Reference Number: SADC/IARM/10/2020

Title: SUPPLY OF VULNERABILITY SCANNING SOFTWARE LICENCES

Number of Lots: **1**

1. **SADC Secretariat** is inviting product partners and authorised resellers only to submit a bids for the Supply of the following items

Lot	Item	Qty
1	Vulnerability Scanning Software (Annual Licenses or Cover up to 10 scans of hosts as outlined in specification)	1

2. You should send only **one bid** for this requirement.

IMPORTANT : INCLUDE RELEVANT DOCUMENTATION BELOW:

1. **The Certificate of Incorporation**
2. **The Trading License**
3. **Valid Tax Clearance Certificate**
4. **The PPADB Certificate or equivalent**
5. **Banking details**
6. **Company Profile**

3. Your **bid** should be titled as shown below and addressed to:
"**SUPPLY OF VULNERABILITY SCANNING SOFTWARE LICENCES**".
Head – Procurement unit
SADC Secretariat
Plot 54385 CBD
Gaborone
BOTSWANA

Late submissions and faxed quotations are not acceptable

5. Bids should be emailed to the following email address:
iarmsoftware2020@sadc.int

4. The deadline for submission of your bids, to the email addresses indicated in Paragraph 3 is: **27th October 2020; 14:30hrs.**

5. Your bids should be submitted as per the following instructions, and in accordance with the Terms and Conditions of the Standard Purchase Order for SADC which is available on request.

(i) PRICES: The prices should be convertible to the local Pula currency (Include exchange rate to Pula if using foreign currency), including all duties attached to the sale of the ***goods*** (such as VAT, customs duties, etc) and transport to the final destination.

(ii) EVALUATION AND AWARD OF PURCHASE ORDER: Bids determined to be administrative (see Paragraph 2,3,4 and 5 and technically compliant to the requirements will be evaluated by comparison of their prices per lot (defined as above). The award will be made to the bidder offering an administratively and technically compliant quotation at the lowest total price for the lot.

(iv) VALIDITY OF THE OFFER: Your Bid should be valid for a period of 90 days from the date of deadline for submission of quotation indicated in Paragraph 4 above.

8. The software ***licenses*** are expected to be delivered within ***1weeks*** from the signature of the Purchase Order. Hardware equipment are expected within 8 weeks from date of purchase order.

7. Additional information and clarifications can be requested **in writing,** via email addresses below no later than **21st October 2020; 14:30hrs.**
Email: tenders@sadc.int and imoatshe@sadc.int; cc: okamau@sadc.int; ***during working hours.***

Annexes: 1

Sincerely,

Name: Veronica Chingalawa
Title: Acting Head - Procurement
Date: 13th October 2020

ANNEX 1

TECHNICAL SPECIFICATIONS

ID	IT AUDITING TOOLS REQUIREMENT	M / HD / D
1	**Scope of Assessment**	
1.1	The tool or software should be able to scan the following type of hosts 1. Operating system of servers (Microsoft) 2. Databases Systems 3. Webservers (Microsoft IIS and Linux) 4. Virtual OS 5. Cisco routers and switches 6. Wireless Networks 7. Firewalls	**M**
1.2	A combination of tools or software can be evaluated to achieve the stated scope.	**HD**
2	**Features**	
2.1	Assess user accounts management and provide report on any incorrect user assignments including but not limited to; ✓ Assignment of privileged accounts e.g. administrator account. ✓ Management of user accounts e.g. date of creation, date last login, date disabled, date deleted. ✓ Management of user group e.g date created, modified and or deleted. ✓ Management of assets – ability to discover assets including date created, modified and deleted.	**M**
2.2	Assess configuration and provide report on any misconfigurations against best practice. ✓ The best practice that the system is using as a reference should be disclosed. E.g OWASP top 10., PCI standard, baselines	**M**
2.3	Assess if servers and network components have been patched and provide report of missing patches. ✓ The tool should be able to provide information on the sources from which signatures are derived e.g MITRE Common Vulnerabilities and Exposures database, Common Vulnerability Scoring System.	**M**

	✓ The tool should indicate how frequently are updates sourced and pushed into the vulnerability software.	
2.4	Clearly identify vulnerability severity levels in dashboard displays and reports. ✓ Severity should be scored and ranked using either qualitative measures or quantitative measures e.g 1 to 5 or high, medium, low.	**M**
2.5	Provide recommendation and or how issues are to be resolved. ✓ Recommendation should be verifiable and from relevant source such vendors eg Microsoft, Cisco.	**M**
2.6	The tools should provide downloadable reports in different formats such as word, excel and PDF. ✓ The report should detail identified vulnerabilities. ✓ The reports should be flexible to produce details in different presentation including graphical presentations.	
3	**Ease of Use**	**M**
3.1	Clearly define the user accounts required to run the tool or software e.g administrator account, sa, normal user.	**M**
3.2	The tool or software should have standard policies embedded e.g Audit, Compliance.	**M**
3.3	The tool or software should also provide for custom policies to be used (design user scripts).	**HD**
3.4	The tool or software should not be intrusive, that is its impact on the network performance e.g vulnerability assessment should be carried out during working hours.	**M**
3.5	The tool or software should provide for option to be run on premise. Where the software is cloud based how long reports are retained before been pursed.	**HD**
4	**Licensing**	
4.1	The licensing agreement should be cost effective. ✓ Understand whether licensing is based on annual fee or host based pricing.	**HD**
5	**Management of the Tool**	
5.1	The tool or software should be easy to manage and allow for access of scanned reports over a period of at least 3 months. ✓ Establish if the tool requires patches ad backup.	**HD**
6	**Support**	
6.1	The vendor should provide different options for providing support including email, online chats and telephone.	**M**

7	**Demos**	
7.1	The tool or system should provide demos that can be used to evaluate the tools functionality. ✓ Type of reports produced by the tools should be easily available to provide better evaluation.	**M**

Note:

M	Mandatory
HD	Highly Desirable
D	Desirable