ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061
www.icta.go.ke

ADDENDUM NO.1

TENDER NO. ICTA/OT/12/2022-2023 *14th February, 2023*

TENDER NAME: SUPPLY, DELIVERY AND INSTALLATION OF A SECURITY INCIDENCE AND EVENTS MANAGEMENT SYSTEM FOR SECURITY OPERATION CENTRE

S.No	BIDDERS' CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE/CLARIFICATIONS
1.	Request customer to share asset list of devices and applications to be integrated to ensure integration and estimated effort for implementation? This includes following: a> Servers -Windows b> Desktops c> Non Windows Servers d> Network Devices - Routers, Switches, Wireless LAN Access Point, Controllers etc. d> Security Devices- Firewalls, IPS/IDS, VPN,Web Security, Email Security etc. e> Applications - Web Servers (IIS, Apache, Tomcat) etc. f> Databases - Database (MSSQL, Oracle, Sybase) * g> Email Servers (Exchange, Sendmail, BES, etc.) h> Antivirus / DLP Server etc. i> Other Applications (ERP, In-house, etc.)	We require an implementation for a 5k EPS license which will be prioritized depending on the asset criticality.
2.	RFP has asked for software based solution. Is ICTA going to provide the virtualization resources and storage to host the SIEM and SOAR or they need to be proposed with compute and storage infrastructure?	ICTA will provide the virtual Infrastructure.
3.	Please suggest What is the log retention period for online and archival data?	3 Months online, 1 year offline archival

ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061
www.icta.go.ke

S.No	BIDDERS' CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE/CLARIFICATIONS
4.	RFP asked for High Availability / Non-Production licenses. Is this requirement related to having the solution in high availability or you need a test environment license included?	HA and DR licenses should be part of the proposed licenses . In addition to this, lab licenses are also to be included.
5.	RFP requested for a minimum of 10 active sessions at any given time. Does ICTA already have 10 SOC Analysts that will be accessing the system concurrently or they are split in different shifts? Please confirm	There should not be any limit on number of users.
6.	We assume that ICTA have an SMS Server for sending SMS notifications? Is the understanding correct?	Yes
7.	In the RFP, ICTA has asked for "License should be optimal, filtered logs should not be calculated for licenses and it should be calculated on average of 45 days EPS sustained and post Filtering." Please suggest if a SIEM vendor has an alternate or equivalent way of ensuring EPS bursts are taken care of within their license enforcement mechanism, we understand that will be acceptable to ICTA.?	License should be calculated after filtering and average of 45 days EPS.
8.	The RFP talks about solution should be based on Big Data platform. Please suggest if ICTA already have this Big Data Platform? Additionally please suggest what technology is it based on? If a Big Data Platform needs to be proposed, will ICTA provide the compute and storage or vendors need to propose appropriately? Please confirm.	Big Data needs to be part of SIEM solution.
9.	The RFP talks about solution should support message bus to enable integration with 3rd party Data Lakes. Please suggest which 3rd party Data Lakes does ICTA intend to integrate to the SIEM Platform?	Hadoop, ELK etc.,
10.	In the RFP, SOAR has been requested. Does ICTA have any runbooks developed and how many playbooks need to be created for the different scenarios that ICTA has? This is to assist with effort estimation.	Consider 25 playbooks.
11.	Please suggest if the licenses proposed should they be perpetual or subscription based?	Perpetual
12.	RFP defines that support period for 3 years. Please confirm if OEM and bidder support for SIEM and SOAR should also be 3 years? Please confirm	This should be for One (1) year support.
13.	RFP talks about Product should be internationally rated (Gartner) and has consistently been placed in the Visionaries and Leaders Quadrant. Please suggest	Only products in leaders or visionaries to be considered.

S.No	BIDDERS' CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE/CLARIFICATIONS
	if ICTA is considering products in the Visionary and Leader quadrants only. As per Gartner products in challengers quadrant has better Ability to Execute the SIEM functionality than Visionaries. Is ICTA willing to consider vendors in Challenger quadrant also for the SIEM solution?	
14.	As per RFP, it is mandatory to have a full-fledged SOAR with playbooks and approval-based action taking capabilities without additional licenses. By additional licenses is ICTA referring to custom modules, connectors, playbooks, etc? Kindly clarify what this entails and also a full-fledged SOAR which modules do you expect? For example: Dashboards, Threat Intelligence Management, Queue & Shift Management, Alerts, Incidents, Vulnerability Management, Automation (Playbooks, Connectors, Schedules, SLA templates), Mitre Attack, Attachments, Assets, Reports, War Rooms, etc. Please confirm	All mentioned features are needed.
15.	On Support and maintenance, it is started that: Support period will be 3 years (deployment time included). This will be the contract period. 3. – Please confirm if license subscription and support both vendor and local support required and to be quoted is for 3 years.	This should be for One (1) year support.
16.	Kindly advise/ list the data lakes in use.	Hadoop, ELK etc.,
17.	Kindly advise and list the systems (including model and versions) that require integration with the SOAR.	This includes following: a> Servers -Windows b> Desktops c> Non Windows Servers d> Network Devices - Routers, Switches, Wireless LAN Access Point, Controllers etc. d> Security Devices- Firewalls, IPS/IDS, VPN,Web Security, Email Security etc. e> Applications - Web Servers (IIS, Apache, Tomcat) etc. f> Databases - Database (MSSQL, Oracle, Sybase) *

ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061
www.icta.go.ke

S.No	BIDDERS' CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE/CLARIFICATIONS
		g> Email Servers (Exchange, Sendmail, BES, etc.) h> Antivirus / DLP Server etc. i> Other Applications (ERP, In-house, etc.)
18.	Kindly advise and list the data sources (including model and versions) that require log collection and correlation.	This includes following: a> Servers -Windows b> Desktops c> Non Windows Servers d> Network Devices - Routers, Switches, Wireless LAN Access Point, Controllers etc. d> Security Devices- Firewalls, IPS/IDS, VPN,Web Security, Email Security etc. e> Applications - Web Servers (IIS, Apache, Tomcat) etc. f> Databases - Database (MSSQL, Oracle, Sybase) * g> Email Servers (Exchange, Sendmail, BES, etc.) h> Antivirus / DLP Server etc. i> Other Applications (ERP, In-house, etc.)

S.No	BIDDERS' CONCERNS/OBSERVATIONS/COMMENTS		ICTA RESPONSE/CLARIFICATIONS
19.	What are the business drivers for the SIEM	☐*Compliance Initiative ☐*Centralized Log Management ☐ *Incident Response ☐*Security Threat Correlation ☐ Other: * means selected	The Authority is keen to achieve the following along with any additional functionality that the proposed solution will offer. Compliance Initiative Centralized Log Management Incident Response Security Threat Correlation
20.	How long must be the logs kept (in days) offline.		3 Months online, 1 year offline archival

ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
Tel: +254 20 2089061
www.icta.go.ke

S.No	BIDDERS' CONCERNS/OBSERVATIONS/COMMENTS	ICTA RESPONSE/CLARIFICATIONS
21.	How long must be the logs kept (in days) online.	3 Months online, 1 year offline archival
22.	how is your data network distributed geographically (number of sites/branches,…) a network drawing would be helpful.	Data will be received from government datacentres, Government Application Servers and network devices across regions/COUNTRY.
23.	To be able to provide pricing for the SIEM based solution, we would like to request for the below additional scoping/sizing information.	We don't have the exact numbers however, kindly ensure the proposed solution is able to handle at least 5,000k logs per second and is able to collect log data using syslog, SNMP, and APIs.

The addendum & clarification form part of the bidding document and is binding on all bidders. All other terms and conditions of the tender remain the same.

CEO, ICT Authority