EASTERN AND SOUTHERN AFRICAN TRADE AND DEVELOPMENT BANK (TDB)
BANQUE DE L'AFRIQUE DE L'EST ET AUSTRALE DE COMMERCE ET DÉVELOPPEMENT

TDB
TRADE & DEVELOPMENT BANK

TERMS OF REFERENCE

REQUEST FOR PROPOSAL (RFP) FOR THE SUPPLY, INSTALLATION AND COMMISSSIONING OF A CYBER DEFENSE SOLUTION FOR EASTERN AND SOUTHERN AFRICAN TRADE AND DEVELOPMENT BANK, (TDB)

Background

The Eastern and Southern African Trade and Development Bank, also known as Trade and Development Bank (TDB), is a specialized African multilateral financial institution serving most of the Eastern and Southern Africa. The Bank's objective is to provide short, medium- and long-term financing to viable projects and trade finance activities in member states.

Through its Information Services unit, the Bank seeks to acquire, implement and maintain a Cyber Defense solution capable of using Machine Learning (ML) and Artificial Intelligence (AI).

REQUIREMENTS
The specifications of which are detailed in the table below:

ITEM	DESCRIPTION
1.1	It must use several algorithms of artificial intelligence as well as several techniques of machine learning, containing at least: deep learning, supervised machine learning and unsupervised machine learning
1.2	After the initial learning period, the technology must automatically provide a complete audit trail of all devices in the environment, pre-sorting at least the device type, hostname, mac address, the first and last time the device was seen on the network
1.3	i. It must provide full network visibility, including traditional and non-traditional I.T. ii. The Proposed solution should integrate with every device residing on the network, off the network as well as cloud

	based. Examples of such devices are as below but they are not limited to: a) Servers (physical or VM) b) PC/Laptops c) Smart Mobile phones/Tablet PCs/iPads d) VPN Based Solutions e) Any Other Device bearing an IP and connecting to the network.
1.4	After the initial learning period, the technology must automatically provide a complete audit trail of all subnets found in the network It must be a self-learning platform and have an adaptive approach, that uses proven artificial intelligence to learn about the environment in which it finds itself and detect and respond to deviations from normal activity. i. the network's baseline must be adaptive and dynamic enough to suit any changes in the environment's behavior. ii. it should operate completely based on behavior, where technologies that make use of rules and/or signatures will not be allowed. iii. It must be able to take autonomous action to contain in-progress threats, giving the security team time to investigate and remediate as needed.

1.5	The autonomous response must: a) rely on an understanding of normal activity and be able to surgically interrupt the unusual activity only. b) take proportionate action in real time - from connection-specific interruptions through to full device quarantines either directly or via c) integrations with firewalls and/or Network Access Controls d) this action should not rely on agents installed on different devices to perform its response. e) this should not require the appliance to sit in-line but rather remain passive in the network
1.6	It must be based on behavior analysis, being able to highlight at least: i. all unusual connectivity in the network ii. all unusual activities on the network iii. be able to do a detailed tracking of the device, indicating even its history of IPs, if it is in a DHCP scope. iv. be able to do a detailed tracking of the user indicating even all the hostnames associated to a certain credential. v. be able to identify a significantly unusual volume of connections. vi. identify the level of rarity of a device on the network as well as the rarity level of an external site access
1.7	It must be able to automatically alert the monitoring team to all unusual and abnormal activities on the network.
1.8	It must provide simple and fast filters in order to enable the analysis of violations by Users, Devices, and type of violation.
1.9	It should have an omni search bar that makes it possible to search immediately for a device, IP, subnet, or network host

1.10	It must have a user interface where it can be possible to consult the complete System status including: i. Software version used disk space, CPU and memory consumption. ii. the detailing of all active interfaces and respective traffic received through each of them. iii. the total bandwidth currently processed, the average bandwidth processed to date, the bandwidth recorded in the last 7 days and 2 previous weeks. iv. a detailed analysis of all the traffic received in the device as well as the last time the main protocols were seen, among them, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, among others
1.11	It must be able to identify new and unknown attack behaviors without making use of signatures or rules
1.12	It must be able to identify any anomalous behavior in the environment and highlight these behaviors in real time
1.13	It must be able to identify any new device inserted in the network and be able to profile it to ensure alignment with network policy requirements
1.14	It must be able to automatically group devices into clusters by their behavior similarity
1.15	It must have a user interface for the visualization of threats in 3D being able to plot in real time the map of any connection made by the internal devices
1.16	It must have a feature capable of enabling retrospective analysis of the incident's logs, returning the connection in seconds, minutes, hours or days before a certain anomaly had been identified
1.17	It should provide an instant overview of what is happening in the organization globally
1.18	It should visually represent all network activity and connections between all machines and users (internally and externally)
1.19	It should be based on probabilistic mathematical methods, analyzing and correlating distinct dimensions within the package: i. creating unique modeling techniques for each user and device, as well as for the relations between them

	ii. It must be able to group the anomalies intelligently and by level of criticality. iii. It must be able to do a packet capture in real time permitting a thorough analysis of the incident at the time of the occurrence. iv. It must offer the option of analyzing the package in both Wireshark and inside its own user interface by itself
1.20	It must enable the customization and adaptation of the machine learning to specific conditions and characteristics of the network. i. It must have LDAP integration. ii. It must allow the advanced customization of the technology, allowing to consider multiple data parameters when checking a certain behavior, among the parameters it should be possible to at least have the following options: Connections, external connections, internal connections, data transfer, external data transfer, internal SMB connections, closed-port connections, broadcasts, connected devices, data transfer (client), data transfer (server), among other relevant metrics. iii. It must allow to import of external whitelists and blacklists
	EXTERNAL INTEGRATIONS AND REPORTING
2.0	It should enable the automatic creation of executive reports covering at least one overview of: i. The entire deployment summary indicating the total number of devices, total number of subnets and processed media bandwidth. ii. A summary of breaches per attack phase iii. A devices breach summary iv. A TOP devices summary breaching high priority conditions. v. Summary of the most frequent breaches to main compliance items such as misuse of USB, google drive, outbound RDP, external SQL, among others. vi. a TOP devices summary that most breaches the compliance conditions generating risk to the organization. It must have a Dynamic Threat Dashboard for a simplified overview of real-time threats that is simple and intuitive and that enables at least:

	i. an immediate understanding of breaches with a description of what that breaches means. ii. a recommendation for the action that could be taken. iii. a filtering for breaches more critical as well as for devices more critical iv. a complete breach detailing with device data, history, tags, connections, logs, and device history v. a possibility of opening a more detailed and detailed investigation of the logs and connections with the topology plotted in 3D. vi. The system must be OPEN API, supporting integrations with other security elements at least in the following formats: a. CEF, LEEF, JSON, SYSLOG, TAXII, among others vii. The technology must have its own mobile app available in both Google Play and Apple Store in order to enable remote management of incidents.
	ARCHITECTURE
3.0	It must support a complete and scalable architecture through the licensing of additional components required to integrate with the various digital environments, including on-premise, cloud and hybrids, if the contractor wishes to acquire them in the future, supporting at least: i. Amazon AWS SaaS, EC2, IAM, S3, VPC and LAMBDA ii. Microsoft Azure iii. Office 365 iv. Virtual components (virtual machines) v. Scripts for analysis of local servers (sensors for operating systems) It must support a distributed architecture with components working in the MASTER-SLAVEs architecture where all data analysis and correlation is performed locally and only metadata is forwarded to the central site for centralized administration so as not to burden the network. It must consume and analyze raw data (raw packets) through port mirroring.

	It will not be accepted if it only uses partial analysis of the packages making use of sflow, jflow, netflow, among others. A single hardware appliance must be capable of handling up to 5Gbps of throughput. The hardware specified must not exceed standard rack mount 2U size. The hardware specified must have at least the following physical interfaces: i. 1x 10/100/1000 BASE-T to act as an administration interface. ii. 1x 10/100/1000 BASE-T to act as a remote management interface. iii. 3x 10/100/1000 BASE-T to act as copper interfaces for traffic analysis. iv. 2 x 10Gbe/1Gbe SFP+ to act as analysis ports SFP+ The hardware specified must have a redundant power supply
	SUPPORT AND TRAINING
4.0	It must have an online portal available for client access by providing at least: i. two factor authentications (2FA) ii. Pre-scheduled periodic training sessions, without additional cost for the client iii. a complete library of solution documents, as well as specific fields where the latest product updates, release notes, and FAQs can easily be validated. iv. contain specific feature for the opening of support tickets, which enables fast, simple opening and case detailing. All ticket updates. v. must be updated in the system and be forwarded via email and must have a complete call history track. vi. it must have fields of debate about Cyber Threats and publications of security experts about current questions. It must provide helpdesk / diagnostic and remote support for issues. Official training must be provided about the tool, covering essential items for its deep and correct use which should fulfil the following:

	i. It must be scheduled 5 business days in advance. ii. It must be done during business hours, with a duration of 6 hours iii. The official timeline and main topics to be addressed should be presented.

PROPOSALS

The proposal pack should include.

1. Company profile
2. Separate Financial and Technical proposal in one pack
3. Delivery period clearly stated.

Interested Vendors are requested to submit their proposals through e-mail to procurement@tdbgroup.org with subject line **"PROCUREMENT OF A CYBER DEFENSE SOLUTION**" by 5:30pm on Wednesday 30th June 2021.

Requests for further information and clarifications on requirements should be directed to rfpenquiries@tdbgroup.org with subject line **"CYBER DEFENSE SOLUTION"**

Disclaimer: TDB Group reserves the right to independently verify submitted documents, listed clients and similar works. TDB Group is not obliged to give reason for not selecting any persons/ firm. TDB Group reserves the right to discontinue this process without reference to any entity.