BANCO CENTRAL DE HONDURAS
AL SERVICIO DE LA NACIÓN

Centro Cívico Gubernamental, Bulevar Fuerzas Armadas
Teléfono: (504) 2262-3702, Apartado Postal #3165
Tegucigalpa, Honduras, C.A., www.bch.hn

Tegucigalpa, MDC,
8 de marzo de 2022

ABN-2148/2022

Señores
OFERENTES
Ciudad

Ref.: Licitación Pública No.04/2022

Estimados señores:

Hacemos referencia a la Licitación Pública No.04/2022, para la contratación del suministro, instalación, configuración, puesta en funcionamiento y capacitación de una (1) solución denominada Next Generation Security Information and Event Management (SIEM), para colectar, almacenar y analizar eventos o bitácoras de servidores, equipo de telecomunicación, base de datos, equipos de seguridad y aplicaciones del Banco Central de Honduras; al respecto, se les informa que se han efectuado las consultas siguientes:

Consulta No.1:

"¿El banco permite que al ser una plataforma de SIEM en premisa, pudiera darse que la capa de colección sea en premisa y que la capa de análisis de comportamiento de usuario (UEBA) pueda ser en la nube del mismo fabricante?".

Respuesta
La capa de análisis de comportamiento de usuario (UEBA) debe ser on-premise.

Consulta No.2:

"Teniendo en cuenta que:

1. *En caja: el cliente tiene costos ocultos como espacio en DC, refrigeración, cableado estructurado, monitoreo.*
2. *En caja: el cliente tiene que contemplar la infraestructura para almacenar los logs de acuerdo a la retención que requiere, estamos hablando de dispositivos NAS o Storage que son externos al fabricantc de SIEM y que al ser parte activa del componente van a requerir inversión y administración de lado del cliente.*
3. *En caja: el cliente es responsable del SLA del servicio, es decir tiene que contemplar HA y DRP del hardware para poder operar con un SLA mayor a 99.5%.*
4. *El cliente tiene que contemplar repuestos en sitio, y pagarlos por adelantado.*

Adicional a esto, con todo este problema de supply chain a nivel global los tiempos de entrega de Hardware son de más de 180 días, y los repuestos.

Sabiendo todo esto consultamos podríamos ofertar un ambiente hibrido, en el cual la capa de recolección se haga en premisa, ¿y la inteligencia, procesamiento y correlación en nube?".

Respuesta
La capa de inteligencia, procesamiento y correlación debe ser on-premise.

Consulta No.3:

"3.1.6 Alcance de la Solución.
Brindar un listado de los dispositivos por cada tipo y que tecnología
3.1.6.1.1-2-3-4-5-6".

Respuesta
Dicha consulta fue atendida mediante nota aclaratoria ABN-2079/2022 del 03/03/2022 y publicada en la dirección electrónica:https://www.bch.hn/administrativas/ABN/LIBAdquisiciones/Aclaratoria%20No.1-LPU%20No.04-2022.pdf.

Consulta No.4:

"3.1.9.1 Se menciona un sistema Progress, que versión es y como éste genera los logs para hacer una validación sobre la integración con el SIEM".

Respuesta
Dicha consulta fue atendida mediante nota aclaratoria ABN-2079/2022 del 03/03/2022 y publicada en la dirección electrónica:https://www.bch.hn/administrativas/ABN/LIBAdquisiciones/Aclaratoria%20No.1-LPU%20No.04-2022.pdf.

Consulta No.5:

"Según lo establecido en el punto 3.1, inciso 3.1.6 descrito en la página 60 indica que la solución inicialmente debe ser configurada para colectar, almacenar y analizar los eventos o bitácoras de los activos catalogados como críticos. Podrían, por favor, indicarnos lo siguiente:

- *Cantidad total de servidores en la red (no importa si se piensan monitorizar o no, por favor brindar el número total de servidores), esto con el fin de evaluar el método óptimo de licenciamiento.*
- *Cantidad de usuarios en la red del Banco.*
- *Cantidad de equipos que deben ser integrados al SIEM.*
- *Especificar marca, modelo y versión de los equipos que se deben integrar. Para efectos, podrían completar el siguiente cuadro:"*

Equipo/Fuente de log	***Marca***	***Versión/Modelo***	***Ubicación***

Respuesta

- Entre 100 y 150 servidores.
- Entre 950 y 1500 usuarios.
- De ser posible se espera integrar inicialmente entre 120 y 172 equipos.

Equipo/Fuente de log	**Marca**	**Versión/Modelo**	**Ubicación**
Servidores-Sistema Operativo	Windows, Linux y Unix	Se indican en las Especificaciones Técnicas, Numeral 3.1.9	Edificio Principal y Sucursales
Servidores-Aplicación	.Net, Java, SAP/ERP, entre otros		
Servidores-Base de Datos	Oracle, SQL Server, entre otros		
Switches Core	Cisco	Series Nexus	
Switches	Cisco	Series Catalyst	
Wireless LAN Controller	Cisco	Series 5500	
Firewalls	Cisco, Juniper, Fortinet, entre otros	ASA, SRX, Fortigate	

Nota: Los valores proporcionados son estimaciones, considerar lo indicado en el numeral 3.1.9.3 del Pliego de Condiciones de la Licitación Pública No.04/2022.

Consulta No.6:

"Sección VI. Lista de Requisitos
Numeral 3. Especificaciones Técnicas
3.1 Condiciones, Especificaciones y Requerimientos Técnicos
Con el objetivo de validar la compatibilidad nativa de las tecnologías a integrar y verificar el almacenamiento correcto de las bitácoras procesadas en el período no menor de 3 meses solicitados en los puntos 3.1.3, 3.1.5, 3.1.6 y 3.1.9, agradeceremos que nos detallen las fuentes de datos a monitorizar con el siguiente detalle:

1. *Throughput en la red local: (En Gbps):*
2. *Información detallada de las fuentes de datos a integrar:"*

Tipo de Tecnología	***Sistema Operativo/Marca***	***Versión***	***Cantidad***	***Configurado en HA?***	***Físico/Virtual***	***Observaciones***

Respuesta

1. En la actualidad no se posee ese dato; sin embargo, su oferta debe apegarse a lo requerido en el pliego de condiciones.
2. Información detallada de las fuentes de datos a integrar:

Tipo de Tecnología	**Sistemas Operativo/Marca**	**Versión/Modelo**	**Cantidad**	**Configurado en HA**	**Físico/ Virtual**	**Observaciones**
Servidores-Sistema Operativo	Windows, Linux y Unix	Se indican en las Especificaciones Técnicas, Numeral 3.1.9	De ser posible se espera integrar inicialmente entre 120 y 170 equipos	No	Si	Edificio Principal y Sucursales
Servidores-Aplicación	.Net, Java, SAP/ERP, entre otros			No	Si	
Servidores-Base de Datos	Oracle, SQL Server, entre otros			No	Si	
Switches Core	Cisco	Series Nexus		Si	No	
Switches	Cisco	Series Catalyst		No	No	
Wireless LAN Controller	Cisco	Series 5500		Si	No	
Firewalls	Cisco, Juniper, Fortinet, entre otros	ASA, SRX, Fortigate		Algunos Si	Ambos	

Nota: Los valores proporcionados son estimaciones, considerar lo indicado en el numeral 3.1.9.3 del Pliego de Condiciones de la Licitación Pública No.04/2022.

Consulta No.7:

"1. En referencia al numeral 3.1.8.1 Favor indicar cuantos dispositivos se deberán integrar para que el banco acepte de conformidad cierre proyecto. Asimismo, detallar: Tipo de dispositivo, marca y modelo."

Respuesta

De ser posible se espera integrar inicialmente entre 120 y 170 equipos.

Equipo/Fuente de log	**Marca**	**Versión/Modelo**	**Ubicación**
Servidores-Sistema Operativo	Windows, Linux y Unix	Se indican en las Especificaciones Técnicas, Numeral 3.1.9	Edificio Principal y Sucursales
Servidores-Aplicación	.Net, Java, SAP/ERP, entre otros		
Servidores-Base de Datos	Oracle, SQL Server, entre otros		

Equipo/Fuente de log	Marca	Versión/Modelo	Ubicación
Switches Core	Cisco	Series Nexus	Edificio Principal y Sucursales
Switches	Cisco	Series Catalyst	
Wireless LAN Controller	Cisco	Series 5500	
Firewalls	Cisco, Juniper, Fortinet, entre otros	ASA, SRX, Fortigate	

Nota: Los valores proporcionados son estimaciones, considerar lo indicado en el numeral 3.1.9.3 del Pliego de Condiciones de la Licitación Pública No.04/2022.

Consulta No.8:

"2. En referencia al numeral 3.1.31.1. La capacitación teórica puede ser impartida de manera virtual?"

Respuesta
Si.

Consulta No.9:

"3. En referencia al numeral 3.1.29.1. La funcionalidad que se solicita del SIEM es tener capacidades de File Integrity Monitor (FIM) para la auditoria de archivos de servidores/aplicaciones? En caso ser afirmativo favor indicar cantidad y tipo de servidores/aplicaciones"

Respuesta
Si, entre 10 y 15 servidores, el tipo es el indicado en el numeral 3.1.9 de las Especificaciones Técnicas del pliego de condiciones.

Nota: Los valores proporcionados son estimaciones, considerar lo indicado en el numeral 3.1.9.3 del Pliego de Condiciones de la Licitación Pública No.04/2022.

Atentamente,

BANCO CENTRAL DE HONDURAS
ADQUISICIONES Y CONTRATACIONES
Al Servicio de la Nación

OMAR HUMBERTO ZÚNIGA ZÚNIGA
Secretario de la Comisión de Compras y Evaluación y
Jefe Departamento de Adquisiciones y Bienes Nacionales

IMP/TMG