

Standard

Transmission

Title: **REQUIREMENT SPECIFICATION** Unique Identifier:

FOR A NTCSA OPERATIONAL **TECHNOLOGY (OT) SIEM**

SOLUTION

240-185000083

Alternative Reference Number: N/A

Area of Applicability:

Engineering

Documentation Type:

Standard

Revision:

1

Total Pages:

19

Next Review Date:

As required

Disclosure Classification:

Controlled **Disclosure**

Compiled by

Approved by

Authorized by

Bongani Shezi

Chief Engineer

Date: 02 September 2024

Cornelius Naidoo

Middle Manager Telecoms and Physical Security T&S

Date: 9 September 2024

Senior Manager PTM&C

Engineering

Date: 09 September 2024

Supported by

Ernest Mpshe

SCOT SC/Chairperson

Date: 04 September 2024

PCM Reference: 240-53458797

SCOT Study Committee Number/Name: Systems & Tools Study Committee

REQUIREMENT SPECIFICATION FOR A NTCSA OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

1

Revision:

Page: 2 of 20

Content

				Page
1.	Intro	duction		4
2.	Supp	orting o	clauses	4
	2.1	Scope		4
		2.1.1	Purpose	4
		2.1.2	Applicability	4
	2.2	Norma	ative/informative references	4
		2.2.1	Normative	4
		2.2.2	Informative	5
	2.3	Definit	ions	5
		2.3.1	General	5
		2.3.2	Disclosure classification	6
	2.4	Abbre	viations	6
	2.5	Roles	and responsibilities	8
		2.5.1	Eskom's responsibilities	8
		2.5.2	Supplier's responsibilities	8
	2.6	Proces	ss for monitoring	8
	2.7	Relate	d/supporting documents	8
3.	SIEN	/I Solution	on for NTCSA OT	8
	3.1	Functi	onal Requirements	8
		3.1.1	Log Management	8
		3.1.2	Monitoring, logging and tracking	10
		3.1.3	Correlation	10
		3.1.4	Threat intelligence	10
		3.1.5	User and Entity Behaviour Analysis	11
		3.1.6	Threat alerting, contextualization, and response	11
		3.1.7	Analytics	12
		3.1.8	Dashboards	13
		3.1.9	Reporting and Notifications	
	3.2	Gener	al Requirements	
		3.2.1	Location	
		3.2.2	Communication between System Components	
		3.2.3	Availability	
		3.2.4	Sanitisation	
		3.2.5	Backup and Recovery	
		3.2.6	Data Retention Strategy	
		3.2.7	Monitoring, Operation and Administration	
		3.2.8	Integration	
		3.2.9	Access Control	
			Documentation	
	3.3		e Requirements	
		3.3.1	Supply and Delivery	
		3.3.2	Installation, Configuration and Commissioning	
		3.3.3	Support and Maintenance	
		3.3.4	Training	
		3.3.5	Monitoring	18

REQUIREMENT SPECIFICATION FOR A NTCSA OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

			Page:	3 of 20	
	3.3.6	Threat Investigations and Analysis			
	3.3.7	Augment Incident Response			18
4.	Authorizatio	n			19
5.	Revisions				19
6.	Developme	nt team			19
7.	Acknowledg	ements			20
Tak	oles				
Tab	ole 1: High Av	railability and Disaster Recovery requirements			14

REQUIREMENT SPECIFICATION FOR A NTCSA OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 4 of 20

1. Introduction

This document details Eskom NTCSA's Operational Technology (OT) requirements for a complete Security Information and Event Management (SIEM) solution. 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 details the requirements for NTCSA's OT requirements for SIEM solution to ensure the sustainability of such system 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 SIEM for three separate critical OT systems within NTCSA which are titled System 1 and System 2. The scope is to include the deployment of SIEM into development environments within the said OT systems. The SIEM shall be on-premises and not require external communications for normal operations. Updates to the systems shall occur through offline mechanisms. The systems shall interface to enterprise SIEM and Security Orchestration, Automation and Response (SOAR) if required.

2.1.1 Purpose

The purpose of this document is to provide the SIEM requirements together with system and operational service requirements.

2.1.2 Applicability

This document is applicable to Eskom's NTCSA.

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] 240-135101235 Application Design for: Basic Design for OT SIEM Solution
- [3] 240-84323647 Network Management Centre Redundancy Standard.
- [4] 240-60725641 Specification for standard (19 inch) Equipment Cabinets.
- [5] EN-50174-1 Information technology Data centre facilities and infrastructures Part 1: General

Document Classification: Controlled Disclosure
REQUIREMENT SPECIFICATION FOR A NTCSA

OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: **5 of 20**

concepts.

- [6] EN-50174-2 Information technology Data centre facilities and infrastructures Part 2-2: Power supply and distribution.
- [7] 240-89797258 The Safe Handling. Transportation and Disposal of Cells, Batteries and Electrolyte.
- [8] IEC 60529 Degrees of Protection Provided by Enclosures (IP Code).
- [9] 240-52599753 Workplace Space and Furniture Standard for Commercial Properties.
- [10] 240-156552996 Generic Technical Specification for Eskom Real Estate (ERE) type Projects for Fire Protection Systems and Fire Detection Systems.
- [11] 240-55410927: Cyber Security Standard for Operational Technology.
- [12] 240-110767932: Sanitisation of Data and Storage Media

[13]

2.2.2 Informative

- [14] 32-894 Eskom Server Rooms and Data Centre Standard.
- [15] 32-1203 Eskom Telecommunications User Requirements.
- [16] Searching for a SIEM Solution? Here Are 7 Things It Likely Needs. Available At: https://www.gartner.com/en/articles/searching-for-a-siem-solution-here-are-7-things-it-likely-needs [Date: 07 May 2024]
- [17] SIEM solutions definition & overview. Available At: https://www.sumologic.com/glossary/siem-solutions/ [Date: 07 May 2024]
- [18] The Minimum Requirements for Enterprise SIEM Solutions. Available At https://solutionsreview.com/security-information-event-management/the-minimum-requirements-for-enterprise-siem-solutions/ [Date: 24 May 2024]
- [19] SIEM Library. Available at: https://www.manageengine.com/ [Date: 23 June 2024]

2.3 Definitions

2.3.1 General

Definition	Description
Agent-based log collection	This means an agent is installed on network devices that generates logs. These agents are responsible for collecting the logs from the devices and forwarding them to the central SIEM server. Apart from these responsibilities, they can also filter the log data at the device level based on predefined parameters, parse them, and convert them to a suitable format before forwarding. This customized log collection and forwarding technique helps in optimal usage of bandwidth. The agent-based log collection method is predominantly used in closed and secured zones where communication is restricted.

Document Classification: Controlled Disclosure
REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 6 of 20

Definition	Description
Agentless log collection	This technique does not involve the deployment of agents in any network device. Instead, configuration changes have to be made in the device so they can send any generated logs to the central SIEM server in a secure manner. In devices such as switches, routers, firewalls, etc., the installation of third-party tools for log collection is often not supported, so collecting log data through an agent becomes difficult. In such cases, an agentless log collection technique can be used. It also reduces the load on the network device as the deployment of an additional agent is not necessary.
API-based log collection	In this technique, logs can be collected directly from the network devices with the help of application programming interfaces (APIs). Virtualization software provides APIs, which enable the SIEM solution to collect logs from virtual machines remotely.
Data enrichment	Improving the accuracy and reliability of raw data by adding new and supplemental information.
Log	Log data is an ongoing record of events in an organization's network environment. This includes everything from user activities to system operations and even warnings or error messages from software applications. Essentially, logs serve as a form of "black box" for information, security and communication networking systems, offering a comprehensive timeline of activities.
Real time	The actual time during which a process or event occurs.
SIEM	SIEM is a unified management and integration layer that sits on top of the security and detection infrastructure. As organizations scale and grow, they deploy more hardware, applications, and endpoints which, in turn, increase computer logs. The SIEM collects and integrates all the computer-generated log data (captured by each hardware, software, applications, and endpoints) and display them in real-time through easy-to-read formats. As well as providing real-time analysis on security threats throughout digital infrastructure. By aggregating log data from various network sources, SIEM enables the early detection of potential attacks and data breaches, ensuring a robust defence against cyber threats

2.3.2 Disclosure classification

Controlled disclosure: controlled disclosure to external parties (either enforced by law, or discretionary).

2.4 Abbreviations

Abbreviation	Description	
AD Active Directory		
Al	Artificial Intelligence	
API Application Programming Interface		
CEF Common Event Format		
CIP Critical Infrastructure Protection		
CPS	Cyber Physical Systems	
CPU Central Processing Unit		
ETL	Extract, Transform, Load	

Document Classification: Controlled Disclosure
REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: **7 of 20**

Host Intrusion Detection System			
Industrial Control System			
Information and Communications Technology			
Intrusion Detection System			
Indicators of Compromise			
Internet Protocol			
Lightweight Directory Access Protocol			
Machine Learning			
Network Element			
North American Electric Reliability Corporation			
Network Intrusion Detection System			
National Institute of Standards and Technology			
National Transmission Company of South Africa			
Operational Technology			
Protection, Telecommunications, Metering & Control			
Recovery Point Objective			
Republic of South Africa			
Recovery Time Objective			
Security Information and Event Management			
Security, Orchestration, Automation and Response			
Security Operations Centre			
Structured Threat Information eXpression			
Terminal Access Control System			
Trusted Automated eXchange of Intelligence Information			
Virtual Local Area Network			
Virtual Routing and Forwarding			

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 8 of 20

2.5 Roles and responsibilities

2.5.1 Eskom's responsibilities

- a) Create a conducive environment for the supplier by making relevant resources (people and workspace) available.
- b) Provide network access in accordance with the relevant Eskom security policies/procedures.
- c) Provide support functions and services required for the solution.
- d) Provide technical support and specialist knowledge of the OT domain/environment (power, cooling, cabling, cabinet space, wiring, Local Area Network (LAN)/ Wide Area Network (WAN), systems, applications).

2.5.2 Supplier's responsibilities

- a) Design, development, implementation, testing, installation, commissioning, and support of the solution.
- b) Training and skills transfer on the operation, administration and maintenance of the solution.
- c) Handover of solution documents (design, planning, maintenance, administration and operation)

2.6 Process for monitoring

This standard's stakeholders shall monitor changes in the SIEM requirements for NTCSA's OT environment, as well as changes in technology and if necessary, this standard shall be revised through SCOT.

2.7 Related/supporting documents

240-86458714 Generic Requirements Specification for a Telecommunications Network Management Solution 240-135089195 Generic Technical Requirements for Eskom Telecoms Contracts

3. SIEM Solution for NTCSA OT

SIEM combines security information management (SIM) and security event management (SEM) into one security management system. SIEM collects data on security events in real time and provides historical analysis of such events from a wide variety of data sources. It can also flag and report events that require investigation and assist with validating (and responding to) issues that may cause harm to the organization.

3.1 Functional Requirements

3.1.1 Log Management

The solution shall offer an effective log management function. These should include a mechanism for the collection, storage, and analysis of log data from various sources across the OT network.

A primary role of log management within SIEM is to collect and store this vast amount of log data generated from various sources such as servers, databases, networks, and applications. This broad-based collection ensures that a comprehensive view of the organization's IT environment is captured, providing the necessary context for identifying security incidents.

But collecting and storing log data is just the tip of the iceberg. The data drawn from different sources can vary greatly in format and structure. Because of this, normalization and parsing (transforming the data into a consistent format) are critical for effective analysis. This process enables the SIEM system to analyze diverse log data collectively, allowing for more accurate threat detection and response.

REQUIREMENT SPECIFICATION FOR A NTCSA OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 9 of 20

Last but certainly not least, log management within SIEM takes into account log retention and compliance considerations. Many organizations are often legally required to retain their log data for a certain period of time, primarily for audit and compliance purposes. SIEM systems can automate this process, ensuring that organizations meet their log retention requirements while also providing valuable data for future security investigations and audits.

Log management involves the collection, normalization, and analysis of log data, and is used to gain better visibility into network activities, detect attacks and security incidents, and meet the requirements of IT regulatory mandates. For effective log analysis, SIEM solutions employ different processes such as log correlation and forensics, which help detect data breaches and attacks in real time. Log management also includes securely archiving log data to retain logs for a custom time period.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 10 of 20

3.1.2 Monitoring, logging and tracking

- a) **Real time ingestion**. The solution shall have the ability to ingest logs in real or near real-time and allow for instant searching. The following methods/techniques shall be supported:
 - 1) Agentless based collection
 - 2) Agent-based collection
 - 3) API-based log collection
- b) At minimum logs from network security devices and products such as firewalls, virtual private networks, intrusion prevention systems, email and web security gateways, and antimalware products, physical and virtual appliances and software.
- c) The solution shall have the ability to consume log events using the Common Event Format (CEF) or known technology log formats without additional ETL processes. Where CEF is not possible, the solution should allow for custom ingestion scripts. As a minimum, the solution shall be able to natively integrate with the following sources:
 - 1) Windows, Linux and Unix type event logs
 - 2) Network management and routing devices and appliances
 - 3) Anti-virus, anti-malware, security auditing software, vulnerability management technologies and identity and access management logs.
 - 4) For maximum effectiveness, the solution shall be able to integrate with customized data sources and feeds, such as legacy applications to homegrown databases.
 - 5) Database logs such as Microsoft SQL, Oracle, Postgre.
 - 6) Application logs, including those from telecommunications network management systems (OSS/BSS), physical security information management systems (PSIM) and transmission energy management systems (TEMSE).
 - 7) Networking and perimeter security appliances such as Cisco, Huawei, Sophos etc.
- d) Normalization. The solution shall support data normalization functions for ease of analysis of logs created in different languages and formats. This entails parsing (transforming the log data into a consistent format). Solution shall be able to normalize logs by formatting them into a standardized format. Supported formats shall be specified.
- e) Aggregation. The solution shall aggregate systems logs and security data from various applications and sources into one, unified place. Aggregation is the process of collecting and combining multiple log entries to streamline analysis. The solution shall store and manage all aggregate data in one place, allowing for centralized log data for disparate systems that can be viewed and correlated by security analysts.
- f) The solution shall offer capabilities to generate raw log data on behalf of other hosts.

3.1.3 Correlation

- a) Correlation engines have the ability to put different security incidents together to give a holistic view of security attacks. They are capable of detecting signs of suspicious activity, compromise, or potential breach early in the network.
- b) The solution shall support correlation functions, by analysing the collected log data for any relationships existing between different network activities, common attributes, or patterns that might be present.
 - 1) The solution shall have predefined correlation rules based on indicators of compromise (IOCs)
 - 2) The solution shall support user-defined correlation rules.
 - The solution shall offer capabilities to modify and improve correlation rules on a need basis.

3.1.4 Threat intelligence

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 11 of 20

a) The solution shall be capable of ingesting threat intelligence feeds. These feeds, could be from separate subscriptions, contain up-to-date information on threat activity observed all over the world, including which hosts are being used to stage or launch attacks and what the characteristics of these attacks are. At minimum open-source threat feeds available in STIX/TAXII format shall be supported.

- b) The solution shall have threat intelligence capability essential for preventing an attack from occurring rather than reacting to the incident after it happens.
- c) The solution shall have the ability to combine the knowledge gained from evidence, contextual information, indicators, and action responses collected from various threats, and producing concrete instances of IOCs.
- d) The solution shall utilize log correlation, threat intelligence, and anomalous user behaviour analytics to quickly recognize pattern deviations or unusual activity.
- e) The solution shall be able to gather some threat intelligence and be compatible with plugins to collaborate and bolster the ability to identify external threats.
- f) The solution shall be able to provide information about the tactics, techniques, and procedures (TTPs) involved in the emerging threats and monitoring current network activities to spot anomalous patterns.

3.1.5 User and Entity Behaviour Analysis

- a) The solution shall incorporate artificial intelligence (AI) and machine learning (ML) tools and techniques including user and entity behaviour analysis (UEBA) to distinguish regular and irregular patterns in a network to determine if an activity poses a threat to the network. This means:
 - 1) Capability to analyse the normal work pattern of a user, or the typical way a particular user accesses the network on an everyday basis.
 - 2) Employ machine learning techniques to develop a behaviour model based on the normal behaviour of users and machines in a network. Any event that deviates from this behaviour model should be considered as an anomaly and be further assessed for potential threats. A risk score be assigned to the user or entity, the higher the risk score, the greater the suspicion.
 - 3) Detect deviations from normal behaviour, raise an alert, and notify the security administrator immediately.
 - 4) Use ML techniques and Al algorithms to process the information, learn the patterns of threats, and identify if a particular pattern in the network is similar to a threat anomaly that has previously taken place. With this detection,
 - Assist in the detection, mitigation, and prevention of data breaches by continuously monitoring user behaviour.
 - 6) Track accesses to critical data and identify unauthorized accesses or access attempts.
 - 7) Track and audit the actions of privileged users and generate real-time alerts for abnormal activities (e.g., privilege escalations in user accounts, and any changes to data made by those accounts).
 - 8) Generate real-time alerts and leverages automation in threat prevention to make it more reliable.
- b) MITRE ATT&CK Integration. The solution must be able to align its threat detection indicators to the MITRE ATT&CK framework.
- c) Business and organizational impact. The solution shall use a variety of analysis techniques, including correlation, statistical deviation and machine learning to identify threats and other events of interest. This should allow the organization to turn raw alert data into actionable intelligence.

3.1.6 Threat alerting, contextualization, and response

- The solution shall support automated notifications and security alerts providing real-time updates on any detected threats.
 - 1) Alert notifications shall be configurable to be sent via email or SMS in real time.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 12 of 20

2) Alert notification shall be categorized based on priorities assigned to them, e.g., high, medium, or low

- The severity and urgency/priority of the alert notification shall be customizable to align with business needs.
- b) The solution shall support dashboard features to allow for simplified, real-time monitoring that is customizable to prioritize the visibility of the most important data.
- c) The solution shall provide threat contextualization functions. Contextualization should assist in:
 - sorting out what actors were involved with the security event, what parts of the network they operated with, and when.
 - 2) sorting through the alerts to find actual potential threats.
 - 3) automatically filtering threats and reducing the number of alerts received.
- d) **Investigation Workspace.** The solution must have a built-in incident case management system that will generate incident investigation tickets and case management processes. The workspace should include a security workflow that will allow analysts to visualize the security monitoring stages, the incident response process, and the events that occur across each of these stages.
- e) The solution shall provide various workflows that can be automatically executed when an alert is triggered. These workflows should assist in preventing attacks from spreading laterally within the network.
- f) The solution shall have capabilities to assign workflows to security incidents so that when an alert is raised, the corresponding workflow can be executed automatically.

3.1.7 Analytics

- a) The solution shall use real-time analytics to detect and prioritize events or activities that may represent a threat, compliance issue or anything else of interest to users. These include cases such as:
 - 1) Predictive maintenance and resource monitoring
 - Inexplicably missing (offline) systems
 - 3) Transient asset spotting (potentially even rogue devices)
 - 4) Security alarms for traditional cyber threats or unauthorized accesses
 - 5) Unexpected system access or erroneous system behaviours
 - 6) Workflow/process failures, shutdown alerts, or manual alarm silencing
 - 7) Regulatory and compliance requirement
- b) The solution should offer batch analytics to identify and correlate weak signals in data not detected in real time.
- c) The solution should have forensic capabilities. As a minimum, the ability to:
 - Perform full packet captures for a network connection associated with malicious activity.
 - Perform host activity logging; the solution can perform such logging at all times, or the logging could be triggered when the solution suspects suspicious activity involving a particular host.
 - Perform a root cause analysis and generating an incident report that provides a detailed analysis of an attack attempt or an ongoing attack that helps security personnel take appropriate remedial action immediately.
 - 4) Generate forensic reports and discover the time at which a particular security breach occurred, systems and data that were compromised, actors behind the malicious activity, as well as the point of entry.
- d) The solution must provide an analytics interface in which events can be searched or displayed in a timeline format. The interface must allow for search queries based on an open search query language and regular expressions.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 13 of 20

e) The solution shall provide interfaces to assist in security analytics and facilitate security investigations. The interfaces should include at minimum sophisticated search capabilities and data visualization capabilities.

3.1.8 Dashboards

- a) The solution shall have pre-built dashboards for known and common activity reporting use cases, as well as the ability for custom dashboards to be created. The dashboards shall:
 - 1) be live and update automatically,
 - 2) present security data in the form of graphs and charts
 - 3) assist the security team in identifying malicious activities quickly and resolve security issues.
 - 4) assist, security analysts to detect anomalies, correlations, patterns, and trends that might be present in the data, and gain various insights into events taking place in real time.
 - 5) SIEM solutions also provide users an option to create and customize their own dashboards.

3.1.9 Reporting and Notifications

- a) The solution shall offer predefined reports built based on known IOCs, which assists in providing visibility into security events, detecting threats, and easing security and compliance audits.
- b) The solution should serve as a system of record for compliance, audit, forensics data and general reporting.
 - 1) The solution shall offer functions to automatically generate security compliance reports.
 - 2) The solution shall offer built-in support to generate reports that meet the requirements of various security compliance initiatives.
- c) The solution shall offer highly customizable reporting capabilities. The content of the reports shall be configurable and flexible.
- d) The solution shall provide users capabilities to filter, search, and drill down into the reports, set schedules for report generation as per the user's needs, view data in the form of tables and graphs, and export the reports in different formats.
- e) It shall be possible to send notifications via email via an SMTP server.
- f) Notification shall support a variety of flexible notification triggers such as detected events, failed console login attempts, exceeding of performance thresholds, etc.

3.2 General Requirements

- a) This solution shall be off-the-shelf, and no specific development should be necessary.
- b) NTCSA's OT environments require a SIEM solution on three critical systems. Monitoring shall primarily be performed locally by the respective OT environment.

3.2.1 Location

- The system shall be on-premises without any communication to external servers or websites.
- b) The system shall be capable of running autonomously and in a fully functional state.

3.2.2 Communication between System Components

- Dataflow shall be uni-directional from client devices to master consoles only, unless the system functionality calls for otherwise explicitly.
- Client devices and master station consoles shall use a fixed port for the network connection to allow strict firewall rules to be set.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: **14 of 20**

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

3.2.3 Availability

- a) The system shall have a 99.95% availability without any redundancy design translating to 21.92 minutes of downtime per month.
- b) Failed agents, probes, services or processes shall have auto-restart capability rendering an autonomous function across all components.
- c) 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 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.

Table 1: High Availability and Disaster Recovery requirements

Heading	OT System 1	OT System 2	OT System 3
High Availability	Yes	Yes	No
Disaster Recovery	Active- active, full continuous availability, preferred Active- hot standby, acceptable	Active- active, full continuous availability, preferred Active- hot standby, acceptable	Active- standby (cold)
Recovery Time Objective (RPO), acceptable system loss time	0-1 hour, preferred 8-24 hours, acceptable	0-2 hour, preferred 8-24 hours, acceptable	>72 hours
Recovery Point Objective (RPO)	No data loss	No data loss	>24 hours

3.2.4 Sanitisation

a) The solution shall enable the *Purchaser's* personnel to perform the required sanitization procedures as per **Error! Reference source not found.**.

3.2.5 Backup and Recovery

- a) The solution shall have a mechanism that allows the automation of system backups.
- b) The solution shall allow for backups to be kept on long-term storage on offsite locations.
- c) The solution shall have a mechanism that allows the for the restoration from system backups.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 15 of 20

3.2.6 Data Retention Strategy

- a) The solution shall assist with retention management. It should have enough data storage capacity for optimal operation, as well as required file types, location and processes, such as extraction or eradication.
 - 1) Data required for immediate searching should be in a hot state for 30 days.
 - 2) Data that is older than 30 days should be kept in a warm state for 90 days.
 - 3) Data older than 90 days should be archived or snapshot, however, it must still be searchable.
- b) The solution's storage shall be scalable, without impacting on performance.
- c) The solution shall keep historic alarms and alerts and aggregated data from which the alarms were derived in order to assist with forensic investigations.
- d) The period for which this data can be kept for shall be configurable.
- e) Export mechanisms to long-term storage shall be supported. Supported export formats shall be of are to be specified.
- f) The solution shall support for exporting and archiving of data to the following:
 - 1) local storage (i.e., the storage of the physical device on which the application is being accessed from, e.g., workstation, mobile device, etc.)
 - 2) network storage
 - 3) email recipients

3.2.7 Monitoring, Operation and Administration

- a) The solution shall offer functions to monitor relevant security alerts and data, allowing a single source of truth on real-time, prioritized alerts across the OT domain in which it is deployed. The monitoring shall primarily be performed locally by the relavant OT domain. The monitoring functions shall include the following:
 - 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).
- b) The solution shall provide tools to administer, maintain and support complex functions, such as:
 - 1) Log and data source management
 - 2) Analytics and detection content,
 - Reporting,
 - 4) User roles and access control, along with technical integration and
 - 5) Response workflows.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: **16 of 20**

c) Natively available content management. The solution shall provide data collectors, parsers, analytics rules and models, use cases, compliance packages and response workflows, actions and plays. Administrators can enable, access and update this content through an included management framework.

- d) **Product usability.** The solution shall provide easy-to-understand and user-friendly interfaces featuring intuitive designs to better facilitate user engagement.
- e) **Use cases.** The solution shall have predefined and common use cases ready to use. The use cases should also focus on performance and resource utilization for priority issues. The solution should also support a capability to allow for custom use cases to be written and deployed.

3.2.8 Integration

- a) The solution shall integrate with all relevant applications, data sources and technologies. The natively supported plug-ins, third-party apps and other software shall be specified.
- b) Data enrichment. The integration capability must allow for data enrichment at the time of data collection but prior to data ingestion into the SIEM data set. An example is enriching webserver event logs where IP addresses are immediately mapped according to geolocation tagging and all supporting telemetry chosen to be sent to the SIEM.
- c) It shall be possible to forward critical alerts and information from the solution to other enterprise systems such as a SIEM or SOAR or Security Operations Centre (SOC).

3.2.9 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.

3.2.10 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.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: **17 of 20**

c) The documentation shall be provided in English.

3.3 Service Requirements

3.3.1 Supply and Delivery

- a) The solution shall be off-the-shelf, and no specific development shall be allowed.
- b) The solution shall be supplied and delivered as hardware, software and/or licences to selected locations of within the Republic of South Africa (RSA).

3.3.2 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*.

3.3.3 Support and Maintenance

- a) The supplier shall provide an annual maintenance agreement 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).

3.3.4 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.

REQUIREMENT SPECIFICATION FOR A NTCSA
OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 18 of 20

3.3.5 Monitoring

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

- 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,
 - undergo threat investigation and analysis conducted by the Supplier or the Purchaser (if requested by the Purchaser).

3.3.6 Threat Investigations and Analysis

Detected threats by the SIEM will require further investigation and analysis on the alerts generated by the SIEM. 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 the 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".

3.3.7 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

REQUIREMENT SPECIFICATION FOR A NTCSA OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 19 of 20

4. Authorization

This document has been seen and accepted by:

Name and surname	Designation
Alison Maseko	Senior Manager – NTCSA Telecoms
Judith Malinga	Senior Manager – NTCSA PTM&C Engineering
Lenah Mothata	Senior Manager – NTCSA Grids
Johan Pieterse	Chief Engineer – NTCSA Secondary Plant, Work Planning and Centralised Services
Richard McCurrach	Senior Manager – NTCSA IM
Aletta Mashao	Senior Manager – PTM&C DX
Malcolm Van Harte	Senior Manager – DX Smart Grid and Network Operations COE
Ezzard de Lange	Senior Manager – DX Operational Technology and Cyber Security
Christoph Kohlmeyer	Senior Manager – GX Engineering (Acting)
Sithembile Songo	Senior Manager – IT Information Security
Tebogo Makhwelo	Senior Manager - IT Infrastructure Operations
Varsha Pillay	Senior Manager – IT Application Operations
Cornelius Naidoo	Middle Manager – Telecommunication and Physical Security T&S
Ernest Mpshe	Chairperson – Systems and Tools SC
Kholofelo Halefose	Chairperson – NTCSA Cybersecurity CG

5. Revisions

Date	Rev.	Compiler	Remarks
June 2024	1	B. Shezi	Document required for the procurement of a NTCSA OT SIEM solution

6. Development team

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

- Bongani Shezi
- Oscar Ngwenya
- Phelokazi Ndlovu
- Xabiso Dolonga
- David Thakadu
- Johan Botha
- Fefe Ngalonkulu
- Philla Kgole

REQUIREMENT SPECIFICATION FOR A NTCSA OPERATIONAL TECHNOLOGY (OT) SIEM SOLUTION

Unique Identifier: 240-185000083

Revision: 1

Page: 20 of 20

- Thomas Makhubela
- Mthuthuzeli Shibani
- Oscar Ngwenya
- Kholofelo Halefose
- Eric Mohlatlola
- Joel Mataboge
- Gideon Gqomfa
- Tshepiso Sekano

7. Acknowledgements

Jason Hector

Tjaart Visser

Elekanyani Mugivhi