

	<b>Specification</b>	<b>Telecommunications</b>
---	----------------------	---------------------------

Title: **OT SIEM Scope of Work**

Document Identifier: 559-489505716

Alternative Reference  
Number:

Area of Applicability: **National Transmission  
Company South Africa SOC  
Ltd**



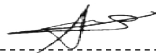
Functional Area: **NTCSA Telecommunication**

Revision: **1**

Total Pages: **12**

Next Review Date: **July 2027**

Disclosure  
Classification: **Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
		
<b>BCD Thakadu</b> <b>S Engineer</b>	<b>TP Mahlangu</b> <b>ND Manager</b>	<b>M Hina</b> <b>NPAE Manager</b>
Date: 28/05/25	Date: 28/05/2025	Date: 25/05/2025

## Content

### Page

1. Introduction.....	4
2. Supporting Clauses .....	4
2.1 Scope.....	4
2.1.1 Purpose.....	4
2.1.2 Applicability .....	4
2.1.3 Effective date.....	4
2.2 Normative/Informative References .....	4
2.2.1 Normative.....	4
2.2.2 Informative.....	5
2.3 Definitions .....	5
2.4 Abbreviations .....	5
2.5 Roles and Responsibilities .....	5
2.5.1 NTCSA's responsibilities .....	5
2.5.2 Supplier's responsibilities .....	5
2.6 Process for Monitoring.....	6
2.7 Related/Supporting Documents.....	6
3. Statement of Work.....	6
3.1 Design requirements .....	6
3.1.1 Design assurance.....	6
3.1.2 Solution description requirements.....	7
3.1.3 Design constraints and parameters .....	7
3.1.4 Design documentation/artefacts requirements.....	8
3.2 Project management requirements.....	8
3.2.1 Project schedule.....	8
3.3 Implementation requirements .....	9
3.3.1 Supply and delivery requirements.....	9
3.4 Support and maintenance requirements.....	9
3.4.1 Network support requirements.....	9
3.4.2 Maintenance, repair and replacement service .....	10
3.4.3 Spares requirements .....	10
3.4.4 Testing requirements.....	10
3.4.5 Ad hoc support requirements.....	10
3.5 Training requirements.....	10
3.5.1 On the job training/mentoring/job shadowing .....	10
3.5.2 Formal training .....	10
3.6 Skills, expertise and experience requirements.....	11
3.6.1 Solution delivery experience.....	11
3.6.2 Solution support, maintenance and training experience.....	11
4. Acceptance.....	12

### CONTROLLED DISCLOSURE

5. Revisions .....

6. Development Team .....

7. Acknowledgements .....

12

12

12

Figures

N/A

Tables

N/A

CONTROLLED DISCLOSURE

## 1. Introduction

There is a requirement within NTCSA for the deployment of an Operational Technology (OT) Security Event and Incident Management (SIEM) system. The 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 specifies the requirements for a turnkey solution to upgrade the OT SIEM solution.

## 2. Supporting Clauses

### 2.1 Scope

This document details requirements and scope for the provisioning of the OT SIEM solution.

#### 2.1.1 Purpose

The purpose of this document is to define the minimum requirements for turnkey solution for the OT SIEM solution. This document is intended to be used to select a suitable supplier that can develop the required solution, in full.

#### 2.1.2 Applicability

This document shall apply throughout NTCSA.

#### 2.1.3 Effective date

This document is effective from the date of the last authorizing 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] 240-185000083 Requirement Specification for a NTCSA Operational Technology (OT) SIEM
- [3] 240-86458714 Generic Network Management Specification Standard
- [4] 240-130816381 Scope of Work for Support of Telecommunications Network and Related Systems
- [5] 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts
- [6] 240-170001061 Transmission Cyber Security Standard for Operation Technology
- [7] 240-79669677 Demilitarised Zone (DMZ) Designs for Operational Technology
- [8] 32-85 Eskom Information Security Policy

**CONTROLLED DISCLOSURE**

[9] 32-214 IT/OT – Third Party Access Control Procedure

[10] 240-127964348 Technical Evaluation Criteria for NTCSA OT SIEM Solution

### 2.2.2 Informative

[11] 32-9 Definition of Eskom Documents

[12] 32-644 Eskom Documentation Management Standard

## 2.3 Definitions

**Security Information and Event Management** system is a system that collects, analyses and correlates security data from various sources within an organization's networks.

## 2.4 Abbreviations

Abbreviation	Explanation
DCN	Data Communications Network
NMC	Network Management Centre
NPAE	National Planning and Application Engineering
NTCSA	National Transmission Company of South Africa
OEM	Original Equipment Manufacturer
OT	Operational Technology
SHEQ	Safety Health Environmental Quality
SIEM	Security Information and Event Management

## 2.5 Roles and Responsibilities

### 2.5.1 NTCSA's responsibilities

- Create a conducive environment for the supplier by making relevant resources (people and workspace) available
- Provide network access and all support functions and services required for the solution
- Provide technical support and specialist knowledge of the telecommunications network services and the NTCSA Telecommunications Wide Area Network (WAN)

### 2.5.2 Supplier's responsibilities

- Respond to the enquiry with a technical proposal, accompanied by a high level design and project schedule to address the requirements specified in **Error! Reference source not found.** 240-185000083 Requirement Specification for a NTCSA's Operational Technology (OT) SIEM and [2] 240-86458714 Generic Network Management Specification Standard
- Develop the solution, this entails obtaining technical governance approval for the High Level Design, and developing the High Level Design into a Low Level Design and project management.

**CONTROLLED DISCLOSURE**

- c) Produce the Network Implementation Plan documentation and obtain change management approval for implementing the solution
- d) Produce Installation Test Procedures and Acceptance Test Procedures for the solution
- e) Implement the solution, this entails, supply, delivery, installation and commissioning of the solution
- f) Support and maintain the solution, this entails technical support services, software and hardware support services
- g) Training and handover, this entails knowledge transfer and handover of the solution to NTCSA staff for operating and maintenance.

## 2.6 Process for Monitoring

The implementation of this document will be through a procurement/commercial process. The management of the document will be done according to NTCSA's document and records management standards.

## 2.7 Related/Supporting Documents

This document is supported by the following documents:

- a) 240-55410927 Cyber Security Standard for Operation Technology
- b) 240-185000083 Requirement Specification for a NTCSA Operational Technology (OT) SIEM solution.
- c) 240-86458714 Generic Network Management Specification Standard
- d) 240-130816381 Scope of Work for Support of Telecommunications Network and Related Systems
- e) 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts
- f) 240-127964348 Technical Evaluation Criteria for NTCSA's OT SIEM solution.

## 3. Statement of Work

### 3.1 Design requirements

#### 3.1.1 Design assurance

- a) All designs produced shall be submitted for review by the relevant NTCSA design review committees, the supplier shall be able to present these, if required, and to take on full design accountability.
- b) OEM validation of designs shall be obtained where applicable.
- c) Penetration tests shall accompany all security and cybersecurity designs.
- d) The supplier shall be OEM accredited to offer the solution (letter from OEM shall be provided as proof of accreditation).

**CONTROLLED DISCLOSURE**

- e) The supplier shall be OEM accredited to offer the design and planning services on the offered solution (letter from OEM shall be provided as proof of accreditation).
- f) Supplier shall provide case studies demonstrating use of offered solution. The case studies should be clear on the level of skills and expertise the supplier has with delivery of similar solutions (i.e., design, planning, installation, commissioning, SHEQ, and project management).

### 3.1.2 Solution description requirements

- a) Supplier shall provide a design for the NTCSA's SIEM solution. The scope of the solution is for Highly Available (HA) SIEM solution.
- b) The data centre sites where the SIEM solution are to be hosted are: Simmerpan NMC in Germiston (Gauteng), Emkhuweni in Malahleni (Mpumalanga)
- c) The source of data will be various network devices installed in the field throughout the country and the servers within the data centres mentioned above.

### 3.1.3 Design constraints and parameters

- a) This design shall at minimum address the following functional and technical requirements:
  - 1) System specification
    - i. 240-185000083 Requirement Specification for a NTCSA Operational Technology (OT) SIEM
  - 2) Network management specification
    - i. 240-86458714 Generic Network Management Specification Standard
  - 3) Support requirements
    - i. 240-130816381 Scope of Work for Support of Telecommunications Network and Related Systems
    - ii. 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts
  - 4) Security specifications
    - i. 240-55410927 Cyber Security Standard for Operation Technology
    - ii. 240-79669677 Demilitarised Zone (DMZ) Designs for Operational Technology
    - iii. 32-85 Eskom Information Security Policy
    - iv. 32-214 IT/OT – Third Party Access Control Procedure
- b) Supplier shall clearly document and motivate for any deviations to any of the standards specified above.
- c) The core of the system shall be designed to support or be extended to support the entire NTCSA requirements, if required.

**CONTROLLED DISCLOSURE**

### 3.1.4 Design documentation/artefacts requirements

#### 3.1.4.1 High level design (HLD)

- a) The solution shall be accompanied by an HLD. An HLD comprises of document(s) detailing the overall architecture, solutions/systems configuration/layout and equipment and/or software selected. Data Communications Network (DCN) design choices if applicable. This should include information on design options, costing, constructability, procure-ability, operability, sustainability, reliability, availability, inspect-ability, test-ability, expandability, decommission-ability and all other risks considered prior to arriving at the recommended option. At least two options should be documented at this level.
- b) The estimated costs associated with the design, including travel and subsistence to all the sites applicable shall be quoted for as a single line item per Data Centre in the Bill of Material (BoM) for the HLD.
- c) The HLD shall be a returnable, as part of the technical proposal. It shall be accompanied by a detailed Bill of Materials (BoM) with associated quantities, costing/pricing and assumptions made (if any).

#### 3.1.4.2 Low level design (LLD)

- a) An LLD comprises of document(s) detailing the selected equipment, interfaces, modules, ports, software, firmware, operating systems, and applications for the solution. IP addressing plan, licensing and configuration templates. This should include information on Bill of Materials (BoM) and/or Quantities (BoQ). A complete DCN design forms part of this documentation set.
- b) The supplier shall provide the template(s) for the LLD for evaluation purposes.
- c) The supplier shall develop the LLD after contract award, as part of the solution development process.

#### 3.1.4.3 Design Guide

- a) The supplier to develop a design guide (detailed planning and ordering document). This is a non-billable document that is expected from the supplier.

#### 3.1.4.4 Blue Book

- b) The supplier to develop blue books (planning blueprint, of what is to be implemented). This is a non-billable document that is expected from the supplier at the end of the implementation and covers the changes made to the design during the implementation stage.

### 3.2 Project management requirements

#### 3.2.1 Project schedule

- a) Supplier shall develop a Project Management plan. This detail shall at minimum address the following:
  - 1) Project Schedule

**CONTROLLED DISCLOSURE**



- 2) Task Responsibility Assignment
  - 3) Task Sequencing
  - 4) Duration Estimation
  - 5) Work Breakdown Structure
  - 6) Risk Management Plan
- b) The Project Management Plan is a returnable and shall accompany the HLD.

### **3.3 Implementation requirements**

#### **3.3.1 Supply and delivery requirements**

This is as described in [5] 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts

##### **3.3.1.1 Installation and commissioning requirements**

- a) Network Implementation Plan (NIP) comprises of document(s) detailing the installation and commissioning activities, site survey forms, staging plans, installation test plans (ITPs) and knowledge transfer plans (operator, administrator and technician), training plans (planner, operator, administrator and technician), and cutover plans.
  - 1) The supplier shall provide the template(s) for the NIP for evaluation purposes.
  - 2) The supplier shall develop the NIP after developing the LLD, as part of the solution development process.
- b) Network Ready for Use (NRFU) comprises of document(s) detailing the acceptance test plans (ATPs), commissioning, and change management plans, operator readiness plans, maintenance, administration, disaster recovery plans and procedures.
  - 1) The supplier shall provide the template(s) for the NRFU for evaluation purposes.
  - 2) The supplier shall develop the NRFU after developing the NIP, as part of the solution development process.
- c) The supplier to develop as-built documentation for each installation.
- d) The remainder of the requirements are as described in [5] 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts

### **3.4 Support and maintenance requirements**

#### **3.4.1 Network support requirements**

This is as described in [4] 240-130816381 Scope of Work for Support of Telecommunications Network and Related Systems

**CONTROLLED DISCLOSURE**

### 3.4.2 Maintenance, repair and replacement service

This is as described in [4] 240-130816381 Scope of Work for Support of Telecommunications Network and Related Systems

### 3.4.3 Spares requirements

This is as described in [5] 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts

### 3.4.4 Testing requirements

This is as described in [5] 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts

### 3.4.5 Ad hoc support requirements

- a) Any other support (including design, design alterations, testing and development) required by NTCSA and not part of SLA shall be on time and material basis. The following sub-clauses shall be adhered to when applicable:
- 1) New designs shall be submitted for approval to relevant NTCSA's technical governance committees, the supplier shall be able support this process as part of the design output.
  - 2) Alterations to existing designs shall be documented as engineering instructions (EIs) and be subjected to NTCSA's approval process, the supplier shall be able support this process as part of the design output.
  - 3) Design guidelines, in NTCSA's required format, shall be documented and be subjected to NTCSA's approval process, the supplier shall be able support this process as part of the design output.
  - 4) Configuration changes shall be subjected to NTCSA's change management process, the supplier shall be able to support this process as part of the ad hoc technical support

## 3.5 Training requirements

### 3.5.1 On the job training/mentoring/job shadowing

The requirements for informal training are as specified in [4] 240-130816381 Scope of Work for Support of Telecommunications Network and Related Systems

### 3.5.2 Formal training

The requirements for formal training are as specified in [5] 240-135089195 Generic Technical Requirements for NTCSA Telecoms Contracts.

**CONTROLLED DISCLOSURE**

### **3.6 Skills, expertise and experience requirements**

#### **3.6.1 Solution delivery experience**

- a) Supplier shall be able to demonstrate the functionality of the equipment at own premises or facilities, and should be able to accommodate a site visit by NTCSA as part of technical evaluation.
- b) Supplier shall provide details on available resource capacity. This detail shall at minimum address the following:
  - 1) Numbers of OEM certified professionals for each offered equipment. Highlight level and type of certification (e.g., associate / junior).
  - 2) Numbers of in-house project managers and/or solution/service delivery managers and/or SHEQ resources that have handled similar projects and/or solutions involving equipment/solutions being offered.
  - 3) National footprint and/or resource distribution
  - 4) Available test facilities for functionality testing of equipment being offered
  - 5) Delivery lead times (for each offered equipment, module, software and associated licences)

#### **3.6.2 Solution support, maintenance and training experience**

- a) The supplier shall be OEM accredited to offer the support and maintenance services on the offered equipment/solution (letter from OEM shall be provided as proof of accreditation).
- b) Supplier shall provide case studies supporting their service offering. The case studies should be clear on the level of skills and expertise the supplier has with telecommunications service delivery (i.e., service provisioning, operation, administration, maintenance, and training).
- c) Supplier shall offer Support & Maintenance (S&M) for all technologies and/or solutions offered.
- d) Support services to be broken down into varying service category options indicating varying SLA options.
- e) Supplier shall provide details of S&M being proposed, with details such as e.g., “follow the sun” support model, access to global (world-wide) teams, service desk/portal (logging and management of incidents), SLA tracking, etc.
- f) Supplier shall provide details on processes, systems and available resources for:
  - 1) Fault Management – fault identification (root-cause analysis), isolation and resolution
  - 2) Configuration Management – service provisioning, network configuration templates, change management
  - 3) Accounting Management – user accounting, resource utilization, service accounting
  - 4) Performance Management – equipment health reports, network health reports, node performance monitoring, end-to-end service reports

#### **CONTROLLED DISCLOSURE**

- 5) Security Management – user role & grouping, role-based security, user authentication, authorisation and accounting,
- g) Supplier shall provide details on customer relationship management this includes:
- 1) Processes, procedures and service contracts (SLAs)
  - 2) Available helpdesk, service desk, and/or call centre facilities for support ticket logging, routing and tracking.
  - 3) Business continuity plans for offered service, and associated support systems (i.e., service desk and call centre operations).
- h) Supplier shall provide details on available resource capacity. This detail shall at minimum address the following:
- 1) Spares holdings, testing, and distribution (spares management philosophy/policy), indicate location of warehouses to support NTCSA's operations.
  - 2) Support lead times (for each offered equipment, module, software and associated licences)
  - 3) Equipment and/or module repair turnaround times
  - 4) Training proposal (knowledge and skills transfer plan)

#### 4. Acceptance

This document has been seen and accepted by:

Name	Designation
Cornelius Naidoo	Telecoms T&S Engineering Manager
Mfundiso Hina	Middle Manager NPAE
Thabang Mahlangu	Network Development Manager

#### 5. Revisions

Date	Rev.	Compiler	Remarks
April 2025	1	BCD Thakadu	First draft

#### 6. Development Team

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

- Bongani Shezi
- David Thakadu
- Phelokazi Ndlovu

#### 7. Acknowledgements

None

**CONTROLLED DISCLOSURE**