LICITACIÓN PÚBLICA NACIONAL SBE N° 26/2016
"ADQUISICION DE SOFTWARE DE CONSOLIDACION DE LOGS PARA EL IPS"

ADENDA N° 3

Asunción, 23 de junio de 2016.

AL OFERENTE:

Con relación a la **LICITACIÓN PÚBLICA NACIONAL SBE N° 26/2016 "ADQUISICION DE SOFTWARE DE CONSOLIDACION DE LOGS PARA EL IPS"**, informamos que se realizan las siguientes modificaciones:

1. **En la Sección III. Suministros Requerido. 2 Especificaciones Técnicas, en los Requerimientos Técnicos de la Solución queda de la siguiente manera:**

REQUERIMIENTOS TÉCNICOS DE LA SOLUCIÓN

1. El sistema operativo del o los "appliance" debe ser basado en Linux, y deberá estar previamente reforzado por el fabricante (hardening) para garantizar un adecuado desempeño de la solución.
2. La solución no debe tener limitación para poder registrar fuentes de eventos.
3. El o (los) appliance(s) deberá contar con mecanismos de redundancia, y tolerancia a fallas tales como fuentes de poder duales, configuración de arreglo de discos RAID; para garantizar la disponibilidad en el caso de presentarse alguna contingencia, garantizando la recolección continua de los log's y eventos de seguridad. DEPENDE DEL MODELO ELEGIDO BASADO EN CALCULO DE EPS.
4. La solución deberá contar con almacenamiento interno de 8 TB o superior, tomando en cuenta los 12.000 EPS. El almacenamiento interno deberá estar configurado con el tipo de RAID adecuado para garantizar su óptimo rendimiento. Adicionalmente de debe hacer un buen uso del almacenamiento mediante la compresión de eventos (1:14, 1:17 y 1:20) DE ACUERDO A MODELO ELEGIDO BASADO EN CALCULO DE EPS
5. La solución deberá permitir la integración con soluciones de almacenamiento (SAN – Storage) de terceros, brindando escalabilidad y crecimiento para ir archivando los log's y eventos históricos. Se debe incluir la tarjeta de SAN para hacer la conexión con el Storage
6. La solución deberá ofrecer una capacidad de correlación de hasta 12.000 Eventos por Segundo (EPS) y permitir picos de eventos adicionales sin que exista pérdida de eventos. La solución debe brindar la respectiva escalabilidad para aumentar la cantidad de eventos soportados vía upgrade de licencia o appliances, si se requiere a futuro.
7. La solución deberá incluir componentes (agentes) dedicados a la recolección, normalización y categorización de eventos de seguridad.
8. La solución deberá tener la capacidad de realizar la correlación en "TIEMPO REAL" sin necesidad de consultar la base de datos donde se almacenan los eventos para este propósito.
9. La solución deberá 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.
10. La herramienta deberá adquirir logs como mínimo de las siguientes plataformas
    Servidores,
    Windows Server 2008,20088 R2, 2012, 2012R2
    Linux RHEL, 5x, 6x, 7x
    Routers
    Firewalls
    Directorio Activo MS
    Base de Datos MSSQL 2008R2 ,Oracle 9i, 10g, Postgres 8.x,9x

    Los logs serán adquiridos mediante cualquiera de estas tecnologías SYSLOG, SNMP, NETFLOW, WMI

11. El concepto posterior abarca correlación de logs y eventos de seguridad informática, reportes, consultas, detectar por medio de la correlación, ataques y eventos específicos dentro de la infraestructura.

INSTITUTO DE PREVISION SOCIAL
LIC. MANUEL ASTIGARRAGA
JEFE
Departamento de Licitaciones
DGBS - I.P.S.