MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

t. +34 94 657 40 00
info@azti.es | **www.**azti.es

Anuncio de licitación

Sukarrieta, 22 de abril de 2020

1. OBJETO

La Fundación AZTI anuncia la apertura de un procedimiento de licitación por concurso público para la **contratación del servicio de detección, desinfección de malware, y de protección completa de todos los equipos (puestos de trabajo de usuarios y servidores) del parque informático de FUNDACIÓN AZTI – AZTI FUNDAZIOA mediante el PANDA ACTIVE DEFENSE 360**.

Este servicio permitirá la clasificación de todo el software que se ejecuta en el puesto de trabajo, monitorizará el comportamiento de este, asegurará la identificación del software confiable y no confiable y bloqueará la ejecución del software no confiable.

Se debe incluir también un servicio de gestión y mantenimiento de equipos que permita el control del estado de los equipos, así como poder aplicar políticas e instalar remotamente.

Los servicios a contratar serán,

- Adaptive defense 360 sobre Aether Platform.
- Systems Management.

2. DURACIÓN DEL SERVICIO

El período mínimo para el que se contratará este servicio será de 24 meses (2 años) y con un máximo de 36 meses (3 años) a partir de la fecha de la firma del contrato. En función de las ofertas recibidas, se decidirá dicho periodo.

3. OFERTA ECONÓMICA

La oferta económica máxima que se aceptará para esta licitación es de **sesenta y cinco euros (65,00€)** por cada licencia, para los 24 meses, impuestos no incluidos. AZTI, garantiza una compra mínima de 360 licencias.

La facturación se realizará a la firma del contrato, y la factura será pagada a los 60 días de la fecha de su emisión.

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

4. CRITERIOS DE VALORACIÓN DE LAS PROPUESTAS

Las propuestas recibidas serán valoradas en base a los siguientes criterios:

Oferta económica	70%
Certificaciones técnicas	20%
Mejoras	5%
Políticas RSC	5%

5. PRESENTACIÓN DE LAS PROPUESTAS

Los licitadores podrán presentar sus propuestas a la atención de Irati Velez a la dirección de correo electrónico ivelez@azti.es y en cualquiera de los centros de AZTI, desde la publicación de este anuncio en la web de Fundación AZTI, **hasta las 12 horas del próximo día 15 de mayo de 2020**.

Los licitadores podrán dirigirse a la siguiente dirección para recabar información técnica adicional:

AZTI

Atte. Cesar Idokiliz

Telf. 34 656 784 978

Mail: cesar@azti.es

6. ADJUDICACIÓN

Recibidas las ofertas en la fecha señalada para su presentación, en el plazo de 15 días laborales, se publicará en la página web de Fundación AZTI el resultado de la licitación.

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

7. CONDICIONES PARA LA CONTRATACION

- La entidad seleccionada, en el tiempo que dure la relación de servicios con AZTI, deberá cumplir con la normativa vigente en materia laboral, Seguridad Social y de Seguridad y Salud en el Trabajo, estando sujetos si procede a realizar la coordinación de actividades empresariales de acuerdo al RD 171/2004 según procedimiento y especificaciones establecidas (disponibles en http://www.azti.es/es/coordinacion-de-actividades-empresariales/)
- La entidad seleccionada en todo caso e independientemente de cualquier otra documentación, deberá presentar antes de la formalización del contrato, certificado que acredite que se halla al corriente del cumplimiento de las obligaciones tributarias y con la Seguridad Social
- La entidad seleccionada, deberá presentar la documentación necesaria para formalizar el contrato en un plazo no superior a 20 días desde la adjudicación. Cualquier cuestión adicional podrá consultarse en la Normativa interna de Contratación publicada en www.azti.es
- Las empresas licitadoras que se presenten deberán presentar un Certificado de titularidad bancaria expedido por la entidad, en la que indique el número de cuenta bancario que utilizaremos para abonar los servicios prestados o materiales adquiridos
- Adicionalmente a las condiciones técnicas, administrativas, AZTI valorará positivamente, a aquellos proveedores que demuestren mantener políticas de Calidad, Seguridad y Salud, Medio Ambiente, Movilidad Sostenible, así como de Responsabilidad Social Corporativa.

  El proveedor incluirá en su propuesta aquellos documentos o registros que permitan verificar dichas políticas (certificados de calidad, medioambientales, documentación relativa a las actuaciones en asuntos de responsabilidad social, etc.)

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

8. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Responsable: Identidad: FUNDACION AZTI - AZTI FUNDAZIOA - CIF: G48939508 Dir. postal: TXATXARRAMENDI UGARTEA Z/G SUKARRIETA (BIZKAIA) Teléfono: 946574000 Correo electrónico: lopd@azti.es.

“Desde FUNDACIÓN AZTI tratamos la información que nos facilita con el fin de realizar su pedido y facturar los servicios y mantener las relaciones comerciales. La base jurídica del tratamiento de sus datos personales es nuestro interés legítimo en mantener las relaciones comerciales y ejecutar la prestación de los servicios, siendo estrictamente necesarios para esta finalidad. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales y, una vez resuelta la relación, en la medida en que pudieran surgir responsabilidades. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal, así como a aquellos proveedores de servicios técnicos e informáticos y auditoría. En ningún caso, llevará a cabo transferencias internacionales de sus datos personales. Usted tiene derecho a obtener confirmación sobre si en FUNDACION AZTI - AZTI FUNDAZIOA estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios, así como ejercer su derecho de oposición, limitación o portabilidad de sus datos, en los términos previstos en la normativa aplicable en materia de protección de datos, mediante comunicación escrita a la dirección arriba indicada. Asimismo, podrá presentar una reclamación ante la autoridad de control competente.”

9. CLAUSULAS TÉCNICAS ESPECÍFICAS

9.1.- ACTIVOS A PROTEGER

La solución deberá ser capaz de proteger al menos 360 equipos (CPU)

9.2.- UBICACIÓN PLATAFORMA

Con el fin de reducir los costes de mantenimiento y explotación de la solución, no deberá ser necesario el uso de una plataforma interna, se precisa una solución basada en cloud. Es requisito mínimo que la plataforma donde se aloje la infraestructura se encuentre fuera de nuestras instalaciones y operada por el fabricante de la solución en un modelo cloud, en el que no haya un inconveniente en el crecimiento y escalabilidad de la plataforma. Asegurando que independientemente del número de nodos de la instalación la plataforma funcione en el mismo nivel de eficiencia.

La ubicación de la plataforma debe estar alojada en la Unión Europea.

Existen nodos que están distribuidos por diferentes sedes e incluso en movilidad por lo cual estos aprovecharan la disponibilidad de la infraestructura cloud para que estén integrados de forma completa en la configuración y actualización de la solución.

La plataforma de gestión debe cubrir los principales niveles de certificación como son: ISO 27001 y se valorara positivamente cualquier otra certificación que disponga la infraestructura.

9.3.- COMPONENTES DEL SERVICIO

9.3.1. Infraestructura Cloud

El adjudicatario proveerá, desde la nube, el conjunto de servidores, bases de datos y procesos de tratamiento de la información relacionada con el servicio. Los procesos capturados de los clientes serán tratados en la nube de tal forma que el impacto sobre los sistemas corporativos sea mínimo. La gestión de los equipos se realizará desde la nube permitiendo que puedan ser gestionados equipos en diferentes ubicaciones e incluso en movilidad

9.3.2. Agente, a desplegar en los equipos.

El agente desplegado permitirá la comunicación y gestión de tanto la protección de antivirus tradicional, así como de la protección de procesos desconocidos y la gestión y conexión remota a los equipos.

Recogerá la información correspondiente a los eventos y los componentes que los producen, sin recopilar información, ni documentos de usuario. El impacto sobre los

dispositivos del parque deberá ser menor al 5 % de rendimiento de la CPU, memoria y disco

El agente debe ser capaz de proteger equipos de sobremesa y portátiles con los siguientes sistemas operativos:

- Desde Microsoft Windows XP SP3 hasta Microsoft Windows 10.

Deberá proteger equipos servidores con las versiones de sistema operativo:

- Desde Microsoft Windows 2003 hasta Microsoft Windows 2019.

La desinstalación de la protección deberá protegerse mediante contraseña.

La solución debe poder desplegarse de manera silenciosa mediante los siguientes mecanismos: por dirección IP, rango de direcciones IP, nombre de máquina y grupos de Directorio Activo de Microsoft basado en políticas de dominio.

9.3.3. Consola Web

El adjudicatario proporcionará un interfaz en el que se puedan consultar datos en tiempo real, descargar informes/alertas, acceder a la configuración y políticas y disponer de las actualizaciones de los agentes.

Los administradores del servicio podrán gestionar desde una única consola y de manera centralizada, mediante cualquier navegador web la seguridad y productividad de todas las estaciones de trabajo y servidores Windows incluso ordenadores portátiles y oficinas remotas.

9.4.- PROTECCIÓN

La protección solicitada se dividirá en tres partes:

- Endpoint Protection Platform (EPP)
- Endpoint detection and response (EDR)
- Remote Monitoring & Management (RMM)

Las dos primeras partes deben estarán combinadas y fusionadas a nivel de configuración, tan solo estarán divididas a nivel de funcionalidades. Y estar compuesto por un solo agente y una sola solución. No se permitirá el uso de diferentes componentes. Con el fin de conseguir una protección contra amenazas desconocidas en la que colabore el antivirus tradicional con la protección avanzada.

9.4.1.- Endpoint Protection Platform

Se requiere una solución de EPP (Endpoint Protection Platform) con las siguientes funcionalidades:

- Antivirus para archivos, correo y web. Permitiendo la detección y desinfección de cualquier tipo de amenaza. Detectando malware por comportamiento. El correo detectara en POP3. En cuanto a la protección web se detectarán los intentos de acceso a páginas web que contengan elementos maliciosos, bloqueándolos.

- Firewall personal gestionado en local o de forma centralizada desde la consola web.

  Debe permitir:

  - Bloquear las conexiones entrantes y/o salientes de las aplicaciones que desee
  - Prevención de intrusiones
  - Crear reglas de firewall para permitir/denegar el tráfico en sentido entrante/saliente de las máquinas que quiera para los protocolos/puertos que desee.

- Bloqueo de todos los dispositivos o dispositivos específicos (unidades de almacenamiento extraíbles, dispositivos de captura de imágenes, unidades de CD/DVD, módems USB, Bluetooth, etc.), impidiendo la entrada de malware y fugas de información. Permitiendo la definición de diferentes acciones para cada tipo de dispositivo (bloqueo, acceso, lectura/escritura).

- Bloqueo de acceso a páginas web no deseadas. Deberá ser posible configurar esta protección basada en categorías, aunque se podrán también añadir listas blancas y negras de sitios y dominios permitidos.

9.4.2.- Endpoint detection and response

Se requiere una solución de tipo EDR (endpoint detection and response) para proteger de las siguientes amenazas:

- Malware avanzado
- PUP (potential unwanted programs)
- Amenazas zeroday tipo ransomware
- Troyanos de nueva generación indetectables por los antivirus.

Esta solución tendrá que evitar al máximo las infecciones de forma proactiva, nunca reactiva. La solución debe aportar contramedidas diferentes a las siguientes:

- Firmas locales, que requieren de constantes actualizaciones
- Motores heurísticos, que necesitan de un uso de CPU y pueden producir falsos positivos.
- Sistemas de listas blancas, ya que no disponemos de personal suficiente para la administración de este tipo de sistemas.
- Sistemas de sandboxing que consume recursos y el malware puede eludirlos.

El sistema de protección tiene que ser capaz de clasificar el 100% de los procesos ejecutados en las maquinas, generando una clasificación de malware o goodware.

Es un requisito que se produzca el bloqueo de los procesos desconocidos que se intente ejecutar para evitar la posibilidad dañar los datos accesibles por la maquina (como puede ser el cifrado no deseado) o el robo o acceso de datos.

Debe incluir un sistema Anti-Exploit que permite la detección y bloqueo del uso de exploits conocidos o desconocidos.

Se debe poder establecer diferentes niveles de bloqueo (más o menos restrictivos) así como diferentes niveles en la capacidad de los usuarios de poder desbloquear individualmente los procesos bloqueados por el sistema.

La solución debe incluir la posibilidad de bloquear aplicaciones por nombre y por hash que el administrador desee.

9.4.3.- Servicio de alerta de amenazas (Threat Hunting)

Se requiere un servicio que alerte y tome las medidas correctivas adecuadas cuando sea detectado una actividad anómala en los equipos basada en el comportamiento normal auditado anteriormente en el parque de equipos.

Este servicio deberá estar ofrecido por el fabricante de la solución EDR por técnicos especializados usando los datos que haya recogido en la auditoria forense.

Deben poder realizar la alerta y la inclusión en la inteligencia del sistema EDR de las medidas correctivas

9.4.4.- Remote Monitoring & Management

Se requiere una solución de tipo RMM (remote monitoring and management) para conseguir los siguientes objetivos:

- Obtener información centralizada de hardware y software.
- Control de licencias utilizado
- Capacidad de hacer filtros por la información obtenida en el inventario
- Registro de cambios producidos en el equipo a nivel de hardware o software.
- Monitorización de procesos, servicios, memoria, CPU, registro, tamaño de archivos o carpetas
- Posibilidad de crear nuevos monitores personalizados
- Monitorización de dispositivos de red.
- Capacidad de realizar tareas de forma automática cuando se produzca un hecho determinado en un monitor.
- Gestión de parches de Microsoft, independientemente de donde se encuentre el equipo.
- Instalación, desinstalación y parcheo de software de terceros.
- Ejecución remota de scripts para automatizar tareas

- Control remoto a equipos conectados a Internet independientemente de donde se encuentren.
- Sistema de comunicación con el usuario mediante Chat.
- Control de smartphones y tabletas, con funcionalidad mínima de borrado del dispositivo, bloqueo y localización.

Todas estas funcionalidades estarán integradas como parte de un solo agente y permitirá tanto la gestión como el control remoto.

9.5.- ESQUEMA NACIONAL DE SEGURIDAD

La solución obligatoriamente tiene que estar incluida en el "Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación." (CPSTIC) Publicado por el CCN (Centro Criptográfico Nacional), dentro de la familia de protección del Puesto de Trabajo como CUALIFICADO.

Tecnología Cloud Pública, es obligatoria que tenga la certificación de conformidad frente al ENS, de categoría alta.

9.6.- INFORMACIÓN

El sistema debe generar información forense relacionada con cada equipo de tal forma que pueda ser explotada posteriormente. El sistema deberá incluir informe por amenaza detectada en la que se correlacione las acciones que ha hecho el proceso o en el contexto que ha estado envuelto, por ejemplo, si ha sido descargado de Internet o ha sido extraído de un fichero comprimido. Se valorará mucho un entorno amigable y fácil de seguir, sin exigir grandes conocimientos de amenazas avanzadas. Además, debe incluir informes de estado de las protecciones, de las detecciones de malware y algún informe ejecutivo con el resumen de la información global.

Los informes se deben de poder obtener de forma inmediata con los datos en tiempo real y también de forma periódica por correo electrónico y en diferentes formatos para su posterior tratamiento.

9.7.- SOPORTE TÉCNICO 24X7X365

Se establecerá el mantenimiento y asistencia técnica que permita asegurar el correcto funcionamiento en todos los puestos y servidores de la organización. Mediante:

- Servicio de soporte ofrecido por el fabricante por teléfono en castellano.
- Service Packs y hotfixes: Acceso a las mejoras técnicas del producto durante el tiempo de activación del servicio
- Web de soporte: Acceso a foros, blogs, información sobre últimas amenazas, enciclopedia de virus, …
- Soporte técnico vía email 24x7x365, por técnicos certificados en la solución implementada

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

- Acceso a análisis online de virus ocultos
- Acceso ilimitado al Helpdesk: sin límite de incidencias