OIL's response to the queries of Pre-Bid Conference held on 17-18th August,2023 in Kolkata against GeM Tender No. GEM/2023/B/3791672 for 'Hiring of Services for Establishing and Maintaining Cyber Security Operations Centre (CSOC) for OIL.'.

A. Bidder's name: M/s. Vara Tech

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1.	3	Pre Qulification -Criteria-2.1.5	The bidder must furnish documentation/declaration from respective OEMs of SIEM (Security Information and Event Management), SOAR (Security Automation, Orchestration, and Response) regarding duration of operation and number of implementations in India substantiating the following conditions: (a) The proposed SIEM solution must be operational in at least ten SOC implementations in	As we wholeheartedly support the "Make in India" initiative and the growth of Indian startups, we kindly request a reconsideration of certain clauses that may inadvertently hinder the participation of emerging startup. Specifically, we would like to address the conditions regarding the number of SOC implementations and the duration of operation required from respective Proposed Clarifications: Duration of Operation: Given the challenges and growth trajectory of new startups, we propose a flexible approach to the duration of operation requirement. Startup need	No Changes. Pl. be guided by the subject clause.

			India for the last 5 years reckoned from the original bid closing date of this tender. (b) The proposed SOAR solution must be operational in at least five SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender.	time to establish themselves and gain a foothold in the market. External factors, such as the recent pandemic, have also introduced unforeseen challenges. Therefore, we kindly request the reconsideration of the stipulated timeframe for operation, allowing new entrants the time they need to establish a solid foundation. Number of Implementations: While we acknowledge the importance of experience, we believe that requiring a high number of SOC implementations may inadvertently deter startups from participating. Startup companies, during their initial stages, may face resource constraints and a learning curve. We request the removal of the restriction on the number of implementations or a reduction in the minimum requirement, to encourage participation from startups that demonstrate potential and innovation. OEMs. We	

				understand the need for quality assurance and experience, yet we believe there is an opportunity to strike a balance that nurtures innovation and allows startups to flourish. We suggest the removal of the terms "proposed SIEM" and "proposed SOAR" from the bid requirements. Instead, we recommend focusing on SIEM and SOAR solutions exclusively. This adjustment would ensure a more welcoming bid process for a wider array of participants, leading to increased competition and a selection of the most suitable and innovative solutions.	
2.	21	Scope Of Work	The solution must provide real time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms	Kindly request further information regarding any existing voice call services your organization currently utilizes. This information will help us better understand the feasibility and compatibility of integrating voice call	Information regarding critical alerts may be conveyed to OIL over phone call to the concerned OIL official. This is not necessarily an automated/system generated voice call.

			such as email, SMS, voice call etc. based on policies.	mechanisms into our proposed solution. we would like to request an amendment to the clause as follows: "The solution must provide real-time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms, such as email, SMS, etc., based on policies."	
3.	22	Scope Of Work	Policy compliance: Built-in and customizable content and reporting that satisfy elements of various regulatory compliance, such as PCI, SOX, and FISMA.	Considering that operations are conducted exclusively on the Indian subcontinent, we kindly request an adjustment to the compliance criteria. In particular, we would like to focus on the FISMA (United States Federal Information Security Management Act) compliance requirement. Given that FISMA pertains to regulations within the United States and is not directly applicable to our operations in India, we kindly request the removal of the FISMA	Requirement for FISMA to be removed. Shall deliver and issue amendment if needed.

				compliance component from the bid requirements.	
4.		General	Preference to Make in India	As per the guidelines set forth by the Ministry of Electronics and Information Technology (MeitY), Government of India no:1(10)/2017- CLES dated: 06.12.2019, We kindly request that you review stipulated eligibility criteria and any associated terms mentioned in the aforementioned Orders and Notifications. We suggest for a heightened emphasis on the "Make in India" initiative, as it plays a crucial role in advancing our nation towards self-reliance.	No Changes. Pl. be guided by the subject clause.

B. Bidder's Name: M/s. SIFY

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1.	2	3. Solutions Sizing	Peak EPS handling capacity of the solution	Please also mention the minimum/maximum brust time till the sought EPS needs to be handeled.	Shall deliver and issue amendment if needed.
2.	6	3.3 Solution Delivery - Discovery and	Capture and review the current security posture, security	This part comes under the auditing and consultancy doesn't comes under SOC in	This clause pertains to information gathering about OIL's existing

		assessment phase	policies and controls.	general, please clarify the need of this in SOW.	infrastructure and security posture for the understanding of the successful bidder.
3.	2	PRE QUALIFICATION CRITERIA (PQC)	2.1.1 Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company.	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 OIL to kindly consider the relevant project experience of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance. Please confirm the acceptance of our request.	Shall deliver and issue amendment if needed.
4.	2	PRE QUALIFICATION CRITERIA (PQC)	2.1.1 Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from	For wider participation we would request OIL to amend the clause as suggested below: Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central	No Changes. Please be guided by the subject tender clause.

			the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company.	Government / State Government Organization / Public Limited Company / BFSI.	
5.	2	PRE QUALIFICATION CRITERIA (PQC)	2.1.3 The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender.	For wider participation we would request OIL to amend the clause as suggested below: The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company / **BFSI** only) to whom they are currently providing managed SOC services using the proposed **similar** SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender.	No Changes. Please be guided by the subject tender clause.
6.	2	PRE QUALIFICATION CRITERIA (PQC)	Notes to Clause 2.1.1 above: A. "SIMILAR Work" mentioned above means, 'Experience in successful	We understand that both onsite and remote CSOC experience would be considered as similar work. Please confirm our understanding.	Acceptable

			completion of establishing and operating Cybersecurity Operations Center (CSOC).'		
7.	2	PRE QUALIFICATION CRITERIA (PQC)- TECHNICAL REQUIREMENT Clause 2.1 Sub Clause 2.1.1	2.1.1 Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company.	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 OIL to **kindly consider the relevant project experience of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance.** Please confirm the acceptance of our request.	Shall deliver and issue amendment if needed.
8.	4	PRE QUALIFICATION CRITERIA (PQC)_ 2.2 FINANCIAL CRITERIA: Sub Clause : 2.2.1	2.2.1 Annual Financial Turnover of the bidder in any of preceding 03 (three) financial / accounting years, reckoned from the original bid closing	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	Shall deliver and issue amendment if needed.

			date should be at least Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only.	subsidiary of the main Parent Company. In view of the above we would request OIL to **kindly consider the relevant project experience of both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance.** Please confirm the acceptance of our request.	

C. Bidder's Name: M/s. INNSPARK

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1.	3	Pre Qualification Criteria- 2.1.5	The bidder must furnish documentation/declaration from respective OEMs of SIEM (Security Information and Event Management), SOAR (Security Automation, Orchestration, and Response) regarding duration of operation and number of implementations in India substantiating the following conditions: (a) The proposed SIEM solution must be operational in at least ten SOC implementations in	As we wholeheartedly support the "Make in India" initiative and the growth of Indian startups, we kindly request a reconsideration of certain clauses that may inadvertently hinder the participation of emerging startup. Specifically, we would like to address the conditions regarding the number of SOC implementations and the duration of operation required from respective Proposed Clarifications:	**No changes.** With respect to "Preference to Make in India", please refer to 1.1 ELIGIBILITY CRITERIA in 1691238008.pdf document (PRE-QUALIFICATION CRITERIA (PQC)).

			India for the last 5 years reckoned from the original bid closing date of this tender. (b) The proposed SOAR solution must be operational in at least five SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender.	Duration of Operation: Given the challenges and growth trajectory of new startups, we propose a flexible approach to the duration of operation requirement. Startup need time to establish themselves and gain a foothold in the market. External factors, such as the recent pandemic, have also introduced unforeseen challenges. Therefore, we kindly request the reconsideration of the stipulated timeframe for operation, allowing new entrants the time they need to establish a solid foundation. Number of Implementations: While we acknowledge the importance of experience, we believe that requiring a high number of SOC implementations may inadvertently deter startups from participating. Startup companies, during their initial stages, may face resource constraints and a learning curve. We request the removal of the restriction on the number of implementations or a	

				reduction in the minimum requirement, to encourage participation from startups that demonstrate potential and innovation. OEMs. We understand the need for quality assurance and experience, yet we believe there is an opportunity to strike a balance that nurtures innovation and allows startups to flourish. We suggest the removal of the terms "proposed SIEM" and "proposed SOAR" from the bid requirements. Instead, we recommend focusing on SIEM and SOAR solutions exclusively. This adjustment would ensure a more welcoming bid process for a wider array of participants, leading to increased competition and a selection of the most suitable and innovative solutions.	
2.	21	Scope Of Work	The solution must provide real time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms such as email, SMS, voice call etc. based on policies.	Kindly request further information regarding any existing voice call services your organization currently utilizes. This information will help us better understand the feasibility and compatibility of integrating voice call	Information regarding critical alerts may be conveyed to OIL over phone call to the concerned OIL official. This is not necessarily an automated/system generated voice call.

				mechanisms into our proposed solution. we would like to request an amendment to the clause as follows: "The solution must provide real-time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms, such as email, SMS, etc., based on policies."	
3.	22	Scope Of Work	Policy compliance: Built-in and customizable content and reporting that satisfy elements of various regulatory compliance, such as PCI, SOX, and FISMA.	Considering that operations are conducted exclusively on the Indian subcontinent, we kindly request an adjustment to the compliance criteria. In particular, we would like to focus on the FISMA (United States Federal Information Security Management Act) compliance requirement. Given that FISMA pertains to regulations within the United States and is not directly applicable to our operations in India, we kindly request the removal of the FISMA compliance component from the bid requirements.	Requirement for FISMA to be removed. Shall deliver and issue amendment if needed.
4.		General	Preference to Make in India	*As per the guidelines set forth by the Ministry of*	**No changes.**

				Electronics and Information Technology (MeitY), Government of India no:1(10)/2017- CLES dated: 06.12.2019, We kindly request that you review stipulated eligibility criteria and any associated terms mentioned in the aforementioned Orders and Notifications. We suggest for a heightened emphasis on the "Make in India" initiative, as it plays a crucial role in advancing our nation towards self-reliance.	With respect to "Preference to Make in India", please refer to 1.1 ELIGIBILITY CRITERIA in 1691238008.pdf document (PRE QUALIFICATION CRITERIA (PQC)).

D. Bidder's Name: M/s. Prime Infoserv

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1	PQ Page 2	2.1.1.	Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company.	Request to amend the clause with work vale 1 crore	**No change**
2	PQ Page 3	2.1.7	The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 2 certified and shall have to furnish copies of the same.	SOC2 Type 2 is having no relevance with with SOC services. Hence would request you to delete this point. Rather if more validations needed, may add	Shall deliver and issue amendment if needed. SOC2 is Service Organization

				CERT-In Empanelled clause as this is endorsed by Meity	Control (SOC) audit on how a cloud-based service provider handles sensitive information. Since the proposed solution shall be hosted on cloud platform and OIL's confidential security data will reside here, SOC2 will ensure OIL that OIL's data is kept private and secure while in storage and in transit and is available for OIL to access at any time. This is in line with the "Cloud Security Best Practices" for Government departments published by MeitY.
3	SOW Page 13	3.5.3	SOC MANAGER: BE/B-Tech/MCA • Minimum 10 years of experience in working in IT service management out of which minimum 3 years is in managing SOC operations • Professional certification: Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM)	CISSP or CISM may not be that relevant for SOC Manager profile. Rather Certified SOC Analyst would be better to comply the needs.	**No change**

E. Bidder's Name: M/s. ESDS

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1	2	PQC	2.1.1 Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company.	BFSI Sector is handling large financial data and transactions which also required hardend security for which BFSI sector is also utilizing CSOC. Hence, we request that the previous experience of BFSI sector may also kindly be accepted. The clause may kindly be changed as follows: Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company / **BFSI sector.**	**No change**
2	36	SOW	13.0 PERFORMANCE SECURITY: 10% of Annualized Contract value. Validity of the performance security / contract performance	As per the Office Memorandum issued by Government of India,	No change

			guarantee shall be valid for 03 (three) months beyond the contract period.	Ministry of Finance, Department of Expenditure, Procurement Policy Division vide OM No. F.1/2/2023-PPD dated 03 Apr 2023 regarding Amendment in General Financial Rules, 2017 - Rule 171 (i) Performance Security. The Performance Security should be for an amount of 3-10%. Hence, we request that the Performance Security may kindly be reduced to 3% instead of 10%.	
3	33	PROFORMA-XII - COMMERCIAL CHECK LIST	1. Bidding structure	Kindly clarify what kind of confirmation is required from Bidder's regarding this line item.	Bidding structure mainly refers to the structure of the participating firm i.e. Company, Partnership firm, Proprietary firm etc.
4	33	PROFORMA-XII - COMMERCIAL CHECK LIST	Confirm that the offer shall remain valid for acceptance up to 90 (Ninety) days from original Bid Due Date / Date of opening of bids.	As per RFP document Introduction and Instruction to Bidders the validity of Bid should be 120 days from Original Bid Closing date. Kindly confirm the Bid Validity period 90 days or 120 days.	**120 days** from Bid Closing Date bid validity is required.
5	8	PROFORMA-VIII - FORM OF BID SECURITY	PROFORMA-VIII - FORM OF BID SECURITY (BANK GUARANTEE FORMAT) & PROFORMA-XV - FORM OF BID SECURITY (BANK GUARANTEE FORMAT)	Bank Guarantee Format have been provided in Two Performa. Kindly confirm,	Please note that Proforma-VIII is the FORM OF BID SECURITY (BANK

		(BANK GUARANTEE FORMAT)		which proforma needs to be used for preparation of BG.	GUARANTEE FORMAT), whereas Proforma-XV is IP (Integrity Pact)
6		TECHNICAL EVALUATION CRITERIA_ 4 (F)	"SIMILAR Work" mentioned above means, 'Experience in successful completion of establishing and operating Cybersecurity Operations Center (CSOC).'	Experience of executing similar work through 'sub-contracting' shall not be considered for evaluation. As per various government tender CSOC is only a part of overall contract and as we are the OEM for SOC orders allocated to us are of Sub contracting nature. Request you to accept subcontracting. Subcontracting in such services is totally different from other orders.	No Change.

F. Bidder's Name: M/s. CISCO

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1		SOW	The solution should have user behaviour analytics for minimum 7500 users and UEBA to monitor at least 1000 Entities/ Users.	The solution is based on the active throughput of the NetFlow. Solution works on Netflow and telemetry from various sources in the network. Requested to add total throughput.	**No change**
2		SOW	UEBA solution shall leverage the data in Security Big Data Lake	The solution leverages data from the network using NetFlow and SPAN where	**No change**

				required. Requesting to please change as "Solution should leverage the data and telemetry from the network using NetFlow and SPAN"	
3		SOW	UEBA shall leverage the following data sources: a. User authentication and access control systems like Windows domain controller logs and VPN systems b. Next gen firewall and NIDS/NIPS c. Host sensors, including anti-virus and EDR	User login data comes by using an agent on the machine or using a NAC solution integration with UEBA. Please clarify the ask	Data source for user login data shall be Windows domain controller logs and VPN systems and other application logs.

G. Bidder's Name: M/s. EY

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1		General		Can we propose Log Collection, processing and storage at Oil India DC & DR Premises and centralized correlation/ monitoring from EY Shared model ?	Please refer to 3.1 Provisioning of the Technology Components in the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)).
2		General		Please provide list of domain for Brand Monitoring & Anti-Rouge services	Maximum number of takedown requests during the contract period: 50.
3		General		Please clarify, Offsite DR location for business continuity should be considered for Entire SIEM,	Business continuity should be considered for Entire SIEM, UEBA,

				UEBA, TIP & SOAR infra or we should consider from SOC resources between DC & DR	TIP & SOAR infra AND SOC resources between DC & DR. Shall deliver and issue amendment if needed.
4		General		Can we proposed Gartners Magic quadrant Leader NG SIEM solution which is best adopted in industry or you want bidder to provide only Make in India products ?	No Change. Please be guided by the subject Clauses of the tender.
5		General		What is the advance notice duration for exit management? We propose a minimum of 3 months from either of the parties. Please confirm	Please refer to 3.6 Exit Management in the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)).

H. Bidder's Name: M/s. INFOSYS

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1	31	1691238015_RFP Scope CSOC	Maximum penalty for non-performance deduction in a quarter shall not exceed 15% of the total Quarterly Service Fee	Request COMPANY to limit cumulative penalty at a project level to 10% of TCV	No change
2	6	1691238015_RFP Scope CSOC	3.3 Solution Delivery - Installation, commissioning, integration, and acceptance testing: v. The Contractor shall constitute team(s) of suitably qualified and OEM certified engineers for each phase of the project and share the details of the team with OIL along with CVs and copies of relevant	Here OEM certified engineers means any OEM or Proposed OEM?	OEM here means OEM for the proposed solution.

			professional certificates of the team members prior to the project kick-off meeting.		
3	9	1691238015_RFP Scope CSOC	3.5 Managed Security Services Provider (MSSP) services for the CSOC solution Notes: 1. OIL's existing tools to be used for vulnerability management.	Will OIL provide licence separately for VAPT testing or will provide remote access?	OIL shall provide remote access to use the existing tools to be used for vulnerability management.
4	3	1691238008_ Notes to Clause 2.1.1 above_PQC	B. For proof of requisite Experience (refer Clause No. 2.1.1), the following documents / photocopy (self-attested / attested) must be submitted along with the bid: (a) Contract document / LoA / WO showing details of work, (b) Job Completion Certificate showing: (i) Gross value of job done (ii) Nature of job done and Work order no. / Contract no. (iii) Contract period and date of completion OR (c) SES (Service Entry Sheet) / Certificate of Payment (COP) issued by the company indicating the following: (i) Work order no. / Contract no. (ii) Gross value of jobs done (iii) Period of Service (iv) Nature of Service	Due to existing NDA constraints, we will be unable to share name (email/ landline/ mobile) & contact details (Contract document & Job Completion Certificate) of customers .In such case, we request Bank to allow the bidder to share a self-certificate by the Company Secretary or certificate by the Statutory Auditor for SIMILAR Work Details	No Change. Note: Bidder may blur out the confidential portion. However, the bidder must furnish sufficient documents to substantiate the requisite experience as per the tender conditions.
5	2	1691238008_PQC_Clause No. 2.1.1	"SIMILAR Work" mentioned above means, 'Experience in successful completion of establishing and operating Cybersecurity Operations Center	Request you to change the clause as "'SIMILAR WORK' means "Experience in successful completion of establishing and operating	No Change

			(CSOC).'	Cybersecurity Operations Center (CSOC)"in any sector sector	
6	16/17	1691239662_STC	b) this limitation shall not apply to the cost of repairing or replacing defective equipment by the CONTRACTOR, or to any obligation of the CONTRACTOR to indemnify the COMPANY with respect to Intellectual Property Rights.	Request you to keep indemnification due to IPR under the LoL cap	Please be informed that the GCC of the tender are standard approved Clauses, therefore deviation to these Clauses is not possible. However, the Clauses of SCC shall supplement and / or amend the GCC. Whenever there is a conflict, the provisions in SCC shall prevail over those in the GCC.
7	17	1691239662_STC	Further, OIL shall retain the right of forfeiture of Performance Bank Guarantee and any other action as deemed fit. In certain operational situations OIL reserves the right to take over the site including the service equipment at the risk and cost of the	Request you to limit the Risk purchase to respective milestone value, instead of having it uncapped.	Please be informed that the GCC of the tender are standard approved Clauses, therefore deviation to these Clauses is not possible. However, the Clauses of SCC

					shall supplement and / or amend the GCC. Whenever there is a conflict, the provisions in SCC shall prevail over those in the GCC.
8	73	1691239662_STC	Payment Terms-	Request to have separate payment term/ milestones as per project timelines to avoid negative cashflows . Please consider the following as (payment on resource mobilization, Training, Discovery and Assessment, Solution Design, Installation and Commissioning, completion of UAT, Start of MSSP services, Exit Management services)	No Change.
9	2	1691238008_PQC_Clause No. 2.1.3	The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender.	If the bidder has implemented similar in an On-premises dedicated SIEM setup, would that be an acceptable previous experience as per 2.1.3 session of PQC.	Acceptable
10	3	1691238015_RFP Scope CSOC	Table Sl. No.: ix. Other data (apart from log data) retention requirement	We understand the SIEM and its related log retention	Log data and any data generated

				requirement which is specified in Table Sl.No: viii. We request OIL to elaborate the other data retention requirement in detail, to clarify what constitutes 'other data'	upon usage of the CSOC solution like but not limited to : Configuration Database, Documentation, knowledge base etc.
11	19	1691238015_RFP Scope CSOC	Log Management: The solution should be able to collect the logs, parse, normalize and store events from the below mentioned systems/formats.	We would like to know about the existing log collection mechanism and specify who will be responsible to forward the logs to the proposed local log Aggregator or Forwarder (MSSP or OIL IT Team)	MSSP team will provide the details of the configuration changes necessary to forward the logs and concerned OIL team will make the changes.
12	3	1691238015_RFP Scope CSOC	Solution Sizing Table Sl. No.: ii. Peak EPS handling capacity of the solution	As per RFP scope document, the minimum sustained EPS handling capacity of the log forwarder/aggregator shall be 20,000 in each location, during peak hours (burst) the expected is 1.5 times of sustained EPS is 30,000 is our understanding correct.	Yes
13	1	1691238015_RFP Scope CSOC	PREAMBLE: The primary and near DR (Disaster Recovery) datacentres of OIL is in Duliajan, Assam. The far DR datacentre of OIL is in Noida, UP	During normal operations Duliajan only will be sending logs to SIEM, as Noida is far DR site, the log aggregator or forwarder will send logs in case of Disaster only or both	Both locations will be active at any point of time.

				location will send the logs to SIEM, kindly clarify.	
14	5	1691238015_RFP Scope CSOC	Solution Delivery - Installation, commissioning, integration, and acceptance testing	Please provide clarity on the responsibility for the integration of CIs/Data sources for log forwarding other than CSOC related components. The responsibility should be with the OIL IT Team for log forwarding.	Please refer to 3.5.1 Scope in the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)) - Integration of new log sources into the CSOC solution as per OIL's requirement shall be MSSP's responsibility. **Note:** MSSP team will provide the details of the configuration changes necessary to forward the logs and concerned OIL team will make the changes.
15	19	1691238015_RFP Scope CSOC	6. The solution should be able to collect the logs, parse, normalize and store events from the below mentioned systems/formats natively (without the need for custom parser):	The Functional Specifications of the CSOC solution Section 5 provides enough information of the proposed solution. It does not say about the existing SIEM, SOAR, UEBA setup, should the MSSP need to	Migration of data from the existing setup is not in the scope of this project.

				transfer the already existing Use cases and Dashboards of SIEM.	
16	7	1691238015_RFP Scope CSOC	The scope of MSSP services, in the Notes it is specified about Real time monitoring of security alert feeds shall be done remotely on 24/7 basis from the Contractor's datacentres.	Does the Contractor's SOC facility should be located in the cloud datacenter or can it be in contractor's remote office location? Does the OIL have any specific definition and location requirements for the contractor's SOC ODC or facility?	There is no restriction on the location of cloud datacenter and SOC facility as long as other requirements of the tender are met.
17	12	1691238015_RFP Scope CSOC	Human Resources requirement for L3 SOC analyst & SOC Manager availability: OIL's office schedule: 7 AM – 6 PM IST (Monday –Saturday)	Does the availability means the on call availability of the SOC manager during the OIL's office schedule of 7 AM to 6 PM (Monday to Saturday) or does it imply physical presence in office for the office schedule hours.	Availability means on call availability.
18	12	1691238015_RFP Scope CSOC	Human Resources requirement for Dedicated On-site Resident Engineer	Is the OIL's Business hours is different from OIL's Schedule working hours. If Business hours is different, please specify the working hours. Is on-site Resident Engineers should be 2 at any point of time in Duliajan OIL's office location?	Shall deliver and issue amendment if needed.
19	6	1691238015_RFP Scope CSOC	ii. The Contractor will designate one of its suitably qualified personnel as the Project Manager (PM) for the solution delivery phase. The PM shall be the single point of contact for OIL during this phase and shall be present on-site in Duliajan throughout this phase.	The Project Manager should work from Duliajan OIL's office location during the OIL's office schedule working hours 7 AM to 6PM (From Monday to Saturday).	OIL's office schedule at Duliajan is : (7 AM to 11 AM, 12:30 PM to 3:30 PM)

				Is our understanding correct?	

I. Bidder's Name: **M/s. AIRTEL**

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1	115		The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 2 certified and shall have to furnish copies of the same.	The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later)/**CMMI Level 3** and SOC 2 Type 2 certified and shall have to furnish copies of the same. **Justification:** ISO 20000 is a standard for the requirements of an IT service management system. It can complement CMMI for Services, or vice versa. • But ISO 20000 does not provide a way to measure improvement. • Since CMMI can provide a framework to support implementing improvement, some organisations have used a tailored version of	No Change

				CMMI-DEV (prior to CMMISVC release) within their service teams to interpret ISO 20000.	
2		Log sources	There should be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users, or data source count changes, till maximum sustained EPS handling capacity is reached.	Please fix some numbers of devices. Justification: It will help to finalize overall commercials to bid.	**No change.** The payment terms are based on sustained EPS handling capacity.
3	63	3.5.2 Terms & Conditions: Xii	The Contractor shall ensure that offered CSOC services must comply with PII data security standard - ISO 27018.	We request you to remove this from RFP or make it optional for those who has privately hosted in their own data center. **Justification:** ISO 27018 gives generic agreed guidance on information security categories. The standard targets public cloud services providers that act as PII processors. Its key objectives are to: Help the public cloud PII processor meet their obligations, including when they're under contract to provide public cloud services. ISO/IEC 27001 and SOC TYPE 2 full fill all the requirement related to customer data protection in CSP environment	No change
4	65	3.5.3 Human Resources:iV	The deployed human resources must be permanent employees of the Contractor.	The deployed human resources can be permanent	No change

				or off role employees of the Contractor. **Justification:** This helps to bidder for better commercials and options in terms of technical manpower.	
5	70	5. Functional Specifications of the CSOC solution: Viii	Centralized Authentication: The proposed solution must be integrated with a central authentication system with two factor authentication enforced.	Please clarify that this two factor authentication for onsite person or for everyone who can access the dashboard.	Two factor authentication shall be enforced for everyone with access to the proposed solution.
6	72	5.1 Log Management:7	Solution must support log collection (via agent based and agentless methods). There should be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users, or data source count changes, till maximum sustained EPS handling capacity is reached.	Please fix some numbers of devices. Justification: It will help to finalize overall commercials to bid.	No change. The payment terms are based on sustained EPS handling capacity.
7	72	5.1 Log Management:13	Caching & Batching: The proposed solution must support local caching and batching at collection level in case of connectivity failures.	Please specify the duration for local caching.	Please refer to (v) in 3.1 Provisioning of the Technology Components in the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)).
8	72	5.1 Log Management:14	Compression: The proposed solution must provide at least 50% compression which can be customized for the data to provide further bandwidth conservation.	Compression: The proposed solution should provide 30% compression which can be customized for the data to provide further bandwidth conservation.	No Change

				Justification: Overall solution log collection does not consume much bandwidth.	
9	73	5.1 Log Management:16	No events shall be dropped during spikes, even when the License limit has been 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.	Some event can be dropped during unforeseen situation like DDoS or WAF attack.	No Change
10	113	TECHNICAL EVALUATION SHEET FOR BEC-BRC / PQC	2.1.3 The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender. In support of substantiating the above experience, the bidder must submit copies of relevant pages of the Contract(s) executed showing detailed address(es) of client(s), scope of work along with any of the following documentary evidence to substantiate the above-mentioned experience: (i) Completion certificate(s) issued by the client(s) (OR) (ii) Certificate(s) of Payment issued/acknowledged by the client(s) (OR)	Any other document(s) like CA certificate which substantiate the aforesaid experience criteria as defined above in PQC Clause No. 2.1.3.	No change. Already covered in "Any other document(s)"

			(iii) Any other document(s) which substantiate the aforesaid experience criteria as defined above in PQC Clause No. 2.1.3.		
11	Page No.46	3.5.1 Scope: Cyber Threat Intelligence, Hunting, and AnalyticsPage /Attack Simulation and Assessments/	Performing red teaming, penetration testing, adversary emulation, purple teaming, breach and attack simulation, or other testing detections with the goal of improving SOC operations and the constituency's overall defensive posture.	Breach and attack simulation is not part of regular SOC operation , It comes under advance ,Breach and Attack Simulation (BAS) Tools enable organizations to gain a deeper understanding of security posture vulnerabilities by automating testing of threat vectors such as external and insider, lateral movement, and data exfiltration etc, Hence need to understand the frequency and Volume of This particular requiremnet , We also request OIL to provide details of primetre Security/Email Security Solution to offer BAS solution. **Justification:** We request OIL to provide deep understanding for below: BAS and red teaming is not part of regular SOC operation hence need to understand The exact requirement/Frequency and Volume to size the requirement, Which will help	The scope for Attack Simulation and Assessments under Expanded SOC Operations shall be the entire CSOC constituency. Other modalities like boundaries & limitations for red teaming activities shall be decided mutually by OIL and MSSP for each exercise during contract execution.

				MSSP to bid a relevant techno commercial	
12	64	Terms and Condition: XIV / point a to f for IR services	Whenever OIL feels that Contractor's IR team must be present onsite for IR and remediation activities during major security incidents, the following procedure shall be followed:	Need to clarify do we need to submit and documentary evidence at apart from report and Bill at the time of billing for IR services	Please be guided by pt. xiv of 3.5.2 Terms & Conditions in in the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)).
13	64	Qualification and skill requirement of the deployed human resources for the CSOC solution is as per the following table. Ii Shared L3 SOC analyst and SOC Manager:BE/B-Tech/MCA • Minimum 10 years of experience in working in SOC operations and incident response	We request OIL to provide relaxation and add certifications like CISA and CEH or equivalent		No Change

		• Professional certification: Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) or OSCP •Incident Coordination •Fly-Away Incident Response •Threat Hunting •Attack Simulation and Assessments • Cybersecurity Exercises SOC Manager •BE/B-Tech/MCA			
14	89	13.0 PERFORMANCE SECURITY:	PERFORMANCE SECURITY: 10% of Annualized Contract value. Validity of the performance security / contract performance guarantee shall be valid for 03 (three) months beyond the contract period.	We request OIL to lower the performance security amount 2 to 3 % of yearly billing	No Change
15		Functional Specifications of	ii)The proposed solution should have central data repository which should act as common	Requesting Dept to consider MACHINE LEARNING AND	

		the CSOC solution	data lake (Security Big Data Lake) for SIEM and UEBA to avoid maintaining multiple data repositories. iii)The solution shall work by leveraging the Security Big Data Lake along with machine learning technology to deliver advanced threat detection beyond rules and signatures, automated incident response, incident analysis, customized security intelligence & Threat/Vulnerability advisories, as one solution.	ARTIFICIAL INTELLIGENCE instead of BIG DATA LAKE. Justification: Big data concept has been phased out 2 to 3 years back and MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE is the latest	Shall deliver and issue amendment if needed.
16					

J. Bidder's Name: **M/s. TATA Advanced**

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1.	2.	2.1.1 PQC	Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company.	We are assuming that experience of On-Premise SOC/SIEM implementation and support will be considered. Please confirm.	Acceptable

2.	2.	2.1.3 PQC	The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender.	For wider participation, request to amend the clause as below:- The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution ~~leveraging Big Data Analytic Platform and machine learning~~ for at least one year reckoned from the original bid closing date of this tender.	Shall deliver and issue amendment if needed.
3.	2.	2.1.3 PQC	In support of substantiating the above experience, the bidder must submit copies of relevant pages of the Contract(s) executed showing detailed address(es) of client(s), scope of work along with any of the following documentary evidence to substantiate the above-mentioned experience: (i) Completion certificate(s) issued by the client(s) (OR) (ii) Certificate(s) of Payment issued/acknowledged by the client(s) (OR) (iii) Any other document(s) which substantiate the aforesaid	We are assuming that Work Order/Purchase order with Invoice copy will be acceptable against the mentioned point. Please confirm.	Only WO/PO with Invoice copy will not suffice to the requirement. Please be guided by the subject Clauses of the tender.

			experience criteria as defined above in PQC Clause No. 2.1.3.		
4.	2.	2.1.4 PQC	The bidder must be operating SOC in India for at least last 5 years reckoned from the original bid closing date of this tender with minimum EPS handling of 1000 EPS. In support of substantiating the above experience, the bidder must submit copies of relevant pages of the Contract(s) executed showing detailed address(es) of client(s), scope of work along with any of the following documentary evidence to substantiate the above-mentioned experience: (i) Completion certificate(s) issued by the client(s) (OR) (ii) Certificate(s) of Payment issued/acknowledged by the client(s) (OR) (iii) (iii) Any other document(s) which substantiate the aforesaid experience criteria as defined above in PQC Clause No. 2.1.4.	We are assuming that Work Order/Purchase order with Invoice copy will be acceptable against the mentioned point. Please confirm.	Only WO/PO with Invoice copy will not suffice to the requirement. Please be guided by the subject Clauses of the tender.
5.	3	2.1.7 PQC	The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 2 certified and shall have to furnish copies of the same.	For Wider participation, request to amend the clause as below:- The bidder must be ISO 27001:2013 (or later) or ISO 20000-1:2011 (or later) or SOC 2	Shall deliver and issue amendment if needed.

				Type 2 certified and shall have to furnish copies of the same.	
6.	3	Notes to clause 2.1.1	"SIMILAR Work" mentioned above means, 'Experience in successful completion of establishing and operating Cybersecurity Operations Center (CSOC)'.	We are assuming that experience of On-Premise SOC/SIEM implementation and support will be considered as similar work. Please confirm.	Acceptable
7.	4	Notes to clause 2.1.1	Only Letter of Intent (LOI) / Letter of Award (LOA) and/ or Work Order(s), Job Completion certificate are not acceptable as evidence of experience. However, if Letter of Intent (LOI) / Letter of Award (LOA) and/ or Work Order(s) are issued from OIL, then the same will be considered as evidence subject to successful verification with OIL's own records of execution.	In Govt. Procurement, LOI and Purchase Order/Work Order are issued post RFP award. Please clarify the expectation here.	Clarified. The aforesaid Clause is self-explanatory
8.	30	PQC	ANNEXURE-C; Sample Format of authorization letter from OEM	Kindly remove this format as most of the OEM's issue authorization in standard legal approved format.	No Change. Note: OEM's approved format covering & complying to all the points as mentioned in ANNEXURE-C shall be accepted.
9.		SOW & SCC of STC	Payment Terms	Request to amend as below:- For Licenses- 100% against Delivery Installation & Training:- 100% against installation & Traninig Manpower-Quaterly in arrears.	No Change.

K. Bidder's Name: **M/s. TCL**

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1.	1	Special Terms and Conditions (STC) - Section 1 GCC - Applicability - Clause 1.1	Applicability All clauses in the General Conditions of Contract [GCC] shall apply to all transactions except as otherwise stated in the Special Conditions of Contract [SCC] and/or BEC-BRC. Furthermore, in the event if there is any conflict between the Principal text of the Agreement and the Appendixes, the Principal text will prevail.	Need clarifications on BEC-BRC	**Clarified**
2.	3	Bid Document	Scope of Work link takes us to both General Conditions of Contract (GCC) and Special Conditions of Contract (SCC)	whether the Special Conditions of contract forming part of Scope of work link is same as the Special conditions of Contract stated in Special Terms and Conditions. The document Special Terms and conditions (STC) has both GCC and SCC. Please clarify	Please note that Scope of Work (SOW) link only leads to SCC of the subject tender. However, STC (Special Terms & Conditions) consists both of GCC & SCC.
3.	10 of 45	Scope of Work - Special Conditions of contract (SCC) - 3.5.2(iii)	OIL reserves the right to audit the CSOC solution for evaluation of effectiveness by OIL appointed 3rd party auditor as and when OIL feels necessary during the period of the contract. The Contractor shall co-operate with the auditor and provide	We propose to limit the frequency of audit to once a year with due notice of 30 days to be issued to us. We also request that the cost of audit be borne by OIL. We would also not be in a position to permit our partners/vendors to execute	Shall deliver and issue amendment if needed.

			the requested details/documentation pertaining to the solution.	tools or run scripts in our infrastructure.	
4.	31 & 32 of 45	Scope of Work - Special Conditions of contract (SCC) - Clause 8	Penalty terms - Non Performance Deductions	We propose applicable credit allowances pursuant to the applicable Service schedule as your sole remedy for damages arising out of or relating to any act or omission relating to the provision or failure to provide services .	No change
5.	39 of 45	Scope of Work - Special Conditions of contract (SCC) - Clause 16	16.18, 16.19 & 16.29 - compensation/ penalties applicability during the scenarios stated in these clauses.	We propose to limit for all liabilities a cap not exceeding 12 months of charges collected by us pursuant to the applicable Purchase Order /Order giving rise to the said liability	No Change.
6.	11 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 12.4.8	Claim for payment of GST / Statutory variation, should be raised within two [02] months from the date of issue of 'Government Notification' for payment of differential (in %) GST, otherwise claim in respect of above shall not be entertained for payment of arrears.	We propose to suggest any claim for payment of GST/Statutory variation should be raised within the period permissible by applicable laws.	No Change.
7.	15 to 16 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 15	Liability	We propose to modify this clause to :- Each Party shall indemnify the other from and against any claims by third parties (including any	No Change

				Governmental Authority) and expenses (including legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such Party's negligence or wilful misconduct.	
8.	16 to 17 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 16	Limitation of Liability	We propose to modify this clause to :- Notwithstanding any other provisions to the contrary, neither party shall be liable for (i) any indirect, incidental, special, consequential exemplary or punitive damages or (ii) 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 other performance of failure to perform under this RFP, whether or not caused by the acts of or omissions or negligence of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. Contractor shall in no event ne liable in an amount that exceeds, in the aggregate for	No change

				all such liabilities, the most recent 12 months of charges collected by it pursuant to the applicable PO/Order giving rise to the liability	
9.	17 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 18	Consequential Damage	We propose to modify this clause to :- Notwithstanding any other provisions to the contrary, neither party shall be liable for (i) any indirect, incidental, special, consequential exemplary or punitive damages or (ii) 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 other performance of failure to perform under this RFP, whether or not caused by the acts of or omissions or negligence of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages.	No Change.
10	17 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 19	Risk Purchase	Product team/ Commercial Ops team to assess this clause	No Change
11	18 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 20	Indemnity Agreement	We propose to modify this clause to :- Each Party shall indemnify the other from	No Change

				and against any claims by third parties (including any Governmental Authority) and expenses (including legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such Party's negligence or wilful misconduct.	
12	18 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 22	Royalty Patents	We would like to retain the indemnification obligation cast upon Company. However we propose include the below mentioned clause :- In the event of a third party claim of intellectual property infringement, Contractor may, at its sole option, (i) obtain for Company the right to continue using the Services, (ii) modify the Services so that the Services are non-infringing, (iii) replace the Services with a functionally equivalent, non-infringing service, or (iv) if the alternatives above are not available, Company may so notify Customer and terminate such infringing Services without penalty to either Party. Notwithstanding anything in this Agreement to the	No Change

				contrary, this Section is Company's sole and exclusive remedy for any intellectual property infringement claims.	
13	19 to 20 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 26	Confidentiality, Use of documents and Information	We propose to make this applicable to both Contractor and Company.	No Change
14	23 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 30	Timely Mobilization and Liquidated damages	We propose applicable credit allowances pursuant to the applicable Service schedule as your sole remedy for damages arising out of or relating to any act or omission relating to the provision or failure to provide services.	No Change
15	24 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 32	Set-off	We propose the deletion of set off against other contracts.	No Change
16	25 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 34	Applicable Laws	We propose exclusive jurisdiction of Courts in Mumbai.	No Change.
17	26 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 35	Labour Laws	We propose to modify that Contractor would comply with labour laws that are applicable to it.	No Change.
18	30-31 of 83	Special Terms and Conditions (STC) - Section 1 GCC - Clause 42	Settlement of Disputes	We propose the appointment of Sole Arbitrator to be done both by Company and Contractor and not just Company. Also, we propose the seat of Arbitration at Mumbai.	No Change.
19	35 of 83		Notwithstanding any provisions herein to the	We propose deletion of 44.9 clause. We also propose	No Change.

		Special Terms and Conditions (STC) - Section 1 GCC - Clause 44	contrary, the Contract may be terminated at any time by the COMPANY on giving 30 (thirty) days written notice to the CONTRACTOR due to any other reason not covered under the above Article from 44.1 to 44.8 and in the event of such termination the COMPANY shall not be liable to pay any cost or damage to the CONTRACTOR except for payment of services as per the Contract upto the date of termination.	Contractor should also be in a position to terminate for breaches on part of Company.	
20	1 of 2	Service Level Agreement	WHEREAS, the Contractor has furnished to Company the performance security in the form of _____ for ₹ _____ (being 3% of annualized Contract value).	Need clarity on the percentage of Performance Security.	To read the Performance Security in SLA as 10 % of Annualized Contract Value in lieu of the existing. May refer to the Performance Security Clause in Forwarding Letter/ SCC etc. of the tender
21	Proforma XV	Any other document as per specific requirement of Buyer 1 & Buyer 2	Proforma XV deals both with Form of Bid Security (Bank Guarantee Format) & Integrity Pact	Would request clarity on the same proforma reference number.	Proforma-XV is for IP) Integrity Pact) whereas Proforma-VIII is the form of Bid

					Security Format of the tender.
22	29/45	7.3.4 SLA matrix		We would like to propose the following SLA's Security Notification P1,P2,P3 - 30,60,120 minutes respectively Security Event Updates P1,P2,P3 - 2,4,8 hours respectively	No Change
23	41/83	Special Conditions of Contract, Paragraph 3.1	The RPO and RTO for the SOC solution shall be 0 hours and 4 hours respectively.	The RTO of archival data from offline to online will be dependant on the EPS / Storage Volume. While 4 hours is okay for upto 5000 EPS this will need to be revised once the EPS count scales upto 20000. This clause needs to be amended to RTO of 4 hours for upto 5000 EPS only.	Shall deliver and issue amendment if needed.
24	9	1691238015	Dark Web Monitoring and Anti-rogue Services	For sizing dark web monitoring please share the below sizing parameters: 1. No of domains 2. No of Social Media Links 3.	Maximum number of takedown requests during the contract period: 50
25	9	1691238015	Dark Web Monitoring and Anti-rogue Services	Are there any Digital asset file to be monitored.	Please be guided by the relevant scope of work mentioned in the tender.
26	9	1691238015	Dark Web Monitoring and Anti-rogue Services	Do OIL India needs the below:	Please be guided by the relevant scope of work

				Data Loss Recovery – Dark Web Monitoring Monitoring of the Dark and Deep web and other repositories to identify and recover stolen assets including compromised such as compromised credentials, accounts, credit cards, leaked data, hacking tools, leaked source code and indicators of compromised	mentioned in the tender.

L. Bidder's Name: M/s. INSPIRA

Sl. No.	**Page No.**	**Section**	**Tender Clause**	**Clarification Sought/Recommendations**	**OIL's Response**
1.	2	PRE QUALIFICATION CRITERIA (PQC) Point 2.1.3	The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution **leveraging Big Data Analytic Platform** and machine learning for at least one year reckoned from the original bid closing date of this tender.	Requesting for Modification of the Clause as : The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company / Private Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution for at least one year	Shall deliver and issue amendment if needed..

				reckoned from the original bid closing date of this tender. **Justification:** For wider participation	
2.	3	PQC Point 2.1.8	(d) Location address, contact person name / email / phone number for DC and DR **locations of SOC datacentre** on company's letterhead, duly signed by authorized signatory / Company Secretary.	Requesting for Modification of the Clause as : The bidder must provide the SOC services from MeitY empanelled cloud service providers having their DC and DR in India. **Justification:** This existing clause is only allowing "Datacentre/Telco Service Provider" to participate in this bid	Shall deliver and issue amendment if needed.
3.	2	Scope of Work; 3. Solution Sizing, Point vi. SOAR	Minimum 2 concurrent user license **with no limitation on creation of number of user accounts.**	Requesting for Modification of the Clause as : Bidder SOAR license must be provisioned with minimum 2 concurrent user from day 1 of the services. **Justification:** For wider participation	Shall deliver and issue amendment if needed.
4.	25	5.4 SOAR (Security Automation Orchestration, and Response), Point xi	SOAR should have minimum 2 concurrent user license **with unlimited action and without any limitation on creation of number of user accounts**	Requesting for Modification of the Clause as : Bidder SOAR license must be provisioned with	Shall deliver and issue amendment if needed.

				minimum 2 concurrent user from day 1 of the services. **Justification:** For wider participation	
5.	14	3.5.4 Report Management and Communication	Priority Level - Reporting Criteria 1 (Critical) – On detection - **immediate** 2 (High) – On detection - **immediate**	1 (Critical) – this should be within 15 min 2 (High) – this should be within 30 min **Justification**: there will be a parameter to respond	No Change
6.	32	Scope Of Work (9. Payment Terms, Point 10)	Onsite IR and Remediation services, Man Hours 5000	Request for clarification : Any onsite efforts under MSSP Scope is inclusive in IR Services ? or Not, please specify	Please be guided by the scope of work as mentioned in the tender.
7.	3	PQC	(b) The proposed SOAR solution must be operational in at least five SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender.	Requesting for Modification of the Clause as : (b) The proposed SOAR solution must be operational in at least 2 SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender **Justification:** For wider participation	No Change
8.	25	PQC; ANNEXURE-B, Point 67	The solution shall be able to assign risk score for various identified entities based on the threats or	Requesting for Modification of the Clause as : The solution shall be able to assign risk score / risky	No Change

			correlations that particular entity has contributed.	behaviour for various identified entities based on the threats or correlations that particular entity has contributed. Justification: For wider participation	
9.	Page 23, Scope of Work	5.3, Point iii.	The solution shall be able to assign risk score for various identified entities based on the threats or correlations that particular entity has contributed.	Requesting for Modification of the Clause as : The solution shall be able to assign risk score / risky behaviour for various identified entities based on the threats or correlations that particular entity has contributed. Justification: For wider participation	No Change
10.	Page 27, PQC	ANNEXURE-B, Point 78	The solution shall have Case management capabilities i.e. the SOAR platform shall be used as end-to-end incident management, incident response, incident remediation, investigation platform and single evidence repository. The platform shall be capable to provide detailed post incident documentation about all the actions taken, root cause, controls implemented etc.	Requesting for Clarification : Case management should complement the SOAR platform, for end-to-end incident management, incident response, incident remediation, investigation platform and single evidence repository. SOAR platform with Case management shall be capable to provide detailed post incident documentation	No Change

				about all the actions taken, root cause, controls implemented etc.	
11	24	5.4, Point vii.; Scope of Work	The solution shall have Case management capabilities i.e. the SOAR platform shall be used as end-to-end incident management, incident response, incident remediation, investigation platform and single evidence repository. The platform shall be capable to provide detailed post incident documentation about all the actions taken, root cause, controls implemented etc.	Requesting for Clarification : Case management should complement the SOAR platform, for end-to-end incident management, incident response, incident remediation, investigation platform and single evidence repository. SOAR platform with Case management shall be capable to provide detailed post incident documentation about all the actions taken, root cause, controls implemented etc.	No Change
12	9	Scope of Work (Vulnerability Management)	3.5 Managed Security Services Provider (MSSP) services for the CSOC solution 3.5.1 Scope:	Request for clarification : 1. Total Number of Asset count 2. Asset breakup 3. Is the solution to be deployed onsite or remote will be fine? 4. How often will vulnerability scans be conducted for different assets (e.g., daily, weekly, monthly)?	Please refer to Notes of vulnerability management in Page No 9 of the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)). Please refer to 4.1 & 4.2 in the same document for

				5. Will there be regular scans and also on-demand scans for specific situations? **Justification:** this above data is required effort estimation and sharing the required commercial.	asset count & asset breakup. Vulnerability scans will be conducted on regular basis at a predetermined frequency decided during project execution. On-demand scans should be done for specific situations, as and when required.
13	8 & 9	Scope of Work (Attack Simulation and Assessments)	3.5 Managed Security Services Provider (MSSP) services for the CSOC solution 3.5.1 Scope:	Request for clarification: 6. Are there specific scenarios or attack vectors you want the red team to focus on? 7. Which systems, applications, networks, or physical locations will be included in the red teaming exercise? 8. Will the red team focus on a specific part of the infrastructure or conduct a comprehensive assessment? 9. What are the boundaries and limitations of the red teaming exercise? 10. Will the red team include physical security	The scope for Attack Simulation and Assessments under Expanded SOC Operations shall be the entire CSOC constituency. Other modalities like boundaries & limitations for red teaming activities shall be decided mutually by OIL and MSSP for each exercise during contract execution.

				assessments or social engineering attacks? 11. What types of penetration testing will be conducted (e.g., external network testing, internal network testing, web application testing, wireless network testing)? 12. Total Asset count and breakup for penetration testing **Justification:** this above data is required effort estimation and sharing the required commercial.	
14	Page 3	PRE QUALIFICATION CRITERIA (PQC)_ 2.1 TECHNICAL REQUIREMENTS: Point 2.1.5	(b) The proposed SOAR solution must be operational in at least five SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender.	Requesting for Modification of the Clause as : (b) The proposed SOAR solution must be operational in at least 5 SOC implementations for global customers for the last 2 years reckoned from the original bid closing date of this tender. Justification: For wider participation	No Change
15	3	PQC, 2.0 TECHNICAL EVALUATION CRITERIA, 2.1.7	The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 2 certified and shall	Requesting for Modification of the Clause as :	No Change

			have to furnish copies of the same.	The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 2 certified with CMMISVC /5 and shall have to furnish copies of the same. **Justification:** The bidder selection criteria along with the ISO certificate and CMMISVC /5 will benefit to choose a bidder having quality and efficiency of their existing service processes with set of best practices for continuous improvement.	
16	Page 1 File name Pre Qualification Criteria (PQC) etc if any required	1.1 ELIGIBILITY CRITERIA:_PQC	The bidder must be incorporated in India and must maintain more than 20% local content (LC) for the offered services to be eligible to bid against this tender. Regarding calculation of local content and submission of documents during bidding & execution of contracts, provision of Purchase preference under Public Procurement (Preference to Make in India) Order, 2017 of Department for Promotion of Industry and Internal Trade (DPIIT), Govt. of India and as amended time to time with modifications as notified vide	As per MII guidelines laid by meity Reference No DPIIT Notification No P-45021/2/2017-(BE-II) dated 16.09.2020 Revised on 16th November 2021 no:- A-1/2021-FSC-Part(5) Page 8 (7) it is clearly mentioned that the services such as transport, insurance, installation and commissioning, training and after sales services support like AMC/ CMC etc. shall not be considered as local value addition. Bidders offering imported products will fall under the	No changes. May please refer to the relevant PQC Clause of the tender.

			MoPNG Order No. FP-20013/2/2017-FP-PNG-Part (4) (E-41432) dated 26th April 2022 (including subsequent amendments thereof, if any) shall be applicable. If such local content is not maintained during execution of contract, OIL reserves the right to invoke the Performance Securities submitted by the bidding and supporting companies, in addition to resorting to other options as may be deemed appropriate. Whether or not the bidders want to avail PPP-MII benefit against this tender, it is mandatory for them to meet the following at the bidding stage: (a) Without specifying the unit rates and bid amount in the technical bid, the bidder must specify the percentage (%) of local content in their bid as per format prescribed in PROFORMA-XVI (duly signed & sealed by the Power of Attorney holder), without which the bid may be rejected being non-compliant. Such undertaking shall become a part of the contract, if awarded.	category of Non- Local suppliers. As this is a managed SOC bid, no product is involved and we are an Indian Organization with our managed SOC (DC & DR) located in India. In that case local content percentage is 100% . What documentary evidence we have to provide to justify this clause. Requesting honourable tendering committee to clarify on this point.	

			(b) The aforesaid undertaking of the bidder shall also be supported by a certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of other than companies) giving the percentage of local content. (c) Alongwith the technical bid, bidder must submit a copy of their Certificate of Incorporation/Registration or any other valid document(s) which substantially establishes its constitution in India		
17	3	PQC_2.1 TECHNICAL REQUIREMENTS: Point 2.1.5	(b) The proposed SOAR solution must be operational in at least five SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender.	Requesting for Modification of the Clause as : (b) The proposed SOAR solution must be operational in at least 2 SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender Justification: For wider participation	No Change
18	Page 2	Point 2.1.3 of PQC_2.0 TECHNICAL	The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization	Requesting for Modification of the Clause as :	Shall deliver and issue amendment if needed.

		EVALUATION CRITERIA: 2.1 TECHNICAL REQUIREMENTS:	/ Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender.	The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company / Private Limited Company only) to whom they are currently providing managed SOC services using the SIEM solution for at least one year reckoned from the original bid closing date of this tender. Justification: For wider participation	

M. Bidder's Name: **M/s. SISA**

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1.		PQC	ANNEXURE-B	Is it expected by Vendor/Partner to deploy Hardware's to support MDR/SIEM Solution at OIL Premises? Does Vendor/Partner has to include the Hardware cost in the Proposal?	Please refer to 3.1 Provisioning of the Technology Components in the 1691238015.pdf document (SPECIAL CONDITIONS OF CONTRACT (SCC)).
2.		SOW (5. X)	Logical Data Segregation: The proposed solution must	Please share the list of Teams/Departments which	Here the operating teams mean different

			provide logical segregation of log data that can be viewed by different teams. Various operating teams can only see “their” device event data which provides separation of duties.	requires segregation of Users/Assets.	teams working in the MSSP.
3.		SOW (5.3.1)	The solution should have user behaviour analytics for minimum 7500 users and UEBA to monitor at least 1000 Entities/ Users.	What is meant by “Entities”? , could you please share the details	Here entity refers to the industry-standard definition of "entity" in UEBA which include but are not limited to, routers, servers, applications, and other network devices etc.
4.		SOW	Incident resolution would require Forensic expertise, hence request that Forensic capabilities be also added in SoW	Vendor/Partner should be a known Forensic Investigator	No Change
5.		PQC (1.1)	The bidder must be incorporated in India and must maintain more than 20% local content (LC) for the offered services to be eligible to bid against this tender	With increased focus of Govt of India on 'Make In India', We request that Local Content should also be increased in the PQC. Increase Local Content (LC) to at least 50%	No change. Please be guided by the relevant Clause as mentioned in the tender document.
6.		PQC (2.1)	Bidder must have experience of successfully completing at least one SIMILAR work of value Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred) only in previous 07 (seven) years reckoned from	We request that along with PSUs / Central Government / State Government Organization / Public Limited Company, OIL should also consider all enterprises including pvt limited companies. All	No change

			the original bid closing date with PSUs / Central Government / State Government Organization / Public Limited Company	enterprises in India to be included	
7.		PQC (2.1.3)	The bidder must have minimum two (02) customers (PSUs / Central Government / State Government Organization / Public Limited Company only) to whom they are currently providing managed SOC services using the proposed SIEM solution leveraging Big Data Analytic Platform and machine learning for at least one year reckoned from the original bid closing date of this tender.	We request that along with PSUs / Central Government / State Government Organization / Public Limited Company, OIL should also consider all enterprises including pvt limited companies. All enterprises in India to be included	No change
8.		PQC (2.1.7)	The bidder must be ISO 27001:2013 (or later), ISO 20000-1:2011 (or later) and SOC 2 Type 2 certified and shall have to furnish copies of the same.	Organizations which are in the process of SOC 2 Type 1 should also be considered as Type 2 will be reviewed only after 6 months of completion of Type 1. ISO 27001 is fine. However instead of ISO 20000, IS 9001 may be included. Organizations which are in the process of SOC 2 Type 1 should also be considered as Type 2 will be reviewed only after 6 months of completion of Type	Shall deliver and issue amendment if needed.

				1. ISO 27001 is fine as it talks about ISMS policies. However instead of ISO 20000, IS 9001 may be included as it focuses on Quality Management.	
9.		PQC (2.2.1)	Annual Financial Turnover of the bidder in any of preceding 03 (three) financial / accounting years, reckoned from the original bid closing date should be at least **Rs. 3,63,50,100.00 (Rupees Three Crore Sixty-Three Lakh Fifty Thousand One Hundred)** only.	Annual Turnover should be at least 30 Crores. Also, organisation should be in the cybersecurity business for a minimum 10 years in India to provide best services/support to Oil India.	No Change.

N. Bidder's Name: **M/s. GOOGLE CLOUD**

Sl. No.	Page No.	Section	Tender Clause	Clarification Sought/Recommendations	OIL's Response
1.	3	PQC_ Clause 2.1.8 (E)	An Undertaking on company's letterhead, duly signed by authorized signatory/ Company Secretary stating that their data shall never move outside India for any purpose.	Are you ok to accept solution which shall be provided from India before the deployment for the project begins. The solution shall be provided from India or shall not move out of India . For all solutions where this provision is in progress , they are to confirm that the same shall be provided before Purchase order /supply order is awarded to them.	The Contractor shall be responsible for ensuring that all data, data functions and processing are performed within the boundaries of India. This will be applicable once the solution gets deployed for Oil India Limited.

2.	3	PQC, Clause 2.1.5 (A & B)	The proposed SIEM solution must be operational in at least ten SOC implementations in India for the last 5 years reckoned from the original bid closing date of this tender. (b) The proposed SOAR solution must be operational in at least five SOC implementations in India for the last 2 years reckoned from the original bid closing date of this tender.	Are you ok to accept solution which shall be provided from India before the deployment for the project begins. The solution shall be provided from india or shall not move out of India . For all solutions where this provision is in progress , they are to confirm that the same shall be provided before Purchase order /supply order is awarded to them.	The Contractor shall be responsible for ensuring that all data, data functions and processing are performed within the boundaries of India. This will be applicable once the solution gets deployed for Oil India Limited subject to the condition of fulfilling other tender requirements.
3.	63	STC_Clause No 5.5 TIP (Threat Intel Platform)	TIP must have active subscription to minimum one premium threat intel feed (like but not limited to: CrowdStrike Falcon, Talos etc.) during the entire duration of the contract	There are no dedicated specifications for Threat Intelligence feed. In RFP it mentions "one Premium Threat Intel feed". Please elaborate "Premium" as this word is very generic and no benchmark is associated to it. We would request OIL India to have dedicated Threat Intelligence feed specifications as part of this RFP. Suggestions: We recommend to include the below Threat Intelligence	Shall deliver and issue amendment if needed.

				Feed specifications as a part of this RFP 1) The provider should be in the leader quadrant under the Forrester "External Threat Intelligence Services" in last three reports release. 2) Threat Intel provider must have more than 15 years of threat intelligence collection experience, analysis and tracking of threat groups 3) The Threat Intel provider must provide browser extension/plug-in to perform lookups from within the browser for Threat Intel search. 4) The Threat Intel provider must have the capability of Curation of trending cyber threat news on a daily basis through the vendor's threat analysts'. Analysis to confirm the validity of the news, and reference to similar past intelligence reports. 5) Threat Intel feed provider must be experienced in	

				direct observations via incident response engagements and access to the sensors that observe threat activity. 6) Threat Intel provider must have Intel collection of more than 180+ intelligence analysts across the globe speaking 30+ languages. 7) Threat Intelligence feed should be integrated with SIEM,SOAR,TIP via an API. 8) The proposed TI should have an in-built sandboxing/File Analysis feature, without the need to partner or bundle with third party/external sandboxing vendors. 9) The proposed TI feed solution should not be an product operating in silo and should be part of a platform which helps it to be plugged into other modules that help operationalize Threat intel when required, including the option of running the active TTPs of the Threat actor in live environment for validation	

				of security controls to test the security effectiveness. 10) The portal should include a minimum of at least 20 portal login accounts and there should not be any limitation on it.	
4.	46	STC_ clause 3.5 "Managed Security Services Provider (MSSP) services for the CSOC solution" Clause Name : Attack Simulation and Assessments	Performing red teaming, penetration testing, adversary emulation, purple teaming, breach and attack simulation, or other testing detections with the goal of improving SOC operations and the constituency's overall defensive posture.	Contractor is required to provide an on-premise attack simulation platform and should be able to run all simulations as and when required during the contract period. Contractor to bring the required hardware for the platform 1) The platform must include attacks for malware, ransomware, and other technical-oriented malicious activity 2) The platform must include attacks for adversary tactics, techniques, and procedures. 3) The platform must include attacks from nation-state and espionage threat groups and actors.	No Change

				4) The platform must include attacks for network reconnaissance, probes, and scanning activities 5)The platform must include attacks that tunnel through common protocols. 6) The platform must include attacks for living off the land techniques 7)The platform must include attacks for spear phishing techniques 8) The platform must include attacks that take advantage of common application vulnerabilities 9) The platform must support attacks running against production and validation-specific systems and networks. 10) The platform must support attacks across the security controls (Endpoint,Perimeter,Email)of the organization 11)The platform must support the ability of users	

				to define the specific path of the attack. 12) The platform must support the ability to test real queries to malicious URLs and for malicious DNS names without those queries reaching the adversary servers. 13)The platform must execute attacks safely in ways that should not affect other excluded systems or networks 14) The platform must include attack library search filters by attack vector, behaviour, control, and operating system 15) The platform must support the ability for users to execute an attack once or on a user-defined periodic and ongoing basis 16) The platform must include usecase for SIEM optimization, DLP validation, for live production exercises, proactive adversary attack	

				preparation, red teaming, purple teaming 17) The platform should be capable to emulate the latest TTP's leveraged by attackers, malwares as seen in threat intelligence feeds.	
5.	46	STC_under the clause 3.5 "Managed Security Services Provider (MSSP) services for the CSOC solution" Clause Name : Cybersecurity Exercises	Formulating and facilitating cybersecurity scenario based simulations and exercises, such as mock critical severity incidents.	In RFP the scope for " Cyber Security Exercises" is an open ask which is not specific to the scope of the mock exercises.. We would request OIL India to incorporate the specific details of the "CyberSecurity Exercises" testing via attack emulation platform. Contractor is required to provide an on-premise attack simulation platform and should be able to run mock attacks as part of cybersecurity exercises as and when required during the contract period. Contractor to bring the required hardware for the platform 1) The platform must include attacks for malware, ransomware, and	No Change.

				other technical-oriented malicious activity 2) The platform must include attacks for adversary tactics, techniques, and procedures. 3) The platform must include attacks from nation-state and espionage threat groups and actors. 4) The platform must include attacks for network reconnaissance, probes, and scanning activities 5)The platform must include attacks that tunnel through common protocols. 6) The platform must include attacks for living off the land techniques 7)The platform must include attacks for spear phishing techniques 8) The platform must include attacks that take advantage of common application vulnerabilities	

				9) The platform must support attacks running against production and validation-specific systems and networks. 10) The platform must support attacks across the security controls (Endpoint,Perimeter,Email)of the organization 11)The platform must support the ability of users to define the specific path of the attack. 12) The platform must support the ability to test real queries to malicious URLs and for malicious DNS names without those queries reaching the adversary servers. 13)The platform must execute attacks safely in ways that should not affect other excluded systems or networks 14) The platform must include attack library search filters by attack vector, behavior, control, and operating system	

				15) The platform must support the ability for users to execute an attack once or on a user-defined periodic and ongoing basis 16) The platform must include usecase for SIEM optimization, DLP validation, for live production exercises, proactive adversary attack preparation,red teaming, purple teaming 17) The platform should be capable to emulate the latest TTP's leveraged by attackers,malwares as seen in threat intelligence feeds.	