INFORME VALORACIÓN SOBRE B (CRITERIOS EVALUABLES MEDIANTE UN JUICIO DE VALOR) DE LAS PROPOSICIONES PRESENTADAS EN EL EXPEDIENTE DE CONTRATACIÓN Nº "2023/86C SER" PARA DEL SERVICIO DE UNA OFICINA DE CIBERSEGURIDAD PARA LA DIPUTACIÓN DE PALENCIA

En la reunión de la mesa de contratación celebrada el día 16 de febrero de 2024 se procedió a la apertura de los sobres A y B correspondientes a la tramitación del expediente para la contratación, mediante procedimiento Nº "2023/86C SER" "Servicio de una oficina de ciberseguridad para la Diputación de Palencia", por petición de la mesa procedo a la valoración de los criterios evaluables mediante un juicio de valor sobre (B).

El único licitador presentado ha sido: CIENCIA E INGENIERIA ECONÓMICA Y SOCIAL S.L.

A la vista de la documentación aportada se procede a la valoración de los criterios del apartado H4 del PACP "criterios cuya evaluación depende de juicio de valor", según los siguientes apartados:

1. **Resumen ejecutivo,**

   El resumen establece los retos y riesgos del proyecto, el valor diferencial, los aspectos claves y enfoque global tales como los siguientes:

   - Descripciones metodológicas individualizadas para cada uno de los servicios prestados (operación de la oficina OCS, Soporte ENS, despliegue SOC,etc.)
   - Para cada una de las herramientas propuestas o trabajos a realizar (agrupados en fases y tareas)
   - Se aportan diversos ejemplos de informes y entregables del proyecto.
   - Planificación detallada por servicio. Se define una tabla con más de 25 hitos.
   - Equipo de trabajo multidisciplinar, especialista en modelos de cumplimiento ENS para entidad local.

2. **Metodología,**

   Se utiliza una metodología de gestión de proyectos interna cumpliendo con la planificación expuesta. Se asegurará la calidad de los trabajos en cada parte y trabajo del proyecto y se creará una extranet con todos los interlocutores para el seguimiento del proyecto. Se entregarán los informes de seguimiento del proyecto

Se han descrito pormenorizadamente la metodología y descripción de las soluciones propuestas por cada servicio que se va a prestar en el marco del proyecto

Fases del proyecto.

- Oficina Técnica de Ciberseguridad /Gobernanza
- Mejora de las capacidades del actual SOC
- OCS/OTS e Implementación ENS
- Formación
- Plan de auditorías y conformidad ENS
- Vigilancia y mejora continua

3. Plan de ejecución,

Se ha presentado un cronograma detallado donde se han descrito pormenorizadamente los hitos y tareas de cada fase y por cada elemento, servicio o herramienta a implantar. Las tareas se distribuyen según 7 perfiles de trabajo.
Se han propuesto 25 hitos, 5 jornadas de apoyo al ENS para definir las directrices generales del proyecto.
Se ponen a disposición del proyecto los recursos necesarios para la correcta ejecución tanto materiales como personales.

Se han mejorado las prestaciones de servicios iniciales incluyendo las siguientes:

PRINCIPALES MEJORAS DE LA PROPUESTA ALINEADOS CON EL OBJETO DE LA CONTRATACIÓN:

A) SOC con SIEM propio con las siguientes mejoras

- Mejora en el número de tipos de fuentes a analizar: La solución permitirá la ingesta de al menos **18 tipos de fuentes diferentes** (DC, Firewall, WAF, IPS, etc. Características mínimas pliego: 15 tipos de fuente)
- Mejora en el Número de reglas concurrentes: Más **de 6.500 reglas**. Al menos **400 reglas funcionan de forma simultánea.** (Características mínimas pliego: 5.000 reglas y 250 reglas simultáneas)
- Eventos por Seguro soportados (EPS): Superior **a 6.000 EPS.** Características mínimas pliego: 5.000 EPS)
- Periodo de retención: Se almacenará eventos durante un mínimo de 12meses, de los cuales, al **menos 3 meses estarán en caliente.** (Características mínimas pliego: 2 meses en caliente)
- Ubicación de **backup:** Copias de seguridad diarias ubicadas de forma externa, con un **plazo de retención superior a 1 año**. Mejora nueva

B) Módulo CSIRT

Se ha incluido en la propuesta los servicios de respuesta ante incidentes, con el que se atenderán y aplicarán los protocolos necesarios para una adecuada gestión de posibles incidentes de seguridad. Se incluye disponibilidad del servicio y atención temprana, con un esfuerzo máximo de **2 jornadas, destinadas a la potencial coordinación del Comité de Crisis**.

El proyecto incluye el servicio de CSIRT: Disponibilidad del servicio y atención temprana, con un esfuerzo máximo de 2 jornadas, destinadas a la potencial coordinación del Comité de Crisis.

C) Respuesta ante incidencias de nivel MUY CRÍTICO

Dado que estos tipos de eventos pueden materializarse en horarios en los que el personal de la Diputación no esté disponible, se incluye en la propuesta un conjunto de acciones de respuesta rápida por parte del SOC que permitan contener una posible

intrusión o por ejemplo minimizar la propagación de un Ransomware. A modo de propuesta, y previa validación por parte de la Diputación, se plantean una serie de escenarios en los que se considera necesaria una rápida actuación, pudiendo el personal del SOC en esos casos tomar acciones proactivas para mitigar la amenaza.

D) Herramienta de Vigilancia Digital

La propuesta incluye adicionalmente una potente solución de vigilancia digital de gran reconocimiento, que permitirá hacer un seguimiento continuo del estado de seguridad de la Diputación de Palencia consultando tanto fuentes abiertas como (OSINT), como Dark y Deep web. La herramienta vigilará de manera continua la identidad digital de la Diputación, buscando información relativa a la misma. La información buscada puede atender a múltiples criterios, como dominios de la organización, direcciones IP, redes sociales, términos específicos de personas, puestos o servicios, etc. Adicionalmente la herramienta cuenta con personal infiltrado en foros criminales para detectar la venta de credenciales de la organización, planificación de ataques o cualquier otro tipo de comentarios que son difícilmente accesibles si no se dispone de entrada en las fuentes adecuadas. Ello permitirá adelantarse a la venta de la información de la Diputación en la web oscura y tomar las medidas correctivas oportunas.

E) Control de la superficie de Exposición

Para el control de la superficie de exposición se utilización diferentes soluciones que, trabajando conjuntamente, permitan tener una visión y control completo de la superficie de exposición de la Diputación.
Se potenciará el uso de las soluciones CCN (Amparo, Clara, Rocío y EMMA) que se complementarán con otras soluciones dentro del SIEM e integraciones con terceros fabricantes.

F) Análisis del Riesgo "Real Risk"

Los análisis de riesgos serán alimentados a través de diferentes pruebas técnicas que permitan conocer el denominado riesgo real. Para ello, se pondrá a disposición un equipo de seguridad ofensiva (Red Team) que se ocupará de realizar diferentes pruebas. El proyecto dispone de la posibilidad de realizar un hacking, desde el punto de vista de un atacante interno o insider, sobre los recursos corporativos que permitirá verificar la eficacia de las actuales medidas de seguridad y su correcto bastionado. Para realizar estas pruebas se deberá disponer de una conexión de red y autorización por parte de la Diputación.

G) Piloto herramienta EMMA

Durante el proyecto se realizará un piloto de EMMA con los módulos de Visibilidad, Control y EMMA-VAR (Vigilancia en Accesos Remotos):

Conclusión La propuesta presentada muestra una información muy detallada, demostrando conocimiento del sector y aportando mejoras muy significativas respecto a los requisitos iniciales, y presentando una total integración con la solución actual de la Diputación, minimizando el impacto en su mejora/puesta en marcha, aspectos que aseguran un alto nivel de calidad de los trabajos.

A la la vista de lo expuesto anteriormente se **otorga al licitador CIENCIA E INGENIERIA ECONÓMICA Y SOCIAL S.L. la PUNTUACIÓN de 28 puntos.**

Firmado electrónicamente por:

Jefa Servicio Informática
Beatriz Bahillo Sáez
22-02-2024