PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR LA CONTRATACIÓN DE UN SISTEMA EDR PARA PROTECCIÓN DE EQUIPOS DE USUARIO CON CONSOLA CENTRALIZADA EN LA NUBE

1. OBJETO

El Ayuntamiento tiene por objeto celebrar un contrato administrativo para la contratación de un servicio EDR (Endpoint Detection & Response) gestionado en la nube para la protección integral de los datos en puestos informáticos de usuarios, smartphones y servidores que además cuente con mecanismos de detección y desinfección en caso de infección con cualquier tipo de malware.

Actualmente, el Ayuntamiento tiene licencias del sistema Panda Adaptive Defense 360 que permite la gestión en entorno cloud del sistema antivirus en el parque, por lo que se pretende disponer de una solución que ofrezca, de base, las mismas prestaciones y funcionalidades.

El sistema EDR deberá contar con módulos adicionales que aporten funcionalidades de seguridad tales como doble factor de autenticación, gestión de parches de seguridad de software o recopilación y análisis de eventos de seguridad. Todas estas funcionalidades se gestionarán bajo una misma consola de gestión y estarán integradas en el mismo producto.

El sistema ofertado, deberá estar avalado por el CCN-CERT, a través del Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación CCN-STIC-105 del CCN con categoría ENS ALTA, para la categoría EDR, como garantía de que la solución está alineada con los requisitos del ENS.

Las licencias suministradas permanecerán activas durante la vigencia del actual contrato y desde el momento en que se realice y se valide el despliegue por parte del Ayuntamiento de Valdepeñas.

2. ALCANCE

Mediante este pliego se pretenden establecer los requisitos mínimos que deberá cumplir el sistema EDR a implantar en el Ayuntamiento y que, atendiendo a los informes sobre amenazas publicados periódicamente por el CCN-CERT, deben proteger a los equipos de trabajo y servidores del Ayuntamiento (con sistema operativo Windows) contra cualquier malware, siendo éste conocido o no. Además, el sistema proporcionado deberá estar disponible para su uso en dispositivos móviles Android e iOS.

Para ello, la solución propuesta por los licitadores debe cumplir con estos objetivos:

- Proporcionar una protección antivirus tradicional (EPP, Endpoint Protection Platform) basada en técnicas como firmas, métodos heurísticos, técnicas de sandboxing, etc., que proteja a los equipos contra amenazas conocidas e identificadas por el fabricante.
- Proporcionar protección contra amenazas no conocidas (EDR, Endpoint Detection and Response), mediante técnicas no basadas en las del anterior apartado, realizando un análisis del comportamiento de los procesos ejecutados en cada estación de trabajo y bloqueando su ejecución en caso de sospecha. Igualmente, la solución tendrá que disponer de una política que aplique distintos tipos de bloqueo teniendo al menos, auditoría y bloqueo.

  Para cumplir con estos dos objetivos la solución ha de utilizar e instalar en los equipos cliente un solo agente.

- Proporcionar una consola en entorno cloud para la gestión de las amenazas de todo el parque informático que permita, además, tareas avanzadas relacionadas con la configuración del agente, generación de informes, etc.
- La consola del EDR deberá incluir un módulo de análisis y alertas que permita detectar accesos, vulnerabilidades en equipos o servidores, consumo inusual de ancho de banda, así como emitir alertas con objeto de tener un mayor grado de detección de amenazas sobre el sistema.
- Suministrar una utilidad de MFA (Multi-Factor Authentication), para poder implementar el doble factor de autenticación en los sistemas de información del Ayuntamiento.
- Suministrar un módulo que permita el control de parches y actualizaciones de software de los equipos de usuario, válido tanto para las actualizaciones del sistema operativo como para el software de terceros.
- El sistema suministrado deberá estar incluido en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación CCN-STIC-105 del CCN con categoría ENS ALTA, para la categoría EDR.

3. REQUISITOS TÉCNICOS

El número de licencias Endpoint a suministrar es el siguiente:

a. Licencias EDR y EPP: 380 unidades (para desplegar en 380 equipos informáticos).

b. Licencias para solución MFA: 300 (para uso de 300 usuarios).

3.1. Componentes del servicio

- **Infraestructura cloud.** El adjudicatario proveerá, desde la nube (alojada dentro del territorio de la Unión Europea), el conjunto de servidores, bases de datos y procesos de tratamiento de la información relacionada con el servicio. Los procesos capturados de los clientes (archivos ejecutables, DLL, COM) serán tratados en la nube de tal forma que el impacto sobre los sistemas corporativos sea mínimo.
- **Agente, a desplegar en los equipos.** El agente desplegado permitirá la comunicación y gestión de, tanto la protección antivirus tradicional, como la protección de procesos desconocidos. Recogerá la información correspondiente a los eventos y componentes que los producen, sin recopilar información, ni documentos de usuario.

  El impacto sobre los equipos informáticos debe ser menor del 5% de rendimiento de CPU, memoria y disco.

  El agente debe ser capaz de proteger equipos informáticos con las versiones del sistema operativo dentro del ciclo de vida definido por el fabricante, y deberá adaptarse a suscesivas versiones.

  El agente también ofrecerá soporte y funcionará bajo sistemas operativos legacy: versiones a partir de Windows XP SP2, y Windows Server 2003 R2.

  La desinstalación del agente, así como los servicios deberán estar protegidos mediante contraseña con doble factor de autenticación, imposibilitando su desinstalación o parada no autorizada.

La solución deberá poder desplegarse de forma automatizada y centralizada por los siguientes mecanismos:

- Dirección IP.
- Rango de direcciones IPs.
- Nombre de máquina.
- Grupos de *Active Directory* basado en políticas de dominio.

Igualmente, la solución ofertada ha de ser capaz de realizar el descubrimiento e instalación del agente sobre dispositivos sin protección, aunque estos no estén registrados en el Directorio Activo de la entidad.

Tal y como se ha indicado, el módulo de gestión de parches de seguridad no requerirá de la instalación de un agente distinto al del EDR. El mismo agente permitirá controlar ambas funcionalidades.

El adjudicatario será el encargado de distribuir e instalar el agente en todos los equipos cliente, así como de realizar la desinstalación del agente actual, en su caso.

- **Consola web.** La solución dispondrá de una interfaz web en la que se puedan realizar, al menos, las siguientes acciones:
  - Consultar datos en tiempo real. Estado de la protección, de los equipos, amenazas detectadas por el antivirus, ciclo de vida del malware en el equipo (detalles de actividad del malware).
  - Realizar acciones sobre los puestos de trabajo finales (análisis, recopilación de datos, desinstalación del agente, etc.).
  - Visualizar el detalle sobre el hardware y el software de los equipos en los que esté instalado el agente.
  - La consola deberá integrarse con Active Directory de modo que los equipos con el agente obtengan la clasificación en unidades organizativas y dominios implementada en AD.
  - Generar informes y enviarlos de forma automatizada.
  - Crear alertas con avisos por correo electrónico sobre amenzas.
  - Gestionar las actualizaciones de versión de los agentes.

  Los administradores del servicio podrán gestionar desde una consola única, y de forma centralizada, la seguridad y productividad de todas las estaciones de trabajo y servidores Windows, incluyendo ordenadores portátiles y oficinas remotas.

  La consola web estará disponible para cualquier navegador del mercado y en idioma castellano.

- **Compatibilidad con sistemas firewall.** Se pretende disponer de una solución que integre la información recogida por el firewall con la que aporte el antivirus, por lo que el antivirus propuesto deberá disponer de una integración nativa con un sistema firewall, con el acceso a la información de ambos sistemas bajo la misma consola.

Debido a la mejora de productividad y funcionalidades que proporciona disponer de soluciones homogéneas, se valorará que la solución propuesta sea integrable con la solución actual del Ayuntamiento (Watchguard Firebox).

4.2. **Sistema de protección para endpoint**

El sistema de protección ante malware estará dividido en dos partes:

- Protección antivirus tradicional (EPP).
- Protección basada en detecciones y análisis de procesos por comportamiento (EDR).

Estas dos partes estarán combinadas y fusionadas a nivel de configuración, tan solo estarán divididas a nivel de funcionalidad. En todo caso, el sistema estará compuesto de un solo agente, y una sola plataforma o solución. No se permitirá el uso de diferentes módulos.

4.2.1. Protección antivirus tradicional (EPP, Endpoint Protection Platform)

Se trata de una parte del sistema que conste de las funcionalidades clásicas de los antivirus tipo endpoint, entre las que se deberán encontrar las siguientes:

- Antivirus basado en firmas para ficheros y contenido web.
    - Debe permitir la detección y desinfección de cualquier tipo de amenaza detectada por comportamiento.
    - En cuanto a la protección web, se detectarán los intentos de acceso a páginas web que contengan elementos maliciosos, siendo bloqueados en ese caso.
- Firewall personal, que podrá ser gestionado de forma local, en el propio equipo, o de forma centralizada en la consola web. Debe permitir:
    - Bloquear las conexiones entrantes y/o salientes de un conjunto de aplicaciones determinadas.
    - Prevención de intrusiones y ataques (Smart DNS, TCP Port Scan, SYN flood, OS Detection, etc).
    - Crear reglas de firewall para permitir o denegar el tráfico en sentido entrante/saliente a una serie de máquinas y a unos protocolos y/o puertos determinados.
- Bloqueo de todos los dispositivos o de 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. Se debe permitir 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. Se podrán añadir listas blancas y negras de sitios y dominios permitidos.

4.2.2. Protección basada en detecciones y análisis de procesos (EDR, Endpoint Detection and Response)

La solución ofertada contará con una funcionalidad de protección basada en detección predictiva basándose en el análisis de comportamiento de un determinado proceso y que sea capaz de dar una respuesta (bloqueo), a los procesos que clasifique como malware. De este modo se podrá hacer frente a las siguientes amenazas:

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

Esta solución deberá contar con mecanismos que eviten, al máximo, las infecciones de forma proactiva, nunca reactiva. Esto se realizará con **contramedidas diferentes** a las siguientes:

- Firmas locales, que requieren de actualizaciones constantes.
- Motores heurísticos, que hacen uso de CPU y pueden producir falsos positivos.
- Sistemas de listas blancas, que requieren de una alta dedicación para su gestión.
- Sistemas de sandboxing, que consume recursos y pueden ser eludidos por el malware.

El sistema de protección será capaz de clasificar el 100% de los procesos ejecutados en las máquinas en las que se encuentre instalado el agente generando una clasificación de malware o aplicaciones sin riesgo, de modo que todo proceso que se ejecute en la máquina debe haber sido clasificado previamente como bueno; en caso contrario, debería impedir que se ejecutase.

El sistema de protección bloqueará los procesos desconocidos que intenten ejecutarse para evitar la posibilidad de dañar los datos accesibles por la máquina, por ejemplo, el cifrado de los mismos, o el robo o acceso a datos.

El sistema de protección debe incluir un sistema anti-exploit que permita la detección y bloqueo del uso de exploits conocidos o desconocidos.

Se deben poder establecer diferentes niveles de bloqueo, con mayor o menor nivel de restricción, así como diferentes niveles en la capacidad de los usuarios para poder desbloquear individualmente los procesos bloqueados por el sistema.

El sistema debe ser capaz de bloquear la ejecución de aplicaciones que por su comportamiento y naturaleza no estén considerada como aplicaciones seguras.

El EDR permitirá la búsqueda de indicadores de compromiso (IoC) basados en hash de fichero, nombre, ubicación o conexión y reglas Yara, en tiempo real. Además deberá tener la posibilidad de importación masiva de reglas Yara o IoC a través del formato STIX 2.x.

En caso de aislamiento de equipos, se permitirá autorizar la conexión selectiva de aplicaciones.

4.2.3. Módulo de gestión de parches de software

El sistema ofertado incluirá un módulo de gestión de parches y actualizaciones de software que permita detectar y reducir las vulnerabilidades a las que están expuestas los equipos del parque informático.

El módulo estará integrado en el mismo agente, no siendo necesario el despliegue de un nuevo componente.

El sistema de actualización de aplicaciones deberá contar con las siguientes funcionalidades:

- Aplicación de actualizaciones de sistema operativo Microsoft Windows.
- Aplicación de actualizaciones de software de terceros entre los que se incluirán: Adobe, 7-zip, Microsoft, Oracle, Apple, Google, Mozilla, Apache, Autodesk, Filezilla, Foxit, Keepass, LibreOffice, Notepad++, y Zoom.
- Posibilidad de despliegue en tiempo real o programado con una periodicidad.
- Información gráfica que muestre el estado del parque.
- Filtros de búsqueda de parches por búsquedas por CVE (Common Vulnerabilities and Exposures) o por equipo.
- Auditoría de parches no presentes en los equipos
- Control sobre el reinicio de los equipos
- La gestión de parches de seguridad permitirá el control de dependencias de parches, de reinicio de parches y definir un procedimiento para descarga de parches protegidos con contraseña (ejemplo: Java).
- Realizar la función de almacenamiento local de los parches y actualizaciones para compartirlas con el resto de equipos.
- Registro (log) de las acciones relacionadas con las actualizaciones.
- Posibilidad de generar reglas para el parcheo automático, según su criticidad, fabricante y software.
- Detección de aplicaciones fuera del ciclo de actualización del fabricante (EoL).

4.2.4. Módulo para múltiple factor de seguridad

El sistema ofertado dispondrá de un software que permita establecer un segundo factor de seguridad para el acceso a aplicaciones, entre las que estarán incluidas, al menos, Microsoft Office 365, sistemas Windows y la consola de administración del sistema antivirus objeto de este contrato.

El software se basará en una aplicación móvil (disponible para Android e iOS) o tokens hardware de modo que los usuarios de las aplicaciones reciban códigos de acceso de un solo uso para evitar suplantaciones de identidad o accesos no autorizados a las aplicaciones.

4.2.5. Plataforma de gestión de información auditada

El sistema debe generar información forense relacionada con cada equipo, de tal forma que pueda ser explotada posteriormente. La información generada por el sistema de protección se dividirá en tres partes:

1. Información incluida en la consola cloud. El sistema incluirá un informe por cada amenaza detectada en el que se correlacione las acciones que ha ejecutado el proceso o en el contexto en el que ha estado envuelto, por ejemplo, si se ha descargado de Internet o se ha extraído de un fichero comprimido. Se valorará un entorno amigable e intuitivo, sin que para su uso sea necesario un conocimiento amplio de amenazas avanzadas.

1. Información de eventos. Deberá disponer de un sistema SIEM en la nube que permita recopilar datos de los eventos producidos en los procesos. Este deberá almacenar tanto los eventos producidos por amenazas como aquellos que no lo son. El sistema debe ser capaz de gestionar los datos almacenados para poder realizar las funciones normales de un sistema de base de datos, como son: filtrado, agrupaciones o campos calculados. Debe incluir la posibilidad de exportar la información y la posibilidad de realizar gráficos representativos de los datos almacenados. La información que debe almacenar este sistema es, al menos, la siguiente:
    a. Información relacionada con las alertas detectadas en los equipos, debe incluir información de si se produjo la ejecución del proceso o no y de que proceso se trata.
    b. Información de los archivos ejecutables y comprimidos descargados de otras ubicaciones.
    c. Información de los procesos que acceden a ficheros de datos como son, por ejemplo, archivos de Word, Excel, Acrobat PDF, etc. Se valora mucho la posibilidad de saber qué equipos y con qué usuarios han accedido a un archivo concreto, de modo que se puedan detectar posibles fugas de datos.
    d. Información relacionada con los procesos ejecutados en la máquina controlando qué usuarios los lanzan.
    e. Información de las conexiones que se producen desde un equipo, tanto externas como internas, incluyendo el proceso que las realiza.
    f. Información relacionada con los accesos al registro de Windows.
    g. Acciones de interceptación de eventos de los drivers existentes en el sistema operativo (hooks de teclado, pantalla, etc.), así como toda instalación, borrado, modificación y ejecución de “drivers” (controladores de dispositivos del sistema operativo) involucrados en el incidente de seguridad.
    h. Información relacionada con el consumo de ancho de banda relacionado con aplicaciones y usuarios.
    i. Relación de aplicaciones vulnerables en los equipos y cuáles de ellas se están ejecutando.
2. El sistema deberá incluir paneles pre-configurados con información maquetada de las diferentes informaciones que se incluyen en las tablas en bruto. Al menos, incluirá los siguientes paneles:
    a. Procesos ejecutados en las máquinas por fabricante de procesos.
    b. Aplicaciones instaladas y ejecutadas.
    c. Consumo de ancho de banda usado por las aplicaciones y usuarios.
    d. Destino de las conexiones.
    e. Máquinas en las que ha habido acceso de los usuarios.

En base a esta información, también se incluirán alertas que permitan la detección de actividades no deseadas, como la ejecución de diferentes aplicaciones, ancho de banda usado, acceso a determinados equipos, apertura de ficheros, etc.

4.2.6. Servicio de alerta de amenazas (Threat Hunting)

La solución propuesta incluirá un servicio que alerte y tome las medidas correctivas adecuadas cuando sea detectada una actividad anómala en los equipos basada en el comportamiento normal auditado con anterioridad en el parque de equipos.

Este servicio lo ofrecerá el propio fabricante de la solución EDR y por parte de técnicos especializados usando los datos que haya recogido en la auditoría forense, incluyendo, incluso, ataques del tipo “living-off-the-land”.

Se debe poder realizar la alerta y la inclusión en la inteligencia del sistema de protección EDR de las medidas correctivas a realizar.

4. SOPORTE TÉCNICO

El servicio de soporte técnico se extenderá a todos los elementos que componen la solución ofertada, sin límite de incidencias. Se establecerá el mantenimiento y asistencia técnica que permita asegurar el correcto funcionamiento en todos los puestos y servidores del Ayuntamiento.

Se establecerán distintos canales de acceso al soporte, con disponibilidad 24x7x365 (24 horas diarias, 7 días semanales, 365 días al año):

- Soporte telefónico en castellano con recursos, exclusivamente, del propio fabricante.
- Soporte técnico vía email por técnicos certificados en la solución implementada.
- Helpdesk, en el cual se pueda abrir un número ilimitado de incidencias.
- Web de soporte: con acceso a foros, blogs, información sobre últimas amenazas, base de conocimiento sobre virus, etc.

Durante el tiempo de activación del producto, se dará acceso a actualizaciones, mejoras técnicas y parches desarrollados por el fabricante, a fin de que el sistema se mantenga siempre con las últimas actualizaciones.

El fabricante deberá ofrecer herramientas para el análisis online de virus ocultos.