



LANDBANK

SERVING
THE NATION

**SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-HOBAC-ITB-CS-20220802-01**

PROJECT : **Supply, Delivery, Installation and Configuration of Network Detection and Response (NDR) Solution with Three (3) Years Support Services**

IMPLEMENTOR : **HOBAC Secretariat**

DATE : **September 29, 2022**

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

- 1) The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.
- 2) The Terms of Reference (Annexes D-1 to D-14), Technical Specifications (Section VII), List of LANDBANK Officers, Employees and Consultants (Annex F) and Checklist of Bidding Documents (Item 12 of Technical Documents, and Item 18 of Other Documents to Support Compliance with Technical Specifications) have been revised. Please see attached Annexes D-1 to D-14 and F, and specific sections of the Bidding Documents.
- 3) Responses to bidders' clarifications/queries (Annex G-1 to G-6).
- 4) The submission and opening of bids is re-scheduled on **October 7, 2022** at 10:00 A.M. through videoconferencing using Microsoft (MS) Teams.


ATTY. HONORIO T. DIAZ, JR.
Head, HOBAC Secretariat

Technical Specifications

Specifications	Statement of Compliance
<p>Supply, Delivery, Installation and Configuration of Network Detection and Response (NDR) Solution with Three (3) Years Support and Services</p> <ol style="list-style-type: none">1. Minimum technical specifications and other requirements per attached Revised Annexes D-1 to D-14.2. The documentary requirements enumerated in Revised Annex D-13 and D-14 of the Terms of Reference shall be submitted in support of the compliance of the Bid to the technical specifications and other requirements. <p>Non-submission of the above documents may result in the post-disqualification of the bidder.</p>	<p>Bidders must state below either “Comply” or “Not Comply” against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered.</p> <p>Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer’s un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.</p> <p>Please state here either “Comply” or “Not Comply”</p>

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position

Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Components (PDF File)

- *The Eligibility and Technical Component shall contain documents sequentially arranged as follows:*

- **Eligibility Documents – Class “A”**

Legal Eligibility Documents

1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);

Technical Eligibility Documents

2. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).
3. Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).
4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar to the contract to be bid within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

Financial Eligibility Documents

5. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized

institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

6. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

○ **Eligibility Documents – Class “B”**

7. Duly signed valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.
8. For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos, Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder.

○ **Technical Documents**

10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
11. Section VI – Schedule of Requirements with signature of bidder's authorized representative.
12. **Section VII – Revised Specifications with response on compliance and signature of bidder's authorized representative.**
13. Duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

Note: During the opening of the first bid envelopes (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary "pass/fail" criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.

- **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**
 14. Manufacturer's authorization (sample form - Form No. 9) or its equivalent document, confirming that the bidder is authorized to provide the product/ solution supplied by the manufacturer, including any warranty obligations and after sales support as may be required.
 15. Notarized Certification that bidder has at least five (5) years existence in the IT industry with reference to SEC Registration document.
 16. Certificate of Employment, Curriculum Vitae, Training Certificates and Valid Certifications of at least three (3) locally based technical engineers for the solutions/brand being offered.
 17. Certificate of Employment and Curriculum Vitae of the dedicated Project Manager to be assigned in the project with at least 3 years experience and handled at least 1 Commercial or Universal bank and 1 non-bank client.
 18. **List of at least one (1) installed based of the same brand being offered in a Philippine Commercial or Universal bank with name of client/bank, contact person, contact number, address and email address.**
 19. Detailed Escalation and Support Plan Procedure.
 20. List of manufacturer's local sales and technical office in the Philippines with address, contact person and contact number.
 21. Certification or product data sheet that the product being offered is in the Gartner's Network Detection and Response (NDR) Market Guide.
 22. Certification or product data sheet that the product being offered is included and listed in the top-right corner of the latest EMA Radar for Network-based Security Analytics.
- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**

24. Business Tax Returns per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.
25. Latest Income Tax Return filed manually or through EFPS.
26. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
27. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
28. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

Financial Component (PDF File)

- ***The Financial Component shall contain documents sequentially arranged as follows:***
 1. Duly filled out Bid Form signed by the Bidder's authorized representative (sample form - Form No.1).
 2. Duly filled out Schedule of Prices signed by the Bidder's authorized representative (sample form - Form No.2).
 3. Duly filled-out Bill of Quantities Forms signed by the Bidder's authorized representative (Annex E).

Note: The forms attached to the Bidding Documents may be reproduced or reformatted provided the information required in the original forms and other requirements like signatures, if applicable, are complied with in the submittal.

September 22, 2022

**Supply, Delivery, Installation and Configuration of Network Detection and Response (NDR)
Solution Term of Reference**

Objective: To provide real-time visibility, perform real-time analysis, automatically discover and classify key events in the entire network. Detects suspicious events and automatically investigate using threat intelligence capabilities for both north-south and east-west traffic flows.

	Technical Specifications	Comply
Deployment and Architecture		
1	The propose solution must be a Hardware or Virtual Appliance deployed on-premise at the LANDBANK Head Office	
2	Virtual appliances should have exact same functionalities and software versions as the physical appliances	
3	The solution must support a hardware and virtual deployment including KVM, VMware ESXi and Hyper-V. Hardware appliances should be performant, support growth yet efficient and minimal in size.	
4	The solution must support for central deployment of physical and virtual sensors.	
5	The solution must be passive, and not introduce latency to the network and minimise risk or impact on deployment to existing services and applications.	
6	The solution must primarily leverage raw network traffic capture and extraction of metadata as its primary data source across hybrid, cloud and IoT, complemented with third party telemetry and logs for enrichment, additional context.	
7	The solution must have a capability to support virtual and/or physical appliances that range from 1Gbps to 100Gbps in a single virtual/physical form factor	
8	Support modern Switch Port Analyzer (SPAN) capabilities such as Encapsulated Remote Switch Port Analyzer (ERSPAN) and Remote Switch Port Analyzer (RSPAN) so that one does not need to deploy an appliance or probe at every physical hypervisor server or individual Leaf Switches for visibility	
9	The NDR platform must provide the same visibility regardless of on-premise, private cloud, or public cloud deployments.	
10	Must be deployed agentless as well as no dependencies for external logs and should be self-sufficient and NOT a module or add-on to a dependent component (e.g. SIEM, Firewall, EDR/XDR platform)	
11	Must not require the configurations of network devices to generate NetFlow-type data.	
12	Must provide and correlate Layer 2 to 7 real-time security analytics without reliance on protocol parsing of written-to-disk packet captures	
13	Must have a real-time analytics and alerting and must be deployed with a single virtual or physical appliance.	

14	Must have an all management, dashboard, reporting and traffic analysis should be performed through an individual centralized web console.	
15	The platform must be able to analyze: - All TCP & UDP traffic - extract and display any Layer 2 to 7 metrics, including from the payload, in real-time - The proposed maximum throughput, must be sustained 24x7 continuously for at least a month and able to store all collected metrics within the single platform.	
16	The NDR platform must provide the same visibility regardless of on-premise, private cloud, or public cloud deployments.	
17	Must be able to Auto-Detect & Discover all devices; automatically begin monitoring their protocol communication out of the box.	
18	Cloud Deployment offerings must include Amazon Web Services, Microsoft Azure, and Google Cloud Platform	
19	Platform must be able to centrally manage visibility across any of the aforementioned hybrid and multi-cloud deployments and must be capable of detecting threats in the cloud control plane such as, but not limited to: - Amazon Web Service (AWS): - Across Microsoft Azure - Google Computing Cloud	
20	Must be able to Detect & Discover and monitor the communication interrelationships by port and protocol between devices and/servers.	
21	Must be able to provide an asset list of all discovered devices and allow for ad-hoc drill-downs into each device for historical and real-time analytics (regardless if there are any detections)	
22	Must be able to auto-classify and auto-group servers and clients based on behaviour: such as Web, Domain Name Server (DNS), Storage, LDAP, VoIP Phones, etc. to prioritize critical assets and be dynamically updated	
23	Should leverage Machine Learning to auto-detect "High Value Assets" within the dynamic environment	
24	Should not need to rely on pre-configured static configurations of list of IP addresses or IP and Port mappings for logical device groupings	
25	Able to provide an auto-classified or user-defined device groups that can be reported, alerted, and drilled-down into	
26	Alerting should have basic threshold-based capabilities as well as sophisticated anomalous detections based on unsupervised machine learning and statistical trending.	
27	Detection notifications should have built-in email capabilities as well as template webhooks to common systems such as: Slack, Microsoft Teams, Google Chat, etc.	
28	Proposed solution must have a self-maintained datastore for historical metrics and configurations. Data should be collected on monitored assets regardless if a detection has fired and should allow direct access to datastore via APIs	
29	In multi-appliance and hybrid-cloud environments, individual appliances should be able to be rolled up and seen in a single pane of glass on a centralized monitoring console	
30	Must have a software base Centralized monitoring console with no additional costs. Centralized console should be able to push configurations, perform firmware software updates, and periodic report generations.	
31	Proposed solution should place no restrictions on monitoring of unlimited number of concurrent users being monitored	
32	The proposed solution should be able to store the network transaction record to support forensics investigations with purpose built hardware and expansion storage.	

33	The solution must be capable of identifying threats in encrypted traffic and able to decrypt them to provide L7 visibility and detection	
34	The solution must be flexible, scalable and provide enterprise-wide threat detection and response across all hosts, without technical platform limitation.	
35	The solution must have the ability to automatically update. To reduce the operational burden of the solution, software updates must be an automated process that doesn't require any human intervention.	
36	Software system should be updated with a regular frequency to adapt to the constantly evolving threat landscape.	
37	Must be able to alert on individual threats or suspicious hosts via email and syslog	
38	Must provide granular role-based access control (RBAC) into the various elements of the product so security analysts can define custom roles with limited access if desired	
39	Must have the ability to send audit log over syslog for actions such as login, logout and changes to settings that impact the security posture of the product	
40	Proposed solution should have the option to include 24/7 MDR (Managed Detection and Response) service delivered by the solution provider.	
41	The solution must prioritise critical and high-risk hosts to drive analyst focus, minimise noise and improve time to detect and respond.	
42	The solution must identify hosts and accounts impacted by a particular attack campaign allowing analysts to identify all affected hosts and account to understand source of origin (patient zero) and sequence of events.	
Security Analytics and Detection Capabilities		
43	Must be able to provide visibility into advanced threats for both north-south and east-west traffic flows to augment existing security tools that focus on threat signatures and perimeter security,	
44	Must leverage unsupervised machine learning for security anomaly detection	
45	As Machine Learning becomes exponentially more effective with more data - ML must be able to leverage a wealth of data locally (depth & scale of traffic locally) and globally (crowd-sourced)	
46	Machine Learning must leverage a continuous development and delivery model	
47	Proposed solution must be able to detect Command & Control activities such as: suspicious outbound activity, suspicious IPs/URIs, suspicious connections (e.g. DNS/SSH tunneling), abnormal geolocation.	
48	Proposed solution must be able to detect Reconnaissance activities such as: port scans, user enumeration, login attempts, reverse DNS lookups, DNS zone transfers, Web Scans, SSL Scans, etc.	
49	Proposed solution must be able to detect Exploitation activities such as: LLMNR poisoning, IP Fragmentation Overlap, RDP Brute Force, Drupal Exploitation, Suspicious File Activity: Brute force, Enumeration, Kerberos Brute force, NET-NS Poisoning, etc.	
50	Proposed solution must be able to detect Lateral Movement activities such as: Suspicious RDP/SSH, Peer Group Anomalies, Share & File Access, Transaction Failures, Network Privilege Escalation, PSEXEC Activities, WMI Activities, WSMAN Activities, etc.	
51	Proposed solution must be able to detect Action on Objectives activities such as: Sensitive Data, Encrypted Data, External Data Transfer, Database Exfiltration, Ransomware, Cryptocurrency Mining	
52	Must have Machine Learning detection capabilities to track and learn behavioural profiling of Internet of Things (IoT) devices & models	

53	Must be able to detect Unusual Internet of Things (IoT) Protocol activity based on unusual traffic for a specific IoT make and model.	
54	Must understand application-level details (SQL statements, usernames, database tables, DB error messages, etc.) on common database such as: MS-SQL, Oracle, DB2, Informix, Sybase, MongoDB.	
55	Must be able to detect attacks like Database Enumeration, Rare Database Table access, Database Takeover attack, etc.	
56	Proposed solution must allow users to flexibly develop their own unique custom detections to fulfill specific security detection requirements. These detections should be able to easily leverage a protocol API to access relevant application metadata such as Source/Destination IPs, Hostnames, URIs, User-Agents, SQL Statements, SessionIDs, Filenames, HTTP/DB/NAS method, Error Codes, Request Types, and any other specific metadata in a request or response network packet. Custom Detectors should not be limited to any existing built-in models	
57	For usability, detections that are deemed by a human analyst to be irrelevant, there should be the ability to hide the detection (and set a policy to also hide historical and future detections) based on the Type of Detection, Offender (such as a Vulnerability Scanner), Victim, and other potential relevant detection properties	
58	Must provide in-GUI MITRE ATT&CK Framework alignment. Visualizations must have a mapping of MITRE TTP's that can be detected by the NDR as well as the observed MITRE TTP's currently seen in environment. The MITRE TTP detectors should be searchable based on category, type, and technique	
59	Proposed solution must be able to track the following activities: <ul style="list-style-type: none"> - Behavioral Analytics - Privileged user logins - e.g.: database user accessing via root or sa ; LDAP/Radius logins - Unauthorized connections - Lateral network traversal - Brute force attacks - Scan Detection - Active Directory Monitoring - Storage/DB access - Fraudulent transactions - Large data transfers - Identify potential sources of data exfiltration (FTP, DNS tunneling, SSH, storage) - Detect Anomalous DHCP or Web Proxy Auto Discovery activities 	
60	Allow security operations and security analysts to focus on cyber kill chain activities that require greater attention allowing for more timely response. Detections should be categorized under common Kill Chain steps such as Command and Control, Reconnaissance, Exploitation, Lateral Movement, Data Exfiltration, etc.	
61	Solution needs to be able to integrate with external threat intelligence feeds for additional context to malicious IPs, threat actor techniques, and other indicators of compromise.	
62	Solution should provide an existing and periodically updated, curated list of Threat Intelligence out of the box	
63	Must support ingesting Structured Threat Information eXpression (STIX) format for standardizing, conveying, and sharing data about cyber threat intelligence data.	
64	Must be able to auto-categorize high value assets based on the behaviors discovered devices play (e.g. Database Server, Authentication Server, DNS, Web Server, Storage, etc.)	

	Auto-prioritize what's important in the environment and apply extra scrutiny to your most valuable assets	
65	Proposed solution should not just be detection anomalous behaviours but providing constant auditing and reporting of Security Hygiene: <ul style="list-style-type: none"> - Certificate expiration - passively identify soon to expire, or already expired certificates that are still being actively accessed. - Insufficient Key length - detect insecure key lengths - Weak Cipher Suites - RC4, DES, 3DES, Null, IDEA, etc. - Outdated SSL sessions - auditing for insecure SSL sessions that use SSLv3, TLSv1.0 - MD5/SHA-1 cert signing - detect vulnerable certificate signing - SSL traffic by port - Email encryption detection - Wild card certificates - detect potential eavesdropping and impersonation attacks - Long-lived Certificates - detect certificates that have unreasonable expirations that are vulnerable 	
66	Must have a Real-time and historical metrics for monitoring Active Directory including services such as: User Accounts, Computer Accounts, DNS, LDAP, Global Catalog, and Group Policy loads. <ul style="list-style-type: none"> - Invalid Passwords - Account Lockouts - Disabled Accounts - Expired Password - Policy Errors - Privileged Accounts tracking - Kerberos Tracking: Time Skew Errors, Unknown SPN, Duplicate Tickets, Suspected Golden Tickets - Active Directory metrics must be retained for at least a month - Must have the ability to decrypt AD-encrypted traffic to detect attacks such as a Golden Ticket Attack 	
67	Proposed solution must be able to detect in real-time ransomware activities	
68	Proposed solution must be able to detect Common Vulnerabilities and Exposures (CVE), including: Windows 10 SMBv3 Exploit, Zerologon, Windows TCP/IP Stack Exploit, Windows DNS Server Exploit, Windows 10 SMBv3 Exploits, Windows Print Spooler Exploit, etc.	
69	Proposed solution must have ability to automatically update new ransomware definitions, TOR nodes, device software/models, public DNS servers, malicious C2/botnet IP addresses)	
70	Proposed solution must have official and proven integrations with established firewall, EDR, and SIEM vendors	
71	Allow for automated intelligent firewall and Network Access Control (NAC) actions with native REST API integration	
72	Native integration of detections and raw data to external SIEM NDRs for correlation and forensic investigation.	
73	Integration with Security Orchestration and Automation Response (SOAR) vendors	
74	Integration with Ticketing and Case Management Systems	
75	The proposed solution should not store any data in any cloud rather all the data should be stored on-premises	
76	The proposed solution must provide an integrated visibility of hosts and accounts and detection and response capability across networks and cloud.	

77	The proposed solution must be capable of identifying threats in encrypted traffic without requiring, relying on decryption.	
78	The proposed solution must provide real-time 24/7 monitoring and detection.	
79	The proposed solution must be flexible, scalable and provide enterprise-wide threat detection and response across all hosts, without technical platform limitation.	
80	The proposed solution must provide an integrated visibility of hosts and accounts and detection and response capability across networks and cloud.	
81	The proposed solution must be capable of early-stage threat detection.	
82	The proposed solution must have an efficient architecture of headend and sensors and inter-component communication across multiple networks be it on-premise and cloud, must not introduce unnecessary and excessive load on bandwidth or hidden costs.	
83	The proposed solution must be capable of detecting attacker behaviours and equally capable of identifying potential malicious activity and compromise based on context and observed behaviour across hosts, accounts and services.	
84	The proposed solution must be able to provide anomaly detection with user accounts, and be capable of detecting misuse of privileged accounts e.g., has the user account been used in unexpected ways on other devices, or using services on hosts it normally does not use?	
85	The proposed solution must be easy to manage and operate, and limit ongoing overhead. Configuration and management must occur centrally and distributed automatically across all solution components.	
86	The proposed solution must provide detection filter function including AI generated filter recommendations. The filtered detection should not add to the detection score	
87	The proposed solution must aggregate individual detections at a host-level and account-level, and prioritise based on threat and certainty.	
88	The proposed solution must map detections to the kill chain and MITRE ATT&CK framework.	
89	The proposed solution's machine learning must leverage unsupervised, supervised and deep learning algorithms and provide broad coverage for attacker behaviours such as command and control, hidden tunnels, reconnaissance, lateral movement, and data gathered and exfiltration, and capable of providing visibility in early stages of an attack. The Machine learning algorithms must be updated frequently, and new algorithms must be released on a regular basis.	
90	The proposed solution must be capable of identifying and tracking hosts, including when connecting over VPN, and how attackers moved laterally and what other hosts are affected building out a campaign view, and overlay this with a unique view of the relationship and notion of observed privilege between hosts, accounts and services used.	
91	The proposed solution's Machine Learning algorithms must be capable of triggering detections immediately in a new environment and its detections capability must not rely on a learning period.	
92	The proposed solution must provide AI-derived high-fidelity security-enriched metadata that can be streamed to a SIEM and/or data lake and correlate with other data sources to allow for deeper conclusive incident investigation, threat hunting and proactive search.	
93	The proposed solution's security-enriched metadata must be searchable for events of interest and novelties e.g., beacons, ingress and egress traffic on services and protocols of interest, data gathered prior exfiltration, hosts contacted by the same command-and-control IP address, other accounts and hosts that may be implicated.	
94	The proposed solution must aggregate individual alerts into incidents with intelligent PCAP technology for forensic investigation.	

95	The proposed solution must provide advanced threat detection in Office 365 allowing for the detection of account-based attacks and behaviours including account takeover, compromise of credentials, discovery, lateral movement that traverses from SaaS to IaaS and on-premise.	
96	The proposed solution should be able to support Detections for Azure Active Directory	
97	The proposed solution should have a machine learning capabilities in the cloud.	
98	The proposed solution should have (a) supervised and (b) unsupervised machine learning	
99	The proposed solution must store detections and PCAP's on box for a period of no less than 3 months	
Investigative Analysis Capabilities and Usability		
100	Must be able to provide Automated Weekly Executive Report such as: <ul style="list-style-type: none"> - Summary of the number of detections - Highest Risk Scores - Details on Devices and Assets: Active, New devices - Network Hygiene Health Indicators (Expired Certificates, Self-Signed Certificates, Insecure SSL/TLS sessions, etc.) - Breakdown of Detections by Device Role - Breakdown of Detections by Killchain - Top Offenders - Summary of Top Risk Score detections observed 	
101	Proposed solution must be able to provide details on recent high-profile vulnerabilities and exploits and relate this to existing environment for potential vulnerabilities, attack surface, or past breaches that may have already occurred.	
102	Ability to auto-update in GUI on recent high-profile vulnerabilities and exploits	
103	Ability to correlate such recent vulnerabilities/exploits with actual observed traffic in environment: retrospective analysis of historical data and real-time detection of potential threats and IOCs.	
104	Customised reports should be supported with the ability to create and customise via easy to use drag-and-drop workflows. There should be no need for customised services to build any pull data from backend databases for basic reporting	
105	Proposed solution must have a high-level executive summary of detections detected, providing information on: <ul style="list-style-type: none"> - Breakdown of Detections by Killchain Category - Breakdown of Detections based on Critical Assets - Highlighting the top risk score detections - Top Detections by Frequency 	
106	Proposed solution must have a high-level executive summary of North/South traffic, providing information on: <ul style="list-style-type: none"> - Suspicious Inbound and Outbound connections based on Threat Intelligence - Clean and dense volumetric visualizations of suspected Exfiltration and Command & Control activities - Clean visualisations of outbound traffic by Country and Cloud Services 	
107	One-click drill-down to forensic artifacts such as meta-data details and transactions of a fired detection	
108	Automated investigation should provide the following details: <ul style="list-style-type: none"> - Automatic timeline campaign of correlated events (based on identical offender / victim) - Proper context into the relevant forensic artifacts based on the detection (relevant filenames, usernames, parameters, URLs, Database Transactions, etc.) - Contextual drilldowns into transaction records and raw packets 	

109	Proposed solution must be able to assign detections to different users of the NDR	
110	Must be also able to export individual detection incidents into PDF	
111	The proposed solution must provide context and details on detections: - Recommended context-driven investigative steps with logical drilldown views - Short Description and Explanation of Attack - Context to Risk Factors: Likelihood, Complexity, Business Impact	
112	Native capability to track the status of a detector, annotate the detection findings, and assign detections to other SOC analysts without integrating with any external ticketing systems	
113	Ability to add and view multiple detections into a single timeline and visual map to help with grouping detections into a larger attack campaign.	
114	Must have the ability to add SOC analyst's investigation notes as an annotation	
115	The proposed solution must be able to drill-down to individual devices and understand: - Layer 7 dashboards and metrics for the device's role as a client and/or server - Automatic OS Fingerprinting without integrations with 3rd party solutions - Automatic listing of Logged in Users, this Device to User Mapping should be accomplished without explicit integrations with DHCP/LDAP/AD - Automatic classification of device role based on behavior observed by device (e.g. Domain Controller, Proxy, Web Server, Storage, DNS, Database Server) - Ability to view 'Similar Devices' in the environment as determined by Machine Learning	
116	Instant mapping of which user(s) are logged into a specific device	
117	Quick visual with mapping which specific devices a single user has logged into User to Device mapping should be correlated automatically without requiring integrations with LDAP/AD/DHCP servers	
118	Must be able to create custom rules based on various factors for dynamic device grouping. Criteria must include: DNS/NetBIOS/CDP/DHCP Name, IP Address, Vendor (F5, IBM, Apple, HP, Oracle, VMware, etc.) , Device Role (mobile device, database, DHCP, web, etc.), Discovery Time	
119	For deep and rapid forensic investigation and analytics - must have capability to record and index all detailed transaction information (web, database, DNS, Citrix, etc.) in a structured, searchable, filterable interface, using an integrated big data NDR without any sampling	
120	Big data solution should not require complex scripting and querying language to attain desired views.	
121	Demonstrate the ability to look up a specific user ID, isolate that user's traffic and follow it through the infrastructure to perform detailed 360 degrees investigation. This investigation should not be dependent on whether a relevant detection has been fired.	
122	Demonstrate ability to leverage Global Search to find a specific client IP, identify all network/application traffic associated with that IP (either through Application records or unique FlowID search) to perform detailed 360 degrees investigation. This investigation should not be dependent on whether a relevant detection has been fired.	
123	Demonstrate ability to create a custom record format include custom application data records	
125	Capability of automatically generated maps showing relationships and dependencies between systems, servers, and applications without any pre-configurations or step-through validation	
126	Activity Maps must have a visualize live traffic activity with indications of directional traffic flow and volume of traffic allowing for drill-down into individual devices and transaction records	

126	Capability to provide a graphical real-time geographic world map of any inbound OR outbound connectivity - configurable for any protocol metric: HTTP, FTP, DNS, Database, etc.	
127	Built-in flexible comparison of activity over different time intervals, by minutes, hours, days, weeks, months and years, for rapid analysis, trending, and baselining.	
128	Built-in and custom Dashboards should allow for customizable and descriptive "playbooks" to interpret dashboard visualizations and metrics to a novice user.	
129	Proposed solution must include the ability to collect and store layer 2 to 7 and any custom defined payload metrics, for rapid retrieval, for a minimum of 1 year.	
130	Proposed solution must allow the writing and storing of metrics to an external storage device for extended historical lookback and NOT be limited by the hard disk capacity provided by solution. This should not be confused with a backup & restore capability, but a datastore extension into external storage capability.	
131	Demonstrate ability to store detailed flow records for historical lookback	
132	Full IPv6 support for both management IP as well as all types of monitored traffic (HTTP, DB, DNS, etc.)	
133	Proposed solution must allow the capability for human analysts to perform an unbiased analysis and identify improvement areas in the IT infrastructure. Deliverables include periodic (e.g. monthly, quarterly) reports with specific security findings and recommendations.	
134	The proposed solution must be able to provide a simple and extensible means to rapidly define custom user-defined metrics of desired data in application headers or payloads.	
Traffic Performance Capabilities		
135	Availability of a NDR that can analyze traffic for real-time extraction of layer 2 to 7 and payload metrics, up to 100 Gbps continuous sustained throughput of analysis on a single appliance.	
136	Availability of a NDR that can analyze traffic for real-time extraction of layer 2 to 7 and payload metrics, up to 10 million packets per second continuous sustained throughput of analysis on a single appliance.	
137	Physical Appliances should have a dedicated SSL/TLS decryption chipset to handle high volume processing of SSL traffic loads	
138	Must have a Perfect Forward Secrecy (PFS) mode of encryption whereby session keys are not negotiated over the wire (contrast with traditional RSA key exchange), solution must have some capabilities to perform real-time decryptions in a Perfect Forward Secrecy encrypted environment (e.g. TLS 1.3 with Diffie-Hellman key exchange).	
139	PFS Decryption technique must allow for both software key forwarder approach as well as Load Balancer integration techniques	
140	PFS Decryption must not require intermediate Man-in-the-Middle type of solutions to perform decryption and shall use out-of-band decryption techniques	
141	Ability to decrypt NTLM and Kerberos-encrypted traffic in order to detect potential attacks that cannot be accurately detected when encrypted: SMBv3.0 exploits such as Ransomware and PrintNightmare, Kerberos Golden Ticket, WMI/RPC lateral movement launches/exploits.	

Network Layer	
142	Monitor Layer 2,3 and 4 protocols out of the box
143	Support for Network Virtualization using Generic Routing Encapsulation (NVGRE), Virtual Extensible Local Area Network (VXLAN), Multi Protocol Label Switching (MPLS), TRILL, Cisco FabricPath, Transparent Ethernet Bridging traffic network decapsulation
144	Provide real-time metrics for dashboarding, alerting, and historical reporting: - L2 frame sizes especially the detection of JUMBO frames - Detect devices that use different L2 frame types like ipv4, ipv6, ARP, IPX, STP, MPLS, LACP - L2 Metrics must be retained for at least a month
145	Provide real-time metrics for dashboarding, alerting, and historical reporting: - Determine L3 protocols being utilized: ICMP, ICMP6, TCP, UDP - Determine packets/bytes sent differentiated by DSCP markers to validate QoS configurations - Must have full support for analyzing all IPv6 traffic for real-time analysis - parity in capabilities as IPv4 traffic (regardless of application payload type) - L3 Metrics must be retained for at least a month
146	Provide real-time metrics for dashboarding, alerting, and historical reporting: - TCP Connections, Aborts, Resets, Timeouts due to retransmissions Zero Windows, Nagle's Delay, Out of Order packets - L4 TCP Metrics mentioned above must be retained for at least a month
147	Must be able to analyze over 50 network protocols in order to get deep-level analytics to be fed into Machine Learning anomaly detection
148	Automatically identify and analyze all HTTP based traffic. HTTP stats, errors and performance as related to target environments. Including decrypting SSL encrypted HTTP traffic.
149	Provide real-time metrics for dashboarding, alerting, and historical reporting: HTTP 3XX/4XX/5XX response codes, and their corresponding URIs/clients and server IP
150	Provide real-time metrics for dashboarding, alerting, and historical reporting: - Determine the slowest running HTTP requests - Indication of HTTP service abuse by tracking: server processing, request, response delays - Detect HTTP requests that have been aborted and not completely finished - Determine which individual HTTP objects (js,gif,jpg,css,html,etc.) being requested the most often and/or abused - All HTTP Metrics must be retained for at least a month
151	Provide real-time metrics for dashboarding, alerting, and historical reporting: - Record all GET/POST/PUT/HEAD transactions and their corresponding URIs, clients, and server IP
152	Create custom real-time metrics based on customizable conditions such as URI, response time, response size, payload content, cookies and referrer etc. *Custom web Metrics must be retained for at least a month
153	Monitor database protocols out of the box at Layer-7 (application) level such as but not limited to: *Oracle *Microsoft SQL *MongoDB *DB2 *Sybase & Sybase IQ *REDIS *Postgres

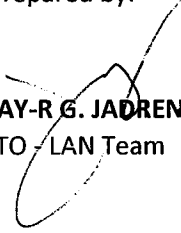
	<p>*Informix *MySQL</p> <p>Provide: real-time SQL statements, stats, errors and performance as relates to database traffic.</p>	
154	<p>Provide real-time metrics for dashboarding, alerting, and historical reporting SQL methods/procedures.</p> <ul style="list-style-type: none"> - Detection and record trail of user activities e.g. LOGIN attempts, DROP TABLES, SELECT , INSERT statements 	
155	<p>Provide real-time metrics for dashboarding, alerting, and historical reporting of all DB errors observed (at-least a month retention of errors)</p>	
156	<p>Real-time metrics for dashboarding, alerting, and historical reporting of DNS traffic. Ability to monitor:</p> <ul style="list-style-type: none"> - DNS Security issues (NXDomain attack, Malware utilizing Domain-Generation Algorithms, Data Exfiltration using TCP/IP Tunneling via DNS, irregular Web Proxy auto-discoveries) - DNS performance issues that may indicate abuse (long response times, time outs, excessive requests, etc.) - DNS Configuration issues (IPv6 DNS misconfiguration, DNS errors, etc.) - DNS Metrics must be retained for at least a month 	
157	<p>Real-time metrics for dashboarding, alerting, and historical reporting of network-based Storage (CIFS/NFS) traffic. Show impact of transport performance (network) on Storage performance. Also show important security elements such as files accessed by users and deleted files.</p> <ul style="list-style-type: none"> - Ability to detect login usernames accessing files. - Ability to detect real-time storage errors (permissions, locked files, etc.) - Ability to detect filenames that are accessed - Ability to detect vulnerable SMBv1 directories - Storage Metrics mentioned must be retained for at least a month 	
158	<p>Real-time metrics for dashboarding, alerting, and historical reporting of SMTP and POP3 traffic such as sender/recipient addresses, processing time, errors, SMTP/POP3 response/status codes.</p> <ul style="list-style-type: none"> - Email Metrics must be retained for at least a month 	
159	<p>Provide real-time metrics for dashboarding, alerting, and historical reporting for all of the following protocols -</p> <p>LDAP Kerberos RADIUS DIAMETER</p> <p>*Login failures, errors, usernames, processing time, status codes. etc. *Authentication and authorization metrics must be retained at least a month</p>	
160	<p>Real-time metrics for dashboarding, alerting, and historical reporting of Websocket traffic: # of messages transmitted & received, WebSocket buffer data, successful upgrades, status codes, etc.</p> <p>*Websocket metrics must be retained for at least a month</p>	
	<p>Real-time metrics for dashboarding, alerting, and historical reporting of protocols such as but not limited to :</p> <ul style="list-style-type: none"> -Extensive Markup Language (XML) -Simple Object Access Protocol (SOAP) -Apache Jserv Protocol (AJP) 	
161	<p>Must have a real-time metrics for dashboarding, alerting, and historical reporting of both Signaling and Voice traffic: MoS Scores, Packet Drops, Duplicate Packets, Jitter, Out-of-Order Messages, R-Factor, CallID, Latencies, bandwidth consumption, and QoS Markings for proper prioritization of latency-sensitive Voice calls.</p>	

162	Call Detail Record (CDR) inclusive of MoS Scores, DSCP (QoS) Markings, and any associated network performance issues such as high latency, retransmission timeouts, windowing, etc.	
163	Real-time metrics for dashboard, alerting, and historical reporting for Remote Desktop Protocol (RDP): sessions, sessions by client, sessions by server, etc.	
164	Real-time metrics for dashboard, alerting, and historical reporting for Remote Frame Buffer Protocol (RFB) leveraged in VNC deployments: opens, sessions, sessions by client, sessions by server, session duration, error messages, unknown authentication, etc.	
Integration Features		
165	The solution must support a native (UI-based) and API integrations with a broad ecosystem of network, security and cloud technologies.	
166	The solution must have off the shelf available Splunk applications for its Incident Detector and Response as well as Threat Hunting applications.	
167	The solution must integrate with threat intelligence feeds (commercial, industry specific or internal)	
168	The solution must be capable of integrating with endpoint and identity solutions such as Active Directory to increase host coverage in remote work scenarios and support an identity focused, Zero Trust security strategy.	
169	The solution must have integrations with Gartner leading solution for SIEM, NGFW. The response should explain how this is achieved? E.g., native API or custom scripts.	
170	The solution must integrate with leading EDR solutions for the purpose of identifying endpoints connected to the corporate VPN.	
171	All Integrations are configured and managed centrally	
Response, Enforcement Requirements		
172	The solution must integrate seamlessly into existing detection, alerting and incident response workflow.	
173	The solution must have a built-in response capability either manual or automated, and that is enterprise grade reliable and functions on assets both on premise and in cloud.	
174	The solution must have broad integrations with third party technologies to provide a block or contain response to ongoing attacks.	
175	The solution must have a strong integration with Active Directory and allow for either a manual or automated disabling, lockdown of accounts in the platform's UI.	
176	The solution must have a native, UI-based two-way integration with leading EDR technology vendors that allows for manual or automated host blocking. The solution must have a native, UI-based two-way integration with leading EDR technology vendors that allows for manual or automated host blocking such as Sentinel1, CrowdStrike, Cyberreason, FireEye, CarbonBlack	
177	The solution must have native, UI or API based response capability with leading NGFW, please explain how the solution can respond? i.e., block via global blacklist	
178	(a) The solution must have native, UI or API based response capability with leading SIEM, please explain how the solution can respond? i.e., provide details on tuning within the SIEM and enrich metadata with host ID tracking. (b) Information sent to SIEM should be in industry standard Zeek/Bro format	

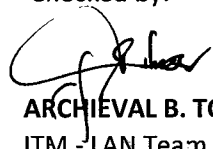
179	The solution must have native, UI or API based response capability with leading SOAR, please explain how the solution can respond? Do you have native playbooks available?	
180	Integration should be using REST APIs and Python and not using javascripts etc	
181	The solution must have native, UI or API based response capability with leading NAC, please explain how the solution can respond? i.e., move a host into a quarantine VLAN.	
Supplier's Eligibility Requirements		
182	The supplier must be at least five (5) Years of existence in the IT Industry. Information should be based from SEC (Security and Exchange Commission) incorporation information, that the vendor is at least five (5) years. The bidder must submit a notarize certification from them with reference to SEC documents.	
183	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.	
184	The supplier must have at least three (3) certified local engineers of the solution provided to support the installations, configurations and 24x7 uptime series within the warranty period. Must submit Certificate of employment and Resume/Curriculum Vitae (that the local IT support engineers has at-least 3 years work experience in handling of the product being offered or other related products, include list of trainings, unexpired certification and seminars attended)	
185	The supplier must have a dedicated Project Manager (PM) to oversee the project. Must submit Certificate of Employment and Resume/Curriculum Vitae (that the PM has at-least 3 years work experience and handled at least One (1) Commercial or Universal bank and one (1) non-bank clients as proof of his/her experience or how to handle projects.)	
186	The Manufacturer's must have local sales and technical office in the Philippines for guaranteed support. Bidder must submit the Manufacturer's address, contact number, and contact person	
187	The supplier must have of at least one (1) installed based of the same brand being offered in the Philippines (universal/commercial bank or financial institution) . Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed.	
188	The Bidder must have a local Helpdesk to provide 24 x 7 technical assistance. The Bidders must submit the escalation procedure and support plan flow chart/details.	
189	The Bidder must provide knowledge transfer training for at-least five (5) LBP IT personnel	
190	Three (3) years warranty on hardware and software. Warranty shall also cover any reconfiguration/integration after successful implementation. (The warranty certificate will be submitted by the winning bidder)	
Other Requirements		
191	The Winning Bidder must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank internal audit and external audit such as Bangko Sentral ng Pilipinas (BSP), Commission on Audit (COA), etc. Must submit [e.g. Latest Financial Statement (FS), Business Continuity Plan (BCP) that are related to the Bank, and List of Updated Technical Support (include name, contact numbers and email address), etc]	
192	The product being offered must be in the Gartner's Network Detection and Response (NDR) Market Guide. Must provide certification or product data sheet	

193	The product being offered must be included and listed in the top-right corner of the latest EMA Radar for Network-based Security Analytics. Must provide certification or product data sheet.	
Delivery Terms and Condition		
194	Delivery after receipt of NTP: 60 calendar days	
194	Installation will start 7 calendar days after delivery and will end 90 calendar days after	

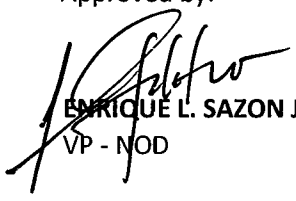
Prepared by:


JAY-R G. JADREN
 ITO - LAN Team

Checked by:


ARCHIEVAL B. TOLENTINO
 ITM - LAN Team

Approved by:


ENRIQUE L. SAZON JR.
 VP - NOD

List of LANDBANK Officers, Employees and Consultant(s)

A. Board of Directors

Ex-Officio Chairman: Sec. Benjamin E. Diokno, Department of Finance
 Vice Chairperson: Ms. Cecilia C. Borromeo, President and CEO
 Members: Pres. Ferdinand R. Marcos Jr., Department of Agriculture
 Sec. Bienvenido E. Laguesma, Department of Labor and Employment
 Sec. Conrado M. Estrella III, Department of Agrarian Reform
 Mr. Virgilio D. Robes, Representative - Agrarian Reform Beneficiaries Sector
 Mr. Jaime L. Miralles, Representative - Agrarian Reform Beneficiaries Sector
 Ms. Nancy D. Irlanda, Representative - Private Sector

B. President and CEO: Ms. Cecilia C. Borromeo**C. Bids and Awards Committee (HOBAC)**

Chairman: Mr. Reynaldo C. Capa, First Vice President – Banking Services Group
 Vice Chairman: Mr. Alwin I. Reyes, Vice President – Procurement Department
 Regular Members: Ms. Adelfa R. Masacupan, First Vice President – Asset and Liability Management Group
 Mr. Emmanuel G. Hio, Jr., Vice President – Facilities Engineering Services Group
 Ms. Marife Lynn O. Pascua, Vice President – Agrarian Services Group
 Ms. Reo S. Andarino, Assistant Vice President - Branch Banking Sector
 Provisional Member: Atty. Joseph Dennis C. Castro, Legal Manager - Legal Services Group

D. HOBAC Secretariat

Head: Atty. Honorio T. Diaz Jr.
 Officers and Staff: Ms. Remedios S. Lacaden, Senior Management Associate
 Ms. Ruby S. Cortez, Acting Procurement Specialist III
 Ms. Farah Eva B. Esguerra, Administrative Specialist II
 Ms. Maribel J. Paredes, Procurement Specialist I
 Mr. Mark Anthony C. Pantalla, Procurement Analyst
 Ms. Jenica V. De Vicente, Procurement Assistant
 Mr. Jerome C. Relucio, ASO I

E. Technical Working Group

Chairman: _____
 Vice Chairman: _____
 Members: _____

F. Procurement Department

Head: Mr. Alwin I. Reyes, Vice President
 Officers and Staff: Ms. Ma. Victoria C. Viray, Acting Senior Procurement Officer/Team Leader
 Ms. Rosemarie S.J. Mirando, Acting Senior Procurement Officer/Team Leader
 Ms. Leonor F. Santos, Acting Senior Procurement Specialist/Team Leader
 Mr. Joel R. Perez, Acting Senior Procurement Specialist/Team Leader
 Ms. Helen S. Purificacion, Acting Senior Procurement Specialist/Team Leader
 Mr. Donato DR. Cariaga, Acting Senior Procurement Specialist/Team Leader
 Ms. Kristi Ann P. Rutab, Acting Senior Procurement Specialist/Team Leader
 Atty. Karla May M. Temporosa, Administrative Officer
 Mr. Rommel C. Pascua, Acting Procurement Specialist III

- Ms. Cathrina Marie A. Garcia, Acting Procurement Specialist III
- Mr. Ruel V. Marca, Procurement Specialist II
- Mr. Rosalino V. Cruz, Procurement Specialist II
- Ms. Lubelle B. Lumabas, Procurement Specialist II
- Ms. Nadia G. Ileteo, Procurement Specialist I
- Mr. Jerome V. Bueno, Acting Procurement Specialist I
- Ms. Ma. Angela Q. Ematerio, Procurement Analyst
- Ms. Jeramae F. Concepcion, Procurement Analyst
- Ms. Kimberly Joy A. Sto. Tomas, Procurement Analyst
- Mr. Jollianiz Jenkin G. Dy, Procurement Analyst
- Ms. Charmaine F. Mangilit, Procurement Analyst
- Ms. Jeah Crysel L. Escalona, Procurement Analyst
- Mr. Marlon R. Faraon, Acting Procurement Analyst
- Mr. Aaron V. Sedanto, Procurement Analyst
- Mr. Rudyrick B. Silva, Administrative Analyst
- Ms. Fretch Camille J. Capole, Procurement Assistant
- Mr. Mark Anthony M. Abad, Administrative Assistant
- Ms. Almay Joyce B. Ruz, Procurement Assistant
- Ms. Ma. Theresa N. Cruz, Acting Executive Assistant
- Mr. Roman R. Eala, ASO I
- Mr. Jesus David, SCW
- Mr. Emil Dela Cruz, SCW
- Mr. Erikson Guani, SCW
- Mr. Vicente Gutierrez, Jr, SCW
- Mr. Andrew Palma, SCW
- Mr. Dexter Naguit, SCW
- Mr. Ramil Pendilla, SCW
- Mr. Frederick Reyes, SCW
- Mr. Pablo Tenoria, SCW

G. Implementing Unit

Head:

Officers and Staff:

H. End-user Unit

Please see annex F 1.1 – 1.3

I. Project Consultants

Team Lead:

Members:

Project Identification Number	LBP-HOBAC- ITB-GS-20220802-01
Project Name	Supply, Delivery, Installation and Configuration of Network Detection and Response (NDR) Solution with Three (3) Years Support Services
Subject	Response to Bidder's Queries

Queries	Responses
1. BID Submission - September 30, 2022 - Requesting for bid submission extension until October 7, 2022.	Amenable for bid submission extension until October 7, 2022.
2. TOR Item #186 : Manufacturer Certification as the Gold Partner Query: Would like to request to change to Authorized Partner	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from distributor or principal.
3. TOR Item #190 : Two (2) installed base of the brand being offered and one (1) is Commercial or Universal Bank in Philippines Query: Requesting that the installed base would be for only ONE (1) from the Commercial or Universal Bank in the Philippines	The supplier must have of at least one (1) installed based of the same brand being offered in a Philippine commercial or universal bank. Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed.
4. TOR Item #32 : Store raw packets for more than three (3) months Query: Requesting to change to "Network Transaction record" instead because storing a "raw packet" for three months would need 10 Petabyte storage	The proposed solution should be able to store the network transaction to support forensics investigations with purpose built hardware and expansion storage.
5. TOR Item #94 : The solution must only start collecting PCAPs once behavior of interest is triggered. Query: Please elaborate and clarify the second sentence OR can just delete this portion.	Item removed
6. TOR Item #97 and 98: Work in air-gapped and on-box machine learning not dependent on the cloud. Query: Requesting to delete as this would cap the efficiency of the technology. The technology itself would be more efficient with their cloud intelligence database and would be beneficial to the bank to maximize the technology.	Item removed.
7. How many locations	Head Office
8. Any cloud VPC in scope	On the pipeline
9. What EDR are you using	Must support leading EDR brand

10. What SIEM are you using	Must support leading SIEM brand
11. What Firewall are you using	Must support leading Firewall brand
12. What is the throughput of each location in scope	~10G
13. How many users, servers IP in the scope	~5,000++
14. 164 - Some of the compliances are more for network performance such as VOIP, MOS score, which are not related to security	Not Related to Security
15. 55 - Regarding database detection and response, does Landbank have any DAM (Database Activity Monitoring) solution - so is database visibility optional.	NDR solutions even if they detect database anomalies, they do not act on it and provide
16. 124 - Demonstrate ability to create custom record format include custom application data record -	This is more of Network performance metrics
17. TOR Item #131: Demonstrate ability to store detailed flow records for historical lookback - is this compliance requesting for Netflow support and as requested in the RFP Netflow data should stay on premises ? Is that correct. Please elaborate	This does not require netflow specially. More like transaction records with metadata that can be searched within the tool
18. TOR Item #136: Provide programmability NDR allowing for the real-time analysis of any custom protocol based on TCP or UDP. Examples may include extensibility to support: ISO8583, SCADA, NTP, Custom XML, etc. - Question- this is a metrics specific to network monitoring tools. Is the solution looking into OT networks such as SCADA ? Also custom XML and programmability requested is a big risk and not recommended because that allowing such languages can lead to risks if these languages are not securely written for rules and allowing 3rd party or custom developer code such as javascripts can cause risks as anyone with access to NDR or with stolen admin credentials can write custom script and run it from the NDR system, which is highly unrecommended.	Item removed.
19. TOR Item #137: Availability of NDR that can analyze traffic for real-time extraction of layer 2 to 7 and payload metrics, up to 100Gbps continuous sustained throughput of analysis on a single appliance - Is the network throughput in scope 100Gbps? If not, please indicate the actual throughput for each location in scope	10G, but must be scalable since there will be an expected increase of throughput with the growing
20. TOR Item #139: Physical Appliances should	Yes. We can install certificate in the NDR

<p>have a dedicated SSL/TLS decryption chipset to handle high volume processing of SSL traffic loads- Is Landbank allowing private certificates to be stored on 3rd party NDR appliances ? Also. are agents allowed to be installed with admin privileges on Landbank servers for decryption?</p>	<p>appliance to monitor SSL traffic.</p>
<p>21. TOR Item #140: Must have a Perfect Forward Secrecy (PFS, mode of encryption whereby session keys are not negotiated over the wire (contrast with traditional RSA key exchange), solution must have some capabilities to perform realtime decryptions in a Perfect Forward Secrecy encrypted environment e.g. TLS 1.3 with Diffie-Hellman Key exchange. - Is landbank allowing installation of agents on all the servers which needs TLS 1.3 decryption ?</p>	<p>Yes. We can allow the installation of an agent to decrypt for more visibility</p>
<p>22. TOR Item #141: PFS decryption technique must allow for both software key forwarder approach as well as Load Balancer integration techniques - Is LandBank allowing Man in the middle approach of sending the keys for PFS decryption to 3rd party NDR solution ?</p>	<p>No. Man-in the middle approach is not allowed. Should be done out of band</p>
<p>23. TOR Item #148: Provide real-time metrics for dashboarding, alerting, and historical reporting: '- TCP Connections, Aborts, Resets, Timeouts due to retransmissions, Zero Windows, Nagle's Delay, Out of Order packets L4 TCP Metric' mentioned above must be retained for atleast a month - All the above are Network performance metrics and not security metrics. Kindly elaborate if these metrics are optional as they will not assist risk or SOC team in any investigations</p>	<p>The features can be helpful in application and network troubleshooting. The team is not only focus on the security but also assist in application and network troubleshooting.</p>
<p>24. TOR Item #153: Provide real-time metrics for dashboarding, alerting, and historical reporting: Record All GET/POST/PUT/HEAD transactions and their corresponding URIs, clients, and server IP - this is a Network performance metrics</p>	<p>The features can be helpful in application and network troubleshooting. The team is not only focus on the security but also assist in application and network troubleshooting</p>
<p>25. TOR Item #155: Monitor database protocols out of the box at Layer-7 (application) level such as but not limited to: *Oracle *Microsoft SQL *MongoDB *DB2 *Sybase & SyBase IQ *REDIS *Postgres *Informix *MySQL Provide: real-time SQL statements, stats, errors and performance as relates to database traffic. - What is the expectation from the above</p>	<p>Current DAM licenses is limited to a number of databases. Having this feature will add more visibility on the database traffic so that the team can check any abnormalities or help in threat hunting against database attacks.</p>

<p>requirement as this is more towards DAM. Does Landbank already have a DAM and if so does it need this in NDR.</p>	
<p>30. TOR Item #160: Real-time metrics for dashboarding, alerting, and historical reporting of SMTP and POP3 traffic such as sender/recipient addresses, processing time, errors, SMTP/POP3 response/status codes. Email Metrics must be retained for at least a month -Above are network performance metrics. Is Landbank looking at Email security solution ?</p>	<p>As long as the product can comply with real-time dashboarding and alerting using SMTP/POP3</p>
<p>31. TOR Item #163: Real-time metrics for dashboarding, alerting, and historical reporting of protocols such as: -Extensive Markup Language (XML) -Simple Object Access Protocol (SOAP) -Apache Jserv Protocol (AJP) - Is Landbank looking for Network performance metrics or application security metrics from the above protocol and if so then this will be best addressed by a SAST or a DAST solution</p>	<p>The features can be helpful in application troubleshooting. The team is not only focus on the security but also assist in application troubleshooting.</p>
<p>32. For Form No. 3 (Statement of Ongoing Contracts) and Form No. 4 (Statement of Single Largest Contract) Query: What if the clients are covered by non-disclosure agreement, is there a special form to be used if there is NDA</p>	<p>No alternative form Necessary to determine the SLCC compliance of bidder</p>
<p>33. TOR Item #189: - Is it possible that the local partner will provide the first level of support, thus the local partner will be the one to provide the details?</p>	<p>Yes, local partner must provide the 1st level support and bidder must submit a detailed escalation procedure and support plan</p>
<p>34. Item No. 7: Capability for a single virtual appliance to monitor up to 10 Gbps of real-time traffic and 200 GB daily of packet capture storage - Can Landbank please confirm that by "200GB daily of packet capture storage" they are referring to network transaction metadata (such as stored by ExtraHop Reveal(x) 360)?</p>	<p>Capability to support virtual and/or physical appliances that range from 1Gbps to 100Gbps in a single virtual/physical form factor</p>
<p>35. Item No. 32: The proposed solution should be able to store the raw packets for more than 3 months - Is Landbank referring to storing continuous raw PCAP collection for over 3 months? At 10Gbps sustained this equates to 108TB per day of storage for full packet capture (PCAP).</p>	<p>The proposed solution should be able to store the network transaction to support forensics investigations with purpose built hardware and expansion storage.</p>

<p>36. Item No. 40: Proposed solution should have the option to include 24/7 MDR (Managed Detection and Response) service delivered by the solution provider.</p> <p>- May we add this as an optional item in the proposal? (note that the question says "should have the option")</p>	<p>This is an optional requirements for future deployment/integration.</p>
<p>37. Item No. 75: The proposed solution should not store any data in any cloud rather all the data should be stored on-premises</p> <p>- ExtraHop Reveal(x) 360 utilises cloud based Cloud Record Store for network transaction metadata. Reveal(x) Enterprise can be deployed to use on-premise record datastore.</p>	<p>Network Transaction Metadata is acceptable.</p>
<p>38. Item No. 97: The proposed solution should be able to work in air-gapped environment without depending on the external network connectivity and should not send any data outside the customer data center</p> <p>- Why does Landbank require an air-gapped solution? ExtraHop can be deployed in air-gapped environment with reduced functionality.</p>	<p>Item removed.</p>
<p>39. Item No. 98: The proposed solution should have on-box machine learning and should not be dependant on machine learning on the cloud</p> <p>- Why does Landbank want to be restricted by the limits of on-board machine learning with limited datasets that can be processed? ExtraHop is not limited to restricted on-box ML capabilities - ExtraHop uses cloud-scale ML services to ensure the best possible threat and anomaly detection</p>	<p>The proposed solution should have a machine learning capability in the cloud.</p>
<p>40. Item No. 100: The proposed solution must store detections and PCAP's on box for a period of no less than 3 months</p> <p>- Is Landbank referring to detection data and supporting metadata needed to support investigations? Detections and related metadata are stored for 3 months. If needed, the EDA can use extended Data Store for longer metrics and detection retention</p>	<p>Yes. To support forensic investigation.</p>
<p>41. Item No. 134: Proposed solution must allow the capability for human analysts to perform an unbiased analysis and identify improvement areas in the IT infrastructure. Deliverables include periodic (e.g. monthly, quarterly) reports with specific security findings and recommendations.</p> <p>- May we add this as an optional item in the</p>	<p>This is an optional requirement for support analysis, can be an added service provided by an NDR vendor to check and help with the bank security posture.</p>

proposal? This overlaps with item 40 MDR services	
42. Item No. 170: The solution must be capable of integrating with endpoint and identity solutions such as Active Directory to increase host coverage in remote work scenarios and support an identity focused, Zero Trust security strategy. - May we request for additional information or use cases for the integration with endpoint and identity solutions?	This is to help track Active Directory activity
43. Item No. 170: The solution must integrate with threat intelligence feeds (commercial, industry specific or internal) - Will the integration be used to derive user information from parsed network traffic?	Intelligence feed as other data sources.
44. Item No. 173: Deduplication of data should happen at the sensors and also in-addition at the centralized management appliance - Deduplication of what data? ExtraHop sensors perform native deduplication packets collected in the datafeed.	Deduplication of packet data
45. Item No. 178: The solution must have a strong integration with Active Directory and allow for either a manual or automated disabling, lockdown of accounts in the platform's UI. - What is the desired functionality for this integration?	This is to help track Active Directory activity. And prevent AD attacks.
46. Item No. 180: The solution must have native, UI or API based response capability with leading NGFW, please explain how the solution can respond? i.e., block via global blacklist - Does industry standard format include CEF or _EEF?	CEF is acceptable