

**BS/2022/RFB469 - Security, Information and Events Management (SIEM)**

**Non Compulsory Virtual briefing Session response Feedback**

**Date : 26 May 2022 at 11h00**

**N.B: BANKSETA have a staff complement of between 70 to 100.**

**Q 1 – Is BANKSETA looking for a SIEM solution or SIEM monitoring tool**

**A1 –** BANKSETA is requested or required to deliver the SIEM Solution as part of the security to enhance the security in the organization. The SIEM solution is what is required.

**Q2 - Does it matter whether the solution is on-prem or cloud-based?**

**A2 –** What is critical is a solution that can deliver as per our terms of references, whether it's hosted internally or it's hosted on the service providers environment that should not be a defining matter.

**Q3 – What is the closing date for questions?**

**A3 –** The tender is closing 20 June 2022 there the last day to ask questions would be 13 June 2022. The Q&A from the briefing session will be responded to by 31 May 2022.

**Q4 – Pricing for licencing will it be billed monthly or yearly**

**A4 –** Billing will be yearly

## **BELOW IS THE INFORMATION REQUESTED:**

### **1. Internal BANKSETA Bandwidth**

- Centurion 100Mbps (upload and /or download)
- Regional Offices: Polokwane and East London (20Mbps upload and/or download).

### **2. Endpoints and data sources**

- 200 Endpoints
- Router x3 (Centurion and Regional Offices)
- Firewall x1 (Firewall and Web Content Gateway)
- Switches x10 (Inclusive of Regional offices)
- Azure Cloud x1 (Currently running Active Directory and DR Backups)
- Servers x 10 (Physical and Hyper-V Managed servers): The servers are hosting services such as:
  - ✓ Domain Controllers x2
  - ✓ Active Directory
  - ✓ Backup Solution
  - ✓ DHCP
  - ✓ Shared Files and Folders
- Laptops x 70 (All staff Members laptops events must be recorded)

### **3. Third Party Hosted Application**

- Six Applications hosted externally by the third-party service providers.
- Microsoft Office 365 applications suite
- SQL Databases
- PABX Solution

### **4. Critical Endpoints**

- **Critical endpoints** include All Servers, Applications, service accounts, cloud, firewall and 20 Laptops.

### **5. Service Accounts**

- **Service Accounts**
  - ✓ 10x On-premises & Cloud Service Accounts.
  - ✓ 20x Hosted applications and portals.

## **6. Total Log estimate per month**

- We have no estimates in terms of the log sizes however, we believe the information provided will be sufficient to assist in determining the log sizes.

## **7. IP Addresses**

- One IP range for external communications and / or access
- Multiple subnets for internal services
- Lastly, third party hosted applications Ip ranges for the hosted solutions.

## **8. Operating Systems**

- Servers (Windows Server 2012 and later Versions)
- Workstations (Windows 10 and Later versions (11))