|  |  |  |
| --- | --- | --- |
| No. | Questions | Answers |
| 1 | How many assets and endpoints across various platforms should be monitored to ensure scalability? |  +50000 end-users +200 critical application  |
| 2 | Describe the current security systems and tools in place for better alignment? |  Tools can only be revealed to successful bidder  |
| 3 | Specify the existing tools that require integration, such as SIEM, EDR, and ITSM? Are there any proprietary systems or custom platforms in use that need special consideration? |  Follow the API model for integration |
| 4 | What types and formats of data (e.g., structured, unstructured, logs, metrics) will the solution need to handle? |  structured, unstructured, logs, metrics |
| 5 | Are there specific location preferences for data storage (e.g., on-premises, cloud-native, hybrid solutions)? Do you have existing infrastructure that the solution needs to integrate with? |  Hybrid This is managed services |
| 6 | Describe your current data center setup or cloud services? Are there specific APIs or interfaces for integrating with these data storage solutions? |  This is managed servicesThe solution must be able to integrate with other services |
| 7 | What are the existing processes and tools in place for incident detection and response? |  There is group-wide incident management process and systems |
| 8 | How do you currently gather and utilize threat intelligence? Are there particular threat intelligence feeds or sources that the scorecard should incorporate? |  SOC or SIEM |
| 9 | How is continuous monitoring currently performed, and what gaps or improvements have you identified that need addressing? |  SOC or SIEMTicket logging  |
| 10 | Are there automation or orchestration tools currently deployed in your operations? |  XSIAM |
| 11 | What methods and tools are currently used for asset discovery and inventory management in your organization? |  CMDB |
| 12 | How frequently is asset discovery conducted? |  As discovered  |
| 13 | Do you scanners that are continuously scanning various sources? Vulnerability Scanners?Threat intel applications? |  yes |
| 14 | Do you use any existing AI tools ? LLM? | Autonomous Threat detection software’s |
| 15 | Do you have any ITAM tool? |  No  |
| 16 | How are you currently managing and omonitoring your end points? Do you have an EDR system? |  SOCYes  |
| 17 | Are you using any tool for ITSM? |  To be revealed to successful bidder |
| 18 | What is SIEM tool you are using? |  Splunk |
| 19 | If you are open for SAAS solution?  |  Must be within SA borders |
| 20 | What is the user count who will be using the platform?  |  +200 |