

APPOINTMENT OF A SERVICE PROVIDER TO IMPLEMENT A FULLY MANAGED VULNERABILITY MANAGEMENT AND SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM).

PART 2: BACKGROUND, OVERVIEW AND SCOPE OF REQUIREMENTS

1. INTRODUCTION

CEF SOC Ltd is a state-owned company involved in the search for appropriate energy solutions to meet the energy needs of South Africa and the sub-Saharan African region. It also manages the operation and development of the oil and gas assets of the South African government. The company falls under the auspices of the Department of Mineral Resources and Energy (DMRE). For more information on the company, you can visit our current website: www.cefgroup.co.za

2. BACKGROUND AND OVERVIEW

CEF currently has a robust information security management program in place however, because of the level of importance the company attaches to information security; IT periodically reviews its information security infrastructure and apply required changes in order to stay abreast with changes in information security.

The digital revolution is driving business innovation and growth but it is also exposing us to new and emerging threats.

Today's threat landscape is unimaginably different, with thousands of new vulnerabilities reported annually. Various security breach reports show an increasing trend in the number of vulnerabilities identified. The sheer volume of launched attacks demands best-in-class vulnerability management solutions that deliver comprehensive discovery to support the entire vulnerability management lifecycle.

Given this context, CEF seeks to appoint as service provider who can implement cloud based solutions to identify and manage vulnerabilities as well as pro-active security monitoring of the IT infrastructure.

To this end, implementing a Vulnerability Management and Security Incident and Event Management (SIEM) as a managed service hosted in the cloud has become an attractive option to address various security-related business objectives.

3. THE SCOPE SHALL INCLUDE –

3.1 Vulnerability Management as a managed service

The managed vulnerability management must follow a full cycle of vulnerability management process of **preparation, vulnerability scan, defining remediating actions, implementing remediating actions**, and **rescanning**, on a quarterly basis; as well as penetration testing on an annual basis.

The managed Vulnerability Management service must have the ability to do the following:

- Effective management of vulnerabilities associated with critical infrastructure components

- Ability to manage increase in scale and complexity of the environment
- Integration of Vulnerability Management with SIEM, which must be implemented as part of this scope
- Deep dive analysis of vulnerabilities along with correlation of threats and events.
- Penetration testing from within and outside firewall

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:-

- Workstations consisting of laptops and desktops
- Servers consisting of operating systems such as Windows, UNIX, etc.
- Network gear consisting of routers, switches, access points, load balancers, video conference units, etc.
- Applications, including web facing
- Databases,
- eMail security
- Firewall security
- File shares
- other IT infrastructure components

Penetration testing from within and outside firewall must include but not limited to:-

- Current Cyber Security threats that could exploit the CEF infrastructure
- Emerging Cyber Security threats that could exploit the CEF infrastructure.
- Exploitation of found vulnerabilities that are exploitable.
- Penetration results report and recommendations.

Structure of proposal

The proposal must include amongst other elements the following:-

- What the vulnerability assessment/scanning will cover in fair amount of detail,
- Frequency of vulnerability assessments
- What the penetration testing will cover in fair amount of detail
- Frequency of penetration testing
- Integration of vulnerability management with SIEM
- The methodology, approach and tools to be used for the assessment / testing exercise,
- Any resource and support requirements from CEF
- Timeline and cost of implementation as well as cost of conducting the periodic vulnerability assessments

3.2 SIEM as a managed service

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.

Data sources will originate from systems located in Head Office in Sandton.

Structure of proposal

The SIEM proposal must include amongst other elements the following:-

- Its integration with Vulnerability Management,
- The methodology, approach and tools to be used for the SIEM
- Any resource and support requirements from CEF
- Timeline and cost of implementing the SIEM as a managed service
- The managed SIEM service must have the ability to do the following: -

- **LOG MONITORING:**

The proposed solution must provide a built-in platform for centralized log monitoring and management. It must ingest logs from different sources such as Windows servers, VMWare, SQL DBs, Network Devices, etc

- **DETECTION OF BRUTE FORCE ATTACK**

With the evolution of faster and more efficient password cracking tools, brute force attacks are on the increase. The solution must be able to count the frequency of login attempts (failed or successful), multiple logins from the same IP address or geo-location, and any modification to system files, etc., so that a possible attack underway can be noticed and can generate an alert before the attack succeeds. Given the correlation of login attempts across the network, SIEM can uniquely identify patterns that would be missed on an individual device.

- **DETECTION OF MALWARE ACTIVITY**

With logs being produced from multiple sources that include end-point devices, firewalls, etc it is important to have the capability to correlate these logs and security events to be able to detect potential malware activity.

- **DETECTION OF SUSPICIOUS USER BEHAVIOR**

Reportedly, more than 30 percent of attacks initiate from malicious insiders within an organization. Insider behaviour may be more challenging to detect given that they already have access to the network. It is imperative that SIEM rules discover activity patterns of insiders that can alert on suspicious behaviour.

- **DETECTION OF SUSPICIOUS NETWORK BEHAVIOR**

The solution must, in the minimum, be able to collect and correlate the following information to identify the suspicious behaviour:

- ✓ Suspicious connections, connection patterns, and geo-locations
- ✓ Suspicious data transfers
- ✓ Excessive connections
- ✓ Account access attempts
- ✓ Connectivity to blocked and backlisted sites
- ✓ Backdoor connections

- ✓ IDS/IPS exploits
- ✓ Spyware activity
- ✓ Man-in-the-middle activity

- **SUSPICIOUS DEVICE BEHAVIOR**

An attacker, after gaining control over a compromised machine/account, tends to stop or reduce logging services so that their unauthorized and illegitimate behaviour goes unnoticed. The service must be able to counter such malicious actions and raise an alert if a host stops or dramatically reduces forwarding logs after a threshold limit.

Another common pattern found among compromised log sources is that attackers tend to change the configuration files of endpoint agents installed and forward a lot of irrelevant files to the SIEM Platform, causing a bandwidth choke between the endpoint agent and manager. This affects the performance of real time searches, storage capacity, dashboards and reporting. The SIEM rules and analytics must be able to handle this suspicious behaviour of log sources.

- **TRACK SYSTEM CHANGES AND AUTHENTICATION**

Typical attackers will install files, modify systems, use existing accounts or create new accounts to execute their attack. The attacker will leave a trail of user authentication, source locations and system and file changes. All of these factors can be evidence that an attack is underway. The solution must be able to track changes and administrative actions across internal systems and matching them to allowed policy. It must be able to detect policy violations or behaviour that is not normal.

- **CONTINUOUS COMPLIANCE MANAGEMENT**

A log management capability to maintain an audit trail of activity is paramount. The solution must provide a mechanism to rapidly and easily deploy a log collection infrastructure that directly supports this requirement, and allow instant access to recent log data, as well as archival and retrieval of older log data.

- **DETECTION OF UNKNOWN THREATS**

The solution must be able to correlate logs from various sources across the enterprise and be able to detect threats that are unknown.

4. REQUIREMENTS

4.1 Implementation 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 vendor (if any)

In terms of SIEM, the supplier shall:

- Conduct a pre-installation workshop with designated CEF staff
- Connect out-of-the-box log sources
- Connect custom log sources
- Configure security analytics to identify threats and prioritize alarms
- Integrate threat intelligence feeds, vulnerability assessment reports, and other contextual information
- Proactively monitor and investigate events to provide early threat notification and helpful remediation advice;
- Perform a post-implementation health check to confirm whether any further customization or performance improvement is needed; and
- Take necessary measures to rectify issues identified during the health check.

In terms of Vulnerability Management, the supplier shall:

- Conduct risk identification and analysis
- Identifying and confirming the types of Vulnerability Scans to be conducted
- Agree with CEF any additional infrastructure components to be scanned
- Configuration of the vulnerability scan
- Perform the scan
- Evaluate and consider possible risks
- Produce a report and interpret the scan results
- Create a remediation process and mitigation plan
- Remediate the vulnerabilities (To be done by CEF)
- Perform penetration testing annually and produce a report and remediation recommendation
- Ensure integration between vulnerability management and SIEM

4.2 Supplier Requirements

In terms of SIEM the supplier shall:

- Be an authorized reseller for the Solution provided and maintain such authorization for the duration of the Agreement.
- Perform work in accordance with the Standards for the Professional Practice of the International Information System Security Certification Consortium (ISC)², Information Systems Audit and Control Association (ISACA) and other applicable
- Provide the solution as a managed service and must provide support services to setup, manage, operate and maintain the SIEM to enable CEF to prevent, detect, respond and recover from security threats, events and incidents.
- Services should include, but are not limited:

- Operate on 24x7x365 basis
- Provide incident management support, forensics, and malware analysis
- Provide threat analysis and intelligence, and mitigation strategies and recommendations
- Ensure logging, correlation to SIEM from data sources
- Tune SIEM to reduce false positives
- Provide reports on summary of SOC activities, security events, etc. as requested.

In terms of Vulnerability Management, the supplier shall:

- Be an authorized reseller for the Tools used to conduct the scanning
- Use qualified engineers to conduct the assessment
- Provide vulnerability management as a managed service to design, configure and conduct the scan, reporting and interpretation of scan results, remediation plan, and ongoing quarterly re-scanning of the environment
- Services should include, but are not limited:
 - Vulnerability scanning on quarterly basis
 - Vulnerability report and remediation plan
 - Penetration testing, Report and recommendations

5. DELIVERABLES

5.1 Vulnerability Management

- Vulnerability Management program as a managed service
- Quarterly Vulnerability Assessments
- Vulnerabilities Report, including vulnerability severity ratings and detailed remediation recommendations
- Remediated vulnerabilities (To be done by CEF based on Vulnerability Report)
- Penetration Report and recommendations. The report must show penetration testing report results at each stage of the test stages, evidence of successful exploitation such as screenshots, logs and data leaked and detailed recommendations

5.2 SIEM

- A fully configured and functional SIEM solution as a managed service.
- Incident management support, forensics, and malware analysis
- Threat analysis and intelligence, and mitigation strategies and recommendations

5.3 Integration

- Integration between Vulnerability Management and SIEM

6. COMPULSORY REQUIREMENTS

6.1 Certifications

Proof of the following certifications is required

- ISO 27002 standard

- Certified Information Systems Security Professional (CISSP),
- Certified Cloud Security Professional (CCSP)
- Offensive Security Certified Professional (OSCP),
- Certified Ethical Hacker (CEH),
- Certified Information System Auditor (CISA),
- Certified Information Security Manager (CISM)