Vendor 1

No	Feature	Minimum Specification	Comments	Answer from Sri Lanka CERT	Clarification Needed	Sri Lanka CERT Clarification
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	Total EPS mentioned in the RFQ is 120,000. But individual collectors needs to be placed in all the mentioned 40 locations. So we will need to know the minimum and maximum of a location to size the hardware needed and software requirements for the collector.	1000 EPS to 5000 EPS → 25site 5000EPS to 10000EPS → 10 site 10000EPS to 150000EPS → 5 site
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	EDR is requested for 10,000 users. Is this conformed for 20,000 users?	Sri Lanka CERT request 10 000 EDR licences for End point 20000 User UEBA
126	File Integrity Monitoring (FIM)	The proposed solution shall have File Integrity Monitoring solution	Total number of licenses needed for FIM?	20 000 total users for 3 years	FIM is mostly used in Servers. So need a clarification on this?	Total FIM licences count is 1600 for 3 years Bidder shall provide 100 Fim licences for each 7500 EPS slab

Vendor 2

Do we need to provide hardware for log collectors?

Yes. if required The bidder should provide any necessary hardware for log collectors for remote locations (tenants). Proposed solution shall not have any limitations based on the agents/connector and devices count.