COMMUNICATIONS AUTHORITY OF KENYA

Ref. No: CA/SCM/OT/15/2025-2026

April 7th, 2026, **Addendum No. 2**

To All Bidders,

OPEN NATIONAL TENDER FOR PROVISION OF CYBER THREAT HONEYNET AUTOMATED SYSTEM TENDER NO: CA/SCM/OT/15/2025-2026

Please refer to the above-mentioned tender.

Pursuant to ITT 9.1 of the tender document shared with bidders, the Authority wishes to respond to the clarifications sought out as follows:

NO.	CLARIFICATION QUESTIONS	CA RESPONSE
1.	The technical Capacity evaluation criteria require vendors/OEMs to provide copies of contracts or LPOs to demonstrate experience in cyber threat honeynet automated system. Given the sensitive nature of these implementations and the NDAs governing them, the vendor/OEM is unable to share such documents. Kindly confirm whether reference letters may be accepted as an alternative form of evidence.	Kindly note that reference letters will be accepted as an alternative form of evidence and **MUST** be of similar projects. The Authority reserves the right to carry out due diligence to confirm the authenticity of the documents provided.
2.	Kindly clarify the requirement for a KES 200 million bank Letter of Credit addressed to the Director General, Communications Authority of Kenya, for this tender. Given that the annual project cost may not justify this amount, could the requirement be reviewed or waived? Additionally, can alternative forms of financial capacity (e.g., cash reserves, distributor or manufacturer credit) be considered? Noting that credit lines are revolving facilities, would the Authority consider aligning this requirement with the actual annual project value?	The requirement remains unchanged as previously stated.
3.	Confirmation of technical compliance requirements	The technical compliance requirements as revised **REPLACES** the earlier issued in the tender document (*Detailed Revised Requirements are as detailed below after this table*).

NO.	CLARIFICATION QUESTIONS	CA RESPONSE
4.	We respectfully request a **seven (7) day extension** of the tender submission deadline to allow sufficient time for the preparation of a comprehensive and responsive proposal	The request to extend the tender submission deadline is granted. The new tender submission deadline is **April 15th, 2026, at 10:30 AM EAT.**

REVISION OF THE TECHNICAL COMPLIANCE EVALUATION CRITERIA FOR TENDER FOR PROVISION OF CYBER THREAT HONEY AUTOMATED SYSTEM (CTHAS)

The following requirements are mandatory. Bidders MUST respond to each requirement on the space provided with a "Complied" if their solution meets the requirement. Bidders should respond with a "Not Complied" if their solution does not meet the requirement or if they do not intend to comply with the requirement. A response of "Not Complied" to any of the requirements shall disqualify the bidder and the firm will not be evaluated further. Where there is no response to any one or more of the requirements, the bidder will be disqualified and shall not be evaluated further.

Bidders MUST also provide explanation of compliance with reference to the technical solution proposal writeup, Bill of Quantities, data sheets/brochures which must be attached and provided with specific page numbers. In case of inconsistency, the datasheet information would take precedence. This section will test the technical compliance of the proposed solution to meeting the Authority's requirements. The bidder must meet all requirements to be considered to the next stage of Technical Capacity Evaluation.

The Revised Technical Compliance Requirements are as detailed below:

No.	Technical Requirement	Complied / Not Complied	If complied, Bidders MUST provide explanation of compliance with reference to datasheet or bill of materials with the specific page number and section of the reference
A.	**GENERAL DECEPTION PLATFORM REQUIREMENTS**		
1.1	Turn-key Solution: The Service Provider/Vendor/OEM must provide all the required hardware, software, and system licenses.		
1.2	Deployment Scope: The solution must provide an external deception platform capable of covering at least 50 distinct remote entity sites.		
1.3	Platform Hosting: The centralized management, data lake, and decoy hosting must be deployed in a secure, scalable on-premise or local (Kenya) cloud environment.		
1.4	Support for MSSP-operated and managed deployment: The solution must allow an MSSP provider to operate and manage the deployment. Data would be within the MSSP's control and stored in a location determined by the MSSP.		

No.	Technical Requirement	Complied / Not Complied	If complied, Bidders MUST provide explanation of compliance with reference to datasheet or bill of materials with the specific page number and section of the reference
1.5	Scalability: The architecture must be capable of scaling to support at least 250 individual decoy web applications across the ecosystem.		
1.6	Non-Intrusive Design: The solution must not require disruptive changes to an entity's existing production network.		
1.7	Proprietary Technology: The honeypot/deception technology must be proprietary to the OEM/Vendor.		
1.8	No AD Dependency: The solution must not require privileged access to Active Directory.		
1.9	Rack Mountable: All physical equipment must be rack mountable.		
1.10	Vendor Reputation: The solution must have a Gartner Peer Insights Rating of not less than 4.5.		
B.	**DEPLOYMENT & REDIRECTION REQUIREMENTS**		
2.1	The solution must support configuration via an entity's existing on-premise proxy server to seamlessly redirect traffic to the deception platform to maintain separation of configuration.		
2.2	The solution must provide Virtual Machine-based sensors for deployment at the DMZ of at least 50 entities to act as an independent proxy/redirector.		
2.3	The Service Provider/OEM/Vendor must provide small form-factor physical hardware appliances to be installed at the DMZ for entities that cannot utilize a Virtual Machine (VM) or existing proxy setups.		
2.4	The solution must be capable of sitting behind standard Content Delivery Networks (CDNs) or Cloud Web Application Firewalls if required by an entity.		
2.5	Site Hardware: The Service Provider/OEM/Vendor must provide physical sensors for at least 50 monitored sites/locations.		
C.	**SENSOR SYSTEM REQUIREMENTS**		
3.1	Local sensors (VM or Hardware based) must communicate with the on-premise or local (Kenya) cloud platform via a unidirectional, outbound-only secure tunnel over the open internet.		

No.	Technical Requirement	Complied / Not Complied	If complied, Bidders MUST provide explanation of compliance with reference to datasheet or bill of materials with the specific page number and section of the reference
3.2	The DMZ sensors must strictly act as traffic redirectors and must not store sensitive threat telemetry or attack payloads locally.		
3.3	The master console must provide real-time health monitoring for at least 50 deployed remote sensors.		
3.4	The solution must support secure configuration updates and patching for the sensors.		
3.5	The solution must support time synchronization across the platform.		
D.	**DECOYS & DECEPTION REQUIREMENTS**		
4.1	The solution must support the deployment and management of at least five (5) distinct decoy web services per entity.		
4.2	The solution must support traffic redirection via standard DNS, allowing the participating entity to configure fake subdomain records on their existing DNS infrastructure.		
4.3	The Service Provider/Vendor/OEM must provide a framework to build custom decoy replicas mimicking specific, targeted web services without violating third-party trademarks.		
4.4	IT Decoy Support: The solution must support IT web decoys representing third-party applications including VPN admin, webmail, routers and gateways.		
4.5	Customization: The solution must allow uploading of custom HTML login pages on web server decoys/sensors and enable login credential capture.		
4.6	Templates: The solution must offer different types of decoys/sensors and provide ready templates to simplify deployment.		
4.7	OT Support: The solution must support Operational Technology (OT) web interface decoys.		
4.8	IoT Support: The solution must support Internet of Things (IoT) web interface decoys.		
4.9	Asset Protection: The solution must support protection of key web services using deception technology and advanced analytics.		
E.	**CYBER THREAT DETECTION & INTELLIGENCE REQUIREMENTS**		

No.	Technical Requirement	Complied / Not Complied	If complied, Bidders MUST provide explanation of compliance with reference to datasheet or bill of materials with the specific page number and section of the reference
5.1	Reconnaissance Detection: The solution must identify and log all types of reconnaissance activity, brute-forcing, and vulnerability probing.		
5.2	The solution must capture interactive attacks including credential stuffing and password brute-force attempts on decoy login portals.		
5.3	The solution must detect stolen credentials activities.		
5.4	Threat Summary: The solution must provide actionable intel including unique threats, attacker methods (CVEs), and OWASP Top 10 patterns.		
5.5	Integrated Web Application Firewall (WAF): The solution must utilize an integrated WAF at the cloud edge to capture and analyze malicious payloads.		
5.6	CTI Ingestion: The solution must natively support the ingestion of external third-party Cyber Threat Intelligence (CTI) feeds.		
5.7	IoC Extraction: The solution must automatically extract actionable Indicators of Compromise (IoCs) including IPs, user agents, and credentials.		
5.8	Containment: The solution must provide the ability to contain adversary blowback attempts without impact to a production network.		
F.	**DASHBOARD, ANALYTICS & MANAGEMENT REQUIREMENTS**		
6.1	Central Data Lake: The solution must aggregate all telemetry and logs from at least 50 distinct entity deployments into a single unified database.		
6.2	Unified Interface: The solution must provide central management of all system capabilities from a single web-based dashboard.		
6.3	Master Dashboard: The solution must provide a master unified dashboard allowing the Authority to view country-wide trends and analyze aggregate threat data.		
6.4	Sector Dashboard: The solution must provide a master unified dashboard allowing the Authority to view sector-wide trends and analyze aggregate threat data.		
6.5	Organizational Dashboard: The solution must provide a master unified dashboard allowing the Authority to		

No.	Technical Requirement	Complied / Not Complied	If complied, Bidders MUST provide explanation of compliance with reference to datasheet or bill of materials with the specific page number and section of the reference
	view organizational-level trends and analyze aggregate threat data.		
6.6	Logically Isolated Tenant Views: The solution must support Multi-Tenancy/isolated views so one entity cannot view another's data.		
6.7	Data Export/API: The solution must support exporting cyber threat intelligence via standard APIs (STIX/TAXII, Syslog) to SIEM tools.		
6.8	Real-time Alerting: The solution must provide real-time alerting mechanisms for high-severity interactions.		
6.9	Technical Reports: The solution must support automated deep-dive technical cyber threat and forensics reports.		
6.10	Executive Reports: The solution must support automated high-level cyber threat and forensics reports.		
6.11	Custom Reports: The solution must support the generation of custom cyber threat and forensics reports.		
G.	**PLATFORM ACCESS & SECURITY REQUIREMENTS**		
7.1	Role-Based Access Control (RBAC): The solution must support granular role-based access control.		
7.2	Single Sign-On (SSO): The solution must support Single Sign-On for administrative access.		
7.3	Encryption: All telemetry and attacker traffic must be encrypted in transit to the on-premise or local (Kenya) cloud platform.		
7.4	Low Resource Footprint: The deployed DMZ sensors must operate with minimal CPU and memory requirements.		
H.	**CUSTOMIZATION & PRODUCT DEVELOPMENT REQUIREMENTS**		
8.1	Open-Source Baselines: The solution must include a library of generic, open-source web application templates for rapid customization.		
8.2	Decoy Operational Security (OPSEC): Hosted decoys must share external characteristics (IP ranges, response times) with real websites to avoid fingerprinting.		

No.	Technical Requirement	Complied / Not Complied	If complied, Bidders MUST provide explanation of compliance with reference to datasheet or bill of materials with the specific page number and section of the reference
8.3	Product Roadmap: The Service Provider/Vendor/OEM must provide an active roadmap for deception, including new capabilities being added to the platform.		
I.	**IMPLEMENTATION, SUPPORT & TRAINING REQUIREMENTS**		
9.1	Phased Rollout Capability: The Service Provider/Vendor/OEM must support a flexible, phased implementation model during the onboarding of individual entities.		
9.2	Knowledge Transfer & Training: The Service Provider/Vendor/OEM must provide comprehensive training to the Authority's team on custom deployment, management, and analysis.		

ALL other terms and conditions of the tender remain unchanged.

This addendum forms part of the tender document and shall be read together with the original tender document.

Yours Faithfully,

Peter Mwangi
FOR: DIRECTOR GENERAL /CEO