Eskom National Transmission Company South Africa ™	Standard	National Transmission Company South Africa

Title:	**Network Intrusion Detection and Endpoint Detection & Response Systems Requirements for NTCSA's OT Systems**	Document Identifier:	**240-170000847**
		Alternative Reference Number:	**<N/A>**
		Area of Applicability:	**National Transmission Company South Africa**
		Functional Area:	**Engineering**
		Revision:	**2**
		Total Pages:	**16**
		Next Review Date:	**April 2030**
		Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Approved by**	**Authorized by**
		J Malinga
Thendo Ramulondi	**Mpumelelo Mathe**	**Judith Malinga**
CATS – Chief Engineer	**CATS – Middle Manager**	**PTM&C – Senior Manager** Engineering
Date: 14/05/2025	Date: 2025/05/15	Date: 19/05/2025

Supported by SCOT/SC

Ernest Mpshe

SCOT/SC Chairperson

Date: 19/05/2025

PCM Reference: **N/A**

SCOT Study Committee: **Tools and Systems**

Reference - Template ID: 559-751375159 Document Template

Content

1. Introduction

This document details National Transmission Company South Africa (NTCSA) [as the *Purchaser*] Operational Technology [OT] requirements for Network Intrusion Detection and Endpoint Detection & Response systems. The complete two component solution 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.

This document details the requirements for NTCSA's OT requirements for a Network Intrusion Detection solution and Endpoint Detection & Response to ensure the sustainability of such systems in terms of:

a) Functional requirements

b) General requirements

c) Service requirements.

2. Supporting Clauses

2.1 Scope

The scope is to enable the provision of a Network Intrusion Detection and Endpoint Detection & Response for critical OT systems within NTCSA. The scope includes the deployment of the solution into development environments within the said OT systems including virtual machines. The offered solution shall be on-premise and not require external communications for normal operations. Updates to the systems shall occur through offline mechanisms. The systems shall interface to enterprise Security Information and Event Management [SIEM] and Security Orchestration, Automation and Response [SOAR] if required.

The scope also includes operational services on an “as and when required” basis for threat monitoring, threat investigation, threat analysis and providing an augmented service to incident management and response.

2.1.1 Purpose

The purpose of this document is to provide requirements for a Network Intrusion Detection solution, Endpoint Detection & Response system and operational service requirements.

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

This document is effective from the authorisation date.

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

2.2.2 Informative

[2] 240-55410927: Cyber Security Standard for Operational Technology.

[3] 240-110767932: Sanitisation of Data and Storage Media

[4] 240-185000083: Requirement Specification for a NTCSA Operational Technology (OT) SIEM Solution

2.3 Definitions

2.3.1 General

Definition	Description
Application Whitelisting	Preventing applications to run that don't have hashes that matches allowed hashes in a database of authorised applications.
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.
Host Network Intrusion Detection System	Monitors and analyses individual computer host internals such as files systems, log files, network interfaces, configuration and registry settings for malicious activity.
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.

2.4 Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
AD	Active Directory
CIP	Critical Infrastructure Protection
CPS	Cyber Physical Systems
CPU	Central Processing Unit
EDR	Endpoint Detection and Response
ET	Eskom Telecoms

Abbreviation	Explanation
HIDS	Host Network Intrusion Detection System
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDS	Network Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol
ML	Machine Learning
NE	Network Element
NERC	North American Electric Reliability Corporation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OT	Operational Technology
PTM&C	Protection, Telecommunications, Metering and Control
RPO	Recovery Point Objective
RSA	Republic of South Africa
RTO	Recovery Time Objective
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
TACACS	Terminal Access Controller Access Control System
VLAN	Virtual Local Area Network
VM	Virtual Machine
VRF	Virtual Routing and Forwarding

2.5 Roles and Responsibilities

It is the responsibility of the relevant stakeholders to ensure the offered solution is correctly implemented in their respective departments and it is their role to ensure successful operation.

2.6 Process for Monitoring

Changes in the Intrusion Detection and Endpoint Detection & Response requirements for OT NTCSA, as well as changes in technology shall be monitored by this standard's stakeholders and if necessary, this standard shall be revised by the PTM&C Cybersecurity Centre of Excellence.

2.7 Related/Supporting Documents

None

3. Network Intrusion Detection and Endpoint Detection & Response Solution for NTCSA

NTCSA's OT environments require a Network Intrusion Detection system on critical OT systems. Network Intrusion Detection shall be applied on both the network and the hosts of the system. Monitoring shall primarily be performed locally by the *Purchaser*. These systems shall be off-the-shelf, and no specific development shall be necessary for the *Purchaser*

The Endpoint Detection & Response required 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. Centralised monitoring and configuration for this system shall also be local by the Purchaser.

3.1 Network Intrusion Detection System (NIDS) Requirements

3.1.1 Functional Requirements

The NIDS:

a) shall be self-learning using Artificial Intelligence [AI].

b) shall be capable of learning typical/normal patterns of network traffic between different nodes on the network.

c) shall flag and alarm network packets that do not conform to the learnt normal traffic patterns.

d) shall be able to mark anomalous traffic that has been flagged as a false positive, as normal to prevent it from being flagged again.

e) shall support Industrial Control Systems [ICS] related protocols within OT environments.

f) shall support Information and Communications Technology [ICT] infrastructure within OT environments.

g) shall support Cyber Physical Systems [CPS] infrastructure within OT environment.

h) shall not allow two networks to be bridged through itself.

i) shall have any network probe installed not to interfere with the normal operation of the network and not introduce more than 5% of additional network load and more than 10% of additional CPU load on any network equipment.

j) shall be able to run autonomously.

k) shall be able to automate the categorisation and prioritisation of detected threats.

l) should preferably be able to automate threat investigations.

m) should preferably be able to automate threat analysis.

n) shall have the ability to interrupt and prevent threats in near-real time, but turn off this functionality if required by the *Purchaser.*

o) Shall be able to use network tapping where required for example with unidirectional SPAN ports.

4. Endpoint Detection and Response

4.1.1 Functional Requirements

Endpoint Detection and Response:

a) shall function on computers with Windows operating systems that includes servers and workstations.

b) shall function on computer with Linux operating systems that includes servers and workstations.

c) shall provide anomaly-based detection using AI methods and not be based on signature-based detection.

d) shall detect and raise flags and alarms (that would indicate the presence of malware, virus', worms or an intruder) for malicious changes on the following computer internals:

1) File system including attributes

2) Log files

3) Network interfaces

4) Configurations

5) Registry settings

e) shall be able to 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

f) shall be able to generate compliance reports for the configuration and policies of the host against international standards.

g) shall be able to configure host policy.

h) shall have configuration checking rules.

i) shall have high-use and idle times of hosts to be configurable.

j) shall be able to create image snapshots of the hosts performed manually or according to a configurable schedule.

k) shall be able to restore image snapshots to hosts.

l) shall be fully deployable and manageable on local, on-premises infrastructure.

m) shall reside (all components including, management console, updates, threat intelligence, and logging) within the Purchaser's private network i.e. no reliance on external cloud servers for processing, storage, or updates.

n) shall have a local centralised management system with the ability to push rules to protected machines.

o) The Management system shall include displays which collects the logs of applications attempting execution, alerting the operator and displaying all relevant information to be able to identify host, time and application.

p) Workstations and servers who have lost connection to the master system shall also be reported with last connection time and date.

q) shall integrate with the virtualization layer to minimize resource overhead and avoid performance degradation. Features like agentless scanning or lightweight agents tailored for VMs are ideal.

r) shall detect threats and apply updates without internet connectivity.

s) Shall update threat signatures and behavioural rules via the Purchaser's internal networks.

t) shall not require cloud-based processing for artificial intelligence based threat detection

u) shall allow detailed, customizable security policies for specific VM roles such as servers and administrators workstations.

v) shall have whitelisting capabilities to lock down approved processes block unauthorized ones.

w) shall implement hashes for whitelisting and not only filenames to whitelist applications.

x) shall use whitelisting to to allow applications that have been permitted to execute

y) shall offer comprehensive, on-premise logging and reporting capabilities.

z) shall provision for access to real-time alerts and detailed reports via an on-premises management console.

aa) shall be able to integrate with the existing Security Information and Event Management (SIEM) system if required.

bb) shall operate with low resource utilization on the host. Light weight agents or agentless options that don't overload CPU, memory or disk I/O are preferred.

cc) Shall have any client or agent required to run on a host to not interfere with the normal operation of that host, and not consume more than 5% of any of the memory or CPU on the node during operations/ high-use times

dd) shall provide protection across multiple server operating systems such as; windows 2008 and or later as well as Redhat Enterprise Linux version 6 or later and SUSE Enterprise Linux version 11 or later variants.

ee) shall provide protection across multiple workstation operating systems such as; Windows XP, Windows 7, Windows 10, and Windows 11 and Ubuntu Linux version 22 or later variants.

5. General Requirements

The general requirements apply to NIDS and EDR.

5.1.1 Location

ff) The system shall be on-premise without any communication to external servers or websites.

gg) The system shall be capable of running autonomously and in a fully functional state.

5.1.2 Communication between System Components

a) Dataflow shall be uni-directional from client devices to master consoles only, unless the system functionality calls for otherwise explicitly.

b) Client devices and master station consoles shall use a fixed configurable port for the network connection to allow strict firewall rules to be set.

c) Communication between master consoles and client devices shall be encrypted.

5.1.3 Availability

a) Failed agents, probes, services or processes shall have auto-restart capability rendering an autonomous function across all components.

b) The system shall support the following functions:

1) Periodic and/or scheduled maintenance activities performed on the system (such as, firmware updates, configuration changes, etc.) shall not create blind spots in the system's Network Intrusion Detection functionality.

2) In the case of system failure/collapse, the system's restoration tools shall not be a hinderance in restoring from a backup to a fully functional state within 24hours.

5.1.4 Sanitisation

a) The NIDS and EDR devices shall enable the *Purchaser's* personnel to perform the required sanitization procedures as per 240-110767932: Sanitisation of Data and Storage Media.

5.1.5 Backup and Recovery

a) The systems shall have a mechanism that allows the automation of system backups.

b) The system shall allow for backups to be kept on long-term storage on offsite locations.

c) The systems shall have a mechanism that allows for the restoration from system backups.

5.1.6 Data Retention Strategy

a) The system shall keep historic alarms and alerts and aggregated data from which the alarms were derived in order to assist with forensic investigations.

b) The period for which this data can be kept for shall be configurable.

c) Export mechanisms to long-term storage shall be supported.

d) Supported export formats shall be of commodity types and are to be specified by the *Supplier*.

e) Support for exporting and archiving of data to the following:

1) local storage

2) network storage

3) email recipients

5.1.7 Monitoring

a) Monitoring of intrusion alarms, events, alerts and incidents shall primarily be performed locally by the *Purchaser.*

b) The monitoring solution shall support the following functions:

1) Collating and reporting on inventory data, resource usage metrics including maintenance windows
2) Enable a complete audit trail against detected events
3) Definition and monitoring of performance measurements and thresholds (e.g., false positives, etc.)
4) Device and module/card health data monitoring, such as overall throughput, per-(sub) interface utilization, response time, CPU load, memory consumption, etc. This shall be supported for real-time monitoring and for historical (user configurable periods).

5.1.8 Reporting and Notifications

a) It shall be possible to provide scheduled and ad-hoc reports.

b) The content of the reports shall be configurable and flexible.

c) It shall be possible to send notifications via email via an SMTP server.

d) Notification shall support a variety of flexible notification triggers such as detected events, failed console login attempts, exceeding of performance thresholds, etc.

5.1.9 3rd Party Integrations

a) It shall be possible to forward data and alarms from the system to other enterprise systems such as a SIEM or SOAR or Security Operations Centre (SOC).

5.1.10 Access Control

a) Role based access (per role, per user) shall be provided– each role, or user, shall have access to specific functions, views and objects.

b) Both local authentication (for fall-back authentication method only) and remote authentication shall be provided.

c) For remote authentication, integration to TACACS, active directory (AD) and/or Lightweight Directory Access Protocol (LDAP) shall be supported.

d) Strong authentication shall be provided through the support of password expiration, enforcement of strong passwords and an increasing time to retry or account lockout on successive failed logon attempts.

e) User account management shall be provided enabling 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.

f) Role creation and removal (by the administrator) shall be provided.

g) Multiple users per role shall be allowed.

5.1.11 Documentation

a) Detailed technical documentation shall be provided that includes (but is not limited to):

1) product manuals,
2) installation manuals,
3) user manuals,
4) quick start guides,
5) maintenance guides,
6) troubleshooting guides
7) drawings where applicable

b) The documentation shall be available online for the user to download when required.

c) The documentation shall be provided in English.

6. Service Requirements

6.1.1 Supply and Delivery

a) These systems shall be off-the-shelf, and no specific development shall be allowed.

b) The *Supplier* shall supply and deliver the solution's hardware, software and licences to selected locations of the *Purchaser* within the Republic of South Africa (RSA).

6.1.2 Installation, Configuration and Commissioning

a) The *Supplier* shall install, configure and commission the solution.

b) The *Supplier* shall obtain the required clearances for access to the *Purchaser's* premises.

c) The *Supplier* shall provide the installation test plan and acceptance test procedure for review and acceptance by the *Purchaser.*

6.1.3 Support and Maintenance

a) The *Supplier* shall provide maintenance agreement, for the period of the contract duration, in the proposal to keep the system up to date including any 3rd line of support that may be required. The required 3rd line support shall include:

1) Firmware and software updates, maintenance, administration, configuration activities and security patching.

2) Hardware support and maintenance.
3) Technical assistance during threat monitoring.
4) Technical assistance during threat investigation and analysis.
5) Technical assistance during incident response (depending on the nature of the detected intrusion).

6.1.4 Training

a) The *Supplier* shall provide training on the system to be held in RSA.

b) The training provided shall include the following:

1) system overview and operations and use
2) system configuration and maintenance
3) threat monitoring, investigation and analysis
4) advanced system functionality and customisation (if available)
5) hands-on practical training on the material covered.

c) Training interventions shall occur just prior to the initial installation, configuration and commissioning of the system.

d) All material used for training shall be available online on the system.

e) The preferred mode for content delivery for all formal training is direct contact (in person). Other modes of content delivery such as e-training can be proposed for consideration by the *Purchaser*.

f) The *Supplier* shall provide a list of all courses offered, brief course descriptions and syllabi.

6.1.5 Monitoring

The systems are to be self-contained on-premise with no connectivity to external networks and monitoring or operations centres. The *Purchaser's* primary intent is to use its own workforce to monitor the systems on-premise. However, the option for the *Supplier* to provide the monitoring as a service shall be provided as follows:

a) This service shall be **"as and when required"** defined by the *Purchaser*.

b) Monitoring of the system shall be provided by the *Supplier*.

c) Events detected and verified by the *Supplier* as true positives shall:

1) undergo categorisation and prioritisation conducted by the *Supplier*,
2) be communicated to the *Purchaser,*
3) undergo threat investigation and analysis conducted by the *Supplier* or the *Purchaser* (if requested by the *Purchaser*).

6.1.6 Threat Investigations and Analysis

Detected threats by the offered solution will require further investigation and analysis. The Purchaser's primary intention is to use its own workforce together with the automated facilities in the tools to conduct threat investigation and analysis. However, the option for the *Supplier* to provide threat investigation and analysis as a service shall be provided as follows:

a) This service shall be **"as and when required"** defined by the *Purchaser*.

b) Threat investigations shall be provided by the *Supplier* after a threat has been detected and verified.

c) Threat analysis shall be provided by the *Supplier* after a threat has been detected and verified. The analysis to include the *"why"*, *"how"*, *"where"* and *"what"*.

6.1.7 Augment Incident Response

On the successful confirmation of a cyber event, the *Purchaser's* incident management and response procedure will be triggered. This includes but is not limited to identification, prioritisation, solving and restoration of system or service performed by the *Purchaser.* However, the option for the *Supplier* to provide augmented services around incident management and response shall be provided as follows:

a) This service shall be **"as and when required"** defined by the *Purchaser*.

b) Augmented support services shall be provided by the *Supplier* for any of the following incident management steps:

1) Preparation
2) Detection and analysis
3) Categorisation and prioritisation
4) Notification
5) Containment
6) Forensic investigation
7) Eradication
8) Recovery
9) Post-incident activities

7. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Martin Kopa	Senior Manager – Transmission Technical Operations (acting)
Richard McCurrach	Senior Manager – Transmission Information Management (acting)
Ernest Mpshe	Middle Manager – National Control Systems Support
Andre De La Geurre	Middle Manager – PTM&C Protection Technology
Cornelius Naidoo	Middle Manager – PTM&C Telecommunications Technology
Alison Maseko	– Telecommunications Operations
Meenal Vala	Chairperson – SCOT Cybersecurity Study Committee
Mondli Dlamini	Chief Engineer - Cybersecurity

8. Revisions

Date	Rev.	Compiler	Remarks
March 2025	2	T Ramulondi	• Changed template to NTCSA • Re-phrased the title of the document • Included Endpoint Detection & Response requirements • Merged the HIDS requirements with EDR • Moved systems sizing details to the Scope of Work document
May 2022	1	J Hector	First issue.

9. Development team

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

- Bongani Shezi
- Jason Hector
- Johan Botha
- Oscar Ngwenya
- Tjaart Visser
- Ian Naicker
- Elekanyani Mugivhi

10. Acknowledgements

The following people contributed to the revision of this standard:

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorized version on the system. No part of this document may be reproduced in any manner or form by third parties without the written consent of National Transmission Company South Africa SOC Ltd Reg No 2021/539129/30

- Johan Botha
- Kholofelo Halefose
- Mondli Dlamini
- Kgomotso Manyapetsa
- Sipho Sithole