PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA EL SERVICIO DE DIAGNÓSTICO DEL GRADO DE MADUREZ DE CIBERSEGURIDAD DE LA INDUSTRIA DE GIPUZKOA EN EL ENTORNO ICS (EXPTE. ZIUR2022027)

I.- OBJETO Y ALCANCE DEL SERVICIO

El objeto del contrato es la prestación de la asistencia técnica necesaria a la fundación Ziur para la realización de 3 campañas, en las que se realizará un servicio de evaluación de la seguridad de los entornos ICS (en inglés Industrial Control Systems) en diferentes empresas de diferentes sectores industriales, en las condiciones definidas en este Pliego de Prescripciones Técnicas, a través de las cuales se puede evaluar el estado actual del grado de madurez en materia de ciberseguridad en el entorno industrial de empresas de diferentes sectores industriales, y se puedan obtener los datos necesarios para:

- Obtener una visión global del grado de madurez de los sistemas de protección existentes, específicamente en los entornos productivos e industriales en las empresas de Gipuzkoa.
- Investigar sobre las diferentes medidas de seguridad implementadas en los sistemas industriales.
- Identificar las principales vulnerabilidades que afectan a los dispositivos desplegados dentro de la industria de Gipuzkoa, tanto en la red OT como de la parte IT dentro de la planta industrial,
- Comprobar cómo los procesos y la tecnología está desplegada y configurada para responder antes posibles comportamientos efectuados en ataques reales, antes de que se produzcan,
- Generar un listado de dispositivos más utilizados en las empresas industriales de Gipuzkoa, que permita a ZIUR orientar futuras acciones.

II.- DESCRIPCION DEL SERVICIO

El adjudicatario, para el desarrollo de la actividad objeto del contrato, deberá:

a) ZIUR dispone de una herramienta de autodiagnóstico accesible a través del siguiente portal Web https://diagnostikoa.ziur.eus. El adjudicatario deberá evolucionar el autodiagnóstico existente, y que actualmente tiene un alcance generalista, hacia un autodiagnóstico de ciberseguridad ICS avanzado orientado a la PYME industrial de Gipuzkoa.

b) Disponer de, al menos una herramienta, capaz de analizar las vulnerabilidades dentro de un entorno industrial, que cumplan con los requisitos técnicos establecido en el apartado IV del presente pliego de prescripciones técnicas, que sea posible emplear para todas las empresas participantes en las diferentes campañas objeto del proyecto.
   El despliegue de la/s sonda/s, de uno o más fabricantes en las empresas objeto del estudio, deberá realizarse en modalidad black box a cargo del adjudicatario, de forma que se puedan recabar datos relativos a los siguientes objetivos:
   - Descubrimiento de inventario pasivo
   - Análisis de vulnerabilidad pasivo
   - Análisis de tráfico circulante
   - Análisis de exposición externa

- Análisis de la arquitectura
- GAP frente a IEC 62443-3-3
- Propuesta de recomendaciones de mejora, en base a los hallazgos encontrados en los puntos anteriores

Todas las licencias de hardware y software, requeridos para el despliegue del aplicativo y de todos sus componentes en la empresa final, correrán a cargo del licitador.

c) Formar en el uso de la/s herramienta/s al equipo técnicos de la Fundación Ziur.

d) Realizar las 3 campañas contempladas en el servicio, con una duración de 4 meses cada una, con relación a las empresas designadas por la Fundación ZIUR, quien procederá a la identificación y selección de las empresas, 6 empresas participantes por campaña, sin perjuicio de la ampliación del número de participantes en los términos de la propuesta realizada por parte del adjudicatario.

   Para ello, los trabajos de puesta en marcha contemplarán todo lo necesario para el inicio del servicio en cada una de las campañas, y para cada una de las empresas contemplada en las mismas.

   La Fundación ZIUR contactará con las empresas sobre las que deberá llevarse a efecto la prestación del servicio, siendo la relación jurídica - en todo caso- entre la Fundación Ziur y cada una de las empresas participantes. En este sentido, se formalizarán los correspondientes convenios de colaboración, entre la Fundación y las empresas participantes, a través de los que se posibilite, para el cumplimiento del objeto del contrato, el acceso necesario a los medios de la empresa.

e) Realizar en cada campaña, con cada empresa, las siguientes actividades:
   - Acompañamiento en la realización del autodiagnóstico ICS en cada empresa objeto del estudio.
   - Despliegue de la/s tecnología/s en cada empresa objeto del estudio, teniendo como alcance las redes industriales conectadas, así como redes industriales no conectadas con células OT no conectadas en red. El número de sondas y tipo estará determinado por los escenarios modelos. Estas sondas serán:
     - Máquinas Virtuales, o sondas físicas, desplegadas en zonas específicas de la red industrial de la empresa, a elección de cada empresa industrial.
     - Acompañamiento y ayuda a la empresa, si fuera necesario, para preparar su red (a nivel de configuración) para el correcto funcionamiento de las sondas.

f) Análisis de resultados

   - A la mitad de cada campaña (a los 2 meses del despliegue de la/s herramienta/a) y por cada empresa analizada, el adjudicatario deberá realizar un análisis inicial de los resultados y valoración de estos.

   - El adjudicatario realizará un informe individualizado por cada empresa participante, a la finalización de cada campaña, en el que se recoja información relevante de cada empresa, su grado de madurez en materia de seguridad OT (IEC 62443), así como un listado de

vulnerabilidades, un inventario de activos, análisis de la arquitectura, recomendaciones de mejora, hallazgos relevantes encontrados. etc.

g) Entregables:

Como parte del listado de entregables, para cada campaña, se deberán presentar al menos los siguientes informes, para cada una de las empresas contempladas en la campaña:

1. Informe de despliegue de la/s solución/es, donde se detalle la arquitectura de despliegue de la/s herramienta/s, las redes monitorizadas y los accesos disponibles. Dicha arquitectura se consensuará con cada una de las empresas participantes, y la propuesta estará sujeta a cambios propuestos por las mismas.
2. Informe general de cada campaña, a la finalización de cada una de ellas, en el que se recoja información relacionada con amenazas y vulnerabilidades más relevantes. Se trata de un análisis retrospectivo que recoge parcialmente la información que será utilizada en el informe final objeto del estudio.
3. El adjudicatario realizará un informe individualizado por cada empresa participante, a la finalización de cada campaña, en el que se recoja información relevante de cada empresa, su grado de madurez en materia de seguridad OT (IEC 62443), así como un listado de vulnerabilidades, un inventario de activos, análisis de la arquitectura, recomendaciones de mejora, hallazgos relevantes encontrados, etc.
4. A la finalización del proyecto se procederá al análisis conjunto de toda la información recopilada en las diferentes campañas para la elaboración del **estudio final sobre el diagnóstico del grado de madurez de ciberseguridad de la industria de Gipuzkoa en el entorno ICS**. Este informe es el principal resultado del estudio y debe contener al menos los siguientes apartados:
    a. Desarrollo de las campañas
    b. Sectores analizados
    c. Madurez de las empresas vs IEC62443-3-3
    d. Identificación y gestión de vulnerabilidades
    e. Listado de principales activos
    f. Tipología de arquitecturas detectadas
    g. Análisis de soluciones de gestión de vulnerabilidades
        i. Según el sector afectado
        ii. Según el tamaño de las empresas
    h. Recomendaciones o puntos de mejora generales, a la vista de los hallazgos encontrados
    i. …

III.- METODOLOGIA

La empresa adjudicataria deberá facilitar el ejercicio de las funciones de inspección y control que sobre el desarrollo de los trabajos corresponden a la Fundación ZIUR, dando estricto cumplimiento a las observaciones y recomendaciones que reciba.

La fundación Ziur al objeto de facilitar el desarrollo y seguimiento de los trabajos podrá, dependiendo de las necesidades del servicio, requerir a la empresa adjudicataria para que presente cuantos documentos se estimen como necesarios y asista a cuantas reuniones de trabajo o informativas se consideren

oportunas para el correcto desarrollo del servicio, pudiendo efectuarse de manera presencial y/ o telemática, a elección de la adjudicadora.

Quedará en todo caso a criterio de la Fundación ZIUR la modificación de la forma de seguimiento (reuniones, actas, informes, …) en caso de que lo considere necesario.

Los documentos y acciones desarrolladas en el seno del presente contrato se efectuarán de conformidad al manual de identidad corporativa de Ziur.

La ejecución material del contrato se realizará siguiendo las fases siguientes:

Fase 1.- Trabajos preliminares:

1. Elaboración framework autodiagnóstico ICS (IEC62443-3-3)
2. Despliegue de la/s herramienta/s.

Fase2.- Desarrollo, ejecución y evaluación de la campaña 1.

Fase 3.- Desarrollo, ejecución y evaluación de la campaña 2.

Fase 4.- Desarrollo, ejecución de la campaña 3 y evaluación final.

Para la ejecución de la Fase 1 en el primer mes de servicio el director de la Fundación Ziur dará a conocer al responsable del Proyecto los objetivos perseguidos en cada campaña, así como el listado de las empresas participantes. A su vez, aprobará el cronograma de actuaciones a desarrollar para la prestación del servicio en atención a la propuesta de la empresa y la planificación y contenido del plan de formación a compartir por la adjudicataria a las personas que designe la Fundación Ziur en el uso de la herramienta.

En el desarrollo de las siguientes, y previamente al inicio de cada una de las campañas, se procederá por las partes a concretar de manera pormenorizada las acciones a desarrollar.

A la finalización de cada una de las campañas se realizará un análisis retrospectivo cuatrimestral del servicio, evaluando el grado de cumplimiento de los objetos predeterminados por Ziur y la idoneidad de la metodología de trabajo y tras la finalización de la última campaña, se realizará, asimismo, una valoración global del servicio y de los resultados obtenidos.

Todos los documentos y acciones se realizarán con un planteamiento bilingüe, en euskera y castellano, sin que ello suponga un precio o cargo adicional, y se elaborarán de acuerdo con el manual de identidad corporativa de ZIUR.

Se aplicarán políticas de comunicación que garanticen el uso no sexista y no androcéntrico del lenguaje, imágenes y contenidos.

IV.- REQUISITOS TECNICOS DE LA/S HERRAMIENTA/S

Dado que para recabar la información de la situación actual de los entornos industriales es necesario el despliegue de soluciones tecnológicas, éstas han de cumplir con una serie de requisitos mínimos para

garantizar la obtención de información de calidad, asegurarse que se cubre todo el alcance deseado y que la dependencia y necesidades requeridas de las empresas participantes sea lo menor posible.

Dado que es necesario el despliegue de soluciones tecnológicas para llevar a cabo el estudio, las características de las soluciones serán, pudiendo cumplirse dichas características con una o más de una solución tecnológica:

- Debe tratarse de una solución especifica de monitorización pasiva, que no afecte al buen desempeño de las empresas participantes.
- Debe tener la capacidad de analizar el tráfico en modo “fuera de línea”, mediante el análisis de copias del tráfico generadas en la red y enviadas a la herramienta.
- Dispondrá de la posibilidad de realizar consultas activas, siempre bajo demanda y bajo previa aceptación de la empresa participante.
- En caso de que algunas de las empresas participantes no dispongan de switches gestionables en algunos de los segmentos de red que se quieran estudiar, la empresa adjudicataria deberá disponer de la tecnología necesaria para poder generar las copias del tráfico de interés, para, así poder ser reenviadas a la sonda.
- Capacidad de despliegue tanto en medio físico como virtual
- Posibilidad de conexión directa con un centro de control remoto
- Exportación offline de la información recabada (vulnerabilidades, activos, anomalías, etc.) por si no existiese conexión con el centro de control
- Visibilidad total de las operaciones convergentes de IT/OT.
- Detección de amenazas que afectan a las operaciones industriales
- Identificación y rastreo de activos de IT y OT con obtención de conocimiento profundo del funcionamiento y el estado, siempre y cuando tenga visibilidad sobre ellos
- Identificación y priorización de las vulnerabilidades y amenazas potenciales antes de que se conviertan en exploits y afecten a las operaciones industriales.
- Seguimiento de los cambios de configuración con capacidades de seguimiento de auditoría completas.
- No habrá limitación en el número de vulnerabilidades o anomalías identificadas
- Posibilidad de creación de cuadros de mando
- Posibilidad de disponer políticas configurables y granular
- Debe ser capaz de identificar activos y amenazas y vulnerabilidades mediante el uso de múltiples medios de detección, para que el análisis sea lo más completo y real.

72724351F KOLDOBIKA PECIÑA (R: G75203067)
Digitalki sinatuta norengandik: 72724351F KOLDOBIKA PECIÑA (R: G75203067)
Data: 2022.07.01 09:34:55 +02'00'