QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

Sites

Number of sites	**2**

Applications

Application Type	**Vendor/Version**	**Quantity**
Anti-Virus	Bitdefender	
Database	Windows SQL and Oracle	6 MSSQL & 6 Oracle
Email	MS O365	
Proxy	N/A	
Vulnerability Scanner	N/A	
Web servers	Windows	15
Any other		

Operating System

Operating System	**Vendor/Version**	**Quantity**
Workstation	We only want the SIEM for Servers	
Servers	Windows	50
Domain Controller	Windows	4

Network devices

Device Type	**Vendor/Version**	**Quantity**
External firewall	N/A	
Internal Firewall	Fortigate	2
IDS/IPS	Firewall	
Load balancer	N//A	
VPN appliance	Fortigate	
Router	N/A	
Switch	Cisco & Dell	30

- Does the solution have to be 100% on-prem. Can data be stored in the Cloud? – Collection of data should be centralized on the LAN, not each device should send the data to the cloud. Centralized data can be sent to the cloud for analysis.
- What is the total number of assets in the customer's environment? – 50 Windows Servers, 5 ESXi hosts, 30 Switches, 2 vCenter's, 2 WLAN controllers, 12 AP's, 2 Fortigate Firewalls.
- Please confirm that we will provide you with the software and licenses and Letjeka will manage the customer's environment. – Software and licenses, Letjeka to provide support for the Software e.g Montlhy reports, maitenaince etc.

Please may I ask as to how many users (Seat count) do you have with your environment. – 400

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

TECHNOLOGY	QUANTITY	COMMENTS (OS, Version, Brand, Model, etc.)
Users	400	Number of Organisational Users
Number of External Domains	1	
Domain Controllers	4	
Active Directory/AzureAD/Auth	1	On prem ADsync to Azure
DNS Servers	4	
DHCP Servers	2	
Web Servers	15	
Exchange/Mail Servers	MS O365	
Database Servers	12	6 MSSQL & 6 Oracle
Proxy Servers	n/a	
Application Servers	n/a	
*UX Servers	n/a	
General Purpose Windows Servers	n/a	
Firewalls	2	
WAF	n/a	
IDS/IPS	Firewall integrated	
VPN	Firewall	
Load Balancers	n/a	
Email Gateways (Mimecast, Proofpoint, etc.)	Mimecast	
O365/Gsuite/Etc.	MS O365 E3	
Cloud Containers	n/a	

MONITORED ENVIRONMENTS	
On-Prem/DC	Yes
Azure	No
AWS	No
Gcloud	No
Other (please specify)	

Breakdown of the number of devices at SAHPRA as follows:

- Servers: - 50
- User workstations: - 400
- Switches: 30
- Routers: N/A
- Firewalls: 2
- WLC: 2
- AP's: 12

The reason for the question is that our licensing is based on number of devices generating events, this does include end user devices as well as critical infrastructure.

Are you looking for:

1. A managed SIEM; OR
   This means
   a. The SIEM solution - Yes
   b. The training on how to operate it - Yes
   c. Ongoing support for the SIEM solution – Yes
   d. NO technical engagement regarding the outputs from the SIEM or what t do with them – Assist in creating/generating reports and actions to take from the output (Someone to do the analytics required when running a SIEM)
   e.
2. A Managed SOC service with a SIEM
   This means:
   a. A managed SIEM; AND all of the following:
      i. Someone to run the SIEM
      ii. Someone to provide 24x7 monitoring and alerting
      iii. Someone to do the analytics required when running a SIEM
      iv. Someone with whom to collaborate in order to achieve better remediation outcomes

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

SAHPRA
South African Health Products Regulatory Authority

Device Type	Device Count	
Windows Domain Controller	4	
Windows Application Server	0	
Windows Exchange Server Logs	0	Using MS O365
Windows IIS Web Server	15	
Windows DNS Server	4	
Windows DHCP Server	2	
Windows Database Server	6 MSSQL & 6 Oracle	
Linux Application Server	0	
Linux Email Server	0	
Linux (Apache) Web Server	0	
Linux DNS Server	0	
Linux DHCP Server	0	
Linux Database Server	0	
Other FSM agent features eg FIM	0	
VMWare ESX Host	5	5 ESX hosts
AV Manager / Vulnerability Scanner	0	
Load Balancer/Web FW	0	
WLAN Controller	2	Cisco
Next Gen Firewall - Large	0	
Next Gen Firewall - Medium	2	501 & 200F Fortigate
Next Gen Firewall - Small	0	
Firewall - Large	0	
Firewall - Medium	0	
Firewall - Small	0	
Network IDS/IPS - Large	0	
Network IDS/IPS - Medium	0	
Network IDS/IPS - Small	0	
Web App Firewall - Large	0	
Web App Firewall - Medium	0	
Web App Firewall - Small	0	
Web Proxy	0	
Network Switch Netflow enabled	0	
Network Switch	30	Cisco and 3 dell switches
Network Router	0	
VPN (if not on FW)	0	VPN on the Firewall
Antispam/eMail GW	0	
0	0	
0	0	
0	0	
0	0	
AV on Server or Endpoint	bitdefender	cloud managed
FSM UEBA Endpoint Agent	0	

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

SAHPRA
South African Health Products Regulatory Authority

Submission Date:		*Required
Customer Name:		*Required
Sales Representative Name:		*Required
Sales Representative ATTUID:		*If Available
Security Expert (ASE/TSC/SCOE) Name*:		*If Available
Security Expert (ASE/TSC/SCOE) ATTUID*:		*If Available
Sales Buiness Sector (ex:National,Global,Private Sector ect.):		*If Available
Product Being Sold:	USM Anywhere - Only	*Required
Salesforce Opportunity Link:		*If Available

Overview

Does your company policy allow logs to be off premise and hosted on AWS?:	Yes	*Required
What goal is customer trying to achieve with USM Anywhere? (New solution, replace existing solution, or supplement existing solution):	Replace	*Required
What Subdomain name does customer require?		*If Available
Does customer have geographic requirements?	Select Input	*If Available
Does customer have an existing security teams?	No	*Required

SCOPING GENERAL NOTES & CONSIDERATIONS	
Please include all the notes related to the scope or any valuable information. Things like: Describe the topology of the network - LAN - two sites connected through MPLS Is there interconnectivity between the sites? - YES Do all of the sites have VMWare/HyperV infrastructure? - YES Does the form have the infrastructure that needs to be monitored or the entire inventory? - YES URL of the client? - sahpra.org.za Type of industry? - Health regulatory	*Required

Known EPS numbers

AWS Environment	Number	
Estimated EPS	0	*Will add to calculations below!
Azure Environment	**Number**	
Estimated EPS	0	*Will add to calculations below!
GCP Environment	**Number**	
Estimated EPS	0	*Will add to calculations below!
On Prem Environment	**Number**	
Estimated EPS		*Will add to calculations below!

Estimated numbers based on environment input

amazon web services

AWS Environment	Qty
Accounts - How many accounts do you have?	0
EC2 Windows/Linux - How many instances?	0
S3 Buckets - How many S3 Buckets to Monitor?	0
Native AWS logs	**Yes/No**
CloudTrail	No
CloudWatch	No
VPC Flow Logs (Very Noisy)	No

Azure

Azure Environment	Qty
# of Azure ARM subscriptions	0
# of Web Apps/IIS	0
# of VMs	0

Google Cloud Platform

GCP Environment	Qty
Accounts - How many accounts do you have?	
# of Virtual Private Clouds (VPCs)	
# of Zones	
# of GKE Clusters	
# of VMs	
Logs to collect	**Yes/No**
Firewall Logs	Yes
VPC Flow Logs	No

ALIENAPPS		
Cloud Hosted Applications	**Qty**	**Name**
O365 - How many Office365 users?	400	
G-Suite - How many Gsuite users?	0	
Okta - How many Okta users?	0	
Zscaler Nanolog - How many users?	0	
Cisco Umbrella - How many users?	0	
Cisco Amp/Secure Endpoint - How many endpoints?	0	
McAfee ePO - How many McAfee ePO endpoints?	0	
Sophos - How many Sophos endpoints and/or devices?	0	
Carbon Black - How many Carbon Black endpoints?	0	
Crowdstrike - How many Crowdstrike endpoints?	0	
SentinelOne - How many SentinelOne endpoints?	0	
CASB Solution - How many users?	0	
Vulnerability Manager/Scanner (DDI/Qualys) - How many endpoints?	0	
Other. State name and Qty (Any relevant info add to notes section)	0	

ON-PREMISE LOCATIONS	Input
Total concurrent domain users across all locations	400
Working Hours	Select Input
Total Users Across All Locations	1680
Are your sites Interconnected?	Yes
If interconnected how?	Yes
Does each site have its own internet breakout?	Yes

Location types with direct internet access	Datacenter	HQ/Main	Branch
Number of locations (sensor deployment)			
Network Data Sources			
Fortinet Fortigate firewalls	2	yes	yes
UTMs/NGFW/dedicated active firewalls (Enterprise)		yes	yes
Small low activity firewalls (SMB)			
Alienvault NIDS (Yes - 1, No - 0/Blank)	No	Yes	Yes
Dedicated IPS/IDS	no		
Dedicated Web Filter/Proxy	no		
Other network devices (Routers, Switches, etc…)	30		
Server/Endpoint Data Sources			
User workstations being monitor (Laptops/Desktops)	No		
AD, DC, DNS, DHCP, IPAM servers	yes		
Web/IIS Windows servers	yes		
Other Windows/Linux Servers	yes		

50 Windows Servers, 5 ESXi hosts, 30 Switches, 2 vCenter's, 2 WLC, 12 AP's, 2 Fortigate Firewalls.

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

SAHPRA
South African Health Products Regulatory Authority

The purpose of the survey is to collect necessary information for successful preparation and testing of the SIEM solution Kaspersky Unified Monitoring and Analysis Platform.

Below questions are for license configuration only. If you need to understand HW costs or services, additionally fill in the other spreadsheets of this book

General Information	
Organization Name	SAHPRA
Contact details (contact person, email, etc.)	

Is a different SIEM Solution currently being used? Please specify which one	Yes, ManageEngine
If other SIEM is used, please specify for how many EPS or GbD it's licensed	400 worksations, 15 Servers, 10 syslog devices.
Additional option: "TI bundle". Is Kaspersky TI required to be bought with SIEM? (Ability to use a few feeds with KUMA exclusevly (feeds: Malicious URL, BotnetCnC URL, Phishing URL, IP reputation, Ransomware URL).	
Additional option: "Unlimited netflow collection". Is Netflow data collection required? (Netflow v5, v9, IPFIX, sFlow).	

Please fill in the blue cells below for EPS and license calculation (be aware you should indicate only infrastructure, that should be monitor by SIEM. It may be all your infrastructure, or only part of it)

Event Source	Amount	Avg. EPS	EPS
Workstations/Servers			
Windows Servers - Total *	0		50
Windows Servers - HIGH EPS	*0*	50	0
Windows Servers - MED EPS	*0*	3	0
Windows Servers - LOW EPS	*0*	1	0
Windows Desktops	0	1	0
Windows AD Servers	0	10	400
Linux / Unix Servers	0	1	0
Network Devices			
Routers	0	1	0
Switches (disregarding Netflow events)	0	2	30
Wireless LAN	0	5	12 AP's, 2 WLAN Controllers
Load Balancers	0	5	0
WAN Accelerator	0	14	0
DNS	0	40	4 DNS Servers
Other Network Devices	0	10	0
Security Devices			
Firewalls (Internal)	0	20	2 Fortigate firewalls
Firewalls (DMZ)	0	50	0
Next Generation Firewall (NGFW)	0	150	0
IPS/IDS	0	15	0
VPN	0	2	Firewall
AntiSpam	0	10	0
DLP	0	10	0
Proxy	0	15	0
UEBA/UBA	0	10	0
NTA	0	15	0
Network Sandbox	0	5	0
Other Security Devices	0	5	0
Applications			
Web Servers (IIS, Apache, Tomcat)	0	1	15
Database (MSSQL, Oracle, Sybase)	0	1	6 MSSQL & 6 Oracle
Email Servers (Exchange, Sendmail и т.д.)	0	2	0
Number of EDR agents (for telemetry collection)	0	1	0
Number of AntiVirus agent	0	0.2	bitdefender
Гипервизор (Vmware, VirtualBox и т.д.)	0	5	5 ESXi, 2vCenter
Other	0	5	0
		Total EPS	**445**
		Kaspersky KUMA licenses to buy	**5**

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

Sr. no	Splunk Sizing - Queries	Answers from End User	Notes \ Remarks
1	Daily Volume in GB\day to be calculated to come up with the Licensing	Next Sheet (Splunk Sizing)	
	Types of Licensing - Term based (Years)		
2	Retention Period in days\years needed for (Online \ Offline or Archived) data	12 Months	
	Online Data (Searchable data) 3 Months, 6 Months etc..		
	Archived Data - 6 Months OR 1 Year	2 Years	
3	Number of **Locations\Sites** on which the customer data is distributed and want to monitor?	2	
4	Number of **Employees** accessing underlying infrastructure **(Users)**	400	
5	Please specify the High availability/Clustering requirements for below points;		
	a. Do you require High availability for Splunk access?	N/a	
	b. Do you require High availability/Clustering For data?	N/a	
	c. Is DC/DR Scenario to be considered?	N/a	
6	Number of users going to access Splunk Console (Search Head) and their purpose?		
	Number of Analyst	1	
	Number of Administrator	4	
	Number of End Users		
7	Number of "concurrent" users accessing the Splunk Console on a daily basis?	2	
8	Number of Users needed trainings on Splunk and what level? User Level OR Administrative Level	4	Administrator
	Splunk Fundamental 1		
	Splunk Power User Fast start		
	Splunk Enterprise System Administrator	4	
	Splunk Enterprise Data Administrator		
	Troubleshooting Splunk Enterprise		
	Splunk Enterprise Cluster Administrator		
	Splunk Architect		

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

SAHPRA
South African Health Products Regulatory Authority

Data Source	Number of Servers, Appliances or Applications
Active Directory	4 Domain controllers
Apache Server	n/a
Application Servers	n/a
Aruba Networks	n/a
AWS/AZURE	On-prem Adsync to Azure
Bluecoat ProxySG	n/a
box.com	n/a
Cisco ACS	n/a
Cisco ASA	n/a
Cisco ESA	n/a
Cisco FWSM	n/a
Cisco IPS	n/a
Cisco ISE	n/a
Cisco Router	n/a
Cisco Swtich	25
Cisco WLC	2
Cisco WSA	n/a
F5 WAF	n/a
FireEye	n/a
Fotigate	2
HP Tippingpoint	n/a
HP-UX Server	n/a
Infoblox DDI	n/a
Juniper SRX	n/a
Linux Server	n/a
McAfee Email Gateway	n/a
McAfee EPO	n/a
Microsoft DNS	4
Microsoft Exchange	MS O365
Microsoft IIS	10
MSSQL Server	6
MySQL Server	1
Office365	Yes
Oracle Server	6
Palo Alto Networks Firewall	n/a
Symantec Brightmail	n/a
Symantec CSP	n/a
Symantec Endpoint Protectic	n/a
Tripwire	n/a
Vmware ESX	5
Vmware vCenter	2
WebSense Content Gateway	n/a
Antivirus	Bitdefender gravityzone

QUESTION AND ANSWERS: SAHPRA/2024/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION/RFB004

Sl.No	Questions	Response
1	What is the deployment Type?	
2	Deployment - Operating System	*Windows Server*
3	Indexer clustering	
4	Search head clustering	
5	List of add-ons to be installed/configured (from Splunkbase)	
6	List of devices, make/model and Count for integration with Splunk	*SAHPRA devices* *Cisco C9200L-24P-4X x 21, Cisco C9300-24UX x 1, Cisco C9404R x 2* *Dell Networking N4032 x 3* *Windows Server 50, Firewall Fortigate 2,* *Antivirus - Bitdefender gravityzone, ESXi x 5, WLC Cisco 3500 x 2*
7	List of apps to be installed/configured (from Splunkbase)	
8	List of other integrations with Splunk	
9	List of Use cases to be implemented with Splunk	*Only Default*
10	List of dashboards to be configured	*Only Default*
11	List of Splunk Modules	*1.Splunk Enterprise* *2.Splunk Enterprise Security* *3. Splunk ITSI*
12	Splunk license capacity	*1.Splunk Enterprise - 30GB* *2.Splunk Enterprise Security – 30GB* *3. Splunk ITSI*
13	Retention Policy (Searhable and Archived)	
13	Implementation location	
14	Expected Project Start Date	
15	Expected Production Go-live Date	
17	Project Management to be included?	
16	Any other available relevant details	