STATEMENT OF WORK

For: Network Detection and Response (NDR)-Three (3) year

Project Name: Trans-NDR-01
Project Number:

Author:
Owner: Transnet
Client: <Client>
Project Sponsor: <Xolani Lukhele>
Project Manager: <Nhlanhla Shongwe>

Revision Number: Trans-NDR-01
Approved by:

Release Date:
Print Date: 10/02/2026
Template Date: 01/01/2012

Distribution	
Name	Location

DOCUMENTATION DISTRIBUTION, REVISION AND APPROVAL HISTORY

REVISION NUMBER	DATE	DISTRIBUTION/ REVISION	PREPARED BY	REVIEWED BY	APPROVED BY
Trans-NDR-01	19/09/2025	10/02/2026	Zukile Wayini	Barend Pretorius	Xolani Lukhele

Statement of Work

Planned start:	**1 April 2026**
Planned finish:	**31 July 2026**
Key contact name:	**Nhlanhla Shongwe**

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, behavioural analysis, and threat intelligence to identify anomalies and mitigate risks before they can cause significant harm.

While our current security infrastructure can address some aspects of network protection, it falls short in delivering comprehensive coverage and real-time response capabilities. This limitation leaves Transnet at a disadvantage in today's rapidly evolving threat landscape, where cyberattacks are increasingly sophisticated and frequent. Addressing this gap is essential to safeguarding the organisation's digital assets and maintaining the trust of our stakeholders.

To strengthen our defences against advanced threats, we propose implementing an NDR solution by deploying monitoring sensors across 50 Transnet Campus Sites, as listed in **Appendix A**. These sensors must support trunk ports and be VLAN tag-aware to ensure comprehensive network monitoring. By improving our ability to detect and respond to suspicious activities promptly, we can protect sensitive data, maintain operational integrity, and ensure compliance with regulatory requirements.

Transnet is seeking a service provider to implement a service-based NDR solution, where the service provider will deliver the solution as a service to Transnet, without Transnet owning the software or physical devices. The proposals will be thoroughly assessed to ensure alignment with Transnet's strategic objectives, operational needs, and cybersecurity requirements, ultimately supporting our long-term goals.

Investing in an NDR solution is not just a strategic move but a critical step in securing Transnet's digital infrastructure. Adopting this technology can enhance our cybersecurity posture, reduce risks, and strengthen our resilience against increasingly sophisticated cyber threats.

Responsibility of parties

Transnet Group ICT will be responsible for the first-line support of the NDR solution.

Deliverables

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.
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. **Behavioural Analytics:** Use of machine learning and Artificial Intelligence to establish a baseline of normal network behaviour and identify deviations indicative of potential threats.
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.
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 Behaviour Analytics (UEBA):** Monitoring user and entity behaviour 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.
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.

NETWORK DETECTION AND RESPONSE SOLUTION– OVER THREE (3) YEARS

#	Item	QTY	Description
1	**Number of Endpoints**	40602	▪ 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)	▪ 47 Campus Sites geographically dispersed across the country. ▪ 3 TERACOs
3	**Support and Maintenance**	3 years	▪ Costs for support and maintenance over three years.
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 organisations.

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		