	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

Description of Request	The provision of continuous threat exposure management (CTEM) professional managed services for a period of five (5) years.
------------------------	---

1. Background Information

The Information Technology Security Services (hereafter ITSS) provides Eskom with information security services such as information control assurance and information security strategy. Eskom requires a high degree of confidence that the implemented controls are operating as intended, such controls have effectively operated, and the threat exposure management must be performed on a regular basis.


2. Business Motivation & Benefits

Eskom requires five (5) years professional managed service for a cloud-based or Software as a Service (SaaS), artificial intelligence (AI)-powered continuous threat exposure management service. The CTEM solution must encompass the following but not limited:

- a) Vulnerability Management (All Platforms)
- b) Web application security assessment,
- c) OT security exposure
- d) Cyber security exposure
- e) Cloud security exposure
- f) Open-source intelligence scanning, and
- g) Identity and authentication security assessments.

The Service Provider must be a local company registered in South Africa and an official supplier of the OEM. The service must support Eskom's hybrid (both on-premises and multi-cloud) environments. 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 service must include the following features, functions, and capabilities, which are not exhaustive:

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

3. Scope of work/Business requirements

3.1 SCOPING PHASE

3.1.1 Vulnerability Management

- Perform vulnerability scans on Servers and Workstations' Operating Systems, Applications, APIs, and Databases.
- Conduct vulnerability scans on IT Infrastructure Devices (firewalls, routers, switches, etc)
- Assess adherence to best practise configuration standards (such as the CIS, NIST, ISO 27000 series, etc.)

3.1.2 Web App Scanning

- Perform comprehensive static and dynamic application security testing (S/DAST).
- Conduct third-party component security testing (such as API, and open-source components)
- Assess adherence to best practise configuration standards (OWASP Top 10, SANS Top 25, OSSTMM, etc.)

3.1.3 OT Security Exposure


- Discover OT/IT assets.
- Identify possible security risks to OT environment.
- Automate OT asset detection and provide a visual map of network assets (such as PLCs, and IoT devices).

3.1.4 Identity-Based Attack Detection

- Discover potential threats to Eskom's IAM (such as Active Directory and LDAP).
- Identify risky trust relationships.
- Detect IAM unauthorised changes and malicious activities.

3.1.5 Cloud Security Exposure

- Provide insight into how cloud resources are accessed.
- Detect misconfigurations and security vulnerabilities.
- Automate remediation to address configuration flaws and security vulnerabilities.

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

3.2 DISCOVERY PHASE

3.2.1 Open-Source Intelligence (OSINT)

- a) Detect Eskom internet-facing assets.
- b) Assess the Eskom's external attack surface.
- c) Execute security assessment of newly discovered internet-facing assets.

3.3 PRIORITIZATION PHASE

3.3.1 Prioritize Threats for Remediation

- a) Identify the high value assets.
- b) Assess the level of risk posed to the organization.
- c) Prioritize the threats most likely to be exploited.

3.4 VALIDATION PHASE

3.4.1 Validate Attack Vectors

- a) Verify whether the vulnerability can be exploited in practice (POC).
- b) Analyse and verify detected attack vectors.
- c) Agree on the triggers that lead to remediation and the accompanying processes.

3.5 MOBILIZATION PHASE


3.5.1 Cyber Security Exposure

- a) Seamlessly integration with the implemented security capabilities.
- b) CTEM solution must support on-prem and cloud environments.
- c) Provide an objective assessment of cyber risk throughout the enterprise.
- d) Track trend improvements over time.
- e) Benchmark against industry peers for gaps and strengths.

3.6 REPORTING PHASE

3.6.1 Clear Reporting

- a) The platform should provide customisable reports.
- b) The platform should provide different types of reports that include but not limited to technical reports, executive reports, and detailed remediation reports.
- c) Clear and concise reporting for management feedback
- d) Provide a comprehensive view of the entire attack surface.
- e) The platform should provide a comprehensive view of the entire attack surface.
- f) Provider a clear and user-friendly interface

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

- g) The platform should be scalable to meet future security requirements.

4. Landscape

- a) 44000 Workstations
- b) 8000 Servers

5. Safety

The third-party resources will provide the service remotely/online, with ad-hoc onsite support at MWP as needed.

6. Training/Transfer of Skills

- a) Provide web-based or online training for Eskom resources to enable them to perform the scan, interpret the results and remediate identified security vulnerabilities.
- b) Onboarding assistance of the IT Security test must be provided.
- c) Mentor, transfer skills and knowledge to Eskom resources assigned to the project through the installation, configuration, testing, and deployment stages using a defined skills transfer program.
- d) Expert level training with relevant certification.

7. Service Level Agreement Requirements

- a) The Service Provider must provide 24/7/365 (24*7*365) support and monitoring of the CTEM for the period of Five (5) years.
- b) IT Service provider must provide ad-hoc assessment.
- c) IT Security Services requires 24/7/365 (24*7*365) support throughout the year.
- d) IT Security Services department requires MTTR (Mean time to resolve) of 4 hours.
- e) The availability of the system must 95,9%.

8. Cross function team members (CFT)

Name	Surname	Designation	Role
Neo	Lemao	Senior Advisor: IT Security	Technical Evaluator
Grant	Domingo	Officer Security: IT Security	Technical Evaluator
Ronald	Netshishivhe	Chief Advisor: IT Security	Technical Evaluator
Skhumbuzo	Gama	Middle Manager Cyber Security	Reviewer

	TENDER SCOPE OF WORK Group Information Technology	Template Identifier	240-IT042	Rev	1
		Effective Date	April 2023		
		Review Date	April 2028		

9. Approvals:

End user / requestor:	Name:	Ronald Netshishivhe
	Designation:	Chief Advisor: IT Security
	Date:	06 / 06 / 2025
	Signature:	
Middle Manager:	Name:	Skhumbuzo Gama
	Designation:	Middle Manager Cyber Security
	Date:	06/06/2025
	Signature:	
Senior Manager:	Name:	Sithembile Songo
	Designation:	Senior Manager: IT Security
	Date:	11-06-2025
	Signature:	