African Reinsurance Corporation
Société africaine de réassurance

1st July, 2022.
INVITATION TO TENDER – SELECTION OF VENDOR FOR THE IMPLEMENTATION OF SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTION

1.0 BACKGROUND

Established in 1976 by 36 member States of the African Union and the African Development Bank Group (AfDB), The African Reinsurance Corporation (AFRICA-RE), the leading reinsurance company in Africa and the Middle East, is a pan-African financial institution whose shareholding is split between African (75%) and Non-African (25%) investors. African shareholding comprises 41 African states, the AfDB and more than 100 African insurance/reinsurance companies from the 41 member countries. Headquartered in Lagos (Nigeria), Casablanca (Morocco), Nairobi (Kenya), Abidjan (Cote d'Ivoire), Ebene (Mauritius), Cairo (Egypt) and Addis Ababa (Ethiopia) as well as two subsidiaries: Africa Re (South Africa) Ltd in Johannesburg and Africa Retakaful Ltd in Cairo (Egypt).

The corporation is currently in the process of implementing a Next-Generation Security Information and Events Management (SIEM) solution to help the corporation analyze events data in real-time for early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response, forensics, and regulatory compliance. This solution must have a vast variety of capabilities beyond enhanced visibility such as proactive threat detection, continuous compliance, automatic containment and elimination of potential threats that will decrease the risk exposure of the corporation.

2.0 OBJECTIVES

Africa Re is requesting proposals from interested and qualified firms to supply and implement a Security Incident and Event Management solution. The purpose of this project is to aid the corporation with improved visibility, functionality and overall enhanced security monitoring while providing a holistic and real-time view of its information security landscape.

The corporation is seeking a modern, feature-rich, and comprehensive Security Incident and Event Management solution, capable of supporting log management across a wide range of systems and devices, including custom-developed applications and providing relevant contextual detail.

The SIEM is required to provide high-performance advanced threat detection, near real-time event processing and correlation, historical data analysis, and the integration of contextual and threat intelligence data. This component also must include compliance and incident reporting, automated alerting of common security events, historical analysis for detected incidents and interoperate with other information security systems using industry-standard protocols.

The corporation seeks qualified vendors with the necessary technical skills, experience and business knowledge to implement a robust SIEM that must include:

- Log Management
- Host Forensics,
- User and Entity Behaviour Analytics (UEBA),
- Network Traffic Analysis
- Security Analytics,
- Real-Time Notification & Alerting
- Automated Security Workflows
- Big Data Analytics,
- Security Automation and Orchestration engine (including, but not limited to Incident Management and Response),
- Best practices and Triage / Fix Recommendations
- Advanced Log Correlation & Threat Intelligence / analysis within the same platform
- Robust Reporting functionality with customizable templates and Dashboards

Below is an overview of Africa Re's current network infrastructure:

- Africa Re currently host its services in AWS (Amazon Web Services) in VMWare containers across 2 Data Centers.
- Africa Re operate in multiple branches (Cairo, Casablanca, Abidjan, Nairobi, Addis-Ababa, Mauritius, Johannesburg) with active users in these branches.
- The connectivity between Africa Re HQ and branches is through IPSec VPN using Fortinet firewalls.
- The current total number of assets within our environment to be covered within this SIEM scope is 500 assets which includes network devices, servers and personal computers.
- The operating systems on endpoints i.e. PCs and mobile devices in Africa Re environment is a mix of Windows, MAC OS, and Linux.

3.0 DELIVERABLES

The solution and implementation services required from vendors must have the following capabilities:

1. **Data Aggregation**
    a. The solution must aggregate data from network, hosts, servers, databases, applications, and other security systems like firewalls, anti-virus and Intrusion Detection Systems (IDS).
    b. Machine intelligence and big data analytics capability to aggregate evidence and identify threats.

2. **Correlation**
    a. The solution should link events and related data to construct a real security incident, threat, vulnerability or forensic finding.
    b. Solution should be capable to correlate events irrespective of time slicing

c. Solution should be able to detect when data/logs stop being received.
d. Solution should be able to use correlation rules that are predefined.
e. Solution should have capabilities in creating data visualizations, creating reports, execute scripts, and take Remediation Actions based on event correlations.
f. Solution shall have support for identity-oriented monitoring — real-time views and reporting.

g. Solution should have capabilities to detect when a user login occurs from multiple, geographically distant locations within a short time span.
h. Solution should offer capabilities in terms of geolocation functionality.
i. Solution should have capabilities in using user defined thresholds when authoring correlation rules.
j. Solutions shall support real-time event correlation and shall trigger alerts based on event correlations.

3. User Entity and Behavior Analytics (UEBA)

a. The UEBA must be fully integrated within the proposed solution – not through any separate integrated software.
b. The UEBA must be able to detect and respond to insider threats, compromised accounts and privileged account abuse.
c. The UEBA must collect machine data from across the environment and complete forensic gaps with endpoint and network monitoring.

4. Threat Intelligence

a. The solution should combine internal data with threat intelligence data to form a more comprehensive security outlook.
b. Solution should be able to leverage combination of behavioral analysis, machine learning and dynamic threat intelligence to detect and contain/eliminate known as well as unknown cyber security threats.
c. Unparalleled Visibility: Advanced behavioral and machine learning technologies that gives customers full visibility of both internal and external adversary activity
d. Multi-Layer Detection: Detection of known as well as never-before-seen threats at the earliest phase of the chain
e. Automated Response: Enabling rapid, surgical responses at scale to eradicate threats
f. Threat Impact Analysis: Comprehensive interactive visual interface to drill down threats and effected sources and targets

5. Incident Response

a. The solution should provide case management, collaboration and knowledge sharing around security incidents, providing a centralized portal for SOC analysts to manage, track and coordinate the threat response.

6. Data Collection:

a. Solution should be capable of collecting information from an external system via a RESTful API, capable of monitoring remote files and directories for changes, AND retrieving and storing data from a remote system via FTP, SFTP, and SCP.
b. Solution should be able to collect data from cloud hosted services, especially for log collection.
c. Solution should support PARSER or equivalent module for identification to differentiate data from incoming sources, and then should be able to normalize such data from multiple sources.
d. Solution should be capable of creating custom parsers (including for non-syslog data)
e. Solution shall be capable of supporting multi-line logging data.
f. Solution should be able to import data from Windows devices, network devices, cloud services, applications and other security systems.

7. Alerting:

a. Solution should support email-based alerts and should support pre-defined alerts.
b. Solution should support email or text notifications, along with functionality to email comprehensive periodic reports and dashboards
c. Solution should be capable of suppressing alerts if required by defining "Not an Alert" Action
d. Solution should support display alerts in the solution's UI

8. Reporting:

a. Solution should be able to produce reports on-demand and produce scheduled reports.
b. Solution should be able to schedule reports at varying granularities, i.e. monthly, weekly, or daily as required.
c. Solution should provide support for creating user-configurable reporting, creating customized dashboards, and creating data visualizations (such as maps, graphs, etc.)
d. Solution should have capability for automatically emailing reports.
e. Solution should have capabilities for automatic asset grouping and classification based on application.
f. Solution should support client-defined asset grouping and classification
a. The solution must provide comprehensive reporting with built-in and customized reporting capabilities. It should contain existing and customizable templates for various roles e.g. senior executive, mid-level management, and various administrator levels.
b. Solution should be able to retain Threat Alerts Data based on retention policy to assist with regards to forensic data retention, organization, and access.

c. Solution should be able to control which type of data/reports/query results can be exported based on user access.

Other Functional and Technical Requirements

a. The solution must support auto-discovery of assets that are being protected or monitored.
b. The solution must support both agent-based and agent-less log collection. The logs must be able to be compressed to support efficient collection over low bandwidth networks.
c. The solution must support log compression of both data in transit and at rest.
d. The solution must be able to collect logs in real-time and start processing as soon as possible.
e. The solution must have built-in ticketing/incident workflow management and also have the capability to integrate with an external ticketing system.
f. The solution must have built-in evidence locker capability to preserve forensic data and support proper chain-of-custody.
g. The proposed solution must have predefined use cases out of the box.
h. The solution must allow the admin to visualize the attack through a simple diagram showing the connection from the source to the destination.
i. The solution being offered must include full packet capture and network forensics capabilities and session replay.
j. Solution must integrate with a LDAP or AD solution for access provisioning to the SIEM system.
k. The solution must have the ability to categorize event/alerts into various levels such as critical, high, medium and low, etc.
l. The solution must report on devices that are no longer actively sending logs to the SIEM solution.
m. The solution must not drop any events if the EPS exceeds the purchased license volume.
n. Data must be encrypted in transit, in storage and integrity checking should be enforced by the system.
o. The solution must allow custom parsers for custom applications.
p. The solution must support Information Lifecycle Management, i.e. archiving old logs out of the system into an active archive/online archive solution where they can be used for future compliance needs and free up space on the appliance/solution itself.
q. The solution must be capable of gathering, documenting and preserving detailed event information, allow for the analysis of evidence and maintain a complete audit trail of the investigation process.
r. The solution must be capable of detecting high-risk administrative actions/activities on critical assets, like out-of-policy configuration changes to high-risk assets, or unusual privilege delegation.
s. The solution must be capable of detecting suspicious user activity.

t. The solution must support role-based access with predefined and customizable options.

4.0 EVALUATION PROCESSES AND SELECTION CRITERIA

Responses to this RFP will be evaluated and scored based on the following criteria:

- In-depth knowledge of the information system architecture & design for (re) insurance businesses will be a minimum requirement.
- Experience of the service provider in implementing Security Information and Events Management Solution (specifically Rapid 7 InsightIDR SIEM solution).
- Technical approach and methodology
- Organization and staffing
- Proposed Cost
- Financial Information
- Similar projects delivered previously
- Quality, clarity and presentation of proposal

5.0 PRESENTATION OF TENDER

In order to facilitate the analysis of responses to this RFP, the responding vendors are required to prepare their proposals in accordance with the instructions outlined in this section. The firms/vendors whose proposals deviate from these instructions would be considered non-responsive and may be disqualified at the discretion of Africa Re.

Proposals should be clear and comprehensive. It should provide a straightforward, concise description of the vendor's capabilities to meet the requirements of the RFP. Emphasis should be laid on accuracy, completeness and clarity of content. All parts, pages, figures and tables should be numbered and clearly labeled. The proposal should be organized into the following major sections:

Section Title

1.0 Executive summary
2.0 Company Experience / Expertise
3.0 Technical approach and methodology
4.0 Organization and staffing
5.0 Cost quotations
6.0 Financial information
7.0 Resumes of key staff to be deployed

5.1 Executive summary

This part of the response to the RFP should be limited to a brief narrative highlighting the vendor's proposal. The summary should contain as little technical details as possible and should be oriented towards non-technical personnel. The Executive summary should not include cost quotations.

5.2 Experience of the Vendor

The vendor must provide the following information about their company so that Africa Re can evaluate their stability and ability to support the commitments set forth in response to the RFP. Africa Re may require the vendor to provide additional documentation to support and/or clarify requested information.
[Using the format below, provide information on each relevant assignment for which your organization, and each associate for this assignment, was legally contracted either individually, as a corporate entity or, as one of the major companies within an association, for carrying out projects similar to the ones requested under the Terms of Reference included in this document. The Proposal must demonstrate that the Vendor has a proven track record of successful experience in providing services similar in substance, complexity, value, duration, and volume of services sought in this procurement.]
Maximum 20 pages

Assignment name:	Approximate value of the contract (in currency US$):
Country: Location within country:	Duration of assignment (months):
Name of client:	Total No of staff-months of the assignment:
Address:	Approximate value of the services provided by your firm under the contract (in currency US$):
Start date (month/year): Completion date (month/year):	No of professional staff-months provided by associated vendors:
Name of associated consultants, if any:	Name of proposed senior professional staff of your firm involved and functions performed:
Narrative description of review engagement:	
Description of actual services provided by your staff within the assignment:	
Description of challenges encountered, and the strategy used to address and successfully close the project including time and resources:	

Authorised Signatory:

Name of Vendor:

5.3 Approach and Methodology
In this chapter, you should explain your understanding of the objectives of the assignment, approach to the services, methodology for carrying out the activities and obtaining the expected output and the degree of detail of such output. You should highlight the problems being addressed and their importance and explain the technical approach you would adopt to address them. You should also explain the methodologies you propose to adopt and

highlight the compatibility of those methodologies with the proposed approach.

5.4 Organization and Staffing

In this chapter, you should propose the structure and composition of your team. You should list the main disciplines of the assignment, the key expert responsible, and proposed technical and functional staff.

5.5 Cost Quotations

Your proposal should include supply and installation of items in the Bill of Material below:

S/N	SKU	Description	Qty	Unit
A	**Rapid7 InsightIDR**			
1	Rapid7:IDR-ADV-SUB	IDR-ADV-SUB - InsightIDR Advanced 1 YR Subscription	250	No
2	Services	Implementation Services	1	Lots
3	Training	Certificated Training for up to 3 Delegates	3	Delegates

5.6 Financial Information

The vendor's financial information should be included in this section. Financial information must include audited financial information for the past three years if applicable.

5.7 Resumes

The vendor must make every effort to select staff for the assignment based on Africa Re's needs. Applicable resumes should be included in this section.

6.0 COMPANY AND OTHER GENERAL REQUIREMENTS

No.	Requirement	Vendor Response
6.1	**Company Information Requirements**	
a)	How long has company been in business?	
b)	How long has the company been in business providing the proposed Network Security services for complex implementation projects?	
c)	State number of employees in the company.	
b)	State total number of employees dedicated to this assignment.	

7.0 CLARIFICATION AND AMENDMENT OF REQUEST FOR PROPOSAL

The vendor may request for clarification only up to 7 days before proposal submission date. Any request for clarification must be sent in writing by letter or email to the Africa Re's address indicated below. Africa Re will respond by letter or email to such requests and will send written copies of the response (including an explanation of the query but without identifying the source of the inquiry) to all firms which intend to submit proposals.
Contact for clarification: icttender@africa-re.com

8.0 PROPOSAL SUBMISSION
The Proposals should be submitted through the email address tender@africa-re.com not later than July 28, 2022, and the subject of the email should read "**IMPLEMENTATION OF SECURITY INFORMATION AND EVENT MANAGEMENT SOLUTION**". Any proposal received by Africa Re after the submission deadline shall be rejected.

9.0 AFRICA RE RIGHTS RESERVED
AFRICA RE reserves the right, in its sole discretion, to take actions deemed in AFRICA RE's best interest that may include any one or more of the following without thereby incurring any liability to the affected bidder(s) of any obligation to inform the affected bidder(s)
• Accept or reject any or all proposals in whole or in part, at any time prior to award of Contract
• Waive any minor irregularities or informalities in a proposal
• Vary any timetable or schedule, or suspend or modify the RFP process
• Negotiate the details of a proposal prior to contracting

10.0 OWNERSHIP AND RETURN OF PROPOSAL
All materials submitted in response to this RFP shall become the property of AFRICA RE and shall not be returned to the respondent.

For: African Reinsurance Corporation

Dr. Corneille KAREKEZI

Group Managing Director / Chief Executive Officer