



**Sri Lanka CERT (Pvt) Ltd.**

**ADDENDUM NO. 01 – TO THE BIDDING DOCUMENT**

**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)**

**16<sup>th</sup> September, 2025**



**Sri Lanka CERT (Pvt.) Ltd.**

**ADDENDUM NO. 01 – TO THE BIDDING DOCUMENT**

**FOR THE**

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


**IFB No. CERT/GOSL/SER/ICB/2025/22**

1. Subsequent to the Bidding Document issued by Sri Lanka CERT for “Procurement of Cyber Threat Intelligence and Attack Surface Management Solution for Malware Analysis and Threat Hunting Lab” dated 26<sup>th</sup> August 2025, a pre-bid meeting was conducted on 09<sup>th</sup> September 2025. Based on the clarifications sought by the Bidder’s, it is felt necessary to provide additional information to the bidders to further clarify on certain areas of the Bidding Document.
2. All the bidders are required to perform careful assessment of the information provided in the Addendum 01.

Chairman,  
Department Procurement Committee (DPC)  
Sri Lanka CERT (Pvt) Ltd  
Room No.4-112  
BMICH  
Colombo 07  
Sri Lanka.  
16, September, 2025

## Amendments to the original Bidding Document

Sr.No.	RFP Reference	Amendment
01	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	<p>Revised the clause as follows:</p> <p>The bidder shall be of either;</p> <ul style="list-style-type: none"> <li>• Local OEM (Original Equipment Manufacturer) – a legally registered entity in Sri Lanka.</li> <li>• JV or Consortium where one party should be a Local party which is a legally registered entity in Sri Lanka and having physical presence (office) in Sri Lanka that has been in operation for the last Five (05) years. The OEM (Original Equipment Manufacturer) shall be the Lead Partner of the JV or Consortium of the proposed solution. Maximum number of JV partners or parties of the Consortium are three (3).</li> <li>• An authorized reseller or authorized distributor of OEM. Authorised reseller or distributor shall be a legally registered entity in Sri Lanka and having physical presence (office) in Sri Lanka that has been in operation for the last Five (05) years.</li> </ul>
02	Section II. Bidding Data Sheet → ITB 4.1 → Pg. No. 37	<p>Clause reworded as follows:</p> <p>“Bidder (if a single entity) or either partner (in case of “JV” or “Consortium” or “Partnership”), shall be registered under the Public Contract Act No. 3 of 1987.”</p>
03	Section II. Bidding Data Sheet → ITB 4.8 → Pg. No. 38	<p>Any other documents ITB 14.3 are updated as follows:</p> <p>New item XIII and XIV are appended:</p> <p style="margin-left: 40px;">XIII. A valid letter or certificate issued by the OEM, confirming that the bidder is an authorized distributor or reseller of the OEM.</p> <p style="margin-left: 40px;">XIV. Letters acknowledging receipt of all addendums issued by the Employer.</p> <p>Item II and V are reworded:</p> <p style="margin-left: 40px;">II. In the case of a JV, the JV agreement or a</p>

		<p>letter indicating the intention to form a JV shall be submitted. This should include the terms and conditions of the intended JV. Such intention letter shall be signed by the authorised signatories of the JV partners. In case of a consortium, consortium agreement signed by the parties shall be submitted.</p> <p>V. Audited Financial Statements 2019/20, 2020/21, 2021/22, 2022/23, 2023/24 (all the partners, authorised resellers or authorised distributors).</p>
04	<p>Section II. Bidding Data Sheet → ITB 24.2 → Pg. No. 40</p> 	<p>Clause (d) reworded as follows:</p> <p>“For bids submitted by a Joint Venture (JV) or Consortium or Partnership, each party to the such JV, Consortium or Partnership shall issue a Power of Attorney (POA) authorizing the nominated representative to act on its behalf. Such POA(s) may be:</p> <ul style="list-style-type: none"> <li>(i) a single joint POA, signed by all JV or Consortium or Partnership parties; or</li> <li>(ii) separate POAs, each signed by the respective parties, provided that all such POAs designate the same nominated representative.</li> </ul> <p>Each POA shall be either notarized or attested by an appropriate authority in the Proposer’s home country.”</p>
05	<p>Section II. Bidding Data Sheet → ITB 10.4 → Pg. No. 38</p>	<p>Note is appended as follows:</p> <p>Note: The minutes of the Pre-Bid meeting, clarifications and all addendums will be published on Employer’s official website.  <a href="https://www.cert.gov.lk">https://www.cert.gov.lk</a></p>
06	<p>Section III. Evaluation and Qualification Criteria → 3.7 1 Eligibility and Qualification Requirements of the Bidder → Pg. No. 51</p>	<p>Revised the NOTE as follows:</p> <p>The bidder shall be of either;</p> <ul style="list-style-type: none"> <li>• Local OEM (Original Equipment Manufacturer) – a legally registered entity in Sri Lanka.</li> <li>• JV or Consortium where one party should be a Local party which is a legally registered entity in Sri Lanka and having physical presence (office) in Sri Lanka that has been in operation for the last Five (05) years. The OEM</li> </ul>

		<p>(Original Equipment Manufacturer) shall be the Lead Partner of the JV or Consortium of the proposed solution. Maximum number of JV partners or parties of the Consortium are three (3).</p> <ul style="list-style-type: none"> <li>An authorized reseller or authorized distributor of OEM. Authorised reseller or distributor shall be a legally registered entity in Sri Lanka and having physical presence (office) in Sri Lanka that has been in operation for the last Five (05) years.</li> </ul>
07	Section III. Evaluation and Qualification Criteria → 3.3.1 Evaluation components and marking scheme → Pg. No. 46.	<p>Sr.No. 7 reworded as follows:</p> <p>“System Implementation Approach and Methodology of the Bidder”</p>
08	Section III. Evaluation and Qualification Criteria → 3.7 Eligibility and Qualification Requirements of the Bidder → 3.7.6.4 → Pg. No. 52 & 53	Impacted clauses are reworded as in the Annexure 01 and Annexure 02.
09	Section III. Evaluation and Qualification Criteria → 3.1 Preliminary Examination of Technical Bids → Pg. No. 44	<p>New Item (i) is appended as follows:</p> <p>(i) A valid letter or certificate issued by the OEM, confirming that the bidder is an authorized distributor or reseller of JV partner of the OEM.</p> <p>Reworded as follows:</p> <p>“(d) PCA form under public contract Act no.3 of 1987 before awarding the contract”</p>
10	Section III. Evaluation and Qualification Criteria → 3.7.9 OEM Non-Disclosure → Pg. No. 54	<p>Revised the clause as follows:</p> <p>“Require a signed letter from the OEM committing that the collected attack surface data and related information shall not be shared with any third party (other than Sri Lanka CERT) that could be used for malicious activities against Sri Lanka cyber-attack surface.”</p>

11	Section III. Evaluation and Qualification Criteria → 3.3 Detailed Evaluation of Technical Bids → Pg. No. 45	Demonstration should be carried out with real time data.
12	Section IV. Bidding Forms → 4.11 Price Schedule Summary → Pg. No. 75	Number of takedowns required during the subscription are 150.
13	Section IV. Bidding Forms → 2. Implementation and Payment Schedule → Pg. No. 83	Impacted clauses are reworded as in the Annexure 05.
14	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 7.8 Bulk/Batch & Free-Text IOC Import (XLS/CSV/JSON/XML) → Pg. No. 106	Revised the clause as follows: “The solution must support bulk-import, batch-import, and free-text import of threat intelligence data from third-party sources, including XLS, CSV, JSON, and XML formats.”
15	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.13 Multilingual NLP → Pg. No. 103	Revised the clause as follows: “The platform should translate and analyze content with NLP support for more than 10 languages”
16	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	Revised the clause as follows: “The solution must include support for playbook-based alerts, automated workflows, and best practices for attack surface and threat intelligence management to accommodate SIEM or SOAR integration”
17	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110 & 111	Section 6.1 deleted and changes are incorporated as per the Annexure 05.
18	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.2 → Pg. No. 111	Revised the section 6.2 as per the Annexure 03.
19	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.3 → Pg. No. 112	Revised the section 6.3 as per the Annexure 04.
20	Section VI. Schedule of Requirements → Table 7 –	Revised the clause as follows:

	Technical Specification → 1.13. Parent & Child Tenant - Wide Alerting → Pg. No. 89	<p>The platform should provide the facility to alert;</p> <p>a) All the authenticated users on the platform based on their granted role.</p> <p>on</p> <p>a) Changes in the attack surface b) Alerts on cyber threat intelligence c) Alerts on deep &amp; dark web monitoring</p>
21	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.15. Single -Provider Solution & Unified Accountability → Pg. No. 90	<p>Revised the clause as follows:</p> <p>“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.”</p>
22	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.2. CTI Source Traceability → Pg. No. 94	<p>Revised the clause as follows:</p> <p>“The platform shall provide the facility to provide evidence to understand why an IOC is risky and reference to the source, if any.”</p>
23	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.12. Botnet & black -market surveillance → Pg. No. 103	<p>Revised the clause as follows:</p> <p>“The platform should scan for PII exposed to the unauthorised parties, botnet activity, and black-market transactions linked to monitored organizations.”</p>
24	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 3.16. Open-Standard, Multi-Format CTI Export (Non Proprietary Formats) → Pg. No. 97	<p>Revised the clause as follows:</p> <p>“The platform shall provide the CTI exportable in multiple formats such as STIX/TAXII, JSON, XML, PDF, CSV, DOCX/PPTX and no vendor-proprietary formats to be exported to other systems.”</p>
25	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 5.11. Breach & leak detection → Pg. No. 103	<p>Revised the clause as follows:</p> <p>“The platform should generate alerts when sensitive keywords, credentials, or account details appear across dark-web platforms, forums, marketplaces, and messaging apps, with</p>



		malicious-content and credential-leak detection.”
26	Section VI. Schedule of Requirements → 6. General Warranty Terms & Service Level Agreement → 6.1 → Pg. No. 110	Revised the clause as follows: “Migration Support. The bidder shall perform export of threat intelligence, IOCs, alerts, and vulnerability data in open standard formats.”
27	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.11. Cloud -Native, 99.98 HA & Multi -Unit Scalability → Pg. No. 89	Revised the clause as follows: “The solution must be cloud-native, highly available (99.95 uptime), and scalable to accommodate organizational growth and multiple business units.”
28	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.19 Post-Transfer Permanent Data Deletion & Written Confirmation → Pg. No. 91	Revised the clause as follows: “Upon successful export and transfer of all Tenants’ Historical Data pursuant to Item 1.18, the bidder shall permanently delete all such data from the Platform and its systems, backups, DR sites and provide the Purchaser written confirmation of destruction.”
29	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.3 Coverage → Pg. No. 92	Revised the clause as follows: “Within the scope specified in Item 2.1, .lk, gov.lk and other subdomains of gov.lk should be covered.”
30	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 2.6 Self-Service Organization Add/Remove → Pg. No. 93	Revised the clause as follows: “The client should be able to add/remove organizations to/from the platform at any given time to perform the functions listed in Item 2.1 with minimum involvement of the supplier.”
31	Section VI. Schedule of Requirements → Table 7 – Technical Specification → 1.10 Role-Based Access for 10 Concurrent Parent-Tenant Users → Pg. No. 89	Revised the clause as follows: “The Platform shall support role-based access for at least ten concurrent Parent-Tenant administrators to manage all Child Tenants (up to 150 organizations)”



## Annexure 01

### 3.6 Eligibility and Qualification Requirements of the Bidder

Evaluation Criteria	Bidder				Document submission Requirements
	Single Entity (Local OEM or local authorised reseller or local authorised distributor)	In case of a JV or Consortium or Partnership			
		All Members Combined	Each Member	At Least One Member	
3.7.1 Conflict of Interest : No-conflicts of interest as described in ITB 4.3.	Must meet requirement	Must meet requirement	Must meet requirement		Letter of Technical Bid
3.7.2 Debarment: Not having been declared ineligible as described in ITB 4.4.	Must meet requirement	Must meet requirement	Must meet requirement		Letter of Technical Bid
3.7.3 Average Annual Turnover: Bidder should have minimum average annual turnover - 2 times of the bid price calculated as total certified payments received for contracts in progress or completed, within the <b>last 3 years</b>	Must meet requirement	Must meet requirement	Must meet 20% of the requirement	Must meet 60% of the requirement	Form 4.3
3.7.4 Financial Resources: Bidder must demonstrate access to or availability of financial resources, such as liquid assets, lines of credit, or	Must meet requirement	Must meet requirement	Must meet 20% of the requirement	Must meet 60% of the requirement	Form 4.4/4.4.1

other financial means, to meet the cash flow requirement of not less than 50% of the bid price, net of the Bidder's other commitments for this project.					
---	--	--	--	--	--

- \* Form 4.3, 4.4, 4.4.1, and 4.5 are also applicable for Local OEM, JV, Consortium, Partnerships, Authorised Local Reseller and Authorised Local Distributor.
- \* Form 4.3 – Provide average annual turnover for financial year 2019/20, 2020/21, 2021/22, 2022/23, 2023/24.

#### **Qualification Criteria of the Proposed Solution**

Evaluation Criteria	OEM	Document submission Requirements
3.7.5 General Experience: The OEM should have experience in providing cyber security SaaS solutions for 20 clients during last Five (05) years prior to the Bid Submission Deadline.	Must meet requirement	Form 4. 5
3.7.6.1 Specific Experience: The OEM should have experience with the ability to provide cyber threat intelligence for 20 clients during last Five (05) years prior to the Bid Submission Deadline.	Must meet requirement	Form 4.6.1
3.7.6.2 Specific Experience: The OEM should have experience with the ability to provide attack surface management for 20 clients during last Five (05) years prior to the Bid Submission Deadline.	Must meet requirement	Form 4.6.2

3.7.6.3 Specific Experience: The OEM should have experience with the ability to provide deep & dark web monitoring for 20 clients during last Five (05) years prior to the Bid Submission Deadline	Must meet requirement	Form 4.6.3
3.7.6.4 Specific Experience: The OEM'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 last Five (05) years prior to the Bid Submission Deadline.	Must meet requirement	Form 4.6.4
3.7.6 Quality and Security Requirements: OEM shall be certified with ISO 27001 or Similar.  Note Bidder must submit valid certificate with the Technical Bid	Must meet requirement	Bidder must submit valid certificate with the Technical Bid

## **Annexure 02**

### **Other Specific Requirements**

Impacted clauses are changed as follows. Other clauses remain as in the original RFP.

Criteria	Requirement	Compliance	Reference
3.7.7 Prime Accountability	Require a signed letter from the bidder committing OEM responsibilities are fully aligned to the bidder's commitment to provide the proposed solution.	Must meet requirement	Letter from the bidder
3.7.8 OEM Backing Letter	Require a signed letter from the OEM committing to continuity of services/licenses/support regardless of bidder changes.	Must meet requirement	Letter from the OEM

## Annexure 03

### 6.2. Incidents Response

Severity Level	Definition	Response Time Target	Measurement Criteria	Penalty for Breach
Critical	Failure of system/services/components that cause full or partial outage of the provided solution; or urgent security-alert-driven actions (e.g., phishing takedown initiation).	≤ 30 minutes (24×7)	Time from Sri Lanka CERT escalation (ticket/email/phone) until Contractor acknowledgement with reference ID.	2% of contract value per breach, capped at 10% of total contract value.
High	Failures/degradations that significantly impact availability/performance but not total outage.	≤ 45 minutes (24×7)	Same as above.	1% of contract value per breach, capped at 10% of total contract value.
Low	Minor queries or issues not affecting availability/performance.	≤ 120 minutes (business hours)	Same as above.	0.5% of contract value per breach, capped at 10% of total contract value.


## Annexure 04

### 6.3. Resolution Time

Severity Level	Definition	Resolution Time Target	Measurement Criteria	Penalty for Breach
Critical (Contractor-controlled)	Failures of system/services/components that cause outage/partial outage of the solution.	≤ 4 hours	Time from Sri Lanka CERT escalation until restoration of solution functionality.	2% of contract value per breach, capped at 10% of total contract value.
High (Contractor-controlled)	Failures/degradations impacting availability/performance without full outage.	≤ 8 hours	Same as above.	1% of contract value per breach, capped at 10% of total contract value.
Low (Contractor-controlled)	Minor bugs/features not affecting availability/performance.	≤ 3 business days	Same as above.	0.5% of contract value per breach, capped at 10% of total contract value.
Third-party dependent incidents (e.g., takedown, de-indexing)	Actions requiring registrar/host/platform cooperation beyond Contractor's control.	Not subject to resolution SLA. Instead, must meet governance KPIs: Time to Initiate Mitigation ≤ 60 min, follow-up at least every 24 hrs, and audit trail of evidence/outcomes until closure/refusal.	Measured against KPIs; no monetary penalties, but repeated non-compliance may affect performance reviews and contract continuation.	

## **Annexure 05**

Impacted clauses are changed as follows.

<b>Item No</b>	<b>Description of the Activity</b>	<b>Implementation Time Schedule (Bidder/Contractor)</b>	<b>Payment Schedule</b>
1	Complete installation of Cyber Threat Intelligence, Attack Surface Management, Deep & Dark Web Monitoring, Takedowns and Analysis & Reports Solution.	It is required to completely implement the solution within 30 days from the date of award.	50% of the total contract price on the successful implementation, acceptance of the solution and user training completed.
2	User Training and Manuals 	It is required to successfully deliver training for staff nominated by Sri Lanka CERT within 14 days from the date of award.  During this period, it is required to complete training manuals, user guides by the bidder/contractor.	20% of the total contract price on the successful integration and acceptance of the solution by client.
3	Integration with SIEM	It is required to completely integrate the solution with the SIEM within 35 days from the date of award.	10% of the total contract price on the successful integration and acceptance of the solution by client.
4	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 + 365 days.	10% of the total contract price at the end of the subscription period.
5	Migration Support and Post-Transfer Permanent Data Deletion.	The contractor is required to provide migration support and post-transfer permanent data deletion after the subscription period. Date of award + 365 + 28 days.	10% of the total contract price after the migration and post-transfer data deletion.

Chairman,  
Department Procurement Committee (DPC)  
Sri Lanka CERT (Pvt) Ltd  
Room No.4-112  
BMICH  
Colombo 07  
Sri Lanka.

Dear Sir,

**PROCUREMENT OF CYBER THREAT INTELLIGENCE AND ATTACK SURFACE  
MANAGEMENT SOLUTION FOR MALWARE ANALYSIS AND THREAT  
HUNTING LAB. IFB NO. CERT/GOSL/SER/ICB/2025/22**

We hereby certify that Fourteen (14) Pages of Addendum 01 and Annexure 01 to Annexure 05 has been received by us and considered for pricing and bidding as a part of the original Procurement Document in accordance to the “Instructions to the Bidders” Clause 14- Documents Comprising the Bid, in Procurement Document.

Yours Truly

Signature of the Bidder

Company Seal

Date

.....

.....

.....

**“Bidders shall enclose this letter with the ORIGINAL” of Technical Bid submission as a bid validity and completeness requirement.**