

**THE APPOINTMENT OF A SERVICE PROVIDER TO IMPLEMENT A FULLY MANAGED VULNERABILITY MANAGEMENT AND SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) SOLUTION FOR CEF OVER A PERIOD OF THREE (3) YEARS.**

**1. Evaluation Criteria**

**1.1 PHASE 1**

**Administrative Evaluation Criteria**

**Initial Screening Process:** At this phase bidder's response are reviewed to check if bidders have responded according to CEF (SOC) Ltd RFP document.

**1.2 PHASE 2: TECHNICAL EVALUATION**

**1.2.1 MANDATORY REQUIREMENTS**

Description	Comply	Not comply
1.2.1.1 The bidder must submit a valid ISO 27002 standard certificate or an equivalent		
Substantiate (if necessary) and provide relevant proof		
1.2.1.2 The bidder must state who the team lead is and the team lead must have at least one of the following valid Certifications: 1. Certified Information Systems Security Professional (CISSP), 2. Certified Cloud Security Professional (CCSP) 3. Offensive Security Certified Professional (OSCP), 4. Certified Ethical Hacker (CEH), 5. Certified Information System Auditor (CISA), 6. Certified Information Security Manager (CISM)		
Substantiate (if necessary) and provide relevant proof		
1.2.1.3 The bidder must provide two (2) reference/recommendation letters from a company they assisted with proactively picking up a cyber /vulnerability/security breach issue in the past		
Substantiate (if necessary) and provide relevant proof		

### 1.2.2 PHASE 2 Technical/Functionality evaluation

Bidders will be evaluated according to the below technical evaluation criteria. Minimum Technical Threshold is **75%**. It must be noted that if the Bidder does not meet the **75%** minimum threshold, the bidder will be disqualified and not be evaluated further.

#### 1.2.1 Experience of the Bidder – Vulnerability Management

Company experience related to implementation of Vulnerability Management as a managed service.

*Previous Vulnerability Management implementations completed by the Company*

5 and more assignment completed	5	Signed reference letters on client letter head, detailing previous work done with contactable details	15%
4 assignments completed	4		
3 assignments completed	3		
2 assignments completed	2		
1 assignment completed	1		
0 assignment completed/bidder submitted letters that are not relevant	0		

#### 1.2.2 Experience of the Bidder – SIEM

Company experience related to implementation of SIEM as a managed service.

*Previous SIEM implementations completed by the Company*

5 and more assignment completed	5	Signed reference letters on client letter head, detailing previous work done with contactable details	15%
4 assignments completed	4		
3 assignments completed	3		
2 assignments completed	2		
1 assignment completed	1		
0 assignment completed/ bidder submitted letters that are not relevant	0		

1.2.3 The extent to which the proposed SIEM solution meet the Scope of Work			
Meets 9 scope items and more	5	Bidder's comments in terms of extent to which their solution meet each of the 9 scope items in section 3.2 of the scope/Table 1	25%
Meets 6 to 8 scope items	3		
Less than 6 scope items	0		

1.2.4 The extent to which the Vulnerability Management solution covers the various infrastructure components listed in section 3.1			
Scanning covers 8 infrastructure components and more	5	Bidder's comments in terms of extent to which the scanning covers infrastructure components listed in section 3.1 of the scope/Table 2 below	25%
Scanning covers 5 to 7 infrastructure components	3		
Scanning covers less than 5 infrastructure components	0		

1.2.5 The extent to which the supplier meets implementation requirements in section 4.1 of the scope of work			
Meets 100% requirements and more	5	Bidder's comments in terms of extent to which the requirements will be met as per Table 3 below	10%
Meets 80% - 99% requirements	3		
Meets less than 80%	0		

1.2.6 The extent to which the supplier meets supplier requirements in section 4.2			
Meets 100% requirements and more	5	Bidder's comments in terms of extent to which the requirements will be met as per Table 4 below	10%
Meets 80% - 99% requirements	3		
Meets less than 80%	0		



## BUSINESS REQUIREMENTS TABLES

### Business Requirements for SIEM solution

The bidder must indicate its compliance / non-compliance to the requirements and should substantiate its response in the space provided below. If more space is required to justify compliance, please ensure that the substantiation is clearly cross-referenced to the relevant requirement.

Item no	Requirements	Comply or Not comply	Provide details of how your solution satisfies CEF requirements
	The SIEM solution requirements include the supply, cloud installation, configuration of a new SIEM software, its integration with Vulnerability Management, and the ongoing management of the SIEM as a service The managed SIEM service must have the ability to do the following:		
1	Log Monitoring		
2	Detection of Brute Force Attack		
3	Detection of Malware Activity		
4	Detection of Suspicious User Behaviour( Threats Detections)		
5	Detection of Suspicious Network Behaviour( Threat Detections)		
6	Suspicious Behaviour ( Threat Detections)		
7	Track System Changes and Authentication ( Threat analysis)		
8	Continuous Compliance Management		
9	Detection of known and unknown threats		

Table 1: The extent to which the proposed SIEM solution meet the Scope of Work



Item no	Requirements The assessment or scanning must accurately locate threats and vulnerabilities, assess their risk to the environment, and propose remediation plans; and must cover, inter alia the following:	Comply or Not comply	Provide details of how your solution satisfies CEF requirements
1	Workstations consisting of laptops and desktops		
2	Servers consisting of operating systems such as windows, Unix, etc		
3	Network gear consisting of routers, switches, access points, load balancers, video conference unit, etc		
4	Applications, including web facing		
5	Databases		
6	Email security		
7	Firewall security		
8	File Shares		
9	Other IT Infrastructure components		

Table 2: The extent to which the Vulnerability Management solution covers the various infrastructure components listed in section 3.1

Item no	Requirements Provide key personnel who will be responsible for the implementation of the project and determine the roles, responsibilities and the team structure of such personnel. All key personnel dedicated to the project shall be properly qualified, possess valid certifications issued by the relevant authority (if any)  In terms of SIEM, the supplier shall:	Comply or Not comply	Provide details of how your solution satisfies CEF requirements
1	Conduct a pre-installation workshop with designated Cef staff		
2	Connect out-of-the-box log sources		
3	Connect custom log sources		
4	Configure security analytics to identify threats and prioritize alarms		
5	Intergrade threat intelligence feeds, vulnerability assessment reports, and other contextual information		



6	Proactively monitor and investigate events to provide early threat notification and helpful remediation advice		
7	Perform a post-implementation health checks to confirm whether any further customization or performance improvement is needed		
8	Take necessary measures to rectify issues identified during the health check		

Table 3: **The extent to which the supplier meets implementation requirements in section 4.1 of the scope of work**

Item no	Requirements	Comply or Not comply	Provide details of how your solution satisfies CEF requirements
	Provide key personnel who will be responsible for the implementation of the project and determine the roles, responsibilities and the team structure of such personnel. All key personnel dedicated to the project shall be properly qualified, possess valid certifications issued by the relevant authority (if any)  In terms of vulnerability management, the supplier shall:		
1	Conduct risk identification and analysis		
2	Identify and confirming the types of Vulnerability Scans to be conducted		
3	Agree with CEF on any additional infrastructure components to be scanned		
4	Configurations of the vulnerability scan		
5	Perform the scan		
6	Evaluate and consider possible risks		
7	Produce a report and interpret the scan results		
8	Create a remediation process and mitigation plan		
9	Remediate vulnerabilities ( To be done by CEF)		
10	Perform internal penetration testing annually and produce a report and recommendation		
11	Ensure integration between vulnerability management and SIEM		

Table 4: **The extent to which the supplier meets supplier requirements in section 4.2**