EXP. L5/2024

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE UN SISTEMA DE DETECCIÓN Y RESPUESTA NDR (NETWORK DETECTION AND RESPONSE)

SIGMA GESTIÓN UNIVERSITARIA,

A.I.E. (M.P.)

ÍNDICE

1. Introducción

Fundada en 1996, SIGMA Gestión Universitaria, A.I.E. (MP) (en adelante, SIGMA) es una agrupación sin ánimo de lucro presidida por 15 de las instituciones académicas más importantes del país. Su actividad se centra en ayudar a las instituciones de educación superior a optimizar su gestión con tecnologías de la información (TI), aportando las mejores soluciones posibles para la gestión académica, docencia e investigación.

La prestación de los servicios de SIGMA se soporta mediante una infraestructura crítica, que da servicio actualmente a 38 Universidades, a más de 218.000 alumnos y más de 50.000 personas PAS y PDI de las Universidades Españolas.

Esta infraestructura cubre las necesidades de gestión académica e investigación de alumnos, profesores, personal laboral e investigadores de las Universidades Españolas. SIGMA, reconociendo y valorando la importancia estratégica de las tecnologías de la información y las comunicaciones, tiene entre sus objetivos contar con la disponibilidad de infraestructuras avanzadas y calidad del servicio. En este sentido, SIGMA presenta unas necesidades específicas derivadas de la dispersión de sus clientes que sólo se pueden satisfacer mediante una infraestructura cercana que garantice de forma fiable tanto los flujos de información internos como los externos.

2. Objeto.

El objeto del presente Pliego de Prescripciones Técnicas Particulares es fijar las condiciones de índole técnico que deben regir la contratación de un sistema de detección y respuesta NDR (Network Detection and Response) para poder detectar y responder a las amenazas que puedan ocurrir en cualquier de los Centros de Procesamiento de Datos (CPD's) distribuidos de que se compone la infraestructura técnica de SIGMA, según las condiciones específicas y características técnicas detalladas en este pliego.

Actualmente SIGMA cuenta con múltiples dispositivos de red (equipos, electrónica de red, AP's, IoTs, etc.) distribuidos por los diferentes CPD's que requieren de visibilidad para poder tener un control de los accesos que se realizan y los riesgos que pueden suponer y así poder mejorar la seguridad de la red.

Por este motivo surge la necesidad de garantizar la confidencialidad de los datos de las Universidades y la disponibilidad de los sistemas, para lo cual es imprescindible la implantación de medidas de seguridad en las redes de comunicaciones que componen la infraestructura de SIGMA. Actualmente, SIGMA está certificada en el Esquema Nacional de Seguridad que entre sus requerimientos se enmarca la implantación de sistemas de seguridad que cuenten con la certificación de seguridad que en el caso SIGMA es de nivel MEDIO.

Por todo esto la presente licitación tiene por objeto la contratación de un sistema NDR (Network Detection and Response), incluyendo la adquisición de hardware de red NDR, así como de tareas de implantación, puesta en marcha y soporte ligados a la adquisición del producto teniendo en cuenta las siguientes ubicaciones de centros de datos de SIGMA:

- Datacenter ubicado en las oficinas centrales en Sant Cugat del Vallés
- Datacenter ubicado en la ciudad de Barcelona
- Datacenter ubicado en la ciudad de Madrid

- Además, cabe tener en cuenta que SIGMA dispone de recursos en cloud pública AWS.

Asimismo, la licitación debería incluir los posteriores servicios MDR de acuerdo con lo indicado en este pliego.

3. Requisitos generales

3.1. Descripción del sistema NDR

El sistema de NDR requerido debe analizar continuamente el tráfico de red que recorre esa infraestructura de red sin procesar para crear modelos que reflejen el comportamiento normal de la red. Utilizan principalmente técnicas no basadas en firmas, por ejemplo, aprendizaje automático u otras técnicas analíticas, para detectar tráfico malicioso.

Cuando estas herramientas requeridas detecten tráfico malicioso deben generar alarmas. Además, se requiere la monitorización del tráfico 365 grados, es decir, monitorizando tanto el tráfico que entra y sale de las redes corporativas como los movimientos laterales entre redes internas al analizar el tráfico de sensores de red ubicados estratégicamente y convenientemente configurados.

La respuesta también es una característica importante de la solución NDR requerida. Respuesta automática, por ejemplo, para enviar avisos a un firewall para que bloquee un cierto tráfico sospecho o a un EDR/XDR para que aísle un equipo (portátil/servidor/contenedor/…) que esté generando o recibiendo tráfico sospechoso, o también pudiendo soportar respuestas manuales.

Con la implantación de este sistema se pretende:

- Dotar a SIGMA de tecnología de monitorización de tráfico centralizada en un único punto.
- Mejorar la seguridad y la protección de las redes internas, así como las redes que nos comunican con las Universidades que forman parte de la agrupación.
- De forma sencilla controlar en todo momento el estado de todas las redes de comunicaciones.
- Tener un inventario continuamente actualizado con todos los riesgos y vulnerabilidades que pueden afectar a la infraestructura.

3.2. Disponibilidad del servicio

El servicio prestado deberá de realizarse ininterrumpidamente en la modalidad 24x7. Se garantizará como mínimo una disponibilidad prevista en el SLO o SLA propuesto para todos los servicios.

3.3. Interrupción del servicio prestado

El adjudicatario deberá informar debidamente a SIGMA de las interrupciones temporales del servicio que se requieran para la realización de actualizaciones, mejoras o reparaciones técnicas y acordar, con SIGMA, las fechas y horas de actuación que supongan cualquier tipo de parada de alguno de los servicios, con una semana de antelación, salvo casos de fuerza mayor.

3.4. Asistencia Técnica

El adjudicatario deberá asistir al personal de SIGMA, o al que éste determine, en la configuración, instalación y optimización de los sistemas y aplicaciones desplegadas, efectuando las propuestas y recomendaciones que, a criterio de aquel, puedan redundar en la mejora del servicio.

3.5. Costes hardware y software

Se consideran incluidos todos los gastos de reparaciones ocasionados por fallos de funcionamiento o averías, incluidos mano de obra, piezas, desplazamientos, impuestos, o de cualquier otra índole durante el proceso de implantación y durante la ejecución del servicio, cuando dichos gastos derivaran de responsabilidades del adjudicatario.

3.6. Requisitos de Seguridad

El adjudicatario, dentro de sus obligaciones de mantener la conectividad de SIGMA, realizará estas funciones con el adecuado nivel de seguridad, incluyendo entre los servicios todos los necesarios para el mantenimiento de la seguridad perimetral y de las aplicaciones (antivirus, antimalware, IDS, firewall…).

En cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, deberá asegurarse la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas. En consecuencia, se exigirá que los licitadores presenten documentación acreditativa de la correspondiente inclusión en el **catálogo de productos y servicios de Seguridad** de las Tecnologías de la Información y la Comunicación del CCN o su tramitación con el CCN si es el caso, o bien en el Catálogo Common Criteria o equivalente.

El adjudicatario está obligado a comunicar lo antes posible a SIGMA cualquier incidencia en el ámbito de la seguridad en el momento en que se detecte, por el método que se determine de común acuerdo. En particular, el adjudicatario estará obligado a la comunicación inmediata de cualquier detección de intentos para quebrantar la seguridad de los sistemas de SIGMA en el ámbito de esta contratación.

En el caso de llegar a producirse algún incidente de seguridad, el adjudicatario tomará las medidas correctivas y de previsión necesarias para evitar su repetición e informará inmediatamente a SIGMA, generando un documento detallado del evento de seguridad producido y tomando las medidas necesarias para intentar localizar el origen y la causa.

En caso de producirse cualquier intrusión, de cualquier tipo o naturaleza, en el sistema, el adjudicatario se obliga con SIGMA a poner su disposición toda la información escrita o digital necesaria para la investigación del evento de seguridad.

4. Requisitos Técnicos de la Solución NDR

4.1. Situación Actual

La volumetría de los activos es la siguiente:

- 650 IPs privadas
- 200 cuentas de Microsoft365

4.2. Arquitectura de la solución a implantar

La arquitectura de la solución que deberá implatarse para la prestación del servicio estará compuesta por tres sondas hardware en cada Data Center solicitado en este pliego, siendo una de ellas la sonda principal con función de consola de gestión.

Los requisitos de las sondas son los siguientes:

- Datacenter de Sant Cugat. La sonda debe cumplir los siguientes requisitos mínimos:

  - Match Troughput: 4,6 Gbps en caso de funcionamiento como sonda y consola y 9 Gbps en caso de funcionamiento únicamente como consola.
  - Puertos de Captura:
    - 2 x 10 Gbps SFP+
    - 2 x 1 Gbps
  - Puertos de Gestión
    - 2 puertos 10/100/1000 ó 1 puerto 10Gbps SFP+
  - Soporte IDRAC
  - Deben ser enrackables y ocupar 1 U como máximo

- Data Center Madrid y Barcelona. Cada sonda (una en cada ubicación) debe cumplir los siguientes requisitos mínimos:
  - Match Troughput: 1,2 Gbps
  - Puertos de Captura
    - 2 x 1 Gbps
  - Puertos de Gestión
    - 2 puertos 10/100/1000
  - Soporte IDRAC
  - Deben ser enrackables y ocupar 1 U como máximo

4.3. Características y funcionalidades de la herramienta

La solución NDR deberá proporcionar una forma rápida y eficiente de encontrar y detener a los posibles atacantes, así como visibilidad de ataques en tiempo real y exponer los detalles del ataque para potenciar la acción inmediata para lo cual deberá tener en cuenta las siguientes características y/o requerimientos:

- Debe poder capturar el tráfico de red desde múltiples puntos de captura (sondas) con un impacto mínimo en la infraestructura actual de SIGMA.
- Debe poder analizar el tráfico de hosts y cuentas utilizando únicamente la sonda a instalar en cada una de las tres ubicaciones, además de las soluciones implantadas en AWS y las cuentas Microsoft 365, estas 2 opciones se valorarán opcionalmente.
- En la parte de AWS, debe proporcionar un componente de análisis del plano de control de AWS que pueda detectar posibles comportamientos maliciosos y metodologías de ataque que pongan en riesgo la computación, las redes, los servicios de almacenamiento y los datos de AWS.
- La solución no debe requerir la instalación de agentes, ni en la fase de análisis ni en la de respuesta.
- Debe utilizar diferentes algoritmos de aprendizaje automático, incluido el aprendizaje supervisado, no supervisado y profundo, para detectar comportamientos de atacantes dentro de la red y reducir los falsos positivos.
- Debe tener claramente definidas cada una de las detecciones que realiza y las categorías asociadas a estas. A tal efecto, el licitador deberá adjuntar un listado detallado de cada una de las detecciones disponibles, así como su descripción y mapeo con el marco MITRE ATTACK, teniendo en cuenta que las capacidades de detección deben ser reconocidas por el marco MITRE D3FEND.
- Deberá ser capaz de realizar detecciones de ataques desde el primer minuto de funcionamiento sin necesidad de aprendizajes o entrenamientos iniciales.
- Debe proporcionar y mantener automáticamente fuentes de inteligencia sobre amenazas, altamente confiables, que deben ser utilizadas en el análisis del tráfico.
- Automatizar las investigaciones de seguridad con respuestas concluyentes.
- Realizar un seguimiento persistente de las amenazas en todas las fases del ataque.
- Cubrir todos los activos: cualquier sistema operativo, incluyendo Smartphones, Tablets de los usuarios…
- Asegurar toda la infraestructura, física y virtual.
- Debe incorporar una solución de Data Lake para poder albergar, como mínimo, 30 GBs de los metadatos generados por los sensores de, al menos, las dos semanas

anteriores, durante como mínimo 1 año, con el fin de poder realizar un threat hunting avanzado.

- Debe poder funcionar en modo aislado (sin acceso a Internet), con la posibilidad de cargar paquetes de actualización fuera de línea.

4.4. Integraciones

La solución propuesta deberá poder integrarse con los principales SIEM, firewalls, NAC y soluciones EDR. En concreto, deberá poder integrarse con:

- CrowdStrike
- Windows Defender
- SentinelOne
- Fortinet
- Fireeye Endpoint Security
- Elasticsearch

5. Fases y especificaciones para la prestación de los servicios

5.1. Plan de Trabajo

Se presentará un Plan de Trabajo que garantice la CONTINUIDAD del servicio durante el periodo de implantación. Se valorará en los criterios de adjudicación la viabilidad y garantía de dicha disponibilidad durante el periodo de implantación. Este Plan de Trabajo será aprobado por SIGMA.

Se presentará por parte del adjudicatario un cronograma detallado de fases y tareas. Igualmente se presentará una lista de la documentación a entregar.

5.2. Fase 1: Instalación, configuración y puesta en marcha.

Esta fase se iniciará con la instalación física de las sondas en las ubicaciones del Datacenter de Barcelona, Madrid y Sant Cugat. En esta última ubicación, la instalación física de la sonda será realizada por SIGMA con el soporte del proveedor.

La instalación física irá continuada con la configuración lógica de las sondas y consola en las tres ubicaciones indicadas en el apartado 2, que permita prestar el servicio descrito en la fase 2.

Los servicios incluidos en esta Fase 1 consistirán en:

- La instalación física, conexionado a la red eléctrica, conexionado a la red de datos, instalación de las sondas de monitorización, etc.
- Configuración de los elementos de red para hacer posible la monitorización de todo el tráfico.
- Configuración de accesos desde y hacia Internet de todos los servicios que lo precisen.
- Configuración de las integraciones con elementos de terceros como Firewalls, en las 3 sedes, y EDR/XDR.
- Configuración de las políticas de seguridad recomendadas por el fabricante/proveedor.
- Configuración de las políticas de calidad de servicio a nivel de aplicación y tuning específico.
- Pruebas de verificación.
- Puesta en marcha del sistema.

5.3. Fase 2: Prestación del servicio

Una vez instalado y puesto en marcha el sistema de NDR, se iniciará el servicio de ciberseguridad que permita detectar, investigar y responder a las amenazas en modalidad 24/7/365.

Los requisitos específicos que debe cumplir el servicio de Ciberseguridad que compone esta Fase 2 son los siguientes:

- Modalidad 24x7 los 365 días del año
- El alcance del servicio debe incluir los recursos en la nube pública (Azure/AWS), sistemas de identidad e infraestructura de red, cuyas amenazas deben poder ser detectadas en tiempo real.
- El servicio debe de trabajar de forma conjunta con los resultados ofrecidos por mecanismo de IA (Inteligencia Artificial), para la detección, clasificación y priorización de ataques modernos, evasivos u sofisticados.
- Debe poder permitir detectar y priorizar las amenazas de forma automática.
- El servicio debe incluir la priorización de alertas.
- Debe incluir un proceso de triaje o filtrado, valorando la creación de filtros personalizados para aprobar comportamientos autorizados. El adjudicatario debe colaborar mediante sugerencias individualizadas para conseguir un proceso de triaje eficaz.
- Debe incluir, al menos 1 reunión mensual de los analistas de seguridad del adjudicatario con la(s) persona(s) designada(s) por SIGMA, para discutir tendencias globales y específicas de SIGMA, posturas de seguridad y eventos detectados en la red.

Para que todo ello sea posible, los analistas de seguridad del adjudicatario y el responsable del servicio de SIGMA trabajarán de forma colaborativa.

En Sant Cugat, 01 de agosto de 2024.