KENYA REVENUE AUTHORITY
ISO 9001:2015 CERTIFIED

CLARIFICATION SET "3"

6th April, 2020

To all Prospective Bidders,

TENDER NO. KRA/HQS/NCB-063/2019-2020: SUPPLY, DELIVERY, IMPLEMENTATION AND COMMISSIONING OF CYBER SECURITY OPERATIONS CENTER SOLUTION

Kenya Revenue Authority wishes to inform prospective bidders of the clarifications highlighted below for the above tender.

	PAGE	SECTION	DESCRIPTION	CLARIFICATION QUESTION	CLARIFICATION RESPONSE
2	28	Technical requirement (b)	The solution MUST have ability to centralize collection and monitoring of cyber threats and tax intelligence from both internal and external threat intelligence feeds. The bidder is required to explain/show/ demonstrate how the solution meets this requirement.	Are you looking for Threat intelligence platform, generally it collect, normalizes feeds received from external/internal third parties, and feeds it on to SOAR and different security tools. Kindly let us know if we should proposed Threat Intelligence Platform (TIP) solution. Also requesting to kindly share more details on the requirements for the TIP.	Threat Intelligence is a critical component of the SOC solution being sought. Tax intelligence sources to include but not limited: a. *Internal sources - KRA internal systems etc.* b. *External sources - deep web, Dark web, social media etc.*

KENYA REVENUE AUTHORITY
ISO 9001:2015 CERTIFIED

3	28	Technical requirement (d)	The solution should have endpoint detection/response tools (EDR) capabilities to enable digging deep into security alerts by monitoring and investigating. The bidder is required to explain/show/ demonstrate how the solution meets this requirement.	Kindly share the no of endpoints. Also please confirm. if you already using Endpoint protection solution. Please share more details on the requirements.	Approximately 6.000 endpoints.
4	29	Technical requirement (i)	The solution should support ability to deploy agents on all identified targets. The bidder is required to explain/show/ demonstrate how the solution meets this requirement.	Kindly clarify on this point. What is the purpose of installing agents? Is it for Endpoint Detection and Response (EDR)?	If the proposed solution or solution component uses agents. it should support remote deployment of such agents on its targets e.g. log sources. servers. endpoints etc.
5	29	Technical requirement (k)	The solution should support network security analytics to allow analysis of flow and packets The bidder is required to explain/show/ demonstrate how the solution meets this requirement	Kindly clarify on this point. There are multiple products which can understand the flow and does packet analysis. Are you specifically looking for Network behaviour anamoly detection (NBAD) kind of solution.	The solution is expected to have network security analytics capability to enable analysis of network flows and packets.
6	29	Technical requirement (n)	The solution MUST have ability to support minimum 5 users and scalable to 50 users. The bidder is required to explain/show/ demonstrate how the solution meets this requirement.	Kindly confirm on the no of user count. Is it for SOAR SOC Analyst license.	Minimum of 5 users. scalable to 50 users.
			Request you to kindly provide the existing device list to calculate the EPS count. Also please mention about the future growth.		Approximately 500 log sources. SIEM Solution in use – QRADAR has an EPS of 5.000.
Considering the critical nature of the business of KRA, and with our global experience of working on these cyber security solutions we would like to recommend the below points for KRA's consideration. Additionally as requested above please provide detailed specs for TIP, EDR, and Network analytics solution.					

7			It should be Big data analytics platform and should be present in Gartners leader quadrant as per the latest report.	Looking at the growing threats and attack landscape we recommend you to have Artificial Intelligence (AI) & Machine Learning (ML) based Big data platform as an analytics tool, also it will help with User and entity behavioral analytics capabilities to mitigate insider threat.	Big-data powered intelligence and machine learning capability is a mandatory requirement. ***Refer to technical requirements (a)*** Bidders are also free to recommend additional solution capabilities that would enhance SOC operations.
8			One single syntax that can be used universally for search queries, alerts, reports or dashboards		
9			The solution must be scalable and have a distributed architecture.		
10			The solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes.		
11			The solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes.		
12			The solution must have advanced analytical capabilities to address advanced persistent threats, fraudulent activities and insider threats.		
13			have advanced unsupervised machine learning analytics models, patterns analysis and rules to perform monitoring, detection and alerting against insider threats, user and entity behavior anomaly or any other unknown/hidden threats. Submit details of unsupervised machine learning analytics models, patterns analysis performed by solution.		
14			include following as entity for threat monitoring and detection purpose without relying on any 3rd party solutions: Endpoints, on premise applications, networks, clouds, mobile and any external threats.		
15			provide raw and normalized logs/data storage as per data retention requirement outlined in scope of work.		

16			have low-latency, high throughput and quick response to highly complex queries. Submit details: - Latency, throughput provided by proposed solution at each architecture node/layer. - Data/Log query response time & benchmarking for simple, medium and highly complex queries. dashboards and reports on proposed storage technology from: a. 1 day of data b. 5 day of data c. 30 day of data		
17			be capable to consume and process raw/native logs, contexts or any other security related data from all the IT, Operational and emerging technologies deployed in the Britam.		
18			provide option to have agent-less as well as agent-based capability.		
19			analyse user & entity behaviour across time, on peer group as well as individual baselines. List out the capabilities of solution for user & entity behaviour monitoring.		
20			provide daily, weekly, monthly insights into risky users and entities based on risk score rating in the form of dashboards and reports.		
21			detect slow attacks, advance persistent threats, file less attacks, zero-day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI / ML.		

KENYA REVENUE AUTHORITY
ISO 9001:2015 CERTIFIED

22			detect and protect against following (not limited to) below security threats: 1. Insider threats including compromised account/compromised machine/ malicious insider 2. Data exfiltration 3. Lateral Movement 4. Advance Malware detection 5. Exploit chain 6. Unusual on premise or remote logins 7. Unusual data access 8. Web shell activity 9. Command & Control 10. Phishing 11. Account take over 12. Identity and privileged access management 13. Email activity, application usage, file activity, printer activity etc. Provide details capability what all security threats solution can monitor, detect and predict.		

The addendum/clarifications form part of the bidding document and is binding to the bidder. All other terms and conditions of the tender remain the same. You are therefore required to immediately acknowledge the receipt of this addendum/clarifications.

Regards,

Rhodah Nzovila
For: Deputy Commissioner - Supply Chain Management

KENYA REVENUE AUTHORITY

ISO 9001:2015 CERTIFIED