Sri Lanka CERT (Pvt) Ltd.

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/2025/22

International Competitive Bidding (ICB)

16th September, 2025

CLARIFICATIONS TO THE QUERIES

Set 01

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
01	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	In case of JV, Can the bidder make this commitment share more than 2 parties? And, approval to incorporate reseller model in addition to the JV partnership.	Yes. The commitment may be shared among more than two JV partners as specified in the Addendum 01. A reseller model also be incorporated. (Refer Addendum 01).
02	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	In case of JV, Can the local partner be the Lead Partner?	OEM shall be the lead partner.
03	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	As this is a SaaS solution, OEM can handle entire thing without a JV partner. Can OEM directly bid?	In case of local OEM, the OEM can bid. However, for foreign OEMs, a local partner or local reseller/distributor is mandatory to bid.
04	Section II. Bidding Data Sheet → ITB 7.1 → Pg. No. 37	Can subcontracts be allowed?	Clause remains same. Comply to the original requirement.
05	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.6.4 → Pg. No. 52 & 53	Can the prior product implementation experience of the Bidder be changed to OEM?	Yes. Prior "specific experience" may be satisfied by the OEM, provided valid reference letters are produced. (Refer the Addendum 01)

06	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.9 → Pg. No. 54	Data collected by the proposed solution are already available publicly. Exploiting such vulnerability by an attacker wouldn't mean that the data has gone out from this particular platform. When signing a NDA this fact is requested to be considered.	Even if some data is public, aggregation and contextualization create sensitive insights. Hence, the 3.7.9 in the RFP ensures proper safeguards, preventing misuse and protecting the reputation and security posture of government organizations.
07	Section III. Evaluation and Qualification Criteria → 3.7.9 OEM Non-Disclosure → Pg. No. 54	Need access to data sharing anonymously for risk ranking, creating graphs, trending etc.	Permitted for analytical and statistical purposes only, provided all organization-specific identifiers are anonymized. (Refer the Addendum 01)
08	Section III. Evaluation and Qualification Criteria → 3.7.6 Quality and Security Requirements → Pg. No. 54	It was enquired if the partners are required to possess ISO 27001 certification.	ISO 27001 (or equivalent ISMS certification) is required for the OEM. Other partners are not required to hold separate ISO certifications, provided OEM certification covers the delivered solution. (Refer the Addendum 01)
09	Section IV. Bidding Forms → 4.11 Price Schedule Summary → Pg. No. 76	How do you want to break down 150 organizations in to multitenancy into with .gov.lk and .lk diversity?	The bidder must demonstrate tenant segregation methodology during the technical presentation. Clear separation between organizations should be proposed to ensure data isolation and secure multi-tenancy.
10	Section IV. Bidding Forms → 4.11 Price Schedule Summary → Pg. No. 76	How are 150 organizations defined? What is the scope of one organization?	One organization is defined as all parent domains of that entity (including new ones added during subscription) plus all subdomains under those parent domains.
11	Section IV. Bidding Forms → 4.11 Price Schedule Summary → Pg. No. 75	Indicate the volume of takedowns required during the subscription.	Bidders are expected to propose scalable takedown capacity. However, a baseline annual volume is defined to ensure minimum capability, with scope for expansion as threats evolved. (Refer the Addendum 01)
12	Section IV. Bidding Forms → 2. Implementation and Payment Schedule → Pg. No. 83	It is requested that the 20% retention from the total contract price be reduced to 10%, or alternatively, that operational compliance be secured through a performance guarantee.	Retention is reduced to 10%. (Refer the Addendum 01).
13	Section VI. Schedule of	Two clauses contradict.	The solution must be cloud-native SaaS but must be

	Requirements → Table 7 – Technical Specification → 1.7 SaaS & Hybrid On-Prem Deployment Support and 1.11 Cloud-Native, 99.98 HA & Multi-Unit Scalability → Pg. No. 88 & 89		able to integrate with on-premises threat intelligence platforms in future projects. Current procurement requires SaaS readiness with future compatibility.
14	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.18 30-Day End-of-Term Data Export & Handover → Pg. No. 90	Compliance is not possible.	Clause remains same. The purchaser requires data portability to ensure continuity and avoid vendor lock-in. Export must be in standard open formats.
15	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 Product usage reviews & feedback-driven improvement → Pg. No. 90	Requested to elaborate.	The vendor must regularly review how the tool is being used, ensure it keeps improving with new features and updates, and provide clear ways for users to report problems or suggest enhancements. The tool should not be static but should evolve continuously based on user feedback and changing threat needs.
16	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.16 24/7 Multichannel Support & Local Support Engineer → Pg. No. 90	Availability of local support engineer for the compliance was requested.	A qualified local support engineer must be available in Sri Lanka to ensure timely resolution of issues and compliance with SLA.
17	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.19 Post-Transfer Permanent Data Deletion & Written Confirmation → Pg. No. 91	Compliance is not possible.	Clause remains same. Bidder must ensure permanent deletion of government data post-transfer and provide written confirmation. This safeguards national security and data privacy.
18	Section VI. Schedule of	Are you flexible to bring the retention	Clause remains same. Longer retention ensures visibility

	Requirements → Table 7 – Technical Specification → 3.12 Historical threat intelligence data. → Pg. No. 97	period down to 3 years?	into persistent threats and long-term campaigns. Minimum 5 years retention is required.
19	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.6 Tools for hunting. → Pg. No. 102	What is the volume of malware analysis expected?	Approximately 15–30 malware samples per day across 10 analysts in the first year. This estimate may evolve with the threat landscape.
20	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.5 Safe dark-web access. → Pg. No. 102	What are the required platforms for sandboxing?	Windows, Linux, and macOS are mandatory. Additional OS support is considered value addition.
21	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.10 C2/DDoS visibility (Sri Lanka). Reporting C2/DDoS across Sri Lankan IP ranges → Pg. No. 103	Too broad. It is requested to re-visit this clause.	Clause remains same. Requirement remains. Visibility must cover IPs of 150 organizations, and CIDR ranges will be specified contract-award. This ensures national visibility of C2/DDoS activity.
22	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.13 Multilingual NLP → Pg. No. 103	Preserving the context and intent was difficult with limitations of the NLP out there.	Refer the Addendum 01.
23	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.1 Brand & keyword surveillance → Pg. No. 104	Defining the scope was requested.	Scope is defined under Section VI (Scope of Work). All brand assets, keywords, and organizational identifiers across the 150 organizations are in scope.

24	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.8 Bulk/Batch & Free-Text IOC Import (XLS/CSV/JSON/XML) → Pg. No. 106	Minimize the import part at the threat intelligence.	Refer the Addendum 01
25	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 9.6 Playbook-Based Alerts, Automation & Best Practices for attack Surface & Threat Intelligence → Pg. No. 109	Elaboration of expectation from this clause was requested.	Requirement revised. Changed to the clause was accommodated. (Refer the Addendum 01)
26	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110 & 111	Migration Support & Post-Transfer Permanent Data Deletion penalty clause requested to be revised or removed.	Penalty cannot be removed. (Refer the Addendum 01)
27	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.2 → Pg. No. 111	The response times 15 minutes are very stringent. It is requested to change the time window 2 to 4 hours.	SLA response times remain strict for critical incidents. For low/medium incidents, a longer response may be acceptable. (Refer the Addendum 01).
28	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112	The resolution times are also very stringent. It is requested to re-visit.	Resolution timelines remain strict for critical incidents. However, flexibility is allowed for lower severity incidents, with extended resolution windows. (Refer the Addendum 01).
29	Section III. Evaluation and Qualification Criteria → 3.3 Detailed Evaluation of	What are the specific organizations to be tested against during the demonstration?	It is up to the bidder to select critical 5 organizations.

	Technical Bids → Pg. No. 45		
30	Section III. Evaluation and Qualification Criteria → 3.3 Detailed Evaluation of Technical Bids → Pg. No. 46	Playbook arrangement is requested to demonstrate the methodology to integrate with ELK SIEM .	The diversity of potential solutions available for this procurement is significant. The Purchaser will not be in a position to fully assess the technical architecture of the proposed solutions until the submission of detailed technical proposals. Accordingly, the Purchaser requires the Bidders to propose an appropriate methodology and to demonstrate the integration of their solution with the ELK SIEM.

Set 02

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
31	Pg. No. 2 → General Experience	Change to "The Bidder/OEM 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."	Refer the Addendum 01.
32	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.9 → Pg. No. 51	Change to "The bidder shall be of either; • Local OEM (Original Equipment Manufacturer). • Local partners/Resellers of Foreign Companies/OEM products bidding for this tender registered in Sri Lanka and having MAF certificate from the OEM (at most 2 such partners from OEM) • JV where one party should be a Local party, which is a legally registered company in Sri Lanka and having physical presence (office) in Sri Lanka that has been in operation for the last Five (05) years. The other JV partner shall	Refer the Addendum 01.

		be an OEM (Original Equipment Manufacturer) of the proposed solution. The OEM shall be the Lead Partner."	
33	Section III. Evaluation and Qualification Criteria → 3.7.9 OEM Non-Disclosure → Pg. No. 54	May please be deleted.	Clause remains same. Non-disclosure obligations remain critical to safeguard sensitive information derived from CTI and ASM operations. This ensures proper handling of Sri Lankan government data.
34	Section III. Evaluation and Qualification Criteria → 3.7.10 OEM Data Residency & Sub-Processor → Pg. No. 54	May please be deleted.	Clause remains same. Data residency and sub-processor restrictions remain mandatory. Comply to the original requirement.
35	Section III. Evaluation and Qualification Criteria → 3.7.11 Cross-Border Transfer Notice → Pg. No. 55	May please be deleted.	Clause remains same. The cross-border transfer notification requirement remains unchanged to ensure full visibility into data flows and maintain compliance with government security controls. Comply to the original requirement.
36	Section VI. Schedule of Requirements → 1. Scope of Work → Pg. No. 82	Help with following information: a. List of 150 organisations with their respective domain names (TLD & subdomains) b. What is your understanding around multi tenancy? How many tenants are required? c. Will Cert SL be just monitoring these 150 organisations or it will also pass on the alerts and data to these organisations ?	a. List of organizations and domains will be shared only with the winning bidder. b. One tenant per organization is suggested. c. Sri Lanka CERT should be enabled by the proposed solution for monitoring, passing alerts and providing remedial actions to 150 organizations.

37	Section IV. Bidding Forms → 2. Implementation and Payment Schedule → Pg. No. 83	May please change to: 10% of the total contract price may be released against submission of CPG or to be released on quarterly basis.	No quarterly release/advance is envisaged under the current schedule. Refer Addendum 01.
38	Section IV. Bidding Forms → 4.2. Technical and Operational Manuals → Pg. No. 84	Requested to offer access to online support portal having access to latest and updated technical manuals/documentation.	Clause remains same. Comply to the original requirement. Online portals may be provided as an additional, but cannot replace the requirement.
39	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 10. Solution Licensing shall provide for 10 concurrent users.→ Pg. No. 86	Solution Licensing shall provide for 10 concurrent/named users.	Clause remains same. Platform must support 10 concurrent users in total. One account will be designated for the administrator, and the remaining nine can be named users based on their role. Concurrent access must be guaranteed.
40	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section B → Pg. No. 88	Please suggest if 5 tenants/projects would be sufficient to manage monitoring of 150 organisations. For ASM can we consider putting the domains in two groups. One with gov.lk domains and other with .lk domains ?	Distinct tenant for each of the 150 organization is the perceived requirement to ensure strict data segregation and accountability. The purchaser is expecting the bidder to propose the solution.
41	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.5. Multi -Tenancy, RBAC & Audit Logging → Pg. No. 88	May be changed to: “The solution must support multi - tenancy, role-based access control, ~~and audit logging~~ for secure, granular access management”	Clause remains same. Comply to the original requirement. Secure RBAC and audit trails are required for visibility and compliance.
42	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.6. Organization Add/Remove History Retention → Pg. No. 88	May please be deleted.	Clause remains same. Comply to the original requirement. Maintaining add/remove history is critical for auditability and traceability. This ensures visibility into changes of organizational coverage over time.

43	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.7. SaaS & Hybrid On-Prem Deployment Support → Pg. No. 88	May be changed to: SaaS Deployment Support: The solution should be supporting both SaaS based installation.	Clause remains same. Comply to the original requirement. Requirement remains cloud-native SaaS with future support for hybrid integration to on-prem Threat Intelligence Shared Platform. This ensures future scalability.
44	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.8. Secure RBAC, Granular Access & Audit Logging → Pg. No. 88	May be changed to: Secure RBAC, Granular Access & ~~Audit Logging~~: The platform must provide access for authorized users, with role-based access controls and audit logging. The portal should support secure, granular access management and ~~comprehensive activity tracking~~.	Reply to Sr.No. 41 is relevant.
45	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.11. Cloud -Native, 99.98 HA & Multi -Unit Scalability → Pg. No. 89	May be changed to: 1.11. Cloud -Native, 99.5 HA & Multi -Unit Scalability: The solution must be cloud-native, highly available (99.5 uptime), and scalable to accommodate organizational growth and multiple business units.	Refer Addendum 01.
46	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.12. Special Investigations Support → Pg. No. 89	May please be deleted.	Clause remainssame. Comply to the original requirement. Bidder must provide special investigations support to assist CERT with exceptional or unforeseen cases, including zero-day or advanced persistent threats.
47	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.13. Parent & Child Tenant -Wide Alerting → Pg. No. 89	May be changed to: 1.13. User Role Based Alerting: The platform should provide the facility to alert; a) All the authenticated users on the platform based on their granted role.	Requirement revised to support role-based alerting for authenticated users, covering attack surface, CTI, and dark web monitoring. (Refer the Addendum 01)

		a) Changes in the attack surface b) Alerts on cyber threat intelligence c) Alerts on deep & dark web monitoring	
48	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.16. 24/7 Multichannel Support & Local Support Engineer → Pg. No. 90	Please clarify if the bidder can provide a local support engineer directly from the bidder as OEM resource may not be available within Sri Lanka.	Clause remains same. Comply to the original requirement. Local engineer shall be provided by bidder, but must be Sri Lanka-based and available for business-hour support and escalations. OEM/global pool can supplement.
49	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.15. Single -Provider Solution & Unified Accountability → Pg. No. 90	May change as: 1.15. Single -Provider Solution & Unified Accountability: 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. However for seamless operations the platform should have the capability to raise takedown requests directly from the core OEM solution portal.	OEM solution provider may tie up with a reputed third party **only** for takedown services, provided takedown requests can be initiated directly through the OEM platform.
50	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.18. 30-Day End-of-Term Data Export & Handover → Pg. No. 90	May please be deleted.	Reply to Sr. No. 14 is relevant.
51	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.19. Post-Transfer Permanent	May please be deleted.	Reply to Sr.No. 17 is relevant.

	Data Deletion & Written Confirmation → Pg. No. 90		
52	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.2. Multi-Tenant Services for 150 Government Organizations → Pg. No. 92	Please suggest if 2 tenants would be sufficient to manage monitoring of 150 organisations one for gov.lk and other for .lk	Reply to Sr.No. 40 is relevant.
53	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.4. All Subdomains Treated as One Organization → Pg. No. 92	Please share either the list of 150 organisations and all the subdomains which are to be considered against each organisation	Reply to Sr.No. 36 (a) is relevant.
54	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.5. Parent–Child Multi-Tenancy with Segregated Policies → Pg. No. 92	May please be changed as: 2.5. Multi-Tenancy with Segregated Policies: The platform should support multi tenancy in its platform having separate admins and independent in a set of rules, policies, alerts and notifications.	Clause remains same. Comply to the original requirement. Requirement remains for parent–child multi-tenancy to ensure hierarchical segregation and enforce independent policies, rules, and alerts.
55	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.2. CTI Source Traceability → Pg. No. 94	May change to: CTI Source Traceability: The platform shall provide the facility to ~~trace the originated sources from where the CTI is collected~~. provide evidence to understand why an IOC is risky and reference to the source, if any.	Refer the Addendum 01
56	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.3. Essential Data Feed Attributes → Pg. No. 94	May change to: 3.3. Key CTI Attributes: The proposed platform must provide the following threat intel including but not limited to: a) IP	Clause remains same. Comply to the original requirement. Current attributes already meet operational requirements. Bidders may provide additional attributes as value-adds, but baseline scope remains unchanged.

		b) Domain c) Hashes d) CVEs e) Threat actors ~~f) Vectors~~ ~~g) Impacted systems~~ ~~h) Hostility~~ ~~i) Reputation~~ ~~j) Behavior~~ ~~k) Impacted systems~~ ~~l) Geo-location attributes~~ m) Industry attributes n) IP/Domain ownership attributes o) IP/Domain registration attributes p) Attack behavior details q) Malware, ransomware behavior details r) Phishing behavior details ~~s) Fraud behavior details~~ t) Bot behavior details u) C2 behavior details	
57	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4. Comprehensive Threat Intelligence Requirement → Pg. No. 95	May change to: 3.4. Comprehensive Threat Intelligence Requirements: The platform must provide detailed threat intelligence that include, but are not limited to: a) Goals of the threat actor ~~b) Conditions under which the threat is likely to exploit a vulnerability~~ c) Variants of the threat d) Current activity implicating the threat ~~e) Potential outcome for the organization~~	Clause remains same. Comply to the original requirement. Core requirement already encompasses comprehensive CTI. Additional parameters listed may be proposed as enhancements.

		~~if the threat is successful~~ ~~f) Indicators that the threat is currently acting against or impairing assets~~ ~~g) Recommended defense measures~~ ~~h) Assessment of the reliability of the source~~ ~~i) Reliability of the information itself~~ ~~j) Period of relevance of the threat~~ ~~k) Attribution confidence and supporting evidence~~ l) TTPs used m) Impact /Diamond Model analysis (operational, reputational, financial) n) Suggested detection and mitigation strategies/Threat Hunting packages ~~o) Visual elements (e.g., diagrams, timelines, attack paths) for clarity and engagement.~~	
58	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.5. Global, Regional & Sector-Specific Threat Feeds & IOCs → Pg. No. 95	May please be deleted.	Clause remains same. Comply to the original requirement. Global, regional, and sector-specific feeds are mandatory for contextual threat awareness at national and sectoral levels.
59	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.6. Organization -Specific Threat Feeds & IOCs → Pg. No. 96	May please be deleted.	Clause remains same. Comply to the original requirement. Organization-specific feeds are mandatory to deliver tailored intelligence relevant to each agency.
60	Section VI. Schedule of Requirements → Table 7 –	May be changed as: 5.12. Botnet & black -market	Refer the Addendum 01.

	Technical Specification → 5.12. Botnet & black -market surveillance → Pg. No. 103	surveillance: The platform should scan for ~~PH~~ exposure, botnet activity, and black-market transactions linked to monitored organizations.	
61	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.4. Multiple mitigation actions → Pg. No. 104	May please be deleted.	Clause remains same. Comply to the original requirement.
62	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.7. Continuous post-mitigation monitoring → Pg. No. 104	May please be deleted.	Clause remains same. Comply to the original requirement.
63	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.8. Technology -Specific Threat Feeds & IOCs → Pg. No. 96	May please be deleted.	Clause remains same. Comply to the original requirement.
64	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.12. Historical threat intelligence data → Pg. No. 97	May be changed to: 3.12. Historical threat intelligence data: The platform should provide at least 10 years of historical threat intelligence data, accessible via the portal and included in query results. This historical data should be available for advanced analytics and long -term trend analysis.	Clause remains same. Comply to the original requirement.
65	Section VI. Schedule of Requirements → Table 7 – Technical Specification →	May be changed to: 3.16. Open-Standard, Multi-Format CTI Export (Non Proprietary Formats): The	Refer the Addendum 01.

	3.16. Open-Standard, Multi-Format CTI Export (Non Proprietary Formats) → Pg. No. 97	platform shall provide the CTI exportable in multiple formats such as ~~JAON/XML~~, STIX/TAXII, JSON, XML, PDF, CSV, DOCX/PPTX ~~email~~ and no vendor-proprietary formats to be exported to other systems.	
66	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.19. Validation → Pg. No. 98	May please be deleted.	Clause remains same. Comply to the original requirement.
67	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.21. Threat Hunting → Pg. No. 98	May be changed to: 3.21. Threat Hunting: The platform must provide pre-build threat hunting tools/facility/packages such as SIGMA, YARA and Snort rules.	Clause remains same. Comply to the original requirement. Bidders may provide additional packages/rules as value-adds.
68	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.2. Automated assets discovery → Pg. No. 98	May be changed to: 4.2. Automated assets discovery: The platform should automatically identify all assets and sensitive information across the internet (the platform should not request the user to provide any information about the digital assets for monitoring on a specific organization). All exposed assets includes but not limited to external IPs, IP ranges, analysis of domain registrations to associate an WHOIS record, ~~cloud services~~, domains, subdomains, IP addresses, ~~cloud storage buckets~~, APIs, web applications, and third -party services, DNS records,	Clause remains same. Comply to the original requirement.

		digital certificates, technologies, ~~and associated personnel~~.	
69	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.3. Real-Time Attack Surface Monitoring & Alerts → Pg. No. 99	May be changed to: 4.3. Real-Time Attack Surface Monitoring & Alerts: The solution must provide ~~real-time~~/weekly monitoring and alerting for changes in the attack surface, including new assets, configuration changes, exposed services, and emerging vulnerabilities, enabling rapid detection and response.	Clause remains same. Comply to the original requirement. Real-time or near real-time updates are mandatory for effective threat prevention. Latency degrades security value.
70	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.7. External exposure identification → Pg. No. 100	May be changed to: 4.7. External exposure identification: The platform should enumerate all possible exposures to pinpoint exploitable weaknesses, but not limited to the following. a. Exploitable ports b. Exposed web interfaces & admin pages c. Legacy software d. Externally facing technologies with their versions e. Certificates issues ~~f. Email issues~~ g. Database issues open ports ~~h. Highjackable domain/subdomains~~ ~~i. Mail servers in black lists~~ j. Exposed cloud storage k. Leaked employee credentials (on exposed apps) l. Misconfigurations	Clause remains same. Comply to the original requirement.

71	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.9. Security score & prioritization for a specific organization → Pg. No. 100	May please be deleted.	Clause remains same. Comply to the original requirement.
72	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.10. Security score & prioritization for across the multiple organizations → Pg. No. 101	May please be deleted.	Clause remains same. Comply to the original requirement.
73	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.12. Multiple organization visibility → Pg. No. 101	May please be deleted.	Clause remains same. Comply to the original requirement.
74	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.5. Safe dark-web access → Pg. No. 102	Please suggest how many analysis per day needs to be done via sandbox Please suggest what environment types are required on sandbox (Eg windows, linux, mac and android)	Minimum 15-30 malware samples per day across 10 analysts is this year forecast.
75	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.6. Tools for hunting → Pg. No. 102	May change to: 5.6. Tools for hunting: The platform should provide tools for analyzing malware families and APT groups for hunting to speed investigation and detection including but not limited to SIGMA, YARA and Spark/Snort packages directly available via OEM web portal.	Clause remains same. Comply to the original requirement.

76	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.9. Brand & web presence protection → Pg. No. 103	May change to: 5.9. ~~Brand & web presence protection~~: The platform should track brand/domain abuse, ~~impersonations~~, phishing, and website defacements affecting Sri Lankan organizations.	Clause remains same. Comply to the original requirement.
77	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.11. Breach & leak detection → Pg. No. 103	May change to: 5.11. Breach & leak detection: The platform should generate ~~real-time~~ alerts when sensitive keywords, credentials, or account details appear across dark-web platforms, forums, marketplaces, and messaging apps, with malicious-content and credential-leak detection	Refer the Addendum 01.
78	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.4. Prebuilt report library → Pg. No. 105	May be changed to: 7.4. Prebuilt report library: The Platform should access ready-made reports/facility to create custom reports such as ~~Technical Executive~~, Executive Summary/Threat landscape Report, Phishing Domain, Account Breach, Incident, Regional, Industry, Ports & Services/Inventory Report, and Vulnerability reports. The solution may also offer ready use sector specific Intelligence Kits with sample queries to help with report creation.	Clause remains same. Comply to the original requirement.
79	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.6. Monitoring & trend insights → Pg. No. 105	May be changed as: The platform should support running scheduled and on demand scans with periodic monitoring ~~that includes monthly fraud/scam campaign reporting~~	Clause remains same. Comply to the original requirement.

		~~and seasonal trend reports to inform mitigation strategies.~~	
80	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.7. Alerting & noise reduction → Pg. No. 105	May be changed as: 7.7. Alerting & noise reduction: The platform should be able to configure alarm-based notifications and high-criticality alerts, deliver real-time alarm/alerts, ~~and leverage AI to reduce false positives and analyst alert fatigue.~~	Clause remains same. Comply to the original requirement.
81	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.8. Bulk/Batch & Free-Text IOC Import (XLS/CSV/JSON/XML) → Pg. No. 106	May please be deleted.	Reply to Sr.No. 24 is relevant.
82	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.4. Automated Open-Standard TI Ingestion & Export (No Lock-In) → Pg. No. 107	May be changed to; 8.4. Automated Open-Standard TI ~~Ingestion~~ & Export (No Lock-In): The platform must allow for automated ~~ingestion~~ and export of threat intelligence, IOCs, alerts, and vulnerability data in open standard formats (STIX, TAXII, JSON, CSV, XML) without vendor lock-in	Clause remains same. Comply to the original requirement.
83	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110	May please change to: Migration Support. The bidder shall perform ~~ingestion and~~ export of threat intelligence, ~~IOCs~~, alerts, and vulnerability data in open standard formats.	Refer the Addendum 01

84	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 111	"Post-Transfer Permanent Data Deletion" clause may be deleted.	Reply to Sr.No. 26 is relevant.
85	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.2 → Pg. No. 111	The asked SLAs are quite aggressive hence may please be changed as requested. The OEM may not be accepting the SLAs and hence the bidder may be penalized excessively for no reason. hence these may please be amended as per prevailing OEM SLA norms.	Reply to Sr.No. 27 is relevant.
86	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112 & 113	The asked SLAs are quite aggressive hence may please be changed as requested. The OEM may not be accepting the SLAs and hence the bidder may be penalized excessively for no reason. hence these may please be amended as per prevailing OEM SLA norms.	Reply to Sr.No. 28 is relevant.

Set 03

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
87	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section A → 6 → Pg. No. 86	a. Please clarify, are all these distinct 150 organizations/brands or 150 domains fall under CERT. b. Do we need Tenants for each organization/brand, because it adds operational overhead, we can manage all domains from a single tenant too, and generate different alerts per organizations	a. All 150 are distinct organizations. Each represents a separate legal/operational entity b. A dedicated tenant for each organization is the expected requirement. This ensures data segregation, compliance, and independent alerting. However, bidders may propose efficient approaches for centralized monitoring, but tenant isolation must remain enforceable.
88	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Section A → 8 → Pg. No. 86	Consider revising the SLA on all items, because a lot of cases are dependent on regulators and Hosting service providers, we can share our SLO (Service Level Objectives)	SLA requirements remain mandatory to protect critical services. While regulatory or third-party delays are acknowledged, bidders may propose reasonable exceptions supported by evidence. SLOs can be shared for internal benchmarking, but contractual SLA obligations cannot be diluted. Refer the Addendum 01
89	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.4. Multi-Tenant Management → Pg. No. 88	Managing 150 tenants or 150 companies will add a lot of workload and operational challenges. Clarify if Sri Lanka CERT wants to monitor all 150 departments from a single console and alert the respective department when required.	Sri Lanka CERT requires a centralized management console to oversee all 150 organizations while maintaining individual tenants. Alerts must be routed to each respective organization through the platform's multi-tenant architecture as per the RFP and the Addendum 01.
90	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.5. Multi-Tenancy, RBAC &	Managing 150 tenants or 150 companies will add a lot of workload and operational challenges. Clarify if Sri Lanka CERT wants to monitor all 150	Requirement is identical to Sr.No. 89. Sri Lanka CERT mandates centralized visibility combined with tenant-level segregation. RBAC and audit logging must ensure granular user access, accountability, and compliance.

	Audit Logging → Pg. No. 88	departments from a single console and alert the respective department when required.	Reply to Sr.No. 89 is relevant.
91	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.7. SaaS & Hybrid On-Prem Deployment Support → Pg. No. 88	Remove Hybrid from the tender for now, as Phase I is about availing TI & ASM intelligence to CERT via SAAS only.	Reply to Sr.No. 43 is relevant.
92	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.11. Cloud-Native, 99.98 HA & Multi-Unit Scalability → Pg. No. 89	CTI & ASM solutions are cloud-native, 99.5% HA. It is requested to consider changing HA to 99.5%	Reply to Sr.No. 45 is relevant.
93	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.18. 30-Day End-of-Term Data Export & Handover → Pg. No. 90	It is requested to remove this point from tender. Since the transfer of any data to a service provider that poses a risk of losing our proprietary or confidential information cannot be supported, assistance can definitely be provided in exporting eligible data.	Reply to Sr.No. 14 & 50 are relevant.
94	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.19. Post-Transfer Permanent Data Deletion & Written Confirmation → Pg. No. 91	It is requested to remove this point from tender. As only public information from the internet is collected and no PII or confidential information.	Reply to Sr.No. 17 & 51 are relevant.
95	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.2. Multi-Tenant Services for	Managing 150 tenants or 150 companies will add a lot of workload and operational challenges. Clarify if Sri Lanka CERT wants to monitor all 150	Reply to Sr.No. 89 is relevant.

	150 Government Organizations → Pg. No. 92	departments from a single console and alert the respective department when required.	
96	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.5. Parent–Child Multi-Tenancy with Segregated Policies → Pg. No. 92	Managing 150 tenants or 150 companies will add a lot of workload and operational challenges. Clarify if Sri Lanka CERT wants to monitor all 150 departments from a single console and alert the respective department when required.	Reply to Sr.No. 89 is relevant.
97	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.1. Coverage → Pg. No.101	Managing 150 tenants or 150 companies will add a lot of workload and operational challenges. Clarify if Sri Lanka CERT wants to monitor all 150 departments from a single console and alert the respective department when required..	Reply to Sr.No. 89 is relevant.
98	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.9. Brand & web presence protection → Pg. No.103	Monitoring 150 Different organizations for any brand abuse or impersonation cases will create 150 Brands for Monitoring, which will boost total cost of the license, we request you to revisit the ask and give some estimates of number of keywords or domains to be monitored.	Reply to Sr.No. 10 & 76 are relevant.
99	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.1 Brand & keyword Surveillance → Pg. No.104	Monitoring 150 Different organizations for any brand abuse or impersonation cases will create 150 Brands for Monitoring, which will boost total cost of the license, we request you to revisit the ask and give some estimates of number of keywords or domains to be monitored.	Reply to Sr.No. 98 is relevant.

100	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.2 Impersonation detection → Pg. No.104	Monitoring 150 Different organizations for any brand abuse or impersonation cases will create 150 Brands for Monitoring, which will boost total cost of the license, we request you to revisit the ask and give some estimates of number of keywords or domains to be monitored.	Reply to Sr.No. 98 is relevant.
101	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.2 Impersonation detection → Pg. No.104	Monitoring 150 Different organizations for any brand abuse or impersonation cases will create 150 Brands for Monitoring, which will boost total cost of the license, we request you to revisit the ask and give some estimates of number of keywords or domains to be monitored.	Reply to Sr.No. 98 is relevant.
102	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.8 Bulk/Batch & Free-Text IOC Import (XLS/CSV/JSON/XML→ Pg. No.106	Request you to remove or limit this point up to only importing files to sandbox, as ingesting any unverified 3rd party information can impact overall data integrity and overall quality of service. Hence, vendor TI Platform doesn't allow importing any IOC externally within the platform to protect the integrity and quality of the Intelligence. The only import possible is Sandboxing.	Reply to Sr.No. 24 & 81 are relevant.
103	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 9.6 Playbook-Based Alerts, Automation & Best Practices for Attack Surface & Threat Intelligence → Pg. No.109	Please clarify, what is the meaning of playbook-based alerts automation & best practice - is it about API integration support with SOAR?	Reply to Sr.No. 25 is relevant.

104	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110 & 111	It is requested to remove this point and penalty from the tender. As the transfer of any data to a new service provider that poses a risk of losing proprietary or confidential information cannot be supported, assistance can nevertheless be provided in exporting eligible data.	Reply to Sr.No. 26 is relevant.
105	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110 & 111	It is requested to remove this point and penalty from the tender. As only public information from the internet is collected and no PII or confidential information.	Reply to Sr.No. 26 is relevant.
106	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112 & 113	The asked SLAs are quite aggressive hence may please be changed as requested during the pre-bid meeting.	Refer the Addendum 01

Set 04

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
107	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.1. Unified Cyber Threat Intelligence (CTI), Attack Surface Management (ASM), Dark Web Monitoring, Takedowns & Reporting → Pg. No. 92	How many takedown credits required? Unlimited or 100/250/500 per organization ?	Reply to Sr.No. 11 is relevant.
108	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.4. All Subdomains Treated as One Organization → Pg. No. 92	Based on point 2.4, for the mentioned 150 government organization, can we consider that there will be only one domain/organization. 150 organization means 150 domains in total?	Each organization may have more than one parent domains.
109	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.1. Comprehensive Risk Reporting & Analysis for CTI, ASM, Deep/Dark Web & Takedowns → Pg. No. 105	Is reporting and alerting required on a daily or weekly or monthly basis?	Reporting is required on demand. Alerting is required as and when CTI, ASM & Depp/Dark Web is detected.
110	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.1. Brand & keyword	Provide the tentative count for the keywords for Brand & keyword surveillance ?	Reply to Sr.No. 23 & 99 are relevant.

	surveillance → Pg. No. 104		
111	Section I. Instruction to the Bidders → ITB 5.1 → Pg. No. 9	Kindly confirm whether the product should be deployed on-premises or in the cloud?	Reply to Sr.No. 13 is relevant.
112	Section VI. Schedule of Requirements → 4.1 Guidelines for Preparation of Submission → Pg. No. 84	Will having a subcontractor for takedown services be considered under this point ?	Reply to Sr.No. 04 is relevant.
113	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.7 SaaS & Hybrid On-Prem Deployment Support → Pg. No. 88	In the event, bidder propose to provide SaaS based platform hosted on cloud, or on-prem installation is also required?	Reply to Sr.No. 43 and Section IV. Bidding Forms → 4.11 Price Schedule Summary → Pg. No. 75 is also relevant.
114	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.12. Historical threat intelligence data → Pg. No. 97	Generally, threat intel data is considered obsolete after a few days or months, depending upon severity of the threat gathering and keeping 5 years of data would not be suggested. Is it okay if 3 years of historic data is provided, any critical threat, if arises, and where five-year-old intel data is required, we will go an extra mile to arrange the relevant information .	Reply to Sr.No. 64 is relevant.
115	Section IV. Bidding Forms → 4.5 General Experience → Pg. No. 64	Due to the Non-Disclosure Clause (NDC) in client engagements for ASM, CTI, and takedown services, confidential information such as client names, contract details including contract value, and employer details for 20 clients cannot be shared. It is also requested that	Clause remains same. Comply to the original requirement.

		this number be limited to 10 instead of 20.	
116	Section IV. Bidding Forms → Form 4.6.1 → Pg. No. 67	Three references may be obtained upon confirmation from the client employer. It is also requested that this number be limited to 10 instead of 20.	Clause remains same. Comply to the original requirement.
117	Section IV. Bidding Forms → Form 4.6.2 → Pg. No. 68	Three references may be obtained upon confirmation from the client employer. It is also requested that this number be limited to 10 instead of 20.	Clause remains same. Comply to the original requirement.
118	Section IV. Bidding Forms → Form 4.6.3 → Pg. No. 69	Three references may be obtained upon confirmation from the client employer. It is also requested that this number be limited to 10 instead of 20.	Clause remains same. Comply to the original requirement.
119	Section IV. Bidding Forms → Form 4.6.4 → Pg. No. 70	Multitenancy is supported by the platform; however, providing detailed information may be difficult. Kindly confirm whether this is mandatory	Clause remains same. Comply to the original requirement.
120	Section IV. Bidding Forms → Form 4.12 → Pg. No. 79	It is understood that the platform will be procured and training will be provided to 10 users. Clarification is requested on whether support in delivery by consultants is also required, and further elaboration is requested regarding the requirement for professional staff.	As per Section III. Evaluation and Qualification Criteria → 3.8 Key Personnel and Details → Pg. No. 55
121	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.3 Real-Time Attack Surface Monitoring & Alerts → Pg. No. 99	Do you prefer us to manually validate the data and send the alert via e-mail as in some cases automated mechanism may trigger false positive alerts?	Manual validation and e-mail alerts are not preferred. Alerts should be delivered through an automated mechanism with appropriate tuning and filtering to minimize false positives.

122	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.4 Automated Critical Vulnerability Detection & Reporting (Internet-Facing Assets) → Pg. No. 99	Critical vulnerabilities such as remote code execution, cross-site scripting (XSS), server information disclosure, default or unauthenticated access, and other high-risk issues require active testing for detection. Confirmation is requested on whether active testing of the internet-facing assets should be performed by the professional team, and clarification is further requested on the number of internet-facing assets to be considered.	The bidder's staff shall not be authorized to conduct any form of active scanning under, or in association with, the solution acquired by the purchaser unless or otherwise requested to comply with Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.12 1.12. Special Investigations Support → Pg. No. 89. Internet facing assets vary based on the organization.
123	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.13 High-accuracy, evidence-backed findings → Pg. No. 101	Preference is requested on whether the threats identified in the proposed platform for all tenants should be reviewed by the bidder's professional staff, with false positives removed and verified threat alerts and reports provided, or whether the requirement is to receive all findings directly from the platform itself.	Requirement is to receive all findings directly from the platform itself. Comply to the original requirement.
124	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.8 Messaging & social media platform monitoring → Pg. No. 103	In this case, some parts will need to be performed manually, as no fixed API may exist to monitor hacking forums. It is requested to confirm whether the use of HUMINT for manual execution may be proposed.	Manual execution is not accepted. Comply to the original requirement.
125	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.10 C2/DDoS visibility (Sri Lanka) → Pg. No. 103	Confirmation is requested on whether manual monitoring for mentions of C2/DDoS for 150 organizations by the professional team is acceptable.	Manual monitoring for mentions of C2/DDoS for 150 organizations by bidder's staff is not acceptable. Comply to the original requirement.

126	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.11 Breach & leak detection → Pg. No. 103	Confirmation is requested on whether it is acceptable for the breach and leak data to be validated by the professional team and the alert to then be sent via e-mail.	Not acceptable. Comply to the original requirement.
127	Section VI. Schedule of Requirements → Table 7 – Technical Specification → Reports/Analysis → Pg. No. 105	How frequently you want the report - Weekly / Monthly ?	Reporting is required on demand.
128	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 9.4 Dedicated/Shared Intelligence Analyst → Pg. No. 108	Clarification is requested on the number of dedicated professional analysts required, as well as the specific requirements for these analysts.	A dedicated or shared intelligence analyst. Requirement is as per the clause 9.4.
129	Section VI. Schedule of Requirements → 5. Other Documents to be submitted by the bidder → 5.1 → Pg. No. 110	It is preferred that Software Architectural Diagrams, As-built Documents, Troubleshooting Guides, Operational Checklists, and User Manuals be shared in both soft and hard copies upon award of the contract. Confirmation is requested on whether this will be acceptable.	Not acceptable. Comply to the original requirement.
130	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.2 → Pg. No. 111	For the SLA on incident response, clarification is requested on the types of incidents being referred to.	Refer the Addendum 01.
131	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112	For the SLA on incident resolution, clarification is requested on the types of incidents being referred to. Further clarification is also requested on how incidents classified as critical or high are	Refer the Addendum 01.

		defined, and on what types of incidents fall under these categories.	
132	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112	Some relaxation with respect to the incident response time SLA is requested. For example, in the case of a phishing incident, the time of resolution is completely dependent on the hosting provider's investigation and resolution process; therefore, no SLA can be committed in such cases.	Refer the Addendum 01.
133	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.4 Multi-Tenant Management → Pg. No. 88	What level of data and operational isolation is required between Child Tenants? (e.g., full logical isolation, RBAC, encryption boundaries).	The bidder to provide the multitenancy management in their proposal in detail and present them during the demonstration.
134	Section VI. Schedule of Requirements → 2. Implementation and Payment Schedule → 3. User Training and Manuals → Pg. No. 83	Will CERT accept virtual on boarding and training sessions supplemented by an online portal, or is in-person training mandatory?	In-person training mandatory.
135	Section III. Evaluation and Qualification Criteria → 3.3.1 Evaluation components and marking scheme Implementation and Payment Schedule → Pg. No. 46	Is there a preferred method of integration (e.g., API, log shipping via Filebeat/Logstash, syslog)?	Reply to Sr.No. 30 is relevant.
136	Section VI. Schedule of Requirements → 2. Implementation and Payment Schedule → 2. Integration with SIEM → Pg. No. 82	Is the 35-day integration timeline negotiable based on complexity, or is it a hard deadline?	Comply to the original requirement.

137	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.1 Threat feeds & integrations → Pg. No. 94	What is the required retention period for Indicators of Compromise (IOCs) within the platform? Should all IOCs be stored indefinitely, or only for a defined period (e.g., 30 days, 90 days, 1 year)	As per Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.12 Historical threat intelligence data → Pg. No. 97
138	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.2 Seamless Push/Pull Integrations with TISP, EDR, Firewalls & DNS Proxy → Pg. No. 107	Will SL CERT handle integration with existing tools (TISP, EDR, etc.), or is the bidder expected to provide engineering support?	Bidder is required to do Installation, Configuration, System Integration and Tune-up. Section IV. Bidding Forms → 4.11 Price Schedules → Pg. No. 75 is also relevant.
139	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.3 Robust REST & STIX/TAXII APIs for Push/Pull Integrations → Pg. No. 107	Confirm if there are any limits on the number of API requests (per minute/hour/day) for push/pull integrations via REST or STIX/TAXII. If so, kindly specify the rate limits, burst thresholds, and any throttling or quota policies that apply.	The Purchaser sets no explicit API rate caps. The Contractor shall disclose any platform-side throttling or quotas and ensure integrations function reliably via queuing, backoff, and retry mechanisms.
140	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.2 Multi-Level Reporting: Global, Country, Sector & Organization → Pg. No. 105	Clarify whether the global, country, sector, and organization-level reports are expected to be auto-generated by the platform or manually curated. Additionally, will SL CERT provide a predefined sector taxonomy for reporting purposes, or should the platform support customizable sector definitions?	Global, country, sector, and organization-level reports are expected to be auto-generated by the platform.
141	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.6 Tools for hunting → Pg. No. 105	Should threat hunting tools include behavioural analysis, sandboxing, and YARA rule support?	Yes.

142	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.8 Secure RBAC, Granular Access & Audit Logging → Pg. No. 88	Clarify whether user account creation, role assignment, and deactivation within the platform will be managed directly by Sri Lanka CERT, or if these administrative functions will be handled by the bidder during and after deployment	The purchaser shall be enabled to handle these function using the proposed solution. However, Bidder is required to do Installation, Configuration, System Integration and Tune-up during the deployment.
143	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.4 Comprehensive Threat Intelligence Requirements → Pg. No. 95	The incidental points, including impact analysis, will be performed using Threat Hunting and Malware Analysis tool which will be deployed additionally.	Comply to the original requirement.
144	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.7 Asset-Aware Threat Visualization & Contextual Mapping → Pg. No. 96	Confirm whether the platform is expected to integrate with the organization's asset inventory or CMDB to enable real-time contextual mapping of threats. Please clarify if it is required in the same platform?	Required in the same platform
145	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.8 Technology-Specific Threat Feeds & IOCs → Pg. No. 96	Clarify which technologies are in scope for technology-specific threat feeds and IOC data (e.g., Windows, Linux, cloud services, network devices, applications).	Should cater the target organization’s technologies discovered through the ASM discovery.
146	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.16 Open-Standard, Multi-Format CTI Export (No Proprietary Formats) → Pg. No. 97	Confirm whether all listed export formats (e.g., STIX/TAXII, JSON, XML, PDF, CSV, email) are mandatory for compliance, or if support for a subset is acceptable.	Reply to Sr.No. 65 is relevant.

147	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.21 Threat Hunting → Pg. No. 98	Bidder will provide a third party solution to perform Threat Hunting activity and kindly confirm if any existing security solution (EDR, SIEM) is deployed in the environment.	Proposed solution shall have in-built threat hunting tools/facility. Comply to the original requirement.
148	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 9.2 Unlimited Online Training Portal & Mandatory Courses → Pg. No. 108	Clarify the frequency of training sessions and the type of training expected.	On demand online training portal is expected.

Set 05

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
149	Section III. Evaluation and Qualification Criteria → 3.3 Detailed Evaluation of Technical Bids → (i) → Pg. No. 46	Is it possible to share the required POC scope, which the bidder needs to demonstrate to showcase the platform's capabilities, by 13th or 14th October? It is suggested to define at least 5 entities from the 150 entities planned for onboarding to the platform at the time of live implementation and request the respective bidders to demonstrate their solutions based on the captured data of those 5 entities.	Reply to Sr.No. 29 is relevant.
150	Section IV. Bidding Forms → 4.11 Price Schedules → Pg. No. 75	Clarify regarding the user access requirements. Specifically, does Sri Lanka CERT require platform access for all 150 government organizations individually, or would providing 10 logins for SL CERT analysts to manage the solution across all 150 organizations be sufficient?	Sri Lanka CERT requires 10 analyst accounts with full privileges to administer and monitor all 150 organizations individually.
151	Section IV. Bidding Forms → 4.11 Price Schedules → Pg. No. 75	Clarify regarding the RFP requirement for takedown support under the one-year subscription. To ensure clarity and proper service planning, we request that the RFP specify a definite number of takedown requests included within the subscription period, rather than leaving it open-	Reply to Sr.No. 11 is relevant.

		ended.	
152	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.16 24/7 Multichannel Support & Local Support Engineer → Pg. No. 90	Is it required 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. Reply to Sr.No. 48 is also relevant.
153	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 Product Usage Reviews & Feedback-Driven Improvement → Pg. No. 90	Not applicable: since we are only looking at publicly available data and are not processing any internal/confidential data.	Even though data is public, the value-added intelligence, integrations, and service performance require structured evaluation. Reply to Sr.No. 15 is relevant.
154	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.18 30-Day End-of-Term Data Export & Handover → Pg. No. 90	Not applicable: since we are only looking at publicly available data and are not processing any internal/confidential data.	Even if the platform ingests only public-source information, the historical tenant data and all derivative artifacts (correlations, enrichments, scoring, alerts, takedown case trails, audit logs, reports, dashboards/configs, etc.) are contract deliverables and must be exportable within 30 days of term end, at no additional cost, in an industry-standard, machine-readable format with integrity checks and documentation. This is necessary to ensure continuity of operations and investigations when transitioning to a new provider. Reply to Sr.No. 14 & 50 are relevant.
155	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.20 Takedown, Incident Response & Escalation Support → Pg. No. 91	<u>Scope of Takedown Requests</u>: We request clarification on the types of content, platforms, or threats for which takedown support is expected. Additionally, it would be helpful to understand any jurisdictional or	<u>Scope of takedown support:</u> Malicious or impersonating domains/URLs, fake or infringing social-media accounts/pages/groups, fraudulent app-store listings (official/unofficial), and illicit listings of government-related data discovered through CTI/ASM and dark-web monitoring.

		regulatory limitations that may apply, so that bidders can accurately define the boundaries of their support while ensuring compliance with legal requirements. <u>Incident Response Expectations</u>: Please clarify the level of incident response support required. Specifically, whether the support is limited to advisory services, includes on-site intervention, or requires full technical remediation. Furthermore, it would be beneficial to understand any predefined Service Level Agreements (SLAs) or expected response times based on incident severity to ensure timely and effective response. <u>Escalation Process & Points of Contact</u>: We seek details on the internal escalation hierarchy and decision-making authority for critical incidents. Clarification on any restrictions regarding the number of escalation levels, as well as the involvement of external stakeholders, will help ensure a clear and structured escalation process. <u>Risk Considerations & Scope Limitations</u>: To manage operational and legal risks effectively, we request confirmation on	<u>Incident-response expectations:</u> Incident-response under 1.20 is primarily related to incidents detected by the platform (e.g., phishing domains, brand abuse, breach sightings) and platform unavailability. The bidder shall maintain documented playbooks for triage, containment recommendations, evidence preservation, takedown initiation, and stakeholder communications. <u>Escalation process & points of contact:</u> The bidder must provide a 24×7 L1 contact, with L2/L3 OEM escalation contacts and named service manager. CERT will designate authorised POCs and approval authorities post-award. <u>Exclusions & boundaries (risk considerations):</u> Internal system forensics or hands-on remediation inside government networks is not included in 1.20 scope. The bidder should provide clear approach in the proposal for takedown requests, incident response, and escalation of critical threats, with clear processes and points of contact.

		any exclusions or boundaries related to the support scope. This includes clarifying limitations concerning content types, platforms, or legal constraints. Additionally, we would like to confirm whether the expected support includes proactive monitoring of threats or is purely reactive based on reported incidents.	
156	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.3 Coverage: .lk, gov.lk & All gov.lk Subdomains → Pg. No. 92	We seek clarification regarding the coverage requirement specified in Item 1.2. Specifically, we would like to understand whether the coverage needs to include all subdomains of gov.lk, including any newly created subdomains during the subscription period. Additionally, we request confirmation on whether there are any exceptions or exclusions within the .lk, gov.lk, or its subdomains that should not be included in the scope. Finally, please clarify whether the solution is expected to provide continuous monitoring and protection for all these domains and subdomains, or if the coverage is limited to specific services or URLs under these domains. This clarification will help ensure that the proposed solution aligns accurately with the expected scope and avoids any gaps in coverage.	Reply to Sr.No. 10 is relevant.
157	Section VI. Schedule of Requirements → Table 7 –	Need clarification.	Reply to Sr.No. 21 and 125 are relevant.

	Technical Specification → 5.10 C2/DDoS visibility (Sri Lanka → Pg. No. 103		
158	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.13 Multilingual NLP → Pg. No. 103	Need clarification.	Reply to Sr.No. 22 is relevant.
159	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 57.8 Bulk/Batch & Free-Text IOC Import (XLS/CSV/JSON/XML) → Pg. No. 106	Need clarification.	Reply to Sr.No. 24 is relevant.
160	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110 & 111	Not applicable since we are only looking at publicly available data and are not processing any internal/confidential data	Reply to Sr.No. 26 is relevant.
161	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.2 & 6.3 → Pg. No. 111 & 112	We kindly request Sri Lanka CERT to provide their response regarding the possibility of considering the bidder's suggested timeframes. As discussed during the meeting, most bidders proposed an automated response within 15 minutes for escalated incidents, and we seek formal confirmation from Sri Lanka CERT on the acceptance of this timeframe. Additionally, it is suggested to categorize	Reply to Sr.No. 130, 131 & 132 are relevant.

		incidents as Critical, High, Medium, and Low, with separate SLAs and resolution timeframes defined for each category in line with industry standards. We also recommend aligning the server credits accordingly to reflect the differentiated treatment of incident categories.	

Set 06

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
162	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7 → Pg. No. 86	Provide the list of all the main & related domains to be monitored for the whole 150 organizations, as this would be required for a proper sizing of the solutions.	Reply to Sr.No. 36 (a) is relevant.
163	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.2 OEM Authorization Letter for Full-Scope Service Delivery → Pg. No. 87	OEM provides solutions under reseller model for SaaS products and services. We would like to know the feasibility of accommodating a Master Service Agreement with the OEM to provide the proposal for the project.	Reply to Sr.No. 32 is relevant.
164	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.6 Organization Add/Remove History Retention → Pg. No. 88	Confirm the retention time for this historical data?	5 years.
165	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.7 SaaS & Hybrid On-Prem Deployment Support → Pg. No. 88	Request you to remove this point as most solutions are cloud native.	Reply to Sr.No. 13 & 43 are relevant.
166	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.12 Special Investigations	The specification does not outline the context where the services should be included and what would be the conditions for an investigation to be	Reply to Sr.No. 46 is relevant.

	Support → Pg. No. 89	considered as a special investigation. This is far more open-ended to understand an exact scope and would you be able to specify the context applicable for this solution.	
167	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.20 Takedown, Incident Response & Escalation Support → Pg. No. 90	The specification does not include the number of hours or incidents that should be covered under the contracts for the engagement. It would be required to specify a number of engagements or hours the IR and Takedown services would be required.	Reply to Sr.No. 11 is relevant.
168	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.3 Coverage: .lk, gov.lk & All gov.lk Subdomains → Pg. No. 92	Provide a list of all the main & related domains to be monitored for the whole 150 organisations, this would be required for proper sizing of the solutions.	Reply to Sr.No. 36 (a) is relevant.
169	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.10 IOC enrichment & risk → Pg. No. 96	Confirm how many IOC enrichments queries will be performed by all the organisations in 1 year, as this would be required for solution sizing.	Enrichment and risk scoring shall be performed automatically for every IOC ingested or generated by the platform across all tenants. No annual query quota is specified.
170	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.11 Advance Search → Pg. No. 96	Confirm how many advance threat hunting search queries will be performed by all the organisations in 1 year, as this would be required for solution sizing.	No annual numeric limit on advanced search queries is prescribed. The platform shall support advanced searches across IOCs, malware, threat actors, and TTPs and allow alerting directly from saved searches. Searches shall cover at least five (5) years of historical TI data. The Contractor shall guarantee performance suitable for 10 concurrent CERT users, stating minimum sustained throughput and typical search response times for representative workloads.

171	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.13 Malware analysis capability → Pg. No. 97	Explain this point to help understand the exact requirement? How many malware file analysis are required by all organisations in 1 year, as this would be required for solution sizing.	Reply to Sr. No. 19 is relevant.
172	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.14 Multilingual capability → Pg. No. 97	Remove this point as most threat actor specific data and attack threats are in English language over the dark web, as this would be required for solution sizing.	Clause remains same. Comply to the original requirement.
173	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 4.1 Continuous active/passive reconnaissance → Pg. No. 98	Provide a list of all the main & related domains to be monitored for the whole 150 organizations, as this would be required for solution sizing.	Reply to Sr.No. 36 (a) is relevant.
174	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.2 Native Multilingual Analysis & Translation (No Third-Party Plugins) → Pg. No. 102	Remove this point as most threat actor specific data and attack threats are in English language over the dark web, as this would be required for solution sizing.	Clause remains same. Comply to the original requirement.
175	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.4 Advanced search → Pg. No. 102	Remove it from here. Regarding dark web monitoring, please let us know the approximate keywords for all the 150 organizations to be monitored. This information is required for the sizing of the solution.	Clause remains same. Comply to the original requirement. Scope is as per the Section VI. Schedule of Requirements → 1. Scope of the Work. Reply to Sr.No. 10 also relevant.
176	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.13 Multilingual NLP → Pg. No. 103	Remove this point as most threat actor specific data and attack threats are in English language over the dark web.	Clause remains same. Comply to the original requirement. Reply to Sr.No. 22 is relevant.

177	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.3 Takedown initiation & portal → Pg. No. 104	How many yearly takedowns are required by all the organizations, as this would be required for solution sizing.	Reply to Sr. No. 11 is relevant.
178	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.4 Multiple mitigation actions → Pg. No. 104	Deindexing requested in this point cannot be done by vendors as it can only be done with search engines and web hosting providers or domain owners. Request you to kindly remove this point.	The Contractor shall initiate and manage requests for de-indexing, blacklisting, and browser-alerting using the official processes of the relevant platforms/hosts/registrars, provide evidence packs, track and document progress to closure, and conduct post-mitigation monitoring.
179	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.5 Anti-Phishing Web Tokens → Pg. No. 104	Let us know how many anti-phishing web tokens are required by all the organizations, as this would be required for solution sizing.	Minimum 5 tokens per organization.
180	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.1 Integration with Existing SOC (ELK SIEM) → Pg. No. 106	Confirm how many such integrations are needed across all the organizations? Also, please confirm if it would a central integration or individual separate integrations for each of the organisation?	The platform must support integration with existing SOC tools and security infrastructure, including ELK SIEM which is currently operated by Sri Lanka CERT.
181	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 8.2 Seamless Push/Pull Integrations with TISP, EDR, Firewalls & DNS Proxy → Pg. No. 107	Confirm how many such integrations are needed across all the organizations? Also, please confirm if it would a central integration or individual separate integrations for each of the organisation?	The platform must support integration with TISP which will be implemented and operated by Sri Lanka CERT. The platform must also support integration with EDR, Firewalls & DNS Proxy integrations of individual 150 organizations via the TISP.
182	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 9.2 Unlimited Online Training	Training portal access is based on users, and hence could you please provide the approximate number of users required to be trained across all organizations?	Ten (10) analysts.

	Portal & Mandatory Courses → Pg. No. 108		
183	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 9.4 Dedicated/Shared Intelligence Analyst → Pg. No. 108	The OEM support analysts will be assigned from a global pool, based on the type of query or the request raised. Therefore, we would like to know whether the requested resource would be from the local bidder or in case of OEM, the resource allocation would be based on the request raised.	Reply to Sr.No. 48 is relevant.
184	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112	The resolution times outlined for different service levels are tough to meet as the entire solution would encompass of IR and Takedown service, which depends on number of external counterparts including law enforcements. Further, none of the OEMs provide these strict resolution timeframes for the associated services while the guaranteed response times are provided. Therefore, it is requested to either remove the resolution times to provide a far more lenient timeframe, owing to the nature of the solution and services requested.	Reply to Sr.No. 27 & 28 are relevant.
185	Section IX. Contract Forms → Appendix 7. Terms and Procedures for Payment → 7.2 Terms of payment → Pg. No. 207	The deployment type of the solution requires payments to be made for the vendors in-advanced to gain the required license to access the platform. The current payment terms outlined is to provide 80% of the payment at the completion of the deployment in 3 stages, with remainder of 20% being on-	Reply to Sr.No. 12 is relevant.

		hold for the period of 1 year. We are making to request to reduce this 20% to 10%, while accepting a performance bond issued from a license bank in Sri Lanka.	
186	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	The concern raised in the pre-bid meeting includes a request to increase the number of parties in JV from 2 to more. This would make bidding parties to have paused their legal processes until the clarification is received on the on the number of eligible parties. Therefore, we would further request to consider an extension for the project submission.	Refer the Addendum 01. No extension to the submission deadline.

Set 07

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
187	Pg. No. 2 → 2 (a)	Given this deployment is relatively new in Sri Lanka we request change to show references is from the OEM.	Reply to Sr.No. 05 is relevant.
188	Pg. No. 2 → 2 (b)	Regarding reference letters it should be taken into consideration that certain customers may not agree to provide reference letters citing confidentiality. We request the number be lowered to 2.	Comply to the original requirement.
189	Pg. No. 51	Regarding JV, we would request to have 1. A triparty agreement between SL CERT, local partner and the OEM (or) 2. The local partner provides the implementation and support services directly with a back-to-back agreement with the OEM We request in change the JV requirement to either of the above.	Eligible Bidders are as per the Addendum 01.
190	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.6.1 to 3.7.6.4 → Pg. No. 52 & 53	Given this deployment is relatively new in Sri Lanka we request change to show references is from the OEM.	Reply to Sr.No. 05 is relevant.

191	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.7 → Pg. No. 54	It is requested this to be updated in line with request made in Sr. No. 190.	Reply to Sr.No. 05 is relevant.
192	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.8 → Pg. No. 54	It is requested this to be updated in line with request made in Sr. No. 190.	Reply to Sr.No. 05 is relevant.
193	Section IV. Bidding Forms → 4.11 Price Schedules → Pg. No. 75	Clarify if 150 government organizations mean 150 domains (URLs)	Reply to Sr.No. 10 is relevant.
194	Section IV. Bidding Forms → 4.11 Price Schedules → Pg. No. 75	Clarify number of takedowns per year.	Reply to Sr.No. 11 is relevant.
195	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.12. Special Investigations Support → Pg. No. 89	Clarify if remote resources based out of Sri Lanka can fulfil this task.	Reply to Sr.No. 46 is relevant.
196	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.16 24/7 Multichannel Support & Local Support Engineer → Pg. No. 90	Clarify if remote resources based out of Sri Lanka can fulfil this task.	Reply to Sr.No. 16 & 48 are relevant.
197	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.18. 30-Day End-of-Term Data Export & Handover →	Note that by nature of the solution it aggregates and compiles output based on its internal IP which will vary from solution to solution. Therefore, it will not be possible to migrate data from one	Reply to Sr. No. 14 is relevant.

	Pg. No. 90	solution to another. We request to kindly remove this requirement.	
198	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.19 Post-Transfer Permanent Data Deletion & Written Confirmation → Pg. No. 91	Kindly note that the data is collected based on what is available in the public domain. Even if the solution provider deletes the data from their system, it does not imply the data has been completed deleted from all external sources. We request to take this into consideration to update the wording.	Reply to Sr.No. 17 is relevant.
199	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.10 C2/DDoS visibility (Sri Lanka). Reporting C2/DDoS across Sri Lankan IP ranges → Pg. No. 103	We request to modify this requirement since threat actors from Sri Lanka can use public cloud services to launch attacks that does not have Sri Lankan IP ranges.	Reply to Sr. No. 21 is relevant.
200	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.9. Brand & web presence protection → Pg. No. 103	We request to define and list the brands, keywords and sites to be monitored.	Reply to Sr. No. 10 and 36 (a) are relevant.
201	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.13 Multilingual NLP → Pg. No. 103	Given NLP are still in its maturing stages when it comes to multilingual capabilities, we request change requirement to simple translation and remove requirement to preserve context and intent.	Reply to Sr. No. 22 is relevant.
202	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 6.2 Impersonation detection →	We request to define the scope for impersonation detection.	Reply to Sr. No. 10 is relevant.

	Pg. No.104		
203	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.17 Product Usage Reviews & Feedback-Driven Improvement → Pg. No. 90	We request to define the scope of usage reviews, feedback session and continuous improvement for clarity.	Reply to Sr.No. 15 is relevant.
204	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 111	"Post-Transfer Permanent Data Deletion" clause may be deleted.	Reply to Sr.No. 26 is relevant.
205	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.2 → Pg. No. 111	Clarify if incidents are referring to incidents related to platform or arising from alerts that the system generates (e.g. fake domain alert for takedown). We also request to have incident tiers and provide definition for Critical, High and Low incidents Given this is SaaS based and we have an availability SLA. We request to revise the response SLA from 15 mins for a) Critical Incidents – 30 mins b) High Incidents – 45 mins c) Low Incidents – 2 hours	Reply to Sr.No. 27 is relevant.
206	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 →	As above please clarify what incidents are being referred here. If incidents related to platform, we	Reply to Sr.No. 28 is relevant.

	Pg. No. 112	request to remove resolution time, given that this is passive monitoring solution and the data will remain with no operational impact. Solution should be measured based on availability SLA. If incidents related to alerts, the rectification will depend on external party. E.g. for takedown services it depends on the hosting provider and there for we request to remove this SLA as well. We request to remove penalty clauses as well.	
207	Section II. Bidding Data Sheet → ITB 7.1 → Pg. No. 37	We request to change this given takedown services are generally performed by sub-contractors.	Reply to Sr.No. 04 is relevant.
208	Section IX. Contract Forms → Appendix 7. Terms and Procedures for Payment → 7.2 Terms of payment → Pg. No. 207	We request reduction of payment terms to 10%. This will increase the price of the solution given that the bidder has to factor in finance cost as well for up to 12 months.	Reply to Sr.No. 12 is relevant.

Set 08

Sr.No.	RFP Reference	Query	Clarification Provided by Contracting Authority
209	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	Considering the scope of the project, please increase the number of JV members.	Reply to Sr.No. 01 is relevant.
210	Section II. Bidding Data Sheet → ITB 24.2 → Pg. No. 40	Clause states "Bids submitted by a joint Venture: Power of Attorney (either notarized or attested by an appropriate authority in the Proposers home Country; It shall include an undertaking Signed by all parties…." Please elaborate the exact requirement of the POA, including the requirement "signed by all parties". Generally, different countries have different legal requirements and methodologies in arranging a POA, and hope to separate either notarized or attested by an appropriate authority in the Proposer's home Country. In case a POA is obtained in Sri Lanka, it shall be registered.	Refer the Addendum 01.
211	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.6.1 to 3.7.6.4 → Pg.	The bidder's proposed solution with the ability to provide services mentioned from 3.7.5.1 to 3.7.5.3 in a multitenant environment for 5 clients during the last five (05) years prior to the Bid	Comply to the original requirement.

	No. 52 & 53	Submission Deadline. Please reduce the number of project experiences.	
212	Section VI. Schedule of Requirements	**Attack Surface Management (ASM) Requirements** • What types of assets are to be monitored (e.g., domains, IPs, cloud resources, SaaS)? • Is continuous, passive, and/or active scanning required? • Should ASM include dark web, surface web, and deep web monitoring? • Are capabilities for risk scoring and asset classification expected? **Malware Analysis & Sandbox Environment** • Should the solution include static, dynamic, and behavioural malware analysis capabilities? • Are there specific sandbox environments or OS variants required (e.g., Windows 11, Android, Linux)? • Should the malware lab support automated report generation and YARA rule matching?	The client requirements have been clearly defined in the RFP technical specification. It is the responsibility of the bidder to propose a suitable solution architecture to fulfil the needs of the client.

		Integration & Interoperability • What existing security infrastructure (SIEM, SOAR, EDR, etc.) should the CTI/ASM system integrate with? • Are APIs required for integration with third-party tools? • Is bidirectional data sharing expected (e.g., exporting threat intel to SIEM)? **Multi-Tenant & Scalability** • Is the solution expected to be multi-tenant with role-based access control (RBAC)? • What is the projected number of tenants/users per tenant? • Should the platform support horizontal scaling for cloud or hybrid deployments? **Automation & Response** • Should automated enrichment and correlation of alerts from CTI/ASM be implemented? • Is integration with SOAR for	

		automated response playbooks required? • Are there specific types of alerts or incident response workflows to be embedded? **Data Privacy & Localization** • Are there data residency requirements (e.g., must data remain within Malaysia)? • Should the platform provide encryption at rest and in transit? • Are data anonymization or redaction features needed? **Reporting & Visualization** • What are the expectations for dashboards, customizable or predefined? • Should reporting support regulatory compliance standards (e.g., NIST, ISO 27001)? • Is multi-language report generation required? **Deployment & Architecture** • Is the solution expected to be on-	

		premises, cloud-based, or hybrid? • Are there preferred cloud providers or restrictions (e.g., GovCloud, MyGovUC)? • Is containerization (e.g., Docker, Kubernetes) supported or preferred? **Support & Maintenance** • What are the required SLAs for support (e.g., 24x7, on-call)? • Are local support and training services mandatory? • Is a managed service option being considered?	