TERMS OF REFERENCE FOR THE APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY AND CONFIGURE A SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) TOOL.

1. INTRODUCTION.

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

1.2 For more information about QCTO visit: https://www.qcto.org.za.

2. PURPOSE.

2.1 The purpose of this RFQ is to appoint a suitable service provider to supply, provision, configure, and support a Security Information and Event Management (SIEM) solution for the Quality Council for Trades and Occupations (QCTO).

2.2 The SIEM solution must integrate with QCTO's existing security technologies, including the Forti DLP data loss prevention and data discovery solution.

2.3 The SIEM solution must include software licensing, support, and maintenance for a period of twenty-four (24) months.

2.4 The SIEM platform must be licensed directly to QCTO as the primary account holder with the original equipment manufacturer (OEM). The appointed service provider shall not retain ownership, primary control, or exclusive rights over the SIEM tenant, subscription, or licences.

2.5 The appointed service provider shall operate only as a delegated administrator or managed services partner and must not introduce any dependency that restricts QCTO from independently renewing, changing, or terminating the service provider

3. QCTO'S CURRENT ICT LANDSCAPE.

3.1 The QCTO has one site situated in Hatfield, Pretoria. The current ICT infrastructure and system supports about 150 staff across the different departments.

3.2 The QCTO currently utilises a Security Information and Event Management (SIEM) solution, Seceon

3.3 The QCTO ICT unit provides various ICT services on different infrastructure platforms and systems products.

3.4 The QCTO has a local network of about 150 end user workstations, Four (4) HP physical servers that are hosting fifteen (17) virtual machines running Windows operating systems and four (4) Cisco switches.

3.5 QCTO has amongst other systems implemented the following which should form part of the integration with the proposed system:

a) Active directory.
b) Sophos Intercept X endpoint protection for all its endpoints.
c) Microsoft Office 365 Exchange Online.
d) Fortinet hosted Firewall.
e) MicroFocus Content Manager.
f) Cisco switches.
g) SQL databases.
h) FortiDLP
i) Forcepoint Data Classification

4. SCOPE OF WORK AND DELIVERABLES FOR THE SIEM SOLUTION.

4.1 The SIEM solution must provide the following capabilities:

a) Focuses on combining event data from different sources to assist with the identification of any suspicious activity and policy violations for the QCTO ICT environment.
b) Performs real-time monitoring (24 X 7 X 365) of event data generated by workstations, network devices, security appliances, servers, databases and applications providing the ability to consolidate monitored data to help avoid missing crucial events.
c) Contains a correlation engine to identify and detect patterns across the ICT environment with basic predefined correlation rules available at set-up to start analysing and correlating activity out-of-the-box that reduces false-positives automatically, detects authentication failures and operational events in real time without the need to specify device types.
d) Perform behaviour profiling to identify anomalies and deviations from normal behavior.
e) Identify the actual user of the source or destination, preferably through an

Active Directory (AD) connection.

f) Include or add any application with logging capability that may not already be available, and also provide a native out-of-the-box capability to collect application log data from custom/in-house developed web applications.

g) Includes a module that can be used to provide compliance auditing, alerting and reporting for governance.

h) Integrate with existing authentication directories to import context related to users and roles, which will then correlate and attribute every event to an actual user, regardless of the event source and be able to alert or report on any activity for identities not automatically synchronised with authentication directories.

i) Take event data and turn it into informational charts to assist in seeing patterns or identifying activity that is not forming a standard pattern.

j) Long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements.

k) Is capable of discovering patterns of subverted activities that would otherwise go unnoticed, i.e. slow and low attacks.

l) Is capable of triggering scripts or execute integration commands with third-party solutions, Next Generation Intrusion Prevention systems in order to quarantine or block malicious activity in real-time.

m) Is capable of monitoring several databases in different servers and generates daily, weekly reports alerting of activities taking places within SQL and oracle database environments to mitigate against malicious acts such as SQL injection attacks and unauthorized activities by administrators.

n) Provide support for Cyber security incident response in cases of major cyber security incidents. The support hours to be used over the duration of the contract.

o) Be able to produce alerts for the following incidents:

active Directory group policy violation change. Suspicious traffic to malicious sites.

4.2 The appointed service provider shall propose an architecture and deployment options for its selected SIEM solution including licensing model, product support, performance estimation, scalability, and High Availability/Disaster Recovery (HA/DR) options.

4.3 The SIEM solution should be compatible to integrate with the Forti DLP Solution which has been rolled out and should not clash with current systems

within the organisation's Landscape (Sophos, FortiGate Firewall, Cisco, MS365).

5. VENDOR PARTNERSHIP/ CERTIFICATION

5.1 Interested service providers are required to have a suitable Partner status with their chosen product vendor at the time of responding to this RFQ and throughout the duration of the contract.

5.2 At least one member of the service provider's key personnel assigned to the project shall hold a valid certificate of the product vendor at any time during their assignment to the project and have a minimum of three (3) years of professional experience in SIEM implementations.

6. MAINTENANCE AND SUPPORT

6.1 The QCTO intends to enter into a one (2) year support and maintenance contract after the implementation stage.

6.2 The successful bidder will be required to support the ICT unit in deciphering and interpreting the logs generated by the SIEM.

6.3 The successful bidder will be required to provide monthly logs for audit purposes for the duration of the contract.

7. AUDIT AND REPORTING

7.1 The successful bidder will be required to generate and provide monthly audit logs/ reports from the SIEM.

8. PROJECT TIMELINE

8.1 The successful bidder must be able to supply, configure and install the required security systems within 7 days from the date of receiving a purchase order.

***.**

9. EVALUATION CRITERIA

No.	Evaluation Criteria	Guideline	Scoring	Points
1	Consultant/organisation experience related to provision of SIEM solution referral letters must be on company letterhead, dated and signed by the company representative	Bidder's extensive knowledge and experience in proposed SIEM tool implementation and roll out. Reference Letters for SIEM implementation with the name of the SIEM rolled out. ***NB: Please provide signed and dated reference letters from the company they provided SIEM for, in that company's letter head with contact person and their contact numbers.***	No evidence that bidder has undertaken SIEM implementation projects (0 reference letter) = **0 points** • Bidder has successfully undertaken 1 to 2 SIEM Implementation projects (1-2 reference letters) = **10 Points.** • Bidder has successfully undertaken 3 or more SIEM Implementation projects (3 reference letters) = **20 points**	**20**

2	Project plan with Technical Support Resource: Bidder's personnel/resource must have 1 or more Information Security Certification. NB: such as CISM, CEH, CISSP etc. (Profile of Certified member with relevant certified qualifications must be supplied). ***Capable of supporting the environment, technical abilities to solve technical issues, provide solutions for escalations***	Project Plan: Proposal clearly states who on the bidder's team will support the environment. Bidders team technical personnel **signed cv and certified Information Security qualifications**; (Detailed Project plan with activities of the project must be provided) with Information security qualification and experience of consultants/team members and roles, responsibilities of technical resource outlined.	• No project plan, no technical support resource cv submitted = **0 Points** • The project plan was submitted but does not clearly demonstrate knowledge of what needs to be done. without cv of technical support resource = **15 Points** • Detailed project plan with clearly demonstrate knowledge of what needs to be done with CV of Technical Support Resource and qualifications of support personnel • = **25 Points**	**25**
3	Partner Certification.	Bidder Partner Certification/Training with Vendor ***NB: Please provide valid certification***	Bidder has NO valid Vendor SIEM certificate = **0 Points.** Bidder has valid SIEM Vendor Certificate = **20 Points.**	**20**

4	SIEM Tool Sample Monthly Reports.	Sample Monthly report from existing SIEM implementation to show event types and categories the SIEM Captures. Sample Monthly report from existing SIEM implementation.	• Bidders provided no sample report. =**0 Points** • Bidders provided sample reports from active environment, but don't show proper understanding of work(duties) to be carried out. =**10 Points** • Bidders provided monthly sample reports from active environment, that shows the different events the SIEM captures to be carried out. =**20 Points**	**20**
5	Chosen SIEM ability to Integrate with **Forti DLP.**	Provide proof (screenshots) that the chosen SIEM has the capability of Integrating with NEXT DLP. ***Chosen SIEM has a compatible API to facilitate integration with the existing Forti DLP***	• Bidder provided No proof nor addressed that SIEM can Integrate with Nex DLP= **0 Points** • Bidder provided some proof that SIEM can Integrate with Next DLP but not in the form of API as advised. = **10 Points** • Bidder provided proof that SIEM can Integrate with Forti DLP in a form of API = **15 Points**	**15**
Total Points				**100**

10. INQUIRIES

10.1 For further information, don't hesitate to get in touch with the following QCTO staff members:

Technical inquiries can be directed to:

Mr H Tshfaro
Tel no: 012 003 1829
Email: Tshifaro.h@qcto.org.za

Ms. Nkhensani Maluleke
Tel no: 012 003 1856
Email: Maluleke.n@qcto.org.za

SCM Inquiries can be directed to: RFQ@qcto.org.za