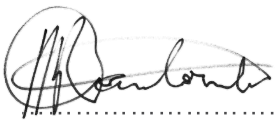
Eskom National Transmission Company South Africa ™	**Scope of Work for Supply and Delivery of an NTCSA OT Network Intrusion Detection System & Endpoint Detection and Response Solution**

SCOPE OF WORK: NTCSA OT Supply and Delivery of a Network Intrusion Detection System (NIDS) and Endpoint Detection and Response (EDR) Solution

Compiled by:	Supported by:	Responsible person:
		
.....	.....	.....
Thendo Ramulondi	**Ernest Mpshe**	**Mpumelelo Mathe**
Chief Engineer – PTM&C Control and Automation	**Middle Manager – NCSS System Operator**	**Middle Manager – PTM&C Control and Automation**
Date: 29/05/2025	Date: 29/05/2025	Date: 2025/05/30

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

Eskom
National Transmission Company South Africa TI

CONTENTS

1. INTRODUCTION

The purpose of this document is to outline the scope of work for the supply and delivery of an Network Intrusion Detection System (NIDS) and Endpoint Detection Response (EDR) for National Transmission Company South Africa (NTCSA) Operational Technology [OT]. The NIDS and EDR will provide the necessary cybersecurity controls to enable monitoring and surveillance of OT critical systems and provide alerts, triage and reporting when suspicious activity or known threats are detected.

Supply services for installation, configuration, commissioning, maintenance, support and training of the NIDS & EDR, operational services for threat monitoring, threat investigations, threat analysis and augmented incidents response are outlined in this document.

The standard detailing the requirements for both NIDS and EDR is 240-170000847, *Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems.*

The document also outlines the safety and evaluation criteria.

2. SUPPORTING CLAUSES

2.1 SCOPE OF WORK

2.1.1 Purpose

The purpose of this document is to ensure that the *Supplier* complies with the requirements of the *Purchaser* on site. The *Supplier's* duties are required to comply with the following but not limited to:

- Ensuring the safety of persons, equipment and infrastructure at the *Purchaser's* premises or National Key Point.

2.1.2 Applicability

The scope of this document is applicable to the NTCSA OT business area and the selected supplier.

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] Occupational Health and Safety Act

[3] 240-170000847 Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems

2.2.2 Informative

N/A

3. DEFINITIONS AND ABBEVIATIONS

3.1 DEFINITIONS

Definitions	Explanations
Supplier	A Person or Company that undertakes a contract to provide materials or labour to perform a service or do a job.
Purchaser	A Person or Company that through a contract consumes materials or labour for a service or a job.

3.2 ABBREVIATIONS

EDR	Endpoint Detection and Response
NEC	New Engineering Contract
NIDS	Network Intrusion Detection System
NTCSA	National Transmission Company South Africa
OT	Operational Technology
VM	Virtual Machine
TEMSE	Transmission Energy Management System Evolution

4. SCOPE OF WORK

The scope of work is for the supply and delivery of a Network Intrusion Detection System and Endpoint Detection Response Solution for NTCSA Operational Technology for a duration of five (5)

years. Supply and operational services are included in the scope of work. The *Purchaser* shall retain an option to extend the production contract/s by a further five (5) year term. The *Purchaser* reserves the right not to award or extend contract/s.

The required solution comprises NIDS and EDR as complete separate systems. Each system may comprise hardware, software and associated licensing.
The required solution will provide the necessary cybersecurity controls to enable monitoring, threat detection & analysis (known and unknown), incident response, management and malware defense for OT critical systems.

There are six OT systems that need to be serviced through this scope of work.

One enquiry shall be issued to the market with two distinct packages for NIDS and EDR that can be tendered on separately. This could result in different suppliers for different systems or a single supplier for all.

The scope of work for each includes the following:

1. supply and delivery of:
    a. hardware
    b. software
    c. licensing
2. deployment services for:
    a. installation,
    b. configuration,
    c. commissioning,
    d. maintenance,
    e. support,
    f. training
3. operational services for:
    a. threat monitoring,
    b. threat investigations,
    c. threat analysis,
    d. augmented incidents response

Each contract will be on an **"as-and-when-required"** basis.

5. ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities of the *Purchaser* and the *Supplier.*

5.1 ROLE OF THE PURCHASER

NTCSA the *Purchaser* shall provide:

- Access to facilities as and when required.

5.2. SUPPLIER RESPONSIBILITIES

1. The *Supplier* shall:
    a. supply and deliver;
        i. hardware
        ii. software
        iii. licensing
    b. supply services for;
        i. installation,
        ii. configuration,
        iii. commissioning,
        iv. maintenance,
        v. support,
        vi. training
    c. operational services for;
        i. threat monitoring,
        ii. threat investigations,
        iii. threat analysis,
        iv. augmented incidents response

6. OCCUPATIONAL HEALTH AND SAFETY REQUIREMENTS

The *Supplier* shall provide the following:

- Annexure B (Acknowledgement of Eskom's rules & requirements)
- Valid Letter of Good Standing or equivalent (LOGs)

7. Sizing Requirements

In order to assist with pricing, the following approximate numbers are provided. The impacted pricing shall be reviewed on an annual basis (and/or if the installed base grows/reduces by over 10%).

7.1 NIDS Sizing

The NIDS shall be sized as follows

7.1.1 System 1

Table 1: System 1 NIDS sizing

Host/Device Type	Quantity	Comment
Master station consoles	3	Master station consoles from where monitoring can be done comprising of: • main system, • networking equipment that is managed out of band, • development environment
Probes	To be determined by *Supplier* as part of the design	Probes to monitor 15 segments split over 2 rooms and a standby site. Most of the utilisation is low, so it may be possible to aggregate using switches. Links between the 2 rooms must be fibre.
Additional information	-	The two networks for System 1 consist of around 330 IP addresses for the one, and around 400 IP addresses for the other network

7.1.2 System 2

Table 2: System 2 NIDS sizing

Host/Device Type	Quantity	Comment
Master station consoles	2	Master station (including a workstation) and a development environment
Probes	2	Probes for the core infrastructure to monitor System 2's IP network.
Additional information	-	System 2's IP Network is segmented on 43 VRFs and 1000+ VLANs. There are about 842 network devices.

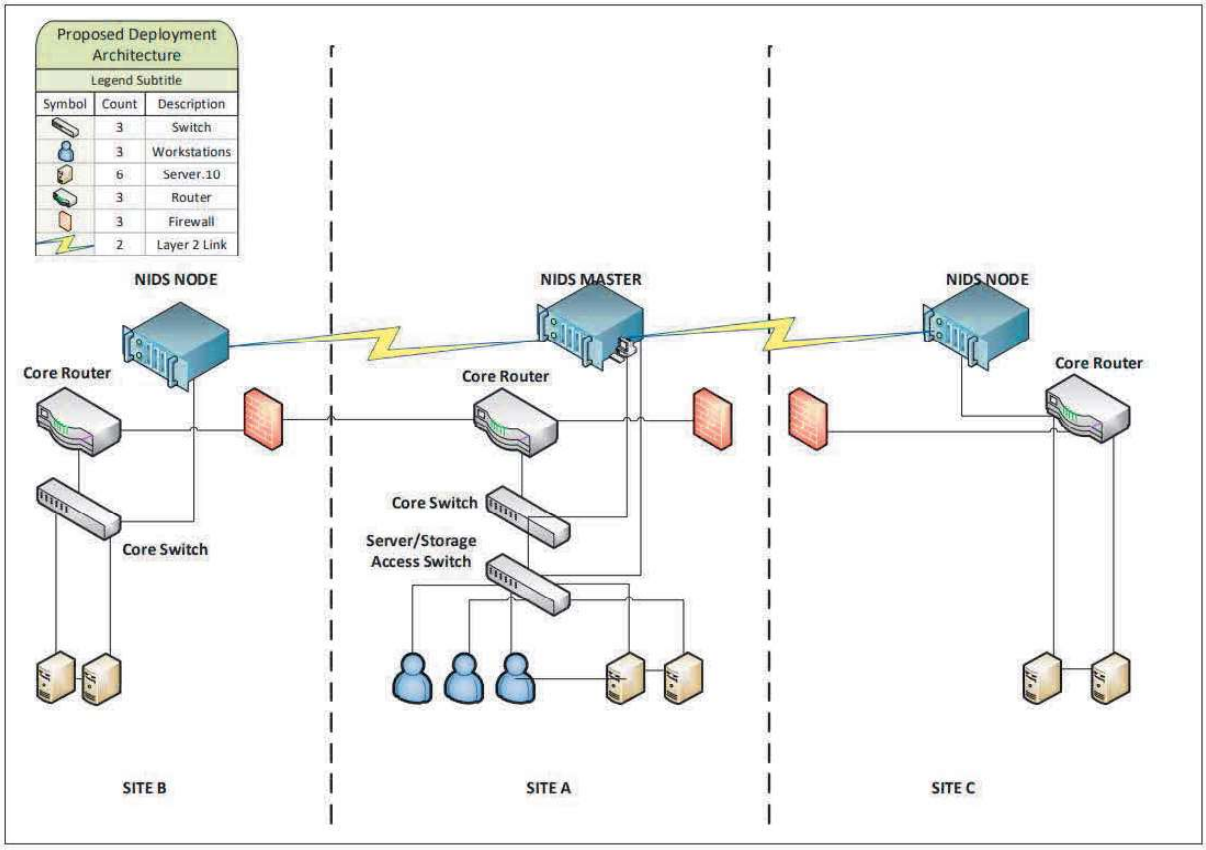


Figure 1: Target NIDS Deployment Architecture for System 2

7.1.3 System 3

Host/Device Type	Quantity	Comment
Master station consoles	2	Master station (including a workstation) and a development environment
Probes	2	Probes for the core infrastructure to monitor System 3's IP network.
Additional information	2	Physical security network traffic will be monitored through the core switches at Zero Control and eMkhiweni (disaster recovery site)

7.2 EDR Sizing

The EDR shall be sized as follows:

7.2.1 System 1

Table 3: System 1 EDR sizing

Host/Device Type	Quantity	Comment
Master station consoles	2	Master station consoles from where monitoring can be done – one for the main system, and one for the networking equipment that is managed out of band.
Windows servers	21	
Linux servers	86	Linux servers with Red-hat Package Manager based distributions
Linux workstations	102	Linux Workstations with Debian based distributions
Windows 7/10 guests	98	Windows 7/10 guests on Workstations
Network routers	16	
Network switches	72	
Network firewall pairs	3 pairs = 6	
Standalone network firewalls	3	

7.2.2 System 2

Table 4: System 2 EDR sizing

Host/Device Type	Quantity	Comment
Master station consoles	5	Production, DR and DMZ.
Windows servers	10	
Linux servers	31	25 Linux and 6 Unix servers
Windows workstations	91	3 Windows XP Workstations and 88 Windows 10 Workstations.
Network routers	1500	
Network switches	64	60 network switches and 4 Voice Gateways.
Network firewall pairs	10 pairs = 20	
Standalone network firewalls	0	

7.2.3 System 3

Table 5: System 3 EDR sizing

Host/Device Type	Quantity	Comment
Master station consoles	4	2 for the operation environment and 2 for DMZ environment.
Windows servers	4	4 current installed base but project 1 recovery server at eMkhiweni and 152 servers for telecoms sites and 119 servers for Transmission substations.
Linux servers	0	This may change pending IPSS contract
Windows workstations	2	2 windows 10 workstations currently installed but project 1 workstation at eMkhiweni and 152 workstations for telecoms sites and 119 workstations for Transmission substations.
Windows 7/10 guests	0	This may change pending IPSS contract
Network routers	0	
Network switches	21	1 at Zero Control and 20 at Bernina-Hera Substation but project 4 more at Zero, 5 at eMkhiweni and 2710 projected for Telecoms site and Transmission substations.
Network firewall pairs	0	
Standalone network firewalls	4	2 at Zero Control and 1 at Bernina-Hera, project 1 at eMkhiweni and 271 firewalls for Transmission substations and Telecoms sites.

7.2.4 System 4

Table 6: System 4 EDR sizing

Host/Device Type	Quantity	Comment
Scanning Masters	15	
Windows Servers	4	

7.2.5 System 5

Table 7: System 5 EDR sizing

Host/Device Type	Quantity	Comment
Windows Servers	4	
VMs (Windows)	11	
VMs (Linux)	5	

7.2.6 System 6

Table 8: VMs EDR Sizing

Host/Device Type	Quantity	Comment
Virtual Machines (Windows)	2500	Windows XP, 7, 10 and 11