INDIA INTERNATIONAL BULLION EXCHANGE IFSC LTD

Unit No. 1302A, Brigade International Financial Centre,

13th Floor, Building No. 14A, Block 14, Zone 1, GIFT SEZ, GIFT CITY, Gandhinagar, 382 050, Gujarat

Phone: +91 79 6969 7100

Email: info@iibx.co.in

REQUEST FOR PROPOSAL (RFP) - AMENDED

Hybrid Security Operations Centre

Issue Date
12-Sep-2025

CONTENTS

1. ABOUT INDIA INTERNATIONAL BULLION EXCHANGE IFSC LTD

India International Bullion Exchange IFSC Limited is India's first international bullion trading platform, inaugurated by Hon'ble Prime Minister Shri Narendra Modi on **July 29, 2022**, at GIFT City in Gandhinagar, Gujarat. It operates under the regulatory framework of International Financial Services Centres Authority (IFSCA) and is promoted by key national market infrastructure institutions viz., NSE, MCX, NSDL, CDSL and BSE (through India INX and India ICC) whereby these MIIs have equal stake in the holding company, India International Bullion Holding IFSC Ltd (IIBH) and in turn IIBH holds 100% stake in IIBX.

Key Points about IIBX

- **Spot Market Platform & BDRs**

IIBX offers T+0 trading in the form of Bullion Depository Receipts (BDRs) for Gold & Silver stored in Vaults registered with IFSCA and empanelled by India International Depository IFSC Ltd. (IIDI).

- **Launch of Futures Contracts (USD-denominated)**

Futures Trading in Gold and Silver was launched on IIBX in June 2024 and August 2025 respectively with comparable international pricing, offering Indian stakeholders an onshore hedge against price volatility.

- **Direct Import Access for Qualified Jewellers & TRQ Holders**

Qualified Jewellers and TRQ holders under the India–UAE CEPA can directly import bullion using IIBX.

- **Clearing & Settlement Infrastructure**

IFSCA-regulated IFSC Banking Units (IBUs) act as Clearing Banks, facilitating trade settlement in U.S. Dollars.

- **Regulatory Improvements**

With the introduction of the IFSCA (Bullion Market) Regulations, 2025, the Exchange expanded trading hours and relaxed net worth criteria for many categories of participants to foster broader access to its products and services.

- **Transparent Price Discovery & Quality Assurance**

  IIBX ensures transparent access to live bullion prices and quality-assured supplies & elevating market integrity.

- **Hedging in U.S. Dollars**

  With futures trading in USD, participants gain the ability to hedge bullion exposure onshore—avoiding reliance on overseas Exchanges.

✅ **In Summary**

IIBX represents a significant leap forward in India's bullion ecosystem—offering a transparent, efficient, and well-regulated marketplace for gold and silver. By combining onshore price discovery, direct import access, extended trading hours, and USD-settled Futures, the platform empowers domestic jewellers, bullion traders, refiners, and international suppliers to manage risk, enhance liquidity, and participate in an emerging global bullion hub centred in GIFT City.

2. EXECUTIVE SUMMARY

IIBX is emerging as a focal point for import of Bullion in India. IIBX also provides products for hedging the price risk in bullion. IIBX endeavours to provide best in class technology to gain the competitive edge in the market.

IIBX would like to setup a Security Operations Centre (SOC) at its own Data Centre at GIFT City Gandhinagar and inviting the proposals from the Technology partners / Original Equipment Manufacturers (OEM) of the Security Products for setting up and managing the SOC for IIBX.

3. TECHNICAL SPECIFICATIONS (SCHEDULE 1)

A. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

1. Architecture & Scalability

- Must support 150 devices and 4500 EPS from Day 1, scalable up to 1,00,000 EPS or 500 devices/servers.
- Provide scale-out distributed architecture with collectors (virtual or physical appliances) that can cache logs if the storage/correlation tier is unavailable, compress logs before sending, and limit bandwidth usage.
- Storage and correlation tier (SIEM Cluster) must support both virtual and physical appliances, with no license limit based on storage size.
- Support 10:1 log compression, HA at all layers (collectors, database, leader nodes), and automatic failover with DR Support.
- Must support big-data storage and long-term historical data retention (at least 6 months online + 24 months offline).
- Support policy-based data archiving and restoration via GUI.
- No additional license fees for extra collection/processing nodes or HA.

2. Log Collection & Data Handling

- Collect logs via agent-based and agentless methods (syslog, JDBC, API, WMI, FTP/SFTP/SCP, SNMP, MQ, etc.).
- Collect additional context from devices via protocols like SNMP, WMI, SSH, Telnet, JDBC, OPSEC, JMX, and PowerShell.
- Support collection of flow data (S-Flow, J-Flow, NetFlow) and correlate all fields.
- Allow real-time event filtering at collectors without license impact.
- Collect and store raw, parsed, and enriched data in a tamper proof manner.
- The solution must support automatic parser generation and provide a parser development framework. The framework should allow customization and editing of parsers through a graphical user interface (GUI), without requiring command-line interface (CLI) operations.
- Must ingest logs from any source without prior parser creation.

- Support local log caching, encrypted transfer, and multiple destinations for log forwarding.
- Enrich logs with business context at collection layer.
- Support monitoring of Windows/Linux devices, network configurations, file integrity, registry changes, certificate status, and application/process lists.
- The solution should provide built-in forensic investigation capabilities, including support for remote queries, system state analysis, and baseline comparisons.

3. Analytics & Search

- Unified analytics interface for logs and performance data, with nested queries and real-time search before data is stored.
- Support searches combining CMDB and event data (e.g., non-reporting critical servers).
- The solution should provide an extensive library of pre-built reports, correlation rules, and use cases relevant to security monitoring and compliance. The vendor must deliver regular content updates (reports, rules, use cases, detection logic) that are independent of core software release cycles.
- Detect anomalies, algorithmically generated domains, and unusual spikes in activity.
- Support UEBA (User & Entity Behaviour Analytics) with baselining, anomaly detection, off-network log collection, USB monitoring, data exfiltration alerts, and application detection (e.g., TOR, gaming, uncommon VPNs).

4. Threat Intelligence & AI

- Include native OEM threat intelligence feed (CTA member) and integrate external TI feeds (REST API, CSV, domains, hashes, URLs, malware process names from organizations like NCIIPC, CERT-IN, NIST).
- Correlate TI data in real-time and historically with event data.
- The SIEM should provide an open scripting framework (preferably Python) to enable seamless integration of custom Threat Intelligence (TI) feeds and connectors.
- Integrate with Generative AI (e.g., OpenAI/ChatGPT 4.0) for:

- SOC health queries
- Risk predictions
- Report creation from aggregation/raw queries
- Case analysis and enrichment
- Incident response guidance based on threat category

- Support custom Machine Learning (ML) model creation, training, and automated rule triggering.

5. Incident, Case & Response Management

- Provide built-in case/ticketing system or integrate with tools like ServiceNow, Service Desk Plus (Manage Engine), ConnectWise, Remedy.
- Support escalation policies, SLA monitoring, PDF/PNG attachments, assignments, timelines, MTTR metrics.
- Provide automated case creation/assignment, SLA violation detection, and case dashboards (health, KPI, handling metrics).
- Enable automated/manual incident response and remediation via integrated playbooks or SOAR integration.
- Support false positive detection (CVE-based IPS analysis, IOC validation) and automated incident resolution recommendations via ML.
- Integrate with EDR tools without dependency on EDR agents for log collection.

6. Compliance, Dashboards & Reporting

- Provide dashboards for PCI status, MITRE ATT&CK mapping, SLA breaches, risk scoring (based on severity, criticality, rarity, frequency, vulnerabilities), and entity ranking.
- The solution should provide out-of-the-box compliance and regulatory reports as part of the standard offering, without additional licensing or cost.
- Support configurable watch lists for critical violators, location/user-IP mapping, and event enrichment without user context.
- The proposed solution shall allow setting SLA's for different milestones within each incident investigation and response action.

- There shall be a live timer on the dashboard that shows SLA time remaining for each milestone for the analyst to keep a track of live incidents.

7. Security, Access & Integration

- Role-based access control for data and GUI, with authentication via RADIUS/Microsoft AD.
- Maintain full audit logs of all administrative and system activities.
- Integrate with Phone/SMS/email gateways for alert notifications.
- Send alerts via SMTP, syslog, Kafka (producer/consumer).
- Support integration with on-prem and cloud devices, and with both log and flow data in a single interface.

B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)

1. General Solution Requirements

- Must be an on-premises solution, scalable in use cases and performance to ensure quick response to attacks.
- HA and automatic failover with DR Support
- Accept security alerts from all data sources in any format, supporting unlimited alerts/incidents and unlimited action executions without license limits.
- Integrate across platforms for event triage, case management, ticketing, and security actions (e.g., firewall blocking, DNS updates, Windows/Linux tasks, application geo-location scripts).
- Provide an intuitive GUI and wizard for incident creation via manual entry, API, web URL, or SIEM.
- Support LDAP authentication and creation of users/groups with role-based access.
- Allow storage of incident-related files (malware, logs, screenshots, etc.).
- Licensed for at least two users from day one.
- SOAR Solution should be proposed with both options, and IIBX will decide which option to adopt. [Mandatory to propose both options]

  Option 1 (Subset Model) – SOAR deployed as a subset of the Managed Service Provider platform under a Master Controller at MSSP's premise, integrated with MSSP services.

  Option 2 (Dedicated Instance) – SOAR deployed as a dedicated tenant on the IIBX environment. If IIBX opts for this option, no connectivity except remote access for configuration will be provided to the MSSP cloud.

2. Playbook Features

- Visual playbook builder supporting manual actions, decision steps, nested playbooks, loops, conditions, Python scripting, rich-text emails, tagging, and troubleshooting.

- Enable remediation and system actions (e.g., block user, disable account, update ticket, request approvals).
- Store playbooks in a structured manner with version control, rollback, cloning, and ability to mark public/private.
- Execute playbooks manually, on schedule, on data update, or via API triggers.
- Support concurrent playbook execution with scalability via additional nodes/licenses.
- Include built-in debugging tools, error-handling options, mock outputs, and step alignment.
- Allow bulk editing of steps (delete/copy across playbooks) and categorization (e.g., data ingestion vs. others).
- Resume execution from a failed step and export playbooks (single or linked) with all saved versions.
- Enable approval before automated actions and track playbook runs per incident.

3. Connectors & Integrations

- Provide at least 500+ vendor-validated connectors on day one with related documentation.
- Support custom connector development via SDK, with health monitoring dashboards and RBAC controls for actions.
- Include in-life connector updates without requiring full system upgrades.
- Offer user-friendly data ingestion wizards and remote SOAR agents for segmented networks with auto-upgrade capability.

4. Indicators & Threat Intelligence

- Maintain a central "Indicators" database with correlation across multiple alerts.
- Bulk import, update, and export indicators, assign reputations (manual or via threat intel feeds), and tag by event, campaign, attacker, and vector.
- Link indicators to Cyber Kill Chain phases and retrospectively check new IOCs against historical alerts.
- The solution should include a vendor-neutral Threat Intelligence Platform (TIP) that provides at least one built-in OEM threat feed (preferably from a

Cyber Threat Alliance member) and supports ingestion of multiple threat intelligence sources and formats (e.g., JSON, XML, STIX, free text), along with TAXII-based export for integration with external systems.

- Support custom tagging/scoring of indicators and native integration for running multiple custom playbooks from TIP.

5. Audit Trails & Logging

- Maintain granular audit trails for incidents (manual and automated actions) and system events (logins, updates, configuration changes) with details like category, user, IP, and timestamp.
- Present incident audit trails in clear timelines showing action sequences.
- The solution should support bidirectional integration with SIEM platforms, including the ability to forward logs/events to external systems via standard protocols (e.g., syslog/CEF) and ingest data from multiple SIEM sources.

6. Dashboards & Reporting

- Provide multiple configurable role-based dashboards (e.g., analyst, SOC manager) showing alerts, tasks, SLA breaches, ROI, KPIs, and SOC metrics (MTTD, MTTC, etc.).
- Include integration health and connector status dashboards, plus a framework for building/importing custom widgets (HTML/JSON/JS).
- Support custom dashboards without extra cost.

7. Incident & Alert Management

- Automatically group duplicate alerts into single incidents and prioritize based on environmental context.
- Support manual/automated evidence collection, war-room collaboration, and correlation of incidents across IOCs and artifacts with timeline visualization.
- Provide false-positive detection mechanisms and visualization of incident resolution progress.
- Maintain central web-based incident administration.

8. Security, Compliance & Authentication

- Provide compliance reporting and monitoring content packs for major regulations (e.g., GDPR, PCI DSS, HIPAA, SOX, ISO27001) and enable extension/customization for emerging regulations such as DPDP.
- RBAC enforcement for connectors, dashboards, and system actions.

9. AI & Automation Features

- Include bots for automated threat investigation.
- ML-based risk scoring for incident prioritization.
- Generative AI to provide contextual responses on schedules, expressions, procedures, etc.

C. THREAT INTELLIGENCE PLATFORM (TIP)

1. Deployment & Infrastructure

- Must be an on-premises solution with details of required hardware infrastructure and storage provided.
- No limitation on number of user accounts or devices to which threat feeds can be sent.

2. **Threat Feed Capabilities**

- Provide threat feeds for ransomware, malware, phishing, and hash values at a minimum.
- Include risk scoring with threat feeds.
- Support multiple data formats for exporting feeds to destinations.
- TIP should provide automation and workflow capability, including a threat library or database, which allows for easy searching, manipulation and enrichment of data.
- TIP should be able to consume intel from multiple structured data format like JSON, XML, STIX, free text and any other text data. It should support export of data through TAXII.

3. Integration & Data Sharing

- Support bi-directional integration with platforms such as SIEM, next-gen firewalls, and other security systems to send and store matched values.
- Allow querying and reporting on data correlated with threat feeds.

4. Detection & Asset Reporting

- Report internal assets/devices communicating with entities in threat feeds.
- Provide a geographical attack view to visualize threat origin and spread.

5. Dashboards & Reporting

- Offer a single centralized dashboard showing the latest indicators of compromise (IOCs) and enable customized reporting.

D. REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE

1. SOC Deployment & Project Management

- MSSP to assign a dedicated project team to plan, install, configure, conduct UAT, and move SOC technologies to production.
- Engage with IIBX SPOC to define execution approach, develop a project plan, identify prerequisites, schedule activities, and define sign-off criteria.
- Conduct regular governance meetings, provide progress reports, and share installation/integration/configuration documentation.
- Develop SOC blueprint design and architecture/SOP documentation for approval before implementation.
- Interface with technology leads for log source integration and custom parser development if required.
- Configure initial threat detection rules, reports, and dashboards based on infrastructure.

2. SIEM & SOAR Setup and Customization

- Set up and configure SIEM and SOAR platforms. Integration with all IIBX Infra devices.
- Unlimited custom log parser development for any proprietary or legacy format.
- Integration of non-standard log sources (text files, custom APIs).
- Create custom connectors for unsupported tools.
- Configure SLA parameters in SOAR and share SLA reports (daily/weekly/monthly).
- Develop and tune SOAR playbooks as per environment and agreed workflows, including automated case logging, enrichment, and response.
- Support playbook chaining, nested logic, and custom automation scripts (Python/Bash).
- Manage SIEM use case lifecycle, rule creation, and enhancements.

3. Threat Monitoring, Detection & Hunting

- Provide 24x7x365 monitoring for SIEM/SOAR alerts, incidents, and forensic investigations.

- Advanced threat hunting mapped to MITRE ATT&CK, using UEBA behaviour modelling for insider threat detection.
- High-fidelity alert tuning with weekly fine-tuning and duplicate alert suppression strategies.
- Threat feed integration, including CERT-In, with real-time alert enrichment from external feeds.
- Monthly threat landscape analysis and briefs.

4. Incident Response & Forensics

- Real-time alert validation, enrichment with environmental/historical data, and notification to IIBX post-triage.
- Provide incident response workflows within SOAR, with custom workflows for IR.
- Automated audit log extraction for compliance reviews (IFSCA, SEBI, RBI,ISO).
- Perform digital forensics and support investigation activities.
- Facilitate DR & BCP tabletop exercises.

5. Reporting & Dashboards

- Bespoke dashboard and reporting customization for stakeholders.
- Role-based dashboards showing real-time incidents, alerts, and status of actions.
- Analytical reporting on daily, weekly, monthly, and on-demand basis.

6. Compliance & Audit Support

- Full audit support for compliance frameworks (ISO, IFSCA, SEBI, RBI).
- Correlate threat feeds with events and document threat detection frameworks.
- Maintain and regularly review SOC process/procedure documentation.

7. Resource Management

- Provide remote L1, L2, L3 SOC analysts, SOC manager, and platform administrators for 24x7x365 operations.
- Ensure no resource replacement without prior IIBX approval; replacements must have equal or better experience. Maintain at least a one-month transition/handover period for resource changes.
- Conduct background verification for all SOC resources.

4. DETAILS OF IIBX FOR SOLUTION SIZING

A. SPECIFIC REQUIREMENTS FOR SOLUTION SIZING

Component	Current Requirement	Scalability Requirement	Notes
SIEM – EPS Capacity	4500 EPS from Day 1	Scalable up to 1,00,000 EPS	EPS = Events Per Second
SIEM – Device Count	150 devices from Day 1	Scalable up to 500 network devices/servers	Includes on-prem and cloud devices
SOAR – Playbook Execution	Support multiple concurrent playbooks	Scalable with additional nodes	Must support high-volume automation
SIEM – Storage Retention (Online)	6 months (raw + normalized logs)	Expandable as per retention policy	Online data must be fast-searchable
SIEM – Storage Retention (Offline)	24 months (raw logs should be compressed format)	Expandable as per retention policy	Offline data must be searchable /restorable
SOAR – User Licensing	Minimum 2 concurrent users in shift from Day 1.	Scalable without functionality limits	RBAC must be supported
SIEM – Flow Data Handling	Support S-Flow, J-Flow, NetFlow	Scalable with infrastructure growth	Full field correlation required
SOAR – Integrations	At least 500+ vendor integrations on Day 1	Expandable without license limits	Includes connectors for SIEM and security tools
SIEM/SOAR – HA & DR	HA & DR from Day 1 for collectors, database, and leader nodes	DR capability as per SLA	Must ensure zero data loss during failover

B. INFRASTRUCTURE DETAILS TO BE SUPPORTED

Device Type	Make
Routers & Switches	Cisco ISR 4400, Cisco Switch-Nexus & Catalyst 9000, Cisco Smart Business Switches 350
Firewall	Checkpoint 6600 / 6700, Checkpoint Smart Console GAIA OS, Fortinet 100F
WAF	F5 Cloud Firewall
XDR	Trend Micro Vision One (Apex One)
Database	Microsoft SQL 2019 &2022, MySQL 8.0, Mongo DB 6.0, HANA
Operating Systems	Microsoft Windows Server 2019 & 2022, Microsoft Windows 11, RedHat Linux, SUSE Linux
Storage	Power Max 2000 Storage, Cisco MDS SAN Switch 9000
Servers	DELL Servers, Dell Open Manager/SCG
Email / Office	Office 365 Suite
Application/Web Server	IIS, Tomcat, In-House Application, PAM

5. ELIGIBILITY CRITERIA

Only those Bidders who fulfil the following criteria are eligible to respond to the RFP document. Offers received from the bidders who do not fulfil following criteria are considered as ineligible bidder.

No	Eligibility Criteria	Documents Required
1	Bidder must be legally registered entity i.e. Registered Firm / Limited Liability Partnership / Registered Domestic Company	Registration certificate issued by Registrar of Firms / Ministry of Corporate Affairs etc. Also Shop & Establishment License issued by local authority
2	Valid / Active Shop & Establishment, PAN and GST registration numbers	Self-certified S&E Certificate, PAN and GST copies
3	Bidder must be CERT-In empanelled.	Confirmation letter from CERT-In with valid expiry date.
4	Work Experience: - The bidder / supplier should have a minimum of Five year of experience in supply of SIEM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc.	Copies of purchase orders from the organizations shall be submitted.
5	The bidder / suppliers should not have been blacklisted by any Company in the past or services terminated due to poor performance	An undertaking stating that the Company / Firm have not been blacklisted should be submitted.

6. SELECTION CRITERIA

1. The bidder would be evaluated based on scores obtained by them on Technical and Financial Parameters mentioned in Annexure 1 and Annexure 2 respectively.
2. The Financial bids would be invited only from the bidders scoring more than 70 marks out of 100 on Technical Parameters mentioned in Annexure 1.
3. The Financial bids received from the successful technical bidders would be given scores based on Financial Parameters mentioned in Annexure 2.
4. The Financial bids would be compared against the lowest financial bid (L1) to arrive at the score of the bidder.
5. The final score of the bidder would be calculated by assigning 70% weightage to the Technical Scores & 30% weightage to the Financial Score of the bidder.
6. The bidder having the highest technical score (H1), may be asked to match the bid with the Lowest (L1) bidder. If the H1 bidder matches bid with the L1 bidder, it may be considered for the award of contract, else the bidder scoring highest based on 70:30 ratio would be considered for the award of contract.

7. TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)

Sr. No	Parameter	Select the Option Applicable						Total
1	Compliance to Solution Requirements (SIEM, SOAR, TIP) – Refer Schedule 1	Above 80 (50)	76-80 (45)	71-75 (40)	66-70 (35)	61-65 (30)	56-60 (25)	50
2	Compliance to MSSP Requirements (Implementation and Maintenance) – Refer Schedule 1	Above 30 (15)		26-30 (10)		20-25 (5)		15
3	Total number of similar Solutions implemented by the Bidder at BFSI	More than 50 (10)		26 to 50 (8)		10 to 25 (5)		10
4	Total Staff Strength of Bidder	More than 100 (10)		50 to 100 (8)		25 to 50 (5)		10
5	Technical Proposal & Bidder Presentation	Score would be given by the Committee						15
Total								**100**

Note:

1. The Technical Requirements (Chapter 3) for SIEM, SOAR, TIP, Implementation and Maintenance are provided in Excel format as Schedule 1. Click on below icon to download the Technical Requirements in Excel format file. (Schedule 1)

Schedule 1-Technical Requirei

2. The bidders are required to submit their compliances against each of the Technical Requirements mentioned in the Excel File.
3. The Parameter No. 1 i.e. compliance to Solution requirements is given a total weightage of 50 marks out of 100. The score would be allotted to each bidder out of 50 based on the compliances confirmed as "Y" by the bidder for the SIEM, SOAR and TIP sheets in Schedule 1. The applicable scores are mentioned for each option in the table.
4. The Parameter No. 2 i.e. compliance to MSSP requirements is given a total weightage of 15 marks out of 100. The score would be allotted to each bidder out of 15 based on the compliances confirmed as "Y" by the bidder for the MSSP sheet in Schedule 1. The applicable scores are mentioned for each option in the table.

5. The scores would be assigned for Parameter No. 3 & 4 based on the response of the bidder against these parameters. The applicable scores are mentioned for each option in the table.

8. FINANCIAL BID FORMAT (ANNEXURE 2)

This commercial bid provides pricing details for the perpetual licensing of SIEM, SOAR, UEBA, TIP solutions, and associated OEM support as per the RFP requirements. All prices are exclusive of applicable taxes.

Sr. No.	Description	Cost	Quantity	Price (INR)
1	Security Information and Event Management (SIEM – 150 Devices & 4500 EPS*)	Perpetual License		
2	Security Orchestration, Automation & Response (SOAR – 2 Concurrent Users) – **Sub-Set Model**	2 Year Price **[Sub-Set Model]**		
		Extended 1 Year Price **[Sub-Set Model]**		
3	Security Orchestration, Automation & Response (SOAR – 2 Concurrent Users) – **Dedicated Instance**	2 Year Price **[Dedicated Instance]**		
		Extended 1 Year Price **[Dedicated Instance]**		
4	User & Entity Behaviour Analytics (UEBA)	Perpetual License		
5	Threat Intelligence Platform (TIP)	2 Year Price		
		Extended 1 Year Price		
6	OEM Support (SIEM, SOAR, UEBA, TIP)	Annual Support & Subscription for 2 Years		
		Extended Annual Support & Subscription for 1 Years		
7	SOC Services by MSSP	Annual Charges for 2 Years		
		Extended Annual Charges for 1 Years		
8	SIEM - Pro-rate charges for 100 EPS**	Perpetual License		
9	SIEM - Pro-rate charges for 10 Devices	Perpetual License		
Total				

The bidders considering data Ingestion per day instead of EPS can consider:

* 375 GB per day (against 4500 EPS) for quoting the price.
** 8 GB per day (against 100 EPS) for quoting the price.

Note:

1. Prices should be quoted in Indian Rupees (INR) and should be exclusive of applicable taxes.
2. OEM support includes updates, patches, and technical assistance during the subscription period.
3. Quantity and final pricing to be filled as per project sizing and tender requirements.
4. Please provide a year-wise breakup of *Subscription* and *Support* costs separately, in a separate sheet, with complete details.
5. In case the proposed solution is software based, the indicative infrastructure hardware cost & configuration for implementing the solution needs to be specified by bidder in a separate sheet. IIBX will provide the required hardware.

9. ASSUMPTIONS AND CONSTRAINTS

1. There should be regular review and follow-up meetings, and the selected bidder shall provide the status of implementation. The same may be held through video conferencing.
2. All costs and expenses shall be incorporated into the project proposal and the Exchange shall not be liable for any expenses above and beyond the quoted project costs.
3. All software and hardware required by the project team shall be discussed and finalized before the award of project.
4. Timely delivery of the project is of utmost importance and any delay in the project shall be financially penalized based on mutually agreed upon criteria.
5. This assignment is non-transferable and the obligations and rights under this assignment, including the delivery of services, are not transferable or assignable to any other party without the express written consent of IIBX. Any attempt to transfer or assign the rights and obligations hereunder without such written consent shall be null and void.
6. No party will disclose any of the Confidential Information to any person except those of their employees, consultants, contractors and advisors having a need to know whole or part of such information in order to accomplish the purpose and will require each employee(s), consultants, contractors and advisors before he or she receives direct or indirect access to the Confidential Information to acknowledge the confidential and proprietary nature of the Confidential Information and agree to be bound by the obligations of the Client and/or the Bidder, as the case may be, under this Agreement.

10. TERMS AND CONDITIONS

1. This RFP does not commit to award a contract or to pay any costs incurred in the preparations or submission of proposals, or costs incurred in making necessary studies for the preparation thereof or to procure or contract for services or supplies.
2. Notwithstanding anything contained in this Request for proposal, IIBX reserves the right to accept or reject any Proposal and to annul the process and reject all Proposals, at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons thereof.
3. At any time, prior to the deadline for submission of Bids, IIBX, for any reason, suo-moto or in response to clarifications requested by a prospective bidder may modify the Request for proposal by issuing amendment (s). IIBX may, at its discretion, extend the last date for the receipt of Bids.
4. IIBX makes no commitments, explicit or implicit, that the process under this Request for proposal will result in an engagement of the bidder. Further, this Request for proposal does not constitute an offer by IIBX.
5. The Proposals must be signed by a duly authorized person of the firm.
6. Bidders must provide all requisite information as required under this RFP and clearly and concisely respond to all points listed out in this RFP. Any proposal, which does not fully and comprehensively address this RFP, may be rejected.
7. Bidders must adhere strictly to all requirements of this RFP. No changes, substitutions, or other alterations to the requirement as stipulated in this RFP document will be accepted unless approved in writing by the Exchange.
8. IIBX reserves the right to negotiate with any of the bidders or other firms in any manner deemed to be in the best interest of the Exchange.
9. The solution should support 99.99% uptime to ensure the reliability and compliance of the service levels to the users.
10. The system should be highly available and automatically use failover servers/components in case of failure of any hardware or software component.
11. The system should be easily scalable with the introduction of additional hardware components or software components.

12. The bidder should be able to demonstrate that the system is fault tolerant and has resilient architecture and that there is no single point of failure.
13. The bidder must present implementation time for the project under consideration.
14. The bidder should also provide a framework on its support services and further development post implementation of the project.
15. The bidder should provide details on Service Level standards for implementation till go live and for continuous support while system is being used in production.
16. The Bidder will be required to submit the Performance Bank Guarantee (PBG) after the award of contract. The initial PBG would be towards the delivery performance and subsequent PBG would be towards the performance during the Maintenance Period. The PBG amount would be decided based on the contract value.
17. The bidder should provide detailed cost breakup containing the year wise breakup.
18. Any disputes of claims would be subject to the exclusive jurisdiction of Courts in Ahmedabad and governed by laws of India.

11. CONFIDENTIALITY STATEMENT

This document and any attachments thereto, is intended only for use by the recipient (as addressed above) and may contain legally and/or confidential, copyrighted, trademarked, patented or otherwise restricted information viewable by the intended recipient only. If you are not the intended recipient of this document (or the person responsible for delivering this document to the intended recipient), you are hereby notified that any dissemination, distribution, printing or copying of this document, and any attachment thereto, is strictly prohibited and violation of this condition may infringe upon copyright, trademark, patent, or other laws protecting proprietary and, or, intellectual property.

If you have received this document in error, please respond to the originator of this message or email him/her at the address below and permanently delete and/or shred the original and any copies and any electronic form this document, and any attachments thereto and do not disseminate further.

12. SUBMISSION DETAILS

All interested bidders are requested to respond to Request for Proposal based on the details sought under various sections of these documents. The following are the tentative timelines for the various stages of RFP.

Sr. No.	Milestone	Date
1.	Floating of Request for Proposal	01-Sep-2025
2.	Submission of queries by the bidders	09-Sep-2025
3.	Meeting to answer the queries raised by the bidders	11-Sep-2025
4.	Publishing the replies of the queries raised by the bidders	12-Sep-2025
5.	**Last date for Submission of Technical Bids in specified format**	18-Sep-2025
6.	Technical Presentation by the bidders. (Presentation Dates would be communicated over email to respective bidders)	19-Sep-2025 to 23-Sep-2025
7.	Evaluation of Technical Bids by IIBX	24-Sep-2025
8.	Intimation to the Technically qualified bidders for submission of Financial Bids in specified format	25-Sep-2025
9.	**Submission of Financial Bids in specified format by qualified bidders in a Password-Protected file***	29-Sep-2025
10.	Communication of Password of Financial Bid by the bidder	30-Sep-2025
10.	Opening of Password-Protected Financial bids in presence of bidders	30-Sep-2025
11.	Declaration of the selected bidder	Will intimate through email.

All queries and proposals may be emailed to ProcurementcommitteeIIBX@iibx.co.in.

13. RESPONSE TO QUERIES RECEIVED AGAINST INITIAL RFP

RESPONSE TO QUERY SET – 1

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
1	Tech Spec - SIEM	6	Multi-tenant by default for departmental data segregation and analytics.	Do you need multi tenancy license to seggerate each dept wise diff SIEM Console , generally a lot of enterprises do grouping instead of multi tenance license	This clause shall be removed in the amended RFP.
2	Tech Spec - SIEM			hope shared SOC setup / MSSP is ok with IIBX or you need a dedicated on prem solution	IIBX need a dedicated on prem SOC solution
3	Tech Spec - SIEM	6	Must support big-data storage	Can you pls eleborate what big data features as all the SIEM are capable of storing data	While baseline SIEM solutions can store logs, the requirement for big data capabilities ensures that the SOC platform can operate at scale, remain cost-efficient, and deliver advanced analytics for proactive threat detection and compliance — not just store raw data.
4	Tech Spec - SIEM	6	Long-term historical data retention (at least 6 months online + 24 months offline).	Since the data will be at IIBX premises we assume the hardware will be provided by IIBX	Yes.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
5	Tech Spec - SIEM	6	Support collection of flow data (S-Flow, J-Flow, NetFlow) and correlate all fields.	Do you need QNI / NBAD solution as well	We do not have an immediate requirement for QNI / NBAD.
6	Tech Spec - SIEM	7	Must ingest logs from any source without prior parser creation	Generally this is doeable for industry standard solutions like server, network devices, etc however for custom applications etc you will hv to create a parser	The MSSP should create the custom parsers as per IIBX requirements.
7	Tech Spec - TIP	7	Integrate with Phone/SMS/email gateways for alert notifications	for SMS you will need additional gateway same should be provisioned by IIBX	Yes.
8	Threat Monitoring	12	Provide 24x7x365 monitoring for SIEM/SOAR alerts, incidents, and forensic investigations	We assume forensics is limited to SOC / SOAR tool here, in case of any additional tools required than that services would be extra (Hard disk data extraction tools, etc)	Correct
9	Threat Monitoring	13	Ensure no resource replacement without prior IIBX approval; replacements must have equal or better	This is a shared setup from our MSSP , there are no dedicated resources for IIBX hence this cluase is not applicable	This is applicable even for the shared resources which are engaged with IIBX for SOC Operations.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
			experience. Maintain at least a one-month transition/hand over period for resource changes.		
10	TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)	19	Total number of similar Solutions implemented by the Bidder by BFSI	Are you looking for 50 BFSI implementation in India / Globally ? We request you to pls reduce the count to as well	The minimum BFSI implementation required is 10 to score 5 Marks out of 10 as per the Technical Bid & Scoring Format - Annexure 1
11	TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)	19	Total number of similar Solutions implemented by the Bidder by BFSI	We request you to pls amend this as SOC Solutions implemented or managed by the Biddder, a lot of the BFSI clients buy software seperately and hence many at times supply / implementation is not in scope , however managing the SOC Solution should be in bidders scope	The clause cannot be amended because SOC Implementation is also the part of the RFP.
12		21	FINANCIAL BID FORMAT (ANNEXURE 2)	Since this will be a shared setup, SIEM / SOAR licenses will be bundled with services cost	IIBX requires Hybrid SOC i.e. the Licenses for SIEM, SOAR and TIP will be owned by IIBX, whereas managed remotely by MSSP.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
13	Threat Hunting	12	Threat Hunting (Page No 12)	Which EDR tool are you using as for advanced Threat Hunting we will need EDR to support the hunt	Trendmicro
14	Reporting	14	Reporting & Dashboarding	We will provide standard reports & Dashboarding (Samples Available).	IIBX will require Standard as well as custom reports and dashboards.
	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	
15	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	"Must support 150 devices and 4500 EPS from Day 1, scalable up to 1,00,000 EPS or 500 devices/servers. "	The scalability requirement mentions "1,00,000 EPS or 500 devices/servers." Please clarify if the solution should be designed to accommodate both maximum EPS and maximum device count simultaneously, or if these are independent maximums? For instance, if 500 devices generate more than 1,00,000 EPS, which metric takes precedence for sizing?	Different SIEM solutions follow different licensing models (EPS-based or data volume-based). The EPS-to-GB/day conversion has been provided only as a reference to enable bidders to align their commercials with their respective licensing approach. Compliance will be evaluated as per the licensing model proposed by the bidder, and exceeding one parameter while remaining within the limits of the other will not automatically be

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
					considered a breach, unless it contravenes the specific licensing terms of the selected solution.
16	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	"Provide scale-out distributed architecture with collectors (virtual or physical appliances) that can cache logs if the storage/correlation tier is unavailable, compress logs before sending, and limit bandwidth usage."	For physical appliances, does IIBX provide the hardware specifications, or is the bidder expected to propose suitable hardware, including model, make, and specifications?	The indicative infrastructure hardware cost & configuration for implementing the solution needs to be shared by bidder. IIBX will provide the required hardware.
17	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	"Multi-tenant by default for departmental data segregation and analytics."	How many distinct "departments" or tenants are anticipated for segregation, and what are the specific requirements for their data isolation, access controls, and administrative privileges?	This clause shall be removed in the amended RFP.
18	3.A.1.	SECURITY INFO	"Must support big-data storage and long-term	What are the specific requirements for	Restoration Timeframe can be 24 hours.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		RMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	historical data retention (at least 6 months online + 24 months offline)."	searching and restoring the 24 months of offline historical data, including expected search performance and restoration timeframes? Does "offline" imply warm or cold storage?	"Offline" implies cold storage.
19	3.A.2.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Log Collection & Data Handling	"Collect additional context from devices via protocols like SNMP, WMI, SSH, Telnet, JDBC, OPSEC, JMX, and PowerShell."	Please specify which devices or systems within IIBX's environment require context collection via these various protocols, and what specific context attributes (e.g., user, process, configuration) are desired from each.	This is a generic requirement.
20	3.A.2.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM	"Build parsers automatically; custom parsers editable in GUI without CLI."	How frequently are new, non-standard, or proprietary log sources expected to be introduced that would necessitate custom parser development, and what is the typical	This is a generic requirement. Any custom parser needs to be developed in 15 days.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		) - Log Collection & Data Handling		turnaround time expected for such development?	
21	3.A.3.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Analytics & Search	"Provide built-in forensic investigation tools (OSQUERY, remote queries, baseline comparisons)."	Is OSQUERY a mandatory requirement for the built-in forensic investigation tools, or are other equivalent built-in tools that provide similar capabilities (e.g., host-based visibility, remote data acquisition) acceptable?	The clause would be re-phrased in the amended RFP as - "The solution should provide built-in forensic investigation capabilities, including support for remote queries, system state analysis, and baseline comparisons."
22	3.A.4.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Threat Intelligence & AI	"Integrate with Generative AI (e.g., OpenAI/ChatGPT 4.0) for: o SOC health queries o Risk predictions o Report creation from aggregation/raw queries o Case analysis and enrichment o Incident response guidance based on threat category"	Given the sensitive nature of SOC operations and potential data exposure, where would the Generative AI be hosted (e.g., on-premises, IIBX's cloud, or vendor's cloud). Can OEM propose their own AI solutions for integration to enrich incident data?	IIBX prefers native Gen AI which would fall in the responsibility of the bidder. The Gen AI needs to be hosted on-premises.
23	3.A.6.	SECURITY INFORMAT	"Out-of-the-box compliance reports at no extra cost."	Beyond general compliance, are there specific regulatory	The clause would be re-phrased in the amended RFP as- "The solution

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		ION AND EVENT MANAGEMENT (SIEM) - Compliance, Dashboards & Reporting		frameworks (e.g., IFSCA, SEBI, RBI) for which IIBX requires out-of-the-box reports, and if so, please list all applicable frameworks?	should provide out-of-the-box compliance and regulatory reports as part of the standard offering, without additional licensing or cost".
24	3.A.6.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Compliance, Dashboards & Reporting	"The proposed solution shall allow setting SLA's for different milestones within each incident investigation and response action. There shall be a live timer on the dashboard that shows SLA time remaining for each milestone for the analyst to keep a track of live incidents."	What are the specific milestones within incident investigation and response (e.g., triage, containment, eradication, recovery, post-incident review) for which SLAs need to be tracked, and what are the associated timeframes or tiers?	This is a generic requirement. The specific SLAs shall be decided later.
25	3.B.2.	SECURITY ORCHESTRATION, AUTOMATI	"Support concurrent playbook execution with scalability via additional nodes/licenses."	What is the anticipated number or volume of concurrent playbooks or automated actions that the	In Clause 4.B Infrastructure Details (Device Type & Make) has been already shared in the RFP, based on which

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		ON & RESPONSE (SOAR) - Playbook Features		SOAR solution should be capable of supporting at peak load without performance degradation?	the estimates may be made.
26	3.B.3.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Connectors & Integrations	"Provide at least 500+ vendor-validated connectors on day one with related documentation."	Beyond the infrastructure devices listed in Section 4.B, are there other specific security tools, platforms, or business applications for which vendor-validated connectors are immediately required or highly desirable for SOAR integration?	No, IIBX has already provided infrastructure devices in clause 4.B. This is a generic requirement.
27	3.B.4.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Indicators & Threat Intelligence	"Include a vendor-neutral Threat Intelligence Platform (TIP) with one native OEM feed (CTA member) and support for multiple sources/formats (JSON, XML, STIX, free text) with TAXII export."	Since a separate TIP is also listed as a distinct requirement in Section 3.C, please clarify the scope of the TIP functionality expected within the SOAR solution. Is this for basic, integrated TIP functionality, or does it imply a deeper integration with	The clause would be re-phrased in the amended RFP as - "The solution should include a vendor-neutral Threat Intelligence Platform (TIP) that provides at least one built-in OEM threat feed (preferably from a Cyber Threat Alliance member) and supports ingestion of multiple threat intelligence

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
				the standalone TIP (Section 3.C)?	sources and formats (e.g., JSON, XML, STIX, free text), along with TAXII-based export for integration with external systems". Further, this is required for deeper integration.
28	3.B.5.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Audit Trails & Logging	"Support log forwarding to syslog/SIEM (Fortinet, Splunk, Microsoft, QRadar, etc.) and ingestion from multiple SIEM sources."	Does IIBX currently use one of the listed SIEMs for SOAR log forwarding, or is the intention for SOAR logs to be forwarded to the new SIEM solution being procured as part of this RFP?	This would be new SOC Setup.
29	3.B.9.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - AI & Auto	"Generative AI to provide contextual responses on schedules, expressions, procedures, etc."	Similar to the SIEM's Generative AI, where would the Generative AI for SOAR be hosted, and can the OEM propose their own AI solutions as part of the technical bid?	IIBX prefers native Gen AI which would fall in the responsibility of the bidder.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		matio n Featur es			
30	3.C.1.	THRE AT INTEL LIGE NCE PLAT FORM (TIP) - Deplo yment & Infrast ructur e	"Must be an on-premises solution with details of required hardware infrastructure and storage provided."	Is the Threat Intelligence Platform expected to be from the same OEM as the OEM supplying SIEM and SOAR?	Yes
31	3.C.2.	THRE AT INTEL LIGE NCE PLAT FORM (TIP) - Threat Feed Capab ilities	"TIP should provide automation and workflow capability, including a threat library or database, which allows for easy searching, manipulation and enrichment of data."	What specific types of automation and workflow capabilities are expected within the TIP beyond basic feed consumption, enrichment, and export (e.g., integration with vulnerability management, asset management for context-aware prioritization)?	This is a generic requirement.
32	3.C.3.	THRE AT INTEL LIGE NCE PLAT FORM (TIP) - Integr	"Support bi-directional integration with platforms such as SIEM, next-gen firewalls, and other security systems to send and	Beyond SIEM and next-gen firewalls, what other specific security systems (e.g., EDR, WAF, email security gateways, proxy servers) are	Need to be integrated with current EDR & WAF. However, this is a generic requirement and it may need to be integrated with other solution like

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		ation & Data Sharing	store matched values."	critical for bi-directional integration with the TIP?	PAM etc. in future.
33	3.D.2.	REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE - SIEM & SOAR Setup and Customization	"Set up and configure SIEM and SOAR platforms. Integration with all IIBX Infra devices."	Can IIBX provide a detailed and exhaustive list of all devices, applications, and cloud services expected to be integrated, beyond those listed in Section 4.B, to ensure comprehensive integration planning and effort estimation?	Number of Windows Servers: 93 Number of Windows Workstations: 50 Number of Linux Server: 6 Number of Network Components Switches: 24 San Switches: 4 Routers : 6 Firewall:12 Number of Domain Controllers:5 Number of Windows File Server:1 Number of MSSQL Servers:5 Number of IIS Sites:21 Number of Tomcat:7 Number of JBoss: 1 Number of O365 tenants:1 WAF : 20 URLs XDR: 1
34	4.A.	DETAILS OF IIBX FOR SOLUTION	"SIEM – Storage Retention (Online) 6 months (raw + normalized logs) Expandable as	What is the expected maximum timeframe for restoring or searching offline data? Does	Restoration Timeframe can be 24 hours. "Searchable/restorable" imply direct searching of offline archives.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		SIZING - Specific Requirements for Solution Sizing	per retention policy Online data must be fast-searchable" and "SIEM – Storage Retention (Offline) 24 months (raw logs should be compressed format) Expandable as per retention policy Offline data must be searchable /restorable"	"searchable/restorable" imply direct searching of offline archives, or restoration to online storage before searching, and what are the performance expectations for either method?	
35	4.B.	DETAILS OF IIBX FOR SOLUTION SIZING - Infrastructure Details to be Supported	"Application/Web Server IIS, Tomcat, In-House Application, PAM"	For "In-House Application" under Application/Web Server, can IIBX provide details or documentation on the expected log formats, typical volume, and any available APIs for these custom applications to facilitate parser and connector development?	This is a generic requirement. The details can be provided later.
36	7 (Note 3)	TECHNICAL BID & SCORING FORMAT (ANN	"The Parameter No. 1 i.e. compliance to Solution requirements is given a total weightage of 50 marks out of 100. The score would be	Note 3 under the Technical Bid & Scoring Format states that scores for "Compliance to Solution Requirements" will be allotted based on compliances	Only Full compliance (Y) receives points for a given requirement.

Sr. No.	Clause No.	Page No.	RFP Clause	Clarification	IIBX Response
		EXURE 1)	allotted to each bidder out of 50 based on the compliances confirmed as "Y" by the bidder for the SIEM, SOAR and TIP sheets in Schedule 1. The applicable scores are mentioned for each option in the table."	confirmed as "Y". Could IIBX clarify if partial compliance (e.g., indicated with a 'P' or 'N' with a detailed explanation of how it can be met or a roadmap) will be accepted and how it would be scored, or if only full compliance ('Y') receives points for a given requirement?	

RESPONSE TO QUERY SET – 2

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
1	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	"Must support 150 devices and 4500 EPS from Day 1, scalable up to 1,00,000 EPS or 500 devices/servers."	The scalability requirement mentions "1,00,000 EPS or 500 devices/servers." Please clarify if the solution should be designed to accommodate both maximum EPS and maximum device count simultaneously, or if these are independent maximums? For instance, if 500 devices generate more than 1,00,000 EPS, which metric takes precedence for sizing?	Different SIEM solutions follow different licensing models (EPS-based or data volume-based). The EPS-to-GB/day conversion has been provided only as a reference to enable bidders to align their commercials with their respective licensing approach. Compliance will be evaluated as per the licensing model proposed by the bidder, and exceeding one parameter while remaining within the limits of the other will not automatically be considered a breach, unless it contravenes the specific licensing terms of the selected solution.
2	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEM	"Provide scale-out distributed architecture with collectors (virtual or	For physical appliances, does IIBX provide the hardware	The indicative infrastructure hardware cost & configuration for implementing

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
		ENT (SIEM) - Architecture & Scalability	physical appliances) that can cache logs if the storage/correlation tier is unavailable, compress logs before sending, and limit bandwidth usage."	specifications, or is the bidder expected to propose suitable hardware, including model, make, and specifications?	the solution needs to be shared by bidder. IIBX will provide the required hardware.
3	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	"Multi-tenant by default for departmental data segregation and analytics."	How many distinct "departments" or tenants are anticipated for segregation, and what are the specific requirements for their data isolation, access controls, and administrative privileges?	This clause shall be removed in the amended RFP.
4	3.A.1.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Architecture & Scalability	"Must support big-data storage and long-term historical data retention (at least 6 months online + 24 months offline)."	What are the specific requirements for searching and restoring the 24 months of offline historical	Restoration Timeframe can be 24 hours. "Offline" implies cold storage.

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				data, including expected search performance and restoration timeframes? Does "offline" imply warm or cold storage?	
5	3.A.2.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Log Collection & Data Handling	"Collect additional context from devices via protocols like SNMP, WMI, SSH, Telnet, JDBC, OPSEC, JMX, and PowerShell."	Please specify which devices or systems within IIBX's environment require context collection via these various protocols, and what specific context attributes (e.g., user, process, configuration) are desired from each.	This is a generic requirement.
6	3.A.2.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Log	"Build parsers automatically; custom parsers editable in GUI without CLI."	How frequently are new, non-standard, or proprietary log sources	This is a generic requirement. Any custom parser needs to be developed in 15 days.

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
		Collection & Data Handling		expected to be introduced that would necessitate custom parser developmen t, and what is the typical turnaround time expected for such developmen t?	
7	3.A.3.	SECURITY INFORMATI ON AND EVENT MANAGEM ENT (SIEM) - Analytics & Search	"Provide built-in forensic investigation tools (OSQUERY, remote queries, baseline comparisons)."	Is OSQUERY a mandatory requirement for the built-in forensic investigatio n tools, or are other equivalent built-in tools that provide similar capabilities (e.g., host-based visibility, remote data acquisition) acceptable?	The clause would be re-phrased in the amended RFP as - "The solution should provide built-in forensic investigation capabilities, including support for remote queries, system state analysis, and baseline comparisons."
8	3.A.4.	SECURITY INFORMATI ON AND EVENT MANAGEM ENT (SIEM) - Threat	"Integrate with Generative AI (e.g., OpenAI/Chat GPT 4.0) for: o SOC health queries o Risk predictions o	Given the sensitive nature of SOC operations and potential data	IIBX prefers native Gen AI which would fall in the responsibility of the bidder. The Gen AI needs to

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
		Intelligence & AI	Report creation from aggregation/raw queries o Case analysis and enrichment o Incident response guidance based on threat category"	exposure, where would the Generative AI be hosted (e.g., on-premises, IIBX's cloud, or vendor's cloud). Can OEM propose their own AI solutions for integration to enrich incident data?	be hosted on-premises.
9	3.A.6.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Compliance, Dashboards & Reporting	"Out-of-the-box compliance reports at no extra cost."	Beyond general compliance, are there specific regulatory frameworks (e.g., IFSCA, SEBI, RBI) for which IIBX requires out-of-the-box reports, and if so, please list all applicable frameworks ?	The clause would be re-phrased in the amended RFP as- "The solution should provide out-of-the-box compliance and regulatory reports as part of the standard offering, without additional licensing or cost".
10	3.A.6.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) - Compliance,	"The proposed solution shall allow setting SLA's for different milestones within each	What are the specific milestones within incident investigation and	This is a generic requirement. The specific SLAs shall be decided later.

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
		Dashboards & Reporting	incident investigation and response action. There shall be a live timer on the dashboard that shows SLA time remaining for each milestone for the analyst to keep a track of live incidents."	response (e.g., triage, containment , eradication, recovery, post-incident review) for which SLAs need to be tracked, and what are the associated timeframes or tiers?	
11	3.B.2.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Playbook Features	"Support concurrent playbook execution with scalability via additional nodes/licenses ."	What is the anticipated number or volume of concurrent playbooks or automated actions that the SOAR solution should be capable of supporting at peak load without performance degradation ?	In Clause 4.B Infrastructure Details (Device Type & Make) has been already shared in the RFP, based on which the estimates may be made.
12	3.B.3.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Connectors & Integrations	"Provide at least 500+ vendor-validated connectors on day one with related documentation ."	Beyond the infrastructure devices listed in Section 4.B, are there other specific security	No, IIBX has already provided infrastructure devices in clause 4.B. This is a generic requirement.

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				tools, platforms, or business applications for which vendor-validated connectors are immediately required or highly desirable for SOAR integration?	
13	3.B.4.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Indicators & Threat Intelligence	"Include a vendor-neutral Threat Intelligence Platform (TIP) with one native OEM feed (CTA member) and support for multiple sources/formats (JSON, XML, STIX, free text) with TAXII export."	Since a separate TIP is also listed as a distinct requirement in Section 3.C, please clarify the scope of the TIP functionality expected within the SOAR solution. Is this for basic, integrated TIP functionality, or does it imply a deeper integration with the standalone TIP (Section 3.C)?	The clause would be re-phrased in the amended RFP as - "The solution should include a vendor-neutral Threat Intelligence Platform (TIP) that provides at least one built-in OEM threat feed (preferably from a Cyber Threat Alliance member) and supports ingestion of multiple threat intelligence sources and formats (e.g., JSON, XML, STIX, free text), along with TAXII-based export for integration with

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
					external systems". Further, this is required for deeper integration.
14	3.B.5.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - Audit Trails & Logging	"Support log forwarding to syslog/SIEM (Fortinet, Splunk, Microsoft, QRadar, etc.) and ingestion from multiple SIEM sources."	Does IIBX currently use one of the listed SIEMs for SOAR log forwarding, or is the intention for SOAR logs to be forwarded to the new SIEM solution being procured as part of this RFP?	This would be new SOC Setup.
15	3.B.9.	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR) - AI & Automation Features	"Generative AI to provide contextual responses on schedules, expressions, procedures, etc."	Similar to the SIEM's Generative AI, where would the Generative AI for SOAR be hosted, and can the OEM propose their own AI solutions as part of the technical bid?	IIBX prefers native Gen AI which would fall in the responsibility of the bidder.
16	3.C.1.	THREAT INTELLIGENCE	"Must be an on-premises solution with	Is the Threat Intelligence Platform	Yes

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
		PLATFORM (TIP) - Deployment & Infrastructure	details of required hardware infrastructure and storage provided."	expected to be from the same OEM as the OEM supplying SIEM and SOAR?	
17	3.C.2.	THREAT INTELLIGENCE PLATFORM (TIP) - Threat Feed Capabilities	"TIP should provide automation and workflow capability, including a threat library or database, which allows for easy searching, manipulation and enrichment of data."	What specific types of automation and workflow capabilities are expected within the TIP beyond basic feed consumption, enrichment, and export (e.g., integration with vulnerability management, asset management for context-aware prioritization)?	This is a generic requirement.
18	3.C.3.	THREAT INTELLIGENCE PLATFORM (TIP) - Integration & Data Sharing	"Support bi-directional integration with platforms such as SIEM, next-gen firewalls, and other security systems to send and store	Beyond SIEM and next-gen firewalls, what other specific security systems (e.g., EDR, WAF, email	Need to be integrated with current EDR & WAF. However, this is a generic requirement and it may need to be integrated with other solution

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
			matched values."	security gateways, proxy servers) are critical for bi-directional integration with the TIP?	like PAM etc. in future.
19	3.D.2.	REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE - SIEM & SOAR Setup and Customization	"Set up and configure SIEM and SOAR platforms. Integration with all IIBX Infra devices."	Can IIBX provide a detailed and exhaustive list of all devices, applications, and cloud services expected to be integrated, beyond those listed in Section 4.B, to ensure comprehensive integration planning and effort estimation?	Number of Windows Servers: 93 Number of Windows Workstations: 50 Number of Linux Server: 6 Number of Network Components Switches: 24 San Switches: 4 Routers : 6 Firewall:12 Number of Domain Controllers:5 Number of Windows File Server:1 Number of MSSQL Servers:5 Number of IIS Sites:21 Number of Tomcat:7 Number of JBoss: 1 Number of O365 tenants:1 WAF : 20 URLs XDR: 1

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
20	4.A.	DETAILS OF IIBX FOR SOLUTION SIZING - Specific Requirements for Solution Sizing	"SIEM – Storage Retention (Online) 6 months (raw + normalized logs) Expandable as per retention policy Online data must be fast-searchable" and "SIEM – Storage Retention (Offline) 24 months (raw logs should be compressed format) Expandable as per retention policy Offline data must be searchable /restorable"	What is the expected maximum timeframe for restoring or searching offline data? Does "searchable/ restorable" imply direct searching of offline archives, or restoration to online storage before searching, and what are the performance expectations for either method?	Restoration Timeframe can be 24 hours. "Searchable/restorable" imply direct searching of offline archives.
21	4.B.	DETAILS OF IIBX FOR SOLUTION SIZING - Infrastructure Details to be Supported	"Application/ Web Server IIS, Tomcat, In-House Application, PAM"	For "In-House Application" under Application /Web Server, can IIBX provide details or documentation on the expected log formats, typical volume, and any available	This is a generic requirement. The details can be provided later.

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				APIs for these custom applications to facilitate parser and connector developmen t?	
22	7 (Note 3)	TECHNICAL BID & SCORING FORMAT (ANNEXURE 1)	"The Parameter No. 1 i.e. compliance to Solution requirements is given a total weightage of 50 marks out of 100. The score would be allotted to each bidder out of 50 based on the compliances confirmed as “Y” by the bidder for the SIEM, SOAR and TIP sheets in Schedule 1. The applicable scores are mentioned for each option in the table."	Note 3 under the Technical Bid & Scoring Format states that scores for "Compliance to Solution Requiremen ts" will be allotted based on compliances confirmed as “Y”. Could IIBX clarify if partial compliance (e.g., indicated with a 'P' or 'N' with a detailed explanation of how it can be met or a roadmap) will be accepted and how it would be	Only Full compliance (Y) receives points for a given requirement.

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				scored, or if only full compliance ('Y') receives points for a given requirement ?	
23				Kindly provide details on the payment terms	The payment will be linked to Delivery and implementation milestones. Post Implementation, the payment for MSSP would be on Quarterly advance basis.
24				what will be the implementation mode: Remote or Onsite or Hybrid ?	Either
25				Does the bidder require to share the infrastructure hardware cost for implementing the solution or IIBX will help cater to it.	Yes in case the solution is software base, then the indicative infrastructure hardware cost & configuration for implementing the solution needs to be shared by bidder.
26				Is there a need for onsite or remote support after	L3 remote support is expected

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				implementation ?	
27				Could you please confirm if there are any preferred OEMs/vendors or existing technology stack in use by IIBX for SIEM, SOAR, UEBA, or TIP solutions?	No, Preferred OEM / Vendors. This would be new SOC Setup.
28				For the integration of Generative AI (e.g., OpenAI/ChatGPT), is there an existing license or API subscription provided by IIBX, or is it the responsibility of the bidder?	IIBX prefers native Gen AI which would fall in the responsibility of the bidder.
29				Please specify the expected RTO (Recovery Time Objective)	Recovery Time Objective (RTO) is 45 minutes Recovery Point Objective (RPO) is 15 minutes,

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				and RPO (Recovery Point Objective) targets for HA and DR setups.	
30				Should DR infrastructure be provisioned at a specific site (e.g., remote DC, cloud)?	Remote DC of IIBX
31				Is IIBX expecting MSSP to provide the complete set of SOC staffing (L1, L2, L3 Analysts, SOC Manager), or will there be any existing internal SOC team working in parallel?	Required complete set of SOC staffing from MSSP.
32				Should SOC analysts be onsite at IIBX or operate remotely from MSSP premises?	Operate remotely from MSSP Premises. However no logs or data shall be shared outside IIBX SOC.
33				Is there a preferred compliance	Yes, SEBI & ISO

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				framework (IFSCA, SEBI, RBI, ISO) to prioritize?	
34				Will IIBX provide existing compliance audit templates, or should the bidder propose full compliance documentation?	Bidder should propose full compliance documentation.
35				Are there any existing external threat intelligence feed subscriptions (e.g., CERT-In, commercial TI providers) that IIBX currently uses?	Yes, IIBX has subscribed CERT-In's threat intelligence feed.
36				Does IIBX require bi-directional sharing of IOCs to external stakeholders or only internal usage?	Yes, Bi-Directional sharing is required.
37				Are there any data	No logs or data shall be shared

Sr No	RFP Section Number	RFP Section Heading	Exact Statement from RFP	IBM Query	IIBX Response
				residency or encryption standards mandated by IIBX for log storage, TIP, or playbook files?	outside IIBX SOC. There is no specific standard mandated for encryption.

RESPONSE TO QUERY SET – 3

Sr No	Questionnaire	IIBX Response
SIEM / SOAR / TIP Functional Clarifications		
1	Could you please confirm if there are any preferred OEMs/vendors or existing technology stack in use by IIBX for SIEM, SOAR, UEBA, or TIP solutions?	No, Preferred OEM / Vendors. This would be new SOC Setup.
2	For the integration of Generative AI (e.g., OpenAI/ChatGPT), is there an existing license or API subscription provided by IIBX, or is it the responsibility of the bidder?	IIBX prefers native Gen AI which would fall in the responsibility of the bidder.
High Availability (HA) & Disaster Recovery (DR)		
3	Please specify the expected RTO (Recovery Time Objective) and RPO (Recovery Point Objective) targets for HA and DR setups.	Recovery Time Objective (RTO) is 45 minutes Recovery Point Objective (RPO) is 15 minutes,
4	Should DR infrastructure be provisioned at a specific site (e.g., remote DC, cloud)?	Remote DC of IIBX
MSSP Operations Clarification		
5	Is IIBX expecting MSSP to provide the complete set of SOC staffing (L1, L2, L3 Analysts, SOC Manager), or will there be any existing internal SOC team working in parallel?	Required complete set of SOC staffing from MSSP.
6	Should SOC analysts be onsite at IIBX or operate remotely from MSSP premises?	Operate remotely from MSSP Premises. However no logs or data shall be shared outside IIBX SOC.
Compliance Framework		
7	Is there a preferred compliance framework (IFSCA, SEBI, RBI, ISO) to prioritize?	Yes, SEBI & ISO
8	Will IIBX provide existing compliance audit templates, or should the bidder propose full compliance documentation?	Bidder should propose full compliance documentation.
TIP Feed Sources		
9	Are there any existing external threat intelligence feed subscriptions (e.g., CERT-In, commercial TI providers) that IIBX currently uses?	Yes, IIBX has subscribed CERT-In's threat intelligence feed.

Sr No	Questionnaire	IIBX Response
10	Does IIBX require bi-directional sharing of IOCs to external stakeholders or only internal usage?	Yes, Bi-Directional sharing is required.
11	Are there any data residency or encryption standards mandated by IIBX for log storage, TIP, or playbook files?	No logs or data shall be shared outside IIBX SOC. There is no specific standard mandated for encryption.

RESPONSE TO QUERY SET – 4

Sr. No.	RFP Page No. / Section	Clause / Requirement	Bidder's Query / Clarification Sought	Remarks (if any)	IIBX Response
1	Page 6 / SIEM (4. Threat Intelligence and AI)	Provide Python-based framework for custom TI integrations.	Threat intelligence can be fetched in using the STIX and TAXII feeds, Requesting clarifications for the need for Python-based Framework.	Requirement aligns to IDE specific and does not align to Threat Intelligence platform.	The clause would be re-phrased in the amended RFP as - "The SIEM should provide an open scripting framework (preferably Python) to enable seamless integration of custom Threat Intelligence (TI) feeds and connectors."
2	Page 6 / SIEM (4. Threat Intelligence and AI)	Integrate with Generative AI (e.g., OpenAI/ChatGPT 4.0) for: SOC health queries Risk predictions Report creation from aggregation/ raw queries Case analysis and enrichment Incident response guidance	Please confirm that Bring Your Own Key (BYOK) integration is supported for the Generative AI components. Additionally, request removal of the phrase 'SOC Health queries' from the Threat Intelligence scope, since such queries rely on contextual, generative LLM responses and do not constitute threat-intelligence operations.		IIBX prefers native Gen AI which would fall in the responsibility of the bidder. The "SOC Health queries" has been kept in this section since this section includes Threat Intelligence as well as AI.

Sr. No.	RFP Page No./ Section	Clause / Requirement	Bidder's Query / Clarification Sought	Remarks (if any)	IIBX Response
		based on threat category			
3	Page 7 / SIEM (Incident, Case & Response Management)	Support false positive detection (CVE-based IPS analysis, IOC validation) and automated incident resolution recommendations via ML.	Proposed Solutions natively support IOC Validation and CVE-linked correlation/suppression for false-positive reduction. Requesting the removal for "automated incident resolution recommendations via ML."	Native ML-generated resolution recommendations are not available; enforcing them as mandatory would exclude compliant solutions. Rule/runbook guidance (with analyst-in-the-loop) maintains governance with incident recommendations	It's a functional requirement / capability statement.
4	Page 10 / SOAR (Dashboards & Reporting)	Include integration health and connector status dashboards, plus a framework for	The Proposed solution would have SOAR built-in along with the central console hence health and connector status would not be required. Requesting to make it optional /	Analytics platform would be proposed for the dashboards and reporting where	It's a functional requirement / capability statement. Further framework for building/im

Sr. No.	RFP Page No./ Section	Clause / Requirement	Bidder's Query / Clarification Sought	Remarks (if any)	IIBX Response
		building/importing custom widgets (HTML/JSON/JS).	removal for the requirement clause	custom widgets shall be created not imported.	porting custom widgets is mentioned where "/" is equivalent to "or". So importing is not mandatory.
5	Page 14 / 4. Details of IIBX for Solution Sizing	A. SPECIFIC REQUIREMENTS FOR SOLUTION SIZING	Request to provide the split count for the below mentioned components : Number of Windows Servers, Number of Windows Workstations, Number of Linux Server and Desktops, Number of Network Components (Switches, Routers, Firewall, Gateway, IDS and IPS Unix Machines),Number of Domain Controllers, Number of Windows File Server, Number of Linux File Servers< Number of Netapp/ Synology / EMC NAS device, Number of MSSQL Servers, Number of IIS Sites, Number of O365 tenants, Number of AWS Accounts, Number of Exchange Servers.	Proposed solution is device based, Request to provide the split up count for the device components so that BOQ can be derived for the commercial proposal.	If the solution is device based, then the split up count for the device components should not have any impact on commerical proposal.
6	Page 12 / 3. Threat Monit	Provide 24x7x365 monitoring for	How many endpoints, servers, and network devices need to be monitored?		As mentioned in Clause 4.B

Sr. No.	RFP Page No./ Section	Clause / Requirement	Bidder's Query / Clarification Sought	Remarks (if any)	IIBX Response
	oring, Detection & Hunting	SIEM/SOAR alerts, incidents, and forensic investigations.			
7	Page 12 / 3. Threat Monitoring, Detection & Hunting	Provide 24x7x365 monitoring for SIEM/SOAR alerts, incidents, and forensic investigations.	Is there an in-house security team to collaborate with, or is the MSSP fully managing the SOC?		The SOC should be fully managed by MSSP by keeping the IIBX team in loop.
8	Page 12 / 3. Threat Monitoring, Detection & Hunting	Provide 24x7x365 monitoring for SIEM/SOAR alerts, incidents, and forensic investigations.	Would you prefer our SOC services to include end-to-end incident response and remediation, or limit our scope to detection and escalation only?		IIBX prefers SOC services to include end-to-end incident response and remediation. However, in case any credentials are required for response or remediation, IIBX security team will get involved.
9	Additional Query	Payment Terms are not mentioned in RFP. Kindly confirm milestonewise payment terms.	Payment Terms are not mentioned in RFP. Kindly confirm milestonewise payment terms.	-	The payment will be linked to Delivery and implementation milestones. Post Implementat

Sr. No.	RFP Page No. / Section	Clause / Requirement	Bidder's Query / Clarification Sought	Remarks (if any)	IIBX Response
					ion, the payment for MSSP would be on Quarterly advance basis.
10	Eligibility Criteria (RFP Page no. 17) Point no. 4	Work Experience: - The bidder / supplier should have a minimum of Five year of experience in supply of SIEM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc.	As per our understanding, PO reference of SIEM solution older than 5 years will suffice this requirement. Kindly confirm		The work experience should be for at least 5 years and must continue till date. So the PO reference of SIEM solutions older than 5 years would meet the requirement for 5 years experience. However, the PO reference within 5 years including recent year would serve as evidence for continuous experience.
11	TECHNICAL BID & SCORING	Total number of similar Solutions implemented by the Bidder by BFSI	Request for clarity on below points. 1. 50 nos. of implementation is required (irrespective of no. of customers		1. 50 nos. customers required in BFSI sector where similar SOC

Sr. No.	RFP Page No. / Section	Clause / Requirement	Bidder's Query / Clarification Sought	Remarks (if any)	IIBX Response
	FORMAT (ANNEXURE 1) (RFP Page no. 19) Point 3	More than 50 - 10 Marks	and solutions) or 50 nos. of customers required? kindly clarify 2.Can we submit PO references of different customers where same solutions are imlemented and can it be considered different count as per RFP clause. 3. What type of documents we need to submit to support this clause		solution is implemented . 2. Refer answer to point no. 1. 3. Provide PO Reference. We will verify with client.
12	TECHNICAL BID & SCORING FORMAT (ANNEXURE 1) (RFP Page no. 19) Point 4	Total Staff Strength of Bidder More than 100 (10)	What type of document we need to submit to support this clause		The Professional Tax statement (Returns) can be submitted as evidence.
13	Additional Query	Delivery Timelines is not mentioned in RFP.	Kindly clarify on delivery timelines		The Bidder should propose.

RESPONSE TO QUERY SET – 5

Sr. No	RFP Document Reference(s) Section	Page Number	Content of RFP requiring clarification(s)	Points of Clarification	IIBX Response
1	RFP Document Reference(s) Section	5.0	Provide built-in forensic investigation tools (OSQUERY, remote queries, baseline comparisons).	This requirement appears to be from a proprietary OEM specification. We kindly recommend removing this clause from the RFP.	The clause would be re-phrased in the amended RFP as - "The solution should provide built-in forensic investigation capabilities, including support for remote queries, system state analysis, and baseline comparisons."
2	Main Section: A. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Sub Section: 3. Analytics & Search Point No.02	6.0	Support searches combining CMDB and event data (e.g., non-reporting critical servers).	This requirement appears to be from a proprietary OEM specification. We kindly recommend removing this clause from the RFP.	This is not vendor-specific. It's a functional capability that many SIEM platforms can support
3	Main Section: A. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Sub Section: 3. Analytics & Search Point No.03	6.0	Provide 3000+ reports and 2000+ correlation rules with content updates independent of software releases.	The count seems too specific for an OEM. Kindly requesting you to generalise the specifications or Kindly amend the clause as	The clause would be re-phrased in the amended RFP as - "The solution should provide an extensive library of pre-built reports, correlation

Sr. No	RFP Document Reference(s) Section	Page Number	Content of RFP requiring clarification(s)	Points of Clarification	IIBX Response
				"Provide compliance reports aligned to standards such as ISO, PCI-DSS, and IIBX requirements and 2,000+ correlation rules /equivalent correlation rules covering the complete MITRE ATT&CK framework, with continuous content updates independent of software releases."	rules, and use cases relevant to security monitoring and compliance. The vendor must deliver regular content updates (reports, rules, use cases, detection logic) that are independent of core software release cycles.
4	Main Section: A. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) Sub Section: 6. Compliance, Dashboards & Reporting Point No.04	8.0	There shall be a live timer on the dashboard that shows SLA time remaining for each milestone for the analyst to keep a track of live incidents.	This requirement appears to be from a proprietary OEM specification. We kindly recommend removing this clause from the RFP.	This is not vendor-specific. It's a functional requirement that can be implemented in most SIEM/SOAR platforms.
5	Schedule 1-Technical requirement Point N0. 10		SIEM Vendor proposed should be listed in Gartner's Magic Quadrant for	Kindly Requesting to give Exemption or Waive Off for this Clause,This will help more	Suggestion accepted. This requirement shall be waived off.

Sr. No	RFP Document Reference(s) Section	Page Number	Content of RFP requiring clarification(s)	Points of Clarification	IIBX Response
			latest report of 2024	Make In India startups to come forward and particpate in this opportunity" "With Reference to Public Procurement (Preference to Make In India) Order 2019 from MeitY Point No.8:-In any procurement process, the procuring entity shall not specify any mandatory qualification criteria, any eligibility specifications or certification(s) issued by any foreign testing/security lab(s)/analyst reviews which restricts eligibility of Indian cyber security products as defined in this order.	

RESPONSE TO QUERY SET – 6

Sr. No	Page No.	Section No.	Clause No.	Reference/ Subject Clarification Sought	IIBX Response
1	9	3.B	1	SOAR Deployment Options: Since the RFP requires proposing both a Subset and a Dedicated Instance model for SOAR, will IIBX provide a preference, or should bidders assume one for the primary commercial evaluation? How will the final commercial value (L1) be determined if two distinct options are quoted?	IIBX will decide between the Subset model and the Dedicated Instance model based on the commercial offers received. For evaluation purposes, bids will be compared on a like-for-like (at par) basis to ensure fairness across vendors. The final determination of L1 will take into account the most commercially viable option for IIBX.
2	21	8		SIEM Sizing (EPS vs. GB/day): The financial format provides a conversion of 4500 EPS to 375 GB/day. Could you please clarify which metric (EPS or GB/day) will be the primary measure for licensing and compliance? If the data volume exceeds the GB/day limit while EPS remains within its limit, will it be considered a breach of the license?	Different SIEM solutions follow different licensing models (EPS-based or data volume-based). The EPS-to-GB/day conversion has been provided only as a reference to enable bidders to align their commercials with their respective licensing approach. Compliance will be evaluated as per the licensing model proposed by the bidder, and exceeding one parameter while remaining within the limits of the other will not automatically be considered a breach, unless it contravenes the specific licensing terms of the selected solution.
3	12, 13	3.C, 3.D	1, 1	Hardware and Infrastructure Provisioning:	The indicative infrastructure hardware cost & configuration for

Sr. No	Page No.	Section No.	Clause No.	Reference/ Subject Clarification Sought	IIBX Response
				Regarding the on-premises deployment of the SIEM, SOAR, and TIP solutions at the IIBX Data Centre, could you please clarify if IIBX will provide the required hardware (servers, storage) based on the specifications provided by the bidder, or if the bidder is expected to supply the hardware as part of the commercial bid?	implementing the solution needs to be shared by bidder. IIBX will provide the required hardware.
4	13	3.D	2	Scope of "Unlimited" Custom Parsers: The RFP states a requirement for "Unlimited custom log parser development". Could IIBX please provide an estimate of the number of custom log sources anticipated in the first year? Additionally, is there a defined Service Level Agreement (SLA) for the development of new parsers for non-standard or undocumented log sources?	In Clause 4.B Infrastructure Details (Device Type & Make) has been already shared in the RFP, based on which the estimates may be made. Any custom parser needs to be developed in 15 days. The exact SLA can be defined subsequently.
5	13	3.D	2	SOAR Playbook Development Scope: Could IIBX provide	In Clause 4.B Infrastructure Details (Device Type & Make) has been already

Sr. No	Page No.	Section No.	Clause No.	Reference/ Subject Clarification Sought	IIBX Response
				an indicative list of initial use cases or the number of custom SOAR playbooks that are expected to be developed during the implementation phase? What is the anticipated number of new playbooks to be developed per year during the maintenance period?	shared in the RFP, based on which the estimates may be made.
6	11	3.B	8	DPDP Compliance Module: The RFP mentions an "Out-of-the-box DPDP compliance module" for SOAR. Could you please elaborate on the specific functionalities and reports expected from this module? Is this a reference to standard reporting capabilities mapped to DPDP requirements or a dedicated, certified module?	The claused would be re-phrased in the amended RFP as - "Provide compliance reporting and monitoring content packs for major regulations (e.g., GDPR, PCI DSS, HIPAA, SOX, ISO27001), and enable extension/customization for emerging regulations such as DPDP"
7	21	8	-	Commercials for Scalability: The financial format requests pro-rata charges for incremental SIEM EPS and devices. For future scalability, will the pricing for all other components (e.g.,	No. The pricing for other components need not be considered.

Sr. No	Page No.	Section No.	Clause No.	Reference/ Subject Clarification Sought	IIBX Response
				additional SOAR users, TIP feed capacity, etc.) also be based on a pre-agreed pro-rata basis? If so, should we provide a rate card for all scalable components?	
8	14	3.D	7	Onsite vs. Remote Resources: The RFP states a requirement to "Provide remote L1, L2, L3 SOC analysts...". Please confirm that no onsite presence of these resources is required at the IIBX Data Centre at any point during the contract, including during critical incidents or audits.	If remote resource is not able to monitor & take action remotely due to any incident, then onsite support will be required. For Audit purpose, onsite support may be required.
9	15, 21	4.A, 8	-	SOAR User License Scalability: The RFP specifies a requirement for a minimum of 2 concurrent SOAR users. While the solution must be scalable, the financial bid does not request pro-rata pricing for additional users. Could you please clarify the commercial model for adding more concurrent SOAR users in the future? Should we provide	No. The pricing for additional concurrent SOAR users not be considered at this stage.

Sr. No	Page No.	Section No.	Clause No.	Reference/ Subject Clarification Sought	IIBX Response
				this as part of a rate card?	
10			General	Kindly mention the Payment Terms for the project	The payment will be linked to Delivery and implementation milestones. Post Implementation, the payment for MSSP would be on Quarterly advance basis.
11			General	Kindly mention the Project Timelines for the entire project	The Bidder should propose.
12	19	7	3	Kindly consider the similar solutions implementations by the bidder from BFSI, PSU, State/Central Govt and Enterprise sector	The clause cannot be modified.
13	21	8	1	Can we propose the tools and security services licensed on Bidder Name as a shared Managed Security Services from the Bidder SOC	No.
14	21	8	1	Hosting of Tool is required at Customer premises or it can be hosted on Bidder SOC premises with dedicated instance	Hosting of SOC Solution will be at IIBX Premises.
15	21	8	1	All the OEM may not offer perpetual license from SOC, Kindly request to change for annual subscription model	The Licensing needs to be perpetual.

RESPONSE TO QUERY SET – 7

Sr. No.	Page No	Section	RFP Clause Point	Response : Comment / Clarification	IIBX Response
1	6	2. Log Collection & Data Handling	Build parsers automatically; custom parsers editable in GUI without CLI.	This point is favouring a specific OEM, for wider participation requesting you to modify this point as, Request to re-phrase / ammend as Build parsers automatically / provide parser development framework; custom parsers editable in the framework GUI without CLI.	Suggestion Accepted. The clause would be re-phrased in the amended RFP as - "The solution must support automatic parser generation and provide a parser development framework. The framework should allow customization and editing of parsers through a graphical user interface (GUI), without requiring command-line interface (CLI) operations."
2	7	2. Log Collection & Data Handling	Provide built-in forensic investigation tools (OSQUERY, remote queries, baseline comparisons).	This point is favouring a specific OEM, for wider participation requesting you to modify this point as, Request to re-phrase / ammend as Provide forensic investigation through remote search, threat hunting, and baseline comparison features, with	Suggestion Accepted. The clause would be re-phrased in the amended RFP as - "The solution should provide built-in forensic investigation capabilities, including support for remote queries, system state analysis, and baseline comparisons."

Sr. No.	Page No	Section	RFP Clause Point	Response : Comment / Clarification	IIBX Response
				integration options for external tools	
3	8	5. Incident, Case & Response Management	Support false positive detection (CVE-based IPS analysis, IOC validation) and automated incident resolution recommendations via ML.	This point is favouring a specific OEM, for wider participation requesting you to modify this point as, Request to re-phrase / ammend as Support false positive reduction through CVE-based IPS analysis, IOC validation, and ML-driven risk scoring, with automated response actions and playbook-guided recommendations via SOAR.	This requirement is not vendor-specific. It's a functional requirement / capability statement. Cannot be amended.
4	8	6. Compliance, Dashboards & Reporting	Out-of-the-box compliance reports at no extra cost.	Request to re-phrase / ammend as Provide out-of-the-box compliance reports and regulatory content packs (e.g., PCI DSS, HIPAA, GDPR, SOX), with	The clause would be re-phrased in the amended RFP as- "The solution should provide out-of-the-box compliance and regulatory reports as part of the standard offering, without additional licensing or cost".

Sr. No.	Page No	Section	RFP Clause Point	Response : Comment / Clarification	IIBX Response
				updates maintained regularly. Licensing may apply depending on compliance frameworks required.	
5	9	1. General Solution Requirements	Accept security alerts from all data sources in any format, supporting unlimited alerts/incidents and unlimited action executions without license limits.	Request to re-phrase / ammend as The soultion should accept alerts from ArcSight SIEM, with flexible playbook-driven response actions and scalable action execution capacity, without license limits	It's a functional requirement / capability statement. Cannot be amended.
6	10	3. Connectors & Integrations	Offer user-friendly data ingestion wizards and remote SOAR agents for segmented networks	Request to re-phrase / ammend as Provide data ingestion for log sources, and support secure integration with systems in segmented networks through API-based	It's a functional requirement / capability statement. Cannot be amended.

Sr. No.	Page No	Section	RFP Clause Point	Response : Comment / Clarification	IIBX Response
			with auto-upgrade capability.	connections, with centralized upgrade and management of integrations.	
7	10	4. Indicators & Threat Intelligence	Include a vendor-neutral Threat Intelligence Platform (TIP) with one native OEM feed (CTA member) and support for multiple sources/formats (JSON, XML, STIX, free text) with TAXII export.	This point is favouring a specific OEM, for wider participation requesting you to modify this point as, Request to re-phrase / ammend as Integrate with a vendor-neutral Threat Intelligence Platform (TIP), supporting ingestion of multiple feed formats (JSON, XML, STIX, free text) and TAXII export, with at least one native OEM threat feed available.	The clause would be re-phrased in the amended RFP as - "The solution should include a vendor-neutral Threat Intelligence Platform (TIP) that provides at least one built-in OEM threat feed (preferably from a Cyber Threat Alliance member) and supports ingestion of multiple threat intelligence sources and formats (e.g., JSON, XML, STIX, free text), along with TAXII-based export for integration with external systems"
8	10	4. Indicators & Threat Intelligence	Support custom tagging/ scoring of indicators and native integration for running	This point is favouring a specific OEM, for wider participation requesting you to modify this point as, Request to re-phrase /	This is not vendor specific requirement. It's a functional / capability statement. Cannot be amended.

Sr. No.	Page No	Section	RFP Clause Point	Response : Comment / Clarification	IIBX Response
			multiple custom playbooks from TIP.	ammend as The solution should support custom tagging and scoring of indicators, and enable native integration with Threat Intelligence Platforms (TIPs) to trigger and run multiple custom playbooks	
9	11	5. Audit Trails & Logging	Support log forwarding to syslog/SIEM (Fortinet, Splunk, Microsoft, QRadar, etc.) and ingestion from multiple SIEM sources.	This point is favouring a specific OEMs ((Fortinet, Splunk, Microsoft, QRadar, etc.), for wider participation requesting you to modify this point as, Request to re-phrase / ammend as Support forwarding of alerts and cases to third-party SIEM platforms via Syslog/CEF, and integrate with multiple SIEMs at the alert/case level.	The clause would be re-phrased in the amended RFP as -"The solution should support bidirectional integration with SIEM platforms, including the ability to forward logs/events to external systems via standard protocols (e.g., syslog/CEF) and ingest data from multiple SIEM sources"

Sr. No.	Page No	Section	RFP Clause Point	Response : Comment / Clarification	IIBX Response
10	11	8. Security, Compliance & Authentication	Out-of-the-box DPDP compliance module for SOC operations.	Request to re-phrase / ammend as Provide compliance reporting and monitoring content packs for major regulations (e.g., GDPR, PCI DSS, HIPAA, SOX, ISO27001), and enable extension/customization for emerging regulations such as DPDP	Suggestion Accepted. The claused would be re-phrased in the amended RFP as - "Provide compliance reporting and monitoring content packs for major regulations (e.g., GDPR, PCI DSS, HIPAA, SOX, ISO27001), and enable extension/customization for emerging regulations such as DPDP"
11	11	9. AI & Automation Features	Include bots for automated threat investigation.	Request to re-phrase / ammend as Include automation capabilities to support threat investigation, using playbooks, scripts, and integrations to enrich alerts, validate IOCs, and recommend or execute response actions.	It's a functional requirement / capability statement. Cannot be amended.

RESPONSE TO QUERY SET – 8

Sr. No.	Page No	Section (Name & No.)	Statement as per tender document	Query by bidder	IIBX Response
1	12	3.C. THREAT INTELLIGENCE PLATFORM (TIP)		Threat intelligence platform to be required from same OEM as SIEM & SOAR? Or any other OEM leading OEM's can collobrate	TIP should be from same OEM of SIEM & SOAR. Threat Feed can be from Multiple providers.
2	6	3.A.1.	Multi-tenant by default for departmental data segregation and analytics	Do we need multitannet architcture for SIEM solution or just multiple site need to be integarted into the SIEM solution?	This clause shall be removed in the amended RFP.
3	7	3.A.4	Integrate with Generative AI (e.g., OpenAI/ChatGPT 4.0) for: o SOC health queries o Risk predictions o Report creation from aggregation /raw queries o Case analysis and enrichment o Incident response guidance based on	integration with Open AI required out of the box or can be integarted with customized connector to answer the specific quiries	IIBX prefers native Gen AI which would fall in the responsibility of the bidder.

Sr. No.	Page No	Section (Name & No.)	Statement as per tender document	Query by bidder	IIBX Response
			threat category		
4	8	3.A.6	There shall be a live timer on the dashboard that shows SLA time remaining for each milestone for the analyst to keep a track of live incidents.	SLA timer shuld be in count douwn fashion for each incident or spcific timer for critical, High, medium shuld be okay.	SLA timer for Critical, High, Medium should be okay.
5	9	3.B.1	SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	SOAR required to be from the same OEM as SIEM or collobration with other SIEM is okay	SOAR required to be from same OEM as SIEM.
6	10	3.A.	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	Full fledge UEBA with anytices shuld be required as part of curent RFP if yes what is the license required for UEBA.	Bundle license is prefered.
7	17	5	Bidder must be CERT-In empanelled.	Can be given exemption for the MSME registered vendor or Selected bidder needs to submit the Cert-In Empanelled confirmation within 10 months of the project awarded.	Must be CERT-In Empanelled.

RESPONSE TO QUERY SET – 9

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
1	13.0	7. Resource Management	Provide remote L1, L2, L3 SOC analysts, SOC manager, and platform administrators for 24x7x365 operations	Please confirm whether the resources are expected to be dedicated exclusively to the IIBX 's SOC or can be shared across multiple MSSP engagements	Can be shared.
2	13.0	7. Resource Management	Provide remote L1, L2, L3 SOC analysts, SOC manager, and platform administrators for 24x7x365 operations	Kindly clarify the minimum team size expected per shift (L1, L2, L3 analysts, SOC manager, platform administrators).	Bidder should propose the team size to support the operations smoothly.
3	13.0	7. Resource Management	Provide remote L1, L2, L3 SOC analysts, SOC manager, and platform administrators for 24x7x365 operations	For platform administrators, please confirm if these are to be permanent staff for continuous monitoring or on-demand resources for platform upgrades, patches, and troubleshooting.	On-demand
4	5.0	A. SECURITY INFORMA	Provide scale-out distributed	Please clarify that the SIEM solution	It will deploy in DC with HA and also deploy at DR without

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
		TION AND EVENT MANAGEMENT (SIEM	architecture with collectors (virtual or physical appliances) that can cache logs if the storage/correlation tier is unavailable, compress logs before sending, and limit bandwidth usag	should be deployed in only DC or it will deploy in DC & DR both with HA capablity in IIBX data center.	HA with automatic failover
5	7.0	5. Incident, Case & Response Management	Provide built-in case/ticketing system or integrate with tools like ServiceNow, Service Desk Plus (Manage Engine), ConnectWise, Remedy	Please clarify whether IIBX has any ticketing solution or not and if yes please share the name of the ticketing tool	Yes, we have Manage Engine Service Desk Plus.
6	8.0	B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	Option 1 – Subset Model: SOAR deployed as part of the Managed Service Provider (MSSP) platform under a Master Controller at the MSSP's	please confirm whether the IIBX expects licensing, hardware, and platform costs to be borne by the MSSP or factored into the proposal pricing.	Yes

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
			premise, integrated with MSSP services.		
7	8.0	B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	Option 2 - (Dedicated Instance) SOAR deployed as a dedicated tenant on the IIBX environment. If IIBX opts for this option, no connectivity except remote access for configuration will be provided to the MSSP cloud.	please confirm whether the IIBX will provide the required infrastructure (compute, storage, and network resources) for hosting the dedicated SOAR instance, or whether the bidder is expected to provision and quote for these.	The indicative infrastructure hardware cost & configuration for implementing the solution needs to be shared by bidder. IIBX will provide requried Infrastructure
8	8.0	B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	Option 1 – Subset Model: SOAR deployed as part of the Managed Service Provider (MSSP) platform under a Master Controller at the MSSP's premise, integrated with MSSP services.Option 2 - (Dedicated	Please clarify if the scope of integration with third-party tools (SIEM, ITSM, threat intel, etc.) remains identical in both deployment models	Yes

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
			Instance) SOAR deployed as a dedicated tenant on the IIBX environment. If IIBX opts for this option, no connectivity except remote access for configuration will be provided to the MSSP cloud.		
9	8.0	B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	Must be an on-premises solution, scalable in use cases and performance to ensure quick response to attacks.	Please confirm if the MSSP-hosted subset model (Option 1) also needs to comply with HA and DR requirements, or if this is only applicable to the Dedicated Instance model.	Applicable to both.
10	8.0	B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	HA and automatic failover with DR Support	Please specify if the client expects an active-active or active-passive HA architecture for the proposed solution.	Active-Passive

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
11	8.0	B. SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR)	HA and automatic failover with DR Support	For DR, please clarify if the client will provide a secondary DR site, or if the bidder is expected to propose and provision DR infrastructure as part of Option 1	IIBX will provide a secondary DR site
12	12.0	D. REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE	MSSP to assign a dedicated project team to plan, install, configure, conduct UAT, and move SOC technologies to production	Please confirm whether the dedicated project team is expected to be deployed onsite at IIBX premises or if a remote project management team will be acceptable.	Remote Poject Management Team will be acceptable.
13	12.0	D. REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE	MSSP to assign a dedicated project team to plan, install, configure, conduct UAT, and move SOC technologies to production	For UAT and production sign-off, kindly confirm the success criteria (e.g., rule hits, incident generation, dashboard availability, log coverage) that must be met before final acceptance.	Can be decided subsequently.

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
14	12.0	D. REQUIREMENTS FOR IMPLEMENTATION & MAINTENANCE	MSSP to assign a dedicated project team to plan, install, configure, conduct UAT, and move SOC technologies to production	Kindly clarify the composition of the project team expected from MSSP (e.g., Project Manager, Solution Architect, Implementation Engineers, SOC Consultants).	Bidder to propose.
15	12.0	2. SIEM & SOAR Setup and Customization	Unlimited custom log parser development for any proprietary or legacy format.	The requirement mentions "unlimited custom log parser development". Please confirm if the expectation is for MSSP to develop parsers on demand throughout the contract period, or only during the initial deployment phase.	The expectation is from MSSP to develop parsers on demand throughout the contract period.
16	12.0	2. SIEM & SOAR Setup and Customization	Integration of non-standard log sources (text files, custom APIs).	Please confirm the types of non-standard log sources (e.g., flat text files, syslog variations, APIs) that	This is a generic requirement.

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
				must be supported.	
17	12.0	2. SIEM & SOAR Setup and Customization	Integration of non-standard log sources (text files, custom APIs).	Is the MSSP expected to provide continuous support for onboarding new non-standard sources during the entire contract period?	Yes
18	12.0	2. SIEM & SOAR Setup and Customization	Create custom connectors for unsupported tool	Please clarify the scope for "custom connectors for unsupported tools." and please confirm whether IIBX will provide API/SDK documentation for such tools	This is a generic requirement. IIBX will provide API/SDK as required.
19	13.0	3. Threat Monitoring, Detection & Hunting	Threat feed integration, including CERT-In, with real-time alert enrichment from external feeds.	Please confirm if CERT-In threat feeds will be made available directly by IIBX	Yes, IIBX has subscribed CERT-In's threat intelligence feed.
20	13.0	Incident Response & Forensics	Perform digital forensics and support investigation activities.	Kindly confirm whether the forensic tools and licenses (e.g., EnCase,	Bidder's Scope

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
				FTK, Volatility) will be provided by IIBX or are expected to be included in the bidder's scope.	
21	13.0	Incident Response & Forensics	Facilitate DR & BCP tabletop exercises.	Please clarify the expected frequency of Disaster Recovery & Business Continuity tabletop exercises (e.g., quarterly, half-yearly, annually) and the extent of bidder's involvement (design, execution, or only support)	Quarterly
22	11.0	C. THREAT INTELLIGENCE PLATFORM (TIP)	Must be an on-premises solution with details of required hardware infrastructure and storage provided.	Kindly confirm whether the TIP solution should require cloud base or on premise	On Premise
23	17.0	ELIGIBILITY CRITERIA	Work Experience: - The bidder / supplier should have a minimum of Five year of	Since this bid will be Submitted by SDSL (SIFY Digital Services Ltd) which is	You may specify this while submitting the bid for consideration.

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
			experience in supply of SIEM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc	hived out of its parent company i.e SIFY Technologies LTD, as wholly owned subsidary, request you to add the below clause to comply with Eligibility and Technical Scoring parameters: "In case the bidding company/ firm is hived off from the demerged company, the experience, eligibility etc. as per the requirement of the RFP may be considered as of the demerged company, provided the demerged company doesn't apply in the same RFP process and Novation / Other Relevant	

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
				Agreement is in place. In that case, Relevant Novation / Other Relevant Agreement need to be submitted. " The same has been added in multiple other PSU, Banks & Government RFP's that we participated.	
24	19.0	TECHNICAL BID & SCORING FORMAT	Total number of similar Solutions implemented by the Bidder by BFSI	The count for total implementations seem to be too high, request to change it as per below for scoring marks : More than 10 – 10 marks More than 7 – 8 marks Upto 5 – 0	This clause cannot be amended.
25		Others	Others	How do we submit our bids, is it through Email / Hardcopy / Through a submission portal. The mode of submission of	Please fefer to last page of RFP - Section 12 - Submission Details, which states in last line - All queries and proposals may be emailed to ProcurementcommitteeIIBX@iibx.co.in.

Sr No.	Page No.	Section	Contents	Remark	IIBX Response
				proposal is not clear. Similarly, once qualified how do we submit our commercial bid, is it through Email / Hardcopy / Through a submission portal	

RESPONSE TO QUERY SET – 10

Sr No.	Eligibility Criteria	Document Required	Remark	IIBX Response
1	Bidder must be CERT-In empanelled.	Confirmation letter from CERT-In with valid expiry date.	Please remove it as a mandatory requirement or consider consortium with experience of lead bidder as we have deployed solution in consortium	IIBX prefers a single entity as a point of contact even if the deployment is done by a consortium. The single entity acting as bidder for IIBX must have the CERT-in empanelment.
2	Work Experience: - The bidder / supplier should have a minimum of Five year of experience in supply of SIEM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc	Copies of the purchase orders from the organization shall be submitted	Please consider consortium with experience of lead bidder as we have deployed solution in consortium	IIBX prefers a single entity as a point of contact even if the deployment is done by a consortium. The single entity acting as bidder for IIBX must have the prescribed work experience.