Tegucigalpa, MDC
12 de octubre de 2021

ABN-10529/2021

Señores
OFERENTES LICITACIÓN PÚBLICA No. 49/2021
Ciudad

Estimados señores:

Referente a la Licitación Pública No.49/2021, para la contratación del suministro, instalación, configuración, puesta en funcionamiento y capacitación de una (1) solución denominada Security Information and Event Management (SIEM) de próxima generación con funcionalidad XDR para colección y análisis de eventos o bitácoras de servidores, equipo de telecomunicación, base de datos, equipos de seguridad y aplicaciones del Banco Central de Honduras; así como a consultas recibidas mediante nota del 22 de septiembre de 2021, a continuación, se informa lo siguiente:

Consulta 1:
De acuerdo el requerimiento expresado en el punto 3.1.6 de la página 61, solicitamos nos proporcionen la siguiente información, con el objetivo de realizar un dimensionamiento apropiado del proyecto:

a. Cantidad de Eventos por Segundo que requieren monitorizar.
b. Cantidad de servidores en la red.
c. Cantidad de estaciones de trabajo (desktops/laptops en la red).
d. Cantidad de usuarios en la red.
e. Completar el siguiente cuadro con los activos que desean monitorizar:

Tipo de dispositivo (Firewall, IPS, DNS, AD, Bases de Datos, etc.)	***Cantidad***	***Ubicación (Sitios 1, Sitio 2, DMZ, Azure, AWS, etc.)***

f. Cantidad de casos de uso que requieren configurar en el SIEM.
g. Cantidad de Playbooks de automatización de respuesta a incidentes que requieren configurar en la plataforma.
h. Cantidad de usuarios que ingresarán al portal de orquestación y respuesta a incidentes.

Respuestas

a. 15k EPS mínimo.
b. Entre 250 y 300 servidores en la red.
c. Entre 1500 y 1900 estaciones de trabajo.
d. Entre 950 y 1500 usuarios en la red.
e.

Tipo de dispositivo (Firewall, IPS, DNS, AD, Bases de Datos, etc.)	**Cantidad**	**Ubicación (Sitios 1, Sitio 2, DMZ, Azure, AWS, etc.)**
Firewall	30	Ubicados en Centro de Datos Principal y Alterno.
Switch Capa 3	5	
Switch Capa 2	116	
Wireless Controller	2	
AD	Incluidos en el inciso b.	
Bases de Datos		
DNS		

Nota: en las cantidades indicadas están incluidos los activos críticos que deben ser configurados inicialmente en la solución según se indica en la condición 3.1.6 Alcance de la Solución

f. Entre 35 y 40 casos de uso.
g. Entre 10 y 15 Playbooks de automatización de respuesta a incidentes.
h. Entre 8 y 10 usuarios.

Consulta 2:
De acuerdo el requerimiento expresado en el punto 3.1.9 de la página 62, el cual indica lo siguiente:

"La colección de datos de los equipos antes descritos debe realizarse basada en agentes, con lo cual no afecta
en gran medida el rendimiento de la red."

Existen soluciones de correlación de eventos que además del uso de agentes, utilizan métodos o protocolos adicionales, dependiendo de la fuente de datos, con el objetivo de optimizar y enriquecer la información a ser analizada sin afectar significativamente el rendimiento de la red. ¿Aceptarían una solución que utilice la combinación de agentes y métodos adicionales?

Respuesta
Si

Consulta 3:
Con respecto requerimiento expresado en el punto 3.1.22 de la página 65, es claro que el objetivo que busca el Banco Central de Honduras es proteger la integridad de los datos almacenados:

"La solución debe tener la capacidad de cifrar y aplicar algún algoritmo a los datos de archivo de registro de actividades antes de almacenarlos en la base de datos, todo esto para mantener la integridad de los mismos y puedan ser confiables en la investigación forense de incidentes de seguridad."

Como es de su conocimiento, existen soluciones que tienen la capacidad de proteger la integridad y controlar el acceso a los datos asociados a los eventos e incidentes de seguridad almacenados en la solución SIEM. Estos métodos son aceptados en la industria, ya que ofrecen el nivel de inmutabilidad necesario para que la información no sea vulnerada y sea confiable para llevar a cabo la investigación forense de incidentes. ¿Aceptarían una solución que utilice estos mecanismos alternos de protección y resguardo de la información sensible?

Respuesta
Se podría considerar la solución, previa evaluación.

Nota: los valores proporcionados son estimaciones, que podrán variar.

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/KAC/OMC