Independent Communications Authority of South Africa
350 Witch-Hazel Avenue, Eco Point Office Park
Eco Park, Centurion
Private Bag X10, Highveld Park 0169

Appointment of a service to provide a Security Information and Event Management (SIEM) solution for a period of three (03) years on an 80/20 PPPFA 2000, Preferential Procurement Regulation: 2017

1. Background

Security Information and Event Management (SIEM) solutions are defined by the need to analyze event data in real time for the early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response, forensics and regulatory compliance.

The SIEM system will be installed at ICASA Head Office with the capability to collect and monitor system events at ICASA head office as well as all regional offices. Currently the number of event sources are 160, this includes servers, switches, firewalls, databases and security appliances at head office and regional offices.
The SIEM solution will provide IT with the following capability:

Data aggregation: Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
Correlation: Looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information.
Alerting: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues.

Dashboards: Tools can take event data and turn it into informational charts to assist in seeing patterns or identifying activity that is not forming a standard pattern.
Compliance: Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.
Retention: employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. Long term log data retention is critical in forensic investigations.
Forensic analysis: The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands of logs.

2. Terms of Reference

Please refer to Annexure A for the Terms of Reference for the SIEM solution.

3. Period of Assignment

All work is to be carried out in accordance with the time schedule as agreed with ICASA. The services are required for 3 (three) years starting in October 2019.

4. Briefing Session

There will be a compulsory briefing session before the closing date.

5. Bid Evaluation

The bid will be advertised for a period of 21 working days in the e-portal as well as the Government Tender Bulletin on an 80/20 procurement principle.

Bidders will be evaluated on;
a) submission of the required documents,
b) functionality and
c) price/BB-BEE.

Only bidders who meet the cut-off score of 80 points out of 100 points for functionality will be considered further for price evaluation. All bid proposals submitted will be evaluated in accordance with the 80/20 procurement principle as prescribed by National Treasury Regulations.

Meets the FUNCTIONAL requirements as per the scope of work, Annexure A, Section 4 — **40**

No	Functionality	Score
1	Meets 20 or more functional requirements with explanations for each item	5
2	Meets 20 or more functional requirements with no explanation	4
3	Meets 17-19 or more functional requirements	3
4	Meets 14-16 or more functional requirements	2
5	Meets 13 or less functional requirement	1

Meets the REPORTING requirements as per the scope of work, Annexure A, Section 5 — **30**

No	Functionality	Score
1	Meets ALL 5 reporting requirements with explanations for each item	5
2	Meets all 5 reporting requirements with no explanation	4
3	Meets 4 reporting requirements	3
4	Meets 3 reporting requirements	2
5	Meets only 0-2 reporting requirements	1

Experience and proven track record with SIEM technology — **30**

No	Functionality	Score
1	Service provider can demonstrate that they have been supporting SIEM solutions and Security Operations Centre for 4+ years by providing reference letter showing that they provided SIEM and SOC support for 4+ years.	5
2	Service provider can demonstrate that they have been supporting SIEM solutions and / or Security Operations Centre for 3+ years by providing	4

		reference letter showing that they provided SIEM support for 3+ years.		
	3	Service provider can demonstrate that they have been supporting SIEM solutions and / or Security Operations Centre for 2+ years by providing reference letter showing that they provided SIEM support for 2+ years.	3	
	4	Service provider can demonstrate that they have been supporting SIEM solutions for 1+ years by providing reference letter showing that they provided SIEM support for 1+ years.	2	
	5	Service provider can demonstrate that they have been supporting SIEM solutions for less than 1 year by providing reference letter showing that they provided SIEM support for less than a year.	1	
TOTAL				**100**

Only bidders who passed the threshold of **80/100** for functionality will be evaluated further for price.

Annexure A – Terms of Reference

Appointment of a service provider to provide a Security Information and Event Management (SIEM) solution the Authority. The solution should include training for ICASA resources, licensing, software and hardware maintenance and support over a period of 3 (three) years.

1. SUMMARY OF ENVIRONMENT

The ICT environment consists primarily of Windows and Linux servers with SQL and Oracle databases, Cisco devices and other network security appliances totalling approximately 160 event sources.
Further sizing, storage and event rate information will be made available at the compulsory briefing session.

2. MANDATORY REQUIREMENTS

#	Requirement
1	Provide evidence to demonstrate that your organisation adheres to good IT governance practises and complies with information security and privacy best practises. Examples ISO 27001, COBIT, FISMA, POPI, HIPAA, SOX
Comment:	
2	Provide on-going system training / familiarisation for ICASA IT resources using the SIEM solution (skills transfer for max 3 IT resources)
Comment:	

3	Provide all software updates and required patches for the SIEM solution for the duration of the contract (at least at the N -1 Level).
Comment:	
4	Provide service level agreement (SLA) hours over the 3-year period for the support of the SIEM solution
Comment:	

IF THE MANDATORY REQUIREMENTS ARE NOT MET THEN BIDDER WILL BE DISQUALIFIED

3. FUNCTIONAL REQUIREMENTS

The service provider will be required to provide a solution that satisfies the following requirements:

*All requirements should be addressed in proposal

#	**Requirements**
1	Focuses on combining event data from disparate sources to assist with the identification of any suspicious activity and policy violations for the Authority's ICT environment.

Comply	Yes	No
Please explain how this requirement is met:		

2	Performs real-time monitoring (24 X 7 X 365) of event data generated by workstations, network devices, security appliances, servers, databases and applications.

Comply	Yes	No
Please explain how this requirement is met:		

3	Contains a correlation engine to identify and detect patterns across the ICT environment with basic predefined correlation rules available at set-up to start analysing and correlating activity out-of-the-box that reduces false-positives automatically, detects authentication failures and operational events in real-time without the need to specify particular device types.

Comply	Yes	No
Please explain how this requirement is met:		

4	Can perform behaviour profiling to identify anomalies and deviations from normal behaviour.

Comply	Yes	No
Please explain how this requirement is met:		

5	Is user aware, i.e. identify the actual user of the source or destination, preferably through an Active Directory (AD) connection.

Comply	Yes	No
Please explain how this requirement is met:		

6	Service provider has a security operations centre (SOC) that is managed 24X7

Comply	Yes	No
Please explain how this requirement is met:		

7	Provides an agent-less solution that can automatically scan network for the list of servers to be monitored and will automatically accept events and start to monitor devices without any administrator intervention. There should also be an option to install an agent.

Comply	Yes	No
Please explain how this requirement is met:		

8	Can retrofit virtually any application with logging capability that may not already be available and also provide a native out of the box capability to collect application log data from custom/in-house developed web applications, without explicit custom parser development.

Comply	Yes	No
Please explain how this requirement is met:		

9	Guarantees delivery of events to the log management system and that no events will get lost if the log management system is unavailable, even if the license has been exceeded, the solution must not drop incoming events.

Comply	Yes	No
Please explain how this requirement is met:		

10	Provides inline options to reduce event data at the source by aggregating event data. Aggregation must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows.

Comply	Yes	No
Please explain how this requirement is met:		

11	Includes a module that can be used to provide compliance auditing, alerting and reporting for governances such as National Institute of Standards and Technology (NIST) Special Publication 800-53 and ISO/IEC 27002.

Comply	Yes	No
Please explain how this requirement is met:		

12	Natively integrate with existing authentication directories to import context related to users and roles which will then correlate and attribute every event to an actual user, regardless of the event source and be able to alert or report on any activity for identities not automatically synchronized with authentication directories.

Comply	Yes	No
Please explain how this requirement is met:		

13	Define whitelist/blacklists that can be used as inclusion or exemption during the correlation process. The correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, session tracking, attack history and privileged system access.

Comply	Yes	No
Please explain how this requirement is met:		

14	Is capable of discovering patterns of subverted activities that would otherwise go unnoticed, i.e. slow and low attacks.

Comply	Yes	No
Please explain how this requirement is met:		

15	Provide the ability to import context and keep an inventory of all data as it relates to assets like hostname, IP & MAC address, business purpose, owner,

	vulnerability data, exemptions, compliance, criticality and other business-related data. The asset inventory must be able to integrate with vulnerability scanners to keep asset information up to date.

Comply	Yes	No
Please explain how this requirement is met:		

16	Is able to map IT Assets to Business Functions, and report on the Business Risk in the form of heat maps, reports, and scores against Key Performance Index (KPI).

Comply	Yes	No
Please explain how this requirement is met:		

17	Is capable of correlating activity between enterprise users and source code repositories. Users accessing repositories that are not developers or developers that are extracting sensitive intellectual property from the systems must be detected and alerted upon in real-time.

Comply	Yes	No
Please explain how this requirement is met:		

18	Is capable of allowing the restoration of a year's worth of historical log files to perform complex pattern searches and reporting against terabytes of data in a

	short period of time. The entire process from restoring the data to reporting results must take less than two days.

Comply	Yes	No
Please explain how this requirement is met:		

19	Provides the ability to visually represent event data into a dynamically updated graph to assist staff in determining the expanse of attacks and pinpoint the original attacker during incident response and remediation.

Comply	Yes	No
Please explain how this requirement is met:		

20	Provides out-of-the-box real-time detection and response capabilities on communications with known malicious hosts such as botnet and/or other hosts on the Internet known to host/facilitate data exfiltration by malwares.

Comply	Yes	No
Please explain how this requirement is met:		

21	Is capable of triggering scripts or execute integration commands with third-party solutions, Next Generation Intrusion Prevention systems in order to quarantine or block malicious activity in real-time.

Comply	Yes	No
Please explain how this requirement is met:		

22	Is capable of monitoring several databases in different servers and generates daily, weekly reports alerting of activities taking places within SQL and oracle database environments to mitigate against malicious acts such as SQL injection attacks and unauthorized activities by administrators.

Comply	Yes	No
Please explain how this requirement is met:		

4. REPORTING REQUIREMENTS

1	Capable of producing reports that monitor activities of IT administrators and report on their activities within servers hosting services such as Active directory.

Comply	Yes	No
Please explain how this requirement is met:		

2	Be able to produce daily reports of all activities within the network for a 24-hour period covering aspects such as:

	Malware & Anti-virus activities. Suspicious traffic to malicious sites or using backdoor or Torrent ports Perimeter Security scans and exploits. AD security correlated events- Failed and Lockout accounts including service accounts, multiple host logging from single AD account, Brute force attempts from a single source. Correlated internal reconnaissance events, horizontal scans. Database activity monitoring.

Comply	Yes	No
Please explain how this requirement is met:		

3	Be able to produce weekly reports of all activities within core servers: Weekly Active Directory activities report. Weekly Linux operating system report showing all login activities. Weekly Windows OS server activities showing all login activities. Weekly SQL and Oracle database activity reports.

Comply	Yes	No
Please explain how this requirement is met:		

4	Be able to produce alerts for the following incident: Active Directory group policy violation change. Firewall rules changes. Suspicious traffic to malicious sites. Attempt to remove endpoint security protection clients. Malware/virus not removed by endpoint security protection client. Network exploit attempts and NIPS violation from McAfee endpoint protection.

Comply	Yes	No
Please explain how this requirement is met:		

5	Be able to produce Monthly security overview report showing aspect such as: Monthly Risk rating and three-month trend security posture. Malware overview report based on McAfee endpoint protection. Top account login failures. Top account lockouts. TOR/Back-door traffic overview Perimeter security overview Overview of incident reported during the month and SLA monthly report

Comply	Yes	No
Please explain how this requirement is met:		