Section E: Scope of Services

1. Brief Scope of Work

- As part of this RFP, LIC intends to implement a next generation SOC with following technologies seamlessly integrated to each other:
  - I. Security information and event management (SIEM) (with common security data lake for SOAR, UEBA, CTH)
  - II. Next Generation Security Operations Center (NGSOC)
  - III. Security Orchestration, Automation and Response (SOAR)
  - IV. User and Entity Behavior Analysis (UEBA)
  - V. Cyber Threat Hunting (CTH)
  - VI. Cyber Threat Intelligence (CTI)
  - VII. Packet Capture (PCAP)
  - VIII. Network Behavior Anomaly Detection (NBAD)/ Network Detection and Response (NDR)
  - IX. Endpoint Detection and Response (EDR)

- The bidder shall perform the below activities as part of the scope of work for all above technologies. Please note, the below list of activities is only indicative and not an exhaustive list. The deliverables mentioned shall be provided for each solution as part of this RFP.

Phase No.	Phase Name	Activities to be performed	Deliverables
1	**Planning**	• Conduct kick-off meeting. • Study of present architecture at Data centers. • Study of LIC's existing security environment and guidelines. • Identify business objectives & technical requirements. • Define pre-requisites if any. • Outline an implementation strategy and detailed plan with timelines and milestones for entire duration of the project. • Ensure that security and compliance requirements are integrated into the design and develop a plan for addressing them. • Ensure compatibility and interoperability between different security solutions. • Define the allocation of resources including personnel, equipment, and tools. • Outline the accurate placement of devices or appliances to ensure industry best practices are followed. • Conduct workshops with all the departments of LIC and any other identified vendor for (but not limited to) solution engineering, identifying gaps, crown jewels of LIC, integration, custom parser creation, creation of rules, use case development, finetuning, etc. • Use case workshop to be conducted by OEM/ OEM certified partner to discuss on existing use cases to be migrated, new use cases as per MITRE ATT&CK, CIS, compliance requirements of LIC, etc. as per the latest threat trends. The use case priority should also be captured so that the bidder can implement the use cases accordingly. • Use case workshop should arrive at the use cases based on priorities and detailed implementation approach of those use cases. The workshop should also include details of the data sources required and what events in each data source	Detailed Project Plan for each solution as part of this RFP. Note: Separate plan document to be submitted for each in-scope solution.

Phase No.	Phase Name	Activities to be performed	Deliverables
		is required for optimal use of license and exact threat detection. • Use case workshop should mandatorily have list of top threats as per attack vectors, industry, recent attack patterns and then should have recommendations for the same which needs to be implemented at LIC.	
2	**Designing**	• **Architecture Diagram:** o OEM should design the overall implementation architecture (high-level diagram and low-level diagram) for each in-scope solution. o Architecture workshop to be conducted by OEM/OEM certified partner to design the architecture as per industry best practices. o Connectivity and data flow diagram for each in-scope solution. • **Policy & Procedure Documents:** o Solution implementation documentation. o Acceptance procedures, Test cases & test plans, etc. o BCP/DR/Failover Strategy and process document. o Incident Response strategy and process document.	• Architecture Diagrams (High-level and low-level) • Connectivity and data flow diagram • Policy & Procedure documents Note: Above documents shall be prepared in a mutually agreed template. Bidder shall submit soft and hard copies for all the above documents in the finalized template.
3	**Implementing**	• **Supply and Installation:** o Supply of appliances wherever applicable and software for in-scope solutions. o Installation and implementation of the solutions as per the architecture design. o Installation will include proper mounting, labeling, tagging of all the equipment. o The bidder is responsible for supply of hardware required for setting up all the in-scope solutions at LIC data centres. The hardware is inclusive of but not limited to servers, Storage, Backup, Switches, Racks, Passive cabling, etc. LIC shall only be responsible for providing the required room space, cooling and power supply. o As per LIC's requirement, the successful bidder of the project shall be ready to shift, occasionally, the equipment from one place to other, uninstall and reinstall all the equipment without any additional cost to LIC. • **Configuration & Integration:** o Configuring the solutions as per defined MBSS/SCD. Configuration to meet industry standards and regulatory guidelines. o Integrating the solutions with: ▪ Its own components as applicable. ▪ Other existing security solutions and any security solutions procured in future as applicable. ▪ Active directory, servers, network devices, endpoints and other applicable IT assets. o Bidder shall recommend ways for secure communication and assist LIC in defining the use cases as applicable for the solutions. All such configurations/ changes shall be documented as part of the	• Site Ready Document/Site Not Ready Document as applicable. • Successful deployment confirmation • Validation report by OEM

Phase No.	Phase Name	Activities to be performed	Deliverables
		policy/process documentation. The use cases created should be undergoing the full use case lifecycle such as creation, testing, finetuning of false positive, automation, notification to the LIC specified personnel, etc. o Bidder shall provide the details of all scripts and configurations created or used at LIC, including their purpose, functionality, and relevance to the scope of work. • **Optimizing & Deployment Validation:** o Fine tuning of the solutions to be done based on the criteria defined in Technical Specification of each solution and should assure a false positive rate not more than 10 % after 1 year for all solutions/services. o Monitor and resolve issues as per the defined SLAs in this RFP. o Validation of deployment of the solutions/services to be performed based on industry best practices by respective OEM of the deployed solution/service. In case OEM is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a separate report to LIC accordingly. Bidder shall perform necessary changes as recommended by the OEM. o The OEM is required to conduct the audit, at the end of implementation and once in end of every year during the contract period. The recommendations/ remediation changes required after each audit should be completed within 3 months. o Bidder should discuss about the Governance structure and Project milestones and provide weekly updates to LIC on implementation status.	
4	**Sustaining**	• Post- deployment (after sign-off from LIC) bidder shall manage & monitor proposed solutions. • Facilitation & operation for continuous monitoring, performance optimization, upgradation, maintaining compliance with LIC policies, industry standards and regulatory guidelines, change management, incident response, etc. • **Policy & Procedure Documents:** o SOP for operations of the solution. o Detailed roles and responsibilities defined in RACI matrix. o Minimum Baselines Standard Document (MBSS)/Secure Configuration Document (SCD). o Access controls and security measures implemented document.	• Periodic reports such as (but not limited to) Daily, Monthly, Weekly, Ad-hoc, Audit requirement reports, etc. • Dashboards • End-end view of the incident lifecycle should be given in a report or in a single dashboard as requested by LIC.

- **Compliance with IS Security Policy:**
  The SI shall have to comply with LIC's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder. Some of the key areas are as under:
    - Responsibilities for data and application privacy and confidentiality.

- Responsibilities on system and software access control and administration
- Custodial responsibilities for data, software, hardware and other assets of LIC being managed by or assigned to the Vendor.
- Physical Security of the facilities
- Physical and logical separation from other customers of the Vendor
- Incident response and reporting procedures.
- Password Policy
- Access management Policy
- Acceptable usage Policy (Authentication and Identity Management, Authorization and access control)
- Data Encryption / Protection requirements of LIC
- Cyber Security Policy
- Auditing
- In general, confidentiality, integrity and availability, non-repudiation, authenticity, privacy of data/information must be ensured.
- Responsibilities in carrying out background verification of personnel deployed from vendor side regularly and submit the report as and when needed by LIC.

- **Right to Audit:**

a. It is agreed by and between the parties that the Service Provider shall get itself annually audited by external empaneled Auditors appointed by LIC/ inspecting official from the IRDAI or any regulatory authority, covering the risk parameters finalized by LIC/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to LIC and the vendor shall submit such certification by such Auditors to LIC. The vendor and or his / their outsourced agents /sub – contractors (if allowed by LIC) shall facilitate the same. LIC can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by LIC.

b. Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by LIC or in the certification submitted by the Auditors, it is agreed upon by the Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. It is also agreed that the Service Provider shall provide certification of the auditor to LIC regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed. All costs for such audit shall be borne by the service provider/vendor.

c. Service Provider further agrees that whenever required by LIC, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the LIC/ IRDAI and or any regulatory authority required for conducting the audit. LIC reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the Service Provider (e.g., financial, internal control and security reviews) & findings made on the Service Provider in conjunction with the services provided to LIC.

- **Asset Inventory (Indicative)**

Please find below the indicative asset inventory list of LIC:

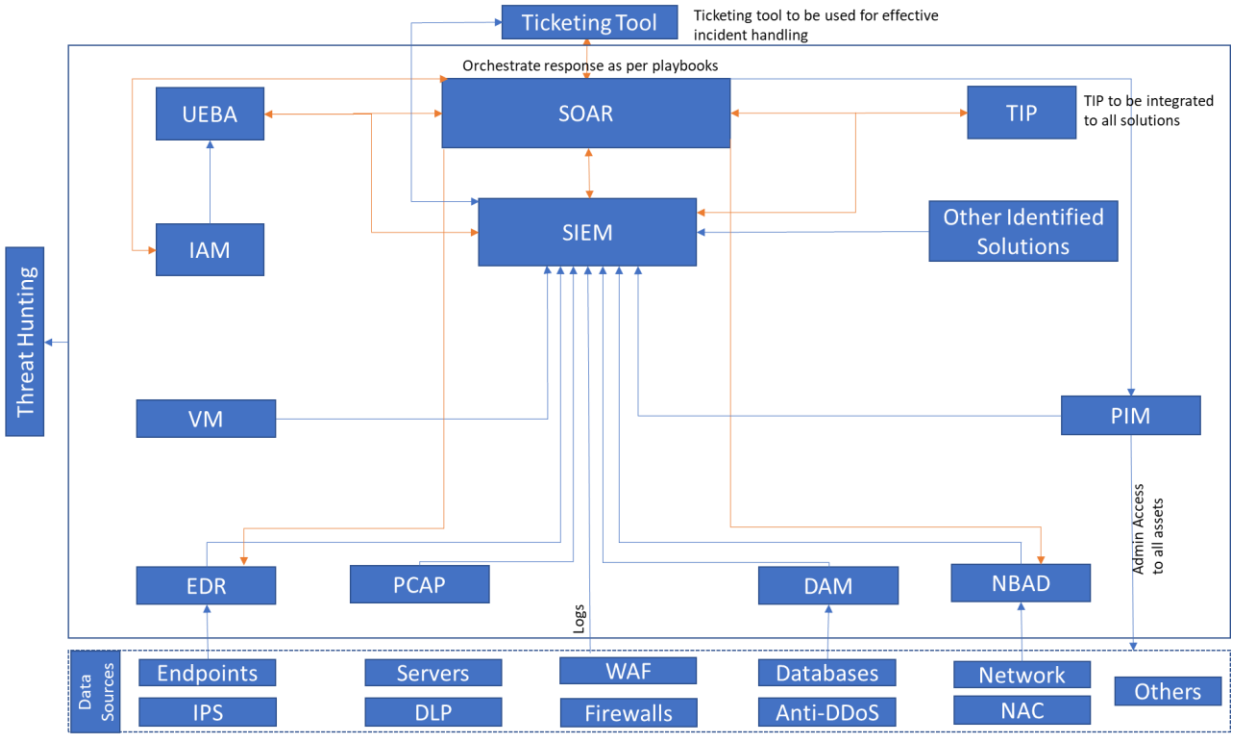
S.No.	Type	Total
1	OS Servers - Linux	6

S.No.	Type	Total
2	OS Servers - Windows	18
3	OS Servers - CentOS	8
4	OS Servers - Juno OS	1
5	OS Servers - Forti OS	2
6	OS Servers - SUSE Linux	58
7	OS Servers - RHEL	119
8	DB Servers - MySQL	69
9	DB Servers - Oracle	21
10	DB Servers - Postgres	22
11	DB Servers - Apex	2
12	DB Servers - phpmyAdmin	8
13	DB Servers - SAP Hana	18
14	Appliance/Network Device	11845
15	Application Inventory	233
16	Asset Inventory	2248
17	Web servers - Apache	14
18	Web servers - JBOSS	70
19	Web servers - Wildfly	3
20	Web servers - Glassfish	3
21	Web servers - PHP	6
22	Web servers - IIS	1
23	Mobile Applications	5
24	Storage Devices - NAS storage server	1
25	Storage Devices - SAN storage server	2
26	Storage Devices - IBM	31
27	Storage Devices - Dell	3
28	Storage Devices - Tape Library	2
29	Switches	115
30	API	722
31	Windows Endpoints	35000
32	Linux Endpoints	45000

The detailed list of devices will be supplied to the finalized bidder.

- **Functional NGSOC Architecture (Indicative)**

  Please find below the indicative functional NGSOC architecture of LIC:



The SI and OEM should be designing the detailed architecture diagram for LIC to ensure the optimal alignment of technological components within the LIC's framework.

- **Documentation**
  a. All the documents shall be supplied in properly bound volumes of A4 size sheets.
  b. Three sets of hardcopies as applicable and one softcopy on USB shall be supplied as final document.
  c. Documents for high level design, detailed design, configuration of individual features set on various appliances, general testing, scenario based fail-over testing, Standard Operating Procedure, best practices etc. shall form the complete set for fulfilling the documentation criteria.
  d. Standard Operating Procedures for all in scope solution , and all processes should be designed by the bidder, reviewed and updated on a half yearly basis and/or on any changes/in compliance to the laws of the land .
  e. Vendor shall also submit Delivery and Installation Report, Warranty certificates, License Copies for all the items supplied along with the supplies.
  f. Installation report should contain the part numbers of all the components supplied by the selected bidders.
  g. Vendor shall ensure to guarantee that the documentation of all the process related to the NGSOC such as (but not limited to) tenant provisioning, implementation, onboarding of data sources, 24/7 monitoring, threat hunting, incident management, threat intelligence, forensic investigation, forensic investigation, severity SLA, incident response plan, regulatory guidelines (CERT-In, RBI, IRDAI, SEBI, etc.) should be documented and submitted as part of the process documentation.
  h. All documentation prepared a part of this RFP needs to be updated annually and/or basis changes in regulatory requirements or any other requirements as per the law of the land .

- **Training & Certification**

Bidder shall train specified LIC employees for operational Management of the system. Training shall be provided on each of the following modules to specified LIC personnel. Training shall be provided at no additional cost to LIC through OEM/OEM certified partners. All trainings have to be imparted at LIC's premises for maximum 25 participants.

a. Pre-Implementation: Provide training to the LIC personnel/ Onsite support team on the product architecture, functionality and the design for each solution under the scope of this RFP.
b. Post Implementation: Provide hands-on training to the LIC personnel/ Onsite support team on day to day operations, alert monitoring, policy configuration, rule creation, report generation for all solutions etc.
c. Documentation and knowledge transfer after each patch/version update.
d. The bidder and OEM/OEM approved Authorized agencies/faculties are required to provide training jointly table for people nominated by the LIC for each solution specified in the scope of work.
e. The bidder and OEM/OEM certified partners are required to provide ad-hoc trainings to the LIC staff as required by LIC, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. LIC has the right to exercise this training option at its discretion.
f. The bidder is required to provide all trainees with detailed training material and 3 additional copies to the LIC for each solution as per the scope of work of the LIC. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
g. All out of pocket expenses related to training shall be borne by the selected bidder.
h. The vendor may utilize the OEM resources in case the bidder does not have adequately experienced resources for providing training.

The detailed training documents should be given to the training participants. The detailed theory & hands-on training should be imparted by the OEM Authorized personnel at LIC premises.
The training facilities shall be made available by LIC, the Bidder will have to ensure that training is imparted in a professional manner through certified and experienced personnel (other than on-site Personnel) and proper courseware is given to every person attending the training.

- **Support Process Requirement:**

a. The vendor shall provide an escalation matrix in consultation with the IT/BPR Department, Central Office, LIC for different categories of support calls.
b. Day-to-day maintenance of the complete solution setups made.
c. All the support Personnel should be dedicated resources to LIC.
d. The support Personnel provided should be conversant with the regular configuration from scratch, integration with other log sources, creation of rules and policies as per LICs requirements, administration tasks, patch management, user management, backup procedures, etc.
e. The on-site support Personnel should be able to troubleshoot the problems raised and should maintain a log of them, also report it to the LIC in detail with root cause analysis and problem resolution.
f. The Bidder should ensure that there will be a proper change & configuration management, backup management, security management as per IRDAI Guidelines. These procedures should be well documented, followed and maintained (copy of the same should be submitted to LIC Central Office – IT dept.)
g. The onsite support Personnel should re-install/ reconfigure any component/ system of the security equipment supplied by the vendor, in case of crash of those components /

system on problem or patch/upgrades. The on-site Support Personnel also needs to support, if any security installations done by a separate vendor.

h. The support Personnel should also keep track of the issues /ticket raised through the ticketing tool/telephone/mail etc. and should provide the remediation for the same.
i. Upgradation of products to the latest version at all the locations, whenever applicable by following a risk-based approach. The procedures have to be documented and submitted to LIC before carrying out any such activity.
j. The vendor has to do necessary implementations required from business continuity perspectives with respect to all the solutions.
k. Root cause analysis of any event has to be done and proper corrective action has to be taken with information to LIC officials. Based on that, the vendor should recommend for improvement to policies, procedures, tools and other aspects.
l. Alert LIC officials for any unusual occurrence/threat/attacks etc. observed.

- The vendor has to comply with the following attributes related to all the in scope solutions:
  m. LIC has a right to review their processes.
  n. SOPs for the processes.
  o. LIC has a right to assess the skill sets of vendor resources.
  p. Advance information about the resources deployed is to be communicated and proper hand-over of charge with complete documentation has to be done for the new resources, which should be approved by LIC.
  q. All necessary steps/changes have to be made in security infrastructure as per the requirements of ISO27001, Certifying Authority/ Body etc. or any third party security audit / inspection report.

Note:

r. No telephone connection will be provided by LIC to the onsite support persons.
s. The on-site L1 and L2 support may also be required to work on Sunday/LIC holidays or beyond office hours on working days, for which an advance notice will be given.

- **Ticketing Tool:**

  - The bidder shall ensure that for all incident management, change management and problem management of IT infrastructure included in RFP is done through ticketing tool which shall be implemented by LIC.
  - The bidder shall integrate all solutions with the ticketing tool of LIC for effective reporting and logging of information security incidents.
  - The bidder shall ensure to track and monitor the closure of information security incidents and escalation of these incidents to appropriate teams/ individuals in LIC if required.
  - The bidder shall ensure that all alerts/offences would be integrated and managed through the LIC's ticketing tool.

- **Security Dashboards:**

As part of deliverables, bidder must provide integrated dashboard along with Display Panel / TV set covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc. The dashboard should be an easy-to-use web user interface with search function, create reports, as well as access cases and applications, with just a few clicks. The bidder should implement an integrated online security dashboard for services provided to LIC. Security dashboard should be implemented onsite in LIC's premises.

a. The dashboard should be secure web based with multi factor authentication enabled online portal available over desktop, Mobile, Tablet and iPad. This should have the automated facility of sending e-mails and SMSs. Dashboard should be available through mobile app if feasible.
b. The dashboard should be provided as integrated view by integrating with the following tools:
    - Risk baseline
    - Asset database
    - Security event/log monitoring tool
    - Incident management process
    - Anti-phishing services Security Analysis, Mitigation and reporting
    - Other security solutions proposed as part of this RFP
    - Other security solutions, Technologies and devices as required by LIC.

c. Dashboard should display asset list and capture details including name, location, owner, branch, IP address, platform details etc.
d. Dashboard should display risk baseline corresponding to multiple categories for IT infrastructure, applications and processes.
e. There should be features to identify unique alerts between a particular period.
f. There should be feature for sending unique alert between a particular period to the identified stake holder official for further necessary action and this should be configurable and customizable.
g. The summary should be available in respect of event generated, event generated, opens, closed, outstanding etc. between two periods.
h. There should have option for reports like but not limited to diskspace utilization, peak memory utilization, etc.
i. The dashboard should display the security status of IT infrastructure assets of LIC. Dashboard should have graphical display of asset security status based on locations, business units, value, platform, owner, branch, etc.
j. Dashboard should capture the status of all applications of LIC. Dashboard should have a graphical display of application security status based on locations, business units, etc.
k. Dashboard should capture risks in each asset. Dashboard should have the provision to click on the asset and track mitigation status corresponding to risks.
l. There should be a graphical representation of risks across business units/locations. Dashboard should support drill down graphs to move to the level of individual assets and should support wide array of analytics and intelligence capabilities.
m. LIC should be able to benchmark and track mitigation for new global threats and vulnerabilities using the dashboard. The applicability of new threats to LIC assets should also be displayed. A drill down of assets affected by new threats, vulnerabilities and status of mitigation should also be supported.
n. SLA data should be captured in the dashboard with compliance details.
o. SLA reports as agreed upon by LIC should be generated on daily/monthly/quarterly frequency. Exclusive dashboard for uptime / down time of IT Assets, No of Log generated / Analyzed/recommendation etc.
p. Dashboard should be available for following:
    • The Dashboard should be context oriented like Security, Business, Control & Risk etc.
    • Top Management (Company View) Department Heads (View to the data associated with their function group / business line)
    • CISO & CIO (complete and detailed dashboard of Security posture of the organization set-up being monitored through this NGSOC)
    • System Administrator (for the systems associated with this administrator).
    • Network / Security Administrator (for devices / equipment for which he is administrator)

• Application Administrator Auditor (Internal Auditors, IT Auditor, ISO Certification Auditor or any other authorized official of the organization)

- **Transition from existing SOC to NGSOC:**

a. Manage day to day operations of currently running SOC setup within two months from the date of issuance of PO while concurrently managing the implementation and enhancement of the new setup. The current SIEM platform is ArcSight.
   - The responsibilities of the vendor with respect to existing operational SOC include but not limited to –
     - Running existing SOC in parallel with NGSOC until all existing log sources are integrated with NGSOC
     - Maintain steady state of SOC ensuring uptime, collation of logs in real-time, correlation.
     - Raise the incidents / alerts in NGSOC or existing SOC
     - Ensure security and other required patches are applied from time to time by obtaining same from respective OEMs.
     - Maintain rules, configuration and other settings and change them as per LIC's requirements / security requirements.

   - Once all the log sources integrated with existing SOC are migrated to NGSOC, ensure the existing SOC is up & running in steady state with security patches by obtaining same from respective OEMs, settings etc. for two years. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs from backup, is required to extract old logs for forensic investigation, in case required.
   - The vendor needs to provide all those services which are being provided by existing vendor as per SLA in force (refer SLA Section).

b. Bidder must ensure that the existing data remain usable for necessary searching, link analytics, hunting, regulatory requirements, forensic investigation etc.

c. LIC has currently deployed SIEM, SOAR and UEBA. Vendor shall plan for the complete transition of the existing LIC's SOC architecture, network, applications, processes etc.

d. Bidder must submit the project plan & transition timelines from current SOC to NGSOC as a part of the RFP response.

- **On-Site Support Services for EDR**
  a. 8x5 real-time monitoring uptime, availability, health performance of EDR devices with mitigation support.
  b. Track and follow-ups with stack-holders for resolution of reported incidents tickets.
  c. Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, updates, upgrades, bug fixes, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
  d. Manage and monitor antivirus and EDR solutions to detect and prevent malware, viruses, and other malicious activities on endpoints
  e. Deploy antivirus and EDR agents, manage updates and patches, and monitor antivirus and
  f. EDR events to identify potential security incidents

g. Ensure the antivirus and EDR solutions are configured correctly, up-to-date with the latest threat intelligence, and are functioning correctly
h. Ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration and reporting issues.
i. Ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management
j. Perform periodic review and fine tuning of these devices to fit organization network environment and requirement, subsequence management, monitoring and support (8x5)
k. The change management of all the devices must be adhering to standards and policies of LIC.
l. Create, update, and delete access control rules, groups, and policies in EDR after obtaining approval.
m. Quarterly review of rules, policies etc. of security devices and recommend optimization of the same.
n. In case of any hardware/virtualized malfunctioning, patch management, firmware Upgradation and other OEM related tasks of the device, the vendor must coordinate with stakeholders for faster resolution.
o. Monitor and report the hardware and software related SLA's of EDR.
p. SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned.
q. Quarterly review of capacity planning of security devices. Details of underutilized and over utilized security devices.
r. Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis
s. Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
t. Provide LIC with a root cause analysis in case of any faults, security events including preventive measures being taken to prevent future similar incidents outages
u. Coordinate delivery with all stake holders including help desks, network team, IT team, application team and all appropriate third parties, as necessary
v. Maintain security product configuration, based on industry best practices, and as requested
w. Participate in technical and business planning sessions to establish security standards where the security products may impact the network
x. Provide infrastructure security planning & analysis, recommendations for installation and upgrade
y. Tracking/Alerting the required license, software subscription for all hardware & virtual components of devices in scope
z. Set up and manage admin and user accounts. Perform access control on need basis
aa. Quarantine the devices if in case the device reported any critical incident or malware.
bb. Conduct Recovery exercise of above backup on quarterly basis or as per the LIC guidelines. Submit the Periodic Reports on the backup status. (As per compliance to IRDAI cybersecurity guidelines/audits NC CA, VA PT non-compliance DR Drills needs to be done as per LIC standard)
cc. Provide relevant support for external and internal security audits that LIC is subject to from time to time
dd. Support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time
ee. Responsible for reinstallation of the EDR agents whenever there is a change in the infrastructure or operating systems
ff. EDR analysis shall be performed by the SOC team
gg. On call availability of the SMEs over weekends

2. Detailed Scope of Work

A. General Requirements

i. The specifications given are minimum. Bidders can quote equivalent or higher technical specifications to meet the requirements of LIC. The RFP and annexures together constitute the overall requirements of the solution.

ii. The bidder / System Integrator shall engage the services of respective OEMs/ OEM Certified partner for plan, design and implementation of the solution. The OEM(s)/ OEM Certified Partner must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.

iii. The bidder is responsible for integrating all assets within the LIC environment and this responsibility shall rest exclusively with the bidder. The bidder shall ensure that the OEM(s)/ OEM Certified Partner has end to end responsibility for plan, design, implementation, maintenance and adoption of the total solution leveraging the behaviour modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.

iv. The bidder shall ensure that the configuration, implementation and testing of the solution components to be carried out by resources from the OEM/ OEM Certified Partner as decided by LIC at the time of implementation.

v. The bidder shall also engage the services of the respective OEMs for post implementation audit, validation and certification by the OEM that the solution has been implemented as per the plan & design provided by them. In case any deficiencies are pointed out during the OEM audit the same has to be remedied by the bidder without any extra cost to LIC.

vi. The bidder is responsible for the AMC, licenses, uptime, availability and management of the devices/solutions implemented and managed as part of the NGSOC.

vii. All the licenses provided as part of BoQ should strictly adhere to requirements of the RFP. If during the contract period, it is observed by LIC that provided licenses are not adhering to the RFP requirements then all the additional hardware/software/licenses should be provided and configured without any additional cost to LIC.

viii. The bidder shall Supply, Design, Install, Implement, Integrate, Support & Maintain all the in scope solutions within this RFP.

ix. The bidder should consider the detailed technical specifications as stated in the Annexure F while proposing for the solution, which forms a part of the scope of work . Bidder needs to provide complete end to end solution including applicable appliances, software, necessary accessories, active and any components for efficient functioning of the proposed solution.

x. The bidder should provide backup solution for proposed setup. The backup taken should be SHA-256 encrypted. This backup refers to the configuration backup for the solutions provided by the bidder and is different from the log retention policy. The backup should be taken daily. The backup should be stored in the server in DC, with an additional copy in the NAS server and a replicated copy to be saved at the DR. Any configuration at DC should be replicated to DR on a real time basis. Additionally, it is essential that backups for the past 30 days remain accessible on a daily basis.

xi. Bidder has to quote for highest/ premium support available from the OEM along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features, etc. for all the OEMs.

xii. The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period.

xiii. The bidder shall build a baseline of each data source, what events are required for compliance, threat detection, monitoring, threat hunting, etc. and help to get the relevant logging enabled from data source.

xiv. The bidder shall make sure that the data or logs which are not required for security monitoring, threat detection, threat hunting, compliance, etc. create filtering policies at the data collection layer and make sure it is not counted for license to use the platform optimally and effectively.

xv. The bidder needs to make sure that the solution deployed in DR has real time replication of data of DC. DR should be used for reporting, threat hunting, searching, etc.

xvi. The bidder and OEM/OEM certified partner's services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:

- Solution architecture, sizing, policy configuration, High availability, BCP/ DR scenarios, etc.
- Integration of each solution with other NGSOC solutions and other Network and Security solutions currently deployed in the environment as decided by the LIC.
- Testing strategy and test cases for Acceptance Testing of the solution.
- Identifying gaps, crown jewels of LIC, custom parser creation, creation of rules, use case development, finetuning, etc.

xvii. The bidder and OEM/ OEM certified partner's services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.

xviii. All the solutions should be seamlessly integrated with the LIC's NTP solution and must be compatible with any provided NTP version.

xix. The Bidder needs to architect solution to collect logs from across LIC environment and over private cloud.

xx. Each solution should have the log storage capability as defined in the technical specification and to retrieve them within 48 hours from the time of request.

xxi. In case there is a cost incurred to LIC due the wrong BoM/Specification/feature-set of security equipment/device/appliance at any location, the same will have to be replaced by vendor at no extra cost to LIC.

xxii. Prepare test-plan, implementation plan, integration plans and rollback strategies.

xxiii. The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and once in end of every year during the contract period. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. The recommendations/ remediation changes required after each audit should be completed within 3 months. The audit needs to be done only by the employees in the payroll of the OEM (necessary evidence needs to be submitted).

xxiv. The vendor is required to plan and execute red team and purple team exercises at end of every six months. The red team activities should be performed only from external parties/ vendors/ resources and should not be related with blue team and purple team. Bidder shall provide and implement patches/ upgrades/ updates for hardware/software/ operating system / middleware, etc. as and when released by service provider/ OEM or as per requirements of LIC. Bidder should bring to notice of LIC all releases/ version changes.

xxv. The successful bidder needs to install all the associated equipment needed to complete the job as per the technical specification described in this tender.

xxvi. The successful bidder shall co-ordinate and co-operate with the other vendors appointed by the LIC so that the work shall proceed smoothly without any delay and to the satisfaction of LIC.

xxvii. No extra claim shall be entertained on account of all/part of any job redone on account of bidder's negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be

provided by the successful bidder. All such cost shall be borne by the bidder.

xxviii. The vendor has to provide complete escalation matrix which should be updated and sent to LIC as and when there is a change.

xxix. Bidder has to architect the solution deployment after understanding the following details:

- Understanding the environment in terms of application, network, server and Security appliances, LAN, WAN & Internet Links and segments, privileged users etc. to ensure creation of use cases related to targeted attacks and early breach detection.
- Prepare the designs and implement the solution in line with IRDAI's guidelines on Information and cyber security for Insurers, ISO27001:2013/ISO22301/IT Act 2001/CERT-In (along with its amendments) standards as modified from time to time. Study of LIC's existing security and application environment and guidelines and recommend best practices to implement and roll out the same. To suggest plan for network integration of various devices/appliances etc. with the proposed solutions.
- Bidder needs to prepare a detailed execution plan. The complete documented plan must be submitted to LIC with supported designs and drawings (if any) within 5 weeks of placing the order. The actual execution will start only after approval of plan by LIC officials.
- The Detailed Design Document shall include the following aspects:
  i. Technical objectives and requirement fulfilment.
  ii. High-level and low-level solution design requirements.
  iii. Design recommendations.
  iv. Proposed network, Security topology and Architecture.
  v. Network - Logical and Physical topology.
  vi. Security design.
  vii. Sample configuration templates for hardware devices and other devices for which configurations need to be made.
  viii. Hardware and Software release recommendations based on features and/or functionality.
  ix. The Design Document shall also document the management of DR scenarios and DR Drills of the solution.
  x. Use cases for each of NGSOC solutions.
  xi. End-user manuals and SOPs, wherever applicable.

- The plan shall include information related to required downtime, changes to existing architecture, log level parameters, deployment schedule etc.
- The installation of the appliances shall be done as a planned activity on a date & time of approved deployment schedule within office hours or with the mutual agreement from LIC.
- The bidder has to ensure that both High-Level Design (HLD) and Low-Level Design (LLD) are OEM certified. This has to be implemented by the successful bidder. The implementation may be tracked using a standard IT Project Management Template like Gantt chart or timeline chart.

B. Next-Generation Security Operations Center (NGSOC)

i. The scope of work of NGSOC service would encompass technical specifications as well.

ii. The vendor should deliver continuous security management and monitoring services 24x7x365.

iii. The vendor holds responsibility for configuration, integration and interfacing in scope solutions with all devices and components under scope.

iv. The vendor should have advance security monitoring services to detect threats that are not

addressed by traditional defense in depth measure and monitoring solution.

v. The vendor and OEM should develop out of the box use cases to identify and detect security incidents.

vi. The vendor should design security monitoring standard operating procedures that are required to be followed for LIC.

vii. The vendor should ensure 24x7x365 service availability for monitoring of the devices / servers /applications under scope and support for troubleshooting.

viii. The vendor should be Cyber-Ready to identify, respond to and recover from attacks swiftly.

ix. The vendor should offer complete analysis and correlation of logs from all the devices/solutions under scope.

x. The vendor should ensure the remediation time as per defined SLA.

xi. The vendor should analyze events and alerts according to the established escalation matrix.

xii. The vendor should ensure real-time alerts for priority tickets via email and calls.

xiii. The vendor should offer fine-tuning of use-cases periodically.

xiv. The vendor should automate security processes to reduce resource drain and threat response times.

xv. The vendor should conduct workshop with different departments of LIC to develop process manual, identification of crucial assets, the establishment of use cases, etc. at regular intervals.

xvi. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.

xvii. The OEM should perform audits once after the implementation and once in every year and report the overall efficiency of the NGSOC. The remediations after the audit should be given. Additionally, should present an efficiency improvement plan to ensure continuous progress in detection.

xviii. The vendor should provide a per incident report for critical incidents to the LIC Information Security Steering Committee that includes evidence, observations, remediations and resolution actions. The incident report should be shared with customer committee within 6 hours post noticing and within 24 hours post closure of the incident.

xix. The vendor should ensure that the solutions should support an integrated MITRE ATT&CK Framework and provide an interface to visualize the various correlation rules. The solutions must report coverage of detection across the MITRE ATT&CK framework. Vendor should provide complete lifecycle of attack in an integrated view to enable LIC to take quick and corrective action.

xx. Reporting:

All the reports should be provided with actionable insights. The bidder should also conduct necessary workshop to identify and create necessary reports as per the requirements of LIC. All reports shall be generated from the common data lake. Following is the indicative list of reports, the bidder shall provide to LIC:

- Daily reports:
  - Top attacker, attacks and attack targets, trends report
  - Top firewall ports access report (inbound/outbound)
  - Top signature triggered
  - Top account brute forced
  - Top systems infected
  - Top virus infection in the network
  - Performance report for all solutions in scope
- Weekly reports:
  - Weekly security incidents status report
  - Daily device utilization report
  - Device availability report
  - Device: Incident, service request and change status report
  - Weekly threat advisory and vulnerability report

- Top signature triggered
- Top account brute forced
- Top systems infected
- Top virus infection in the network

- Monthly reports:
  - Executive summary report for all the services
  - Monthly Security incident status report
  - Monthly security incident trend analysis
  - Monthly device availability report
- Quarterly reports:
  - Quarterly Security incident status report
  - Quarterly security incident trend analysis
  - Quarterly cyber security activities report
- Ad-hoc and audit related reports at any frequency desired by LIC

C. Security Information and Event Management (SIEM)

i. The scope of work of SIEM solution would encompass technical specifications as well.
ii. The vendor should integrate, and review logs collected from LIC's infrastructure for log analysis, identification of issues, and to ensure that they meet the desired criteria or standards.
iii. The vendor should perform manual/automatic analysis using pre-configured use cases and based on observed deviations from normal behavior to uncover activities that could undermine security of information assets.
iv. The vendor should review and confirm security alerts through detailed investigation of logs and additional information obtained from the monitored assets. The vendor should assess and prioritize alerts for communication and action.
v. The vendor should notify the identified LIC's representative based on the severity of the security alert and nature of services impacted. The notification channel includes (but not limited to) ITSM, voice and email.
vi. The provision for creation of custom parsers (300 nos.) will be carried out by the OEM and they should transfer the logic of making it to the successful bidder. The unit price of the custom parsers will be derived from the commercial sheets on a pro-rata basis and this rate will be frozen for 5 years. However, the payment for custom parsers will be based on the actual parsers deployed by LIC. LIC also reserves the right to increase the requirement of custom parsers as per the actual requirement.
vii. The vendor should provide alert details and outline preliminary alert response activities that can help contain the impact of the threat including logs that needs to protected and additional investigation that may be subsequently required.
viii. Pending alerts, incident & root cause analysis should be taken-up after transition phase. Existing vendor to close older alerts before handover.
ix. The vendor should provide software-level management for the SIEM components.
x. The vendor should manage user access, including updates to user and group permissions.
xi. The vendor should review application performance, capacity, and providing recommendations when necessary.
xii. The vendor should review SIEM disk space usage.
xiii. The vendor should verify log collection.
xiv. The vendor should regularly backup logs as per defined backup and archival frequency as per technical specification. The vendor should restore logs as required or for the purpose of testing.
xv. The vendor should ensure the integration of devices with SIEM including but not limited to network devices logs, server logs, system logs, application logs, etc. for existing as well as

future technologies which LIC might procure.

xvi. The vendor should create custom parsers for log sources as necessary, in accordance with LIC's requirements.

xvii. The vendor should configure extra Device Support Modules (DSMs) when required.

xviii. The vendor should have out of the box capability to create and customize dashboards.

xix. The vendor should correlate low-priority alerts with subsequent alerts to identify multi-vector attacks or Advanced Persistent Threats (APTs).

xx. The vendor should provide a centralized portal/dashboard for capturing LIC's risk posture and maturity levels at any given time.

xxi. The vendor should ensure asset discovery and maintenance of integrated asset inventory and precise EPS/GB per day calculation.

xxii. The vendor should maintain the ability, ideally automated, to continuously detect and discover new assets and connections within the LIC ecosystem.

xxiii. The vendor should ensure that the data is encrypted both in transit and at rest to maintain data privacy.

xxiv. The vendor should conduct root cause analysis (RCA) and provide RCA reports for security incidents as outlined by LIC's requirements. The Root Cause Analysis (RCA) timelines are defined as follows: P1 within 4 hours, P2 within 8 hours, P3 within 24 hours, and P4 within 48 hours.

xxv. The vendor should implement additional add-on modules from the OEM as needed.

xxvi. The vendor should recommend new security configurations based on the global best practices.

xxvii. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.

xxviii. Deploying and finetuning of SIEM solution and its components:

- Log integration to the new setup after reviewing the same in consultation with LIC.
- Design and document the priority use cases, policies and rules to be configured on the SIEM solution in consultation with LIC.
- Creating and applying default policies after analyzing traffic pattern for correlation purpose.
- Modifying and fine-tuning the default policies for correlation controls in line with LICs security policy, IRDA guidelines, ISO 27001 / ISO 22301/IT Act 2000 (including all amendments), details provided in the technical specifications and best practices which will be jointly decided by the representatives from LIC and the Project Manager / Engineer from the bidder.
- Optimize Alerts, Normalize, and Aggregate; apply Correlation Rules based on Priority of Alerts.
- The provision for creation of customize parser will be carried out by OEM and they should transfer the logic of making it with delivery team.
- Setting up basic system health monitoring and log analysis through Management and Reporting appliance.
- Vendor has to do end-to-end configuration of the solution and implementation and customization as per best practices and LIC's requirements. The vendor will ensure seamless integration of its appliances for functioning of existing as well as future gateway security appliances with no/minimum possible downtime.

xxix. Configuration of Management, Logging and Reporting Server/Appliance/Components would involve following tasks:

- Configuring device management and reporting functionality in consultation with LIC.
- Enable capturing of logs, log retention period and mechanism for archiving logs.
- Review of rules/policies every six months to identify the unwanted and overlapping rules.
- Creating Out-of-the-box reports and customized reports templates based on the needs of LIC. The reports should be available for the following (but not limited to): a).

Indian Information Technology Act 2000 including all amendments b). IRDA guidelines c). Payment Card Industry (PCI) d). ISO27001 e). SO22301 f) COBIT g) CERT-In etc.

- Scheduling of backup for device used for management purpose.
- Checking up of restoration of management hardware from backup.
- Bidder has to provide an integrated case management workflow in the SIEM as well as integrate with the service desk solution for incident management workflow and create process as per best practices in consultation with LIC.
- Configure incident based alert mechanism supported by appliance such as (but not limited to) Visual Alerts, e-mail and SMS.

D. Security Orchestration, Automation and Response (SOAR)

i. The scope of work of SOAR would encompass technical specifications as well.
ii. The solution must enable the orchestration and automation of security workflows, eliminating manual intervention to reduce mundane tasks.
iii. The vendor should leverage the automated playbooks as per the technical specification and create customized automated playbooks tailored for LIC's processes.
iv. Playbooks should objectively enable security teams to meet the dynamic security landscape of LIC.
v. The vendor should ensure seamless integration with other in scope security tools and systems for effective automated response.
vi. The vendor should allow the prioritization of incidents based on predefined criteria and threat severity.
vii. The vendor/ SOC team should track metrics, measure the effectiveness of automated processes, and generate reports.
viii. The bidder should guarantee that the solution allows for the inclusion of manual changes within automated workflows within 4 hours.
ix. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.

E. User and Entity Behavior Analytics (UEBA)

i. The scope of work of UEBA solution will encompass technical specifications as well.
ii. UEBA should leverage data from SIEM and should not create its own repository. The bidder must ensure the integration with other tools and workflows to enhance investigation and response.
iii. The bidder must be able to finetune behavioral analysis of user and entity activities to identify deviations from normal patterns.
iv. The bidder must ensure the integration of the solution from multiple sources (but not limited to), including logs, applications, endpoints, and network traffic.
v. The bidder should ensure the ability to create custom behavioral rules based on the LIC's unique environment and requirements.
vi. The bidder should prioritize alerts based on the level of risk to aid efficient incident response in consultation with LIC.
vii. The bidder should utilize a solution that will AI, machine learning, behavioral analysis, and security analytics to effectively detect known as well as unknown threats.
viii. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.

F. Threat Intelligence (TI)

i. The scope of work of TI solution would encompass technical specifications as well.
ii. The vendor should gather information from various sources, including open-source intelligence (OSINT), commercial threat feeds, internal logs, honeypot, government organization and reports from industry-specific organizations, enabling the identification of emerging global threats.
iii. The vendor should consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies.
iv. The vendor has to ensure that the threat intelligence collected via multiple feeds needs to be validated for active threats, eliminating false positives, eliminating redundant data, reducing false positive and providing contextual insights applicable to LIC/BFSI sector. Data curation should be automated and done by the TIP only.
v. The vendor should create, and update use cases based on MITRE ATT&CK framework.
vi. The vendor should identify patterns and trends in threat data to understand the evolving tactics, techniques, and procedures (TTPs) used by threat actors.
vii. The vendor should proactively inform about potential security threats and vulnerabilities, new global security threats or zero-day attacks in circulation and recommend implementing appropriate countermeasures to safeguard LIC assets and data against such evolving threats or attacks along with the analysis.
viii. The vendor should ensure classifications of threats and attacks.
ix. The vendor should customize rules based on Threat Intel feeds, as applicable to LIC's requirement.
x. The vendor should produce regular reports and alerts for stakeholders, including senior management and incident response teams, to keep them informed about potential threats
xi. The vendor should integrate threat intelligence feeds and indicators into security tools and systems, such as (but not limited to) SIEM, UEBA, NBAD, etc., to automate threat detection and response.

G. Threat Hunting (TH)

i. The scope of work of TH service would encompass technical specifications as well.
ii. The vendor should ensure proactive threat hunting on continuous basis.
iii. The vendor must ensure to have the automated playbooks for threat hunting. The vendor should deliver proactive threat hunting services across networks, endpoints, and unusual user behavior. This aids in identifying advanced attacks such as (but not limited to) lateral movement, malware beaconing, data exfiltration, watering hole attacks, process anomalies, service anomalies, and account takeovers.
iv. The vendor should initiate proactive searches for signs of malicious activity within LIC's network that may not be detected by automated security measures.
v. The vendor should possess the ability to conduct advanced threat detection and threat hunting using artificial intelligence and machine learning models.
vi. The vendor should formulate hypotheses about potential threats based on knowledge of current threat landscapes, vulnerabilities, and industry-specific risks.
vii. The vendor should conduct in-depth, manual investigations into network and system logs, looking for anomalies, unusual behavior, or indicators of compromise (IOCs).
viii. The vendor should ensure fine-tuning processes necessary to improve security posture and to streamline cyber security process.
ix. The vendor should ensure that malware scanning, protection, presentation, and reporting are implemented according to LIC's specific requirements.
x. The vendor should provide recommendations for mitigating threats and vulnerabilities based on findings, often working closely with incident response teams.
xi. The vendor should thoroughly document all findings, actions taken, and lessons learned during the threat hunting process to improve future efforts and maintain a historical record.

xii. The vendor should continuously refine and adapt threat hunting techniques and processes based on lessons learned and emerging threats.

H. Packet Capture (PCAP)

i. The scope of work of PCAP solution would encompass technical specifications as well.
ii. The vendor should design PCAP Solution considering the traffic throughput at each Internet facing and MPLS Colo site as described in the PCAP Technical Specifications and Sizing Information. The PCAP Solution components should capture packets at line rate at each site and store the packet level data on the packet capture appliance at each site. Accordingly, the vendor should provide packet capture appliance at each site with at least four interfaces of type 10G Fiber MM LC.
iii. The bidder needs to conduct a workshop with LIC for providing the best of the PCAP solution engineering. Bidder should directly engage OEM Professional Services for Solution Design and Implementation.
iv. The PCAP solution should support continuous, always-on capture and store packets and support extraction and replay of packets as an when required by LIC.
v. The vendor should define capture rules for specific traffic types as per LIC's requirement.
vi. The vendor should ensure the smooth deployment and configuration on network segments. The vendor should confirm high-speed data processing and adaptable scalability of the solution. The Packet Capture Solution should support horizontal scaling architecture considering future growth at each site.
vii. The PCAP Solution should provide packet like data for security investigation and forensics supporting key requirements like Host Analysis, Session Analysis, Session Reconstruction, Packet Analysis, etc.
viii. The vendor should ensure interoperability and data sharing.
ix. The vendor must provide maintenance, updates, and training resources as needed.
x. The vendor must address secure storage options and should have data storage duration and capacity to ensure that packet captured at line rate by sensors at each site shall be stored for 7 days and metadata to be stored for 1 year.
xi. The vendor must ensure the capability to capture packets at specific points in the network with configurable granularity. To ensure packets are captured at all the key vantage points from security perspective, the vendor must provide Network Packet Broker at each site that is populated with at least 16 ports of 1G/10G with a non-blocking throughput of at least 480G.
xii. To ensure data privacy of captured packet data, the Packet Capture solution should not store sensitive and confidential information or shall have capability to mask all such information.
xiii. The Solution should support for any speed, protocol, physical, virtual, and cloud network environment provides continuous and comprehensive packet-level network visibility.
xiv. The Solution should have capability to convert raw packets into a rich source of layer 2 -7 metadata to be used for more advanced Network Detection and Response.
xv. The Solution should intelligently index, compress and locally store metadata and packets to be used for real-time and longer-term back-in-time investigations before, during, or after an attack occurred.
xvi. The Solution should have features to perform deep-dive, protocol-level analysis and forensic evidence collection using real-time data captures and historical data mining, or by saving trace files for future decode analysis.
xvii. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.

I. Network Behavior Anomaly Detection (NBAD)

i. The scope of work of NBAD solution would encompass technical specifications as well.

ii. The vendor should be responsible for network, user and events behavior monitoring and analytics services as part of overall SOC operations.
iii. The vendor should calculate precise flows per second or traffic throughput (bps) to determine the level of network traffic.
iv. The vendor must analyze network traffic for unusual patterns, traffic spikes, and anomalies.
v. The vendor has to implement use cases in consultation with LIC, after conducting appropriate workshops along with the OEM/OEM certified partner.
vi. The vendor should observe the network traffic and create a baselining of the network and provide the baselining report to LIC.
vii. The vendor should ensure the ability to establish a baseline of normal network behavior and detect deviations.
viii. The vendor should ensure to provide real-time alerts for anomalies that could indicate potential threats.
ix. The vendor should ensure the compatibility with other security systems, such as (but not limited to) SIEM, incident response tools, etc.
x. The vendor should ensure to correlate network anomalies with potential threats, aiding in early threat detection.
xi. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.

J. Endpoint Detection and Response (EDR)

i. The vendor should assess the existing endpoint security infrastructure and identify any gaps or vulnerabilities.
ii. The vendor should deploy EDR agents on endpoints, servers, and critical systems within the organization's network.
iii. The vendor should configure EDR agents to collect and analyze security events and activities on endpoints.
iv. The solution should monitor endpoints for suspicious activities, such as malware infections, unauthorized access attempts, and unusual user behavior.
v. The solution should use behavioral analysis and machine learning to detect advanced threats and zero-day attacks.
vi. The solution should generate real-time alerts for potential security incidents and provide guidance for incident response and remediation.
vii. The vendor should enable endpoint forensics capabilities to investigate security incidents and identify the root cause of attacks.
viii. The solution should capture and store detailed endpoint activity logs and artifacts for further analysis.
ix. The vendor should integrate the tool with vulnerability management systems to assess the endpoint's security posture.
x. The EDR solution should be able to rollout patches or upgrades from the EDR management console for agents onboarded on the platforms.
xi. The solution should alert and remediate endpoints with outdated or vulnerable software configurations.
xii. The solution should provide real-time alerts for anomalies that could indicate potential threats.
xiii. The vendor should ensure the compatibility with other security systems, such as (but not limited to) SIEM, incident response tools, etc.
xiv. The solution should correlate network anomalies with potential threats, aiding in early threat detection.
xv. The vendor is expected to deliver reports at periodic intervals as per LIC's requirements.
xvi. The vendor should re-deploy the agent as and when there is a change in the infrastructure or

the operating systems.

xvii. The scope of work of EDR would encompass technical specifications as provided in Annexure F.

xviii. Bidder to ensure the proposed EDR solution is capable of coexisting with the currently implemented Antivirus solution in LIC until its end of validity. Presently LIC is having Antivirus solution i.e., EPP solution Trend Micro Apex One for 30000 Windows and Trend Micro Deep security for 65000 Linux. and Trend Micro Server Security for Servers -500 licenses valid till 25th Dec 2025 and Trend Micro Server Security-1433 licenses for Servers-valid till June 2026.

3. Sizing Requirements

SN	Solution	Proposed Sizing
1	Security Operations Centre	24/7/365 days
2	Security incident and event management	80000 EPS / 3862 GB Per Day
3	SOAR (Security Orchestration, Automation and response)	12 user licenses
4	User and Entity Behavior Analysis	License for 1 lakh users & entities
5	Packet Capture	30 Gbps or its equivalent Packets per Second
6	Network Behavior Anomaly Detection	30 Gbps or its equivalent Flows Per Second or Packets per Second
7	Cyber Threat Intelligence	6 authorized user licenses 300 External Facing Applications
8	Cyber Threat Hunting	As a resource-based service (refer Section E 5: Resource Deployment)
9	Endpoint Detection and Response	30000 Windows OS desktops /laptops and 45000 RHEL OS desktops 4000 Servers

4. RACI Matrix

SN	Service	Activity	SI	OEM/ OEM Certified Partner	LIC
1	Solution Operations and Management	Plan, Design, Implementation	R,A	R,A	C,I
		Service Request Handling	R,A	C	C,I
		Problem Management- Root Cause Analysis	R,A	R,A	C,I
		Configuration Change Plan	R,A	C	C,I
		Software Implementation	R	A	C,I
		Software Security Vulnerability Assessment	R	A	C,I
		Capacity Audit and Benchmarking	A	R	C,I
		Performance Audit	R,A	R	C,I
		Inventory Management	R,A	C	C,I
		License Management	R,A	C	C,I
		SLA Performance	R,A	I	C,I
		SLA Reporting	R,A	I	C,I
		Service Delivery Review and Governance	R,A	R,A	C,I
		Business Continuity Management	R,A	I	C,I
2	Security Monitoring	Security Monitoring	R,A	C	C,I
		Incident severity assignment	R,A	C	C,I
		Alert Analysis	R,A	C	C,I
		Incident Notification	R,A	C	C,I
		Incident Escalation	R,A	C	C,I
		Daily Reporting	R,A	C	C,I
		Monthly Reporting	R,A	C	C,I
		Metrics and SLA Reporting	R,A	I	C,I
3	SIEM	SIEM Platform Administration	R,A	I	C,I
		Use Case Content Creation/Review/Modification	R,A	C,I	C,I
		Log Source Integration	R,A	C	C,I
		Custom Parser	R,A	C,I	C,I
		Use Case Definition	R,A	C	C,I
		Correlation Rule Creation	R,A	C	C,I
		Dashboard Development	R,A	I	C,I
		Performance Optimization	R,A	I	C,I
4	Incident Analysis & Response	Incident Detection	R,A	I	C,I
		Incident investigation	R,A	I	C,I
		Incident remediation	R,A	C,I	C,I
		Knowledge Management	R,A	I	C,I
5	Impact analysis on incidents	Triaging	R,A	I	C,I
		Enrichment of the incidents	R,A	I	C,I
		Assess impact of incidents	R,A	I	C,I
		Threat modelling	R,A	C,I	C,I

		Validate CIA to assets in SIEM	R,A	I	C,I
6	Threat Intelligence	Threat Research and Reporting	R,A	I	C,I
		IOC / Threat Feed Management and Integration	R,A	A,I	C,I
		Threat Briefings	R,A	I	C,I
7	Threat Hunting	Periodic Threat Hunting Scenarios	R,A	C,I	C,I
		Threat Remediation	R,A	C	R,I
		Threat Hunting Reporting	R,A	C,I	C,I
8	User and Entity Behavior Analysis	Profiling	R,A	C,I	C,I
		Report Incidents	R,A	C,I	C,I
		Rules and policy creation	R,A	C,I	C,I
		Incident Analysis	R,A	C,I	C,I
		UEBA Platform administration	R,A	I	C,I
9	Automation on SOAR	Integration with other solutions	R,A	A,C,I	C,I
		Playbook development	R,A	C	C,I
		Automation Configuration	R,A	C,I	C,I
		SOAR Platform administration	R,A	C,I	C,I
10	NBAD	Monitoring and Alerting	R,A	C	C,I
		Anomaly and Threat Detection	R,A	C	C,I
		Dashboard and Reporting	R,A	C	C,I
		Incident Analysis	R,A	C	C,I
		NBAD Platform administration	R,A	C,I	C,I
11	PCAP	Packet Capturing Setup	R,A	C	C,I
		Data Filtering	R,A	C	C,I
		Data Storage	R,A	C	C,I
		Data Analysis	R	A	C,I
		PCAP Platform administration	R,A	C,I	C,I
12	EDR	Implement	R,A	C	C, I
		Configure/ UAT	R,A	C	C, I
		Monitor and upkeeping	R,A	C	C, I
		Investigate and Respond to Incidents/ Remediation	R,A	C	C, I
		Report Incidents and update SOPs	R,A	C	C, I
		Review and Update EDR configuration and Policies	R,A	C	C, I

5. Resource Deployment

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
1	SOC Manager	• Troubleshooting technical issues to ensure project success. • End-end integration of all soc solutions health check as per the sign-off • Implementing changes to align with LIC's demands and specifications. • Providing guidance, direction, and instructions to the team to achieve specific objectives. • Developing and executing a timeline for the team to achieve its goals. • Monitoring incident detection and closure. • Presenting regular metrics and reports. • Identifying new alert requirements. • Ensuring services meet SLA parameters. • Conducting periodic DR drills. • Following up with departments to close various reports/incidents and escalating long outstanding issues. • Designing SIEM solutions to enhance security value, service management, and scalability. • Identify, resolve, and conduct root-cause analysis for security incidents which is essential for maintaining a proactive	L3	1	General Shift (8x5)	10 Years	CISSP/CISM

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		and responsive security posture. • Develop and document incident response procedures. • Ensuring the SIEM system is optimized for efficient performance is vital. This includes handling data volume effectively and maintaining responsiveness for timely threat detection and response. • Align reports SIEM rules and alerts with security policies and compliance reports requirements ensures that the system contributes to overall security and regulatory adherence. • Developing customized and dashboards provides meaningful insights into the LIC's security posture, aiding in decision-making and monitoring. • Integration with other solutions/devices (including security solutions) to enhance overall security monitoring and incident response capabilities, creating a more comprehensive security infrastructure. • Collaborate with SIEM solution vendors for updates, patches, and support to ensure the system's reliability and effectiveness.					

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
2	SOC Analyst	• Configure and maintain the SIEM system, ensuring that it's properly set up to collect and analyze security event data. • Develop, customize, and manage security rules within the SIEM to detect and respond to security threats. • Monitor SIEM alerts, investigate them, and take appropriate actions based on the severity and nature of the alerts. • Oversee the collection, normalization, and storage of log data from various sources. • Develop and document incident response procedures, and lead or assist in incident response efforts when security incidents occur. • Analyze and investigate security events from various sources. • Manage security incidents through all incident response phases to closure. • Utilize SIEM, SOAR, UEBA, EDR, NBAD, PCAP, Vulnerability Scanning, and Malware analysis technologies for event detection and analysis. • Update tickets, write incident reports, and document actions to reduce false positives. • Develop knowledge of attack types and fine-tune detective capabilities. • Identify log sources and examine system logs to	L2	6	2 Resources in each shift	4 Years	CEH
			L1	9	3 Resources in each shift	2 Years	CEH

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		reconstruct event histories using forensic techniques. • Align SIEM rules and alerts with the LIC's security policies and compliance requirements. • Conduct computer forensic investigations, including examining running processes, identifying network connections, and disk imaging. • Maintain and support the operational integrity of SOC toolsets. • Collaborate with SIEM solution vendors for updates, patches, and support to ensure the system's reliability and effectiveness. • Maintain thorough documentation of the SIEM system's configuration, procedures, and incident response plans. • Proactively identify and report system security loopholes, infringements, and vulnerabilities to the Security Operations Centre Manager in a timely manner. • Work closely with other IT and security teams during incident response, coordinating efforts and sharing information to mitigate security incidents effectively. • Ensure that the SIEM system helps the LIC meet regulatory compliance					

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		requirements and is ready for security audits. • Continuously optimize the SIEM system for efficient performance, ensuring it can handle the volume of data and remain responsive. • Develop automation scripts and workflows to streamline common security response tasks and enhance efficiency.					
3	Dashboard Experts	• Design visually appealing and intuitive dashboards that display key security metrics, incidents, and trends, using data visualization tools and scripting languages for automation. • Develop and maintain customized reports that provide meaningful insights into security data, ensuring they are accurate, comprehensive, and suitable for management and regulatory purposes. • Collect, aggregate, and analyze data from various security tools, logs, and sources to identify security anomalies, patterns, and trends that may indicate potential threats or vulnerabilities. • Generate detailed incident reports, outlining the nature of security incidents, their impact, and the actions taken for resolution. • Assist in creating reports and	L1	1	General Shift (8x5)	3 Years	-

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		documentation required for compliance with industry standards and regulations (e.g., IRDAI, SEBI, RBI, ISO 27001). • Develop and implement automated reporting processes to streamline the generation of routine reports, reducing manual effort and increasing efficiency. • Integrate threat intelligence feeds and data into reporting processes to enhance situational awareness and proactive threat hunting. • Maintain accurate documentation of reporting and dashboard configurations, data sources, and data transformation processes for knowledge sharing and troubleshooting. • Provide training and support to SOC analysts and other stakeholders on how to interpret and utilize dashboards and reports effectively. • Assist in coordinating incident response efforts by providing real-time updates through dashboards and reports during security incidents. • Evaluate new security tools and technologies that could improve reporting and dashboard capabilities within the SOC.					

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
4	Forensic Analyst	• Respond to and investigate security incidents, breaches, or suspicious activities. This involves identifying the nature and scope of the incident, containing it, and gathering evidence for further analysis. • Collect and preserve digital evidence from various sources, including computers, servers, mobile devices, and network logs. Ensure that the evidence is gathered in a forensically sound manner to maintain its integrity. • Employ specialized tools and techniques to recover data from compromised or damaged systems, with an emphasis on preserving the original data and maintaining a chain of custody. • Create forensic images of digital devices to create an exact copy of their contents. This image is used for analysis while preserving the original evidence. • Maintain a detailed record of the handling and custody of digital evidence to ensure its admissibility in legal proceedings. • Examine digital evidence to identify signs of compromise, unauthorized access, or other security incidents. Collaborate with other	L2	1	120 hours in a year on need only basis	5 Years	CHFI

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		teams, such as cybersecurity and legal, to support investigations. • Document all forensic procedures, findings, and analysis in comprehensive reports. These reports may be used in legal proceedings or for internal reviews. • In some cases, provide expert testimony in legal proceedings to explain findings, methodologies, and the importance of digital evidence. • Offer recommendations and guidance to improve security based on findings from forensic investigations. This may include suggesting security enhancements, policy changes, or staff training.					
5	Threat Intelligence platform Analyst	• Collaborate with LIC to address challenging issues in cyber, analytics, machine learning, optimization, and computer networking to research solutions. • Propose new research projects to tackle complex cyber, analytics, machine learning, optimization, and networking problems. • Possess expertise in comprehending advanced persistent threats, emerging threats, and malware within a corporate	L2	1	General Shift (8x5)	5 Years	CTIA/CEH/CSA

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		environment. • Understand attacks, attack vectors, and kill chain methodology. • Demonstrate proficiency in working with big data and executing complex queries across multiple platforms. • Exhibit a strong grasp of malware analysis, threat taxonomy, and threat indicators. • Competently engage with various security technologies.					
6	Threat Hunter	• Continuously monitor network traffic and system logs to identify signs of potential security threats or anomalies. • Formulate hypotheses about potential threats based on analysis of existing data and threat intelligence. • Collect and analyze data from various sources, including logs, network traffic, and security tools, to validate or refute hypotheses. • Identify patterns and behaviors that may indicate malicious activity, such as unusual traffic patterns or unauthorized access attempts. • Utilize a variety of cybersecurity tools and technologies, including SIEM, UEBA, PCAP, NBAD, etc. • Document findings, actions taken, and recommendations in detailed reports for	L2	1	General Shift (8x5)	5 Years	CEH/CSA

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		internal stakeholders and management. • Recommend improvements to security policies, procedures, and controls based on threat hunting insights.					
7	SOAR Playbook Expert	• Create and maintain security playbooks for automating incident response procedures. • Analyze security incidents and determine automation opportunities. • Continuously improve existing playbooks for efficiency and effectiveness. • Conduct thorough testing and validation of playbooks to ensure accuracy. • Develop integrations with various security tools, systems, and APIs. • Map data flows between different systems and ensure data consistency. • Create custom scripts and connectors to facilitate integrations. • Implement robust error handling and troubleshooting mechanisms for integrations.	L2	1	General Shift (8x5)	6 Years	Proposed OEM Level Certification

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
8	Security Engineer with 3 Years of experience of UEBA, NBAD & PCAP	UEBA Engineer - • Integrating UEBA with other security systems. • Managing and configuring UEBA tools and agents. • Conducting threat modelling and risk assessments. NBAD Engineer - • Implement NBAD solutions within the network infrastructure and ensure proper configuration. • Continuously monitor network traffic for anomalies and suspicious behavior. • Respond to alerts and incidents identified by the NBAD system, investigate root causes, and initiate appropriate actions. • Maintain and update NBAD systems, ensuring they remain effective against evolving threats. • Document configurations, incidents, and solutions for future reference and reporting. • Develop test plans and strategies for evaluating the performance and accuracy of NBAD systems. • Execute various testing methodologies, including functional, regression, and performance testing. • Identify and report any issues or defects in the NBAD system, working	L2	3	3 Resources in General Shift (8x5)	3 Years	Proposed OEM Level Certification

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		closely with the development team for resolution. • Validate that the NBAD system meets the specified requirements and delivers accurate results. • Implement test automation where possible to streamline testing processes. PCAP Engineer - • Configuring network devices for traffic capture. • Ensuring proper routing of captured packets to storage. • Monitoring network health and performance. • Installing and configuring PCAP software and storage. • Managing system health and availability. • User access control and permissions.					
9	EDR Analyst	• Defined incident response processes based on detected threats. • Configure detection rules, policies, and response actions within the EDR solution. • Design the integration of EDR with incident response processes and workflows. • Use cases to be configured (Compliance & Security related) • Plan how to correlate endpoint data with network and threat intelligence.	L2	2	2 Resources in General Shift (8x5)	7 years	CEH
			L1	12	General Shift (8x5) at dedicated locations across India	3 years	CEH

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		• Identify the endpoints (devices) that require EDR protection and deploy agents on the endpoints. • Review and redeploy malfunctioning agents in the endpoints. • Analyze the diversity of endpoints, operating systems, and applications. • Evaluate existing endpoint security measures and tools. • Identify gaps in visibility, threat detection, and incident response capabilities. • Weekly update to LIC on implementation status					

Note:

a. The provision of on-site support is required in Mumbai.
b. To ensure required Minimum Level of Resource quality, following floor limit for Resource Cost to be quoted / factored –
    - L1 Resource – Rs. 7 Lakhs per year.
    - L2 Resource - Rs. 9 Lakhs per year.
    - L3 Resource - Rs.14 Lakhs per year.

    Note: The minimum compensation for the resources shall be at least as per the above figures. LIC reserves the right to verify the same.
c. LIC will conduct interviews of the proposed resources for NGSOC and other security solutions. It reserves the right to reject any resource which is not suitable for the proposed role.
d. All the deployed resources will be monitored based on their skills and performance for the initial six months of the project. In case the performance of the deployed resources is not up to the mark during this period, LIC reserves the right to replace such resources. In this case, the Bidder has to onboard suitable resource with relevant skillset at no additional cost to the LIC.
e. In case of exigencies, or as and when required by the LIC the onsite resources should be available on Sundays and Public Holidays as well.

6. Project Timelines

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder.	T
2	Delivery of all the equipment (software and hardware) as quoted in the bill of materials for each solution/ service in-scope. Date of delivery of last item shall be taken as date of delivery for all items.	T + 12 Weeks
3	Implementation of in-scope solutions/ services. Date of implementation of last device shall be taken as date of installation of all devices.	
	Phase 1: Implementation of SIEM, SOC, SOAR and UEBA	T + 42 Weeks
	Phase 2: Implementation of CTI and CTH	T + 14 Weeks
	Phase 3: Implementation of PCAP and NBAD	T + 20 Weeks
4	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go-Live Certificate from LIC.	T + 46 Weeks
5	Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.	T+ 52 Weeks

The Phase Wise Project Timelines of EDR as below:

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder.	T
2	Delivery of all the equipment as quoted in the bill of materials for each solution/ service in-scope. Date of delivery of last item shall be taken as date of delivery for all items.	T + 8 Weeks
3	Implementation of EDR and roll out of agents in the endpoints. Date of implementation of last device shall be taken as date of installation of all devices.	T + 24 Weeks
4	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go Live Certificate from LIC.	T + 33 Weeks
5	Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.	T+ 35 Weeks

Note: New security solutions/infrastructure (if any) which will be introduced at LIC in the future should be integrated into the Security Operations Center (SOC) within one month of their deployment and any associated activities such as but not limited to the creation of custom parser, use case or rule developments, finetuning, etc. shall be part of the scope.