Vendor 1

No	Feature	Minimum Specification	Comments	Answer from Sri Lanka CERT
29	Deployment, Architecture and Monitoring	Solution shall be delivered as a Centralized solution with a local collectors on-premises for distributed architecture to gather log and alerts from remote locations	Total Locations count? **40** Collection EPS required per collector?	Total Locations count 40 Total EPS requirement mentioned in the IFQ
30		Proposed Solution shall provide a minimal hot/warm data retention capability of 30days for real time analytics and threat correlation	Is Offline (Raw) log retention needed?	30 days
35		SOC solution should be able to correlate Events Packets & Flows together to generate incidents.	Is it Events or Packets?	Events, Packets & Flows
36		SOC solution should utilize Artificial Intelligence(AI) and Machine Learning Algorithms as well as rules on logs, packets, and network flows collected to provide user behavior analytics	Is UEBA needed? If so please mention the total users.	Yes needed ,20 000 total users for 3 years
126.	File Integrity Monitoring (FIM) Capabilities	The proposed solution shall have File Integrity Monitoring solution	Total number of licenses needed for FIM?	20 000 total users for 3 years
127.		The proposed solution shall have Capability of capturing the information changes such as What, when, how, who made the changes and etc.		Yes
128.		Proposed solution shall have Support file directory recursion		Yes

No	Feature	Minimum Specification	Comments	Answer from Sri Lanka CERT
218		Bidder must supply of appliance based Next Generation Firewalls with provision of version upgrades/patches	Clarification needed.	**Sri Lanka CERT will remove this line item from IFQ**

Vendor 2

1. Please provide an extension at least up to the 19th of April 2024, vendor requests more time to propose the needed solution.

- Sri Lanka CERT already extended to 17th April 2024

2. Also, provide the editable formats for SOC and EDF specifications (RFP).

- Sri Lanka CERT will not be able to provide editable format

Vendor 3

1. The updated price schedule of the Addendum No 01 has mentioned the implementation fee for the initial license slabs of 7500EPS and 1000 EDR licenses as the item 1, while the item numbered 2 and 3 requests the license pricing for the subsequent slabs from 2 to 16

- Yes,

- **[1]. Supplier is required to provide 7500 EPS in slabs. Upon the usage of the EPS, the purchaser shall request to provide additional slabs up to 120,000 EPS during the 3-year contract period (16 slabs * 7500 EPS). However, suppliers shall agree to provide the same price for each slab starting from slabs no 2 to 16 during the contract period (pricing for each slab shall be fixed except slab no 1(initial slab).

- **[2]. Supplier is required to provide 1000 EDR Licenses in slabs. Upon the usage of the EDR Licenses, the purchaser shall request to provide additional slabs up to 10,000 EDR Licenses during the 3-year contract period (10 slabs * 1000 EDR Licenses). However, suppliers shall agree to provide the same price for each slab starting from slabs no 2 to 10 during the contract period (pricing for each slab shall be fixed except slab no 1(initial slab)).

2. We would like to clarify whether the new item number 1 is to request an all inclusive price of licenses (7500EPS and 1000EDR) and implementation, integration and support charges for a period of three years. If else, would like to raise your attention regarding the missing component of initial license slabs of 7500EPS 1000EDR licenses.

- Yes, all-inclusive price of licenses

3. Further, with regard to the line items #3 '7500 EPS Slab implementation, log integration, playbook, etc.' and #5 '1000 EDR Slab implementation, agent installation, etc.', we would like to know whether this price request includes on-going L2 support for the mentioned license period of 3years in addition to the implementation and integration requirements

- Yes

Vendor 4

1. Which specific message queuing platforms should our solution be flexible to integrate with?
- Bidder shall provide a list of supported message queuing platforms for the proposed solution (Including Open source)

2. Which specific third-party log management UIs should our solution support integration with?
- Proposed NCSOC solution shall have user friendly UI to integrate log sources.

3. Which third-party systems should our solution be capable of integrating security alerts with?
- Bidder shall provide a list of supported alerting systems Email, SMS, etc. (Including Open source)

4. We require additional details on the customization options for dashboards and monitoring of specific websites/pages.
- Please list the required additional details

5. Please elaborate on the requirements for customized report generation.
- Proposed solution shall have the capability to customise out of the box reports and create customise reports from scratch.

6. What is the expected level of support for generating unlimited reports?
- Bidder shall provide technical guidance to create reports to Sri Lanka CERT.

7. Possibility of providing the Performance bond yearly 10% for the yearly committed contract price
- Not Possible

8. Clarity of Payment terms and how payments will be released over 3 years
- Please check the Amended RFP terms that shared with you and also you can find it on cert.gov.lk web site Procurement section.