etc. due to which there is a world wide crisis of availability of IT equipment. In view of the above, we would request TPCODL to kindly extend the delivery timeline to 180 days from date of receipt of Release Order / CAT-A GTP approval, whichever is later.		Remains as per the original Tender terms.
18	16	**I) Terms of Payment:**	a. Supply part: On delivery of the software complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. The payment a payment of 60% of the Invoice basic value along with 100% tax as applicable, shall be made within 90 days of the submission of the invoices along with all the requisite documents However, for MSME Bidders, the payment shall be released within 45 days of the submission of the bills/invoice.	To align with the industry wide accepted payment terms for similar projects we would request TPCODL to kindly amend the clause as suggested below: a. Supply part: On delivery of the solution complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. A payment of 70% of the Invoice basic value along with 100% tax as applicable, shall be made within 30 days of the submission of the invoices along with all the requisite documents.		Remains as per the original Tender terms.
19	16	**I) Terms of Payment:**	b. Installation, Testing & Commissioning: Upon Installation, Testing & Commissioning of the software complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. The payment a payment of balance 40% of the Invoice basic value along with 100% tax as applicable, shall be made within 90 days of the submission of the invoices along with all the requisite documents. However, for MSME Bidders, the payment shall be released within 45 days of the submission of the bills/invoice.	To align with the industry wide accepted payment terms for similar projects we would request TPCODL to kindly amend the clause as suggested below: b. Installation, Testing & Commissioning: Upon Installation, Testing & Commissioning of the software complete in all respect and certification of acceptance by certified official, Associate shall submit the Bills/ Invoices in original along with all the requisite documents, in the name of TP Central Odisha Distribution Limited to Invoice Desk. The payment a payment of balance 30% of the Invoice basic value along with 100% tax as applicable, shall be made within 30 days of the submission of the invoices along with all the requisite documents.		Remains as per the original Tender terms.
20	30	**11. Liquidated Damages**	In case uptime commitment of device (as mentioned in clause 2 (a), (c), 3, 5, 6, 7, 8)) of this SLA) is not met, the same would attract a Penalty @ Rs1000 per hour per device. The penalty money will be recovered from the payment due to vendor.	We would request TPCODL to kindly introduce a overall cap of the penalty charges. Please confirm that the cumulative maximum penalty charges for the project will be a maximum of 5% of the contract value.		Remains as per the original Tender terms.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
21	28	**3 Scope of Work**	h) Provide Hands on Training to TP Odisha discoms Team (Minimum 12 Engineer) by OEM only.	Kindly confirm that Training will be in single batch. Also confirm the training location i.e. bidder or customer location		The Clause stands as 1. Need to Provide Hands on Training to TP Odisha discoms Team (Minimum 12 Engineer) by OEM /OEM certified resource under the supervision of OEM against which OEM needs to share the consent on their Letter Head mentioning the responsibility lies completely on them. 2. Training needs to be arranged on Discom wise Single Batch under mutual consensus . The quantity of Engineers of each batch may vary based on the availability/requirement of engineers. 3. Training location will be customer/Bidder location baed on mutual consensus.
22	28	**3 Scope of Work**	j) OEM Team/Engineer should do the implementation services at site	We would request for amending the clause as - "OEM Team / Engineer or OEM certified partner should do the implementation services at site".		Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
23	29	**3 Scope of Work**	K) Supply and installation of necessary cables, accessories (Power cord for Indian standard, cable tie etc.) (Optical patch card/Cat6) & SFP for interconnecting to Firewall/Router/Servers/Leaf switches/Management switches with sufficient quantity. Quantity will be decided at the time of Implementations.	Please provide the existing network architecture, details of device type & list of devices which needs to be integrated with SIEM and SOAR.		This clause is deleted as if it is Software Based Solution.
24	29	**4 Maintenance Services**	TP Odisha discoms will allow vendor to carry out required Preventive Maintenance of the device. The down time required for Preventive Maintenance will be included in total down time of system to calculate quarterly uptime and communicated to TP Odisha discoms management by the vendor.	We would request not to consider Preventive Maintenance down time for SLA calculation as it comes under planned downtime. Please confirm the acceptance of our request.		Accepted & the Clause stands as follows- 1.Preventive Maintenance down time should be exempted from SLA calculation as it comes under planned downtime. 2. In case of software/service outage due to VM corruption/failure, restoration of service/software will be lies on Bidder & OEM as per SLA clause subject to pre-requisites/resource availability from customer End. Bidder needs to share their acceptance against the aforsaid clause on OEM Letter Head.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
25	29	**5 Spares Availability/ Support for OS Patch**	Access to OEM Diagnostic Solutions Database.	Kindly elaborate this clause as we log call with OEM for any support during the contract period.		This clause stands as 1. Continuous communication from Threat Intel to the SIEM_SOAR solution should be available but update needs to be configured in scheduled manner instead of High/Critical updates as it should be downloaded as per the hourly update schedule. 2. TPODL should have access to OEM portal for Major/Minor upgrade/patch/bug-fixes/EOS etc. download & Install. 3. TPODL should have access to OEM Market community portal for latest content/reports/playbooks download & intimation. 4. All the logged fault tickets should carries the RCA/Cause of Issue/Resolution mentioned in the same so that it can be reffered in future on requirement basis. The responsibility of the same lies with OEM . OEM needs to share their consent on letter Head against the above mentioned 4 nos. clauses.
26	29	**7 Delivery Time**	The devices should be delivered within 6-8 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation. (Client will intimate date to bidder for installation of equipment's).	We would request TPCODL to increase the delivery timeline to 24 weeks. Further, please let us know what will be time gap between devices delivery and the intimation date for initiating the installation of equipment.		The **software solution** should be delivered within 6-8 weeks from order issuance date and HLD/LLD/Installation of the same should be done in Four (4) weeks from the date of intimation post delivery. Client will intimate date to bidder for installation of solution.
27	30	**9. Level of specialist assistance to engineer.**	The vendor will ensure that all required specialist /Technical Support will be provided to his engineer so that the guaranteed uptime will be achieved	Kindly confirm if successful bidder needs to provide onsite manpower support.		Bidder will ensure that they will maintain the SLA as per RFP.
28	30	**Generic Points**	The solution proposed should be an Intelligent Next Generation SIEM and must be able to detect any anomalies, report in real time and take action as programmed having SIEM AND SOAR capabilities accessible within single User Interface.	Kindly confirm if the successful Bidder needs to provide ticketing tool or integration with existing ticketing tool. Please provide details of existing ticketing tool.		Proposed soluion should have ticketing tool / case management capability inbuilt. Bidder needs to propose solution accordingly & share compliance against the same on OEM letter Head.
29	30	**Generic Points**	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.	Kindly confirm if bidder needs to provide hardware for SIEM or TPCODL will provide the required infrastructure.		TPCODL/TPWODL/TPNODL/TPSODL will provision the required infrastructure, Bidder needs to submit the HW/SW pre-requisites on OEM letter head. The Data retention period is as follows- 1. latest 6 months data will be online & accessible. 2. 6 month onwards till 12th month end data will be stored on the storage device & should be restorable in the SIEM_SOAR solution as & when required. 3. data beyond 1 year should be stored on Storage/tape-Library/VTL & should be restorable in the SIEM_SOAR solution as & when required. 4. For such archival & restoration , the responsiblity lies with Bidder & OEM. In this regard, Bidder/OEM shall provide script/SOP to enable such backup/restoration on demand along with handholding support to the concerned team from TPCODL/TPWODL/TPNODL/TPSODL End.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
30	35	**Services**	74 OEM should be part of SIEM & SOAR deployment (at least 20% efforts should be from OEM including architecture design, governance, training etc)	This point is contradictory with point (j) given in scope of work which states that OEM need to do complete deployment. Kindly confirm the required delivery mechanism acceptable / recommended by TPCODL.		Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
31	General		General Query	Are TPCODL TPWODL TPNODL looking for management of SIEM/SOAR solution for contract period. Any resources need to be deployed by bidder for operations		Bidder will ensure that they will maintain the SLA as per RFP.
32	17 (9)		General Condition of Contract	Please provide the General Condition of Contract for our review		Already enclosed on the websites of ODISHA DISCOMS.
33	General Query		General Query	Will Tata power be open to have on have a cloud based deployment ?		No. Proposed solution should be deployed on-premise only
34	General Query		General Query	Will Tata Power require On Prem resources to manage the setup or can this be done remotely or a hybrid setup SOC for this setup		TPODL requires On-Prem resource to manage the setup.
35	Page No. 18	**ANNEXURE-I - Schedule of Items**	SITC of Security information and Event Management (SIEM) and Security Orchestration and Automated Response (SOAR) in HA with Perpetual License including 05-year Warranty and Support.	are we to implement 3 distinct SIEM-HA in each (Central , Western and Northern) or HA among all the three?		Presently 3 nos. of complete different standalone Solutions will be implemented in HA but all the 3 nos. of standalone proposed SIEM_SOAR solutions should have the capability to integrate with one Central common TPODL SIEM_SOAR solution which can be deployed in future along with capability of provisioning of traffic in syslog, CEF format in bidirectional way (i.e. Individual SIEM_SOAR to Central SIEM_SOAR & vice versa). However the exact solution architecture shall be finalised will the selected Bidder. Bidder needs to provide the necessary confirmation from OEM against the aforsaid clause on OEM letter Head.
36	Page No. 28	**Scope of Work & Service Level Agreement**	OEM Team/Engineer should do the implementation services at site	While the above says only three sites/locations, below highlights four sites. Southern region should be considered only for data-ingestion or do we have to deploy locally any device?		Installation can be carried out by OEM Personnel or OEM Authorized Person/Bidder at site Under OEM responsibility including architecture design, governance, training etc. The bidder must have at least 1 or more of the same OEM certified engineers. Installation will be carried out by OEM certified resources as per OEM validated design standards and best practices. OEM needs to share the declaration on their Letter head (TPSODL/TPCODL/TPWODL/ TPNODL) as taking the responsibility of the installations to be completed on Time as per Tender Clause.
Technical Queries						
1	Page No: 31	**Technical Specification Point No-10**	Proposed SIEM solution must have at least 2 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations)	Proposed SIEM solution must have at least 2 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations- 3 govt po...is fine without any EPS count...pl put up in prebid, there are PO with us, but deployment is not completed.		Proposed SIEM solution must have at least 3 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 15K EPS from any Government of India organizations)
2		**Technical Specifications for SIEM And SOAR**	Generic Query on License		Analyst license is asked for 15 Analyst. Please confirm, if these 15 analyst license required are with analyst (admin, read, write) rights or with only read rights.	All 15 Analyst licenses should be provide with complete rights (i.e. Super user, admin, read & write)

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
3		**Technical Specifications for SIEM And SOAR**	Generic Query on License		There are some points in technical specifications which talks about user behaviour based analytics/correlation. So, kindly help with the number of user count.	please consider 3000 users Discom wise.
4	Important Point	**Technical Specifications for SIEM And SOAR**	Generic Query on License	We understand that 15 Analyst are required here with complete analyst (admin, read, write) rights. Kindly confirm		All 15 Analyst licenses should be provide with complete rights (i.e. Super user, admin, read & write)
5	Important Point	**Technical Specifications for SIEM And SOAR**	Generic Query on License	There are some points in technical specifications which talks about user behaviour based analytics/correlation. So, kindly help with the number of user count. This is important Point to have Clear Clarity on the Requirement.		please consider 3000 users Discom wise.
6	& Page No. 31	**Technical Specifications For 'SIEM and SOAR**	Proposed SIEM solution must have at least 2 deployments for more than15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations)	Kindly remove the EPS Count only Proposed SIEM solution must have at least 2 deployments for more than in Govt of India organizations. (At least 3 sign-off copies must be provided from Government of India organizations		Proposed SIEM solution must have at least 3 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 15K EPS from any Government of India organizations)
7	11	**SECOND PART: "TECHNICAL BID"**	SECOND PART: "TECHNICAL BID" shall contain the following documents ii) Type Test Certificate of Lightning Arrester of same or higher rating	This seems to be an error, as firewall requirement may not have need for Lightning Arrester		This clause is deleted
8	18	**ANNEXURE-I - Schedule of Items**	ANNEXURE-I - Schedule of Items SITC of Security information and Event Management (SIEM) and Security Orchestration and Automated Response (SOAR) in HA with Perpetual License including 05-year Warranty and Support.	Normally, SIEM log collectors are given in HA. SIEM/SOAR solutions are not provided in HA. However, please confirm if TPCODL TPWODL TPNODL are still looking for SIEM & SOAR solution in HA (Qty 2) at each site - Total 6 Also please share DC and DR locations		Presently 3 nos. of complete different standalone Solutions will be implemented in HA but all the 3 nos. of standalone proposed SIEM_SOAR solutions should have the capability to integrate with one Central common TPODL SIEM_SOAR solution which can be deployed in future along with capability of provisioning of traffic in syslog, CEF format in bidirectional way (i.e. Individual SIEM_SOAR to Central SIEM_SOAR & vice versa). However the exact solution architecture shall be finalised will the selected Bidder. Bidder needs to provide the necessary confirmation from OEM against the aforsaid clause on OEM letter Head.
9	30	**Technical Specifications For 'SIEM and SOAR'**	Technical Specifications For 'SIEM and SOAR' The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources	There can't be unlimited devices, based on device count the SIEM appliance sizing varies. Kindly share device count and physical location details where assets are available, network and bandwidth for links		The cluase Stands as follows- Technical Specifications For 'SIEM and SOAR' The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from all devices or sources available/operational in DC/DR environment for each Discoms.
10	33	**Technical Specifications For 'SIEM and SOAR'**	SIEM Solution should be proposed for 10000 Sustained EPS and 15000 Peak EPS from Day 1. Solution should not drop or queue logs in case of license exceeds in case of sudden rise in EPS during any unwanted situation (e.g., Cyber-attack). Solution shall be able to scale up to at least 30000 EPS in future (in span of next 5 years).	Please share with us log sources (assets) and quantity to understand log collectors deployment.		No Change. The Clause remains same.
11	Page 30		Bidder to specify make and Model			No Change. The Clause remains same.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
12	Page 30	**Technical Specifications For 'SIEM and SOAR'**	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.	The SIEM solution should be software based with a clear logical and physical separation of the collection module and correlation module.	Every OEM has a different Architecture wherein the physical layer separation is based on architecture. Logging module is integrated accordingly	TPCODL/TPWODL/TPNODL/TPSODL will provision the required infrastructure, Bidder needs to submit the HW/SW pre-requisites on OEM letter head. The Data retention period is as follows- 1. latest 6 months data will be online & accessible. 2. 6 month onwards till 12th month end data will be stored on the storage device & should be restorable in the SIEM_SOAR solution as & when required. 3. data beyond 1 year should be stored on Storage/tape-Library/VTL & should be restorable in the SIEM_SOAR solution as & when required. 4. For such archival & restoration , the responsiblity lies with Bidder & OEM. In this regard, Bidder/OEM shall provide script/SOP to enable such backup/restoration on demand along with handholding support to the concerned team from TPCODL/TPWODL/TPNODL/TPSODL End.
13	Page 30	**Technical Specifications For 'SIEM and SOAR'**	The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from unlimited devices or sources	The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from 1000 devices or sources	Devices cant be unlimited, Must be defined with a quantified value	The cluase Stands as follows- Technical Specifications For 'SIEM and SOAR' The SIEM Solution should be EPS based at both log management and Correlation layer and must support logs from all devices or sources available/operational in DC/DR environment for each Discoms.
14	Page 30	**Technical Specifications For 'SIEM and SOAR'**	The SIEM solution support high availability feature and should be proposed in HA mode for all layers at DC.	The SIEM solution support high availability feature and should be proposed in HA mode for all critical layers	Must be discussed as this will include additional cost and comprexity as this will include load balancer from different OEM	No Change. The Clause remains same.
15	Page 31	**Technical Specifications For 'SIEM and SOAR'**	Proposed SIEM solution must have atleast 2 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations)	Proposed SIEM solution must have atleast 2 deployments for more than 15000 EPS in Govt of India organizations. (Atleast 3 sign-off copies must be provided for more than 30K EPS from any Government/Enterprise/Private of India organizations)	Reference should not be restricted to Govt.	Proposed SIEM solution must have at least 3 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 15K EPS from any Government of India organizations)
16	Page 31	**Technical Specifications For 'SIEM and SOAR'**	The solution must provide the ability to reduce event data through filtering or aggregation before it is sent to the log management system. License count should be performed post filtering of logs.	The solution must provide the ability to reduce event data through filtering. License count should be performed post filtering of logs.	Log Management is not a separate componenet in most of the OEMs. Ideally the functionality will be accomplised	No Change. The Clause remains same.
17	Page 32	**Technical Specifications For 'SIEM and SOAR'**	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic		No Change. The Clause remains same.
18	Page 32	**Technical Specifications For 'SIEM and SOAR'**	Solution must support searching and reporting of logs at logging layer with machine learning capabilities.	Solution must support searching and reporting of logs with machine learning capabilities.	Log Management is not a separate componenet in most of the OEMs. Ideally the functionality will be accomplised	No Change. The Clause remains same.
19	Page 32	**Technical Specifications For 'SIEM and SOAR'**	All logs must get auto archived on centralized storage directly from Log management layer and archived logs must be readable from archival/ central storage directly	All logs must get auto archived on centralized storage directly and archived logs must be readable from archival/ central storage directly		No Change. The Clause remains same.
20	Page 32	**Technical Specifications For 'SIEM and SOAR'**	Proposed SIEM & SOAR solution should be perpetual software based solution. To deploy the proposed Software based SIEM & SOAR, the HW, OS and Storage related configuration details should be submitted over OEM letterhead and same would be provisioned by TataPower.	Proposed SIEM & SOAR solution should be perpetual software based solution. To deploy the proposed Software based SIEM & SOAR, the HW, OS and Storage related configuration details should be submitted over Partner letterhead and same would be provisioned by TataPower.	Storage will be provided by Partner. It should be on Patner letter head rather than OEM	Proposed SIEM & SOAR solution should be perpetual software based solution. To deploy the proposed Software based SIEM & SOAR, the HW, OS and Storage related configuration details should be submitted over OEM letterhead and same would be provisioned by TPWODL/TPNODL/TPCODL/TPODL

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
21	Page 33	**Technical Specifications For 'SIEM and SOAR'**	SIEM Solution should be proposed for 10000 Sustained EPS and 15000 Peak EPS from Day 1. Solution should not drop or queue logs in case of license exceeds in case of suddden rise in EPS during any unwanted situation (eg. Cyber-attack). Solution shall be able to scale up to atleast 30000 EPS in future (in span of next 5 years).	SIEM Solution should be proposed for 10000 Sustained EPS and 15000 Peak EPS from Day 1. Solution should not drop or queue logs in case of license exceeds in case of suddden rise in EPS during any unwanted situationfor Specific duration 45 min-2 hours (eg. Cyber-attack). Solution shall be able to scale up to atleast 30000 EPS in future (in span of next 5 years).	For Specific duration 45 min-2 hours	No Change. The Clause remains same.
22	Page 33	**Technical Specifications For 'SIEM and SOAR'**	No Events should be dropped during Spikes, even if license limits gets exceeded: The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and mitigate threats during an attack or other unforeseen spikes in event volumes.	No Events should be dropped during Spikes, even if license limits gets exceeded (5x surge): The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and mitigate threats during an attack or other unforeseen spikes in event volumes.	we support 5x surge	No Change. The Clause remains same.
23	Page 33	**Technical Specifications For 'SIEM and SOAR'**	SOAR solution can be from same or different OEM, however there should be out of the box integration avialble between both SIEM & SOAR. The SOAR solution shall be licensed for atleast 15 analysts	SOAR solution can be from same or different OEM, however there should be out of the box integration avialble between both SIEM & SOAR. The SOAR solution shall be licensed for atleast 5 Concurrent analysts and must be in HA		No Change. The Clause remains same. SIEM & SOAR will be from same OEM & all 15 Analyst licenses should be provide with complete rights (i.e. admin, read & write)
24	Page 33	**Technical Specifications For 'SIEM and SOAR'**	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc.	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Real time, Heuristics based, Behavioral based, Risk based etc.	Real time needs to be included instead of historical as there is more logical having real time logs rather than historical	No Change. The Clause remains same.
25	Page 33	**Technical Specifications For 'SIEM and SOAR'**	Solution should provide a heatmap dashboard against all use cases which are active in the system which should help to strategies the security posture.	Solution should provide a Mitre dashboard against all use cases which are active in the system which should help to strategies the security posture.	Mitre dashboard has more meaningful information than a Heatmap dashboard	No Change. The Clause remains same.
26	Page 34	**Technical Specifications For 'SIEM and SOAR'**	SOAR must be integrated platform with SIEM on same user interface	SOAR must be integrated platform with SIEM on same or different user interface	Integration is possible however the soar will have separate UI	No Change. The Clause remains same.
Suggested Clause						
1	General		**Suggested Clause**	The RFP does not identify the Limitation of Liability or exclusion of Indirect Damages for the Bidder. In such circumstances Bidder may be exposed for unlimited liability and Hence the following clause is identified to be incorporated : Suggested following clause: Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence (including gross negligence or wilful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. For any liability not excluded by the foregoing, with respect to all claims including those for intellectual property claims and indemnifications, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent twelve (12) months of charges collected by supplier pursuant to the applicable po/order giving rise to the liability. The liability for Service defaults matters to be limited to the Service credits.		Shall be as per the relevant clause mentioned in the General Condictions of Contract of TPCODL/TPWODL/TPNODL/TPSODL.
2			**Suggested Clause**	Phishing Email Classifier is a Machine Learning based classifier that helps to predict Phishing Emails and helps to speed up the triage and overall investigation processing. Solution should support either the pre-trained module or creating a new ML model and train it on users own local phishing emails.		No Change. The Clause remains same as per Tender.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
3			**Suggested Clause**	The SOAR system should provide a visual playbook and assists with troubleshooting by visually identifying failed playbook steps		No Change. The Clause remains same as per Tender.
4			**Suggested Clause**	SOAR should allow add mock output to steps to simulate a step output even without the presence of network connectivity on which the step relies		No Change. The Clause remains same as per Tender.
5			**Suggested Clause**	SOAR Solution must read PDF and data can be extracted to indicators		No Change. The Clause remains same as per Tender.
6			**Suggested Clause**	SOAR must provision a War Room for analysts to ensures that the task force is well-equipped to handle and coordinate all aspects of critical situations. War room helps establish an effective communicate for both internal and external stakeholders and coordinate between teams. It also helps to investigate the root cause, and resolve the problem by allocating tasks to specialists, agreeing on milestones, taking notes of technical analysis and solution proposals, and getting feedback on all points.		No Change. The Clause remains same as per Tender.
7			**Suggested Clause**	The system should provide granular and flexible Role Based Access Control (RBAC). RBAC should allow administrators to configure both what areas of the GUI a user is able to access, and which data sets (eg which alerts) they are able to access. RBAC and user configuration should be possible via the GUI RBAC should be granular, allowing administrators to specify Create Read Update Delete permissions down to the feature level		No Change. The Clause remains same as per Tender.
8			**Suggested Clause**	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.	Hope EPS licensing across all layers - collection , logging and correlation should be uniform?here might me performance issue if EPS is not same across all the layers, we request to change the clause for better performance.	No Change. The Clause remains same as per Tender.
9			**Suggested Clause**	The SIEM Solution should support security data lake concept for future scalability and expansion perspective.	Security Data Lake is not required for future scalability and expansion .	No Change. The Clause remains same as per Tender.
10			**Suggested Clause**	The proposed solution must provide inline options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed. Log Filtering needs to be available across all tier to filter out logs as wherever required.	Request to change the clause as " The proposed solution must provide options to reduce event data at the source by filtering out unnecessary event data. Filtering must be simple string-based or regular expressions and must delete the event data before it is processed. Log Filtering needs to be available across all tier to filter out logs as wherever required." **Justification :** SIEM Event Collectors never be used inline in any network but consumes data in promiscuous mode, its not recommended and not a best practice as it creates a latency and bandwidth bottle neck, also there is a risk of network going down in case of device failure, hence we request to please change the clause.	No Change. The Clause remains same as per Tender.
11			**Suggested Clause**	Proposed SIEM solution must have at least 2 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 30K EPS from any Government of India organizations)	Hope 2 sign-off copies for more than 30K EPS from any Government of India organizationshould meet the PQ criteria ?	Proposed SIEM solution must have at least 3 deployments for more than 15000 EPS in Govt of India organizations. (At least 3 sign-off copies must be provided for more than 15K EPS from any Government of India organizations)

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
12			**Suggested Clause**	Solution should have 6 month's online and 1 year offline storage.	We understand that the ask is for total 1 years data storage, i.e. 6 Months online and 6 months Archival data, that will be one year data. (If data storage is asked for 1.5 years this will increase the cost of the project) please clarify.	No Change. The Clause remains same as per Tender.
13			**Suggested Clause**	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioral based, Risk based etc. Solution should have capability to detect identity breaches and threats even when the account is not active	The Functionality asked is for UBA (User Behaviour Analysis) we request to mention the number of UBA license required to propose the solution, this will help that all bidders propose same solution without any assumptions.	No Change. The Clause remains same as per Tender. Please consider 3000 users Discom wise.
14			**Suggested Clause**	Log Management - Collection, Compliance, Forensics, Integrations, Reporting & Searching and Storage	**Justification :** In the RFP Network Forensic is considered as a part of the SIEM Functionality however there is no Specification related to the SOW of Data Forensics we suggest to add Data Forensic in terms of Deep Packet Inspection as log information is not sufficient for forensics. Most SOC RFP' include log and packet capture for complete visibility at all layers of the OSI stack (Layer 2-7)	No Change. The Clause remains same as per Tender.
15			**Suggested Clause**	**Additional Clause to meet forensics capability**	The collectors should be able to store/retain both normalized & raw data (Logs and Packets)for forensic purposes, should support throughput upto 100 Mbps for incoming & outgoing data through Internet, Solution should store RAW packet DATA for 7 days and normalized packet data for 15 days for forensics	No Change. The Clause remains same as per Tender.
16			**Suggested Clause**	**Additional Clause to meet forensics capability**	Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data should support session and application reconstruction.	No Change. The Clause remains same as per Tender.
17			**Suggested Clause**	**Additional Clause to meet forensics capability**	SIEM Should have single GUI for Logs and Packet data for quick response	No Change. The Clause remains same as per Tender.
18			**Suggested Clause**	**Additional Clause to meet forensics capability**	Solution should have the ability to convert traffic from raw packets to meaningful arti facts like email, FTP data files, and VoIP conversations including PHP, JavaScript.	No Change. The Clause remains same as per Tender.
19			**Suggested Clause**	**Additional Clause to meet forensics capability**	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets.,The Analyst UI must be a common interface to investigate data collected and normalized for SIEM (Logs), DPI (Packet data)	No Change. The Clause remains same as per Tender.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
20			**Suggested Clause**	5.7. Proposed SOAR technology should have Threat intel platform inbuilt with OEM threat intel feeds and support for both commercial and open source threat intel feeds. The Threat Indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources. SOAR solution must allow to add IOC sources in platform such as TOR Project official exit nodes, Ransomware Tracker, Cyber Crime tracker etc. based on IP Address, URLs, Domain, Files hashes (MD5)	We request to add additional clause as : "SOAR should have inbuilt features for security incident orchestration, Automation (SOA), case management, incident workflow (SIRP), Threat intelligence platform and Threat Intelligence Process (TIP) to address the needs for a security operations centre." **Justification :** As per analysts like Gartner and Forrester a full functioanl SOAR has three components - SOA (Security Automation and Orchestartion) ; Incidence Response Platform (SIRP) and Threat Intel Platform (TIP). The RFP only mentions SOAR with no description of functionalities and capabilities other than playbooks. SIRP and TIP (Process) is compeltely missing . What has been asked is a Threat Intel feed and not a platform. Request you to add the functionalities	No Change. The Clause remains same as per Tender.
21			**Suggested Clause**	**Additional Clause for TIP**	We request to add additional clause as :SOAR should provide in-built threat intelligence (IOC) platform, feed unlimited structure, unstructed threat intelligence gathered from a combination of commercial, Open Source, user led, community, and industry driven and provide complete advisory of threats to plan countermeasures and proactive actions to reduce the risk. Solution should de-dupe, aggregate, normalize, enrich and process threat intelligence in a holistic and actionable manner. the solution should be able to import threat intelligence in following formats - Structured / finished intelligence analysis reports (.txt, .pdf) - Automatically ingest email lists with threat information. Automatically ingest email files (.msg, ,eml) with fully supported mailbox integration. ingest phishing emails using email forwarding to SOAR - Formatted CSV files , formatted MS office products - XML based structured intelligence - STIX, OPENIOC, Yara, TAXII - Provide a visual interface of threat data with a graphical map view of associated intelligence. - Automate indicator ingestion via	No Change. The Clause remains same as per Tender.

Pre-bid Queries Responses for TENDER NOTICE NO: TPCODL/CCG/23-24/040 SIEM and SOAR						
S.No	**Page No**	**Clause No**	**Clause Details**	**Queries/Clarification requested**	**Justification**	**TPODL Response**
22			**Suggested Clause**	**Additional Clause for Incidence Response Platform**	We request to add additional clause as : Should support all workflow and case management features. Below are minimum features - OOTB workflow templates for managing cases - Full feautured case management platform that can integrate with external systems - Automated tasks within cases such as executing playbooks - Ease to convert incident artificats into threat intelligence - Read/write workflow API for integrations or custom apps - Workflow playbook apps - Automated timeline generation for cases - Correlation of related cases	Clause details as per tender