PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA EL SERVICIO DE OBSERVATORIO DE CIBERSEGURIDAD CONTINUO (THREAT INTELLIGENCE Y THREAT HUNTING) PARA FUNDACIÓN ZIUR (Exp. ZIUR2023-018)

I.- OBJETO Y ALCANCE DEL SERVICIO

El objeto del presente contrato es la puesta en marcha de 2 servicios continuados dentro observatorio de ciberseguridad de ZIUR. Los contenidos a generar serían los siguientes:

- Incorporación de una tecnología de **Cybercrime Threat Intelligence**, con el objetivo de monitorizar de forma continua la empresas y activos más representativos del sector industrial de Gipuzkoa, y detectar posibles activos comprometidos.

- Incorporación de una tecnología de **Deception**, con el objetivo de crear una red de engaño fabricada a través de la implementación automática de máquinas virtuales y señuelos de fraude, con la finalidad de analizar de forma continua si las empresas del sector industrial de Gipuzkoa son objetivos de ataques dirigidos o no.

II.- DESCRIPCION DEL SERVICIO

Lote 1: Incorporación de una tecnología de Cybercrime Threat Intelligence

La propuesta debe incluir:

1. Suministrar una solución de inteligencia de amenazas automatizada, que sea capaz de analizar y contextualizar las amenazas, observando la superficie de ataque desde la perspectiva de los ciberdelincuentes mediante la monitorización de las principales fuentes del cibercrimen en Internet.
2. Todas las licencias de hardware y software, requeridas para el despliegue del aplicativo y de todos sus componentes en la empresa final, correrán a cargo del licitador.
3. Formar en el uso de la herramienta a las personas que designe ZIUR Fundazioa.
4. Dar soporte a ZIUR Fundazioa, durante la duración del servicio, en el despliegue de la herramienta en las diferentes empresas industriales donde se utilice la herramienta.

La licencia, con todas sus funcionalidades, todos los elementos asociados y necesarios para su uso, y su mantenimiento, debe tener validez durante toda la vigencia del contrato.

Lote 2: Adquisición de una tecnología de Deception, con el objetivo de crear una red de engaño fabricada a través de la implementación automática de máquinas virtuales y señuelos de fraude

La propuesta debe incluir:

1. Suministrar una solución de Deception, que permita crear una red de engaño fabricada a través de la implementación automática de máquinas virtuales y señuelos de fraude
2. Todas las licencias de hardware y software, requeridas para el despliegue del aplicativo y de todos sus componentes en la empresa final, correrán a cargo del licitador.
3. Formar en el uso de la herramienta a las personas que designe ZIUR Fundazioa.
4. Dar soporte a ZIUR Fundazioa en el despliegue de la herramienta en las diferentes empresas industriales donde se utilice la herramienta, mientras dure la prestación del servicio.

La licencia, con todas sus funcionalidades, todos los elementos asociados y necesarios para su uso, y su mantenimiento, debe tener validez durante toda la vigencia del contrato.

III.- METODOLOGIA

Lote 1: Incorporación de una tecnología de Cybercrime Threat Intelligence

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

ZIUR Fundazioa, 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 ZIUR Fundazioa 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.

En todo caso, la adjudicataria deberá acometer las siguientes prestaciones:

1. Trabajos preliminares y despliegue de la herramienta.
2. Formación a ZIUR en el uso de la herramienta
3. Soporte y mantenimiento a ZIUR durante la vigencia del contrato

Lote 2: Adquisición de una tecnología de Deception, con el objetivo de crear una red de engaño fabricada a través de la implementación automática de máquinas virtuales y señuelos de fraude

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

ZIUR Fundazioa, 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 ZIUR Fundazioa 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.

En todo caso, la adjudicataria deberá acometer las siguientes prestaciones:

1. Trabajos preliminares y despliegue de la herramienta.
2. Formación a ZIUR en el uso de la herramienta
3. Soporte y mantenimiento a ZIUR durante la vigencia del contrato, en el despliegue de los entornos que se lleven a cabo para las diferentes empresas industriales. Será el personal de ZIUR el que se encargue de seleccionar dichas empresas.
4. Elaboración de Informes con los resultados arrojados por la herramienta para cada uno de los despliegues, de cada empresa, que se realicen durante la prestación del servicio.
5. Elaboración de un informe final, para la Fundación ZIUR, con un resumen de todos los despliegues realizados.

Todos los informes deberán presentarse en castellano y en euskera.

IV.- REQUISITOS TECNICOS DE LA HERRAMIENTA

Lote 1: Incorporación de una tecnología de Cybercrime Threat Intelligence

La tecnología debe estar basada en una plataforma, que, haciendo uso de inteligencia de amenazas automatizada, analice y contextualice las amenazas para que, de esta manera las organizaciones puedan anticiparse a los posibles ciberataques.

La plataforma debe disponer de las siguientes funcionalidades:

- Amplia recopilación de fuentes - La solución debe ser capaz de recopilar y analizar continuamente información de diversas fuentes de difícil acceso, como foros y mercados clandestinos, canales cerrados de mensajería instantánea y otros servicios ilícitos que utilizan los ciberdelincuentes.
- Informes relevantes - La tecnología tiene que disponer de la generación automática de informes de inteligencia legibles a máquina, informando de potenciales filtraciones de sus bases de datos, puertos y servidores expuestos en su red, cuentas amenazadas o tarjetas de crédito robadas.
- Recopilación de datos en tiempo real – La solución debe recopilar continuamente y de forma automática información de fuentes dinámicas de difícil acceso que se esconden en el ecosistema del cibercrimen.
- Funciones avanzadas de análisis de imagen – La solución propuesta, durante el rastreo de las fuentes, debe ser capaz de recopilar texto, metadatos y también imágenes, aplicando análisis de imagen para extraer inteligencia crítica en formatos habilitados para la búsqueda.
- Anonimidad y total seguridad - La solución de inteligencia debe ser capaz de rastrear y acceder a las fuentes de forma segura y en tiempo real, sin llamar la atención y sin incumplir políticas de seguridad.
- Cobertura multilingüe – la solución debe ser capaz de buscar y acceder a datos sin procesar en más de 100 idiomas y, traducir dichos resultados automáticamente, para su consulta.
- Consultas complejas – La solución debe ser capaz de llevar a cabo consultas y búsquedas de alta complejidad y recopilar resultados relevantes de forma inmediata. Dichas consultas deben poder guardarse para ser reutilizadas.
- Inclusión continua de nuevas fuentes – La solución debe dar acceso a inteligencia obtenida, como mínimo, de volcados de bases de datos, grupos de Telegram, mercados de botnets, foros de hackers y otras fuentes clandestinas.
- Búsquedas securizadas – La solución debe permitir llevar a cabo investigaciones securizadas sin necesidad de exponer nuestros objetivos obteniendo acceso directo a datos sin procesar de nuestro lago de datos de seguridad (Data Leak).
- Alertas precisas en tiempo real – La solución debe permitir el rastreo automático y la notificación inmediata de amenazas contra activos específicos de la organización.
- Una única vista de datos – La solución debe disponer de una plataforma única de gestión, en la que se integre toda la inteligencia disponible en un centro de datos unificado, ofreciendo una clara visión general de toda la superficie externa de ataque.
- Las cuentas de acceso a la plataforma, de las que hará uso el personal técnico de ZIUR, deben hacer uso de 2FA.
- La plataforma de servicio debe estar basada 100% en entorno nube, sin que sea necesario el despliegue de ningún servicio adicional on-premise.
- La solución debe permitir acceso a un histórico de 24 meses del "Data Leak" del fabricante.
- La solución debe estar dimensionada para:
    - 2500 búsquedas sobre la base de datos de Inteligencia de la solución
    - Acceso a informes y estudios de inteligencia de amenazas, basados en diferentes fuentes, llevadas a cabo por el equipo de investigación del fabricante de la solución propuesta
    - Soporte técnico 24x7, durante la prestación del servicio

Lote 2: Adquisición de una tecnología de Deception, con el objetivo de crear una red de engaño fabricada a través de la implementación automática de máquinas virtuales y señuelos de fraude

1. El sistema central de gestión de despliegue de los entornos debe ser formato appliance, y se desplegará en el CPD que la fundación posee en sus oficinas.
2. El despliegue de señuelos en cada uno de los entornos puestos en marcha debe ser automatizado, basado, mayoritariamente, en el inventario de activos de red existente en la herramienta. La solución debe permitir llevar a cabo modificaciones, sobre la base de estos señuelos automáticos, para adaptarlo a los entornos de cada empresa.
3. La herramienta debe estar integrada con MITRE ICS, haciendo uso de sus matrices, mediante el perfilado de los atacantes que lleguen a los entornos desplegados, con respecto a las técnicas que usen dichos atacantes.
4. La herramienta debe disponer de una plataforma central de gestión, donde se pueden gestionar todos los entornos desplegados.
5. La herramienta debe ser capaz de exponer la actividad e interacción con una detección temprana y precisa y alertas procesables. Permitiendo rastrear y correlacionar el movimiento lateral de los atacantes y notificando a los administradores de seguridad a través de la interfaz web, correo electrónico, SNMP TRAP, registros y eventos a través de SYSLOG/CEF. Permitiendo realizar el análisis forense de la información, la cual nos permite detallar los movimientos y actividades laterales de los atacantes y correlacionar la información de incidentes y campañas atacantes.
6. La herramienta debe ser capaz de detectar ataques de Capa 2 como MITM, Responder, ICMP swiping y más.
7. La solución debe posibilitar el análisis de malware en profundidad capturado por las máquinas señuelo mediante la integración con soluciones Sandbox y con la herramienta Virus Total.
8. La solución debe ser capaz de generar informes completos de las alertas de incidentes en formato PDF/CSV, incluyendo la opción de enviar alertas por correo electrónico.
9. La solución debe permitir "Monitorizar y Correlacionar" Incidentes y Campañas proporcionando información sobre:
    a. inicios y cierres de sesión
    b. seguimiento de movimientos laterales,
    c. archivos añadidos/modificados/eliminados/ejecutados en máquinas señuelo.
10. La herramienta debe estar dimensionada para:
    a. Soportar 500 direcciones IP, asociadas a los señuelos desplegados
    b. Soportar 20 señuelos (basados en sobre VM, y 128 VLANs
11. El sistema debe ser capaz de soportar las siguientes maquinas, sistemas operativos, protocolos y servicios virtuales para usarlos como señuelos en los entornos desplegados:
    - Windows (SO y servicios asociados)
    - VPN
    - Linux
    - IoT
    - Cloud
    - Servicios SCADA

  - HTTP
  - FTP
  - TFTP
  - MODBUS
  - S7COM
  - BACNET
  - IPMI
  - TRIXONEX
  - GUARDIAN-AST
  - IEC 60870-5
  - DNP3
  - TRICONEX
  - SRTP
  - PROFINET
- SIEMENS
- SCHNEIDER
- RODWALL
- TRIDIUM
- VERTIV
- GENERAL ELECTRIC
- PHOENIX CONTACT

Donostia-San Sebastián, 29 de septiembre del 2023.

DIRECTOR GENERAL DE ZIUR FUNDAZIOA



Koldo Peciña Txintxurreta