PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN Y GESTION DE SEGURIDAD AVANZADA CON LA HERRAMIENTA DEL CCN-CERT "NG SIEM MONICA"

Ref.: NS-2021-003

INTRODUCCIÓN

BILBAO EXHIBITION CENTRE (en adelante BEC), necesita potenciar la recogida de logs y la seguridad TIC de sus principales sistemas informáticos, comunicaciones y de seguridad perimetral mediante la implantación de un Security Information and Event Management (SIEM) que correlacione eventos potencialmente peligrosos para la seguridad de los sistemas de información de BEC.

El SIEM elegido para implantar es la solución NG SIEM MONICA del Centro Criptológico Nacional, puesta a disposición de las Administraciones Públicas sin coste de licenciamiento.

OBJETO DEL CONTRATO

El objeto del contrato es la contratación de un servicio para la implantación de un sistema de seguridad de la información y gestión de la seguridad con la herramienta del CCN-CERT "MONICA" y su mantenimiento, de forma que permita a BEC la recolección y almacenamiento centralizada de logs, gestionar eficazmente las alertas de las ciberamenazas de seguridad (detección y gestión avanzada de amenazas, gestión eficaz de la respuesta y análisis forense) que potencialmente afecten a los sistemas de información de BEC, y dar respuesta rápida a aquellas que lleguen a materializarse.

Este servicio ha de englobar un conjunto de medidas encaminadas a mejorar la seguridad de la información de BEC, permitiendo disponer de capacidad de detección, análisis y respuesta ante incidentes de seguridad que puedan suceder en las redes y sistemas de información de BEC.

Los requisitos generales de este servicio para la implantación de un sistema de seguridad de la información y gestión de seguridad son:

- Provisión de la licencia gratuita NG SIEM MONICA para 5 fuentes de información (formato de log diferente) en tiempo real/17 fuentes en forense.
- Soporte y mantenimiento del Fabricante NG SIEM MONICA 8x5
- Servicios técnicos especializados para la instalación, configuración de 5 fuentes de información (formato de log diferente), casos de uso y optimización del sistema suministrado.
- Servicio de 24x7 de monitorización automatizado
- Servicio de soporte 8x5, prestados por la empresa adjudicataria del presente pliego, para la atención y gestión de incidentes críticos de forma remota, servicio ofrecido a través de (* bolsa de 100 horas), con atención remota de Incidentes de severidad alta o crítica.
- Formación al equipo técnico de BEC sobre las herramientas de trabajo (15 horas mínimo).
- Suministro plataforma de Remediación - AntiRansomware (hasta 120 dispositivos no servers 24/7).

ALCANCE DE DESPLIEGUE Y OPERACIÓN

Son objeto de este contrato los trabajos necesarios para instalación y parametrización de la herramienta NG SIEM MONICA, así como la administración y operación posterior de la infraestructura instalada. El personal del equipo técnico de BEC tendrá acceso igualmente a la operación de la plataforma.

La explotación deberá permitir mantener un equilibrio entre la detección de alertas de seguridad y el esfuerzo preciso para solucionarlas y documentarlas.

En general, deberá ser posible:

- Recoger, analizar y presentar información de dispositivos de red y de seguridad.
- Facilidades de identificación de accesos (logs).
- Detección de vulnerabilidades y comprobación de cumplimiento de políticas de seguridad.
- Capacidad de incluir información de NDR y EDR.
- Posibilidad de inclusión del contexto de la actividad de la red, el contexto de los usuarios/activos, registros de aplicaciones y reducción de incidentes en alertas reales.
- Trazabilidad de información de la infraestructura objeto del alcance.
- Detección, análisis, gestión y contención/remediación de incidentes de seguridad.

También deberá ser posible configurar diferentes paneles de información, casos de uso personalizados y modelos de informes en formatos explotables externamente.

En el ciclo de vida de la prestación de los servicios contratados distinguimos tres fases:

- **Fase 1:** Instalación, parametrización y formación de la herramienta NG SIEM MONICA.
- **Fase 2:** Prestación de los servicios avanzados de Gestión de Incidentes de Seguridad sobre la herramienta NG SIEM MONICA.
- **Fase 3** Servicios de soporte y mantenimiento del fabricante en modalidad 8x5 de NG SIEM MONICA.

Fase 1: Instalación, parametrización y formación de la herramienta NG SIEM MONICA

Al tratarse de una herramienta integrada y compacta, los requisitos a aportar por parte de BEC para la instalación en esta fase inicial de implantación serán:

- BEC suministrará la infraestructura necesaria para la implantación de la máquina virtual (VM).
- Conexión VPN desde la hipervisora a BEC.
- Hoja Excel de requisitos para la Integración de las fuentes de Logs a monitorizar.

En esta fase del servicio se enmarcan las siguientes actividades por parte del adjudicatario, salvo en los casos en que expresamente se indique que serán realizadas por BEC:

- Diseño de la arquitectura de la herramienta NG SIEM MONICA a instalar definitivamente, incluyendo requisitos hardware en base a logs monitorizados.
- Definición de los requerimientos técnicos sobre los que se instalará la herramienta NG SIEM MONICA.

- Preparación, documentación y despliegue de la herramienta NG SIEM MONICA en formato físico dentro del CPD principal.
- Despliegue de la herramienta integrada NG SIEM MONICA
- Provisión de la licencia gratuita NG SIEM MONICA para 5 fuentes de información.
- Integración de las fuentes acordadas en el arranque del proyecto en la herramienta NG SIEM MONICA y que tendrán un alcance de 5 fuentes de información (formato de log diferente).
- Definición de cuadro de mandos de las fuentes de información integradas.
- Aplicación de inteligencia mediante casos de uso, personalización y desarrollo de nuevos casos de uso.
- Al finalizar la fase de instalación e implantación, se deberá proporcionar al personal del equipo técnico de BEC acceso a la consola de gestión de la herramienta NG SIEM MONICA con rol de operación y la formación necesaria sobre las herramientas de trabajo.

Documentación a entregar en esta fase
La documentación entregada por el adjudicatario y validada por BEC servirá como punto de partida para la fase de instalación y deberá incluir:

- Plan detallado de puesta en marcha y configuración, incluyendo estimación de tiempos para cada una de las tareas. Proceso de instalación, que incluya todos los elementos que son necesarios para disponer del equipamiento y las herramientas totalmente operativas.
- Identificación de partes involucradas en el despliegue y dependencias entre ellas: necesidades de infraestructura hardware, conectividad de red, direccionamiento IP necesario,...
- Plan de configuración del sistema.
- Propuesta de integración con sistemas externos.
- Propuesta de políticas generales de configuración.
- Propuesta de definición de alertas e incidentes.
- Arquitectura del sistema desplegado. Diagramas físicos y lógicos.

Fase 2: Prestación de los servicios avanzados de Gestión de Incidentes de Seguridad sobre la herramienta NG SIEM MONICA

Este servicio vendrá soportado por el personal adscrito al CiberSOC del adjudicatario. Los servicios de gestión de la seguridad desarrollado por el CiberSOC incluirán las siguientes funciones:

1. Servicio de Monitorización 24X7 automatizado:
    - Monitorización de eventos de seguridad mediante la plataforma MONICA.
    - Correlación y análisis de eventos
    - Operación y notificación de alertas
    - Coordinación de respuestas a incidentes

2. Gestión de eventos e incidentes de seguridad críticos con atención remota (*bolsa de horas):

Respuesta ante incidentes, englobando la notificación de los incidentes detectados, conforme a los procedimientos establecidos, así como la gestión del ciclo completo de los mismos, coordinando, de forma alineada y bajo la supervisión del equipo

técnico de BEC, las actuaciones necesarias sobre los sistemas/redes entre los grupos que los administran.

Documentación a entregar en esta fase
Al menos contemplará los siguientes entregables:

- Protocolos de actuación ante alertas de seguridad: Del funcionamiento habitual del sistema de gestión centralizada de la seguridad se extraerán informaciones consecuencia de la monitorización y de la correlación de eventos. A partir de la experiencia aportada por el adjudicatario se definirá una clasificación de severidades para las alertas de seguridad, así como los protocolos de actuación asociados para cada una de ellas.
- Informe de incidente: El adjudicatario se compromete a entregar en un plazo inferior a 48 horas posterior a un incidente grave un informe donde incluya la descripción del incidente, afectación (objeto o servicio afectado, tiempo total, tiempo de inicio y fin de incidencia), antecedentes, causa raíz del incidente, solución y acciones realizadas.

Fase 3: Servicios de soporte y mantenimiento del fabricante en modalidad 8x5 de NG SIEM MONICA

El servicio de soporte y mantenimiento de la herramienta NG SIEM MONICA incluirá:

- Actualizaciones de fixes y su instalación.
- Administración y operación de la configuración de la plataforma NG SIEM MONICA

La implantación de la herramienta NGSIEM MONICA (FASE 1) y la puesta en marcha del servicio de gestión de amenazas de seguridad (FASE 2), englobando los aspectos iniciales de reconocimiento o puesta en contexto de las personas que lo integran con el entorno tecnológico y organizativo de BEC, y la formalización del proceso de gestión de incidentes de seguridad, tendrán comienzo como máximo en diez (10) días tras la formalización del contrato, con una reunión de lanzamiento del servicio, y tendrá una duración máxima de cuatro (4) semanas desde la citada formalización del contrato.

FORMACIÓN
El adjudicatario deberá incluir en su propuesta formación en capacitación de al menos quince (15) horas. La formación debe incluir:

- Arquitectura del sistema desplegado. Funcionalidades de sus componentes.
- Administración básica de la plataforma.
- Administración y gestión de casos de uso.
- Administración y gestión de recolección de datos.
- Gestión de alerta temprana.

El número de asistentes a dichas sesiones será como máximo de 4 personas. Se expedirá certificado de asistencia al curso a los asistentes. Las sesiones de capacitación serán realizadas en las oficinas de BEC en Barakaldo, y si las condiciones de Salud Pública lo desaconsejaran, mediante videoconferencia.

Esta formación se prestará a la finalización de la fase de instalación, como finalización de esta etapa, antes de comenzar la fase de Gestión de Incidentes de Seguridad, salvo modificaciones aprobadas junto con el responsable de BEC.

Otros:
Deberá acreditar mediante certificado que la empresa es MÓNICA Partner certificado. Esta es una certificación de empresa, requisito para la operación con garantías de

MÓNICA en aquellos organismos públicos en los que MÓNICA se distribuye libre de costes de licencias, como parte del acuerdo con el CCN-CERT.

***Bolsa de horas**

Se contratará inicialmente un bloque de bolsa de horas de 100h a consumir en un periodo máximo de 3 años. Una vez consumidas, si fueran necesarias más horas, se contratarán en bloques de 25 horas.

La facturación de la bolsa de horas se realizará por minutos con un mínimo de facturación de 15 minutos.

El servicio de bolsa de horas solo se realizará a petición de personal de BEC.

Por cada petición de uso de la bolsa de horas se realizará un informe con las tareas realizadas y el tiempo consumido.