centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo B.2-M: EDR (*Endpoint Detection Response*)

Agosto 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.08.10 10:14:39 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Agosto de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia ***EDR (Endpoint Detection Response)*** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado, desde el punto de vista de la seguridad, para ser empleado en los sistemas de información del sector público para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS) Categoría MEDIA**. Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia ***EDR (Endpoint Detection Response)*** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Debido a que las herramientas anti-virus/EPP no aportan una protección completa, ha surgido una nueva categoría de aplicaciones llamadas EDR (*Endpoint Detection and Response*) que añaden características de seguridad enfocadas a detectar y bloquear el malware desconocido.

7. La funcionalidad de los EDR ha evolucionado a lo largo del tiempo. En su concepto original se trataba de herramientas para monitorizar y observar la ejecución de procesos. Actualmente las herramientas EDR han evolucionado, de tal forma que abarcan parte de las características EPP e incorporan funcionalidades IR (*Incident Response*), hacia una nueva categoría llamada *Next Generation Endpoint Protection Platform* (NGEPP).

2.2 CASOS DE USO

8. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal y como se definen a continuación.

2.2.1. CASO DE USO 1– GESTIÓN CENTRALIZADA

9. Se realiza una gestión centralizada, que permite monitorizar y controlar la ejecución de varias instancias de la aplicación EDR (normalmente llamados Agentes) que se ejecuta sobre un grupo heterogéneo de sistemas.

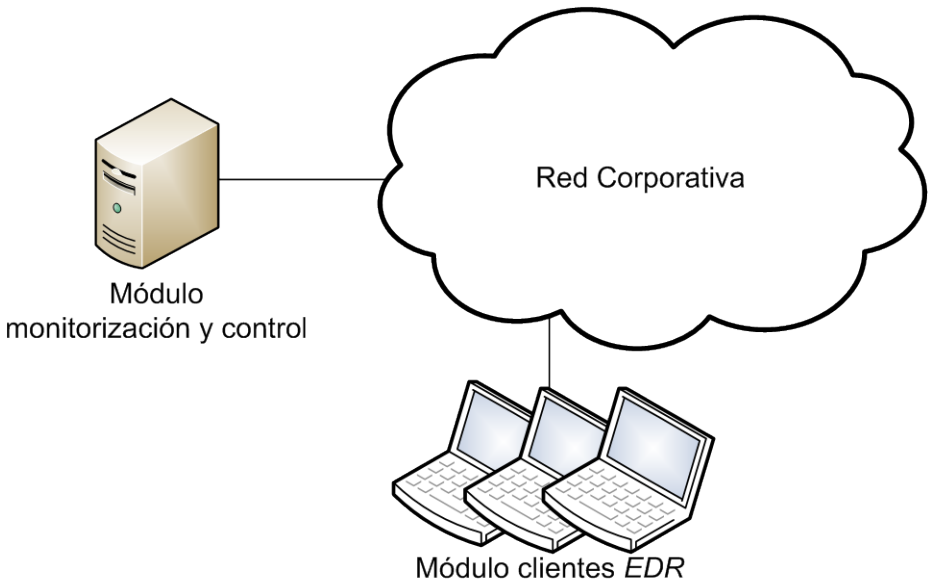

Figura 1 – Ejemplo de Caso de Uso: Gestión centralizada

2.2.2. CASO DE USO 2 - GESTIÓN INDIVIDUALIZADA

10. La gestión es autónoma en cada equipo, la monitorización y control de ejecución de la aplicación EPP/EDR forma parte de la propia aplicación.

2.3 ENTORNO DE USO

11. Para la utilización en condiciones óptimas de seguridad de las herramientas Antivirus/EPP, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
    - **Acceso:** El producto tiene acceso a todos los datos del sistema necesarios para llevar a cabo todas sus funciones.
    - **Administración confiable**: El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
    - **Actualizaciones periódicas:** El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

12. Este tipo de productos son herramientas que suelen presentarse en formato de software que se instala en un sistema de ficheros proporcionado por un sistema operativo. Se ejecutan en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

2.5 CERTIFICACIÓN LINCE

13. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría MEDIA, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

[1] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

14. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

- AC.Comunicación. Comunicaciones del producto.
- AC.Datos. Información almacenada en la plataforma sobre la que se instala y ejecuta el producto.
- AC.Actualizaciones. Actualizaciones del producto y la plataforma susceptible de afectar a la configuración y funcionalidad.

3.2 AMENAZAS

15. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo al caso de uso expuesto en la sección 2.1, serían:

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través de la red entre el producto y otras entidades autorizadas o modificar sus comunicaciones.
- **A.LOCAL. Ataque local.** Un atacante puede actuar a través de software no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante podía acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
- **A.MAL. Malware**. Un agente dañino podría intentar introducir un virus vía red o medios removibles que comprometa el sistema.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

16. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 AUDITORÍA

17. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
18. **AUD.1** El producto deberá generar registros de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:

    a) *Login* y *logout* de personal autorizado.

    b) Cambio en las credenciales de usuarios.

    c) Cambios en la configuración del producto.

    d) Eventos relativos a la funcionalidad de EPP/EDR.
19. **AUD.2** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica).
20. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:

    a) Lectura: sólo usuarios autorizados.

    b) Modificación: ningún usuario.

    c) Borrado: administradores.

4.2 CANALES DE COMUNICACIÓN CONFIABLES

21. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
22. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

4.3 IDENTIFICACIÓN Y AUTENTICACIÓN

23. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional**.
24. **IAU.1** Cada usuario del producto deberá ser autenticado correctamente antes de permitir cualquier otra acción sobre éste.

4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

25. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
26. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del firmware/software, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
27. **ACT.2** El producto deberá ofrecer mecanismos, conforme a la criptografía de empleo en el ENS, a través de hashes o firma digital para autenticar las actualizaciones de firmware/software antes de instalarlas.
28. **ACT.5** El producto deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
29. **ACT.6** El producto no descargará ni modificará su propio código binario.
30. **ACT.7** El producto solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.5 CAPACIDAD ANTI-EXPLOTACIÓN

31. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
32. **EXP.1** Capacidades anti-explotación. El producto se auto-protegerá cuando se encuentre en ejecución, de tal forma que tenga acceso exclusivo a su zona de memoria asignada.
33. **EXP.2** El producto está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

34. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
35. **CRD.1** Almacenamiento de credenciales y datos sensibles. En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.
36. **CRD.2** En el caso en el que el producto utilice sus propias credenciales de acceso, el producto obligará al cambio/establecimiento de credenciales cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales.

4.7 ANTI-VIRUS

37. Esta funcionalidad de seguridad mitiga la amenaza (A.MAL).
38. **MAL.1** Una vez detectado un *malware* basado en memoria, se deberá bloquear su ejecución.

39. **MAL.2** Una vez detectado un *malware* basado en fichero, se deberán tomar las acciones previamente definidas previamente por el administrador (limpiar fichero de virus, poner el fichero en cuarentena, borrar el fichero).
40. **MAL.3** Una vez detectado un *malware*, el producto deberá mostrar una alerta en el equipo donde se ha detectado el virus. Se deberá mostrar el virus detectado y las acciones tomadas.
41. **MAL.4** Una vez detectado un *malware*, el producto deberá alertar al administrador, indicando el nombre del equipo infectado, el *malware* detectado, las acciones tomadas por el producto.
42. **MAL.5** El producto deberá escanear en tiempo real la memoria del sistema para detectar *malware* basado en memoria.
43. **MAL.6** El producto deberá escanear a tiempo real, de forma programada y a demanda para detectar *malware* basados en ficheros.
44. **MAL.7** El producto deberá escanear de forma programada a la hora y frecuencia definida por el administrador.
45. **MAL.8** El producto permitirá escanear de forma manual, a petición de un usuario el equipo donde se ejecuta.
46. **MAL.9** El producto deberá crear alertas basadas en reglas sobre la monitorización de los registros de la actividad del sistema. Dicha monitorización deberá realizarse mediante comparación de firmas, patrones o heurísticas.
47. **MAL.10** El producto deberá monitorizar los ficheros que determine la política de la organización utilizando funciones de resumen admitidas en la guía CCN-STIC-807 Criptología de empleo en el ENS (Categoría MEDIA) como SHA2 o SHA3.
48. **MAL.11** El producto deberá bloquear procesos en ejecución en caso de detectar una posible violación en la seguridad.

4.8 REQUISITOS CRIPTOGRÁFICOS

49. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
50. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría Media del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
51. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.9 NOTAS DE APLICACIÓN

52. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea

proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente.

En el caso de uso 1 – Gestión Centralizada, los requisitos podrán ser de aplicación al Cliente EDR (Agente) y al Módulo de Monitorización y Control (Gestor Central) dependiendo de la arquitectura del producto. Independientemente de lo anterior, todos los requisitos indicados en la tabla anterior deberán formar parte de la declaración de seguridad o *Security Target* asociada a la certificación.

5. ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
EPP	*Endpoint Protection Platform*
EDR	*Endpoint Detection and Reaction*
LINCE	Certificación Nacional Esencial de Seguridad
RFS	Requisitos Fundamentales de Seguridad
TOE	*Target of Evaluation*