Sri Lanka CERT (Pvt) Ltd.

PREBID MEETING MINUTES

(CLARIFICATIONS 01 TO THE QUERIES)

FOR THE

Procurement of Cyber Threat Intelligence and Attack Surface Management Solution for Malware Analysis and Threat Hunting Lab

INVITATION FOR BIDS No: CERT/GOSL/SER/ICB/2026/08

International Competitive Bidding (ICB)

Date and Time of the Pre-bid meeting : 21st July 2026 (10.00 AM)

July, 2026

CLARIFICATIONS TO THE QUERIES

Set 01

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section II. Bidding Data Sheet → ITB 10.5 → Pg. No. 38	What is the deadline for submitting requests for clarification, and when will the responses / addendum be published?	Requests for clarification must reach the Employer on or before 1500hrs (Sri Lankan Time) on 23rd July 2026. Clarifications and any resulting addendum will be published on or before 30th July 2026 via the SL CERT procurement portal (https://www.cert.gov.lk/procurements).
2	Section II. Bidding Data Sheet → ITB 26.1 → Pg. No. 41	Can the bid submission deadline be extended?	No extension will be granted. Bids must be submitted on or before 1400hrs (Sri Lanka Time) on 13th August 2026; late bids will be rejected. Bidders are advised to ensure submissions are complete and accompanied by all valid required documents (e.g., ISO certification, OEM authorization, Bid Security).
3	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Can the list of the 250 organizations / tenants, and their domains and subdomains, be shared to enable accurate sizing of the solution?	The list of organizations (subject to change based on the purchaser discretion) are shared in the Sr. No. 1 of Addendum 01. Domains and subdomains will not be disclosed prior to award.
4	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.2 → Pg. No. 115	Is one 'organization' equal to one domain, or can it include multiple domains / subdomains?	An organization may comprise multiple domains and subdomains. All domains / subdomains belonging to a single organization are counted as one (01) organization, not as separate organizations.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
			Example: cert.gov.lk and onlinesafety.lk together constitute one organization.
5	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1 → Pg. No. 96	What is the approximate asset volume per tenant, and in total, to size the EASM component?	Asset counts depend on each solution's definition of an 'asset' (domain, subdomain, IP, cloud bucket, etc.). Assets may be anticipated across the 250 tenants when such elements are counted separately.
6	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5 → Pg. No. 88	Can a ballpark figure be given for expansion beyond 250 organizations?	No fixed figure is specified. The platform must be scalable and support license allocation for expansion beyond 250 organizations. Future phases may include commercial entities (e.g., banks, universities).
7	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.2 → Pg. No. 101	Why is the historical look-back period set at 5 years rather than 7 or 10?	Five (05) years is set as a minimum baseline to ensure fair and broad competition. It is a minimum requirement; a longer historical look-back is acceptable and will be considered a value addition.
8	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 → Pg. No. 95,96	Investigation credits are allocated per calendar month (min. 5 per child). Can allocation instead be on an annual (×12) basis? Also, what is the definition of an 'investigation'?	Allocation of investigation credits on an annual basis is allowed. (Refer the Sr. No. 2 of Addendum 01) An 'investigation' means any analyst-initiated deep-dive analysis (including threat hunting, malware analysis, data-leak / breach investigation, and similar).
9	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.12 → Pg. No. 107	Is the 'unlimited keyword configuration' requirement mandatory? A defined count (e.g., 5 per tenant) plus ad-hoc search is recommended to control pricing and false positives.	Number of keyword configuration requirement is set to minimum 50 per custom search. (Refer the Sr. No. 3 of Addendum 01)

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
10	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.7 → Pg. No. 106,107	Does the platform require live in-platform dark-web browsing, or is analyst access to cached artifacts (posts, images, thread context) sufficient?	Either approach is acceptable: (i) safe in-platform dark-web browsing (e.g., routed through the platform's proxy so analyst systems are not exposed to direct .onion connections); or (ii) analyst access to dark-web source posts, images and thread context cached / collected within the platform. (Sr. No. 4 of Addendum 01)
11	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.6 → Pg. No. 110	Is there an upper limit on the number of files for sandbox / malware analysis during the contract?	No fixed file count is specified. The requirement is a sandbox-based malware analysis capability applied to malware identified or received by the MATH Lab.
12	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.5 → Pg. No. 109	Are the workflows / playbooks executed by an internal or external team?	Operational playbooks and hunt workflows are executed by the Sri Lanka CERT MATH Lab team.
13	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.2 → Pg. No. 111 Section IV. Bidding Forms → 4.11 → Price Schedules → 4 → Pg. No. 76 & 77	What is the absolute number of takedowns, and is it per tenant or aggregate?	The number of takedowns required during the one-year subscription is 250 in aggregate.
14	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 7.2 → Pg. No. 125,126,127,128,129	Take-down resolution depends on third parties (Meta, TikTok, LinkedIn, hosting providers). Should the response / resolution-time penalty SLAs apply to take-downs? Should resolution time relate only to platform availability?	Takedown response and resolution times shall be as specified in Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement (SLA) → 6.5 & 6.6. (Refer the Sr. No. 5 of Addendum 01)

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.3 → Pg. No. 111		Severity level of Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.3 is classified as TP1, TP2, TP3 & TP4. (Refer the Sr. No. 6 of Addendum 01)
15	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 → Pg. No. 118	MCP is a transport protocol and does not itself consume tokens; the 'minimum context window of 200,000 tokens' is therefore inaccurate as an MCP attribute. Is 200,000 a per-day figure?	Refer the Sr. No. 7 of Addendum 01
16	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.4 → Pg. No. 113	Is MCP intended as the primary report-generation method, or should the platform generate reports natively?	The platform must provide native, standard reporting through the platform. MCP / AI-assisted report generation is intended to provide flexible report generation in the Purchaser's preferred formats, with minimal dependency on the OEM / local partner. Both native and MCP-assisted generation are required; bidders may propose suitable report formats.
17	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4 → Pg. No. 117	Is there a minimum API query volume, and how many integrations are envisaged?	Bidders must disclose the maximum API query volume per minute and per day; undisclosed throttling that materially reduces functionality is a contractual breach. Required integrations include the ELK SIEM and OpenCTI; approximately two (02) integrations are envisaged, supporting both push and pull mechanisms.
18	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1 → Pg. No. 116	Clause 2.1 requires 10 concurrent users at Parent level with 'no hard cap on user accounts per Child Tenant'. Are these named or concurrent users, and can a defined floating pool be provided instead?	The ten (10) concurrent authenticated users at Parent-Tenant level are the MATH Lab analysts with global visibility across all tenants. (Refer the Sr. No. 8 of Addendum 01)

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
19	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → 1 → Pg. No. 83	Must all 250 tenants be provisioned at the outset, or is phased onboarding permitted?	All 250 Child Tenants must be on boarded within 30 days of the Date of Award. No phased onboarding is permitted.
20	Section III. Evaluation and Qualification Criteria → Table 3.3.1 – Evaluation Components and Marking Scheme → 1 → Pg. No. 46	What is the expected volume for the 15-minute self-service tenant add / remove, and does it apply to all products?	The 15-minute self-service add / remove applies universally across all platform components. The requirement is to instantiate or remove an individual tenant as operationally required.
21	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3 → Pg. No. 88	Is an on-premises deployment expected, or is a SaaS solution acceptable?	The proposed solution shall be implemented as a SaaS solution, as specified.
22	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → 7 → Pg. No. 85	What data can be exported and what must be deleted at exit, including audit trails?	On contract expiry, termination or non-renewal, the bidder shall export all Purchaser and Child-Tenant data (including alerts and asset records) in open formats, and thereafter permanently delete all data from production systems, backups, DR copies and sub-processor systems, providing written deletion certification within 5 business days of confirmed export.
23	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3, 4 → Pg. No. 54	Can the 'similar / specific experience' requirement be met through the OEM's experience rather than the bidder's?	Yes. As per the Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3, 4 → Pg. No. 54

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
24	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3, 4 → Pg. No. 54,55	Clarify the specific-experience client counts and which forms apply; and please provide the forms in editable (MS Word) format.	Forms 4.6.1–4.6.4 correspond to CTI (20 clients), ASM (20 clients), Deep & Dark Web Monitoring (20 clients) and multitenant environment (05 clients). The same client references may be used to satisfy more than one criterion where applicable. Editable soft-copy (Word) forms (Section 4) will be provided to bidders who have purchased the bidding document.
25	Section IV. Bidding Forms → Table 4.5 → 3.7.5, 3.7.6.1 – 3.7.6.4 → Pg. No. 65 - 71	The reference forms require e-mail and telephone contact details for 20 clients; NDAs frequently prevent this. May fewer references be provided, with reference calls arranged on request?	Clause remains same. Comply to the original requirement.
26	Section II. Bid Data Sheet → ITB 14.3 → Pg. No. 38,39	Is a prescribed format provided for the non-collusion affidavit, or may a legal format be used?	A prescribed format for the non-collusion affidavit will be issued. (Sr. No. 9 of Addendum 01)
27	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → 6,7 → Pg. No. 84	Can the payment for support (Milestone 6) and migration / data-deletion (Milestone 7) be brought within the 12-month contract period?	Clause remains same. Comply to the original requirement.
28	Section III. Evaluation and Qualification Criteria → Table 3.3 – Detailed Evaluation of Technical Bids → Pg. No. 45	When is the demonstration, what data is used, and who must present?	As per the Section III. Evaluation and Qualification Criteria → Table 3.3 – Detailed Evaluation of Technical Bids → Pg. No. 45 Five (05) common tenants will be named at demonstration time; synthetic data is permitted where a live tenant cannot demonstrate a given scenario.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
29	Section IV. Bidding Forms → Price Schedule Summary → Pg. No. 78	Is the evaluation for one year or for three years?.	The price evaluation will be done considering only 1 Year subscription Price as per Section IV. Bidding Forms → 4.11 Price Schedules → Price Schedule Break down and Price Schedule Summary → Pg. No. 76 & 77. Bidders may also quote pricing for Year 2 and Year 3, which may be exercised at the Purchaser's discretion to renew the contract, subject to satisfactory performance of the solution.
30	Section III. Evaluation and Qualification Criteria → 3.3 – Detailed Evaluation of Technical Bids → Pg. No. 45 Section VI. Schedule of Requirements → Pg. No. 82 to 132	Who qualifies for the demonstration, and how do demonstration and how do demonstration points feed the evaluation?	As mentioned in Section III. Evaluation and Qualification Criteria → 3.3 Detailed Evaluation of Technical Bids→ (a),(b) and (c) → Pg. No. 45 technically responsive bidder will be requested to do presentation to demonstrate the technical capabilities of the product. Technically responsive bidder must meet all the requirements stipulated in Section VI. Schedule of Requirements → Pg. No. 82 to 132.

Set 02

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section III. Evaluation and Qualification Criteria → Other Specific Requirements → 3.7.9 → Pg. No. 55	This requirement may please be removed as Attack Surface intelligence data is utilized for risk scoring of companies for use cases like Third Party risk monitoring by most OEMs.	Permitted for analytical and statistical purposes only, provided all organization-specific identifiers are anonymized. (Refer the Sr. No. 10 of Addendum 01)
2	Section III. Evaluation and Qualification Criteria → Other Specific Requirements → 3.7.10 → Pg. No. 55	This requirement may please be removed as this is internal information and cannot be shared due to ISO 27001 guidelines.	Clause remains same. Data residency and sub-processor restrictions remain mandatory. Comply to the original requirement.
3	Section VI. Schedule of Requirements → 4.2 Operational Manuals → Pg. No. 86	Please confirm if a hosted version of the Support documentation/operating manuals is acceptable instead of hard and soft copies. The online documentaon version is always up to date, readily searchable and handy for access.	Clause remains same. Comply to the original requirement. Online portals may be provided as an additional, but cannot replace the requirement.
4	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7 → Pg. No. 88	Do we need to provide dedicated resources to administer and manage the solution on behalf of SL CERT, or will Sri Lanka CERT manage it using their in-house resources? If we are required to provide resources, this will incur an additional cost on top of the platform license.	The bidder is required to provide a dedicated local support engineer available 24/7. However, administration of the platform will remain with CERT analysts.
5	Section VI. Schedule of Requirements → Table 7 –	SaaS solutions do not have follow a specific scheduled maintenance window. At best advance information regarding downtime or maintenance will be made available via status page/email.	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 1.2 → Pg. No. 92	Please confirm if this shall be acceptable. It is requested that the clause may be revised to "The platform shall maintain a monthly availability of 99.5% or higher."	
6	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.3 → Pg. No. 92,93	This following may be removed as each child tenant shall have its own aggregated metrics "The Parent Tenant shall have an aggregated read-only visibility view across all Child Tenants displaying consolidated statistics."	Clause remains same. Comply to the original requirement.
7	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.4 → Pg. No. 93	The customer will need to work with the assigned TAM or support team for any addition, removal or modification to Child Tenant. The asset discover and scanning will only be operational at the time of next scheduled scan as 15 mins is too small a window and shall lead to penalties. May please be modified as, "1.4 The Purchaser shall have full self-service capability to add, remove and modify Child Tenants configuration without any bidder involvement. Tenant additions and removals shall propagate and become fully operational including initial asset discovery and alert configuration within 15 minutes of the Purchaser's action (except for external attack surface monitoring wherein an engineer/TAM involvement may be required)."	Clause remains same. Comply to the original requirement.
8	Section VI. Schedule of Requirements → Table 7 –	May please be changed to "The platform/bidder team should maintain historical data of	Sr. No. 11 of Addendum 01

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 1.5 → Pg. No. 93	added/removed organization for persistent period of time during the subscription."	
9	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.7 → Pg. No. 93	Please confirm if the alert recipient will be among the platform admins only i.e. the users having logins to the platform or any additional users required for alerting.	Receipt of alerts will be applicable for users indicated in Sr. No 08 of Addendum 01
10	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.8 → Pg. No. 93,94	Please change as "1.8 Alert exports shall support a minimum of 10,000 records per export operation in each of the following formats: CSV OR JSON OR XLSX"	Sr. No. 12 of Addendum 01
11	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.11 → Pg. No. 94	Please suggest if this can be achieved via custom services from the bidder. If yes, may please be changed as "The platform/bidder shall provide a capability that allows the Purchaser to customize logos, headers, and footer text in all generated reports with the Purchaser's own branding. This configurationon shall be completed by the Bidder during deployment, before Operational Acceptance. The Purchaser shall be able to do customization without bidder involvement at any me."	Clause remains same. Comply to the original requirement.
12	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.12 → Pg. No. 94, 95	May please be deleted as not supported by many OEM platforms. The LLM generated reports may possibly used to achieve the required time stamp changes, similar to one asked in Section B clause 8.1	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
13	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.16 → Pg. No. 95	May please be changed as "The platform/bidder shall maintain logs related to user logins, watchlist related configuration changes etc. The alerts generated should capture information related to state change or historical information if any."	Clause remains same. Comply to the original requirement.
14	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.18 → Pg. No. 96	May please be deleted as not supported by many OEM platforms	Clause remains same. Comply to the original requirement.
15	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.8 → Pg. No. 99	May please be deleted as not supported by many OEM platforms	Sr. No. 15 of Addendum 01 is relevant
16	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.17 → Pg. No. 105	Please suggest if this is in scope of the Bidder onsite analysts	This is a shared responsibility between the Platform (automated correlation and enrichment) and the OEM/Bidder analysts (manual validation), working together to eliminate false positives.
17	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.3 → Pg. No. 106	May please be changed as: "Credential leak alerts and reports shall accurately indicate data elements such as usernames, passwords and URLs , End user PC details (if available) like Hostname, IP Address, AV present etc, date and time related to exposure, Malware that lead to the leakage etc (but not limited to)"	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
18	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.7 → Pg. No. 106,107	Please indicate the number of analysis per day or per month required for sandbox based analysis.	Clarification provided in Serial No. 11 of Set 01 is relevant
19	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.3 → Pg. No. 108	May be changed as "5.3 The platform/bidder must provide pre-build threat hunting packages/tools/facility."	Sr. No. 16 of Addendum 01 is relevant
20	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.6 → Pg. No. 110	Please suggest the various types sandbox environment for the sandbox e.g. Windows, Linux, Android, Mac	Minimum Windows, Linux, Android are required.
21	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.2 → Pg. No. 111	Please suggest if the scope of this clause can be limited to malicious sites only and not for trademark infringements. In case of trademark infringement cases the individual organizations may need to takedown directly. It is requested if the trademark infringement related takedowns may be kept beyond the scope.	Clause remains same. Comply to the original requirement.
22	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.1 → Pg. No. 112,113	Please suggest if this can be achieved via bidder onsite analysts.	Clause remains same. Comply to the original requirement.
23	Section VI. Schedule of Requirements → Table 7 –	Please change to "Upon onboarding a new Child Tenant, the platform/bidder shall initiate an intial asset	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 1.4 → Pg. No. 116	discovery scan and subsequent scan(s) should be without requiring any manual trigger by the Purchaser or the Bidder. Except for Attack Surface scan wherein an engineer/TAM involvement may be required"	
24	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1 → Pg. No. 116	Please suggest how many additional floatng numbers of users are needed beyond 10 users. Wil these users be CERT-SL employees or third pares belonging to the 250 monitored entities.	Sr. No 08 of Addendum 01 relevant
25	Section IV. Bidding Forms → Table 4.5 → 3.7.5, 3.7.6.1 – 3.7.6.4 → Pg. No. 65 - 71	Contract Name, Email, and Telephone are all confidential data and have PII (Personally Identifiable Informaon) related exposure aspects. This may be limited to the following information please and changed as: Brief Description of the Products/Services supplied by the Bidder: Name of Employer: Address: To facilitate verification, a direct phone call can be arranged with the references by the OEM/Bidder, subject to the customer's availability.	Clause remains same. Comply to the original requirement.
26	Section IV. Bidding Forms → 4.6 Specific Experience → Pg. No. 66	Contract values of previous customers are strictly confidential and protected under Non-Disclosure Agreements (NDAs). Therefore, the Bidder cannot disclose specific monetary figures.	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		It is requested that this requirement be modified to allow the Bidder to demonstrate project scale using one of the following methods: Option A: Indicang value bands (e.g., "Project value between $100,000 – $200,000" or "Above $100,000"). Option B: Confirming that the contract value exceeds a specific minimum threshold required for this RFP (e.g., "Contract value is greater than the required annual turnover threshold"). Option C: Providing a percentage range relative to the current project's esmated budget. Please confirm if providing project scale via value bands or threshold confirmation is acceptable.	
27	New Clause	Suggested additional specifications for Malware analysis platform requirement	Specification with regards to the Malware Analysis is as stipulated in Page No. 110 and 111 of RFP.
28	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.2 → Pg. No. 125,126	May please be changed to ≤ 30 minutes (24×7×365) as the asked response time is too aggressive.	Clause remains same. Comply to the original requirement.
29	Section VI. Schedule of Requirements → General	May please be changed as asked response time is too aggressive and Resolution time may vary on	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Warranty Terms & Service Level Agreement (SLA) → 6.3 → Pg. No. 127,128,129	case to case basis. Also most OEMs may not agree to the aggressive resolution timelines. May be changed as Max Resolution Time : "Provide relief to the Customer within twenty-four (24) business hours and provide a Fix within seven (7) business days"	However, Resolution times for takedown service as provisioned in Sr. No. 5 of Addendum 01
30	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.3 P1 Critical→ Pg. No. 127	May please be changed as asked response me is too aggressive and Resolution time may vary on case to case basis. Also most OEMs may not agree to the aggressive resolution timelines. May be changed as Max Resolution Time : "Provide relief to the Customer within twenty-four (24) business hours and provide a Fix within seven (7) business days"	Clause remains same. Comply to the original requirement. However, Resolution times for takedown service as provisioned in Sr. No. 5 of Addendum 01
31	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.3 P2 High → Pg. No. 127,128	May please be changed as asked response me is too aggressive and Resolution time may vary on case to case basis. Also most OEMs may not agree to the aggressive resolution timelines. May be changed as Max Resolution Time : "Within seven (7) business days"	Clause remains same. Comply to the original requirement. However, Resolution times for takedown service as provisioned in Sr. No. 5 of Addendum 01
32	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.3 P2 Medium → Pg. No. 128,129	May please be changed as asked response me is too aggressive and Resolution time may vary on case to case basis. Also most OEMs may not agree to the aggressive resolution timelines. May be changed as Max Resolution Time : "Within seven (7) business days"	Clause remains same. Comply to the original requirement. However, Resolution times for takedown service as provisioned in Sr. No. 5 of Addendum 01

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
33	Section II. Bidding Data Sheet → ITB 14.3 → Pg. No. 38	Please share the format	A prescribed format for the non-collusion affidavit as per Sr. No. 9 of Addendum 01
34	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.5, 3.7.6.1, 2, 3, 4 → Pg. No. 54	Need clarity on Form 4.5 and 4.6 mapping to Pg, 54 sections	Form 4.5 → Page 65 of RFP Form 4.6.1 → Page 68 of RFP Form 4.6.2 → Page 69 of RFP Form 4.6.3 → Page 70 of RFP Form 4.6.4 → Page 71 of RFP
35	Section IV Bidding Forms → Pg. No. 58 to 80	Please share the softcopy of the Section IV	Clarification provided in Serial No. 24 of Set 01 is relevant
36	Section III. Evaluation and Qualification Criteria → Detailed Evaluation of Technical Bids → Pg. No. 45	Please confirm the final weightage of the Commercial and Technical evaluation including the Demonstration up until LOA issuance.	Page Nos. 45 to 50 of RFP is relevant

Set 03

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.6 → Pg. No. 98	Kindly remove OWASP Top Vulnerability scanning requirements (cross-site scripting (XSS), SQL injection, default or unauthenticated access, remote code execution) from this clause. Platform is designed for outside-in attack surface discovery and passive vulnerability identification, not authenticated web-application penetration testing. OWASP Top 10 web vulnerability detection is typically delivered by dedicated DAST / SAST or WAF-tier solutions such as Acunetix, Invicti, Rapid7 InsightAppSec, or Burp Suite.	Sri Lanka CERT clarifies the underlying scope concern: Clause 2.6 must be read together with Section VI. Schedule of Requirements → Table 7 - Technical Specification → 2.5 → Pg. No. 97,98, which frames this detection as occurring through "active and passive reconnaissance" for external exposure discovery i.e., an outside-in EASM model. The Purchaser is not requiring authenticated web-application penetration testing, credentialed scanning, or a dedicated DAST/SAST engine. Detection of RCE, XSS, SQL injection, and default/unauthenticated access is expected through unauthenticated, non-intrusive external probing e.g., identifying vulnerable/unpatched components, exposed admin panels, default credentials, and known misconfigurations that expose these vulnerability classes to an outside attacker consistent with how EASM/ASM platforms typically surface such exposures without full application-layer exploitation.
2	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1 → Pg. No. 96,97	Kindly remove Mobile Application scanning as a requirement for ASM. Platform (EASM) is focused on domain/IP/cloud/certificate/technology-layer attack surface discovery. Native mobile application code analysis, permissions review, and mobile app store presence scanning are typically delivered by Mobile Application Security Testing (MAST) tools or Digital Risk Protection (DRP) modules. Platform DRP (proposed under Item #4 Takedowns) covers mobile app impersonation	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		detection and takedowns on Google Play / Apple App Store, but SAST/MAST scanning of the mobile app package (APK/IPA) itself is outside the scope of an EASM platform.	
3	Section IV. Bidding Forms → 4.11 → Price Schedules → 1 → Pg. No. 76	Kindly consider revising to 'Unlimited users per tenant'. Platform Threat Intelligence provides unlimited authenticated user accounts per Branch (tenant) by default — there is no per-user licensing model in Platform's URP platform.	Discrepancy in the RFP Reference Cited by the Bidder in the Query
4	Section IV. Bidding Forms → 4.11 → Price Schedules → 2 → Pg. No. 76	Kindly consider revising to 'Unlimited users per tenant'. Platform Attack Surface Management provides unlimited authenticated user accounts per Branch (tenant) by default.	Discrepancy in the RFP Reference Cited by the Bidder in the Query
5	Section IV. Bidding Forms → 4.11 → Price Schedules → 3 → Pg. No. 76	Kindly consider revising to 'Unlimited users per tenant'. Platform Deep & Dark Web Monitoring is delivered as part of the Platform TI platform with unlimited users per Branch.	Discrepancy in the RFP Reference Cited by the Bidder in the Query
6	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → 7 → Pg. No. 85	Please confirm that this clause is applicable ONLY to Attack Surface Management (ASM) data (i.e., asset inventory, vulnerabilities, exposure findings collected specifically for the Purchaser and Child Tenants). Threat Intelligence and Deep & Dark Web feed data is aggregated, non-tenant-specific intelligence produced by Platform globally from multiple sources — this cannot be 'exported and deleted' as it is not customer-specific data.	Clarification provided in Serial No. 22 of Set 01 is relevant
7	Section VI. Schedule of Requirements → Table 7 –	Please share the estimated count of assets (primary domains + subdomains + IPs + cloud storage + APIs + mobile apps + email infrastructure) per	Clarification provided in Serial No. 12 of Set 12 is relevant

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 12 → Pg. No. 89	tenant. This is essential for accurate ASM licensing and platform sizing. Without asset count clarity, commercials cannot be finalised.	
8	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.7 → Pg. No. 106,107	Kindly remove 'sandboxed dark web browsing within platform' from this clause. Platform provides direct access to dark web content (posts, messages, screenshots) via its portal without requiring an in-browser sandbox — this is safer than an in-platform browser as analysts view captured content rather than actively browsing dark web sites. In-platform sandboxed browsing is a niche feature not offered by most leading TI vendors including Platform, Recorded Future, Mandiant, and CrowdStrike.	Sr. No. 4 of Addendum 01 is relevant
9	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.3 → Pg. No. 115,116	Kindly consider revising to: 'Self-service Child Tenant management (add / remove / modify) shall be supported for Attack Surface Management (ASM) and Digital Risk Protection (DRP) modules without Bidder involvement. For Threat Intelligence (CTI) module, initial Child Tenant provisioning may be facilitated via a support ticket to the Bidder's Service Desk to ensure correct RBAC / branch configuration; subsequent day-to-day modifications shall be self-service.' Rationale: TI branches typically involve threat actor scope, threat landscape tuning, and feed configuration best set up by an analyst on first onboarding.	Clause remains same. Comply to the original requirement. Clarification provided in Serial No. 07 of Set 02 is also relevant.
10	Section VI. Schedule of Requirements → Table 7 –	MCP (Model Context Protocol) integration is on Platform's product roadmap. Please confirm that delivery of MCP integration during the contract	This will be evaluated during the procurement cycle. Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 3.7 → Pg. No. 118	period (i.e., within the 12-month subscription window) is acceptable, rather than requiring MCP support at bid submission or Go-Live. The clause is marked P2 (Preferential) — please clarify whether P2 items are scored/evaluated at bid stage or accepted as future deliverables.	
11	Section VI. Schedule of Requirements → Table 6.2 – Incidents Response → Pg. No. 125	Kindly revisit the P1 SLA. 15-minute response SLA on 24×7×365 basis with per-breach penalties is very tight for a service-desk-model engagement across 250 tenants. Industry-standard P1 response for Threat Intelligence / DRP / ASM platform incidents is 30-60 minutes. Also request removal of per-breach penalty and moving to a monthly performance-review credit model.	Clause remains same. Comply to the original requirement.
12	Section VI. Schedule of Requirements → Table 6.2 – Incidents Response → Pg. No. 125,126	Kindly revisit the P2 SLA. 30-minute response is aggressive for a Preferential-severity incident. Industry-standard P2 response is 2-4 hours. Also request removal of per-breach penalty in favour of monthly performance credit model.	Clause remains same. Comply to the original requirement.
13	Section VI. Schedule of Requirements → Table 6.2 – Incidents Response → Pg. No. 126	Kindly revisit the P3 SLA. 2-hour response on 24×7×365 basis for Medium severity (non-critical, usability/quality impact) is tight. Industry-standard P3 response is 4-8 business hours. Request move to business-hours SLA and monthly credit model.	Clause remains same. Comply to the original requirement.
14	Section VI. Schedule of Requirements → Table 6.2 – Incidents Response → Pg. No. 125,126	Kindly revisit the P4 SLA. 4-hour response 24×7×365 for Low-severity administrative/informational tickets is aggressive. Industry-standard P4 is 1-2 business days. Request move to business-hours SLA.	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
15	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and Qualification Requirements of the Bidder → 3.7.6.4 → Pg. No. 54,55	Please clarify: (a) Does 'multi-tenant deployment for 5 clients' mean 5 total OEM deployments where each supports multiple tenants, OR 5 distinct customers each with their own sub-tenant hierarchy? (b) What is the minimum number of Child Tenants per reference to qualify as 'multi-tenant'?	(a) 5 distinct customers each with their own sub-tenant hierarchy. (b) Bidder to provide specific details.
16	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.1 → Pg. No. 119	Please clarify whether 'on-site' means at Sri Lanka CERT premises in Colombo (which requires physical travel by trainers), or whether hybrid delivery (initial on-site + follow-up virtual) is acceptable. Platform can deliver on-site training at Sri Lanka CERT via India-based trainers, but full multi-week programs may benefit from hybrid delivery.	The bidder shall arrange comprehensive analyst training for 20 MATH Lab analysts at a suitable venue selected by the bidder.
17	Section VI. Schedule of Requirements → Table 2.1 – Implementation and Payment Schedule → 1 → Pg. No. 83	Please clarify whether the 30-day deployment window starts from (a) Date of Award, or (b) receipt of complete tenant onboarding data (250 organization domain lists, brand names, IP ranges, cloud asset lists, etc.). Please also confirm the format and schema in which Sri Lanka CERT will supply the 250 tenant onboarding data.	• 30-day deployment window starts from (a) Date of Award. • In accordance with the migration support and data provided by the incumbent solution provider following the transfer/handover.
18	Section VI. Schedule of Requirements → Table 3.3.1 – Evaluation Components and Marking Scheme → 8 → Pg. No. 47,48	Please clarify: (a) For ELK SIEM integration — is a reference letter for any SIEM integration (Splunk, QRadar, Sentinel, ELK) acceptable, or is an ELK-specific reference mandatory? (b) For OpenCTI — since OpenCTI natively ingests STIX/TAXII feeds (which Platform delivers as standard), please confirm whether STIX/TAXII-	(a) A reference letter for any SIEM integration acceptable (b) Acceptable as compliance

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		based integration into OpenCTI is acceptable as compliance.	
19	Section IV. Bidding Forms → 4.11 → Price Schedules → Pg. No. 77	Consider adding unlimited takedown package to cover 250 brands	Clause remains same. Comply to the original requirement.
20	Takedown SLA	Please revise the SLA for Takedowns/shutdowns of any Attacks. <=24 Hours for Fake, Duplicate & Typosquat Domains with Phishing Content Google Safe Browser - Danger Banner on Website Phishing & Malicious URLs on TLD Phishing & Malicious URLs using Dynamic DNS service Phishing & Malicious URLs on a compromised web server <=7 Days Scam & Trademark abuse detection on the web Scam & Trademark Abuse Detection on Social Media Scam & Trademark Abuse Detection Using Image Scam & Trademark abuse detection for Mobile apps Scam & Trademark abuse detection for VIPs <=20 Days Scam & Trademark abuse detection for instant messaging services such as Telegram Scam & Trademark abuse detection for WhatsApp	Sr. No. 5 of Addendum 01 is relevant

Set 04

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 → Pg. No. 95,96	Could you please define what constitutes a "deep-dive investigation" (e.g., RFI request, DFIR engagement, or platform-based analysis)? Additionally, will a parent-governed credit model with per-tenant allocation and reallocation be acceptable?	Clarification provided in Serial No. 8 of Set 01 is relevant. Sr. No. 2 of Addendum 01 is also applicable.
2	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.2 → Pg. No. 97	Can you confirm whether continuous asset discovery (beyond a weekly cadence) satisfies the requirement? Also, how should the 7-day SLA for new asset detection be measured, considering external propagation delays?	The clause sets weekly as a floor, not a ceiling. The wording "minimum weekly schedule" means weekly is the least frequent cadence acceptable; anything more frequent (daily, hourly, or continuous/always-on discovery) automatically satisfies and exceeds this requirement. The clause itself anchors the SLA to "first appearance", the point at which the asset becomes externally discoverable/observable.
3	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.6 → Pg. No. 98	Should vulnerability de+F13:F18based solely on external indicators such as signatures, CVE mapping, and configuration analysis, without performing intrusive exploitation on assets?	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.5 → Pg. No. 97,98 relevant.
4	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.9 → Pg. No. 99	For exposures identified only at the IP level (e.g., shared hosting), can alerts be raised against the IP address with associated possible domains, where deterministic attribution is not feasible?	Considered as a compliance.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
5	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.10 → Pg. No. 99	Could you clarify what qualifies as a “material change” for assets (e.g., IP change, SSL certificate update, new subdomain) for re-detection purposes?	A "material change" means any post-removal change in the asset's DNS resolution (new IP, CNAME, or nameserver), hosting/ASN/cloud provider, SSL/TLS certificate (issuer, subject, or SAN set), WHOIS/registrant details, or the exposure of a new subdomain/service under the same parent asset; any one of these is sufficient to justify re-detection
6	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.5 → Pg. No. 102	Will logical grouping of tenants and aggregated dashboards meet the requirement for multi-organization visibility?	Clause remains same. Comply to the original requirement.
7	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.5 → Pg. No. 110	Can the requirement for malware variant detection be satisfied through malware analysis reports, YARA/hash-based tracking, and DFIR support, instead of a fully automated native code similarity engine? What type of evidence would be acceptable?	No, manual malware analysis reports, YARA/hash-based tracking, and DFIR support alone are not acceptable substitutes.
8	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.7 → Pg. No. 114	Will periodic, analyst-curated reports on threat campaigns and trends meet the requirement for seasonal trend reporting?	Clause remains same. Comply to the original requirement.
9	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → Pg. No. 83,84	We request to amend the payment terms in the RFP as below:	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority

Item No	Milestone	Deliverables & Acceptance Conditions	Timeline from Date of Award	Payment (% of Total Contract Price)
1	**Data Migration, Installation, Configuration & Tune-up and Platform Operational Acceptance**	Full deployment of the CTI, EASM, Deep & Dark Web Monitoring, Takedown, and Reporting modules in a cloud-native SaaS environment. All 250 government organizations onboarded as Child Tenants with automated asset discovery initiated. MFA, RBAC, audit logging, and per-tenant alert configuration verified operational. Parent Tenant dashboard confirmed functional. Formal Operational Acceptance Certificate issued by Sri Lanka CERT following successful Operational Acceptance Testing (OAT).	Within 30 days of Date of Award	30%
2	**User/Analyst Training Completed**	In-person onboarding user/analyst training delivered on-site at Sri Lanka CERT premises for minimum 20 MATH Lab analysts, covering all modules specified in Table 7 Section C (Training). Training manuals, user guides, and all soft copy and hard copy documentation delivered and accepted. Written confirmation of training completion signed by Sri Lanka CERT Project Manager.	Within 14 days of Date of Award	10%
3	**ELK SIEM Integration Accepted**	Full integration of the platform with Sri Lanka CERT NCSOC ELK SIEM tested and confirmed operational. IOC feeds verified as filtered for Sri Lankan government context relevance. OpenCTI integration confirmed. Push and pull mechanisms tested and documented. MCP integration configured and tested. Integration acceptance signed off in writing by Sri Lanka CERT.	Within 35 days of Date of Award	15%

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority

4	**Operational Playbooks Delivered & First SLA Review Passed**	Operational playbooks tailored to the Sri Lankan government context delivered covering all scenarios specified in Table 7 Section C. First quarterly SLA performance review conducted by Sri Lanka CERT. Bidder must demonstrate zero unresolved P1 breaches and no more than two unresolved P2 breaches during the preceding quarter. Payment withheld if SLA review is not passed.	Operational Acceptance Testing (OAT) + 1 month	15%
5	**Second SLA Review Passed**	Second quarterly SLA performance review. Bidder demonstrates continued platform availability ≥ 99.5%, timely alert delivery, and zero outstanding unresolved P1 or P2 incidents. Sri Lanka CERT Project Manager issues written confirmation of satisfactory performance. Any outstanding penalty deductions under Section 6.2 and 6.3 will be applied against this instalment before release.	Operational Acceptance Testing (OAT) + 9 months	10%
6	**Operationalisation of the solution by providing Cyber Threat Intelligence, Attack Surface Management, Deep & Dark Web Monitoring, Takedowns and Analysis & Reports.**	The contractor is required to provide operational support during the subscription period.	Date of Award + 12 months	10%
7	**Migration Support & Post-Transfer Permanent Data Deletion**	Complete export of all Purchaser and Child Tenant data in machine-readable open formats delivered and verified by Sri Lanka CERT. Written deletion certification provided within 5 business days of confirmed export. Permanent deletion of all data from production systems, backups, DR copies, and sub-processor systems confirmed in writing by the Bidder.	Date of Award + 12 months + 30 days	10%
	Total			**100%**

Set 05

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.5 → Pg. No. 54	Request the customer reference requirement be reduced from 20 to 10 customers to encourage wider OEM participation while maintaining adequate proof of capability.	Clause remains same. Comply to the original requirement.
2	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1 → Pg. No. 54	Request reduction from 20 clients to 10 clients. Technical capability will already be assessed through compliance evaluation, demonstration and live product validation.	Clause remains same. Comply to the original requirement.
3	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.2 → Pg. No. 54	Request reduction from 20 clients to 10 clients.	Clause remains same. Comply to the original requirement.
4	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the	Request reduction from 20 clients to 10 clients.	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Bidder → 3.7.6.3 → Pg. No. 54		
5	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.4 → Pg. No. 54	Request reduction to 3 multitenant deployments, considering such deployments are uncommon and capability will be demonstrated during technical evaluation.	Clause remains same. Comply to the original requirement.
6	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3 → Pg. No. 54	Kindly confirm that a single integrated customer deployment including CTI, ASM and Dark Web Monitoring may be counted against all three qualification requirements.	Considered as compliance
7	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6 → Pg. No. 55	Kindly confirm whether the requirement refers to unique customers or cumulative module references.	Quality and security requirements will be assessed based on whether the OEM holds ISO 27001 certification or an equivalent recognized standard.
8	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the	Kindly confirm that government, commercial, telecom, financial services, MSSP and critical infrastructure customer references are all acceptable.	Quality and security requirements will be assessed based on whether the OEM holds ISO 27001 certification or an equivalent recognized standard.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Bidder → 3.7.6 → Pg. No. 55		
9	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6 → Pg. No. 55	Kindly confirm that global customer references from any country are acceptable.	Quality and security requirements will be assessed based on whether the OEM holds ISO 27001 certification or an equivalent recognized standard.
10	Section II. Bid Data Sheet → ITB 7.1 → Pg. No. 37	Since takedown services are frequently delivered through specialized global service providers, kindly confirm whether OEM nominated specialist takedown partners are permitted.	Refer to Section VI. Schedule of Requirements Table 7 – Technical Specification Section - A 16 Pg. No. 90
11	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section - A → 16 → Pg. No. 90	Request clarification whether OEM-owned/acquired technologies forming part of a common platform are acceptable under this requirement.	Considered as compliance
12	Section VI. Schedule of Requirements → Scope of Work → 1.3 → Pg. No. 83	Kindly provide the approximate number of domains, subdomains and public IP addresses expected across 250 organizations for sizing purposes.	Clarification provided in Serial No. 3 of Set 01 is relevant
13	Section VI. Schedule of Requirements → Scope of Work → 1.5 → Pg. No. 83	Kindly confirm whether Years 2 and 3 pricing will be used for commercial evaluation or only for budgeting purposes.	Years 2 and 3 pricing will be used for budgeting purposes, in the event the subscription is extended.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
14	Section IV. Bidding Forms → Price Schedule Summary →Pg. No. 78	Kindly clarify whether renewal pricing shall be considered during commercial evaluation.	Years 2 and 3 pricing will be used for budgeting purposes, in the event the subscription is extended.
15	Section IV. Bidding Forms → Price Schedule Break Down → Pg. No. 77	Kindly specify minimum annual expected consumption of investigation credits, dark web lookups, analyst investigations and API calls for sizing.	For sizing purposes, annual expected consumption of investigation credits, dark web lookups, analyst investigations, and API calls should be calculated on the following basis: 250 organizations, 10 users, 5 investigations/tenant/month, unlimited dark web lookups, and self-disclosed API throughput.
16	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 → Pg. No. 95	Kindly confirm minimum annual investigation volume expected across all 250 tenants.	Sr. No. 2 of Addendum 01 is relevant
17	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4 → Pg. No. 117	Kindly confirm anticipated daily API consumption and expected OpenCTI/ELK integration load.	Clarification provided in Serial No. 17 of Set 01 is relevant
18	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.6 → Pg. No. 98	Kindly clarify whether authenticated vulnerability assessment is required or only external non-intrusive EASM scanning.	Section VI. Schedule of Requirements □ Table 7 – Technical Specification □ 2.5 □ Pg. No. 97,98 relevant.
19	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.4 → Pg. No. 97	Kindly confirm whether third-party rate limits and scanning restrictions imposed by cloud providers are acceptable.	Clause remains same. Comply to the original requirement.
20	Section VI. Schedule of Requirements → Table 7 –	Kindly clarify if OEM-owned intelligence sources qualify under this requirement.	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 3.1 → Pg. No. 101		
21	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4 → Pg. No. 102	Kindly clarify whether integrated third-party translation services are acceptable.	Sr. No. 17 of Addendum 01 is relevant
22	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4 → Pg. No. 102	Kindly confirm that full machine translation for Sinhala is not mandatory.	Clause remains same. Comply to the original requirement.
23	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.2 → Pg. No. 106	Kindly confirm that detection time is measured from source collection by OEM and not necessarily from actual public exposure.	Clause remains same. Comply to the original requirement.
24	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.4 → Pg. No. 106	Kindly confirm acceptable evidence sources for ransomware attribution.	The Purchaser does not mandate a specific proprietary source list; the Bidder shall confirm which of the sources their platform natively monitors and how source evidence and timestamps are captured, retained, and presented within the alert.
25	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.7 → Pg. No. 106	Kindly confirm whether browser isolation technology is acceptable in lieu of an integrated sandbox.	Sr. No. 4 of Addendum 01 is relevant
26	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.3 → Pg. No. 108	Kindly clarify whether hunt workflows integrated with CTI platform satisfy this requirement.	Considered as compliance

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
27	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.6 → Pg. No. 110	Kindly confirm whether OEM integrated cloud sandbox technology is acceptable.	Considered as compliance
28	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.8 → Pg. No. 110	Kindly clarify expected operational use case and evaluation criteria.	Operational Use Cases (but not limited to): • Enable MATH Lab analysts to identify malware being sold, distributed, discussed, or advertised on dark web sources that may target or be relevant to the 250 monitored organizations. • Support proactive detection of emerging malware campaigns before they materialize as incidents against monitored organizations, feeding into the hunt case management and sandbox detonation workflows.
29	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.2 → Pg. No. 111	Kindly confirm that Sri Lanka CERT will provide legally accepted master authorization documentation.	Yes
30	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.3 → Pg. No. 111	Kindly confirm acceptable verification methods for social media and mobile application takedowns.	As per Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.4 → Pg. No. 111 in the RFP
31	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.1 → Pg. No. 112	Kindly provide expected maximum annual alert volume for sizing purposes.	For sizing purposes, annual expected alert volume should be calculated based on findings generated from the platform.
32	Section VI. Schedule of Requirements → Table 7 –	Kindly clarify whether Microsoft Copilot, OpenAI, Anthropic, Gemini or equivalent enterprise LLM platforms are acceptable.	Yes

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 3.7 → Pg. No. 118		
33	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 → Pg. No. 118	Request removal of benchmark-specific criteria as model rankings change frequently and may unfairly restrict competition.	Clause remains same. Comply to the original requirement.
34	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 → Pg. No. 118	Kindly confirm that models with lower context windows but equivalent retrieval mechanisms will be accepted.	Clause remains same. Comply to the original requirement.
35	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → 2 → Pg. No. 84	Request training delivery timeline be measured from completion of deployment rather than contract award. Request training delivery timeline be measured from completion of deployment rather than contract award.	Clause remains same. Comply to the original requirement.
36	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → 3 → Pg. No. 84	Request timeline start after successful platform onboarding and access provisioning.	Clause remains same. Comply to the original requirement.
37	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.2 → Pg. No. 125	Request clarification that SLA measurement begins upon ticket logging through designated support channels.	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
38	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.3 → Pg. No. 127	Request clarification that incidents requiring third-party provider intervention are excluded from resolution calculations.	Sr. No. 5 of Addendum 01 is relevant
39	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.3 →Pg. No. 127	Kindly clarify force majeure and third-party dependency exclusions.	Force majeure will be in effect except for the third-party dependency applicable for the services affected for Sr. No. 5 of Addendum 01.
40	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 6.2 → Pg. No. 125	Request clarification whether cumulative penalties are capped at 10% of total contract value.	Sr. No. 13 of Addendum 01 is relevant.
41	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section - A → 15 → Pg. No. 89	Kindly confirm that necessary processing by disclosed subprocessors is permitted.	Clause remains same. Comply to the original requirement.
42	Section III. Evaluation and Qualification Criteria → Table 3.8 – Key Personal and Details → Pg. No. 56	Request that OEM-certified consultants and contracted specialists also be accepted for project delivery.	Clause remains same. Comply to the original requirement.
43	Section III. Evaluation and Qualification Criteria → Table 3.8 – Key Personal and Details → Pg. No. 57	Kindly confirm whether equivalent cybersecurity experience including threat intelligence, SOC, DFIR and threat hunting is acceptable.	Considered as compliance

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
44	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section - A → 21, 22 → Pg. No. 90	Kindly clarify expected data retention volume and estimated data size to be exported at contract closure.	Expected data retention volume should be estimated based on findings generated for 250 organizations.
45	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.3 → Pg. No. 117	Kindly request Sri Lanka CERT to provide baseline filtering criteria and operational requirements during implementation.	Sri Lanka CERT will not be issuing a pre-defined baseline filtering criteria document. As per Milestone 3 in Implementation and payment schedule, the responsibility for developing and applying the IOC feed filtering methodology rests with the Bidder. Sri Lanka CERT will provide relevant operational context to support this, and will work with the Bidder to calibrate and validate feed relevance during the integration phase.
46	-	Kindly confirm if Bidder along with its affiliate including its subsidiaries can participate and can submit credentials of the parent company. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary.	Only the bidder or if there is a JV/Consortium agreement the party who is authorized in the JV/Consortium can submit the Invoice.
47	Section IV. Bidding Forms → Form 4.7 → Pg. No. 72	Amount and validity period of Bid Security. Validity period of performance guarantee	Refer to Section II – Bid Data Sheet of the RFP
48	Section VI. Schedule of Requirements → Scope of Work → 2 → Pg. No. 83	Whether separate invoices to be raised for each steps as bidders credit period is only 30 days.	Refer to Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → Pg. No. 83
49	Section VII. General Conditions → 17 Confidential Information → Pg. No. 156	We request the Customer to make this provision mutual	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
50	Section VII. General Conditions → 32 Intellectual Property Rights Indemnity → Pg. No. 179	We request the Customer to replace the said clause with the below mentioned language: Intellectual Property Infringement Claims. In the event of a third party claim of intellectual property infringement, Successful Bidder may, at its sole option, (i) obtain for Bank the right to continue using the Services, (ii) modify the Services so that the Services are non-infringing, (iii) replace the Services with a functionally equivalent, non-infringing service, or (iv) if the alternatives in Section (i)-(iii) are not available, Successful Bidder may so notify Bank and terminate such infringing Services without penalty to either Party. Notwithstanding anything in this Agreement to the contrary, this Section is Bank's sole and exclusive remedy for any intellectual property infringement claims.	Clause remains same. Comply to the original requirement.
51	Section VII. General Conditions → 33 Limitation Liability → Pg. No. 181	we request the entire clause be replaced by below mentioned language: "i. The maximum aggregate liability of successful bidder, with respect to any liability and/ or all indemnity claims under the RFP including intellectual property claims, shall in no event exceeds, the most recent twelve (12) months of charges collected by successful bidder pursuant to the applicable PO giving rise to the liability. ii. Under no circumstances shall either Party be liable for any indirect, consequential or incidental	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		losses, damages or claims including loss of profit, loss of business or revenue."	
52	Section VII. General Conditions → 34 Criminal Charges and Convictions → Pg. No. 181	We request deletion of this clause. We also ensure that we will take all reasonable measures to disclose, to the extent possible.	Clause remains same. Comply to the original requirement.
53	Section VII. General Conditions → 46 Termination for Employer's Convenience → Pg. No. 201	We propose this clause to be made mutual and any termination shall be subject to early termination charges	Clause remains same. Comply to the original requirement.
54	Section VII. General Conditions → 47 Termination for Contractor's Default → Pg. No. 203	We request the Customer to specify an explicit notice period for termination in the event of a default by the Bidder for all the events mentioned under the clause. Further, we request that the Bidder be provided with a cure period of 30 days to remedy the default before any termination notice is issued.	Refer Section VII. General Conditions □ 47.2 Termination for Contractor's Default □ Pg. No. 203 in the RFP.

Set 06

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section VI. Schedule of Requirements →4.3 Licensing→ Pg. No. 86	Is the solution expected to be licensed on a perpetual basis or annual subscription?	Subscription based licensing
2	Section VI. Schedule of Requirements →4.3 Licensing→ Pg. No. 86	Is the quoted price required to include all third-party licenses?	Yes
3	Section II. Bidding Data Sheet → ITB 21.1 → Pg. No. 39	Shall prices be quoted in USD or LKR?	As per Section II. Bidding Data Sheet → ITB 21.1 → Pg. No. 39 in the RFP
4	Section III. Evaluation and Qualification Criteria → Section 3.7 → Pg. No. 53	Is there any local preference applicable to Sri Lankan companies?	No
5	Section VI. Schedule of Requirements →2 Implementation and Payment Schedule→ Pg. No. 83-85	What are the payment milestones after contract award?	As per Section VI. Schedule of Requirements →2 Implementation and Payment Schedule→ Pg. No. 83-85 in the RFP
6	Section VII. General Conditions → Section 13.3 → Pg. No. 151	Is performance security required in addition to bid security?	Yes
7	Section VII. General Conditions	Will travel and accommodation costs for implementation be reimbursed separately?	Travel and accommodation costs will not be reimbursed.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	→ Section 13.3 25.2 Pg. No 168		
8	Section VI. Schedule of Requirements →Table 7 →2.User Management → Pg. No. 116	Please confirm the expected number of users (administrators, analysts, viewers).	Sr. No. 8 of Addendum 01 is relevant
9	Section VI. Schedule of Requirements →Table 7 → Section – A → 11 → Pg. No. 89	Please confirm whether all 250 organizations require dedicated tenant instances or logical multi-tenancy.	As per Section VI. Schedule of Requirements →Table 7 → Section – A → 11 → Pg. No. 89 in the RFP
10	Section VI. Schedule of Requirements →Table 7 → Section – A 5 → Pg. No. 88	Is there any expected future expansion beyond 250 organizations?	Clarification provided in Serial No. 6 of Set 01 is relevant
11	Section VI. Schedule of Requirements →Table 7 → Section – B → 3.2 → Pg. No. 101	What is the expected retention period for CTI data?	As per Section VI. Schedule of Requirements →Table 7 → Section – B → 3.2 → Pg. No. 101 in the RFP
12	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section - A → 21, 22 → Pg. No. 90	What are the expected storage requirements?	Clarification provided in Serial No. 44 of Set 05 is relevant
13	Section VI. Schedule of Requirements →Table 7	Are High Availability (HA) and Disaster Recovery (DR) mandatory?	Yes

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	→ Section – A → 3 → Pg. No. 88		
14	Section VI. Schedule of Requirements →Table 7 → Section – A → 3 → Pg. No. 88	Is cloud deployment acceptable, or is the solution required to be fully on-premises?	As per Section VI. Schedule of Requirements →Table 7 → Section – A → 3 → Pg. No. 88 in RFP
15	Section VI. Schedule of Requirements →Table 7 → Section – B → 3.1 → Pg. No. 101	How many commercial threat intelligence feeds are expected?	The Purchaser does not mandate a specific proprietary source list; the Bidder shall confirm which of the sources their platform natively monitors and how source evidence and timestamps are captured, retained, and presented within the alert.
16	Section VI. Schedule of Requirements →Table 7 → Section – B → 3.1 → Pg. No. 101	Are open-source intelligence feeds acceptable where commercial feeds are unavailable?	The Purchaser does not mandate a specific proprietary source list; the Bidder shall confirm which of the sources their platform natively monitors and how source evidence and timestamps are captured, retained, and presented within the alert.
17	Section VI. Schedule of Requirements →Table 7 → Section – C → 3.1 → Pg. No. 116	Is support for STIX/TAXII 2.1 mandatory?	Integration and export capabilities shall be supported via either a REST API or STIX/TAXII 2.x, with documentation provided accordingly.
18	Section VI. Schedule of Requirements →Table 7 → Section – B → 3.3 → Pg. No. 101	Is MITRE ATT&CK framework integration mandatory?	Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
19	Section VI. Schedule of Requirements →Table 7 → Section – B → 3.10 → Pg. No. 103	Is automatic IOC enrichment required?	Yes
20	Section VI. Schedule of Requirements →Table 7 → Section – B → 6.6 → Pg. No. 110	Should malware sandbox integration be included?	Yes
21	Section VI. Schedule of Requirements →Table 7 → Section – B → 2.1 → Pg. No. 96-97	Approximately how many internet-facing assets will be monitored?	Clarification provided in Serial No. 4 and 5 of Set 01 is relevant
22	Section VI. Schedule of Requirements →Table 7 → Section – B → 2.1 → Pg. No. 96-97	Does the scope include cloud asset discovery?	Yes
23	Section VI. Schedule of Requirements →Table 7 → Section – B → 2.1 → Pg. No. 96-97	Is third-party/vendor attack surface monitoring required?	No
24	Section VI. Schedule of Requirements →Table 7 → Section – B → 2.4 → Pg. No. 97	Is continuous vulnerability scanning required?	Yes

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
25	Section VI. Schedule of Requirements →Table 7 → Section – B → 4.1 → Pg. No. 105	Is dark web monitoring mandatory?	Yes
26	Section VI. Schedule of Requirements →Table 7 → Section – C → 3.3,3.5,3.6 → Pg. No. 117	Please provide the list of existing security solutions to be integrated, including SIEM, SOAR, EDR, IAM, firewalls, and ticketing systems.	SIEM, OpenCTI and MCP
27	Section VI. Schedule of Requirements →Table 7 → Section – C → 3.1 → Pg. No. 116-117	Are REST APIs available for integration with the Malware Analysis Lab?	Bidder to provide the APIs through the solution
28	-	Is integration with Active Directory/LDAP mandatory?	No
29	-	Is email security gateway integration required?	No
30	Section VI. Schedule of Requirements →Implementation and Payment Schedule→ Pg. No. 83-85	What is the expected project completion timeline?	As per the Section VI. Schedule of Requirements →Implementation and Payment Schedule→ Pg. No. 83-85 in the RFP.
31	Section VI. Schedule of Requirements →Table 7 → Section – A → 3 → Pg. No. 88	Will Sri Lanka CERT provide implementation infrastructure before deployment?	As per the Section VI. Schedule of Requirements →Table 7 → Section – A → 3 → Pg. No. 88 in the RFP.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
32	Section VI. Schedule of Requirements →Table 7 → Section – A → 3 → Pg. No. 88	Will staging and production environments be available?	As per the Section VI. Schedule of Requirements →Table 7 → Section – A → 3 → Pg. No. 88 in the RFP.
33	Section VI. Schedule of Requirements → 3. Acceptance and Testing → Pg. No. 86	Who will be responsible for User Acceptance Testing (UAT)?	As per the Section VI. Schedule of Requirements → 3. Acceptance and Testing → Pg. No. 86 in the RFP
34	Section VI. Schedule of Requirements → Section 6 → 5.1 → Pg. No. 119	How many administrators require training?	Clarification provided in Serial No. 16 of Set 03 is relevant
35	Section VI. Schedule of Requirements → Section 6 → 5.1 → Pg. No. 119	How many SOC analysts require training?	Clarification provided in Serial No. 16 of Set 03 is relevant
36	Section VI. Schedule of Requirements → Section 6 → 5.1 → Pg. No. 119	Should training be conducted on-site, online, or in a hybrid mode?	Clarification provided in Serial No. 16 of Set 03 is relevant
37	Section VI. Schedule of Requirements → Section 6 → 5.1 → Pg. No. 119	Is training material required in editable format?	Yes
38	Section VI. Schedule of Requirements → Section 6 General Warranty Terms & Service Level	What are the required SLA response and resolution times?	As per the Section VI. Schedule of Requirements → Section 6 General Warranty Terms & Service Level Agreement (SLA) → Pg. No. 122- 131 in the RFP and Sr. No. 5 of Addendum 01 is also relevant

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Agreement (SLA) → Pg. No. 122- 131		
39	Section VI. Schedule of Requirements →Table 7 → Technical Specification. → 7 → Pg. No. 88	Is 24×7 support mandatory throughout the warranty period?	Yes
40	Section VI. Schedule of Requirements →Table 7 → Technical Specification. → 7 → Pg. No. 88	Will OEM engineers be required onsite during the warranty period?	As per the Section VI. Schedule of Requirements →Table 7 → Technical Specification. → 7 → Pg. No. 88 in RFP
41	-	How many preventive maintenance visits are expected annually?	As decided by the Bidder/OEM
42	Section III. Evaluation and Qualification Criteria →3.3-3.3.1 → Pg. No. 45-48	Please confirm the evaluation methodology and technical scoring matrix.	As per the Section III. Evaluation and Qualification Criteria →3.3-3.3.1 → Pg. No. 45-48 in RFP
43	Section III. Evaluation and Qualification Criteria →3.3.1 → Pg. No. 46-48	Will the live demonstration be evaluated only on mandatory requirements or will additional features receive extra marks?	As per the Section III. Evaluation and Qualification Criteria →3.3.1 → Pg. No. 46-48 in RFP
44	Section III. Evaluation and Qualification Criteria →3.3 → Pg. No. 45	Can the demonstration be conducted remotely if international OEM experts participate?	No
45	Section III. Evaluation and Qualification Criteria	Is an offline demonstration environment acceptable if internet access is unavailable?	No

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	→3.3-3.3.1 → Pg. No. 45-48		
46	Section III. Evaluation and Qualification Criteria →3.7.5-3.7.6.4 → Pg. No. 54-55	Does experience with CTI and ASM projects in countries other than Sri Lanka satisfy the "similar project" requirement?	Yes
47	Section III. Evaluation and Qualification Criteria →3.7 → Pg. No. 53-54	Can consortium partners jointly satisfy the experience requirements?	As per the Section III. Evaluation and Qualification Criteria →3.7 → Pg. No. 53-54 in RFP
48	Section III. Evaluation and Qualification Criteria →3.7 → Pg. No. 54-55	Will projects completed by OEM implementation partners be accepted as reference projects?	No
49	Section III. Evaluation and Qualification Criteria →3.7.5-3.7.6 → Pg. No. 54-55	Can one project satisfy both CTI and ASM experience requirements?	Yes
50	Section III. Evaluation and Qualification Criteria →3.7.6 → Pg. No. 54-55	Are customer completion certificates mandatory, or are purchase orders and reference letters sufficient?	While purchase orders and reference letters from clients are sufficient, customer completion certificates may be submitted.
51	Section VI. Schedule of Requirements → Table 7 → Section – B → 3 → Pg. No. 101-105	What are the functional acceptance criteria for CTI?	As per the Section VI. Schedule of Requirements → Table 7 → Section – B → 3→ Pg. No. 101-105 in RFP

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
52	Section VI. Schedule of Requirements → Table 7 → Section – B → 2→ Pg. No. 96-101	What are the acceptance criteria for ASM?	As per the Section VI. Schedule of Requirements → Table 7 → Section – B → 2→ Pg. No. 96-101 in RFP
53	Section VI. Schedule of Requirements → Inspection and Testing → Pg. No. 132	Will penetration testing be part of final acceptance?	No
54	Section VI. Schedule of Requirements → 2. Implementation and Payment Schedule → 7 → Pg. No. 85	What reports and documentation are required for project closure?	As per the Section VI. Schedule of Requirements → 2. Implementation and Payment Schedule → 7 → Pg. No. 85 in RFP
55	Section VI. Schedule of Requirements → 2. Implementation and Payment Schedule → 4 → Pg. No. 85	Is there a post-implementation stabilization period before final acceptance?	As per Section VI. Schedule of Requirements → 2. Implementation and Payment Schedule → 4 → Pg. No. 85 in RFP
56	Section VI. Schedule of Requirements →Table 7 → Technical Specification. Section B→ 2 → Pg. No. 96	Will Sri Lanka CERT provide existing asset inventories and domain lists for onboarding?	Clarification provided in Serial No. 17 of Set 03 is relevant
57	-	What is the expected daily volume of IOCs, alerts, and threat feeds?	Daily expected IOCs, alerts and threat feeds volume should be calculated based on findings generated from the platform.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
58	Section V. Eligible Countries → Pg. No. 81	Are there any restrictions on the country of origin of the OEM solution?	As per the Section V. Eligible Countries → Pg. No. 81 in RFP
59	Section VI. Schedule of Requirements →Table 7 → Technical Specification. Section C→ 3.1- 3.7 → Pg. No. 116-118	Is integration with future national cyber platforms expected within the warranty period?	As per the Section VI. Schedule of Requirements →Table 7 → Technical Specification. Section C→ 3.1- 3.7 → Pg. No. 116-118 in RFP
60	-	Can proposed solutions exceed the minimum technical specifications without affecting evaluation?	Yes
61	Section VI. Schedule of Requirements →Table 7 → Technical Specification. Section A→ 6 → Pg. No. 88	Will software upgrades and version changes during the support period be included under the contract price?	As per the Section VI. Schedule of Requirements →Table 7 → Technical Specification. Section A→ 6 → Pg. No. 88 in RFP

Set 07

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6→ Pg. No. 55	Please confirm whether the ISO 27001 certification must be held by: • The primary supplier/vendor; • The backend support/service provider; or • Both the primary supplier/vendor and the backend support/service provider.	As per the Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6→ Pg. No. 55 in RFP

Set 08

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section III. Evaluation and Qualification Criteria → Table 3.3 – Detailed Evaluation of Technical Bids → Pg. No. 45	SL Cert has mentioned that the local partner should conduct the demonstrate the technical capabilities. Would it be possible for the principal and partner in tandem to demonstrate the technical capabilities of the product?	Clause remains same. Comply to the original requirement.
2	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Bidder would also like to request a full list of the 250 organizations SL Cert plans to onboard to the platform?	Sr. No. 1 of Addendum 01 is relevant
3	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Bidder would also like to request full list of FQDNs (TLDs) that SL Cert plans to onboard onto the platform? If not possible Bidder would like to request the total number of domains that SL Cert plan to add to the platform? This may differ from the organization count since some organizations may have multiple domains.	Clarification provided in Serial No. 3 of Set 01 is relevant
4	Section IV. Bidding Forms → Table 4.5 → 3.7.5, 3.7.6.1 – 3.7.6.4 → Pg. No. 65 - 71	You have requested for information such as name, address, email and telephone numbers these are considered PII information for the principal and they cannot share such information without signing an NDA with SL Cert. They are comfortable to share the registered company name of the customer but for any other PII related information it is required that an NDA will need to be signed. Therefore, can we change this to only providing the name of the organization or please advise on	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		the way forward to handle this? Also please note that sharing such information puts the vendor in direct risk of violating GDPR and or the respective Personal Information Security Laws of the respective countries where the reference companies are based out of. Therefore please consider this when requesting this information.	
5	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3, 4 → Pg. No. 54	you have mentioned that the 'The Bidder must have successfully supplied, installed, implemented, and configured Cyber Threat Intelligence (CTI) and Attack Surface Management (ASM) solutions within the five (05) years immediately preceding the Bid Submission Deadline.' and 'Bidder should have delivered at least Five (5) similar multitenant solution shown by valid reference letters.' In this context of the Bidder do you mean the Local Bidder or the OEM? This point was also brought up during the pre-bid meeting and it was stated that 'The Bidder' was meant to refer to the OEM. Can you confirm and clarify this?	Clarification provided in Serial No. 23 of Set 01 is relevant
6	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.7 to 3.7.11 → Pg. No. 55,56	(a) SL Cert has requested a letter from the OEM authorizing the partner can we take all these letters to be the Manufacturer Authorization Letter? If not please specify what each of these letters are and what is the difference? (b) Bidder would also like to verify if SL Cert has any issues with the request of utilizing an advanced bond upon awarding of the contract for the total value of the solution? Meaning the	(a) As per Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.7 to 3.7.11 → Pg. No. 55,56 in RFP\ (b) As per Appendix 7 → Terms and Procedures for payments → 7.1 → Page No. 225 Advanced payment is not applicable, hence submitting an advance bond is not required. However Bidder is required to submit a performance bond Section VIII Paticular Conditions →

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		bidder would promise to deliver the solution within the stipulated timeline and if the bidder fails to deliver the solution on time SL Cert would get a full refund of the amount.	13.3(a) and 13.3(b) → Page No. 214. Further Appendix 7 Terms and Procedure for Payments →7.2 Terms of Payment →Page No. 226 term applicable for Liquidated Damage charges is applied.
7	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 → Pg. No. 118	SL Cert has mentioned "Native MCP integration meeting: 200K+ token context, native MCP server/client, enterprise API access with data residency, zero training on customer data by default, SOC 2 Type II, top-3 frontier model benchmark ranking". During the pre-bid number of concerns revolving around this was raised and it was mentioned that a rectified addendum would be provided. It would be great if SL Cert could clarify the exact requirement for LLM models, MCP server and the AI integration capabilities along with the token requirement (amount and duration) from the models be changing and updating this point can you provide some clarity on this ?	Sr. No. 7 of Addendum 01 is relevant
8	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 → Pg. No. 95,96	SL Cert has mentioned that they require a minimum of 5 investigation credits per month per child tenant. Do you refer that these requested 5-credits per month is on the basis that, these investigations would be carried out by the OEM analyst and provide a comprehensive report by the OEM themselves?	Sr. No. 2 of Addendum 01 is relevant
9	Section VI. Schedule of Requirements → Table 7 –	Can SL Cert outline what is the exact expectation of these investigation credits as different solutions,	Sr. No. 2 of Addendum 01 is relevant

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 1.17 → Pg. No. 95,96	uses different terminologies for specific tasks and actions related to investigations?	
10	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 → Pg. No. 95,96	SL Cert has mentioned that they require a minimum of 5 investigation credits per month per child tenant. Does that mean that from the outset SL Cert requires 250 (child tenant) x 12 (months) x 5 (investigation credits) which would equal 15000 investigation credits ? Can you specify the investigation credits that SL Cert will require initially per month for how many tenants? Also is SL Cert going to buy all the investigation credits together or in increments? This point is vague on how these credits are to be rolled out can this be clarified?	Sr. No. 2 of Addendum 01 is relevant
11	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.6 → Pg. No. 110	How many sandbox submissions does SL Cert require per month? Do you also need this per child tenant or as a overall count? Please specify.	Clarification provided in Serial No. 11 of Set 01 is relevant
12	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 7.2 → Pg. No. 125,126,127,128,129	SL Cert have mentioned the resolution times for the incidents but these resolution times are not feasible instead we would like to propose the following resolution times P1 – Root Cause Analysis (8 hours) and resolution within 24 hours P2 – resolution within 2 business days P3 – Resolution within 5 business days P4 – At Vendor Discretion (Since these issues are minor in nature they may not be prioritized	Sr. No. 5 of Addendum 01 is relevant

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		immediately since other priorities also need to be taken into consideration) The resolution timelines that SL Cert has requested is not very practical and we hope this can be amended and clarified accordingly	

Set 09

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3, 4 → Pg. No. 54,55	We kindly request clarification on whether this requirement can be fulfilled by either the **Bidder or the OEM (Original Equipment Manufacturer)**. Specifically, please confirm whether reference letters demonstrating the successful delivery of five (5) similar multitenant solutions by the OEM can be accepted as meeting this requirement, or whether the experience must be exclusively demonstrated by the bidding entity itself.	Clarification provided in Serial No. 23 of Set 01 is relevant
2	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1 → Pg. No. 116 Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Would you be so kind to confirm the number of possible tenants. Will those tenants represent users within various Sri Lanka CERT units, or also possible 3d parties (or inter-agency organizations besides Sri Lanka CERT).	Clarification provided in Serial No. 18 and 3 of Set 01 and Serial No. 1 of Addendum 01 also relevant.
3	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 → Pg. No. 118	Would you be so kind to confirm particular MCP server you plan to use, or this point related to the availability of vendor to provide own MCP server to process queries. Do you suggest to use vendor solution, frontier models to handle those requests, or integrate available subscriptions on your end?	Purchaser will use own Docker container based MCP server for this requirement; Sr. No. 7 of Addendum 01 is also relevant
4	Section VI. Schedule of Requirements → Table 7 –	Would you be so kind to confirm if the preferred solution would be cloud-based (SaaS) or on-premises, which may guarantee better data	Clarification provided in Serial No. 21 of Set 01 and Serial No. 13 of Set 06 are relevant.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Technical Specification → 3 → Pg. No. 88	residency and compliance for regulated environments. In case cloud hosting providers are acceptable, are there any specific requirements on the geography of data storage. As for references to backup and disaster recovery, would you be so kind to confirm that this related to the vendor itself, or you are also looking for backup and disaster recovery implementation for the solution to be deployed on your site?	

Set 10

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Schedule of Requirements → Table 7 – Technical Specification → 16 → Pg. No. 90	Clarification regarding the "**single solution provider**" requirement –"The complete solution must be from a single solution provider, not multiple solution providers, to ensure unified support and accountability. The OEM solution provider may tie up with a reputed third party for takedown services."	As per Section VI. Schedule of Requirements Table 7 – Technical Specification Section - A 16 Pg. No. 90
2	Section II. Bidding Data Sheet → ITB 20.1 → Pg. No. 39 Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7 → Pg. No. 53	All components must be procured as a "single lot as a complete solution," and that partial bids will be rejected. Please clarify if it is acceptable to **split the core technical modules between different OEMs** if we are bidding as a Joint Venture/Consortium and acting as the single point of accountability?	Clarification provided in Section II. Bidding Data Sheet → ITB 20.1 → Pg. No. 39 and Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7 → Pg. No. 53 are relevant

Set 11

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.11 → Pg. No. 56	**Can we request OEM to confirm if they can comply with this requirement.** The RFP requires OEM to commit that data will be encrypted both at rest and in transit, and to provide prior notice to Sri Lanka CERT of any future cross-border data transfers. This is an ongoing obligation rather than a one-time commitment, and any future infrastructure changes involving cross-border data flows would require advance disclosure.	As per Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.11 → Pg. No. 56 is relevant.
2	Section VI. Schedule of Requirements → 6 General Warranty Terms & Service Level Agreement (SLA) → Pg. No. 122 to 131	**Please confirm whether OEM can comply with the prescribed service level and operational requirements, including service availability, incident response and resolution timelines, operational support, service reviews, and other performance commitments.** Although these obligations are imposed on the Contractor, the proposed solution and managed services will be delivered using OEM's platform and may expose OEM to contractual remedies or financial consequences through the bidder.	Clause remains same. Comply to the original requirement. However, Resolution times for takedown service as provisioned in Sr. No. 5 of Addendum 01
3	Section VII – General Conditions → 28.2 → Pg. No. 174–175 and	Please confirm whether these obligations are intended to be flowed down to OEM on a back-to-back basis. **We would not be comfortable accepting back-to-back liability for these**	Depends on the nature of the bidder mentioned in the Section III → 3.7 → Pg. 53. The back-to-back liability will be raised in cases where the bidder's agreements with the OEM (e.g. JV or Consortium)

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Section VIII – Particular Conditions → 28.2 → Pg No. 215	**obligations.** Under the RFP, the Contractor is liable for liquidated damages for delays in achieving Operational Acceptance, and the Employer may terminate the contract if the maximum liquidated damages threshold is reached.	
4	Section VII – General Conditions → 30 → Pg. No. 177,178	Please confirm whether these obligations are proposed to be back-to-back with OEM. **We would not recommend accepting this position**. The Bidder guarantees that the solution will meet the specified functional requirements at Operational Acceptance and must rectify any deficiencies at its own cost or pay liquidated damages. Although the contractual obligation rests with the Bidder, compliance depends on OEM's platform performance.	Depends on the nature of the bidder mentioned in the Section III → 3.7 → Pg. 53. The back-to-back liability will be raised in cases where the bidder's agreements with the OEM (e.g. JV or Consortium)
5	Section VII – General Conditions → 32 – 33 →Pg. No. 179 – 182	Please confirm whether these obligations are proposed to be passed through to OEM. **We would not recommend accepting uncapped liability**. The Contractor is required to indemnify the Employer against claims arising from actual or alleged intellectual property infringement. As OEM is the owner of the proposed solution, any such claims relating to the software or services could ultimately be passed on to OEM. Further, GC Clause 33 excludes the IP indemnity obligations under GC Clause 32 from the contractual limitation of liability, resulting in potentially uncapped exposure. While aggregate	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		liability is otherwise capped at the Contract Price (with no multiplier specified in the Particular Conditions), the IP indemnity appears to fall outside that cap. Further Cyfirma standard is only third party claims on Intellectual property.	
6	Section VII. General Conditions → 46 Termination for Employer's Convenience → Pg. No. 201	The RFP permits the Employer to terminate the contract for convenience. **This is generally not aligned** with the SaaS subscription model and should be reviewed from a commercial perspective.	Clause remains same. Comply to the original requirement.
7	Section VII – General Conditions → F. Guarantees and Liabilities → 28 →Pg. No. 174,175 Appendix 7. Terms and Procedures for Payment →Pg. No. 225, 226	**Please confirm whether these liquidated damages provisions are proposed to be passed through to OEM**. Liquidated damages are set at 0.5% per week of the Total Contract Price (excluding recurrent costs), capped at 10% of the Contract Price, for delays or failure to meet the functional guarantees. This exposure is directly linked to OEM's delivery timelines and platform performance.	Depends on the nature of the bidder mentioned in the Section III → 3.7 → Pg. 53. The back-to-back liability will be raised in cases where the bidder's agreements with the OEM (e.g. JV or Consortium)
8	Section VII – General Conditions → C. PAYMENT →11. Contract Price → 11.2 →Pg. No. 150	The Contract Price is fixed for the entire contract period with no price adjustment mechanism. Accordingly, **any future licence fee increases or pricing revisions cannot be passed on to the Employer once the contract is executed.**	Clause remains same. Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
9	Section VII – General Conditions → B. Subject Matter of Contract → 9.7 → Pg. No. 147	Where the Contractor is a joint venture or consortium, all members are jointly and severally liable to the Employer. **Please confirm whether this provision has any implications for OEM if obligations are intended to be flowed down on a back-to-back basis.**	Depends on the nature of the bidder mentioned in the Section III → 3.7 → Pg. 53. The back-to-back liability will be raised in cases where the bidder's agreements with the OEM (e.g. JV or Consortium)
10	Section VII – General Conditions → 29. Defect Liability → Pg. No. 175	The contract requires all products to be free from defects in design, engineering and workmanship. **This wording is not appropriate for a SaaS/software offering, where software is continuously updated and defects may be addressed through patches, fixes and subsequent releases rather than an absolute warranty that the software is defect-free.**	This will be applicable to the defects which cannot be patched or resolved permanently that cannot meet the SLA.
11	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Considering that the proposed solution will support more than 250 government organisations, could the procuring entity clarify whether preference will be given to platforms built on a native Parent-Child multi-tenant architecture with centralized administration and complete logical isolation of tenant data, rather than multiple independent deployments managed centrally?	Comply to the original requirement in Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89 of RFP
12	Section VI. Schedule of Requirements →Table 7	Could the procuring entity clarify whether Attack Surface Management is expected to provide continuous, external, attacker-perspective	Comply to the original Section VI. Schedule of Requirements →Table 7 → Section – B → 2.1,2.2 → Pg. No. 96-97 of RFP

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	→ Section – B → 2.1,2.2 → Pg. No. 96-97	discovery of internet-facing assets without reliance on deployed agents, authenticated access, or customer-managed connectors?	
13	Section VI. Schedule of Requirements →Table 7 → Section – B → 2.1,2.2 → Pg. No. 96-97	Would the evaluation place additional emphasis on platforms capable of autonomously discovering newly exposed external assets without requiring manual asset registration or periodic inventory updates?	Comply to the original Section VI. Schedule of Requirements →Table 7 → Section – B → 2.1,2.2 → Pg. No. 96-97 of RFP
14	Section VI. Schedule of Requirements → Table 7 – Technical Specification	For cyber risk prioritisation, could the procuring entity clarify whether greater importance will be placed on contextualised, validated, and actionable risk intelligence, rather than solely on the volume of discovered indicators or findings?	Greater importance on contextualised, validated, and actionable risk intelligence over the raw volume of discovered indicators or findings. This is reflected in the RFP's Clarification provided in Section VI. Schedule of Requirements → Table 7 – Technical Specification
15	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Given the shared services operating model, could the procuring entity confirm whether each government organisation is expected to operate as an independent child tenant with dedicated assets, users, dashboards, alerts, reports, and policies while allowing Sri Lanka CERT to maintain centralized governance and visibility through a parent tenant?	The purchaser will exclusively manage all child tenants centrally to comply with original requirement in Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89 of RFP
16	Section III. Evaluation and Qualification Criteria	During the technical evaluation, will preference be given to vendors demonstrating capabilities using	Clarification provided in Serial No. 28 of Set 01 is relevant

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	→3.3-3.3.1 → Pg. No. 45-48	live operational data rather than simulated environments or static presentations?	
17	Section VI. Schedule of Requirements → Table 7 – Technical Specification	Could the procuring entity clarify whether risk validation, contextual enrichment, confidence scoring, and prioritization will form part of the technical evaluation in addition to raw discovery capabilities?	Risk validation, contextual enrichment, confidence scoring, and prioritization form part of the technical evaluation. Further committee will evaluate features indicated in Section III → 3.3 Detailed Evaluation of Technical Bids page no. 46 to 48 in addition to the requirements specified in Section VI. Schedule of Requirements → Table 7 – Technical Specification.
18	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.11, 2.15, 2.16 → Pg. No. 99, 100	For vulnerability prioritisation, is the expectation that solutions should correlate external exposure, exploitability, asset criticality, and contextual cyber risk, rather than relying solely on CVSS severity ratings?	The expectation is that vulnerability prioritisation correlates external exposure, asset context, and business impact - not a bare severity/CVE label alone. Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.11, 2.15, 2.16 → Pg. No. 99, 100 also relevant.
19	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.8 → Pg. No. 112	Will additional consideration be given to platforms that provide an integrated capability to identify, manage, and coordinate remediation of digital risks, including phishing, impersonation, rogue mobile applications, fraudulent domains, and online brand abuse?	Baseline requirements specified in Section VI. Schedule of Requirements □ Table 7 – Technical Specification is mandatory. If the bidder offers additional capability will be considered as value addition.
20	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.3, 3.5 → Pg. No. 117	Could the procuring entity clarify whether the proposed solution is intended to function as an External Intelligence Layer complementing existing SOC, SIEM, SOAR, EDR, and	Yes, complementing existing SOC by providing IOC feeds, specifications provided in Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.3, 3.5 → Pg. No. 117 is relevant.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		Vulnerability Management investments, rather than replacing them?	
21	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.1, 3.2, 3.3,3.6, 3.18 → Pg. No. 116, 117, 105	Will preference be given to solutions supporting open integration standards, including REST APIs, STIX/TAXII, and standard interoperability frameworks, to facilitate seamless integration with existing government security infrastructure?	Baseline requirements specified in Section VI. Schedule of Requirements → Table 7 – Technical Specification is mandatory. If the bidder offers additional capability will be considered as value addition.
22	-	Could the procuring entity clarify whether threat hunting capabilities are expected to include externally observable attack surface intelligence, exposed infrastructure, digital risk indicators, and vulnerability intelligence, in addition to IOC search?	It explicitly requires hunting to operate across the full breadth of intelligence the platform holds, not as a narrow IOC-lookup tool.
23	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section - A → 20 → Pg. No. 90	Will the evaluation recognise the value of platforms supported by dedicated cyber analysts responsible for validation, contextual analysis, and advisory services alongside the technology platform?	As per the Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section - A → 20 → Pg. No. 90 in RFP.
24	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5 → Pg. No. 88	As the platform is expected to support government organisations over the long term, could the procuring entity clarify whether scalability beyond the initial deployment scope, without architectural	The platform must be scalable and support expansion based on the extending external digital government infrastructure in future procurements.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		redesign or additional platform instances, will be considered during evaluation?	
25	Section VI. Schedule of Requirements → Table 7 – Technical Specification	For automation capabilities, could the procuring entity clarify whether evaluation will consider the ability to accelerate asset discovery, vulnerability prioritisation, investigation, reporting, and operational workflows, while maintaining appropriate validation before escalation?	Baseline requirements specified in Section VI. Schedule of Requirements → Table 7 – Technical Specification is mandatory. If the bidder offers additional capability will be considered as value addition.
26	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	Will additional consideration be given to platforms capable of delivering Attack Surface Management, Vulnerability Intelligence, Digital Risk Protection, Brand Protection, and Third-Party Risk Management through a unified platform, thereby reducing operational complexity and integration overhead?	Baseline requirements specified in Section VI. Schedule of Requirements → Table 7 – Technical Specification is mandatory. If the bidder offers additional capability will be considered as value addition.
27	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.1,8.3 → Pg. No. 112,113	Could the procuring entity clarify whether reporting capabilities will be assessed based on the ability to generate technical, operational, management, and executive-level reports for both the parent tenant and individual child tenants from a common platform?	As per the Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.1,8.3 → Pg. No. 112,113 in RFP.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
28	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.3 → Pg. No. 92,93	Given the strategic objective of strengthening Sri Lanka's national cyber resilience, could the procuring entity clarify whether solutions will be evaluated on their ability to provide centralised oversight of cyber exposure across all participating organisations while preserving complete tenant isolation and organisational autonomy?	Yes, As per the Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.3 → Pg. No. 92,93 in RFP.

Set 12

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
1	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 11 → Pg. No. 89	SL CERT indicated it may be able to share the names or count of the 250 participating organizations, and where possible their associated domain counts, via the Evaluation Committee (though not a detailed domain/subdomain list). Kindly confirm whether this list can now be shared, even in summary form, to assist with accurate bid sizing.	Clarification provided in Serial No. 3 of Set 01 is relevant
2	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6.1, 2, 3, 4 → Pg. No. 54	SL CERT confirmed this can be accommodated and would refer the point to the Evaluation Committee for formal clarification. Kindly provide the Committee's written confirmation / format.	Clarification provided in Serial No. 23 of Set 01 is relevant.
3	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.6 → Pg. No. 110	SL CERT acknowledged the absence of a fixed cap could be a pricing consideration and agreed to raise this with the Evaluation Committee for possible clarification or amendment. Kindly advise whether an estimated volume or cap will be issued.	Clarification provided in Serial No. 11 of Set 01 is relevant
4	Section IV. Bidding Forms → Price Schedule Break Down → Pg. No. 77	SL CERT agreed to issue formal clarification via the Evaluation Committee on the definition of an "investigation," and on whether monthly credits may be pooled and allocated annually. Kindly provide this clarification.	Clarification provided in Serial No. 15 of Set 05 is relevant

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
5	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.12 → Pg. No. 107	SL CERT indicated a cap of approximately 5 keywords per tenant (plus ad hoc search) could be workable, to be finalized with the Technical Evaluation Committee. Kindly confirm the final position and whether the Bidding Document will be amended accordingly.	Clarification provided in Serial No. 09 of Set 01 is relevant
6	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 → Pg. No. 118	SL CERT confirmed the requirement should refer to the LLM's context-window/benchmark capacity rather than an MCP server token limit and committed to correcting this clause. Kindly confirm the corrected clause language or the addendum reference in which it will appear.	Clarification provided in Serial No. 15 of Set 01 is relevant
7	Section VI. Schedule of Requirements → General Warranty Terms & Service Level Agreement (SLA) → 7.2 → Pg. No. 125,126,127,128,129 Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.3 → Pg. No. 111	SL CERT agreed to take the concern regarding excluding externally dependent takedown resolution timelines from strict SLA penalties to the Technical Evaluation Committee for review. Kindly confirm the Committee's determination.	Clarification provided in Serial No. 14 of Set 01 is relevant
8	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1 → Pg. No. 116	SL CERT agreed to bring the proposed compromise (10 fixed concurrent parent-level users plus 10–15 floating/reassignable accounts, totaling 20–25 provisioned accounts) to the Technical Evaluation Committee. Kindly confirm	

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		whether this model will be adopted and the Bidding Document amended accordingly.	
9	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4 → Pg. No. 117	SL CERT asked bidders to indicate how many external integrations (e.g., STIX/TAXII, OpenCTI) can accommodate their platform. Kindly confirm whether CERT will specify a minimum required number of concurrent external integrations, or whether this remains open for bidders to propose.	Clarification provided in Serial No. 17 of Set 01 is relevant
10	-	Expected Asset Volume per Tenant (EASM Sizing) SL CERT indicated a rough, non-binding estimate of approximately 300,000 assets across the 250 organizations, if counted at a granular level (domains, IPs, marks, etc. counted separately). As this estimate directly affects the sizing and pricing of the Attack Surface Management component, kindly confirm: (a) whether this 300,000-asset estimate can be formalized in writing as an indicative baseline for bid pricing purposes; (b) the breakdown of this estimate by asset type (domains, subdomains, IP addresses, brand/marks, certificates, etc.), to the extent available; and (c) whether this figure is expected to grow materially during the contract term as the	(a) Asset counts depend on each solution's definition of an 'asset' (domain, subdomain, IP, cloud bucket, etc.). Assets may be anticipated across the 250 tenants when such elements are counted separately. As of the day clarifications are issued estimated asset count is approximately 30,000. (b) Due to the diversity of proposed 250 organisations indicating the breakdown of asset types would vary. However the details of assets across 250 organisations will be provided during the onboarding process for validation after the auto discovery of assets by the proposed solution. (c) Growth of asset count should be expected marginally during the one year subscription period, however due to the expansion of external digital infrastructure of the government organisations figure could not be indicated before such expansion.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		additional 100 organizations are onboarded and shadow-IT discovery matures, so bidders can size elastic/overage capacity accordingly.	
11	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.6 → Pg. No. 55	ISO 27001 (or 'similar') is required of the OEM. Kindly provide the list of certifications Sri Lanka CERT will accept as 'similar' to ISO 27001 (e.g., SOC 2 Type II, ISO 27017/27018), so that bidders can confirm compliance in advance.	Any other internationally recognized information security management certification issued by an accredited/independent certification body, provided the bidder demonstrates its scope is equivalent to ISO 27001 To be accepted, any such certification must: 1. Be current and valid as of the Bid Submission Deadline; 2. Be issued by an accredited, independent certifying body (self-assessments, internal audits, or vendor-issued attestations are not acceptable); 3. Cover the OEM entity and the specific product/platform being proposed under this tender; and 4. Be submitted with the Technical Bid, as required under the Note to Clause 3.7.6. Sri Lanka CERT reserves the right, at its sole discretion, to assess whether a submitted certification constitutes an acceptable equivalent to ISO 27001 based on its scope, audit rigor, and independence, during technical evaluation.
12	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the	Kindly confirm whether all platform hosting/data storage must remain within Sri Lanka (data residency), or whether global cloud regions are acceptable provided they are disclosed, given the sensitivity of monitoring 250 Sri Lankan government organizations.	As per the Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.10 and 3.7.11→ Pg. No. 55,56 in RFP.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
	Bidder → 3.7.10 and 3.7.11→ Pg. No. 55,56		
13	Section III. Evaluation and Qualification Criteria → Table 3.7 – Eligibility and the Qualifications Requirements of the Bidder → 3.7.5 and 3.7.6.1 to 3.7.6.4 → Pg. No. 54,55 Section IV. Bidding Forms → Table 4.5 → 3.7.5, 3.7.6.1 – 3.7.6.4 → Pg. No. 65 - 71	For international OEM client references and experience certificates, is notarization and/or apostille/consular legalization required, or are reference letters/contracts acceptable as issued on the client's letterhead?	As per the forms templates specified in Section IV. Bidding Forms → Table 4.5 → 3.7.5, 3.7.6.1 – 3.7.6.4 → Pg. No. 65 – 71 in RFP.
14	Section VI. Schedule of Requirements → Table 2 – Implementation and Payment Schedule → Pg. No. 83 to 85	The Bidding Document sets out a 7-milestone phased payment schedule (30% / 10% / 10% / 10% / 20% / 10% / 10%) tied to deployment, training, SIEM integration, and SLA review acceptance. Kindly clarify: a) The maximum number of days within which Sri Lanka CERT will process and release payment following the Bidder's invoice and the corresponding written acceptance/certification for each milestone b) Whether payments will be made in the same currency mix (USD/LKR) as quoted in the Price	(a) As per Section VII General Conditions → C. Payments → 12.4 → Page No. 150 in RFP. (b) Sr. No. 14 of Addendum 01 is relevant (c) Comply to the original requirement.

Sr. No.	RFP Reference	Query	Clarification Provided by Contracting Authority
		Schedule, or converted at the time of each payment using a prevailing exchange rate c) Whether a larger portion of the total contract value can be allocated upfront — e.g., a higher percentage at Milestone 1 (Deployment/Operational Acceptance) rather than spreading it evenly across the 12-month subscription term given that platform licensing, onboarding, and infrastructure costs are largely front-loaded for the Bidder ahead of the SLA-review milestones.	