CLARIFICATION QUESTIONS AND ANSWERS

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

BATCH 1 - CLARIFICATION QUESTIONS AND TRANSNET RESPONSES

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
1	Please advise if we comply as a ISO 27001 company but are not certified, can we submit our compliance documents, will they be allowed?	Only ISO 27001 certifications will be accepted and not just compliance.
2	OEMs do not provide letters that confirm that we confirm that we are an authorised reseller/distributor of NDR Solution however it states that we are partners, please advise if that standard letter will be acceptable for Transnet. **Pre-qualification Criteria/Mandatory** • 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. • ISO 27001 certification: 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. • 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	Partners with letter from OEM will be accepted, a letter with an OEM letterhead.

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	authorised reseller/distributor of the Network Detection and Response (NDR) Solution.	
3	In order for NDR vendors to scope the deployment we need the following confirmed please: a) Total number of Internet Breakouts and where are they located. b) Where is DNS, Kerberos and DHCP served from? Local to each site or centralised from Teraco/HQ? c) Are there PACKET BROKERS or taps installed already at the Teraco sites? Packet brokers allow all traffic Mic to be monitored and reduces the hardware deployment requirements. i. Would Transnet prefer the NDR vendors to install with packet brokers?	a. 3 Internet breakouts. Details will be provided to the winning bidder. b) DNS, and Kerberos are hosted in 141 Sivewright. DHCP is decentralized and is configured on gateways, which are dispersed across the country. We don't have packet brokers anymore.
4	Under 3.3 Expected Functional Requirements (q), cloud asset monitoring is included, does Transnet expect full Cloud Detection and Response (CDR) capabilities as an extension of the NDR?	Yes
5	Under 3.3 Expected Functional Requirements (i), User and Entity Behaviour Analytics is included for compromised account detection, does Transnet want Detection and Response extended into their SaaS environment? For example, advanced monitoring of OMice 365 for account protection and data loss prevention?	This should cover the Transnet cloud-based Identity provider, and the corresponding tenant….not necessarily every SaaS solution Transnet has. The details about the cloud platform will be shared with the successful bidder. Bidders must list all the cloud

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
		platforms their proposed solution is compatible with.
6	If query 2 and 3 are a requirement then is it possible to please add Cloud Workloads and SaaS Account Protection as line items to the quote?	The quote cannot be changed.
7	Is multi-tenant support available for managing multiple environments? Please elaborate on what is meant by multi-tenant?	Transnet has multiple divisions, for example: TCC, TNPA, TFR, TPT, TPL, TP, and TE. Multi-tenant support means allowing each operating division to have its own isolated network security monitoring environment while sharing the same underlying NDR infrastructure. We also want the solution to provide Transnet's central security team with aggregated threat intelligence across divisions to identify enterprise-wide attack patterns or coordinated threats targeting multiple operating divisions.
8	Can it operate effectively with limited bandwidth environments? Is Transnet referring to smaller span traffic bandwidth?	Yes.
9	Can it identify and report misconfigured devices or services? As NDR is a network solution, what details are you looking for on misconfigured devices?	This, for example mean detecting default credentials still in use, unnecessary open ports, disabled security features, or overly permissive access controls.
10	Does the solution integrate with leading endpoint detection and response (EDR) tools? What is the EDR tool that needs	The details about the currently deployed technology /solutions will be shared with the successful bidder.

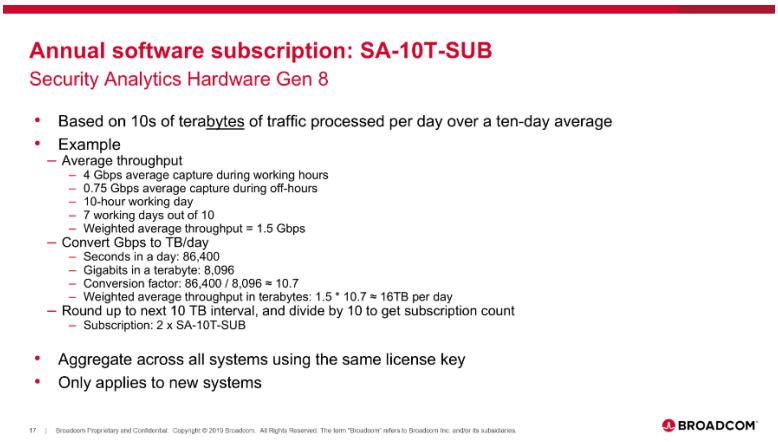
No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	integration? Also can you advise what integration is needed or is the integration to be done at a SOAR/SIEM level?	Bidders must list all the security systems their proposed solution can integrate with natively, and advise the level of integration for each system.
11	Can it connect to threat intelligence platforms (TIPs) for enhanced threat detection? What is the current TIP platform that needs integration?	The proposed NDR solution must have connections to reputable threat intelligence databases to continuously learn about new threats.
12	Does it support integration with third-party vulnerability management solutions? What is the solution being used?	The details about the currently deployed technology /solutions will be shared with the successful bidder. Bidders must list all the security systems their proposed solution can integrate with natively.
13	Is the solution interoperable with existing identity and access management (IAM) systems? What is the IAM solution being used?	The details about the currently deployed technology /solutions will be shared with the successful bidder. Bidders must list all the security systems their proposed solution can natively integrate with.
14	Does this solution integrate with SOAR platforms? What is the SOAR solution being used?	The SOAR platform is used for automating incident investigations and responses. The details about the currently deployed technology /solutions will be shared with the successful bidder. Bidders must list all the security systems their proposed solution can integrate with natively.
15	Transnet Campus Sites	There are no hypervisors in these sites. We have a data throughput of about 1

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	What is the infrastructure at these sites? Is there hyper visors available, if so what vendor? Also what is the throughput of the switch per site and can the swich do span traffic?	Gig in most of these sites. Yes the switches have the span capability.
16	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. Please advise what technology and integrations are required?	The details about the currently deployed technology /solutions will be shared with the successful bidder. Bidders must list all the security systems their proposed solution can integrate with natively.
17	Automated Response: Automated actions in response to detected threats, such as isolating affected devices, blocking malicious traffic, and alerting security teams – From and automated response such as isolating devices, as this is a network solution, what is the expectation to isolate devices? Can this be achieved using the SOAR/SIEM at Transnet? What is the firewall vendor being used to understand integration between the 2 solutions.	We expect the solution to integrate with existing Palo Alto, Network Access Control, and SIEM/SOAR tools to facilitate the blocking and isolation capabilities.
18	Encrypted Traffic Analysis: Ability to inspect encrypted traffic without compromising privacy, using techniques such as SSL/TLS decryption or machine learning. Is this required across the sites or only the main sites? SSL interception is very hardware intensive and virtual solution don't have this capabilities.	Main sites (3 internet breakouts).
19	Scalability and Performance: Capability to handle high volumes of traffic across large, distributed networks without significant performance degradation.	I Gig

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	Please provide core switch throughput per site that will be sent to the NDR appliance.	
20	Compliance Reporting: Generation of reports to assist with compliance requirements for various regulations (such as POPIA) and standard (e.g., CIS). As various compliance requirements cover a number of different security controls (eg, Endpoint, Email ,Server, Network etc), how does this requirement go back to a NDR solution as the NDR solution only covers the network control. Should the compliant template only cover network?	Compliance reporting in a Network Detection and Response (NDR) solution should support the automated generation of reports that demonstrate adherence to regulatory requirements and industry standards. For POPIA compliance, the solution should provide evidence showing how network monitoring contributes to the protection of personal information, supported by access control and encryption insights through integration with existing tools such as Microsoft E5 or NAC. It should facilitate breach notification reporting by generating automated incident records, tracking detection and response timeframes, and producing documentation aligned with Section 21 requirements. The NDR should offer continuous monitoring and anomaly detection to strengthen data protection efforts. In alignment with CIS Controls, the solution should deliver reporting capabilities for network monitoring (Control 12), including traffic analysis and anomaly detection; data protection (Control 13), with visibility into data loss and

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
		unauthorised access attempts; access control monitoring (Control 6), through inferred access patterns; and incident response (Control 19), by documenting security events and response timelines. These capabilities are expected to be enhanced through seamless integration with the organisation's existing security infrastructure, including SIEM, XDR, NAC, firewalls, and Microsoft E5 security solutions.
21	Multi-cloud and Hybrid Environmental support: Capability to monitor and protect assets across on premises, azure cloud and hybrid environments. Can you advice on what cloud platforms are being used and also what hyper visors.	The details about the currently deployed technology /solutions will be shared with the successful bidder. Bidders must list all the cloud platforms and hypervisors their proposed solution is compatible with.
22	Data Retention and Archiving: Long-term storage of network traffic data for historical analysis and compliance purposes Please advise on the data retention requirements, can it be shipped off to a SIEM/SYLOG for storage by Transnet?	At least six months of hot storage. It should be possible to move (archive) the logs to an external low-cost storage
23	Price book refers to a service type agreement license paid annually as NDR requires network probe devices in the environment how will equipment purchase be handled? This equipment will be for the exclusive use of Transnet and could possibly be financed over the period but as it is annual payments costs will increase and not be a true reflection of the actual costing, how does Transnet want this handled or can this be part of the transition costs?	This must be covered under Transition Costs - Mobilizing and Installation cost.

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
24	Are there network diagrams available as well as full utilization stats?	Details will be provided to the winning bidder.
25	Is 1 gig per campus site sufficient?	Yes
26	Your reference list says 3 references per category. Thats a total of 9 references from a single service provider. This is a bit high, previous bid were 1 each?	No, only 3 reference letters. They will determine the scoring. I.e. if • 0 points for no reference letters or for less than 5 000 end points • 9 points for 3x client reference letters of Network Detection and Response Solution tool between 5 000 and 10 000 end points. • 15 points for 3x client reference letters of Network Detection and Response Solution tool between 10 000 and 15 000 end points • 24 points for 3x client reference letters of Network Detection and Response Solution tool more than 15 000 end points
27	What is the intended time to start the project?	As soon the contract is awarded.
28	You requested four months to complete. Resources will be calculated based on these 4 months, what happens if Transnet delays the process for various reasons like change control and downtime or access safety files etc. how will that be treated as contracts are usually fixed term fixed value?	Transnet estimated the process to take 4 mouths. The Service provider must quote for the time specified. Should there be delays Transnet will follow its internal procurement processes.
29	Is there a chance of this being cancelled like XDR on the last day as a lot of effort goes into these submissions?	No.

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
30	With the Roe so volatile and payments done annually will subject to roe be acceptable for year 2 and 3?	Bidder must provide a fixed prices for a period of three (3) year cost considering also the ROE.
31	Total capturing throughput (Please refer to the below for throughput sizing)	In each campus site, the switches have 1 Gigabit throughput, and the switches in each of the three teracos have 10 Gigabit throughput.
32	Retention period: Usually customer ask for 1 week or 2 weeks (this will help you to decide small storage or large one.)	At least six months of hot storage. It should be possible to move (archive) the logs to an external low cost storage
33	Capturing sources: We need to understand how many links or the network where the customer would like to capture and interface type (this is to size the SSLV)  **Annual software subscription: SA-10T-SUB** Security Analytics Hardware Gen 8 • Based on 10s of terabytes of traffic processed per day over a ten-day average • Example – Average throughput – 4 Gbps average capture during working hours – 0.75 Gbps average capture during off-hours – 10-hour working day – 7 working days out of 10 – Weighted average throughput = 1.5 Gbps – Convert Gbps to TB/day – Seconds in a day: 86,400 – Gigabits in a terabyte: 8,096 – Conversion factor: 86,400 / 8,096 ≈ 10.7 – Weighted average throughput in terabytes: 1.5 * 10.7 ≈ 16TB per day – Round up to next 10 TB interval, and divide by 10 to get subscription count – Subscription: 2 x SA-10T-SUB • Aggregate across all systems using the same license key • Only applies to new systems 17 | Broadcom Proprietary and Confidential. Copyright © 2019 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. BROADCOM	100 links (this caters for both active and passive links)
34	Please provide a recording and minutes for the briefing session for the above tender.	The briefing presentation and minutes are published on the National Treasury e-tender portal and Transnet e-tender portal.
35	We are writing to respectfully request clarification on whether the RFP is indeed an open tender, as advertised via the National Treasury and Transnet portals, or if it is restricted to a predefined list of vendors. Our understanding from the published RFP is that it is open to	Refer to the minutes published; the RFP is open to ALL Service Providers rendering NDR Solution.

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	all compliant bidders. However, we have received conflicting feedback from the market suggesting otherwise. As such, Palo Alto Networks' eligibility and interest in participating via our authorized partners and seeks confirmation that compliant OEMs not explicitly listed by Gartner BuySmart may still be considered. We would appreciate your confirmation on this matter to ensure that our partners are positioned to respond correctly and in accordance with Transnet's expectations.	
36	Number of Internet Breakouts and where they are located?	3 Internet breakouts. Details will be provided to the winning bidder.
37	Where is DNS, kerberos and DHCP served from? Local to each site or centralised?	DNS service is centralized, and DHCP is decentralized (local to each site).
38	How are the sites connected to one another? (MPLS, SD-WAN, Site to site VPN)?	A combination of MPLS and SD-WAN
39	Do they have an estimate of the throughput of the core switches at the Teraco sites?	10 Gigs
40	Do they have packet brokers or taps installed already at Teraco?	No, but the switchports support tap mode
41	Is SaaS account protection in scope for this RFP	Refer to ques. 5 above
42	With reference to TCC/2024/12/0001/84866/RFP – NDR provision for 3 years. Has Transnet been made aware of the crucial importance in including a packet-broker solution as part of an NDR sourcing? Network Packet Brokers (NPBs) are crucial for Network Detection and Response (NDR) by providing a central point	This is not needed at this moment.

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	for traffic aggregation, filtering, and distribution, enabling security tools to access the necessary data for threat detection and response. They enhance visibility, optimize tool performance, and facilitate efficient network analysis, ultimately improving cybersecurity posture. I would urge Transnet to please reach out to explore this, as inclusion of a NPB would ultimately make NDR solutions viable. Without a NPB in place together with the NDR, it becomes expensive to scale the NDR solution, with limited visibility. Could we please discuss?	
43	Price book refers to a service type agreement: Licenses paid annually - as NDR requires network probe devices in the environment how will equipment purchase be handled? the equipment will be for exclusive use of Transnet and could possibly be financed over the period but as it is, annual payments costs increase and might not be a true reflection of the actual costing, how does Transnet want this handled or can this be part of transition costs	Repeat of Q23
44	Is there network diagrams available as well as utilization stats	Repeat of Q24
45	Is 1gig per campus site efficient	Repeat of Q25
46	Kindly advice how many references are required?	3 references. Refer to response Q26.
47	What is the intended time to start the project?	Repeat of Q27. As soon as awarded.
48	Project timeline is set at 4 months, resources will be calculated based on these 4 months,	Repeat of Q28.

No:	CLARIFICATION QUESTIONS	TRANSNET RESPONSE
	what happens if there's a delay in process for various reasons like change control/downtime how will that be treated as contracts are usually fixed term fixed value?	
49	We respectfully request that Transnet SOC Ltd consider allowing Palo Alto Networks to participate in this RFP process and submit a proposal for the NDR solution, despite our potential absence from an initial vendor list. We believe that evaluating our offering would be beneficial to Transnet in ensuring the most effective and potentially cost-efficient solution is selected.	Refer to the minutes published; the RFP is open to ALL Service Providers rendering NDR Solution.
50	Given the complexity of this tender and the detailed requirements, we'd like to kindly request an extension to the current submission deadline to ensure a thorough and complete response. Thank you for your consideration.	Refer to Addendum 1 of the RFP. The RFP closing date has been extended to 30 June 2025.