



REQUEST FOR PROPOSAL

RFP FOR ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT

RFP-2025-002/006

RELEASE DATE: 28th February 2024

CLOSING DATE: 19th March 2024

RFP for ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT.

Table of Contents

1 INTRODUCTION.....	5
1.0 Purpose of the Tender	5
1.1 Acknowledgement of Bidding Documents	5
1.2 Point of Contact	6
2 ABOUT BRITAM HOLDINGS PLC.....	6
2.0 Organization Profile	6
2.1 Britam's Vision.....	6
2.2 Britam's Mission.....	7
3 OVERVIEW OF THE PROPOSAL	8
3.0 Overview.....	8
3.1 Objective of the RFP.....	8
3.2 Scope of Work.....	8
3.2.1 Solutions to Consider.....	9
3.2.2 Quantity.....	9
3.3 Qualifying Criteria and Requirements:.....	10
3.4 Technical Proposal	11
3.5 Financial Proposal	12
4 FORMAT OF RESPONSE TO TENDER.....	13
4.0 MANDATORY Information to be provided by bidders.....	13
4.1 General Information about the firm.....	13
4.2 Bid Preparation and Submission.....	14
5 GENERAL CONDITIONS OF CONTRACT.....	15
5.1. INTRODUCTION	15
5.2. AWARD OF CONTRACT.....	15
5.3. APPLICATION OF GENERAL CONDITIONS OF CONTRACT.....	15
5.4. BID VALIDITY PERIOD	15
5.5. NON-VARIATION OF COSTS.....	15
5.6. DELAYS IN THE BIDDER'S PERFORMANCE	15
5.7. LIQUIDATED DAMAGES FOR DELAY	16
5.8. GOVERNING LANGUAGE.....	16
5.9. APPLICABLE LAW	16
5.10. SUCCESSFUL BIDDER'S OBLIGATIONS	16
6 BRITAM SUPPLIER CODE OF CONDUCT.....	18
6.1 GENERAL.....	18
6.2 PROVISIONS	18
6.2.1 Relations with competitors.....	18
6.2.2 Bribes, Conflicts of Interest, Gifts and other Courtesies	18
6.2.3 Compliance and implementation.....	19
6.2.4 Violations.....	20
6.2.5 Variations.....	20

EXPRESSSION OF INTENT TO PARTICIPATE IN TENDER

This form is to be completed on receipt of the tender document from Britam Holding PLC.

This page is to be completed immediately and scan copy in PDF format e-mailed to Procurement tenders@britam.com. The data contained in this form will be used to send out any addenda that may arise. Firms that do not register their interest by completing this form may not be sent addenda that may arise.

Name of the firm's representative completing this form:

Firm's

Name:

Address:

Tel

No:

Email

Address:

Signature: _____ Date: _____

Signed by (Name): _____

Position

in

Firm:

1 INTRODUCTION

1.0 Purpose of the Tender

The Britam Holding Company Limited ("Britam") invites qualified firms to submit their proposals for Endpoint Detection and Response (EDR) Solution Deployment.

This Request for Proposal (RFP) is being made available to interested service providers on a restricted tender basis. This document is intended to provide vendors with sufficient understanding of the Britam's requirements to enable them to respond.

For the purposes of the RFP, it is necessary to disclose information in this document, and its schedules, which is considered confidential and should therefore not be used (otherwise other than in furtherance of this tender) or disclosed to any third party without explicit prior written consent of Britam.

Britam on its part also acknowledges that it is requesting through this RFP for information that is confidential and therefore commits in equal terms to reciprocal confidentiality.

1.1 Acknowledgement of Bidding Documents

Britam invites proposals for **RFP for Endpoint Detection and Response (EDR) Solution Deployment** in accordance with the requirements set out in this document.

Within **three (3) working days** of receipt of the RFP, the Bidder is required to acknowledge receipt of the RFP and notify his intention to submit a bid by email to Britam at tenders@britam.com. The mail will include the signed registration template on Page 4 of this document.

Working days are defined as being any day of the week between Monday and Friday (0800 – 1700 Hrs) excluding weekends and gazetted public holidays in the Republic of Kenya).

Failure to do so shall be perceived as an intention not to submit a bid and the Bidder will be eliminated from the bid process and required to destroy the RFP document in keeping with confidentiality requirements.

RFP for ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT.

1.2 Point of Contact

All enquiries or correspondence concerning the details of this tender should be addressed, in the first instance by e-mail to: tenders@britam.com . The subject on the email should be **"CLARIFICATION ON THE RFP FOR ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT"**.

- All responses from Britam to the Bidder shall be channelled through the Procurement Officer.
- It is the responsibility of the Bidder to obtain any further information required to complete this RFP.
- Any clarification request and their associated response will be circulated to all Bidders.
- All clarifications must be sought at the latest 5 days prior to the close of the RFP.

2 ABOUT BRITAM HOLDINGS PLC

2.0 Organization Profile

Britam Holdings PLC ("Britam") is a leading diversified financial services group, listed on the Nairobi Securities Exchange. The group has interests across the Eastern and Southern Africa region, with operations in Kenya, Uganda, Tanzania, Rwanda, South Sudan, Mozambique, and Malawi. The group offers a wide range of financial products and services in Insurance, Asset management, Banking and Property. For more information, please visit <http://www.britam.com>.

The Group offers a wide range of products and services to individuals, small businesses, corporations, and government entities. The range of products includes life insurance, pensions, health insurance, and general insurance through its insurance businesses in the region. The financial solutions which include, unit trusts, investment planning, wealth management, offshore investments, retirement planning and discretionary portfolio management which are offered through its asset management business. In addition, the company carries out property development and has substantial investments in the banking sector. For More information, please visit <http://www.britam.com>

2.1 Britam's Vision

To be LEADING diversified financial services company in our chosen markets across Africa.

2.2 Britam's Mission

Providing you with financial security EVERY STEP OF THE WAY.

3 OVERVIEW OF THE PROPOSAL

3.0 Overview

3.1 Objective of the RFP

The scope of this RFP is to acquire and deploy a comprehensive EDR solution that improves the detection and response capabilities for endpoint devices across the organization. This solution must provide continuous endpoint monitoring, behavioral analysis, incident response, and forensic capabilities to identify and mitigate advanced threats. It must integrate seamlessly with the existing security infrastructure and provide centralized visibility and management.

The primary objectives of the EDR solution deployment are:

1. **Enhanced Threat Detection and Response:**
 - Detect and respond to advanced threats, including malware, ransomware, and fileless attacks that may bypass traditional endpoint protection mechanisms.
 - Improve visibility into endpoint activity and quickly investigate suspicious events.
2. **Proactive Threat Hunting:**
 - Enable proactive threat hunting by empowering security teams to search for hidden or unknown threats across endpoints.
 - Provide actionable intelligence and insights to prevent potential breaches before they impact the organization.
3. **Advanced Forensics and Incident Response:**
 - Provide detailed forensic analysis to understand the root cause of security incidents.
 - Offer rapid incident response capabilities, such as endpoint isolation, containment, and remediation.
4. **Seamless Integration with Existing Infrastructure:**
 - Ensure that the new EDR solution integrates seamlessly with the existing security environment without disruptions to operations.
 - Offer centralized visibility and reporting to simplify endpoint security management.
5. **Zero-Day and Advanced Threat Detection:**
 - Enhance detection and prevention capabilities against zero-day exploits, advanced persistent threats (APTs), and sophisticated malware.

3.2 Scope of Work

The proposed EDR solution must address the following requirements:

Use Case	Description
Advanced Threat Detection	Detect sophisticated threats such as malware, ransomware, and APTs that may evade traditional defenses.
Proactive Threat Hunting	Enable security teams to conduct proactive searches for hidden or undetected threats.

Use Case	Description
Malware and Fileless Attack Prevention	Prevent advanced malware and fileless attacks that evade traditional detection methods.
Behavioral Analytics	Provide behavioral analysis to identify suspicious patterns and potential threats.
Zero-Day Exploit Protection	Detect and mitigate zero-day exploits that are not detected by traditional signature-based methods.
Root Cause Analysis and Forensics	Provide comprehensive forensic capabilities to investigate and determine the root cause of attacks.
Incident Response	Enable rapid isolation and remediation of compromised endpoints to minimize damage.
Cloud and On-Premises Deployment Support	Support both cloud-based and on-premises deployment models to meet the organization's needs.
Integration with Existing Security Infrastructure	Seamlessly integrate with existing security tools, such as SIEM systems, for centralized monitoring and management.
Automated Remediation and Orchestration	Automate incident response actions such as endpoint isolation, remediation, and reporting.
Scalability	Ensure the solution can scale to accommodate an increasing number of endpoints and evolving security threats.

3.2.1 Solutions to Consider

The following EDR solutions are recommended for consideration:

1. **CrowdStrike Falcon** – Offers next-gen endpoint protection, threat intelligence, and behavioral analytics with advanced incident response capabilities.
2. **SentinelOne Singularity** – Provides autonomous endpoint protection, real-time detection, and prevention of fileless and advanced malware.
3. **Microsoft Defender for Endpoint (EDR)** – Offers integrated protection, detection, investigation, and response for endpoints within the Microsoft ecosystem, including advanced threat detection, machine learning-based analytics, and automated response capabilities. This solution leverages the existing Microsoft ecosystem for seamless integration with other security tools like Microsoft Sentinel and Microsoft Defender for Identity.

Vendors should demonstrate how their solutions address the requirements identified above and complement the existing endpoint security measures.

3.2.2 Quantity

Seats Required: 1350 devices (desktops, laptops and servers across the organization.

3.3 Qualifying Criteria and Requirements:

The proposed solution must meet the following criteria:

- **Vendor Expertise:** Must be a recognized leader in the EDR space, with a proven track record of successful deployments in large-scale organizations.
- **Seamless Integration:** The solution should integrate smoothly with the existing security tools and infrastructure.
- **Advanced Threat Detection:** Must provide advanced detection of zero-day threats, APTs, and sophisticated malware.
- **Incident Response and Automation:** Must include incident response automation and efficient remediation workflows.
- **Scalability:** The solution should be scalable to meet the growing number of endpoints and evolving threat landscape.
- **Regional Support:** The vendor must be capable of providing regional support for the implementation and ongoing management of the solution.
- **Support and Maintenance:** Ongoing support, software updates, and incident response assistance should be part of the vendor offering.

3.4 Technical Proposal

Potential respondents to provide the following **mandatory** information.

- I. Company Profile:** Document detailing the company including its background, products & services, clients, and expertise.
- II. Functional documentation:** Comprehensive product/system documentation detailing the systems functional capabilities.
- III. Technical documentation:** Comprehensive system technical documentation detailing the following
 - Detailed System architecture and proposed deployment architecture and Deployment specification (e.g. server and storage specifications)
 - Security overview of the system
 - System dependencies and accompanying products.
 - API catalogue for out of the box APIs
 - Integration Capabilities: Demonstrate how the proposed solution integrates with existing IT systems. How the EDR solution integrates with existing network infrastructure and other security tools (SIEM, firewall, etc.).
 - Scalability: Ensure that the solution is scalable to meet future organizational needs, both in terms of users and data growth.
 - Compliance Requirements – Does the vendor help meet ISO 27001, NIST, GDPR, HIPAA, SOC 2, PCI-DSS compliance needs.
- IV. Product roadmap:** Comprehensive Product/System roadmap detailing past and future releases
- V. Project execution Plan and Methodology:** Comprehensive and clear project execution plan with timelines for each activity.
- VI. Project Team:** Documentation detailing the proposed project team including the Professional qualifications, experience, and role. Briefly highlight the profiles and technical qualifications of the staff to be involved in the project. This could include the numbers of years of experience in a role; level of professional qualification with reputable bodies; and any other relevant qualification.
- VII. References:** Potential vendor to provide references and summary of similar jobs undertaken in last 3 years. To include the following details project baseline and actual timelines, project scope, project outcomes.
- VIII. Performance Metrics:** Provide benchmarks on the performance of the EDR solution, including False positive rate, Response automation effectiveness and Dwell time reduction.

RFP for ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT.

IX. Project governance structure: document detailing the Respondent project governance structure detailing the escalation matrix, risk management and problem management policy.

X. Support & Maintenance

1. SLA Reports from Existing Clients – Mean time to resolution (MTTR), uptime statistics, false positive rates.
2. Customer Success Metrics – Retention rate, customer satisfaction scores (CSAT/NPS).
3. Availability of 24/7 SOC & Incident Response Team – Track record in handling major security incidents.

3.5 Financial Proposal

Provide a competitive financial proposal inclusive of all cost (taxes and disbursements).

- Detailed pricing structure (setup fees, recurring costs, licensing fees, customization costs).
- Implementation costs and any other cost related to the implementation of an EDR solution.

4 FORMAT OF RESPONSE TO TENDER

4.0 MANDATORY Information to be provided by bidders.

All bids should contain **ALL INFORMATION REQUESTED IN SECTIONS 4.1 to 4.5**. The information should be in the following order.

4.1 General Information about the firm

Provide the following documentation in respect of your company.

- (i) **Certificate of registration** (or its equivalent) that is valid in accordance with any legally recognised jurisdiction.
- (ii) **Tax compliance certificate** (or its equivalent) that is valid in accordance with any legally recognised jurisdiction.
- (iii) Current County **Trade license/Business permit**
- (iv) **Accreditations** or a licence where applicable
- (v) **OEM Partnership Letter/Authorization letter**
- (vi) **Company Profile**, with a clear **organogram** and area of speciality
- (vii) List of **Directors** (Name, ID Number/passport number, Nationality, Telephone, and physical address)
- (viii) Britam **Non-Disclosure Agreement** (document to be provided to accompany this RFP)
- (ix) Britam **Supplier Code of Conduct** (document to be provided to accompany this RFP)
- (x) Britam Business Litigation and Probity; and Lead Time and Credit Period Declaration Form (document to be provided to accompany this RFP).

4.2 Bid Preparation and Submission

RFP For ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT RFP-2025-002-006

All Tenders may also be posted/ delivered earlier than the deadline to the below email:

tenders@britam.com

with a clear subject line "*RFP FOR ENDPOINT DETECTION AND RESPONSE (EDR)
SOLUTION DEPLOYMENT RFP-2025-002/006*"

Offers must be submitted in two separate documents, 1(one) technical- and 1 (one) commercial bid, **password protected** and clearly identified as:

- The file with the technical proposal should be identified as follows:

**NAME OF THE COMPANY, TECHNICAL PROPOSAL FOR ENDPOINT DETECTION
AND RESPONSE (EDR) SOLUTION DEPLOYMENT.**

- The file with commercial proposal should be identified as follows:

NAME OF THE COMPANY, COMMERCIAL / FINANCIAL PROPOSAL

5 GENERAL CONDITIONS OF CONTRACT

5.1. Introduction

Specific terms of contract shall be discussed with the bidder whose proposal will be accepted by the Company. The resulting contract shall include but not be limited to the general terms of contract as stated below from 5.2 to 5.14.

5.2. Award of Contract

Following the opening and evaluation of proposals, the Company will award the Contract to the successful bidder whose bid has been determined to be substantially responsive and has been determined as the best evaluated bid. Britam will communicate to the selected bidder its intention to finalize the draft conditions engagement in consultation with the bidder.

5.3. Application of General Conditions of Contract

These General Conditions (sections 5.2 to 5.14) shall apply to the extent that they are not superseded by provisions in other parts of the Contract that shall be signed.

5.4. Bid Validity Period

Bidders are requested to hold their proposals valid for ninety (90) days from the closing date for the submission.

5.5. Non-variation of Costs

The prices quoted for the service and subsequently agreed and into the contract shall be held fixed for the contract period.

5.6. Delays in the Bidder's Performance

- 5.6.1. Delivery and performance of the Transaction shall be made by the successful Bidder in accordance with the time schedule as per Agreement.
- 5.6.2. If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify the Company in writing of the fact of the delay, its likely duration and its

RFP for ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION DEPLOYMENT.

cause(s). As soon as practicable after receipt of the Bidder's notice, the Company shall evaluate the situation and may at its discretion extend the Bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

- 5.6.3. Except in the case of "force majeure" as provided in Clause 5.14, a delay by the Bidder in the performance of its delivery obligations shall render the Bidder liable to the imposition of liquidated damages pursuant to Clause 5.7.

5.7. Liquidated damages for delay

The contract resulting out of this RFP shall incorporate suitable provisions for the payment of liquidated damages by the bidders in case of delays in performance of contract.

5.8. Governing Language

The Contract shall be written in the English Language. All correspondence and other documents pertaining to the Contract which are exchanged by the parties shall also be in English language.

5.9. Applicable Law

This agreement arising out of this RFP shall be governed by and construed in accordance with the laws of Kenya and the parties submit to the exclusive jurisdiction of the Kenyan Courts.

5.10. Successful Bidder's Obligations

The successful bidder:

- 5.10.1. Is obliged to work closely with Britam staff, act within its own authority, and abide by directives issued by the Company that are consistent with the terms of the Contract.
- 5.10.2. Will abide by the job safety measures and will indemnify the Company from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Company responsible or obligated.

- 5.10.3. Will be responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanours.
- 5.10.4. Will not disclose the Company`s information it has access to, during the course of the work, to any other third parties without the prior written authorization of the Company. This clause shall survive the expiry or earlier termination of the contract.

6 BRITAM SUPPLIER CODE OF CONDUCT

6.1 GENERAL

This Code is applicable to all Britam suppliers (hereinafter "Supplier" or "Suppliers") and their employees (be they temporary, casual or permanent) and sub-contractors throughout the world. Britam requires all Suppliers to conduct their business dealings with Britam in compliance with this Code and in compliance with all laws applicable to the Supplier's business, wherever conducted. By entering business transactions with Britam, the Supplier agrees to abide by the terms of this Code and acknowledge that compliance with this Code is required to maintain the Supplier's status as a Britam Supplier. Britam shall have the right to terminate any Supplier's contract for failure to comply with the provisions of this Code. Britam recognizes that local laws may in some instances be less restrictive than the provisions of this Code. In such instances Suppliers are expected to comply with the Code. If local laws are more restrictive than the Code, then Suppliers are expected to comply with applicable local laws.

6.2 PROVISIONS

In particular, Suppliers must comply with the following:

6.2.1 Relations with competitors

Suppliers will be required to comply with applicable antitrust or competition laws and will not engage in any restrictive trade practices. Suppliers will at all times act in a manner that will uphold and encourage healthy competition.

6.2.2 Bribes, Conflicts of Interest, Gifts and other Courtesies

6.2.2.1 Bribes

Suppliers shall not make or offer bribes or payments of money or anything of value to any Britam employee or any other person including officials, employees, or representatives of any government or public or international organisation, or to any other third party for the purpose of obtaining or retaining business with Britam. For the avoidance of doubt Britam considers an act of bribery to include the giving of money or anything of value to anyone where there is belief that it will be passed on to a government official or Britam employee for this purpose. Suppliers are required to comply with all applicable local anti-bribery laws.

6.2.2.2 *Gifts and other business courtesies*

Suppliers shall ensure that any expenditure incurred in relation to any particular Britam employee or government official is in the ordinary and proper course of business and cannot reasonably be construed as a bribe or so as to secure unfair preferential treatment. A general guideline for evaluating whether a business courtesy is appropriate is whether public disclosure would be embarrassing to the Supplier or Britam.

Britam employees may accept unsolicited gifts from Suppliers provided:

- they are items of nominal value – Kes1500 or less, or
- they are advertising or promotional materials having wide distribution e.g. calendars, stationaries, diaries, etc.; and
- Acceptance of the gift does not violate any applicable law.

6.2.2.3 *Conflicts of Interest*

No supplier shall enter into a financial or any other relationship with a Britam employee that creates a conflict of interest for Britam. A conflict of interest arises when the material personal interests of the Britam employee are inconsistent with the responsibilities of his/her position with the company. All such conflicts must be disclosed and approval to the transaction given.

6.2.3 **Compliance and implementation**

6.2.3.1 *Licenses and Returns*

The Supplier will be required to obtain and renew, in accordance with any law or regulations all permits, licenses and authorizations required for it to carry out its business. In addition, the Supplier will be required to prepare and file any returns that it may be required to file under its incorporation statute, the Companies Act.

6.2.3.2 *Taxation, Financial Integrity and Retention of Records*

- The Supplier will comply with all revenue laws and will not evade tax.
- Suppliers will be required to maintain accurate and reliable financial and business records and shall not have any false or inaccurate accounting books or records related to Britam for any reason. Suppliers shall maintain all business records at the minimum in

compliance with the provisions outlined by the Kenya Revenue Authority or local revenue authorities from time to time.

- When any government investigation or audit is pending or ongoing then Suppliers will not destroy any relevant records until the matter has been investigated and closed.

6.2.4 Violations

If a Supplier becomes aware of any known or suspected improper behaviour by another Supplier in relation to their dealings with Britam or if a bribe or other inducement is requested from a Supplier by any Britam employee or any other person with the promise of influencing Britam's position as far as that Supplier is concerned or if the Supplier feels that a conflict of interests exists with one of Britam's employees then all pertinent details should be reported in confidence to the following Contact Address

Procurement procurement@britam.com

6.2.5 Variations

Britam reserves the right to vary this Code at any time.