BCU
SERVICIOS INSTITUCIONALES
Gestión de Bienes y Servicios

CONSULTAS Y SOLICITUDES DE PRÓRROGA RECIBIDAS EN EL MARCO DE LA LICITACION ABREVIADA Nº 202-LA-PC-00013

OBJETO: Adquisición e instalación de una solución de seguridad para prevención de ataques de día cero (sandbox) incluyendo un año de garantía y un año de soporte de hardware y software conforme a lo establecido en este Pliego de Bases y Condiciones Particulares.

- Consulta 1

Referencia: Técnico
Anexo III.
Consulta:
Por este medio hacemos llegar a ustedes las siguientes consultas con respecto a la licitación de referencia:

1. Considerando que al día de hoy las soluciones virtualizadas ofrecen mayor flexibilidad desde el punto de vista de escalabilidad y crecimiento a futuro, ¿BCU acepta soluciones de sandbox virtualizadas?
2. En caso de responder afirmativamente a la consulta anterior, ¿se deberá suministrar el servidor junto con la solución? ¿o es posible alojar la solución en servidores ya existentes del BCU?

Respuesta: No, sólo hardware appliance on premises en línea a lo mencionado en el Anexo III del pliego de bases y condiciones particulares.

- Consulta 2

Referencia: Técnico
Anexo III.
Consulta:

1- Qué tipo de integración requieren hacer sobre Trend ISMVA y FrotiMail? Agradecemos dar mayores detalles al respecto.

Respuesta: La posibilidad de bloquear temporalmente correos electrónicos entrantes con adjuntos hasta tanto no se tenga un veredicto del análisis de esos adjuntos por parte del sandbox, sin requerir de un componente externo a la solución para su integración. Ese veredicto determinará el bloqueo permanente o no del correo electrónico asociado.

2- Con respecto a la "Capacidad de análisis de archivos provenientes de servidores de archivo corporativos". Por favor explicar mejor este caso de uso ¿es requerido que se tenga un agente en el servidor que analice archivos en un servidor de archivos?

Respuesta: No es requerido un agente sino contar con la posibilidad de análisis de archivos bajo demanda.

3- Con respecto al punto en que se solicita "Licenciamiento de las múltiples instancias de análisis con soporte de al menos 2 imágenes de sistemas

operativos personalizadas provistas por el Banco Central (Windows, Linux)", por favor indicar versiones específicas de dichos sistemas operativos.

Respuesta: Plataforma Windows: versiones 7, 10, 2016, 2019. Plataforma Linux: RHEL 7,8 o superior y CentOS 7,8 o superior.

- Consulta 3

Referencia: Técnico
Anexo III.
Consulta:

En relación al objeto del pliego, solicitamos:

Se solicita a la entidad ampliar el alcance de la adquisición e instalación de una solución de seguridad de prevención de ataques de día 0 basada exclusivamente en sandbox a una solución de seguridad de prevención de ataques de día 0 basadas en otros mecanismos de detección más sofisticados y con menos probabilidad de evasión, como la inteligencia artificial y machine learning no supervisado, basado en el comportamiento de los dispositivos de la red y el modelamiento de tráfico.
Las soluciones de detección de amenazas basadas exclusivamente en sandbox son potencialmente evadidas por las amenazas persistentes avanzadas que utilizan novedosas técnicas conocidas y/o propias de sus operaciones de seguridad, lo que minimiza el campo de protección para las organizaciones.
Se sugiere a la entidad ampliar el alcance para permitir soluciones de detección y protección de amenazas de día 0 que se basen en la inteligencia artificial y el machine learning no supervisado, modelando el comportamiento de todos los dispositivos de la red, con el fin de maximizar la protección solicitada y minimizar los riesgo de evasión y no detección de dichas amenazas.

Respuesta: Agradecemos la sugerencia pero el alcance es el mencionado en el objeto del pliego de bases y condiciones particulares de acuerdo a lo dispuesto en el literal 3.1 inciso final del Capítulo II del referido pliego: "La omisión de la cotización de alguno de los conceptos especificados en el Anexo II o su presentación en una modalidad diferente a lo establecido invalidará toda la oferta. Cualquier otra observación o propuesta alternativa que la empresa considerase necesario agregar, deberá formularse en forma separada"