COMMUNICATIONS AUTHORITY OF KENYA

Ref. No: CA/SCM/OT/01/2025-2026

March 13th, 2026 **Addendum No. 2**

To All Bidders,

OPEN NATIONAL TENDER FOR PROVISION OF A CYBER RANGES SIMULATION PLATFORM - CA/SCM/OT/01/2025-2026

Please refer to the above-mentioned tender.

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

No.	Clarification Sought		CA Response
1	**A. General Platform Requirements** The solution must be capable of integrating seamlessly with third- party systems and tools.	Which third-party systems, tools, or security platforms do you expect the simulation arena to integrate with?	These third-party systems, tools or security platforms may include the following: ▪ Security Information and Event Management (SIEM) systems ▪ Security Orchestration, Automation and Response (SOAR) platforms ▪ Threat Intelligence Platforms (TIP) ▪ Endpoint Detection and Response (EDR) systems ▪ Identity and Access Management (IAM) systems ▪ Directory services and authentication systems ▪ Vulnerability scanning and management tools, among others
	A. General Platform Requirements The system must support separate simulation environments for different users.	▪ Should these environments support individual learner isolation, team-based exercises, or both? ▪ Are these environments intended for different exercises/scenarios running	▪ The system should support both individual learner isolation and team-based exercises. ▪ The system should support both environments intended for different exercises/scenarios running

No.	Clarification Sought		CA Response
		concurrently, or just logical separation of data?	concurrently and should have logical separation of data.
2	**B. Industry-Level Requirements** The system should support IoT-related and emerging technology security concepts through simulated scenarios and datasets.	▪ Should IoT components be physically installed on-premise, or should they be simulated/virtualized within the cloud? ▪ If physical IoT is required, where should these devices be hosted? ▪ Should IoT devices communicate with the cloud platform as part of the simulation?	▪ IoT components should be simulated/ virtualized within the cloud environment. ▪ No physical devices are required. ▪ Yes.
	The system must include a management module that allows for the creation, configuration and control of separate simulation environments for each group or individual user.	▪ How many environments should be operable in parallel? ▪ Should administrators be able to manage environments per individual or per group?	▪ The system should support multiple parallel environments to allow simultaneous training sessions, exercises and scenarios for different users or teams. ▪ Both.
	B. Industry-Level Requirements The system must support the design and deployment of virtual infrastructures, systems and applications using both predefined and customizable templates.	▪ What types of templates are required (e.g., Windows servers, Linux servers, industrial networks, cloud-native apps)? ▪ Are there industry-specific environments we must include (e.g., finance, healthcare, ICS/SCADA)?	▪ The system should support commonly used cloud-based templates for multiple environments. ▪ The system must be capable of simulating most standard operating traffic types, including: - Enterprise application transactions (ERP, HR, Finance systems) - Database queries and updates - Industrial control signals (PLC to SCADA communication) - Point-of-Sale (POS) transaction data - Background system processes and updates

No.	Clarification Sought		CA Response
			- Authentication and access control logs - Backup and replication operations - Among others.
		▪ Should templates adhere to any specific standards (e.g., MITRE ATT&CK, NIST CSF)?	▪ The system should adhere to the MITRE ATTACK framework and others.
	B. Industry-Level Requirements The system must have the capability to create and manage diverse simulations to meet the varying requirements of different users.	▪ What categories of simulations are required (e.g., ransomware, fraud, network intrusion, IoT compromise)?	▪ The system should support multiple categories.
		▪ Should simulations be tailored to different difficulty levels, job roles, or organizational maturity levels?	▪ Yes.
		▪ Will different training courses need separate simulation logic or shared base environments?	▪ The different training courses should share a common base environment while using customized simulation logic or scenarios tailored to each specific training objective.
3	**II. Traffic and Attack Simulation** Video streaming	How should video streaming be incorporated into the simulation (e.g, bandwidth tests, detection of malicious streams, traffic pattern analysis)?	Video streaming should be incorporated into the simulation by generating realistic streaming traffic to test bandwidth performance, analyze traffic patterns and train participants to detect anomalies or malicious streaming activities within the network.
	II. Traffic and Attack Simulation Voice over IP (VoIP) calls	Should VoIP be fully simulated via traffic generators, or do you require functional VoIP services and call flows?	VoIP should be implemented using functional VoIP services and call flows, supplemented by traffic generators to simulate scalable voice traffic and attack scenarios.

No.	Clarification Sought		CA Response
	II. Traffic and Attack Simulation Peer-to-Peer (P2P) file sharing	Should P2P activity be simulated strictly through traffic generators, or do you require realistic P2P platforms to be deployed?	P2P activity should use realistic P2P platforms to emulate authentic network behavior, supplemented by traffic generators to simulate large-scale peer traffic and attack scenarios.
	II. Traffic and Attack Simulation Industrial control signals (PLC to SCADA communication)	▪ Do you require physical PLC units, or is virtual/soft-PLC simulation sufficient? ▪ If physical PLCs are required, where will they be hosted, and how should they connect to the simulation?	▪ Virtual or soft-PLC simulation is sufficient. ▪ We do not require physical PLC units.
	II. Traffic and Attack Simulation Point -of-Sale (POS) transaction	Is simulated POS traffic sufficient, or do you require a functional POS application within the environment?	Simulated POS traffic is sufficient. We do not require a functional POS application.
	II. Traffic and Attack Simulation Background system processes and updates	Should these be generated purely as simulated traffic, or should real background processes operate within virtual machines?	These should be generated as simulated traffic.
4.	**III. Program Content and Training Scripts** The system must be capable of providing a library of more than 500 ready-to-use simulation scenarios with varying degrees of difficulty on several topics, based on both simple and complex infrastructures.	How do you define a "scenario" (attack chain, traffic pattern, full environment, or training storyline)? ▪ Should scenarios follow standardized frameworks (MITRE ATT&CK, MITRE CALDERA, Metasploit modules)? ▪ Do you require all 500 scenarios at launch, or can they be delivered in phases?	▪ A scenario is complete training programme that integrates the simulated environment, traffic patterns and attack chain to achieve specific learning objectives. ▪ Yes, the system must have the capability to automatically simulate common attacks in line with the MITRE ATT&CK and others. ▪ The system must be capable of providing a library of at least 500 individual courses and labs or alternatively a minimum of 250 hours of course content with

No.	Clarification Sought		CA Response
			varying degrees of difficulty on several topics, based on both simple and complex infrastructures. It should not be delivered in phases.
	III. Program Content and Training Scripts The system must allow users to create their own training lessons based on personalized training routes by organizing content into defined categories.	▪ Does "user" refer to your administrators/instructors , or end-user trainees? ▪ Should lessons be created using drag-and-drop modules, scripts, or custom environment builds? ▪ Should training routes be linked to certifications or competencies?	▪ In the system, "user" can refer to both administrators/instructors who manage scenarios and environments and end-user trainees who participate in the training exercises. ▪ It should allow for both scenarios. ▪ Both.
5	**V. Simulation Exercises** The system must support the design, development, delivery and support of cyber exercises drawing participants from different organizations.	▪ How many exercises must be done simultaneously (e.g., two, three, or more)? ▪ Should the system support cross-organization participation, each with isolated access? ▪ Should monitors/instructors have an overview of all active exercises at once?	▪ The platform should support multiple exercises running simultaneously. ▪ Yes. ▪ Yes.
6.	▪ **Subscription Ownership**	Should the cloud resources for this engagement be deployed under: ▪ Your organization's subscription, or Our company's subscription, with appropriate access granted to your team?	▪ The service provider's subscription, with appropriate access granted to the Authority's team.

No.	Clarification Sought		CA Response
		▪ Who is covering the cost of the cloud subscription? The vendor or the customer?	▪ Vendor
7	▪ **Environmental Management Scope**	Should our team manage only the **cloud infrastructure**, or also the **arena/lab environment** within the cloud (including configuration, updates, user access, and support)?	They should manage both
8	▪ **Training Delivery Model**	How do you prefer users to access the training environment: ▪ **On-site/physically at your training centre,** ▪ **Fully remote access**, or ▪ **A hybrid model**? ▪ Do we need to train your team for RED and White team? Or we should provide it per training	▪ Fully remote access ▪ The initial training and knowledge transfer is for on-site or remote administrator and instructor training for a minimum of ten (10) staff covering platform administration, exercise management and reporting
9	**Deployment Architecture & Sovereign Control**	For governmental cyber ranges supporting red teaming, SOC training, and infrastructure simulation, international best practice typically favours deployment on dedicated on-premises infrastructure or within a sovereign/national cloud environment under direct governmental control. Could you please clarify the rationale for the intended hosting model for this project?	The system must be a cloud-based solution. This is the prefered deployment method.
10	**Data Sovereignty & Security Governance**	Cyber range platforms of this scope generate sensitive exercise data, attack logs, and infrastructure replicas. We would appreciate clarification regarding if the hosting is not	Under the Data Protection Act, 2019, any organisation that collects or processes personal data is required to ensure that such data is securely stored within Kenya.

No.	Clarification Sought		CA Response
		done under governmental control, then what are the ▪ Data residency requirements? ▪ Jurisdictional considerations?	Where personal data is stored or processed outside the country, the organisation must ensure that an accessible local copy of the data is maintained and that the transfer complies with applicable data protection safeguards and regulatory requirements. **The tender document also requirres that bidders posses the following:** A valid Data Controller Certificate of Registration from the Office of the Data Protection Commissioner. A valid Data Processor Certificate of Registration from the Office of the Data Protection Commissioner.
	Data Sovereignty & Security Governance	Security accreditation expectations for the hosting environment?	The bidder is required to have the following: A valid Certificate of Accreditation from the ICT Authority for Information Security (Minimum Category ICTA 1 Accreditation). A valid Certificate of Accreditation from the ICT Authority for ICT Consultancy (Minimum Category ICTA 1 Accreditation). A valid Certificate of Accreditation from the ICT Authority for ICT Networks (Minimum Category ICTA 1 Accreditation).
11	**Hosting Capacity**	A cloud-based platform supporting 500+ scenarios, IT/OT/IoT simulations, live attack capabilities, and 30+ concurrent users typically require substantial compute, storage, and orchestration resources. Could you advise whether: Infrastructure capacity has been pre-provisioned, or hosting is	The tender requirement is for a turn-key solution.

No.	Clarification Sought		CA Response
		expected to be fully bundled within the bidder's scope.	
12	**Revision of criteria for Program Content and Training Scripts (Page 74):**	**Current Specification:** The system must be capable of providing a library of more than 500 ready-to-use simulation scenarios with varying degrees of difficulty on a number of topics, based on both simple and complex infrastructures.	The criterion has been revised to read as follows: The system must be capable of providing a library of at least 500 individual courses and labs or alternatively a minimum of 250 hours of course content with varying degrees of difficulty on a number of topics, based on both simple and complex infrastructures.

ALL other conditions of the initial tender remain unchanged.

Yours Faithfully,

Philip Kiplagat
FOR: DIRECTOR GENERAL /CEO