**Questions and Answers** for the tender: Provisioning of a **SIEM (Security, Information and Event Management) Solution** and **24X7X365 Security Operations Centre (SOC) Services** to EPPF for a for a period of **36 months**, as a **managed service** in order to protect information assets against attacks, including cyber-attacks and also enhance the security posture of EPPF

1. In terms of Log Volume
   a. What is the existing log volumes? **We allocate 500GB per month for the current SIEM. The current SIEM does not work on data allocation.**
   b. How much log data is there in total? See response above
   c. How long do you want to retain data for? (Very Important for sizing and pricing) . **90 Days**
   **d.** What is the current EPS? (Very Important for sizing and pricing) **See response above**
**2.** Any requirements for geo hosting? (UK or EU, US, APJ) S**outh Africa region is the first preferred option**
3. Can you provide a list of log sources other than what was mentioned? (1 x FW, 40 systems you mentioned and FW, AD, AV). Please specify any others that may be relevant. **Mimecast, 365, Azure AD, OneDrive, SharePoint, Defender for Endpoint, Defender for Cloud, Fortinet, Windows Server Security and Event logs.**
4. Pricing is provided on a consumption based (*GB per day average*). How much data in Gigabyte Per Day is required? 50 Gig or 100Gig, or other, please specify. **We allocate 500GB per month for the current SIEM. The current SIEM does not work on data allocation**
5. Would you like full stack solution? **Yes**
   a. Log Management
   b. SIEM with Correlation
   c. Ability to Investigate
   d. Analytics
   e. Automation
   f. Playbooks
   g. Case Management (SOAR)

6. Are Honey pot devices included in the scope of the tender opportunity? **No**
7. We need to know how many network segments and sites that you have? **1 site**
8. We need to determine how many Honeypots devices that are needed? **Not required**
9. Does the implementation require VM or physical hardware? **Cloud hosted SIEM is the requirement**
10. How many devices will be tracked on the SIEM? **This question has been addressed as part of the other questions**
11. How many events per second will be tracked? **This question has been addressed as part of the other questions**
12. How many Windows servers do you have? **40 Virtual Machines**
13. How many Linux servers do you have? **None**
**14.** How many Exchange servers do you have? N**o exchange servers – we are using Microsoft 365 services**
15. How many Domain Controllers do you have? **2 Active Directory devices**
16. Number of network devices (switches, routers, wireless controllers, security surveillance controllers etc)? **See response on (17)**

17. Number of security devices (firewalls, email security gateway, endpoint management etc)?

    **Firewall**

    **Network devices – routers and switches**

    **M365 Services**

    **Azure and AWS services**

    **VMWare Infrastructure**

    **Email Security**

18. Will the licensing be Subscription or Perpetual based? **Licences will be paid on annual basis**
19. How many years of support and services? **36 months**

20. **Current Setup Information**

| | | |
|---|---|---|
| Do you already have a SIEM solution | Yes | We have a managed SIEM solution and SOC Services in place |
| What is the SIEM product is being used | N/A | We will not be providing the current SIEM tool name due to security reasons |
| Total Log Sources | Refer to table below | Firewall (Network) , Servers , Workstations , Applications, Azure , AWS |
| Detailed list – product version along with count - to be filled in Annexure 1 | Refer to table below | Refer to table below |
| Total expected EPS to be monitored (Share if you are aware of this information) | 170 | We have a total of 170 endpoints / workstations in the environment. We can also include an estimate of 170 mobile devices that connect to the office WIFI network |
| Share approx. number of data centres from where logs need to be collected | 3 | Microsoft Azure, AWS Cloud and Onpremise HPE VMWare Simplivity environment |

**21. Detailed list – product version along with count**

| **Type** | **Count** | **Comments (Make/Model)** |
|---|---|---|
| **Linux / Unix Servers** | 4 | RedHat - used monitoring purposes |
| **Windows Servers** | 30 | Total of servers Onprem (15%) + Azure(70%) + AWS)15%) |
| **Active Directory** | 2 | Onprem and Azure hosted |
| **Network Routers** | 2 | Cisco Routers |
| **Network Switches** | 10 | Cisco Switches |
| **Network Wireless LAN** | 15 | 15 AP's and 1 Wireless Controller |
| **Network Load-Balancers** | 2 | In Azure and AWS |
| **Other Network Devices** | 0 | None |
| **Network Firewalls (Internal)** | 2 | Onprem and Azure hosted |

| | | |
|---|---|---|
| **Network Firewalls (DMZ)** | 1 | In place |
| **Network IPS/IDS** | 1 | Part of the Firewall Service |
| **Network VPN / SSL VPN** | 2 | FortiGate and Palo Alto |
| **Network AntiSpam** | 2 | Mimecast and Defender |
| **Network Web Proxy** | 0 | None |
| **Other Security Devices** | 0 | None |
| **Web Servers (IIS, Apache, Tomcat)** | 2 | Hosted in Azure |
| **Database (MSSQL, Oracle, Sybase)** | 2 | Hosted in Azure - MSSQL |
| **Email Servers (Exchange, Sendmail, BES, etc)** | 1 | Exchange Online |
| **AntiVirus / DLP Server** | 2 | Microsoft applications are being used |
| **Other Applications (ERP, Inhouse, etc)** | 0 | Microsoft applications are being used |
| **Total** | **76** | |

### 22. MDR Professional/Advanced/Enterprise

| | | |
|---|---|---|
| **Which MDR service would you be interested in** | MDR Enterprise | We need a 24X7X365 Managed SIEM solution and SOC Services |
| **Do you want the SIEM to be in MDR model or on-prem** | MDR model | Cloud based SIEM solution |

### 23. Services Catalogue

| | | |
|---|---|---|
| **SIEM-as-a-Service** | Yes | We need a 24X7X365 Managed SIEM solution and SOC Services |
| **SOC Monitoring (24x7)/(18x5)/18X7)/(8x5)** | Yes | We need a 24X7X365 Managed SIEM solution and SOC Services |
| **EDR-as-a-Service (EDR= End Point detection & Remediation as a service)** | Yes | EDR-as-a-Service (EDR= End Point detection & Remediation as a service) |
| **Device Management (Management of Security devices)** | Yes | The SIEM solution should be able to support Mobile Device Manahement (estimated to be 170) |
| **FIM-as-a-Service(File Integrity Monitoring as a service)** | Yes | Weekly reporting |
| **Threat Hunting as a service** | Yes | We need a 24X7X365 Managed SIEM solution and SOC Services |
| **Incident Response (24x7)/(18x5)/18X7)/(8x5)** | Yes | We need a 24X7X365 Managed SIEM solution and SOC Services |
| **Forensics Retainer(as a service)** | Yes | Retainer hours to be procured as and when required |

| | | |
|---|---|---|
| **Brand Monitoring & Anti Phishing As a service** | Yes | We need a 24X7X365 Managed SIEM solution and SOC Services |

24. **Vulnerability Scanner –** Vulnerability management is conducted through M365 Defender as well as Nessus tool.
25. Please clarify the following: Operator Privacy Due Diligence Form
    (a) Are we required to completed in the document now or that is to be completed in after award? The EPPF Operator Privacy Due Diligence Form and Operator Privacy Compliance Self-Assessment Forms are to be submitted as part of the RFP response.