SOUTH AFRICA

Electoral Commission

Bid Specifications

Auction 0010447043

Security Incident and Event Management Solution

IMPORTANT NOTICE

Failure to comply with the completion of the auction conditions and the required information or submission of the required stipulated documents indicated above (i.e. non submission of the required reseller authorisation details and maintenance stipulations) shall invalidate a bid.

1 Introduction

The Electoral Commission seeks to appoint a suitably qualified service provider to supply, install, configure and maintain a Security Incident and Event Management Solution (SIEM). The maintenance period of the proposed SIEM solution will be over a three-year period.

2 Background Information

The Electoral Commission has invested extensively in ICT technologies, which provide a platform to effectively support and enable its business processes and to meet its goal of providing a free and fair election process in an open and transparent environment. The Electoral Commission's ICT Department intends to continue running a highly efficient and stable ICT environment making full use of industry standards, best practices and disciplines based upon stable and reliable technologies.

The Electoral Commission requires a SIEM solution that will provide real-time analysis of security alerts generated by applications and network hardware.

The SIEM solution will be connected to the Storage Area Network for storage and querying of logs collected.

Bidders must place a bid on the Votaquotes (eProcurement) system and then provide all the required documentation before the closing dates as specified in this document and on the Votaquotes web site.

3 Functional Specifications

The functional specification for the required product is as specified below. It must be noted that the functional specifications below are the minimum requirements; the only deviation that may be accepted will be in case where the bidder's specification is better. Anything below specification will be disqualified.

The maintenance period will be for a three-year period from the date of commission.

3.1 Technical Requirements

Bidders must adhere to the specifications stipulated in the table below as part of the submission.

TECHNICAL REQUIREMENTS
a) COLLECTION OF LOGS: The system must be able to collect and read events and security logs from servers running on: • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • VMware (Microsoft server 2003 and 2008 • Linux (Ubuntu,Red Hat ,and Suse)
b) The system must be able to warn with messages or inform if data collection was/is: • Unsuccessful (e.g corrupt/incomplete) • Successful • Busy (Log data collection in progress) • The system must be able to archive collected server log data
c) The system must provide standard of what security and events logs data to be collected for what type of report.
d) EVENTS AND SECURITY LOG: The data must be collected in any of the following forms/format i.e: • ODBC • Logs • Syslogs • NetBIOS • APIs • Plug-ins • SNMP
e) The system must allow for addition, modification and/or deletion of servers from where logs data should or not be collected.
f) The system must provide security access grouping rights with respect to who and what users can access/view from the system i.e.: • IT security compliance administration users (i.e administer system server) • IT management users (i.e IT management team) • IT server administration users (i.e administer IDC servers) • Audit users (i.e for audit staff)
g) The system must be able to collect security and events logs data:

TECHNICAL REQUIREMENTS
• On a periodic basis (e.g. daily at 7am,11 am and 3 pm) • On an ad hoc basis (as and when required)
h) The system must be able to allow for download of data from the IT security compliance server to personal computer.
i) The system must be able to verify the collected/uploaded security and events logs data against the source server log data
The system must be able to log collection of security and events log data.
j) The system must be able to discover and display all servers/devices with their IP addresses and server names that are: • Currently being monitored (collection server log data) • Not being monitored
k) The system must allow for the defined group of people/users, devices/servers, and systems to be monitored and reported.
l) The system must be compatible with the following client/end user system: • Windows 7 • Windows 8 • Windows 10
m) The proposed SIEM must support the following Databases: • Microsoft SQL 2005 • Microsoft SQL 2008 • Microsoft SQL 2010 • Microsoft SQL 2016 • Oracle
n) The system must provide custom security and events logs collection for standard and custom reports
o) The reports from analysed logs must show: • Who did what (User/Processes), • When was it done (Time/Date), • From Where (Locations), • Where to (Locations) and • On What (Objects)

TECHNICAL REQUIREMENTS
• The system reporting must be able to classify as per following grouping types: • Events • Devices & Servers • Processes & Users • Time/Periods • Objects • The system must provide the drill down capability per each event to establish and view: • Severity of the event (severity classification required) • When, What, Where, Who, From Where, To Where, and on What.
p) The system must provide: • Event classes and • Event statuses
q) The system must provide for schedule running of certain reports and notification such email the required (chosen reports)
r) The system must be able to provide presentation of reports in a: • Web based format (compatible with Internet Explorer, Google Chrome and Mozilla Firefox) • Windows based graphical user interface (Irrespective of the underlying reporting tool used)
s) The system must be able to monitor and report on a specific users (user access to IDC systems/assets),servers, and devices with their severity or priority levels.
t) The system must continuously monitor and report on (potential/suspected) security breaches on IT servers (Including systems/software solutions) and devices.
u) The system must allow for new security compliance policies/rules to be created and activated and/or deleted if not required.
v) The system must have standard security compliance policies/rules (with sensitivity or priority) which adhere to the following frameworks and/or industry best practice: • ITIL • COBIT • ISO27002
w) In the event that a user, process, and/or servers or device (through log data analysis) violated security compliance policies/rules depending on the level of sensitivity or priority, the system must alert the authorized user (IT security management) using the following methods: • E-mail

TECHNICAL REQUIREMENTS
• On screen (live from the system) • SNMP traps
x) All hardware must come with three year warranty and all software must be licensed for three years.
y) All proposed systems must come with logging and reporting capabilities: • Local log • Syslog
z) The system must have redundancy (Including failover) and high availability.

4 General Auction Conditions

The following standard auction conditions must be adhered to and complied with, failing of which the bid will be disqualified.

a) Service providers must place bids online on the Electoral Commission's eProcurement website by not later than the stipulated closing date and time on the auction.
b) Technical Requirements must be adhered to as specified in the table in section 3.1.
c) The service provider must be authorised to sell the product supplied.
d) A letter of proof of the reseller agreement either from the OEM or an authorised distributor (i.e. if the reseller is authorised by a distributor). If the reseller agreement is from a distributor, then proof from the OEM authorising the distributor needs to be included.
e) Three-year OEM warranty must be provided together with the bid.
f) Pricing must be firm for a minimum of one hundred and eighty (180) days from close of auction.
g) The service provider is required to provide proof of available local (South African) support for the proposed solution.
h) The bidder must be accredited to configure, install and maintain the proposed solution.
i) The bidder must provide at least three (3) contactable references where the proposed system is installed. These references should be at sites where system has been or is currently installed, configured, deployed and is providing the functionality required as per the table in section 3.1
j) The Electoral Commission will issue a formal purchase order to the successful service provider before any services can be delivered.
k) Delivery of the required product shall only be accepted by the Electoral Commission on the basis of presentation of the service provider's own delivery note. Such notes shall not be substituted by another service provider's delivery notes.
l) Delivery of all the products to be made no later than one (1) month after the issuing of the purchase order.

m) Awarding of the auction to any successful service provider shall be subject to the Electoral Commission's due diligence audit requirements, where applicable.
n) No payment shall be made until full and final delivery has taken place and the product has been confirmed and delivered in accordance with the specifications.

5 Quality Control

The following quality control conditions must be adhered to and complied with, failing of which the bid will be disqualified.

a) The successful bidder will have the primary responsibility of ensuring that the proposed product complies with the required specifications in terms of functionality and technical specification including quantity and quality.
b) The proposed solution must be complete, fully functional and ready for deployment without dependencies on additional equipment, software or components that may be required to make it work.
c) It must be noted that the Electoral Commission seeks to gain the best product technically, functionally and financially, and will select the solution that it deems to give the best investment.
d) Preference will be given to solutions that are based on a standard existing solution in the market and not solutions specifically designed and/or cloned for this bid. The Electoral Commission may require market penetration indicators and references.
e) Upon a successful bid being accepted, the Electoral Commission reserves the right to request an inspection of the preferred service provider's facilities.
f) The successful service provider has the primary responsibility to ensure that quantity and quality are in accordance with the bid specifications.

6 Pricing Requirements

The total bid price must be an all-inclusive price. When pricing bid proposals, service providers are advised to take into account that the following issues are factored into the price. The Electoral Commission will not entertain additional charges on these items.

a) SIEM solution
b) Three-year maintenance
c) Professional services for configuration and installation
d) Delivery costs to the Electoral Commission's national office in Centurion, Gauteng, South Africa.
e) Quoted prices must be firm for a period one hundred and eighty (180) days.
f) Bid price must be submitted online on the eProcurement (Votaquotes) portal.

7 Award of Order

a) The selection process may include short-listing, presentation and demonstration of the products by short-listed potential service providers.
b) A contract/purchase order will be awarded to a bidder whose bid complies with these specifications and in accordance with the terms of the provisions of the Preferential Procurement Policy Framework Act, 2000 and more specifically the Preferential Procurement Regulations, 2017.
c) The Electoral Commission will issue a formal order before any services or products can be delivered.
d) It should be noted that the Electoral Commission seeks to gain the best product technically and financially and will select from the results of the auction a solution it deems to give the best investment.

8 Special Requirements

a. Latest version(s) of software and hardware should be supplied when providing the solution.
b. A standard OEM warranty agreement should be provided to the Electoral Commission stating the terms, conditions and a period

9 Delivery and Implementation Timeframe

a) The successful service provider will be required to complete delivery within one (1) month from receipt of an order for these services.
b) If that is not possible, the bidder must state in the bid conditions and in the written bid submission the reasons and the earliest date that implementation may start and be completed.

10 Written Submissions

All submissions must be received before the closing date and time for submissions, as stipulated on the e-Procurement website https://votaquotes.elections.org.za. Submissions received after the final date and time will lead to bids being disqualified and not considered. Written submissions must be delivered to the Electoral Commission's Procurement and Asset Management Department. Delivery can be through any of the following means, before the closing date and time as stipulated in the auction:

- Uploading on the auction
- Place in the Commission's tender box situated in the foyer of the Electoral Commission's national office in Centurion at the following address:

Election House
Riverside Office Park,
1303 Heuwel Avenue,
Centurion,
0157

Note: Clearly mark your submission: For the attention of Procurement and Asset Management – Auction 0010447043

In addition, the Electoral Commission may also call on bidders to make further submissions and/or presentations in order for the Electoral Commission to ensure full compliance with all its requirements and as part of the auction evaluation process and prior to the conclusion of the adjudication of the auction.

Failure to submit all of the required documentation (See summary list of submission points below) before the closing time will 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.

10.1 Summary List of Submission Requirements

a) Completed the technical response sheet, annexure A.
b) A letter of proof of the reseller agreement either from the OEM or an authorised distributor; (i.e. if the reseller is authorised by a distributor), as per section 4 C & D.
c) Proof of the OEM warranty, as per section 4 E.
d) Proof of available local (South African) support, as per section 4 G.
e) References, as per section 4 I.

11 Closing Date

The closing date and time of this auction will be 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 the closing date and time.

Annexure A – Technical Bid Response Sheet

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
a	COLLECTION OF LOGS: The system must be able to collect and read events and security logs from servers running on: • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • VMware (Microsoft server 2003 and 2008 • Linux (Ubuntu,Red Hat ,and Suse)			
b	The system must be able to warn with messages or inform if data collection was/is: • Unsuccessful (e.g corrupt/incomplete) • Successful • Busy (Log data collection in progress) • The system must be able to archive collected server log data			
c	The system must provide standard of what security and events logs data to be collected for what type of report.			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
d	EVENTS AND SECURITY LOG: The data must be collected in any of the following forms/format i.e: • ODBC • Logs • Syslogs • NetBIOS • APIs • Plug-ins • SNMP			
e	The system must allow for addition, modification and/or deletion of servers from where logs data should or not be collected.			
f	The system must provide security access grouping rights with respect to who and what users can access/view from the system i.e.: • IT security compliance administration users (i.e administer system server) • IT management users (i.e IT management team) • IT server administration users (i.e administer IDC			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
	servers) • Audit users (i.e for audit staff)			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
g	The system must be able to collect security and events logs data: • On a periodic basis (e.g. daily at 7am,11 am and 3 pm) • On an ad hoc basis (as and when required)			
h	The system must be able to allow for download of data from the IT security compliance server to personal computer.			
i	The system must be able to verify the collected/uploaded security and events logs data against the source server log data			
j	The system must be able to discover and display all servers/devices with their IP addresses and server names that are: • Currently being monitored (collection server log data) • Not being monitored			
k	The system must allow for the defined group of people/users, devices/servers, and systems to be monitored and reported.			
l	The system must be compatible with the following client/end user system:			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
	• Windows 7 • Windows 10			
m	The proposed SIEM must support the following Databases: • Microsoft SQL 2005 • Microsoft SQL 2008 R2 • Microsoft SQL 2021 • Microsoft SQL 2014 • Microsoft SQL 2016 • Oracle 12.2 c • Mongo DB			
n	The system must provide custom security and events logs collection for standard and custom reports			
o	The reports from analysed logs must show: • Who did what (User/Processes), • When was it done (Time/Date),			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
	• From Where (Locations), • Where to (Locations) and • On What (Objects) • The system reporting must be able to classify as per following grouping types: • Events • Devices & Servers • Processes & Users • Time/Periods • Objects • The system must provide the drill down capability per each event to establish and view: • Severity of the event (severity classification required) • When, What, Where, Who, From Where, To Where, and on What.			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
p	The system must provide: • Event classes and • Event statuses			
q	The system must provide for schedule running of certain reports and notification such email the required (chosen reports)			
r	The system must be able to provide presentation of reports in a: • Web based format (compatible with Internet Explorer, Google Chrome, Edge and Mozilla Firefox) • Windows based graphical user interface (Irrespective of the underlying reporting tool used)			
s	The system must be able to monitor and report on a specific users (user access to IDC systems/assets),servers, and devices with their severity or priority levels.			
t	The system must continuously monitor and report on (potential/suspected) security breaches on IT servers (Including systems/software solutions) and devices.			
u	The system must allow for new security compliance policies/rules to			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
	be created and activated and/or deleted if not required.			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
v	The system must have standard security compliance policies/rules (with sensitivity or priority) which adhere to the following frameworks and/or industry best practice: • ITIL • COBIT • ISO27002			
w	In the event that a user, process, and/or servers or device (through log data analysis) violated security compliance policies/rules depending on the level of sensitivity or priority, the system must alert the authorized user (IT security management) using the following methods: • E-mail • On screen (live from the system) • SNMP traps			
x	All hardware must come with three year warranty and all software must be licensed for three year.			
y	The system must come with logging and reporting capabilities:			

Completion of this technical response sheet by responding to each item is compulsory. Failure to complete and submit this technical bid response sheet shall lead to disqualification.				
	Technical Requirements	**Bidder must indicate whichever is applicable**		**Bidder's response/technical specification for proposed solution – as per OEM specification**
		Yes	**NO**	
	• Local log • Syslog			
Z	The system must redundancy (Including failover) and high availability.			

BID EVALUATION SHEET
Auction 0010447043
Security Incident and Event Management Solution

Service Provider:	
Date of Bid Evaluation:	

Phase 1 - Disqualifying Factors- Failure to adhere to one of the below will result in bid being disqualified			
No.	**Description**	**Yes/No***	**Comments**
1	Completed the technical response sheet, annexure A.		
2	A letter of proof of the reseller agreement either from the OEM or an authorised distributor; (i.e. if the reseller is authorised by a distributor). If the reseller agreement is from a distributor, then proof from the OEM authorising the distributor needs to be included, as per section 4 C & D, provided?.		
3	Proof of the OEM warranty, as per section 4 E, provided?.		
4	Proof of available local (South African) support, as per section 4 G, provided?.		
5	References, as per section 4 H, provided?		

Result of phase 1: Bid qualifies/does not qualify for further consideration.

Phase 2 – Technical Evaluation – Technical Disqualifying Factors		
Failure to comply with any of the requirements below will result in the bid being disqualified		
TECHNICAL REQUIREMENTS	**Confirm Compliance**	
	Yes	**No**
a) COLLECTION OF LOGS: The system must be able to collect and read events and security logs from servers running on: • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • VMware (Microsoft server 2003 and 2008 • Linux (Ubuntu,Red Hat ,and Suse)		
b) The system must be able to warn with messages or inform if data collection was/is: • Unsuccessful (e.g corrupt/incomplete) • Successful		

• Busy (Log data collection in progress) • The system must be able to archive collected server log data		
c) The system must provide standard of what security and events logs data to be collected for what type of report.		
d) Events and security log: The data must be collected in any of the following forms/format i.e: • ODBC • Logs • Syslogs • NetBIOS • APIs • Plug-ins • SNMP		
e) The system must allow for addition, modification and/or deletion of servers from where logs data should or not be collected.		
f) The system must provide security access grouping rights with respect to who and what users can access/view from the system i.e.: • IT security compliance administration users (i.e administer system server) • IT management users (i.e IT management team) • IT server administration users (i.e administer IDC servers) • Audit users (i.e for audit staff)		
g) The system must be able to collect security and events logs data: • On a periodic basis (e.g. daily at 7am,11 am and 3 pm • On an ad hoc basis (as and when required)		
h) The system must be able to allow for download of data from the IT security compliance server to personal computer.		
i) The system must be able to verify the collected/uploaded security and events logs data against the source server log data		
j) The system must be able to discover and display all servers/devices with their IP addresses and server names that are: • Currently being monitored (collection server log data) • Not being monitored		
k) The system must allow for the defined group of people/users, devices/servers, and systems to be monitored and reported.		
l) The system must be compatible with the following client/end user system: • Windows 7		

• Windows 10		
m) The proposed SIEM must support the following Databases: • Microsoft SQL 2008 R2 • Microsoft SQL 2021 • Microsoft SQL 2014 • Microsoft SQL 2016 • Oracle 12.2 c • Mongo DB		
n) The system must provide custom security and events logs collection for standard and custom reports		
o) The reports from analysed logs must show: • Who did what (User/Processes), • When was it done (Time/Date), • From Where (Locations), • Where to (Locations) and • On What (Objects) • The system reporting must be able to classify as per following grouping types: • Events • Devices & Servers • Processes & Users • Time/Periods • Objects • The system must provide the drill down capability per each event to establish and view: • Severity of the event (severity classification required) • When, What, Where, Who, From Where, To Where, and on What.		
p) The system must provide: • Event classes and • Event statuses		
q) The system must provide for schedule running of certain reports and notification such email the required (chosen reports)		
r) The system must be able to provide presentation of reports in a: • Web based format (compatible with Internet Explorer, Google Chrome, Edge and Mozilla Firefox) • Windows based graphical user interface (Irrespective of the		

underlying reporting tool used)		
s) The system must be able to monitor and report on a specific users (user access to IDC systems/assets), servers, and devices with their severity or priority levels.		
t) The system must continuously monitor and report on (potential/suspected) security breaches on IT servers (Including systems/software solutions) and devices.		
u) The system must allow for new security compliance policies/rules to be created and activated and/or deleted if not required.		
v) The system must have standard security compliance policies/rules (with sensitivity or priority) which adhere to the following frameworks and/or industry best practice: • ITIL • COBIT • ISO27002		
w) In the event that a user, process, and/or servers or device (through log data analysis) violated security compliance policies/rules depending on the level of sensitivity or priority, the system must alert the authorized user (IT security management) using the following methods: • E-mail • On screen (live from the system) • SNMP traps		
x) All hardware must come with three year warranty and all software must be licensed for three year.		
y) All proposed systems must come with logging and reporting capabilities: • Local log • Syslog		
z) The system must have redundancy requirements (Including failover) and high availability.		

Result of phase 2: Bid qualifies/does not qualify for further consideration

Phase 3 - Evaluation Based on the 80/20 Preference Point System (PPPFA Scoring)
Only bids that comply with the requirements and conditions of the tender and that meet the minimum criteria in the bid evaluation process as stipulated above will be considered for bid adjudication purposes. Adjudication of qualifying bids will be done in accordance with the 80/20 preference point system provided for in the Preferential Procurement Regulations, 2017. Pre-scoring of bids on the eProcurement system is illustrative only in respect of the potential outcome of the tender and serves to enhance transparency in the bidding process as well as to encourage competitive bidding and B-BBEE compliance. Qualifying bids will be scored in the final PPPFA scoring to conclude the bid evaluation process and final price and total bid points may change accordingly. The ranking of the qualifying bids in terms of the scoring will be confirmed. The order of ranking of the qualifying bids will, however, remain the same since price, B-BBEE status levels and preference points claimed will not change once the tender has closed.

Bid Evaluation Committee

	Name	Signature
1		
2		
3		
4		
5		