TITLE	**STANDARD FOR ICT CYBER SECURITY ENHANCEMENT – NDR SOLUTION**	REFERENCE **CP_TSSTAN_156**	REV **1**
		DATE:	**JULY 2026**
		PAGE: **1**	OF **27**

COMPILED BY	FUNCTIONAL RESP	SUPPORTED BY	SUPPORTED BY
APPROVED BY	AUTHORIZED BY		

TABLE OF CONTENTS

FOREWORD

This Request for Standard Services was prepared by the following Work Group member/s:

The work group was appointed by ICT Leadership, which at the time of approval comprised of the following members:

Mphethe Andries Mokoakoe	Information Communication Technology

The work group was appointed by the ICT Planning Committee, which at the time of approval comprised of the following members:

Humbulani Manyaga	Information Communication Technology
Ushailen Naicker	Information Communication Technology
Khathu Muambadzi	Information Communication Technology

Recommendations for corrections, additions or deletions should be addressed to the:

Research and Development General Manager
City Power Johannesburg SOC Ltd
P O Box 38766
Booysens
2016

INTRODUCTION

The threat landscape is increasingly dynamic, with advanced cyber threats emerging continuously. To proactively detect, analyse, and respond to these threats, City Power requires an intelligent network detection and cyber threat-hunting capability that leverages advanced analytics, automation, and machine-learning techniques. Such a solution is essential for identifying malicious activity, reducing exposure, and strengthening the overall security posture of the ICT environment.

City Power requires this capability to be delivered as a complete turnkey solution. The appointed Service Provider shall be responsible for the end-to-end delivery of the solution, including the pre-deployment assessment, solution design, supply of all hardware, software and licensing, installation, configuration, integration with the existing ICT and security environment, testing, commissioning, documentation, training, knowledge transfer, and ongoing support and maintenance for the duration of the contract. City Power shall take receipt of a fully operational, tested and supported solution and shall not be required to source, integrate or commission any component of the solution separately.

1. SCOPE OF WORK

City Power requires the appointment of a suitably qualified and experienced ICT Security Services Partner to design, supply, implement, and support an advanced Network Detection and Response (NDR) solution.

The solution shall be procured, delivered and implemented on a turnkey basis. The appointed Service Provider shall carry single-point accountability for the complete solution, and the price offered shall be all-inclusive of every item, service and activity necessary to place the solution into full production use, whether or not each such item is expressly listed in this specification.

The scope of work includes, but is not limited to, the following:

1.1 Solution Acquisition and Implementation

1.1.1 Supply and implementation of an intelligent ICT security solution capable of proactively detecting, analysing, and responding to cyber threats across the network environment.

1.1.1 Ensure the solution incorporates advanced analytics, artificial intelligence (AI), and machine-learning capabilities to identify malicious activity, information leakage, and potential attack vectors.

1.2 Threat Detection and Hunting

1.2.1 Implement systems that continuously analyse network events and security logs to detect anomalous and malicious behaviour.

1.2.2 Provide cyber threat-hunting capabilities that enable proactive identification, investigation, mitigation, and remediation of security threats.

1.3 Prevention of Cyber Incidents

1.3.1 Ensure the implemented solution effectively prevents malicious attacks, data breaches, and business disruptions resulting from cyber-attacks.

1.3.2 Strengthen City Power’s overall ICT security posture and resilience against evolving cyber threats.

1.4 Licensing, Support, and Maintenance

1.4.1 Provide all required software licensing for the duration of the contract.

1.4.2 Deliver ongoing technical support, maintenance, updates, and patches to ensure optimal system performance and security effectiveness.

1.5 Secure Operational Environment

1.5.1 Ensure the solution operates within a secure and compliant environment, aligned with City Power's ICT security policies and best-practice standards.

1.6 Pre-Deployment Assessment

1.6.1 Conduct a mandatory pre-deployment assessment of the City Power ICT and operational technology environment prior to finalising the solution design, sizing, licensing and implementation plan.

1.6.2 Produce and present a Pre-Assessment Report covering the technical readiness of the environment for deployment, an analysis of the user accounts that actively log on to the environment, an inventory of the machines and devices connected to the environment, and a history of the attacks experienced by City Power together with their associated types.

1.7 Turnkey Delivery, Commissioning and Handover

1.7.1 Deliver, install, configure, integrate, test, commission and hand over a fully operational solution as a single, complete package under one point of accountability.

1.7.2 Provide all hardware, software, licences, subscriptions, connectors, cabling, mounting and ancillary infrastructure required for the solution to operate at the required capacity, including items not expressly listed but necessary for full functionality.

1.7.3 Provide as-built documentation, operational run-books and formal acceptance testing prior to handover.

2. NORMATIVE REFERENCES

The following documents contain provisions that, through reference in the text, constitute requirements of this specification. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

COBIT: *Control Objectives for Information and Related Technology. It is a framework created by the ISACA (Information Systems Audit and Control Association) for IT governance and management*

KING IV: *Technology and Information Governance*

TOGAF: *The Open Group Architecture Framework is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture.*

POPI Act: *Protection of Personal Information Act, 2013*

GWEA: *Government-Wide Enterprise Architecture framework*

ISO/IEC 27001:2022: *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

ISO/IEC 27002:2022: *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27035: *Information technology — Information security incident management*

MITRE ATT&CK: *Globally accessible knowledge base of adversary tactics and techniques based on real-world observations, incorporating both the Enterprise and ICS matrices*

NIST CSF: *National Institute of Standards and Technology Cybersecurity Framework*

3. DEFINITIONS

The definitions and abbreviations in the above document (Normative Reference) shall apply to this specification. In addition, the following terms and acronyms are used in this document:

TERM	MEANING
ICT	Information and Communication Technology
SLA	Service Level Agreement
IT	Information Technology
DR	Disaster Recovery
IPS	Intrusion Prevention System
NDR	Network Detection and Response
SOC	Security Operations Centre
SIEM	Security Information and Event Management
NAC	Network Admission Control
NGFW	Next-Generation Firewall
AES	Advanced Encryption Standard
IPsec	Internet Protocol Security
CMDB	Configuration Management Database
VPN	Virtual Private Network
IoT	Internet of Things
OT	Operational Technology
API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge (MITRE framework)
AWS	Amazon Web Services
BOM	Bill of Materials
C2	Command and Control
DNS	Domain Name System
DPI	Deep Packet Inspection
eBPF	Extended Berkeley Packet Filter
EDR	Endpoint Detection and Response
HTTP/S	Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure
IOC	Indicator of Compromise
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond

TERM	MEANING
NetFlow	Network flow record protocol used to collect IP traffic information
PCAP	Packet Capture
POPIA	Protection of Personal Information Act, 2013
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
SaaS	Software as a Service
SOAR	Security Orchestration, Automation and Response
SPAN	Switched Port Analyser (port mirroring)
TAP	Test Access Point
TLS	Transport Layer Security
UEBA	User and Entity Behaviour Analytics
VM	Virtual Machine
VPC	Virtual Private Cloud
XDR	Extended Detection and Response

4. REQUIREMENTS

4.1 General Requirements

The following requirements shall be considered in the proposal to strengthen City Power security:

4.1.1 Network Detection and Response (NDR) solution

4.1.2 Turnkey delivery of the NDR solution, inclusive of all hardware, software, licensing, integration, commissioning, documentation, training and support.

4.1.3 A mandatory pre-deployment assessment of the City Power environment, as set out in the Pre-Deployment Assessment section of this specification.

4.1.4 Full compliance with the Functional Requirements and the Technical Requirements set out below.

4.2 Functional Requirements

The functional requirements set out below describe what the solution shall do in operational use. The Service Provider shall indicate compliance with each requirement as Fully Compliant, Partially Compliant or Not Compliant, and shall substantiate every response. Failure to meet a mandatory requirement may render a bid non-responsive.

4.2.1 Turnkey Solution Delivery

4.2.1.1 The solution shall be delivered as a complete turnkey solution, with the Service Provider accountable for design, supply, delivery, installation, configuration, integration, testing, commissioning, documentation, training, handover and support.

4.2.1.2 The Service Provider shall supply all hardware, software, licences, subscriptions, connectors and ancillary components required for the solution to operate at the required capacity.

4.2.1.3 The Service Provider shall provide all professional services required to place the solution into full production use, including project management, design workshops, migration and cut-over.

4.2.1.4 Any item not expressly listed in this specification but reasonably necessary for the correct and complete functioning of the solution shall be deemed to be included in the Service Provider's offer.

4.2.1.5 The Service Provider shall provide a documented implementation plan with milestones, deliverables, dependencies, resource allocations and acceptance criteria.

4.2.1.6 Formal acceptance testing shall be conducted against agreed criteria and signed off by City Power before the solution is regarded as commissioned.

4.2.2 Network Visibility and Monitoring

4.2.2.1 The solution shall continuously monitor and analyse both north-south and east-west traffic across the corporate, data centre, cloud and operational technology environments.

4.2.2.2 The solution shall provide continuous, passive monitoring that does not degrade network performance, latency or availability.

4.2.2.3 The solution shall automatically discover, classify and profile all devices communicating on the monitored networks, including unmanaged, IoT and OT devices.

4.2.2.4 The solution shall maintain an up-to-date inventory of monitored assets, exportable and reconcilable against the City Power CMDB and asset register.

4.2.2.5 The solution shall present real-time and historical views of network communications, including peer relationships, protocols, volumes, directions and session detail.

4.2.2.6 The solution shall identify and report on blind spots where traffic is not being observed.

4.2.3 Threat Detection

4.2.3.1 The solution shall detect known and unknown threats, including malware, ransomware, command-and-control activity, data exfiltration, insider threats and zero-day attacks.

4.2.3.2 The solution shall detect reconnaissance, credential abuse, privilege escalation and lateral movement between hosts, segments, sites and zones.

4.2.3.3 The solution shall detect anomalous behaviour relative to learned baselines for users, devices and network segments.

4.2.3.4 The solution shall detect policy violations and unauthorised services, protocols, connections and shadow IT.

4.2.3.5 The solution shall assign a risk score and severity to every detection, with the underlying rationale exposed to the analyst.

4.2.3.6 The solution shall detect threats crossing the IT and OT boundary and shall raise these with appropriate priority.

4.2.4 Threat Hunting and Investigation

4.2.4.1 The solution shall enable analysts to proactively hunt for threats using flexible queries across live and historical data.

4.2.4.2 The solution shall provide retrospective search across retained metadata and packet data for the full retention period.

4.2.4.3 The solution shall reconstruct the full sequence of events for an incident, including source, destination, protocol, timing and payload evidence where captured.

4.2.4.4 The solution shall support pivoting between entities such as host, user, IP address, domain, file hash and session within a single investigation workflow.

4.2.4.5 The solution shall allow hunting hypotheses and queries to be saved, shared and converted into custom detections.

4.2.4.6 The solution shall provide guided investigation workflows to support analysts of varying experience levels.

4.2.5 Alerting, Triage and Case Management

4.2.5.1 The solution shall generate prioritised, deduplicated and correlated alerts, grouping related detections into a single incident.

4.2.5.2 The solution shall provide a case management capability enabling incidents to be created, assigned, tracked, escalated, annotated and closed with disposition codes.

4.2.5.3 The solution shall maintain a complete, tamper-evident audit trail of all analyst actions taken on a case.

4.2.5.4 The solution shall support configurable notification by email and SMS and through integration with City Power's service management and collaboration platforms.

4.2.5.5 The solution shall track and report incident lifecycle metrics, including mean time to detect and mean time to respond.

4.2.6 Response and Containment

4.2.6.1 The solution shall support both automated and analyst-initiated response actions, including host isolation, session termination, blocking and quarantine, through integration with NGFW, NAC, EDR and directory services.

4.2.6.2 The solution shall allow response playbooks to be configured, tested and executed, with approval gates where required.

4.2.6.3 The solution shall ensure that no automated response action is applied to operational technology or critical operational systems without explicit prior authorisation by City Power.

4.2.6.4 The solution shall log every response action taken, whether automated or manual, together with the initiating rule or user and the outcome.

4.2.6.5 The solution shall support safe roll-back of response actions where a detection is subsequently found to be a false positive.

4.2.7 Reporting and Dashboards

4.2.7.1 The solution shall provide role-based dashboards suitable for executives, ICT management, SOC analysts and auditors.

4.2.7.2 The solution shall provide scheduled and on-demand reporting in at least PDF, CSV and Excel formats.

4.2.7.3 The solution shall provide standard reports covering threat activity, incident trends, asset risk, detection coverage and compliance posture.

4.2.7.4 The solution shall allow custom reports and dashboards to be built and modified by City Power without vendor intervention or additional cost.

4.2.8 Administration and Access Control

4.2.8.1 The solution shall provide role-based access control with granular permissions, integrated with City Power's directory service.

4.2.8.2 The solution shall enforce multi-factor authentication for all administrative and analyst access.

4.2.8.3 The solution shall maintain a complete audit log of all configuration changes, logons and data access within the solution.

4.2.8.4 The solution shall support configuration backup and restore, and disaster recovery of the solution itself.

4.2.9 Availability, Data Handling and Retention

4.2.9.1 The solution shall retain detection metadata and incident records for a minimum of twelve (12) months, and packet or metadata evidence in accordance with the retention requirements of this specification.

4.2.9.2 The solution shall ensure that all data collected, processed and stored is handled in accordance with POPIA and City Power's information security policies.

4.2.9.3 The solution shall provide high availability for all critical components, with no single point of failure.

4.2.9.4 The solution shall support secure export of evidence in standard formats suitable for forensic and legal use, preserving chain-of-custody integrity.

4.2.10 Knowledge Transfer and Operational Handover

4.2.10.1 The Service Provider shall provide a documented operational handover, including run-books, standard operating procedures and an escalation matrix.

4.2.10.2 The Service Provider shall ensure that City Power personnel are able to independently operate, tune and administer the solution on completion of handover.

4.2.10.3 The Service Provider shall provide as-built documentation accurately reflecting the deployed configuration.

4.3 Technical requirements

4.3.1 Network Detection and Response (NDR) solution

A security solution that analyses raw network traffic, flow records, and metadata using AI and behavioural analytics to detect, investigate, and respond to malicious activity. They provide comprehensive visibility into both north-south and east-west traffic, allowing security teams to identify threats that bypass traditional perimeter defences.

Key Components and Capabilities

4.3.1.1 Behavioural Analysis & AI: Identifies anomalies in normal network patterns, including insider threats and zero-day attacks.

4.3.1.2 Traffic Analysis: Monitors network traffic, focusing on metadata to analyse encrypted traffic without decryption.

4.3.1.3 Rapid Response: Automates security actions to stop threats in real-time.

4.3.2 Data Collection Layer

The Service Provider shall deliver a data collection layer that provides complete, continuous and non-disruptive visibility of all monitored environments.

4.3.2.1 Traffic Visibility

4.3.2.1.1 The solution shall collect traffic from SPAN or mirror ports on all core and distribution switches, and from network TAPs at critical aggregation points, data centre interconnects and the internet edge.

4.3.2.1.2 The solution shall collect cloud workload traffic, including through virtual private cloud (VPC) traffic mirroring for cloud-hosted environments.

4.3.2.1.3 The solution shall ingest flow logs from Microsoft Azure (NSG and VNet flow logs) and Amazon Web Services (VPC flow logs), together with NetFlow, sFlow, IPFIX and J-Flow records from network devices.

4.3.2.1.4 The solution shall collect host-level telemetry from servers using eBPF-based sensors, or equivalent kernel-level agents, providing process-to-connection attribution on Linux, with equivalent supported sensors for Windows servers.

4.3.2.1.5 The solution shall collect traffic from remote sites, VPN concentrators and remote access gateways.

4.3.2.1.6 The solution shall collect operational technology and substation network traffic passively and without any impact on operational systems.

4.3.2.1.7 The solution shall provide visibility of east-west traffic between virtual machines within hypervisor environments.

4.3.2.1.8 The Service Provider shall confirm all required collection points during the pre-deployment assessment and shall specify any additional aggregation, packet broker or optical infrastructure required.

4.3.2.2 Packet Capture and Retention

4.3.2.2.1 The solution shall support full packet capture (PCAP) at monitored collection points or, as a minimum, full protocol metadata extraction where full PCAP is not practicable.

4.3.2.2.2 Where full PCAP is provided, capture shall be continuous and shall additionally be triggerable on detection to capture extended context around an event.

4.3.2.2.3 Packet or metadata retention shall be a minimum of thirty (30) days, and the solution shall be sized and licensed to support a target retention of ninety (90) days.

4.3.2.2.4 Enriched metadata and detection records shall be retained for a minimum of twelve (12) months to support trend analysis and compliance reporting.

4.3.2.2.5 Retained data shall remain searchable and retrievable for the full retention period without restoration delays that would impede an investigation.

4.3.2.2.6 The Service Provider shall state the storage volumes, storage type, and any compression or roll-off behaviour on which the stated retention periods are based.

4.3.2.2.7 Storage shall be expandable to extend retention without replacement of the deployed platform, and the incremental cost shall be stated.

4.3.2.2.8 Captured data shall be encrypted at rest, and all access to it shall be restricted by role and logged.

4.3.2.3 Protocol Support

4.3.2.3.1 The solution shall decode and extract metadata from information technology protocols, including DNS, HTTP, HTTPS/TLS, SMB/CIFS, LDAP and LDAPS, Kerberos, RDP, SSH, FTP and SFTP, SMTP, IMAP, POP3, NTP, DHCP, SNMP, ICMP, SIP and common database protocols.

4.3.2.3.2 Directory, authentication and remote access protocols shall be parsed to the level required to establish user, host and session context.

4.3.2.3.3 The solution shall decode operational technology and industrial protocols, including Modbus/TCP, DNP3, IEC 60870-5-104, IEC 61850 (MMS, GOOSE and Sampled Values) and OPC UA/DA, together with any other protocols in use in the City Power operational environment.

4.3.2.3.4 Application-layer decoding and metadata extraction shall be provided, rather than port-based classification alone.

4.3.2.3.5 Tunnelled and encapsulated traffic, including GRE, VXLAN, MPLS, IPsec and QinQ, shall be decapsulated and analysed.

4.3.2.3.6 The Service Provider shall provide a full list of supported protocols and decoders, and shall state the process, timeframe and cost, if any, for adding support for protocols not currently supported.

4.3.2.4 Encrypted Traffic Analysis

4.3.2.4.1 The solution shall analyse encrypted traffic without requiring decryption, using metadata, certificate and handshake analysis and fingerprinting techniques such as JA3, JA3S and JA4.

4.3.2.4.2 Detect malicious or anomalous use of encryption, including self-signed and expired certificates, weak cipher suites, deprecated TLS versions, domain fronting, encrypted command-and-control channels and covert tunnelling.

4.3.2.4.3 Where decryption is required, the solution shall integrate with existing decryption or TLS inspection infrastructure rather than mandating a proprietary approach.

4.3.2.4.4 Any decryption capability shall be selectively applicable by policy and shall be capable of excluding categories of traffic protected under POPIA or City Power policy.

4.3.2.4.5 Detection efficacy on encrypted traffic shall be demonstrated during the proof of concept or acceptance testing.

4.3.3 Detection Engine

The detection engine shall combine multiple, complementary detection methods so that the solution is not dependent on any single technique.

4.3.3.1 Artificial Intelligence and Machine Learning Anomaly Detection

4.3.3.1.1 The solution shall establish and continuously maintain behavioural baselines for every user, device, application and network segment.

4.3.3.1.2 The solution shall detect statistically significant deviations from baseline without reliance on signatures.

4.3.3.1.3 Models shall self-tune as the environment changes, and the Service Provider shall state the required learning period before the solution reaches full effectiveness.

4.3.3.1.4 Detections shall be explainable, with the analyst able to see which features and observations drove the score.

4.3.3.1.5 The Service Provider shall confirm whether models are trained locally, in the cloud or both, and shall confirm that no City Power data is transferred outside the Republic of South Africa without prior written authorisation.

4.3.3.2 Threat Intelligence Feeds

4.3.3.2.1 The solution shall ingest commercial, open-source, government and sector-specific (including electricity utility sector) threat intelligence, as well as City Power-specific indicators.

4.3.3.2.2 The solution shall support STIX and TAXII, MISP and custom feed formats, together with manual indicator upload.

4.3.3.2.3 The solution shall automatically match live and historical traffic against indicators of compromise, including retrospective matching of newly received indicators against retained data.

4.3.3.2.4 Threat intelligence updates shall be delivered continuously and at no additional cost for the duration of the contract.

4.3.3.2.5 The solution shall support intelligence confidence scoring, ageing and suppression of low-quality indicators to limit noise.

4.3.3.3 Signature and Rule Engine

4.3.3.3.1 The solution shall provide a vendor-maintained signature and rule set that is updated continuously for the duration of the contract.

4.3.3.3.2 The solution shall support industry-standard rule formats, such as Suricata or Snort, YARA and Sigma, and allow City Power to author, import, test and deploy custom rules at no additional cost.

4.3.3.3.3 The solution shall provide rule versioning, staged roll-out, testing against historical data, and roll-back.

4.3.3.3.4 Signature and rule updates shall not require an outage or result in any reduction of monitoring coverage.

4.3.3.4 MITRE ATT&CK Mapping

4.3.3.4.1 Every detection shall be mapped to the relevant MITRE ATT&CK tactic or tactics and technique or techniques, including sub-techniques.

4.3.3.4.2 Both ATT&CK for Enterprise and ATT&CK for ICS shall be supported, in view of the City Power operational technology environment.

4.3.3.4.3 The solution shall provide an ATT&CK coverage heat map indicating which techniques are covered, partially covered or not covered by the deployed configuration.

4.3.3.4.4 Incidents shall present the observed attack chain mapped to the corresponding ATT&CK stages.

4.3.3.4.5 ATT&CK mappings shall be maintained current with successive releases of the framework.

4.3.3.5 Behavioural Analytics

4.3.3.5.1 The solution shall provide user and entity behaviour analytics across users, devices, service accounts and applications.

4.3.3.5.2 The solution shall detect abnormal authentication, access, data movement, timing and volume patterns.

4.3.3.5.3 The solution shall detect insider threat indicators, including unusual data staging, mass file access and off-hours activity.

4.3.3.5.4 The solution shall support peer group analysis and cumulative risk scoring that aggregates related low-severity events into a meaningful signal.

4.3.3.5.5 The solution shall correlate identity context from directory services so that activity is attributed to a user and not only to an IP address.

4.3.3.6 Lateral Movement Detection

4.3.3.6.1 The solution shall detect lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, golden and silver ticket use, remote service creation, WMI and PsExec-style remote execution, RDP and SSH chaining, SMB administrative share access and living-off-the-land activity.

4.3.3.6.2 The solution shall detect internal reconnaissance and scanning, including port, service, share and directory enumeration.

4.3.3.6.3 The solution shall detect east-west movement across VLANs, segments and sites, and specifically across the IT and OT boundary, flagging any traffic that crosses a segmentation boundary in violation of policy.

4.3.3.6.4 The solution shall visualise the lateral movement path across hosts and accounts on a timeline, showing the chain from initial foothold to current position.

4.3.3.6.5 The solution shall detect anomalous use of administrative and service accounts across multiple hosts.

4.3.3.6.6 Related lateral movement detections shall be correlated into a single incident rather than raised as isolated alerts for each hop.

4.3.3.7 Detection Accuracy and Management of False Positives

4.3.3.7.1 The solution shall be tuned to deliver a low false positive rate, and the Service Provider shall state the expected false positive rate together with the basis for that figure.

4.3.3.7.2 The solution shall provide tuning capabilities including allow-listing, exception handling, environment-specific baselines, alert suppression and threshold adjustment, all of which shall be performable by City Power without vendor intervention or additional cost.

4.3.3.7.3 The solution shall provide alert deduplication and correlation so that a single incident does not generate repeated or fragmented alerts.

4.3.3.7.4 The solution shall provide analyst feedback mechanisms, such as true and false positive marking, that measurably improve subsequent detection quality.

4.3.3.7.5 The solution shall report on detection quality metrics, including alert volumes, false positive rates and time to triage.

4.3.3.7.6 A dedicated tuning and optimisation period shall be included in the implementation, and the Service Provider shall conduct tuning reviews at least quarterly for the duration of the contract at no additional cost.

4.3.3.7.7 The Service Provider shall commit to a sustained alert volume that is within the reasonable handling capacity of the City Power security operations function, as agreed during implementation.

4.3.4 Response and Integration

The solution shall integrate with the wider City Power security ecosystem and shall not operate as an isolated point product.

4.3.4.1 SIEM Integration

4.3.4.1.1 The solution shall provide native, bi-directional integration with the City Power SIEM platform.

4.3.4.1.2 The solution shall forward alerts, enriched metadata and raw or summarised logs in standard formats, including CEF, LEEF, Syslog and JSON, with configurable verbosity.

4.3.4.1.3 The solution shall preserve full context in forwarded records and provide a link from the SIEM record back to the source detection and supporting evidence.

4.3.4.1.4 The solution shall support field normalisation to a common schema to simplify correlation with other data sources.

4.3.4.1.5 The Service Provider shall configure, test and document the SIEM integration as part of the implementation, at no additional cost.

4.3.4.2 API Access

4.3.4.2.1 The solution shall provide a fully documented, versioned REST API, and a streaming interface where available, giving access to alerts, incidents, assets, metadata, detections, configuration and reporting.

4.3.4.2.2 The API shall support both read and write operations, including the creation and update of cases and the triggering of response actions.

4.3.4.2.3 Authentication shall be by token or certificate, with role-scoped API credentials, disclosed rate limits and full audit logging of API activity.

4.3.4.2.4 API documentation and any software development kits shall be provided to City Power at no additional cost, and API access shall be included in the licensing.

4.3.4.2.5 The Service Provider shall state its policy on backward compatibility and the notice period given before deprecation of API versions.

4.3.4.3 Case Management

4.3.4.3.1 The solution shall provide native case management, including creation, assignment, prioritisation, SLA tracking, escalation, evidence attachment, analyst notes, linking of related cases and closure with disposition codes.

4.3.4.3.2 The solution shall support customisable workflows and case states aligned to the City Power incident response process.

4.3.4.3.3 The solution shall integrate with the City Power IT service management platform to allow bi-directional synchronisation of tickets.

4.3.4.3.4 The solution shall maintain a complete and immutable audit trail for each case, suitable for use as evidence.

4.3.4.3.5 The solution shall provide case metrics and reporting, including mean time to detect, mean time to respond, backlog and analyst workload.

4.3.4.4 SOAR Integration

4.3.4.4.1 The solution shall integrate with the existing or future City Power SOAR platform, or provide equivalent native orchestration and automation capability.

4.3.4.4.2 The solution shall provide pre-built connectors and playbooks for common enrichment and containment actions.

4.3.4.4.3 The solution shall support automated enrichment on alert creation, including threat intelligence lookup, asset and identity context and sandbox detonation.

4.3.4.4.4 The solution shall support automated containment with configurable approval gates, and mandatory manual approval for any action affecting operational technology or critical systems.

4.3.4.4.5 Playbooks shall be editable by City Power, version-controlled, and testable in a non-production mode before deployment.

4.3.4.4.6 The Service Provider shall list all supported integrations with security and network products and shall confirm compatibility with the incumbent City Power NGFW, NAC, EDR, email security and directory platforms, as verified during the pre-deployment assessment.

4.3.5 Deployment and Scalability

The solution shall be capable of deployment in a manner that suits the City Power environment and shall scale with the organisation over the contract term.

4.3.5.1 Cloud-Native Architecture

4.3.5.1.1 The solution shall be cloud-native in design, based on containerised microservices, capable of horizontal scaling and supporting automated deployment and upgrade.

4.3.5.1.2 The solution shall support monitoring of workloads in Microsoft Azure and Amazon Web Services, including native integration with cloud flow logs and traffic mirroring services.

4.3.5.1.3 The solution shall provide unified visibility and a single management plane across on-premises, cloud and hybrid environments.

4.3.5.1.4 The solution shall support segregation of data and views by site, business unit or environment where required.

4.3.5.2 Throughput and Capacity

4.3.5.2.1 The solution shall be sized for peak traffic and not average traffic and shall sustain peak throughput without packet loss or any reduction in detection capability.

4.3.5.2.2 The Service Provider shall state the rated throughput of each sensor and of the aggregate deployment, expressed both in Gbps and in flows or events per second.

4.3.5.2.3 Sizing shall include a minimum of thirty percent (30%) headroom above the current measured peak traffic and shall accommodate a stated growth rate over the contract term.

4.3.5.2.4 Final sizing shall be confirmed against the traffic volumes actually measured during the pre-deployment assessment.

4.3.5.2.5 The Service Provider shall state any performance impact on monitored systems and networks and shall confirm that collection is passive.

4.3.5.2.6 Capacity shall be expandable by the addition of sensors or nodes without redesign or wholesale replacement, and the incremental cost shall be stated.

4.3.5.2.7 Licensing shall be transparent; the Service Provider shall state the licensing metric applied, whether bandwidth, sensors, assets, users or data volume, and shall state the behaviour of the solution should a licensed limit be exceeded.

4.3.5.3 Deployment Options

4.3.5.3.1 The solution shall support deployment on-premises as a physical appliance, as a virtual appliance or virtual machine on the City Power hypervisor platform, as a cloud SaaS service, or as a hybrid combination of these.

4.3.5.3.2 The Service Provider shall recommend the deployment model best suited to the City Power environment, with justification, and shall price both the recommended model and the alternatives.

4.3.5.3.3 Where a SaaS or cloud-hosted component is proposed, the Service Provider shall state the hosting location and shall comply with POPIA requirements on data residency and cross-border transfer; personal information shall be hosted within the Republic of South Africa unless expressly authorised in writing by City Power.

4.3.5.3.4 Migration between deployment models during the contract shall be possible without loss of historical data or additional licensing cost.

4.3.5.3.5 All components shall support high availability and, where applicable, shall integrate with the City Power disaster recovery arrangements.

4.3.5.3.6 Sensors shall continue to collect and buffer data during loss of connectivity to the management plane and shall forward buffered data on restoration.

4.3.6 Infrastructure Requirements

The Service Provider shall specify in full the infrastructure required to deliver the solution and shall clearly distinguish between items it will supply as part of the turnkey solution and any items to be provided by City Power. Any item required for the solution to function that is not expressly identified as a City Power responsibility shall be deemed to be included in the Service Provider's offer.

The Service Provider shall state, as a minimum:

4.3.6.1.1 A complete bill of materials listing all hardware, appliances, sensors, collectors, aggregation devices, packet brokers, TAPs, optics and transceivers, cabling and mounting hardware.

4.3.6.1.2 Compute requirements for each component, including CPU cores, memory and the hypervisor platforms and versions supported.

4.3.6.1.3 Storage requirements, including capacity, storage type, IOPS and throughput, together with the basis of the calculation against the required retention periods.

4.3.6.1.4 Network requirements, including the number, speed and type of interfaces, VLANs, IP addressing, routing, and the firewall rules and ports required between components.

4.3.6.1.5 Rack space in rack units, power in kilowatts and feed type, redundancy and cooling requirements at each site.

4.3.6.1.6 Operating system, database and any third-party software required, and confirmation of whether the associated licences are included in the offer.

4.3.6.1.7 Time synchronisation and DNS requirements, including NTP source and accuracy.

4.3.6.1.8 Certificate, public key infrastructure and directory integration requirements.

4.3.6.1.9 Requirements at each site where sensors are to be deployed, including substations and remote sites.

4.3.6.1.10 Environmental and physical requirements for equipment to be installed in operational or substation environments, including operating temperature range and ingress protection rating.

4.3.6.1.11 Backup, restore and disaster recovery infrastructure for the solution itself.

4.3.6.1.12 Bandwidth required between sensors, collectors and the analysis platform, and between on-premises components and any cloud-hosted component.

4.3.6.1.13 Additional infrastructure required to support the stated growth over the contract term.

4.3.6.1.14 Final infrastructure requirements shall be confirmed in the Pre-Assessment Report, and any material deviation from the tendered bill of materials shall be subject to the prior written approval of City Power.

4.3.7 Compliance and Regulatory Reporting

4.3.7.1.1 The solution and its implementation shall comply with the Protection of Personal Information Act, 2013 (POPIA), and the Service Provider shall describe how personal information captured in network traffic is identified, minimised, masked, protected and lawfully processed.

4.3.7.1.2 The solution shall provide POPIA-aligned reporting, including the evidence required to support notification of a security compromise to the Information Regulator and to affected data subjects.

4.3.7.1.3 The solution shall provide reporting mapped to ISO/IEC 27001:2022, including the Annex A controls relevant to monitoring, logging, threat intelligence, network security and information security incident management, in support of the City Power information security management system.

4.3.7.1.4 The solution shall provide reporting aligned to ISO/IEC 27002:2022 control guidance and to ISO/IEC 27035 information security incident management practice.

4.3.7.1.5 The solution shall provide reporting mapped to the MITRE ATT&CK framework and, where applicable, to the functions of the NIST Cybersecurity Framework.

4.3.7.1.6 The solution shall provide reporting to support King IV and COBIT governance, risk and assurance reporting requirements.

4.3.7.1.7 The solution shall provide audit-ready reports, on demand and on schedule, evidencing monitoring coverage, detection activity, incident handling and response times, in a form acceptable to internal and external auditors.

4.3.7.1.8 All logs and records shall be tamper-evident and shall be retained in accordance with the retention requirements of this specification and the City Power records retention policy.

4.3.7.1.9 Reports shall be exportable in PDF, CSV and Excel formats and shall be schedulable for automatic distribution to nominated recipients.

4.3.7.1.10 City Power shall be able to create and modify compliance report templates without vendor intervention or additional cost.

4.3.8 Security of the Solution

4.3.8.1.1 The solution shall enforce role-based access control and multi-factor authentication, and shall encrypt data in transit and at rest using AES-256 or a stronger equivalent.

4.3.8.1.2 All components shall be deployed on hardened builds, and the Service Provider shall be responsible for vulnerability and patch management of the solution for the duration of the contract.

4.3.8.1.3 The Service Provider shall provide evidence of independent security testing of the product and shall remediate identified vulnerabilities within agreed severity-based timelines.

4.3.8.1.4 Remote access by the Service Provider for support purposes shall be brokered, logged, time-limited and subject to prior City Power approval.

4.4 Enhancements

The Service Provider shall provide enhancements, support, and maintenance services for existing and future ICT Security solutions. The enhancements shall be provided as and when needed.

4.4.1 Forensic services as and when required.

4.4.2 ICT risk detection and treatment services.

4.4.3 Penetration testing.

5. PRE-DEPLOYMENT ASSESSMENT

A pre-deployment assessment shall be undertaken by the appointed Service Provider before the final solution design, sizing, licensing and deployment plan are confirmed. The assessment is a mandatory deliverable, and it shall be completed and formally accepted by City Power before implementation commences. The cost of the assessment shall be included in the Service Provider's turnkey price and shall not be charged as a separate variation.

5.1 Objectives of the Assessment

The objectives of the assessment shall be to:

5.1.1 Establish an accurate, evidence-based understanding of the City Power ICT and operational technology environment.

5.1.2 Confirm the technical requirements for deploying the solution, including collection points, sizing, infrastructure and integration effort.

5.1.3 Establish a baseline of user, device and threat activity against which the effectiveness of the solution can subsequently be measured.

5.1.4 Identify risks, constraints and dependencies that may affect deployment.

5.1.5 Confirm the final bill of materials, licensing quantities and implementation plan.

5.2 Technical Assessment for Solution Deployment

The technical assessment shall include, as a minimum:

5.2.1 Review of the network architecture and topology, covering the core, distribution and access layers, data centres, DMZ, remote sites, substations, cloud environments and OT networks.

5.2.2 Identification of all required collection points, including SPAN and mirror ports, TAP locations, packet broker requirements, cloud mirroring and flow log sources, and server sensor coverage.

5.2.3 Measurement of current traffic volumes and peaks at each collection point, together with the growth trend, in order to confirm sensor sizing and licensing quantities.

5.2.4 Assessment of the segmentation model and the IT and OT boundary, and identification of blind spots where traffic is currently not visible.

5.2.5 Assessment of the existing security toolset, including SIEM, SOAR, NGFW, NAC, EDR, email security and directory services, and the integration effort required for each.

5.2.6 Assessment of available infrastructure, including rack space, power, cooling, compute, storage, virtualisation and network capacity, and identification of any shortfalls.

5.2.7 Assessment of the cloud environments in use, including subscriptions, VPCs and VNets, workloads, and the flow log and traffic mirroring capability available in each.

5.2.8 Confirmation of the protocols in use, including operational technology protocols, and confirmation that the proposed solution decodes each of them.

5.2.9 Identification of constraints, change control requirements, outage windows and operational risks associated with deployment.

5.2.10 A proposed deployment architecture, phased implementation plan and cut-over approach.

5.3 User and Access Analysis

The assessment shall establish which users actually log on to and use the environment, as distinct from the accounts that merely exist within it.

The analysis shall report, as a minimum:

5.3.1 The total number of user accounts in the directory, and the number of those accounts that have actually authenticated during the assessment period.

5.3.2 A breakdown of active, inactive, dormant, disabled, expired and stale accounts, with the dormancy thresholds applied clearly stated.

5.3.3 Identification and count of privileged and administrative accounts, and of the individuals who actually make use of them.

5.3.4 Identification and count of service, application, shared and generic accounts, together with their usage patterns and the systems on which they are used.

5.3.5 Identification of third-party, vendor, contractor and remote support accounts, and the access held by each.

5.3.6 Logon patterns and volumes, including logon counts per user, peak and average concurrent sessions, logon times and days, and off-hours activity.

5.3.7 Logon locations and methods, distinguishing on-premises, remote and VPN, and cloud access, and identifying the devices used.

5.3.8 Identification of accounts exhibiting anomalous behaviour, including concentrations of failed logons, improbable travel, multiple simultaneous sessions, and accounts logging on to an unusually large number of machines.

5.3.9 Accounts that have never logged on, and accounts belonging to individuals who have left the organisation.

5.3.10 A reconciliation of active accounts against the human resources establishment in order to identify orphaned accounts.

5.3.11 Where personal information is processed in the course of this analysis, it shall be handled strictly in accordance with POPIA and City Power policy.

5.4 Device and Machine Inventory

The assessment shall establish how many machines are present and communicating in the environment.

The inventory shall report, as a minimum:

5.4.1 The total count of devices observed on the network, broken down by type, including workstations, laptops, physical and virtual servers, network devices, security appliances, printers, mobile devices, IoT devices and OT or ICS devices.

5.4.2 Counts per site, per network segment and per environment, distinguishing corporate, data centre, cloud and operational technology environments.

5.4.3 The operating system and version distribution, including unsupported and end-of-life systems.

5.4.4 Identification of unmanaged, unknown, rogue or unauthorised devices, and of devices not recorded in the CMDB or asset register.

5.4.5 The count of virtual machines and cloud workloads, per platform.

5.4.6 Identification of devices with no endpoint protection or monitoring agent installed.

5.4.7 Device-to-user mapping where determinable, and identification of devices used by multiple users.

5.4.8 A reconciliation of the observed device count against the City Power asset register and CMDB, with discrepancies quantified.

5.4.9 The resulting device count shall be used to confirm licensing quantities where the licensing metric is asset-based.

5.5 Historical Attack and Incident Analysis

The assessment shall include an analysis of the attacks that City Power has experienced, covering a period of not less than the preceding twelve (12) months, based on available logs, security tooling data, incident records and any other evidence made available by City Power.

The analysis shall report, as a minimum:

5.5.1 The total number of security incidents and attempted attacks recorded over the period, with the monthly trend.

5.5.2 A breakdown of attacks by type, including as a minimum phishing and business email compromise, malware, ransomware, credential attacks such as brute force, password spraying and credential stuffing, exploitation of vulnerabilities, web application attacks, denial-of-service, insider misuse, data exfiltration attempts, lateral movement, command-and-control activity and unauthorised access attempts.

5.5.3 Mapping of the observed attacks to MITRE ATT&CK tactics and techniques.

5.5.4 The sources of attacks, including geographic origin, whether internal or external, and the identification of repeat sources.

5.5.5 The targets of attacks, including the users, systems, applications, network segments and sites most frequently targeted.

5.5.6 The severity distribution of the incidents recorded and the business impact of each.

5.5.7 The detection method for each incident, identifying which control detected it, and highlighting incidents detected late or only after impact had occurred.

5.5.8 Attacker dwell time where determinable, and the mean time to detect and mean time to respond achieved over the period.

5.5.9 Incidents that recurred or were not fully remediated, together with the underlying causes.

5.5.10 Identification of the attack types that the existing City Power controls would not have detected, and an explanation of how the proposed solution addresses each of them.

5.5.11 Any indicators of current or historical undetected compromise identified during the assessment, which shall be reported to City Power immediately on discovery.

5.6 Pre-Assessment Report and Acceptance

5.6.1 The findings shall be consolidated into a Pre-Assessment Report, submitted in both electronic and hard copy.

5.6.2 The report shall include an executive summary suitable for ICT and executive management, together with detailed findings supported by evidence and data.

5.6.3 The report shall include the analysis of the users who log on to the environment, the machine and device inventory, and the history of attacks and their associated types, in addition to the technical assessment for solution deployment.

5.6.4 The report shall include the confirmed solution design, bill of materials, licensing quantities, infrastructure requirements, integration plan, implementation plan and risk register.

5.6.5 The report shall include prioritised recommendations, distinguishing between items to be addressed by the solution, items requiring action by City Power, and items falling outside the scope of this contract.

5.6.6 The Service Provider shall present the report to City Power ICT Security and shall address any queries arising from it.

5.6.7 The report shall be formally accepted and signed off by City Power before implementation commences, and implementation shall not proceed on the basis of an unaccepted report.

5.6.8 The report shall be delivered within the timeframe agreed at contract award and, in any event, within thirty (30) working days of commencement of the assessment, unless otherwise agreed in writing.

5.7 Conduct of the Assessment

5.7.1 The assessment shall be conducted passively and non-intrusively and shall not disrupt or degrade any production, operational or substation system.

5.7.2 No active scanning, testing or other intrusive technique shall be used without prior written authorisation from City Power and adherence to the City Power change control process.

5.7.3 All work shall be performed by suitably qualified and vetted personnel, and the Service Provider shall provide the names, qualifications and security clearance status of assessment personnel in advance.

5.7.4 All data obtained during the assessment shall be treated as confidential, shall be processed in accordance with POPIA, shall not be removed from the City Power environment without authorisation, and shall be securely destroyed or returned on completion, with written confirmation of destruction provided.

5.7.5 The Service Provider shall not disclose the findings of the assessment to any third party.

5.7.6 City Power shall provide reasonable access to the environment, documentation, personnel and log data required for the assessment.

5.7.7 Where the assessment identifies a material change to scope, sizing or price, this shall be raised in writing and agreed before implementation; no variation shall be claimed in respect of items that a competent bidder ought reasonably to have allowed for.

6. TRAINING

6.1 City Power requires the necessary training for system administrators at no cost to City Power.

6.2 The Service Provider shall clearly outline the layout of the recommended enhanced training at no cost.

6.3 The solution provider shall work closely with City Power's resources during the implementation in a live environment to ensure practical knowledge transfer.

6.4 Training shall be on-site and form part of the implementation process.

6.5 The Service Provider shall also be required to provide training to City Power technical representatives on the system when enhanced features and functionality become available as the system is upgraded at no cost.

6.6 The suppliers shall provide technical support on system and equipment queries for the duration of the contract as of the go-live date of the implemented solution at no cost.

7. SUPPORT AND MAINTENANCE

The Service Provider shall provide support and maintenance services on the proposed solution.

7.1 SUPPORT DESK

7.1.1 The Service Provider shall provide the Support Centre, which shall be a single point of contact for the resolution of system problems.

7.1.2 Support requests shall be submitted by phone, email, or on a support portal.

7.1.3 The Service Provider shall respond to all support requests.

7.1.4 The Support Centre shall be available for support requests on Monday to Friday from 08:00 AM – 5:00 PM (each "Business Day") and on Standby after-hours including weekends and public holidays.

7.1.5 The Support Centre shall be responsible to perform the following functions:

7.1.5.1 Document all support and all logged requests and issue a reference number for each incident.

7.1.5.2 Monitor and manage the resolution of incidents from the initial support request to resolution.

7.1.5.3 Route incidents to the appropriate resource for resolution.

7.1.5.4 Perform problem diagnosis.

7.1.5.5 Answer queries regarding the usage and performance of the system.

7.1.5.6 Access the system remotely for diagnosis and correction of problems.

7.1.5.7 Contact the City Power Representative at regular intervals to provide status and/or resolution of problems.

7.2 CITY POWER'S RESPONSIBILITIES. SHALL BE RESPONSIBLE FOR THE FOLLOWING FUNCTIONS:

City Power shall provide 1st line support, which entails the following:

7.2.1 Response to End-user queries regarding the usage or performance of the system.

7.2.2 Resolve system problems with support from the Service Provider where necessary.

7.2.3 Swap defective hardware components using spare parts.

7.2.4 Hand over complex system problems to the Service Provider through the Support Desk.

7.2.5 File a support request with the Support Desk for software and hardware support.

7.2.6 Inform and update the service provider of all information related to the encountered software or hardware problem.

7.3 ON-SITE SUPPORT

On-site support shall be the responsibility of the appointed service provider.

The service provider shall ensure that at least one qualified support resource is available to conduct physical on-site visits to City Power premises weekly and when required.
All on-site support services shall be delivered in accordance with the agreed Service Level Agreement (SLA), including defined response times, resolution targets, and escalation procedures.

7.4 SYSTEM MAINTENANCE

7.4.1 The Service Provider shall perform on-site routine system maintenance once every week, the weekly site visits shall include but not be limited to the following:
7.4.2 General routine checks of the system status.
7.4.3 Resolving system alarms.
7.4.4 Routine tests of the equipment's performance against the relevant equipment specifications.

7.5 SOFTWARE UPGRADE

7.5.1 The Service Provider shall be responsible for providing software upgrades as may be required to fix bugs, introduce added functionality, and keep the system fully functional.
7.5.2 Upgrades shall be made available either on-premises or via a VPN connection.

7.6 INCIDENT MANAGEMENT

PRIORITY AND RESPONSE TIMES

TABLE: A PRIORITY LEVEL RATING OF ALL SUPPORT QUERIES IS AS PER THE TABLE BELOW:

PRIORITY	DESCRIPTION	CONDITION
1	Critical	Total system failure
2	High	Unavailability of major system functionality
3	Medium	Unavailability of minor system functionality
4	Low	All configurations and minor ad hoc programming on request
5	Configuration and programming	Includes all configurations and minor ad hoc programming on request

TABLE B: RESPONSE TIMES SHALL BE AS FOLLOWS:

PRIORITY	RESPONSE TIME	COMMENCEMENT	FEEDBACK	MAXIMUM TIME TO REPAIR
1	½ HR	1 HR	ON SITE	4 HOURS
2	1 HRS	2 HRS	ON SITE	5 HOURS
3	2 HRS	3 HRS	ON SITE	6 HOURS
4	6 HRS	8 HRS	DAILY	12 HOURS
5	24 HRS	36 HRS	DAILY	48 HOURS

8. DOCUMENTATION

The Service Provider shall provide all documentation required, including but not limited to manuals, licenses, and catalogues.

Documentation shall be in both hard and soft copies.

9. QUALITY MANAGEMENT

A quality management system/plan shall be set up to assure quality during manufacture, installation, removal, transportation, and disposal. Guidance on the requirements for a quality management system may be found in the following standards: ISO 9001:2015. The details shall be subject to an agreement between the purchaser and the supplier.

10. HEALTH AND SAFETY

A health and safety system/plan shall be set up to ensure proper management and compliance during manufacture, installation, removal, transportation, and disposal. Guidance on the requirements of a health and safety plan shall be found in ISO 45001:2018 standards. The details shall be subject to an agreement between City Power and the Supplier.

11. ENVIRONMENTAL MANAGEMENT

An environmental management system/plan shall be set up to ensure the proper environmental management and compliance is adhered to during manufacturing, installation, removal, transportation, and disposal. Guidance on the requirements for an environmental management system shall be found in ISO 14001:2015 standards. The details shall be subject to an agreement between City Power and the Supplier. This is to ensure that the asset created conforms to environmental standards and City Power SHERQ Policy.

ANNEXURE A – BIBLIOGRAPHY

None

ANNEXURE B - REVISION INFORMATION

DATE	REV. NO.	NOTES
September 2024	0	First issue
August 2026	1	Second issue Technical requirements changes and general editing