GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo B.2: Herramientas EDR

Julio 2018

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.07.10 12:08:57 +02'00'

NIPO: 785-18-034-0.
Publicación incluida en el programa editorial del suprimido Ministerio de la Presidencia y para la Administraciones Territoriales (de acuerdo con la reestructuración ministerial establecida por Real Decreto 355/2018, de 6 de junio).

Fecha de Edición: julio 2018

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 **Herramientas *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 a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). 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 **Herramientas *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 o 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 abarcando parte de las características EPP e incorporando 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 que se ejecuta sobre un grupo heterogéneo de sistemas.

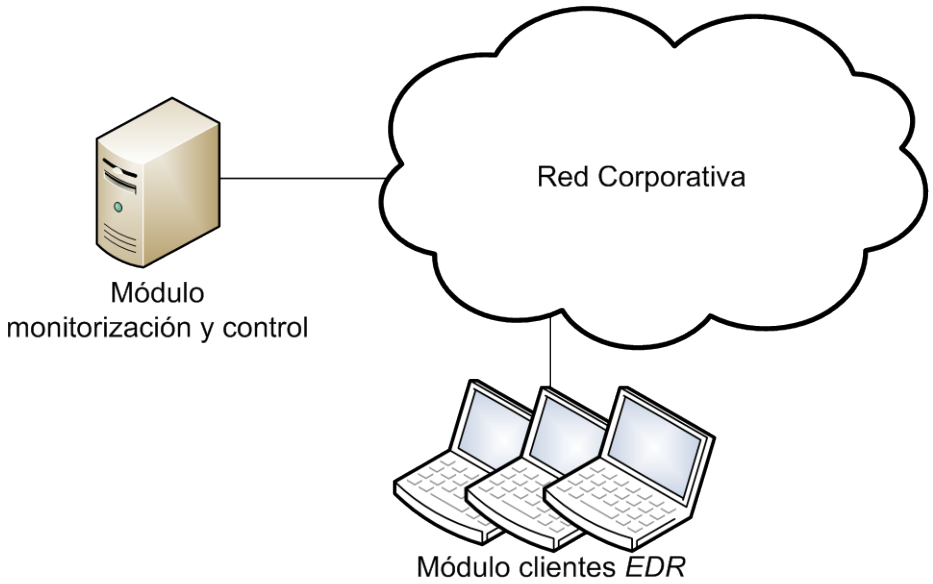

Figura 1 – Ejemplo de Caso de Uso: Gestión centralizada

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 EDR forma parte de la propia aplicación.

2.3 ENTORNO DE USO

11. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público, como parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.
12. Para la utilización en condiciones óptimas de seguridad de los sistemas para la prevención de fuga de datos, 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

13. 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 ejecuta en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

14. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
15. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.

16. Los productos dentro de esta familia deberán cumplir con los SFR (*Security Functional Requirements*) que se especifican en el siguiente perfil de protección certificados de acuerdo a la norma *Common Criteria,* junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[1]	1.2	25/04/2016	NIAP

Tabla 1. Perfil de protección

17. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

- **El determinado por el perfil de protección** para aquellos SFR incluidos en el perfil exigido cuando los productos se encuentren certificados contra éste.
- **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro del perfil.
- **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra el perfil.

[1] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

18. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

    - Comunicaciones con el producto.
    - Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
    - Datos de configuración del producto y de auditoría generados por éste.
    - Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

19. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    - **Ataque a la red.** Un atacante, que acceda al canal de comunicación, puede modificar las comunicaciones entre los distintos módulos del producto.
    - **Monitorización del tráfico.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada entre los distintos módulos de la aplicación.
    - **Ataque local.** Un atacante puede actuar a través de Software 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.
    - **Acceso físico.** Un atacante podía acceder a información sensible almacenada en el sistema.
    - **Auditoria.** Un usuario o proceso podría causar la pérdida o modificación de registros de auditoría del producto de forma maliciosa.
    - **Código dañino.** La instalación de un software en el sistema cuyo objetivo sea dañarlo.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

20. 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 PERFIL DE PROTECCIÓN

21. **REQ. 1** El producto debe cumplir con los SFR (*Security Functional Requirements*) que se especifican el siguiente perfil de protección certificados de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[2]	1.2	25/04/2016	NIAP

Tabla 2. Perfil de protección

22. **REQ. 2** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

23. **REQ. 3** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 (Categoría ALTA).

4.3 REGISTROS AUDITORIA

24. **REQ. 4** Se debe proporcionar un medio para almacenar los eventos relacionados con la seguridad, de forma que permita interpretarse por un usuario.

25. **REQ. 5** 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.

26. **REQ. 6** Se registrarán en la auditoria los siguientes eventos:

    a. Acción tomada en respuesta a una detección de virus.
    b. Detección de virus.

[2] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

c. Iniciar o detener la auditoria de la aplicación.
d. Cambios en el grupo de usuario que tiene el rol de administrador.
e. Utilización por parte del usuario de los mecanismos de autenticación.
f. Cualquier utilización de los mecanismos de autenticación del producto.
g. Cambios de la configuración del producto.

27. **REQ. 7** Los registros de auditoría, no podrán modificarse por ningún usuario.
28. **REQ. 8** Sólo podrán leer los registros de auditoría los usuarios autorizados.
29. **REQ. 9** Los administradores serán los únicos usuarios que puedan borrar registros de auditoría.

4.4 IDENTIFICACIÓN Y AUTENTICACIÓN

30. **REQ. 10** El producto debe mantener una lista de atributos de seguridad perteneciente a cada usuario. Los atributos serán, al menos, los siguientes:
    a. Identificación única de usuario.
    b. Contraseña / método de acceso.
    c. Rol de usuario y su estado actual (habilitado o no).
31. **REQ. 11** El producto requerirá que cada usuario sea autenticado correctamente antes de permitir cualquier otra acción en el producto en nombre de ese usuario.

4.5 CÓDIGO DAÑINO (*MALWARE*)

32. **REQ. 12** Una vez detectado un programa de código dañino basado en memoria, se deberá bloquear su ejecución.
33. **REQ. 13** Una vez detectado un programa de código dañino basado en fichero, se deberán tomar las acciones previamente definidas con anterioridad por el administrador (limpiar fichero de código dañino, poner el fichero en cuarentena, borrar el fichero)
34. **REQ. 14** Una vez detectado un programa de código dañino, el producto deberá mostrar una alerta en el equipo donde se ha detectado el programa. Se deberá mostrar el programa detectado y las acciones tomadas
35. **REQ. 15** Una vez detectado un programa de código dañino, el producto deberá alertar al administrador, indicando el nombre del equipo infectado, el tipo de programa de código dañino detectado, las acciones tomadas por el producto.
36. **REQ. 16** 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.

37. **REQ. 17** 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 ALTA) como SHA2 o SHA3.
38. **REQ. 18** El producto deberá bloquear procesos en ejecución en caso de detectar una posible violación en la seguridad.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
EDR	*Endpoint Detection and Response*
ENS	*Esquema Nacional de Seguridad*
EPP	*Endpoint Protection Platform*
IR	*Incident Response*
NIAP	*National Information Assurance Partnership*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*