PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS DE CIBERSEGURIDAD DE RED A ADJUDICAR POR PROCEDIMIENTO ABIERTO SIMPLIFICADO CON PLURALIDAD DE CRITERIOS

REF.: 02/2023

1. Objeto

EI objeto del presente Pliego es fijar las condiciones que deben regir la contratación por el Instituto IMDEA Materiales (en adelante, IMDEA Materiales), del Servicio de análisis de tráfico de red inteligente mediante técnicas de Inteligencia Artificial que permita detectar y detener comportamientos anómalos desde el punto de vista de la Ciberseguridad en el tráfico de red de IMDEA Materiales.

Los servicios demandados en el marco del contrato consistirán en el servicio de análisis, monitorización y posible toma de acciones correctoras de la red IP corporativa.

EI servicio autónomo de análisis de tráfico de red inteligente permitirá la detección, investigación, auditoría, y respuesta de posibles ciberamenazas de toda índole, en horario 24x7x365, de modo que el servicio pueda tomar decisiones de forma autónoma o supervisada por especialistas en ciberseguridad.

2. Organización del servicio

2.1. Estructura organizativa

Por parte de IMDEA Materiales, se establecerá un responsable del servicio, que será el responsable de supervisar la prestación del servicio. Será el encargado de dirigir y coordinar la relación con el adjudicatario. Dicho responsable será el responsable de informática o el suplente que por cualquier motivo él decida.

Por parte del adjudicatario, se establecerá un Responsable del Servicio, encargado de garantizar el cumplimiento de los requisitos aquí descritos, asignando los medios adecuados para la correcta prestación del servicio.

En el caso de variación durante la vigencia del contrato de la persona que inicialmente se adscriba a la ejecución del mismo, el contratista deberá proporcionar otra que cumpla igualmente los requisitos exigidos en este procedimiento y los que se hayan ofertado en referencia a los criterios de adjudicación relativos al mismo perfil. Si esto no fuere posible, quedará facultada la Fundación para la resolución del contrato.

2.2. Seguimiento del servicio

Durante la fase de prestación del servicio, se llevarán a cabo reuniones de seguimiento según las necesidades o a petición de cualquiera de las partes.

2.3. Normativa de seguridad de IMDEA Materiales

La solución elegida deberá de estar alineada con el Esquema Nacional de Seguridad nivel MEDIO cumpliendo con sus normas y procedimientos entre los que se encuentran:

- Norma de buenas prácticas para Terceros
- Norma de Acuerdo de Confidencialidad para Terceros
- Norma de utilización de recursos, sistemas de información e instalaciones
- Procedimiento de acceso a las instalaciones
- Procedimiento de desarrollo seguro de aplicaciones
- Procedimiento de Explotación

EI adjudicatario será el responsable de configurar el software o hardware de acuerdo a las recomendaciones de seguridad del fabricante, así como facilitar a IMDEA Materiales las recomendaciones de configuración actualizadas durante toda la vigencia del contrato.

La información proporcionada será únicamente utilizada para los propósitos de este proyecto, comprometiéndose la empresa adjudicataria a:

- No permitir el acceso a la misma a personal no relacionado con el proyecto
- No utilizar la información para otros proyectos
- No ceder la información a terceros
- Devolver y destruir todas las copias realizadas de la información establecida como confidencial, especialmente la referente al tráfico de red de IMDEA Materiales.

3. Fases y entregables

3.1. Auditoría y análisis previo

Sin perjuicio de la definición del servicio descrita en el punto 5.1, toda empresa solicitante **deberá visitar las instalaciones de IMDEA Materiales** dando fe del escenario a cubrir y aceptando y validando los elementos hardware, software e infraestructura de IMDEA Materiales.

A estos efectos se organizará una visita cuya fecha se hará pública en el Perfil del Contratante.

Cualquier error o diferencia de las instalaciones descritas en este pliego con las instalaciones reales no podrá ser motivo de reclamación alguna por parte del adjudicatario.

El concursante deberá incluir en la oferta, un certificado, expedido por la dirección del centro, donde indique haber visitado las instalaciones objeto del contrato.

3.2 Lanzamiento del proyecto

Durante el primer mes del proyecto, la empresa adjudicataria llevará a cabo la toma de datos necesarios para la ejecución del proyecto y proporcionará la siguiente documentación:

- Planificación detallada de la implantación del proyecto
- Arquitectura de la solución propuesta adaptada a la infraestructura de IMDEA Materiales
- Propuesta de despliegue de la solución
- Recomendaciones

3.3. Configuración y puesta en marcha del servicio

Con una duración máxima de seis meses desde la firma del contrato, la empresa adjudicataria llevará a cabo la instalación, configuración y despliegue de la solución de modo que se encuentre completamente funcional y operativa, así como las adaptaciones necesarias para el correcto funcionamiento en función de las necesidades de la infraestructura de IMDEA Materiales para la correcta prestación del servicio de análisis de tráfico de red inteligente mediante técnicas de Inteligencia Artificial.

Antes de la puesta en marcha se impartirá formación al departamento de IT de IMDEA Materiales consistiendo en un mínimo de tres jornadas.

A la finalización de esta fase el adjudicatario entregará la siguiente documentación, o enlace a ella:

- Manual de uso de la herramienta
- Procedimiento de instalación y despliegue
- Arquitectura y diseño de la solución
- Definición de procedimientos de reacción a amenazas

3.4. Prestación del servicio

Una vez finalizada la fase de configuración y puesta en marcha del servicio, comienza la fase de prestación del servicio.

Durante esta fase el adjudicatario será responsable de la elaboración y entrega de la siguiente documentación:

- Actas de las reuniones mantenidas

- Informes de seguimiento del servicio, incluyendo incidencias y propuestas de mejora

4. Infraestructura de IMDEA Materiales

Actualmente IMDEA Materiales dispone de la siguiente infraestructura que da soporte al tráfico de red y aplicaciones:

- Sedes: IMDEA Materiales tiene una única sede situada en la C/ Eric Kandel 2 Getafe.
- Centro de procesado de datos (CPD): el centro de procesado de datos se encuentra en la planta SS del edificio, cuenta con control de acceso, refrigeración redundante, cuadro de energía redundado y sistema de alimentación ininterrumpida.
- Red: los switches de red son del fabricante Force10, DELL. El core es del fabricante DELL. Los puntos de acceso inalámbricos son del fabricante ExtremeCloud IQ
- Firewall: los router utilizados que proporcionan el acceso VPN son dos SonicWall NSa 2700 en configuración de alta disponibilidad HA
- Línea de acceso: se utiliza un enlace de fibra de 1Gbp/s proporcionado por el proveedor Zertia.
- Virtualización: disponemos de 4 servidores VMWare EsxI y 2 servidores Hyper-V
- Escritorio remoto: disponemos de un servidor vdi que proporciona 20 escritorios virtuales en entorno onpremise bajo servidor VMWare con UDS como orquestador.
- Antivirus: tanto los servidores como los equipos cliente cuentan con la suite Bitdefender.
- Servidor de correo: el correo electrónico es un servidor externo en base Linux con Roundcube proporcionado por proveedor externo ASPL. El acceso es mediante IMAP, POP3 y HTTPS
- Equipos clientes: nuestros usuario e investigadores usan ordenadores personales con Windows 7, 10 y 11 tanto profesional como server, equipos Mac, equipos Linux y microcontroladores Raspberry
- Cluster: disponemos de un cluster de alta computación con sistema CentOS controlado por BrightClusterManager con servicio BeeGFS y comunicación InfiniBand

La solución elegida ha de dar soporte a dicha infraestructura. La incompatibilidad con alguno de los sistemas descritos será motivo de exclusión del proceso de licitación.

El equipamiento e infraestructura de IMDEA Materiales está en continua evolución. Es menester por tanto que la solución ofrecida sea flexible y capaz de adaptarse a futuros cambios y/o tecnologías.

5. Requisitos técnicos

Los requisitos técnicos se separarán entre requisitos base de obligado cumplimiento y requisitos evaluables.

Los requisitos de obligado cumplimiento tendrán que ser cumplidos y acreditados de manera independiente y el no cumplimiento de cualquiera de ellos será motivo de exclusión de la propuesta por motivos técnicos.

5.1 Requisitos base de obligado cumplimiento:

La solución ha de ser compatible con la infraestructura de IMDEA Materiales.

La solución elegida tendrá que ser de un solo fabricante.

La solución analizará en tiempo real todo el tráfico de la red de IMDEA Materiales mediante port mirroring "puerto espejo" conectado al/los switch/es CORES de la organización.

El análisis del tráfico de red será de forma pasiva, sin interceptar el tráfico ni mermar el rendimiento de la red de manera alguna.

La solución permitirá examinar la red a tiempo real y consultar lo ocurrido en el último año.

La solución analizará un mínimo de 400 dispositivos de red.

La herramienta deberá de tener implementada seguridad de doble factor, tanto para la solución *per se* como para la plataforma de acceso a información del fabricante, donde se pueda acceder a seguimiento de tickets, documentación y tutoriales.

La herramienta tendrá la funcionalidad de integración nativa con la solución Slack.

La herramienta deberá tener un cliente nativo para Android e IOs que permita disfrutar de la misma funcionalidad que el cliente pesado o nativo.

La herramienta ha de ser capaz de analizar el tráfico entre servidores/equipos virtualizados. Deberá de ser capar por tanto de utilizar sondas compatibles o V-sensors.

La herramienta facilitará La investigación completa y generación de informes automáticos de los incidentes que se hayan detectado, permitiendo así facilitar al personal de IMDEA Materiales poder disponer de herramientas para simplificar la investigación de los incidentes de una forma rápida y eficiente.

EI análisis del tráfico de red se deberá realizar mediante Inteligencia Artificial con aprendizaje automático supervisado y no supervisado. No debe estar basado en reglas, debe

aprender para determinar el comportamiento normal del tráfico de red y detectar comportamiento malicioso.

Será capaz de aprender tanto del tráfico de red como de las acciones dadas por los técnicos de IMDEA Materiales.

De esta manera si una alerta detectada por la solución es dada por buena por el personal de IMDEA Materiales el software tendrá que aprender de dicha acción con el fin de amoldarse al escenario de la organización.

La solución tendrá una funcionalidad de respuesta frente a las amenazas detectadas.

La solución tendrá que contar con una función de remediación o solución ejecutiva del problema detectado a la que llamaremos respuesta. La respuesta podrá venir dada de manera reactiva por el personal de IMDEA Materiales. Tras notificar o alertar la solución de un problema detectado el personal de IMDEA Materiales podrá definir una acción dada: omitir, observar, aislar el equipo, aislar la subred, impedir/bloquear únicamente la acción detectada, etc. Dichas acciones quedarán guardadas para futuras consultas.

La solución podrá llegar a alertar de manera telefónica (directamente o vía app nativa instalada) al personal de IMDEA Materiales según el horario, calendario, o criticidad de la incidencia detectada.

Del mismo modo y sin perjuicio de lo anterior la solución deberá ser capaz de tomar acciones ejecutoras basadas en parámetros definidos por IMDEA Materiales con la ayuda del licitador ganador.

5.2 Requisitos evaluables:

En el apartado 9 de la cláusula 1 del Pliego de Cláusulas Jurídicas se detallan los criterios técnicos evaluables tanto de forma automática como por juicio de valor.