

**Non-compulsory briefing session:
For the provision of Network Detection and
Response (NDR) Solution for a period of
three (3) years
TCC/2024/12/0001/84866/RFP**

Table of Contents



No:	Topic
01	Opening and Welcome
02	Transnet Colleagues Introduction
03	Safety Briefing
04	Key Points to Highlight and General Information
05	Scope and Technical Requirements
06	B-BBEE Scorecard
07	Joint venture
08	Evaluation Criteria
09	Question and closure



Opening/Welcome

Team

- ❖ Welcome the bidders
- ❖ Each Transnet attendee to briefly introduce themselves.

General Disclaimer: This briefing session must not contradict the RFP, and its supporting documents published, and should there be any errors, acts of omissions or misinterpretations, then the RFP and its attachments takes precedence of it.

Respondents will be given an opportunity to ask questions at the end.

All verbal questions must be put in writing on the RFP Clarification form (Section 8) and Transnet will provide a written response.

NB: No verbal feedback must be construed as binding until in writing.



Key Points - General (1/3)

Please note the following submission requirements, but not limited to:

- Final RFP and **all Returnable Documents listed on Section 5 (List of Returnable Documents)** may still be downloaded directly from National Treasury's e-Tender Publication Portal at www.etenders.gov.za and Transnet website, free of charge.
- Respondents who wish to respond to this RFP as a Joint Venture [JV] or consortium with B-BBEE entities, must state their intention to do so in their RFP submission. Such Respondents must also submit a signed JV or consortium agreement between the parties clearly stating the percentage [%] split of business and the associated responsibilities of each party.
- RFP closing date is **19 June 2025, at 12:00**. Respondents must ensure that bids are uploaded timeously onto the system.
- Transnet will not accept bid submission via email. All bids must be loaded on the system.
- Bid Validity period is **180 Business Days from Closing Date**.
- Respondents RFP proposal must **sign documents [sign, stamp and date the bottom of each page] before uploading them on the system. The person or persons signing the submission must be legally authorised by the respondent to do so.**

Respondents must register on the National Treasury's Central Supplier Database CSD prior to submitting/uploading their bids. Business may not be awarded to a Respondent who has failed to register on the CSD, only foreign suppliers with no local registered entity need not register on the CSD.



Key Points - General (2/3)

▪ Communication relating to this RFP:

- For specific clarification relating to this RFP, an RFP Clarification Request Form should be submitted to [**Mahlodi.kganyago@transnet.net** and **Reetsang.Modise@transnet.net**] before **12:00 pm on 29 May 2025** substantially in the form set out in Section 8 hereto. In the interest of fairness and transparency, Transnet's response to such a query will be published on the e-tender portal and Transnet website.
- Specific complaints relating to this RFP before or after the closing date should be formally submitted by emailing to groupscmcomplaints@transnet.net . Once the complaint has been submitted, the Transnet SCM Complaints office will acknowledge your complaint and send you a complaint form for completion.
- After the closing date of the RFP, a Respondent may only communicate with the **Barbara Msomi**, at telephone number 011 308 1892, email **Barbara.Msomi@transnet.net** on any matter relating to its RFP Proposal.
- Respondents are to note that changes to its submission will not be considered after the closing date.
- It is prohibited for Respondents to attempt, either directly or indirectly, to canvass any officer or employee of Transnet in respect of this RFP between the closing date and the date of the award of the business.
- Respondents found to be in collusion with one another will be automatically disqualified and restricted from doing business with organs of state for a specified period.
- Transnet will publish the outcome of this RFP in the National Treasury e-tender portal and Transnet website with 10 days after the award has been finalised. Respondents are required to check the National Treasury e-tender Portal and Transnet website for the results of the tender process. All unsuccessful bidders have a right to request Transnet to furnish reasons for their bid not being successful. This requested must be directed to the contact person stated in the SBD 1 form.



Key Points - General (3/3)

Proposal Submission:

- **Please refer to Section 2, paragraph 3 of the RFP for a detailed process on how to upload submissions.**
- A detailed bidder guide is included as **ANNEXURE K: GUIDANCE FOR BIDDERS.**



Background

- A Network Detection and Response (NDR) solution is a sophisticated cybersecurity technology designed to continuously monitor network traffic, detect anomalous activities, and respond to potential threats in real time. NDR solutions leverage advanced techniques such as machine learning, behavioral analysis, and threat intelligence to identify anomalies and mitigate risks before they can cause significant harm.
- Transnet lacks an NDR solution, which increases the organization's vulnerability to cyber threats. The absence of this critical technology means that north-south traffic (data flow between internal and external networks) and east-west traffic (data flow between systems within Transnet's network) is not adequately monitored. This gap exposes Transnet to potential data breaches, unauthorized access, and other malicious activities that our existing cybersecurity tools may not detect.
- While capable of handling some aspects of network protection, the current security infrastructure falls short in providing comprehensive coverage and real-time response capabilities. This limitation disadvantages Transnet in the rapidly evolving threat landscape, where cyberattacks are becoming more sophisticated and frequent.



Scope of Work

Expected Project deliverables are as follows:

1. **Solution Design Documentation:** Detailed documentation outlining the proposed NDR solution architecture, including network diagrams, component specifications, and integration plans.
2. **Hardware and Software Provisioning:** Procurement and installation of necessary hardware (if applicable) and software components required for the NDR solution.
3. **Installation and Configuration:** Physical or virtual installation and configuration of NDR sensors, collectors, analyzers, or appliances across Transnet network infrastructure.
4. **Integration with Existing Systems:** Integration of the NDR solution with Transnet existing security infrastructure, including SIEM (Security Information and Event Management) systems, PowerBI, Infrastructure firewalls, WAF (Web Application Firewall), NAC (Network Access Control), Vulnerability Management tools, Cloud-based Internet Proxy Servers , and endpoint protection platforms.
5. **Policy and Rule Configuration:** Setting up detection policies, rules, thresholds, and alert configurations tailored to Transnet's security needs and compliance requirements.
6. **Testing and Validation:** Conducting thorough testing and validation of the NDR solution to ensure it accurately detects and responds to network anomalies and threats without impacting network performance.



Scope of Work

7. **Training and Knowledge Transfer:** Providing training sessions or workshops for the Transnet Information Security team on how to use and manage the NDR solution effectively.
8. **Documentation and Handover:** Preparation of comprehensive documentation, including operational manuals, troubleshooting guides, and system documentation, followed by a formal handover to Transnet Information Security operations team.
9. **Ongoing Support and Maintenance:** Establishing a support framework with defined SLAs (Service Level Agreements) for ongoing maintenance, updates, patches, and troubleshooting of the NDR solution.
10. **Monitoring and Reporting:** Setting up monitoring capabilities to continuously track the performance and effectiveness of the NDR solution, along with regular reporting on security incidents, alerts, and system health.

Expected NDR Functional Requirements

1. **Real-time Network Traffic Analysis:** Continuous monitoring of network traffic to detect and analyze anomalies and threats in real-time.
2. **Behavioral Analytics:** Use of machine learning and Artificial Intelligence to establish a baseline of normal network behavior and identify deviations indicative of potential threats.



Scope of Work

3. **Threat Detection:** Detection of known and unknown threats, including advanced persistent threats (APTs), zero-day exploits, and insider threats.
4. **Automated Response:** Automated actions in response to detected threats, such as isolating affected devices, blocking malicious traffic, and alerting security teams.
5. **Threat Intelligence Integration:** Integration with external threat intelligence sources to enhance detection capabilities and stay updated on emerging threats.
6. **Deep Packet Inspection (DPI):** Analysis of packet content for a more thorough inspection beyond basic header information, allowing detection of hidden threats.
7. **Encrypted Traffic Analysis:** Ability to inspect encrypted traffic without compromising privacy, using techniques such as SSL/TLS decryption or machine learning.
8. **Incident Investigation and Forensics:** Tools for detailed investigation of incidents, including packet capture, flow data analysis, and event correlation.
9. **Network Mapping and Visualization:** Visualization of network topology and traffic flows to help identify unusual patterns and understand the scope of incidents.
10. **Scalability and Performance:** Capability to handle high volumes of traffic across large, distributed networks without significant performance degradation.



Scope of Work

10. **Scalability and Performance:** Capability to handle high volumes of traffic across large, distributed networks without significant performance degradation.
11. **Compliance Reporting:** Generation of reports to assist with compliance requirements for various regulations (such as POPIA) and standards (e.g., CIS).
12. **User and Entity Behavior Analytics (UEBA):** Monitoring user and entity behavior to detect insider threats and compromised accounts.
13. **Anomaly Detection:** Identification of unusual patterns or activities within the network that may indicate potential security issues.
14. **Advanced Threat Hunting:** Proactive searching for threats within the network using sophisticated tools and techniques.
15. **Customizable Dashboards and Alerts:** User-friendly interfaces that provide customizable dashboards and alerts to keep security teams informed.
16. **API Support:** APIs for integration with custom scripts and other tools to enhance the functionality and automation of the NDR solution.
17. **Multi-cloud and Hybrid Environment Support:** Capability to monitor and protect assets across on-premises, azure cloud, and hybrid environments.



Scope of Work

18. **Data Retention and Archiving:** Long-term storage of network traffic data for historical analysis and compliance purposes.
19. **Risk Scoring:** Assigning risk scores to detected threats to prioritize response efforts based on severity

No:	Item	QTY	Description
1.	Number of Endpoints	40602	<ul style="list-style-type: none">▪ 31000 Client Computers▪ 2000 Servers▪ 2700 Printers▪ 3612 Network Switches▪ 297 Routers▪ 26 WLAN Controllers▪ 946 Wireless Access Points▪ 21 Firewalls
2.	Number of Core Sites	50 (Appendix A)	<ul style="list-style-type: none">▪ 47 Campus Sites geographically dispersed across the country.▪ 3 TERACOs
3	Support and Maintenance	3 years	Costs for support and maintenance over three years.



Scope of Work

No:	Item	QTY	Description
4	Implementation and Setup	4 months	Costs for initial setup configuration, and integration with existing systems.
5	Training	50 Engineers	Cost for training the Transnet Information Security team on the new system.

Standards of acceptability

- Vendor must be ISO27001 certified.
- POPIA or GDPR compliant.
- Implementation Track Record in large organizations.

Scope of Work



Appendix A

Site ID	Campus Site	Site ID	Campus Site
1	Newcastle	27	Langlaagte
2	Springs	28	Potchefstroom
3	Sentrarand	29	Vereeniging
4	Ermelo	30	Beaufort West
5	Vryheid	31	Bellville
6	Ogies	32	Cape Town
7	Standerton	33	Saldanha
8	Richards Bay Nzesi	34	Worcester
9	Empangeni	35	East London
10	Pietermaritzburg	36	Noupoort
11	Ladysmith	37	PE North End
12	Durban	38	Mossel Bay
13	Bayhead	39	Hoedspruit
14	Isando	40	Nelspruit
15	Heidelberg	41	Polokwane
16	Esselen Park	42	Pretoria North Campus
17	Vooruitsig CTC	43	Rustenburg
18	Richards Bay Port	44	Witbank
19	Bethlehem	45	Koeduespoort
20	Bloemfontein	46	Nzasm
21	Germiston (Kaserne and City Deep)	47	Mafikeng Campus
22	Johannesburg (NSB)	48	Johannesburg Teraco
23	Kimberley	49	Cape Town Teraco
24	Klerksdorp	50	Durban Teraco
25	Kroonstad		
26	Krugersdorp		



Appendix B

Category	Requirement Title	Requirement Description	Requirement Priority
Functional requirements	Alert aggregation	Aggregates individual alerts into structured incidents to facilitate threat investigation. Provides automatic or manual response capabilities to react to the detection of malicious network traffic.	High
Functional requirements	Form factors	Delivers, via physical or virtual sensors, form factors compatible with on-premises and cloud networks to analyze raw network packet traffic or traffic flows. Monitors north-south traffic and east-west traffic.	High
Functional requirements	Network traffic modeling	Models normal network traffic and highlights unusual traffic activity that falls outside the normal range. Provides detection based on behavioral techniques, including machine learning and advanced analytics that detect network anomalies.	High
Functional requirements	Product usability	Provides easily understood, friendly interfaces with intuitive designs to facilitate user engagement.	High
Functional requirements	Detection	Enables more traditional detection techniques, including intrusion detection and prevention system signatures, rule-based heuristics and threshold-based alerts.	High
Functional requirements	Traffic monitoring	Monitors and analyzes traffic in Infrastructure as a Service environments.	High
Functional requirements	Automated responses	Supports automated responses, such as host containment (through integration) or traffic blocking, directly or through integration with other cybersecurity tools.	High
Functional requirements	Low rate of false positives	Enables a low rate of false positives, after initial tuning, to become a trustable source of insight and support automated response use cases.	High
Functional requirements	Security incident alert aggregation	Provides alert aggregation of logical security incidents based on multiple factors (not just alert ID) and repeated alerts through integration with other SOC tools for richer context.	High
Technical requirements	Data storage	Provides required data storage capacity, file types and locations. Supports processes such as disaster recovery, rollbacks, extraction or eradication.	High
Technical requirements	Integration	Integrates with all relevant applications, data sources and technologies.	High
Technical requirements	Performance management	Provides proactive alerts on system events. Enables logging and resolution reporting on all issues.	High
Technical requirements	Security	Enables configurable controls that extend data and transaction security and compliance to third-party platforms or the solution's hosting providers. Documents security policies, audits, attestations or evaluations for compliance needs.	High
Technical requirements	Data management	Enables monitoring, reporting and management of data sharing. Supports encryption and security for data at rest and in motion.	High
Technical requirements	Data sharing	Sends data to external systems such as large language models and uses insights from connected engines such as generative AI to deliver product functionality. Enables users to manage all aspects of data sharing, including full disablement.	Medium
Technical requirements	Disaster recovery and backup	Enables processes such as disaster recovery, rollbacks and version control.	High
Technical requirements	Identity and access management	Supports capabilities such as user authentication, password policy management, two-	High

Scope of Work






























Technical requirements	Network	Leverages network technologies like software-defined wide area networks and over-the-top monitoring to ensure the optimal performance of the solution.	High
Technical requirements	Compliance and third party certification	Complies with relevant standards like CCPA, GDPR and third-party or government certifications such as SOC 2, ISO 27001 and FedRAMP.	High
Technical requirements	Developer tools and customization	Allows customization of the standard deployed solution with custom user interfaces, data tables, process components and business logic.	Medium
Technical requirements	Global delivery	Supports off-the-shelf localization such as insights, language and currency support for required geographies.	Medium
Support and services	Customer support	Delivers required level of user and technical support, e.g., 24/7, multi-language and global support.	High
Support and services	Implementation timeline	Provides implementation resources, including setup, testing and training, to meet the desired go-live date.	High
Support and services	Implementation, onboarding and setup	Provides clear implementation plan and resourcing, including setup, testing and training, to meet the desired go-live date.	High
Support and services	Support formats	Allows access to support across multiple formats including phone, email, chat and online knowledge base.	High
Support and services	Deployment model	Presents clear rollout options such as staggered, proof of concepts or end-to-end enterprise deployments.	High
Support and services	Service levels and SLAS	Meets relevant service level agreements related to system performance, concurrent users, uptime and issue resolution.	High
Support and services	Training and education	Supports best-in-class training and assistance for users using online and offline mediums.	High
Support and services	Services resources	Aligns sufficient expertise via vendor or partners to deliver all implementation objectives.	High
Vendor health	Financial strength	Vendor is in a strong financial position as measured by key metrics such as balance sheet strength and revenue growth rate.	High
Vendor health	Vendor fit	Vendor vision, culture, and team demonstrate that vendor will be a good partner.	High
Vendor health	Customer base	Focus, size, and fit of vendor's customer base shows ability to understand your needs, company and sector.	High
Vendor health	Customer references	Vendor is able to provide minimum of two high quality references with organizations in similar industries or scenarios.	High
Vendor health	User ratings	Online reviews rate vendor at level of 4.2 or higher (out of 5) and include insights where they excel or not.	High
Vendor health	Product strategy and roadmap	Overall strategy and product roadmap aligns well with your future requirements.	High
Pricing and commercial terms	Length of initial contract term and renewal mechanics	Defines initial contract term including, where applicable, implementation periods and billing start dates. Defines how renewals occur if automatic, notice periods and how terms, pricing or other contracted components such as functionality can change.	High
Pricing and commercial terms	License fees	License pricing units (e.g. number of users, sessions or API calls), cost of each, and forecast annual and/or monthly volumes.	High
Pricing and commercial terms	Implementation costs	Cost to implement and deliver software into full production using either vendor or partner resources.	High

Scope of Work



Pricing and commercial terms	Training costs	Expense to train and support current users for launch, provide their continuing education and onboard future new users.	Medium
Pricing and commercial terms	Contract terms and conditions	Provides key terms such as price protection, termination clause, jurisdiction and limitation of liability.	High
Pricing and commercial terms	Service or maintenance fees	Supports fees related to ongoing support services and maintenance, including tiers and precise deliverables.	High

Appendix C

OVERVIEW			CHECKLIST			REQUIREMENTS			VENDORS			QUESTIONNAIRE			SCORECARD			SELECTION		
Vendor			Peer Insights																	
 Darktrace DETECT			 4.7 / 5 (295 reviews)			 Remove from eval														
 Vectra NDR			 4.7 / 5 (288 reviews)			 Remove from eval														
 ExtraHop Reveal(x) NDR			 4.5 / 5 (232 reviews)			 Remove from eval														
 Cisco Secure Network Analytics			 4.4 / 5 (89 reviews)			 Remove from eval														
 Hillstone Breach Detection System			 5.0 / 5 (40 reviews)			 Remove from eval														
 Broadcom Symantec Security Analytics			 4.2 / 5 (12 reviews)			 Remove from eval														
 Trend Vision One — XDR for Networks			 4.7 / 5 (40 reviews)			 Remove from eval														
 Stellar Cyber Open XDR Platform			 4.8 / 5 (34 reviews)			 Remove from eval														
 Sangfor Cyber Command			 4.7 / 5 (11 reviews)			 Remove from eval														



B-BBEE

B-BBEE Definition:

Broad-Based Black Economic (B-BBEE) means the economic empowerment of all black people including women, workers, youth, people living with disabilities and people living in rural areas through diverse but integrated socio-economic strategies.

Purpose:

- To increase the number of black people that manage, own and control enterprises and productive assets.
- To facilitate ownership and management of enterprises and productive assets by communities, workers, cooperatives and other collective enterprises
- To achieve an equitable representation in all occupational categories and levels in the workforce
- To procure from large, medium and small sized black owned enterprises
- To increase investment in enterprises and communities that are owned and managed by black people
- A valid B-BBEE certificate for LE company's OR an Affidavit for QSE and EME's is required

B-BBEE Amended Codes Principles

- Enhanced the recognition status of black owned EMEs and QSEs
- An EME that is 100% owned by black people qualifies as a level 1 contributor;
- An EME that is more than 51% owned by black people qualifies as a level 2 contributor;
- No verification requirements for EMEs; EME to obtain a Sworn affidavit or a CIPC Certificate



Preferential Procurement Regulations 2022

PPPFA provides for a preference points system in terms of which contracts below a prescribed value be evaluated on the basis that 20 out of 80 possible points must be allocated to “specific goals” and 90 points allocated to price.

For contracts above a prescribed value, 10 out of 100 possible points must be allocated to “**specific goals**”, and 90 points allocated to price

- (a) The applicable preference point system as envisaged
- (b) The specific goal in the invitation to submit the tender for which a point may be awarded, and the number of points that will be awarded to each goal, and proof of the claim for such goal .

Bidders who do not submit B-BBEE Status Level Verification Certificates or applicable affidavit copy will be deemed as non-compliant contributors to B-BBEE will score zero for preference points .

This also applies to Bidders who submit letters or expired certificates indicating that their B-BBEE status is in the process of being verified. Where a B-BBEE certificate is to be used for scoring purposes only, such letters indicating that their B-BBEE status is in the process of being verified or expired certificates are submitted, bidders will be scored zero for preference points.



Joint Venture

In 2019 DTI released amendments to the Codes of Good Practice. Joint Ventures are referred to in Revised Code 000, Statement 000: General Principles

- As per paragraph 7 of Amended Code Series 000, Statement 000 of the Codes of Good Practice, unincorporated joint ventures are required to compile a consolidated verification certificate. A consolidated verification certificate will consolidate the verified compliance data of joint venture partners if those Measured Entities were a single Measured Entity.
- A JV will require its own Broad-Based Black Economic Empowerment (B-BBEE) certificate if they would like to tender or enter into a contract that requires a B-BBEE Certificate.
- A trust, consortium or joint venture (including unincorporated consortia and joint ventures) must submit a consolidated B-BBEE Status Level verification certificate for every separate bid.
- A tenderer failing to submit proof of B-BBEE status level of contributor or is a non-compliant contributor to B-BBEE may not be disqualified but may only score points out of 90 for price and (b) scores 0 points applying the 90/10 principle . Refer PPPFA No. 40553 for more info on preference point.
- Respondents who wish to respond to this RFP as a Joint Venture [JV] or consortium with B-BBEE entities, must state their intention to do so in their RFP submission. Such Respondents must also submit a signed JV or consortium agreement between the parties clearly stating the percentage [%] split of business and the associated responsibilities of each party.

Note the following:

- A consolidated verification certificate is required.
- The consolidation is based on the weighting as defined in the joint venture agreement.
- The respective scores are weighted according to their proportionate share in the joint venture.
- A joint venture certificate is valid for 12 months and only applicable to a specific project.



Joint Venture and Specific Goals

Eligibility of a Joint Venture

Joint Ventures are required to compile a consolidated verification certificate. A consolidated verification certificate will consolidate the verified compliance data of joint venture partners in accordance.

ESD (B-BBEE) Proposed Specific Goals

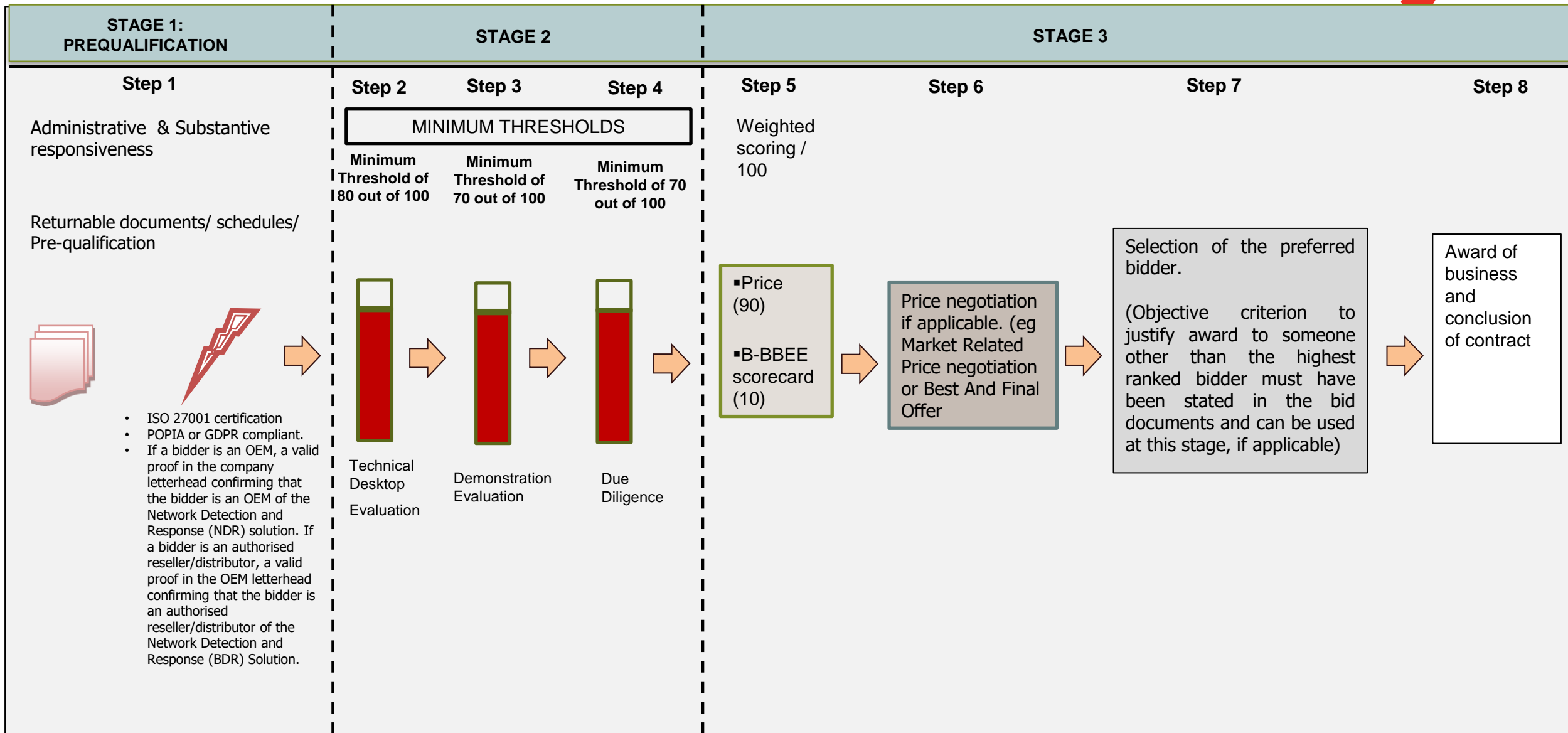
The BBBEE preference for this transaction is 90/10

Preference Point System 90/10

#	Specific Goal	Number of Points	Price
1	B-BBEE Level 1 & 2	5	90
2	Black Owned (51%)	2	
3	Job creation	3	
	Total	10	



Transnet's evaluation methodology





Step One: Test for Administrative Responsiveness

Step 1 : The evaluations are carried out by the procurement department to identify the non-responsive (non-compliant bids), procurement makes an effort to acquire outstanding documents from the respondent before declaring a responder non-responsive and eliminating a bid

Administrative & Substantive responsiveness check	Yes/No
Whether the Bid has been lodged on time	
Whether all Returnable Documents and/or schedules [where applicable] were completed and returned by the closing date and time	
Verify the validity of all returnable documents	
Verify if the Bid document has been duly signed by the authorised respondent	
Whether any general and legislation qualification criteria set by Transnet, have been met	
Whether the Bid contains a priced offer	
Whether the Bid materially complies with the scope and/or specification given	

Mandatory Returnable Documents

Section 4: Pricing and Delivery Schedule	
Annexure A : Pricing Schedule	
<p>Whether any Technical Pre-qualification Criteria/minimum requirements/legal requirements have been met as follows:</p> <ul style="list-style-type: none"> • The bidder must submit a valid ISO 27001 certificate in their company name. If the bidder is entered in a joint venture both companies must provide their valid ISO 27001 certificates. • Bidder to provide a letter, on a company letter head, stating that they are either POPIA or GDPR compliant or alternatively provide a copy of their privacy policy indicating they are POPIA or GDPR compliant. • If a bidder is an OEM, a valid proof in the company letterhead confirming that the bidder is an OEM of the Network Detection and Response (NDR) solution. If a bidder is an authorised reseller/distributor, a valid proof in the OEM letterhead confirming that the bidder is an authorised reseller/distributor of the Network Detection and Response (NDR) Solution. 	

Step One: Test for Administrative Responsiveness

Step 1 : The evaluations are carried out by the procurement department to identify the non-responsive (non-compliant bids), procurement makes an effort to acquire outstanding documents from the respondent before declaring a responder non-responsive and eliminating a bid

Returnable Documents used for scoring	Yes/No
Respondent's valid proof of evidence to claim points for compliance with Specific Goals' requirements as stipulated in Section 9 of this RFP	
Valid proof of Respondent's compliance to B-BBEE requirements stipulated in Section 9 of this RFP (Valid B-BBEE certificate or Sworn- Affidavit as per DTIC guidelines)	
All documents as per Annexure B: Technical / Questionnaire Requirements.	
All documents as per Annexure C: Key Personnel/Team	
Essential Returnable Documents & Schedules	Yes/No
In the case of Joint Ventures, a copy of the Joint Venture Agreement or written confirmation of the intention to enter into a Joint Venture Agreement	
Latest Financial Statements signed by your Accounting Officer or latest Audited Financial Statements plus 2 previous years	
Section 1: SBD1 Form	
Section 2: Notice to Bidders	
Section 3: Background, Overview and Scope of Requirements	
Section 5: Proposal Form and List of Returnable documents	
Section 6 : Certificate Of Acquaintance with RFP, Terms & Conditions & Applicable Documents	
Section 7 : RFP Declaration and Breach of Law Form	
Section 8: RFP Clarification Request Form	
Section 9: Specific Goals Points Claim Form	
Section 11: Job-Creation Schedule	



Step One: Test for Administrative Responsiveness

Essential Returnable Documents & Schedules	Yes/No
Section 12: SBD 5	
Section 13: Protection of Personal Information	
Section 14: Protection of Personal Information Operator	
Annexure D: Online Demo Presentation	
Annexure E: Due Diligence	
Annexure F: Draft Master Agreement	
Annexure G: Transnet's General Bid Conditions	
Annexure H: Non-Disclosure Agreement	
Annexure I: Supplier Declaration Form	
Annexure J: Transnet's Supplier Integrity Pact	

Desktop Technical Evaluation





Step Two: Technical Evaluation Criteria – Refer to Annexure B

Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring guidelines	Maximum score
Bidder's Experience (Capability and Capacity)	<p>1.The proposed Network Detection and Response Solution has featured in Market Analysis with reviews and rating not older than June 2020.</p> <p>2.The bidder's key personnel who will be assigned to the Transnet account with relevant years of experience should have qualifications in the following key sub-sections:</p> <p>a) Service Management: ITIL v3 certification or higher</p> <p>b) Project Management: PMBOK, PRINCE2 or equivalent</p> <p>c) Architecture: TOGAF certification</p> <p>3. The bidder's technical support member who will be assigned to the Transnet account with relevant years of experience should have qualifications in the following key sub-sections:</p> <p>a) Service Management: ITIL v3 certification or higher.</p> <p>b) Technical; Web Application Security qualification or equivalent :</p> <p>c) OEM Product certification</p> <p>Bidder completed Annexure C: Key Personnel</p>	<p>1. Bidder has to provide/submit atleast 1 article/publication with reviews or ratings not older than June 2020, conducted by market research organisations regarding the proposed Network Detection and Response Solution (1 point)</p> <p>2. The bidder must provide the full contact details, curriculum vitae (CV), qualifications, and a minimum of five (5) years of relevant work experience of the Project Manager who will be assigned to the Transnet account (2 points)</p> <p>3. The bidder must provide the full details, including curriculum vitae (CVs), qualifications, and a minimum of five (5) years of relevant work experience, of at least two (2) technical team members who will be responsible for training, technical support, and other related technical services (4 points)</p> <p>4. NB : Bidder will score full points if all the requirements are met. if NOT all information is provided bidder will score (0) , or if insufficient information is provided to meet minimum requirement, or if there is no information and/or most of the information provided is irrelevant to meet the minimum requirement.</p>	7
Bidder's Experience (Reference Letters)	<p>Bidder should provide relevant client references in the company letter from clients who are/were currently using the proposed Network Detection and Response Solution. The following minimum verifiable information should be incorporated (company name, contact person, contact details and confirmation/mention of the specific Network Detection and Response Solution in the reference letter)</p> <p>Transnet reserves the right to contact the clients listed in order to verify the information provided.</p>	<p>Three (3) relevant reference letters not older than June 2020 (i.e. 5 years) from clients on proposed Network Detection and Response Solution. Each letter with the following minimum information (company letterhead, company name, contact person, contact details and confirmation/mention of the specific Network Detection and Response Solution)</p> <p>0 = No reference letters or client reference letters covering installation, configuration, implementation and administration of Network Detection and Response Solution tool for less than 5 000 end points</p> <p>9 = Three client reference letters with full contact details confirming installation, configuration, implementation and administration of Network Detection and Response Solution tool between 5 000 and 10 000 end points</p> <p>15 = Three client reference letters with full contact details confirming installation, configuration, implementation and administration of Network Detection and Response Solution tool between 10 000 and 15 000 end points</p> <p>24 = Three client reference letters with full contact details confirming installation, configuration, implementation and administration of Network Detection and Response Solution tool for more than 15 000 end points</p>	24

Step Two: Technical Evaluation Criteria – Refer to Annexure B



Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring guidelines	Maximum score
		NB: Partial completion (i.e. missing information) on the letter may render the reference as non-responsive. Irrelevant description or insufficient information provided on description of services will render the letter as non-responsive. Bidder will score points for each information provided. Bidder will score (0) points for each element if the minimum requirements are not met, or if insufficient information is provided to meet minimum requirement, or if there is no information and/or most of the information provided is irrelevant to meet the minimum requirement.	
Proposed Network Detection and Response Solution (Functionality)	Evaluation Checklist of Network Detection and Response Solution	<p>Network Detection and Response</p> <ol style="list-style-type: none"> 1. Does the solution support network traffic modelling to identify abnormal behaviours? (Yes/No) (2 Points) 2. Is the solution capable of detecting advanced threats such as zero-day exploits? (Yes/No) (2 Points) 3. Can the product operate in both physical and virtual environments? (Yes/No) (2 Points) 4. Does it aggregate alerts into structured incidents for better analysis? (Yes/No) (1 Point) 5. Is the user interface intuitive and easy to navigate? (Yes/No) (1 Point) 6. Does the solution offer support for encrypted traffic inspection? (Yes/No) (1 Point) 7. Can the solution monitor east-west traffic within a network? (Yes/No) (2 Points) 8. Is there an option for cloud-based deployment? (Yes/No) (1 Point) 9. Does it provide API access for custom integrations? (Yes/No) (1 Point) 10. Is the product scalable for networks with over 30,000 endpoints? (Yes/No) (1 Point) 11. Are updates and threat intelligence feeds provided regularly? (Yes/No) (1 Point) 12. Does the solution allow integration with Security Information and Event Management (SIEM) systems? (Yes/No) (2 Points). 13. Does the solution detection model use one or more filters to detect suspicious behaviours or events based on associated MITRE techniques? (Yes/No) (2 Points) 14. Does the solution provide automated response capabilities to mitigate detected threats? (Yes/No) (2 Points) 15. Can it perform deep packet inspection for detailed traffic analysis? (Yes/No) (2 Points) 16. Does the product include built-in compliance reporting features? (Yes/No) (1 Point) 16. Is multi-tenant support available for managing multiple environments? (Yes/No) (2 Points) 17. Does the solution support machine learning or AI-driven threat detection? (Yes/No) (2 Points) 18. Can it operate effectively with limited bandwidth environments? (Yes/No) (1 Point) 19. Is the vendor's technical support available 24/7? (Yes/No) (1 Point) 20. Does the solution include a sandboxing feature for malware analysis? (Yes/No) (2 Points) 	32

Step Two: Technical Evaluation Criteria – Refer to Annexure B

Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring guidelines	Maximum score
Proposed Network Detection and Response Solution (Functionality)	Evaluation Checklist of Network Detection and Response Solution	Prioritisation 1. Does the solution prioritize alerts based on severity and business impact? (Yes/No) (2 points) 2. Can it suppress or deduplicate recurring false-positive alerts? (Yes/No). (1 point) 3. Is there a mechanism to highlight alerts involving critical assets? (Yes/No). (2 points) 4. Can it provide immediate remediation suggestions for high-priority threats? (Yes/No). (1 point) 5. Does it allow setting custom thresholds for prioritization? (Yes/No). (1 point) 6. Can analysts mark and track the resolution of high-priority incidents? (Yes/No). (1 point) 7. Does the product offer a visual representation of prioritized incidents? (Yes/No). (1 point)	9
		1. Can reports be customized for different stakeholders (e.g., executives, technical teams)? (Yes/No) (1point) 2. Does the solution support automated scheduling of periodic reports? (Yes/No) (1point) 3. Are real-time dashboards available for active monitoring? (Yes/No) (1point) 4. Does it provide a breakdown of incidents by type, severity, and time frame? (Yes/No) (1point) 5. Can historical data be exported for audit or forensic purposes? (Yes/No) (2 point)	6
		Compliance & Configuration Assessment 1. Does the solution provide compliance assessment against industry standards (e.g., NIST, ISO 27001,POPIA,GDPR)? (Yes/No) (2 points) 2. Can it identify, and report misconfigured devices or services? (Yes/No) (2 points) 3. Is the service provider able to provide an assessment of the configuration in terms of best practices. (Yes/No) (1 point) 4. Does the solution include audit trails for all configuration changes? (Yes/No) (1 point)	6
		Administration 1. Is multi-factor authentication supported for administrative access? (Yes/No) (1 point) 2. Can role-based access control (RBAC) be implemented? (Yes/No). (2 points) 3. Is there a centralized customizable dashboard for managing multiple deployments as well as insights to individual devices? (Yes/No). (1 point)	4
		Integration 1. Does the solution integrate with leading endpoint detection and response (EDR) tools? (Yes/No) (1 point) 2. Can it connect to threat intelligence platforms (TIPs) for enhanced threat detection? (Yes/No) (1 point) 3. Is it compatible with cloud platforms like AWS, Azure, and Google Cloud? (Yes/No) (1 point) 4. Can it interface with existing firewalls and intrusion prevention systems (IPS)? (Yes/No) (1 point) 5. Does it support integration with third-party vulnerability management solutions? (Yes/No) (1 point) 6. Can logs be exported to external storage for long-term retention? (Yes/No) (1 point) 7. Is the solution interoperable with existing identity and access management (IAM) systems? (Yes/No) (2 points) 8. Does this solution integrate with SOAR platforms? (Yes/No) (2 points) 9. Are there built-in connectors for popular service management tools like service now ,CASDM, Microsoft Dynamics 365 or Similar tools? (Yes/No) (2 points)	12
Minimum Threshold			80
Total			100

Demo Evaluation





Step Three: Demo Evaluation – Refer to Annexure D

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring criteria	Weightings	Scoring guide
1.1 Verification of Operational tools	High level verification of tools to be utilised for tender	Bidders must be able to demonstrate the tools proposed in tender (Hardware /Software and licensing)	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Online demonstration of tools Partially comply = Offline demonstration of tools Does not comply = No tools demonstrated
1.2 Verification of the Deployment Process and Integration	<ul style="list-style-type: none"> Evaluate how easily the solution integrates with other security infrastructure tools(Firewalls, Microsoft, Network Access Control) Assess the deployment process in terms of complexity, time taken, and any potential disruptions to your operations. 	Bidders must be able to demonstrate on live system: how easy the solution integrates with other security infrastructure tools, and the deployment process in terms of complexity, time taken, and any potential disruptions to business operations.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Integrates with other security tools, deployment processes and potential disruptions Partially comply = Only one of the three demonstrated Does not comply =None demonstrated
1.3 Detection Capabilities	Verification of the Detection Capabilities of the Network Detection and Response Solution	Bidders must be able to demonstrate online: evidence of the solution's ability to detect and respond to various types of threats, including malware, ransomware, phishing attacks, etc. And the solution's approach to detecting and mitigating advanced persistent threats (APTs) and zero-day exploits.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = demonstration detection and responses to various types of attacks including malware, ransomware and phishing. Partially comply = demonstrating one of the two between detection and response. Does not comply = no demonstration



Step Three: Demo Evaluation – Refer to Annexure D

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring criteria	Weightings	Scoring guide
1.4 Data Collection and Analysis	Verification of the Data Collection and Analysis Capabilities of the Network Detection and Response Solution	Bidders must demonstrate online: how the solution collects, stores, and analyses security data from different endpoints and network sources. And the platform's capabilities for real-time monitoring, threat hunting, and forensic analysis.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Demonstrate how it collects, stores ,analyse data and do forensic analysis Partially comply = demonstrate on two of the listed items above Does not comply = No reporting demonstrated
1.5 Response and Remediation	Verification of the Response and Remediation Capabilities of the Network Detection and Response Solution	Bidders must demonstrate online: the solution's automation capabilities for responding to security incidents. And the range of response actions available and their effectiveness in containing and mitigating threats.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Could demonstrate automation capabilities for incidents and response actions and mitigating threats Partially comply = Could demonstrate one of the three items listed above Does not comply = Could not demonstrate the capabilities
1.6 Scalability and Performance	Verification of the Scalability and Performance Capabilities of the Network Detection and Response Solution	Bidders must demonstrate on online: the solution's capability to accommodate the business growth and evolving security needs. And its performance in handling large volumes of data and maintaining operational efficiency during peak loads	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Could effectively demonstrate the scalability, efficiency and performance in handling large volumes . Partially comply = Could only demonstrate one of the three listed items above Does not comply =Could not support all the three items listed



Step Three: Demo Evaluation – Refer to Annexure D

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring criteria	Weightings	Scoring guide
1.7 Business Continuity	To verify that the bidder has an effective Business continuity and DR setup in place.	Bidders must be able to demonstrate online their current Business continuity and Disaster Recovery setup for the proposed Network Detection and Response system.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Could demonstrate the Business continuity and Disaster Recovery setup via online system Partially comply = Could only demonstrate the Business continuity and Disaster Recovery setup via an offline system Does not comply = Could not demonstrate the Business continuity and Disaster Recovery setup
1.8 Integration	To verify that the bidder's Network Detection and Response system integrates smoothly with the security platform and generates reports.	Bidders must demonstrate online: that their solution does integrate with security systems and generate reports for all outputs in csv, pdf and be able to generate executive summary reports	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = Could demonstrate all the required elements Partially comply = Could not demonstrate one of the required elements Does not comply = Could not demonstrate more than one of the required elements
1.9 Compliance and Reporting	Verification of the Compliance and Reporting Capabilities of the Network Detection and Response Solution.	Bidders must demonstrate online: that their solution meets relevant compliance requirements for the logistics industry. And the capabilities for generating compliance reports and security insights.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully comply = demonstration of Compliance and Reporting Capabilities Partially comply = demonstration of one Capability Does not comply = no demonstration



Step Three: Demo Evaluation – Refer to Annexure D

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring criteria	Weightings	Scoring guide
1.10 Staff capacity and capability verification	To verify that the bidder has sufficient current staff capacity and capability.	Bidders must be able to demonstrate that they have capable staff already in place to deliver the proposal in the following key areas : 1) Service Management 2) Cyber Security Services 3) Project Management	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully Complies: Capable personnel representing all area with full organizational structure provided Partially Complies: 1-2 areas not represented with full organizational structure provided Does not Comply: > 2 areas not represented, or no full organizational structure provided
			Minimum Threshold	70	
			Total	100	

Due Diligence Evaluation





Step Four: Due Diligence – Refer to Annexure E

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring Criteria	Weightings out of 100%	Scoring guide
2.1 Sourcing goals	To verify with reference that the bidder has successfully delivered on a outsourcing contract's sourcing goals	The reference client will be interviewed to verify the delivery track record of a past project(s) the bidder did in terms of whether the original RFP/Contract goals were met: e.g. reduce cost, increase flexibility, access to best practice, improve service delivery	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	<p>Fully comply: > =80% of sourcing goals met. The bidder must indicate three or more of the following:</p> <ul style="list-style-type: none"> - Reduce cost, - Increase flexibility, - Access to best practice, - Improve service delivery <p>Partially comply : > 50% and < 80% of sourcing goals met. The bidder must indicate atleast two of the following:</p> <ul style="list-style-type: none"> -Reduce cost, - Increase flexibility, - Access to best practice, - Improve service delivery <p>Does not comply : < =50% of sourcing goals met</p>
2.2 Supplier performance	To verify the supplier's capability to consistently perform according to the scope of the contract	The reference client will be interviewed to evaluate the bidder's past project performance, specifically to determine whether they successfully improved performance or if it declined.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	<p>Fully comply: Improvement of performance</p> <p>Partially comply :No improvement</p> <p>Does not comply : Deterioration of performance</p>



Step Four: Due Diligence – Refer to Annexure E

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring Criteria	Weightings out of 100%	Scoring guide
2.3 Quality	To verify that the bidder has provided a good quality solution in key areas for the reference client	The reference client will be interviewed to verify the reference's satisfaction (Yes or No) with bidders delivery quality in the following key areas: 1) Service Management 2) Cyber Security Services on (Network Detection and Response) 3) Architecture 4) Project Management 5) Service Delivery	Fully complies = 2 Partially complies = 1 Does not comply = 0	20%	Fully Complies: All areas satisfied Partially Complies: 1 or 2 areas not satisfied or not delivered Does not Comply: > 2 areas not satisfied or not delivered
2.4 Transition project delivery	To verify that the bidder has effectively delivered on a transition project from a previous service provider for the reference client	The reference client will be interviewed to verify the reference's satisfaction (Yes or No) with bidders delivery quality in the following key areas for a transition project: 1) On time execution 2) On budget delivery 3) Effective Change Management 4) Effective testing 5) Effective overall project Management	Fully complies = 2 Partially complies = 1 Does not comply = 0	15%	Fully Complies: <=1 area not satisfied Partially Complies: 2 areas not satisfied Does not Comply: > 2 areas not satisfied or not delivered



Step Four: Due Diligence – Refer to Annexure E

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring Criteria	Weightings out of 100%	Score guide
'2.5 Relationship management	'To verify the bidder's capability to provide effective relationship management	The reference client will be interviewed to verify their overall perception of the bidders capability to provide effective relationship management	Fully complies = 2 Does not comply = 0	10%	Fully Complies: Satisfied relationship management Does not Comply: Dissatisfied relationship management
'2.6 Effectiveness in Threat Detection and Response	'To verify the bidder's capability in providing NDR Solution to mitigate cyber attacks	The reference client will be interviewed to get feedback on the solution's effectiveness in detecting and responding to security threats.	Fully complies = 2 Partially complies = 1 Does not comply = 0	10%	Fully Complies: Satisfied on feedback regarding detecting security threats, and examples. of incidents detected and responded to. Partially Complies: if one of the two is provided Does not Comply: Dissatisfied by the answers given
2.7 NDR	To verify the bidder's capability to provide an effective Network Detection and Response solution	The reference client will be interviewed to verify their overall experience of the bidders capability to provide and run an Network Detection and Response Solution for the services in scope	Fully complies = 2 Does not comply = 0	10%	Fully Complies: Fully satisfied with the bidder's capability to provide the Network Detection and Response solution. Does Not Comply: Not satisfied with the services within the defined scope.



Step Four: Due Diligence – Refer to Annexure E

Area	Requirements	Provide Evidence /Supporting Documents and Include as an Appendix to this Annexure and indicate reference hereunder	Scoring Criteria	Weightings out of 100%	Score guide
'2.8 Technical staff capability	'To verify the bidder's qualify of technical staff	The reference client will be interviewed to verify their overall perception of the bidders technical staff quality (certification, training, professionalism, etc) in the following key areas: 1) Deployment services 2) Network Detection and Response services 3) Maintenance services	Fully complies = 2 Does not comply = 0	15%	Fully Complies: all areas satisfied Does not Comply: =/ >1 areas not satisfied or not delivered
Total	100				
Minimum Threshold	70				



Step Five : Price and B-BBEE

Broad-Based Black Economic Empowerment criteria [Weighted score 10 points]

- ☐ B-BBEE - current scorecard / B-BBEE Preference Points Claims Form
- ☐ Preference points will be awarded to a bidder for attaining the B-BBEE status level of contribution in accordance with the table indicated in Section 9 no. 1.4 of the B-BBEE Preference Points Claim Form in Section 9 of the RFP.

Preference Point System 90/10			
#	Specific Goal	Number of Points	Price
1	B-BBEE Level 1 and 2	5	90
2	Black Owned (51%)	2	
3	Job creation	3	
	Total	10	

Evaluation Criteria	Final weighted score
Price and Total cost of ownership	90
*BBBEE scorecard	10
Total	100

Pricing Schedule Refer to Annexure A

**FOR THE PROVISION OF NETWORK DETECTION AND RESPONSE (NDR) SOLUTION FOR A PERIOD OF THREE (3) YEARS.
TCC/2024/12/0001/84866/RFP**

Annexure A Service-Based

#	Item Description	Unit of Measure	Baseline QTY	Year1 (Incl. VAT (ZAR))	Year2 (Incl. VAT (ZAR))	Year3 (Incl. VAT (ZAR))	Total
1	Recurring Cost	Support and Maintenance (Reporting and Monitoring)					R -
2	Licenses	End Points	40602		R -	R -	R -
3	Transition Costs	Mobilizing cost and Installation Cost					R -
4	Training Costs		50 Engineers	R -			R -
	Total including VAT			R -	R -	R -	R -

Notes to Pricing:

a) Respondents are to note that if the price offered by the highest scoring bidder is not market-related, Transnet may not award the contract to that Respondent. Transnet may-

(i) negotiate a market-related price with the Respondent scoring the highest points or cancel the RFP;

(ii) if that Respondent does not agree to a market-related price, negotiate a market-related price with the Respondent scoring the second highest points or cancel the RFP;

(iii) if the Respondent scoring the second highest points does not agree to a market-related price, negotiate a market-related price with the Respondent scoring the third highest points or cancel the RFP.

If a market-related price is not agreed with the Respondent scoring the third highest points, Transnet must cancel the RFP.

b) Prices must be quoted in South African Rand inclusive of VAT.

c) Any disbursement not specifically priced for will not be considered/accepted by Transnet.

d) Transnet will be paying licences annually.

e) To facilitate like-for-like comparison bidders must submit pricing strictly in accordance with this pricing schedule and not utilise a different format. Deviation from this pricing schedule could result in a bid being declared non-responsive.

f) Please note that should you have offered a discounted price(s), Transnet will only consider such price discount(s) in the final evaluation stage if offered on an unconditional basis.



Step Six: Post Tender Negotiations (if applicable)

- Respondents are to note that Transnet may not award a contract if the price offered is not market-related. In this regard, Transnet reserves the right to engage in PTN with the view to achieving a market-related price or to cancel the tender. Negotiations will be done in a sequential manner i.e.:
 - first negotiate with the highest ranked bidder or cancel the bid, should such negotiations fail,
 - negotiate with the 2nd and 3rd ranked bidders (if required) in a sequential manner.
- In the event of any Respondent being notified of such short-listed/preferred bidder status, his/her bid, as well as any subsequent negotiated best and final offers (BAFO), will automatically be deemed to remain valid during the negotiation period and until the ultimate award of business.
- Should Transnet conduct post tender negotiations, Respondents will be requested to provide their best and final offers to Transnet based on such negotiations. Where a market related price has been achieved through negotiation, the contract will be awarded to the successful Respondent(s).



Step Seven: Objective Criteria (if applicable)

- Transnet reserves the right to award the business to the highest scoring bidder/s unless objective criteria justify the award to another bidder. The objective criteria Transnet may apply in this bid process include:
 - all Risks identified during a risk assessment exercise/probity check (which may be conducted by an authorised third party) that would be done to assess all risks, including but not limited to:
 - the financial stability of the bidder based on key ratio analysis, which would include, but not be limited to Efficiency, Profitability, Financial Risk, Liquidity, Acid Test, and Solvency;
 - A commercial relationship with a Domestic Prominent Influential Person (DPIP) or Foreign Prominent Public Official (FPPO) or an entity of which such person or official is the beneficial owner; and
- the tenderer is not under restrictions, or has principals who are under restrictions, preventing participating in the employer's procurement,
- the tenderer is not undergoing a process of being restricted by Transnet or other state institution that Transnet may be aware of



Step Eight: Award

- Immediately after approval to award the contract has been received, the successful bidder(s) will be informed of the acceptance of his/their Bid by way of a Letter of Award. Thereafter the final contract will be concluded with the successful Respondent(s) where applicable.
- Alternatively, acceptance of a letter of award by the Successful Respondent will constitute the final contract read together with their RFP response and the Standard Terms and Conditions. This will be stated in the letter of award.



How to Improve Success of Bid Submission

Most common mistakes/reasons bidders are not successful in their bid submissions

Prequalifying Criteria

- Failure to meet mandatory requirements.
- Non-submission of mandatory requirements/supporting as per RFP requirements.
- Invalid / expired mandatory documents submitted.

Functional Requirements

- Failure to respond to the requirements as per the RFP.
- Response to requirements not clearly articulated in the bid submission.
- Non-submission of supporting documents.
- Not using the technical evaluation criteria as a guide to respond to key requirements for points allocation.

Administrative

- Bid submission not reviewed internally for completeness, accuracy and relevance to the RFP terms of reference.
- Documents not signed by duly authorised person.
- Documents partially completed
- Last minute submission.



Questions and Closure

All questions arising from this compulsory briefing session must be put in writing on the (Section 8) RFP Clarification Form submitted on the system and sent to Mahlodi.Kganyago@trasnet.net Reetsang.Modise@transnet.net before **12h00** pm on **29 May 2025**.

TRANSNET



Thank you

