|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** |  |  | **Question** | **Answer** |
| 1 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Can you list out the tools that would need to be integrated as part of the API Ecosystem | Revealing the tools would undermine Eskom security.  If the solution follow open architecture and having flexibility of microservices API model for supported and non-supported solution it should work within Eskom. |
| 2 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Do you already have a data lake that consolidates your data coming from different cybersecurity tools | We don’t have data lake.  Solution must cater for that. |
| 3 | Scope | 3.1 AI/ML-Driven Risk Intelligence | If yes, Can you specify what platform you are using as Data Lake? | None |
| 4 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Can you indicate what cloud infrastructure are you currently using? | Azure, AWS, Oracle, Google |
| 5 | Scope | 3.1 AI/ML-Driven Risk Intelligence | What types of cybersecurity risks or issues should the AI/ML system focus on? *e.g: Should it detect things like failed login attempts, unauthorized access to sensitive folders, or malware activity?* | All risks and activities |
| 6 | Scope | 3.1 AI/ML-Driven Risk Intelligence | What are the total set of data source and how we do the prioritiazation (*for each phase*)? | To be shared with nominated supplier |
| 7 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Does the AI/ML engine need to continuously learn and adapt over time using Eskom’s internal data, or is a one-time model training sufficient? | Both learn and adapt over time also allow model training |
| 8 | Scope | 3.1 AI/ML-Driven Risk Intelligence | What kind of detail is expected in the AI-generated risk cards and alerts? *e.g: Should it include severity level, affected system, root cause, and suggested actions?* | Decision making data |
| 9 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Are there any integration rules we should follow for APIs? *e.g: Should the API send and receive data in intervales, or support token-based authentication?* | API send and receive data in intervals |
| 10 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Should the AI-generated remediation advice follow any standard frameworks (e.g., NIST, MITRE ATT&CK)? | NIST Cybersecurity Framework (CSF) 2.0  MITRE ATT&CK framework |
| 11 | Scope | 3.1 AI/ML-Driven Risk Intelligence | What level of automation is expected for risk handling—just recommendations or full remediation workflows? | Full remediation workflow but with approval or rejection ability |
| 12 | Scope | 3.1 AI/ML-Driven Risk Intelligence | What are the primary data sources to be integrated (e.g., logs, assets, user activity)? | All data sources |
| 13 | Scope | 3.1 AI/ML-Driven Risk Intelligence | Should the AI/ML engine generate alerts based on fixed rules, machine learning, or both? *e,g: Should it follow set rules (e.g., more than 5 failed logins = alert) or improve based on past incidents?* | Both |
| 14 | Scope | 3.2. Real-Time Monitoring & Hygiene Management | Do you already have a tool for Continuous Asset Visibility? If yes, can you indicate which solution? | CMDB |
| 15 | Scope | 3.2. Real-Time Monitoring & Hygiene Management | What is the tool you are using for network monitoring? | Advanced threat detection solution  SIEM and SOC |
| 16 | Scope | 3.2. Real-Time Monitoring & Hygiene Management | What is the tool you are using for the mobile device security posture? | Intune |
| 17 | Scope | 3.2. Real-Time Monitoring & Hygiene Management | Are you having different tools for the monitoring of IT and OT systems and devices?If yes, can you list them? | Splunk |
| 18 | Scope | 3.2. Real-Time Monitoring & Hygiene Management | Are there any latency or performance benchmarks for “near real-time” monitoring? | Near real time means as it happens or few minutes of it happening without propagation. |
| 19 | Scope | 3.2. Real-Time Monitoring & Hygiene Management | Should the solution support monitoring for both IT and OT environments? | Yes |
| 20 | Scope | 3.3. Compliance & Reporting | Do you already have a tool for assessment as per the listed framework: NIST, ISO 27001, CIS, GDPR, PoPIA? | No |
| 21 | Scope | 3.3. Compliance & Reporting | If yes, can you specify the tool(s)you are using? | n/a |
| 22 | Scope | 3.3. Compliance & Reporting | What the IT other frameworks that need to be integrated as part of the reporting? | Nist  ISO27000 series |
| 23 | Scope | 3.3. Compliance & Reporting | What the OT other frameworks that need to be integrated as part of the reporting? | ISO 62443 |
| 24 | Scope | 3.3. Compliance & Reporting | Will Eskom provide existing mappings or should the solution generate them from scratch? | Both |
| 25 | Scope | 3.3. Compliance & Reporting | What level of automation is expected for audit-ready documentation? | It would be preferably that the system automate or make required data available |
| 26 | Scope | 3.3. Compliance & Reporting | Are there specific regulatory reporting formats or templates Eskom uses? | None |
| 27 | Scope | 3.4. Asset Discovery & Classification | Do you already have a set of tools for External/Internal Asset Inventory? | Refer to question 14 |
| 28 | Scope | 3.4. Asset Discovery & Classification | Do you have a tool for Dynamic classification and SSL evaluation? | Not available |
| 29 | Scope | 3.5. Threat Intelligence & Response | Will Eskom provide its own threat intelligence feeds, or should the solution include third-party sources? What are the different sources of feeds are you currenly using? | Both provided and eskom will share |
| 30 | Scope | 3.5. Threat Intelligence & Response | Should the system support integration with existing SOC or incident response platforms? | Yes |
| 31 | Scope | 3.5. Threat Intelligence & Response | Do you have any any tool in place to perform Simulated Attack Validation (e.g. phishing, ransomware simulations) to validate security controls and metric accuracy ? | No |
| 32 | Scope | 3.6. Remediation & Playbooks | Does Eskom already use any playbook automation tools (e.g., Power Platform, SOAR)? | XSIAM |
| 33 | Scope | 3.6. Remediation & Playbooks | Do you already have automated playbook in place? | XSIAM |
| 34 | Scope | 3.6. Remediation & Playbooks | What solution do you have for your ITSM? | No |
| 35 | Scope | 3.6. Remediation & Playbooks | What level of integration is expected with patch management and ticketing systems? | Fully integrated |
| 36 | Scope | General | Are you considering to have dedicated resources be part of the project to support on the deliverables? | This is a managed service |
| 37 | Scope | General | Who will be the main stakeholders from Eskom involved with the project team? | Group IT |
| 38 | Scope | 3.7.5 Dashboards | What are the different audience type for the dashboards? (e.g., executive, operational, compliance)? | Executive, Operational, Management, Compliance |
| 39 | Scope | 3.7.5 Dashboards | What level of customisation is expected for executive dashboards? | Must have drill down |
| 40 | Scope | 3.7.5 Dashboards | Will Eskom provide sample reporting formats or KPIs to be tracked? | Upon drafting of the SLA |
| 41 | Scope | 3.7.5 Dashboards | Do you require executive dashboards only? | Refer line 38 |
| 42 | Scope | General | Is the purpose of the platform to correlate data from different tools only for benchmarking, progress, tracking? | To also give decision making data and forums updates |
| 43 | Scope | General | Or do you require the platform to act a s a middleware to trigger assessment, scans, and other activities on the different tools? | Yes decision making support tool |
| 44 | Scope | User Management | Should the dashboard support segmentation by business unit, geography, or function? | Yes |
| 45 | Scope | User Management | what are the different departments that will need to have access to the platform | Eskom-wide |
| 46 | Scope | User Management | How would you considerate providing user access rights as per the different roles? | System must provision access |
| 47 | Scope | Integration | Will Eskom provide access to existing data sources and APIs during implementation? | Yes |
| 48 | Scope | 3.7.5 Dashboards | What level of customisation is expected for executive dashboards? | Refer line 39 |
| 49 | Scope | 3.7.5 Dashboards | Will Eskom provide sample reporting formats or KPIs to be tracked? | Refer line 40 |
| 50 | Scope | 3.5. Threat Intelligence & Response | What is the expected frequency and scope of simulated attack validations? | Refer line 31 |
| 51 | Scope | 5. Professional Service | Can Eskom confirm whether the two expert personnel must be onsite or remote? | Refer to scope document |
| 52 | Scope | 5. Professional Service | Is there flexibility in the capped hours or scope of work for the support resources? | As an when needed |
| 53 | Scope | 5. Professional Service | Scope of Enhancements: Could you clarify the types of enhancements expected during the four-year support period? Are these limited to configuration changes or do they include new feature development? | Feature improvement |
| 54 | Scope | 6. Training/Transfer of skills | Training Format Preference: Among onsite, classroom-based, and web-based training, is there a preferred delivery method or a blended approach? | Classroom based |
| 55 | Scope | General | Will Eskom provide guidelines for data residency and handover procedures? | Solution should be hosted within borders of SA and data escrow will be applicable |
| 56 | Scope | General | Are there specific encryption or data protection standards required for storage and transmission? | Data security is paramount |
| 57 | Scope | 3.7.5 Dashboards | Are there predefined KPIs or metrics for cybersecurity hygiene and compliance, or should we propose a baseline? | Propose based on system |
| 58 | Scope | 3.7.5 Dashboards | Will historical data be provided for trend analysis, or should the system build this over time? | System curated |
| 59 | Scope | Data Sources & APIs | Can you provide a comprehensive list of all existing security tools (e.g., SIEM, EDR, vulnerability scanners, firewalls, IAM, DLP, CASB) that the solution must integrate with? | To be shared with the successful supplier |
| 60 | Scope | Authentication & Access Control | What identity and access management (IAM) protocols are currently in place (e.g., SSO, LDAP, Azure AD)? Should the dashboard integrate with these for role-based access? | All protocols are available and should integrate |
| 61 | Scope | Data Residency & Storage | Is there an existing data lake or warehouse we should integrate with for aggregation and long-term storage? | Refer to same question answered above |
| 62 | Scope | 7.Service Level Agreement (SLA) Requirements | Will Eskom provide a monitoring tool or dashboard to track SLA compliance, or should the service provider propose one? | This is managed services |
| 63 | Scope | Hosting & Deployment | Will the solution be deployed on Eskom’s infrastructure (on-premises or Eskom Cloud)? | On-premises or Eskom cloud |
| 64 | Scope | Data Residency & Storage | Will Eskom provide access to a centralized data lake or should the solution include its own data aggregation layer? | Refer to same question answered above |
| 67 | Scope | Remote Access & Deployment Support | Will service provider personnel be granted remote access to Eskom servers or infrastructure for deployment, configuration, and troubleshooting activities? If so, what are the access protocols and security controls in place? | VPN |
| 68 | Scope | Platform Interoperability & Extensibility | Custom Connectors: Are there any legacy or proprietary systems that may require custom connectors? | Yes |
| 69 |  |  | Considering the complexity of the scope, we respectfully request for an extension of at least 2 weeks to consult with team members (subject matter experts) based across multiple time zones and refine our submission accordingly. | To be looked into |