|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Reference Section** | **Reference** | **Question** | **Answer** |
| 1 | 3.1.1 Vulnerability Management | Perform vulnerability scans on Servers and Workstations’ Operating Systems, Applications, APIs, and Databases. | Please specify the frequency of vulnerability scans on network infrastructure (e.g. servers, workstations, network devices) and applications (web, mobile, API) on an annual basis? | Eskom requires scans to be conducted on monthly basis. Ad-hoc scans will be scheduled as and when required. |
| 2 | 3.1.2 Web App Scanning | a) Perform comprehensive static and dynamic application security testing (S/DAST). b) Conduct third-party component security testing (such as API, and open-source components) | Please clarify if the expectation on application security testing is to include both automated and manual assessment (i.e. detailed business logic and security tests on app functionality) ? | Yes, Eskom will require both Dynamic and Static analysis |
| 4 | 3.1.3 OT Security Exposure | a) Discover OT/IT assets. | How many OT plants/locations are to be covered? | Over forty (40) plants/locations however the number of assets is unknown at this stage |
| 5 | 3.5.1 Cyber Security Exposure | a) Seamlessly integration with the implemented security capabilities | What are the current security solutions in use for web app scanning, cloud scanning, end point security and network defenses ? E.g.- EDR, CNAPP,SAST? Are these solutions required to be integrated with the proposed CTEM solution? | Eskom has various security tools and the proposed solution is required to integrate with industry leading security tools |
| 6 | 3.5.1 Cyber Security Exposure | b) CTEM solution must support on-prem and cloud environments. | What are the cloud environments used? (E.g. - Azure, AWS) How many subscriptions/accounts to be covered as part of this scope? | Azure is the current cloud instance in use however Eskom has adopted a multi-cloud strategy with over forty (40) subscriptions |
|  | 3.1.5 Cloud Security Exposure | c) Automate remediation to address configuration flaws and security vulnerabilities. | Please elaborate on what remediations are to be automated? Are there any existing solutions to enable this? | Automated remediation will include but not limited to patching using tools such as Intune and SCCM |
| 7 | 3.1.4 Identity-Based Attack Detection | c) Detect IAM unauthorized changes and malicious activities. | Is this a periodic point in time check or continuous monitoring required? | The proposed solution should be capable of providing both point in time check or continuous monitoring |
| 8 | 3.4 VALIDATION PHASE | a) Verify whether the vulnerability can be exploited in practice (POC). | Is this validation on a requirement basis only or for all the observations from the CTEM solution? If it's only confined to specific requirement/cases, please suggest an approximate count of PoCs | The validation will be performed as and when required. Not all detected vulnerabilities will require validation |
| 9 | 3.6 REPORTING PHASE | 4. Landscape a) 44000 Workstations b) 8000 Servers | Provide an overview of the number of network devices and OT assets present in the environment that needs to be covered? | Number of network devices and OT assets are unknown at this stage |
| 10 | 3.6 REPORTING PHASE | c) Agree on the triggers that lead to remediation and the accompanying processes. | What is the current process to track vulnerabilities? Is there any ticketing solution such as ServiceNow used? | Eskom has a formal process for vulnerability management and BMC Helix is used as a ticketing/service desk solution. |
| 11 | Service Level Agreement Requirements | d) IT Security Services department requires MTTR (Mean time to resolve) of 4 hours. | What kind of issues should meet this SLA? | The SLA should meet the High, Critical, and zero-day vulnerabilities |
| 12 | Description of Request | In addition, the service must include professional services, software licenses, subscription services, maintenance, and ongoing support (24/7/365) throughout the term of the contract. | The proposal will include implementation, operationalization and support for 5 years. Please confirm | Yes, the proposal should include implementation, operationalization and support for 5 years |
| 13 | Description of Request | IT Security Services requires 24/7/365 (24\*7\*365) support throughout the year. | The support will be remote with ad-hoc onsite support at MWP as needed. Please confirm | Yes |