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

Title: **Technical Evaluation Criteria for NTCSA OT SIEM Solution**

Document Identifier:	**240-185000177**
Alternative Reference Number:	**N/A**
Area of Applicability:	**National Transmission Company South Africa**
Functional Area:	**Engineering**
Revision:	**1**
Total Pages:	**33**
Next Review Date:	**N/A**
Disclosure Classification:	**Controlled Disclosure**

.

Compiled by	**Approved by**	**Authorized by**
Bongani Shezi	**Cornelius Naidoo**	**Judith Malinga**
Chief Engineer	**Middle Manager Telecoms and Physical Security T&S**	**Senior Manager PTM&C Engineering**
Date: 04 October 2024	Date: 9 October 2024	Date: 16/10/2024

Content

Page

Tables

1. Introduction

This document covers the technical evaluation criteria for the NTCSA OT SIEM Solution enquiry.

2. Supporting Clauses

2.1 Scope

2.1.1 Purpose

This document sets out the technical evaluation criteria to be used for evaluating submissions for the NTCSA OT SIEM Solution enquiry.

2.1.2 Applicability

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

2.1.3 Effective date

The effective date is the date of the authorising signature.

2.2 Normative/Informative References

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

2.2.1 Normative

[1] ISO 9001 Quality Management Systems

[2] 240-185000083 Requirements Specification for a NTCSA Operational Technology (OT) SIEM Solution

[3] 240-135089195 Generic Technical Requirements for Eskom Telecommunications Contracts

[4] 240-60725641 Specification for standard (19 inch) equipment cabinets

[5] 240-170001061 Transmission Cybersecurity Standard for Operational Technology

[6] 240-79669677 Demilitarized Zone Designs for Operational Technology

[7] 240-132190480 Telecommunications Equipment Installation Standard

2.2.2 Informative

[8] 240-48929482 Tender Engineering Evaluation Procedure

2.3 Definitions

Definition	Description
Enquiry	A collective and generic term for requests for information, expressions of interest, request for quotations, invitations to tender or requests, proposals made to the supplier, group of suppliers or market at large.
Submission	The tender in accordance with the requirements of the enquiry.
Technical evaluator	Technical experts nominated by the end-user and divisional technical functionaries with the necessary technical expertise.
Tender	A tender refers to a written competitive offer, quotation, and/or proposal made by the supplier in a prescribed or stipulated form in response to an invitation to tender/competitive enquire for provision of assets/goods or services and or the disposal thereof.

2.4 Abbreviations

Abbreviation	Explanation
CFT	Cross Functional Team
DES	Desktop Evaluation Score
OEM	Original Equipment Manufacturer
PRES	Product Risk Evaluation Score
TES	Technical Evaluation Score
TET	Technical Evaluation Team

2.5 Roles and Responsibilities

1) Procurement: Enquiry Process Owner

2) Technical Evaluation Team (TET) Member: The delegated engineers/technical specialists who are responsible to review and evaluate technical aspects of the tender documentation as per the Tender Technical Evaluation Strategy.

2.6 Process for Monitoring

Not applicable.

2.7 Related/Supporting Documents

Not applicable.

3. Technical Evaluation

Evaluations are performed to assess a supplier's capability to enter into a contract with Eskom. This report and any actions that are listed or recommended as a result of the assessments are by no means a confirmation or guarantee that any contract will be entered into with Eskom.

Any actions undertaken by a supplier, as a consequence of this report, are for the supplier's account. Any liability for the said actions undertaken by the supplier is not transferrable to Eskom, in any way.

The evaluation team has no authority or responsibility in the decision taken by Eskom with respect to contracting for a product, solution or service.

Any statements, intentions, and/or actions expressed by the evaluation team during and after the assessment shall not be interpreted as the awarding of a contract and does not constitute any liability to Eskom with regard to contract placement or post-contract performance guarantees.

3.1 Technical Evaluation Guideline

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

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

STEP 1: TET to assess the technical tender returnable for completeness as per section 3.2, if the technical submission is not complete, then it should be noted as such.

STEP 2: TET to evaluate the mandatory requirements as per section 3.3. Only submissions that meet the mandatory requirements will be evaluated further.

STEP 3: Assess the submission qualitatively using the Qualitative Evaluation Criteria as per Section 3.4. Each individual member of the TET shall evaluate the submission.

STEP 4: Consolidation of the individual TET member scores to come to a single Desktop Evaluation Score (DES) per submission. If the DES is less than 70%, then it should be noted as such and cannot be evaluated any further.

STEP 5: TET to assess the submission qualitatively using the Product Risk Evaluation Criteria as per Section 0. Each individual member of the TET shall evaluate the product during site visit/demonstration.

STEP 6: Consolidation of the individual TET member scores to come to a single Product Risk Evaluation Score (PRES) per submission.

STEP 7: The final Technical Evaluation Score (TES) is the average of the DES and the PRES per submission. Where no PRES is required, the TES will be the final score of the DES.

STEP 8: Technical Evaluation Report will recommend submissions with a TES of 70% or more.

3.2 Submission of Tender Returnable

The technical evaluation team (TET) will go through the returned submissions. The first level of evaluation will be to ensure that the following information has been received as per the table below:

Table 1: Submission of tender returnable

No.	Tender Returnable Document	Reference/Source	Purchaser's Requirement	Supplier's Statement (Submitted/Not Submitted)	Evaluator's Assessment (Submitted/Not Submitted)
1.	Supplier equipment tender declaration form	Appendix A of this document	To be completed and submitted.		
2.	Letter of accreditation from Original Equipment Manufacturer (OEM)	240-135089195 Generic Technical requirements for Telecoms Contracts (Section 3.2.3 only)	Signed and up-to-date letter to be submitted.		
3.	Technical proposal	a) 240-185000083 NTCSA Requirements for OT SIEM Solution b) 240-135089195 Generic Technical requirements for Telecoms Contracts	Written technical response to the requirements specified		
3.	Completed Appendix B – Compliance Schedules A&B for 240-185000083 NTCSA Requirements for OT SIEM Solution	Appendix B of this document	To be completed and submitted together with supporting documents/evidence.		
4.	Product roadmap	240-135089195 Generic Technical requirements for Telecoms Contracts (Section 3.2.7 only)	To be submitted.		
5.	A written acknowledgement of compliance with the following documents. Any clauses the tenderer fails to comply with shall be clearly stated in the "Schedule of Deviations and Exclusions".	a) 240-135089195 Generic Technical requirements for Telecoms Contracts b) 240-60725641 Specification for standard (19 inch) Equipment Cabinets c) 240-170001061 Transmission Cybersecurity Standard for Operational Technology d) 240-79669677 Demilitarized Zone Designs for Operational Technology e) 240-132190480 Telecommunications Equipment Installation Standard	Letter to be compiled, signed, dated and to be submitted.		

3.3 Mandatory Requirements

The technical evaluation team (TET) will go through the returned submissions. The first level of evaluation will be to ensure that the following information has been received as per the table below:

Table 2: Mandatory requirements

No.	Requirement	Reference/Source	Purchaser's Requirement	Supplier's Statement (Compliant/Not Compliant)	Supplier's Comment	Evaluator's Assessment (Compliant/Not Compliant)	Evaluator's Comment
1.	The system shall be on-premises AND be capable of running autonomously in a fully functional state without any communication to external servers or websites	Clause(s) 3.2.1 a & b of 240-185000083 NTCSA Requirements for OT SIEM Solution	Comply. Provide Evidence				

3.4 Qualitative Evaluation Criteria

Qualitative Evaluation Criteria are weighted evaluation criteria used to identify the highest technically ranked tenderer after all the Mandatory Evaluation Criteria have been met. The Qualitative Evaluation Criteria are weighted to reflect the relevant importance of each criterion.

The detailed evaluation scoring template is described in Appendix B of this document. Each of the clauses in Appendix B will be scored according to Table 2.

Table 3: Qualitative Scoring Definition

Score	(%)	Definition
5	100	**COMPLIANT** • Meet technical requirement(s) AND; • No foreseen technical risk(s) in meeting technical requirements
4	80	**COMPLIANT WITH ASSOCIATED QUALIFICATIONS** • Meet technical requirement(s) with; • Acceptable technical risk(s) AND/OR; • Acceptable exceptions AND/OR; • Acceptable conditions

Score	(%)	Definition
2	40	**NON-COMPLIANT** • Does not meet technical requirement(s) AND/OR; • Unacceptable technical risk(s) AND/OR; • Unacceptable exceptions AND/OR; • Unacceptable conditions.
0	0	**TOTALLY DEFICIENT OR NON-RESPONSIVE**

The weighting for the scoring is defined in Table 3. The QES will be the score obtain from Table 3.

Table 4: Section Weighting for Specification

Criteria	Weight (%)	Reference
Functional Requirements	60	Appendix B – Compliance Schedules A&B for 240-185000083 NTCSA Requirements for OT SIEM Solution
General Requirements	15	Appendix B – Compliance Schedules A&B for 240-185000083 NTCSA Requirements for OT SIEM Solution
Product Roadmap	5	240-135089195 Generic Technical requirements for Telecoms Contracts (Section 3.2.7 only)
Service Requirements	20	Appendix B – Compliance Schedules A&B for 240-185000083 NTCSA Requirements for OT SIEM Solution

Each TET members shall provide a scoring form detailing all allocated scores for each evaluated criteria for each tenderer. The individual TET member scores are combined to a single DES per submission. The required threshold is 70% for DES score.

3.5 Product Risk Evaluation Criteria

Only the suppliers that scored a DES of 70% or higher can be engaged with for this stage. This stage of the evaluation allows clarification on any risks that may have been identified in the qualitative evaluation.

NTCSA reserves the right not to perform factory or practical evaluations for bidders whose product(s) had passed technical evaluation in the immediate previous enquiry or are currently supplying the products. Such equipment will automatically be recommended for further commercial evaluation. For NTCSA to make this assessment, all suppliers are required to complete the supplier equipment tender declaration form in ***Appendix A – Supplier Equipment Tendered Declaration Form*** and attach all the necessary supporting documents.

Tenderers shall be advised of their qualification for the visit, and on the exact date of the visit within two weeks prior to the demonstration. A questionnaire based on the risks identified during the qualitative evaluation will be submitted to tenderers during this phase of the evaluation.

This evaluation may be in the form of a site visit to the supplier's designated site, or that of one of their customers, or at an Eskom site (where possible). There will be no factory evaluation in this enquiry.

During the demonstration, the tenderer will be required to demonstrate functionality/capability of their offering, this will be assessed according to **Appendix C – Product Risk Evaluation Form**. The tenderer shall also supply all equipment (including simulators) to successfully complete the demonstration items required. NTCSA shall not supply any equipment. In addition to the demonstration items, tenderers have the option to include a supplementary presentation on their proposed solution. The presentation shall not exceed 20 minutes.

The scoring definition for each functionality/capability demonstrated scoring table is described in Table 4.

Table 5: Product Risk Evaluation Scoring Definition

Score	(%)	Definition
5	100	**CAPABILITY DEMONSTRATED** • All technical risks raised at desktop evaluation were clarified and resolved AND; • No foreseen technical risk(s) in meeting technical requirements
4	80	**CAPABILITY DEMONSTRATED WITH ASSOCIATED QUALIFICATIONS** • Technical risks raised during desktop evaluation were clarified but not all were resolved AND; • Acceptable technical risk(s) AND/OR; • Acceptable exceptions AND/OR; • Acceptable conditions

Score	(%)	Definition
2	40	**CAPABILITY NOT DEMONSTRATED** • Technical risks raised during desktop evaluation were clarified AND; • Unacceptable technical risk(s) AND/OR; • Unacceptable exceptions AND/OR; • Unacceptable conditions.
0	0	**TOTALLY DEFICIENT OR NON-RESPONSIVE**

The weightings for each functionality/capability section demonstrated is described in Table 5.

Table 6: Section Weighting for Specification

Criteria	Weight (%)	Reference
1. Functional Requirements	60	Appendix C – Product Risk Evaluation Form
2. General Requirements	20	Appendix C – Product Risk Evaluation Form
3. Service Requirements	20	Appendix C – Product Risk Evaluation Form

The final PRES per submission will be the average of the individual PRESs.

3.6 Final Scores and Ranking

Technical Evaluation Score (TES) = Average (DES, PRES).

If no product risk evaluation was completed, then the TES = DES.

Submissions that obtain a final TES of 70% or higher will be recommended for further commercial evaluation.

4. Acceptance

This document has been seen and accepted by:

Name	Designation
Cornelius Naidoo	Middle Manager – Telecommunication and Physical Security T&S
Ernest Mpshe	Chairperson – Systems and Tools SC
Mervin Mottian	Middle Manager – IM Cybersecurity
Unathi Dyantyi	Middle Manager – Telecommunications NMC
Mfundiso Hina	Middle Manager – Telecommunications NPAE
Johan Botha	Senior Consultant – Energy Management (National Control)
Judith Malinga	Senior Manager – NTCSA PTM&C Engineering

5. Revisions

Date	Rev.	Compiler	Remarks
September 2024	1	B. Shezi	Document required for technical evaluation of the NTCSA OT SIEM Solution enquiry.

6. Development Team

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

- Bongani Shezi

7. Acknowledgements

None.

Appendix A – Supplier Equipment Tendered Declaration Form

NTCSA reserves the right not to perform factory or practical evaluations for bidders whose product(s) had passed technical evaluation in the immediate previous enquiry or are currently supplying the products. Such equipment will automatically be recommended for further commercial evaluation. For NTCSA to make this assessment, all suppliers are required to complete the declaration form below and attach all the necessary supporting documents. There will be no factory evaluation in this enquiry, functionality tests will be done at NTCSA.

Number	Question	Supplier commitment	Supplier general comments
1	Is all the offered equipment already implemented/installed in Eskom?		
2	Are the implemented/installed equipment the same as the offered equipment for this enquiry?		
2.1	If yes, provide a list of project names		
2.2	Approximately how many units are installed in Eskom?		
3	Was the offered equipment tested as part of the Eskom prequalification process? If yes, provide the Eskom Contract number and the year of testing.		
3.1	Were there any changes after testing the equipment?		
3.2	List the hardware changes after testing and the impact		
3.3	List the software changes after testing and the impact		
4	Are there any specific tests (routine and type) that you think you will not be compliant with, please list those test cases?		
5	Do you foresee any operational/functional risk(s) with signing a contract with Eskom before testing?		
6	Do you confirm that you will be able to supply and support the tendered equipment for the duration of the contract?		
Supplier name	Supplier representative	Supplier signature	
Division (if applicable)	Designation	Date	

Appendix B – Compliance Schedules A&B for 240-185000083 NTCSA Requirements for OT SIEM Solution

Name of Evaluator : _____

Date: : _____

Supplier : _____

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
3	SIEM Solution for NTCSA OT					
3.1	Functional Requirements					
3.1.1	Log Management	Comply. Provide Evidence				
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	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
f)	The solution shall offer capabilities to generate raw log data on behalf of other hosts.	Comply. Provide Evidence				
3.1.3	Correlation					

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
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.	Comply				
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. 3) The solution shall offer capabilities to modify and improve correlation rules on a need basis.	Comply. Provide Evidence				
3.1.4	Threat intelligence					
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.	Comply. Provide Evidence				
b)	The solution shall have threat intelligence capability essential for preventing an attack from occurring rather than reacting to the incident after it happens.	Comply				
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.	Comply. Provide Evidence				
d)	The solution shall utilize log correlation, threat intelligence, and anomalous user behaviour analytics to quickly recognize pattern deviations or unusual activity.	Comply				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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 AI 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, 5) 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.	Comply. Provide Evidence				
b)	MITRE ATT&CK Integration. The solution must be able to align its threat detection indicators to the MITRE ATT&CK framework.	Comply. Provide Evidence				

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
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.	Comply. Provide Evidence				
3.1.6	Threat alerting, contextualization, and response					
a)	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. 2) Alert notification shall be categorized based on priorities assigned to them, e.g., high, medium, or low 3) The severity and urgency/priority of the alert notification shall be customizable to align with business needs.	Comply. Provide Evidence				
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.	Comply				
c)	The solution shall provide threat contextualization functions. Contextualization should assist in: 1) 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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply				
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.	Comply. Provide Evidence				
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 2) 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	Comply. Provide Evidence				
b)	The solution should offer batch analytics to identify and correlate weak signals in data not detected in real time.	Comply. Provide Evidence				
c)	The solution should have forensic capabilities. As a minimum, the ability to: 1) Perform full packet captures for a network connection associated with malicious activity. 2) 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. 3) 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.	Comply. Provide Evidence				

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
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.	Comply				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
c)	The solution shall offer highly customizable reporting capabilities. The content of the reports shall be configurable and flexible.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
e)	It shall be possible to send notifications via email via an SMTP server.	Comply. Provide Evidence				
f)	Notification shall support a variety of flexible notification triggers such as detected events, failed console login attempts, exceeding of performance thresholds, etc.	Comply. Provide Evidence				
3.2	General Requirements					
a)	This solution shall be off-the-shelf, and no specific development should be necessary.	Comply				
b)	NTCSA's OT environments require a SIEM solution on three critical systems. Monitoring shall primarily be performed locally by the respective OT environment.	Comply				
3.2.1	Location					
a)	The system shall be on-premises without any communication to external servers or websites.	Comply. Provide Evidence				
b)	The system shall be capable of running autonomously and in a fully functional state.	Comply. Provide Evidence				

<table>
<tr><th>Number</th><th>Description</th><th>Schedule A (Purchaser's compliance statement)</th><th>Schedule B (Supplier's compliance statement)</th><th>Reference (Page X of File Y, Section Z)</th><th>Score</th><th>Comments</th></tr>
<tr><td>3.2.2</td><td>Communication between System Components</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>a)</td><td>Dataflow shall be uni-directional from client devices to master consoles only, unless the system functionality calls for otherwise explicitly.</td><td>Comply</td><td></td><td></td><td></td><td></td></tr>
<tr><td>b)</td><td>Client devices and master station consoles shall use a fixed port for the network connection to allow strict firewall rules to be set.</td><td>Comply</td><td></td><td></td><td></td><td></td></tr>
<tr><td>c)</td><td>Communication between master consoles and client devices shall be encrypted</td><td>Comply</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3.2.3</td><td>Availability</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>a)</td><td>The system shall have a 99.95% availability without any redundancy design translating to 21.92 minutes of downtime per month.</td><td>Comply</td><td></td><td></td><td></td><td></td></tr>
<tr><td>b)</td><td>Failed agents, probes, services or processes shall have auto-restart capability rendering an autonomous function across all components.</td><td>Comply. Provide Evidence</td><td></td><td></td><td></td><td></td></tr>
<tr><td>c)</td><td>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
<table>
<tr><th>Heading</th><th>OT System 1</th><th>OT System 2</th><th>OT System 3</th></tr>
<tr><td>High Availability</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td>Disaster Recovery</td><td>Active- active, full continuous availability, preferred
Active- hot standby, acceptable</td><td>Active- active, full continuous availability, preferred
Active- hot standby, acceptable</td><td>Active- standby (cold)</td></tr>
<tr><td>Recovery Time Objective (RPO), acceptable system loss time</td><td>0-1 hour, preferred
8-24 hours, acceptable</td><td>0-2 hour, preferred
8-24 hours, acceptable</td><td>>72 hours</td></tr>
<tr><td>Recovery Point Objective (RPO)</td><td>No data loss</td><td>No data loss</td><td>>24 hours</td></tr>
</table></td><td>Comply. Provide Evidence</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3.2.4</td><td>Sanitisation</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>a)</td><td>The solution shall enable the Purchaser's personnel to perform the required sanitization procedures.</td><td>Comply</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3.2.5</td><td>Backup and Recovery</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>a)</td><td>The solution shall have a mechanism that allows the automation of system backups.</td><td>Comply. Provide Evidence</td><td></td><td></td><td></td><td></td></tr>
<tr><td>b)</td><td>The solution shall allow for backups to be kept on long-term storage on offsite locations.</td><td>Comply. Provide Evidence</td><td></td><td></td><td></td><td></td></tr>
</table>

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
c)	The solution shall have a mechanism that allows the for the restoration from system backups.	Comply. Provide Evidence				
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. .	Comply. Provide Evidence				
b)	The solution's storage shall be scalable, without impacting on performance.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
d)	The period for which this data can be kept for shall be configurable.	Comply. Provide Evidence				
e)	Export mechanisms to long-term storage shall be supported. Supported export formats shall be of are to be specified.	Comply. Provide Evidence				
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	Comply. Provide Evidence				
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: 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). .	Comply. Provide Evidence				
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, 3) Reporting, 4) User roles and access control, along with technical integration and 5) Response workflows.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
d)	Product usability. The solution shall provide easy-to-understand and user-friendly interfaces featuring intuitive designs to better facilitate user engagement.	Comply				
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	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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).	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
b)	Both local authentication (for fall-back authentication method only) and remote authentication shall be provided.	Comply. Provide Evidence				
c)	For remote authentication, integration to TACACS, active directory (AD) and/or Lightweight Directory Access Protocol (LDAP) shall be supported.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
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.	Comply. Provide Evidence				
f)	Role creation and removal (by the administrator) shall be provided.	Comply. Provide Evidence				
g)	Multiple users per role shall be allowed.	Comply. Provide Evidence				
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.	Comply				
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).	Comply				
3.3.2	Installation, Configuration and Commissioning					

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
a)	The supplier shall install, configure and commission the solution.	Comply				
b)	The supplier shall obtain the required clearances for access to the Purchaser's premises.	Comply				
c)	The supplier shall provide the installation test plan and acceptance test procedure for review and acceptance by the Purchaser.	Comply. Provide Evidence				
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).	Comply. Provide Evidence				
3.3.4	Training					
a)	The supplier shall provide training on the system to be held in RSA.	Comply				
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.	Comply. Provide Evidence				
c)	Training interventions shall occur just prior to the initial installation, configuration and commissioning of the system.	Comply				
d)	All material used for training shall be available online on the system.	Comply				
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.	Comply				
f)	The supplier shall provide a list of all courses offered, brief course descriptions and syllabi.	Comply. Provide Evidence				
3.3.5	Monitoring					
a)	This service shall be "as and when required" defined by the Purchaser.	Comply				
b)	Monitoring of the system shall be provided by the Supplier.	Comply				
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).	Comply				
3.3.6	Threat Investigations and Analysis					
a)	This service shall be "as and when required" defined by the Purchaser.	Comply				
b)	Threat investigations shall be provided by the Supplier after a threat has been detected and verified.	Comply				
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".	Comply				
3.3.7	Augment Incident Response					

Number	Description	Schedule A (Purchaser's compliance statement)	Schedule B (Supplier's compliance statement)	Reference (Page X of File Y, Section Z)	Score	Comments
a)	This service shall be "as and when required" defined by the Purchaser.	Comply				
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	Comply				

Appendix C – Product Risk Evaluation Form

Name of Evaluator : _____

Date: : _____

Supplier : _____

Table 1: Section Weighting for Specification

Criteria	Weight (%)	Score	Requirements/Objectives
1. Functional Requirements	**60**		
1.1.Log Management	2		Demonstrate the collection and storage of log data generated from various sources such as servers, databases, networks, and applications. Demonstrate normalisation and parsing (transforming data into a consistent format) Demonstrate log retention and compliance consideration for security investigations and audits

Criteria	Weight (%)	Score	Requirements/Objectives
1.2. Monitoring, Logging and Tracking	8		a) Real time ingestion. The solution shall have the ability to ingest logs in real or near real-time and allow for instant searching. 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 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.
1.3. Correlation	5		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.

Criteria	Weight (%)	Score	Requirements/Objectives
1.4. Threat Intelligence	10		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.
1.5. User and Entity Behaviour Analysis	10		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. 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.

Criteria	Weight (%)	Score	Requirements/Objectives
1.6. Threat Alerting, Contextualization, and Response	5		a) The solution shall support automated notifications and security alerts providing real-time updates on any detected threats. 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 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.
1.7. Analytics	10		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. 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. 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. 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.

Criteria	Weight (%)	Score	Requirements/Objectives
1.8. Dashboards	5		a) Demonstrate 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. b) Demonstrate the capability to create and customize their own dashboards.
1.9. Reporting and Notifications	5		a) Demonstrate 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.
2. General Requirements	**20**		
2.1. Location	N/A – mandatory requirement		a) 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.

Criteria	Weight (%)	Score	Requirements/Objectives
2.2. Communication between System Components	2.5		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 port for the network connection to allow strict firewall rules to be set. c) Communication between master consoles and client devices shall be encrypted.
2.3. Availability	2.5		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. 4) Demonstrate High Availability and Disaster Recovery: Modes: Active-Active, Active- (hot) Standby, Active – (cold) Standby Demonstrate RTO (hours) and RPO (hours)
2.4. Sanitisation	2.5		a) The solution shall enable the Purchaser's personnel to perform the required sanitization procedures.
2.5. Backup and Recovery	2.5		a) Demonstrate mechanisms that allows the automation of system backups. b) Demonstrate for backups to be kept on long-term storage on offsite locations. c) Demonstrate mechanisms that allow for the restoration from system backups.

Criteria	Weight (%)	Score	Requirements/Objectives
2.6. Data Retention Strategy	2.5		a) Demonstrate the capacity/capability for: 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) Demonstrate the scalability of the solution's storage. c) Demonstrate historic alarms and alerts and aggregated data from which the alarms were derived in order to assist with forensic investigations. d) Demonstrate the configurability of the period for which data can be kept on the solution. e) Demonstrate export and archiving mechanisms to long-term storage and supported export formats. Exporting and archiving of data to the following: 1) local storage 2) network storage 3) email recipients

Criteria	Weight (%)	Score	Requirements/Objectives
2.7. Monitoring, Operation and Administration	2.5		a) Demonstrate 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 functions shall include the following: 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). b) Demonstrate tools to administer, maintain and support complex functions, such as: 1) Log and data source management 2) Analytics and detection content, 3) Reporting, 4) User roles and access control, along with technical integration and 5) Response workflows. c) Demonstrate natively available content management. Data collectors, parsers, analytics rules and models, compliance packages, actions and plays. Administrators can enable, access and update this content through an included management framework. d) Demonstrate product usability. Easy-to-understand and user-friendly interfaces featuring intuitive designs. e) Demonstrate use cases. Predefined and common use cases ready to use. The use cases should also focus on performance and resource utilization for priority issues. Capability to allow for custom use cases to be written and deployed.

Criteria	Weight (%)	Score	Requirements/Objectives
2.8. Integration	2.5		a) Integration with all relevant applications, data sources and technologies shall be demonstrated. The natively supported plug-ins, third-party apps and other software shall be specified. b) 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. Data enrichment shall be demonstrated. c) The capability to forward critical alerts and information from the solution to other enterprise systems such as a SIEM or SOAR or Security Operations Centre (SOC) shall be demonstrated.
2.9. Access Control	2.5		a) Role based access (per role, per user) shall be demonstrated. b) Both local authentication (for fall-back authentication method only) and remote authentication shall be demonstrated. c) For remote authentication, integration to TACACS, active directory (AD) and/or Lightweight Directory Access Protocol (LDAP) shall be demonstrated. 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. Service Requirements	**20**		

Criteria	Weight (%)	Score	Requirements/Objectives
3.1. Support and Maintenance	4		The supplier shall demonstrate the capability to provide an annual maintenance to keep the system up to date including any 3rd line of support that may be required. This 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).
3.2. Training	10		The supplier shall demonstrate the capability to 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. 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.
3.3. Monitoring	2		The option for the Supplier to provide the monitoring as a service shall be demonstrated as follows: 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).

Criteria	Weight (%)	Score	Requirements/Objectives
3.4. Threat Investigations and Analysis	2		The option for the Supplier to provide the threat investigation and analysis as a service shall be demonstrated as follows: 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”.
3.5. Augment Incident Response	2		The option for the Supplier to provide augmented services around incident management and response shall be demonstrated 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