Central Bank of The Bahamas Response to Vendor Questions

Re: ISU20211004 - Acquisition and Implementation of a Next Generation Security Incident and Event Monitoring Solution

Question: What we required is any information in order to get a sizing on your needs. If you have the amount of EPS required.

Answer: The Bank projects that the solution would require the capacity to manage approximately 15,000 EPS.

Question	RFP Reference	Answers
What are the compliance requirements in terms of standards? PCI / ISO27001?	4.1	N/A
What standard is the bank following for the controls implementation?	4.1	ISO 270001
How many assets and what are the types of assets on each site of the bank which you plan to integrate with the SIEM solution? If possible, please fill our the attached architectural discovery document.	4.2	See site information listed in the Architectural Discovery Document
How many Windows & Linux Servers are being planned to be integrated?	4.2	Approximately 250
What are the roles of the servers in the environment mentioned in question 4?	4.2	See site information listed in the Architectural Discovery Document

How many parameter devices (such as IDS/IPS, Firewall, Routers etc.)?	4.2	4
How many custom applications to be integrated with non-standard log format? What kind(s) of log format?	4.2	Approximately 10
Any other device in the environment that will be integrated with SIEM?	4.2	Physical Access Control System and Meeting Room Video/Teleconferencing Software
How are the sites (production and DR) connected to each other? (i.e. site to site VPN? If not VPN, please advise)	4.2	Combination of MPLS and secure VPN connections between sites
If not sure about Compliance What is retention period for the data?	4.1	At a minimum, 3 months of hot log data storage and 1 year of cold log data storage
What is the SLA Expectation?	4	24/7
FIM Requirement is for how many servers/Nodes (all or certain critical nodes)?	6.1	Approximately 100 Windows based systems, 30 Linux servers, and 2 AS/400 LPAR's.
Threat Intelligence - does the bank expect to have paid subscription to threat feeds? Such as CrowdStrike, Symantec, Cisco AMP Threat Grip, etc.?	6.6	Yes
What version of OS is running on the IBM platform?	4.1	N/A
For the Hybrid managed option, how do you envision the hybrid option to look? For example, from our experience: customer is responsible for management during business hours and service provider takes over responsibility after business hours.	4.3.1	The hybrid managed option that the Bank would like to engage in 24/7 coverage that would enable the Bank's internal team to manage the solution during business hours with the option to escalate to the MSSP for incidents over a certain severity level.

Question	Response	Comments
Number of Sites	2	There are also approximately 15 VPN tunnels connecting to third-parties.
Number of Network Users	300	Great than 300 network users
Number of Domains	1	
Number of DMZs	2	
Compliance Requirements: PCI, HIPAA,SOX, etc.	N/A	
High Availability – Primary Site	Yes	The bank requires that in an instance where the primary site goes down that the secondary site can failover to allow for Business Continuity.
High Availability – Remote Site (s)	YES	
Additional System Features (Optional): **1. Network Monitoring** **2. Process Monitoring** **3. User Activity Monitoring** **4. Data Loss Defender**	Yes, options 1, 2, and 3	

Question	Response
Number of Identical-Sites	N/A
Location Site 1	Main Site
Location Type	Primary
Main Site Question	**Quantity**
1. Operating System Information:	
Windows Server	354
Windows Workstation	350
Windows Domain Controller	2
iSeries	1
Other Operating System	48
2. Applications:	
Email	2

Database	20
Web Server	30
Web Server	30
Proxy	N/A
Antivirus/Security Application	1
POS Software	N/A
Other Application	N/A
3. Network Devices:	
Firewall	4
Router	N/A
Switch	30
IDS/IPS	N/A
VPN Appliance	N/A
Load Balancer	2
Other Network Device	N/A

Question	**Response**
Number of Identical-Sites	N/A
Location Site 2	DR Site
Location Type	Secondary
Main Site Question	**Quantity**
1. Operating System Information:	
Windows Server	177
Windows Workstation	N/A
Windows Domain Controller	2
iSeries	1
Other Operating System	66
2. Applications:	
Email	2
Database	30
Web Server	20
Proxy	N/A
Antivirus/Security Application	1
POS Software	N/A
Other Application	N/A

3. Network Devices:	
Firewall	4
Router	N/A
Switch	10
IDS/IPS	N/A
VPN Appliance	N/A
Load Balancer	2
Other Network Device	N/A