SOUTH AFRICA

Electoral Commission

Auction 0010556456

PARALLEL SECURITY OPERATIONS CENTRE (SOC)

IMPORTANT NOTICE

Failure to comply with the completion of the bid conditions and the required information or submission of the required stipulated documents indicated in the bid shall invalidate a bid.

1 Introduction

The Electoral Commission (IEC) seeks to procure a parallel security operations centre (SOC) also referred to as a Managed Detection and Response (MDR) service for a period of thirty-six (36) months. This will form part of the integrated security monitoring and response activities to secure the Local Government Elections 2026 and beyond.

Gartner defines managed detection and response (MDR) services as those that provide customers with remotely delivered security operations center (SOC) functions. These functions allow organizations to perform rapid detection, analysis, investigation and response through threat disruption and containment. They offer a turnkey experience, using a predefined technology stack that commonly covers endpoints, networks, logs and cloud. Telemetry is analyzed within a provider's platform using a range of techniques. The MDR provider's analyst team then performs threat hunting and incident management to deliver recommended actions to their clients.

The primary function of the required service will be to assist the Electoral Commission to detect, analyse, investigate and actively respond to cybersecurity events, including threats and incidents, employing people, processes and technology for a period not exceeding 36 months.

Bidders must place a bid on the Votaquotes (e-Procurement) system and then provide all the required documentation before the due dates as specified in this document and on the Votaquotes web site. Bidders must be registered and approved to bid on this auction.

2 Background Information

The Electoral Commission has invested extensively in ICT technologies, which provide a platform to effectively support and enable its business processes, in an effort to meet its goal of delivering free and fair elections in an open and transparent environment.

The Electoral Commission has also adopted a net-centric architecture that operates on a wide area network connecting more than 300 offices at various locations around the country and around 2000 users, using a combination of platforms including the Multi-Protocol Label Switching (MPLS) Network. In addition, the Electoral Commission has an extensive online presence with various websites and web portals including mobile

applications, which provide real-time and online data processing capabilities in various forms. The Electoral Commission also has a fleet of 40,000 Voting Management Devices and over 1,200 laptops that connect to the back-end via an Access Point Name (APN). The following is a breakdown of the various components of the system:

2.1 National office: The Electoral Commission has adopted a centralized architecture, with a data-centre at national office, all major computing equipment are deployed and processing from the data-centre.

2.2 The national data-centre has over 400 physical and virtual servers, including associated data-centre computing equipment such storage systems, backup systems, networking, security, etc.;

2.3 Disaster recovery (DR) site: An alternative site hosting a business continuity and disaster recovery capability for key critical systems, the disaster recovery site also caries similar computing capability as the national data centre, although at a lower scale and capacity.

2.4 Provincial offices: nine (9) offices country wide hosting one server and an average of thirty (30) workstations, located in each of the 9 South African provinces;

2.5 Warehouses: ten (10) country-wide, one in each province and one at national level, hosting between two (2) and thirty (30) workstations;

2.6 Local municipal offices: approximately three hundred (300) offices countrywide hosting an average of three (3) computers with routers and switches.

2.7 Network structure: The Electoral Commission uses Virtual Private Network service to provide connectivity to the entire wide area network (WAN) with Voice-Over-IP capability at some sites. The network is also extended by GSM based Access Point Name (APN) connecting the Voting Management Devices (VMDs) and laptops in the field.

2.8 During election periods, that is during the period envisaged for this service, the network gets expanded to connect an additional data-centre at the national results operations centre, additional sites such as 9 provincial results operations centres and various results capturing sites at the municipal level averaging around 50.

2.9 Also during the election periods, the Commission’s website gets hosted at an Internet Service Provider (ISP).

The Electoral Commission is increasingly using digital assets such as websites, social media and mobile applications to interact with its stakeholders to among others, register voters, enable the nomination of political party candidates, enable the application for jobs, tendering for business opportunities and disseminate information. This growing use of digital assets brings many operational benefits including that interactions with our stakeholders are not limited to office hours or location, but our stakeholders can interact with the Electoral Commission anytime from anywhere.

"The Internet, despite all the societal benefit and economic value it has helped create, has also created an arena of strategic competition and criminal activity. Elections have begun to attract the attention of a wider spectrum of threat actors. Threat actors may have a range of motives, from mischief to malice to manipulation. Actors seeking to manipulate the results of an election may have purely political or financial objectives, while others may not have an interest in seeing a particular candidate or party prevail, but rather seek to undermine the credibility of the electoral process or erode trust in democracy. There are well-known examples of cyber-attacks that have focused on elections launched by well-resourced foreign state actors with the aim of undermining trust in democratic processes and the legitimacy of their outcomes"1

3 Bid Requirements

The Electoral Commission is seeking to establish a Parallel Security Operations Centre (SOC) service as an extension of its security team, providing continuous 24/7 monitoring of the IT environment for potential threats considering the following:

3.1 The bidder will use the existing Electoral Commission's cyber security tools that cover endpoint, network, logs and cloud at the Electoral Commission. These tools deposit logs into the Electoral Commission's Security Information and Events Management (SIEM) environment

3.2 The bidder will assist to fine-tune these tools including the SIEM within the Electoral Commission's space so that the bidder can get all the information required from these tools.

3.3 Telemetry injected from the Electoral Commission's Security Information and Events

[1] Primer: Cybersecurity and Elections – July 2022

Management (SIEM) environment into the service provider's platform is to be analysed using a range of techniques.

3.4 The service will act as an extension of the Electoral Commission's security team, offering threat hunting, incident response, and proactive measures to protect against cyberattacks.

4 Technical Specifications

The technical specification for the required products and services is as per the bid specifications provided below. It must be noted that the technical specifications below are the minimum requirements. The only deviation that may be accepted will be in case where the service provider's specification exceeds the minimum requirements. Any offers below the minimum specification requirement will be disqualified.

The Electoral Commission is looking for a Parallel SOC solution service that uses a combination of threat intelligence, security monitoring capabilities, and experienced and certified cybersecurity analysts to not only detect threats but to also define and execute appropriate threat responses that align with the Electoral Commission's incident response plan, policies, security team, and response capabilities.

The analysts may be required to undergo security clearance. The bid must demonstrate the bidder's skills, experience and capacity to deliver SOC alternatively known as MDR services.

The Parallel SOC service is to operate on a 24/7 basis and must have the following features and characteristics:

4.1 Features and Characteristics

4.1.1 SOC Management

The bidder must have skill, experience and technological systems and tools to be able to deliver on the following capabilities:

4.1.1.1 Ingest – All data to determine security relevance. The ability to ingest data from any source, structured or unstructured, at scale and the ability to organize that data to make it actionable by machine or human.

4.1.1.2 Detect – The ability to detect security event.

4.1.1.3 Predict – The ability to predict a security event allows the SOC to proactively escalate the incident to a human or to streamline a response with a predefined process.

4.1.1.4 Automate – Usage of automation tools to take standard operating procedures and turns them into digital playbooks to accelerate investigation, enrichment, hunting, containment and remediation.

4.1.1.5 Orchestrate – The ability to plug in and connect everything that is inside and outside of your SOC.

4.1.1.6 Recommend – The ability of the platform powering the SOC to tell the analysts what to do next by making a recommendation.

4.1.1.7 Investigate – Investigation requires detailed, precise analysis with the assistance of intuitive security tools which can prioritize what needs to be investigated.

4.1.1.8 Collaborate- to collaborate and connect the tools, people, process and automation into a transparent workplace, bringing information, ideas and data to the forefront and enabling security teams to better collaborate.

4.1.1.9 Manage – The ability to arm security teams with everything necessary to manage the response process when incidents have happened.

4.1.1.10 Report – Having the right reporting tools helps inform on what's performing, so security teams can accurately measure where they are and where they need to go.

4.1.2 Correlation, Security Monitoring, Data Aggregation and Alerts

The platform used by bidder collects and aggregates data from security systems and network devices, routers, switches, servers, and endpoints. It also links events and related data into security incidents, threats or forensic findings, analyses events and sends alerts

to notify security staff of immediate issues. The bidder is to state which Security Information and Events Management (SIEM) and Security Orchestration, Automation and Response (SOAR) tool the bidder is using for the provision of the service.

4.1.3 Search, Data Exploration and Reporting

The platform must be able to search vast amounts of security data without reviewing raw data and without data science expertise, actively explore data to discover patterns and hunt for threats, create and schedule reports on important data points.

4.1.4 Threat Intelligence and Hunting

The platform must combine internal data from all the sources (switches, routers, servers, endpoints etc.) within the Electoral Commission with third-party threat intelligence feeds on threats and vulnerabilities. The solution must provide visibility and situational awareness of the Electoral Commission's environment by identifying and investigating cyber-attacks and correlating events across multiple sources to identify indicators of attack.

The platform used by the bidder enables security staff to run queries on log and event data, and freely explore data to proactively uncover threats. Once a threat is discovered, automatically pulls in relevant evidence for investigation. The platform also helps security teams identify and respond to security incidents automatically, bringing in all relevant data rapidly and providing decision support.

4.1.5 Advanced Analytics

The platform used by the bidder must use statistical models and machine learning to identify anomalies and detect advanced threats, detect unknown threats, detect lateral movements within a network, and enrich the context of security alerts to make it easier to investigate and detect elusive threats.

4.1.6 Dashboards

The Electoral Commission must have remote access to the bidder's data dashboards (whether at the Electoral Commission's premises or bidder's premises) created to let staff review event data, identify patterns and anomalies.

4.1.7 Forensic Analysis

The platform used by the bidder enables exploration of log and event data to discover details of a security incident, with automated attachment of additional evidence organized in a situation timeline. Data on the platform can be used for forensic analysis.

4.1.8 Retention

The platform used by the bidder stores long-term (at least 36 months) historical data, useful for compliance and forensic investigations. The platform allows for collection of large data sets and the analysis thereof. The bidder is to describe how the platform achieves this. The data must however reside within the borders of South Africa.

4.1.9 Compliance

The platform used by the bidder gathers log data for standards like POPIA, PCI/DSS and GDPR and generates compliance reports. The solution helps to meet compliance and security regulations requirements, for example by alerting about security conditions for protected data.

4.1.10 User and Entity Behaviour Analytics (UEBA)

The platform includes User Behaviour Analytics Tools to detect anomalies in the behaviour of not only the users in the network but also the routers, servers, and endpoints in that network

4.1.11 Reporting

Reporting on a daily, weekly and monthly basis, as well as a full close out report at the end of the project is required as part of the service. Timeous reporting for all the defined alerts and issues will also be required.

4.1.12 Vulnerability & compliance management

The service must include regular scans on devices on the network to identify vulnerabilities and incorrectly configured systems. The SOC security experts must analyse and prioritize the findings and help resolve any detected vulnerabilities. The scans should include cyber security war-games which are organized around a business scenario (such as cybercriminals using “spear phishing” attacks). It is to be structured to simulate the experience of a real attack.

The bidder must perform vulnerability assessments on the Electoral Commission’s network every 6 months.

4.1.13 Attack Surface Monitoring

The service must also include an early warning of any malicious activity targeted at the Electoral Commission to enable fast detection and mitigation. The services must include an adversary’s view of the Electoral Commission’s digital attack surface and prioritizes risks and exposures, enabling the SOC together with the Electoral Commission to mitigate threats in a controlled manner before they become a problem.

4.1.14 Incident Response Plan

The service provider will integrate their platform with the Electoral Commission’s helpdesk in a way that calls will be logged on both systems. The service provider will also assist the Electoral Commission in further developing its cybersecurity incident response plan and provide opportunities and mechanisms of testing it during the course of the contract.

4.1.15 Accreditations and Certifications

It is expected that the bidder is already running their own SOC. It is required that their current SOC must have valid certifications such as ISO 27001, ISO 27035 (Incident Management), ISO/IEC 20000-1 (IT Service Management), SOC 2 Type II (System and Organization Controls), NIST SP 800-53 / NIST Cybersecurity Framework or other ICT Security standards. It must also have accreditations from internationally recognized institutions such as TF-CSIRT Trusted Introducer. The bidder is to include a copy of such certification with the bid submission.

4.2 Implementation

4.2.1 The bidder will use Electoral Commission's existing cyber security tools that cover endpoint, network, logs and cloud at the Electoral Commission. The bidder will assist to fine-tune these tools within the Electoral Commission's space so that the bidder can get all the information required from these tools.

4.2.2 The tools at the Electoral Commission include the following:

4.2.2.1 Security Incidents and Events Management (SIEM)

4.2.2.2 Endpoint Detection and Response (EDR)

4.2.2.3 Firewalls and IPSs

4.2.2.4 Remote and on-premises DDOS Facilities

4.2.2.5 Web Application Firewalls

4.2.2.6 Anti-virus system

4.2.2.7 Vulnerability management tools

4.2.2.8 Email Security Tools

4.2.2.9 Telemetry injected from the Electoral Commission's SIEM environment into the service provider's platform (SIEM and SOAR) is to be analysed using a range of techniques. The bidder may recommend other utilities that they require within the Electoral Commission's environment that will then feed into the SIEM, the data will then be injected into the bidder's platform.

The solution option should include the following:

4.2.2.10 Health Check on the Electoral Commission Environment

A health check and rule review of the Electoral Commission Security Environment including the SIEM configuration, will be required as well as fine tuning of current rules and new rules sets. The bidder takes full accountability and responsibility for the accuracy of incident monitoring, reporting and alerting.

4.2.2.11 Integrations

The bidder's solution must integrate with the SIEM solution deployed at the Electoral Commission. The SIEM will collect logs and other necessary data and inject this information into the bidder's platform for further aggregation and analysis.

4.2.2.12 Remote Access

The bidder's "environment" should be accessible remotely from the Electoral Commission for access by Electoral Commission's employees. This can be in the form of web access. A secure tunnel can be created between the bidder's SOC and the Electoral Commission.

5 Planning Assumptions

The Electoral Commission has made the following assumptions:

5.1 The Electoral Commission will provide technical resources for all Electoral Commission's designated work including setup and configuration of own applications and databases. Included are the provision of servers, desktops and switching at its premises.

5.2 The successful bidder shall setup their environment and integrate to the Electoral Commission's environment.

5.3 The recommended service provider shall provide all relevant details needed to ensure successful operations capability within the organization.

5.4 The bidder's change control management process must be flexible enough to facilitate speedy deployment and resolution of problems without compromising management controls and security.

6 General Bid Conditions

The following standard bid conditions must be adhered to and complied with; failing which the bid proposal will be disqualified.

6.1 All bids must be placed online on eProcurement website https://votaquotes.elections.org.za.

6.2 Bidders must complete and submit Appendix A - Technical Bid Response Sheet to

demonstrate compliance with the required technical specification.

6.3 The bidder must provide at least five (5) contactable references of past and current services of a similar nature that the bidder provided or is currently providing (Security Operations Centre (SOC)). Reference details must include the following: customer name, contact person, contact details (telephone, email, physical address) and service description and value of services defined in terms of estimated contract value and length of time of the service. The Electoral Commission prefers to work with a service provider that shows that they are currently providing such services to clients. The table in Appendix C – Reference Guideline Table is attached as a guideline for the compilation of the required reference information to be submitted for each reference.

6.4 Bidder must have at least five (5) years' experience in providing the services required. Bidder must provide a profile or letter to confirm.

6.5 Bidders must adhere to the delivery schedule in section 12.

6.6 The successful bidder will be required to enter into a Service Level Agreement (SLA) with the Electoral Commission. The bidder is to include as part of the bid submission an example SLA.

6.7 Bidder must provide an organogram for their SOC and skills matrix of their current employees including analysts. The SOC must have the following capabilities at a minimum (e.g. Incident Triage, Analysis and Response; Cyber Threat Intelligence, Hunting and Analytics; Vulnerability Management; SOC Tools Configuration; SOC Operations Management etc.)The table in Appendix D – Skills Matrix Table is attached as a guideline for the compilation of the required skills matrix information to be submitted.

6.8 The bidder must submit an example Incident Response Plan as part of the submission. The Electoral Commission is interested to see the steps employed by the bidder in terms of Incident Response.

7 Quality Control

7.1 The bidder takes responsibility for the completeness and quality of their bid submission.

7.2 The Electoral Commission may also call on bidders to make presentations in order to

ensure full compliance with all its requirements and as part of the bid evaluation process prior to the conclusion of the adjudication of the bid. Any such request for presentations shall only be for clarification purposes in support of mandatory requirements that must be adhered to as part of the written submission requirements of this bid. Failure to submit mandatory requirements shall not be rectified by the call for presentations.

7.3 Any restrictions or conditions associated with any elements of the service offering/s must be detailed. The Electoral Commission reserves the right to reject conditions which are considered unfavourable to its business or unacceptable.

7.4 The submission of a bid implies acceptance of the terms specified in the provisions laid down in the specifications, the procurement and, where applicable, additional documents.

7.5 Bidders are expected to examine carefully and respect all instructions and standard formats contained in these specifications.

7.6 A bid that does not contain all the required information and documentation will be disqualified.

7.7 Although the Electoral Commission will only deal with the principal service provider, if a bidder plans to sub-contract any of the services in this bid, they are required to attach copies of sub-contracting agreements in their bid response documentation.

7.8 Notwithstanding any shortcomings in these specifications, service providers must ensure that the proposed solution will form a workable and complete solution.

7.9 The Electoral Commission will issue a formal purchase order to the successful bidder before any services can be delivered.

7.10 The bidder’s personnel working in the SOC may be subjected to security clearance.

7.11 The bidder will be required to enter into a Non-Disclosure Agreement (NDA) with the Electoral Commission.

7.12 The Electoral Commission reserves the right and discretion to amend the quantities or cancel or not award this bid based on any reason including operational or financial

requirements.

7.13 The supplier must undertake and warrant that all goods and services shall at the time of delivery comply with the bid specifications.

8 Supplier Performance

8.1 Contracting of any service provider to render goods and/or services to the Electoral Commission are subject to the fulfilment of the Electoral Commission's due diligence audit requirements.

8.2 An essential component of the Electoral Commission's due diligence audit requirements may involve site visits to potential suppliers/contractors as well as inspection of various key documents underpinning the establishment of the companies involved in bids of the Electoral Commission. This also includes confirmation of capability and capacity requirements to execute the services specified in such bids.

8.3 Upon notification of the Electoral Commission's intention to award a contract, the successful bidder shall be required to enter into a service level agreement (SLA/contract) with the Electoral Commission.

8.4 The purpose of the SLA (if applicable other than what the Electoral Commission's standard purchase orders provide for) is to fix performance criteria within the key requirements of this request for quotation, namely quantity, quality and delivery.

8.5 The SLA may contain elements such as supplier progress milestones, delivery schedules, quality checkpoints and invoicing procedures.

8.6 The Electoral Commission reserves the right to reject any services delivered not conforming to the bid specification.

8.7 Where previously-agreed delivery schedules are not met by a supplier, the Electoral Commission shall have the right to appoint an alternative supplier to make good the shortfall in supply. Any additional costs incurred by the Electoral Commission in obtaining such corrective services or products from another source will be for the

account of the defaulting supplier.

9 Data Protection and Confidentiality of Information

Due to the sensitive nature of the information and data which will become available to the successful bidder, it will be required that the successful bidder sign a Service Level Agreement which will, *inter alia*, incorporate a clause addressing the protection of same in line with paragraphs 9.1 and 9.2 below (read together with the Technical Bid Response Sheet).

9.1 Data Protection

9.1.1 During the course of executing on this contract, the successful bidder will have access to the data collected or provided and stored by the Electoral Commission on the service provider's disk storage units and data backup facilities. The successful bidder shall have the responsibility for protecting information resources against accidental or intentional damage or loss of data, interruption, or the compromise of this information into the hands of third parties. The successful bidder or its members of staff, whether employed or contracted shall also not process the data without a prior written agreement with the Electoral Commission or without written instructions from the Electoral Commission beyond what is necessary to fulfil its obligations towards the Electoral Commission.

9.1.2 The successful bidder shall keep confidential all the Electoral Commission's information that they have in their possession. The successful bidder shall ensure that each member of the*ir* staff, whether employed or contracted, having access to or being involved with the processing of the Electoral Commission's data undertakes a duty of confidentiality and is informed of and complies with the data privacy obligations of this bid.

9.1.3 The successful bidder shall also ensure that the Electoral Commission's data in its possession is returned to the Electoral Commission and/or deleted from its computer systems as per instruction by the Electoral Commission at the end of the contract period.

9.2 Confidentiality of Information

9.2.1 "Confidential Information" means irrespective of its format, confidential trade, commercial, financial and management information and data, or other proprietary

information which is either designated as confidential or by its nature is confidential howsoever such confidential information may be disclosed or made available to the Recipient including, without limiting the afore-going, whether direct or indirect, orally, visually or in electronic format or by reason of inspection of documentation or other matter on or at the Discloser's premises or elsewhere including, but not limited to:

9.2.2 The successful bidder shall irrevocably undertake and agree:

9.2.2.1 to protect all confidential information that they may get access to in course of executing the resulting contract. Without limiting the generality of confidential information, Confidential Information shall include any information that falls within the definition of 'Personal Information' as defined in the Protection of Personal Information Act 4 of 2013, as amended or substituted and/or

9.2.2.2 not to divulge or disclose to any third party in any form or manner whatsoever, either directly or indirectly, any confidential information of the Discloser without the Consent of the Discloser;

9.2.2.3 not to, directly or indirectly, detract from, expand on, amend, decompile, reverse engineer, use, exploit, permit the use of, or in any other manner whatsoever apply the confidential information for its own benefit or the benefit of any other person or for any purpose whatsoever other than for the Engagement and otherwise than in accordance with the provisions of this Agreement;

9.2.2.4 to take reasonable security (including IT security) measures in line with its own security measures to keep the confidential information confidential;

9.2.2.5 to treat all Information as confidential information where it is uncertain of the nature of the Information until written notice to the contrary is received from the Electoral Commission;

9.2.2.6 to immediately notify the Electoral Commission upon discovery of any unauthorised use or disclosure of the confidential information or any other breach of this clause;

9.2.2.7 to take all necessary steps or assist the Electoral Commission to regain possession of the confidential information or to prevent its further unauthorised use;

9.2.2.8 to immediately at the Electoral Commission's reasonable request or in any event at the completion of an engagement to forthwith return all originals, copies, reproductions, summaries or extracts of the confidential information, or at the Electoral Commission's option destroy these and certify that it has done so; and

9.2.2.9 that all confidential information is and shall remain the property of the Electoral Commission and that disclosure thereof does not grant the Receiver any express or implied license to use such Confidential Information or right other than as provided for in this Agreement.

9.2.3 Notwithstanding the above, the successful bidder shall be entitled:

9.2.3.1 in compliance with the applicable laws and its professional obligations, to retain copies of all Information of the Electoral Commission which is relevant to or forms part of the Services;

9.2.3.2 to share the confidential information with its Personnel and any of the Service Provider's parties to the extent required to render the Services; and

9.2.3.3 to share the confidential information with its Professional Advisors or insurers in the event of a claim arising from or in connection with this Agreement, provided that the provisions of this clause shall still apply to such copies.

9.3 This clause shall not apply to:

9.3.1 information in the public domain otherwise than by breach of this Agreement;

9.3.2 information that was not obtained under any obligation of confidentiality; and

9.3.3 information obtained from a third party who the Receiving Party believes, after reasonable inquiry, is free to divulge the information so long as such information was not obtained by the receiving Party under any obligation of confidentiality to the third party.

10 Pricing Requirements

Completion of the detailed Pricing Schedule by responding to each item is compulsory. Failure to complete and submit this detailed pricing schedule as part of the bid submission shall lead to disqualification.

10.1 Total bid price must be submitted online on the eProcurement (Votaquotes) portal. The bid price in Appendix B: Pricing Schedule must be the same as the bid price submitted online. If there is a discrepancy between the Pricing Schedule bid price and the online submitted bid price, the online submitted bid price will be used for adjudication.

10.2 All costs associated with any appliance, software licensing, implementation services, associated support and maintenance, and 24/7 SOC services must be included in the total bid price. The total bid price must be inclusive of all factors which may contribute the cost of fulfilling the bid, factors such as:

10.2.1.1 Any appliances and Software costs.

10.2.1.2 Configuration and/or customization services costs.

10.2.1.3 Support and maintenance costs for all appliances and licenses provided for a period of 36 months.

10.2.1.4 24/7 SOC Services for a period of 36 months

10.3 Bid prices must be firm for a period of one hundred and eighty (180) days and must be inclusive of VAT. Once awarded the price will be firm for the duration of the contract.

10.4 Payment for SOC services will be monthly.

10.5 The Electoral Commission reserves the right to adjust costs by excluding some cost factors.

10.6 All costs associated with the solution must be captured in the Appendix B: Pricing Schedule - no additional costs will be entertained.

10.7 The solution must be a complete solution.

11 Adjudication and Award of Contract

Bidders are advised to refer to the Bid Evaluation Criteria to ensure that they have addressed all critical bid requirements.

11.1 The bid will be awarded to a bidder whose service successfully conforms to the bid specifications.

11.2 The Electoral Commission will issue an official purchase order before any services can be delivered

11.3 It should be noted that the Electoral Commission seeks to gain the best solution technically and financially and will select from the results of the bid a solution it deems to give the best investment.

11.4 Awarding the bid to a successful bidder is subject to the bidder entering into a service level agreement (SLA) with the Electoral Commission that will formalize and regulate the final deliverables and associated processes and procedures.

12 Delivery and Implementation Timeframe

12.1 The successful bidder will be required to complete delivery within six (6) weeks from receipt of an official purchase order.

13 Duration

13.1 The SLA/contract is for a period not exceeding 36 months and may be extended at the sole discretion of the Electoral Commission as may be deemed necessary.

14 Enquiries

14.1 Bid enquiries must be directed to Yash Sookan at 012 622 5700 or email SookanY@elections.org.za

15 Briefing Session

15.1 A non-mandatory virtual briefing session will be held. Details will be posted online on the bid publication on the Electoral Commission's procurement portal at https://votaquotes.elections.org.za/eproc_inter/

16 Written Submissions

All submissions must be received before the closing date and time for submissions as stipulated on the eProcurement website https://votaquotes.elections.org.za

Submissions received after the final date and time will lead to bids being disqualified and not considered.

All bids must be placed online on eProcurement website https://votaquotes.elections.org.za. Supporting documentation can be submitted in any or both of the following options:

16.1 Upload to the auction site.

16.2 Place in the Electoral Commission tender box situated in the foyer of the Electoral Commission National Office in Centurion at the following address before the closing date and time of this auction

Election House

Riverside Office Park,
1303 Heuwel Avenue,
Centurion,
0157

Note: Clearly mark your submission: For the attention of Procurement and Asset Management Department – Auction 0010556456

Failure to submit all of the required documentation before the closing date and time shall invalidate the bid. It remains the responsibility of the bidder to confirm receipt of the required documentation with the Electoral Commission Procurement and Asset Management Department.

17 Summary of Submission Requirements

17.1 All bids must be submitted online on eProcurement (Votaquotes) portal.

17.2 All written supporting documentation must be submitted as stipulated on the bid requirement.

17.3 Submissions received after the closing date and time will lead to the bidder's proposal being disqualified and not considered.

17.4 The following supporting documents must be submitted as part of the written submissions. Failure to submit these will lead to the bid being disqualified:

17.4.1 Completed technical specifications in accordance with the requirements in Appendix A - Technical Bid Response Sheet to demonstrate compliance with the bid specification as per 6.2.

17.4.2 Five (5) relevant contactable References, Appendix C - Guideline Reference Table as per 6.3

17.4.3 Completed pricing schedules Appendix B: Pricing Schedule as per 10.1

17.4.4 A profile or company letter (on a letterhead) showing five years' experience as per 6.4

17.4.5 A valid SOC accreditation or certification as per 4.1.15

17.4.6 An example SLA document as per 6.6.

17.4.7 SOC Organogram and Skills matrix as per 6.7

17.4.8 An example Incident Response Plan document as per 6.8

18 Closing Date

The closing date and time of this auction is specified on the eProcurement (Votaquotes) website in accordance the bidding requirements. The closing date and time is determined by the clock on the Electoral Commission's servers and is not negotiable. Bidders must also take note supporting documentation must be delivered before closing date and time.

19 Appendix A: Technical Bid Response Sheet

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
SOC Management	1.	The bidder must have skill, experience and technological systems and tools to be able to deliver on the following capabilities:	4.1.1			
	2.	Ingest – All data to determine security relevance. The ability to ingest data from any source, structured or unstructured, at scale and the ability to organize that data to make it actionable by machine or human.	4.1.1.1			
	3.	Detect – The ability to detect security event.	4.1.1.2			
	4.	Predict – The ability to predict a security event allows the SOC to proactively escalate the incident to a human or to streamline a response with a predefined process.	4.1.1.3			
	5.	Automate – Usage of automation tools to take standard operating procedures and turns them into digital	4.1.1.4			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification**.						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
		playbooks to accelerate investigation, enrichment, hunting, containment and remediation.				
	6.	Orchestrate – The ability to plug in and connect everything that is inside and outside of your SOC.	4.1.1.5			
	7.	Recommend – The ability of the platform powering the SOC to tell the analysts what to do next by making a recommendation.	4.1.1.6			
	8.	Investigate – Investigation requires detailed, precise analysis with the assistance of intuitive security tools which can prioritize what needs to be investigated.	4.1.1.7			
	9.	Collaborate- to collaborate and connect the tools, people, process and automation into a transparent workplace, bringing information, ideas and data to the	4.1.1.8			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification**.						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
		forefront and enabling security teams to better collaborate.				
	10.	Manage – The ability to arm security teams with everything necessary to manage the response process when incidents have happened.	4.1.1.9			
	11.	Report – Having the right reporting tools helps inform on what's performing, so security teams can accurately measure where they are and where they need to go	4.1.1.10			
Correlation, Security Monitoring, Data Aggregation and Alerts	12.	The platform used by bidder collects and aggregates data from security systems and network devices, routers, switches, servers, and endpoints.	4.1.2			
	13.	The platform also links events and related data into security incidents, threats or forensic findings, analyses	4.1.2			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
		events and sends alerts to notify security staff of immediate issues.				
	14.	The bidder is to state which SIEM and SOAR the bidder is using for the provision of the service.	4.1.2			Name of SIEM andSOAR SIEM:_____ SOAR:_____
Search, Data Exploration, Dashboards, Reporting and Forensic Analysis	15.	The platform must be able to search vast amounts of security data without reviewing raw data and without data science expertise, active explore data to discover patterns and hunt for threats, create and schedule reports on important data points	4.1.3			
	16.	The Electoral Commission must have remote access to the dashboards (whether on premises or bidder's	4.1.6			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
		premises) created to let staff review event data, identify patterns and anomalies				
	17.	Event Data on the platform can be used for Forensic Analysis and investigations	4.1.7			
	18.	POPIA Compliance reports can be generated from the platform. i.e. The platform can store log data according to POPIA standards.	4.1.9			
UEBA, Threat Intelligence and Hunting	19.	The platform combines internal data from all the sources (switches, routers, servers, endpoints etc.) within the Electoral Commission with third-party threat intelligence feeds on threats and vulnerabilities.	4.1.4			
	20.	The platform uses User Behaviour Analytics tools to detect anomalies not only the users on the network, but	4.1.10			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification**.						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
		also routers, switches, servers and endpoints in that network				
	21.	The platform provides visibility and situational awareness of the Electoral Commission's environment by identifying and investigating cyber-attacks and correlating events across multiple sources to identify indicators of attack.	4.1.4			
	22.	The platform used by the bidder enables security staff to run queries on log and event data, and freely explore data to proactively uncover threats.	4.1.4			
	23.	Once a threat is discovered, the platform automatically pulls in relevant evidence for investigation.	4.1.4			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification**.						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
	24.	The platform also helps security teams identify and respond to security incidents automatically, bringing in all relevant data rapidly and providing decision support.	4.1.4			
Advanced Analytics	25.	The platform uses statistical models and machine learning to:	4.1.5			
	26.	identify anomalies and detect advanced threats,	4.1.5			
	27.	detect unknown threats,	4.1.5			
	28.	detect lateral movements within the network,	4.1.5			
	29.	and enrich the context of security alerts to make it easier to investigate and detect threats	4.1.5			
Vulnerability and Compliance Management	30.	The service includes regular scans on the network to identify vulnerabilities and incorrectly configured systems.	4.1.12			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
	31.	The findings reports are analysed and prioritized by the SOC experts who also help to resolve any detected vulnerabilities..	4.1.12			
	32.	The scans include cyber-security war games.	4.1.12			
Attack Surface Monitoring	33.	The service includes early warning of any malicious activity targeted at the Electoral Commission to enable fast detection and mitigation	4.1.13			
	34.	The service includes adversary's view of the Electoral Commission's digital attack surface and prioritizes risks and exposures	4.1.13			
Incident Response Plan	35.	The successful bidder shall integrate their platform into the Electoral Commission's HelpDesk environment in a way that calls can be logged on both systems	4.1.14			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
	36.	The successful bidder shall assist the Electoral Commission in further developing its cybersecurity incident response plan and mechanisms of testing the plan during the course of the contract.	4.1.16			
Accreditation and Certification	37.	The bidder's SOC has accreditation certification. Please attach a copy of the certificate	4.1.15			
Implementation	38.	The bidder will assist to fine-tune the tools below so that the required information can be obtained from the SIEM i. SIEM ii. Endpoint Detection and Response (EDR) iii. Firewalls and IPSs iv. Remote and on-premises DDOS v. Web Application Firewalls vi. Antivirus Solution vii. Patch Management viii. Vulnerability Management Tools ix. Email Security Tools	4.2			

Technical Bid Response Sheet **Completion of this technical response sheet by the bidder is compulsory.** **Bidder must respond to each and every item in the response sheet to indicate compliance** **Failure to complete and submit this technical bid response sheet as part of the bid submission shall lead to disqualification.**						
		Compliance Minimum Requirements	**Reference**	**Bidder must indicate whether they COMPLY (Yes) or NOT (No)**		**Bidder to substantiate their Compliance choice by either providing more information or referencing a document with more information**
				Yes	**No**	
	39.	The bidder has a SIEM and SOAR environment at the remote SOC	4.2.2.9			
	40.	The bidder will a Health Check on the Electoral Commission's environment	4.2.2.10			
	41.	The bidder will integrate their SIEM and SOAR environment to the SIEM environment at the Electoral Commission.	4.2.2.11			
	42.	Remote access to the Electoral Commission's "tenant" at the bidder's environment will be allowed	4.2.2.12			
Data Confidentiality and Privacy Requirements	43.	The bidder undertakes to agree and comply will the Electoral Commission's requirements on data protection and confidentiality of information, as stated in 9 of this bid specification	9			

20 Appendix B: PRICING SCHEDULE

Detailed Pricing Schedule **Completion of this Price Breakdown response sheet by the bidder is compulsory. All prices must be inclusive of VAT** **Bidder must respond to each and every item in the response sheet. Where there are no quantities, bidder should indicate the quantities.** **Failure to complete and submit this pricing schedule sheet as part of the bid submission shall lead to disqualification.**					
	Category	**Description**	**Quantity**	**Monthly Unit Costs Inclusive of VAT**	**Total Costs Inclusive of VAT**
1.	**Preparatory Work**	a) Health check of the Electoral Commission's Environment b) Fine-Tuning of the Electoral Commission's tools c) Integration of Electoral Commission's SIEM into the bidder's SIEM andSOAR	1		R
2.	**SOC / MDR Services**	a) Provision of Parallel SOC Services on a 24/7 basis for a period of 12 months (months 1 – 12) b) Vulnerability Assessments every 6 months	12	R	R
3.	**SOC /MDR Services**	a) Provision of Parallel SOC Services on a 24/7 basis for a period of 12 months (months 13 – 24) b) Vulnerability Assessments every 6 months	12	R	R

Detailed Pricing Schedule

Completion of this Price Breakdown response sheet by the bidder is compulsory. All prices must be inclusive of VAT
Bidder must respond to each and every item in the response sheet. Where there are no quantities, bidder should indicate the quantities.
Failure to complete and submit this pricing schedule sheet as part of the bid submission shall lead to disqualification.

	Category	Description	Quantity	Monthly Unit Costs Inclusive of VAT	Total Costs Inclusive of VAT
4.	**SOC /MDR Services**	a) Provision of Parallel SOC Services on a 24/7 basis for a period of 12 months (months 25 – 36) b) Vulnerability Assessments every 6 months	12	R	R
5.	**Any other Hardware Rental or Software license (s) for 36 months** **(Bidder to specify)**	a)			
SUB-TOTALS				R	R
TOTAL BID PRICE ***The total bid price is the bid price that must be placed on eProcurement (auction). No any other additional costs will be accepted for bid evaluation and adjudication purposes.**					R……

21 Appendix C: Guideline Reference Table

Reference #1

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Products utilised	
	Services Provided	
Service Value	Contract Value (estimate)	
	Was the service provided in the last 36 months?	

Reference #2

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Products utilised	
	Services Provided	
Service Value	Contract Value (estimate)	
	Was the service provided in the last 36 months?	

Reference #3

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Products utilised	
	Services Provided	
Service Value	Contract Value (estimate)	
	Was the service provided in the last 36 months?	

Reference #4

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Products utilised	
	Services Provided	
Service Value	Contract value (estimate)	
	Was the service provided in the last 36 months?	

Reference #5

EACH REFERENCE MUST CONTAIN THE FOLLOWING DETAILS:		
Customer name		
Contact Person		
Contact Details	Email	
	Telephone	
	Physical address	
Service Description	Products utilised	
	Services Provided	
Service Value	Contract Value (estimate)	
	Was the service provided in the last 36 months?	

22 Appendix D: Skills Matrix Table

	Resource Name	Role	Experience in Years in the role	Capability (e.g. Incident Triage, Analysis and Response; Cyber Threat Intelligence, Hunting and Analytics; Vulnerability Management; SOC Tools Configuration; SOC Operations Management etc.)
1.				
2.				
3.				
4.				
5.				
6.				
7.				

	Resource Name	Role	Experience in Years in the role	Capability (e.g. Incident Triage, Analysis and Response; Cyber Threat Intelligence, Hunting and Analytics; Vulnerability Management; SOC Tools Configuration; SOC Operations Management etc.)
8.				
9.				
10.				

23 Appendix E: Evaluation Criteria

Bidders are advised to refer to Appendix E to ensure that they have addressed all critical bid requirements which will be used for assessing the bids. Bidders are NOT expected to complete and submit this section.

23.1 Stage 1: Assessment of Bidder's Disclosure

All bids received will be evaluated and assessed in respect of the mandatory information provided in the Bidder's Disclosure (SBD4) as well as the register for restricted suppliers and tender defaulters.

Any potential issues that may arise or transgressions that may identified will be pursued in accordance with statutory obligations and requirements.

In this regard, the following must be noted:

23.1.1 The Electoral Commission must, as part of its supply chain management (SCM) processes, identify and manage all potential conflicts of interest and other disclosures made by a person participating in procurement process to enable the accounting officer or delegated authority to make informed decisions about the person participating in the SCM process.

23.1.2 As such, the Bidders Disclosure form, issued as Standard Bidding Document (SBD) 4, is attached herewith for all entities who participate in the bid process.

23.1.3 As part of the evaluation of the procurement process, the information provided by a person on the SBD4 form must be evaluated.

23.1.4 In so doing, it must be noted that if the bid evaluation establishes that:

(a) a person within the bidding entity is an employee of the State, the Electoral Commission's CEO must request the relevant accounting officer/accounting authority whether the person-

(i) Is prohibited from conducting business with the State in terms of Section 8 of the Public Administration Management Act, 2014; or

(ii) has permission to perform other remunerative work outside of their employment, where the PAMA does not apply to such employee;

(b) the conduct of a person constitutes a transgression of the Prevention and Combating of Corrupt Activities Act, 2004;

(c) the conduct of a person constitutes a transgression of the Competition Act, 1998, the conduct must be reported to the Competition Commission; and

(d) the conduct of a person must be dealt with in terms of the prescripts applicable to the Electoral Commission.

23.1.5 If it is established that a person has committed a transgression in terms of the above, or any other transgression of SCM prescripts, the bid may be rejected and the person may be restricted.

23.1.6 The Electoral Commission's CEO must inform National Treasury of any action taken against a person within 30 days of implementing the action.

23.1.7 During the bid evaluation process, the Electoral Commission must in addition to other due diligence measures, establish if a person is not listed in-

(a) the Register of Tender Defaulters; and

(b) the list of restricted suppliers.

23.1.8 A bid related to a restricted bidder or tender defaulter shall be rejected.

23.1.9 The under-mentioned assessment criteria will be used to evaluate the elements relating to SBD4, CSD registration, tax compliance, restricted suppliers and tender defaulters:

	Assessment Criteria	**Bidder Requirement (YES/NO)**	**Comments**
1.	Bidder is registered on the National Treasury Central Supplier Database (CSD). *		
2.	Bidder is tax compliant. **		
3.	The bidder is not an employee of the state.		
4.	Having certified the SBD4, it is accepted that the bidder's conduct does not constitute a		

	Assessment Criteria	Bidder Requirement (YES/NO)	Comments
	transgression of the Prevention and Combating of Corrupt Activities Act.		
5.	Having certified to the SBD4, it is accepted that the bidder's conduct does not constitute a transgression of the Competition Act.		
6.	The bidder is not a tender defaulter as per the register published on the National Treasury website.		
7.	The bidder is not a restricted supplier as per the register published on the National Treasury website.		

* No bid shall be accepted if a supplier is not registered on the National Treasury Central Supplier Database (CSD).

** A bidder must be tax compliant before a contract is awarded. A bid will be disqualified if the bidder's tax affairs remains non-compliant as per the provisions of National Treasury Instruction No 09 of 2017/2018 Tax Compliance Status Verification.

23.2 Stage 2: Key Qualifying Criteria

Stage 2 – Key Qualifying Criteria				
Failure to comply with any of the requirements below will result in the bid being disqualified				
No.	**Description**	**Yes**	**No**	**Comments**
1.	Did the bidder place their bid online as per 6.1			
2.	Did the bidder complete and submit Appendix A: Technical Specification as per 6.2?			
3.	Did the bidder complete and submit Appendix B: Pricing Schedule as per 10.1?			
4.	Did the bidder submit five (5) contactable references as per 6.3?			
5.	Did the bidder submit a profile / letter showing experience as per 6.4?			
6.	Did bidder submit a Skills Matrix as per 6.7?			
7.	Did the bidder include at least one (1) SOC certification as per 4.1.15?			
8.	Bidder has included an example Incident Response Plan as per 6.8			
Overall Stage 2 Outcomes:	**Assessment Comments:**			
	Bid qualifies for further consideration: (YES/NO):			

23.3 Stage 3: Technical Evaluation

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
SOC Management	1.	The bidder must have skill, experience and technological systems and tools to be able to deliver on the following capabilities:	4.1.1			
	2.	Ingest – All data to determine security relevance. The ability to ingest data from any source, structured or unstructured, at scale and the ability to organize that data to make it actionable by machine or human.	4.1.1.1			
	3.	Detect – The ability to detect security event.	4.1.1.2			
	4.	Predict – The ability to predict a security event allows the SOC to proactively escalate the incident to a human or to streamline a response with a predefined process.	4.1.1.3			
	5.	Automate – Usage of automation tools to take standard operating procedures and turns them into digital playbooks to accelerate investigation, enrichment, hunting, containment and remediation.	4.1.1.4			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
	6.	Orchestrate – The ability to plug in and connect everything that is inside and outside of your SOC.	4.1.1.5			
	7.	Recommend – The ability of the platform powering the SOC to tell the analysts what to do next by making a recommendation.	4.1.1.6			
	8.	Investigate – Investigation requires detailed, precise analysis with the assistance of intuitive security tools which can prioritize what needs to be investigated.	4.1.1.7			
	9.	Collaborate- to collaborate and connect the tools, people, process and automation into a transparent workplace, bringing information, ideas and data to the forefront and enabling security teams to better collaborate.	4.1.1.8			
	10.	Manage – The ability to arm security teams with everything necessary to manage the response process when incidents have happened.	4.1.1.9			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
	11.	Report – Having the right reporting tools helps inform on what's performing, so security teams can accurately measure where they are and where they need to go	4.1.1.10			
Correlation, Security Monitoring, Data Aggregation and Alerts	12.	The platform used by bidder collects and aggregates data from security systems and network devices, routers, switches, servers, and endpoints.	4.1.2			
	13.	The platform also links events and related data into security incidents, threats or forensic findings, analyses events and sends alerts to notify security staff of immediate issues.	4.1.2			
	14.	The bidder is to state which SIEM and SOAR the bidder is using for the provision of the service.	4.1.2			Name of SIEM andSOAR SIEM:_____ SOAR:_____

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
Search, Data Exploration, Dashboards, Reporting and Forensic Analysis	15.	The platform must be able to search vast amounts of security data without reviewing raw data and without data science expertise, active explore data to discover patterns and hunt for threats, create and schedule reports on important data points	4.1.3			
	16.	The Electoral Commission must have remote access to the dashboards (whether on premises or bidder's premises) created to let staff review event data, identify patterns and anomalies	4.1.6			
	17.	Event Data on the platform can be used for Forensic Analysis and investigations	4.1.7			
	18.	POPIA Compliance reports can be generated from the platform. i.e. The platform can store log data according to POPIA standards.	4.1.9			
	19.	The platform combines internal data from all the sources (switches, routers, servers, endpoints etc.)	4.1.4			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
UEBA, Threat Intelligence and Hunting		within the Electoral Commission with third-party threat intelligence feeds on threats and vulnerabilities.				
	20.	The platform uses User Behaviour Analytics tools to detect anomalies not only the users on the network, but also routers, switches, servers and endpoints in that network	4.1.10			
	21.	The platform provides visibility and situational awareness of the Electoral Commission's environment by identifying and investigating cyber-attacks and correlating events across multiple sources to identify indicators of attack.	4.1.4			
	22.	The platform used by the bidder enables security staff to run queries on log and event data, and freely explore data to proactively uncover threats.	4.1.4			
	23.	Once a threat is discovered, the platform automatically pulls in relevant evidence for investigation.	4.1.4			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
	24.	The platform also helps security teams identify and respond to security incidents automatically, bringing in all relevant data rapidly and providing decision support.	4.1.4			
Advanced Analytics	25.	The platform uses statistical models and machine learning to:	4.1.5			
	26.	identify anomalies and detect advanced threats,	4.1.5			
	27.	detect unknown threats,	4.1.5			
	28.	detect lateral movements within the network,	4.1.5			
	29.	and enrich the context of security alerts to make it easier to investigate and detect threats	4.1.5			
Vulnerability and Compliance Management	30.	The service includes regular scans on the network to identify vulnerabilities and incorrectly configured systems.	4.1.12			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
	31.	The findings reports are analysed and prioritized by the SOC experts who also help to resolve any detected vulnerabilities..	4.1.12			
	32.	The scans include cyber-security war games.	4.1.12			
Attack Surface Monitoring	33.	The service includes early warning of any malicious activity targeted at the Electoral Commission to enable fast detection and mitigation	4.1.13			
	34.	The service includes adversary's view of the Electoral Commission's digital attack surface and prioritizes risks and exposures	4.1.13			
Incident Response Plan	35.	The successful bidder shall integrate their platform into the Electoral Commission's HelpDesk environment in a way that calls can be logged on both systems	4.1.14			
	36.	The successful bidder shall assist the Electoral Commission in further developing its cybersecurity	4.1.16			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
		incident response plan and mechanisms of testing the plan during the course of the contract.				
Accreditation and Certification	37.	The bidder's SOC has accreditation certification. Please attach a copy of the certificate	4.1.15			
Implementation	38.	The bidder will assist to fine-tune the tools below so that the required information can be obtained from the SIEM x. SIEM xi. Endpoint Detection and Response (EDR) xii. Firewalls and IPSs xiii. Remote and on-premises DDOS xiv. Web Application Firewalls xv. Antivirus Solution xvi. Patch Management xvii. Vulnerability Management Tools xviii. Email Security Tools	4.2			
	39.	The bidder has a SIEM and SOAR environment at the remote SOC	4.2.2.9			

Stage 3 – Technical Evaluation – Technical Disqualifying Factors. Failure to comply with any of the requirements below will result in the bid being disqualified						
		Compliance Minimum Requirements	**Reference**	**Bidder's Indication**		**Comments**
				Yes	**No**	
	40.	The bidder will a Health Check on the Electoral Commission's environment	4.2.2.10			
	41.	The bidder will integrate their SIEM and SOAR environment to the SIEM environment at the Electoral Commission.	4.2.2.11			
	42.	Remote access to the Electoral Commission's "tenant" at the bidder's environment will be allowed	4.2.2.12			
Data Confidentiality and Privacy Requirements	43.	The bidder undertakes to agree and comply will the Electoral Commission's requirements on data protection and confidentiality of information, as stated in 9 of this bid specification	9			
Overall Stage 3 Outcomes		**Assessment Comments:**				
		Bid qualifies for further consideration: (YES/NO):				

23.4 Stage 4: Technical Scoring

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (56.25/75)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
1.	Relevant Reference	50	References: a) Customer name = 1 point b) Contact Person = 1 point c) Email = 1 point d) Telephone = 1 point e) Physical address = 0.5 point f) Product(s) used = 2 points g) Description of Services provided = 2 points. h) Value (Contract Value Estimate) = 1 point i) Was the service provided in the last 36 months = (YES = 0.5 point) **Total for references = maximum 10 points per reference (5 references)**		

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (56.25/75)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
2.	Relevant Experience	**5**	Experience with SOC. (Max 5 points) a) The bidder has five to seven (5-7) years' experience (3 points). b) The bidder has at eight to ten (8-10) years' experience (4 points). c) Bidder has more than 10 years' experience (5 points)		
3.	Bider's Certifications	**10**	Bidder has included relevant ICT security certificates: a) 5 or more certificates (10 points) b) 4 certificates (8 points) c) 3 certificates (6 points) d) 2 certificates (4 points) e) 1 certificate (2 points)		
4.	Skills Matrix	**15**	Bidder's skills matrix shows the following capabilities (Maximum 10 points) a) Incident Triage, Analysis and Response (2 points)		

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (56.25/75)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
			b) Cyber Threat Intelligence, Hunting and Analytics (2 points) c) Vulnerability Management (2 points) d) SOC Tools configuration (2 points) e) SOC Operations Management (2 points) Bidder has at least 5 people in the SOC at present (5 points)		
5.	Incident Response Plan	5	The bidder's Incident Response Plan includes the following steps at a minimum: a) Detect and Analyse (1 point) b) Contain (1 point) c) Eradicate (1 point) d) Recover (1 point) e) Report and Remediate (1 point)		

Bid Evaluation Criteria Stage 4 – Technical Scoring					
To qualify to the next phase of adjudication a bidder must score a minimum of 75% (56.25/75)					
	Product Description	**Available Score**	**Points Allocation**	**Actual Score**	**Comments**
Overall Stage 4 Outcomes:		**Assessment Comments:**			
		Bid qualifies for further consideration: (YES/NO):			

23.5 Stage 5: Adjudication of Bids

Only bids that comply with the requirements and conditions of the bid and that meet the minimum criteria in the bid evaluation process as stipulated above will be considered for bid adjudication purposes.

Acceptable bids must be market related.

This bid is deemed not to exceed R50 million including VAT.

Therefore, the 80/20 preference point system (PPPFA scoring) in terms of the Preferential Procurement Policy Framework Act, 2005 (PPPFA) and the Preferential Procurement Regulations, 2022 shall apply in the adjudication process of this auction where all acceptable bids received are equal to or below R50 million including VAT. Preference points will be allocated as follows:

B-BBEE Status Level of Contributor	Number of Points
1	20
2	18
3	14
4	12
5	8
6	6
7	4
8	2
Non-compliant contributor	0

Bid Evaluation Committee

	Evaluation Committee Member's Name	Signature
1		
2		
3		
4		
5		

Overall Adjudication Outcomes:

_____

_____

_____

_____