



9 de septiembre de 2014

ABN-997/2014

Señores
OFERENTES LICITACIÓN PÚBLICA No.17/2014
Ciudad

Estimados señores:

En relación a la consulta formulada sobre el Pliego de Condiciones de la Licitación Pública No.17/2014, para la contratación del suministro, instalación y configuración de una solución para la administración de bitácoras o logs de servidores, equipo de telecomunicación, base de datos y aplicaciones del Banco Central de Honduras; a continuación se aclara lo siguiente:

Consulta No.1:

Anexo No.2, numeral 6 Visibilidad de alarmas en consola de administración:

Especificación: b) Debe Incluir un (1) monitor tipo LED de 32 pulgadas mínimo que puedan instalarse en escritorio o en pared, que incluya los respectivos cables de poder, los cables de video con una longitud de más o menos 25 pies, también debe incluir dos (2) bracket para instalación en la pared. Estos monitores estarán conectados al CPU del usuario que se le delegue el monitoreo de ciertas bitácoras y la conexión a la interface de la solución se hará vía TCP/IP. (Considerar que la interconexión del monitor a proveer, se hará en un CPU con sistema operativo Windows 7, 32 bit, procesador Intel® I5, 4GB de RAM).

Al inicio habla de un monitor de 32 pulgadas mínimo, luego hablan de 2 braket para instalación en la pared y "Estos monitores están conectados al CPU" ¿Podrían aclarar si requieren solo 1 monitor y 1 braket para la instalación en la pared?

Respuesta:

Se requiere solo un monitor y un bracket (entendiendo que un bracket es lo necesario para instalación del monitor en la pared).

Consulta No.2:

Anexo No.2, numeral 20 Mapa de entorno:

La solución debe brindar la facilidad de elaborar un mapa de dispositivos monitoreados o un inventario en tiempo real, de manera que el Administrador pueda visualizar el entorno desde la consola central.

Pueden aclarar si este requerimiento se refiere a visualizar la ruta de un ataque o conexión maliciosa desde la consola central de forma que el administrador pueda monitorear todos los dispositivos de la red, servidores, etc. que están involucrados en dicho ataque o conexión específica.



Respuesta:

Lo que se requiere es únicamente que la solución permita elaborar un mapa (diagrama) con los 35 dispositivos que inicialmente estarán involucrados en la configuración inicial, de manera que el administrador de la consola central pueda ver cuántos y qué tipos de dispositivos se están monitoreando con dicha solución.

Consulta No.3:

Anexo No.2, Numeral 24 Compatibilidad de formato de archivo de registros:

La solución debe tener compatibilidad con los formatos de archivos de registro de actividades más comunes generadores por bitácoras y protocolos syslog, snmp, WMI, Cisco, SDDE, FTP, SFTP, File Copy entre otros.

La solución a ofrecer utiliza RPC en vez de WMI para la colección de logs en sistemas operativos Windows, ¿Es aceptable este protocolo de colección?

Respuesta:

No se puede proporcionar una respuesta afirmativa o negativa. La evaluación de las ofertas la realizará una comisión evaluadora de acuerdo a la información técnica proporcionada y analizada y será esta quien dictaminará si es o no aceptable este protocolo de colección.

Consulta No.4:

Anexo No.2, numeral 27 Capacitación:

Debe incluir capacitación para seis (6) empleados designados por "El Banco" como mínimo, donde se incluya un mínimo de veinte (20) horas en teoría y dieciséis (16) horas en práctica, la práctica se realizara a medida se esté implementando, configurando y puesta en operación dicha solución.

¿Es posible que cambien "Capacitación para seis (6) empleados designados por "El Banco" como mínimo" a máximo o a un número predefinido diferente? 6 empleados mínimo deja abierta la posibilidad de participantes a un número incierto para el cual sería casi imposible determinar un costo.

Respuesta:

Se requiere capacitación para seis (6) empleados designados por "El Banco".

Consulta No.5:

Anexo No.2, numeral 7 Captura de Bitácoras o logs:

La solución de be tener capacidad de coleccionar datos de las bitácoras generadas por cada equipo servidor Windows Server 2003, 2008 o superior, Solaris 10 o superior, Linux, equipos de telecomunicación, base de datos Oracle 10g, 11g o superior, MS-SQL Server 2005, 2008 o superior y de ser posible también Progress, aplicaciones desarrolladas en NET, Java, Visual Basic y de ser posible también Progress, debe brindar la posibilidad de agregar aquellos dispositivos / activos generadores de bitácoras que no se encuentran definidos en esta sección.



Solicitamos en este punto, aclarar o ampliar que tipo de dispositivos / activos generadores de bitácoras se refieren con la finalidad de considerar el licenciamiento, módulos, protocolos y demás necesarios.

Respuesta:

Ver respuesta en anexo No.1

Consulta No.6:

Anexo No.2, numeral 5, Alcance de la Solución:

En la página No.18 en el documento Especificaciones Técnicas, en el requerimiento No.5: Alcance de la solución, necesitamos se nos dé la siguiente información adicional:

- a) Quince (15) servidores (Windows server versiones 2003 y 2008, Solaris 10 y GNU-Linux Debian): para asegurar el análisis de cumplimiento de lo requerido en las bases, solicitamos un detalle de la cantidad de servidores corriendo Windows describiendo la versión específica de Sistema Operativo en cada equipo, de igual manera necesitamos el mismo detalle para los servidores corriendo Solaris y GNU-Linux (Cantidad de cada uno y versiones de sistema operativo).

Respuesta:

Ver respuesta en Anexo No.1

- b) Cinco (5) equipos de telecomunicación (Ruteadores y Switches): para asegurar el análisis de cumplimiento de lo requerido en las bases, solicitamos un detalle de cuantos son Router y cuantos son Switches y de ser posible marca y modelo de los equipos.

Respuesta:

Ver respuesta en Anexo No.1

- c) Cinco (5) equipos de seguridad perimetral (Firewalls, IPS, UTM): para asegurar el análisis de cumplimiento de lo requerido en las bases, solicitamos el detalle de cuantos son Firewall, cuantos son IPS y cuantos UTM, así como el modelo, marca y en el caso del UTM que funcionalidades están habilitados en el mismo.

Respuesta:

Ver respuesta en Anexo No.1

- d) Diez (10) aplicaciones (arquitectura, Net y Java). Para asegurar el análisis de cumplimiento de lo requerido en las bases, solicitamos se indique la funcionalidad requerida para el SIEM es en base a los eventos generados por la plataforma donde se ejecutan las aplicaciones o si es para los eventos generados por cada aplicación. Si es el caso de eventos generados por la aplicación se requiere que se indique de qué forma son enviados (emitidos), si es por medio de un Syslog o un Eventlog y si están integradas a una plataforma de sistema operativo (indicar cuál).



Respuesta:

Ver respuesta en Anexo No.1

- e) Cinco (5) bases de datos, (Motores Oracle y MSSQL Server); favor indicar la cantidad de bases de datos por cada tipo y la versión de cada una. Adicionalmente se requiere conocer el alcance de la funcionalidad de monitoreo de eventos que se desea en relación a las bases de datos, si es monitoreo a nivel de la plataforma donde corren las bases de datos o si es a nivel de la estructura interna de la base de datos.

Respuesta:

Ver respuesta en Anexo No.1

En relación a si el alcance es a nivel de plataforma donde corren las bases de datos o si es a nivel de la estructura interna de la base de datos, confirmamos que la solución debe tener la capacidad de capturar eventos generados en la plataforma y en la estructura interna de la base de datos, quedará a discreción de "El Banco" definir la configuración requerida, ya sea para capturar eventos generados en la plataforma o en la estructura interna de la base de datos.

Consulta No.7:

Anexo No.2, numeral 2.1 Instalar, configurar y poner en funcionamiento el objeto del suministro, en las instalaciones de "El Banco" en la ciudad de Tegucigalpa, MDC., bajo la supervisión de personal técnico que designe "El Banco".

Podemos asumir que "el objeto del suministro" son los 35 activos críticos? Es decir, el Banco desearía que se instalen, configuren y pongan en funcionamiento estos 35 activos críticos. O por el contrario, se refieren a dejar funcionando el o los equipos que se suministrarán y el Banco se encargaría de activar esos 35 activos críticos? O desean que se instalen solamente un número finito de esos activos críticos, en cuyo caso la pregunta sería ¿De cuántos estarían hablando?

Respuesta:

El proveedor debe instalar, configurar y probar la solución de manera que quede funcionando correctamente para coleccionar la bitácora de los 40 activos críticos descritos en el Pliego de Condiciones y en el anexo No.1.

Consulta No.8:

Si la respuesta a "a)" ("a" es la consulta anterior) es dejar funcionando todos o una parte de los activos críticos, dado que el tiempo para instalar, configurar y dejar funcionando cada uno de esos activos crítico variaría dependiendo del fabricante y sus modelos, para poder calcular el número de días que se utilizarían para completar los 35 activos críticos (o los que el Banco determine sería los que se dejarían funcionando), sería posible nos indicaran la siguiente información:

1. Marca
2. Modelo
3. Sistema operativo y versión
4. Firmware/software y versión



Respuesta:

Ver respuesta en Anexo No.1

Consulta No.9:

De los quince (15) servidores que se mencionan en los términos, cuales son:

- Windows, sus versiones
- Debian Linux, sus versiones
- Solaris, sus versiones

Respuesta:

Ver respuesta en Anexo No.1

Consulta No.10:

De las quince (15) bases de datos mencionadas cuantas son:

- SQL Server, sus versiones
- Oracle, sus versiones

Respuesta:

Ver respuesta en Anexo No.1

Consulta No.11:

Adicionalmente mencionan la base de datos Progress, referente a esta base, ¿Cuántas instancias estarán consideradas en este proyecto?

Respuesta:

Considerar una instancia

Atentamente



SANTOS EMILIO FLORES SOSA
Secretario del Comité de Compras y
Jefe Departamento de Adquisiciones y Bienes Nacionales

IMP/IROF



ANEXO No.1

1) Marca, Modelo, Sistema Operativo, Versión y Firmware /Software.

Equipos Servidores			
Marca	Modelo	Sistema Operativo	Versión
DELL	PowerEdge 6800	Windows Server 2008 Enterprise (X64) Service Pack 2	Service Pack 2 64 bits
DELL	PowerEdge 2800	Windows Server 2008 Standard (x64) Service Pack 2	Service Pack 2 64 bits
VMware, Inc	VMware Virtual Plataform (ESX 5.5)	Windows Server 2003 Standar Edition Service Pack 2	Service Pack 2 32 bits
DELL	PowerEdge 1800	Windows Server 2003 Standar Edition Service Pack 2	Service Pack 2 32 bits
DELL	PowerEdge R520	Windows Server 2008 R2 Enterprise	Service Pack 1 64 bits
IBM	eServer BladeCenter HS21	Windows Server 2003 Standar Edition	Service Pack 2 32 bits
DELL	PowerEdge 2900	Windows Server 2003 R2 Enterprise	Service Pack 2 64 bits
DELL	Power Edge R520	Windows Server 2008 R2 Enterprise	Service Pack 1 64 bits
HP	ProLiant DL380 G7	Windows Server 2008 R2 Standard	64 bits
HP	ProLiant DL380 G7	Windows Server 2008 R2 Standard	64 bits
IBM	eServer BladeCenter HS21	Windows Server 2012 R2 Standard	64 bits
SUN	Sun T5140	Oracle Solaris 10	5.1
SUN	M4000	Oracle Solaris 10	5.1
SUN	Sun T2000	Oracle Solaris 10	5.1
HP	6200 PRO	LINUX DEBIAN	2.6.32-5-686

Equipos de Telecomunicación			
Marca	Modelo	Sistema Operativo	Versión
Cisco	Switch Catalyst 4507r	IOS	12.2 (31)
Cisco	Switch Catalyst 4507r	IOS	12.2 (31)
Cisco	Switch Catalyst 4503	IOS	12.2 (31)
Cisco	Router 3660 Series	IOS	12.2 (46a)
Cisco	Switch Catalyst 3560	IOS	12.2

Equipos de Seguridad Perimetral			
JUNIPER	SRX240H	JunOS	11.4r10.3
3COM	X506	Tipping Point	X3.2.0.2327
Fortigate	80C	FortiOS	4.0 Build0665,130514
Cisco	PIX 515	IOS	7.0 (2)
Cisco	PIX 520	IOS	6.3 (4)

2) Plataforma de desarrollo:

- a) NET: Microsoft Visual Studio 2005-2012
- b) JAVA: Glassfish, Tomcat, Jboss



3) Bases de datos:

Marca	Versión
Oracle	10.2.0.4.0
Oracle	11.2.0.3.0
Oracle	10.1.2.5.0
Microsoft	SQL 2005/2008
Microsoft	2012

4) Bases de datos Progress: Una instancia versión 9.1b

IMPM/IROF

