| **#** | **Question** | **Answer** |
| --- | --- | --- |
| 1 | Do you have a plan to integrate CTEM program with existing SIEM or SOC solutions to enhance threat detection, prioritization, and automated response workflows? If yes what kind of data or insights from CTEM will be ingested into the SIEM | Critical and high vulnerabilities alerts. |
| 2 | In RFP document Scope of work it is mentioned as "Service Provider must provide 24/7/365 support and monitoring of the CTEM" could you please clarify this section is it specific to CTEM platform availability and support? or a proactive approach of continuous monitoring of infrastructure, assets by resource. | This specific to CTEM platform availability and support. |
| 3 | What is the plan of action for migrating existing vulnerability, asset, and threat data into the CTEM solution any data need to be imported? | Assets configuration data will need to be imported into the new platform. |
| 4 | CTEM implementation and support will involve collaboration across security, IT operations, and risk management functions? | Yes. |
| 5 | Deployment of CTEM solution be in phases, or is a full-scale rollout planned, are there any specific timelines or milestones associated with implementation. | Deployment of CTEM solution be in phases e.g., first phase the IT servers and workstations, second, IT network security devices e.g., firewalls, etc |
| 6 | Please share the ticket dump or count of security incidents of last 1 year for Vulnerability management, OT, Cloud & IAM etc | We are unable to share such sensitive security artifacts at this stage. |
|  | **Please find below additional queries 3 and 4 with regards to the above-mentioned RFP.  We would also like to follow up with regards to the answers for questions 1 and 2 raised on Tuesday, 09 September 2025 16:56** |  |
| 7 | What is the old technology that Eskom requires migration and transitioning plans from? | Nessus |
| 8 | We seek clarification on the mandatory technical requirement in Annexure Q, Item #6, which calls for an "IEC 62443 compliance certificate in good standing from the OEM."  For our proposed solution, we can provide an official OEM letter confirming the technology’s deep alignment with and support for the IEC 62443 standard. Could Eskom please confirm if this official letter from the OEM will, on its own, be considered sufficient and acceptable proof to fulfill this mandatory "showstopper" requirement? | The OEM can provide a letter that confirm the “IEC 62443 compliance” of the proposed solution. |
| 9 | Please share the total count of servers hosted on cloud | The total count of servers hosted on the cloud as of 29 September 2025 is 23. However, this number will increase over time. |
| 10 | Please share the total count of OT sensors, PLCs, SCADA | The total count of OT assets is unknown at this stage. The asset count on the scope is for IT. However, the solution should be able to cater for OT assets. |