KENYA REINSURANCE CORPORATION LTD

ADDENDUM 2

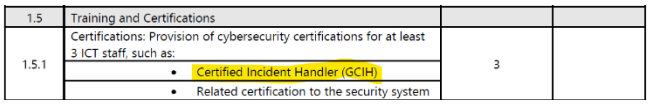
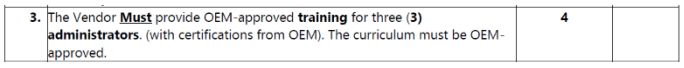
Pursuant to section 75 of the PPADA 2015, **Kenya Reinsurance Corporation Limited** wishes to clarify to various aspects of the tender for SUPPLY, INSTALLATION OF SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SOLUTION WITH REAL TIME MONITORING AS AN OUTSOURCED SERVICE: **KRC/2025/2568/235**

Clarification	**KenyaRe Response**
Send clarifications below: 1. Clarify on the number/capacity of licenses to be supplied (EPS for events and capacity for network flows). 2. For the outsourced monitoring aspect, are you looking for an in-house SOC analyst sitting at your site or remote. If you are in-house, do you want 24Hrs shift or 8Hrs duration. 3. We are requesting extension by a week.	1. 10,000 EPS, with scalable options available in increments of 5,000 EPS to accommodate future growth. 2. Fully remote Outsourced 24/7/365 SOC. **3. Addendum 1 is on Kenya Re's website extending the tender opening date to 11th September 2025.**
<u>QUERIES</u> **A. Requirement:** Acquisition and deployment of an online Security Information and Event Management (SIEM) solution, with warranty. **Clarification Request:** 1. What are the online and archive log retention periods required for this online SIEM service? **B. Requirements:** 1. The solution should have SOAR Integration capabilities, Optional Security Orchestration, Automation, and Response (SOAR)	**What are the online and archive log retention periods required for this online SIEM service?** Logs will be retained online and accessible for a period of 12 months. Archive retention at 7 years, the best international standards.

capabilities for automated workflows (e.g., isolating an endpoint or blocking an IP). 2. The solution should have Prebuilt and customizable incident response playbooks for common scenarios (e.g., ransomware, phishing). **Clarification Request:** 1. Should SOAR playbooks subscription be included as part of the proposal or is this to be considered in the future? **C. Requirement:** Certification Training for three (3) KRC ICT staff 1. **Clarification Request:** Should this be online or physical training? If Physical training, is it within Kenya or outside Kenya. If outside Kenya, we can include the Air Tickets, Visa, Accommodation and we would like to know the Per diem charges to be included.	This is not a mandatory requirement, however, is it highly preferred. The SIEM system should also be able to have seamless integration with any SOAR Platform in the future. **Certification Training for three (3) KRC ICT staff** 1. This is expected to be a comprehensive OEM-curriculum-and-venue-approved physical training, it can be either in the country or outside – but outside the Corporation office, depending on the bidder's technical capacity. Other details like Visa and accommodation requirements will be provided anytime on request.
Requirement: Acquisition and deployment of an online Security Information and Event Management (SIEM) solution, with warranty. **Clarification Request:** 1. What are the online and archive log retention periods required for this online SIEM service? **Requirements:** 1. The solution should have SOAR Integration capabilities, Optional Security Orchestration, Automation, and Response (SOAR) capabilities for automated workflows (e.g., isolating an endpoint or blocking an IP). 2. The solution should have Prebuilt and customizable incident response playbooks	**What are the online and archive log retention periods required for this online SIEM service?** - Logs will be retained online and accessible for a period of 12 months. Archive retention at 7 years, the best international standards

<table>
<tr>
<td>for common scenarios (e.g., ransomware, phishing).
Clarification Request:
1. Should SOAR playbooks subscription be included as part of the proposal or this is to be considered in the future?

Requirement: Certification Training for three (3) KRC ICT staff
Clarification Request: Should this be online or physical training?</td>
<td>Should SOAR playbooks subscription be included as part of the proposal or this is to be considered in the future?
This is not a mandatory requirement, however, is it highly preferred. The SIEM system should also be able to have seamless integration with any SOAR Platform in the future.

Certification Training for three (3) KRC ICT staff
This is a comprensive physical training.</td>
</tr>
<tr>
<td>Question 1. The tender document gives two different values for the tender security requirement. Are we providing a bid security of Kes 450,000.00 or 500,000.00?</td>
<td>Correct bid security is 450,000.00</td>
</tr>
<tr>
<td>Make the Joint Venture Option open for at least two members in a single JV</td>
<td>Joint venture option is allowed. However, a Joint Venture Agreement MUST be submitted between the parties involved together with the bid document, with clear roles and responsibilities defined in the agreement.</td>
</tr>
<tr>
<td>1> On Page 37 you have asked for Training from OEM and an additional 3rd party training. This is a very costly training from SANS which cost USD 8900 + USD 999 per person for virtual training with certification.
Please suggest if we need to quote for the same.
 
<table>
<tr><td>1.5</td><td>Training and Certifications</td><td></td><td></td></tr>
<tr><td rowspan="3">1.5.1</td><td>Certifications: Provision of cybersecurity certifications for at least 3 ICT staff, such as:</td><td rowspan="3">3</td><td rowspan="3"></td></tr>
<tr><td>• Certified Incident Handler (GCIH)</td></tr>
<tr><td>• Related certification to the security system</td></tr>
</table>
However, Page No 32, Talks about OEM Approved Training and not SANS training. Please suggest what needs to be quoted.
 
<table>
<tr><td>3.</td><td>The Vendor <u>Must</u> provide OEM-approved training for three (3) administrators. (with certifications from OEM). The curriculum must be OEM-approved.</td><td>4</td><td></td></tr>
</table></td>
<td>Comprehensive physical OEM training and certification, along with additional cybersecurity certifications focused on incident handling specifically for the proposed SIEM solution.</td>
</tr>
</table>

2> Is Kenya RE is looking for on-premises deployed or cloud deployed solution delivered as a service.	We require the SIEM system to be hosted within our environment, though we are open to a hybrid deployment model. It is essential that we retain full access to and control over our resources.
How is EventLog Analyzer Licensed?	Propose your license model
How many number of Windows Servers?	80
How many number of Windows Workstations?	Approximate 200 (consider scalability)
How many number of Syslog Devices?	32 Network devices
How many number of Domain Controllers are to be audited?	4
Add-ons	
How many number of Windows File Servers?	3
How many number of Linux File Servers?	The solution should be scalable for future changes
How many number of NetApp/EMC/Synology NAS are to be audited?	2, but the solution should be open to future applications.
How many number of MS SQL Servers?	3
How many number of IIS Sites?	4
How many number of other applications sources (If any) ?	The solution should be scalable for future changes
Cloud Source Auditing : provide the below details:	
Specify the number of O365 tenants	1, The solution should be scalable for more in the future.
How many number of AWS accounts	1, The solution should be scalable for more in the future.
User & Entity Behaviour Analytics (UEBA): Do you require this add-on? Please specify Yes/No.	This is important, yes.
Exchange Server Auditing: How many number of Exchange Servers?	3
License Type	
Required License Type (Annual/Perpetual)	Do propose the license model for your proposed solution
Number of Years for Annual Maintenance & Support (AMS), if Perpetual	Support is throughout the contract period.
I need some clarification on the following. The technical evaluation does not clearly state	**User-based licensing: A set number of users are granted access.**

• User-based licensing: A set number of users are granted access. • Resource-based licensing: A set number of servers, hosts, or other equipment can be managed. The two above will determine part of the pricing; can the above be provided?	At least 1 super user account and 3 Analysts accounts. **Resource-based licensing: A set number of servers, hosts, or other equipment can be managed.** 200 endpoints (scalable), 80 servers and 32 network devices. The system should support concurrent license allocation and use.

The addendum has been sent to all bidders who have so far downloaded the respective tender documents. Any bidder who has not received their relevant addendum may download the same from the Kenya Re website **www.kenyare. co.ke.** All other conditions and requirements in the respective principal tender documents remain the same.

Prospective bidders may download the principal tender document from the Kenya Re website **www.kenyare. co.ke** free of charge

Tenders in sealed envelopes bearing the correct **tender number** should be deposited in the Tender Box located on the 16th floor of Reinsurance Plaza Aga Khan Walk Nairobi or be sent to: -

Managing Director
Kenya Reinsurance Corporation, Ltd
Reinsurance Plaza, Nairobi
Aga Khan Walk
P.O. Box 30271 - 00100
NAIROBI