TENDER CLARIFICATION ON XDR

S/NO	CLARIFICATION SOUGHT	RESPONSE
1	How much data do you plan on ingesting into the SIEM / XDR in GB/s per day? (If you don't have this pls provide EPS for rough extrapolation	Bidders are advised to refer to the **addendum issued on the official procurement website**, which provides clarification regarding the expected data ingestion capacity for the proposed solution. The SIEM/XDR solution should be sized to support approximately: • **3,500 events per second (EPS)**; or • **150 GB of log data per day**
2.	Should incident response retainer be included and if so for what duration?	The incident response referenced in this context forms part of the routine operational activities associated with the monitoring and management of the **Endpoint Detection and Response (EDR) platform**. These activities include continuous detection, investigation, analysis, and remediation of security threats identified within the environment. Accordingly, a **separate incident response retainer is not required** under this tender. The expectation is that the proposed solution will inherently support day-to-day incident detection and response capabilities as part of the standard operational functionality of the EDR/XDR platform.
3.	Breakdown of clients / servers/ Kubernetes (for on-prem and cloud)	The current environment consists of approximately fifteen thousand (15,000) endpoints. Bidders are expected to design solutions that support this baseline while also **allowing for scalability and future expansion** should the organization's infrastructure requirements increase over time.
4.	Cloud providers in use and number of	At present, the Procuring Entity does not operate workloads within any cloud environment.

	workloads per cloud provider	Nonetheless, bidders are encouraged to propose solutions that are capable of supporting hybrid or cloud-based deployments, should such environments be adopted in the future.
5.	Pls confirm if you require 2 years or 3 years	As clarified in the issued addendum, the licensing period for the solution has been revised from three (3) years to two (2) years. This revision has been made to align the procurement with existing solutions and services currently deployed within the organization.
6.	Will you consider both SIEM and XDR from the same solution (1 console fully integrated)	The Procuring Entity is unable to disclose additional architectural preferences at this stage due to **security and confidentiality considerations**. However, bidders are required to propose **flexible and interoperable solutions capable of operating effectively within diverse and heterogeneous ICT environments**.
7.	What is your current endpoint EDR/XDR solution stack?	Information regarding the current endpoint detection and response (EDR/XDR) solution stack cannot be disclosed at this stage due to confidentiality considerations. Bidders should therefore propose solutions that **support integration with a wide range of existing security platforms through standard integration mechanisms**.
8.	What is your current firewall stack	Details regarding the current firewall technology stack cannot be disclosed at this stage due to confidentiality considerations. Relevant technical information necessary for integration will be shared with the successful bidder during the implementation phase where required.

9.	What do you use for ADFS/SAML - AD, Entra, Okta etc	Due to security considerations, the Procuring Entity **cannot disclose the specific identity management infrastructure currently deployed**. However, the proposed solution must be capable of **integrating with commonly used identity and authentication platforms**, including but not limited to: • Active Directory (AD) • Microsoft Entra ID • Okta • Other SAML/ADFS-compatible identity providers
10.	What are the 3rd party data sources you would like to onboard into the SIEM and XDR	The proposed SIEM/XDR solution should support ingestion and correlation of security telemetry from various third-party systems including, but not limited to: • **Network infrastructure devices** (routers, switches, firewalls) • **Web proxy and secure web gateway solutions** • **Threat intelligence feeds** • **Endpoint security platforms**, including EDR/XDR tools The solution should therefore demonstrate **strong integration capabilities and interoperability with diverse security and infrastructure technologies**.

Amos Koech.

DEPUTY DIRECTOR/SCMS