CLARIFICATIONS FOR:

TENDER NO: SDICTDE/T002/2025-2026

SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING, AND SUPPORT OF EXTENDED DETECTION AND RESPONSE (XDR) SOFTWARE WITH EXPOSURE MANAGEMENT

S/No	MANDATORY REQUIREMENTS CLARIFICATION	REMARKS
1.	Page 31/124 19. Bidders **MUST** possess a valid **ISO 9001:2015** in **Quality Management** 20. Bidders **MUST** possess **ISO/IEC27001:2022 in Security Management System** **Can the bidder provide either of the two?**	**Response:** Bidders shall demonstrate possession of atleast one, or both of the following certifications issued by an accredited body: ISO 9001:2015 and ISO/IEC 27001:2022 issued by an accredited certification body. Copies of the valid certificate(s) must be submitted as part of the tender documentation.

CLARIFICATIONS FOR:

TENDER NO: SDICTDE/T003/2025-2026

SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING, AND SUPPORT OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION

S/No	TECHNICAL REQUIREMENTS CLARIFICATION	REMARKS
1.	The tender specifies licensing based on Events Per Second (EPS). Please confirm whether the Ministry would consider an alternative **ingestion-based licensing model measured in GB per day, as this is a more accurate and transparent reflection of actual data volumes.** An ingestion-based model eliminates the complexity of EPS burst calculations and provides more predictable cost management over the contract period.	**Response:** For purposes of this procurement, the licensing model shall remain **Events Per Second (EPS)** as specified in the tender document. The Ministry has provided indicative sizing in the addendum as follows: • **3500 Events Per Second (EPS)** • Approximately **150 GB of data ingestion per day** Bidders should therefore structure their proposals based on the **EPS licensing model** provided in the tender documentation.
2.	To assist with accurate sizing under either model, please confirm whether a formal log source assessment has been conducted across the Ministry's environment. If available, please **share an approximate breakdown of log volumes by source category (endpoints, network devices, cloud platforms, identity systems) either in EPS or GB per day**	**Response:** At this stage, bidders are advised to rely on the indicative ingestion capacity specified in the tender addendum, which provides an estimated requirement of: • 3,500 Events Per Second (EPS), or • Approximately 150 GB of log data per day. A detailed log source assessment and the corresponding categorization of log sources (including endpoints, network devices, cloud platforms, and identity systems) will be undertaken during the solution design and implementation phase with the successful bidder.

		Bidders are therefore expected to propose solutions that are scalable and capable of accommodating diverse log sources, while supporting the indicative ingestion volumes provided in the tender documentation
3.	Kindly confirm the **total number of log sources expected to be onboarded at go-live** versus those planned for onboarding during the contract period, as this will affect **both ingestion sizing and the number of connectors required.**	**Response:** At this stage, the Ministry has not defined a fixed number of log sources to be onboarded at go-live versus those that will be integrated during the contract period. Bidders are therefore advised to base their proposals on the indicative ingestion capacity specified in the tender documentation, namely 3,500 Events Per Second (EPS) or approximately 150 GB of log data per day. The detailed inventory and prioritization of log sources for onboarding will be finalized during the implementation and solution design phase in consultation with the successful bidder.
4.	Please confirm what behavior is expected when the licensed ingestion threshold is reached — **specifically whether events should be throttled, queued, or dropped** — and **whether real-time alerting is required when approaching the licensed limit.**	**Response:** The proposed solution should provide real-time monitoring and alerting when ingestion volumes approach the licensed threshold to enable timely administrative action. Where the licensed ingestion threshold is reached, the system should preferably queue events for processing rather than drop them, so as to preserve the integrity and completeness of security logs required for monitoring and investigation. Bidders should therefore indicate how their proposed solutions manage ingestion thresholds, including alerting, queuing, or other mechanisms to ensure continuous and reliable security monitoring.

5.	Kindly confirm whether the Ministry would consider **a flexible consumption model where ingestion capacity can be scaled up or down during the contract period based on actual usage, rather than a fixed EPS block structure.** This would provide greater flexibility as the Ministry's environment grows and new log sources are onboarded.	**Response:** For purposes of this procurement, bidders are required to structure their proposals based on the specified Events Per Second (EPS) licensing model outlined in the tender document and accompanying addendum. However, bidders may indicate scalability options within their proposed solutions to support future increases in ingestion capacity as the Ministry's environment grows and additional log sources are onboarded during the contract period.
6.	The tender references different retention periods across multiple sections — 180 days in Section 5.4, 3 months online and 11 months archive in Section 5.5, and 30 days standard in Section 5.13. Please provide a single definitive retention requirement, clearly distinguishing between hot/online retention and archive retention periods, as this directly affects storage sizing and cost.	**Response:** The definitive retention requirements shall be as follows: • **Online (Hot) Retention:** Minimum of **90 days** • **Archive Retention: 11 months** This provides a **total data retention period of 12 months**. Bidders should size their storage architecture accordingly.
7.	Kindly confirm whether bidders are expected to include all storage costs for both online and archive retention within the tender price, or whether the Ministry will provide storage infrastructure separately.	Response: Data retention within the platform shall be one (1) year. The Ministry of ICT and Digital Economy will provide its own external storage for any logs requiring retention beyond the one-year period. Accordingly, bidders are required to provision storage capacity to support the one-year on-platform retention requirement within their proposed solution.

CLARIFICATIONS FOR:

TENDER NO: SDICTDE/T001/2025-2026

SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, COMMISSIONING, AND SUPPORT OF SECURITY OPERATIONS CENTER (SOC) EQUIPMENT

S/No	TECHNICAL REQUIREMENTS CLARIFICATION	REMARKS
1.	**Pg 55, 62-63, 69, 87-88, 90** **NETWORK ACCESS CONTROL (NAC) APPLIANCE** Please advise on the purpose of NAC in a SOC since NAC appliance operates at the Network access layer (L2/L3) as preventive network control that enforces access (control plane) solution while the SOC operates at analytics layer (reactive and analytical function focused on detecting and responding to threats), creating a fundamental architectural difference.	**Response:** The inclusion of a Network Access Control (NAC) appliance within the SOC architecture is intended to provide a complementary preventive security control that enhances overall network visibility, access governance, and incident response capabilities. Although NAC operates at the network access layer (L2/L3) as a preventive control, and the SOC functions primarily at the monitoring, detection, and response layer, the two components are complementary rather than conflicting. In this regard, NAC is intended to: • Provide enhanced visibility of devices connecting to the network, including identity and compliance posture. • Enforce access control policies to prevent unauthorized or non-compliant devices from accessing network resources. • Integrate with SOC platforms (e.g., SIEM/XDR) to enrich security event correlation and analysis; • Support incident response through containment actions

		such as isolating compromised endpoints; and • Strengthen policy enforcement and provide audit trails for compliance and forensic investigations. **NAC is considered a foundational preventive control that complements the monitoring, detection, and response capabilities of the SOC, thereby enhancing the overall effectiveness of the security architecture.**

Amos Koech

DDSCMS