CONSULTA PRELIMINAR DE MERCADO PARA LA PREPARACIÓN DE EXPEDIENTE DE CONTRATACIÓN DE Infraestructura, operación y servicios para AndalucíaCERT – Lote I -- Suministro de plataforma de monitorización y servicios asociados

ANEXO. Formulario

IDENTIFICACIÓN DE LA EMPRESA	
Empresa	
NIF	
Sector o ámbito de actividad	
Dirección a efectos de notificación	
Tamaño de la entidad en la actualidad (nº de personal en plantilla)	
DATOS DEL INTERLOCUTOR	
Nombre y apellidos del interlocutor	
Cargo	
Teléfono	
Correo electrónico	

Se ruega que las respuestas sean concisas y escuetas. Si es necesario aportar información adicional puede hacer referencias a la documentación del producto.

1.1. Adecuación de requisitos técnicos

¿Considera que los requisitos de la plataforma de monitorización están correctamente expuestos y son alcanzables con soluciones en el mercado? **¿Considera que existen requisitos adicionales que puedan ser considerados?**

1.2. Adecuación de los servicios I

¿Son adecuados los requisitos establecidos sobre los servicios a prestar? **¿Considera que hay servicios o requisitos adicionales que puedan ser de interés?**

1.3. Adecuación de los servicios II

A la vista de los servicios solicitados y sus requisitos, así como, en su caso, de las propuestas realizadas en el apartado anterior, indique qué servicios solicitados o requisitos pudieran resultar de escasa utilidad o relevancia.

1.4. Solución de sensores de red (NIDS) propuesta.

Indique brevemente las capacidades del NIDS. Indique las capacidades y funcionalidades del sensor recolector de tráfico. Indique el mecanismo de detección de amenazas (basado en reglas SNORT...). Fuentes de inteligencia incorporadas. Otras capacidades: generación de flujos de red, generación de metadatos, ... Indique la gama de productos según las capacidades IDS de procesado de tráfico (bps). Indique si dispone de modelo virtualizado.

1.5. Solución SIEM propuesta. Motivos de éxito

Indique brevemente por qué considera que su propuesta es una solución de éxito. Describa los factores diferenciales de la solución para considerar que ésta sea una propuesta de éxito: capacidad para evitar falsos positivos/negativos, reducción del número de alarmas de seguridad para evitar la fatiga en la monitorización (mediante el uso de tecnología de inteligencia artificial, consultoría experta en la configuración y afinamiento del sistema, …), el empleo de librería de pasos guiados (que simplifica la operación), …

1.6. Solución SIEM propuesta. Arquitectura

Indique brevemente la arquitectura del SIEM. Indique la arquitectura propuesta (física y lógica): centralizada/distribuida. En caso de solución distribuida/mixta, qué elementos conceptuales están desplegados en jerarquías inferiores: sensor recolector de logs, servidor de gestión, ... Indique en que ubicaciones se almacenan los logs. Indique si existe una consola única para acceder a

todos los logs. Indique cómo es la cobertura de las sedes que se añadan en la segunda fase.

1.7. Solución SIEM propuesta. Modelo de despliegue

Indique brevemente el modelo de despliegue del SIEM. Indique si la solución estará alojada en las instalaciones del cliente (on-premise) o en las instalaciones del proveedor (off-premises) o incluso en nube. O, si es mixta, qué elementos conceptuales están en cada lugar. Indique si los elementos conceptuales son dispositivos físicos o virtuales.

1.8. Solución SIEM propuesta. Modelo de servicio

Indique brevemente el modelo de servicio del SIEM. Si la solución está basada en la nube (*cloud*): Describa el modelo de servicio permitido (SaaS/PaaS) y las posibilidades de despliegue (nube pública o privada). Describa qué elementos conceptuales se deben alojar en la instalación del cliente (proxy...). Indique las estimaciones de requisitos de conectividad con Internet (ancho de banda).

1.9. Solución SIEM propuesta. Fuentes de eventos

Indique brevemente el catálogo de fuentes de eventos soportadas por el SIEM. De las fuentes de eventos especificadas en la consulta, indique si alguna no está soportada. Específicamente, indique el grado de integración con los sistemas en la nube de: Azure, Microsoft E365, Microsoft Exchange y Microsoft CASB. Indique si las fuentes de eventos especificadas en la consulta vienen de serie en el producto (*out-of-the-box*) o requieren de un desarrollo a medida.

1.10. Solución SIEM propuesta. Escalabilidad

Indique brevemente la escalabilidad del SIEM. Indique cómo se produce la escalabilidad (horizontal o verticalmente). Indique la agilidad en la escalabilidad (elasticidad). Considere la escalabilidad en términos de capacidad de recolección, procesamiento y almacenamiento y otros parámetros dependientes del licenciamiento. Indique las implicaciones en el licenciamiento.

1.11. Solución SIEM propuesta. Estimación de procesado de eventos de seguridad

Indique brevemente la estimación de los eventos de seguridad representativos del SIEM. Indique si la solución realiza un filtrado y descarte de logs para centrarse en aquellos que considera representativos para la seguridad. Si aplica, indique el porcentaje estimado de eventos correlados frente al total de eventos, respecto a las principales fuentes de logs de infraestructura (proxys web, cortafuegos…).

1.12. Solución SIEM propuesta. Base de datos

Indique brevemente el sistema de base de datos del SIEM. Indique los sistemas para el elemento conceptual de base de datos (de los eventos correlados) y para la base de datos de logs (con todos los eventos). Describa la escalabilidad de las bases de datos y agilidad de las consultas. Indique la estimación de compresión de datos. Indique la capacidad máxima de registros (orden de magnitud).

1.13. Solución SIEM propuesta. Inteligencia de amenazas

Indique brevemente la inteligencia de amenazas del SIEM.

Describa los casos de usos, *playbook* y otras técnicas disponibles para la detección de amenazas. Indique las fuentes de inteligencia (propias y de terceros) y otras contextualizaciones empleadas (valor del activo, reputación de direcciones IP...).

1.14. Solución plataforma propuesta. Requerimientos en CPD

Indique brevemente la estimación de requerimientos en el CPD. Indique la necesidad de espacio de rack (U), tomas y consumo eléctrico, y puertos de red. Si es posible, desglosar por ubicación.

1.15. Certificaciones asociadas al SIEM propuesto

¿Está el SIEM incluido en el Catálogo de Productos de Seguridad TIC (CCN-STIC 105) o está previsto que lo esté próximamente? ¿Está el SIEM certificado en ENS categoría ALTA o está previsto que lo esté próximamente? **¿Está el SIEM o, al menos, la infraestructura (en caso de servicio en la nube) sobre la que se presta, certificada de conformidad con el ENS, en categoría ALTA?** **¿Con qué otras certificaciones cuentan?**

1.16. Certificaciones del SOC del proveedor

¿Está el SOC certificado en el ENS en los sistemas de información con los que presta el servicio gestionado de seguridad? **¿El SOC forma parte de foros de seguridad (CSIRT.es, FIRST, TI TF-CSIRT?**

1.17. Estimación de personal y perfiles

¿Considera que la estimación de personal está sobreestimada o subestimada? ¿Qué estimación de personal plantea para los servicios solicitados? ¿Propone alguna fórmula para el dimensionamiento

de recursos humanos en función de alguna métrica (EPS,…)? **¿Es viable la disponibilidad de guardia con un único técnico, alternativas?** **Identifique las características de los perfiles que deberían prestar cada servicio, especificando formación, certificaciones y experiencia, para las prestaciones presencial y remota.**

1.18. Modelo de prestación

¿Qué modelo de prestación considera más adecuado, teniendo en cuenta los requerimientos de presencialidad/servicio remoto/guardias...? **¿Qué periodos de facturación considera necesarios?** Indique la forma de prestar el servicio (de forma localizada, en las instalaciones del proveedor en Andalucía o en territorio nacional, en teletrabajo…). Indique las periodicidades para la certificación/facturación de los distintos entregables.

1.19. Modelo de licenciamiento

Describa brevemente el modelo de licenciamiento del SIEM que tendría la solución propuesta (duración mínima o máxima, adición de paquetes opcionales…) Indique cómo se realiza el licenciamiento del producto/s y servicios (por EPS, almacenamiento, activos...), si existen tramos de tarifas en función de la cantidad de licencias contratadas o activas, si existen cuotas fijas y cuotas variables, cómo se gestionan y contabilizan las bajas y altas de licencias (pago por uso...), unidades de coste para el servicio deslocalizado del servicio de operación, …

1.20. Plazo de ejecución fase 1

Identifique el tiempo máximo para completar los siguientes hitos en días naturales.
Suministro en las instalaciones (desde la firma del contrato): ___ días Instalación y configuración básica de la fase 1 (desde el hito anterior): ___ días

1.21. Listado de productos y licencias propuestas

Añada tantas filas como crea necesarias.		
Producto	**Descripción**	**Cantidad**

1.22. Desglose económico a cuatro (4) años

Añada tantas filas como crea necesarias.

Indique la unidad de facturación empleada (ejemplo: # EPS, tarifa perfil por hora…)

El supuesto de las fases del despliegue es:

• fase 1: despliegue inicial (con 4 años de duración) de los nodos de interconexión, nodos de troncal

• fase 2: despliegue del resto de sedes (una sede pequeña, mediana y grande) al comienzo del tercer año (con 2 años de duración). Incorporación de los recursos humanos adicionales (con 2 años de duración).

Concepto	**Unidades**	**Coste Unitario**	**Importe (sin IVA)**
Suministro NIDS - modelo 1 (1G bps)			
Suministro NIDS - modelo 2 (10G bps)			
Suministro SIEM			
Servicios profesionales de despliegue inicial NIDS/SIEM (fase 1)			
Suministro switchs			
Servicios profesionales de despliegue switchs			
Suministro ampliación SIEM – sede pequeña (fase 2)			
Suministro ampliación SIEM – sede mediana (fase 2)			
Suministro ampliación SIEM – sede grande (fase 2)			
Servicios profesionales despliegue sede pequeña NIDS/SIEM (fase 2)			
Servicios profesionales despliegue sede mediana NIDS/SIEM (fase 2)			
Servicios profesionales despliegue sede grande NIDS/SIEM (fase 2)			
Servicio de mantenimiento NIDS - modelo 1 (1G bps)			

Servicio de mantenimiento NIDS - modelo 2 (10G bps)			
Servicio de mantenimiento SIEM			
Servicio de mantenimiento switches			
Servicio de coordinación de actividades			
Servicio de experto de la plataforma de monitorización			
Servicio de operación de la plataforma de monitorización (localizado)			
Servicio de operación de la plataforma de monitorización (deslocalizado)			
Servicio de gestión de incidentes de seguridad N1			
Servicio de gestión de incidentes de seguridad N2			
Servicio de administración de sistemas y redes			
Servicio de formación y capacitación			
Otros conceptos (especificar)			