रेलटेल
RAILTEL
A Navratna CPSE
Govt of India

RAILTEL CORPORATION OF INDIA LTD
(A Navratna CPSE)

Southern Region Office
6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road,
Prakash Nagar Metro Station,
Begumpet, Hyderabad – 500016

Corporate Office
Plate-A, 6th Floor, Office Tower2,
NBCC Building, East Kidwai Nagar, New Delhi-110023

www.railtel.in

Invitation for Expression of Interest For "SETTING UP A SECURITY OPERATIONS CENTRE (SOC) at KSITM" from empanelled Business Associates"

EOI No: RailTel/SR/ERS/Mktg/2025-26/EOI/06 Dt.13/10/2025

Issued By
RailTel Corporation of India Ltd
Kerala Territory Office, Southern Region,
1st Floor Eastern Entry Tower Ernakulam Junction Railway Station Ernakulam, 682016

Disclaimer

RailTel Corporation of India Ltd. (herein after called the RailTel) has prepared this Expression of Interest (EOI) document solely to assist prospective bidders in making their decision of whether bid or not to bid.

While the RailTel has taken due care in the preparation of information contained herein and believes it to be accurate, neither the RailTel or any of its Authorities or Agencies nor any of their respective officers, employees, agents or advisors give any warranty or make any representations, express or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it. This information is not intended to be exhaustive and interested parties are required to make their own inquiries and do site visits that it may require in order to submit the EOI. The information is provided on the basis that it is non– binding on RailTel, any of its authorities or agencies or any of their respective officers, employees, agents or advisors. The RailTel reserves the right not to proceed with the bidding/EOI process at any stage without assigning any reasons thereof, or to alter the timetable reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the EOI further with any party submitting an EOI. No reimbursement of cost of any type will be paid to persons or entities submitting the EOI

EOI NOTICE

RailTel Corporation of India Ltd.
Kerala Territory Office
1st Floor, Eastern Entry Tower,
Ernakulam South Railway Station,
Kochi – 682016

EXPRESSION OF INTEREST

EOI No RailTel/SR/ERS/Mktg/2025-26/EOI/06 Dt.13/10/2025

RailTel Corporation of India Ltd., (hereafter referred to as RailTel) invites responses from RailTel System Integrator for exclusive PRE-BID TEAMING ARRANGEMENT for Engagement of an Agency for **Selection of the System Integrator for the Supply, Installation and Commissioning of SIEM, SOAR, UEBA, TIP, NDR and the management of State SOC** from empanelled Business Associates".

The details are as under:

1	Date of Floting EOI	13-10-2025
2	Last date for submission of Bids against EOI	16-10-2025 at 15:30 Hours
3	Date of opening of E-Bids	16-10-2025 at 16:00 Hours
4	Number of Packets	Single Stage (Single Packet System)
5	Estimated Value of EOI	Rs.20 cr
6	Portal for Submission of bids	https://railtel.eNivida.com
7	EOI EMD	Token EMD of Rs. 20,00,000.00/- to be submitted along with the EoI in form of BG or in the form of Insurance Surety Bond or Payment through NEFT/RTGS. Advice of the Bank Guarantee (via SFMS IFN760COV) to be sent to advising bank (RailTel's Bank) through SFMS by the issuing Bank (Applicant's Bank), RailTel Corporation of India Limited Account No: 327301010373007, IFSC Code: UBIN0805050, Bank Name: Union Bank of India. Branch address: Union Bank of India, RP Road Branch, Bungalow no 109, New No 1-7-252 to 254 Oxford Street, SD Road, Near Park Lane Center Secunderabad – 500003 No exceptions to startups and MSMEs for EMD.

Note: RailTel reserves the right to change the above dates at its discretion.

Partner needs to share copy in case of EMD in form of BG & in case of online payment partner to share transfer details like UTR No. date and Bank along with the proposal.
Eligible Partners are required to direct all communications related to this Invitation for EoI document, through the following Nominated Point of Contact persons:

Level:1 Contact: Shri. Suvin Varghese, DM/Mktg/ERS
Email: suvinvarghese@railtelindia.com Contact: +91-8075285582

Level:2 Contact: S Shri. M Pazhanivelan, JGM/TM/ ERS
Email: pazhani@railtelindia.com Contact: +91-90031 44207

SPECIAL CONDITIONS OF EOI

1. The EOI response is invited from RailTel's Empanelled Partners and Prospective Partners who have applied before floating of this EoI for Empanelment with RailTel only.
2. Responsibility of getting valid Letter of Empanelment from RailTel will be responsibility of Partner before finalization of this EoI. LoA / PO / Work Order will only be issued on submission of valid letter of empanelment from RailTel.
3. Partners are required to submit soft copy of response through Online on RailTel's e-nivida portal at https://railtel.enivida.com duly signed by Authorized Signatories with Company seal and stamp.
4. All the documents must be submitted with proper indexing and page no.
5. If, the interested partner is OEM/Distributor of OEM/Direct Partner of OEM, it should submit the supporting document for the same.
6. Consortium is Not Allowed
7. This is an exclusive pre-RFP partnership arrangement with empanelled Partner of RailTel for participating in the end customer RFP. Selected partner's authorized signatory has to give an undertaking that they will not submit directly or indirectly their bids and techno-commercial solution/association against tender Ref No mentioned below with any other organization once selected in this EOI for pre-bid teaming arrangement (before and after submission of bid to end customer organization by RailTel). This undertaking has to be given with this EOI Response.
8. Transfer and Sub-letting. The Partner/consortium has no right to give, bargain, sell, assign, or sublet or otherwise dispose of the Contract or any part thereof, as well as to give or to let a third party take benefit or advantage of the present.
9. Partner/Consortium has to agree to comply with all scope of work and terms and conditions including special terms and conditions, SLA and OEM technical & Financial documentation including technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP & its corrigendum (if any) as mentioned below:

Tender Ref. No	CERT-K/9/2025-KSITM
Date of floating	03-Sep-2025
Floated on portal	https://etenders.kerala.gov.in

10. MAF required for submission to end customer by RailTel in their prescribed format (if any) shall be responsibility of the Bidder.
11. Anything not mentioned in the EOI, Customer RFP and its corrigendum (if any) and addendum (if any) may be referred & considered.
12. Selected partner /Lead Bidder from consortium will be responsible for facilitating RailTel to get/collect /prepare all the documentations related to end customer RFP.
13. Affidavit as per Annexure 4 , Pre – Contract Integrity Pact, and Power of Attorney should be submitted in original and hard copy before signing of agreement with RailTel.

Contents

1 : INTRODUCTION

1.1 RAILTEL – INTRODUCTION

RailTel, a distinguished Nav-Ratna Central Public Sector Enterprise under Ministry of Railways, is recognised as one of the nation's most reliable end-to-end Telecom, IT, ICT, Railway Signalling solution provider. With a focus on excellence and innovation, RailTel has garnered unwavering trust as a partner in delivering cutting-edge services across sectors. RailTel is also working towards creating a knowledge society at multiple fronts and has been selected for implementation of various mission-mode projects for the Government of India in the telecom field. With a team of highly skilled and seasoned experts in Telecom, Signalling and IT, along with an extensive nationwide infrastructure, RailTel possesses the ability to deliver digital transformation services across the country and beyond border.

The ongoing wave of digitalisation is creating new prospects for companies like RailTel. In the specific context of the telecom sector, the advent of 5G is a significant growth factor. The demand for network and allied infrastructures is poised to propel RailTel's business forward. With our experience in setting-up and running Tier-3 Data Centres and cloud office, RailTel is implementing Data Centre services like cloud deployments for various customers. Thus by, leveraging RailTel's network infrastructure, data centres, security operation centre and in house capabilities, RailTel is helping in digitalisation by providing comprehensive ICT services. In essence, RailTel's goal is to be a supportive partner in guiding its customers through their Digital transformation endeavours.

For ensuring efficient administration across India, country has been divided into four regions namely, Eastern, Northern, Southern & Western each headed by Executive Director and Headquartered at Kolkata, New Delhi, Secunderabad & Mumbai respectively. RailTel's business service lines can be categorized into three heads namely B2G/B2B (Business to Government and Business to Business) and B2C (Business to customers).

RailTel's various operations are certified for, ISO 27001:2022-Certified for Information Security Management System, ISO 20000-1:2018-Certified for Information Technology Service Management System, ISO 9001:2015-Certified for Quality Management System, ISO 27017:2015 Certified for Information Security for Cloud Services, ISO 27018:2019-Certified for Data Privacy in Cloud Service, ISO 27033-Certified for Network Security, ISO 14001:2015- Certified for Environmental Management System Standard, ISO 17024:2012-Certified for Telecom Services, Railway Signalling & Telecom Training, Design Testing and Licensing Services and CMMI Maturity Level-4-Certified for Process Improvement. The RailTel's Data Centres are Tier-III (Design & Facility) certified.

2 : EOI OBJECTIVE SCOPE OF WORK

2.1 PROJECT BACKGROUND AND OBJECTIVE OF EOI

RailTel intends to participate in RFP floated by end Customer organization for **"Supply, Installation and Commissioning of Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), UEBA, Threat Intelligence Platform, Network Detection & Response Solutions and the management of the State SOC" at State Data Centre 2, Tejaswini Building, Technopark, Thiruvananthapuram for establishing a State SOC."** with Tender No. "**CERT-K/9/2025-KSITM dt. 03-09-2025**".

RailTel invites EOIs from RailTel's Empanelled Partners for the selection of suitable partner for participating in above mentioned work for the agreed scope of work. The empanelled partner is expected to have excellent execution capability and good understanding of customer's local environment.

2.2 SCOPE OF WORK:

The scope of work will be as mentioned in the pertinent end Customer organization Tender for Engagement of an Agency for "**REQUEST FORPROPOSAL (RFP) FOR SETTINGUPASECURITYOPERATIONS CENTRE (SOC)**" with Tender No. "**CERT-K/9/2025-KSITM dt. 03-09-2025**" on https://etenders.kerala.gov.in/ with all latest Amendment/ Corrigendum/ Clarifications. In case of any discrepancy or ambiguity in any clause/specification pertaining to scope of work area, the RFP released by end customer organization shall supersede and will be considered sacrosanct. (All associated clarifications, response to queries, revisions, addendum and corrigendum, associated prime service agreement (PSA)/MSA/SLA also included.)

#Special Note: RailTel may retain any portion of the work mentioned in the end organization RFP, where RailTel has competence so that overall proposal becomes most winnable proposal.

2.2.1 Broder Scope of Work

RAILTEL intends to implement a Next Generation Security Operations Centre (NGSOC) to safeguard the state's information assets across the State Data Centres, Kerala State Wide Area Network (KSWAN), KFON, SecWAN, and to enable integration and mapping of departmental assets and applications as required. The successful bidder will be responsible for delivering comprehensive SOC management services, including the supply, implementation, customization, integration, and management of NG-SOC services throughout the entire contract period of five years. The proposed solution will be hosted on-premise at State Data Centre (SDC2). KSITM will provide the necessary hardware infrastructure, including virtual servers, storage, and the operating system (either RedHat or Ubuntu) required for deploying SOC components. The bidder's scope of work broadly includes:

1. Supply, installation, configuration, and commissioning of SIEM, SOAR, UEBA TIP and NDR solutions
2. Integration of network devices across State Data Centres, KSWAN, SecWAN, and KFON
3. Final acceptance testing, post-implementation training, and Go-Live support
4. Operations and management of the SOC
5. Warranty and product support services

2.2.2 Project Time Schedule

The total duration of the project is for a period of 90 days from the date of release of work order including final acceptance and testing (FAT), training and submission of documentation.

S. No	Activity	Time of Completion
1	Issuance of Work Order	T
2	Kick-off Meeting	T + 7 days
3	Signing of the Contract Agreement	T + 14 days
4	Supply, Installation and Commissioning of SIEM, SOAR, UEBA and NDR	T + 40 days
5	Deployment of manpower for the management of SOC Solution	T + 50 days
6	Integration of Devices with the supplied solution	T + 70 days
7	Documentation, Post-implementation training, Final Acceptance Test (FAT) and Go Live	T + 90 days (T1)
8	Operations and management of the SOC for five years post Go-Live	T1 + 5 years

3 EOI GUIDELINES

3.1 EOI GUIDELINES

3.1.1 Language of Proposals

The proposal and all correspondence and documents shall be written in English only.

3.1.2 RailTel's Right to Accept/Reject responses.

RailTel reserves the right to accept or reject any response and annul the bidding process or even reject all responses at any time prior to selecting the partner, without thereby incurring any liability to the affected partner or Partner or without any obligation to inform the affected partner or partners about the grounds for RailTel's action.

3.1.3 EOI response Document

The partner is expected to examine all instructions, forms, terms and conditions and technical specifications in the bidding documents. Submission of bids, not substantially responsive to the bidding document in every aspect will be at the partner's risk and may result in rejection of its bid without any further reference to the partner. All pages of the documents shall be numbered and signed by the partner including the closing page in token of his having studies the EOI document and should be submitted along with the bid.

Partner has to agree to comply with all scope of work and terms and conditions including special terms and conditions, SLA and OEM technical & Financial documentation including technical certificates/others as per end-to-end requirement mentioned in the end customer's= RFP & its corrigendum (if any) as mentioned below:

Tender Ref. No	CERT-K/9/2025-KSITM
Date of floating	03-Sep-2025
Floated on portal	https://etenders.kerala.gov.in

Anything not mentioned in the EOI, Customer RFP and its corrigendum (if any) and addendum (if any) may be referred & considered.

3.1.4 Period of Validity of bids and Bid Currency

Bids shall remain valid for a period of 180 days from the end of validity of bids to end Customer organization.

3.1.5 Bidding Process

Online mode through RailTel's e-nivida portal. Single packet system.

3.1.6 Bid Earnest Money (EMD)

1. The Partner shall furnish a sum as given in EOI Notice via in the form of BG/DD/online transfer, before submission of final bid to the end customer as given in EOI Notice.
2. Offers not accompanied with valid EOI Earnest Money Deposit shall be summarily rejected.
3. In case of sole partner/ consortium offer is selected for bidding, sole partner/consortium has to furnish Earnest Money Deposit (for balance amount as mentioned in the customer's Bid as and if applicable) for the bid to RailTel. The selected Partner shall have to submit a Bank Guarantee against EMD in proportion

to the quoted value/scope of work to RailTel before submission of bid to end customer as and if applicable.

4. Return of EMD for unsuccessful Partners: EoI EMD of the unsuccessful Partner shall be returned without interest after completion of EoI process.
   Return of EMD for successful Partner: EoI-EMD & Earnest Money Deposit (balance proportionate EMD) if applicable of the successful partner will be discharged / returned as promptly as possible after the receipt of RailTel's EMD/BG from the Customer and or on receipt of Security Deposit Performance Bank Guarantee as applicable (clause no. 6.2) from Partner whichever is later.
5. Forfeiture of EoI EMD or EoI EMD & EMD (balance proportionate EMD) and or Penal action as per EMD Declaration:
   i. The EoI EMD may be forfeited and or penal action shall be initiated if a Partner withdraws his offer or modifies the terms and conditions of the offer during validity period.
   ii. In case of non-submission of SD/PBG (as per clause no. 6.2) lead to forfeiture of EoI EMD, EMD (balance proportionate EMD) if applicable and or suitable action as prescribed in the EMD Declaration shall be initiated as applicable.

3.1.7 Security Deposit / Performance Bank Guarantee (PBG)

In case the bid is successful, the SD/PBG of requisite amount proportionate to the agreed scope of work will have to be submitted to RailTel. Within 14 (fourteen) days after the receipt of notification of award of the Contract from RAILTEL, the successful bidder shall furnish Contract Performance Guarantee to RAILTEL which shall be equal to 5% of the value of the Work Order and shall be in the form of a Bank Guarantee Bond from a Nationalized/Scheduled Bank. The Bank guarantee shall be renewed on annual basis till 60 days beyond the expiry of all the warranty obligations.

3.1.8 Last date & time for Submission of EoI response

EoI response must be submitted to RailTel at https://railtel.enivida.com specified in the preamble not later than the specified date and time mentioned in the preamble.

3.1.9 Modification and/or Withdrawal of EOI response

EOI response once submitted will treated, as final and no modification will be permitted except with the consent of the RailTel.

No Partner shall be allowed to withdraw the response after the last date and time for submission. The successful Partner will not be allowed to withdraw or back out from the response commitments. In case of withdrawal or back out by the successful Partner, the Earnest Money Deposit shall be forfeited and all interests/claims of such Partner shall be deemed as foreclosed. RailTel may also consider for blacklisting of partner for 5 Years.

3.1.10 Details of Financial bid for the above referred tender

Sole partner with lowest (L1) offer will be selected for exclusive pre-bid arrangement for optimizing technical and commercial solution so that most winnable solution is submitted to end customer. The final bid for the tender may be prepared jointly with the selected Partner/Consortium so that the optimal bid can be put with a good chance of winning the Tender.

3.1.11 Clarification of EOI Response

To assist in the examination, evaluation and comparison of bids the purchaser may, at its discretion, ask the Partner for clarification. The response should be in writing and no change in the price or substance of the EOI response shall be sought, offered or permitted.

3.1.12 Period of Association/Validity of Agreement

RailTel will enter into a pre-bid agreement with selected partner with detailed Terms and conditions.

4 Eligibility Criteria

4.1 Partner's Profile

The partner shall provide the information of the below table on company letterhead.

S N	ITEM	Details
1	Full name of Partner's firm	
2	Full address, telephone numbers, fax numbers, and email address of the primary office of the organization / main / head / corporate office	
3	Name, designation and full address of the Chief Executive Officer/Director of the partner's organization, including contact numbers and email Address	
4	Full address, telephone and fax numbers, and email addresses of the office of the organization dealing with this EoI	
5	Name, designation and full address of the person dealing with the EoI to whom all reference shall be made regarding the EoI enquiry. His/her telephone, mobile, Fax and email Address	
6	Bank Details (Bank Branch Name, IFSC Code, Account number)	
7	GST Registration number	

4.2 Eligibility Criteria for Bidding Business Partner of RailTel

S.N	Description	Document Required
A) General Eligibility		
1	Bidder must be empanelled/in process of empanelment RailTel as Business associate.	i) Copy of Empanelment letter or application details for BA with RCIL OR ii) If the Bidder is not empanelled with RailTel and has applied for empanelment and issue of letter of empanelment is pending, then Bidder has to submit proof of payment of empanelment fee/EMD or acknowledgement letter of submission of empanelment documents.
2	The company must be registered in India.	Incorporation/registration Certificate along with Memorandum & Articles of Association
3	The company must have: I. Valid PAN card. II. Been registered with GST.	I. Copy of PAN Card. II. Copy of GST Certificate
4	The Bidder must not be under any form of blacklisting or debarment by any Central or State Government agency in India as on the bid submission date.	Self-declaration, in case this is discovered to be otherwise, the bidder will be declared ineligible at any stage of the tender.
5	Cover letter of the bid with valid authorization details of the person(s) signing the bid document as on date of bid submission.	a) Cover letter signed by an authorized signatory of the bidder as per Annexure 1 b) Power of Attorney (POA) on Non Judicial stamp paper of Min Value of Rs. 100/- along with Board Resolution.
6	Notarized Affidavit as per Annexure 4	Notarized Affidavit as per Annexure 4
B) Financial Eligibility		

7	The annual turnover of the bidder during any of the last three years ending 31.03.2024 should be at least Rs. 50 Crores. Bidder should have positive Net Worth for each of the last three (3) i.e., (FY 22-23, FY 23- 24 and FY 24-25)	Chartered Accountant (CA) certified turnover statement / Audited balance sheets for the financial years 2021-2022, 2022-2023 and 2023-24.
C) Technical Eligibility		
8	Bidder should have successfully implemented similar projects (including SIEM, SOAR components) in India for any State / Central Govt./PSU/BFSI/Corporate institutions in India, during the last five years ending on 31st July 2025. i. Two projects costing not less than Rs. 50 Lakhs each or ii. One project costing not less than Rs. 75 lakhs	a. Copy of the Work Order or Contract agreement b. Completion certificate/ Letter/Supporting Documents from the customer mentioning the implementation status, if it is an ongoing project.
9	The bidder should have experience in doing at least 3 (Three) Managed SOC Operations for a minimum period of two years for any State/ Central Govt./PSU/BFSI/Corporate institutions in India, during the Last five years ending on 31st July 2025.	1. Copy of the Work Order or Contract agreement 2. Completion certificate / Letter/Supporting Documents from the customer mentioning the period of Operation
10	The bidder should have the following valid certificates 1. ISO 9001:2015 2. ISO 27001:2013 or latest certifications. 3. ISO 20000:2018 (Preferred)	Copy of the certificates.
11	The OEM should submit three references/projects where they have successfully supplied and implemented their Security Solution (SIEM, SOAR, UEBA) in any Corporate Companies/BFSI/Govt. Organization in India in the last 5 years.	a. Letter of confirmation from the OEM b. Copy of Work Order/ Contract agreement c. Letter from the customer mentioning the implementation status
12	The Original Equipment Manufacturer (OEM) for the proposed solution must have a minimum of five (5) years of operational presence in India as of 31st July 2025.	Letter of confirmation from the OEM from the authorized signatory.
13	The bidder must have a minimum of thirty (30) personnel on their payroll in the domain of cybersecurity as of the bid submission date. An undertaking/declaration in company letter head by HR head of bidder's company	The bidder must submit an undertaking/declaration on the company's official letterhead, accompanied by detailed information of the cybersecurity personnel employed, including their names, designations, and roles.
14	The bidder should submit the MAF from the OEM of the proposed products (SIEM, SOAR, UEBA, TIP & NDR)	OEM MAF should be submitted

All the attached Annexures and Forms in Chapter-7 are mandatory and should be submitted along with EOI response.

5 EVALUATION AND PAYMENT TERMS

5.1 Evaluation Criteria

1. The Partners are first evaluated on the basis of the Eligibility Criteria as per chapter 4 above.
2. The Partner who fulfils the Eligibility criteria of Bidding sole partner/ consortium shall be further evaluated on the basis of Technical Evaluation and Financial evaluation.
3. For the opened bid as per outcome of the Eligibility criteria above, the partner will be selected on the lowest quote (L-1) basis for complete 'Scope of Work' as mentioned in the EOI document and documents of technical specifications of End Customer, subject to the respective overall bid is in compliance to the requirements of this EOI. The so selected partner will be termed as 'Commercially Suitable Partner (hereafter referred to as 'PARTNER')'. It is re-mentioned, that the final selection of PARTNER will be on the L-1 basis only.
4. RailTel reserves the right to have negotiation with the PARTNER at any stage before issuing Work Order.
5. The Partner with lowest commercial (L1) offer will be selected for exclusive pre-bid arrangement for optimizing technical and commercial solution so that most winnable solution is submitted to end customer.
6. RailTel reserves the right to accept or reject the response against this EOI, without assigning any reasons. The decision of RailTel is final and binding on the participants. The RailTel evaluation committee will determine whether the proposal/ information is complete in all respects and the decision of the evaluation committee shall be final. RailTel may at its discretion assign lead factor to the Partner as per RailTel policy for shortlisting partner against this EOI.
7. All General requirement mentioned in the Technical Specifications are required to be complied. The solution proposed should be robust and scalable.

5.2 Payment Terms

1. All payments will be made on a back-to-back basis on value basis.
2. Payment will be made after receiving the invoice for the work / services and after RailTel has received the payment from End Customer for the same work / services. Any deduction/Penalties levied by End Customer on invoices of RailTel will be carried back-to-back in value terms and will be deducted from PARTNER's invoices, subject to the cause to deduction / penalty is due to deviation in terms and conditions of service standards by the PARTNER.
3. Invoices should be submitted to RailTel on RailTel's BTS portal https://bts.rcil.gov.in.
4. Documents list required at the time of payment/invoice submission by selected partner shall be:

   a) PO copy issued to selected vendor.

   b) Submission/Declaration of applicable BG amount against PO issued to selected partner/vendor.

   c) Signed Agreement Copy

   d) Original Invoice for the period claimed.

   e) Certified Proof of Completion of Work from RailTel's Representative/RailTel's End Customer.

   f) TDS declaration (Income Tax Declaration – TDS ON Software/Licenses Sales Under Notification No. 21/2012 [F.No.142/10/2012-SO (TPL)J S.O. 1323(E), Dated 13-6-2012).

   g) PAN, GST Registration Certificates.

5. Payment will be on 'back-to-back' basis and as per the payment terms mentioned in the pertinent End Customer's RFP as follows:

SL No	Activity	Payment Terms	Document Required	Condition
Payment for supply and commissioning of SOC components (Capex)				
1	On completion of supply, installation and commissioning of SOC Tools such as SIEM, SOAR, UEBA & NDR	70%	Upon submission of the installation and commissioning report	Back to Back
2	FAT and GO-LIVE	20%	On successful FAT and GO-LIVE report	Back to Back
3	Balance 10% will be released on quarterly basis for a period of 3 years	10%	Upon submission of the quarterly reports after deducting SLA penalties, if any	Back to Back
Payment for Managed SOC services (Opex)				
1	Quarterly payment towards Managed SOC services	Quarterly payment upon submission of the quarterly reports after deducting SLA penalties, if any		Back to Back
Payment for AMC				
1	AMC for 4th and 5th year	Quarterly payment upon submission of the quarterly reports after deducting SLA penalties, if any		Back to Back
Payment for additional Hardware/Software Licenses				
1	Additional SIEM licenses for 10,000 EPS	100% payment against supply, installation and submission of the license documents		Back to Back
2	Additional Log Collectors	100% payment against supply, installation and submission of the warranty documents		Back to Back

##Any deduction/LD/Penalty levied by customer on RailTel will be deducted from Partner in value terms.

#Payment will only be released once proof of submission of GSTR-1 and GST-3B is submitted for claimed invoice.

#The last bills shall be settled after the end of the contract period after adjusting all outstanding dues.

#No interest is payable at any amount whatsoever.

5.3 Submission of Bills

Invoices to be submitted along with necessary reports including SLA's details duly certified by designated official of Customer End and RailTel. Payment will be made based on the timelines and payment milestones of subject work.

5.4 Bill Passing Authority

RailTel's authorized representative as mentioned in Work Order/Agreement

5.5 Bill Paying Authority

RailTel's authorized representative as mentioned in Work Order/Agreement

5.6 Delivery Location

The delivery location will be informed to the selected bidder at a later phase.

5.7 Contract Period and Warranty

The total duration of the project is for a period of 90 days from the date of release of work order including final acceptance and testing (FAT), training and submission of documentation.

a. Warranty of all quoted items shall start from the date of commissioning.

b. The warranty period for the supplied components (SOC Solution, Log Collectors, NDR Appliance) shall be for three years from the date of Go-live and 2 years AMC.

c. Post the completion of warranty period, the successful bidder should provide comprehensive AMC & ATS for proposed solution, including other software, associated modules, hardware and services required to meet the requirements in the RFP.

d. The bidder shall ensure that all additional SOC solution licenses and EPS capacity procured during the contract period are covered under Warranty and Annual Maintenance Contract (AMC) for the fourth and fifth years. All associated costs must be included in the bid price of the additional EPS licenses, and RAILTEL shall not bear any additional charges for Warranty or AMC on these components.

e. Bidder is required to produce OEM's confirmation in OEM's Letter head with serial numbers of goods / products supplied for back-to-back warranty all the equipment supplied through this RFP.

f. OEM support should be provided on 24*7

g. All ongoing software upgrades for all major and minor releases should be provided during the warranty period by the bidder.

h. The AMC/ATS support for the complete solution should include the following:

a. All minor and major version upgrades during the period of contract at no extra cost

b. Program updates, patches, fixes and critical security alerts as required.

c. Documentation updates.

d. 24x7x365 support for all security application-related malfunctions. The support must include the ability to log service requests online through a dedicated portal or support system, ensuring timely response and resolution in accordance with defined SLAs.

e. The Bidder should have back to back agreement with the OEMs for ATS and AMC support.

i. RAILTEL at its sole discretion may place purchase order of any component of additional requirement during the contract period with the discovered price as per RFP. The rate contract will be valid for entire contract period.

5.8 Commencement Period

The selected bidder must commence the work from the date of receipt of the Work Order/LoA

5.9 Contract Agreement

A contract agreement is to be executed on non-judicial stamped paper of Rs. 100. The Draft Agreement will be sent to the selected bidder

6 General Guidelines

6.1 Service Level Agreement (SLA)

The selected partner will be required to adhere to the SLA as given as per RFP for given scope of work and the SLA breach penalty will be applicable back-to-back basis on the selected partner, as specified in the end Customer organization Tender. The SLA scoring and penalty deduction mechanism for in-scope of work area shall be followed as specified in the Tender. All associated clarifications, responses to queries, revisions, addendum and corrigendum, associated Prime Services Agreement PSA/MSA/SLA also included. Any deduction by Customer from RailTel payments on account of SLA breach which is attributable to Partner will be passed on to the Partner on back-to-back basis in terms of value based on its scope of work.

Note: Any deduction/LD/Penalty levied by customer on RailTel will be deducted from Partner in percentage work share terms

6.2 Performance Bank Guarantee (PBG)

i. In case of successful participation the PARTNER shall at its own expense, deposit PBG **within fifteen (15) days** of the notification of award (done through issuance of the Purchase Order/Work Order/LoA etc.) and communicated through email, an unconditional and irrevocable Performance Bank Guarantee (PBG) from a Nationalized/Commercial Scheduled Indian Bank (either private or PSU) but not from any co-operative bank or NBFC as per the format enclosed in this EoI, payable on demand, for the due performance and fulfilment of the contract by the PARTNER. **This PBG will be for an amount of '5 %' of the contract value**. The claim period should be one year more than the expiry date. All charges whatsoever such as premium, commission, etc. with respect to the PBG shall be borne by the PARTNER. Besides, if the total BG amount comes up to ₹5 Lakhs, then same may be deposited through DD/RTGS/NEFT. Along with submission of PBG, PARTNER needs to submit PBG issuing bank's SFMS report.

ii. Under SFMS system, a separate advice of the Bank Guarantee (via SFMS IFN760COV) to be sent to advising bank (RailTel's Bank) through SFMS by the issuing Bank (Applicant's Bank), after which the paper Bank Guarantee would become operative. Similar process to be followed for Bank Guarantee amendment/extension also and separate advice (via SFMS IFN767COV) advising bank (RailTel's Bank) through SFMS by the issuing Bank (Applicant's Bank).

iii. PBG should have validity of **75 months**. The PBG may be discharged / returned by RailTel upon being satisfied that there has been due performance of the obligations of the PARTNER under the contract. However, no interest shall be payable on the PBG. In the event, PARTNER being unable to service the contract for whatsoever reason, RailTel would invoke the PBG at it discern. Notwithstanding and without prejudice to any rights whatsoever of RailTel under the contract in the matter, the proceeds of the PBG shall be payable to RailTel as compensation for any loss resulting from the PARTNER's failure to complete its obligations under the contract.RailTel shall notify the PARTNER in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the PARTNER is in default.

iv. RailTel shall also be entitled to make recoveries from the PARTNER's bills, PBG or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

v. If the service period gets extended by virtue of extension of same by End Customer, PBG should also be extended accordingly.

vi. During the contract period, RailTel may issue Purchase Order(s) for the additional services ordered by End Customer (in case) to RailTel.

vii. In case the End Customer sought PBG of the contract in terms of Indemnity Bond from RailTel, the selected partner has to provide the equivalent value PBG from scheduled Bank to RailTel. No Indemnity Bond from Selected Partner will be accepted in lieu of PBG from Scheduled Bank.

viii. In case End Customer has sought any other types of PBG in this contract at present or in future or else Integrity Pact PBG (presently or in future), same remain applicable on selected Partner/Consortium. The said PBG will be issued by Selected Partner from Scheduled Bank favoring RailTel Corporation of India Limited. No Indemnity Bond in lieu of such PBG will be accepted by RailTel.

ix. If End Customer ask for submission for value more than 5%, same also needs to be submitted by the selected Partner /Consortium.

x. PBG will be discharged/released only after receipt of RailTel's PBG from RailTel's End Customer.

xi. The successful bidder will have to pay additional security deposit of 5% of contract value within 2 weeks of the issuance of the LoA/WO. The validity of the Security deposit should be 12 months.

6.3 Insurance

The selected Partner agrees to take insurances to cover all the elements of the project under this EoI including but not limited to Manpower, Hardware, Software etc. as per End Customer EoI specified terms.

6.4 Liquidity Damages (LD)

If the subject work is not implemented within the stipulated timeline on the receipt of work order/LoA, then **0.5%** of the total work order/LoA for each week of delay will be deducted. The LD can be extended upto 10% of the total work order/LoA value. Any deduction/LD/Penalty levied by customer on RailTel will be deducted back – to – back from Partner in value terms. For all liquidity damages mentioned above are exclusive of GST. Final deduction will include GST values.

6.5 Termination:

In case Bidder/Selected Partner fails to execute the terms and conditions of the contract, RailTel will have the right to terminate the contract with 15 days' notice and carry out the work through another contractor. In such circumstances all the security/BG will be forfeited by RailTel.

6.6 Delivery and Inspection:

Delivery, Installation and Commissioning Period: As per RailTel's Project Delivery Schedule.

All the material should be made available for Inspection by RailTel nominated person/agency if required.

Partner will be custodian of all the material till installation and commissioning of system.

6.7 Provisional Acceptance Certificate (PAC)

Upon completion of the project, and prior to the commencement of Operations & Maintenance (O&M), subject to acceptance by RailTel's end customer and certification by RailTel's representative.

6.8 Final Acceptance Certificate (FAC)

6 months after completion of the entire project including O&M, subject to acceptance by RailTel's end customer and certification by RailTel's representative.

6.9 Pre – Contract Integrity Pact

This EoI is covered under Pre – Contract Integrity Pact Program of RailTel and partners are required to sign the Pre – Contract Integrity Pact and submit the same to RailTel along with the bids. EoI received without signed copy of the Pre – Contract Integrity Pact document may be liable to be REJECTED.

6.10 Other Conditions:

Partner has to agree to comply with all scope of work and term and conditions including special term and condition, SLA and OEM technical & Financial documentation including technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP as mentioned below:

Tender Ref. No	CERT-K/9/2025-KSITM
Date of floating	03-Sep-2025
Floated on portal	https://etenders.kerala.gov.in

Anything not mentioned in the EOI, Customer RFP and its corrigenda (if any) and addenda (if any) may be referred & considered.

#Note: Depending on RailTel's business strategy RailTel may choose to work with Partner who is most likely to support in submitting a winning bid.

7 ANNEXURES AND FORMS

7.1 ANNEXURE 1 - FORMAT FOR PROJECT EXPERIENCE CITATIONS

Sl. No.	Item	Bidder's Response
1	Name of Bidder entity	
2	Assignment Name	
3	Name & Address of Client	
4	Approximate Value of the Contract (in INR Crores)	
5	Duration of Assignment (months)	
6	Start Date (month/year)	
7	Completion Date (month/year)	
8	Narrative description of the project	
9	Details of Work that defines the scope relevant to the	
10	Documentary Evidence attached	

Signature of Bidder ……
Name: ……
Designation …… Seal of BA Organization
Place: ……
Date: ……..

7.2 ANNEXURE 2 - EOI COVER LETTER

(On Organization Letter Head)

EOI Ref No: Date:

To,
The Joint General Manager (ERS)
RailTel Corporation India Limited,
Kerala Territory Office,
1st Floor, Eastern Entry Tower
Ernakulam South Railway Station
Ernakulam – 682016

Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025; latest amendment/ Corrigendum / clarifications. **Floated on e-tender Kerala Portal** (**https://etenders.kerala.gov.in/)**

Dear Sir/ Madam

1. I, the undersigned, on behalf of M/s ....., having carefully examined the referred EOI offer to participate in the same, in full conformity with the said EOI and all the terms and conditions thereof, including corrigendum issued till last date of submission of EOI. It is also undertaken and submitted that we are in abidance of Clause 4 of EOI.
2. I agree to abide by this Proposal, consisting of this letter, our Pre-qualification, Technical and Commercial Proposals, for a period of 180 days from the date fixed for submission of Proposals as stipulated in the EOI and modifications resulting from contract negotiations, and it shall remain binding upon us and maybe accepted by you at any time before the expiration of that period.
3. I acknowledge that the Authority will be relying on the information provided in the Proposal and the documents accompanying the Proposal for selection of the Commercially Suitable Partner (CSP) for there for said Service, and we certify that all information provided therein is true and correct; nothing has been omitted which renders such information misleading; and all documents accompanying the Proposal are true copies of their respective originals.
4. I undertake, if our Bid is accepted, to commence our services as per scope of work as specified in the contract document.
5. Until a formal Purchase Order or Contract is prepared and executed, this Bid and supplement / additional documents submitted (if any), together with your written acceptance thereof in your notification of award shall constitute a binding contract between us.
6. I hereby undertake and give unconditional acceptance for compliance of all terms & **Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025;** latest amendment/ Corrigendum / clarifications. **Floated on e-tender Kerala Portal** (**https://etenders.kerala.gov.in/)** against this EOI based customer's requirement.
7. I hereby undertake that there will be no deviation from the Terms and Conditions of EOI **Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025;** latest amendment/ Corrigendum / clarifications. **Floated on e-tender Kerala Portal** (**https://etenders.kerala.gov.in/)**

Signature of Bidder …….
Name: ……
Designation …….. Seal of BA Organization
Place: ……
Date: ……..

7.3 ANNEXURE 3 - (Local Content Compliance)

EOI Ref. No: Date:

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025; latest amendment/ Corrigendum / clarifications. **Floated on e-tender Kerala Portal** (**https://etenders.kerala.gov.in/)**

Dear Sir / Madam

I, the undersigned, on behalf of M/s ....., hereby submits that our technical solution for the 'Scope of Work' mentioned under the EoI document is in compliance of local content requirement and makes us equivalent to 'Class-I local supplier' / 'Class-II local supplier' (mention whichever is applicable) for the EoI under reference, as defined under the order No. P-45021/2/2017-PP(BE-II) dt. 04-June-2020 issued by Ministry of Commerce and Industry, Govt. of India.

I hereby certify that M/s .....fulfils all requirements in this regard and is eligible to be considered and for the submitted bid Local Content Percentage is % (write in figures as well as in words).

I hereby acknowledge that in the event of acceptance of bid on above certificate and if the certificate is found to be false at any stage, the false certificate would be a ground for immediate termination of contract and further legal action in accordance with the Law, including but not limited to the encashment of Bank Guarantee related to Empanelment and Performance Bank Guarantee (PBG) and Security deposit (SD), as available with RailTel, related to this EoI. Signature of Authorized Signatory.

Signature of Bidder …….
Name: ……
Designation …….. Seal of BA Organization
Place: ……
Date: ……..

7.4 ANNEXURE 4 - CHECKLIST OF DOCUMENTS FOR BID SUBMISSION

KSITM Tender **Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025;** latest amendment/ Corrigendum / clarifications. **Floated on e-tender Kerala Portal (https://etenders.kerala.gov.in/)**

Sl. No.	Document
1	EOI Cover Letter (Annexure-02)
2	Technical compliance sheet
3	Price bid
4	Local Content Compliance & Percentage Amount (annexure-03)
5	**TECHNICAL BID COVER LETTER**
6	**COMMERCIAL BID COVER LETTER**
7	EMD as per EOI document
8	This EOI copy duly Signed and Stamped by the Authorized Signatory Of Bidder
9	All Annexure/ Appendices/Formats/ Declarations as **per KSITM Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025**; addressing to RailTel.
10	Compliance of eligibility criteria related documents as per Clause 3
11	Any relevant document found suitable by bidder

Note:

1. The technical bid should have a 'Index' at the starting and all pages of bid should be serially numbered and should be traceable as per the 'Index'.
2. All the submitted documents should be duly stamped and signed by the Authorized Signatory at each page.
3. The above checklist is indicative only. RailTel may ask for additional documents from the bidders, as per the requirement

Signature of Bidder …….
Name: ……
Designation …….. Seal of BA Organization
Place: ……
Date: ……..

7.5 ANNEXURE 5 - FORMAT FOR TECHNICAL BID COVER LETTER

(On Company Letter Head)

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Sub: Submission of the response to the Tender No. <<tender id>>Request for Proposal for the **"Setting up a security operations centre (SOC) at KSITM".** We, the undersigned, offer to provide services for **"Setting up a security operations centre (SOC) at KSITM"** in response to the request for proposal dated <insert date> and tender reference no <> **"Setting up a security operations centre (SOC) at KSITM"** by KSITM. We are hereby submitting our proposal online, which includes the pre-qualification, technical bid, and commercial bid.

We hereby declare that all the information and statements made in this technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our proposal is accepted, to initiate the implementation services related to the assignment not later than the date indicated in this tender.

We agree to abide by all the terms and conditions of the RFP and related corrigendum(s)/ addendum(s). We would hold the terms of our bid valid for 180 days from the date of opening of the commercial bid as stipulated in the RFP. We hereby declare that as per RFP requirement, we have not been black listed/ debarred by any Central/ State Government and we are not the subject of legal proceedings for any of the foregoing.

We understand you are not bound to accept any proposal you receive.

Signature of Bidder …….
Name: ……
Designation …….. Seal of BA Organization
Place: ……
Date: ……..

7.6 ANNEXURE 6 - FORMAT FOR COMMERCIAL BID COVER LETTER

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Dear Sir,

We, the undersigned Bidder, having read and examined in detail all the tender documents with respect to "Installation, commissioning, testing & maintenance of routing device in the complete link for three years", do hereby propose to provide services as specified in the tender reference No **Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025** Price and Validity

a) All the prices mentioned in our bid are in accordance with the terms & conditions as specified in the RFP. The validity of bid is 8 months from the date of opening of the commercial bid.
b) We are an Indian firm and do hereby confirm that our prices are inclusive of all duties, levies etc., excluding GST.
c) We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on income tax, professional and any other corporate tax is altercated under the law, we shall pay the same.

Unit rates: We have indicated in the relevant schedules enclosed, the unit monthly rates for the purpose of accounting of payments as well as for price adjustment in case of any increase / decrease from the scope of work under the contract.

Deviations:

We declare that all the services shall be performed strictly in accordance with the RFP irrespective of whatever has been stated to the contrary anywhere else in our bid. Further, we agree that additional conditions, if any, found in our bid documents, shall not be given effect to. We had remitted an EMD as specified in the tender document terms.

Tender pricing: we further confirm that the prices stated in our bid are in accordance with your instruction to bidders included in tender documents.

Qualifying data: we confirm having submitted the information as required by you in your instruction to bidders. In case you require any other further information/ documentary proof in this regard before evaluation of our tender, we agree to furnish the same in time to your satisfaction.

Bid price: we declare that our bid price is for the entire scope of the work as specified in the RFP. These prices are indicated in annexure-commercial bid format attached with our tender as part of the tender.

Performance bank guarantee and Security Deposit: we hereby declare that in case the contract is awarded to us, we shall submit the performance bank guarantee. We hereby declare that our tender is made in good faith, without

collusion or fraud and the information contained in the tender is true and correct to the best of our knowledge and belief. We understand that our tender is binding on us and that you are not bound to accept a tender you receive.

Signature of Bidder …….
Name: ……
Designation …..... Seal of BA Organization
Place: ……
Date: ……..

7.7 ANNEXURE 7 - TECHNICAL COMPLIANCE SHEET

TECHNICAL SPECIFICATION

The Service/OEM/MAKE specified are based on the existing network requirement for the present scope of work. This shall be followed as per the special condition of contract as per the relevant conditions of special conditions of contract as appended as per RFP back to basis.

Security Information & Event Management

Sl No.	Specification	Compliance (Yes or No)	Remarks
1	The proposed SIEM solution have a sustained 25000 EPS (Events per Second) and/or equivalent Flow records per second which can be scalable upto 200,000 EPS and/or equivalent flow records per second.		
2	The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system		
3	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.		
4	The solution must support automated classification of assets that are being protected.		
5	Solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, Opsec etc.). Solution can read and interpret events from more than 300 log sources.		
6	The solution must support information (users, groups, etc.) collected from Directories (i.e. AD, LDAP) products. Please describe your level of support for this type of product.		
7	The solution must integrate with other security and network devices		
8	Solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage		
9	Solution must be able to store logs in a separate system which would not be required to perform any real time correlation thereby minimizing the load on the Real time analysis.		
10	Solution must provide agent-less collection of event logs.		
11	Solution must provide an agent to collect logs from windows servers.		
12	Solution must provide the ability to distribute both event collection and processing across the entire SIEM deployment.		

13	SIEM shall support Connector Development tool/SDK /API availability for developing collection mechanism for home-grown or any other unsupported devices/applications. The respective tool should be provided		
14	The solution must provide the ability to encrypt communications between components		
15	SIEM solution collector which is used should be able to send data real-time towards to processing unit.		
16	The solution must normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network		
17	The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.		
18	The system should be able to analyse logs with different event formats which include operational Events / Logs of Security devices including IDS / IPS, Firewalls, Anti-virus and other such devices, Logs / Events from the servers such as Web server, Mail server, DNS Server, Application Servers, Operating systems (Windows, Unix, Linux, AIX, Solaris etc), Virtualization platforms, Databases (Postgres, Oracle, SQL, DB2, MySql, Sqlite, MS- Access etc.), Storage systems, etc. as deemed to be important for the purpose of Security. The system should support, not restricted to, the following log and event collection methods: ➢ Syslog – UDP (as detailed in RFC 3164) TCP (as detailed in RFC 3195) ➢ Flat file logs such as from DNS, DHCP, Mail servers, web servers etc. ➢ Windows events logs – Agent-based or agentless ➢ FTP, S/FTP, SNMP, ODBC, CP-LEA, SDEE, WMI, JDBC, etc. ➢ NetFlow, JFlow, Sflow , AIX etc/ ➢ Single-line Flat Files and Multi-line Flat Files ➢ Compressed Flat Files (single and multi- line)		
19	The solution must provide a common taxonomy of events.		
20	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields		
21	The SIEM must provide searching & data/log management, including free form search.		
22	The solution must provide near-real-time analysis of events.		
23	The solution must provide more advanced event drill down when required.		
24	The solution must provide a real-time streaming view that supports full filtering capabilities		
	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single		

25	logical view. This view should include relevant events, network activity data, correlated alerts, etc..		
26	The SIEM must provide the ability to understand the virtual host to virtual host communications within our virtualized environment looking for suspicious		
	activity. Please describe how your solution meets this requirement.		
27	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events. Please describe how this requirement is met by the solution.		
28	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a failed called “SpecialID from my Custom Application”).		
29	The solution must support and maintain a history of user authentication activity on a per asset basis.		
30	The solution must provide a ‘Dashboard’ for quick visualization of security and network information.		
31	The solution must support the automated distribution of reports		
32	The solution must allow for custom defined tagging of events		
33	The solution must support the capability to provide historical trend reports.		
34	The solution must integrate with 3rd party directory systems as an authentication method. Solution should be integrated with LDAP or Active Directory solution for access provisioning to the SIEM system.		
35	The solution must provide an open API mechanism		
36	The proposed solution should be horizontally scalable to support increase in EPS and should have global correlation capability on raw or metadata/normalized events (i.e. correlation of events if processed on multiple hardware/appliances)		
37	SIEM solution should be configured in High Availability across all components within the system e.g. log correlation, management console etc.		
38	The solution must support a web-based GUI for management, analysis and reporting. There should be no plug-ins, Java, Flash, or thick-client requirements for operating the solution.		
39	Solution should be able to define purging and retention rules for log storage.		
40	Solution should offer a global threat feed which must allow the analyst to perform search across various parameter like IPv4, IPv6, URL, vulnerability, Applications name, Malware, Spam.		

41	Solution should allow analyst to perform manual ad- hoc check to determine if he is infected with any Zero-day attack.		
42	The solution should have out of the box bi-directional integration with proposed SOAR solution.		
43	Proposed solution should support both automatic and manual escalation of incidents to proposed SOAR and should allow the proposed SOAR to query data from the SIEM		
44	The platform shall support provision for dashboard specific to a single offense, which can offer various widgets, provision for sharing notes, representation of data in a graphical manner over a certain period and various rules triggered, rule s, model responsible in triggering of the offense.		
45	There should be provision available to create complex searches by means GUI, to support advance investigation on the data available in the platform.		
46	The platform should Query-less search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values		
47	The solution should not limit the number of non- critical events that need to be collected for compliance reason and doesn't require correlation till the maximum capacity of hardware/storage.		
48	The solution should not require additional license to deploy additional log collectors		
49	For storage calculation, bidder may consider 700 byte as the average raw payload size of the logs		
50	All collected logs must be stored in encrypted form, using industry-standard encryption algorithms such as AES-256 or equivalent/higher. Additionally, the event log data must be compressed at a minimum ratio of 1:8 or better to ensure storage efficiency.		
51	Log collection software should supports proctols like syslog, JDBC, API, WMI, SFTP, FTP, SCP, SNMP, MQ etc on single software/hardware appliance.		
52	Provide user login concurrently for analysis as well as administration activities with a minimum 50 concurrent users.		
53	No logs should be lost due to any kind of disruption for both real time collection as well as long-term storage.		
54	Log security in terms of integrity and availability		
55	The Proposed Solution must offer all of the below built-in Compliance Modules at no additional cost: ➢ ISO 27001 Compliance. ➢ PCI Compliance ➢ ISO 27017		

56	Provides the following but not limited to real time alerting based on observed security threats: i. DDoS ii. Worm outbreak iii. Botnets iv. Exploitation and attack attempts		
57	v. Attack sources vis-à-vis specific attacks and top exploits vi. Compromised systems vii. Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), etc. viii. Other attack vectors such as the following are detected ➢ Web Login brute force attempts ➢ Web Login brute force and successful breach ➢ SQL Injection Attempts ➢ SQL Injection breach, followed Data Exfiltration ➢ DDoS Attack on web server by anomaly detection, unusual continuous request for huge file downloads. ➢ Slow DoS Attacks on Web Server ➢ TCP SYN Flood Attack ➢ Unauthorised Login LDAP, Active Directory, Database ➢ Authorized Login with stolen credentials or via Network Intrusion ➢ APT Attacks ➢ Ransomware Attacks ➢ Botnet Infection ➢ Other Known Malware infections correlating with Threat Intel ➢ Network / IP Scan ➢ URL scan Attempts ➢ Monitored devices hardware failure ➢ Intrusion Attempts ➢ Privilege Escalation		
58	The bidder shall ensure that all log and event data is retained for a minimum period of 30 days on online storage. Additionally, the bidder shall maintain the preceding 6 months of data on offline storage. The data retention strategy must comply with industry best practices and CERT-In guidelines, ensuring data integrity, availability, and security throughout the entire retention period.		
	Correlation & Alerting		
59	The solution must provide alerting based on observed security threats from monitored devices and network activity		
	The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors. (i.e., look for 25 login failures from the same username followed by a single successful login for that same username, where events seen by a single collector do not exceed the threshold of		

	25, but across multiple collectors would exceed the threshold).		
60	SI proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. 2. Flow based threat Detection 3. User Behavior analysis 4. Threat Intelligence		
61	The solution must provide the ability to correlate information across potentially disparate devices and flows information.		
62	The solution must observe anomalies other than just simple threshold basis		
63	The solution must chain alerts into one single incident record, so when different rules are triggered and these activities are related with one single offense, then these triggers will generate only one incident record to avoid overloading the security operation team. Please describe how you solution meets this requirement.		
64	The solution must provide alerting based upon established policy.		
	The system must automatically learn and baseline the normal user and host relationships across the network.		
	The system must alert when a user attempts to log into a host they have not previously accessed.		
	The system must be able to track user activity by host over time, even when the event logs do not contain the username.		
65	The system must automatically detect and baseline all assets and services on the network.		
66	The system must generate an alert when a new, unplanned asset or service appears on the network.		
67	The system must alert on new services running on existing hosts.		
68	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions		
69	The solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results. Please describe how your solution meets this requirement.		
70	The solution must limit the presentation of multiple similar alerts. Describe the solutions ability to minimize duplicate alarms.		
71	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. Please describe how your solution meets this requirement.		

72	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile		
	networks, etc.). These 3rd party data feeds should be updated automatically by the solution. Please describe how your solution meets this requirement.		
73	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes then generate an alert. Please describe how your solution meets this requirement.		
74	The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification. Please describe how your solution meets this requirement.		
75	The solution must support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes. Please describe how your solution meets this requirement.		
76	The solution must support correlation for additive values over time. For example, alert when any SRC IP sends more than 1GB of data to a single port on a single DST IP in a one hour period of time. Please describe how your solution meets this requirement.		
77	The solution must provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity. Please describe how your solution meets this requirement.		
78	The solution must support historical correlation so users can re-run past events and flows on historical data, so new rules can be tested more precisely. Please describe how your solution meets this requirement.		
79	The solution must be able to be updated regularly, to stay aware of the latest threat information and research available.		
80	The solution must be able to analyze user activity to detect malicious insiders and determine if a user's credentials have been compromised.		
81	Platform should be capable of providing insights into your local DNS traffic by identifying malicious activity and allowing security team to be able to detect following A. Domain Generated Algorithm (DGA) B. Tunneling or Squatting domains that are being accessed from within your network.		

82	The Platform shall create a baseline model that contains information about the flows and flow attributes that currently exist on the system.		
83	The platform should analyzes the flow records to determine normal traffic patterns, while comparing all incoming flows to the baseline models. Flow should be assigned an outlier score based on the flow attribute values and frequency of communication is observed on the network.		
84	The platform should Visualize offenses, network data, threats, malicious user behavior, and cloud environments from around the world in geographical maps, and auto updating charts.		
85	The platform should allow to Import and export dashboards or share dashboard links with colleagues.		
86	The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, offense and the generic APIs.		
87	The platform should allow user to fine-tune there with complete flexibility in dashboard layout and dashboard item refresh rates		
88	The platform should allow user to Assign thresholds to Big Number, Time Series, Tabular, and Geographical charts		
89	The platform should offer an interface to help user in browsing the existing rule mapping across MITRE Framework & enabling them to map their custom rules to MITRE ATT&CK tactics and techniques.		
90	The platform should offer user to tune their environment with the help of built-in analysis capability.		
91	The Platform should allow user to Use new insights to prioritize the rollout of new use cases and apps to effectively strengthen your security posture.		
92	The platform shall help user in visually exploring how potential log source type and MITRE-mapping coverage can increase. Also providing the user capability to reduce false positive.		
93	Performs the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: 1. Vulnerability based 2. Statistical based 3. Historical based 4. Heuristics based 5. Behavior based on source entity, applications etc. 6. Information Leak 7. Unauthorized Access 8. Denial of Service		

	9. Service Unavailable 10. Phishing attack 11. Pattern based rules 12. Profiling Whitelist/Blacklist/Reference List		
	AI & Machine Learning:		
94	The solution must incorporate Gen AI and act as cybersecurity expert to provide recommendations leveraging LLM		
95	The solution should not be sending any log data outside of the system by utilising LLMs model. AI working should only be initiated by the user and not automated		
96	Machine learning should be embedded across the platform (SIEM, UBA). It should empower every user in the SOC with ML/DL.		
97	The solution should accurate provide offense summaries that help security analyst to quickly investigate and mitigate risks. By using accurate offense summaries, a security analyst can rapidly comprehend critical details about an offense, including the attack vector, affected users, and assets.		
98	The solution should provide recommended actions with both long-term and short-term measures. This helps to mitigate the immediate risk and to proactively avoid future attacks. This makes it easier to eliminate uncertainty and take prompt action in response to serious risks.		
99	The solution should provide own unique session maintained and stored by the app along with session logs so that a user can revisit their past chat sessions when needed.		

Security Orchestration, Automation, and Response (SOAR)

Sl No.	Specification	Compliance (Yes or No)	Remarks
A	INCIDENT RESPONSE ESCALATION AND WORKFLOW		
1	The solution must include a module, out-of-the- box, that provide incident response playbooks		
2	The solution should support following methods of Incident Creation		
	The solution must be able to create incident by parsing email notification.		
	The solution must provide UI based wizard to manually create incidents.		
	The solution must be able to support creation of incidents via API.		

	The solution must be able to support creation of incidents via Web URL.		
	The solution must be able to support creation of incidents via SIEM.		
	The solution must be able to support creation of incidents via ticketing system.		
3	The solution must be able to automatically extract email attachments from emails and store that for the related incidents as attachments.		
4	The solution must be able to support storing of incident related files not limited to malware specimens, logs, and screenshots.		
5	The solution must include out-of-the-box playbooks based on SANS and NIST for incidents like Malware, Phishing, DDOS and should support creation of multiple playbook based on the SOC's Use case.		
6	The solution must be able to provide incident response playbooks that consist of phases and tasks that guides the user on how to adequately response to the incident; integrating people, processes and technology.		
7	The solution must provide a visual workflow editor that is based on BPMN-Business Process Model and Notation to enforce sequencing of incident response activities		
8	The solution must include a in-product script editor with autocomplete and syntax highlighting, to support automation of incident response workflow.		
9	The solution must include a in-product script editor with run buttons to facilitates debug and perform tests on scripts.		
10	The solution must allow organizations simulate incidents, to test response plans, allowing them to identify gaps and refine processes before a real incident happens.		
11	The Proposed Solution should have out-of-the-box bi-directional integration with the proposed SIEM solution & App on both platform (SIEM & SOAR)		
12	The proposed solution should have out-of-the-box provision for creation of incident from the existing SIEM automatically or manually.		
13	The proposed solution should have out-of-the-box provision of closing incident simultaneously on SIEM and the proposed SOAR platform.		
14	The proposed solution should have out-of-the-box capability to query or add IOC/Artifact to existing reference set of the deployed SIEM solution.		
15	The Proposed solution should have web based application store which should host latest integrations available from the OEM these integration can be downloaded with no additional cost.		

16	The proposed solution should have community portals and knowledgebase which can be used to learn about sample integration and forum to discuss issue or use cases.		
17	The proposed solution should support multi-organisation support wih the proposed SIEM.		
B	**Administration, Configuration, Dash Board & Reports**		
1	The proposed solution should support disaster Recovery and the same shall be offered as the part of solution.		
2	The solution must be offered as a virtual appliance for on premise deployment.		
3	The solution must be able to support multi-tenancy.		
4	The solution must support a web-based GUI for management, analysis and reporting. Please describe how your solution meets this requirement.		
5	The solution must provide central management of incidents and administrative functions from a single web based user interface. Please describe how your solution meets this requirement.		
6	The solution must support creation of user and user groups.		
7	The administrator must be able to define role base access to the solution by incidents. Please describe how your solution meets this requirement.		
8	The administrator must be able to define role based access to various functional areas of the solution. This includes being able to restrict a users access to specific functions of the solution that is not within the scope of a users role including, but not limited to, administration, reporting, incident assignment, playbook creation. Please describe how your solution meets this requirement.		
9	The solution must offer granular license offering for the various modules or supported features.		
10	The solution should be designed considering 5 Authorized users.		
11	The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. Please describe how your solution meets this requirement.		
12	The solution must deliver sample dashboards out- of-the-box (not limited to - Incident Over Time by Type, Open Incidents by Phase, Close Incident by Duration). Please describe how your solution meets this requirement.		
13	The solution must deliver customizable dashboard widgets that can present relevant incident information to the users. Please describe how your solution meets this requirement.		
14	The solution must maintain a database of incidents. The user must be able to search this database using the embedded elastic search. Please describe how your solution meets this requirement.		

15	The solution must support and maintain a history of user activity per incident. Please describe how your solution meets this requirement.		
16	The solution should offer graphical representation of all the artifact associated to a particular incident along with the timeline. It should enable the analyst to take action from within the graphical view on any artifact i.e. this could be blocking a IP address or doing further investigation using any of the threat service available to solution.		
17	The Solution should offer Timeline graph for each incident allowing display that can be set to display days, weeks, and months. It should also allow analyst to add milestones to call out important events within the timeline. Where the analyst can add a date, title, and description of your milestone.		
18	The solution should allow adding custom table to incident layout allowing organisation to track relevant fields based on use case. Such as Approval flow, Response time, Actions performed to name a few.		
19	The solution must provide reporting templates, to report on incident information, for the management team as well as the IT Security team via the GUI. Describe how the solution provides the ability to configure reports.		
20	The solution must provide configurable reporting engine for customized report creation. Please describe how your solution meets this requirement.		
21	The solution must support importing and exporting of configuration settings.		
C	**CORRELATION AND ANALYTICS**		
1	The solution must offer out-of-the-box support for auto creation of incident artifacts. Please describe how your solution meets this requirement.		
2	The solution must out-of-the-box include an analytics engine that displays relationship between incidents based on similar artifacts. Please describe how your solution meets this requirement.		
3	The solution must be able to support logical segregation of incidents. This will be used to assign a specific group of incidents to a specific group of users/analysts		
4	The solution must able to support creation of a Wiki pages. This enables organizations to add important information, guidelines, and reference material for the Incident Response team.		
5	The solution must provide long term trend analysis of incidents. Please describe how this requirement is met by the solution.		

6	The solution must provide more advanced incident drill down when required. Please describe how this requirement is met by the solution.		
7	The solution must support periodic updates of threat intelligence for incident artifacts. Please describe how this requirement is met by the solution.		
8	The solution must provide the ability to correlate artifacts across potentially disparate incidents. Please describe how your solution meets this requirement.		
9	The solution must support the ability to trigger action on external systems, for a related to an incident. For example, the solution should support the ability to block an intruder. Please describe how your solution meets this requirement.		
10	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution. Please describe how your solution meets this requirement.		
11	The solution must dynamically augment incident playbooks in real time to support a specific incident response workflow. Please describe how your solution meets this requirement.		
12	The solution must provide the ability to contextually link incidents with similar artifacts. Please describe how your solution meets this requirement.		
13	The solution must provide the means for analysts to review the enrichments performed on the incident to arrive at conclusions about a security incident.		
14	The solution must out-of-the-box integrate with 7+ threat intelligence feed providers to provide data enrichment of incident artifacts.		
15	The solution must, out-of-the-box, must provide visualization of incident correlation across IOCs and other artifacts automatically with timeline support.		
16	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response.		
	AI & Machine Learning:		
1	The solution must have AI support, scan artifacts and attachments, and address any questions about incidents, artifacts and attachments.		
2	The GenAI assistant should able to provide incident summarisation, artifact analysis, conversational interface, custom playbook automation		

User Behavior Analytics (UEBA)

Sl No.	Specification	Compliance (Yes or No)	Remarks
1	UBA should be proposed as inbuilt capability of offered SIEM solution.		
2	Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency.		
3	Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time.		
4	Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly		
5	Usage deviates from peer group such as User pattern of activity starts deviating from the peer group		
6	Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems		
7	Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing		
8	Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data		
9	Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data		
10	Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users		
11	UBA should activate a rules for a set of users until a specified condition or specified time window.		
12	Solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling.		
13	UBA should be part of the SIEM solution & SI should not require any additional/ Third party component to complete the UBA solution.		
14	UBA UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of users' behaviors, risks and trends from a single screen		
15	UBA should perform the below mentioned scenario's as well.		
16	UBA ML model must cover • Individual user models (by numbers or observed): Like Access Activity, user's general activity by time, Authentication Activity, data		

	that is downloaded or uploaded by user, Lateral Movement, process usage etc • Peer Group Analysis: like Activity distribution, defined peer group, learned peer group etc. Custom Models: like Application Events, Source IP, Destination Port, Office File Access, AWS Access, Process, Website, Risky IP		
17	ML Based UBA Usecases must include		
	Access activity		
	Aggregated activity		
	Authentication activity		
	Data uploaded to remote networks		
	Data downloaded		
	DML events		
	DDL events		
	Large HTTP transfers		
	Outbound transfer attempts		
	Risk posture		
	Suspicious activity		
	Successful access and authentication activity		
	Activity distribution		
	Defined peer group		
	Learned peer group		
	Lateral Movement: Internal Destination Port Activity		
	Lateral Movement: Network Zone Access		
	Lateral Movement: Internal Asset Usage		
	Process Usage		
	Use Case for UBA:		
	Account accessing more high value assets than normal		
	More data being transferred then a normal to and from servers and / or external location		
	Privileged account accessing high-value servers from a new location for the first time		
	Account used for the first time in a long time		
	Rare privilege escalation		
	Accounts being used from peculiar locations		

	User involved in previously malicious or threatening behaviour		
	User an outlier within their peer group.		
	Exfiltration:		
	Data Exfiltration by Print		
	Data Exfiltration by Removable Media		
	Data Loss Possible		
	Initial Access Followed by Suspicious Activity		
	Large Outbound Transfer by High Risk User		
	Multiple Blocked File Transfers Followed by a File Transfer		
	Browsing behavior:		
	Browsed to Entertainment Website		
	Browsed to Gambling Website		
	Browsed to Information Technology Website		
	Browsed to Mixed Content/Potentially Adult Website		
	Network Traffic and Attacks		
	D/DoS Attack Detected		
	Honeytoken Activity		
	Capture, Monitoring and Analysis Program Usage		
	DNS Analysis		
	Potential Access to Blacklist Domain		
	Potential Access to DGA Domain		
	Potential Access to Squatting Domain		
	Potential Access to Tunneling Domain		
	Geography Based		
	Anomalous Account Created from New Location		
	User Access from Multiple Locations		
	User Geography Change		
	User Geography, Access from Unusual Locations		

Network Detection and Response (NDR)

Sl No.	Specification	Compliance (Yes or No)	Remarks
1	The NDR should be an appliance-based solution capable of monitoring 10 Gbps of network throughput from day one, and must include a redundant power supply and 8 × 10G SFP+ ports.		
2	The solution must be horizontally scalable to accommodate growth in network traffic volume to 20Gbps and beyond without the need for a full re-architecture.		

3	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts. Please describe how your solution meets this requirement.		
4	The solution must support application definition beyond protocol and port. The system must support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as		
	Instant messenger - not HTTP). Please describe how your solution meets this requirement.		
5	The solution must use machine learning to dynamically establish and maintain a baseline of normal network behavior for all users, devices, and applications. It shall alert on any significant deviations from this established norm.		
6	The solution must detect and present views of traffic pertaining to observed threats in the network. Describe the types of threats and visualizations for this information in the Security Intelligence system.		
7	The proposed solution must provide deep packet inspection (DPI) capabilities to identify and classify applications and threats regardless of the port or protocol they use.		
8	Solution must support Netflow, JFlow, SFLow, IPFix collection and correlation.		
9	The solution must support traffic profiling associated with logical network design (e.g., Subnet/CIDR).		
10	The solution must identify network traffic from potentially risky applications (e.g. file sharing, TOR, telnet, ftp, p2p.etc.).		
11	The solution must display traffic profiles in terms of packet rate. This capability must be available for simple TCP analysis (TCP Flags, etc.) but rate-based information may be presented for other profiles (e.g., applications).		
12	The solution must profile and present information in multiple timeframes. Profiles must be available for week, day and hour.		

13	The solution must be able to profile communication originating from or destined to the internet by Geographic regions in real-time. Describe how this is accomplished.		
14	The solution must create clearly independent and differentiated profiles from local traffic vs. traffic originating or destined for the internet.		
15	The solution must allow the user to create custom profiles and views using any property of a flow, log, data source or already profiled traffic. Describe how the Security Intelligence system supports this level of customization.		
16	The solution must support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc. Please describe how your solution meets this requirement.		
17	The solution must identify network traffic within a virtual network environment. Please describe how your solution meets this requirement.		
18	The SIEM must roll up all events and network flows into single offenses.		
19	The solution must be able to detect suspicious communication channels Services or applications		
	not running over its standard ports. (i.e. HTTP not over port 80)		
20	The SIEM must have the ability to generate reports on flows and events and to declare higher level aggregation of raw events into meaningful "Security Incidents" worth investigating.		
21	The solution should support importing of YARA rules and use those rules for matching and flagging malicious content.		
22	The Solution should provide app which allow uploading of yara rules and allow testing of these rules against log , flows and files to test.		
23	The App should allow importing YARA rules from opensource such as github, to take advantage of community learning.		
24	The proposed solution must be able to detect and alert on threats hidden within encrypted traffic by analyzing metadata and behavioral patterns without requiring SSL/TLS decryption.		
25	The solution must automatically detect and profile network traffic related to command-and-control (C2) communication, ransomware, malware, and data exfiltration.		
26	The solution must have built-in capabilities to detect and alert on common attack techniques, including DDoS attacks, port scanning, and peer-to-peer (P2P) traffic.		
27	The solution must provide full packet capture (FPC) capabilities to record network conversations for in-depth forensic analysis. The storage and retrieval of this data must be scalable and efficient.		

28	The system shall provide automated threat- hunting capabilities to proactively search historical network traffic for indicators of compromise (IOCs) and indicators of attack (IOAs) that may have been previously undetected		

Threat Intelligence & Analytics

Threat Intelligence is the most important component in analyzing threats and security related incidents. Threat intelligence data need to be fed to the SIEM tool for better detection and quick response in case of security incident.

S. No.	Specification of Threat Intelligence	Compliance / Non-Compliance
	General Features	
1.	Threat Intelligence should deliver a comprehensive range of timely adversary and technical threat intelligence through a customizable portal or Dashboard	
2.	Receive feeds from a threat intelligence repository maintained by the OEM and from leading global intelligence sources. Supports external threat intelligence such as D-Shield, Spam Haus etc. which could be used to identify incidents based on knowledge of global security research, to supplement its own threat feed	
3.	Threat Intelligence should provide data feeds and API's for automated consumption by the SIEM Tool	
4.	Threat Intelligence provided must be relevant, context-rich, timely and accurate	
5.	Threat Intelligence feeds should contain who, how and why are you being targeted	
6.	Threat Intelligence must enable to perform countermeasures for current and future threats	
7.	Threat intelligence feeds should enable efficient security operations and reduce the time for investigation	
8.	Threat Intelligence should be capable to integrate with security, risk and management systems and provide insights about emerging and current threats	
9.	The threat intelligence feeds should be available in multiple formats (CSV, XML, CEF).	
10.	Threat intelligence should provide an insight into current and emerging threats	

Threat Intelligence Portal/Dashboard		
11.	The Threat Intelligence Portal/Dashboard should provide a complete range of adversary and technical intelligence.	
12.	The Threat Intelligence Portal/Dashboard should provide End-to-End picture of threats	
13.	The Threat Intelligence Portal/Dashboard should provide Adversary Intelligence	
14.	Threat Intelligence to provide reputation data feeds for actionable intelligence on IP addresses and Domains/URLs exhibiting malicious activity such as malware distribution and botnet command and control server communication. The data feeds should be derived from activity on the Internet and a reputation score along with additional contextual attributes should be provided for each of the IP address and Domains/URLs.	

Advanced Alert Analytics & Attack Detection Capabilities

S. No.	Specification of alert analytics & attack detection capabilities	Compliance / Non-Compliance
	General Features	
1.	The solution should have capabilities to detect any compromises by linking related alerts collected together over a period of time.	
2.	Solution should have capabilities to correlate alerts between sources & destination IPs to find similar or colluding threat signals.	
3.	Solution should have a knowledge base on methods used by attackers in various past breaches globally to create models to detect such attacks.	
4.	Solution should utilize data science techniques to identify kill chains for attacks such as lateral movements e.g. If a destination IP of one alert later becomes a source IP of another alert this suggests existence of a sequence.	
5.	Solution should have detection models to find out threat's sources are linked to the same attacker by grouping alerts with common characteristics like time, day location, target asset profiles etc.	

Signature of Bidder ……

Name: ……

Designation ……

Place: ……

Date: ……..

Seal of BA Organization

7.8 ANNEXURE 8 - PRICE BID

To be uploaded as pdf (On Organization Letter Head)

EOI NO. RCIL/SR/ERS/2025-26/EOI/06 DTD. 25-09-2025

To,

The Joint General Manager (ERS)
RailTel Corporation India Limited,
Kerala Territory Office,
1st Floor, Eastern Entry Tower
Ernakulam South Railway Station, Ernakulam – 682016

TENDER NO: **Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025**

The RFP published by KSITM for the work vide **Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025** as circulated,please be referred for any clarifications. **The submission of EMD, PBG, SD and Agreement with RCIL Non-Judicial paper by the selected Bidder will be sacrosanct selected Bidder**.

BOQ

Name of the Bidder:

A. Capex: Supply, Installation and Commissioning of SOC equipment- SIEM, UEBA, TIP, SOAR

Sl No.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes	GST	Total Amount with Tax
1	Supply, installation, configuration and commissioning of SIEM, SOAR, UEBA, TIP as per technical specification in RFP and provide OEM's onsite warranty support for three years.	1	No				
2	Supply, installation, configuration and commissioning of NDR as per technical specification in RFP and provide OEM's onsite warranty support for three years.	1	No				
3	Supply, installation, configuration and commissioning of Log Collectors as per the requirements mentioned in the RFP and provide OEM's onsite warranty support for three years.	18	No				

B. Opex: Charges for providing managed SOC services

Sl.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes	GST	Total Amount with Tax

1	Quarterly Charges for providing Managed SOC services as per deliverables/ service requirements mentioned in RFP	20	Per Quarter				

C. Additional manpower (resource) cost

Sl.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes	GST	Total Amount with Tax
1	Quarterly Charges for providing additional L1 resource as per details mentioned in RFP	1	Per Quarter				
2	Quarterly Charges for providing additional L2 resource as per details mentioned in RFP	1	Per Quarter				

D. Additional license cost:

Sl.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes	GST	Total Amount with Tax
1	Additional SIEM licenses for 10,000 EPS	1	LOT				
2	Additional Log Collectors	1	No				

E. Annual Maintenance cost:

Sl.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes	GST	Total Amount with Tax
1	AMC for the SIEM, SOAR, TIP and UEBA for 4th year	1	No				
2	AMC for the SIEM, SOAR, TIP and UEBA for 5th year	1	No				
3	AMC for NDR for 4th year	1	No				
4	AMC for NDR for 5th year	1	No				
5	AMC for Log Collectors for 4th year	18	No				
6	AMC for Log Collectors for 5th year	18	No				

Signature of Bidder …….

Name: ……

Designation …….

Place: ……

Date: ……..

Seal of BA Organization

7.9 ANNEXURE 9 - PROFORMA FOR PERFORMANCE BANK GUARANTEE

(On Stamp Paper of ₹ Two Hundred/requisite value)

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Ref. No.: CERT-K/9/2025-KSITM dated 03-09-2025; latest amendment/ Corrigendum clarifications. Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)

In consideration of the RailTel Corporation of India Limited (CIN: L64202DL2000GOI107905), having its registered office at Plate-A, 6th Floor, Office Block Tower-2, East Kidwai Nagar, New Delhi – 110023 (herein after called "RailTel") having agreed to exempt ..... (CIN: .....) having its registered office at..... (Herein after called "the said Contractor") from the demand, under the terms and conditions of Purchase Order No ..... dated..... made between RailTel and.....for (hereinafter called "the said Agreement") of security deposit for the due fulfilment by the said Contractor of the terms and condition contained in the said Agreement, or production of a Bank Guarantee for Rs. ..... (Rs..... Only). We ..... (Indicate the name and address and other particulars of the Bank) (hereinafter referred to as 'the Bank') at the request of .....contractor do hereby undertake to pay RailTel an amount not exceeding Rs. ..... (Rs ..... Only) against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor of any of the terms or conditions contained in the said Agreement.

1. We, ...the Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage by the said Contractor of any of terms or conditions contained in the said Agreement by reason of the Contractor's failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this Guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs ..... (Rs.....Only).

2. We, ... the Bank undertake to pay the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor shall have no claim against us for making such payment.

3. We, ... the Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said

Agreement have been fully paid an its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said contractor and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before .....We shall be discharged from all liability under this Guarantee thereafter.

4. We, …… the Bank further agree with the RailTel that the RailTel shall have fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for anytime or from time to time any of the powers exercisable by the RailTel against the said Contractor and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

This Guarantee will not be discharge due to the change in the constitution of the Bank or the Contract or (..... indicate the name of Bank ……) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of RailTel in writing.

Dated the …… Day of …… 2025 for .....(Name of Bank) In the presence of Witnesses:

1.Signature with Date & Name

2. Signature With Date & Name

Signature of Bidder …….
Name: ……
Designation …..... Seal of BA Organization
Place: ……
Date: ……..

7.10 ANNEXURE 10 - NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (this "Agreement") is made and entered into on this____day of, 2021 (the "Effective Date") at by and between RailTel Corporation of India Limited, (CIN: L64202DL2000GOI107905), a Public Sector Undertaking under Ministry of Railways, Govt. of India, having its registered and corporate office at Plate-A, 6th Floor, Office Block, Tower -2, East Kidwai Nagar, New Delhi-110023 & Southern Region office at 1-10-39 to 44, 6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road, Opp. Shoppers Stop, Hyderabad- 500016, (hereinafter referred to as 'RailTel'), which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of the ONE PART, and) (CIN:_____), a company duly incorporated under the provisions of Companies Act, having its registered office at , (hereinafter referred to as ' '), which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of OTHER PART RailTel and_____shall be individually referred to as "Party" and jointly as "Parties" WHEREAS, RailTel and_____ , each possesses confidential and proprietary information related to its business activities, including, but not limited to, that information designated as confidential or proprietary under Section 2 of this Agreement, as well as technical and non- technical information, patents, copyrights, trade secrets, know-how, financial data, design details and specifications, engineering, business and marketing strategies and plans, forecasts or plans, pricing strategies, formulas, procurement requirements, vendor and customer lists, inventions, techniques, sketches, drawings, models, processes, apparatus, equipment, algorithms, software programs, software source documents, product designs and the like, and third party confidential information (collectively, the "Information"); WHEREAS, the Parties have initiated discussions regarding a possible business relationship for WHEREAS, each Party accordingly desires to disclose certain Information (each Party, in such disclosing capacity, the "Disclosing Party") to the other Party (each Party, in such receiving capacity, the "Receiving Party") subject to the terms and conditions of this Agreement.

NOW THEREFORE, in consideration of the receipt of certain Information, and the mutual promises made in this Agreement, the Parties, intending to be legally bound, hereby agree as follows:

1. Permitted Use.

(a) Receiving Party shall:

(i) hold all Information received from Disclosing Party in confidence;

(ii) use such Information for the purpose of evaluating the possibility of entering into a commercial arrangement between the Parties concerning such Information; and

(iii) restrict disclosure of such Information to those of Receiving Party's officers, directors, employees, affiliates, advisors, agents and consultants (collectively, the "Representatives") who the Receiving Party, in its reasonable discretion, deems need to know such Information, and are bound by the terms and conditions of (1) this Agreement, or (2) an agreement with terms and conditions substantially similar to those set forth in this Agreement.

(b) The restrictions on Receiving Party's use and disclosure of Information as set forth above shall not apply to any Information that Receiving Party can demonstrate:

(i) is wholly and independently developed by Receiving Party without the use of Information of Disclosing Party;

(ii) at the time of disclosure to Receiving Party, was either (A) in the public domain, or (B)known to Receiving Party;

(iii) is approved for release by written authorization of Disclosing Party; or

(iv) is disclosed in response to a valid order of a court or other governmental body in the India or any political subdivision thereof, but only to the extent of, and for the purposes set forth in, such order; provided, however, that Receiving Party shall first and immediately notify Disclosing Party in writing of the order and permit Disclosing Party to seek an appropriate protective order.

(c) Both parties further agree to exercise the same degree of care that it exercises to protect its own Confidential Information of a like nature from unauthorized disclosure, but in no event shall a less than reasonable degree of care be exercised by either party.

2. Designation.

(a) Information shall be deemed confidential and proprietary and subject to the restrictions of this Agreement if, when provided in:

(i) written or other tangible form, such Information is clearly marked as proprietary or confidential when disclosed to Receiving Party; or

(ii) oral or other intangible form, such Information is identified as confidential or proprietary at the time of disclosure.

3. Cooperation. Receiving Party will immediately give notice to Disclosing Party of any unauthorized use or disclosure of the Information of Disclosing Party.

4. Ownership of Information. All Information remains the property of Disclosing Party and no license or other rights to such Information is granted or implied hereby. Notwithstanding the foregoing, Disclosing Party understands that Receiving Party may currently or in the future be developing information internally, or receiving information from other parties that may be similar to Information of the Disclosing Party. Notwithstanding anything to the contrary, nothing in this Agreement will be construed as a representation or inference that Receiving Party will not develop products, or have products developed for it, that, without violation of this Agreement, compete with the products or systems contemplated by Disclosing Party's Information.

5. No Obligation. Neither this Agreement nor the disclosure or receipt of Information hereunder shall be construed as creating any obligation of a Party to furnish Information to the other Party or to enter into any agreement, venture or relationship with the other Party.

6. Return or Destruction of Information.

(a) All Information shall remain the sole property of Disclosing Party and all materials containing any such Information (including all copies made by Receiving Party) and its Representatives shall be returned or destroyed by Receiving Party immediately upon the earlier of:

(i) termination of this Agreement;

(ii) expiration of this Agreement; or

(iii) Receiving Party's determination that it no longer has a need for such Information.

(b) Upon request of Disclosing Party, Receiving Party shall certify in writing that all Information received by Receiving Party (including all copies thereof) and all materials containing such Information (including all copies thereof have been destroyed.

7. Injunctive Relief: Without prejudice to any other rights or remedies that a party may have, each party acknowledges and agrees that damages alone may not be an adequate remedy for any breach of this Agreement, and that a party shall be entitled to seek the remedies of injunction, specific performance and/or any other equitable relief for any threatened or actual breach of this Agreement.

8. Notice.

(a) Any notice required or permitted by this Agreement shall be in writing and shall be delivered as follows, with notice deemed given as indicated:

(i) by personal delivery, when delivered personally;

(ii) by overnight courier, upon written verification of receipt; or

(iii) by certified or registered mail with return receipt requested, upon verification of receipt.

(b) Notice shall be sent to the following addresses or such other address as either Party specifies in writing.

RailTel Corporation of India limited:

Attn:

Address:

Phone:

Email:

9. Term, Termination and Survivability.

(a) Unless terminated earlier in accordance with the provisions of this agreement, this Agreement shall be in full force and effect for a period of years from the effective date hereof.

(b) Each party reserves the right in its sole and absolute discretion to terminate this Agreement by giving the other party not less than 30 days' written notice of such termination.

(c) Notwithstanding the foregoing clause 9(a) and 9 (b), Receiving Party agrees that its obligations, shall:

(i) In respect to Information provided to it during the Term of this agreement, shall survive and continue even after the expiry of the term or termination of this agreement; and

(ii) not apply to any materials or information disclosed to it thereafter.

10. Governing Law and Jurisdiction. This Agreement shall be governed in all respects solely and exclusively by the laws of India without regard to its conflicts of law principles. The Parties hereto expressly consent and submit themselves to the jurisdiction of the courts of New Delhi.

11. Counterparts. This agreement is executed in duplicate, each of which shall be deemed to be the original and both when taken together shall be deemed to form a single agreement

12. No Definitive Transaction. The Parties hereto understand and agree that no contractor agreement with respect to any aspect of a potential transaction between the Parties shall be deemed to exist unless and until a definitive written agreement providing for such aspect of the transaction has been executed by a duly authorized representative of each Party and duly delivered to the other Party (a "Final Agreement"), and the

Parties hereby waive, in advance, any claims in connection with a possible transaction unless and until the Parties have entered into a Final Agreement.

13. Settlement of Disputes:

(a) The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation or consultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.

b) In the event of any dispute, difference, conflict or question arising between the parties hereto, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator

14. The sole arbitrator shall be appointed by RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both

parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the part.

15.CONFIDENTIALITY OF NEGOTIATIONS

Without the Disclosing Party's prior written consent, the Receiving Party shall not disclose to any Person who is not a Representative of the Receiving Party the fact that Confidential Information has been made available to the Receiving Party or that it has inspected any portion of the Confidential Information or that discussions between the Parties may be taking place.

16. REPRESENTATION

The Receiving Party acknowledges that the Disclosing Party makes no representation or warranty as to the accuracy or completeness of any of the Confidential Information furnished by or on its behalf. Nothing in this clause operates to limit or exclude any liability for fraudulent misrepresentation.

17. ASSIGNMENT

Neither this Agreement nor any of the rights, interests or obligations under this Agreement shall be assigned, in whole or in part, by operation of law or otherwise by any of the Parties without the prior written consent of each of the other Parties. Any purported assignment without such consent shall be void. Subject to the preceding sentences, this Agreement will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns.

18. EMPLOYEES AND OTHERS

Each Party shall advise its Representatives, contractors, subcontractors and licensees, and shall require its Affiliates to advise their Representatives, contractors, subcontractors and licensees, of the obligations of confidentiality and non-use under this Agreement, and shall be responsible for ensuring compliance by its and its Affiliates' Representatives, contractors, subcontractors and licensees with such obligations. In addition, each Party shall require all persons and entities who are not employees of a Party and who are provided access to the Confidential Information, to execute confidentiality or non- disclosure agreements containing provisions no less stringent than those set forth in this Agreement. Each Party shall promptly notify the other Party in writing upon learning of any unauthorized disclosure or use of the Confidential Information by such persons or entities.

19. NO LICENSE

Nothing in this Agreement is intended to grant any rights to under any patent, copyright, or other intellectual property right of the Disclosing Party, nor will this Agreement grant the Receiving Party any rights in or to the Confidential Information of the Disclosing Party, except as expressly set forth in this Agreement.

20. RELATIONSHIP BETWEEN PARTIES:

Nothing in this Agreement or in any matter or any arrangement contemplated by it is intended to constitute a partnership, association, joint venture, fiduciary relationship or other cooperative entity between the parties for any purpose whatsoever. Neither party has any power or authority to bind the other party or impose any obligations on it and neither party shall purport to do so or hold itself out as capable of doing so.

21. UNPULISHED PRICE SENSITIVE INFORMATION (UPSI)

agrees and acknowledges that_____, its Partners, employees, representatives etc.,by virtue of being associated with RailTel and being in frequent communication with RailTel and its employees, shall be deemed to be "Connected Persons" within the meaning of SEBI (Prohibition of Insider Trading) Regulations, 2015 and shall be bound by the said regulations while dealing with any confidential and/ or price sensitive information of RailTel. shall always and at all times comply with the obligations and restrictions contained in the said regulations. In terms of the said regulations_____shall abide by the restriction on communication, providing or allowing access to

any Unpublished Price Sensitive Information (UPSI) relating to RailTel as well as restriction on trading of its stock while holding such Unpublished Price Sensitive Information relating to RailTel

22. MISCELLANEOUS.

This Agreement constitutes the entire understanding among the Parties as to the Information and supersedes all prior discussions between them relating thereto. No amendment or modification of this Agreement shall be valid or binding on the Parties unless made in writing and signed on behalf of each Party by its authorized representative. The failure or delay of any Party to enforce at any time any provision of this Agreement shall not constitute a waiver of such Party's right thereafter to enforce each and every provision of this Agreement. In the event that any of the terms, conditions or provisions of this Agreement are held to be illegal, unenforceable or invalid by any court of competent jurisdiction, the remaining terms, conditions or provisions hereof shall remain in full force and effect. The rights, remedies and obligations set forth herein are in addition to, and not in substitution of, any rights, remedies or obligations which may be granted or imposed under law or in equity.

IN WITNESS WHEREOF, the Parties have executed this Agreement on the date set forth above.

By Name:	RailTel Corporation India Limited:
Title:	By Name :
Witnesses:	Title:

7.11 ANNEXURE 11 - PRE -BID AGREEMENT

(To be executed in presence of public notary on non-judicial stamp paper of the value of Rs. 200/-. The stamp paper has to be in the name of the BA)

This Pre-Bid Agreement (the "**Agreement**") is made at New Delhi on this_____Day of (month) 2025.

BETWEEN

M/s. RailTel Corporation Of India Limited, (CIN: L64202DL2000GOI107905) a company registered under the Companies Act 1956, having its registered and corporate office at Plate-A, 6th Floor, Office Block, Tower-2, East Kidwai Nagar, New Delhi India – 110 023 and Southern Regional office at 1-10-39 to 44, 6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road, Opp. Shoppers Stop, Hyderabad-500 016 (hereinafter referred to as **"RailTel"** which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns) of the **FIRSTPART. AND M/s. _XXXX_**, (CIN:_____) a company registered under the Companies Act 1956, having its registered office at and its Corporate Office located at_____(hereinafter referred to as **"_XXXX_"** which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns) of the **SECOND PART.**

RailTel and_____shall be hereinafter individually referred to as "**Party**" And collectively as "**Parties**. "**Whereas**,

A) RailTel is a "Mini Ratna (Category-I)" CPSU of Ministry of Railways, having exclusive right of way along Indian Railways and has created an OFC backbone and associated transport and network infrastructure to provide carrier class telecom services. RailTel has Unified License issued by DoT to provide a range of telecom services. RailTel also has two tier III certified data centres at Secunderabad and Gurugram. RailTel has created a slew of digital services like cloud, hosting, hosted Video Conferencing service, Aadhar Services, Content delivery platform, WIFI as a service etc. RailTel has strong capabilities in managing telecom infrastructure, MPLS network infrastructure, data centre services like as (Infrastructure as a Service) and PaaS (Platform as a Service).

B) _____(DETAILS OF SECOND PART)

C) RailTel had floated an **EOI No: _ dated_____pursuant to the RFP floated by End Customer for"__ for End Customer Organization for agreed Scope of Work"(hereinafter referred as "The said work/project/tender"),** and subsequently, based on the offer submitted by M/s XXXX towards the RailTel's EOI, M/s XXXX has been selected by RailTel as Business Associate for the said Project.

D) RailTel is in the process of participating in the tender issued by end customer, complete details of which have deliberately not been shared with XXXX and XXXX has waived its right to get the RFP document of end customer owing to confidentiality concern raised by the end customer. However, a limited scope of work on 'need to know basis and as detailed in clause 1.7 below, which will be carried out by XXXX has been shared with XXXX and based on the representation of "XXXX" that "XXXX" has read the said limited Scope of Work and has understood the contents thereof and that "XXXX" has sufficient experience to execute the said limited and defined scope of work, the Parties have mutually decided to form a " Business association" wherein RailTel shall act as the "Bidder" and "XXXX" shall act as the "business associate" in terms of the said Tender and in accordance to the terms agreed hereunder;

E) RailTel shall submit Rupees YYYY as BG against pre integrity pact at the time of submission of bid as an Integrity Pact bank guarantee to end customer and accordingly "XXXX" shall submit Rupees ZZZZ as BG of pre integrity pact on back-to-back basis to RailTel before final submission of the said bid to end customer. **(This is applicable on cases to case basis as per CIAL requirement. May please read in conjunction of the current RFP.)**

F) Party hereby acknowledges that RailTel has received Rs. /- (Rs._____) from M/s XXXX as per the Terms and conditions of EOI no. dated_____.

G) The Parties are thus entering into this Agreement to record the terms and conditions of their understanding and the matters connected therewith.

RailTel has agreed to extend all the necessary and required support to "XXXX" during the entire contract period.

NOW, THEREFORE, in consideration of the mutual covenants set forth herein it is hereby agreed by and between the Parties hereto as under:

1. SCOPE OF CO-OPERATION

1.1. Parties have agreed to form a "business association" to co-operate with each other on an exclusive basis with respect to execution of the said Project.

1.2. It has been further agreed between the Parties that Parties shall not bid individually for the said Project nor shall they enter into any arrangement with other parties for the purpose of bidding for the said Project during the validity of this Agreement.

1.3. The Parties also agree that the terms of the said EOI for limited and defined scope of work along with the Corrigendum's issued thereafter shall apply mutatis-mutandis to this Agreement.

1.4. The Parties further agree that they shall, enter into a 'Definitive Agreement' containing elaborate terms and conditions, role and responsibilities and respective scope of work of this Agreement after declaration of RailTel as the successful bidder of the said Project.

1.5. RailTel shall submit the PBG amounting Rs. XXXXX, earnest money deposit / EMD declaration (whichever is applicable) and performance bank guarantee to **End customer** and accordingly "XXXX" shall submit to RailTel, BG amounting to Rs._____as the earnest money deposit. Further, XXXX shall also pay the performance bank guarantee in proportionate to the extent of its defined scope of work.

1.6. RailTel may further retain some portion of the work mentioned in the end organization's RFP, where RailTel has competence so that overall proposal becomes most winnable proposal.

XXXX agrees, undertakes and acknowledges that following shall be Scope of Work of XXXX out of the total project work.:

2. Technical Terms – As per CIAL/RCIL document

3. TERM AND TERMINATION

3.1. This Agreement shall come into force as of the date of signing and shall continue to be in full force and effect till the complete discharge of all obligations, concerning the carrying out of the said Project, except terminated earlier by the Parties in terms of this Agreement or in terms of the said project, whichever is applicable.

3.2. This Agreement can be terminated by either Parties forthwith in the event of happening of the following events:

(a) End customer announces or notifies the cancellation of the said Project and / or withdrawing the said RFP.

(b) The receipt of an official communication that End customer chooses not to proceed with RailTel for the said Project or RailTel is not short listed by End customer.

(c) Material breach of any of the terms and conditions of this Agreement by either of the Parties and the same is not rectified by the defaulting Party beyond 15 (fifteen) days (ora reasonable time period as mentioned under the notice issued by the other Party) from the date of receipt of notice from the other Party to cure the said breach.

3.3. Parties agree and understand that as of the execution of this Agreement they are contractually bound and obligated to perform the services, obligations and the scope of work entrusted, should RailTel be declared as the successful bidder of the said Project. Any Party shall not withdraw its participation subsequent to execution of this Agreement, at any point in time except in case of material breach of any of the terms of the Agreement.

3.4. In case "XXXX" breach the terms of Agreement i.e. defaulting party in such case the balance unsupplied quantity or service shall be completed by RailTel i.e. non-defaulting party and cost for completion of that balance unsupplied quantity or service of such defaulting party shall be executed by RailTel at the risk and cost of such defaulting party.

4. Liability:

It is understood that the parties are entering into this pre-bid teaming agreement for requirement of submission of bid against the RFP floated by end customer for Implementation of Network Security System and Integration for end

Customer Organization. Parties acknowledge and agree that "XXXX" shall be completely liable for the successful execution of this project, in relation to its defined scope of work (as detailed in clause 1.7 above), fully complying the end customer requirements. Accordingly, it is agreed that notwithstanding anything contained in the RFP document, "XXXX" shall be liable to RailTel with regard to its obligations and liability to complete the agreed and defined scope of work as detailed in clause 1.7 above.

5. EXCLUSIVITY

Parties agree to co-operate with each other for the purpose of the said Project on an exclusive basis with respect to applying for, submitting and execution of the said Project including providing of technical demo, proof of concept for the agreed and defined scope of work.

6. PAYMENT TERMS

The payment terms between the parties shall be only on receipt of payment from end customer.

7. TAXES

Parties agrees that they will comply with the Indian Income Tax Act in force from time to time and pay Indian Income Tax, as may be imposed / levied on them by the Indian - Income Tax Authorities, for the payments received by them for the Project under this agreement and any other taxes, cess, surcharge, etc. for their respective scope of works;

8. INDEMNIFICATION

8.1 Parties agree to and undertake to indemnify and hold each other, its officers, directors, agents and employees harmless, from and against any and all claims, demands, causes of action, losses, damages, costs and expenses (including attorney's reasonable fees, costs of investigation and defence) arising out of or resulting from any claim, action or other proceeding (including any proceeding by any of the indemnifying party's employees, agents or contractors) based upon:

i. any breach or contravention of any of the terms, conditions, covenants of this Agreement by the Party;

ii. Unethical business practices;

iii. any acts or omission of the Party and/ or any of its employees, agents or contractors, and the liability for damages to property arising from or out of party operations in connection with the performance of this agreement;

iv. any claim for taxes that might arise or be imposed due to this performance of Services hereunder;

v. any representation or warranty or information furnished by the Party being found to be false;

vi. Parties failure to pay all applicable compensation to its respective personnel;

vii. death or personal injury to any person;

viii. destruction or damage to any property by acts or omissions of either Party, its representatives or personnel;

ix. any violation/non-compliance by the Party with any applicable laws governmental regulations or orders;

x. any third-party liability;

xi improper handling or misuse of the Confidential Information of the Party(ies) by the Party

8.2 XXXX shall be liable to all risks and consequences (including the risk of payments) suffered in the performance of services under the Project and undertakes to indemnify RailTel from and against any non-payments (of RailTel's share payable to RailTel), recoveries and claim from End Customer or any other cost or losses incurred due to default/non-performance on part of XXXX.

9. COMPLIANCES TO STATUTORY OBLIGATIONS

9.1. Parties shall also obtain and keep in place necessary insurance policies, Mediclaim policies, group insurance schemes of adequate value to cover their workmen, supervisors, etc. with regard to any accidents, injury or the liability under the Employee Compensation Act.

9.2. Parties shall observe and be responsible for the compliance of all labour laws (including labour cess) as per government notifications and shall maintain necessary records for the same and shall submit the same to RailTel when so required.

9.3. Parties shall duly maintain all records / registers required to be maintained by them under various labour laws mentioned above and shall produce the same before the concerned Statutory Authorities whenever required and called upon to do so.

10. LEGAL STATUS

This Agreement constitutes a contractual relationship and shall relate solely to the Project and shall not extend to other activities or be construed to create a corporation, body corporate, partnership or any other form of legal entity.

11. REPRESENTATIONS AND COVENANTS

11.1. Each Party represents and warrants to the other Party as follows:

11.1.1. That it has full capacity, power and authority and has obtained all requisite consents and approvals to, enter into and to observe and perform this Agreement and to consummate the transactions contemplated hereunder. Each of the Persons / personnel executing this Agreement on behalf of the each of the Parties have full capacity and authority to sign and execute this Agreement on behalf of the respective Parties;

11.1.2. The execution, delivery and consummation of, and the performance by it, of this Agreement shall not conflict with, violate, result in or constitute a breach of or a default under, (a) any contract by which it or any of its assets or properties, are bound or affected, and/or (b) its constitutional documents;

11.1.3. This Agreement constitutes its legal, valid and binding obligations, enforceable against it, in accordance with their terms under Applicable Statutory Law(s);

11.1.4. It has the right, authority and title to execute this Agreement;

12. SUBCONTRACTING BETWEEN PARTIES

If a Party subcontracts certain supplies or services pertaining to its scope of work to the other party, then the resulting relationship between such parties shall be governed by a separate subcontract. This Agreement shall not in any way be affected thereby except as stated otherwise in this Agreement

13. GOVERNING LAW AND JURISDICTION

The construction, validity and performance of this Agreement shall be governed in all respects by the Laws of India. The Parties hereby submit to the exclusive jurisdiction of the Indian courts at Delhi only.

14. GOOD FAITH NEGOTIATION AND DISPUTE RESOLUTION

The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation orconsultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.

In the event of any dispute, difference, conflict or question arising between the parties here to, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator.

The sole arbitrator shall be appointed by CIAL/RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and

any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the parties.

15. FORCE MAJEURE

"Force Majeure Event" shall mean any event beyond the reasonable control of the affected Party including acts of God, fires, earthquakes, strikes, pandemic, epidemics, lock down, and labour disputes, acts of war or terrorism, civil unrest, economic and financial sanctions, or acts or omissions of any Governmental Authority occurring on or after the Signature Date.

No Party shall be liable to the other if, and to the extent, that the performance or delay in performance of any of its obligations under this Agreement is prevented, restricted, delayed or interfered with, due to a Force Majeure Event. The Party affected by Force Majeure Event shall promptly inform the other Party in writing and shall furnish within 30 (thirty) days thereafter, sufficient proof of the occurrence and expected duration of such Force Majeure Event. The Party affected by Force Majeure Event shall also use all reasonable endeavours to mitigate the negative effects of such Force Majeure Event on such Party's ability to perform its contractual obligations. In the event of a Force Majeure Event, the Parties shall immediately consult with each other in order to find an equitable solution and shall use all reasonable endeavours to minimise the consequences of such Force Majeure Event. The occurrence of a Force Majeure Event shall however, not relieve a Party of any obligation to pay any sum due under this Agreement prior to the occurrence of the Force Majeure Event. If the Force Majeure lasts for more than 6 (six) months, the Parties may mutually decide in writing on the future course of action with respect to this Agreement.

16. INTELLECTUAL PROPERTY RIGHTS

16.1. Each Party shall remain the sole owner of all industrial or intellectual property rights, Technical Data, Know-How, designs, specifications and the like, generated or acquired before the signature, or beyond the scope of this agreement.

16.2. Each Party shall remain the sole owner of all industrial or intellectual property rights, technical data, know-how, design specifications and the like generated solely by that Party during the course of the performance of this agreement and shall not be free to used it by the other party and if the other party uses that intellectual property rights prior permission shall be taken with paying necessary fees for such rights.

16.3. In case of joint development, the work-share and associated ownership of intellectual property of each Party shall be mutually agreed upon and defined in advance in the definitive agreement for the specific program. However, should any invention be jointly made by the Parties in the performance of this agreement, without neither Party being in a position to reasonably claim the ownership of said intellectual property right, the said right shall be jointly owned by the Parties and the corresponding measures of protection for both Parties of the said right as may be practicable shall be mutually agreed by both Parties and cost for such registration of such right shall be borne by the parties proportionately as per the ownership of the rights.

16.4 As on date, Parties confirms that there are no infringements of any Intellectual Property Rights of the products contemplated under this agreement, in accordance with the laws prevailing in the country.

16.5. The Parties undertake and confirm that the Technology / Knowhow / Design owned by each of them and intended to be put into use for execution of various Projects pursuant to this agreement has been originally developed by each of such Parties. The Parties are entitled to all the Intellectual Property Rights in Technology / Knowhow / Design intended to be put into use for execution of various Projects and no third-party Intellectual Property Rights have been put in to use either in their original or modified form without proper authorisation of such third party. The Parties further vouchsafes that the foregoing undertaking is actuated by truth and accuracy and no misrepresentation is being put into use for inducing each other to enter into this agreement.

17. CONFIDENTIALITY

17.1. During the term of this agreement, either party may receive or have access to technical information, as well as information about product plans and strategies, promotions, customers and related non-technical business in formation which the disclosing party considers to be confidential ("Confidential Information as per RFP tender document"). In the event Confidential Information is to be disclosed, the Confidential Information must be marked as confidential at the time of disclosure, or if disclosed orally but stated to be confidential, and be designated as confidential in writing by the disclosing party summarizing the Confidential Information disclosed and sent to the receiving party within thirty (30) days after such oral disclosure.

17.2. Confidential Information may be used by the receiving party only with respect to the performance of its obligations under this Agreement, and only by those employees of the receiving party and its subcontractors who have a need to know such information for purposes related to this Agreement, provided that such subcontractors have signed separate agreements containing substantially similar confidentiality provisions. The receiving party must protect the Confidential Information of the disclosing party by using the same degree of care to prevent the unauthorized use, dissemination or publication of such Confidential Information, as the receiving party uses to protect its own confidential information of like nature.

17.3. The obligations is not applicable to any information which is:

17.3.1. Already known by the receiving party prior to disclosure;

17.3.2. Publicly available through no fault of the receiving party;

17.3.3. Rightfully received from a third party without being responsible for its confidentiality;

17.3.4. Disclosed by the disclosing party to a third party without being responsible for its Confidentiality on such third party;

17.3.5. Independently developed by the receiving party prior to or independent of the disclosure;

17.3.6. Disclosed under operation of law;

17.3.7. Disclosed by the receiving party with the disclosing party's prior written approval.

17.4. XXXX agrees and acknowledges that XXXX, its Partners, employees, representatives etc. by virtue of being associated with RailTel and being in frequent communication with RailTel and its employees, shall be deemed to be “Connected Persons” within the meaning of SEBI (Prohibition of Insider Trading) Regulations, 2015 and shall be bound by the said regulations while dealing with any confidential and/ or price sensitive information of RailTel. XXXX shall always and at all times comply with the obligations and restrictions contained in the said regulations. In terms of the said regulations, XXXX shall abide by the restriction on communication, providing or allowing access to any Unpublished Price Sensitive Information (UPSI)relating to RailTel as well as restriction on trading of its stock while holding such Unpublished Price Sensitive Information relating to RailTel

17.5 Notwithstanding anything contained in this agreement, XXXX undertakes, agrees and acknowledges that being RailTel’s Business Associate, XXXX shall maintain utmost confidentiality in relation to said Project. XXXX further, undertakes that any information relating to said Project which is or will be disclosed/ divulged by RailTel on need to know basis, will be received and treated by XXXX as strictly confidential and XXXX shall not, without the prior written consent of the RailTel or as expressly permitted herein, disclose or make available to any other person such information.

18. NOTICES

Notices, writings and other communications under this Agreement may be delivered by hand, by registered mail, by courier services or facsimile to the addresses as set out below:

To RailTel Corporation Of India Limited

To: RailTel Corporation of India Ltd

Attn: Executive Director / Southern Region

Address:1-10-39 to 44, 6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road, Opp. Shoppers Stop, Hyderabad-500016 No.: +91-40-27788000

To XXXX

To: XXXX

Kind Attn: _____Address: _____ Mob. No.:
Email:

19. AMENDMENT

No amendment or modification or waiver of any provision of these presents, nor consent to any departure from the performance of any obligations contained herein, by any of the Parties hereto, shall in any event be valid and effective unless the same is in writing and signed by the Parties or their duly authorized representative especially empowered in this behalf and the same shall be effective only in respect of the specific instance and for the specific purpose for which it is given.

20. PRIOR UNDERSTANDING

This Agreement contains the entire Agreement between the Parties to this Agreement with respect to the subject matter of the Agreement, is intended as a final expression of such Parties' agreement with respect to such terms as are included in this Agreement is intended as a complete and exclusive statement of the terms of such agreement, and supersedes all negotiations, stipulations, understanding, Agreements, representations and warranties if any, with respect to such subject matter, which precede or accompany the execution of this Agreement.

21. GENERAL

21.1. Binding Effect:

This Agreement shall be binding upon and inure to the benefit of the Parties here to and their respective legal successors.

21.2. Counterpart:

This Agreement may be executed simultaneously in 2 (two) counterparts, each of which shall be deemed to be original and all of which together shall constitute the same Agreement.

21.3. Non-Partnership:

21.3.1. This Agreement shall be on a principal-to-principal basis and shall not create any principal- agent relationship between the Parties.

21.3.2. Nothing in this Agreement shall be deemed to constitute a partnership or joint venture between the Parties or otherwise entitle either Party to have an authority to bind the other Party for any purpose.

21.4. Severability:

In the event any provision of this agreement is held invalid or un-enforceable by a court of competent jurisdiction, such provision shall be considered separately and such determination shall not invalidate the other provisions of this agreement and annexure/s which will be in full force and effect.

21.5. Waiver:

A failure by any Party to exercise or enforce any rights conferred upon it by this Agreement shall not be deemed to be a waiver of any such rights or operate so as to bar the exercise or enforcement thereof at any subsequent time.

21.6. Time is of essence:

Time is the essence of this agreement and the Parties herein agree and acknowledge to abide by the same.

22. Miscellaneous

22.1. No Party to this agreement will have any rights or obligations arising from or in relation to this agreement in excess of those rights and obligations expressly declared herein.

22.2. No Party to this agreement is entitled to sell, assign or otherwise transfer any of its rights and/or obligations arising from or in relation to this agreement to any third party, without the prior written consent of the other Party of this agreement.

22.3. Each Party shall be solely responsible for its own actions or failures to act and for its own commitments and undertakings. Neither Party shall present itself as the representative or agent of the other Party, nor shall it have the power or the authority to commit the other Party, unless it receives the other Party's prior written consent.

22.4. No release shall be made by any Party to the news media or the general public relating to this agreement and/or the subject matter thereof without prior written approval of the other Party.

22.5. During the term of this agreement, each party shall refrain from taking any action or attempt to take any action with the intent of impairing or causing prejudice to the business relationship, whether existing or prospective that subsists between the other party and its customers and business partners. Each party shall also desist from inducing or influencing or attempting to induce or influence any customer or business partner, whether existing or prospective of the other party, resulting into prejudice or detriment to business prospects of the other party.

Furthermore, Parties shall not compete with or cause detriment to the business prospects of each other by making use of confidential information, whether in its embodied or disembodied form, shared pursuant to this agreement.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the day and year first above written.

For RailTel Corporation Of India Limited	For XXXX
Authorised Signatory	Authorized Signatory
Name:	Name
Designation:	Designation:
In Presence of witness	
Signature:	Signature:
Name:	Name:
Address:	Address:

7.12 ANNEXURE 12 FORMAT FOR AFFIDAVIT TO BE UPLOADED BY BA ALONGWITH THE EOI DOCUMENTS

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 200/-The paper has to be in the name of the BA) **

I_____ (Name and designation) ** appointed as the attorney/authorized signatory of the BA (including its constituents), M/s (hereinafter called the BA) for the purpose of the EOI documents for the work of _____ as per the EOI No.

of (RailTel Corporation of India Limited), do hereby solemnly affirm and state on the behalf of the BA

including its constituents as under:

1. I/we the BA (s), am/are signing this document after carefully reading the contents.

2. I/we the BA(s) also accept all the conditions of the EOI and have signed all the pages in confirmation thereof.

3. I/we hereby declare that I/we have downloaded the EOI documents from RailTel website www.railtelindia.com. I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the EOI document. In case of any discrepancy noticed at any stage i.e., evaluation of EOI, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.

4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.

5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.

6. I/we declare that the information and documents submitted along with the EOI by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.

7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of EOI, it shall lead to forfeiture of the EOI EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the BA) ** and all my/our constituents understand that my/our constituents understand that my/our offer shall be EMD rejected.

8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

VERIFICATION

SEAL AND SIGNATURE OF THE DEPONENT

I/We above named EOI do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT

Place:

Dated:

SEAL AND SIGNAURE OF THE BA

**The contents in Italics are only for guidance purpose. Details as appropriate, are to be filled in suitably by BA. Attestation before Magistrate/Notary Public.

Signature of Bidder ……..
Name: ……
Designation ……..
Place: ……
Date: ……..

Seal of BA Organization

Kerala State IT Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

REQUEST FOR PROPOSAL (RFP)

FOR

SETTING UP A SECURITY OPERATIONS CENTRE (SOC)

TENDER NO: 2025_KSITM_794318_1
SEP 03, 2025

Table of Contents

Section I: Invitation to Bid

This invitation to Bid is for the selection of the System Integrator for the **"Supply, Installation and Commissioning of Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), UEBA, Threat Intelligence Platform, Network Detection & Response Solutions and the management of the State SOC"** at State Data Centre 2, Tejaswini Building, Technopark, Thiruvananthapuram for establishing a State SOC.

The Bidders are advised to study the tender document carefully. Submission of Bids shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications. This section provides general information about the Issuer (i.e., Kerala State IT Mission), important dates and addresses and the overall eligibility criteria for the Bidders.

1.1 Issuer

Kerala State IT Mission herein after refers as KSITM invites proposals for the selection of the System Integrator for the **"Supply, Installation and Commissioning of Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), UEBA, Threat Intelligence Platform, Network Detection & Response and the management of the State SOC"** as per the scope of the Bid.

1.2 Issuer and Address for Bid Submission & Correspondence

The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444
E-Mail: director.ksitm@kerala.gov.in

1.3 Key Events & Dates

Table I – Key Events & Dates

Event	Target Date
Bid Inviting Authority	Kerala State Information Technology Mission
Tender Reference No:	CERT-K/9/2025-KSITM
Mode of Tender Submission	Tender should be submitted online at "https://etenders.kerala.gov.in"
Tender Fee	₹29,500 (Rupees Twenty Nine Thousand Five Hundred only) Inclusive of tax
EMD (Earnest Money Deposit)	₹20,00,000 (Rupees Twenty Lakhs only)
Date and Time for Pre- Bid Conference	09.09.2025; 12:00 PM
Pre-Bid Meeting Venue	➢ Pre-bid meeting will be held online ➢ Link: https://meet.google.com/sjo-iftz-ood ➢ Bidder to submit a maximum of 2 participant's names, contact numbers, designations and e-mail IDs to cert.ksitm@kerala.gov.in at least one day in advance along with pre-bid queries.
Last date & Time for Uploading of e-Bids[Cover1& 2]	Refer https://etenders.kerala.gov.in/
Opening of Technical Bids	Refer https://etenders.kerala.gov.in/
Presentation on Technical Bids by short-listed bidders	Refer https://etenders.kerala.gov.in/
Opening of commercial Bids	Refer https://etenders.kerala.gov.in/

Section II: Instruction to the Bidders

2.1 Definitions

1. "**KSITM**" means Kerala Stata IT Mission
2. "**SDC 1**" means Kerala State Data Centre 1 at Co-bank Towers, Palayam, Thiruvananthapuram
3. "**SDC 2**" means Kerala state Data Centre 2 at Tejaswini, Technopark, Thiruvananthapuram
4. "**DCO**" means Data Centre Operator
5. **"Bidder"** shall mean an Individual Company registered under the Companies Act 1956 or as defined in this document that participates in the Bidding process, also termed as System Integrator (SI)
6. **"KSITM's Representative"** shall mean the person appointed by KSITM from time to time to act on its behalf at the site for overall coordination, supervision and project management at site
7. The **"Successful bidder / System Integrator (SI)**" means the company with whom the order has been placed for providing Services as specified in this tender/contract and shall be deemed to include the Implementation Agency's successors, representatives (approved by KSITM), heirs, executors, administrators and permitted assigns, as the case may be, unless excluded by the terms of the contract
8. **"Contract"** means the Agreement entered into between KSITM and the "Successful Bidder" as recorded in the Contract form signed by KSITM and the "Implementation Agency" including all attachments and Annexes thereto, the Tender and all Annexes thereto and the agreed terms as set out in the Bid, all documents incorporated by reference therein and amendments and modifications to the above from time to time
9. **"Confidential Information"** means any information disclosed to or by any Party to this Contract and includes any information in relation to the Parties, a third party or any information with regard to any taxpayer, or any other person who is covered within the ambit of any commercial taxes legislation including any such information that may come to the knowledge of the Parties hereto / Bidder's Team by virtue of this Contract that:
    a) By its nature or by the circumstances in which it is disclosed is confidential; or
    b) Is designated by the disclosing Party as confidential or identified in terms connoting its confidentiality; but does not include information which is or becomes public knowledge other than by a breach of this Contract
10. "**The Contract Price/Value**" means the price payable to the successful bidder under the Contract for the full and proper performance of its contractual obligations
11. **"Parties"** means KSITM and the successful bidder and "Party" means either of the Parties
12. **"Service"** means facilities/services to be provided as per the requirements specified in this tender document and any other incidental services, such as installation, implementation, support and provision of technical assistance and other such obligations of the Successful bidder covered under the Contract

2.2 Procurement of RFP Document

The tender document can be downloaded from State e-Procurement www.etenders.kerala.gov.in website. Bidders should submit their bids through this e-tendering website.

Bidders should remit tender fee of ₹29,500/- (Rupees Twenty Nine Thousand Five Hundred only) (Non-refundable) towards tender documents fees and Earnest Money Deposit (EMD) of ₹20,00,000/-(Rupees Twenty Lakhs only) at the time of online bid submission. The Bid will not be considered in the absence of payment of the tender fee and EMD.

Bidders are requested to follow the instructions regarding e-tendering given in the download section of www.etenders.kerala.gov.in for understanding the procedures for online bid submission and payment.

2.3 Pre-Bid Meeting

KSITM shall organize Online Pre-Bid Meeting on the scheduled date and time. KSITM may incorporate any changes in the RFP based on acceptable suggestions received during the interactive Pre-Bid Conference. The decision of the KSITM regarding acceptability of any suggestion shall be final and shall not be called upon to question under any circumstances.

The prospective Bidders shall submit their questions in writing, no later than the date and time indicated under section 1.3 above. It may not be possible at the Pre-Bid Meeting to answer questions which are received late. However, prospective Bidders can submit their queries during the meeting and responses / corrigendum will be published by KSITM in the eTenders portal(www.etenders.kerala.gov.in).

2.4 Amendment of RFP Document

At any time before the deadline for submission of Bids, KSITM may, for any reason, whether at own initiative or in response to a clarification requested by a prospective Bidder, modify the Bidding document by amendment. All the amendments made in the document would be published on the website www.etenders.kerala.gov.in. **The Bidders are also advised to visit the aforementioned website on regular basis for checking necessary updates**. KSITM also reserves the right to amend the dates mentioned in section 1.3 of this Bid document. The bidders would be given a period of at least 5 working days for submissions of bids after any such change in the RFP.

2.5 Venue and Deadline for submission of Proposal

Proposals must be received through www.etenders.kerala.gov.in not later than dates specified in Section 1.3 of this volume.

2.6 Procedure for Submission of Bids

2.6.1 Modes of Submission

a) It is proposed to have a Two packet for this e-tender:
   i. Technical Bid - which includes documents for Pre-qualification Criteria and Technical proposal
   ii. Commercial Bid

   Please Note that Prices shall be indicated only in the Commercial Bid. If price is indicated in the Pre-Qualification Bid or Technical Bid, that Bid is liable to be rejected.

b) Bids shall be submitted only through the e-tendering portal www.etenders.kerala.gov.in

2.6.2 Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its Bid including cost of presentation for the purposes of clarification of the Bid, if so desired by KSITM. KSITM will be in no way responsible or liable for those costs, regardless of the outcome of the Tendering process.

2.6.3 Procedure for e-Tendering

Bidders are requested to go through the relevant files in the download section of the www.etenders.kerala.gov.in for understanding the procedure to be followed in submitting proposals and payment.

2.7 Clarification on Tender Document

A prospective Bidder requiring any clarification on the RFP Document may submit his queries, in writing, at the mailing address and as per schedule indicated in “Invitation for Bids / Key Events and Dates” in section 1.3. The queries must be submitted in the following format only to be considered for clarification:

S.No	Page No.	Section No.	Clause No.	Reference/ Subject	Clarification Sought
..		..	..	..	..

The queries not adhering to the above mentioned format shall not be responded. KSITM will respond to any request for clarification to queries on the Tender Document, received not later than the dates prescribed in Invitation for Bids / Key events and dates.

2.8 Language of Bids

The Bids prepared by the Bidder and all correspondence and documents relating to the Bids exchanged by the Bidder and KSITM, shall be written in English language. Any printed literature furnished by the Bidder may be written in another language so long the same is accompanied by a duly attested English translation in which case, for purposes of interpretation of the Bid, the English translation shall govern.

2.9 Documents Comprising the Bids

The Bid prepared by the Bidder shall comprise the following components. The Bids not conforming to the requirements shall be summarily rejected.

2.9.1 Pre-Qualification Bid

In support of eligibility, a Bidder must submit the following documents.

- General information about the Bidder – Format 3
- Compliance to Pre-Qualification Criteria as per Section IV – Table 1
- Undertaking on Acceptance of Terms and Conditions in Tender – Format 8
- Undertaking on Not Being Black-Listed by both OEM and bidder – Format 9
- Turnover – Format 2
- Bidder experience – Format 4
- Receipt of Earnest Money Deposit (EMD)
- Receipt of tender fee

2.9.2 Technical Bid

The Technical Bid, besides the other requirements of the Tender, shall comprise the following:

- Technical Bid Letter – Format 1
- Project plan and schedule (As per Bidder's format)
- OEM Authorisation Letter (MAF) – Format 6
- Compliance Statement – Format 10
- Non-Compliance Statement (should be submitted only in case of non-compliance) – Format 11
- Specification of components including data sheet, Architecture, proposed hardware sizing including storage calculation etc.

2.9.3 Commercial Bid

The Commercial Bid, besides the other requirements of the Tender, shall comprise the following:

- Commercial Bid Letter – Format 5
- Price bid as per the template in the e-tendering website

2.10 Bid Currencies

Prices shall be quoted in Indian Rupees (INR).

2.11 Bid Security (Earnest Money Deposit)

The Bidder shall furnish, as part of its Bid, a Bid security as specified in Section 2.2.
The Bidder shall be disqualified in the Pre-Qualification process if the prescribed EMD is not submitted along with the Bid. The EMD (Bid security) of the unsuccessful bidder/s will be discharged / returned as promptly as possible, but not later than 60 days after the issuance of Letter of Intent (LoI) to the successful bidder. No interest will be payable by KSITM on the amount of the Bid Security.

The Bid security may be forfeited because of the following reasons:

1. If a Bidder withdraws the Bid or increases the quoted prices during the period of Bid validity, or its extended period, without the explicit consent of the department, if any; or
2. In the case of a successful bidder, if the entity fails within the specified time limit to:
    a. Sign the Contract; or
    b. Furnish the required Performance Bank Guarantee (PBG)

As per G.O. (P) No.10/2023/SPD dated 11-12-2023, all the MSMEs with Udyog Aadhar Registration or any other body specified by the Ministry of Micro, Small and Medium Enterprises working within the State of Kerala will be exempted from payment of EMD and tender fee.

2.11.1 Remittance of Tender Document Fee and EMD

Online Payment modes: The tender document fees and EMD can be paid in the following manner through e-Payment facility provided by the e-Procurement system mentioned in Annexure 4

2.12 Bid Validity Period

2.12.1 Period of Validity of Bids

Bids shall remain valid for 180 days after the date of opening of Technical Bids by KSITM. However, the prices finalized after opening the tenders shall not increase throughout the period of implementation and operation. The prices of components quoted in the Financial Bid by the Bidder shall remain valid for the Contract period

2.12.2 Extension of Period of Validity

In exceptional circumstances, KSITM may request the Bidder(s) for an extension of the period of validity. The request and the responses thereto shall be made in writing (or by fax). The validity of EMD shall also be suitably extended.

2.13 Withdrawal of Bids

2.13.1 Written Notice

The Bidder may withdraw its Bid after the Bid's submission, provided that KSITM receives written notice of the withdrawal, prior to the last date prescribed for receipt of Bids.

2.14 Opening of Bids

a) The Kerala State IT Mission will open the Bid as mentioned in Section 1.3.
b) A Technical committee of KSITM will be evaluating the bids. The decision of the committee would be final and binding upon all the Bidders.

2.15 Notification of Award

Before the expiry of the period of validity of the proposal, KSITM shall notify the successful bidder in writing, that its Bid has been accepted. The Bidder shall acknowledge in writing receipt of the notification of selection and shall send his acceptance to enter into agreement within fourteen (14) days of receipt of the notification.

Section III: General Condition of Contract

3.1 Representations & Warranties

In order to induce KSITM to enter into the Contract, the bidder hereby represents and warrants as of the date hereof, whose representations and warranties shall survive the term and termination of the contract for each of the following:

a) That the bidder has the requisite experience in providing the service requested through this RFP and the technical know-how and the financial wherewithal, the power and the authority that would be required to successfully provide the Services sought by the KSITM for the purposes of this Contract.

b) That the bidder is not involved in any major litigation or legal proceedings, pending, existing and potential or threatened that may have an impact of affecting or compromising the performance or delivery of services under the Contract.

c) That the representations and warranties made by the bidder in the Bid or will be made in the contract are and shall continue to remain true and fulfil all the requirements as are necessary for executing the obligations and responsibilities as laid down in the Contract and the Tender and unless KSITM specifies to the contrary, the bidder shall be bound by all the terms of the Bid and the contract through the term of the contract.

d) That the bidder has the professional skills, personnel and resources/authorizations that are necessary for providing all such services as are necessary to fulfil the scope of work stipulated in the Tender and the Contract.

e) That the bidder shall use such assets of State as KSITM may permit for the sole purpose of execution of its obligations under the terms of the Bid, Tender or the Contract. The bidder shall however have no claim to any right, title, lien or other interest in any such property and any possession of property for any duration whatsoever shall not create any right in equity or otherwise merely by fact of such use or possession during or after the term hereof.

f) That the execution of the Services and the Scope of work herein are and shall be in accordance and in compliance with all applicable laws.

g) That neither the execution and delivery by the bidder of the Contract nor the KSITM's compliance with or performance of the terms and provisions of the Contract (i) will contravene any provision of any Applicable Law or any order, writ, injunction or decree of any court or Governmental Authority binding on the Implementation Agency, (ii) will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any Contract, Contract or instrument to which the bidder is a party or by which it or any of its property or assets is bound or to which it may be subject or (iii) will violate any provision of the Memorandum and Articles of Association of the Implementation Agency.

h) That the bidder certifies that all registrations, recordings, filings and notarizations of the Contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the successful bidder which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been made.

i) That time is the essence of the Contract and hence the bidder shall at all times maintain sufficient manpower, resources, and facilities, to provide the Services in a workmanlike manner on a timely basis.

j) That in providing the Services or deliverables or materials, neither bidder nor its agent, nor any of its employees, shall utilize information which may be considered confidential information of or proprietary to any prior employer or any other person or entity.

3.2 Scope of Work / Contract

The successful bidder has to abide all the work as specified in the Scope of Work of this RFP

3.3 End of Support

Bidder should ensure that the quoted items are not declared "End of Support/Maintenance" for the next five years from the date of submission of the bid. If in any case, any of the quoted Item is not available in the market, the

bidder will have to supply higher version/replacement of that Item in the quoted cost in the same time duration. Bidder to clearly state the products/services they cannot support and integrate with their proposed solution.

3.4 Contract Performance Guarantee

Within 14 (fourteen) days after the receipt of notification of award of the Contract from KSITM, the successful bidder shall furnish Contract Performance Guarantee to KSITM which shall be equal to 5% of the value of the Work Order and shall be in the form of a Bank Guarantee Bond from a Nationalized/Scheduled Bank in the Pro forma given at Format 13 for Pro forma for Bank Guarantee. The Bank guarantee shall be renewed on annual basis till 60 days beyond the expiry of all the warranty obligations.

3.5 Bidder's Responsibility

a) The Bidder shall not subcontract any portion of the work, nor outsource manpower for the execution of this project. All personnel deployed must be employed directly by the Bidder and listed on its official payroll. The Bidder shall bear full and exclusive responsibility for ensuring compliance with all applicable labour laws, statutory requirements, and regulatory obligations.
b) Prior to deployment, the Bidder must submit the names and detailed CV (including relevant experience, qualification and certification) of all proposed personnel. KSITM will assess the technical capability of the proposed personnel and will be rejected if found to be not satisfied.
c) The bidder must certify that each personnel assigned for the project is without any criminal records/antecedents. Both the Bidder and every individual assigned to the project must execute a Non-Disclosure Agreement, in a form acceptable to KSITM, prior to the commencement of any work.
d) The bidder shall be responsible for the deployment, transportation, accommodation and other requirements of all its employees required for the execution of the work and for all costs/charges in connection thereof.
e) The bidder shall provide and deploy manpower on the site for carrying out the work, only those manpower resources who are skilled and experienced in the SOC as per Annexure 2.
f) The bidder shall keep KSITM indemnified against claims if any of the workmen and all costs and expenses as may be incurred by KSITM in connection with any claim that may be made by any workmen.
g) KSITM may at any time object to and require the bidder to remove forthwith from the site a supervisor or any other authorized representative or employee of the bidder or any person(s) deployed by bidder, if in the opinion of KSITM the person in question has mis-conducted himself or his deployment is otherwise considered undesirable by KSITM the bidder shall forthwith remove and shall not again deploy the person in question of the work site without the written consent of KSITM.

3.6 KSITM's Obligations

a) KSITM/Representative shall interface with the bidder to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. KSITM shall provide adequate cooperation in providing details, assisting with coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of KSITM is proper and necessary
b) KSITM shall ensure that timely approval is provided to the bidder, where deemed necessary, which shall include all specifications related to equipment/material required to be provided as part of the Scope of Work. KSITM shall approve all such documents as per the above Clause.
c) KSITM shall provide list of devices to be integrated in each location along with necessary permission to visit these locations.
d) KSITM shall provide necessary rack space, power, Virtual Servers, Storage, Operating System (RHEL & Ubuntu) and network connectivity for the proposed solution.
e) KSITM shall ensure necessary support from Data centre operator, KSWAN/KFON operator, SecWAN operator etc in implementing the proposed solution. The configuration changes required in the devices to be integrated with the proposed SIEM & SOAR shall be carried out by the respective operators with the support of the successful bidder.

3.7 Risk Management

The bidder shall at his own expense adopt suitable Risk Management methodology to mitigate all risks assumed by the bidder under this Contract. The bidder shall underwrite all the risk related to its personnel deputed under this Contract, equipment, tools and any other belongings of the bidder or their personnel during the entire period

of their engagement in connection with this Contract and take all essential steps to reduce and mitigate the risk. KSITM will have no liability on this account

3.8 Indemnity

a) The bidder shall Indemnity KSITM against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:
   i. Any negligence or wrongful act or omission by the bidder's Team in connection with or incidental to this Contract; or
   ii. A breach of any of the terms of the bidder's Bid as agreed, the Tender and this Contract by the bidder, the bidder's Team

3.9 Confidentiality

a) The bidder shall not use any Information, name or the logo of KSITM except for the purposes of providing the Service as specified under this contract;
b) The bidder shall preserve the confidentiality of the Information including execution of a confidentiality agreement to the satisfaction of KSITM
c) The bidder shall notify KSITM promptly if it is aware of any disclosure of the Information otherwise than as permitted by this Contract or with the authority of KSITM
d) The bidder shall be liable to fully recompense KSITM for any loss of revenue arising from breach of confidentiality. KSITM reserves the right to adopt legal proceedings, civil or criminal, against the bidder in relation to a dispute arising out of breach of obligation by the successful bidder under this clause
e) The bidder shall not use any information which might have come to its knowledge in whatever manner during the discharge of its obligation under the contract for any purpose except strictly for discharging his obligation under the contract and no more.

3.10 Prices

Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract for the scope of the Contract. The price quoted shall be including all taxes and levies. The bidder will ensure that the prices / cost for all the software licenses discovered during the bid process will be valid for the entire contract period. The bidder shall supply additional licenses, manpower and hardware as required by KSITM during the period of contract at the rates discovered through this tender. KSITM reserves the right to change the quantity of items to be procured or place orders for selected items only as per requirement.

3.11 Payment Schedule

SL No	Activity	Payment Terms	Document Required
Payment for supply and commissioning of SOC components (Capex)			
1	On Completion of supply, installation and commissioning of SOC Tools such as SIEM, SOAR, UEBA & NDR	70%	Upon submission of the installation and commissioning report
2	FAT and GO-LIVE	20%	On successful FAT and GO-LIVE report
3	Balance 10% will be released on quarterly basis for a period of 3 years	10%	Upon submission of the quarterly reports after deducting SLA penalties, if any.
Payment for Managed SOC services (Opex)			
1	Quarterly Payment towards Managed SOC services.	Quarterly Payment upon submission of the quarterly reports after deducting SLA penalties, if any.	
Payment for AMC			
1	AMC for 4th and 5th year	Quarterly Payment upon submission of the quarterly reports after deducting SLA penalties, if any.	
Payment for additional Hardware/software licenses			
1	Additional SIEM licenses for 10,000 EPS	100% payment against supply, installation and submission of the license documents.	

2	Additional Log Collectors	100% payment against supply, installation and submission of the warranty documents.

3.12 Event of default by the bidder

a) The failure on the part of the bidder to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of the bidder. The events of default as mentioned above may include, but not limited to, inter alia, the following also:
   i. The bidder has failed to perform any instructions or directives issued by KSITM which it deems proper and necessary to execute the scope of work under the Contract; or
   ii. The bidder has failed to adhere to any of the key performance indicators as laid down in the Key Performance Measures / Contract or if the bidder has fallen short of matching such standards/targets as KSITM may have designated with respect to any task necessary for the execution of the scope of work under this Contract. The above-mentioned failure on the part of the bidder may be in terms of failure to adhere to timelines, specifications, requirements or any other criteria as defined by KSITM; or
   iii. The bidder has failed to remedy a failure to perform its obligations in accordance with the specifications issued by KSITM despite being served with a default notice which laid down the specific deviance on the part of the bidder to comply with any stipulations or standards as laid down by KSITM; or
   iv. The bidder / bidder's Team has failed to conform with any of the Service / Facility Specifications / Standards as set out in the Scope of Work of this Tender Document or has failed to adhere to any amended direction, modification or clarification as issued by KSITM during the term of this Contract and which State deems proper and necessary for the execution of the Scope of Work under this Contract; or
   v. The bidder has failed to demonstrate or sustain any representation or warranty made by it in this Contract with respect to any of the terms of its Bid or the Tender and this Contract; or
   vi. There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to the bidder; or
   vii. The bidder / bidder's Team has failed to comply with or is in breach or contravention of any applicable laws

3.13 Consequences in Event of Default

a) For cases where permissible time is not indicated in the contract, KSITM will decide, at its discretion, the quantum of reasonable time to cure the default
b) KSITM may impose any such obligations and conditions and issue any clarifications as may be necessary to inter-alia ensure smooth continuation of Services and the project which the bidder shall be obliged to comply with. This may include unilateral re-determination of the consideration payable to the bidder hereunder. The bidder shall, in addition, take all available steps to minimize loss resulting from such event of default
c) KSITM may by a written notice of suspension to the bidder, suspend all payments to the bidder under the Contract provided that such notice of suspension:
   i. Shall specify the nature of the failure, and
   ii. Shall request the bidder to remedy such failure within a specified period from the date of receipt of such notice of suspension by the bidder.
   iii. KSITM reserves the right to terminate the contract with 30 days' notice

3.14 Termination of Contract

KSITM may terminate this Contract in whole or in part by giving the bidder prior written notice indicating its intention to terminate the Contract under the following circumstances:

a) Where it comes to KSITM's attention that the bidder (or the bidder's Team) is in a position of actual conflict of interest with the interests of KSITM in relation to any of terms of the bidder Agency's Bid, the Tender or this Contract
b) Where the bidder's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever including inter alia the filing of any bankruptcy proceedings against the bidder, any failure by the bidder to pay any of its dues to its creditors, the institution of any winding up

proceedings against the bidder or the happening of any such events that are averse to the commercial viability of the bidder. In the event of the happening of any events of the above nature, KSITM shall reserve the right to take any steps as are necessary to ensure the effective transition of the project to a successor Implementation Agency/service provider, and to ensure business continuity

c) Termination for Default: KSITM may, at any time, terminate the Contract by giving 60 days written notice to the bidder without compensation to the bidder in the Event of Default on the part of the bidder which may include failure on the part of the bidder to respect any of its commitments with regard to any part of its obligations under its Bid, the Tender or under this Contract
d) Termination for Insolvency: KSITM may at any time terminate the Contract by giving written notice to the bidder without compensation to the bidder, if the bidder becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to KSITM
e) Pre-mature termination: KSITM shall also have a right to prematurely close this Project at any time without assigning any reason. In this case, KSITM may issue written notice to bidder, at least 3 months in advance to terminate the Contract in whole or in part. The notice of termination shall specify the extent to which performance of work under the Contract is terminated and the date upon which such termination becomes effective.

3.15 Consequences of Termination

a) In the event of termination of this contract, due to any cause whatsoever, except where termination is pre-mature initiated by KSITM, the bidder shall be blacklisted and the contract will stand cancelled effective from the date of termination of this contract
b) Nothing herein shall restrict the right of KSITM to invoke the Bank Guarantee and other Guarantees furnished hereunder, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to KSITM under law.
c) The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of this Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

3.16 Force Majeure

a) Force Majeure shall not include any events caused due to acts/omissions of such Party or result from a breach/contravention of any of the terms of the Contract, Bid and/or the Tender. It shall also not include any default on the part of a Party due to its negligence or failure to implement the stipulated/proposed precautions, as were required to be taken under the Contract.
b) The failure or occurrence of a delay in performance of any of the obligations of either party shall constitute a Force Majeure event only where such failure or delay could not have reasonably been foreseen or where despite the presence of adequate and stipulated safeguards the failure to perform obligations has occurred. In such an event, the affected party shall inform the other party in writing within five days of the occurrence of such event. KSITM will make the payments due for Services rendered till the occurrence of Force Majeure. However, any failure or lapse on the part of the bidder in performing any obligation as is necessary and proper to negate the damage due to projected force majeure events or to mitigate the damage that may be caused due to the abovementioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force majeure, as set out above.
c) In case of a Force Majeure, all Parties will endeavour to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure.

3.17 Liquidated Damages

Liquidated damage shall be levied @ 0.5% of the total value of supply and commissioning of SOC components (Capex**)**, per week or part of the week of project completion, subject to maximum of 10% of the total value of the Work Order. Exemptions shall be considered by KSITM for delays or failures beyond the bidder's scope of responsibility. Such exemptions will be granted upon submission of valid supporting documents.

3.18 Taxes, Duties, Levies and Other Charges

a) GSTIN & PAN No. of the supplier should be mentioned in the payment invoice submitted to KSITM
b) All applicable taxes, duties and levies shall be shown separately
c) Charges towards freight, forwarding, transit insurance, installation, commissioning and warranty support shall be included in the quoted price
d) Loading and unloading of materials is the responsibility of the bidder and any charges in this regard to be borne by the bidder.
e) TDS as applicable will be deducted.
f) The base rates quoted by the bidder shall be firm throughout the project execution period. Any revision in the rate of Taxes, Duties, levies etc. or introduction of new taxes/duties/levies by government shall be honoured by KSITM.

3.19 Risk and ownership

KSITM shall become owners of goods supplied by the bidder but all risks, responsibilities; liabilities thereof in all goods shall remain with selected bidder till project completion.

3.20 Dispute Resolution

a) KSITM and the successful bidder shall make every effort to resolve amicably by direct informal negotiations any disagreement or disputes arising between them under or in connection with the Contract
b) If, after Thirty (30) days from the commencement of such direct informal negotiations, KSITM and the successful bidder have been unable to resolve amicably a Contract dispute, either party may require that the dispute be referred for resolution to the formal mechanism specified in the below clauses
c) In the case of a dispute or difference arising between KSITM and the SUCCESSFUL BIDDER relating to any matter arising out of or connected with this Contract, such dispute or difference shall be referred to the award of two Arbitrators. One Arbitrator to be nominated by KSITM and the other to be nominated by the successful bidder or in case of the said Arbitrators not agreeing then to the award of an Umpire to be appointed by the Arbitrators in writing before proceeding with the reference and in case the Arbitrators cannot agree to the Umpire he may be nominated by the Secretary, Indian Council of Arbitration, State. The award of the Arbitrators in the event of their not agreeing of the Umpire appointed by them or by the Secretary, Indian Council of Arbitration, State, shall be final and binding on the parties
d) The Arbitration and Conciliation Act 1996, the rules there under and any statutory modification or re-enactments thereof, shall apply to the arbitration proceedings
e) The venue of arbitration shall be Kerala, India
f) KSITM may terminate this contract by giving a written notice of termination of minimum 30 days to the successful bidder
g) Continuance of the Contract:
    i. Notwithstanding the fact that settlement of dispute(s) (if any) under arbitration may be pending, the parties hereto shall continue to be governed by and perform the work in accordance with the provisions under the Scope of Work to ensure continuity of operations

3.21 Severance

In the event any provision of this Contract is held to be invalid or unenforceable under the applicable law, the remaining provisions of this Contract shall remain in full force and effect.

3.22 Governing Language

The Agreement shall be written in English language. Language of the Agreement shall govern its interpretation. All correspondence and other documents pertaining to the Contract that are exchanged by parties shall be written in English language only.

3.23 “No Claim” Certificate

The bidder shall not be entitled to make any claim, whatsoever against KSITM under or by virtue of or arising out of this contract, nor shall KSITM entertain or consider any such claim, if made by the bidder after he shall have signed a “No claim” certificate in favour of KSITM in such forms as shall be required by KSITM after the works are finally accepted.

3.24 General Relationship between the Parties

a) Nothing in this Contract constitutes any fiduciary relationship between KSITM and bidder / bidder's Team or any relationship of employer employee, principal and agent, or partnership, between KSITM and bidder
b) No Party has any authority to bind the other Party in any manner whatsoever except as agreed under the terms of this Contract
c) KSITM has no obligations to the bidder's Team except as agreed under the terms of this Contract

3.24.1 No Assignment

The bidder shall not transfer any interest, right, benefit or obligation under this Contract without the prior written consent of KSITM

3.24.2 Survival

The provisions of the clauses of this Contract in relation to documents, data, processes, property, Intellectual Property Rights, indemnity, publicity and confidentiality and ownership survive the expiry or termination of this Contract and in relation to confidentiality, the obligations continue to apply unless KSITM notifies the bidder of its release from those obligations

3.24.3 Entire Contract

The terms and conditions, Scope of Work, etc. laid down in the Tender and all annexure thereto as also the Bid and any attachments/annexes thereto shall be read in consonance with and form an integral part of this Contract. This Contract supersedes any prior Contract, understanding or representation of the Parties on the subject matter

3.24.4 Governing Law

This Contract shall be governed in accordance with the laws of India

3.24.5 Jurisdiction of Courts

The courts of India at Kerala will have exclusive jurisdiction to determine any proceeding in relation to this Contract

3.24.6 Compliance with Laws

The successful bidder shall comply with the laws in force in India in the course of performing this Contract

3.24.7 Notices

A "notice" means:

a) a notice; or
b) consent, approval or other communication required to be in writing under this Contract

All notices, requests or consents provided for or permitted to be given under this Contract shall be in writing and shall be deemed effectively given when personally delivered or mailed by pre-paid certified/registered mail, return receipt requested, addressed to the correspondence address in the contract and shall be deemed received 7 days after mailing or on the date of delivery if personally delivered whichever is earlier.
Any Party may change the address to which notices are to be directed to it by notice to the other parties.

3.24.8 Waiver

a) Any waiver of any provision of this Contract is ineffective unless it is in writing and signed by the Party waiving its rights
b) A waiver by either Party in respect of a breach of a provision of this Contract by the other Party is not a waiver in respect of any other breach of that or any other provision
c) The failure of either Party to enforce at any time any of the provisions of this Contract shall not be interpreted as a waiver of such provision

3.25 Modification

Any modification of the Contract shall be in writing and signed by an authorized representative of each Party.

Section IV: Pre-Qualification Criteria

The Bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements as described in the RFP document. The Bids must be complete in all respect and shall cover the entire scope of work as stipulated in the tender document. The invitation to Bid is open to all Bidders who qualify the eligibility criteria as given below:

Pre-Qualification Criteria – Table 1

S.No	Criteria	Document required
1.	The Bids shall be submitted by only the sole Bidder; no consortium is allowed in this Bid	Declaration in this regard needs to be submitted
2.	The Bidder shall furnish, as part of its Bid, an Earnest Money Deposit (EMD) as specified in Section 2.2	Payment shall be made as specified in section 2.11
3.	The Bidder should be a Company registered in India under the Indian Companies Act 1956 / 2013 or a partnership registered under the India Partnership Act 1932 or Limited Liability Partnership Act, 2008 with their registered office in India for the last five years as on 31st March 2025. The Bidder must be registered with appropriate authorities for all applicable statutory duties/taxes	Valid documentary proof of: a) Certificate of incorporation b) GST & PAN
4.	The average annual turnover of the bidder during the last three years ending 31.03.2024 should be at least Rs. 50 Crores.	Chartered Accountant (CA) certified turnover statement / Audited balance sheets for the financial years 2021-2022, 2022-2023 and 2023-24.
5.	Bidder should have successfully implemented similar projects (including SIEM, SOAR components) in India for any State / Central Govt./PSU/BFSI institutions in India, during the last five years ending on 31st July 2025. i. Two projects costing not less than Rs. 3 Crores each or ii. One project costing not less than Rs. 5 Crores	a. Copy of the Work Order or Contract agreement b. Completion certificate / Letter from the customer mentioning the implementation status, if it is an ongoing project.
6.	The bidder should have experience in doing Managed SOC Operations for a minimum period of two years for any State / Central Govt./PSU/BFSI institutions in India, during the last five years ending on 31st July 2025. a) Two projects costing not less than Rs. 1.5 Crores each or b) One project costing not less than Rs. 3 Crores	1. Copy of the Work Order or Contract agreement 2. Completion certificate / Letter from the customer mentioning the period of Operations, if it is an ongoing project. Work Order /PO should clearly mention the scope of works.
7.	The bidder should have a valid ISO 9001:2015, 20000:2018, 27001:2013 certifications.	Copy of the certificates.

8.	The OEM should submit three references/projects where they have successfully supplied and implemented their Security Solution (SIEM, SOAR, UEBA) in any Corporate Companies/BFSI/Govt. Organization in India in the last 5 years.	a. Letter of confirmation from the OEM b. Copy of Work Order/ Contract agreement c. Letter from the customer mentioning the implementation status
9.	The Original Equipment Manufacturer (OEM) for the proposed solution must have a minimum of five (5) years of operational presence in India as of 31st July 2025.	Letter of confirmation from the OEM from the authorized signatory.
10.	The bidder must have a minimum of fifty (50) personnel on their payroll in the domain of cybersecurity as of the bid submission date. An undertaking/declaration in company letter head by HR head of bidder's company.	The bidder must submit an undertaking/declaration on the company's official letterhead, accompanied by detailed information of the cybersecurity personnel employed, including their names, designations, and roles.
11.	The Bidder must not be under any form of blacklisting or debarment by any Central or State Government agency in India as on the bid submission date.	Declaration in this regard by the authorized signatory of the Bidder.
12.	The bidder should submit the MAF from the OEM of the proposed products (SIEM, SOAR, UEBA, TIP & NDR)	Manufacturers Authorization Form (MAF) to be provided as per the Format 6

Note:

- The bids documents uploaded shall be properly aligned with page numbers and index. Relevant portions, in the documents submitted in pursuance of eligibility criterion (1) to (12) mentioned above, shall be highlighted.
- Bidders must ensure that all required documents have been uploaded along with the bid.

Section V: Criteria for Evaluation of Bids

KSITM shall conduct the pre-qualification evaluation in accordance with the prescribed criteria. Only those Bidders who meet the pre-qualification requirements will be shortlisted for the subsequent technical evaluation as per Section 5.2.1. Financial proposals will be opened and compared only for Bidders who qualify in both the pre-qualification and technical evaluation stages. Conditional Bids are liable to be rejected.

The final evaluation will be based on Quality cum Cost Based System (QCBS).

5.1 Evaluation of Pre-Qualification Bid

Bidders need to fulfil all the pre-qualification conditions mentioned in Section IV of the RFP. KSITM will examine the Bids to determine whether they are complete, whether the Bid format confirms to the Tender requirements, whether required Tender fee and EMD has been furnished, and whether the Bids are generally in order.

KSITM may waive any non-conformity or irregularity in a Bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any Bidder.

KSITM may at its discretion can ask clarifications from the Bidders for any shortfall documents if required.

5.2 Evaluation of Technical Bid

After qualifying the Pre-qualification criteria, Technical Bid document will be evaluated as per the requirements specified in the RFP.

The bidder shall submit the following documentation in detail for the technical evaluation of the bid. The technical bid shall broadly contain the following details:

- Understanding of the project needs.
- Proposed technical solution including architecture, scalability, storage calculation to meet the RFP requirement etc.
- OEM Associations and support agreement for this project.
- Proposed project execution methodology.
- Project Management Plan and week-wise project schedule (with macro and micro activities mentioned).

KSITM may request the Bidders to make a technical presentation and product demo for their proposed solution to the KSITM Technical Committee. KSITM will award scores based on the technical documents and/or the presentation.

Each bidder must score at least 50% of the Max Marks defined for each of the categories A, B, C to qualify. Bidders scoring minimum 70 marks out of 100 marks will be qualified for commercial bid opening and evaluation.

5.2.1 Technical Evaluation Criteria

The technical proposal submitted by the bidders shall be evaluated by the committee and the scores shall be awarded as follows:

S.No.	Criteria	Max Marks
1	Organizational Strength in execution of SOC projects	40
2	Resource Strength	10
3	Technical capability of the Proposed Solution	50
Total		**100**

Break-up of the scores are tabulated below:

S.No.	Criteria	Max Marks	Documentary Proof
A	**Organizational Strength**	**40**	
1	The bidder should have experience in doing Managed SOC Operations for a minimum period of two years for any State / Central Govt./PSU/BFSI institutions in India, during the last five years ending on 31st July 2025. • Two projects – 10 Marks • Additional projects 5 marks each.	20	For completed projects, Work Order or Signed Contract Agreement and Completion Certificate has to be submitted. For ongoing projects the bidder has to submit Client Satisfaction certificate duly signed and sealed, on client's letterhead, along with the Work Order or Signed Contract Agreement.
2	Bidder should have successfully implemented similar projects (including SIEM, SOAR components) with minimum 3000 or above EPS for any State / Central Govt./PSU/BFSI institutions in India, during the last five years ending on 31st July 2025. • 5 Marks per project	10	For completed projects, Work Order or Signed Contract Agreement and Completion Certificate has to be submitted. For ongoing projects the bidder has to submit Client Satisfaction certificate duly signed and sealed, on client's letterhead, along with the Work Order or Signed Contract Agreement.
3	The bidder should have experience of managing the SOC operations for a single project with EPS as mentioned below, for any State / Central Govt./PSU/BFSI institutions in India, during the last five years ending on 31st July 2025. • 5000 EPS up to 10000 EPS - 5 marks • 10000 EPS up to 25000 EPS - 7.5 marks • Above 25000 EPS - 10 marks	10	For completed projects, Work Order or Signed Contract Agreement and Completion Certificate has to be submitted. For ongoing projects the bidder has to submit Client Satisfaction certificate duly signed and sealed, on client's letterhead, along with the Work Order or Signed Contract Agreement
B	**Resource Strength**	**10**	
	Bidder should have the following resources in their payroll: • Technical Resource with certifications in CISM/CISSP/CISA and should have a minimum 3 years' of experience in SOC – 2.5 marks will be allocated for each resource (maximum 5 marks) • Technical Resource (L2, L1) with certifications in CEH/SOC Analyst and should have a minimum 3 years' of experience	10	Undertaking on bidder company's letter head duly signed and sealed by HR head of bidder's company with Employee name, Designation, Qualification, Experience and Certifications, along with resource CV details.

	in SOC – 0.5 marks will be allocated for each resource (maximum 5 marks)		
C.	**Technical capability of the Proposed Solution**	**50**	
1	Proposed SOC solution (SIEM, SOAR & UEBA) should be deployed in any of the State / Central Govt./PSU/BFSI institutions in India, during the last five years ending on 31st July 2025 with following EPS count in a single project: • Greater than 10000 EPS upto 25000 EPS – 10 Marks • Greater than 25000 EPS up to 50000 EPS – 15 marks • Greater than 50000 EPS and above – 20 marks	20	For completed projects, Work Order or Signed Contract Agreement and Completion Certificate has to be submitted. For ongoing projects the bidder has to submit Client Satisfaction certificate duly signed and sealed, on client's letterhead, along with the Work Order or Signed Contract Agreement.
2	Technical Presentation by the bidder on the overall understanding of the requirements, scope of work, Technical solution, Approach & Methodology, scalability of solution, superiority of solution etc. • Understanding the requirements, Technical Proposal - 5 marks • Scalability , Superiority of solutions, Advanced capabilities (with self-learning, analytics models powered by AI/ML, capable of handling extremely high IOPS without latency, OOTB integrations etc.) – 7.5 marks • Product Demo – 15 marks	27.5	Presentation by bidders as part of the technical evaluation process. The team presenting should have at least 2 proposed resources with them during the presentation.
3	The proposed product is listed in latest Gartner's Quadrant for SIEM/Foresters – 2.5 mark	2.5	Copy of Gartner's report
	Total	**100**	

5.3 Evaluation of Financial Bids

Evaluation criteria will be Quality cum Cost Based System (QCBS) where Technical Bid Score will get a weightage of 50% and Commercial Bid Score a weightage of 50%.

- The bidder would be technically evaluated out of 100 marks. All the bidders who secure a minimum of 70% (70 Marks out of 100 across all the components together) will be considered as technically qualified.
- Technical score of all bidders will be calculated based on the following formula:
  - **Technical Score of bidders (TS) = Technical Marks received by the bidder x 50%**
- The Bid having the Lowest Commercial Quote shall be termed as the Lowest Evaluated Bid and will be awarded 100 marks.
- Commercial score of all the other bidders will be calculated based on the following formula:
  - **Commercial score of bidders (CS)** $= \left(\frac{\textbf{Commercial Quote of the lowest bidder}}{\textbf{Commercial Quote of the bidder}} \right) \textbf{x 100 x 50\%}$
- Final Score of the bidder: Final Score of each bidding party will be computed by adding the technical score and Commercial Score on the basis of the following formula:
  - **Total Score = TS + CS**
- The bidder whose bid has secured the "Highest Total Score" out of 100 as per above evaluation will be considered as L1 bidder/Successful bidder. In case of a tie where two or more bidders achieve the same highest overall score, the bidder with the higher technical score will be considered.

Section VI: Scope of Work and Schedule of Requirement

Government of Kerala has set up two State Data Centres (SDC 1 and SDC 2) in Thiruvananthapuram to provide the hosting facilities of the e-Governance application in the State. The summary status of the data centres is as below:

	SDC 1	SDC 2
Location	Co-Bank Towers, Palayam, Thiruvananthapuram	Tejaswini, Technopark, Kazhakuttom, Thiruvananthapuram
Total Area	5000 sq. ft	5000 sq. ft
Server Farm Area	~1350 sq. ft	~1500 sq. ft

Government-owned networks such as Kerala State Wide Area Network (KSWAN), Kerala Fiber Optic Network (KFON) and Secretariat Wide Area Network (SecWAN) provide robust and reliable connectivity to various government institutions across the state.

KSWAN extends to 14 District Head Quarters (DHQs), 152 Block Head Quarters (BHQs), 63 Mini POPs (Taluk level) across the State. The network also connected around 4500 Government Offices through various modes like Leased line, Wireless and LAN. This Infrastructure supports integration of a large number of G2G, G2B & G2C services with the applications hosted in the state data centres. KFON consists of one NOC, 375 Pops and connects around 30,000 Govt offices. Additionally, SecWAN covers strengthening of existing and future connectivity by networking Secretariat, Secretariat Annexe, Offices of Ministers & Secretaries to Government and 37 departments in 6 blocks. Secretariat Wide-Area-Network is the largest Campus-Area-Network (CAN) of the Government of Kerala in the state.

In 2022, the Kerala State IT Mission (KSITM) implemented a Security Operations Centre (SOC) comprising Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), User and Entity Behavior Analytics (UEBA), and Network Traffic Analysis (NTA). The managed security services are provided by CDAC, Trivandrum, with the SIEM, SOAR, and UEBA platforms supplied by ArcSight, and the NTA solution by Vehere. The existing setup currently supports a capacity of 3,500 Events Per Second (EPS), scalable up to 10,000 EPS.

KSITM plans to expand the SOC into a centralized Next-Generation Security Operations Centre (NG-SOC) for the State, integrating State Data Centres (SDCs), Kerala Fibre Optic Network (KFON), Kerala State Wide Area Network (KSWAN), Secure Wide Area Network (SecWAN), and departmental assets and applications. This integration aims to provide a coordinated, efficient approach to threat detection, incident response, and risk mitigation. NGSOC is expected to transition into a SOC-as-a-Service model, offering scalable cybersecurity services to departments and agencies throughout the state.

6.1 Scope of Work

The Kerala State IT Mission (KSITM) intends to implement a Next Generation Security Operations Centre (NGSOC) to safeguard the state's information assets across the State Data Centres, Kerala State Wide Area Network (KSWAN), KFON, SecWAN, and to enable integration and mapping of departmental assets and applications as required.

The successful bidder will be responsible for delivering comprehensive SOC management services, including the supply, implementation, customization, integration, and management of NG-SOC services throughout the entire contract period of five years. The proposed solution will be hosted on-premise at State Data Centre (SDC-2). KSITM will provide the necessary hardware infrastructure, including virtual servers, storage, and the operating system (either RedHat or Ubuntu) required for deploying SOC components.

The bidder's scope of work broadly includes:

1. Supply, installation, configuration, and commissioning of SIEM, SOAR, UEBA TIP and NDR solutions
2. Integration of network devices across State Data Centres, KSWAN, SecWAN, and KFON
3. Final acceptance testing, post-implementation training, and Go-Live support
4. Operations and management of the SOC
5. Warranty and product support services

6.1.1 Supply Installation, Configuration and Commissioning of the SIEM, SOAR, UEAB, TIP and NDR

1. KSITM shall provide the bidder with a comprehensive list of all devices that are to be integrated with the NGSOC solution.
2. **Kickoff Meeting** will be organized by KSITM **within one week from the date of issuance of Work Order**. During this meeting, the bidder shall present a detailed project, high-level solution architecture, prerequisites for deployment, and share the details of the designated Point of Contact (PoC) from their implementation team who will coordinate with KSITM throughout the project lifecycle.
3. The bidder shall work in-coordination with KSITM and the Original Equipment Manufacturer (OEM) to prepare a comprehensive reference architecture for the proposed NGSOC solution. This architecture must clearly define the deployment of SOC components, integration of the SOC solution with all existing devices, identification and placement of log collection and forwarding devices, policies for short/long-term data retention etc.
4. The solution must be seamlessly integrated and must support a unified dashboard, console, and database for all NGSOC components mentioned in the RFP. The proposed solution should feature out-of-the-box (OOTB) integration between all modules and offer a single, centralized dashboard for monitoring and management.
5. The **detailed architecture** shall be validated by the OEM and the bidder shall submit the same to KSITM within **three weeks from the date of the Kickoff Meeting**.
6. The bidder shall be responsible for the installation and configuration of all SOC components, including SIEM, SOAR, UEBA, TIP, and NDR. The bidder must ensure that skilled technical personnel are made available at the designated KSITM locations for the installation, commissioning, and initial setup of the solution.
7. KSITM will provide the necessary hardware infrastructure, including virtual servers, storage, and the operating system (either RedHat or Ubuntu) required for deploying SOC components. Any additional software and its licenses shall be provided by the bidder, without any additional cost to KSITM
8. The bidder shall provide all software licenses and subscriptions in the name of the Kerala State IT Mission.
9. The Bidder shall customize the SOC solution as per KSITM requirements, including Reports, Dashboards, Alerts, Playbooks and incident response workflows etc.
10. The Bidder is responsible for the integration and full commissioning of the SOC solution across all identified systems and devices.
11. All software, hardware, licenses etc provided by the bidder as part of the Bill of Materials (BoM) must fully comply with the requirements outlined in the RFP. If, at any point during the contract period, KSITM determines that the supplied components do not meet the RFP specifications, the bidder shall be obligated to provide and configure the necessary additional hardware, software, or licenses at no additional cost to KSITM.

6.1.2 Integration of the network devices at State Data Centres, KSWAN, SecWAN and KFON

As part of the SOC solution deployment, the bidder shall be responsible for the seamless integration and commissioning of all identified network devices and infrastructure components located across the State Data Centres (SDC-1 and SDC-2), Kerala Fibre Optic Network (KFON), Kerala State Wide Area Network (KSWAN), and SecWAN. The integration must ensure full compatibility and interoperability with existing and future requirements, applications, and solutions deployed by KSITM.

1. The bidder shall ensure integration of the SOC solution with all existing and future technologies within KSITM, including:

a. Security devices such as Firewalls, Intrusion Prevention/Detection Systems (IPS/IDS), Web Application Firewalls (WAF), Extended Detection and Response (XDR), and Distributed Denial of Service (DDoS) protection.
b. Network devices such as routers, switches, Load balancers etc
c. Servers including physical and virtual servers, Hypervisors (VMWare, RedHAT), Container Platforms (RedHAT Open shift), Operating systems(RedHat, Ubuntu Linux, Windows Server Edition), Databases (PostgreSQL, MySQL, MSSQL, MongoDB), Web Servers, Application Servers. Asset details at the State Data Centre are detailed in the Annexure 3 (tentative), which will be integrated to the proposed SOC Solution. The final list will be provided during vendor onboarding.

2. The bidder shall implement mechanisms to collect logs from all assets and platforms, including SDC-1, KFON, KSWAN, SecWAN, and departmental applications, using log connectors. These logs must be securely transmitted to the centralized SOC Platform.
3. The bidder shall ensure the complete integration of all identified applications, solutions, and network devices with the SOC platform. In cases where native or out-of-the-box (OOTB) integration is not available, the bidder shall be solely responsible for coordinating with the respective OEM(s) or third-party vendors to develop and implement the required custom integrations.
4. The bidder shall also ensure that the OEM(s) actively collaborate, as needed, with other OEMs and third-party vendors to achieve seamless, end-to-end integration. This includes, but is not limited to: Development of native and custom parsers and connectors, reducing false positives alerts, Implementation and customization of native and custom playbooks, Fine-tuning of alerts, incident workflows, dashboards, and reports, Customization of templates and dashboards, Execution of additional remediation activities and administrative configurations etc, without any additional cost to KSITM, throughout the entire duration of the contract.
5. The bidder is required to deploy qualified onsite personnel at designated locations to carry out all implementation, testing, and issue-resolution activities.

6.1.3 Final Acceptance Testing, Post-implementation training and Go-Live

6.1.3.1 Final Acceptance Testing

1. The Bidder shall submit a comprehensive draft Acceptance Test Plan (ATP) after the implementation of the solution. This ATP must include all test scenarios, step-by-step procedures, acceptance criteria, roles, responsibilities, and the tools required for testing.
2. Upon receipt, KSITM shall thoroughly review the ATP and either approve it or provide feedback requiring necessary revisions before the commencement of the FAT.
3. The Bidder is responsible for submitting all relevant installation and configuration documentation before FAT starts. This includes system architecture diagrams, detailed network connectivity layouts, and a complete inventory list of all hardware including OEM serial numbers and service tags.
4. The Bidder must provide a formal written confirmation stating that the entire SOC solution including SIEM, SOAR, UEBA, and NDR components is fully installed, integrated, configured, and ready for User Acceptance Testing and FAT.
5. Upon receipt of these documents and readiness confirmation, KSITM will review the submissions and confirm that the system is ready to proceed with FAT.
6. Acceptance tests will be done as per the ATP and shall include the following:
    a. Physical Verification: All the received equipment will be powered on and physical specifications of the hardware supplied will be checked against the tender specifications
    b. Demonstration of all software installed as per tender specifications
    c. Demonstration of configuration, logging, reporting functionalities, test use cases etc. as per the tender requirements.
7. The Bidder is required to provide the necessary test tools, scripts, and technical support personnel either onsite or remotely to facilitate smooth and efficient testing.
8. Upon completion of the FAT, the Bidder shall correct all identified defects or issues and submit a comprehensive FAT completion report that details test results and remediation actions.
9. KSITM will review the final FAT report and provide formal written sign-off once all acceptance criteria have been satisfactorily met.
10. The following documents must be submitted and approved before or during FAT:

a. Operating manuals of all proposed solution
b. Technical write up of the
    i. design and functioning
    ii. System and connectivity architecture diagram
    iii. Detailed active components configuration details
    iv. Security implementation for installed infrastructure components
    v. Threat use-cases, correlation rules configured etc.
c. Draft Acceptance test plan and procedure document
d. Document on variable selection, derivation and validation of the data
e. Document for design of procedures for correlation
f. Document on detection rules to trigger alerts
g. Document on data collection, integration and analysis mechanism
h. Detailed workflow design document including screen shots
i. Design document of visualisation across devices including screen shots
j. A defined set of use cases and related data sets in evaluating alternative analysis, reporting and query tools to address:
    i. Dashboards of data
    ii. Ad-hoc query of data
    iii. Predictive analysis of future trends based on available data.
k. Acceptance test reports, performance test reports of the components.
l. As built system documentation

6.1.3.2 Post-Implementation Training

a) Post Implementation: Provide on-site training to 15 personnel from KSITM on SIEM & SOAR operations, alert monitoring, policy configuration for all solutions etc. for a period not less than three days.
b) The OEM is required to provide training jointly with the bidder.
c) The bidder is required to provide detailed training material for each participant for each solution as per the scope of work. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
d) All out of pocket expenses including the venue arrangements for the training shall be borne by the selected bidder. The training should be conducted in Thiruvananthapuram.
e) The training content must include but not limited to the topics listed below:
    i. Features and capabilities of the supplied solutions
    ii. Administration and management of the supplied solutions
    iii. Troubleshooting and maintenance of the supplied products
    iv. Lab sessions
    v. Installation and Configuration of the supplied solutions.
    vi. Configuration of standard use case templates.
    vii. Configuration of customized use case.
    viii. Development of custom parsers.
    ix. Configuration of net flows.
    x. Dashboard Reporting and workflow customization.
    xi. Data archiving, backups and retrieving.
    xii. Creating, customizing/modifying playbooks.
    xiii. Configuring orchestration and automation of incident response

6.1.3.3 Go-Live Activities

1. Upon successful completion of the FAT, KSITM will issue formal acceptance of the Go-Live phase.
2. The bidder must provide both on-site and remote support during the initial Go-Live period, as defined in the project plan. The Bidder shall share the support contact details and escalation matrix with KSITM during Go-Live.

6.1.4 Operations and Management of the SOC

1. The selected bidder shall be responsible for establishing, operating, and managing the Security Operations Centre includes 24x7 monitoring, incident detection, analysis, response, and resolution as per the defined Service Level Agreements (SLAs).
2. The bidder shall ensure Service Level Agreement (SLA) adherence from day one of operations.
3. The bidder shall deploy qualified and experienced professionals in shifts to ensure round-the-clock operations. The bidder must factor in adequate resources to effectively manage shift rotations, weekly offs, and leave schedules, as per the manpower structure detailed in Annexure 2.
4. KSITM reserves the right to increase the number of personnel deployed at the SOC during the contract period, based on operational requirements (e.g., EPS count exceeding 75,000). In such cases, KSITM will ask the bidder to provide more manpower resources as per the manpower rates discovered in this tender and the bidder shall provide the same. The bidder shall accommodate such changes without affecting the performance or quality of service.
5. KSITM may engage Third Party Auditor (TPA) for the SLA auditing, the bidder shall extend necessary support and documents to TPA based on KSITM instructions.
6. The bidder shall be responsible for the end-to-end management of security incidents to ensure timely detection, response, and resolution in alignment with the defined SLAs and security policies of KSITM. The responsibilities includes, but not limited to:
    a. The bidder shall continuously monitor logs, events, and alerts generated from all integrated systems and network devices using the deployed SIEM, SOAR, UEBA, and NDR tools.
    b. The bidder shall perform real-time correlation, prioritization, and investigation of alerts based on severity levels and predefined risk criteria to ensure prompt and effective response to potential threats.
    c. The bidder shall implement and manage an inbuilt or integrated incident management and ticketing system capable of automatically generating tickets for alert events triggered by the SIEM, SOAR, UEBA, and NDR systems.
    d. The bidder shall customize the incident management workflows, dashboards, and reports as per KSITM's specific requirements and shall modify or update them periodically to accommodate evolving operational and reporting needs.
    e. The bidder shall manage the complete lifecycle of each security alert or incident, including logging, classification, tracking, and resolution, using the ticketing tool in accordance with the defined SLAs.
    f. The bidder shall ensure the timely closure of all incident tickets and carry out necessary follow-up with the respective KSITM teams. All ticket closures must strictly adhere to the agreed SLA timelines and take into account the severity of each incident.
    g. The bidder shall provide appropriate remediation steps along with analysis reports to KSITM. The recommendations and reports must align with the defined and agreed SLA timelines, taking into consideration the severity and impact of the incident.
    h. Bidder shall ensure efficient utilization and monitoring of EPS, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc.
    i. All deployed technologies under the NGSOC must evolve from rule-based systems to advanced analytics-driven platforms powered by Artificial Intelligence (AI) and Machine Learning (ML).
7. The OEM(s) shall design, validate, and review the NG-SOC (Next-Generation Security Operations Center) architecture and all in-scope solutions at least twice a year. This review must be conducted by the respective OEM(s) and shall include a comprehensive evaluation of the implemented NG-SOC solutions. The entire process shall be carried out with the knowledge and concurrence of KSITM.
8. The bidder must ensure that the SOC solution is capable of forwarding raw logs to external SOCs such as National SOC managed by the National Cyber Coordination Centre (NCCC) of CERT-In, XDR Solution (SentinelOne) managed by KSITM.
9. All new device integrations, including complete setup, configuration, and documentation, shall be performed during the contract period at no additional cost to KSITM.
10. Bidder should support for any internal or external security preparedness drills (including CERT-In drills) and carry out activities for setting up of monitoring and response systems required for the drills and participate in all stages of such drills.

11. The bidder shall be responsible for preparing and maintaining all necessary documentation and reports related to SOC operations, incident management, system performance etc.
12. The bidder shall submit weekly and monthly reports detailing security events, incidents, and remediation activities carried out during the respective periods. The bidder is required to provide the following reports at a minimum:
    a. Daily reports:
        i. Top attacker, attacks and attack targets, trends report
        ii. Top firewall ports access report (inbound/outbound)
        iii. Top signature triggered
        iv. Top account brute forced
        v. Top systems infected
        vi. Top virus infection in the network
        vii. SIEM/monitoring tool performance report
    b. Weekly reports:
        i. Weekly security incidents status report
        ii. Daily device utilization report
        iii. Device availability report
        iv. Device: Incident, service request and change status report
        v. Weekly threat advisory and vulnerability report
        vi. Top signature triggered
        vii. Top account brute forced
        viii. Top systems infected
        ix. Top virus infection in the network
    c. Monthly reports:
        i. Executive summary report for all the services
        ii. Monthly Security incident status report
        iii. Monthly security incident trend analysis
        iv. Monthly device availability report
    d. Quarterly reports:
        i. Quarterly Security incident status report
        ii. Quarterly security incident trend analysis
        iii. Quarterly cyber security activities report

6.1.5 Warranty and Product Support

a. Warranty of all quoted items shall start from the date of commissioning.
b. The warranty period for the supplied components (SOC Solution, Log Collectors, NDR Appliance) shall be for three years from the date of Go-live and 2 years AMC.
c. Post the completion of warranty period, the successful bidder should provide comprehensive AMC & ATS for proposed solution, including other software, associated modules, hardware and services required to meet the requirements in the RFP.
d. The bidder shall ensure that all additional SOC solution licenses and EPS capacity procured during the contract period are covered under Warranty and Annual Maintenance Contract (AMC) for the fourth and fifth years. All associated costs must be included in the bid price of the additional EPS licenses, and KSITM shall not bear any additional charges for Warranty or AMC on these components.
e. Bidder is required to produce OEM's confirmation in OEM's Letter head with serial numbers of goods / products supplied for back-to-back warranty all the equipment supplied through this RFP.
f. OEM support should be provided on 24*7
g. All ongoing software upgrades for all major and minor releases should be provided during the warranty period by the bidder.
h. The AMC/ATS support for the complete solution should include the following:
    a. All minor and major version upgrades during the period of contract at no extra cost
    b. Program updates, patches, fixes and critical security alerts as required.
    c. Documentation updates.

d. 24x7x365 support for all security application-related malfunctions. The support must include the ability to log service requests online through a dedicated portal or support system, ensuring timely response and resolution in accordance with defined SLAs.
e. The Bidder should have back to back agreement with the OEMs for ATS and AMC support.

i. KSITM at its sole discretion may place purchase order of any component of additional requirement during the contract period with the discovered price as per RFP. The rate contract will be valid for entire contract period.

6.2 Project Time Schedule

The total duration of the project is for a period of 90 days from the date of release of work order including final acceptance and testing (FAT), training and submission of documentation.

S. No	Activity	Time of Completion
1	Issuance of Work Order	T
2	Kick-off Meeting	T+7 days
3	Signing of the Contract Agreement	T+14 days
4	Supply, Installation and Commissioning of SIEM, SOAR, UEBA and NDR	T+45 days
5	Deployment of manpower for the management of SOC Solution	T+55 days
6	Integration of Devices with the supplied solution	T+75 days
7	Documentation, Post-implementation training, Final Acceptance Test (FAT) and Go Live	T+90 days (T1)
8	Operations and management of the SOC for Five years post GO-Live	T1+ 5 years

6.3 OEM's responsibilities engaged by the Bidder

The bidder will provide the services of OEM during the Solution design and its implementation, post implementation verification, half-yearly review on the configuration, solution's performance and architecture, patches & updates, verification of new integrations etc.

Bidder will provide the confirmation from the OEM to KSITM post implementation, confirming the implementation of their products with best industry practices and the standards.

The bidder is responsible for arranging these reviews at no extra cost to KSITM.

6.4 SCALABILITY

The proposed SOC solution must be highly scalable to support the continuous integration of more devices during the period of contract. It must be able to sustain a baseline performance of 25,000 Events Per Second (EPS) while able to scale to 200,000 EPS without any degradation in performance. The bidder shall provide the details of hardware resources for scaling up the SOC infrastructure to support additional integrations. This scalability is critical for handling future demands from various user departments and new IT component deployments.

6.8 SERVICE LEVEL AGREEMENT

This Service level agreement would be valid for the entire period of contract. This SLA may be reviewed and revised according to the procedures detailed in SLA Change Control.

The KSITM will measure the performance of SOC teams to continuously improve their processes. The following metrics will be used to analyse the activity of the SOC.

Performance Metrics
Performance will be measured using the following metrics to ensure continuous improvement of the SOC team's processes.

Metric	Definition	Metric
Mean Time to Detect (MTTD)	Average time for the SOC to detect an incident.	Mean Time to Detect (MTTD)
Mean Time to Resolution (MTTR)	Average time for the SOC to neutralize a threat after detection.	Mean Time to Resolution (MTTR)
Case Breakdown	Analysis of cases by total volume, type (e.g., web attacks, brute force), and escalation path.	Case Breakdown
Analyst Productivity	Number of alerts or cases processed per analyst (L1, L2).	Analyst Productivity

Service Levels & Thresholds
Bidder shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the bidder shall be reviewed by IT Mission on quarterly basis and shall:

- Check performance of the bidder against defined service levels over the review period of 3 months and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
- Discuss escalated problems, new issues and matters still outstanding for resolution.
- Review of statistics related to rectification of outstanding faults and agreed changes. Obtain suggestions for changes to improve the service levels.

In case, if desired, KSITM may initiate an interim review to check the performance and the obligations of the Agency. The KSITM will conduct quarterly review of the services rendered by the Service Provider at mutually agreed schedules, dates and representatives from both the IT Mission and Service Provider should attend such performance review meetings. The Service Levels may be reviewed periodically i.e. quarterly and revised, if required.

The service levels shall take into consideration the following aspects-

- Equipment Availability Related Service Levels
- Technical Support desk Services
- Compliance and Reporting Procedures
- Quality and Availability of Required Staff

Solution Uptime & Availability
The successful bidder must ensure a solution uptime of 99.9% or above per quarter. This critical measure covers the availability of all core components of the solution.

SLA Parameter	Required Uptime (Per Quarter)	Description	Penalty
Infrastructure Availability			
SOC Solution - SIEM, SOAR, TIP, UEBA	99.9% or above	Average uptime for all the deployed instances will be considered.	Penalties will be applied as outlined in the table - Penalty applicable to Infrastructure and Application availability
SOC Solution – NDR	99.9% or above	Average uptime for the NDR Component	Penalties will be applied as outlined in the table - Penalty applicable to Infrastructure and Application availability
Log Collectors	99.9% or above	Average uptime of all deployed collectors will be considered	Penalties will be applied as outlined in the table - Penalty applicable to Infrastructure and Application availability
SOC Application/Service Availability			
Application availability of SIEM, SOAR, TIP, UEBA	99.9% or above	The average uptime of the SOC applications will be calculated quarterly. Downtime will be measured based on the incident tickets officially reported by KSITM, with the downtime duration calculated from the time of ticket logging until the time of resolution/closure regarding system downtime.	Penalties will be applied as outlined in the table - Penalty applicable to Infrastructure and Application availability
Application availability of NDR	99.9% or above	The average uptime of the SOC application - NDR will be calculated quarterly. Downtime will be measured based on the incident tickets officially reported by KSITM, with the downtime duration calculated from the time of ticket logging until the time of resolution/closure regarding system downtime.	Penalties will be applied as outlined in the table - Penalty applicable to Infrastructure and Application availability
Manpower Availability			
Manpower Availability	100% of scheduled shifts	The bidder shall maintain the number of resources defined in the contract.	Any default in staffing will incur a penalty of 5% per employee from the quarterly charges for Managed SOC services (Opex)

Penalty applicable to Infrastructure and Application availability:

S. No.	Uptime	Penalty %
1	U > = 99.9	0
2	U > = 97 < 99.9	2
3	U > = 97 < 95	5
4	U < 95	10

Note:

- Penalties for Log Collectors will be applied based on the average uptime of all collectors combined. Eg: If 15 collectors achieve 100% uptime and 3 collectors drop to 95%, average uptime = 99.2% penalty falls in 2%.
- Since the hardware infrastructure for the SOC are provided by KSITM, any down-time due to hardware failures shall be exempted from the SLA obligations to the bidder.

Incident Response & Reporting

This section outlines the timeframes for alerting and responding to security incidents.

Service Level	Reporting/Alerting	Penalty
High/Critical	Incident Reporting:- **High/Critical incidents should be reported within two hours** of event identification to KSITM and concerned authority Incident Resolution/Mitigation: 1. **All High/Critical incidents must be resolved or mitigated within one** hour of event identification, in line with the predefined rules, and policies (where the SOC team has the full control to mitigate the incident). 2. If the mitigation process involves dependencies on other stakeholders (such as SDC, KSWAN, KFON, SeCWAN, or relevant departments), the SOC team shall report the incident to the concerned stakeholders along with the recommended mitigation steps within two hours and escalate the matter to KSITM after 24 hours if not resolved, for further action	A penalty of 0.1% of the quarterly charges will be deducted for every hour past the specified timeline for any delays in reporting of high critical incidents.
Medium	Incident Reporting:- **Medium level incidents should be reported**	A penalty 0.025% of the quarterly charges will be deducted for every hour past the

	within six hours of event identification to KSITM and concerned authority Incident Resolution/Mitigation: 1. **All Medium level incidents must be resolved or mitigated within two** hour of event identification, in line with the predefined rules, and policies (where the SOC team has the full control to mitigate the incident). 2. If the mitigation process involves dependencies on other stakeholders (such as SDC, KSWAN, KFON, SeCWAN, or relevant departments), the SOC team shall report the incident to the concerned stakeholders along with the recommended mitigation steps within six hours and escalate the matter to KSITM after 48 hours if not resolved, for further action	specified timeline for any delays in response and resolution of medium incidents.

Note:

- Calculation of penalties for delays in reporting shall be cumulative for each category of incidents (high, medium). For every hour of delay beyond the specified timeline, the applicable penalty rate will be applied, and penalties will be aggregated separately within each incident category for the duration of the contract period.

General Conditions for SLA

- The KSITM will conduct quarterly reviews to assess performance against these service levels.
- The Service Provider is not responsible for SLA impacts caused by delays that are not their fault. All such cases must be properly evidenced.
- The total SLA penalty in any given quarter shall be capped at 50% of the combined quarterly charges for Capex and Opex.
- Penalties for Infrastructure/Application availability will be deducted from the Capex component of the Quarterly Guaranteed Revenue (QGR).
- Penalties for the Manpower Availability, Incident alerting/resolution will be deducted from the Opex component of the Quarterly Guaranteed Revenue (QGR).

ANNEXURE 1: TECHNICAL SPECIFICATION

Security Information & Event Management

Sl No.	Specification	Compliance (Yes or No)	Remarks
1	The proposed SIEM solution have a sustained 25000 EPS (Events per Second) and/or equivalent Flow records per second which can be scalable upto 200,000 EPS and/or equivalent flow records per second.		
2	The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system		
3	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.		
4	The solution must support automated classification of assets that are being protected.		
5	Solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, Opsec etc.). Solution can read and interpret events from more than 300 log sources.		
6	The solution must support information (users, groups, etc.) collected from Directories (i.e. AD, LDAP) products. Please describe your level of support for this type of product.		
7	The solution must integrate with other security and network devices		
8	Solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage		
9	Solution must be able to store logs in a separate system which would not be required to perform any real time correlation thereby minimizing the load on the Real time analysis.		
10	Solution must provide agent-less collection of event logs.		
11	Solution must provide an agent to collect logs from windows servers.		
12	Solution must provide the ability to distribute both event collection and processing across the entire SIEM deployment.		
13	SIEM shall support Connector Development tool/SDK /API availability for developing collection mechanism for home-grown or any other unsupported devices/applications. The respective tool should be provided		
14	The solution must provide the ability to encrypt communications between components		
15	SIEM solution collector which is used should be able to send data real-time towards to processing unit.		

16	The solution must normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network		
17	The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.		
18	The system should be able to analyse logs with different event formats which include operational Events / Logs of Security devices including IDS / IPS, Firewalls, Anti-virus and other such devices, Logs / Events from the servers such as Web server, Mail server, DNS Server, Application Servers, Operating systems (Windows, Unix, Linux, AIX, Solaris etc), Virtualization platforms, Databases (Postgres, Oracle, SQL, DB2, MySql, Sqlite, MS-Access etc.), Storage systems, etc. as deemed to be important for the purpose of Security. The system should support, not restricted to, the following log and event collection methods: ➢ Syslog – UDP (as detailed in RFC 3164) TCP (as detailed in RFC 3195) ➢ Flat file logs such as from DNS, DHCP, Mail servers, web servers etc. ➢ Windows events logs – Agent-based or agentless ➢ FTP, S/FTP, SNMP, ODBC, CP-LEA, SDEE, WMI, JDBC, etc. ➢ NetFlow, JFlow, Sflow , AIX etc/ ➢ Single-line Flat Files and Multi-line Flat Files ➢ Compressed Flat Files (single and multi-line)		
19	The solution must provide a common taxonomy of events.		
20	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields		
21	The SIEM must provide searching & data/log management, including free form search.		
22	The solution must provide near-real-time analysis of events.		
23	The solution must provide more advanced event drill down when required.		
24	The solution must provide a real-time streaming view that supports full filtering capabilities		
25	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, etc..		
26	The SIEM must provide the ability to understand the virtual host to virtual host communications within our virtualized environment looking for suspicious		

	activity. Please describe how your solution meets this requirement.		
27	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events. Please describe how this requirement is met by the solution.		
28	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a failed called "SpecialID from my Custom Application").		
29	The solution must support and maintain a history of user authentication activity on a per asset basis.		
30	The solution must provide a 'Dashboard' for quick visualization of security and network information.		
31	The solution must support the automated distribution of reports		
32	The solution must allow for custom defined tagging of events		
33	The solution must support the capability to provide historical trend reports.		
34	The solution must integrate with 3rd party directory systems as an authentication method. Solution should be integrated with LDAP or Active Directory solution for access provisioning to the SIEM system.		
35	The solution must provide an open API mechanism		
36	The proposed solution should be horizontally scalable to support increase in EPS and should have global correlation capability on raw or metadata/normalized events (i.e. correlation of events if processed on multiple hardware/appliances)		
37	SIEM solution should be configured in High Availability across all components within the system e.g. log correlation, management console etc.		
38	The solution must support a web-based GUI for management, analysis and reporting. There should be no plug-ins, Java, Flash, or thick-client requirements for operating the solution.		
39	Solution should be able to define purging and retention rules for log storage.		
40	Solution should offer a global threat feed which must allow the analyst to perform search across various parameter like IPv4, IPv6, URL, vulnerability, Applications name, Malware, Spam.		
41	Solution should allow analyst to perform manual ad-hoc check to determine if he is infected with any Zero-day attack.		
42	The solution should have out of the box bi-directional integration with proposed SOAR solution.		

43	Proposed solution should support both automatic and manual escalation of incidents to proposed SOAR and should allow the proposed SOAR to query data from the SIEM		
44	The platform shall support provision for dashboard specific to a single offense, which can offer various widgets, provision for sharing notes, representation of data in a graphical manner over a certain period and various rules triggered, rule s, model responsible in triggering of the offense.		
45	There should be provision available to create complex searches by means GUI, to support advance investigation on the data available in the platform.		
46	The platform should Query-less search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values		
47	The solution should not limit the number of non-critical events that need to be collected for compliance reason and doesn't require correlation till the maximum capacity of hardware/storage.		
48	The solution should not require additional license to deploy additional log collectors		
49	For storage calculation, bidder may consider 700 byte as the average raw payload size of the logs		
50	All collected logs must be stored in encrypted form, using industry-standard encryption algorithms such as AES-256 or equivalent/higher. Additionally, the event log data must be compressed at a minimum ratio of 1:8 or better to ensure storage efficiency.		
51	Log collection software should supports proctols like syslog, JDBC, API, WMI, SFTP, FTP, SCP, SNMP, MQ etc on single software/hardware appliance.		
52	Provide user login concurrently for analysis as well as administration activities with a minimum 50 concurrent users.		
53	No logs should be lost due to any kind of disruption for both real time collection as well as long-term storage.		
54	Log security in terms of integrity and availability		
55	The Proposed Solution must offer all of the below built-in Compliance Modules at no additional cost: ➢ ISO 27001 Compliance. ➢ PCI Compliance ➢ ISO 27017		
56	Provides the following but not limited to real time alerting based on observed security threats: i. DDoS ii. Worm outbreak iii. Botnets iv. Exploitation and attack attempts		

	v. Attack sources vis-à-vis specific attacks and top exploits vi. Compromised systems vii. Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), etc. viii. Other attack vectors such as the following are detected ➢ Web Login brute force attempts ➢ Web Login brute force and successful breach ➢ SQL Injection Attempts ➢ SQL Injection breach, followed Data Exfiltration ➢ DDoS Attack on web server by anomaly detection, unusual continuous request for huge file downloads. ➢ Slow DoS Attacks on Web Server ➢ TCP SYN Flood Attack ➢ Unauthorised Login LDAP, Active Directory, Database ➢ Authorized Login with stolen credentials or via Network Intrusion ➢ APT Attacks ➢ Ransomware Attacks ➢ Botnet Infection ➢ Other Known Malware infections correlating with Threat Intel ➢ Network / IP Scan ➢ URL scan Attempts ➢ Monitored devices hardware failure ➢ Intrusion Attempts ➢ Privilege Escalation		
57	The bidder shall ensure that all log and event data is retained for a minimum period of 30 days on online storage. Additionally, the bidder shall maintain the preceding 6 months of data on offline storage. The data retention strategy must comply with industry best practices and CERT-In guidelines, ensuring data integrity, availability, and security throughout the entire retention period.		
	Correlation & Alerting		
58	The solution must provide alerting based on observed security threats from monitored devices and network activity		
59	The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors. (i.e., look for 25 login failures from the same username followed by a single successful login for that same username, where events seen by a single collector do not exceed the threshold of 25, but across multiple collectors would exceed the threshold).		

60	SI proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. 2. Flow based threat Detection 3. User Behavior analysis 4. Threat Intelligence		
61	The solution must provide the ability to correlate information across potentially disparate devices and flows information.		
62	The solution must observe anomalies other than just simple threshold basis		
63	The solution must chain alerts into one single incident record, so when different rules are triggered and these activities are related with one single offense, then these triggers will generate only one incident record to avoid overloading the security operation team. Please describe how you solution meets this requirement.		
64	The solution must provide alerting based upon established policy.		
	The system must automatically learn and baseline the normal user and host relationships across the network.		
	The system must alert when a user attempts to log into a host they have not previously accessed.		
	The system must be able to track user activity by host over time, even when the event logs do not contain the username.		
65	The system must automatically detect and baseline all assets and services on the network.		
66	The system must generate an alert when a new, unplanned asset or service appears on the network.		
67	The system must alert on new services running on existing hosts.		
68	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions		
69	The solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results. Please describe how your solution meets this requirement.		
70	The solution must limit the presentation of multiple similar alerts. Describe the solutions ability to minimize duplicate alarms.		
71	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. Please describe how your solution meets this requirement.		
72	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile		

	networks, etc.). These 3rd party data feeds should be updated automatically by the solution. Please describe how your solution meets this requirement.		
73	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes then generate an alert. Please describe how your solution meets this requirement.		
74	The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification. Please describe how your solution meets this requirement.		
75	The solution must support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes. Please describe how your solution meets this requirement.		
76	The solution must support correlation for additive values over time. For example, alert when any SRC IP sends more than 1GB of data to a single port on a single DST IP in a one hour period of time. Please describe how your solution meets this requirement.		
77	The solution must provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity. Please describe how your solution meets this requirement.		
78	The solution must support historical correlation so users can re-run past events and flows on historical data, so new rules can be tested more precisely. Please describe how your solution meets this requirement.		
79	The solution must be able to be updated regularly, to stay aware of the latest threat information and research available.		
80	The solution must be able to analyze user activity to detect malicious insiders and determine if a user's credentials have been compromised.		
81	Platform should be capable of providing insights into your local DNS traffic by identifying malicious activity and allowing security team to be able to detect following A. Domain Generated Algorithm (DGA) B. Tunneling or Squatting domains that are being accessed from within your network.		

82	The Platform shall create a baseline model that contains information about the flows and flow attributes that currently exist on the system.		
83	The platform should analyzes the flow records to determine normal traffic patterns, while comparing all incoming flows to the baseline models. Flow should be assigned an outlier score based on the flow attribute values and frequency of communication is observed on the network.		
84	The platform should Visualize offenses, network data, threats, malicious user behavior, and cloud environments from around the world in geographical maps, and auto updating charts.		
85	The platform should allow to Import and export dashboards or share dashboard links with colleagues.		
86	The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, offense and the generic APIs.		
87	The platform should allow user to fine-tune there with complete flexibility in dashboard layout and dashboard item refresh rates		
88	The platform should allow user to Assign thresholds to Big Number, Time Series, Tabular, and Geographical charts		
89	The platform should offer an interface to help user in browsing the existing rule mapping across MITRE Framework & enabling them to map their custom rules to MITRE ATT&CK tactics and techniques.		
90	The platform should offer user to tune their environment with the help of built-in analysis capability.		
91	The Platform should allow user to Use new insights to prioritize the rollout of new use cases and apps to effectively strengthen your security posture.		
92	The platform shall help user in visually exploring how potential log source type and MITRE-mapping coverage can increase. Also providing the user capability to reduce false positive.		
93	Performs the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: 1. Vulnerability based 2. Statistical based 3. Historical based 4. Heuristics based 5. Behavior based on source entity, applications etc. 6. Information Leak 7. Unauthorized Access 8. Denial of Service		

	9. Service Unavailable 10. Phishing attack 11. Pattern based rules 12. Profiling Whitelist/Blacklist/Reference List		
	AI & Machine Learning:		
94	The solution must incorporate Gen AI and act as cybersecurity expert to provide recommendations leveraging LLM		
95	The solution should not be sending any log data outside of the system by utilising LLMs model. AI working should only be initiated by the user and not automated		
96	Machine learning should be embedded across the platform (SIEM, UBA). It should empower every user in the SOC with ML/DL.		
97	The solution should accurate provide offense summaries that help security analyst to quickly investigate and mitigate risks. By using accurate offense summaries, a security analyst can rapidly comprehend critical details about an offense, including the attack vector, affected users, and assets.		
98	The solution should provide recommended actions with both long-term and short-term measures. This helps to mitigate the immediate risk and to proactively avoid future attacks. This makes it easier to eliminate uncertainty and take prompt action in response to serious risks.		
99	The solution should provide own unique session maintained and stored by the app along with session logs so that a user can revisit their past chat sessions when needed.		

Security Orchestration, Automation, and Response (SOAR)

Sl No.	Specification	Compliance (Yes or No)	Remarks
A	**INCIDENT RESPONSE ESCALATION AND WORKFLOW**		
1	The solution must include a module, out-of-the-box, that provide incident response playbooks		
2	The solution should support following methods of Incident Creation		
	The solution must be able to create incident by parsing email notification.		
	The solution must provide UI based wizard to manually create incidents.		
	The solution must be able to support creation of incidents via API.		
	The solution must be able to support creation of incidents via Web URL.		

	The solution must be able to support creation of incidents via SIEM.		
	The solution must be able to support creation of incidents via ticketing system.		
3	The solution must be able to automatically extract email attachments from emails and store that for the related incidents as attachments.		
4	The solution must be able to support storing of incident related files not limited to malware specimens, logs, and screenshots.		
5	The solution must include out-of-the-box playbooks based on SANS and NIST for incidents like Malware, Phishing, DDOS and should support creation of multiple playbook based on the SOC's Use case.		
6	The solution must be able to provide incident response playbooks that consist of phases and tasks that guides the user on how to adequately response to the incident; integrating people, processes and technology.		
7	The solution must provide a visual workflow editor that is based on BPMN-Business Process Model and Notation to enforce sequencing of incident response activities		
8	The solution must include a in-product script editor with autocomplete and syntax highlighting, to support automation of incident response workflow.		
9	The solution must include a in-product script editor with run buttons to facilitates debug and perform tests on scripts.		
10	The solution must allow organizations simulate incidents, to test response plans, allowing them to identify gaps and refine processes before a real incident happens.		
11	The Proposed Solution should have out-of-the-box bi-directional integration with the proposed SIEM solution & App on both platform (SIEM & SOAR)		
12	The proposed solution should have out-of-the-box provision for creation of incident from the existing SIEM automatically or manually.		
13	The proposed solution should have out-of-the-box provision of closing incident simultaneously on SIEM and the proposed SOAR platform.		
14	The proposed solution should have out-of-the-box capability to query or add IOC/Artifact to existing reference set of the deployed SIEM solution.		
15	The Proposed solution should have web based application store which should host latest integrations available from the OEM these integration can be downloaded with no additional cost.		

16	The proposed solution should have community portals and knowledgebase which can be used to learn about sample integration and forum to discuss issue or use cases.		
17	The proposed solution should support multi-organisation support wih the proposed SIEM.		
B	**Administration, Configuration, Dash Board & Reports**		
1	The proposed solution should support disaster Recovery and the same shall be offered as the part of solution.		
2	The solution must be offered as a virtual appliance for on premise deployment.		
3	The solution must be able to support multi-tenancy.		
4	The solution must support a web-based GUI for management, analysis and reporting. Please describe how your solution meets this requirement.		
5	The solution must provide central management of incidents and administrative functions from a single web based user interface. Please describe how your solution meets this requirement.		
6	The solution must support creation of user and user groups.		
7	The administrator must be able to define role base access to the solution by incidents. Please describe how your solution meets this requirement.		
8	The administrator must be able to define role based access to various functional areas of the solution. This includes being able to restrict a users access to specific functions of the solution that is not within the scope of a users role including, but not limited to, administration, reporting, incident assignment, playbook creation. Please describe how your solution meets this requirement.		
9	The solution must offer granular license offering for the various modules or supported features.		
10	The solution should be designed considering 5 Authorized users.		
11	The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. Please describe how your solution meets this requirement.		
12	The solution must deliver sample dashboards out-of-the-box (not limited to - Incident Over Time by Type, Open Incidents by Phase, Close Incident by Duration). Please describe how your solution meets this requirement.		
13	The solution must deliver customizable dashboard widgets that can present relevant incident information to the users. Please describe how your solution meets this requirement.		

14	The solution must maintain a database of incidents. The user must be able to search this database using the embedded elastic search. Please describe how your solution meets this requirement.		
15	The solution must support and maintain a history of user activity per incident. Please describe how your solution meets this requirement.		
16	The solution should offer graphical representation of all the artifact associated to a particular incident along with the timeline. It should enable the analyst to take action from within the graphical view on any artifact i.e. this could be blocking a IP address or doing further investigation using any of the threat service available to solution.		
17	The Solution should offer Timeline graph for each incident allowing display that can be set to display days, weeks, and months. It should also allow analyst to add milestones to call out important events within the timeline. Where the analyst can add a date, title, and description of your milestone.		
18	The solution should allow adding custom table to incident layout allowing organisation to track relevant fields based on use case. Such as Approval flow, Response time, Actions performed to name a few.		
19	The solution must provide reporting templates, to report on incident information, for the management team as well as the IT Security team via the GUI. Describe how the solution provides the ability to configure reports.		
20	The solution must provide configurable reporting engine for customized report creation. Please describe how your solution meets this requirement.		
21	The solution must support importing and exporting of configuration settings.		
C	**CORRELATION AND ANALYTICS**		
1	The solution must offer out-of-the-box support for auto creation of incident artifacts. Please describe how your solution meets this requirement.		
2	The solution must out-of-the-box include an analytics engine that displays relationship between incidents based on similar artifacts. Please describe how your solution meets this requirement.		
3	The solution must be able to support logical segregation of incidents. This will be used to assign a specific group of incidents to a specific group of users/analysts		
4	The solution must able to support creation of a Wiki pages. This enables organizations to add important information, guidelines, and reference material for the Incident Response team.		
5	The solution must provide long term trend analysis of incidents. Please describe how this requirement is met by the solution.		

6	The solution must provide more advanced incident drill down when required. Please describe how this requirement is met by the solution.		
7	The solution must support periodic updates of threat intelligence for incident artifacts. Please describe how this requirement is met by the solution.		
8	The solution must provide the ability to correlate artifacts across potentially disparate incidents. Please describe how your solution meets this requirement.		
9	The solution must support the ability to trigger action on external systems, for a related to an incident. For example, the solution should support the ability to block an intruder. Please describe how your solution meets this requirement.		
10	The solution must support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution. Please describe how your solution meets this requirement.		
11	The solution must dynamically augment incident playbooks in real time to support a specific incident response workflow. Please describe how your solution meets this requirement.		
12	The solution must provide the ability to contextually link incidents with similar artifacts. Please describe how your solution meets this requirement.		
13	The solution must provide the means for analysts to review the enrichments performed on the incident to arrive at conclusions about a security incident.		
14	The solution must out-of-the-box integrate with 7+ threat intelligence feed providers to provide data enrichment of incident artifacts.		
15	The solution must, out-of-the-box, must provide visualization of incident correlation across IOCs and other artifacts automatically with timeline support.		
16	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response.		
	AI & Machine Learning:		
1	The solution must have AI support, scan artifacts and attachments, and address any questions about incidents, artifacts and attachments.		
2	The GenAI assistant should able to provide incident summarisation, artifact analysis, conversational interface, custom playbook automation		

User Behavior Analytics (UEBA)

Sl No.	Specification	Compliance (Yes or No)	Remarks
1	UBA should be proposed as inbuilt capability of offered SIEM solution.		
2	Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency.		
3	Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time.		
4	Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly		
5	Usage deviates from peer group such as User pattern of activity starts deviating from the peer group		
6	Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems		
7	Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing		
8	Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data		
9	Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data		
10	Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users		
11	UBA should activate a rules for a set of users until a specified condition or specified time window.		
12	Solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling.		
13	UBA should be part of the SIEM solution & SI should not require any additional/ Third party component to complete the UBA solution.		
14	UBA UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of users' behaviors, risks and trends from a single screen		
15	UBA should perform the below mentioned scenario's as well.		
16	UBA ML model must cover • Individual user models (by numbers or observed): Like Access Activity, user's general activity by time, Authentication Activity, data		

	that is downloaded or uploaded by user, Lateral Movement, process usage etc • Peer Group Analysis: like Activity distribution, defined peer group, learned peer group etc. Custom Models: like Application Events, Source IP, Destination Port, Office File Access, AWS Access, Process, Website, Risky IP		
17	**ML Based UBA Usecases must include**		
	Access activity		
	Aggregated activity		
	Authentication activity		
	Data uploaded to remote networks		
	Data downloaded		
	DML events		
	DDL events		
	Large HTTP transfers		
	Outbound transfer attempts		
	Risk posture		
	Suspicious activity		
	Successful access and authentication activity		
	Activity distribution		
	Defined peer group		
	Learned peer group		
	Lateral Movement: Internal Destination Port Activity		
	Lateral Movement: Network Zone Access		
	Lateral Movement: Internal Asset Usage		
	Process Usage		
	Use Case for UBA:		
	Account accessing more high value assets than normal		
	More data being transferred then a normal to and from servers and / or external location		
	Privileged account accessing high-value servers from a new location for the first time		
	Account used for the first time in a long time		
	Rare privilege escalation		
	Accounts being used from peculiar locations		
	User involved in previously malicious or threatening behaviour		
	User an outlier within their peer group.		
	Exfiltration:		
	Data Exfiltration by Print		
	Data Exfiltration by Removable Media		
	Data Loss Possible		
	Initial Access Followed by Suspicious Activity		
	Large Outbound Transfer by High Risk User		
	Multiple Blocked File Transfers Followed by a File Transfer		

	Browsing behavior:		
	Browsed to Entertainment Website		
	Browsed to Gambling Website		
	Browsed to Information Technology Website		
	Browsed to Mixed Content/Potentially Adult Website		
	Network Traffic and Attacks		
	D/DoS Attack Detected		
	Honeytoken Activity		
	Capture, Monitoring and Analysis Program Usage		
	DNS Analysis		
	Potential Access to Blacklist Domain		
	Potential Access to DGA Domain		
	Potential Access to Squatting Domain		
	Potential Access to Tunneling Domain		
	Geography Based		
	Anomalous Account Created from New Location		
	User Access from Multiple Locations		
	User Geography Change		
	User Geography, Access from Unusual Locations		

Network Detection and Response (NDR)

Sl No.	Specification	Compliance (Yes or No)	Remarks
1	The NDR should be an appliance-based solution capable of monitoring 10 Gbps of network throughput from day one, and must include a redundant power supply and 8 × 10G SFP+ ports.		
2	The solution must be horizontally scalable to accommodate growth in network traffic volume to 20Gbps and beyond without the need for a full re-architecture.		
3	The solution must display visual traffic profiles in terms of bytes, packet rates and number of hosts communicating. These displays must be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views must support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts. Please describe how your solution meets this requirement.		
4	The solution must support application definition beyond protocol and port. The system must support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as		

	Instant messenger - not HTTP). Please describe how your solution meets this requirement.		
5	The solution must use machine learning to dynamically establish and maintain a baseline of normal network behavior for all users, devices, and applications. It shall alert on any significant deviations from this established norm.		
6	The solution must detect and present views of traffic pertaining to observed threats in the network. Describe the types of threats and visualizations for this information in the Security Intelligence system.		
7	The proposed solution must provide deep packet inspection (DPI) capabilities to identify and classify applications and threats regardless of the port or protocol they use.		
8	Solution must support Netflow, JFlow, SFLow, IPFix collection and correlation.		
9	The solution must support traffic profiling associated with logical network design (e.g., Subnet/CIDR).		
10	The solution must identify network traffic from potentially risky applications (e.g. file sharing, TOR, telnet, ftp, p2p.etc.).		
11	The solution must display traffic profiles in terms of packet rate. This capability must be available for simple TCP analysis (TCP Flags, etc.) but rate-based information may be presented for other profiles (e.g., applications).		
12	The solution must profile and present information in multiple timeframes. Profiles must be available for week, day and hour.		
13	The solution must be able to profile communication originating from or destined to the internet by Geographic regions in real-time. Describe how this is accomplished.		
14	The solution must create clearly independent and differentiated profiles from local traffic vs. traffic originating or destined for the internet.		
15	The solution must allow the user to create custom profiles and views using any property of a flow, log, data source or already profiled traffic. Describe how the Security Intelligence system supports this level of customization.		
16	The solution must support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc. Please describe how your solution meets this requirement.		
17	The solution must identify network traffic within a virtual network environment. Please describe how your solution meets this requirement.		
18	The SIEM must roll up all events and network flows into single offenses.		
19	The solution must be able to detect suspicious communication channels Services or applications		

	not running over its standard ports. (i.e. HTTP not over port 80)		
20	The SIEM must have the ability to generate reports on flows and events and to declare higher level aggregation of raw events into meaningful "Security Incidents" worth investigating.		
21	The solution should support importing of YARA rules and use those rules for matching and flagging malicious content.		
22	The Solution should provide app which allow uploading of yara rules and allow testing of these rules against log , flows and files to test.		
23	The App should allow importing YARA rules from opensource such as github, to take advantage of community learning.		
24	The proposed solution must be able to detect and alert on threats hidden within encrypted traffic by analyzing metadata and behavioral patterns without requiring SSL/TLS decryption.		
25	The solution must automatically detect and profile network traffic related to command-and-control (C2) communication, ransomware, malware, and data exfiltration.		
26	The solution must have built-in capabilities to detect and alert on common attack techniques, including DDoS attacks, port scanning, and peer-to-peer (P2P) traffic.		
27	The solution must provide full packet capture (FPC) capabilities to record network conversations for in-depth forensic analysis. The storage and retrieval of this data must be scalable and efficient.		
28	The system shall provide automated threat-hunting capabilities to proactively search historical network traffic for indicators of compromise (IOCs) and indicators of attack (IOAs) that may have been previously undetected		

Threat Intelligence & Analytics

Threat Intelligence is the most important component in analyzing threats and security related incidents. Threat intelligence data need to be fed to the SIEM tool for better detection and quick response in case of security incident.

S. No.	Specification of Threat Intelligence	Compliance / Non-Compliance
General Features		
1.	Threat Intelligence should deliver a comprehensive range of timely adversary and technical threat intelligence through a customizable portal or Dashboard	

2.	Receive feeds from a threat intelligence repository maintained by the OEM and from leading global intelligence sources. Supports external threat intelligence such as D-Shield, Spam Haus etc. which could be used to identify incidents based on knowledge of global security research, to supplement its own threat feed	
3.	Threat Intelligence should provide data feeds and API's for automated consumption by the SIEM Tool	
4.	Threat Intelligence provided must be relevant, context-rich, timely and accurate	
5.	Threat Intelligence feeds should contain who, how and why are you being targeted	
6.	Threat Intelligence must enable to perform countermeasures for current and future threats	
7.	Threat intelligence feeds should enable efficient security operations and reduce the time for investigation	
8.	Threat Intelligence should be capable to integrate with security, risk and management systems and provide insights about emerging and current threats	
9.	The threat intelligence feeds should be available in multiple formats (CSV, XML, CEF).	
10.	Threat intelligence should provide an insight into current and emerging threats	
Threat Intelligence Portal/Dashboard		
11.	The Threat Intelligence Portal/Dashboard should provide a complete range of adversary and technical intelligence.	
12.	The Threat Intelligence Portal/Dashboard should provide End-to-End picture of threats	
13.	The Threat Intelligence Portal/Dashboard should provide Adversary Intelligence	
14.	Threat Intelligence to provide reputation data feeds for actionable intelligence on IP addresses and Domains/URLs exhibiting malicious activity such as malware distribution and botnet command and control server communication. The data feeds should be derived from activity on the Internet and a reputation score along with additional contextual attributes should be provided for each of the IP address and Domains/URLs.	

Advanced Alert Analytics & Attack Detection Capabilities

S. No.	Specification of alert analytics & attack detection capabilities	Compliance / Non-Compliance
General Features		

1.	The solution should have capabilities to detect any compromises by linking related alerts collected together over a period of time.	
2.	Solution should have capabilities to correlate alerts between sources & destination IPs to find similar or colluding threat signals.	
3.	Solution should have a knowledge base on methods used by attackers in various past breaches globally to create models to detect such attacks.	
4.	Solution should utilize data science techniques to identify kill chains for attacks such as lateral movements e.g. If a destination IP of one alert later becomes a source IP of another alert this suggests existence of a sequence.	
5.	Solution should have detection models to find out threat's sources are linked to the same attacker by grouping alerts with common characteristics like time, day location, target asset profiles etc.	

ANNEXURE 2: MANPOWER REQUIREMENT & DESIRED SKILLSET

Bidder shall factor the resource required to meet the below requirement.

Threat & Incident Management				
Analyst Type	**Morning**	**General**	**Afternoon**	**Night**
L1	3	1	3	2
L2	1	0	1	1
L3	0	1	0	0

a) L3 Resource shall have the responsibilities of Project Manager also.
b) Bidder's resources deployment should ensure a 24*7 operational SOC. No additional resources shall be added to the project without the KSITM's explicit approval.
c) Successful bidder will have to submit names and profiles of the resources working the project on a quarterly basis and match the criteria in the RFP. SOC provider will also be required to submit an undertaking on a quarterly basis, hat no one, other than profiles shared with KSITM, are deployed on the project.
d) The bidder shall submit the attendance sheet to KSITM every quarter.
e) KSITM reserves the right to ask for replacement of any personnel on grounds of misconduct and/ or non-performance.

Desired skill set for Onsite resources:

SL No.	Analyst Type	Skills Required
1	**L1 Analyst**	Understanding of networking and security concepts.
2		Familiarity with common cyber threats and attack vectors.
3		Proficiency in using proposed security monitoring tools and SIEM platforms.
4		Analytical skills to assess and validate security alerts.
5		Good communication and documentation skills.
6		Ability to follow established procedures and protocols.
7		The L1 analyst shall have Graduation/PG in science or engineering with minimum 1 years of experience in Monitoring and responding to cyber threats, preferably possess at least one of the following certifications: ➢ Security+/CEH/ECSA/OEM Certification
8	**L2 Analyst**	Strong understanding of networking and security fundamentals.
9		Proficiency in analyzing logs and network traffic.
10		Experience with malware analysis and reverse engineering.
11		Knowledge of scripting and automation (e.g., Python, PowerShell).
12		Excellent problem-solving and analytical skills.
1		Strong communication and documentation skills.
14		The L2 Incident responder shall have Graduation/PG in science or engineering with minimum 3-5 years of experience in Incident response, preferably possess at least one of the following certifications: ➢ Security+/ECSA/GCFA/GCFE/CISSP/OEM Certification

15	**L3 Analyst**	Graduation/PG in science or engineering with Minimum 6-8 Years of experience in Security operation centre and have 3 years as SOC Manager
16		Knowledge of incident response frameworks (e.g., NIST, SANS).
17		Proficiency in using and managing SIEM, SOAR and UEBA
18		Knowledge of relevant security standards and regulations (e.g., ISO 27001, GDPR, HIPAA).
19		Deep understanding of networking, operating systems, and security principles.
20		Expertise in digital forensics, malware analysis, and reverse engineering.
21		Strong analytical and problem-solving skills.
22		Proficiency in using advanced security tools and technologies.
23		Excellent communication and documentation skills.
24		Ability to handle high-pressure situations and make critical decisions.
25		Continuous learning mindset to stay updated with the evolving threat landscape.
26		Preferably shall have any two certifications from the mentioned list, Cyber Security - Any One ➢ CISSP/CISM/CISA Incident and Program Management - Any One ➢ ITIL (Information Technology Infrastructure Library)/PMP (Project Management Professional)

ANNEXURE 3: Assets Details

Operating System	
OS	**Version**
Windows	Windows Server Core 2012, 2016, 2019& 2022 Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Windows Storage Server 2016, 2012 R2, 2012 Windows 10, 11
Linux	CentOS (6,7,8,9) Debian Ubuntu (16,18,20,22,24) Red Hat Enterprise Linux (RHEL- 6,7,8,9) SUSE Linux Enterprise Server Oracle
Virtual environments	Microsoft Hyper-V Vmware RHV RedHat Openshift

Network/Security Devices		
Network/Security Devices	**Make & Model**	**Throughput/Count**
Firewall	Fortinet/FGT-1200D, Fortinet/FGT-1500D	**72Gbps / 80 Gbps**
DP-4412-SDC2	Radware /DefensePro 4412	**4 Gbps**
SDC2-ALTEON	Radware /Alteon 5208 XL	**2 Gbps - 4 Gbps**
DDAN	Deep Discovery Analyzer 1100 v1	
DDI	Deep Discovery Inspector 1100	
XDR	SentinelOne	**1500**
WAN Router at SDC 2	Juniper /Mx 480	**2**
WAN Router at SDC 1	CISCO 9006	**2**

Internet Links		
Internet Edge Router	**Make & Model**	**Provisioned Internet Bandwidth**
Router at SDC2	Juniper /Mx 104 (2 No.s)	7 Gbps
Router at SDC1	CISCO 9006 (2 No.s)	3.5 Gbps

ANNEXURE 4: State Bank of India Multi Option Payment System (SBI MOPS Gateway)

Bidders are required to avail Internet Banking Facility in any of below banks for making tender remittances in eProcurement System.

A) Internet Banking Options (Retail)			
1	Allahabad Bank	32	Kotak Mahindra Bank
2	Axis Bank	33	Lakshmi Vilas Bank
3	Andhra Bank	34	Mehsana Urban Co-op Bank
4	Bandan Bank	35	NKGSB Co-operative Bank
5	Bank of Bahrain and Kuwait	36	Oriental Bank of Commerce
6	Bank of Baroda	37	Punjab and Maharashtra Cooperative Bank
7	Bank of India	38	Punjab National Bank
8	Bank of Maharashtra	39	Punjab and Sind Bank
9	Bassein Catholic Co-operative Bank	40	RBL Bank
10	BNP Paribas	41	Saraswat Cooperative Bank
11	Canara Bank	42	ShamraoVithal Cooperative Bank
12	Catholic Syrian Bank	43	South Indian Bank
13	Central Bank of India	44	Standard Chartered Bank
14	City Union Bank	45	State Bank of India
15	Corporation Bank	46	Syndicate Bank
16	Cosmos Bank	47	Tamilnad Mercantile Bank
17	DCB Bank	48	Tamilnadu Cooperative Bank
18	Dena Bank	49	The Kalyan Janata Sahakari Bank
19	Deutsche Bank	50	TJSB Bank (Erstwhile Thane Janata Sahakari Bank)
20	Dhanalaxmi Bank	51	UCO Bank
21	Federal Bank	52	Union Bank of India
22	HDFC Bank	53	United Bank of India
23	ICICI Bank	54	Vijaya Bank
24	IDBI Bank	55	YES Bank
25	Indian Bank		
26	Indian Overseas Bank		
27	IndusInd Bank		
28	Jammu & Kashmir Bank		
29	Janata Sahakari Bank		
30	Karnataka Bank		
31	Karur Vysya Bank		
B) Internet Banking Options (Corporate)			
1	Bank of Baroda	21	Laxmi Vilas Bank
2	Bank of India	22	Oriental Bank of Commerce
3	Bank of Maharashtra	23	Punjab & Maharashtra Coop Bank

4	BNP Paribas	24	Punjab & Sind Bank
5	Canara Bank	25	Punjab National Bank
6	Catholic Syrian Bank	26	RBL Bank
7	City Union Bank	27	ShamraoVitthal Co-operative Bank
8	Corporation Bank	28	South Indian Bank
9	Cosmos Bank	29	State Bank of India
10	Deutsche Bank	30	Syndicate Bank
11	Development Credit Bank	31	UCO Bank
12	Dhanalaxmi Bank	32	Union Bank of India
13	Federal Bank	33	UPPCL
14	HDFC Bank	34	Vijaya Bank
15	ICICI Bank	35	Axis Bank
16	Indian Overseas Bank		
17	Janta Sahakari Bank		
18	Jammu & Kashmir Bank		
19	Karur Vysya Bank		
20	Kotak Bank		

During the online bid submission process, bidder shall select ***SBI MOPS*** option and submit the page, to view the ***Terms and Conditions*** page. On further submitting the same, the e-Procurement system will re-direct the bidder to MOPS Gateway, where two options namely ***SBI*** and ***Other Banks**** will be shown. Here, Bidder may proceed as per below:

a) *SBI Account Holders* shall click ***SBI*** option to with its Net Banking Facility., where bidder can enter their internet banking credentials and transfer the Tender Fee and EMD amount.

b) *Other Bank Account Holders* may click ***Other Banks*** option to view the bank selection page. Here, bidders can select from any of the 54 Banks to proceed with its Net Banking Facility, for remitting tender payments.

**Transaction Charges for Other Banks vide SBI Letter No. LHO/TVM/AC/2016-17/47 – 1% of transaction value subject to a minimum of Rs. 50/- and maximum of Rs. 150/-*

** Bidders who are using Other Banks option under SBI MOPS Payment Gateway, are advised by SBI to make online payment 72 hours in advance before tender closing time.*

Any transaction charges levied while using any of the above modes of online payment has be borne by the bidder. The supplier/contractor's bid will be evaluated only if payment status against bidder is showing "**Success**" during bid opening.

Department will not be responsible for any delay in receipt of required amount and shall reject such bid(s) where amount has not been credited within the last date and time of bid submission. Also, amount credited after the stipulated last date & time of bid submission shall also not be considered and such bids shall be rejected. The supplier/bidder's bid will be evaluated only if payment status against bidder is showing "Success" during bid opening.

It is necessary to click on "Freeze bid" link/ icon to complete the process of bid submission, failing which the bid will not get submitted online and the same shall not be available for viewing/ opening during bid opening process.

CHECKLIST FOR SUBMISSION

#	Particulars	Bidders Remark Yes/No
1	Certificate of incorporation	
2	GSTN Registration Certificate and PAN	
3	Audited Balance sheets of last three years	
4	Reference Letters / Purchase Orders for Eligibility Criteria 5	
5	Reference Letters / Purchase Orders for Eligibility Criteria 6	
6	Reference Letters / Purchase Orders for Eligibility Criteria 8	
7	Details of Resources on Company's letter for Eligibility Criteria 10	
8	Format 1: Technical Bid Letter	
9	Format 2: Turnover	
10	Format 3: General Information about Bidder	
11	Format 4: Bidder experience	
12	Format 5: Commercial Bid Letter	
13	Format 6: Manufacturer Authorization Form (MAF)	
14	Format 7: Undertaking on three Year Comprehensive Onsite Warranty Support	
15	Format 8: Undertaking on Acceptance of Terms and Conditions in Tender	
16	Format 9: Undertaking on Not Being Black-Listed	
17	Format 10: Compliance Statement	
18	Format 11: Non-Compliance Statement	
19	Format 12: NON-DISCLOSURE AGREEMENT	
20	Format 13: Performance Bank Guarantee (PBG)	
21	Format 14: EMD Declaration	

Format 1: Technical Bid Letter

Date:

Tender No:

To,
The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

Sir / Madam,

Having examined the Tender Documents including Corrigendum / Addendum Nos..... [*insert numbers*], the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver..... (*Description of Services*) in conformity with the said tender documents for the sum stated in the e-Procurement portal for this tender.

We undertake, if our tender is accepted, to deliver the services in accordance with the Project Deliverables, Project Duration & Timelines. If our tender is accepted, we will obtain the guarantee of a bank for a sum equivalent to 3% percent of the total Contract Price for the due performance of the Contract, in the form prescribed in this tender.

We agree to abide by this RFP for the validity period and it shall remain binding upon us and may be accepted at any time before the expiration of that period. Until a formal contract is prepared and executed, this tender, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

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

We understand that you are not bound to accept the lowest or any tender you may receive.

We clarify/confirm that we comply with the eligibility requirements as per clauses of the tender.

Dated this ..... day of ..... 20.....

_____ _____

(Signature) (in the capacity of)
Duly authorized to sign Tender for and on behalf of_____

Format 2: Turnover

[Auditor's certificate shall be issued by the Chartered Accountant Firm/Chartered Accountant who regularly audit the Company's accounts]

TO WHOMSOEVER IT MAY CONCERN

This is to certify that the annual turnover furnished by << COMPANY NAME >> for last 3 years i.e. 2021-22, 2022-23 and 2023-24 as below. This is as per the Statement of Accounts which has been duly verified by me and found correct.

Financial year	Total Turnover of the Company (Rs. in crores)
2021-22	
2022-23	
2023-24	

Chartered Accountant Name:

Signature:

Seal:

Format 3: General Information about Bidder

Details of the Bidder (Company)		
1.	Name of the bidder	
2.	Address of the bidder	
3.	Status of the Company (Public Ltd/ Pvt. Ltd)	
4.	Details of Incorporation of the Company	Date: Ref. #
5.	Details of Commencement of Business	Date: Ref. #
6.	Valid Sales tax registration no.	
7.	Valid Service tax registration no.	
8.	Permanent Account Number (PAN)	
9.	Valid GST registration no.	
10.	Name & Designation of the contact person to whom all references shall be made regarding this tender	
11.	Telephone No. (with STD Code)	
12.	e-Mail of the contact person:	
13.	Fax No. (with STD Code)	
14.	Website	

Format 4: Bidder experience

Project Name	Scope of Work	Date of issue of work order	Total Number of years (as on bid submission date)	Name & Contact details of Client	Project Cost	Current Status (Ongoing / Completed)

Note: The above table has to be filled with the relevant project details for the criteria stated under pre-qualification and technical evaluation criteria.

Format 5: Commercial Bid Letter

To,
The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

Sir,

Subject: "Supply, Installation and Commissioning of Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), UEBA, Threat Intelligence Platform & Network Detection & Response (NDR) Solutions and the management of the State SOC" at State Data Centre 2, Tejaswini Building, Technopark, Thiruvananthapuram.
Reference:

Tender No:<**Tender Reference Number**>Dated<dd/mm/yyyy>

Dear Sir,

Having examined Request For Proposal (RFP) number----------dated ---- ----------the receipt of which is hereby acknowledged, we, the undersigned, offer "Supply, Installation and Commissioning of Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), UEBA, Threat Intelligence Platform & Network Detection & Response (NDR) Solutions and the management of the State SOC" in full conformity with the said RFP, for a total project cost of Rs …… (Rupees …… only). The above amount is in accordance with the Price Schedules herewith made part of this bid as per the Commercial bid template.

We undertake that we shall carry out audit activities in conformity with the bidding documents (and as amended from time to time) for a total cost as provided in the Commercial bid if the contract is awarded to us.

1. We declare that we have studied RFP and are making this proposal with a stipulation that you shall award us Contracts, either in part or whole, "Supply, Installation and Commissioning of Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), UEBA, Threat Intelligence Platform & Network Detection & Response (NDR) Solutions and the management of the State SOC" (meaning as realized in RFP) including all other services specified in the Contract Documents.
2. We have read the provisions of RFP and confirm that these are acceptable to us. All necessary clarifications, if any, have been sought for by us and duly clarified in writing, by KSITM. We understand that any other ambiguous clauses in the RFP, if any, are subject to interpretation KSITM.
3. We further declare that additional conditions, variations, deviations if any, found in the proposal other than those listed in Attachment pertaining to any rebates offered, shall not be given effect to.
4. We undertake, if our bid is accepted, to commence the work on the project immediately upon your Notification of Award to us, and to achieve Completion within the time stated in the Bidding Documents.
5. If our bid is accepted, we undertake to execute all contractual documents and provide all securities & guarantees as required in the bid document (and as amended from time to time).
6. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act".
7. We agree to abide by this bid, consisting of this letter, the tender fee, EMD, Technical bid and Commercial bid, for a period of bid validity from the date fixed for submission of bids as stipulated in the RFP, and it shall remain binding upon us and may be accepted by you at any time before the expiration of that period.

8. Until the formal order is placed and final Contract is prepared and executed between us, this bid, together with your written acceptance of the bid and your notification of award, shall constitute a binding contract between us.

Dated this [insert : number] day of [insert : month] , [insert: year]

Signed : ……. In the Capacity of [insert: title of position]

Duly authorized to sign this bid for and on behalf of [insert: name of the Bidder]

Witness:

Address:

Format 6: Manufacturer Authorization Form (MAF)

(On OEM Letter Head)

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.

Manufacturers Authorization Form (MAF)

Date: dd/mm/yyyy

To,
The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

Sir/Madam,

Sub: Manufacturer Authorization for Supply, Installation and Support of Manged SOC
Ref.: Tender No: <TENDER REFERENCE NUMBER> dated <DD/MM/YYYY>

We, _____ (name and address of the manufacturer), who are established and reputed manufacturers of _____(name and description of goods offered) having factories at _____ (addresses of manufacturing locations) do hereby authorize M/s _____ (name and address of the Bidder) to submit bid, negotiate and sign the contract with you for the items manufactured by us against the above mentioned tender.

We also certify that the Products offered would not be discontinued or be declared end–of–life or end-of-support for a period of 5 years from the date of Purchase Order.

We hereby extend our full guarantee and warranty for three year, as per RFP clauses for the items offered for supply and support by the above firm against this tender, extendable by further two years..

We also undertake that during the period of contract, incase bidder authorized by us fails to perform, we shall provide support services.

Yours faithfully,

(Name)
(Name of the manufacturers and seal)

Format 7: Undertaking on Comprehensive Onsite Warranty Support

(On company letter head)

Undertaking on Three Year Comprehensive Onsite Warranty Support

Date: dd/mm/yyyy

To,

Sir/Madam,

Sub.: Undertaking on Three Year Comprehensive Onsite Warranty support for all items procured under this RFP.
Ref.: Tender No: <TENDER REFERENCE NUMBER> dated <DD/MM/YYYY>

We, _____ (name of the bidder) hereby, confirm to provide comprehensive onsite warranty support for all items procured under this RFP for a period of Three years from the date of acceptance by KSITM, extendable by another two years.

Yours faithfully,

Authorized Signatory

Name of Signatory:
Date:
Place:

Note: This undertaking should be on the letterhead of the bidder and should be duly signed and sealed by the authorized signatory of the bidder.

Format 8: Undertaking on Acceptance of Terms and Conditions in Tender

(On company letter head)

Undertaking on Acceptance of Terms and Conditions in Tender

Date: dd/mm/yyyy

To,
The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

Sir / Madam,

Sub.: Undertaking on acceptance of terms and conditions of this RFP.
Ref.: Tender No: <TENDER REFERENCE NUMBER> Dated <DD/MM/YYYY>

I have carefully gone through the Terms & Conditions contained in this RFP document.

I hereby confirm that all the provisions, terms and conditions of this RFP Document& Corrigendum / Addendum issued are acceptable to my company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours faithfully,

Authorized Signatory

Name of Signatory:
Date:
Place:

Note: This undertaking should be on the letter head of the bidder and should be duly signed and sealed by the authorized signatory of the bidder.

Format 9: Undertaking on Not Being Black-Listed

(On company letter head)

Undertaking on Not Being Black-Listed

Date: dd/mm/yyyy

To,
The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

Sir/Madam,

Sub.: Undertaking on not being blacklisted.
Ref.: Tender No: <TENDER REFERENCE NUMBER> dated <DD/MM/YYYY>

We hereby confirm that << COMPANY NAME >> is not blacklisted by the Government of Kerala or any of its agencies for any reasons whatsoever and not blacklisted by Central / any other State / UT Government or its agencies for indulging in corrupt or fraudulent practices or for indulging in unfair trade practices as on date of publishing of this tender.

Yours faithfully,

Authorized Signatory

Name of Signatory:
Date:
Place:

Note: This undertaking should be on the letter head of the bidder and should be duly signed and sealed by the authorized signatory of the bidder.

Format 10: NON-DISCLOSURE AGREEMENT

We, <name of company>, registered as …. With office at …., acknowledge and accept that, as a potential bidder for the Kerala State IT Mission or Government Departments of Kerala (all hereinafter referred to as "the Department") and as a representative to its Citizens, customers or related clients/Vendors we may have access to and become possessed of proprietary information of the Department, its Citizens, customers or related clients/Vendors. We accept that it is entirely reasonable for the Department to protect its rights and those of its Citizens, customers or related clients/Vendors in this proprietary information.

For purposes of this agreement, "Information" shall include:

1. All documents which are prepared or received by the Department, including all correspondence, memoranda, notes, summaries, analyses, studies, models, extracts of documents and records reflecting, based upon or derived from information, as well as all copies and other reproductions thereof, drafts and files and notings, whether in writing or stored or maintained in or by electronic, magnetic or other means of media or devices.

2. "Trade Secrets", which, as used herein means the whole or any part of any proprietary information regarding the design, and provision of the Department's services including processes and techniques the Department utilizes in its business and activities. "Trade Secrets" also includes the whole or any part or technical information, design, process, procedure or improvement of the Department that is valuable and secret (in the sense that it is not known to or by any other party outside the Department).

3. All oral, written and electronic communication received during the course of consulting concerning the Department, its properties, operations, finances, tender submissions, contracts, agreements, related parties and all information pertaining to its customers and clients.

4. Technical information, methods, processes, formulae, compositions, systems, software, techniques, inventions, computer programs and research projects.

5. Business information, customer lists, pricing data, sources of supply, financial data and marketing, production, or merchandising systems or plans. This shall however be an indicative list and KSITM may notify any other information as part of the NDA.

We therefore agree to keep confidential and not to divulge, both during and after my term of bidding, all such proprietary information which may come to my knowledge, either directly or indirectly, during the course of or by virtue of our bid or preparation for bid with KSITM.

We agree not to make, in our personal capacity or as an representative of the company or Department, any public statement, in any media, touching on any matter relating to the Department's operation, business, clients or related parties without prior written authorization by the Department. We agree neither to divulge nor to authorize anyone else to divulge, either during the time of our engagement or afterwards, any confidential information.

We agree that upon the award of tender by the Department:

1. We shall destroy all documents and property of the Department obtained under NDA, including but not necessarily limited to: drawings, blueprints, reports, manuals, correspondence, letters, and all other materials and all copies thereof. We further agree that we shall not retain copies, notes or abstracts of the foregoing whether in writing or stored or maintained in or by electronic, magnetic or other means of media or devices.
2. This agreement shall be binding upon us and our employees and successors in interest, and shall inure to the benefit of the Department, its successors and assigns.

The above clause shall not be applicable to successful bidder who is awarded contract.

I agree that the department shall be entitled to equitable relief, including injunction, specific action in the event of any breach of the provisions of this agreement, in addition to all other remedies available to the Department at law or in equity. This agreement shall have effect from date of signing of the agreement.

Executed at ……..

Signature of Authorized representative of Company
Name & Designation with full address

Date:

Format 11: Compliance Statement

S.No	Section/ Page No. in RFP	Clause No. as in RFP	Requirement as specified in RFP	Compliance (Yes/No)	In case of deviation, SL.No of the item in non-compliance statement (Section 9.4)

Format 12: Non-Compliance Statement

S.No	Section/ Page No. in RFP	Clause No. as in RFP	Requirement as specified in RFP	Deviation	Remarks / Reasons / Alternatives suggested

Format 13: Performance Bank Guarantee (PBG)

Performance Bank Guarantee (PBG)

To,
The Director
Kerala State Information Technology Mission
Saankethika, Vrindavan Gardens, Pattom. P.O,
Thiruvananthapuram, 695004, Kerala
Tel: 0471 2525444

WHEREAS ..... (Name of Supplier)

hereinafter called "the Supplier" has undertaken , in pursuance of Contract No..... dated,..... 20... to supply..... .....(Description of Goods and Services) hereinafter called "the Contract".

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Supplier a Guarantee:

THEREFORE WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of .... (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without cavil or argument, any sum or sums within the limit of ..... (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the .....day of.....20.....

Signature and Seal of Guarantors
.....
.....
.....

Date.....20....

Address:.....
.....
.....

Format 14: EMD Declaration:

EMD Declaration Form

I, hereby submit a declaration that the tender submitted by the undersigned, on behalf of the tenderer…… (Name of the tenderer), shall not be withdrawn or modified during the period of validity or extended period of validity.

I, on behalf of the tenderer……(Name of the tenderer/bidder), also accept that the fact that in case the tender is withdrawn or modified during the period of its validity/extended validity period or if we fail to sign the contract in case the contract is awarded to us or we fail to submit a performance security and additional performance security, if any, before the deadline fixed in the tender document, then……(Name of the tenderer), will be debarred for participation in the tendering process for the procurements of this procurement entity for a period of one year from date of default.

(Signature of the Authorized Signatory, Official Seal)

Commercial Bid Format
(For reference only the commercial data should not be included as part of the technical bid)

The bidder has to directly enter the prices, on e-Procurement portal and submit the same. The format below is provided for reference purposes only. Bidders should not upload this format on the e-Procurement portal as it will lead to disqualification of their bid.

A. Capex: Supply, Installation and Commissioning of SOC equipment- SIEM, UEBA, TIP, SOAR

Sl. No.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes
1.	Supply, installation, configuration and commissioning of SIEM, SOAR, UEBA, TIP as per technical specification in RFP and provide OEM's onsite warranty support for three years.	1	No		
2.	Supply, installation, configuration and commissioning of NDR as per technical specification in RFP and provide OEM's onsite warranty support for three years.	1	No		
3.	Supply, installation, configuration and commissioning of Log Collectors as per the requirements mentioned in the RFP and provide OEM's onsite warranty support for three years.	18	No		

B. Opex: Charges for providing managed SOC services

Sl. No.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes
(A)	(B)	(C)		(D)	
1	Quarterly Charges for providing Managed SOC services as per deliverables/ service requirements mentioned in RFP	20	Per Quarter		

C. Additional manpower (resource) cost

Sl. No.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes
1	Quarterly Charges for providing additional L1 resource as per details mentioned in RFP	1	Per Quarter		
2	Quarterly Charges for providing additional L2 resource as per details mentioned in RFP	1	Per Quarter		

D. Additional license cost:

Sl. No.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes
1	Additional SIEM licenses for 10,000 EPS	1	LOT		
2	Additional Log Collectors	1	No		

Note: During the contract period, KSITM will issue additional purchase orders based on the requirement and bidder should supply the license/devices at the rate discovered. The payment will be issued upon submission on the invoices against the purchase orders.

E. Annual Maintenance cost:

Sl. No.	Goods / Items	Quantity	Unit	Unit Price	Total Amount without Taxes
1	AMC for the SIEM, SOAR, TIP and UEBA for 4th year	1	No		
2	AMC for the SIEM, SOAR, TIP and UEBA for 5th year	1	No		
3	AMC for NDR for 4th year	1	No		
4	AMC for NDR for 5th year	1	No		
5	AMC for Log Collectors for 4th year	18	No		
6	AMC for Log Collectors for 5th year	18	No		

Note:

a) GST will be paid to the bidder as per actuals at the time of invoice.
b) Price should be quoted only in e-procurement portal. The above table is provided for reference purpose only.
c) Payment will be as per payment terms in RFP.