Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 384307 - ADQUISICIÓN DE SOLUCIONES DE CIBERSEGURIDAD

Consulta 1 - ITEM 1

Consulta	Fecha de Consulta	09-09-2020

En la sección 1.2.19 donde dice "Debe permitir reducir falsos positivos y evaluar de forma dinámica el nivel de riesgo considerando la habilidad de unificar y correlacionar: Eventos, información proveniente de herramientas de análisis de vulnerabilidades y criticidad de los activos o dispositivos."
Solicitamos respetuosamente aclarar si la solución debe incluir incluir un modulo de vulnerability. En caso de no incluir. Solicitamos atendiendo el monto del proyecto que la solución deba incluir el modulo de vulnerability, ya que consideramos esencial para la prevención de incidentes de ciberseguridad.

Respuesta	Fecha de Respuesta	10-09-2020

Favor ajustarse a las especificaciones técnicas establecidas en el PBC. En el mismo no se solicita ningún módulo adicional de gestión de vulnerabilidades. Sin embargo, se exige que la solución SIEM soporte plena integración con soluciones de gestión de vulnerabilidades especializados, a fin de que la información de estas soluciones pueda ser utilizada en la correlación, detección temprana y mitigación de eventos e incidentes de ciberseguridad.

Consulta 2 - ITEM 1

Consulta	Fecha de Consulta	11-09-2020

1.1.7 Dice "Debe poseer capacidad propia (almacenamiento integrado) que permita almacenar estos eventos por lo menos por 6 meses y capacidad para conectarse a una solución SAN redundante por iSCSI (10GbE UTP), para aumentar su capacidad de almacenamiento"

Solicitamos respetuosamente a la convocante poner como opcional, la capacidad de conectase a un storage SAN e indicar la necesidad máxima de storage para almacenamiento del appliance. Encontramos que este punto limita la oportunidad de otras soluciones distintas a splunk por lo que reduce la cantidad de oferentes.

1.1.6
Debe soportar el crecimiento a por lo menos 18.000 EPS, pudiendo ser estos activados solo con la introducción de alguna clave y/o licencia y sin que sea necesario cambiar de dispositivo o agregar hardware al mismo.

El crecimiento en la capacidad de análisis EPS va muy de la mano en la cantidad del hardware disponible. Solicitamos indicar la capacidad de EPS máximo a modo de adecuar el hardware a lo solicitado.

Respuesta	Fecha de Respuesta	11-09-2020

Favor ajustarse a las especificaciones técnicas establecidas en el PBC. El Banco Central ha invertido de manera sostenida en los pasados años en capacidad de almacenamiento externo de tecnología especializada, por lo cual es requerido que la solución ofrecida soporte almacenamiento externo con el tipo de conexión indicada. Esto se alinea a nuestros objetivos de contar con toda información relevante para investigaciones forenses de ciberseguridad, aprovechando al máximo la inversión ya efectuada. No se establece un crecimiento máximo de la plataforma, en el entendido de que los requerimientos mínimos son suficientes para el planeamiento realizado para los próximos 3 años, además de no limitar la participación de ningún oferente.

Consulta 3 - Consulta licencias

Consulta	Fecha de Consulta	23-09-2020

en el punto 2.1.2 hace referencia a
Se requiere una solución de Protección de Bases de Datos (Firewall de Base de datos) basado en agente o agente-controlador para al menos 20 instancias de base de datos

Podría la convocante aclarar el numero de servidores ya sean físicos o virtuales donde corren las instancias de Base de Datos, ya que nuestra solución no se licencia por instancias, sino por cantidad de servidores de DB.-

Respuesta	Fecha de Respuesta	23-09-2020

"Tal como establece el PBC, la cantidad mínima de instancias de base de datos requeridas es de 20 (veinte); favor considerar que, en atención a las buenas prácticas de seguridad, siempre es recomendable instalar un servidor principal y uno secundario para cada instancia a fin de soportar HA".

Consulta 4 - Consulta de Solucion SIEM

Consulta	Fecha de Consulta	28-09-2020

- (Item 1.1.3 + 1.1.9 + 2.1.3 + 2.1.5)Tanto para SIEM como para el firewall de la base de datos, el cliente solicita el hardware y luego informa que hará que el hardware esté disponible.
- (item 1.5.2) El cliente solicita solo mantenimiento, pero no informa la respuesta al incidente. Podría preguntarle al cliente si solo espera soporte de configuración SIEM? El texto deja en claro que no está pidiendo un equipo de respuesta a incidentes.
- (Item 1.1.25) Cliente no habla cual herramienta de ITSM tenemos que hacer la implantacion de SIEM y Firewall de banco de datos. Es nuestro ITSM o del cliente? Si es la solución del cliente, cuál sería?
- Es conocido, que en el mercado solo una marca de SIEM licencia por flujos por minuto. En el requerimiento 1.1.5 se menciona que se debe soportar una cantidad de EPS y, al mismo tiempo, flujos por minuto. Por favor, especificar si se refiere que se puede licenciar por EPS y/o Flujos por minuto
- En el requerimiento 1.1.9 se solicita Alta Disponibilidad. ¿Ambos equipos de Alta Disponibilidad se encontrarán en un único sitio geográfico, o serán dos distintos?
- En el requerimiento 1.3.2, se solicita tener plantillas de reporte de estándares internacionales. ¿Cuáles estándares se necesitan?
- En el requerimiento 1.2.44 especifican "Debe permitir enlazar directamente fuentes externas como Bugtraq, ICE, CVE, Datastorm, MSDB y otros.". A que se refieren con enlazar directamente ? Que tipo de enlace ? Que esperan de este requerimiento funcional específicamente ?
- Por favor indicar los tiempos requeridos de retención de datos. Especificar retención online y offline teniendo en cuenta que la retención en línea se refiere a la cantidad de días en que se necesita tener la información inmediatamente disponible para búsquedas/correlación, y la retención offline corresponde la cantidad de días en que se necesita tener la información disponible en forma poco frecuente, en un archive externo que solo se consultará excepcionalmente. El requerimiento 1.1.7 menciona 6 meses de capacidad de almacenamiento pero no da mayores especificaciones. Este dato es fundamental para las definiciones de sizing y arquitectura.

Respuesta	Fecha de Respuesta	06-10-2020

1.1.3 Favor remitirse a lo establecido en el PBC. Conforme se indica en el mismo, en ambos Items el Proveedor deberá entregar todo el hardware necesario para la puesta en producción del equipamiento primario o principal. En el caso de que el BCP requiera el HA en el futuro, el hardware necesario será entregado por el BCP, por lo que esto no se solicita en el PBC.
1.5.2 Favor remitirse a lo establecido en el PBC. El soporte solicitado es para la implementación y mantenimiento de la herramienta ofrecida, lo que debe incluir soporte del fabricante.
1.1.25 Favor remitirse a lo establecido en el PBC. El propio de SIEM debe ofrecer las funcionalidades de gestión de incidentes y workflow. No se solicita ningún software adicional para este punto.
1.1.5 Favor remitirse a lo establecido en el PBC. Se aclara que el BCP está en conocimiento de que existen diferentes modelos de licenciamiento para soluciones SIEM: Por EPS, por cantidad de dispositivos, por FPM, por cantidad de conectores, por usuarios, entre otros. En el PBC se ofrece suficiente información de referencia para que cualquier solución reconocida del mercado pueda cotizar una versión de licenciamiento adecuada a las necesidades del BCP. Si desde el punto de vista del licenciamiento, el EPS o FPM no es relevante para el fabricante de la solución ofrecida, favor detallarlo en la oferta. Sin embargo, en ningún caso pueden ser limitantes de la funcionalidad requerida.
1.1.9 Favor remitirse a los términos del PBC. La solución debe soportar alta disponibilidad de modo integrado, sin necesidad de software de terceros.
1.3.2 Favor remitirse a la Adenda del PBC.
1.2.44 Favor remitirse a la Adenda del PBC.
1.1.7 Favor remitirse a la Adenda del PBC.

Consulta 5 - ITEM 1

Consulta	Fecha de Consulta	28-09-2020
En el punto 1.3.26 describen "Debe contar con una base preinstalada de reportes y permite creación de reportes distribuidos." A que se refieren con el concepto de "reportes distribuídos" ?		

Respuesta	Fecha de Respuesta	06-10-2020
Favor ajustarse a lo establecido en el PBC. Lo indicado significa que el SIEM soporta la funcionalidad de distribución de los reportes de manera automática a grupos o usuarios de interés.		

Consulta 6 - ITEM N°1 Solución SIEM

Consulta	Fecha de Consulta	30-09-2020
Para el Punto: 1.1.9. Favor confirmar si se requerirá configurar el/los appliances en modo HA desde el inicio de los trabajos o esta configuración se podrá hacer/entregar en etapas futuras del proyecto.		

Respuesta	Fecha de Respuesta	06-10-2020
Favor ajustarse a lo establecido en el PBC. No es requerido desde el principio del proyecto. Sin embargo, se deben prever los servicios para una fase o etapa futura.		

Consulta 7 - ITEM N°1 Solución SIEM

Consulta	Fecha de Consulta	30-09-2020
Punto: 1.1.16. Favor Indicar cual sería un caso de uso de correlación basados en machine learning o inteligencia artificial.		

Respuesta	Fecha de Respuesta	06-10-2020
Favor remitirse a lo establecido en la Adenda del PBC.		

Consulta 8 - ITEM N°1 Solución SIEM

Consulta	Fecha de Consulta	30-09-2020
Puntos: 1.2.15 y 1.2.23. Favor confirmar si para estos puntos se considerarán cubierto si se hace mediante la integración de una fuente de datos del cliente que traiga la información requerida.		

Respuesta	Fecha de Respuesta	06-10-2020
No. Favor remitirse al PBC. Para estas funcionalidades no debe ser requerida una fuente de información externa. La propia solución SIEM debe disponer de capacidades avanzadas de descubrimiento de aplicaciones, incluidas las Shadow IT, gracias a, por ejemplo, inspección de flujos de red o similares.		

Consulta 9 - ITEM N°1 Solución SIEM

Consulta	Fecha de Consulta	30-09-2020
Punto: 1.2.20. Si bien la herramienta de correlación no posee un asistente, posee un pool de casos de uso de fábrica que reduce la ocurrencia de estos eventos acelerando el proceso de puesta en marcha de la solución. ¿Se podría tratar esto como un caso equivalente a tener un asistente?		

Respuesta	Fecha de Respuesta	06-10-2020
No. Favor remitirse al PBC, en el cual se requiere que la solución SIEM soporte la definición de reglas de correlación a través de un Asistente.		

Consulta 10 - ITEM N° 2 - Solución de Seguridad para Protección de bases de datos

Consulta	Fecha de Consulta	30-09-2020
Para los Puntos: 2.1.3 y 2.1.9 ¿Podrá ser válida una solución basada exclusivamente en agentes desplegados en los motores de BD?		

Respuesta	Fecha de Respuesta	06-10-2020
Sí. Favor remitirse a lo establecido en la Adenda del PBC		

Consulta 11 - Cantidad Servidores

Consulta	Fecha de Consulta	01-10-2020
Teniendo en cuenta la respuesta a la consulta sobre el punto 2.1.2 Podría la convocante aclarar el numero de servidores ya sean físicos o virtuales donde corren las instancias de Base de Datos, ya que nuestra solución no se licencia por instancias, sino por cantidad de servidores de DB.- "Tal como establece el PBC, la cantidad mínima de instancias de base de datos requeridas es de 20 (veinte); favor considerar que, en atención a las buenas prácticas de seguridad, siempre es recomendable instalar un servidor principal y uno secundario para cada instancia a fin de soportar HA". Podría la convocante aclarar el numero de servidores ya sean físicos o virtuales donde corren las instancias de DB, por ejemplo si son efectivamente 20 servidores o si en en algun servidor corren mas de una instancia ? ademas como menciona el esquema HA, cual de las instancias posee infraestructura de HA y de ser asi cual seria la cantidad en modalidad Activo - Activo y en Activo - Pasivo, ya que estos datos son necesarios para poder licenciar en forma correcta la solucion		

Respuesta	Fecha de Respuesta	06-10-2020
Favor remitirse a la Adenda del PBC.		

Consulta 12 - Soporte DB

Consulta	Fecha de Consulta	01-10-2020

En referencia al punto 2.1.19 -
La solución deberá soportar al menos las siguientes plataformas de Bases de Datos:
- Oracle 10g y superiores
- SQL Server 2000 y superiores
- Oracle RAC
- Sybase 16 y superiores
- MySQL 5.1 y superiores
- PostgreSQL 9.2 y superiores

Teniendo en cuenta que los fabricantes de las bases en algunas versiones mencionadas en el pliego han dado el EOS (End of Support) que ya no poseen soporte del fabricante, por lo tanto tampoco poseen soporte de la herramienta a ser presentada
- Oracle 10 - EOS 2010
- SQL Server2000 - EOS 2013
- Mysql 5.1 - EOS 2013
- Postgress 9.2 - EOS 2017, podria la convocante aceptar soluciones que soporten desde
Oracle 11gR2
SQL Server 2012
Oracle RAC 11gR2
MySQL 5.7
PostgressSQL 9.4

Respuesta	Fecha de Respuesta	06-10-2020

Favor remitirse a la Adenda del PBC.

Consulta 13 - Punto 2.1.20

Consulta	Fecha de Consulta	01-10-2020

En relación al punto 2.1.20 donde hace referencia a
Debe permitir la creación de alertas de desviaciones de los parámetros establecidos en la línea base

Podria la convocante aclarar a que hace referencia o si hace mencion a la deteccion de un comportamiento anomalo sobre el comportamiento normal de la DB, por ejemplo la deteccion de SQLinjection

Respuesta	Fecha de Respuesta	06-10-2020

No. Favor remitirse al PBC. Esta funcionalidad hace referencia a la capacidad de la solución de detectar comportamiento diferente (anómalo) de los usuarios regulares y autorizados, al conocer el uso normal que realizan en la BD. A manera estrictamente referencial, solo como ejemplo y de manera no limitativa, esto incluye la capacidad de detectar si un usuario que solo hace "select", de manera inusual comienza a intentar "update" o "insert" en la base de datos, con lo cual emitiría una alerta de desviación de línea base.

Consulta 14 - Consulta soporte

Consulta	Fecha de Consulta	01-10-2020

En referencia al punto 2.5.1, hace mencion a la modalidad 24x7x8. Podria la convocante aclarar el punto

Respuesta	Fecha de Respuesta	06-10-2020

Favor ajustarse a lo establecido en la Adenda del PBC.

Consulta 15 - Shadow IT

Consulta	Fecha de Consulta	01-10-2020

En referencia al punto 1.2.23
La solución debe contar con la posibilidad de detectar el uso de cloud applications (Shadow IT) y gestionar cuales de ellas son prohibidas, y cuáles permitidas, pudiendo investigar cuales usuarios incumplen las políticas

Podria la convocante aclarar el punto en cuestion, por ejemplo si hace referencia a la detección del uso de dropbox que pudiera estar comprometiendo la seguridad de la entidad

Respuesta	Fecha de Respuesta	06-10-2020

Su interpretación es correcta.

Consulta 16 - Consulta

Consulta	Fecha de Consulta	01-10-2020

En referencia al punto 1.2.24
Debe detectar el mal uso de los recursos de navegación generados por los usuarios internos. Este monitoreo debe ser realizado a través de la integración con una herramienta tipo Secure Web Gateway (a traves de ICAP u otro protocolo estandard), para el monitoreo de categorías e indicadores de compromiso para identificar posibles accesos a sitios maliciosos no categorizados.

La convocante podría tener en cuenta que para el cumplimiento de este punto, es necesario contar con los datos necesario que deberan ser proveidos por el Secure Gateway, ya que el SIEM solo analiza los datos recibidos

Respuesta	Fecha de Respuesta	06-10-2020

Su interpretación es correcta.

Consulta 17 - ITEM 1 FUNCIONALIDADES 1.2

Consulta	Fecha de Consulta	12-10-2020

En las Especificaciones técnicas del ítem 1, 1.2 Funcionalidades, apartado 1.2.37 se indica:
Debe permitir capturar información a través de: Syslog, SNMPv2, SNMPv3, XML, OPSEC, WMI, RDEP, SDEE, Unix Pipe, API, Windows Event Logs. Así mismo debe permitir la personalización para que también esté disponible para fuentes únicas, como aplicaciones internas.

Solicitamos a la convocante que el punto RDEP sea considerado opcional debido a que no se trata de un estándar de la industria y sólo limita la participación de potenciales oferentes.

Respuesta	Fecha de Respuesta	13-10-2020

Favor remitirse al PBC. Se requiere asegurar compatibilidad con toda la infraestructura de red actual, incluyendo nuestros sensores IDS/IPS, por lo cual el protocolo RDEP es solicitado. Al respecto, les recordamos a los oferentes que tanto WMI como Windows Event Logs no son estándares de la industria, sin embargo son igualmente requeridos porque forman parte de la infraestructura del BCP que debe ser protegida, por lo cual la solución ofertada debe soportarlos.

Consulta 18 - EXPERIENCIA ITEM 1

Consulta	Fecha de Consulta	12-10-2020

Punto Experiencia requerida, se solicita “Demostrar la experiencia en haber proveído e instalado la solución ofertada con contrato/s ejecutado/s, y/o facturas, y/o recepciones finales por un monto equivalente al 30 % como mínimo del monto total ofertado en la presente licitación, de los: años 2015 al 2020”
Solicitamos a la convocante que la experiencia requerida pueda ser demostrada también con la experiencia del fabricante en la instalación y provisión de la solución. De este modo la convocante se estaría asegurando igualmente de la experiencia y el apoyo de la marca ofertada y no afectará de ningún modo con la implementación de la solución.

Respuesta	Fecha de Respuesta	13-10-2020

Favor remitirse al PBC. Para el BCP es fundamental que la contratada cuente con la experiencia necesaria para la implementación y el mantenimiento de la solución ofertada durante toda la duración del contrato, en particular porque esta solución representa uno de los componentes núcleo de toda la estrategia de ciberseguridad del BCP.

Consulta 19 - ítem 1, 1.2 Funcionalidades

Consulta	Fecha de Consulta	12-10-2020

En las Especificaciones técnicas del ítem 1, 1.2 Funcionalidades, apartado 1.2.44 se indica:
Debe permitir enlazar directamente fuentes externas como Bugtraq, ICE, CVE, Datastorm, MSDB y otros.

Solicitamos que éste punto sea considerado opcional debido a que no aplica puesto que el banco NO utiliza ninguna de éstas fuentes externas y sólo limita la participación de potenciales oferentes.

Respuesta	Fecha de Respuesta	13-10-2020

Favor remitirse al PBC.