



BID DESCRIPTCION: APPOINTMENT OF A SUITABLY QUALIFIED BIDDER FOR THE PROVISION OF SPECIALISED SERVICES FOR THREAT DETECTION AND RESPONSE SYSTEM (TDRS) AS A MANAGED SERVICE FOR THE SOUTH AFRICAN NATIONAL ACCREDITATION SYSTEM (SANAS) TO MONITOR THE ENTERPRISE'S SECURITY POSTURE, ADDRESS REGULATORY COMPLIANCE REQUIREMENTS, TO COLLECT, STORE, AND SEARCH THROUGH (ANALYSE) LOGS TO DETECT AND RESPOND TO ANY CYBER-ATTACK FOR A PERIOD OF THREE (03) YEARS.

BID NO: SANAS/THREAT-DETEC/2023-24/11

BRIEFING SESSION HELD ON: 21 FEBRUARY 2024 @11:00

Questions raised by the bidders:	Verdict:
<p>Please confirm the device count for scoping/ how many servers do you have?</p>	<p>We have 30 virtual servers and 2 host servers.</p>
<p>Please advise based on the below I can't find any reference on Google to an Intel Xeon i10 processor. Please confirm how many cores and threads are needed on the CPU.</p> <p>A HPE or Equivalent Gen 10 Host server (Hardware & Software)</p> <ul style="list-style-type: none"> • Minimum Processor Family- Intel® Xeon® i10 • Minimum RAM - 64 GB • Minimum Storage Capacity - 4000 GB (4TB) <p>Preferably SDD & 500GB for OS</p> <ul style="list-style-type: none"> • Preferable Tower / Micro Tower • 1 Year Microsoft Standalone Server License 2022 • 3 Years Onsite support / Warranty 	<p>Kindly find the equivalent if you can't find the exact specification, see above “A HPE or Equivalent Gen 10 Host server (Hardware & Software) “</p>

<p>What is the name of the encryption software tool mentioned in the bid document?</p>	<p>We mentioned Sophos Anti-virus and Encryption, its Sophos DES.</p>
<p>For an on-premises implementation. Would a solution hosted in South Africa be acceptable as deploying a complete server for 3 physical and 30 virtual servers with 80 users would increase expense.</p>	<p>That's the reason we need an on-premises, as mentioned at the briefing, we want to evaluate solutions offered on same level, so on-premise is our preferred proposal.</p>
<p>What other devices do they have that will need to ingest logs from (i.e. firewalls, core switches, WAF, Microsoft365 etc.)</p>	<p>2 x Sophos Firewall, Wi-Fi system, 10 x Aruba Switches, Aruba ClearPass NAC Server, 30 MS Servers, 80 Endpoints and 120 various devices.</p>
<p>By 24x7 managed service do they mean full SOC services or just management of the solution</p>	<p>Yes, depends on your model offering, we are looking some SOC of some kind, but looking after the managed TDRS solution and its events, reporting to ITSO monthly basis.</p>
<p>How long do they need to store logs for?</p>	<p>We required to keep data a minimum of 5 years, however, because of the cost of storing data this solution must be practical, a minimum of 1 year will be adequate for SANAS.</p>
<p>As SANAS requires a Managed Services, will you accept a SaaS Managed Services Solution offering</p>	<p>We are looking for a "on-premises" solution hence the mention of a host server.</p>