Sun Petrochemicals Private Limited
8th,9th & 10th Floor, ATL Corporate Park, Saki Vihar Road,
Powai, Mumbai - 400 072, Maharashtra, BHARAT.
CIN: U24219GJ1995PTC028519
Tel: +91 22 69325300, + 91 22 28470484
Website: www.sunpetro.com; Email Id: info.sunpetro@sunpetro.com

No. SunPetro/Bhaskar/Cyber Security/2025-26/SPPL-242/Bulletin-2 **Date: 14.11.2025**

BULLETIN #2

Sub: Supply & Installation of Cyber Security Operation Centre (SOC) at Bhaskar-I Field in Gujarat

Ref: Tender No. SunPetro/Bhaskar/ Cyber Security /2025-26/SPPL-242

Sun Petrochemicals Private Limited (**SunPetro)**, hereby authorized following amendment / clarification in the above referred RFQ/ Inquiry:

	Bidder Query	SunPetro Response
1.	The delivery model is managed SOC services i.e. the devices to be monitored will be integrated with Our Managed SOC Infrastructure.	Yes, Bidder's understanding is correct
2.	The scope of work does not include the deployment of SOC IT Infrastructure on-premises at SunPetro.	Hybrid MSOC Solution Deployment is to be fully managed by Contractor only
3.	The CISO-as-a-Service will be a managed services or continuous onsite deployment?	Hybrid MSOC Solution Deployment is to be fully managed by Contractor only
4.	The various sections defined under the scope in Section-IV 'Responsibility Matrix' are related only to the MSOC infrastructure and not other assets of SunPetro, Especially Sections L/M/N/O/P/Q/R/U/V/W/X/Y/5/A Our assumption is that the above aspects need to be covered only for the Managed SOC Infrastructure on the assets under monitoring.	Hybrid MSOC Solution Deployment is to be fully managed by Contractor only
5.	In Section-VII, Bill of Quantity (BOQ) the point – 'Monitoring Resource (Dedicated SOC Analyst / Engineer) Optional line item if required onsite. For above requirement, rates to be provided for which level resource – L1 or L2 or L3. Please specify.	Hybrid MSOC Solution Deployment is to be fully managed by Contractor only
6.	Kindly mention the EPS of the expected solution, As the OT assets don't have a fixed number of quantities to calculate the EPS, kindly requesting you mention EPS count of the expected solution /exact count of asset.	The EPS Count is 26
7.	Kindly confirm the details of DC, DR & HA mode if required.	DC would be 2, and no DR, HA
8.	Kindly requesting to amend or modify this clause Bidder should have supplied & commissioned at least 2 SOC which are still operational. The OEM used should be the proposed / similar solution. This clause restricts multiple Bidders and OEMs of different make and models to participate in the tender because in each bid or tender, the products quoted regularly will change and the bidder always looks at the best commercial models quoted by the OEM. So, it will be difficult for bidders as well as OEMs to participate in this opportunity.	BEC Condition shall prevail

	Kindly amend this clause that will help multiple Bidders and OEMs to participate in this opportunity, and it helps the customer also to get the best of the products available in the market to cater the requirement	
9.	Would CERT-IN Empaneled would be ok.	CERT-IN Qualified BIDDER & Cert-In Empaneled VAPT
10.	Kindly share the expected manpower structure (L1, L2, L3, SOC Manager, IR Lead) and shift patterns (8x5 / 24x7). If it is hybrid than what are the manpower structure, it. L1, L2, L3 on site and SOC manager, IR resource should be remote and shared.	No Onsight resource
11.	Please confirm if the bidder should provide hardware, software, licenses, and manpower as part of turnkey scope.	Necessary HW & SW license & implementation/ Integration
12.	Is the bidder required to supply new SIEM/SOAR/EDR tools, or integrate with existing SOC infrastructure?	This is the fresh SOC request
13.	Are the existing OT telemetry sources and vendor systems available for integration, or bidder needs to deploy OT sensors?	Bidder to consider necessary sensors
14.	Should the bidder procure and manage threat intelligence feeds (global, industry-specific), or will the client provide them?	Bidder to consider
15.	Are you looking only for Threat feeds or a complete Threat intel platform solution	Complete solution
16.	Is integration with your existing third-party threat intel platforms (MISP, Anomali, ThreatConnect) required?	Yes
17.	Please clarify whether onsite IR team is required, or remote triage and response through SOC is acceptable.	NO Onsight resource
18.	Please clarify if bidder needs to propose a new VAPT and patch management solution, or to integrate with existing systems.	VAPT & Patch management, this is fresh request hence there is not existing system available apart from AV
19.	Kindly confirm if clients will provide OT network visibility tools (e.g., Nozomi, Claroty) or bidder should include them.	Bidder to consider
20.	Please clarify if firewall, VPN, and MFA systems exist, or bidder has to provide them.	SunPetro Scope
21.	Is integration with CCTV, Access Control, and Perimeter Sensors required, and if yes, which OEMs are used?	Bidder to consider OEM: ALCON
22.	Please confirm whether data encryption and backup solutions are within bidder scope or client's existing setup.	Data encryption in Bidders scope / Backup SunPetro scope
23.	Please clarify the frequency and audience (IT, OT, Management) for training & cyber drills.	Half Yearly
24.	Is there an existing IRP (Incident Response Plan) that the bidder should align with, or should a new IRP be developed?	Bidder to consider
25.	Please confirm whether manual proactive hunts are expected daily/weekly or driven by automated XDR workflows.	Auto XDR
26.	Please confirm scan frequency (weekly/monthly/quarterly) and number of IPs in scope.	Weekly, 24/ 9 Segment
27.	Should OT monitoring be passive only or include active testing as per IEC 62443 compliance?	Active
28.	Is there any GRC or ticketing tool (e.g., ServiceNow, RSA Archer) currently in use for compliance reporting?	Yes Bidder to integrate with
29.	Please confirm whether annual phishing simulations or TTX are part of deliverables, and if so, expected count.	Yes Quarterly
30.	Please clarify if the forensic toolkit and evidence storage should be part of bidder's supply.	Yes
31.	Please confirm if the SOC should be active-active or active-passive between primary and DR sites.	no DR
32.	Please specify duration and number of KT sessions expected post-implementation.	FULL DAY 5
33.	Please confirm if the bidder is required to propose a new VAPT and patch management solution, or only to manage and integrate with existing client tools. Also, clarify expected scan frequency and scope coverage.	Bidder to consider Quarterly

34.	Kindly confirm whether an existing CERP framework is in place, or if the bidder should design and implement a new CERT-IN aligned incident response process.	This is the fresh SOC request, Bidder to consider
35.	Please clarify whether the OT telemetry collection tools (e.g., NDR, Data Diode) will be provided by the client or need to be included in the bidder's proposal.	Bidder to consider
36.	Kindly confirm if a forensic toolkit and evidence management system are already available or if the bidder should propose one. Please also specify data retention expectations for forensic artefacts.	This is the fresh SOC request, Bidder to consider
37.	Kindly confirm if the client has an existing framework or checklist (e.g., Cyber-Satark principles) for supply chain risk validation, or if the bidder is expected to develop and operationalize one.	This is the fresh SOC request, Bidder to consider
38.	Please confirm the expected engagement duration, reporting frequency, and whether the virtual CISO service will be required full-time or on an on-demand basis.	Virtual CISO service to be considered as & when required
39.	Kindly confirm how many awareness sessions and TTX exercises are expected annually and whether both IT and OT teams should be covered.	Quarterly
40.	Please clarify if the client has any preferred reporting format or integration with existing GRC/compliance systems.	This is the fresh SOC request, Bidder to consider
41.	Please clarify whether the SOC needs to be deployed in an active-active or active-passive model and whether the DR site will be provided by the client or should be proposed by the bidder.	This is the fresh SOC request, Bidder to consider
42.	Kindly specify the expected SLA values for MTTD/MTTR and whether performance reporting will be required on a monthly or quarterly basis.	Monthly Basis
43.	Please confirm if network cabling and patch panel termination will be handled by the bidder or existing facility team.	SunPetro Scope
44.	Clarify whether network performance-based tools will be provided by the client or should be included in the bidder's proposal.	This is the fresh SOC request, Bidder to consider
45.	Kindly specify whether endpoint security licenses (AV/DLP/EDR) already exist or need to be provisioned under this project.	SunPetro Scope
46.	Please confirm whether SOC operations will continue to be managed by the bidder post-implementation or transitioned to client resources.	Bidder to manage
47.	Please confirm if existing ticketing or case management system will be used or the bidder must provide one.	Bidder to consider integration with existing ticketing tool
48.	Kindly clarify whether proactive threat hunting frequency (daily, weekly, or ad-hoc) should be defined in the proposal.	Daily
49.	Please confirm whether remote incident response is acceptable or on-site support will be mandatory.	Remote response but as & when required on site as well
50.	Kindly confirm the approximate number and types of log sources (servers, endpoints, OT devices, etc.) expected for onboarding.	Mentioned in scope & Bulletin document
51.	Please clarify if bidder must propose a new patch management solution or integrate with existing systems.	This is the fresh SOC request, Bidder to consider
52.	Please specify if bidder should perform VA/PT internally or coordinate with a third-party auditor.	Third party
53.	Kindly confirm whether compliance audits will be conducted by SunPetro or need to be facilitated by the bidder.	Bidders Scope
54.	Please specify the reporting frequency and format required for incident notifications and escalation to regulatory bodies.	Quarterly, This is the fresh SOC request, Bidder to consider
55.	Kindly confirm if bidder is responsible for DR drill execution or only coordination.	This is the fresh SOC request, Bidder to consider
56.	Please clarify whether firewalls/UTMs exist or be newly proposed under this project.	SunPetro Scope
57.	Kindly specify whether existing information security policies will be shared for alignment or bidder needs to draft new ones.	This is the fresh SOC request, Bidder to consider

58.	Please confirm if redundancy is required across multiple physical sites or only within SOC infrastructure.	SOC Infra
59.	Please clarify whether forensic investigation will be performed using existing client tools or bidder's own solution.	This is the fresh SOC request, Bidder to consider
60.	Kindly confirm whether annual maintenance and patching of SOC tools post-implementation are part of bidder's ongoing scope.	This is the fresh SOC request, Bidder to consider
61.	Please confirm expected frequency (quarterly/bi-annually) of cyber drills.	Quarterly
62.	Kindly confirm whether bidder should include both IT and OT assets in the risk assessment scope.	YES
63.	Please confirm whether the client uses any CMDB tool, and if integration is expected with SOC systems.	IN house CMDB, Bidder to consider integration
64.	Kindly confirm the expected frequency of Change Advisory Board (CAB) meetings and bidder's level of participation.	Annually
65.	Please specify the reporting format, KPIs, and delivery mechanism expected (portal/email/dashboard).	Daily over Portal/Email & dashboard
66.	Kindly clarify if continuous improvement reports (CIRs) are to be submitted quarterly or monthly.	Quarterly
67.	Please confirm whether data migration scope includes legacy SIEM/EDR/Firewall data or only configuration migration.	NO SIEM But Bidder to consider fresh SIEM, EDR/DLP/FW data to be considered
68.	Please specify the expected duration and number of knowledge transfer sessions.	5 Full Day session
69.	Please specify whether the UAT criteria will be defined by SunPetro or jointly developed with the bidder.	Jointly
70.	Does this mean, only SIEM and SOAR to be provided by bidder, rest all the tools like AV, EDR, XDR will be provided by Sun petro? Is the scope just to implement this solution or does the bidder need to provide new AV, EDR, XDR	AV/EDR/XDR already in place