Consulta Preliminar de Mercado para la preparación de expediente de contratación de suministro, instalación, integración y mantenimiento/soporte de una capa de visibilidad de red inteligente para AndalucíaCERT

Andalucía se mueve con Europa

1. Objeto de la consulta

Recabar información de los operadores económicos, relativa al **suministro, instalación, integración y mantenimiento/soporte de una capa de visibilidad de red inteligente para AndalucíaCERT**, con el fin de que la **Consejería de la Presidencia, Administración Pública e Interior** pueda incluir, si procede, la información recabada para elaborar los pliegos del próximo expediente de contratación que, en su caso, se licite al respecto.

1.1. Antecedentes

El CSIRT[1] autonómico AndalucíaCERT es la capacidad de respuesta a incidentes de seguridad de la Junta de Andalucía. Su misión, encomendada por la Política de Seguridad TIC de la Junta de Andalucía[2], es el desarrollo de acciones centralizadas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía. El servicio, bajo la dirección de la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía, se presta desde la localidad sevillana de Tomares por parte de la Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A. (SANDETEL).

Actualmente AndalucíaCERT cuenta con una plataforma de monitorización de eventos y detección de incidentes de seguridad en los Nodos de InterconeXión (también llamados NIX) de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía. Esta plataforma está basado en el producto Alienvault USM Appliance.

Se desea ampliar la capacidad de monitorización de tráfico de red de la actual plataforma y se ha realizado en mayo del presente año una consulta preliminar de mercado acerca de sensores de red para la

1 *Computer Security Incident Response Team* (Equipo de Respuesta ante Incidentes de Seguridad Informática)

2 Artículo 12.1 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio).

detección de amenazas de seguridad[3]. Análisis adicionales han detectado conveniencia de dotar a la actual plataforma y a su posible ampliación de una capa de visibilidad de red inteligente que optimice la monitorización del tráfico de la red corporativa para una detección de amenazas más eficiente.

1.2. Necesidades, características generales y ubicación

Actualmente se dispone de dos *Network Packet Broker* Netscout PFS 5010 que permiten el tratamiento del tráfico fuera de línea, mediante la recepción del mismo y su distribución entre las sondas de que se dispone. Se plantea ampliar esta estructura añadiendo nuevos componentes que aporten una capa de visibilidad de red inteligente y permitan optimizar el tráfico hacia las sondas, descargándolas y permitiendo una detección de amenazas más eficiente.

Los componentes estarán desplegados en dos centros de proceso de datos (CPD) ubicados en la provincia de Sevilla, más concretamente en los municipios de Tomares y Sevilla.

Los requisitos generales son:

- Suministro de componentes de visibilidad de red inteligente en los dos CPD citados, incluyendo todos los elementos software y hardware necesarios para su funcionamiento.
- Se incluirán servicios profesionales para la instalación e integración con la actual estructura.
- Servicios de soporte y mantenimiento de dos años, prorrogables a cuatro:
  - Cobertura de la licencia o licencias requeridas. Acceso a las actualizaciones de parches y nuevas versiones del software y firmware.
  - Soporte del equipamiento hardware y software en modalidad de siguiente día laborable (NBD, Next Business Day) en horario 8x5. Al menos, debe incluir:
    - La reposición e instalación de piezas averiadas o sustitución de equipos por otros de iguales o superiores características, sin coste.
    - Soporte ante incidencias del software.
- Se valorará especialmente la modularidad y la capacidad máxima de crecimiento de los componentes, así como la inclusión de diversos escenarios de configuración de capacidades hardware/software.
- La solución debe proveer, de serie, de una capacidad de agregación, filtrado y replicación del tráfico, de una forma versátil y sin pérdida ni alteración de paquetes:
  - Capacidad para agregar el tráfico de varias entradas.
  - Capacidad para repartir el tráfico entre varias salidas.
  - Capacidad para replicar el tráfico en distintas salidas.
- La solución debe proveer unas funcionalidades avanzadas de filtrado y procesado del tráfico, con objeto de mejorar la eficiencia en el uso de las sondas de detección de amenazas de red:

3 https://juntadeandalucia.es/temas/contratacion-publica/perfiles-licitaciones/consultas-preliminares/detalle/000000220343.html

- Capacidad para filtrar paquetes duplicados.
- Capacidad para filtrar en base a protocolo de red (hasta capa 4 OSI).
- Capacidad para filtrar en base a aplicaciones comunes y propietarias (hasta capa 7 OSI).
- Capacidad para filtrar parte del flujo de datos, mediante la reducción en bytes y/o paquetes, con especial tratamiento para el filtrado de los paquetes cifrados TLS (eliminando o reduciendo paquetes tras la cabecera).
- Capacidad para generar y enviar los flujos de red según Netflow/Ipfix y para extraer metadatos de los mismos.

- También se valorará la recomendación expresa de otras funcionalidades con objeto de lograr la optimización del tráfico dirigido a las sondas de detección de amenazas de red.

Se debe aportar el desglose del coste completo de adquisición y operación (licencias y soportes recurrentes), de los distintos componentes y funcionalidades avanzadas de la solución.

1.3. Dimensionamiento

Los componentes deberán estar dimensionados y correctamente licenciados durante el periodo de ejecución del contrato, incluida su prórroga, para la gestión del tráfico de red indicado en cada Nodo de Interconexión. Por el momento se dispone de una estimación, únicamente.

Puede considerarse que en cada uno de los dos CPD se tendrá un tráfico máximo de entre 20 y 30 Gbps. El número de interfaces por los que se recibirá dicho tráfico se considera en torno a 5x10Gbps fibra en cada CPD. Probablemente sean más, pero se plantea aplicar una primera capa de filtrado y agregación con los actuales NPB Netscout. La forma de adquisición del tráfico, actualmente, es mediante puertos SPAN, pero puede considerarse el uso de TAP, aunque no se conoce actualmente el número de puertos y ubicaciones que serían necesarios.

Los equipos entregarán el tráfico filtrado a la plataforma de monitorización de AndalucíaCERT, actualmente compuesta por sondas AlienVault USM Enterprise Sensor y sondas CCN (SAT-INET y CARMEN). Se estima una salida por cada CPD de 4x10Gbps fibra y 1x1Gbps cobre.

Exclusivamente a modo de referencia, se indica que se han estudiado los modelos del fabricante Gigamon y se estima que los modelos GigaVUE HC1 o GigaVUE HC2 podrían cubrir las especificaciones, aunque el en primero podría ser limitante el módulo GigaSMART integrado.

2. Fundamento jurídico de la consulta

Artículo 115 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

3. Objetivos de la consulta

Recabar información en relación a

- La adecuación de los requisitos establecidos a las capacidades actuales de los productos en el mercado.
- La estimación del valor y precios habituales de mercado de los elementos y acciones que conformarían su suministro, instalación, integración, mantenimiento y soporte.

4. Organismo solicitante de la consulta

Consejería de la Presidencia, Administración Pública e Interior.

5. Procedimiento de consulta

La consulta es pública y se dirige a organismos públicos o privados y empresas que deseen colaborar facilitando información del mercado sobre los asuntos reflejados en la misma.

Se articula a través del cuestionario publicado en el perfil del contratante de la Consejería de la Presidencia, Administración Pública e Interior conjuntamente con este documento. En caso de que se considere oportuno compartir información adicional en otro formato, se puede remitir junto con el cuestionario para su análisis.

Es conveniente que el cuestionario se cumplimente en su totalidad, y que las respuestas sean lo más completas posibles, para lo que se admitirán los comentarios y aclaraciones que se consideren oportunos en cada caso.

Los cuestionarios se remitirán a través de Presentación Electrónica General de la Junta de Andalucía indicando el siguiente destinatario:

Consejería/entidad: Consejería de la Presidencia, Administración Pública e Interior

Órgano/Agencia/etc: Dirección General de Estrategia Digital y Gobierno Abierto

El enlace web a Presentación Electrónica General se puede encontrar en:

https://www.juntadeandalucia.es/servicios.html

Se fija para presentar los cuestionarios debidamente cumplimentados un plazo de diez días naturales desde la publicación de esta consulta.

Para cualquier consulta se puede contactar por correo electrónico con la Unidad de Seguridad TIC Corporativa en la dirección seguridadtic@juntadeandalucia.es, incluyendo en el asunto el texto “CPM-AndalucíaCERT-02”.

Si se considera necesario, la Consejería podrá contactar con participantes concretos para recabar más información sobre las respuestas incluidas en sus cuestionarios o aclarar dudas.

Finalizado el plazo de presentación de cuestionarios y, en su caso, recabada la información adicional que fuera necesaria, se publicará en el Perfil de Contratante de la Consejería de la Presidencia, Administración Pública e Interior el informe a que se refiere el apartado 3 del mencionado artículo 115 de la Ley de Contratos del Sector Público.

6. Aplicación de los principios de transparencia, igualdad de trato y no discriminación ni falseamiento de la competencia

Sin perjuicio de lo establecido en el artículo 115.3 de la Ley de Contratos del Sector Público en relación con el informe que debe publicarse de las actuaciones realizadas, la información contenida en los cuestionarios recibidos será considerada confidencial y tratada como tal por la Consejería de la Presidencia, Administración Pública e Interior.

La Consejería no revelará en ningún caso a los participantes en el mismo la consulta las soluciones propuestas por los otros participantes.

El proceso de la consulta y todas las acciones que se deriven de ella se someterán a los principios de transparencia, igualdad de trato y no discriminación.

La participación en esta consulta no otorgará derecho ni preferencia alguna respecto de la adjudicación de los contratos que puedan celebrarse con posterioridad en el ámbito del objeto de esta convocatoria y, como consecuencia de ello, no conlleva ninguna obligación de financiación o aceptación de las propuestas recibidas.

No obstante lo anterior, la participación en la consulta no impide la posterior intervención en el procedimiento de contratación que en su caso se tramite.