TERMS OF REFERENCE

THREAT SUIVEILLANCE SOLUTION

1. Background

1.1 The Quality Council for Trades and Occupations (QCTO) is a Quality Council established in 2010 in terms of the Skills Development Act Nr. 97 of 1998. Its role is to oversee the design, implementation, assessment and certification of occupational qualifications, including trades, on the Occupational Qualifications Sub-Framework (OQSF).

1.2 The QCTO also offers guidance to skills development providers who must be accredited by the QCTO to offer occupational qualifications.

Visit: https://www.qcto.org.za for more information

2. Project objective

2.1 QCTO is seeking proposals from qualified service providers to deploy a Threat surveillance solution that will automatically and continuously monitor the QCTO ICT Infrastructure to stop anomalies, malicious traffic, vulnerabilities and other advanced human-led attacks in real time.

2.2 Skills transfer to selected QCTO ICT staff and provide support for 12 months.

3. Current ICT landscape

3.1 The QCTO has one site situated in Hatfield, Pretoria. The current ICT infrastructure and system supports about 130 staff across the different departments. The security systems in place include Sophos Endpoint Protection, NEXT DLP, RAPID7 SIEM Solution and a FortiGate Firewall. The QCTO is using Microsoft Configuration Manager for patching its different endpoints.

4. Scope of services:

a) 24/7 Threat Detection, response and remediation.
b) Expert-Led Threat Hunting.
c) Breach Protection.
d) Instant Security Operations Center (SOC).
e) Full-Scale Incident Response Capabilities.
f) Threat Containment actions interrupt the threat and preventing it from spreading to other systems.
g) Customize the Level of Service to Your Specific Needs
h) Provide root cause analysis report.
i) Monthly Reporting for real-time alerts, total detections, protection rating, detection classification summary etc.
j) Systems Integrations i.e (Microsoft security tools, Endpoint protection, Microsoft Audit Logs, Firewall, Email security systems, Network etc)

5. Appointment criteria

In order to be considered for evaluation the bidder should have the below:

a) At least 3 completed similar solutions as a company directly or as sub-contractors within the last 3 years – shown by written/email references.

b) Detailed on boarding plan and project team.
c) At least one CEH, or OSCP certified team member
d) At least one CISSP, CPTE and GPEN or ISO 27001 certification

Technical queries via email to: Mr Tshifaro Hangwelani on Tshifaro.H@qcto.org.za

For SCM related queries via email to: Mr Lekhotla Motloung on Tenders@qcto.org.za.

5. Submission

a) Technical proposal with supporting documents and financial proposal must be sent to Tenders@qcto.org.za. **Please quote the correct RFQ number (RFQ 20) when sending your proposal.**