 **NBS/EDR/NDR/2024**

**04 April 2024**

**REQUEST FOR QUOTATION**

**Procurement Of Endpoint Detection & Response (EDR) System, and Network Detect & Response (NDR) System**

**PRICE SCHEDULE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Description** | **Duration** | **USD$ Annual Price** | **USD$ Total Price** |
|  | **Endpoint Detection & Response (EDR) System** | **3 years** |  |  |
|  | **Network Detect & Response (NDR) System** | **3 years** |  |  |
|  | Vat sum |  |  |  |
|  | **TOTAL** |  |  |  |

1. **SCOPE OF SERVICE FOR EDR SOLUTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Item** | **Description** | **Cost (USD exc. VAT)** | **Required** |
|  | Software:  Perpetual License for an Enterprise Antivirus Solution with EDR with below features: | 430 Endpoints  Desktops - 120  Laptops - 110  Servers - (Linux & Windows) - 200 |  | Mandatory |
|  | Hardware | As sized by the vendor. Include High Availability Architecture in the design |  | Optional |
|  | Implementation and Training | Training for up to 10 people |  | Mandatory |
|  | 1st Year AMC Charges | # See notes below |  | Mandatory |
|  | 2nd Year AMC Charges | As above |  | Mandatory |
|  | 3rd year AMC Charges | As above |  | Mandatory |
|  | Other Costs | Please provide full details |  | Optional |
|  |  | **Total** |  |  |

Notes:

* The vendor should nominate an Account Support Team with an escalation matrix for handling all issues during AMC Period.
* The Account Support Team should be the single point of contact with end-to-end account ownership for all committed deliverables during AMC Period.
* Incident Management/Problem Management: Vendor should have robust problem management tool which can automatically send alert notification to their backend for early intimation and proactive handling of problems such as critical issues.
* The vendor must provide free software updates for any version upgrade for the supplied software required by NBS to support the application requirements.
* The vendor should have a system to send regular alerts to NBS team on any security alerts, product related issues, patch alerts etc.

1. **SCOPE OF SERVICE NDR SOLUTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Item** | **Description** | **Cost (USD exc. VAT)** | **Required** |
|  | Software:  Perpetual License fees NDR | 430 Endpoints  Desktops - 120  Laptops - 110  Servers - (Linux & Windows) - 200 |  | Mandatory |
|  | Hardware | As sized by the vendor. Include High Availability Architecture in the design |  | Optional |
|  | Implementation and Training | Training for up to 10 people |  | Mandatory |
|  | 1st Year AMC Charges | # See notes below |  | Mandatory |
|  | 2nd Year AMC Charges | As above |  | Mandatory |
|  | 3rd year AMC Charges | As above |  | Mandatory |
|  | Other Costs | Please provide full details |  | Optional |
|  |  | **Total** |  |  |

Notes:

* The vendor should nominate an Account Support Team with an escalation matrix for handling all issues during AMC Period.
* The Account Support Team should be the single point of contact with end-to-end account ownership for all committed deliverables during AMC Period.
* Incident Management/Problem Management: Vendor should have robust problem management tool which can automatically send alert notification to their backend for early intimation and proactive handling of problems such as critical issues.
* The vendor must provide free software updates for any version upgrade for the supplied software required by NBS to support the application requirements.
* The vendor should have a system to send regular alerts to NBS team on any security alerts, product related issues, patch alerts etc.

**Manner of Submission**

Bids must be submitted through email or in some other electronic forms are received before the end of the bidding period. Bids must be received at NBS **Celestial Park** Head Office on or before the closing date**, No. 19280 Borrowdale Road, Block 1, Unit L, 2nd Floor, Harare** before **10:00 hours** on the **closing date.** Electronic submission to be sent to: [tinashe.dani@nbs.co.zw;procurement@nbs.co.zw](mailto:tinashe.dani@nbs.co.zw;procurement@nbs.co.zw) Offers not received by 10:00 hours on the closing date will be treated as late tenders, rejected, and returned to tenderer.

**Closing Date for Submission: Wednesday 10th of April 2024 at 10.00hrs**

**YOUR OFFER SHOULD CLEARLY INDICATE THE FOLLOWING:**

**MANDATORY REQUIREMENTS**

|  |  |  |
| --- | --- | --- |
| **SI.** | **REQUIREMENT** | **INFORMATION PROVIDED?** |
| **1.** | Official Registered Name, Address & Main Telephone Number(s) **Key Contact Person:** Name, Position & Title, Address (if different from above), Direct Phone Number, email address. | **YES/NO** |
| **2.** | The bidder must not be insolvent, in receivership, bankrupt or being wound up, not have had business activities suspended and not be the subject of legal proceedings for any of these circumstances; | **YES/NO** |
| **3.** | The bidder must declare that they have no a conflict of interest in relation to this procurement requirement; | **YES/NO** |
| **4.** | The Bidder must not be debarred from participation in public procurement under section 72 (6) of the Act and section 74(1) (c), (d) or (e) of the Regulations or declared ineligible under section 99 of the Act; | **YES/NO** |
| **5.** | **Company Background, Business Profile and Strategy:** Provide brief history and background of the organization, including year established and number of years the company has been offering similar products. | **YES/NO** |
| **6.** | **Service Providers must provide the following Company Documents**:  (i) Certified copies of Company or Firm’s Registration Certificate;  (ii) Form CR14 or equivalent list of Directors;  (iii) Form CR 6 or equivalent registered office/ principal place of business of the company;  (iv) must be registered with the Zimbabwe Revenue Authority (ZIMRA),  (v) must be registered with **National Social Security Authority (NSSA)**;  (vi) must be registered with the **Procurement Regulatory Authority (PRAZ)** as a Supplier and paid the applicable Supplier Registration Fee set out in Part III of the Fifth Schedule to the Regulations.  (vii) must be an **Approved Distributor** of the proposed EDR or NDR solution **(Attach accreditation certificates from the OEM Vendor)**. | **ATTACH PROOF** |
| **7.** | Provide declaration and signed letter/contract if partnering with another supplier to provide the required solution. | **YES/NO** |
| **8.** | The Supplier should have **at least Three (3) traceable reference letters** showing the delivery of **related security solutions** within the past 10 years. | **ATTACH PROOF & COMPLETE ADDENDUM A** |

**TECHNICAL REQUIREMENTS**

**Part A – EDR SOLUTION**

1. **PART A - STATEMENT OF USER REQUIREMENTS**

Below is the list of specifications and capabilities that should be provided by the proposed EDR Solution unless stated otherwise, provide details of the proposed features and specifications where needed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Description | Requirement | Compliance With Requirement | Comments or Supporting  Document(s)  Submitted |
| **A** | **Operational** |  |  |  |
|  | Solution must support on-premises and remote clients regardless of connectivity to management server. | Mandatory |  |  |
|  | Solution must support high availability and disaster recovery functions. | Mandatory |  |  |
|  | The solution must support at least 300 endpoints/clients and is scalable. | Mandatory |  |  |
|  | Policy must be able to define whitelists to implement exceptions to the base policy | Mandatory |  |  |
|  | Solution must have a deeply functional and documented API to support integration and automation across the platform and with other platforms. | Mandatory |  |  |
|  | The solution must have online support 24x7x365 (on-call/Remote) | Mandatory |  |  |
|  | Must provide role-based access to the console to allow specific admins to carry out read/write/read & write as per permission | Mandatory |  |  |
|  | Ability to exclude files and folders from scans. (Example: Exemptions for specific database folders) | Mandatory |  |  |
|  | Ability to completely stop the antivirus/EPP during application installs | Mandatory |  |  |
|  | Granular control of policy based on user/group/device | Mandatory |  |  |
|  | The solution should be able to perform push operations to endpoint clients. | Mandatory |  |  |
|  | The solution should be "Network Aware" and can change the client's policy based on its network location. | Mandatory |  |  |
|  | The solution must have Two-Factor Authentication for logins. | Mandatory |  |  |
|  | Console access should support using 3rd party systems authentication | Mandatory |  |  |
|  | Should support OS like Windows, Mac, Linux, Ubuntu | Mandatory |  |  |
|  | Solution should be aligned and supported to the latest OS releases. | Mandatory |  |  |
|  | The solution should be cloud ready | Mandatory |  |  |
|  | The solution has AI and ML capabilities | Preferred |  |  |
|  | Integration with 3rd party solutions- The solution must be able to integrate with SIEM and other security solution for log collection through API integration |  |  |  |
|  | Threat Intelligence - The solution should be dynamically updated based on a global network of threat sensors by sharing threat data. |  |  |  |
|  | Solution will allow for the searching of multiple type of undetected sensor data including File, Process, Network, Registry, Injection and User data. | Mandatory |  |  |
|  | The solution will allow for remediation of any file or process found through the EDR platform. | Mandatory |  |  |
|  | The solution will allow for forensics analysis and report of any indicator found through the EDR platform. | Mandatory |  |  |
|  | The solution will provide multiple manual remediation options, such as Quarantine, Kill Process and Forensics Analysis with remediation. | Mandatory |  |  |
|  | The solution will provide a central management ability to isolate machines remotely. | Mandatory |  |  |
|  | The solution must have the ability to view MAC addresses for every computer sending data. | Mandatory |  |  |
|  |  |  |  |  |
| **B** | **Deployment** |  |  |  |
|  | Solution must use provide modern and easy remote deployment/installation/uninstallation methods (including script support) The solution must have the ability for native Remote Installation and client deployment without usage of 3rd party tools. | Mandatory |  |  |
|  | The solution must use an “Authentication Token” for securely registering a new client installation to the management server. | Mandatory |  |  |
|  | The solution must allow to manage the agent version and components from the management interface. | Mandatory |  |  |
|  |  |  |  |  |
| **C** | **Logs and reporting** |  |  |  |
| 1 | The solution should be able to provide real time email alerts | Mandatory |  |  |
| 2 | The solution should be able to provide pre-defined and customized Reports as per requirement for Audit and internal reporting purpose | Mandatory |  |  |
| 3 | Should allow advanced customization by providing options to enter custom queries to extract data from database directly. | Preferred |  |  |
| 4 | Should have options to export reports in multiple format such as PDF, HTML, CSV | Preferred |  |  |
| 5 | Should allow reports to be sent out on schedule as daily, weekly, monthly reports | Mandatory |  |  |
| 6 | Should Support Creation of Customized dashboards and reports as per requirement | Mandatory |  |  |
|  |  |  |  |  |
| **D** | **Client Features** |  |  |  |
| 1 | Agent must be lightweight. Present evidence of average CPU, memory, and disk use during different activities with the capabilities below enabled | Mandatory |  |  |
| 2 | Solution is configurable for minimal system resource utilization | Mandatory |  |  |
| 4 | The solution allows upgrade to newer versions without performing a reboot. | Mandatory |  |  |
| 5 | The solution package size will include only the relevant components for deploying in a single installer | Mandatory |  |  |
| 6 | The solution should provide proxy capabilities for clients that are offline and for limiting bandwidth usage. | Mandatory |  |  |
| 7 | The solution should be able to retrieve signature updates for the Internet by an authenticated NTLM proxy with a logged-in user's credentials. | Mandatory |  |  |
| 8 | When performing upgrades, the solution will download only the accumulated changes from the installed version | Mandatory |  |  |
|  |  |  |  |  |
| **E** | **Detection - Device Monitoring** |  |  |  |
| 1 | Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real-time. (Data collected through post-event scripts or live interaction with host is covered in a separate requirement.) Examples must include, but not limited to, process events, file & registry modifications, network connections, cross-process activity, command line arguments, windows events, DNS queries and responses. | Mandatory |  |  |
| 2 | Solution must continuously monitor and report findings as quickly as possible. If an endpoint cannot immediately report findings, results must be stored locally until they can be uploaded to the solution's central management system | Mandatory |  |  |
| 3 | Solution must allow for real-time alerting or logging of notable events based on custom content (behaviors) or atomic indicators of compromise | Mandatory |  |  |
| 4 | Solution must capture detailed metadata around binaries and processes that are executed on endpoints. Details must include, but not limited to, the binary's hash (MD5, SHA- 256), publisher information, code signing details, frequency observed in our environment, version information, and filesystem owner | Preferred |  |  |
| 5 | The solution should have the ability to re-brand user notifications | Mandatory |  |  |
| 6 | The solution should have the ability to control the level of messages to show to users | Mandatory |  |  |
|  |  |  |  |  |
| **F** | **Detection - Response** |  |  |  |
| 1 | Solution must provide a way to isolate a system that ensures preventative controls are preserved through reboots. Isolation settings must be pre-set to allow endpoint to be isolated from threats but able to connect to investigation/remediation systems | Mandatory |  |  |
| 2 | Solution must be able to immediately apply preventive controls (block specific activity or known malicious, etc.) | Mandatory |  |  |
| 3 | Solution must have the ability to search across all endpoints for IOCs or other system attributes that are not captured in real time telemetry data. | Mandatory |  |  |
|  |  |  |  |  |
| **G** | **Compliance - Data and Device Protection** |  |  |  |
| 1 | The solution will require that only an authorized Pre-boot user is allowed to log into Windows. | Preferred |  |  |
| 2 | Users will log on one time (SSO) for authentication to the operating system, Full Disk Encryption, and other Endpoint Security blades. | Mandatory |  |  |
| 3 | The solution should provide management of all endpoint ports, with centralized logging of port activity for auditing and compliance. | Mandatory |  |  |
| 4 | The solution will allow custom user message notifications when connecting a device based on the scenario. | Preferred |  |  |
| 5 | The solution will enforce endpoint computers to comply with security rules that are defined for the organization. Computers that do not comply will be shown as non-compliant and can apply restrictive policies to them. | Mandatory |  |  |
| 6 | The solution will enforce required Applications and Files based on the compliance settings by monitoring for the presence of specified files, registry values, and processes that must be running or present on endpoint computers | Mandatory |  |  |
| 7 | The solution will enforce an Anti-Malware check to verify that computers have an anti-malware program installed and updated. | Mandatory |  |  |
| 8 | Solution should provide Full disk encryption and file level encryption to prevent data leakage via loss of a laptop or a portable hard drive. | Mandatory |  |  |
| 9 | Solution should have Device Control to manage user access to devices that are installed on or connected to the computer. | Mandatory |  |  |
|  |  |  |  |  |
| **H** | **Compliance - Firewall** |  |  |  |
| 1 | The solution will enforce Firewall rules to allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols. | Mandatory |  |  |
| 2 | The solution will be used to determine if users can connect to wireless networks while on the organization's LAN to protect the network from threats associated with wireless networks. | Mandatory |  |  |
| 3 | The solution will define if users can connect to the organization network from hotspots in public places, such as hotels or airports. | Mandatory |  |  |
| 4 | The solution’s client Firewall should remain active during a client upgrade. | Mandatory |  |  |
| 5 | The solution must include an option for Host Isolation to isolate or allow a specific host (access to network) that is under malware attack and poses a risk of propagation. | Mandatory |  |  |
|  |  |  |  |  |
| **I** | **Application Control** |  |  |  |
| 1 | The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block, or terminate applications and processes | Mandatory |  |  |
| 2 | The solution will be able to Whitelist\Blacklist applications | Mandatory |  |  |
| 3 | The solution will be used to restrict network access for specified applications. The Endpoint Security administrator | Mandatory |  |  |
|  |  |  |  |  |
| **J** | **Anti-Malware** |  |  |  |
| 1 | The solution will protect the computer from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers. The solution will centrally manage the detection and treatment of malware on the endpoint computers. | Mandatory |  |  |
| 2 | The solution will allow scheduled scanning of local drives, Mail messages. Optical drives and Removable devices. | Mandatory |  |  |
|  |  |  |  |  |
| **K** | **Ransomware Protection** |  |  |  |
| 1 | The solution will protect against existing and zero-day ransomware without requiring signature updates | Mandatory |  |  |
| 2 | The solution will remediate and restore files that were encrypted during a ransomware attack. | Mandatory |  |  |
| 3 | The anti-ransomware solution has third party-validation. | Mandatory |  |  |
|  |  |  |  |  |
| **L** | **Behavioral Protection** |  |  |  |
| 1 | The solution will leverage multiple sensors to identify generic malware behaviors as well as malware family specific behaviors effectively and uniquely. | Mandatory |  |  |
| 2 | The solution will detect and prevent file less attacks only utilizing Windows processes. | Mandatory |  |  |
| 3 | The solution will immediately prevent or detect malicious behaviors regardless of whether the machine is online or offline | Mandatory |  |  |
| 4 | The solution will detect and prevent file less attacks based on scripting. | Mandatory |  |  |
| 5 | The solution should protect against the "Pass The Hash" technique for credential theft. | Mandatory |  |  |
|  |  |  |  |  |
| **M** | **Machine Learning Models for Static Analysis** |  |  |  |
| 1 | The solution must be able to identify zero-day files even if they are not familiar with any reputation service | Mandatory |  |  |
| 2 | Any ML models used by the endpoint should be frequently updated to protect against fresh, zero-days attacks | Mandatory |  |  |
| 3 | The solution must lock the user from using files until they are checked and found to be clean | Mandatory |  |  |
| 4 | The solution’s Static Detection Engine must monitor the access to files | Preferred |  |  |
| 5 | Solution should have Anti-Bot capabilities. Upon an identified bot attack, the solution will completely remediate the attack leaving the endpoint cleaned. | Mandatory |  |  |
|  |  |  |  |  |
| **N** | **Web Browsing Protection** |  |  |  |
| 1 | Support for most common Browsers like Chrome, Firefox, Safari, etc., and must enforce "Safe Searching" feature when they employ the Google, Bing, Yahoo, or any other search engines. The user must not be able to remove the browsing protection in any way | Mandatory |  |  |
| 2 | The solution must have scrubbing capabilities with no added hardware. Incoming files will be scanned for potential malicious content such as scripts, macros, and active content. | Preferred |  |  |
| 3 | The solution will detect zero-day phishing sites that request user credentials even if unknown to reputation engines. | Mandatory |  |  |
| 4 | The solution must block the user from browsing to known malicious URLs or domains | Mandatory |  |  |
| 5 | The solution must provide URL filtering based on categories with additional Black/Whitelisting | Mandatory |  |  |
|  |  |  |  |  |
| **O** | **Sandboxing & Exploit Prevention** |  |  |  |
| 1 | All files written on the filesystem will be monitored and statically analysed. If found as potentially malicious, the files will be emulated by sandboxing and quarantined if found as malicious. | Mandatory |  |  |
| 2 | The solution will detect and prevent exploitation techniques of trusted software. | Mandatory |  |  |
| 3 | The solution has the capability of blocking against the new RDP RCE attacks like Blue Keep on unpatched systems. | Mandatory |  |  |
|  |  |  |  |  |
| **P** | **Security Awareness Training** |  |  |  |
| 1 | Solution should be able to automate training programs for end users on Cyber security best practices. | Mandatory |  |  |
| 2 | Solution should provide option to customize training programs for end users | Mandatory |  |  |
| 3 | The solution should be able to provide stats of users that were trained. | Mandatory |  |  |
|  |  |  |  |  |
| **Q** | **Forensics Analysis** |  |  |  |
| 1 | Solution will automatically create an incident analysis for every detection/prevention that occurs. This analysis should include process execution trees even across boots if relevant. | preferred |  |  |
| 2 | Forensic report will automatically identify the malicious activity entry point and highlight the potential damage, remediation action and the entire chain of attack. | Mandatory |  |  |
| 3 | The Forensics report will log, present and un-obfuscate PowerShell scripts used during an attack. | Mandatory |  |  |
| 4 | The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information. | Mandatory |  |  |
| 5 | The solution must include the following sensors: Remote Execution  Service Creation  Process Discovery  Application Window Discovery  Screen Capture  Input Capture  DDE (Dynamic Data Exchange) | Mandatory |  |  |
|  |  |  |  |  |
| **R** | **Logging and Reporting** |  |  |  |
| 1 | The solution should generate periodic reports on malware types, types of vulnerabilities exploited etc. | Mandatory |  |  |
| 2 | The solution must have the ability to generate visual reports | Mandatory |  |  |
| 3 | Solution must provide agent health status reports | Mandatory |  |  |
| 4 | The solution should showcase affected process, affected registry keys & affected files in OS environment | Mandatory |  |  |
| 5 | The solution will showcase malicious file emulation screenshots and video in Sandbox environment | Mandatory |  |  |
| **Total Score** | | | |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Professional Services Required** | **Specifications in Brief** | Compliance (Yes/No) |
| 1 | System Installation | * Supply of software and licenses. * Installation of Antivirus Agents in all Endpoints (Laptop/Desktop/Servers etc.) * Configuration of Centralized/ Main Antivirus Server Console. * Creation of Policies, Implementation, Configuration and Testing which includes configuration of scheduled scanning/ implementation of device control mechanism/ configuration of email alerts and reporting. * Training of the New Antivirus Solution deployed along with implementation document and manual. * 24x7 Helpdesk support with trouble ticketing and tracking system. * Upgrade of patches and product version during the support period. |  |
| 2 | System Training and Knowledge Transfer | * Instructor led training (with training material) to 6-8 NBS team members. Training could be Virtual or Onsite as directed and mutually agreed. |  |
| 3 | Services during AMC Period | * The vendor should nominate an Account Support Team with an escalation matrix for handling all issues during AMC Period. * The Account Support Team should be the single point of contact with end-to-end account ownership for all committed deliverables during AMC Period. |  |

**Part B – NDR SOLUTION**

1. **PART B - STATEMENT OF USER REQUIREMENTS**

* Below is the list of specifications and capabilities that should be provided by the proposed NDR Solution.
* Unless stated otherwise, please provide details of the proposed features and specifications where needed.
* The winning bidder should provide the appropriate solution size based on the NBS existing setup.
* Hardware and software needed for the solution should be priced separately on bidder financial proposal.
* The solution must be delivered and installed at the NBS Data Center.
* NOTE: Below specifications are the minimum accepted specifications.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Specification** | **Requirement** | Compliance With Requirement  **Full Compliance** – F [5 Marks]  **Partial** **Compliance** – P  [1 to 3 Marks]  **Not Compliant** – N [0 Marks] | Comments or Supporting  Document(s)  Submitted | |
| The product must be able to retrieve updates using a globally known threat intelligence organization | Mandatory |  |  | |
| Solution provides full flow logging capability | Mandatory |  |  | |
| Solution has real-time analytics, Artificial Intelligence and Machine Learning capabilities to detect known and unknown security incidents | Mandatory |  |  | |
| Solution has Two deployment options (Virtual and Hardware) | Mandatory |  |  | |
| The solution has behavioral technology to detect threats | Mandatory |  |  | |
| The solution must leverage advanced entity modeling to reduce false positives | Mandatory |  |  | |
| The solution must detect malware hidden in encrypted traffic | Mandatory |  |  | |
| The solution must be able to Differentiate key assets from other hosts for risk prioritization. | Mandatory |  |  | |
| The solution must automatically identify and classify threats, including attack phase and risk, without requiring any intervention. | Mandatory |  |  | |
| Provide automatic and manual response capabilities to react to the detection of suspicious network traffic | Mandatory |  |  | |
| The solution should automatically score and prioritize each individual attacker behavior detected. | Mandatory |  |  | |
| The solution should prioritize and detect data exfiltration with encrypted and unencrypted traffic | Mandatory |  |  | |
| The solution should provide Brute Force detection | Mandatory |  |  | |
| The solution should automatically score and prioritize each host/account based on its behaviors over time. | Mandatory |  |  | |
| The solution should provide DoS/DDoS detection (SYN, ICMP or UDP flood) capability | Mandatory |  |  | |
| The solution should provide Network scanning and reconnaissance detection capability | Mandatory |  |  | |
| The solution should provide Rogue server detection capability | Mandatory |  |  | |
| The solution should detect Advanced Threats (Ransomwares / Malwares / RATs … etc) within Encrypted traffic without decryption | Mandatory |  |  | |
| The solution should de-duplicate all traffic for the reports | Mandatory |  |  | |
| The solution should provide a centralized traffic-based view of all traffic on the network including traffic in a virtual environment | Mandatory |  |  | |
| The solution should provide response time behavioral analysis and reporting | Mandatory |  |  | |
| The solution should provide large file transfer detection capability | Mandatory |  |  | |
| The network traffic should be visualized to create an easy, drill-down method of viewing host to host communications | Mandatory |  |  | |
| The solution should have the capability to address false positives | Mandatory |  |  | |
| The solution must have the capabilities to be integrated with some SIEM solutions | Mandatory |  |  | |
| The solution should show alarms by Risk | Mandatory |  |  | |
| The solution should provide a detailed explanation on a detected breach in a human readable format | Mandatory |  |  | |
| The solution should support Active Directory | Mandatory |  |  | |
| The solution should provide the capability to correlate traffic passing through a load balancer | Mandatory |  |  | |
| Reports should be scheduled for automated delivery via email | Mandatory |  |  | |
| The solution should provide security Dashboard Reporting and Analytics | Mandatory |  |  | |
| The solution proposed 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 | Mandatory |  | |  |
| The Proposed solution should integrate with every device residing on the network with an IP Address. Examples of such devices are as below but they are not limited to Servers (physical or VM), PC/Laptops  Smart Mobile phones/Tablet PCs/iPad, Access Points, Bio-Metric Solutions  VPN Based Solutions  Any Other Device bearing an IP and connecting to NBS’ network. | Mandatory |  | |  |
| After the initial learning period, the technology must automatically provide a complete audit trail of all subnets found in the network | Mandatory |  | |  |
| The solution 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. | Mandatory |  | |  |
| The solution should have functionalities where the network's baseline must be adaptive and dynamic enough to suit any changes in the environment's behavior | Mandatory |  | |  |
| The solution should operate completely based on behavior, where technologies that make use of rules and/or signatures will not be allowed | Mandatory |  | |  |
| The solution must be able to take autonomous action to contain in-progress threats, giving the security team time to investigate and remediate as needed. The autonomous response must:  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 integrations with firewalls and/or Network Access Controls  c. this action should not rely on agents installed on different devices to perform its response,  this should not require the appliance to sit in-line but rather remain passive in the network | Mandatory |  | |  |
| It must be based on behaviour analysis, being able to highlight at least:  all unusual connectivity in the network  all unusual activities on the network  be able to do a detailed tracking of the device, indicating even its history of IPs, if it is in a DHCP scope be able to do a detailed tracking of the user indicating even all the hostnames associated to a certain credential be able to identify a significantly unusual volume of connections identify the level of rarity of a device on the network as well as the rarity level of an external site access | Mandatory |  | |  |
| The Solution Proposed must be able to automatically alert NBS to all unusual and abnormal activities on the network | Mandatory |  | |  |
| The Solution Proposed must provide simple and fast filters to enable the analysis of violations by at least Users, Devices, and type of violation. | Mandatory |  | |  |
| The Solution Proposed should have an omni-search search bar that makes it possible to search immediately for a device, IP, subnet, or network host | Mandatory |  | |  |
| The Solution Proposed must have a user interface where it can be possible to consult the complete System status including at least:  the software version, used disk space, CPU consumption and memory consumption.  the detailing of all active interfaces and respective traffic received through each of them the total bandwidth currently processed, the average bandwidth processed to date, the bandwidth recorded minimum in last 6 days and 1 previous weeks 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 | Mandatory |  | |  |
| The Solution Proposed must be able to identify new and unknown attack behaviors without making use of signatures or rules | Mandatory |  | |  |
| The Solution Proposed must be able to identify any new device inserted in the network | Mandatory |  | |  |
| The Solution Proposed must be able to automatically group devices into groups and clusters by their behavior similarity | Mandatory |  | |  |
| The Solution Proposed 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 | Mandatory |  | |  |
| The Solution Proposed 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 | Mandatory |  | |  |
| The Solution Proposed should provide an instant overview of what is happening in the organization globally | Mandatory |  | |  |
| The Solution Proposed should visually represent all network activity and connections between all machines and users (internally and externally) | Mandatory |  | |  |
| The Solution Proposed should be based on probabilistic mathematical methods, analysing, and correlating more than 300 distinct dimensions within the package:  a. creating unique modelling techniques for each user and device, as well as for the relations between them | Mandatory |  | |  |
| The Solution Proposed must be able to group the anomalies intelligently and by level of criticality | Mandatory |  | |  |
| The Solution Proposed must enable the customization and adaptation of the machine learning to specific conditions and characteristics of the network | Preferred |  | |  |
| The Solution Proposed must have LDAP integration | Mandatory |  | |  |
| The Solution Proposed 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. | Preferred |  | |  |
| As previously stated, the solution must operate on a completely agentless system via an integration through the core layer of the NBS environment, where the machine learning is utilizing mathematics and unsupervised AI without the use of rules or signatures or historical data. | Preferred |  | |  |
| NBS has a specific request that this concept must be extended to any devices that disconnect from the core layer to external environments, it must be able to do the following:  Enhance the platform’s decision-making by correlating network/cloud traffic with host events – more data/context means better detections to the agentless system.  Extend visibility to devices off the network or in heavily distributed environments (e.g. tiny branch office where a probe is not deployable)  Enable Autonomous Response at the endpoint – e.g. killing processes, which must not act as a traditional EDR or EPP where rules, signatures or historical data are used to remediate. | Preferred |  | |  |
| Must be powered by the self-learning intelligence of the physical appliance installed at the original core layer and extending this visibility to a single UI. | Mandatory |  | |  |
| The system must have a secure proxy in the DMZ that can facilitate communication between the devices behavior off the network and the appliance within the NBS core layer of the network. | Preferred |  | |  |
| The Solution Proposed must allow to import of external whitelists and blacklists | Mandatory |  | |  |
| The Proposed Solution Should Cover a minimum of 430 Devices across HQ and different Branches of NBS from Day-1 of Deployment | Mandatory |  | |  |
| The Proposed Solution should come with a minimum subscription/support period from Day-1 of Deployment. All upgrades, support, installation and configurations should come completely free from the vendor. |  |  | |  |
| External Integrations and Report |  |  | |  |
| The Solution Proposed should enable the automatic creation of executive reports covering at least one overview of:  the entire deployment summary indicating the total number of devices, total number of subnets and processed media bandwidth a summary of breaches per attack phase a devices breach summary a TOP devices summary breaching high priority conditions a summary of the most frequent breaches to main compliance items such as misuse of: USB, google drive, outbound RDP, external SQL, among others a TOP devices summary that most breaches the compliance conditions generating risk to the organization | Mandatory |  | |  |
| The Solution Proposed must have a Dynamic Threat Dashboard for a simplified overview of real-time threats that is simple and intuitive and that enables at least:  an immediate understanding of breaches with a description of what the breaches means and a recommendation for the action that could be taken  a filtering for breaches more critical as well as for devices more critical  a complete breach detailing with device data, history, tags, connections, logs, and device history  a possibility of opening a more detailed and detailed investigation of the logs and connections with the topology plotted in 3D | Mandatory |  | |  |
| The technology must have its own mobile app available in both Google Play Store and Apple Store in order to enable remote management of incidents with no further investment or costing to NBS. | Preferred |  | |  |
| The proposed Solution should have in-built Analyst Feature with AI and ML Capabilities and should minimum deliver the following:  -Fully automates threat investigations at a speed and scale that no human ever could  -Ability to create a shareable report in different supported formats with all the stake holders within the organization.  -Present a list of related breaches and alerts and have those connect to other breach devices  -Automate and triage all alerts presented through the machine learning | Preferred |  | |  |
| Architecture |  |  | |  |
| The Solution Proposed must consume and analyse raw data (raw packets) through port mirroring (SPAM) or using a TAP | Mandatory |  | |  |
| The proposed technology will not be accepted if it only uses partial analysis of the packages making use of sflow, jflow, netflow, among others, please explain how your technology can comply to this requirement. | Preferred |  | |  |
| The solution should be supplied in the form of an Appliance manufactured by the same Manufacturer as the software. Manufacturer should provide warranty on the Hardware and Software. | Mandatory |  | |  |
| Supplied hardware appliance from the Manufacturer must be capable of handling up to 5Gbps of throughput | Preferred |  | |  |
| A single hardware appliance must be supporting the analysis of up to 50,000 devices | Preferred |  | |  |
| The hardware specified must have a redundant power supply | Mandatory |  | |  |
| Support and Assistance |  |  | |  |
| The Solution Proposed must have an online portal available for client access by providing at least:  two factor authentication  Pre-scheduled periodic training sessions, without additional cost for NBS.  a complete library of solution documents, as well as specific fields where the latest product updates, release notes, and FAQs can easily be validated and  contain specific feature for the opening of support tickets, which enables fast, simple opening and case detailing. All ticket updates must be updated in the system and be forwarded via email and must have a complete call history track.  e. it must have fields of debate about Cyber Threats and publications of security experts about current questions. | Mandatory |  | |  |
| The Solution Proposed must provide helpdesk / diagnostic and remote support for issues | Mandatory |  | |  |
| General Requirements |  |  | |  |
| Bidder should submit Manufacturer Authorization Letter as part of Bid Submission | Mandatory |  | |  |
| Bidder should have minimum two resources certified on the Technology proposed to NBS please submit Valid ID Proof/Passport/Work Permit and Signed Resumes of such resources as part of Bid Submission | Mandatory |  | |  |
| Bidder should submit detailed Project Plan including all the activities of Implementation as part of Bid Submission and the Project Plan should include all the milestones for implementation of the Proposed Solution. | Mandatory |  | |  |
| **Total** | |  | |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Professional Services Details** | **Specifications in Brief** | Compliance (Yes/No) |
| 1 | System Installation | * Supply of software and licenses. * Installation of NDR Solution and Configuration of Centralized system. * Creation of Policies, Implementation, Configuration and Testing which includes configuration of scheduled scanning/ implementation of device control mechanism/ configuration of email alerts and reporting. * Training of the NDR Solution deployed along with implementation document and manual. * 24x7 Helpdesk support with trouble ticketing and tracking system. * Upgrade of patches and product version during the support period. |  |
| 2 | Instructor led Training | * Instructor led training (with training material) up to 10 NBS team members. Training could be Virtual or Onsite as directed and mutually agreed. |  |
| 3 | Services during AMC Period | * The vendor should nominate an Account Support Team with an escalation matrix for handling all issues during AMC Period. * The Account Support Team should be the single point of contact with end-to-end account ownership for all committed deliverables during AMC Period. |  |

1. **Commercial Bid for NDR Solution**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Item** | **Description** | **Cost (USD exc. VAT)** | **Required** |
|  | Software:  Perpetual License fees NDR | 430 Endpoints  Desktops - 120  Laptops - 110  Servers - (Linux & Windows) - 200 |  | Mandatory |
|  | Hardware | As sized by the vendor. Include High Availability Architecture in the design |  | Optional |
|  | Implementation and Training | Training for up to 10 people |  | Mandatory |
|  | 1st Year AMC Charges | # See notes below |  | Mandatory |
|  | 2nd Year AMC Charges | As above |  | Mandatory |
|  | 3rd year AMC Charges | As above |  | Mandatory |
|  | Other Costs | Please provide full details |  | Optional |
|  |  | **Total** |  |  |

Notes:

* The vendor should nominate an Account Support Team with an escalation matrix for handling all issues during AMC Period.
* The Account Support Team should be the single point of contact with end-to-end account ownership for all committed deliverables during AMC Period.
* Incident Management/Problem Management: Vendor should have robust problem management tool which can automatically send alert notification to their backend for early intimation and proactive handling of problems such as critical issues.
* The vendor must provide free software updates for any version upgrade for the supplied software required by NBS to support the application requirements.
* The vendor should have a system to send regular alerts to NBS team on any security alerts, product related issues, patch alerts etc.

**Reviewed & Signed By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Designation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**