BID TITLE: SECURITY INFORMATION EVENT MANAGEMENT (SIEM)

BID NUMBER: FAIS2023/24 – T002

QUESTIONS AND RESPONSES

LINE	QUERY	ANSWER
1	Number of devices that will report to the SIEM solution.	112 IP's
2	Type of devices, printers, firewalls, Switches, Endpoints and so on.	Laptops – acer and dell, servers- Dell ,printers- bizhub, IP Phones, switches, access points and firewall and core switch.
3	If possible, the number of EPS (events per second) per device?	N/A
4	Number of devices that will report to the SIEM solution.	112 IP's
5	Is foreign bidding allowed?	Yes. Ensure you comply fully with requirements outlined in the tender document.
6	Are you looking for onsite services or remote services?	Please proposed the best solution as per the FAIS Ombud infrastructure.
7	Number of Assets covering in SIEM?	112 IP's
8	Are you looking for Cloud based solution or on premise?	Please propose the best solution for FAIS Ombud. Note that some applications are on premise and some on cloud.
9	Please can you tell us how many Firewalls, Switches, proxies and Active Directories you have.?	1 Sonicwall firewall, 4 Switches , 1 Proxy and 1 Active Directory.

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

10	Do you currently have a DR for continuity?	Yes
11	25.1.1.1: Kindly furnish the comprehensive count of devices necessitating monitoring within the Security Information and Event Management (SIEM) system. As the SIEM operates based on events per second, this device count is crucial for strategic planning of license procurement.	112 as There are 112 IP's Scanned each month.
12	26.1.1.2: Could you confirm whether the FAIS is equipped with a Vulnerability Assessment tool, or if it is incumbent upon us to supply the tool and execute the requisite scans?	Supplier must use their own tools
13	26.1.1.3: Please clarify if FAIS possesses a dedicated vulnerability assessment tool for evaluating websites, or if we are required to furnish the tool for conducting the requisite scans.	Supplier must use their own tools
14	26.1.3.1: Is there an existing pentesting tool or Business Application Security (BAS) tool within FAIS for conducting penetration tests, or is it necessary for us to provide the requisite tools?	Supplier must use their own tools
15	26.1.3.2: Could you ascertain if FAIS is equipped with a social engineering tool, or if it is necessary for us to supply the tools for this purpose?	Supplier must use their own tools

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

16	There's a mention for install on site at FAIS would you consider a SAAS or cloud hosted SIEM?	The service provider is expected to propose best solution for the organization looking at the current infrastructure as mentioned on the tender document.
17	Can the SIEM solution be deployed to the existing Virtual Infrastructure? What is the Virtual Infrastructure. VMware / Hyper-V and is there capacity to deploy Forti SIEM if this route is taken vs point above.	Im not sure if I understand the question. Please ask the service provider to elaborate more.
18	How long do they need to keep the data? Online and archived?	Through out the duration of the contract
19	looking at the SIEM calculator you have under 50 devices, must we just go with the base license for 50 devices and 25 agents for the windows stuff and the standard 500 EPS which is included in the base license?	The service provider is expected to propose best solution for the organization looking at the current infrastructure as mentioned on the tender document.
20	Can we go with the VM option with the base license? unless you would require the hardware option.	The service provider is expected to propose best solution for the organization looking at the current infrastructure as mentioned on the tender document.
21	Kindly assist us with the following information relating to your log sources (not individual users pc's as an example, since we normally only poll the AV management server etc) for this opportunity.	
	Device type	Device count
	Windows Domain Server	2
	Windows Application Server	3
	Linux Server	N/A

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

Exchange Server track logs	N/A
Web Server	3
DNS Server	2
DHCP Server	1
Windows DB Server	4
Linux DB Server	N/A
VM Ware	5
Database (SQL) Server	1
Application Servers	3
Vulnerability Scanner	N/A
Load Ballancer/Web FW	N/A
WLAN Controller	1
Next Gen Firewall - Large	1
Next Gen Firewall - Medium	N/A
Next Gen Firewall - Small	N/A
Firewall - Large	1
Firewall - Medium	N/A
Firewall - Small	N/A
Network IDS/IPS - Large	1
Network IDS/IPS - Medium	N/A
Network IDS/IPS - Small	N/A
Web App Firewall - Large	1
Web App Firewall - Medium	N/A

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

	Web App Firewall - Small	N/A
	Web Proxy	1
	Network Switch Netflow enabled	N/A
	Network Switch	4
	Network Router	2
	VPN (if not on FW)	1
	Antispam/eMail GW	1
	End Point/Desktops Monitoring	71
	FSM Adv. Agent FIM	0
	Antivirus on Servers (just app)	7
	Antivirus on End Points (just app)	71
22	Please provide clarity on the following: Please confirm the below details for the number of network devices.	
	Device Type	**Device Count**
	Windows Domain Controller	2(Primary & Secondary)
	Windows Application Server	3
	Windows Exchange Server Logs	N/A
	Windows IIS Web Server	3
	Windows DNS Server	2
	Windows DHCP Server	1
	Windows Database Server	4
	Linux Application Server	N/A

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

Linux Email Server	N/A
Linux (Apache) Web Server	N/A
Linux DNS Server	N/A
Linux DHCP Server	N/A
Linux Database Server	N/A
Other FSM agent features eg FIM	N/A
VMWare ESX Host	5
AV Manager / Vulnerability Scanner	1
Load Balancer/Web FW	N/A
WLAN Controller	1
Next Gen Firewall - Large	1
Next Gen Firewall - Medium	N/A
Next Gen Firewall - Small	N/A
Firewall - Large	1
Firewall - Medium	N/A
Firewall - Small	N/A
Network IDS/IPS - Large	1
Network IDS/IPS - Medium	N/A
Network IDS/IPS - Small	N/A
Web App Firewall - Large	1
Web App Firewall - Medium	N/A
Web App Firewall - Small	N/A

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

	Web Proxy	1
	Network Switch Netflow enabled	N/A
	Network Switch	4
	Network Router	2
	VPN (if not on FW)	1
	Antispam/eMail GW	1
	AV on Server or Endpoint	71
	FSM UEBA Endpoint Agent	0
23	We would like to confirm your preferred service option: a) Onsite Service b) Managed Server/On-Premise Solution	I think providing preference to the service provider will be disadvantaging other service provider who will be bidding for this tender. I suggest that the service provider look at our infrastructure provided and propose the best suited solution for the organization.
24	Number of Core / External / DMZ Firewalls? Please mention if they are HA.	N/A
25	Number of Internal / Data Centre Firewalls? Please mention if they are HA.	1 Sonicwall NS2700
26	Number of Branch Firewalls? Please mention if they are HA.	N/A
27	Number of Windows Servers?	8
28	Number of Linux Servers?	N/A
29	Number of Proxy Servers?	1
30	Number of VPNs?	1

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

31	EDR / Antivirus Servers?	1
32	Active Directory Servers?	2
33	DNS Servers?	2
34	DHCP Servers?	1
35	Cloud Workloads?	I do not understand what they are looking for
36	As it is mentioned to install on site at FAIS. Would you consider a SAAS, or cloud hosted SIEM ?	it will be best for the supplier to propose the best solution since they know the advantages and disadvantages?
37	Can the SIEM solution be deployed to the existing Virtual Infrastructure ? What is the Virtual Infrastructure .i.e. VMware / Hyper-V .	FaisOmbud do not have their own virtual servers.
38	How long do you need to keep the data ? Online and Archived ?	90 days
39	Firewalls- How many firewalls do you have in place and what make and model are they, please specify if any are in High Availability.	1X Sonicwall NS2700 High Availability
40	Network switches- What make and model they are?	2x HP Managed Switches 1x HP Aruba Core Switch
41	Anti-Virus- just to clarify, you are using ESET for your Anti-Virus?	Yes
42	With regards to point 24.2, please could you specify how many servers are internal and how many are external.	6 Internal Servers
43	How many cloud instances, workspaces and tenants do they have?	1XTenant, 4XCloud Instances, 4X Environments
44	Do you a timeline to finalise their migration to the cloud?	Sage has been migrated

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za

45	Do you currently have a virtual environment and what virtualisation technology are they using?	Hybrib Environment VMware ESXI
46	What have any MDR or XDR tools?	Manage Engine Log 360 looks at all servers.

Menlyn Central Office Building, 125 Dallas Avenue, Waterkloof Glen, Pretoria 0010
P O Box 41, Menlyn Park, 0063
Phone: (012) 762 5000; Fax: (012) 348 3447 / (012) 470 9097 Sharecall 086 066 3274
www.faisombud.co.za