Eskom National Transmission Company South Africa ™	**Report**	**National Transmission Company South Africa**

Title:	**Technical Evaluation Criteria for NTCSA OT NIDS and EDR Solution**	Document Identifier:	**240-185000629**
		Alternative Reference Number:	**N/A**
		Area of Applicability:	**National Transmission Companv South Africa**
		Functional Area:	**Engineering**
		Revision:	**1**
		Total Pages:	**27**
		Next Review Date:	**N/A**
		Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Approved by**	**Authorized by**
Thendo Ramulondi	**Mpumelelo Mathe**	**Judith Malinga**
Chief Engineer – CATS - PTM&C Engineering	**Middle Manager – CATS - PTM&C Engineering**	**Senior Manager PTM&C Engineering**
Date: 06/11/2025	Date: 2025/11/07	Date: 07/11/2025

PCM Reference: **240-53458797 PCM for Perform PTM&C Systems Engineering**
SCOT Study Committee: **Tools and Systems Study Committee**
Reference - Template ID: 559-751375159 Document Template

Content

Figures

Tables

1. Introduction

NTCSA Operational Technology (OT) intends to enhance its cybersecurity posture by acquiring a Network Intrusion Detection System (NIDS) and Endpoint Detection & Response (EDR) solution. This document outlines the technical evaluation criteria and provides guidance for Tenderers responding to this enquiry.

2. Supporting Clauses

2.1 Scope

The document covers the technical evaluation criteria for the NIDS and EDR solution for NTCSA's OT systems. This includes technical tender guidelines:

- Evaluation guidelines
- Submission guidelines
- Technical returnables
- Price schedules guidelines

This document does not cover the Network Intrusion Detection System (NIDS) and Endpoint Detection & Response (EDR) specific requirements, those are prescribed in: *240-170000847 Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems*

2.1.1 Purpose

This document sets the context in which the Tenderer should approach this enquiry and defines the technical evaluation criteria that will be used in this enquiry. This is necessary so that Tenderers understand the enquiry's technical context, intent, scope of work and evaluation criteria. This will ensure that Tenderers submit the enquiry returnables which are populated based on a common technical understanding between both the *Purchaser* and *Supplier*.

2.1.2 Applicability

This document shall apply throughout National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30.

2.1.3 Effective date

The effective date is the date of the authorising signature.

2.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

[1] ISO 9001 Quality Management Systems

[2] 240-170000847 Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems – Rev 2

[3] Scope of Work for Supply and Delivery of an NTCSA OT Network Intrusion Detection System and Endpoint Detection Response Solution

[4] 240-170001061 Transmission Cybersecurity Standard for Operational Technology

2.2.2 Informative

[5] 240-48929482 Tender Technical Evaluation Procedure.

2.3 Definitions

Definition	Description
Endpoint Detection & Response System	a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.
Enquiry	A collective and generic term for requests for information, expressions of interest, request for quotations, invitations to tender or requests, proposals made to the Supplier, group of Suppliers or market at large.
Intrusion Detection System	A device or software application that monitors network or system activities and sends alerts to system administrators on possible intrusions.
Network Intrusion Detection System	Placed at a certain point of the network and detects threats on all traffic to and from devices on the network.
Submission	The tender in accordance with the requirements of the enquiry.
Technical evaluator	Technical experts nominated by the end-user and divisional technical functionaries with the necessary technical expertise.
Tender	A tender refers to a written competitive offer, quotation, and/or proposal made by the Supplier in a prescribed or stipulated form in response to an invitation to tender/competitive enquire for provision of assets/goods or services and or the disposal thereof.

2.4 Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
BoQ	Bill of Quantities
CFT	Cross Functional Team

Abbreviation	Explanation
CoE	Centre of Excellence
DES	Desktop Evaluation Score
ML	Machine Learning
NEC	New Engineering Contracts
NTCSA	National Transmission Company South Africa
OEM	Original Equipment Manufacturer
OT	Operational Technology
PRES	Product Risk Evaluation Score
SIEM	Security Information and Event Management
SOAR	Security Orchestration and Response
TER	Technical Evaluation Report
TES	Technical Evaluation Score
TET	Technical Evaluation Team

2.5 Roles and Responsibilities

The *Purchaser*, all Tenderers tendering on the NIDS and EDR for NTCSA's OT Systems enquiry and all the *Suppliers* to which New Engineering Contracts (NEC) have been awarded to, shall be cognisant of the overview of requirements throughout the enquiry process and contract period.

2.6 Process for Monitoring

Not applicable.

2.7 Related/Supporting Documents

This technical criteria document shall be read in conjunction with the following documents:

- 240-170000847 Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems – Rev 2 [2]
- Scope of Work for Supply and Delivery of an NTCSA OT Network Intrusion Detection System and Endpoint Detection Response Solution document [3]

3. Technical Evaluation

Supplier evaluations are conducted to determine their capability to enter into a contract with NTCSA. A report, along with any actions listed or recommended as a result of these assessments, does not constitute confirmation or a guarantee that a contract will be awarded by NTCSA.

Any actions taken by a Supplier based on this report are entirely at the Supplier's own risk and expense. NTCSA assumes no liability for such actions under any circumstances.

The evaluation team has no authority or responsibility regarding NTCSA's final decision to contract for any product, solution, or service. Furthermore, any statements, intentions, or actions expressed by the evaluation team during or after the assessment must not be interpreted as a contract award and do not create any obligation or liability for NTCSA concerning contract placement or post-contract performance guarantees.

This **enquiry,** comprises of two **distinct packages**:

- **Package 1:** Network Intrusion Detection (NIDS) system
- **Package 2:** Endpoint Detection and Response (EDR) system

Suppliers may tender for **one package or both**, based on their capability and interest.

Each package will be evaluated **separately**, following its own evaluation criteria and scoring process.

There is **no dependency between the two evaluations—**performance in one does not affect the other.

3.1 Technical Evaluation Guideline

A technical evaluation team (TET) will be constituted by members of the cross functional team (CFT). Each submission will be independently assessed by at least three (3) members of the TET. Where there are inconsistencies between the independent TET members scores, the reconciliation of those scores will be through the process outlined in section 3.4.2.3 of document 240-48929482 Tender Engineering Evaluation Procedure.

The following outlines the process that will be applied to assess submissions.

Stage 1: Mandatory Requirements

- These are critical compliance checks that ensure the Supplier meets all essential conditions before any technical evaluation begins.
- **NB:** If these requirements are not met, the evaluation shall not proceed to any further stages.

Stage 2: Desktop Evaluation (Pre-requisite for Next Stages)

- **Purpose:** This phase assesses the Supplier's proposed solution against detailed technical specifications and requirements.
- **Weight:** 50%
- **Minimum Overall Score:** 70%
- **Category-Level Minimums:**
  - Functional ≥ 70% (core technical capabilities)
  - General ≥ 70% (integration, compatibility, and governance requirements)
  - Service ≥ 70% (delivery, support, and maintenance commitments)
- **NB:** Suppliers who fail this stage shall not proceed to Product Demonstration or Risk & Support evaluation stages.

Stage 3: Product Demonstration

- **Purpose:** Evaluates the actual performance and functionality of the proposed solution in a live or simulated environment.
- **Weight:** 50%
- **Minimum Score:** The Tenderer shall must achieve a minimum threshold of 70% to be considered for subsequent evaluation phases.

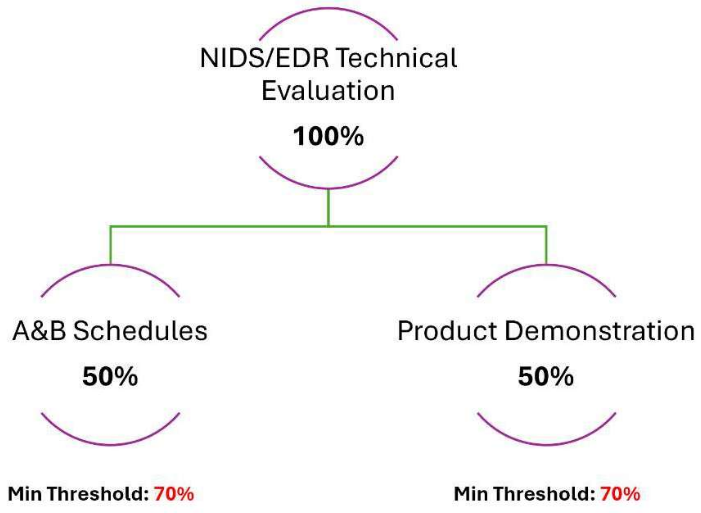

Figure 1: Technical Evaluation Score Weighting Composition Overview

Stage 4: Risk and Support

- **Purpose:** Assesses the Supplier’s ability to provide ongoing support, manage risks, and ensure business continuity.

3.2 Submission of Tender Returnable

3.2.1 Indication of Tendered Solution Package

In this section, the applicable solution(s) being tendered must be indicated. *Table A.1: Indication of Tendered Solution Package* provides three options:

- Select the first row if tendering for the **NIDS Solution only** (Network Intrusion Detection System).
- Select the second row if tendering for the **EDR Solution only** (Endpoint Detection and Response).
- Select the third row if tendering for **both NIDS and EDR Solutions**.

An **"X"** should be placed in the column titled *Mark the applicable option (X)* next to the relevant choice. Only one option should be marked to ensure clarity regarding the scope of the proposal.

3.2.2 Tender submission technical guidelines

These guidelines have been developed to aid in the tender evaluation process for both Tenderer and the *Purchaser's* evaluation team. It is strongly encouraged for Tenderers to comply with the following set of guidelines:

a) Detail all answers sufficiently to give the *Purchaser's* evaluation team a clear understanding of the answer. Unclear and insufficiently detailed answers could result in items being ambiguous and misinterpreted and could result in an unfavourable score.

b) Where a requirement asks for compliance ("State compliance" in Schedule A), please respond in Schedule B with only one of the following:

1) **Comply –** this indicates full compliance to the requirement at time of tender submission
2) **Partially comply –** this indicates that the Tenderer only complies with a part of the requirement.
3) **Non-comply –** this indicates that the requirement is currently not supported and will not be available for this project.

c) Where possible, all responses to Schedule A shall state compliance and provide a reference to supporting documentation in the Reference/Justification column.

d) Where the Tenderer is supplying electronic documentation, arrange the folders and subfolders into a well organised and structured hierarchy making them logical and sensible to navigate.

e) Name the files that constitute the electronic returnables appropriately based on the content of the document or file.

f) Submit returnable digital PDF documents in searchable format as far as possible. This is preferred to scanned documents that cannot be searched.

g) Submit returnable digital PDF documents including a table of contents as far as possible.

h) For the technical electronic submission, the following is required:

1) Create an 'Electronic Technical Tender Returnables' folder with logically structured subfolders .
2) Within the "Electronic Technical Tender Returnables" folder the excel document(s) called "NIDS Technical Schedules" and/or "EDR Technical Schedules" shall be placed**. These technical schedules will constitute the bulk of the electronic technical tender submission and MUST be completed.**
3) Subfolders within the "Electronic Technical Tender Returnables" folder may be created that match the sheet names within the NIDS/EDR Technical Schedules excel files. These folders shall contain the supporting material referenced within the excel sheets.

3.2.3 Returnables Checklist for NIDS and EDR Tender Submission

This section provides a comprehensive checklist intended for the Tenderer. Its primary objective is to facilitate verification that all required technical documentation for the NIDS and/or EDR solutions has been duly completed and included in the submission. Each checklist item corresponds to a specific worksheet referenced within the relevant Technical Schedules.

The Tenderer shall complete Table A.2 **and/or** Table A.3 under *Appendix D: Tender Technical Returnables Checklists* depending on whether they are tendering for the NIDS and/or EDR solutions.

3.3 Mandatory Requirements

Mandatory criteria are non-negotiable and must be met. These criteria shall not be weighted or point scored but shall be assessed on a Yes/No basis as to whether or not the criteria are met. An assessment of 'No' against any criterion shall technically disqualify the Tenderer and shall not be further evaluated against Qualitative Criteria. The Tenderer shall indicate compliance to the mandatory requirements by completing the following worksheets:

- ***01-NIDSTechGatekeepers*** for NIDS under NIDS Technical Schedules spreadsheet **and/or**
- ***01-EDRTechGatekeepers*** for EDR under EDR Technical Schedules spreadsheet

The Tenderer shall also provide evidence in the form of a signed letter in the company letterhead confirming compliance to the mandatory requirements

3.4 General Questionnaire

This section is intended to gather essential details about the Tenderer, the Original Equipment Manufacturer (OEM), and the proposed solution. The information provided will serve as a reference for administrative and record-keeping purposes and will assist in ensuring that all submissions are properly documented. It is not used for evaluation or scoring but is required to maintain completeness and transparency in the tender process. The Tenderer shall complete the following worksheets:

- ***02-GenNIDS*** for NIDS under NIDS Technical Schedules spreadsheet **and/or**
- ***02-GenEDR*** for EDR under EDR Technical Schedules spreadsheet

3.5 Qualitative Evaluation Criteria

Tender responses shall be evaluated using the methodology of the Preferential Procurement Policy Framework Act (Act 5 of 2000).

This section details the methodology to be employed by the *Purchaser* in scoring the qualitative section of the evaluation.

Table 1: Technical Categories

Technical sub-category	Sub-category name	Weight
1	Product A&B Schedules	50%
2	Product Demonstration	50%

Tenderers are allowed to tender on both the NIDS and EDR solutions or on either NIDS or EDR. Taking this into account, the technical evaluation for NIDS and EDR will be separated as to ensure that each solution can be compared across all tenders.

3.5.1 Sub-category 1: Product A&B Schedules

This section shall comprise scoring of the technical schedules of both the NIDS and/or EDR depending on what the Supplier is tendering for.

Each item will be assigned a score by the *Purchaser's* technical evaluation team based upon the tendered response and cross-checked with the supporting documents provided.

Table 2: Scoring of items in Technical A&B Schedules

Criteria	Score
Fully compliant	4
Partially compliant (minor deviation)	1
Non-compliant (major deviation)	0

Table 3 and Table 4 below summarize the weight distribution of the subsections of schedules A&B as well as the minimum threshold that must be acquired on each sub-section.

Table 3: Percentage weight of NIDS specifications

No.	Product	Specification	Weight	Minimum Threshold
1	Network Intrusion Detection System	[2] ,Section 3	60%	42%
2	General requirements	[2] ,Section 5	20%	14%
3	Service requirements	[2] ,Section 6	20%	14%
		Total	**100%**	**70%**

Table 4: Percentage weight of EDR specifications

No.	Product	Specification	Weight	Minimum Threshold
1	Endpoint Detection & Response	[2] ,Section 4	60%	42%
2	General requirements	[2] , Section 5	20%	14%
3	Service requirements	[2] ,Section 6	20%	14%
		Total	**100%**	**70%**

The Tenderer shall indicate compliance to product schedules requirements by completing the following worksheets:

- ***03-NIDS_A&B*** for NIDS under NIDS Technical Schedules spreadsheet **and/or**

- ***03-EDR_A&B*** for EDR under EDR Technical Schedules spreadsheet
- Any deviations from the requirements, as detailed in *240-170000847 Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems* **–** *Rev 2 [2],* shall be clearly captured in the following sheets:
  - ***04-ReqNIDS-DS*** for NIDS under NIDS Technical Schedules spreadsheet **and/or**
  - ***04-ReqEDR-DS*** for EDR under EDR Technical Schedules spreadsheet

3.5.2 Sub-category 2: Product demonstration

This section shall be scored by the technical evaluation team following a visit to each *Supplier's* local offices within South Africa. As far as possible, the *Supplier* shall use physical equipment located at the demonstration premises for the product demonstration which includes the exact equipment proposed in the tender. *Supplier* visits shall be conducted during the tender technical evaluation phase. Only those *Suppliers* that have met the Mandatory Requirements criteria and have also met the minimum requirements on the product schedules A&B shall be visited.

Separate demonstrations will be conducted for NIDS and EDR. Each demonstration shall be assigned a score by the *Purchaser's* technical evaluation team as detailed in Table 5 and Table 6 below. The Tenderer shall achieve a **minimum of 70%** at this stage to be considered successful under product demonstration.

The NIDS and EDR will each have its own specific evaluation criteria and scoring.

3.5.2.1 NIDS Demonstration Evaluation

The test system to be evaluated by the *Purchaser's* technical team during the visit shall comprise a minimum of:

a) Master station console

b) At least 1 probe

The test system shall be configured to represent the communication architecture envisaged for a NIDS solution.

Note: The *Supplier* shall supply all equipment [including simulators] to successfully complete the demonstration items required.

The *Purchaser's* technical evaluation team shall score the demonstration according to the parts indicated in Table 5 below.

Table 5: NIDS Demonstration Evaluation Parts

Demonstration Evaluation Parts	**Weighting**
A **-** NIDS requirements	60%
B **-** General Requirements	20%
C **-** Service Requirements	5%
D **-** Operational Services Questions	15%

The demonstration item for each evaluation part is shown in Table 6. *Suppliers* shall structure their demonstration in sequence with the items in this schedule.

Table 6: NIDS Demonstration Items

Number	Demonstration
	Demonstration preamble
	Suppliers to include a supplementary presentation on their proposed solution, team members, facilities and overview of all off-the-shelf supply items on tendered solution (hardware, software and applicable licenses). This presentation should not exceed 20min.
A	**NIDS Requirements**
A.1	Demonstrate the console dashboard and its situational awareness capability.
A.2	Demonstrate self-learning using Machine Learning [ML] and Artificial Intelligence [AI].
A.3	Demonstrate learning typical/normal patterns of network traffic between different nodes.
A.4	Demonstrate the flag and alarm of network packets that do not conform to the learnt normal traffic patterns.
A.5	Mark anomalous traffic that has been flagged as a false positive, as normal to prevent it from being flagged again
A.6	Demonstrate automation of the categorisation and prioritisation of detected threats.
B	**General Requirements**
B.1	Demonstrate the system's capability to be on-premises without any communication to external servers or websites.
B.2	Demonstrate that failed agents, probes, services or processes shall have auto-restart capability rendering an autonomous function.
B.3	**Explain** the system backup automation, long-term storage offsite capability and mechanism for system back restorations.
B.4	Demonstrate how to keep historic alarms and alerts and aggregated data from which the alarms were derived in order to assist with forensic investigations. Also demo the retention configurations for the above.
B.5	**Explain** which export mechanisms to long-term storage are supported. Outline the supported export formats. Also explain the exporting and archiving of data to local storage, Network storage and email recipients.
B.6	Demonstrate the monitoring of intrusion alarms, events, alerts and incidents.
B.7	Demonstrate collating and reporting on inventory data, resource usage metrics including maintenance windows
B.8	Demonstrate scheduled and ad-hoc reports, including report configurability.
B.9	Demonstrate how notification support a variety of flexible notification triggers such as detected events, failed console login attempts, exceeding of performance thresholds, etc.
B.10	**Explain** how to forward data and alarms from the system to other enterprise systems such as a SIEM or SOAR or Security Operations Centre.
B.11	Demonstrate role-based access (per role, per user).
B.12	Demonstrate how user account management enables the administrator to add users and roles, define privileges, restrict user access to the network, monitor login and logout of users, force users to logout, and lock user accounts.
B.13	Demonstrate role creation and removal (by the administrator)
C	**Services Requirements**
C.1	Demonstrate categorisation and prioritisation of true positive events.
C.2	Demonstrate threat investigation and analysis.

C.3	The *Supplier* to **explain** and outline the way/s in which the *Supplier* will augment the *Purchaser's* incident response process through the *Supplier's* service offering.
D	**Operational Services Questions**
D.1	Demonstrate automated threat investigations.
D.2	Demonstrate automated threat analysis.
D.3	Free form testing 1. (any questions the *Purchaser's* evaluation team might have on the day. No questions asked equal full marks for the line item)
D.3.1	Free form test 2: Demonstrate the loading of the NIDS probe interface by simulating a Denial of Service (DoS) attack to showcase system performance.
D.3.2	Free form test 3: Demonstrate the ability to interrupt and prevent threats in near-real time.
D.3.3	Free form test 4:
D.3.4	Free form test 5:
D.3.5	Free form test 6:

3.5.2.2 EDR Demonstration Evaluation

The test system to be evaluated by the *Purchaser's* technical team during the visit shall comprise a minimum of:

c) Master station console

d) Microsoft Windows Server

e) Microsoft Windows Workstation

f) Linux Server

g) Linux Workstation

h) Network switch

i) Network Router

j) Network Firewall

The test system shall be configured to represent the communication architecture envisaged for a EDR solution.

Note: The *Supplier* shall supply all equipment [including simulators] to successfully complete the demonstration items required.

The *Purchaser's* technical evaluation team shall score the demonstration according to the parts indicated in Table 7 below.

Table 7: EDR Demonstration Evaluation Parts

Demonstration Evaluation Parts	Weighting
EDR requirements	60%
General Requirements	20%
Service Requirements	5%
Operational Services Questions	15%

The demonstration item for each evaluation part is show in Table 8. *Suppliers* shall structure their demonstration in sequence with the items in this schedule.

Table 8: EDR Demonstration Items

Number	Demonstration
	Demonstration preamble
	Suppliers to include a supplementary presentation on their proposed solution, team members, facilities and overview of all off-the-shelf supply items on tendered solution: hardware, software and applicable licenses. This presentation should not exceed 20min.
A	**EDR Requirements**
A.1	Demonstrate the console dashboard and its situational awareness capability.
A.2	Demonstrate EDR functionality on computers with Windows operating systems that includes servers and workstations.
A.3	**Explain** detect and raise flags and alarms (that would indicate the presence of malware, virus', worms or an intruder) for malicious changes on the following **MS Windows** computer internals: 1) File system including attributes 2) Log files 3) Network interfaces 4) Configurations 5) Registry settings
A.4	Demonstrate EDR functionality on computers with Linux operating systems that includes servers and workstations.
A.5	**Explain** detect and raise flags and alarms (that would indicate the presence of malware, virus', worms or an intruder) for malicious changes on the following **Linux** computer internals: 1) File system including attributes 2) Log files 3) Network interfaces 4) Configurations 5) Registry settings
A.6	Demonstrate anomaly-based detection using Machine Learning methods and not be based on signature-based detection.
A.7	**Explain** detect and raise flags and alarms for malicious changes on network devices such as switches, routers and firewalls for the following: 1) Log files 2) Configurations 3) Firmware tampering
A.8	Demonstrate ability to configure host policy.
A.9	Demonstrate configuration checking rules capability.
A.10	Demonstrate remote modification of parameters on multiple hosts at once from a single point on premises.
A.11	Demonstrate high-use and idle times of hosts configurability.
B	**General Requirements**
B.1	Demonstrate the system's capability to be on-premises without any communication to external servers or websites.
B.2	Demonstrate that failed agents, probes, services or processes shall have auto-restart capability rendering an autonomous function.
B.3	**Explain** the system backup automation, long-term storage offsite capability and mechanism for system backup restorations.

Number	Demonstration
B.4	Demonstrate how to keep historic alarms and alerts and aggregated data from which the alarms were derived in order to assist with forensic investigations. Also demo the retention configurations for the above.
B.5	**Explain** which export mechanisms to long-term storage are supported. Outline the supported export formats. Also explain the exporting and archiving of data to local storage, Network storage and email recipients.
B.6	Demonstrate the monitoring of intrusion alarms, events, alerts and incidents.
B.7	Demonstrate collating and reporting on inventory data, resource usage metrics including maintenance windows
B.8	Demonstrate scheduled and ad-hoc reports, including report configurability.
B.9	Demonstrate how notification support a variety of flexible notification triggers such as detected events, failed console login attempts, exceeding of performance thresholds, etc.
B.10	**Explain** how to forward data and alarms from the system to other enterprise systems such as a SIEM or SOAR or Security Operations Centre.
B.11	Demonstrate role-based access (per role, per user).
B.12	Demonstrate how user account management enables the administrator to add users and roles, define privileges, restrict user access to the network, monitor login and logout of users, force users to logout, and lock user accounts.
B.13	Demonstrate role creation and removal (by the administrator)
C	**Services Requirements**
C.1	Demonstrate categorisation and prioritisation of true positive events.
C.2	Demonstrate threat investigation and analysis.
C.3	The *Supplier* to explain and outline the way/s in which the *Supplier* will augment the *Purchaser's* incident response process through the *Supplier's* service offering.
D	**Operational Services Questions**
D.1	Demonstrate automated threat investigations.
D.2	Demonstrate automated threat analysis.
D.3	Free form testing 1: (Any questions the *Purchaser's* evaluation team might have on the day. No questions asked equal full marks for the line item)
D.3.1	Free form test 2: Demonstrate the ability to interrupt and prevent threats in near-real time.
D.3.2	Free form test 3:
D.3.3	Free form test 4:
D.3.4	Free form test 5:
D.3.5	Free form test 6:

3.6 Sub-category 3: Risk and Support

The Evaluation Team shall assess the responses to the Risk and Support Questions to identify any potential risks associated with the proposed solution. Each identified risk shall be evaluated and classified according to its severity—categorized as **Low, High, or Unacceptable.** These risks will be formally considered and addressed during the contracting process.
The subsections below are applicable to both NIDS and EDR. The questionaries listed below **must be completed**, depending on whether the Tenderer is tendering for NIDS only, EDR only or both.

All these worksheets can be found on NIDS and EDR Technical Schedules in Appendix B.

Table 9: Risk and Support Worksheets

Evaluation Parts	Worksheets
Usability	05-Rns Usability
Product Roadmap Capability	06-Rns RoadmapQ
3rd Party Integrations and Interoperability	07-Rns IntegrationsQ
Maintenance and Support	08-Rns MaintSupport
Security Clearances	09-Rns SecClearance
Expertise and Support	10-Rns Expertise
Track Record	11-Rns TrackRecord

Further explanation on the context and intent of this section has been provided under *Appendix C: Risk and Support Context.*

3.7 Bill of Quantities (BoQ)

To support a comprehensive technical evaluation and ensure alignment with the proposed solution architecture, the Tenderer is requested to submit a detailed Bill of Quantities (BoQ) as part of the tender returnables. The BoQ must list all components, equipment, software licenses, services, and any other relevant items included in the proposed solution**—excluding pricing information**. This submission will assist the Purchaser in verifying the completeness of the solution, assessing technical compatibility, and ensuring that all required elements are accounted for in the evaluation process.

Separate BoQs for NIDS and/or EDR shall be submitted, as these solutions will be evaluated independently of each other. The Tenderer shall use their preferred BoQ template.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Judith Malinga	Senior Manager – PTM&C Engineering
Johan Botha	Senior Consultant – Energy Management (National Control)
Ernest Mpshe	Chairperson – Systems and Tools SC
Mpumelelo Mathe	Middle Manager – CATS PTM&C Engineering
Cornelius Naidoo	Middle Manager – Telecoms & Physical Security, PTM&C Engineering
Donald Moshoeshoe	Chief Engineer – Physical Security
Malcolm Govender	Chief Technologist - AFAS
Kgomotso Setlhapelo	Chief Engineer – Telecomms NMC
Kgomotso Manyapetsa	Chief Engineer - CATS PTM&C Engineering

5. Revisions

Date	Rev.	Compiler	Remarks
October 2025	1	T Ramulondi	First Draft

6. Development Team

The following people were involved in the development of this document:

- Bongani Shezi
- Kgomotso Manyapetsa

7. Acknowledgements

Not applicable

Appendix A Returnables

Appendix A.1: Indication of Tendered Solution Package

Tenderer shall indicate which solution they are tendering for, between NIDS, EDR or both, on the table below.

Table A.1: Indication of Tendered Solution Package

Solution Tendered for	**Mark the applicable option (X)**
NIDS Solution **Only**	
EDR Solution **Only**	
Or both NIDS and EDR	

Appendix B: NIDS and EDR Technical Schedules Spreadsheets

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

Appendix B.1: NIDS Technical Schedules

Download the attached spreadsheet and complete the required information.

NIDS Technical
Schedule

Appendix B.2: EDR Technical Schedules

Download the attached spreadsheet and complete the required information.

EDR Technical
Schedules.xlsx

Appendix C: Risk and Support Context

C.1 System Risk

C.1.1 Usability

The *Purchaser* shall operate the NIDS and EDR as a whole or in part and the usability and intuitiveness of the solution will impact the *Purchaser's* operational teams' ability to achieve their goals effectively and efficiently.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules -** *05-Rns Usability (for NIDS)*
- **EDR Technical Schedules -** *05-Rns Usability (for EDR)*

C.1.2 Product Roadmap Capability

Technology roadmaps align Tenderer's products development to their long-term technology direction, as well as align to the industry's continual developments. Non-aligned technologies produce incompatibility and incur addition unforeseen overheads and can present a risk to the *Purchaser*.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules** - *06-Rns RoadmapQ (for NIDS)*
- **EDR Technical Schedules** - *06-Rns RoadmapQ (for EDR)*

C.1.2 3rd Party Integrations and Interoperability

NIDS and EDR are but 2 components in a cyber security system. The ability to easily integrate with other cyber related systems and being interoperable with other vendors' systems will pose less risk and development for alignment to the *Purchaser's* roadmap. This includes versatility when it comes to interoperability of protocols used in mainstream industry vendors.

This evaluation is based on the following interfaces:

a) a SIEM, SOAR and Security Operations Centre
b) EDR only: networking devices (switches, routers and firewalls)

These interfaces are essential to achieve many of the functions defined for each system or product.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules -** *07-Rns IntegrationsQ* ***(****for NIDS)*
- **EDR Technical Schedules -** *07-Rns IntegrationsQ* ***(****for EDR)*

C.2 Support

C.2.1 Maintenance and Support

The Tenderer's strategy with regards to the quantity and magnitude of maintenance activities associated with the tendered solution(s) will have a direct impact on systems' availability and frequency of system interruptions.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules -** *08-Rns MaintSupport* ***(****for NIDS)*
- **EDR Technical Schedules -** *08-Rns MaintSupport* ***(****for EDR)*

C.2.2 Security Clearances

Acceptance of this tender is subject to the condition that both the Tenderer and its personnel providing the services must be cleared by the appropriate authorities to the level of CONFIDENTIAL/SECRET/TOP SECRET. If the principal Tenderer appoints a subcontractor, the same provisions and measures will apply to the subcontractor. [4]

Given that the *Purchaser* is a government institution and the Tenderer's services can be consumed at a national key point, appropriate national security clearances for *Supplier* staff at the appropriate levels will be required.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules -** 09-*Rns SecClearance (for NIDS)*
- **EDR Technical Schedules -** 09-*Rns SecClearance (for EDR)*

C.2.3 Expertise and Support

The amount of knowledge and number of years with relevant experiences will impact the Tenderer's ability to provide expert advice and services. In addition, facilities that consist of well-established research and development, manufacturing, testing, construction/assembly and stock/spares holding areas are essential for effective product supply, maintenance and support.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules -** 10-*Rns Expertise (for NIDS)*
- **EDR Technical Schedules -** 10-*Rns Expertise (for EDR)*

C.2.4 Track Record

A track record is a history of past performance or accomplishments, good or bad. The totality of which may give the *Purchaser* a good idea of the future performance potential of with regards to this enquiry.

If the Tenderer is tendering on both NIDS and EDR, the Tenderer must provide an answer to the question for both NIDS and EDR individually, otherwise, only to the NIDS or EDR being tendered on.

The interface risk questions are outlined in **Spreadsheet/Worksheets:**

- **NIDS Technical Schedules -** 11-*Rns TrackRecord (for NIDS)*
- **EDR Technical Schedules -** 11-*Rns TrackRecord (for EDR*

Appendix D: Tender Technical Returnables Checklists

Appendix D.1: NIDS Tender Technical Returnables

The table below shall be used as a checklist to ensure that the Tenderer has provided all the necessary documentation for assessment of the offered NIDS solution. The worksheets to be completed can be found on the "***NIDS Technical Schedules***" spreadsheet.

Table A.2: NIDS Technical Returnables Checklist

No.	Tender Returnable	Reference Worksheet	Purchaser's Requirement	Supplier's Statement (Submitted/Not Submitted)	Evaluator's Assessment (Submitted/Not Submitted)
1	NIDS Technical Gatekeepers	*01-NIDSTechGatekeepers*	To be completed		
2	General Questionnaire	*02-GenNIDS*	To be completed and submitted together with supporting documents/evidence		
3	Completed – Compliance Schedules A&B for **NIDS** as per the requirements in 240-170000847	*03-NIDS_A&B*	To be completed and submitted together with supporting documents/evidence.		
4	**Deviation Schedule**: NIDS deviation schedule	*04-ReqNIDS-DS*	Any NIDS deviations from the requirements (240-170000847) shall be listed		
5	Risk and Support - System Risk: Usability Questions	*05-Rns Usability*	To be completed and submitted together with supporting documents/evidence		

No.	Tender Returnable	Reference Worksheet	Purchaser's Requirement	Supplier's Statement (Submitted/Not Submitted)	Evaluator's Assessment (Submitted/Not Submitted)
6	Risk and Support - System Risk: Roadmap Capability Questions	*06-Rns RoadmapQ*	To be completed and submitted together with supporting documents/evidence		
7	Risk and Support - System Risk: 3rd Party Intergrations and Interoperability Questions	*07-Rns IntegrationsQ*	To be completed and submitted together with supporting documents/evidence		
8	Risk and Support - Performance Questions: Maintenance and Support	*08-Rns MaintSupport*	To be completed and submitted together with supporting documents/evidence		
09	Risk and Support - Performance Questions: Security Clearance	*09-Rns SecClearance*	To be completed and submitted together with supporting documents/evidence		
10	Risk and Support - Performance Questions: Expertise and Support	*10-Rns Expertise*	To be completed and submitted together with supporting documents/evidence		
11	Risk and Support - Performance Questions: Track Record	*11-Rns TrackRecord*	To be completed and submitted together with supporting documents/evidence		
12	NIDS Bill of Quantities **(Without pricing)**	-	The Tenderer to submit the BoQ in their own template		

Appendix D.2: EDR Technical Returnables

The table below shall be used as a checklist to ensure that the Tenderer has provided all the necessary documentation for assessment of the offered EDR solution. The worksheets to be completed can be found on the "***EDR Technical Schedules***" spreadsheet.

Table A.3: EDR Tender Technical Returnables Checklist

No.	Tender Returnable	Reference Worksheet	Purchaser's Requirement	Supplier's Statement (Submitted/ Not Submitted)	Evaluator's Assessment (Submitted/ Not Submitted)
1	EDR Technical Gatekeepers	*01-EDRTechGatekeepers*	To be completed		
2	General Questionnaire	*02-GenEDR*	To be completed and submitted together with supporting documents/evidence		
3	Completed – Compliance Schedules A&B for **EDR** as per the requirements in 240-170000847	*03-EDR_A&B*	To be completed and submitted together with supporting documents/evidence.		
4	**Deviation Schedule**: EDR deviation schedule	*04-ReqEDR-DS*	Any EDR deviations from the requirements (240-170000847) shall be listed		
5	Risk and Support - System Risk: Usability Questions	*05-Rns Usability*	To be completed and submitted together with supporting documents/evidence		
6	Risk and Support - System Risk: Roadmap Capability Questions	*06-Rns RoadmapQ*	To be completed and submitted together with supporting documents/evidence		
7	Risk and Support - System Risk: 3rd Party Intergrations and Interoperability Questions	*07-Rns IntegrationsQ*	To be completed and submitted together with supporting documents/evidence		
8	Risk and Support - Performance Questions: Maintenance and Support	*08-Rns MaintSupport*	To be completed and submitted together with supporting documents/evidence		

No.	**Tender Returnable**	**Reference Worksheet**	**Purchaser's Requirement**	**Supplier's Statement (Submitted/ Not Submitted)**	**Evaluator's Assessment (Submitted/ Not Submitted)**
9	Risk and Support - Performance Questions: Security Clearance	*09-Rns SecClearance*	To be completed and submitted together with supporting documents/evidence		
10	Risk and Support - Performance Questions: Expertise and Support	*10-Rns Expertise*	To be completed and submitted together with supporting documents/evidence		
11	Risk and Support - Performance Questions: Track Record	*11-Rns TrackRecord*	To be completed and submitted together with supporting documents/evidence		
12	EDR Bill of Quantities **(Without pricing)**	-	The Tenderer to submit the BoQ in their own template		