Tender No: 1i-21708 - Appointment of a service provider for the provision of a managed Security Operations Centre, for a period of 36 months

#	Clarification provided /Queries received	Responses from eThekwini Municipality
1	Submission of tenders	Sealed Tenders should be addressed to the City Manager and marked with the Tender Number and be placed in the Tender Box located in the ground floor foyer of the Municipal Building, 166 KE Masinga Road (Old Fort Rd), Durban (and not any other municipal department), no later than: 27 January 2023, 11:00am. Electronic submission not accepted.
2	Mandatory requirements clarification	If the bidder does not provide any of the required supporting documents required in the Mandatory requirements such as the two relevant reference letters for rendering the same services, valid ISO 27001, ISO 9001 certificates, Comprehensive CVs and qualifications/certificates for the 3 resources, and a detailed proposal that addresses all the key requirements in section 7B, that will disqualify the bidder from further evaluations.
3	Proposal must respond to all requirements	The proposal must address or respond to all key requirements on the specification in section 7B in detail/clearly note how that requirement will be addressed, and not omit responding to any of the requirements noted under that section.
4	Complete the tender form in full and attach all relevant supporting documents	Failure to fully complete the tender documents and complete the mandatory information and sign the Official tender form will invalidate the tender, so Bidders are required to ensure that they complete all the information and sign all the areas that require signatures.
5	Agentless collection only, what about agent based?	Preferable agentless and appliance-based collectors are required, instead of requiring installation of agents on all 540 servers and other network devices, agents can be allowed only on a few servers where such is deemed necessary, but mostly all collections must be from the central log collector server/appliance. Also, if the bidder requires that the Municipality provision one or two servers to act as collection agents/proxy they need to state such upfront (provide hardware specification for the require server), as the Municipality does not have capacity to provision high end servers, hence preferring the Bidders to provide the Municipality with collector appliances for the proposed solution.
6	Are honeypot devices in scope, and how many honeypots are required, how many network segments and sites and do the sites have more than one DMZ, which network segments has more users per site	Yes, At a minimum two honeypots are required, two in the DMZ (public facing webservers) and two on the internal server farm for the main data centre(s). We have one DMZ. In terms of network segments, we have a lot of sites, with a number of big sites or buildings all across Durban central (with over 400 users in each building), and other smaller sites all across Durban (with users ranging from 10 – 300), all the sites connects back to the central routing for the Internet, networks are segmented into different VLANs.
7	Which equivalent certificates would be acceptable for the cybersecurity resources required, are vendor specific certificates acceptable for the Analysts and CISSP for Specialists, and also if having specialists with	For the SOC Analysts, relevant vendor specific certificates can be provided if those show that the analysts are skilled in cybersecurity analysis utilising that proposed security tool/SIEM, and those skills enables the analysts to understand security monitoring, threats and network security fundamentals, threat hunting and how to investigate and respond to cyber-attacks/incidents, and the relevant principles for cyber risks management, compliance and threat intelligence and attack techniques/frameworks. Certificates should be relevant to validate the core skills for the resources to demonstrate that they can

	highest certificates such as Ethical hacking/Offensive pen testing can those be submitted for the analysts?	effectively fulfil that role, entry-level cybersecurity certificates (no attendance certificates) and also the CV's must detail the duties that the resources has been doing (not just state the role only). Having advanced cybersecurity certificates by the analysts is most welcome also. Specify the resources accordingly on the tender response, for ease of noting which resource the CV and qualifications address. For the cybersecurity specialist, relevant advanced professional certificates that require passing exams, and meeting certain prerequisite such as taking relevant training course/practical's and having relevant minimum experience in cybersecurity/information security before the certificate is awarded would be acceptable. The specialist CV must also detail the experience outlining that resource is highly technically experienced in dealing with cybers threats, incident investigation and response, threat hunting, data analysis, vulnerability management, reverse engineering, exploitation of systems, penetration testing, utilisation of attack techniques and reporting and skills for combating cyber-attacks, identifying Indicators of compromise, defending networks from threats, digital forensic, counterintelligence, and other relevant advanced skills etc.
8	Can the Municipality provide the SIEM sizing quantities in the format required by different bidders and with more details on the Vendor Versions utilised for all applications, Operating Systems, and network devices, databases, vulnerability scanner.	For uniformity and to avoid giving too much information around our IT environment, we've highlighted what we believe is relevant and have grouped those accordingly, on the tender document page 40 section 7 B (3) -List of devices/servers (to be covered), all bidders requested to utilise that information, as it does cover all critical devices and provides high level information on platforms utilised (our environment is running mostly on different Microsoft Windows, with a few Linux and Unix servers, as noted on the Tender document). Vulnerability scanner –the Bidders response or proposal must provide a built-in vulnerability scanning/reporting tool for continuous assessments of the critical infrastructure in scope, as part of the SIEM Solution dashboard, or propose a solution that will be implemented to run those and feed into the central SIEM dashboard.
9	Retention of information for 24 months, is that a must have	That is a key requirement, and Bidders must respond accordingly to that and specify where the information will be stored on the cloud environment as part of the solutions proposed for how long, and if proposing on-premise (the bidder must provide the relevant hardware costs as part of the response to implement those servers/appliances on premise to collect, store and process logs).
10	Is the Security Operation Centre/SIEM tool required to pull logs from all servers, endpoints and network devices and respond to threat across all devices connected on the network	The way the Tender is structured the focus for now is on the critical 4 data centres with 540 servers and network infrastructure (Firewalls, routers, gateways and core switches and some critical distributions etc) for the next gen- SIEM, analytics, vulnerability assessments, SOAR, Forensic, compliance reports, honeypots etc, then for the user behavioural analysis, threat intelligence, dark web monitoring for the Durban domains and public IP etc, network connected devices and Microsoft office 365 that will be for all 11100 users on the network plus the servers noted on the list of devices. For the endpoints/workstations the SIEM will rely on the intel pulled from the 5 Management servers (Endpoint protection suite) to pull that into the central reporting and analyse, and where certain computers on the network do not have security agents and causing problems the SIEM tool must pick that up from the core network monitoring and servers and the team should escalate such to Desktop Support to address those. As a note:

		currently utilising the Deep Security on some servers and Apex on some servers, and for all workstations (on-prem), licensed for the XDR with Trend and will be implementing that shortly (cloud).
11	Does the Municipality require dedicated resources, instead of the service provider utilising their current shared resource/staff complement.	As the Municipality will be billed for the resources to be provided as part of the bid response, those resources are expected to be fully focused on monitoring and responding to eThekwini cybersecurity issues and mitigations on a 24X7 basis, how the service provider manages/allocates such is up to them, but the Municipality cannot accept poor services/performance due to shared resource pools being busy with other cybersecurity work/incidents. For the Cybersecurity specialist that resource will be required at any time to do a lot of cybersecurity incidents identification, investigations, response, and proactive threat hunting, looking for IOC, testing security controls and to advise on security gaps and improvements necessary to improve the cybersecurity posture of the Municipality, and can be called to work on-site (Durban Municipality) at any time as the Municipality deems fit for such, hence the local presence is a requirement in ACC6. That resource will be required to report daily or weekly on the security posture for the Municipality, and also assist the relevant Municipality Administrators/Security Teams to address any weaknesses identified.
12	As the tender document that was published has a date that has passed, do bidder utilise that for submissions	Yes, utilise that original tender advert and attach the copy of the First notice that shows that the closing date for that tender was extended.
13	Some Companies are not comfortable with providing written reference letters for Cybersecurity services?	Unfortunately, the Municipality requires written reference letters stating that the Bidder has rendered the required services for other companies, in order to proceed further with evaluations, as that is a mandatory requirement. The Municipality will email annexure A1 to referees email addresses provided on the letters provided with the tender response to verify that the said services have been rendered and will require the referees to fill that form and send back to the Municipality within 10 working days in order to evaluate the responses to the questions on that form. Where certain Companies cannot provide reference letters, the Bidders need to find other companies that can provide such or engage those companies and assure them that the reference letters will only be used for evaluation purposes and the Municipality Team will not share such information with anyone else, besides utilising that for checking the Bidders claimed experience in rendered successfully those services required. Telephonic confirmations cannot be accepted, as we would not have a hard copy record of confirming the Bidders experience. Bidders can advise their referees to please respond to that on time, when the Municipality does reach out for verification, if no responses are received that will disadvantage the bidders.
14	SCC 22.1 how will the penalty percentage work, i.e., for critical 3% of what (for not responding to security alerts/incidents detected within the required response time)?	% of the monthly cost X no of hours beyond required response times will be levied (as a penalty), that will be subject to the General Conditions of Contract clause 22 and 23.

General/Contractual: Siphesihle Makhanya; Tel: 031 322 7189; e-Mail: siphesihle.makhanya@durban.gov.za