PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA ADJUDICACIÓN DEL CONTRATO DE "IMPLEMENTACIÓN DE UNA PLATAFORMA DE PROTECCIÓN DEL ENDPOINT (EDR/XDR) Y SERVICIOS ASOCIADOS PARA EGARSAT MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 276"

1. Objetivos principales del contrato

El objeto del contrato es la implementación de una plataforma de protección del endpoint (servidores, ordenadores de sobremesa y ordenadores portátiles) frente a amenazas avanzadas de ciberseguridad, y formación al personal técnico de EGARSAT. Es necesario que sea una solución escalable de tipo EDR/XDR, y deberá incluir un soporte técnico durante toda la vigencia del contrato.

A efectos de que los licitadores puedan realizar su propuesta:

- Número de equipos (entre servidores, ordenadores de sobremesa y portátiles) a proteger: 700
- Número de usuarios activos en el Directorio Activo de Microsoft que EGARSAT tiene instalado: 950

Solo se aceptarán aquellas propuestas que incluyan en su oferta plataformas que figuren como líderes en los análisis correspondientes al año 2021 de plataformas de protección del endpoint de los principales analistas mundiales independientes del sector, como pueden ser "Gartner Magic Quadrant" y/o "Forrester Wave". Del mismo modo, solo se aceptarán aquellas propuestas que incluyan en su oferta una solución que esté incluida en el 'Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información (guía CCN STIC 105) del CCN-CERT, siendo tipificado como producto "Cualificado" y Categoría ENS "Media" como mínimo, en el momento de la presentación de la oferta.

Del mismo modo y dada la criticidad de la contratación en cuanto a seguridad de toda la infraestructura tecnológica de EGARSAT, los licitadores deberán, para poder ejecutar el contrato, tener la condición de partner del fabricante de la solución ofertada o, en su defecto, acreditar que cuentan con los acuerdos con el fabricante que les capacite para efectuar los servicios objeto de este contrato. Este requisito se acreditará mediante la presentación de un certificado emitido por el fabricante de la solución en el que se acredite este requisito.

Los licitadores deberán presentar dentro del SOBRE B una **memoria técnica** que detalle la solución propuesta. Esta memoria técnica deberá incorporar, como mínimo, los siguientes aspectos:

- En cuanto a la solución propuesta: el licitador deberá describir las características de los distintos componentes de la solución propuesta destacando el cumplimiento de todos los aspectos indicados en el punto 2 del presente pliego de prescripciones técnicas.

- En cuanto a los Servicios relacionados con la implantación y puesta en marcha de la solución el licitador deberá incluir una descripción detallada sobre su propuesta de ejecución de las tareas relacionadas en el punto 3 del presente pliego de prescripciones técnicas.

- En cuanto a los Servicios de soporte en tiempo de operación el licitador deberá incluir una descripción detallada sobre las características del soporte ofertado y el

cumplimiento de los requisitos mínimos relacionadas en el punto 5 del presente pliego de prescripciones técnicas.

- Otra información que las empresas licitadoras estimen necesario incluir para facilitar la comprensión de la oferta presentada

No deberá incluirse en esta memoria ninguna información objeto de valoración en la oferta técnica valorable automáticamente (SOBRE C). Cualquier referencia podrá ser motivo de exclusión de la oferta presentada

Todas las tareas necesarias hasta el despliegue ofertado y puesta en marcha de la solución (en su totalidad) no deberán demorarse más de 90 días naturales desde la fecha de inicio del contrato.

EGARSAT podrá rechazar la oferta cuando, de la información aportada según lo exigido en el este apartado, se desprenda que la solución ofertada no cumple con los requisitos mínimos solicitados, o a juicio del personal técnico de Egarsat, no sea apta para el objeto de licitación.

Serán excluidas de la licitación aquellas empresas que no presenten toda la documentación exigida en este apartado y con el nivel de detalle requerido, dada la necesidad de comprobación de la adecuación de la solución ofertada a las exigencias técnicas incluidas en el presente pliego técnico.

2. Características técnicas de la solución

La solución EDR/XDR deberá estar alojada en la nube en su totalidad (cloud). Dicha nube (tennant) y cualquier dato que contenga deberán estar ubicados en Europa y, por extensión, bajo el cumplimiento del RGPD de la Unión Europea. Adicionalmente, en el supuesto de tener que subir ficheros a la nube para cualquier tipo de análisis por parte de la solución, dichos ficheros deberán ir con el nombre anonimizado o enmascarado, y el tráfico debidamente cifrado. La solución deberá estar basada en tecnología de un único fabricante que permita gestionarse desde una única consola, conviviendo con los actuales sistemas de protección instalados en las infraestructuras de puesto de trabajo y servidor, y sin necesidad de la desinstalación o cambios de configuración de dichos sistemas de protección. El licenciamiento de la solución deberá ser, obligatoriamente, en modo suscripción.

La solución deberá constar de los siguientes componentes:

- Clientes instalables en los servidores, ordenadores de sobremesa y ordenadores portátiles:
  - Deberán proporcionarse todos los elementos software y de licencias necesarios.
  - Por cuestiones de eficiencia y rendimiento, el agente a instalar deberá ser considerado como un agente ligero.
  - El agente deberá poder actualizarse sin necesidad de reiniciar el endpoint después de la actualización.
  - El agente de endpoint deberá operar tanto en el espacio del usuario como en el del núcleo (kernel); el modo de núcleo (kernel) resulta necesario para obtener una visibilidad completa y para eliminar los puntos ciegos.

- Servidores y consolas centrales:
  - Los elementos “core” de la solución deberán suministrarse en la nube (cloud).

Dicha nube (tennant) y cualquier dato que contenga deberán estar ubicados en Europa y, por extensión, bajo el cumplimiento del RGPD de la Unión Europea. Adicionalmente, en el supuesto de tener que subir ficheros a la nube para cualquier tipo de análisis por parte de la solución, dichos ficheros deberán ir con el nombre anonimizado o enmascarado, y el tráfico debidamente cifrado.
    - Deberán proporcionarse todos los elementos software y licencias que resulten necesarios para que la solución sea totalmente funcional y operativa.
    - Deberán incluirse las fuentes de actualización, de vulnerabilidades, reglas de comportamiento, consultas almacenadas (sql), etc., necesarias para que el sistema esté permanentemente actualizado y permita detectar la mayor parte posible de comportamientos anómalos.

La solución deberá cumplir con los siguientes requisitos, como mínimo:

- Personalización y capacidad multi-tenant: la solución deberá poder soportar configuraciones diferenciadas para cada delegación de EGARSAT en la que se instale, adaptándose de esta forma a diferentes casuísticas y comportamientos y generando las reglas particulares correspondientes.

- Integración con Sistemas de gestión de eventos e información de seguridad (NGSIEMs) y con los sistemas de monitorización ya existentes en EGARSAT, y deberá ser capaz de integrarse con fuentes de datos externas, mediante el uso de APIs de fuentes abiertas que permitan la interoperabilidad de la solución.

- Visibilidad y acceso a los equipos portátiles de EGARSAT cuando estos se encuentren en situación de movilidad conectados a internet, sin necesidad de gestionar túneles.

2.1. Integración con puesto de trabajo y servidores existentes

La solución deberá cumplir con los siguientes requisitos, como mínimo:

- El software de agente deberá poder instalarse en equipos de escritorio, portátiles y servidores. Adicionalmente, deberá tener capacidades para instalarse también en dispositivos móviles como smartphones y tablets, mediante tecnología propia o a través de una integración con una solución de terceros (no objeto de esta licitación).

- Capacidad para funcionar de forma coordinada y compatible con otras soluciones de protección de endpoints existentes, especialmente con las principales soluciones antivirus del mercado.

- Capacidad para securizar servicios basados en OneDrive y Sharepoint en modalidad cloud, de modo que ofrezca soporte seguro al trabajo colaborativo con Microsoft 365.

2.2. Capacidades técnicas

La solución propuesta deberá disponer de, como mínimo, las siguientes capacidades o características técnicas clave, que a continuación se relacionan con las distintas fases del ciclo de vida de un incidente de seguridad:

- En fase de detección:

- Deberá utilizar técnicas de IA (inteligencia artificial), Machine Learning, analítica con BigData y 'expertise' de analistas, para reducir la tasa de falsos positivos. El análisis no deberá estar basado únicamente en la detección tradicional basada en firmas de ficheros o vulnerabilidades conocidas, sino en una combinación de técnicas que incluyan, entre otros: técnicas heurísticas avanzadas; análisis de comportamiento; detección de técnicas, tácticas y procedimientos de explotación, siguiendo marcos de referencia como la matriz ATT&CK de MITRE o similares.

- Deberá disponer de un sistema de detección de amenazas basada, al menos, en: indicadores de compromiso (IOCs), y/o indicadores de comportamiento basados en tácticas, técnicas y procedimientos de adversarios que incluyen etiquetado de MITRE (BIOCs), comportamientos inesperados o maliciosos, violaciones de políticas de seguridad, o anomalías en la configuración de los endpoints, usuarios o aplicaciones. Este tipo de reglas de detección deberá soportar reglas relacionadas con procesos (al menos hasta 3 niveles de procesos y líneas de comando asociadas), ficheros y comunicaciones. En todos los casos deberá ofrecerse la posibilidad de ofrecer detección y bloqueo.

- Deberá combinar capacidades de detección tanto basadas en el uso de agentes, como en modos que no requieran de la instalación de agentes, como machine learning local en off-line.

  Por cuestiones de eficiencia y rendimiento, el agente a instalar deberá ser considerado como un agente ligero, y para ello deberá cumplir las siguientes características de referencia:
  - Consumo CPU : inferior a 5% CPU.
  - Consumo RAM : inferior a 100MB de memoria.
  - Consumo I/O : inferior a 100MB de espacio en disco.
  - El instalador del agente no debe ser superior a 100MB.

  El agente de endpoint operará tanto en el espacio del usuario como en el del núcleo (kernel); se considera que el modo de núcleo (kernel) resulta necesario para obtener una visibilidad completa y para eliminar los puntos ciegos.

  Se valorará en oferta técnica la existencia de un único agente para todas las funcionalidades solicitadas (a excepción de los controladores de dominio, tal y como se especifica más adelante).

  Se valorará en oferta técnica que tanto la instalación del agente como su actualización no requiera reiniciar el equipo donde se está instalando/actualizando el agente.

- Deberá disponer de un sistema de inventariado automático y escaneado de red para la detección de nuevos endpoints y aplicaciones conectadas a la red. Adicionalmente, deberá monitorizar en continuo la configuración y políticas de seguridad aplicables a los endpoints: detección de cambios no autorizados en la configuración, violaciones de políticas, modificaciones en ficheros, etc. Control de aplicaciones con listas blancas y negras basadas en categorías de aplicaciones predefinidas.

- En fase de contención:
  - La solución deberá poder transmitir la telemetría EDR/XDR en tiempo real, para la

consulta en vivo, y los resultados deberán ser completos incluso cuando los endpoints estén fuera de línea. Preferentemente, se almacenará telemetría de toda la actividad relacionada con el endpoint, frente a sólo almacenar telemetría en el momento de producirse una alerta de seguridad.

- La solución deberá correlacionar y presentar automáticamente la telemetría y los metadatos (IOC,etc) relacionados con el ataque en una línea de tiempo. Entre otra información: argumentos de línea de comandos, escrituras de archivos, solicitudes DNS, conexiones IP, etc. Se deberá poder tener margen de actuación a modo de acciones de remediación en todos y cada uno de los nodos de esta línea de tiempo o grafo del incidente.

- Deberá ofrecer sandboxing en la nube, siempre en entornos perfectamente aislados.

- Deberá tener capacidades para la contención de ataques 'full scope', con capacidad de contemplar todos los elementos relacionados con el ataque, incluyendo las causas del mismo, máquinas afectadas y usuarios, comunicaciones entrantes y salientes durante el ataque, línea de tiempo del ataque, movimientos laterales, etc. La solución deberá permitir una visibilidad completa del incidente (no sólo de las detecciones), y aportar un scoring a tiempo real sobre la situación del ataque, progreso, detecciones contextuales y grafo a tiempo real. Adicionalmente deberá indicar la existencia de capacidades de pivotaje sobre los atributos del incidente y herramientas de contención automática sobre la totalidad del incidente.

  Se valorará en oferta técnica que el producto disponga de un sistema de protección de fuga de datos, que permita bloquear la transferencia, pedir confirmación al usuario o simplemente monitorizar la transferencia de ficheros. Este sistema de protección deberá permitir establecer políticas de DLP (Data Loss Prevention).

- La solución propuesta deberá disponer de 3 tipos de barreras de protección, como mínimo: pre-ejecución, post-ejecución y post-explotación:

  - Pre-ejecución:
    - Uso de firmas clásicas para detectar malware.
    - Inteligencia artificial (IA), mediante Machine Learning localmente en cada máquina para detectar malware desconocido, incluso estando offline.
    - No se aceptarán sistemas que bloqueen el uso de ficheros a modo de cuarentena en caso de dudas hasta que el equipo disponga de conexión a internet. La respuesta debe ser inmediata tanto en modo on-line como off-line.
    - La solución deberá ofrecer protección de la memoria (ASLR, protección contra la sobreescritura de la gestión de excepciones estructuradas, protección de páginas nulas, preasignación de la pila, etc.).

  - Post –ejecución:
    - Deberá disponer de funcionalidades de prevención de exploits, incluyendo detección tanto remota como local de ataques ransomware.
    - En caso de cifrar algún fichero durante el ataque, deberá permitir la realización de un rollback y devolver todo a su estado original de forma

automática.
- Deberá disponer de funcionalidades que permitan detectar la inyección de código en memoria, evitando que el supuesto atacante consiga una shell remota o reverse meterpreter.
- Deberá disponer de funcionalidades de análisis de vulnerabilidades "0 day" mediante patrones IPS.

- Post-explotación:
  - Deberá ofrecer métodos de protección contra robo de credenciales.
  - Deberá ofrecer métodos de protección contra elevación de privilegios.

- En fase de investigación:
  - Deberá incluir un sistema de investigación de incidentes que permita hacer threat hunting con las siguientes capacidades, como mínimo:
    - Aislar y desaislar máquinas bajo demanda mientras se investiga el incidente.
    - Crear exclusiones, para puertos e IPs, a las medidas de auto- exclusión de las máquinas.
    - Realizar un snapshot forense a una base de datos SQL o JSON (API Rest).
    - Enviar ficheros a los laboratorios del fabricante para que mediante ingeniería inversa e inteligencia artificial pueda averiguar "qué hace" dicho fichero, "a qué" se parece y si es o no malicioso.
    - Detectar ataques de fuerza bruta a un servidor.
    - Acceder a una máquina mediante una shell remota para poder realizar intervenciones sobre ella directamente desde la consola, incluso cuando esta esté en estado de auto-aislamiento.
    - Realizar consultas remotas (live queries) para poder obtener información de una máquina y/o ataque concreto.
    - Categorizar los incidentes para saber si ya han sido investigados, y los resultados de dicha investigación.
    - Obtener un gráfico completo y detallado o sencillo y directo del ataque, donde se vean todos los elementos del ataque.
    - Disponer de indicadores de amenazas que indiquen ficheros sospechosos que no hayan sido detectados por el endpoint pero que deben investigarse. Dichos indicadores deberán permitir:
      - Ver detalles del fichero detectado
      - Enviar el fichero a los laboratorios del fabricante para su análisis mediante inteligencia artificial e ingeniería inversa
      - Obtener el hash del fichero y buscarlo por la red corporativa para detectar su posible existencia en otros endopoints
      - Generar un caso de amenazas a partir de ese fichero para analizar su comportamiento
      - Indicar el número de dispositivos afectados, y si se ha ejecutado
      - Bloquear y limpiar el fichero

  - Deberá permitir correlacionar, siempre que sea posible, el vector de infección y la intención del atacante de la amenaza en relación con la cadena de ataque, correlacionando elementos como la telemetría, el árbol de procesos y la inteligencia de la amenaza.

  - Deberá incluir una serie de consultas predefinidas basadas en diferentes ámbitos (Threat Hunting, ATT&CK, Anomalías, Compliance, etc), y deberá permitir la edición y creación de nuevas consultas utilizando sintaxis similar a SQL.

Adicionalmente deberá disponer, como mínimo, de las siguientes capacidades:

- Posibilidad de realizar consultas directas a equipos con sistemas operativos Windows, MacOs y Linux (también deberá poder realizar dichas consultas a Android e IOs, aun no siendo objeto de esta licitación la protección de este tipo de dispositivos).
- Catálogo de consultas predefinidas categorizadas.
- Interfaz de investigación ad hoc.
- Posibilidad de crear/guardar y compartir consultas personalizadas con variables en las consultas.

- Deberá soportar la ingestión de IOC (hashes, IPs, dominios y URLs) vía API, que se mantendrán en la plataforma por un periodo determinado de tiempo y que serán utilizados durante todo el ciclo de prevención/detección del incidente de seguridad. Deberá permitir la ingestión de 100.000 IoC, como mínimo. Adicionalmente deberá permitir insertar comentarios con información adicional relativa al IoC cargado en la plataforma y su periodo de expiración. Deberá permitir la realización de bloqueo de los IOC de tipo hashes y detección de los IOC de tipo dominio y hash.

- Deberán poderse registrar los eventos relativos a todas las comunicaciones de red, todos los procesos y todos los endpoints del sistema durante al menos 3 meses, para la realización de threat hunting retroactivo. Deberá poderse indicar el tiempo de almacenamiento de la telemetría completa y la relativa a un incidente. Toda esta telemetría deberá poder ser exportable a través de API (FDR) para que se pueda externalizar su almacenamiento de forma indefinida.

Se valorará en oferta técnica que la solución propuesta disponga de un módulo de ciberinteligencia, con las siguientes funcionalidades, como mínimo:

- Disponer de un programa de inteligencia sobre ciberamenazas que ofrezca inteligencia a nivel técnico, de inteligencia táctica operacional y estratégica.
- Permitir correlacionar las detecciones con los principales actores de la amenaza (estado-nación y crimen electrónico) cuando sea aplicable.
- Human Intelligence (HUMINT): deberá disponer de inteligencia derivada de análisis de consultores, tales como reverse malware, operaciones de actores en la Dark web y Deep web.
- OSINT: información obtenida de la web, como redes sociales, Dark/Deep Web, foros, chatrooms, etc
- Deberá incluir datos de digital risk monitoring de tipo: marcas, dominios de compañías, perfiles de ejecutivos, marcas de cadenas de suministro, CVE, bin codes, emails, nombre de compañías, direcciones IP.
- Deberá disponer de inteligencia proveniente del mercado del cibercrimen: actores principales activos, hacktivistas, perfiles Estado/Nación, perfiles de organizaciones de eCrime
- Deberá ofrecer informes periódicos de inteligencia clasificables por Estado/Nación y sus objetivos

- En fase de reparación/respuesta:
  - Deberá permitir accciones mediante herramientas de respuesta automatizadas: aislamiento de la red, inmunización automática de endpoints, reversión del punto final al estado pre-infectado, eliminación de ficheros, puesta en cuarentena de equipos, etc. Deberá permitirse la interacción directa con el endpoint y ofrecer

todas las herramientas forenses necesarias para dar respuesta al incidente.

- Deberá disponer de funciones de reversión de ransomware mediante un proceso de restauración que revierta el daño causado por los ataques de ransomware. Deberá permitir bloquear la actividad ramsomware o similar lo antes posible. Deberá permitir detectar tempranamente esta actividad y bloquear su progreso de forma prácticamente inmediata, y a ser posible en fase de Pre-ejecución.

- Deberá disponer de capacidades de bloqueo de ataques basados en flujos de red antes de que puedan llegarse a ejecutar, tales como los movimientos laterales, los ataques de fuerza bruta o los intentos de robo de contraseñas.

- Deberá permitir el soporte a la seguridad gestionada mediante la creación de una conexión segura con los hosts infectados, con el objetivo de extraer o enviar archivos, eliminar procesos y realizar volcados de memoria.

La solución propuesta deberá disponer de una consola centralizada con las siguientes capacidades o características técnicas clave, como mínimo:

- Monitorizar el estado del conjunto de los equipos. La interfaz de usuario deberá estar protegida con autenticación multifactorial y soportar SSO (SAML 2.0). La consola deberá de poder gestionar diferentes sub-entornos, pudiendo dividir la organización, en diferentes sub-organizaciones (multi-tenant). Existirán súper administradores que tengan acceso a todas las sub-consolas y todos los sub-entornos creados. Cada administrador de una sub-consola, solo tendrá acceso a dicha sub-consola, sin tener por qué tener conocimiento de que existen otras sub-consolas.

- Integración con Directorio Activo: la solución debe permitir la integración de servicios de Directorio y en particular con el Directorio Activo de Microsoft. Esta integración deberá realizarse mediante la instalación de un agente que sincronice con la consola de una manera segura mediante LDAP (Protocolo Ligero de Acceso a Directorios) sobre SSL (Capa de Sockets Seguros). Deberán poder definirse roles personalizados.

Adicionalmente, la solución propuesta deberá incluir un módulo específico para el descubrimiento, análisis y gestión de vulnerabilidades comunes (CVE) en el sistema operativo y aplicaciones instaladas en los endpoints donde se encuentre instalado el agente de la solución. Esta información deberá aparecer en la consola descrita en el apartado anterior de forma detallada y categorizada tanto por su severidad (CVSS) como por su nivel de riesgo real en base a algoritmos de IA, para la óptima gestión de dichas vulnerabilidades. Deberá ofrecer información detallada de las vulnerabilidades y los métodos de remediación aconsejados.

Por último, la solución propuesta deberá incluir un módulo para la protección específica de las identidades alojadas en el Directorio Activo de Microsoft que EGARSAT tiene actualmente instalado. Dicho módulo, que puede requerir de un agente adicional a instalar en los controladores de dominio, deberá mostrar en la consola descrita anteriormente y de forma detallada y categorizada, todas aquellas identidades y/o configuraciones con los perfiles de riesgo asignados, sistemas en los que ha iniciado sesión, ubicaciones del inicio de sesión, privilegios asociados y toda aquella información necesaria para disponer, de forma intuitiva para los Administradores de Sistemas de EGARSAT, del mapa de riesgo global del Directorio Activo en tiempo real. Deberá disponer de funcionalidades para detectar y responder en tiempo real a las amenazas detectadas, y deberá permitir la configuración de

políticas de notificación, bloqueo o acceso condicional en función de la identidad, el riesgo y el comportamiento detectados. Deberá disponer de las siguientes capacidades, como mínimo:

- Detección y prevención de ataques basados en vulnerabilidades de protocolos de autenticación: mediante y el análisis del tráfico de autenticación, deberá ser posible detectar, prevenir y detener ataques apoyados en vulnerabilidades de protocolos de autenticación (Kerberos, LDAP, etc.) y proteger a la organización ante ataques del tipo Passthehash, Kerberos hasting, Golden Ticket, etc.

- Descubrimiento y auditoría de cuentas de Directorio Activo: deberá permitir realizar un descubrimiento de la configuración de Directorio Activo a nivel de cuentas (cuentas de usuario, de sistema, privilegiadas, etc.) y dispositivos facilitando información de las medidas y cambios de configuración recomendados. Esta funcionalidad de descubrimiento deberá permitir a los Administradores de Sistemas de EGARSAT la aplicación de buenas prácticas desde el punto de vista de seguridad y la aplicación de políticas de mejora continua en administración de la seguridad del Directorio Activo.

- Aplicación de políticas de acceso basadas en comportamiento y protección de activos críticos: deberá permitir la aplicación de políticas de acceso basadas en comportamiento, de forma que pueden aplicarse políticas (de detección, bloqueo o acceso condicional) en el acceso de usuarios a activos considerados críticos. Deberán poder habilitarse políticas de acceso basadas en el host desde el que se intenta realizar el acceso o el protocolo con el que se pretende acceder a un activo, de forma que, en caso de que un Administrador de Sistemas intente acceder a un recurso crítico desde un endpoint distinto desde el que normalmente accede, deberá poder bloquearse este acceso o aplicar mecanismos de autenticación de doble factor para garantizar que el acceso es lícito. A partir de la línea base de accesos de un usuario a los distintos activos de la organización, deberán poder establecerse políticas de acceso específicas en base a la desviación respecto a esta línea base.

- Segmentación de acceso a servicios basada en identidad: mediante la aplicación de políticas de acceso condicional, deberá permitir realizar una segmentación de acceso a servicios corporativos basada en identidad y desde el punto de vista de la seguridad. Esta capacidad deberá permitir proteger o limitar los accesos a recursos corporativos.

- Capacidades antiramsonware: mediante la aplicación de políticas de acceso condicional, deberá permitir detectar proactivamente y bloquear los incidentes de ramsonware en las fases más tempranas, detectando (o bloqueará en función de la severidad de las políticas de acceso condicional) intentos de conexión a repositorios de almacenamiento compartido que salgan de los patrones normales de conexión de la cuenta de usuario o servicio, de forma que, en las fases iniciales de un ataque de ramsonware en las que el malware intenta realizar un descubrimiento de las unidades de red a las que poder acceder de cara a realizar la posterior encriptación de los ficheros contenidos en éstas, se puedan bloquear estas conexiones o habilitar la integración con mecanismos de autenticación de doble factor para verificar la maliciosidad del intento de conexión. Deberán poder aplicarse mecanismos de contención que permitan proteger los activos corporativos más importantes.

2.3. Capacidades de servicio

La solución propuesta deberá disponer de las siguientes capacidades o características de servicio clave, como mínimo:

- Deberá permitir la escalabilidad hacia cientos o miles de endpoints, ya sea con almacenamiento centralizado o descentralizado. Asimismo, deberá disponer de alta disponibilidad y tolerancia a fallos.

- Deberá disponer de interoperabilidad con otros entornos haciendo uso de APIs abiertas, basadas en estándares abiertos, para interactuar con las funciones de seguridad de los endpoints, incluyendo la recopilación de información, la adopción de medidas sobre las amenazas descubiertas y el suministro de información sobre las amenazas.

- Deberá disponer de capacidades de XDR (Cross Detection and Response), esto es, capacidades para integrar inteligencia tanto de red como del puesto de trabajo, almacenar y correlar los logs de ambos entornos y, de manera automatizada, generar inteligencia desde los mismos para identificar las amenazas más relevantes, simplificando su gestión y disminuyendo el tiempo de respuesta a los incidentes.

La memoria técnica presentada deberá describir las características de los distintos componentes de la solución propuesta destacando el cumplimiento de todos los requisitos solicitados.

3. Servicios relacionados con la implantación y puesta en marcha de la solución

Todas las tareas desde el inicio de las mismas y hasta la puesta en marcha de la solución deberán ser realizadas sin que suponga ningún corte ni interrupción en ninguno de los servicios que se ofrecen actualmente a los usuarios de EGARSAT, y se realizarán en horario laborable de lunes a viernes, preferiblemente en horario de mañana. Estas tareas podrán realizarse de forma remota (para ese caso EGARSAT dotará a la empresa adjudicataria de una conexión VPN para la realización de las tareas). Para dichas tareas, el contratista deberá tener en cuenta en todo momento las indicaciones de EGARSAT, de tal forma que se prepare todo el entorno de forma consensuada.

Las tareas incluidas en este apartado serán las siguientes:

- Recogida de datos

- Configuración y parametrización del entorno para su puesta en marcha, adecuándose a las necesidades y especificaciones de EGARSAT y siguiendo la documentación de mejores prácticas aportada por el fabricante de la solución. El contratista deberá realizar una propuesta, en base a su experiencia en implantaciones anteriores, de las configuraciones y parametrizaciones óptimas para EGARSAT.

- Colaboración para la integración de la plataforma con sistemas ya existentes en EGARSAT (plataformas de monitorización y/o NGSIEMs).

- Puesta en marcha de la solución:
    - Despliegue de los agentes de forma faseada en los equipos cliente que EGARSAT determine y en los bloques de equipos que EGARSAT decida. Será responsabilidad del adjudicatario desplegar la solución en la totalidad de servidores de EGARSAT

(100 aproximadamente) y en parte del parque de ordenadores de sobremesa y portátiles (mínimo 100 equipos entre ordenadores de sobremesa y portatiles).

- Tareas de tunning para la optimización de las parametrizaciones de la plataforma para su correcta adaptación a la red, sistemas y aplicaciones ya existentes en EGARSAT.

Se valorará en oferta técnica el despliegue de los agentes de forma faseada y en los bloques de equipos que EGARSAT decida, así como las tareas de tunning para la optimización de las parametrizaciones de la plataforma en un número superior de ordenadores de sobremesa y portátiles.

- Entrega de documentación sobre las tareas realizadas: el contratista deberá entregar la documentación técnica necesaria para reflejar con detalle la arquitectura de la solución y las configuraciones, parametrizaciones y políticas desplegadas. La entrega de dicha documentación no deberá demorarse más de 15 días naturales después de la finalización de la puesta en marcha.

- Formación técnica y de gestión a los Administradores de Sistemas de EGARSAT sobre la solución implantada de 8 horas de duración, como mínimo. Esta formación deberá realizarse en horario laboral y mediante videoconferencia, y deberá realizarse de forma inmediatamente posterior a la entrega de documentación solicitada en el punto anterior. Aspectos mínimos a incluir en la formación:
  - Familiarización con los distintos componentes y módulos de la solución implantada.
  - Realización de cambios en la configuración y gestión de la misma.
  - Dimensionamiento y aprovechamiento al máximo la plataforma.
  - Buenas prácticas para su control y seguimiento.
  - Aspectos no incluidos en esta relación y que la empresa adjudicataria considere adecuada su inclusión en la formación

Todas las tareas relacionadas en este apartado deberán ser realizadas por perfiles que dispongan de conocimientos, habilidades y destrezas específicos del ámbito de la seguridad. Deberán estar certificados al máximo nivel técnico y contar con al menos 1 año de experiencia en implantación de la solución ofertada, y disponer de, como mínimo, 3 años de experiencia en implantación de soluciones EDR/XDR.
El esfuerzo requerido para la ejecución de estas tareas se dimensiona en 160 horas aproximadamente. Se valorará en oferta técnica la inclusión de horas adicionales destinadas a este propósito.

La memoria técnica presentada deberá incluir el detalle de todos los servicios relacionados con la implantación y puesta en marcha de la solución.

4. Gestión del proyecto de implantación y puesta en marcha de la solución

Para garantizar la correcta puesta en marcha de la solución, la empresa adjudicataria designará un Jefe de Proyecto que actuará como interlocutor único con EGARSAT y que realizará las siguientes tareas:

- Organizar, dirigir, representar y coordinar al equipo de trabajo que preste los servicios descritos en el apartado anterior (apartado 3 del Pliego de Prescripciones Técnicas).

- Asegurar el nivel de calidad de las tareas realizadas.
- Proporcionar a EGARSAT la información periódica necesaria para el seguimiento de la implantación.

El Jefe de Proyecto deberá disponer de conocimientos, habilidades y destrezas específicos del ámbito de la seguridad. Deberá contar con al menos 1 año de experiencia en gestión de proyectos de implantación de la solución ofertada y disponer de, como mínimo, 3 años de experiencia en gestión de proyectos de implantación de soluciones EDR/XDR.

5. Servicios de soporte en tiempo de operación

Para garantizar la correcta ejecución del contrato, deberán estar incluidos en la propuesta unos servicios de soporte técnico oficial del fabricante de la solución ofertada durante toda la vigencia del contrato. Estos servicios de soporte técnico deberán incluir, como mínimo:

- Horario 8x5 (de lunes a viernes de 9h a 17h)
- Forma de contacto con el soporte técnico (portal web, correo electrónico, chat en vivo y/o teléfono).
- Forma de contacto telefónica en horario 24x7 para casos críticos
- Asistencia ante averías y/o incidencias de funcionamiento de los servicios, sea cual fuere su naturaleza, hasta su resolución
- Asistencia ante consultas relacionadas con el funcionamiento de la plataforma, definición y aplicación de políticas, configuraciones y parametrizaciones.
- Acceso a Base de Datos de conocimiento
- Informes trimestrales de la plataforma y de los servicios de soporte
-

SLA's de tiempos máximos de respuesta a incidencias:

Prioridad	Tiempos de respuesta
Crítica (notificación telefónica)	Inmediato
Alta	1h laborable
Normal	4h laborables

Adicionalmente, la empresa adjudicataria deberá ofrecer de forma anual 2 jornadas trabajo de 4 horas (en horario laboral), destinadas a la revisión y mejora de la plataforma de forma conjunta y consensuada con los Administradores de Sistemas de EGARSAT. A la finalización de cada jornada de trabajo y durante los siguientes 7 días naturales (a más tardar) entregará un informe técnico que refleje las tareas realizadas. Se valorará en oferta técnica la inclusión de horas adicionales destinadas a la revisión y mejora de la plataforma.

Para complementar las 8 horas anuales destinadas a la revisión y mejora de la plataforma, la empresa adjudicataria deberá ofrecer 24 horas adicionales anuales (en horario laboral) destinadas a servicios de consultoría, que se consumirán a demanda de EGARSAT para dar cobertura a sus Administradores de Sistemas ante:

- soporte en configuraciones y parametrizaciones de la plataforma
- soporte en seguimiento y gestión de incidentes de seguridad

- dudas y preguntas sobre la gestión de la plataforma

Tanto las jornadas de trabajo como los servicios de consultoría deberán ser realizados por perfiles que dispongan de conocimientos, habilidades y destrezas específicos del ámbito de la seguridad. Deberán estar certificados al máximo nivel técnico y contar con al menos 1 año de experiencia en implantación de la solución ofertada, y disponer de, como mínimo, 3 años de experiencia en implantación de soluciones EDR/XDR

La memoria técnica presentada deberá incluir el detalle de todas las características de los servicios de soporte en tiempo de operación, incluyendo ejemplos de los informes trimestrales mínimos solicitados.

6. Precio

Desglose de precios:

Precios anuales:

Descripción	Cantidad	P.U. anual máximo	Importe máximo anual
a) Licencia endpoint	700	47,75 €	33.425,00 €
b) Licencia por usuario de Directorio Activo	950	17,75 €	16.862,50 €
c) Servicios de soporte oficial de la plataforma	1	6.000,00 €	6.000,00 €
d) Servicios de consultoría, revisión y mejora de la plataforma (en horas)	32	75,00 €	2.400,00 €
TOTAL			58.687,50 €

Precio de los servicios relacionados con la implantación y puesta en marcha de la solución (a ejecutarse una sola vez al inicio del contrato):

Descripción	Cantidad horas	P.U. máximo	Importe máximo
e) Servicios relacionados con la implantación y puesta en marcha de la solución	160	75,00 €	12.000,00 €
TOTAL			12.000,00 €

Duración inicial del contrato: 3 años.

Forma de pago:

A la finalización de los Servicios relacionados con la implantación y puesta en marcha de la solución se abonará la totalidad de los importes correspondientes a los ítems a, b, c, d y e.

Al inicio del 2º año de contrato (y de forma anual durante la vigencia inicial del contrato) se abonará el importe correspondiente a los ítems a, b, c y d

Prórrogas previstas: 2 prórrogas de 1 año de duración cada una de ellas.

Al inicio de cada una de las prórrogas se abonará (de forma anual) se abonará el importe

correspondiente a los ítems a, b, c y d.

Firmado digitalmente por Jordi Trabal (Jefe del Departamento de Producción y Operaciones TI de EGARSAT)

Jordi Trabal Esquerda

Firmado digitalmente por Jordi Trabal Esquerda
Fecha: 2023.02.07 09:40:42 +01'00'