ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
www.icta.go.ke

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

S.NO	PAGE NO.	SPECIFICATION/DESCRIPTION	CLARIFICATIONS REQUIRED	ICTA RESPONSE
1.	27	The Procuring Entity will publish Minutes of the pre-Tender meeting and the pre-arranged pretender visit of the site of the works at the website https://icta.go.ke/tenders/	There is no date and time specified for the Pre- tender meeting. Please share the details	There was no pre-tender meeting.
2.	33	"**Performance on similar projects:** Provide at least Five (5) similar projects in the last 5 years from the closing date of this tender. Three of which must be in the Public/ Government sector in Kenya. Similarity being in complexity and scope. This must involve supporting and implementation of SIEM for Information Security, Network Security, Application Security, Data Centre Security systems and related Critical Infrastructure Security. (The bidder should provide a completion certificates , LPOs or signed contracts as	We request ICTA to consider the Global references and Not mandatory references from Kenya	Our due diligence will only be limited to Kenya, we can't support Global references.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

		testimonials on performance on similar projects)" Page 33 on Technical Mandatory Evaluation		
3.	97	Form Of Contract, Part ii - Procuring Entity's Requirements, 5.2 Project Scope	Please specify total number of assets to be integrated with SIEM.	This is expected to scale higher but for start we have close to 2500
4.	97	Form Of Contract, Part ii - Procuring Entity's Requirements, 5.2 Project Scope	Please specify if ICTA is already using a SIEM solution.	No, we don't have a SIEM at the moment
5.	97	Form Of Contract, Part ii - Procuring Entity's Requirements, 5.2 Project Scope	Can SIEM implementation be done remotely or it needs to be done onsite?	On Site.
6.	97	Form Of Contract, Part ii - Procuring Entity's Requirements, 5.2 Project Scope	Please specify whether 1 onsite resource required should be L2 or L3?	L2
7.	97	Form Of Contract, Part ii - Procuring Entity's Requirements, 5.2 Project Scope	Will ICTA Be Providing Underlying Hardware Specs & Storage Required For Installing SIEM Components?	Yes.
8.	32	**"Rating** The Product should be internationally rated in Gartner and has consistently	"The Clause is very restrictive since the most of the SIEM players present in Gartner SIEM quadrant are cloud based and the requirement in the RFP is on-premise based.	No, we are interested in the referred to Quadrant;

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

		been placed in the Leaders Quadrant in the last four years. It should also be in the Forrester wave"	Can this be extended to at least include all players present in Gartner SIEM listing for last 4 years. This will allow OEM's with SIEM solution that meet all the outlined technical requirements and be of value and better ROI to the Government SOC. "	and by premise we mean our Virtual environment.
9.	34	"**Session Specification:** The solution should support multi-factor authentication for login, and should have automatic session timeout and logout policies."	Will ICTA be providing a system for integration for 2FA or this should be proposed as part of the bid response to cover the 15 users of the SOC? Please confirm	The system should be able to integrate in 2FAwhci ICTA will have at a later stage
10.	33	**Throughput:** The SIEM solution should be able to process and analyse a minimum of 1,500 log events per second.	We understand that bidder has to provide licenses to cover 1500 Events per second. Please confirm.	Yes, Confirmed.
11.	34	**Traffic and Log Optimization** The solution should be able to handle high volumes of network traffic – 20000 EPS, with the capability to process and analyse 20000 of events per second.	As per the throughput requirement mentioned on Page no 33 of document, Bidder has to provide the licenses for 1500 EPS. However the solution should have capacity to upgrade by addition of collectors and licenses to scale to 20000 EPS. Please confirm if the understanding is correct.	For the Licensing we are considering 1500 EPS which we will scale later.
12.	25	**ITT 4.1** Maximum number of members	We request to allow at least one JV partner in order to provide more cost effective and	JV Partner NOT allowed

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

		in the Joint Venture (JV) shall be: [insert a number] -NONE	efficient solution for the proposed requirements.	
13.	27	**ITT 24.1** The deadline for Tender submission is: Date: 2nd February, 2024 TIME: 10:00 A.M. The electronic Tender submission procedures shall be: NOT APPLICABLE	In order to provide best technical and commercial solution, Request to extend the submission date by at least 10 Days.	Extended upto 9th February,2024 @10.00AM
14.	29	**MR 5** Attach Original Equipment Manufacturer Authorization (OEM) (MAF) for Security Incidents & Events Management Systems (SIEM), Platinum or Gold level of partnership – for the Software.	Request to allow Gold, Platinum and registered partners with Capability, Skills and Experiences as defined in the RFP to participate for the requirement	Allowed.
15.	29	**Training** Bidder shall carry out: i. OEM approved training and certification to ICTA technical staff for at Least 5 (Staff) in English language on Security Incidents & Events Managements in an OEM approved facility	Please suggest if the training facility of OEM is outside Kenya, who will bear the cost for the logistics for travel, accommodation flight etc. Please confirm	We recommend a Kenyan location as a preferred option for this.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

16.	32	**Platform** Solution should Support High availability architecture with redundant components to ensure continuous operation even in the event of a failure Redundancy: The solution shall be setup in an architecture that must collect, process and correlate data from two data centre environments.	Please confirm if the SIEM solution needs to be deployed in HA or DR environment. How many Instances of SIEM solution are required to meet the resiliency. Are we looking for HA i.e. Active Passive instance at one site or Active Instance at One site and Passive at DR site. Please confirm	We looking for HA i.e. Active Passive instance at one site.
17.	33	**Multi-tenancy** Must support Cross Correlation of SOC & NOC Analytics	Please elaborate on the requirement. We understand ICTA is looking for SIEM System to have feature of data collection for network configurations and assert in addition to security alerts and events from IT system and provide cross correlation. Please confirm	Yes. That's right. We would also like the SIEM to have the capability of sharing a specific dashboard for specific resources e.g. A dashboard for applications being analysed on the SIEM to be shared with the applications team for viewing.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

18.	33	**Compatibility:** The solution should be compatible with existing infrastructure, with minimal change in the existing setup.	Please provide details of existing IT infrastructure with which the SIEM system has to be integrate.	Network Devices. Servers, Application Systems And Administrator/Privileged accounts users
19.	34	**Data collection and ingestion**: 1. The solution should be able to collect and ingest log data from a variety of sources, including network devices, servers, applications, and cloud environments	To be assess the service efforts and customization required, it is important for ICTA to provide details of devices with make and software version to define customization and configuration effort. Also provide the details of distribution of the IT devices across locations to access if additional collectors required. Please provide Details in Below Model **a>DeviceType** **b> Device Model**	The devices and systems are within Nairobi Government Datacentres.
20.	37	**Administration** The solution should support integration with 3rd party service monitoring tools for service monitoring	Please suggest what is the service monitoring tool with which the integration is required	The System should be able to Integrate to Systems like Fortinet Firewalls, Web & Patch Management systems, CRM and any other system.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

21.	39	**Function** The solution must enable a phased roll out of log management and security intelligence functions. Introduction of more capabilities should minimize the need for additional system components and be enabled through license key upgrades	Please suggest support and Threat Intelligence subscription should be for 1 year or 3 years?	1 year
22.	43	**Correlation and Alerting** The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e. web servers, database servers etc.) or business purpose, to minimize false positives associated with poor asset classification.	Please elaborate on the requirement. Is ICTA looking for SIEM system to define classification of the assets. Please suggest if ICTA has a asset classification process. Please elaborate	This is a basic Functionality that a SIEM should have to be able to scan and discover assets based on the OS or Ports in order to define type of digital asset device.
23.	44	The solution must dynamically learn behavioural norms and alert on changes as they occur.	We understand the UEBA feature has to be included in the SIEM solution. Please confirm. Also suggest total number of servers and endpoints for which UEBA is required.	Yes, The system has to have UEBA capabilities. As requested earlier, This is expected to scale higher but for a start we have close to 2500 devices.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

24.	82	Managed SIEM Monitoring Resource Analyst (Annual 1 Desk resource)	Please confirm if the bidder has to provide full time onsite Security Analyst at ICTA datacentre for management and operation of SIEM solution. Please confirm	Yes L2/ Can also be available remotely.
25.	82	Software & Licensing Acquisition and Installation LOT	We understand that licenses have to provide for One Year only. Please confirm	1 year
26.	82	Support and Maintenance	We understand that Support and Maintenance is to be provided for One Year. Please confirm	1 year
27.	N/A	Performance on similar projects: Provide at least Five (5) similar projects in the last 5 years from the closing date of this tender. Three of which must be in the Public/ Government sector in Kenya. Similarity being in complexity and scope. This must involve supporting and implementation of SIEM for Information Security, Network Security, Application Security , Data Centre Security systems and related Critical	Please advise and confirm if the requested documents should be specific to SIEM solution or if to involve supporting and implementation of SIEM for Information Security, Network Security, Application Security , Data Centre Security systems and related Critical Infrastructure Security. i.e. completion certificates , LPOs or signed contracts as testimonials on performance on similar projects	The documents to be provided are to be specific to SIEM Solution alone.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

		Infrastructure Security. (The bidder should provide a completion certificates , LPOs or signed contracts as testimonials on performance on similar projects		
28.	N/A	N/A	Please list the use cases that are to be addressed by the required solution.	The SIEM solution is meant to provide for visibility for Security system events on entire spectrum of ICT Digital Assets which will include; Network Devices. Servers, Application Systems And Administrator/Privileged accounts users
29.	N/A	N/A	Please share the redundancy requirements (HA ? or HA+DR?)	We looking for HA i.e. Active Passive instance at one site.
30.	N/A	N/A	What is the online retention requirement?	3 Months.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

31.	N/A	N/A	What is the offline retention requirement?	6 Months
32.	N/A	N/A	How many Branches or isolated zones included for log collection?	The devices and systems are within Nairobi Government Datacentres
33.	N/A	N/A	Any 3rd party Incident workflow/Ticketing tool needed to be integrated, if yes, please share the tool/version details	The System should be able to Integrate to Systems like Fortinet Firewalls, Web & Patch Management systems, CRM and any other system including ticketing which will be done later.
34.	N/A	N/A	Is External Load balancer available to load the share on logs forwarded	Yes,Available
35.	N/A	N/A	Any restrictions on using Virtual infrastructure or providing HW for installing SIEM Applications	No, We are open to a Virtual Set-up on premise.
36.	N/A	N/A	Any existing Vulnerability scanner to be integrated?	Yes, Acunetix.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

37.	N/A	N/A	If we are forwarding the logs from remote branch to main site, how is the connectivity established and what is the bandwidth available?	The Links are supported by an MPLS Architecture of 1G across.
38.	N/A	N/A	Any other specific requirements, please mention	None
39.	N/A	N/A	Number of users in the Organisation	Not Applicable
40.	N/A	N/A	(Also please fill the next sheet with all the devices planned to integrate with SIEM, if needed you could share in phase wise requirement, immediate integration devices and future integration)	The SIEM solution is meant to provide for visibility for Security system events on entire spectrum of ICT Digital Assets which will include; Network Devices. Servers, Application Systems And Administrator/Privileged accounts users

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

41.	N/A	N/A	What are the business drivers for the SIEM	Cyber security systems visibility security assurance.
42.	N/A	N/A	if compliance is needed please list the legislation (PCI, ISO, SOX,…)	N/A
43.	N/A	N/A	How long must be the logs kept (in days) offline	6 Months.
44.	N/A	N/A	How long must be the logs kept (in days) online	3 Months
45.	N/A	N/A	how is your data network distributed geographically (number of sites/branches,…) a network drawing would be helpful	The devices and systems are within Nairobi Government Datacentres.
46.	N/A	N/A	How many years License do you require?	1 YEAR
47.	N/A	N/A	Estimated project start date.	Mid- March 2024

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

48.	N/A	N/A	Do you require UEBA?	Yes.
49.	N/A	N/A	How many devices require UEBA?	All devises within scope.
50.	N/A	N/A	List the system specification for the devices requiring UEBA.	The SIEM solution is meant to provide for visibility for all devices which include; Network Devices. Servers, Application Systems And Administrator/Privileged accounts users
51.	N/A	N/A	Provide a list of data sources that require log collection.	Network Devices. Servers, Application Systems And Administrator/Privileged accounts users

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

52.	N/A	N/A	Do you required SOAR as part of the projects?	YES
53.	N/A	N/A	Is SOAR is required, please list the systems that require integration?	All systems within scope
54.	N/A	N/A	Do you require to outsource events analysis to external SOC analysts or will you use your inhouse SOC analysts?	Within the Tender, The provider is to provide a L2 Soc Analyst
55.	N/A	The Product Should be internationally rated in Gartner and has consistently been placed in the Leaders Quadrant in the last four years. It should also be in the Forrester wave	Can this be extended to at least include Challengers and Leaders for 1 year beginning 2022 since some products are good and can meet all the outlined technical requirements and be of value and better ROI to the Government SOC?	No, we are interested in the referred to Quadrant.
56.	N/A	The solution should support multi-factor authentication for login, and should have automatic session timeout and logout policies.	Will ICTA be providing a system for integration for 2FA or this should be proposed as part of the bid response to cover the 15 users of the SOC?	The system should be able to integrate in 2FAwhci ICTA will have at a later stage.
57.	N/A	The SIEM solution should be able to process and analyse a minimum of 1,500 log events per second.	Which of the above should be considered for licensing? Should the licenses be perpetual or subscription?	For the Licensing – 1500 Licensing should be perpetual

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

		The solution should be able to handle high volumes of network traffic – 20000 EPS, with the capability to process and analyze 20000 of events per second.	Support and Threat Intelligence subscription should be for 1 year or 3 years? Apart from EPS are we able to get an estimate of total devices in the Data Centre to be monitored? Should the solution be hardware or VM-based?	Threat Intelligence subscription should be for 1 year. Total devices can be about 2500 which is expected to increase with time. We are okay with deployment of the solution on a virtual environment which will be provided by ICTA.
58.	N/A	The Product Should be internationally rated in Gartner and has consistently been placed in the Leaders Quadrant in the last four years. It should also be in the Forrester wave	Can this be extended to at least include Challengers and Leaders for 1 year beginning 2022 since some products are good and can meet all the outlined technical requirements and be of value and better **ROI to the Government SOC?**	No, we are interested in the referred to Quadrant.
59.	N/A	The solution should support multi-factor authentication for login, and should have automatic session timeout and logout policies.	Will ICTA be providing a system for integration for 2FA or this should be proposed as part of the bid response to cover the 15 users of the SOC?	The system should be able to integrate in 2FAwhci ICTA will have at a later stage.

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

60.	N/A	The SIEM solution should be able to process and analyse a minimum of 1,500 log events per second. The solution should be able to handle high volumes of network traffic – 20000 EPS, with the capability to process and analyze 20000 of events per second	• Which of the above should be considered for licensing? • Should the licenses be perpetual or subscription? • Support and Threat Intelligence subscription should be for 1 year or 3 years? • Apart from EPS are we able to get an estimate of total devices in the Data Center to be monitored? • Should the solution be hardware or VM-based?	For the Licensing – 1500 Licensing should be perpetual Threat Intelligence subscription should be for 1 year. Total devices can be about 2500 which is expected to increase with time. We are okay with deployment of the solution on a virtual environment which will be provided by ICTA.
61.	N/A	N/A	We are working on the subjected tender and due to its technical complexity and magnitude we were requesting if we can get 14days extension from the closing date so that we can give the institution a well-designed solution	Tender Closing/Opening Date Extended to Friday,9th February,2024 @10.00am

ICT Authority
Telposta Towers 12th Floor, Kenyatta Ave
PO Box 27150 - 00100 Nairobi Kenya
www.icta.go.ke

TENDER NO. ICTA/OT/09/2023-2024 **31st January, 2024**

TENDER NAME: SUPPLY, DELIVERY, DEPLOYMENT & COMMISSIONING OF A GOVERNMENT SECURITY OPERATIONS CENTRE'S SECURITY INCIDENTS AND EVENTS MONITORING SYSTEM (SIEM)

NOTE: The Tender Closing/Opening Date has been extended to Friday, 9th February, 2024 at 10.00am

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