CONSULTA PRELIMINAR DE MERCADO PARA LA PREPARACIÓN DE EXPEDIENTE DE CONTRATACIÓN DE Infraestructura, operación y servicios para AndalucíaCERT -- Lote II – Servicios recurrentes de ciberseguridad

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	

1.1. Adecuación de los servicios solicitados

En líneas generales ¿considera que los requisitos de los servicios están correctamente expuestos y son alcanzables con soluciones en el mercado? ¿Considera que existen requisitos adicionales que puedan ser considerados? ¿Qué servicio o servicios adicionales considera que deberían ser incluidos o ser tomados en consideración? A la vista de los servicios solicitados y sus requisitos, así como, en su caso, de las propuestas realizadas a la pregunta anterior, indique qué servicios solicitados o requisitos pudieran resultar de escasa utilidad o relevancia.

1.2. Servicio de Alerta Temprana de Vulnerabilidades propuesto.

Indique brevemente su propuesta para este servicio. Indique las capacidades y funcionalidades de la plataforma de inventariado, contraste y análisis de vulnerabilidades propuesta. ¿Se trata de un desarrollo propio, o servicio de un tercero? Indique si tendría

posibilidad de despliegue en las instalaciones del cliente (on-premise) o se trata de un servicio en nube, y si dispone de modelo virtualizado. Especifique el modelo de licenciamiento (por tenants, por activos, por tecnologías...). Especifique el ámbito de cobertura (adicional a los sistemas TI estándar, ver documento de la consulta).

1.3. Servicio de Análisis de la Superficie de Exposición en Internet propuesto.

Indique brevemente su propuesta para este servicio. Indique la arquitectura (desde infraestructura propia, nube de un tercero, …) y herramientas que utilizaría, así como el modelo de prestación del mismo.

1.4. Servicio de Análisis de Vulnerabilidades propuesto.

Indique brevemente su propuesta para este servicio Para cada uno de los 3 subservicios describa brevemente las herramientas que utilizaría, así como el modelo de prestación del mismo. ¿Cuán flexible resulta la solución en cuanto a futuros crecimientos en la infraestructura a analizar (licenciamiento, necesidades de hardware a proporcionar, …, etc.)? ¿Observa sinergias a nivel técnico entre este servicio y el de Análisis de la Superficie de Exposición en Internet (p.e. por la utilización de las mismas herramientas) que inciten a la unificación de ambos?

1.5. Servicio de Inteligencia de Amenazas propuesto.

Indique brevemente su propuesta para este servicio. ¿Qué fuentes/servicios de terceros adicionales a los ya indicados contemplaría? ¿Algún servicio propio?

1.6. Servicio de Vigilancia Digital propuesto.

Indique brevemente su propuesta para este servicio. Indique las capacidades y funcionalidades de la plataforma de vigilancia/servicio que propone, con especial foco en la naturaleza de los objetivos a monitorizar, y la flexibilidad/capacidad de adecuación al alcance de interés que se indica (en base a configuraciones y/o filtrado) para obtener alertas de interés. ¿Se trata servicio propio, o proporcionado por un tercero? Indique el modelo de prestación propuesto, y hasta qué punto se trata de un servicio desatendido o con aporte de valor por parte de analistas.

1.7. Servicio de Red Team propuesto.

Indique brevemente su propuesta para este servicio. Indique los recursos, perfiles y herramientas que utilizaría, así como el modelo de prestación del mismo.

1.8. Servicio de gestión de programa de Bug Bounty propuesto.

Indique brevemente su propuesta para este servicio. Indique los recursos, perfiles y herramientas que utilizaría, así como el modelo de prestación del mismo. ¿Cuál sería su propuesta para la definición de los errores/vulnerabilidades/amenazas elegibles para recompensa (y por ende, cuáles descartaría)? En relación a la definición y tipología anterior ¿qué tipo y valoración de recompensa establecería para cada uno de ellos en función de su importancia/criticidad? De cara a la publicación del programa, recepción de reportes, seguimiento, …, etc. ¿Utilizaría alguna herramienta autohospedada para ello (p.e. PwnMachine)?. ¿Utilizaría alguna plataforma de Bug Bounty de un tercero?

1.9. Certificaciones al SOC del proveedor

¿Está el SOC certificado en el ENS en los sistemas de información en los que presta el servicio gestionado de seguridad?

¿El SOC forma parte de foros de seguridad (CSIRT.es, FIRST, TI TF-CSIRT)?

1.10. Estimación de personal y perfiles

¿Qué estimación de personal plantea para los servicios solicitados? Identifique las características de los perfiles que deberían participar en la prestación de cada servicio (% de dedicación a cada uno en caso de tratarse de recursos compartidos), especificando formación, certificaciones y experiencia, y especificando su naturaleza presencial y/o remota.

1.11. Desglose económico a cuatro (4) años

Indique el coste por la unidad de facturación empleada Añada tantas filas como crea necesarias			
Concepto	**Unidades**	**Coste Unitario**	**Importe (sin IVA)**
Servicio de Alerta Temprana de Vulnerabilidades - Plataforma de inventariado, contraste y análisis de vulnerabilidades			
Servicio de Alerta Temprana de Vulnerabilidades - Consultoría y asesoramiento en Amenazas			
Servicio de Análisis de la Superficie de Exposición en Internet (base)			
Servicio de Análisis de la Superficie de Exposición en Internet (ampliaciones)			
Servicio de Análisis de Vulnerabilidades - Servicio atendido			
Servicio de Análisis de Vulnerabilidades - Servicio desatendido para vulnerabilidades Web			
Servicio de Análisis de Vulnerabilidades - Servicio autónomo (base)			
Servicio de Análisis de Vulnerabilidades -			

Servicio autónomo (ampliaciones)			
Servicio de Inteligencia de Amenazas			
Servicio de Vigilancia Digital (base)			
Servicio de Vigilancia Digital (ampliaciones)			
Servicio de Red Team			
Servicio de gestión de programa de Bug Bounty			