MINISTERIO
DEL INTERIOR

GUARDIA CIVIL
DIRECCIÓN GENERAL

Mando de Apoyo
Jefatura de Servicios Técnicos
Servicio de Telecomunicaciones

PLIEGO DE PRESCRIPCIONES TÉCNICAS

SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS CON PROTECCIÓN, DETECCIÓN Y RESPUESTA DE ÚLTIMA GENERACIÓN, NO BASADA EN FIRMAS, Y QUE PERMITA RESPONDER A TÉCNICAS DE ATAQUES Y AMENAZAS SOFISTICADAS DE FORMA EFICIENTE, DANDO VISIBILIDAD COMPLETA CONTRA ANOMALÍAS EN LOS PATRONES DE COMPORTAMIENTO DE APLICACIONES Y RED

1. INTRODUCCION

El panorama de la ciberseguridad ha experimentado cambios dramáticos en los últimos años con la aparición y la evolución de nuevos, crecientes y siempre presentes adversarios informáticos. A medida que la delincuencia informática avanzada y los ataques dirigidos continúan evolucionando y se vuelven cada vez más sofisticados, a las organizaciones cada vez les resulta más difícil mantenerse protegido debido a las limitaciones de recursos humanos y económicos de sus correspondientes departamentos de seguridad.

El entorno de amenazas actual ha demostrado que los adversarios están constantemente perfilando y penetrando su infraestructura corporativa para acceder y recopilar propiedad intelectual, datos de propiedad y secretos comerciales, por lo que es imperativo poder detectar la actividad adversaria en el menor tiempo posible, conocer quién está atacando a la organización, descubrir qué están haciendo en la red y, más específicamente, comprender cómo lo hacen.

El objeto es la contratación de un servicio de Acceso a Bases de Datos (BB.DD.) de ciberamenazas avanzadas, con protección, detección y respuesta de última generación, no basada en firmas, y que permita responder a técnicas de ataques y amenazas sofisticadas de forma eficiente, dando visibilidad completa contra anomalías en los patrones de comportamiento de aplicaciones y red.

La solución estará basada en tecnología de un único fabricante de seguridad, que permita gestionarse desde una única consola, conviviendo con los actuales sistemas de protección instalados en las infraestructuras de endpoint y servidor y sin necesidad de la desinstalación o cambios de configuración de dichos sistemas de protección.

El servicio de acceso a base de datos suministrado realizará la recogida de información de telemetría y metadatos relevantes desde el punto de vista de la ciberseguridad, la cual será transmitida a la plataforma central de la solución. Esta telemetría se utilizará para hacer actividades de búsqueda avanzada de amenazas (Threat Hunting). En concreto permitirá la búsqueda de forma activa de indicadores de ataque y compromiso relativos a organizaciones criminales, con especial foco en aquellas que están operando en España en los últimos meses y, particularmente, las que han afectado a las Administraciones Públicas.

Para ello, se deberá proporcionar visibilidad completa en tiempo real de la situación actual. La detección que proporcione la solución debe combinar técnicas de aprendizaje automático e inteligencia artificial para realizar una observación real del comportamiento de cada ejecutable en su entorno.

2. ALCANCE DEL SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

El alcance del presente pliego es el de definir los requisitos técnicos que debe cumplir la solución de servicio de acceso a base de datos suministrada para un parque de al menos 35.000 endpoints, con sus puertos USB, y al menos 20.000 dispositivos móviles.

3. REQUISITOS GENERALES DE ARQUITECTURA DEL SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

Todos los requisitos técnicos definidos en el presente pliego son de carácter crítico y de obligado cumplimiento. El incumplimiento de los mismos descalificará técnicamente la propuesta.

Con el fin de evaluar las ofertas, éstas deberán incluir en el sobre 2, una Memoria Técnica-matriz de cumplimiento en la que quede claramente explicado como se propone realizar el cumplimiento de cada uno de los requisitos técnicos, con un nivel de detalle que permita valorar el cumplimiento de todos los requisitos. Si de la documentación aportada se concluye que el Licitador no cumple con las especificaciones del PPT, este será excluido del proceso.

RT-1. Todos los requisitos de la solución del SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS demandado en el presente pliego deben ser cubiertos por **un único fabricante de seguridad, una única tecnología y plataforma**. La plataforma deberá ser de un **único fabricante**.

- La solución propuesta debe encontrarse incluida, a fecha de publicación de este expediente, en el Catálogo de Productos de Seguridad de las TIC (Catálogo CPSTIC) recogido en la **Guía de Seguridad de las TIC CCN-STIC-105** "Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación" con Categoría ENS "MEDIA" o superior para las familias: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM) y EDR (ENDPOINT DETECTION AND RESPONSE).
- La solución propuesta debe tener la Certificación de Cloud Security Alliance STAR Level 2, que asegura cumplimiento de las mejores prácticas auditado por terceros para un entorno Cloud confiable.

RT-2. La solución propuesta debe facilitar el acceso a todas las funcionalidades demandadas desde una única interfaz o consola, entendiéndose ésta como un único portal web en el que se recojan todas las capacidades. No se considerarán válidas soluciones que requieran vincular, enlazar o integrar distintas plataformas web, dominios o consolas para cubrir las funcionalidades requeridas.

RT-3. Debe tratarse de una solución 100% nativa en cloud (nube) pública del fabricante de seguridad y no debe requerir la instalación de ningún elemento físico o virtual en las instalaciones de la DGGC para ofrecer todas sus funcionalidades, salvo la instalación de un único agente software en cada elemento de puesto de usuario o servidor.

RT-4. Los servicios en cloud pública del fabricante deben estar alojados en datacenters de la Unión Europea y disponer de, al menos, la certificación:

- ENS nivel ALTO
- Cumplimiento RGPD

RT-5. La solución propuesta debe garantizar la continuidad de servicio y su disponibilidad en horario 24x7x365. La solución debe ser auto escalable y no debe requerir el mantenimiento de ninguna infraestructura garantizando la misma calidad de servicio independientemente de la demanda. Se requieren al menos 200TB de almacenamiento inicial

RT-6. Las tareas de gestión, mantenimiento y actualizaciones de la plataforma a la que da acceso el servicio debe realizarse de forma transparente para el servicio, sin ninguna indisponibilidad del servicio o inactividad total o parcial.

RT-7. La interfaz de usuario debe estar protegida con autenticación multifactorial y soportar (1) SSO SAML 2.0

RT-8. La solución debe requerir una configuración mínima y una gestión continua para lograr los mejores resultados.

RT-9. La solución debe proporcionar la capacidad de agrupar hosts basados en identificadores de host, unidades organizativas de Active Directory o etiquetas para la aplicación de políticas.

RT-10. La solución debe proporcionar un control de acceso basado en roles para permitir el acceso a unidades de negocio o funciones individuales.

RT-11. La solución debe proporcionar una API rica y robusta para integrarse con herramientas de terceros existentes (SIEM, infraestructura, orquestación o sistemas de gestión de casos).

RT-12. La solución propuesta de EDR ha tenido que ser evaluada por la agencia independiente Gartner en los tres últimos años (2019, 2020, 2021) como una de las soluciones líderes del mercado en el cuadrante Gartner.

RT-13. La solución debe proporcionar una API para integrarse con herramientas comunes de orquestación y automatización, así como con sistemas de gestión de casos.

4. REQUISITOS GENERALES DE LOS AGENTES DEL SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

Considerando el amplio ecosistema tecnológico de la DGGC, en el que existe una gran variedad de equipos de puesto de usuario y servidor, con multitud de configuraciones hardware, sistemas operativos, aplicaciones y niveles de actualización, para garantizar el correcto acceso, es necesario que se disponga de una solución que facilite el

despliegue, minimice el impacto en rendimiento en el endpoint o servidor final y cuya implantación no suponga una interrupción en los servicios productivos.

Por este motivo se deberán cumplir con los siguientes requisitos:

RT-14. Para el cumplimiento de **todas** las funcionalidades requeridas en el presente pliego debe disponerse de un **único agente** instalado en los puestos de usuario o servidores no siendo válidas soluciones que requieran distintos agentes para proporcionar todas las funcionalidades solicitadas.

RT-15. Para simplificar, agilizar y minimizar los tiempos de despliegue de la solución, así como para evitar problemas de incompatibilidades durante el despliegue y fallos durante la instalación, el agente software a desplegar y su instalador debe ser el mismo para cada familia de Sistemas Operativos entendiéndose esto como:

- Un único agente para sistemas Windows (incluyéndose en esta familia los sistemas Windows Server en sus versiones 2008R2 y superiores, Windows 10 y superiores y Windows 7SP2 y superiores).

- Un único agente para cada distribución sistemas Linux (en todas las versiones/distribuciones soportadas).

- Un únco agente para sistemas Mac OS

- Un único agente para sistemas iOS y Android en todas sus versiones soportadas.

RT-16. La instalación completa del agente que da acceso al servicio, en cada uno de los endpoints o servidores, debe poder hacerse sin reinicio. Es decir, no debe ser necesario el reinicio del sistema para que el agente instalado proporcione todas las funcionalidades de seguridad requeridas.

RT-17. Para minimizar el impacto en los sistemas productivos y facilitar el despliegue e implantación de la solución, el agente a instalar en los endpoints debe requerir los mínimos recursos hardware del host. Deben garantizarse, para todos los sistemas operativos soportados, un consumo de recursos del endpoint o servidor inferiores a los siguientes:

- Consumo máximo de CPU: el consumo total de los procesos vinculados al agente de la solución debe ser inferior al 3% de la/las CPUs físicas o virtuales. Este consumo máximo de CPU debe ser garantizado no admitiéndose soluciones que, durante la ejecución de procesos y operaciones relacionados con el funcionamiento de la solución, superen el consumo máximo indicado.

- Consumo máximo de Memoria RAM: el consumo total de memoria RAM de los procesos vinculados al agente de la solución debe ser inferior a 100MB. Este consumo de memoria máximo debe ser garantizado no admitiéndose soluciones

que, durante la ejecución de procesos y operaciones relacionados con el funcionamiento de la solución, superen el consumo máximo indicado.

- Requisitos máximos de espacio en disco: el tamaño máximo en disco del agente una vez instalado debe ser inferior a 100MB.

RT-18. El tamaño en disco del instalador del agente descomprimido no debe ser superior a **70MB.**

RT-19. El agente a instalar en los puestos de usuarios o servidores debe ser compatible con infraestructuras físicas y virtuales.

RT-20. Para garantizar que el despliegue de la solución no produce afección a la disponibilidad y continuidad de los servicios productivos, la instalación completa del agente en cada uno de los endpoints o servidores debe poder hacerse sin reinicio y sin intervención del usuario. Se entiende por instalación completa sin reinicio al despliegue del agente en cada uno de los endpoints quedando enrolado en la plataforma cloud y completamente funcional para las funciones requeridas sin necesidad de reiniciar el sistema o intervención manual del usuario. Esta misma condición aplica también a las actualizaciones periódicas del agente.

RT-21. La tecnología del endpoint debe poder desplegarse mediante herramientas de despliegue comunes (políticas de grupo de directorio activo, herramientas de despliegue software, etc.).

RT-22. El agente del endpoint debe admitir actualizaciones de software controladas por políticas desde la plataforma desde la que se provee el servicio. Las actualizaciones del agente serán controladas mediante políticas y grupos pudiendo ser priorizadas. Estas políticas deben permitir realizar controles de cambio N-1, N-2 para cumplir con los requisitos de versionado.

RT-23. El agente del endpoint debe estar habilitado en la plataforma desde la que se provee el servicio, para permitir que se realicen acciones de alerta y respuesta a incidentes en tiempo real cuando los usuarios están en itinerantica o para cargas de trabajo en la nube.

RT-24. El agente debe disponer de capacidades de integración con terceros para disponer de capacidades de detección en elementos IOT/OT.

RT-25. La tecnología de pendpoint debe ser compatible con plataformas en la nube como Amazon Web Servicies EC2, Google Cloud Platform y Azure.

RT-26. La solución propuesta debe tener soporte de [(2)]contenedores (OCI) mediante la captura de la actividad y los metadatos de los contenedores. La solución debe proporcionar una visibilidad completa de los contenedores y añadir seguridad en tiempo de ejecución.

RT-27. La telemetría extraída de los endpoints, así como los detalles forenses, deben poder enviarse a la plataforma desde la que se provee el servicio en tiempo real. En caso de que no exista conectividad entre la consola y el endpoint para el envío de telemetría, el agente instalado se encargará de guardar y custodiar esta información hasta que se retome esta conectividad y pueda realizarse el envío a la plataforma cloud.

RT-28. La instalación del agente debe permitir incluir la parametrización para arquitecturas de red y seguridad basadas en proxy.

RT-29. La instalación del agente debe ofrecer la posibilidad de incluir parametrización para asignación de Tags informativos a los endpoint en los que se realiza el despliegue.

RT-30. Todas las funcionalidades de seguridad requeridas deben proveerse independientemente de la versión de sistema operativo y nivel de parches sobre el que se encuentre instalado el agente. Es decir, la solución propuesta debe cumplir con todas las funcionalidades de seguridad requeridas siempre que se encuentre desplegada en un endpoint que disponga de un Sistema Operativo soportado siendo independiente de su versión o estado de parcheo.

RT-31. El agente de endpoint opera tanto en el espacio del usuario como en el del núcleo (Kernel); el modo de núcleo (Kernel) para una visibilidad completa y para eliminar los puntos ciegos.

RT-32. El agente de endpoint debe capturar continuamente los eventos en bruto, incluso cuando no están asociados a alertas y detecciones.

RT-33. El agente debe transmitir la telemetría EDR en tiempo real para la consulta en vivo y los resultados deben almacenarse en el entorno cloud para ser consultados y disponer de toda la información incluso cuando los puntos finales están fuera de línea.

RT-34. El agente debe proporcionar una grabación continua de los eventos clave para el análisis retrospectivo de todos los eventos recogidos. Se requiere un mínimo de 400 tipos de eventos diferentes. Los eventos de información deben obtener al menos la siguiente información:

- Eventos generales: Sensor On-line (sensor operativo y con conectividad), Identidad de usuario, Crash Notification (notificaciones de bloqueo) (Los eventos básicos requeridos para monitorear la salud del sensor y para permitir a los clientes identificar los dispositivos)
- Eventos de sesión de usuario: creado, conectado, conectado/desconectado, desconectado (Monitorización básica de eventos de sesión de usuario con procesos e hilos asociados)
- Eventos del proceso: Creación del proceso, [(3)]información del PE (Portable Ejecutable), información de la firma, terminación (Datos del proceso por defecto necesarios para la identificación)
- Library Events, Library Load (Identificación de las bibliotecas de software relacionadas con los procesos cargados)

- Eventos de hilos: Creación de hilos, inyección de hilos (Uso enfocado a la supervisión de cadenas de ejecución sospechosas)
- Eventos de Registro: Actualización de [(4)]Clave ASEP, Actualización de Valor ASEP (Supervisión de puntos de carga que permiten a los atacantes establecer persistencia)
- Eventos de archivo: Creación/escritura de archivos, acceso a archivos (Desencadenados y utilizados por un proceso dentro de una cadena de ejecución sospechosa; alcance limitado a los archivos relacionados con dichos procesos)
- Eventos de red: Conexión de entrada/salida, Cierre de red, Resumen de conexión (Enfocado a identificar procesos de actividad de red dentro de una cadena de ejecución sospechosa.)
    - Red: Cierre de conexión, apertura de conexión, conexiones a la Escucha, Recibir/Aceptar para IP4/IP6.
    - Eventos DNS: Solicitudes DNS (Para determinar búsquedas DNS no estándar, centradas en consultas DNS inesperadas)
- Eventos Varios: Creación de Objetos con Nombre, por ejemplo, semáforos (uso enfocado a monitorear cadenas de ejecución sospechosas).
- Proceso: Eventos de información de tokens, creaciones, inyecciones, relaciones de abuelo, padre, hijo.
- Archivo: Escritura, borrado, renombrado, apertura e información.
- Usuario: Inicio de sesión, cierre de sesión, intentos fallidos de login
- DLL: Intentos de inyección y reflexión,
- Detalles del host incluyendo y sin limitarse a lo siguiente:
    - SO: Atributos de la unidad organizativa , nombre de host, tipo de dispositivo, versión del SO, fabricante, modelo
    - Red: MAC, IP local y externa, host vecinos con y sin agente desplegado".

RT-35. El agente debe proporcionar una amplia cobertura de eventos manteniendo menos de 20 MB de datos transmitidos por endpoint o carga de trabajo cada 24 horas.

RT-36. El agente debe recopilar a través de múltiples métodos de recogida eventos en el endpoint de al menos: llamadas api, [(5)]ETW, controlador de filtro del núcleo y eventos del SO.

RT-37. El agente debe asociar el contexto del usuario (local o de dominio) con los eventos relevantes en los sistemas operativos de Microsoft soportados por la plataforma.

RT-38. El agente debe ser compatible en entornos cloud AWS, Google Cloud y Azure

RT-39. El agente debe ofrecer información relativa a workloads (Cargas de Trabajo).

RT-40. El agente debe ofrecer información relativa a las configuraciones de seguridad realizadas en entornos cloud y poder programar análisis de forma periódica relativos a esta funcionalidad.

5. REQUISITOS GENERALES DE FUNCIONALIDADES REQUERIDAS DEL SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

5.1 FUNCIONALIDADES DE SEGURIDAD

RT-41. La plataforma de acceso a base de datos desde la que se presta el servicio debe facilitar la comunicación de alertas de detección en tiempo real, por ejemplo, por correo electrónico, y proporcionar informes y cuadros de mando en tiempo real.

RT-42. Debe mostrarse en la consola una puntuación de riesgo de las amenazas en tiempo real. Esta puntuación de riesgo debe ser dinámica y evolucionar en tiempo real en función de las distintas métricas que se utilicen para su cálculo, permitiendo a los administradores conocer en todo momento el estado y severidad de amenazas y ataques.

RT-43. La plataforma de acceso a base de datos desde la que se presta el servicio debe proporcionar un registro de auditoría de la actividad de los usuarios incluidas las tareas de gestión y respuesta a incidentes. Esta información de auditoría debe ser accesible desde la propia interfaz o a través de API. La información contenida en este registro de auditoría debe contener al menos la siguiente información: creación de administradores, cambios de permisos, login a la plataforma, actividad durante la sesión, conexiones a host, comandos ejecutados, inicio y duración de la sesión, etc.

RT-44. La plataforma de acceso a base de datos desde la que se presta el servicio debe ser accesible desde un navegador web.

RT-45. Para facilitar todas las funcionalidades de seguridad requeridas, los agentes instalados en cada uno de los puestos de usuario o servidor deben requerir únicamente la conexión a un máximo de 2 (dos) dominios de internet correspondientes a la infraestructura cloud del fabricante de seguridad. No serán válidas soluciones que requieran la conexión a un mayor número de dominios o mayores necesidades de visibilidad entre redes.

RT-46. El acceso bajo demanda a los metadatos relacionados con todas las amenazas generadas desde la plataforma debe permanecer accesibles durante el periodo de validez de las suscripciones al servicio.

RT-47. El acceso bajo demanda a los detalles forenses completos de todas las amenazas detectadas por la plataforma debe estar disponibles durante 90 días.

RT-48. El acceso bajo demanda a un registro histórico completo de los eventos de endpoint, utilizados para la detección retrospectiva, la búsqueda de amenazas y las investigaciones debe permanecer accesible en un periodo de 30 días.

RT-49. Debe ser posible facilitar la posibilidad de obtener una réplica offline de los datos enriquecidos de los sensores para su uso.

RT-50. Proporcionar mecanismos que permitan el acceso a la plataforma de múltiples departamentos o divisiones de la organización, pero que formen parte de una gran organización.

RT-51. La solución debe mostrar información relativa a controles de cumplimiento [(6)]CIS, [(7)]NIST y [(8)]PCI en entornos AWS y Google Cloud .

5.2 FUNCIONALIDADES DE ORQUESTACIÓN Y AUTOMATIZACIÓN

Considerando las capacidades de penetración, velocidad de propagación, vectores de ataques y daños ocasionados que están causando los últimos ciberataques registrados en ámbitos público y privado, es necesario disponer de soluciones de acceso a bases de datos que permitan automatizar y orquestar acciones de respuesta y minimizar los tiempos de respuesta ante incidentes.

Se requiere, por tanto, que la solución propuesta permita realizar automatizaciones y orquestaciones de tareas y respuestas automáticas en base a criterios de telemetría y/o detección. La solución propuesta debe incluir estas capacidades en la misma plataforma, no siendo válidas soluciones que requieran la conexión a otras plataformas o servicios, plataformas web o consolas para desarrollar estas funciones.

Las capacidades de automatización de la plataforma deben incluir al menos:

RT-52. Capacidad de creación de flujos de trabajo mediante interfaz visual en la propia plataforma.

RT-53. Los disparadores de acciones deben poder provenir tanto de detecciones como de auditoría de elementos cloud o de la ejecución de un flujo de trabajo previo.

RT-54. Las condiciones han de poder incluirse tanto de forma secuencial como paralela y deben incluir tanto las acciones tomadas por la plataforma durante la detección como cualquier elemento que define las características de un endpoint concreto o su pertenencia a un grupo determinado.

RT-55. Acciones de respuesta: entre las acciones de respuesta posibles deben incluirse al menos las siguientes:

- Contención de red de un endpoint
- Actualización del contenido de la detección
- Exposición de URL para orquestar con elementos terceros.
- Enriquecimiento mediante información de terceros (Virus Total).
- Notificaciones automáticas vía Teams o Slack.
- Obtención y borrado de ficheros del endpoint.

- Obtención de procesos y conexiones activas del endpoint

RT-56. Debe poder disponerse de un versionado de los playbooks o flujos de trabajo creados.

RT-57. Debe proporcionar un log de ejecución del flujo de trabajo creado.

RT-58. Todos los eventos de telemetría del endpoint podrán usarse como elementos de una condición.

5.3 FUNCIONALIDADES PREVENTIVAS Y DE DETECCIÓN

RTC-59. Todas las capacidades preventivas y de detección del servicio deben estar cubiertas por **un único fabricante de seguridad**, **una única tecnología y plataforma**. Es decir, la solución propuesta debe facilitar el acceso a la base de datos, con todas las funcionalidades demandadas, desde una única interfaz o consola, entendiéndose ésta como un único portal web en el que se recojan todas las capacidades. No se considerarán válidas soluciones que requieran vincular, enlazar o integrar distintas plataformas web, dominios o consolas para cubrir las funcionalidades requeridas.

La plataforma propuesta para la prestación del servicio de acceso a la base de datos debe cumplir con al menos las siguientes características:

RT-60. La solución propuesta debe ser una plataforma de seguridad de última generación que utilice técnicas de aprendizaje automático/machine learning para la prevención previa a la ejecución de malware conocido y desconocido. Entre las capacidades de detección y prevención deben incluirse la detección de técnicas, tácticas y procedimientos susceptibles de ser utilizados por agentes maliciosos.

RT-61. Las capacidades preventivas deben estar disponibles tanto en línea como fuera de línea, es decir, deben poder aplicarse las políticas definidas independientemente de si el endpoint o servidor se encuentra o no conectado a la red.

RT-62. Debe permitir la puesta en cuarentena de malware detectado y ofrecer la posibilidad de restaurar o poner en lista blanca los archivos de cuarentena directamente desde la plataforma de gestión.

RT-63. Debe disponer de capacidad de enviar los archivos en cuarentena.

RT-64. Debe disponer de la capacidad para la generación de listas de autorización y bloqueo de hashes de archivo personalizables.

RT-65. La plataforma debe proporcionar capacidades de detección basadas en el análisis de comportamiento posterior a la ejecución de un malware, permitiendo la protección contra las actividades habituales del ransomware (cifrado de archivos, eliminación de archivos de backup, etc.)

RT-66. Proporcionará una detección y prevención basada en el comportamiento posterior a la ejecución, basada en el Indicador de Ataque (IOA) mapeado según el marco [(9)]MITRE ATT&CK. Este tipo de reglas de detección debe soportar reglas relacionadas con procesos (hasta 3 niveles de procesos y líneas de comando asociadas), ficheros y comunicaciones. En todos los casos debe ofrecerse la posibilidad de ofrecer detección y bloqueo.

RT-67. Tendrá capacidad de convertir las detecciones en una prevención, incluidas las detecciones basadas en el comportamiento.

RT-68. Las prevenciones deben detener los ataques antes de que se produzcan daños en el sistema operativo. Por ejemplo, evitar la inyección de procesos antes de que se produzca, de modo que el proceso objetivo no se vea interrumpido o comprometido.

RT-69. La solución debe ofrecer protección de la memoria (por ejemplo, [(10)]ASLR, protección contra la sobrescritura de la gestión de excepciones estructuradas, protección de páginas nulas, preasignación de la pila, etc.).

RT-70. La solución debe ser capaz de prevenir el uso malicioso de [(11)]Powershell y los ataques con scripts.

RT-71. La solución debe ser capaz de realizar controles preventivos contra ataques sin archivos (mientras se está desconectado).

RT-72. La solución debe proporcionar la capacidad de escribir detecciones y bloqueos de comportamiento personalizadas basadas en artefactos relacionados con la creación de procesos, la creación de archivos, las conexiones de red y las búsquedas de dominios.

RT-73. La solución debe detectar las técnicas habituales de robo de credenciales.

RT-74. La solución debe facilitar acciones de Respuesta que incluyan el aislamiento del endpoint o la conexión interactiva con el endpoint.

RT-75. La solución debe correlacionar y presentar automáticamente la telemetría y los metadatos (indicadores de compromiso o IOC) relacionados con el ataque en una línea de tiempo. Por ejemplo, argumentos de línea de comandos, escrituras de archivos, solicitudes DNS, conexiones IP, etc.

RT-76. La solución debe soportar la ingestión de indicadores de compromiso o IOC (hashes, ip, dominios y url) vía API o en la consola, que se mantendrán en la plataforma por un periodo determinado de tiempo y que serán utilizados durante todo el ciclo de prevención/detección de la plataforma. Se debe permitir hasta 100.000 indicadores de compromiso o IOC. Adicionalmente se requiere que sea posible indicar un comentario con información adicional relativa al indicadores de compromiso o IOC cargado en la plataforma y su periodo de expiración. Debe poder realizarse bloqueo de los indicadores de compromiso o IOC de tipo hashes y detección de los IOC de tipo dominio y hash.

RT-77. La solución debe permitir adaptarse a los diferentes niveles de riesgo, para lo cual, deberá ser posible modificar en la consola y de forma independiente para la parte preventiva y parte de detección al menos los siguientes estados:

- Desactivado
- Nivel Cauto
- Nivel Moderado
- Nivel Agresivo
- Nivel extra agresivo

RT-78. La solución debe correlacionar, cuando sea posible, el vector de infección y la intención de los atacantes de la amenaza en relación con la cadena de ataque, correlacionando con la telemetría, el árbol de procesos y la inteligencia de la amenaza.

RT-79. La solución debe correlacionar de forma opcional las detecciones con los principales actores de la amenaza (estado-nación y crimen electrónico) cuando sea aplicable.

RT-80. La solución debe ser capaz de contener remotamente un endpoint utilizando mecanismos no relacionados con el cortafuegos del sistema operativo.

RT-81. La contención debe persistir después de un reinicio.

RT-82. La solución debe proporcionar la capacidad de conectarse remotamente a los sistemas de destino con el fin de recopilar pruebas forenses adicionales (volcados de memoria completos, registro, archivos, etc.) y realizar tareas de remediación tales como cierre de procesos, modificación del registro de Windows, etc.

RT-83. La solución debe proporcionar capacidades para enviar archivos a sistemas remotos, ejecutar archivos, ejecutar scripts, matar procesos, ajustar claves de registro y otras tareas necesarias durante la respuesta a incidentes.

RT-84. La solución debe ofrecer opciones de filtrado para las detecciones realizadas que permitan visualizarlas en función de: Severidad, Táctica, Técnica, Periodo de tiempo de la detección, estado de gestión de la vulnerabilidad, Fichero afectado y analista asignado.

RT-85. La solución debe ofrecer la posibilidad de asignar a un analista el trabajo de respuesta sobre una detección.

RT-86. La solución debe ofrecer información de terceros relativa a una detección (Ej: detecciones en VirusTotal, información en google).

RT-87. La solución debe ofrecer en cada detección la información relativa al usuario, al Host, a las vulnerabilidades presentes en el host, procesos, registro de sistema, actividades de red y resoluciones dns.

RT-88. La solución debe ofrecer una vista gráfica que permita observar el árbol de procesos relacionado con una detección.

RT-89. La solución debe ofrecer a un analista capacidades de inclusión de comentarios relativos a las tareas realizadas en respuesta a una detección.

RT-90. Detección de amenazas basada en comportamiento e inteligencia de amenazas que permita alertar y bloquear amenazas y que adicionalmente ofrezca información relativa a:

- Vector de entrada utilizado por el atacante.
- Compresión de las tácticas y técnicas utilizadas por el atacante.
- Periodo temporal en el que se enmarca la amenaza.
- Activos comprometidos.
- Contextualización de los procesos seguidos por el atacante a lo largo de la cadena de ataque.

5.4 FUNCIONALIDADES DE BUSQUEDA ACTIVA DE AMENAZAS (THREAT HUNTING)

La plataforma propuesta para la prestación del servicio de acceso a base de datos debe proporcionar la capacidad de realizar búsquedas de amenazas (threat hunting) sobre la información de telemetría generada por los endpoints. Al menos debe disponer de las siguientes especificaciones y funcionalidades:

RT-91. La solución propuesta debe supervisar la actividad de procesos de los endpoints enviando de forma continua y en tiempo real información de eventos y detalles forenses a la plataforma cloud.

RT-92. La solución debe incluir capacidades de búsqueda histórica y en tiempo real totalmente personalizables sin afectar a los puntos finales durante la búsqueda.

RT-93. La solución debe proporcionar la capacidad de realizar una búsqueda de eventos sin procesar utilizando un lenguaje de consulta estructurado a través de toda la telemetría de eventos recopilados (apilamiento de datos).

RT-94. La solución debe proporcionar consultas predefinidas para todas las actividades relacionadas con el usuario y el endpoint.

RT-95. La solución debe proporcionar consultas predefinidas para artefactos forenses (por ejemplo, hash, dominio, eventos sin procesar, claves de registro).

RT-96. Las búsquedas simultáneas en toda la organización no deben afectar a los terminales.

RT-97. La telemetría de puntos finales debe permitir la exportación a formatos comunes como CSV, XML y RAW.

RT-98. La solución debe proporcionar informes de búsqueda de amenazas y análisis de líneas de tiempo.

RT-99. La solución debe proporcionar un informe para demostrar la línea de tiempo completa de los eventos que ocurren en un host.

RT-100. La solución debe proporcionar un informe que demuestre la cronología completa de los eventos de un proceso.

RT-101. La plataforma debe permitir realizar búsquedas utilizando la interfaz de usuario. Estas búsquedas deben poder incluir al menos: hashes específicos, nombres de fichero, parámetros de líneas de comandos, direcciones IP, dominios, eventos sin procesar, claves de registro, etc. La solución debe mostrar información detallada de cada endpoint en lo relativo a: Procesos y servicios, comandos ejecutados por herramientas de administración, actividad de Scripts, actividades relativas a registro, tareas programadas, políticas de Firewall y Actividades de red.

RT-102. La solución propuesta para la prestación del servicio debe ofrecer la capacidad de hacer búsquedas proactiva de amenazas (threat hunting) 24 horas al día 7 días a la semana completamente gestionado y proporcionado directamente por el fabricante de seguridad correspondiente a la plataforma tecnológica propuesta. Este servicio de threat hunting gestionado debe apoyarse en los programas internos de inteligencia del fabricante de seguridad propuesto y debe notificar las detecciones o incidentes de relevancia detectados en los que se considere que debe existir respuesta o actuación por parte de la DGGC para responder y/o minimizar el impacto ante un posible ataque. Se valorará el modelo de prestación de este servicio, considerando de valor propuestas que detallen la forma en la que se presta éste: herramientas utilizadas, fuentes de información e inteligencia, integración con la plataforma tecnológica propuesta, mecanismos de comunicación y notificación, etc.

5.5 FUNCIONALIDADES DE GESTION DE DISPOSITIVOS USB

RT-103. Todas las funcionalidades demandadas deben ser accesibles desde la misma interfaz única indicada en puntos anteriores desde la que se prestan todas las funcionalidades de seguridad, entendiéndose ésta como un único portal web en el que se recojan todas las capacidades. No se considerarán válidas soluciones que requieran vincular, enlazar o integrar distintas plataformas web, dominios o consolas para cubrir las funcionalidades requeridas.

La plataforma propuesta para mitigar los riesgos asociados a los dispositivos USB debe disponer de las siguientes funcionalidades:

RT-104. Debe ofrecerse visibilidad de los dispositivos USB en lo relativo a:

- Tipo de dispositivo
- Marca del dispositivo y fabricante
- Uso de los dispositivos USB
- Supervisión de los archivos escritos en el almacenamiento USB

RT-105. Debe posibilitarse el control del uso de los dispositivos USB e implantar políticas específicas.

RT-106. La solución debe ser capaz de restringir el uso de USB mientras se está fuera de línea, incluyendo, pero sin limitarse a, el tipo de dispositivo y la función.

6. GARANTÍA DE CUMPLIMIENTO DE REQUISITOS MINIMOS DEL SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

La solución propuesta para la prestación del servicio debe cumplir con todos y cada uno de los requisitos, funcionalidades y especificaciones técnicas demandadas. En caso de dudas con la documentación presentada, a decisión de la DGGC, se deberá poner a disposición de la DGGC un entorno de pruebas idéntico al ofertado en un plazo máximo de 5 días laborables, con objeto de poder verificar el efectivo cumplimiento de los de los requisitos especificados en el pliego de prescripciones técnicas y los valores ofertados para los criterios de adjudicación, mediante un conjunto de pruebas y exámenes.

7. SERVICIOS DEL ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

La solución contemplará el servicio de monitorización de la seguridad del entorno y la gestión de los potenciales incidentes de seguridad de la manera más eficiente posible, mediante la prestación de servicios basados en recursos técnicos aportados por el licitador.

RT-107. Para prestar el servicio, la empresa licitadora deberá estar en posesión de las acreditaciones de seguridad exigidas en el PCAP en vigor a la fecha de la presentación de la oferta, tanto de la empresa como de los diferentes perfiles ofertados, Además la empresa licitadora deberá estar certificada en el ENS como mínimo en nivel medio. Los servicios no se podrán subcontratar a terceras empresas.

RT-108. La propuesta debe incluir un Ingeniero de Instalación de la solución para las tareas de Instalación, configuración y puesta en marcha del servicio durante 12 meses, con una dedicación exclusiva.

RT-109. La propuesta debe incluir un perfil de Ingeniero de Soporte de Explotación On-Site para la administrador de la plataforma, con una dedicación exclusiva durante 24 meses.

RT-110. La propuesta debe incluir un perfil de Ingeniero de Despliegue On-site para actualización y evolución continua del servicio, con una dedicación exclusiva durante 12 meses.

RT-111. La propuesta debe incluir un perfil de Consultor de Formación On-site, con una dedicación exclusiva de 80 horas para un mínimo de 10 alumnos.

RT-112. La propuesta debe incluir la figura de un jefe de proyecto/gerente del servicio con una dedicación exclusiva de 24 meses.

RT-113. Los recursos materiales y personales ofertados tendrán la dedicación exigida en el pliego y no podrá solaparse y/o compartir dedicación con ningún recurso que actualmente estén prestando servicios para la Guardia Civil en cualquier otro expediente.

RT-114. El prestatario del servicio será partner reconocido del fabricante y deberá aportar tanto un certificado que lo acredite como una autorización expresa de la oficina local del propio fabricante para suministrar e instalar la solución o plataforma necesaria para cubrir los requisitos técnicos definidos en este pliego. Todos los equipos, licencias y componentes que se suministren serán originales del fabricante, adquiridos dentro de la UE, a través de los canales oficiales de comercialización que la delegación del fabricante en España determine y dispondrán de la garantía oficial. El licitador deberá aportar certificado acreditativo de este requisito para esta licitación.

8. DOCUMENTACIÓN DEL SERVICIO DE ACCESO A BASE DE DATOS DE CIBERAMENAZAS AVANZADAS

RT-115. Al inicio del servicio y durante el desarrollo del mismo, se entregará la siguiente documentación de proyecto:

- Documento de instalación y configuración de la solución.
- Plan de instalación inicial.
- Plan de mantenimiento o tareas preventivas si las hubiese.
- Plan de verificación y validación de la solución en su puesta en funcionamiento.
- Manual técnico de operación de la solución.
- Informe mensual de seguimiento de contrato

RT-116. Se entregará en el momento de la oferta la documentación acreditativa de que los técnicos encargados de la instalación, configuración, puesta en marcha y explotación de la solución cuentan con la experiencia profesional y formación académica necesaria para realizar las tareas o cometidos a desarrollar, así como las certificaciones del fabricante.

RT-117. Toda la documentación técnica que sea elaborada en virtud de este Contrato pasará a ser propiedad de la Guardia Civil una vez concluido el mismo.

Glosario:

(1)SSO SAML-2: Servicio de inicio de sesión único (SSO) basado en SAML. El lenguaje de marcado para confirmaciones de seguridad (SAML) es un estándar XML con el que los dominios web seguros pueden intercambiar datos de autenticación y autorización de los usuarios. Mediante SAML, un proveedor de servicios online puede ponerse en contacto con un proveedor de identidades online para que autentique a los usuarios que intenten acceder a contenido seguro.

(2)Contenedores OCI: La Open Container Initiative, también conocida por sus siglas OCI, es un proyecto de la Linux Foundation para diseñar un estándar abierto para virtualización a nivel de sistema operativo. El objetivo con estos estándares es asegurar que las plataformas de contenedores no estén vinculadas a ninguna empresa o proyecto concreto.

(3)Portable Ejecutable: El formato Portable Executable (PE) es un formato de archivo para archivos ejecutables, de código objeto, bibliotecas de enlace dinámico (DLL), archivos de fuentes FON,1 y otros usados en versiones de 32 bit y 64 bit del sistema operativo Microsoft Windows. El término «portable» refiere a la versatilidad del formato en numerosos ambientes de arquitecturas de software de sistema operativo.2 El formato PE es una estructura de datos que encapsula la información necesaria para el cargador de Windows para administrar el código ejecutable que le envuelve. Esto incluye las referencias hacia las bibliotecas de enlace dinámico para el enlazado, la importación y exportación de las tablas de la API, gestión de los datos de los recursos y los datos de almacenamiento local de subprocesos (datos de TLS).

(4)ASEP: Auto-Start Extensibility Point, es una clave del registro windows que podría llevar a la ejecucuión automática de un proceso.

(5)ETW: Seguimiento de eventos para Windows (ETW) es una eficaz instalación de seguimiento de nivel de kernel que permite registrar eventos definidos por el kernel o la aplicación en un archivo de registro. Puede consumir los eventos en tiempo real o desde un archivo de registro y usarlos para depurar una aplicación o para determinar dónde se producen los problemas de rendimiento en la aplicación.

(6)CIS: Los controles críticos de seguridad de CIS son un conjunto de acciones priorizadas para la ciberseguridad que forman un conjunto de defensa en profundidad de mejores prácticas específicas y procesables para mitigar los ataques cibernéticos más comunes. Un beneficio principal de los controles CIS es que priorizan y se centran en una pequeña cantidad de acciones que reducen en gran medida el riesgo de ciberseguridad.

(7)NIST: El Marco de Ciberseguridad o Cibersecurity Framework del Instituto Nacional de Estándares y Tecnología, NIST por sus siglas en inglés, es una herramienta para la gestión de riesgos asociados a la seguridad de la información y si bien es un marco de adopción voluntaria, ofrece diferentes ventajas.

(8)PCI: PCI DSS es la normativa internacional de seguridad para todas las entidades que almacenan, procesan o transmiten datos de titulares de tarjeta o datos sensibles de autenticación.

(9)MITRE ATT & CK: son las siglas de MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT & CK). El marco MITRE ATT & CK es una base de conocimientos y un modelo seleccionados para el comportamiento del adversario cibernético, que refleja las diversas fases del ciclo de vida del ataque de un adversario y las plataformas a las que se sabe que se dirigen.

(10)ASLR: La aleatoriedad en la disposición del espacio de direcciones (conocida por las siglas en inglés ASLR) es una técnica de seguridad informáticarelacionada con la explotación de vulnerabilidades basadas en la corrupción de memoria.

(11)PowerShell: es una interfaz de consola con posibilidad de escritura y unión de comandos por medio de instrucciones. Esta interfaz de consola está diseñada para su uso por parte de administradores de sistemas con el propósito de automatizar tareas o realizarlas de forma más controlada