Guía de Seguridad de las TIC
CCN-STIC 1010

Procedimiento de empleo seguro
FortiEDR



Noviembre 2026

Edita:





CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

ÍNDICE **2**
1. INTRODUCCIÓN **4**
2. OBJETO Y ALCANCE **4**
3. ORGANIZACIÓN DEL DOCUMENTO **5**
4. FASE PREVIA A LA INSTALACIÓN **6**
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 LICENCIAS 6
4.3 OPCIONES DE SOPORTE 8
4.4 CONSIDERACIONES PREVIAS 8
4.4.1 DESPLIEGUE CLOUD 8
4.4.2 DESPLIEGUE HÍBRIDO 8
4.4.3 DESPLIEGUE ON-PREMISE 9
5. INSTALACIÓN **10**
6. FASE DE CONFIGURACIÓN **11**
6.1 AUTENTICACION 11
6.2 ADMINISTRACIÓN 11
6.2.1 ADMINISTRACIÓN LOCAL 11
6.2.2 ADMINISTRACIÓN REMOTA 12
6.2.3 CONFIGURACIÓN DE USUARIOS 12
6.3 ACTUALIZACIONES 12
6.4 THREAT HUNTING 12
6.5 AUDITORÍA 15
6.6 RETENCIÓN DE LA INFORMACIÓN 15
6.6.1 CONFIGURACIÓN SYSLOG 15
6.7 BACKUP 15
7. FASE DE OPERACIÓN **16**
7.1 REVISIÓN DE ESTADO DE COMPONENTES 16
7.2 REVISIÓN DE ESTADO DE COLECTORES 16
7.3 CONFIGURACIONES ESPCÍFICAS PARA COLECTORES 18
7.4 ACCIONES EN COLECTORES 18
7.4.1 ASIGNAR COLECTORES A UN GRUPO 18
7.4.2 ELIMINAR COLECTORES 18
7.4.3 HABILITAR/DESHABILITAR UN COLECTOR 19
7.4.4 AISLAMIENTO DE DISPOSITIVOS 19
7.4.5 DESINSTALAR COLECTOR 19
7.5 CONFIGURACIÓN DE DIRECTIVAS 21
7.6 CONFIGURACIÓN DE PLAYBOOKS 21
8. REFERENCIAS **25**
9. ABREVIATURAS **26**

ÍNDICE DE FIGURAS

Figura 1 Licencia 7
Figura 2 Arquitectura 8
Figura 3 Sección Threat Hunting 13

1. INTRODUCCIÓN

Los ataques avanzados pueden tardar sólo unos minutos, si no segundos, en comprometer servidores y puestos de usuario. Las herramientas de detección y respuesta de *endpoints* (*Endpoint Detection and Response*, o EDR) de anteriores generaciones simplemente no pueden seguir este ritmo; requieren *triaje* manual y respuestas que no sólo son demasiado lentas para las amenazas de rápido movimiento, sino que también generan un gran volumen de indicadores que saturan a los equipos de seguridad, que normalmente ya están sobrecargados. Además, las herramientas de EDR *legacy* aumentan el coste de las operaciones de seguridad y pueden ralentizar los procesos, lo que afecta negativamente al negocio.

FortiEDR ofrece protección avanzada contra amenazas en tiempo real para *endpoints* tanto antes como después de la infección, con la respuesta a incidentes automatizada y orquestada en cualquier dispositivo, incluidas estaciones de trabajo y servidores, con sistemas operativos actuales y *legacy*, en una única plataforma integrada, con opciones de implementación flexibles (cloud, on-prem, etc.) y un coste operativo predecible.

Con FortiEDR se reduce de forma proactiva la superficie de ataque, previene la infección de malware, detecta y desactiva las amenazas potenciales en tiempo real y puede automatizar los procedimientos de respuesta y corrección con *playbooks* personalizables. FortiEDR ayuda a las organizaciones a detener las brechas en tiempo real de manera automática y eficiente, sin abrumar a los equipos de seguridad con una gran cantidad de falsas alarmas o interrumpir las operaciones de negocio.

Mitigación proactiva de riesgos en tiempo real y seguridad IoT: Permite la reducción proactiva de la superficie de ataque, incluida la evaluación de la vulnerabilidad y el riesgo proactivo, permitiendo establecer controles a las comunicaciones de cualquier aplicación descubierta que contenga vulnerabilidades.

Protección previa a la infección: Proporciona la primera capa de defensa a través de un antivirus de nueva generación (NGAV) basado en aprendizaje automático a nivel de kernel, que evita que la infección malware basado en archivos.

Protección posterior a la infección: FortiEDR es la única solución que detecta y detiene ataques avanzados en tiempo real, incluso cuando el *endpoint* ya ha sido comprometido. Sin brechas de seguridad, sin pérdida de datos. FortiEDR elimina el tiempo de permanencia de la amenaza en el *endpoint*, y proporciona un conjunto de capacidades detección automatizada y respuestas (EDR) para detectar, desactivar, investigar, responder y remediar incidentes.

2. OBJETO Y ALCANCE

En la presente guía se recoge el procedimiento de empleo seguro para que el producto FortiEDR se despliegue y se configure de forma correcta y segura. El producto FortiEDR ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF1].

3. ORGANIZACIÓN DEL DOCUMENTO

El presente documento se divide en las siguientes partes fundamentales, de acuerdo con distintas fases que componen el ciclo de vida del producto:

a) **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
b) **Apartado 5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
c) **Apartado 6.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
d) **Apartado 7.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

El producto se obtiene desde el tentant correspondiente a cada cliente. Por ello, es necesario haber establecido un contrato con Fortinet.

Es Fortinet el encargado de dar al usuario tanto las credenciales de acceso como el enlace para acceder.

Una vez se accede al tenant del usuario, se puede proceder con la descarga del producto, siguiendo los pasos descritos en REF7.

Cabe destacar que este modo de descarga es el mismo para cualquier despliegue, ya sea on-premise o cloud.

El producto implementa las siguientes protecciones para garantizar la autenticidad e integridad tras la descarga:

a) Se solicita la contraseña del usuario que ha descargado el producto, para que de esta manera se verifique no ha sido modificado durante el tránsito.

b) Además, el paquete se encuentra firmado, lo cual garantiza que, si es modificado, la firma no coincidirá y por tanto se puede saber que ha sido modificado.

4.2 LICENCIAS

A continuación, se detallan los pasos para registrar y poner en marcha la licencia contratada de FortiEDR:

Este tema explica cómo implementar FortiEDR en la nube. Se asume que ya has adquirido las licencias de suscripción necesarias para tu implementación a través de un socio o distribuidor de Fortinet y que has recibido los códigos de activación de tus licencias.

Para implementar FortiEDR en la nube:

a) Registra el contrato de suscripción de FortiEDR Cloud en tu cuenta de FortiCloud.
b) En el sitio de **Customer Service & Support**, ve a **Asset Management > Register Now**.
c) En el campo **Registration Code**, ingresa tu código de activación de licencia y selecciona **Next** para continuar con el registro del producto.
d) Ingresa tus datos en los demás campos y completa el proceso de registro.
e) Es posible que tengas que esperar unos minutos a que se cree el tenant para continuar con el procedimiento.

Provisiona tu entorno de FortiEDR en la nube:

a) En FortiCloud, ve a Services > Cloud Services y haz clic en FortiEDR.
b) Haz clic en PROVISION.
c) Selecciona la zona horaria y la región de la nube donde deseas aprovisionar tu instancia de FortiEDR Cloud.
d) Haz clic nuevamente en PROVISION para iniciar el proceso de aprovisionamiento, el cual toma aproximadamente 5 minutos para una organización nueva en un entorno compartido y 40 minutos en un entorno dedicado.
e) Una vez que el proceso de aprovisionamiento haya finalizado y el entorno esté listo, haz clic en Agree para acceder a la consola de FortiEDR Central Manager.

El producto FortiEDR incluye unos servicios prestados directamente por el fabricante denominados BPS (Best Practices Services) De cara a activar la licencia el cliente de FortiEDR BPS se compromete a:

a) Registrar el producto FortiEDR. Esta acción debe hacerse desde el portal forticloud.com del cliente
b) Determinar un punto de contacto único que actúe como interfaz principal con Fortinet.
c) Nombrar al personal (hasta 12 personas) que llevará a cabo el despliegue de los Collectors en los Endpoints Cubiertos y la migración de los Collectores al Modo de Protección (el "Personal Designado por el Cliente"). El Cliente se compromete a que el Personal Designado por el Cliente se mantendrá razonablemente constante durante la duración del Servicio e informará puntualmente a Fortinet sobre cualquier cambio.
d) Presentar el plan de cronograma de implementación del Cliente para la instalación de los Collectores en los Endpoints y la posible migración de los Collectores al Modo de Protección.
e) Comunicar una descripción detallada del entorno del Cliente, los Endpoints Cubiertos y cualquier otra información específica que Fortinet solicite.
f) Proporcionar cualquier otro dato que Fortinet pueda solicitar razonablemente durante la duración del Servicio.
g) Registrar el servicio en la cuenta del portal de soporte del Cliente en el momento de la Reunión de Planificación del Servicio.

A continuación, se adjunta la guía con los primeros pasos para instalación y configuración: [REF2]

En la sección Administration\Licensing el cliente podrá consultar el nivel de licenciamiento contratado, cuántos puestos puede cubrir y cuántos de ellos le quedan disponibles sobre la licencia contratada. Así mismo ciertas funcionalidades no estarán disponible dado el nivel de la licencia:

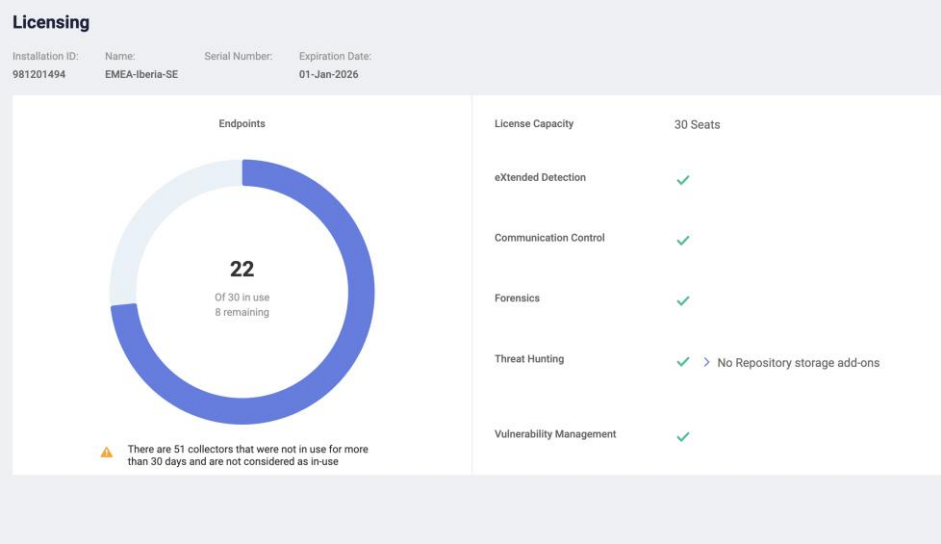


Figura 1 Licencia

4.3 OPCIONES DE SOPORTE

Se recomienda la contratación del servicio de soporte FortiCare para los equipos adquiridos, Fortinet ofrece dos opciones de soporte según cada dispositivo adaptadas a las diferentes necesidades del organismo:

a) FortiCare Premium
b) FortiCare Elite. El servicio Elite proporciona tiempos de respuesta de 15 minutos para las familias de productos clave.

4.4 CONSIDERACIONES PREVIAS

A continuación, se indican las distintas opciones de despliegue soportadas en FortiEDR.

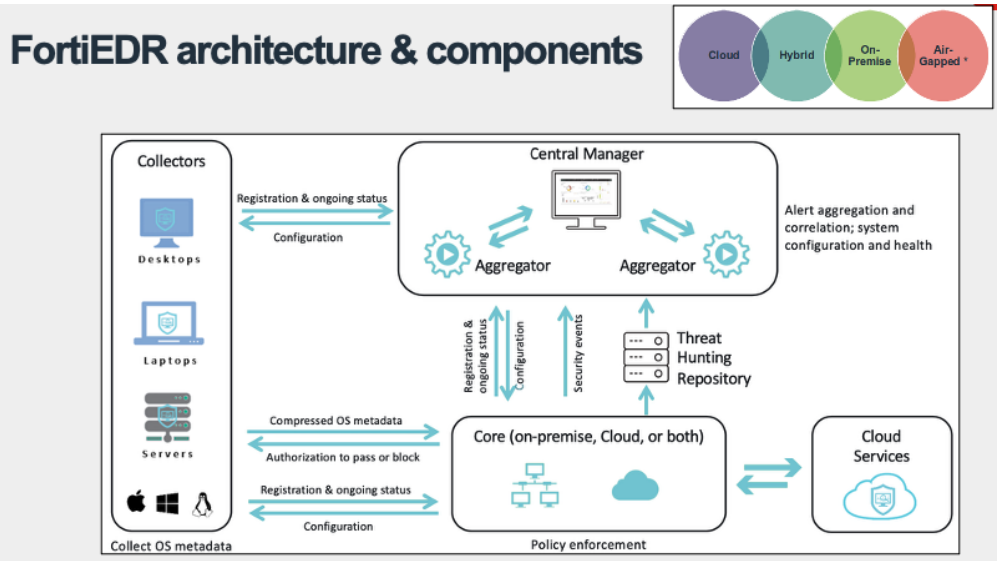


Figura 2 Arquitectura

4.4.1 DESPLIEGUE CLOUD

Es normalmente el modelo de despliegue más solicitado por su sencillez de cara a la administración y mantenimiento. En este caso todos los componentes excepto los colectores (agentes) serán desplegados en infraestructura cloud para ser consumidos como un servicio. **No se encuentra cualificado.**

4.4.2 DESPLIEGUE HÍBRIDO

Si el cliente lo necesita o bien por arquitectura o por cumplimiento de normativas internas. FortiEDR puede desplegarse en formato híbrido, esto es, desplegando ciertos componentes, principalmente cores, directamente en las instalaciones del cliente. **No se encuentra cualificado.**

4.4.3 DESPLIEGUE ON-PREMISE

FortiEDR también, si el cliente lo necesita, puede desplegarse en un formato full on-premise. Esto es desplegando todos los componentes de FortiEDR en las dependencias del cliente. **Se encuentra cualificado.**

Más información sobre los componentes e instalaciones on-premise: REF3

Para funcionar en la configuración evaluada, el producto requiere los componentes operativos que se enumeran en la siguiente tabla:

Componente	Uso
Servidor Syslog	Cualquier servidor syslog al que el producto transmita mensajes syslog a través de TLS.

En cuanto al servidor de Syslog, se puede utilizar cualquiera al que se pueda acceder a través de TLS 1.2. Instale el servidor Syslog siguiendo las instrucciones de instalación que se incluyen con el software del servidor Syslog escogido.

5. INSTALACIÓN

El agente (collector) se instalará siguiendo la guía publicada en el repositorio de documentación pública de Fortinet REF4

Puede revisar en la actual matriz si su sistema operativo está soportado en REF5.

6. FASE DE CONFIGURACIÓN

1. En esta sección facilitaremos las mejores prácticas para la configuración de los agentes (collectors) Para ello es necesario acceder a su consola de gestión a través del enlace que se le facilitó en el proceso de registro.
2. Una vez dentro de la consola, hacemos click en Inventory\Collectors.
3. En este espacio se configurarán los grupos de gestión. La idea es crear grupos en función de las necesidades de sistemas, aplicaciones o unidades de negocio para gestionar la seguridad de los dispositivos.
4. En paralelo a los grupos podemos configurar las directivas de seguridad, para visitar este espacio, debemos hacer click en Security Settings\Security Events\Security Policies.
5. Existen distintos tipos de directivas que se aplican sobre los grupos de trabajo. FortiEDR proporciona un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer nuestros sistemas) como post-ejecución (cuando la amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas. Adicionalmente, en la versión 5 se ha añadido un motor de protección pre-ejecución basado en firmas denominado FortiAV, que añade una capa adicional de protección frente a los ataques más habituales en cada momento.

6.1 AUTENTICACION

FortiEDR permite el acceso a la consola de tres formas:

a) Local User
b) LDAP
c) SAML

En cualquiera de las tres se recomienda habilitar el segundo factor de autenticación. Puede obligar a todos los usuarios de FortiEDR a vincular un 2FA para acceder a la consola. Recomendamos encarecidamente la habilitación de este requisito para segurizar el acceso. Esta acción se realiza en Administration\Users y después en Password Policy. Aquí habilitaremos los siguientes controles en el caso de que se decida optar por la autenticación Local User:

a) Longitud mínima de contraseña: 15
b) Requerir 2FA: Always
c) Marcar la última opción de requerir una contraseña que mezcle minúsculas, mayúsculas, números y símbolos.
d) Habilitar Brute Force Detection.
e) En el caso de utilizar autenticación basada en LDAP o SAML establecer caducidad de contraseñas a 60 días.

6.2 ADMINISTRACIÓN

6.2.1 ADMINISTRACIÓN LOCAL

En el caso de necesitar realizar una intervención local será necesario utilizar el componente FortiEDRCollectorService. Este componente siempre requerirá de la contraseña de registro para poder operar con él. Cualquier actividad realizada incluso por un administrador de sistemas será

considerada como un intento de tampering y será convenientemente bloqueada si no se dispone de dicha contraseña.

6.2.2 ADMINISTRACIÓN REMOTA

FortiEDR sólo puede gestionarse remotamente a través de su propia consola. En este caso todos los comandos enviados desde la consola son apropiadamente cifrados cuando se configura las comunicaciones contra el puerto 559 a través de SSL.

6.2.3 CONFIGURACIÓN DE USUARIOS

FortiEDR facilita una serie de roles para poder dar accesos contenidos a usuarios en función de las necesidades que tengan, siendo siempre la opción de menor privilegio la más recomendable dentro de las necesidades de dicho usuario REF6.

A continuación, se definen los roles de administración:

a) Admin
b) Local Admin
c) Rest API
d) User

6.3 ACTUALIZACIONES

Las nuevas versiones de agente se irán publicando en el tenant cloud del cliente en el siguiente espacio Administration\Licensing\Content.

El despliegue de agentes se hará siempre desde Request Collector Installer, para la actualización usaremos la opción de Update Collectors.

Para organizaciones que quieran tener un control total de los flujos de actualización, se recomienda el siguiente flujo de operaciones. Una vez dentro podremos seleccionar un grupo de control para publicar la actualización, una vez superada esta fase podremos seleccionar otros grupos, así como los restantes para terminar el despliegue de la actualización.

Además, aquellas compañías que deseen tener su parque actualizado lo antes posible pueden marcar la opción de Automatically update Collectors to the latest patch versión.

Una vez configurados los grupos sobre los que se aplica la actualización el proceso puede medirse a través de los dashboards.

6.4 THREAT HUNTING

FortiEDR incluye una consola de Threat Hunting. En un apartado anterior hemos hablado de la conveniencia de configurar distintos perfiles de recolección de telemetría. Es también una buena práctica identificar eventos recursivos que no aportan valor a las labores de detección tales como operaciones de lectura y modificación sobre ficheros contrastados, labores de inventariado o backup por parte de agentes externos. Una correcta adecuación de excepciones en materia de recopilación de eventos garantizará una operativa óptima y hará que los eventos recopilados puedan ser más relevantes de cara a un análisis posterior.

Para identificar eventos recurrentes podemos acceder a la sección de Threat Hunting y desde ahí abrir la ventana de facets, lo cual ayudará a identificar dispositivos u operaciones que tienen una presencia más frecuente:

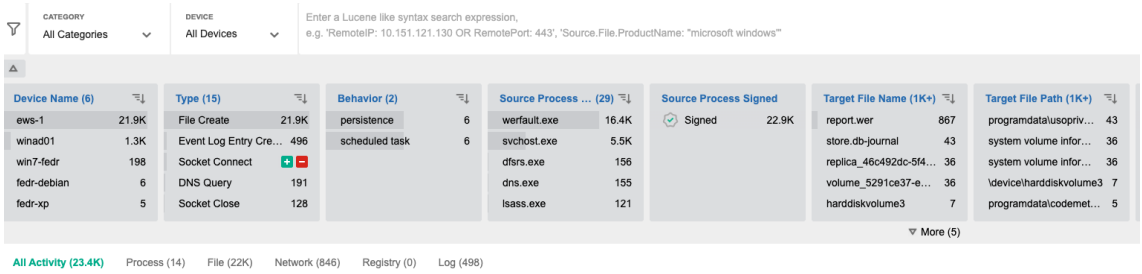


Figura 3 Sección Threat Hunting

Una vez identificado el flujo a excluir debemos irnos a la siguiente sección Security Settings\Threat Hunting\Collection Exclussions

Una vez aquí podemos crear una lista, esa lista se aplicará sobre grupos de colectores a los cuales queramos aplicar esa directiva.

Las exclusiones de threat hunting pueden definirse para:

a) **Origen (proceso)**: Identificado por un atributo de origen, como un firmante (Signer).
b) **Tipo/Acción**: Tipos de eventos de actividad, como se describe en *Threat Hunting*.
c) **Destino (Target)**: Identificado por un atributo de destino, como IP y puerto.

La exclusión puede incluir los tres elementos anteriores o cualquier combinación de ellos. Sin embargo, definir una exclusión que solo contenga un Tipo **no es válido**, ya que este tipo de exclusión debe definirse en un *Perfil de Threat Hunting*.

Por ejemplo, puedes definir una exclusión para eventos de actividad de un Tipo específico que tengan un origen y un destino específicos, o excluir eventos de actividad que tengan un origen específico sin importar la acción o el destino.

Para agregar una exclusión:

a) En el panel izquierdo, haz clic en la **Lista de Exclusiones** a la que deseas agregar la exclusión.
b) En el panel derecho, haz clic en el botón **+ Add Exclusion**. Se mostrará el siguiente formulario:
    i. En el menú desplegable **Operating system**, selecciona el sistema operativo, como **Windows**.
    ii. Para definir que la exclusión incluya un tipo de evento de actividad específico, selecciona el tipo de acción a excluir desde la lista desplegable. También puedes seleccionar la opción **Any** (por defecto), lo cual significa que no estás especificando una acción concreta.
    iii. Todos los tipos de acción disponibles están listados por categoría. Puedes seleccionar una o más acciones dentro de **una misma categoría**, pero **no puedes** seleccionar acciones de categorías diferentes.
    iv. Por ejemplo: puedes seleccionar "Process Termination" y "Process Start" dentro de la categoría de procesos.
    v. Pero no puedes seleccionar "Key Created" y "Thread Created" en una misma exclusión; para ello, debes crear dos exclusiones separadas.

Para definir condiciones de atributo de **Origen:**

a) En la caja de selección, elige **Source attribute**, que puede identificarse mediante:

   i. Nombre de archivo
   ii. Ruta
   iii. Hash
   iv. Firmante (Signer)
   v. Nombre del registro de eventos (para eventos relacionados con logs)

b) Según la opción seleccionada:

   i. **Hash**: especifica el hash.
   ii. **Path**: especifica la ruta (se permiten comodines y puedes marcar la opción de incluir subcarpetas).
   iii. **File Name**: introduce el nombre del archivo.
   iv. **Signer**: puedes subir el certificado del firmante, proporcionar su *thumbprint* o el nombre del firmante.

c) Para definir condiciones de atributo de **Destino:**
   i. Haz clic en el botón **+** y luego selecciona el atributo de destino en la caja de selección.
   ii. Define el criterio del destino, según la categoría del evento:
   iii. Eventos de categoría de **proceso**: identificados por hash, ruta, nombre de archivo o firmante.
   iv. Eventos de categoría de **red**: identificados por IP remota y puerto.
   v. Eventos de categoría de **registro**: identificados por ruta de clave, nombre del valor, tipo o tamaño del valor.
   vi. Eventos de **registro de eventos**: identificados por el ID del evento.

Cuando defines una exclusión con múltiples condiciones, se establece una relación **AND** entre ellas.

Nota: Si necesitas una relación **OR** entre condiciones, simplemente crea otra exclusión separada.

Para finalizar la creación de la exclusión:

a) Haz clic en el botón **Add**.
b) La nueva exclusión aparecerá en la página de **Collection Exclusions**, con un fondo verde y el texto *Pending save* en la columna **LAST UPDATED**.
c) Para que la exclusión entre en efecto, haz clic en **Apply** y luego en **Save** en la ventana emergente.
d) Después de guardar, la columna **LAST UPDATED** mostrará la marca de tiempo.

Para cambiar el estado de una exclusión:

a) El botón **Set State** te permite habilitar o deshabilitar las exclusiones seleccionadas. Por defecto, las exclusiones están habilitadas.

Para eliminar una exclusión:

a) El botón **Delete** permite eliminar las exclusiones seleccionadas.
b) Para eliminar varias exclusiones, marca las casillas correspondientes y haz clic en **Delete** en la barra de herramientas.

6.5 AUDITORÍA

Todas las operaciones realizadas en la consola por parte de los usuarios pueden consultarse a efectos de auditoría. Para acceder a los logs de auditoría tendremos que movernos al siguiente espacio Administration\Settings\Audit Trail, configuramos la ventana de tiempos y descargamos los logs para analizarlos.

6.6 RETENCIÓN DE LA INFORMACIÓN

Para retener la información del producto, tanto eventos de seguridad, eventos del sistema, o registros de auditoría, es posible configurar mecanismos de exportación a través de Syslog.

6.6.1 CONFIGURACIÓN SYSLOG

Para configurar esta funcionalidad deberemos irnos a Administration\Export Settings

Click en Define New Syslog.

a) Configurar nombre: Campo de texto libre que identifica este destino en FortiEDR.
b) Host: IP o FQDN del host .
c) Puerto: Puerto del servidor Syslog.
d) Protocolo: Protocolo del servidor Syslog. Puedes seleccionar **TCP** o **UDP.**
e) TLS: Cuando se selecciona TCP como protocolo, usa esta opción para especificar si deseas habilitar TLS.
f) Si el servidor Syslog requiere un certificado del lado del cliente, debes habilitar TLS antes de poder subir el certificado.
g) Subir certificado de cliente: Si el servidor Syslog requiere un certificado del lado del cliente, habilita **TLS** y utiliza esta opción para cargar el certificado. Por ejemplo, si tu servidor **FortiAnalyzer** requiere un certificado del cliente, contacta con el soporte de Fortinet para obtener los archivos de certificado correspondientes y súbelos aquí.
h) Formato: A elegir entre semicolon, FAZ (para equipos FortiAnalyzer), CEF o LEEF.
i) Seleccionar datos a reenviar: Eventos de seguridad, eventos de sistema y Audit rails.

6.7 BACKUP

Para el despliegue on-premise, el cual es el despliegue cualificado, se recomienda realizar backups periódicos para, en caso de fallo o desastre, se pueda recuperar la información y continuar la normal operación.

7. FASE DE OPERACIÓN

Como parte de las operativas normales dentro de una organización, los clientes pueden apoyarse en distintas vistas para controlar el estado tanto de los componentes como de los colectores (agentes).

7.1 REVISIÓN DE ESTADO DE COMPONENTES

En el caso de una caída de un Core on-premise puede obternerse más información en la siguiente vista: Inventory\System Components

Para obtener más detalle sobre los eventos ocurridos como última conexión debemos visitar Administration\System Events

7.2 REVISIÓN DE ESTADO DE COLECTORES

En el dashboard de FortiEDR se va mostrando información en tiempo real sobre los colectores, si están encendidos o apagados o si tienen alguna acción pendiente, así como vistas en base a Sistema Operativo o versión del colector desplegada, podremos alternar las vistas de estos widgets para obtener información de un simple vistazo.

Para poder operar a un nivel más detallado, deberemos visitar la sección Inventory\Collectors. Aquí los colectores se gestionan por grupos, todo grupo debe tener asignada al menos una directiva de protección y/o control. Cuando existan grupos que no cumplan estas condiciones y que, por lo tanto, impliquen un riesgo para la organización, se señalizarán con iconos especiales para alertar sobre el riesgo de seguridad.

A continuación, se muestra un detalle de todas las opciones que pueden observarse en el panel de gestión de colectores.

La página COLLECTORS muestra una lista de los Grupos de Collectors previamente definidos, los cuales se pueden expandir para ver los FortiEDR Collectors que contiene cada uno.

Puedes definir grupos de Collectors adicionales, como se describe en la sección Definición de un nuevo Grupo de Collectors.

Los Collectors de FortiEDR se registran automáticamente en el sistema después de su instalación.

Por defecto, cada Collector de FortiEDR se agrega al grupo de Collectors llamado "All" (Todos).

Puedes mover cualquier Collector a otro grupo, como se explica en la sección Asignar Collectors a un Grupo de Collectors.

El Grupo de Collectors predeterminado (al que se agregan automáticamente los nuevos Collectors) está marcado con un icono de grupo amarillo.

Puedes cambiar el grupo predeterminado haciendo clic en el icono de grupo de otro Grupo de Collectors.

Haz clic en el icono de expansión para desplegar la lista y mostrar los FortiEDR Collectors que contiene ese grupo.

Se recomienda que, una vez transcurridas las fases iniciales de despliegue, los grupos como el default group tengan directivas configuradas en bloqueo por defecto. Existe un gran riesgo en desplegar un nuevo agente o grupo de agentes y que quede de forma descontrolada sin

protección durante mucho tiempo. Por lo que se recomienda que todos estos grupos por defecto tengan una directiva restrictiva de base.

A continuación, se detalla la información proporcionada para cada **Collector**.

a) Casilla de verificación (Checkbox): Marca esta casilla para seleccionar el Collector. Luego puedes utilizar uno de los botones en la parte superior izquierda de la ventana, como el botón Eliminar (Delete).
b) Nombre del Grupo de Collectors (Collector Group Name): Especifica el nombre del grupo al que está asignado el Collector.
c) Nombre del Dispositivo (Device Name): Especifica el nombre del dispositivo desde el cual se comunica el Collector de FortiEDR instalado.
d) Último Usuario Conectado (Last Logged): Muestra el último usuario que inició sesión en el dispositivo donde está instalado el Collector. Se muestra como dominio/nombre de usuario.
    i. Si nadie ha iniciado sesión en el dispositivo, esta columna aparece vacía.
    ii. Además, si el Collector no tiene la versión V3.0.0.0 o superior, esta columna también estará vacía y los eventos de seguridad no incluirán el usuario desde el cual se disparó el evento.
e) Sistema Operativo (OS): Indica el sistema operativo del dispositivo desde el cual se comunica el Collector.
f) Dirección IP (IP): Especifica la dirección IP del dispositivo donde está instalado el Collector de FortiEDR.
g) Dirección MAC (MAC Address): Especifica la dirección física del dispositivo.
    i. Si el dispositivo tiene múltiples direcciones MAC, se mostrarán tres puntos suspensivos (…).
    ii. Puedes colocar el cursor sobre la dirección MAC para ver el valor o los valores (en caso de múltiples direcciones) en un tooltip.
h) Versión (Version): Especifica la versión del FortiEDR Collector instalada en el dispositivo que se comunica con el sistema.
i) Estado (State): Especifica el estado actual del FortiEDR Collector. Al colocar el cursor sobre el valor del estado (STATE), se muestra la última vez que el estado cambió.

Los posibles valores del estado son los siguientes:

a) Running: El FortiEDR Collector está en ejecución y todo funciona correctamente
b) Disconnected: El dispositivo está **fuera de línea**, **apagado** o **no está conectado** al Aggregator de FortiEDR.
c) Disconnected (Expired): El dispositivo **no se ha conectado durante 30 días o más** de forma consecutiva. Los Collectors en este estado **no se cuentan** para efectos de licenciamiento.

Para ver la lista de Collectors en este estado:

a) Haz clic en la **flecha hacia abajo** en el **cuadro de búsqueda** (Search) ubicado en la parte superior derecha de la ventana.
b) Se mostrará una ventana donde puedes filtrar por estado y visualizar únicamente los dispositivos con ese estado.
c) A continuación, se listan los estados junto a su descripción:
    i. Pending Reboot: Después de instalar el FortiEDR Collector, algunos dispositivos pueden necesitar un reinicio antes de que el Collector pueda comenzar a ejecutarse. Este estado indica que el Collector está listo para

ejecutarse tras el reinicio del dispositivo. El reinicio se realiza normalmente desde el propio dispositivo.

ii. Disabled: Indica que este Collector ha sido deshabilitado desde FortiEDR Central Manager. (Nota: esta función aún no está disponible en la versión 1.2).

iii. Degraded: Indica que el Collector no puede funcionar a plena capacidad, por ejemplo, por falta de recursos en el dispositivo o problemas de compatibilidad.

iv. Last Seen: Cuenta la cantidad de días transcurridos desde la última vez que este Collector se comunicó con el núcleo (Core) del sistema.

7.3 CONFIGURACIONES ESPCÍFICAS PARA COLECTORES

A la hora de desplegar un colector se entiende que este puede tener necesidades específicas, por lo que se han incluido opciones de despliegue adicionales dentro de la configuración del paquete de instalación. Esto puede encontrarse en Administration\Licensing\Content\Request Collector Installer

a) Seleccionar Sistema Operativo entre Windows, MacOS y Linux.
b) Configurar Dirección de Aggregator, sólo en el caso de grandes clientes o infraestructuras híbridas se puede seleccionar un aggregator específico para centralizar comunicaciones en un único punto.
c) Organization, este campo sólo se rellena cuando el entorno del cliente dispone de funcionalidad multi-tenant o multi-entidad.
d) Grupo, por defecto los collectores sin configuración establecida en este campo irán a parar al Default Group.
e) Una vez desplegamos advanced podemos configurar:
    i. VDI: Para Virtual Desktop Infrastructure
    ii. Citrix PVS
    iii. Use system Proxy settings: Utilizar esta configuración para que FortiEDR aplique las configuraciones del sistema a la hora de establecer el proxy.
f) Habilitar integración con Windows Security Center: Para configurar esta integración debemos visitar el espacio de Administration\Settings\Windows Security Center
g) Habilitar Descubrimiento IoT: Podemos encontrarlo también en Administration\Settings\IoT Discovery

7.4 ACCIONES EN COLECTORES

7.4.1 ASIGNAR COLECTORES A UN GRUPO

Como ya se ha tratado anteriormente la forma de aplicar directivas a un colector/colectores es a través de los grupos por lo que será necesario asignar las directivas a los grupos, así como los colectores a dicho grupo, para ello una de las opciones que podemos encontrar en Inventory\Collectors es asignar a un grupo.

7.4.2 ELIMINAR COLECTORES

Eliminar un Grupo de Collectores simplemente significa que estás eliminando una agrupación lógica de Collectores. Estos Collectores no se eliminan del sistema, sino que pasan a estar disponibles dentro del Grupo de Collectors predeterminado.

Nota: No se puede eliminar el grupo que está asignado como Grupo de Collectors predeterminado.

Eliminar un Collector solo lo elimina de la consola del FortiEDR Central Manager.

Si el FortiEDR Collector no ha sido desinstalado en el dispositivo, volverá a aparecer automáticamente en la lista de COLLECTORES del Central Manager.

7.4.3 HABILITAR/DESHABILITAR UN COLECTOR

Puedes habilitar o deshabilitar varios colectores al mismo tiempo desde la página de COLECTORES en FortiEDR Central Manager.

Para habilitar uno o más colectores simultáneamente:

a) En la página COLECTORES, selecciona las casillas de los colectores que deseas habilitar. Todos los colectores seleccionados deben estar en estado Deshabilitado.
b) Haz clic en la flecha hacia abajo del botón Habilitar/Deshabilitar y selecciona Habilitar. Este botón solo estará disponible si se ha seleccionado al menos un colector.

Para deshabilitar uno o más colectores simultáneamente:

c) En la página COLECTORES, selecciona las casillas de los colectores que deseas deshabilitar. Todos los colectores seleccionados deben estar en estado En ejecución.
d) Haz clic en la flecha hacia abajo del botón Habilitar/Deshabilitar y selecciona Deshabilitar.
e) Aparecerá un **mensaje de confirmación** antes de aplicar los cambios.

7.4.4 AISLAMIENTO DE DISPOSITIVOS

Un dispositivo aislado es aquel que está bloqueado para comunicarse con el mundo exterior, tanto para enviar como para recibir datos.

Un dispositivo puede ser aislado manualmente desde:

a) La página Inventario > Colectores, o
b) La vista de Investigación (Investigation View).

Para aislar un dispositivo desde la página Inventario > Colectores:

a) En la página COLECTORES, selecciona la(s) casilla(s) de los colectores de FortiEDR que deseas aislar.
b) Haz clic en la flecha hacia abajo del botón Aislar y selecciona Aislar.

7.4.5 DESINSTALAR COLECTOR

Puedes desinstalar un colector de FortiEDR utilizando los siguientes métodos:

7.4.5.1 DESDE EL CENTRAL MANAGER: INVENTORY > COLLECTORS

Ve a la página INVENTORY > Colectors.

a) Selecciona la casilla del colector que deseas desinstalar.
b) Haz clic en el botón o menú correspondiente para iniciar la desinstalación.
c) A través de la gestión de aplicaciones del sistema operativo: Por ejemplo, **Agregar o quitar programas** en **Windows**.

7.4.5.2 USANDO SCRIPTS DEDICADOS DE FORTIEDR

A continuación, se describe cómo desinstalar un colector utilizando scripts de Fortinet:

Windows:

a) Desinstala el colector ejecutando uno de los siguientes comandos como **administrador**. Reemplaza REGPWD con la contraseña de registro usada durante la instalación (disponible en "Component authentication").

```
msiexec.exe /x GUID /qn UPWD=REGPWD RMCONFIG=1 /l*vx log.txt
```

b) Reemplaza GUID con la **clave de desinstalación** de FortiEDR. Para encontrarla:
c) Haz clic en **Inicio > Ejecutar**.
d) Escribe regedit para abrir el Editor del Registro.
e) Navega a: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
f) Expande las subclaves de **Uninstall** y busca "FortiEDR".
g) Abre la subclave correspondiente y copia el valor de UninstallString, por ejemplo: {01C88AE6-6782-4798-81C6-954E0D14FCF5}.
h) Cierra el Editor del Registro.
i) También puedes usar este comando alternativo:

```
msiexec /x FortiEDRCollectorInstaller_X.msi /qn UPWD=REGPWD
RMCONFIG=1
```

j) **Nota**: Debes ejecutar este comando desde el mismo directorio donde se encuentra el archivo .msi, o usar la ruta completa, por ejemplo: *C:\Users\Allen\Desktop\FortiEDRCollectorInstaller64_4.1.0.491.msi*

macOS:

a) Para desinstalar el colector en macOS **anteriores a Big Sur (11)**, como Catalina o Mojave:

```
sudo /Library/FortiEDR/fortiedr_uninstaller.sh 'CONTRASEÑA DE
REGISTRO'
```

b) Para colectores con versiones anteriores a 6.0:
c) Ejecuta el siguiente comando en Terminal (reemplaza 'CONTRASEÑA DE REGISTRO' por la usada en la instalación): */Applications/FortiEDR.app/fortiedr_uninstaller.sh 'CONTRASEÑA DE REGISTRO'*
d) Para colectores con versión 6.0: */Applications/FortiEDR.app/Contents/Library/LaunchServices/fortiedr_uninstaller.sh 'CONTRASEÑA DE REGISTRO'*

Linux:

a) **Verifica el estado del colector:**

```
/opt/FortiEDRCollector/control.sh –status
```

b) El colector debe estar detenido antes de ejecutar el comando de desinstalación.

c) **Si no está detenido, detén el colector con:**

```
/opt/FortiEDRCollector/control.sh --stop <contraseña_de_registro>
```

d) Ejemplo:

```
/opt/FortiEDRCollector/control.sh --stop 12345678
```

e) Desinstala el colector según la distribución:

f) **CentOS, RHEL, Oracle, AMI, SLES**:

```
yum remove <nombre_del_paquete> o rpm -qa | grep -i fortiedr | xargs
rpm -e
```

g) **Ubuntu**:

```
sudo dpkg --purge fortiedrcollectorinstaller
```

7.5 CONFIGURACIÓN DE DIRECTIVAS

FortiEDR analizará las directivas aplicadas y mostrará señales de advertencia cuando alguna de las directivas de prevención no esté asignada al grupo.

Si se han realizado modificaciones muy drásticas sobre la seguridad de la directiva siempre se puede revertir la directiva a su estado original, para ello tenemos que ir al espacio dentro de Security Settings\Security Events\Security Policies. Seleccionar la directiva en cuestión, desplegar Advanced Data and Rule Data, click en factory settings, Reset Policy.

En cada una de las directivas de seguridad pueden modificarse las reglas a las siguientes acciones:

a) Acciones:
   i. Bloqueo: Se recomienda siempre que sea posible dejar las reglas en bloqueo para un nivel mayor de seguridad
   ii. Log: Registrar la acción, pero no bloquearla (No recomendado)

b) Estado:
   i. Habilitado: Las reglas que tengan este estado (por defecto) se consideran habilitadas y por lo tanto aplicarán las acciones configuradas.
   ii. Deshabilitado: Se puede deshabilitar las reglas y en este caso no se procesarían en el sistema (No recomendado)

7.6 CONFIGURACIÓN DE PLAYBOOKS

En paralelo a las directivas de seguridad se pueden asociar acciones adicionales de acción extendida en base al veredicto de una acción analizada por FortiEDR. Las acciones a realizar son las siguientes:

a) Notificaciones

b) Investigación

c) Remediación

d) Custom

Las **acciones de notificación** envían una notificación cuando se desencadena un evento de seguridad con una clasificación específica. Estas acciones se implementan en ambos modos de FortiEDR (**Simulación** y **Prevención**).

Las notificaciones pueden ser de los siguientes tipos:

a) Correos electrónicos
b) Syslog
c) Apertura de ticket

Cada fila en la sección Notificaciones corresponde a un tipo único de notificación (notificación por correo electrónico, notificación Syslog o notificación de apertura de ticket). En el área de Notificaciones, puedes configurar cada tipo de notificación para indicar si se debe enviar automáticamente la notificación correspondiente cuando se desencadene un evento de seguridad.

Las columnas **Malicioso**, **Sospechoso**, **PUP** (programa potencialmente no deseado), **Inconcluso** y **Probablemente Seguro** corresponden a las posibles clasificaciones (consulta Detalles de Clasificación y el panel de Eventos) de un evento de seguridad. Cuando aparece una marca de verificación en una de estas columnas, significa que se enviará una notificación del tipo especificado cuando se genere un evento con esa clasificación.

De forma predeterminada, la política del Playbook por defecto está configurada en modo Simulación, con envío de notificaciones por correo electrónico para todos los eventos de seguridad, excepto aquellos clasificados como Seguros.

Las acciones de investigación te permiten aislar un dispositivo o asignarlo a un grupo de colectores de alta seguridad, con el fin de investigar más a fondo la actividad del dispositivo en cuestión.

Las acciones de investigación pueden ser uno de los siguientes tipos:

a) Aislar dispositivo con colector
b) Aislar dispositivo con NAC
c) Mover dispositivo a un grupo de alta seguridad

Todas las acciones de investigación se realizan basándose en el resultado de clasificación inicial por el Core, sin considerar una posible reclasificación por el FortiEDR Cloud Service (FCS). Por ejemplo, si se desencadena un evento de seguridad con la acción de aislar un dispositivo que el Core ha clasificado como Inconcluso, el dispositivo se aísla inmediatamente, incluso si luego el FCS lo reclasifica como Seguro.

Aislar dispositivo con colector: Esta acción bloquea la comunicación hacia/desde el colector afectado. Esta acción solo aplica para colectores de endpoint. Por ejemplo, si la política del Playbook está configurada para aislar el dispositivo ante un evento malicioso, entonces cada vez que se desencadene un evento de seguridad clasificado como malicioso desde un dispositivo, ese dispositivo será aislado (bloqueado) para comunicarse con el mundo exterior (tanto para enviar como para recibir). Esto significa, por ejemplo, que aplicaciones que se comunican con el exterior, como Google Chrome, Firefox, etc., serán bloqueadas para comunicaciones salientes.

Una marca de verificación en una columna de clasificación aquí significa que el dispositivo se aísla automáticamente cuando se desencadena un evento de seguridad con esa clasificación.

Aislar dispositivo con NAC: Esta acción bloquea la comunicación hacia/desde el dispositivo afectado deshabilitando este host en un sistema externo de Control de Acceso a la Red (NAC). Para realizar esta acción, debe estar configurado previamente un conector NAC. Para más detalles sobre cómo configurar conectores NAC, consulta la integración de Control de Acceso a la Red (NAC).

En el menú desplegable junto a la acción, puedes especificar qué NAC usar para deshabilitar el host o seleccionar todos ellos.

Mover dispositivo al Grupo de Alta Seguridad. FortiEDR proporciona dos Grupos de Colectores predeterminados: el Grupo de Colectores Predeterminado y el Grupo de Colectores de Alta Seguridad. Ambos grupos predeterminados están asignados inicialmente a la política Default Playbook y no pueden ser eliminados.

Una marca de verificación en una columna de clasificación significa que el dispositivo se mueve automáticamente (se asigna) al Grupo de Colectores de Alta Seguridad cuando se activa un evento de seguridad con esa clasificación. Esta función es útil cuando se desea marcar los Colectores que han activado eventos maliciosos.

Las acciones de remediación te permiten solucionar una situación en el sistema FortiEDR, en caso de que se detecte malware en un dispositivo.

Todas las acciones de remediación de FortiEDR se basan en la clasificación final de un evento de seguridad por parte del Servicio en la Nube de FortiEDR (FCS), que es un servicio basado en la nube, solo de software, que determina con alta precisión la clasificación exacta de los eventos de seguridad.

Terminar Proceso: Esta acción termina el proceso afectado. No garantiza que el proceso afectado no intente ejecutarse nuevamente. Esta acción también puede realizarse manualmente usando el complemento de Forense, como se describe en Remediación de un dispositivo tras la detección de malware.

Una marca de verificación en una columna de clasificación significa que el proceso afectado se termina automáticamente en el dispositivo cuando se activa un evento de seguridad con esa clasificación.

Eliminar archivo: Esta acción garantiza que el archivo no intente exfiltrar datos nuevamente, ya que el archivo se elimina permanentemente del dispositivo. Esta acción también puede realizarse manualmente usando el complemento de Forense, como se describe en Remediación de un dispositivo tras la detección de malware.

Una marca de verificación en una columna de clasificación significa que el archivo afectado se elimina automáticamente en el dispositivo cuando se activa un evento de seguridad con esa clasificación.

Limpiar datos persistentes: Esta acción limpia las claves del registro en Windows. Esta acción también puede realizarse manualmente usando el complemento de Forense, como se describe en Remediación de un dispositivo tras la detección de malware.

Una marca de verificación en una columna de clasificación significa que la clave de registro afectada se limpia automáticamente en el dispositivo cuando se activa un evento de seguridad con esa clasificación.

Bloquear dirección en Firewall: Esta acción garantiza que se bloqueen las conexiones a direcciones remotas maliciosas asociadas con el evento de seguridad. Para realizar esta acción,

debe estar configurado un Conector de Firewall. Para más detalles sobre cómo configurar conectores de firewall, consulte Integración de Firewall en Integración de Firewall.

En el menú desplegable junto a la acción, puede especificar qué firewalls se usan para realizar el bloqueo o seleccionar todos ellos.

Personalizado: Las acciones personalizadas te permiten activar automáticamente una respuesta a incidentes en un sistema de terceros como resultado de un evento de seguridad detectado por FortiEDR, según el conector de Integración Personalizada (y sus acciones) que definas.

8. REFERENCIAS

[REF1] Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

[REF2] https://docs.fortinet.com/document/fortiedr/6.2.0/administration-guide/856850/deploying-fortiedr-cloud

[REF3] https://docs.fortinet.com/document/fortiedr/6.2.0/administration-guide/838338/appendix-c-on-premise-deployments

[REF4] https://docs.fortinet.com/document/fortiedr/6.2.0/administration-guide/186029/installing-fortiedr-collectors

[REF5] https://docs.fortinet.com/document/fortiedr/6.2.0/collector-system-requirements/633631/supported-operating-systems

[REF6] https://docs.fortinet.com/document/fortiedr/6.2.0/administration-guide/776468/users

[REF7] https://docs.fortinet.com/document/fortiedr/6.0.0/administration-guide/204791/requesting-and-obtaining-a-collector-installer

9. ABREVIATURAS

2FA	Two Factor Authenticaton
API	Application Programming Interface
CCN	Centro Criptológico Nacional
EDR	Endpoint Detection and Response
ENS	Esquema Nacional de Seguridad
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
IoT	Internet of Things
LDAP	Lightweight Directory Access Protocol
NAC	Network Access Control
NGAV	New Generation Anti-Virus
OS	Operative System
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
STIC	Sistemas y Tecnologías de Información y Comunicaciones
TCP	Transport Control Protocol
TLS	Transport Layer Protocol
UDP	User Datagram Protocol