POLICIA FEDERAL ARGENTINA

FortiEDR

Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Tabla de contenido

Requisitos mínimos de hardware

FortiEDR Collector se puede instalar en cualquiera de los siguientes sistemas operativos (versiones de 32 y 64 bits):

Procesador: Intel o AMD x86, tanto de 32 bits como de 64 bits, y en hardware Apple M1 (ARM).

RAM: 350 MB de RAM.

Disco: 750 MB a 1GB.

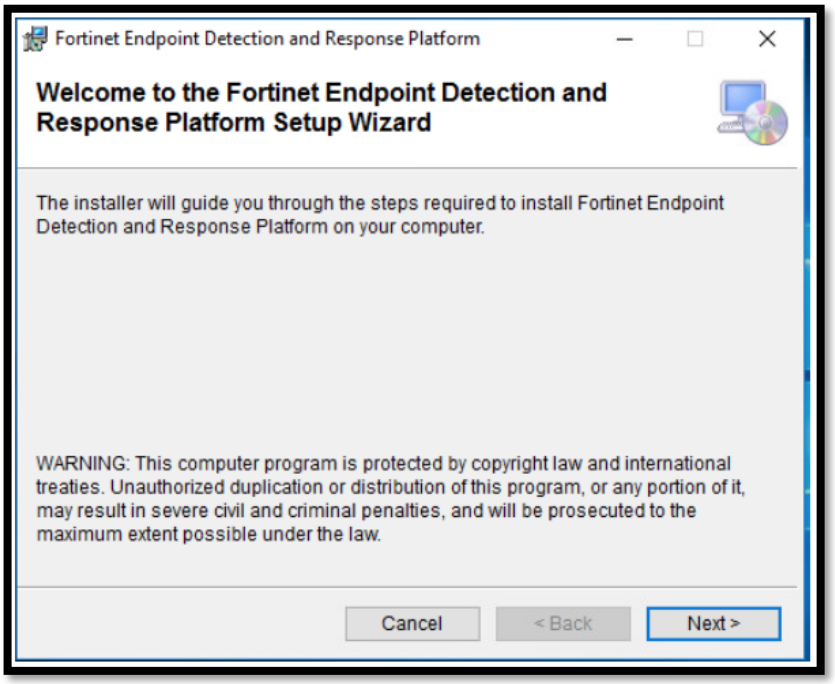
Sistemas Operativos:

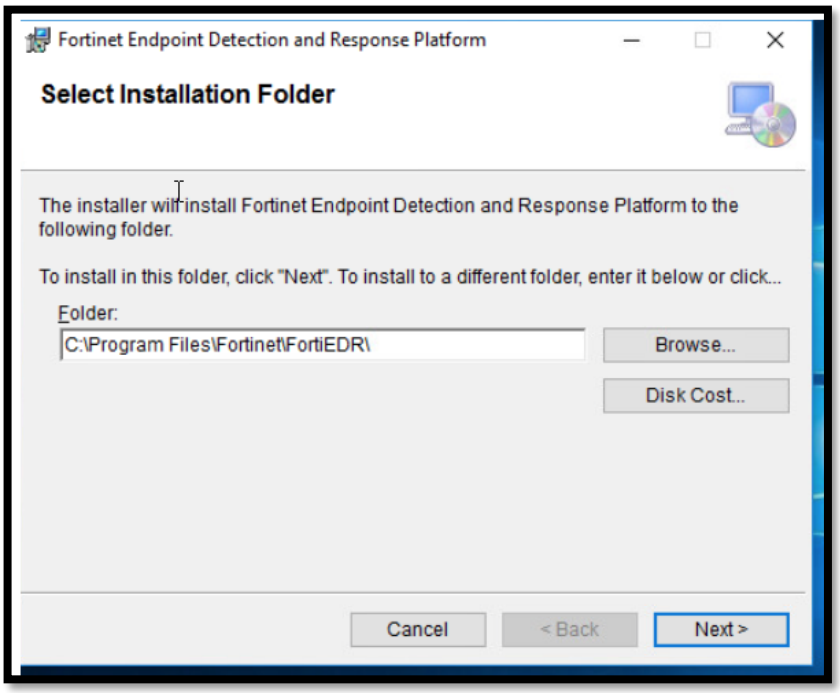
Windows desktop	Windows server	macOS	Linux	VDI environments
• Windows 11 • Windows 10 • Windows 8.1 • Windows 8 • Windows 7 SP1 • Windows XP SP2/SP3	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 SP2 • Windows Server 2008 SP1 • Windows Server R2 SP2 • Windows Server 2003 SP2	• El Capitan (10.11) • Sierra (10.12) • High Sierra (10.13) • Mojave (10.14) • Catalina (10.15) • Big Sur (11) • Monterey (12) • Ventura (13) • Sonoma (14)	• RedHat Enterprise Linux (RHEL) • CentOS 6.8+, 7.2+, 8+, and 9 • Ubuntu LTS 16.04.5+, 18.04/20.04/22.04 server, 64-bit • Oracle Linux 6.10, 7.7+, and 8.2+ • Amazon Linux AMI 2 2018 • SUSE Linux Enterprise Server SLES v12 SP5 and v15 • Open SUSE Leap 15.2 • RedHat 9	• VMware Horizons 6 and 7 • Citrix XenDesktop 7

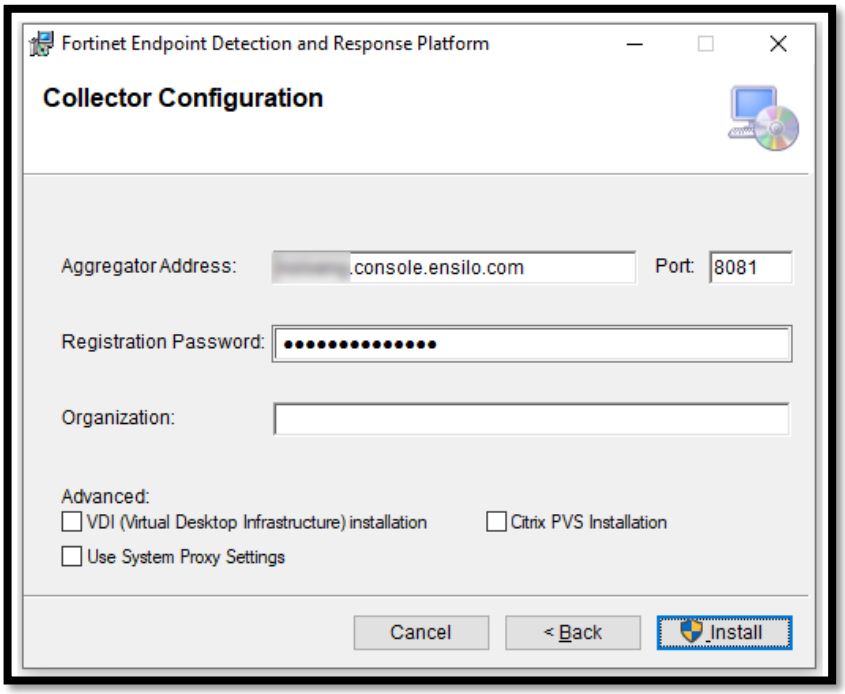
En algunas plataformas Linux, el recopilador puede ejecutarse en modo de aplicación en lugar de en modo kernel. https://community.fortinet.com/t5/FortiEDR/Technical-Tip-Linux-Application-Features-and-Limitations/ta-p/218506

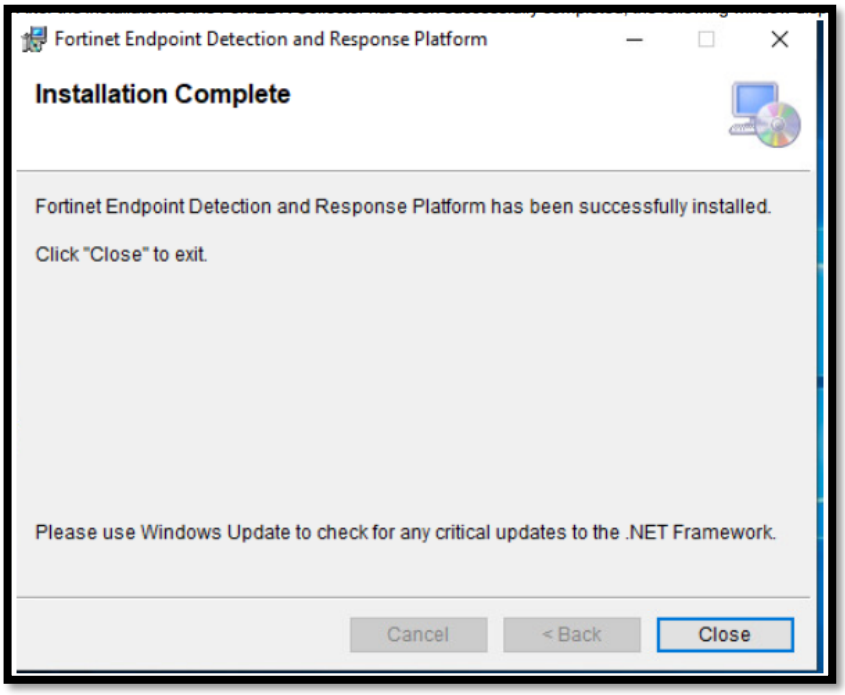
Instalación en Windows

Al contar con un instalador configurador el técnico solo debe hacer clic en siguiente e instalar.

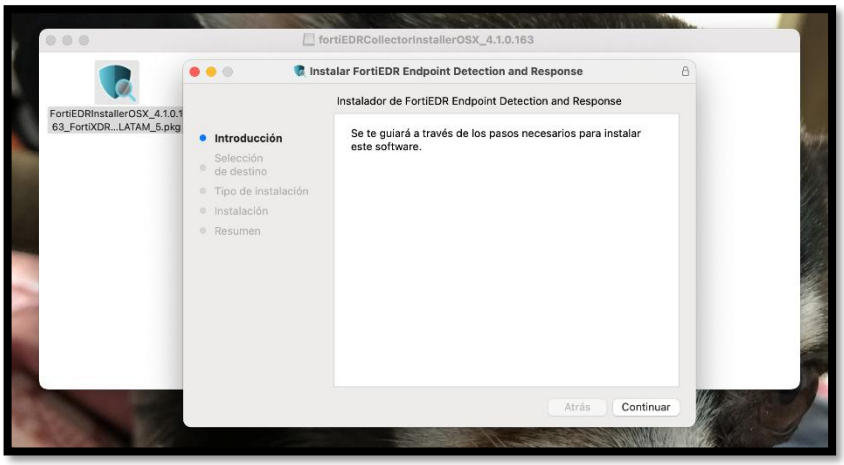


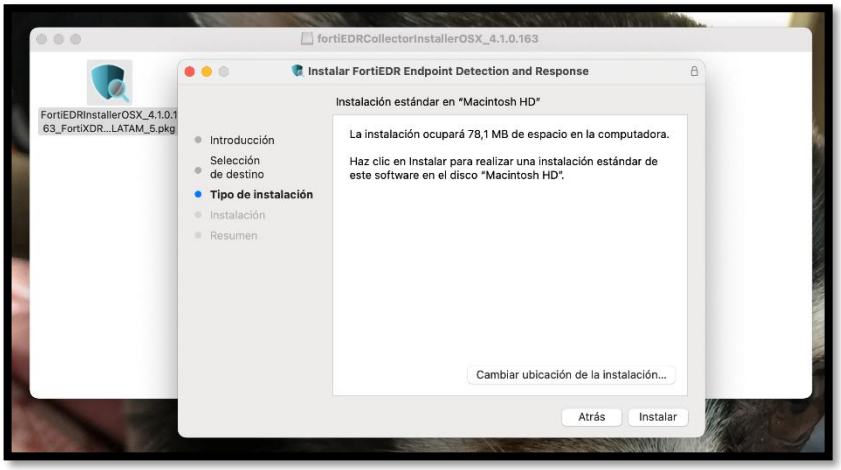



Fortinet Endpoint Detection and Response Platform
Collector Configuration
Aggregator Address:
.console.ensilo.com
Port:
8081
Registration Password:
Organization:
Advanced:
VDI (Virtual Desktop Infrastructure) installation
Citrix PVS Installation
Use System Proxy Settings
Cancel
< Back
Install

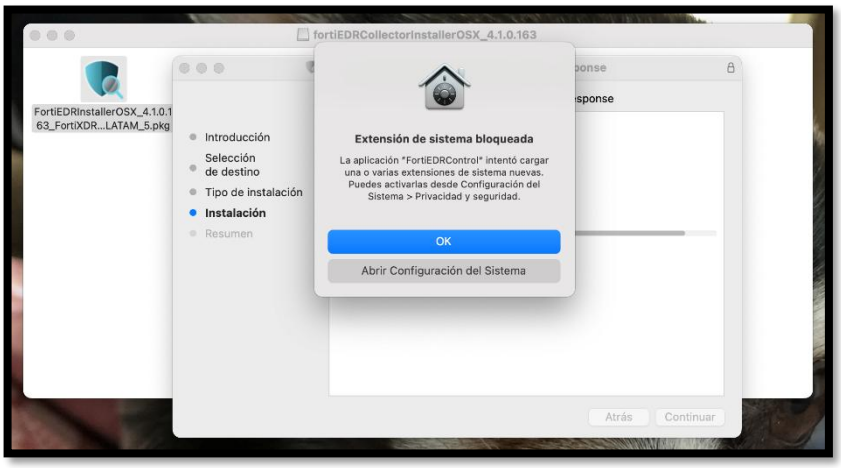

Fortinet Endpoint Detection and Response Platform
Installation Complete
Fortinet Endpoint Detection and Response Platform has been successfully installed.
Click "Close" to exit.
Please use Windows Update to check for any critical updates to the .NET Framework.
Cancel
< Back
Close

Instalación en macOS

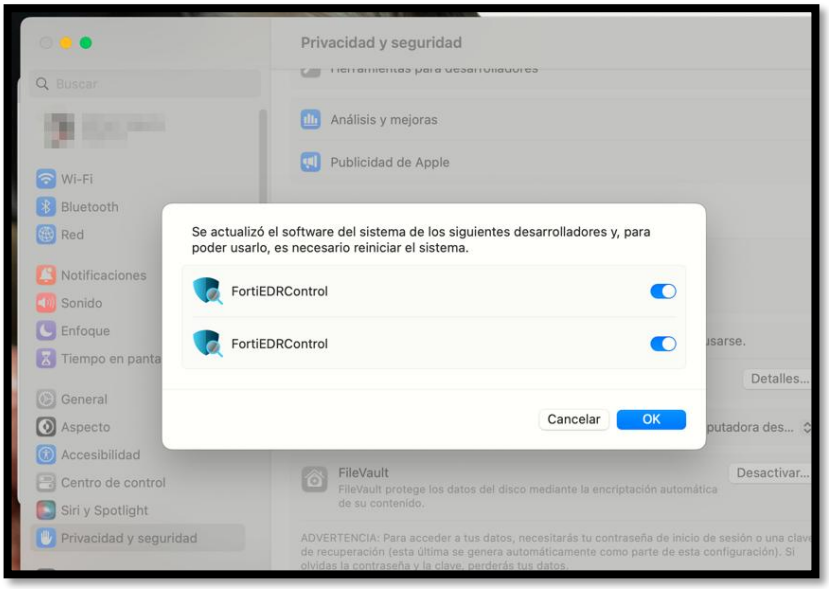




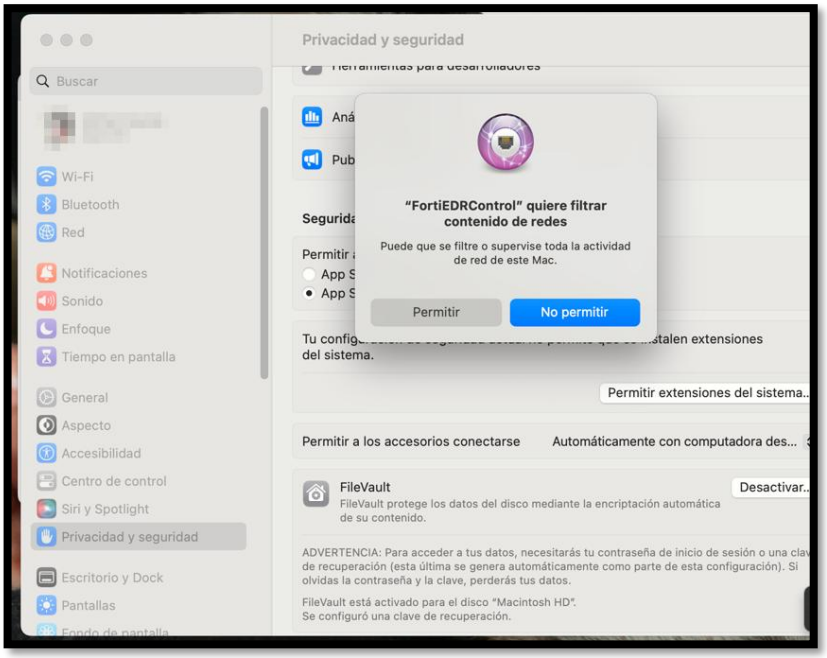
Durante la instalación del FortiEDR macOS se debe permitir las extensiones de FortiEDRControl es por ello por lo que debe acceder en "Abrir Configuración del Sistema"

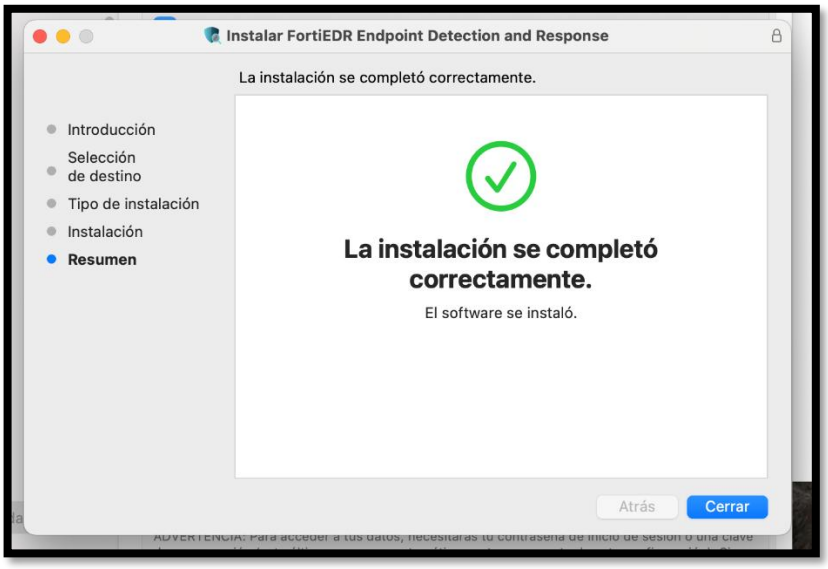


Debe permitir el uso de FortiEDRControl: Configuraciones - Privacidad y Seguridad.

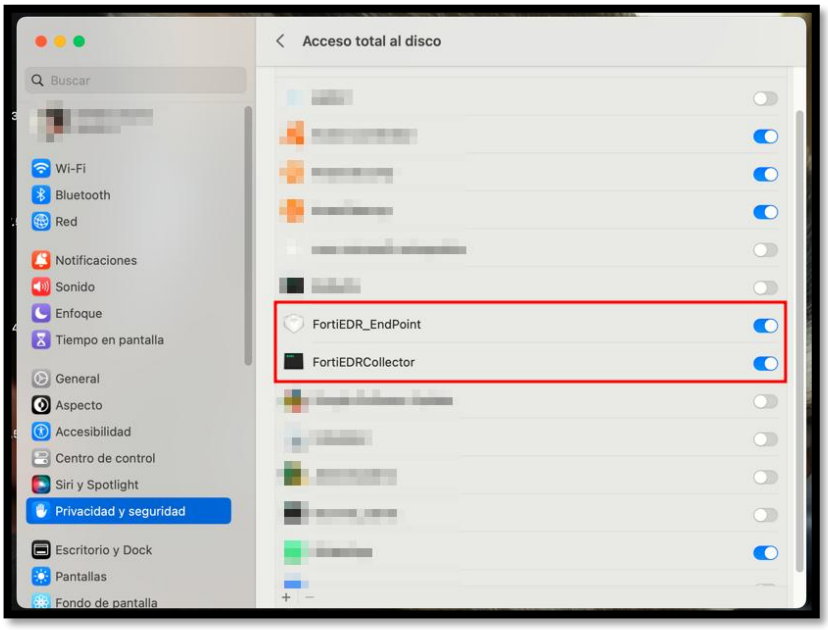


Manteniendo la ruta anterior: Configuraciones - Privacidad y Seguridad, debe permitir el Filtrado de Contenido de Redes.





Finalizada la instalación, en la ruta Configuraciones - Privacidad y Seguridad, ingresar a Acceso total al disco y habilitar FortiEDR_EndPoint y FortiEDRCollector.



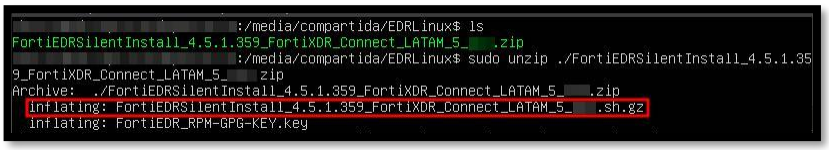
Instalación Linux

La instalación del EDR sea una distro con interfaz gráfica o no, realiza vía terminal. Si usted está instalando en distro exclusivamente vía terminal (ejemplo Ubuntu Server), debe instalar unzip; "*sudo apt install unzip"*.

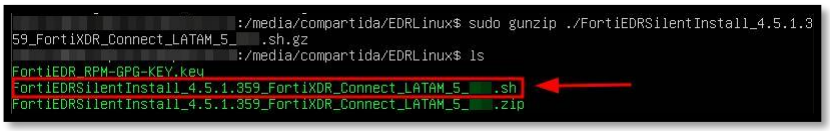
Instalado dicho complemento proceda con la instalación dirigiéndose a la ruta donde se encuentre el instalador comprimido.

Distro Ubuntu:

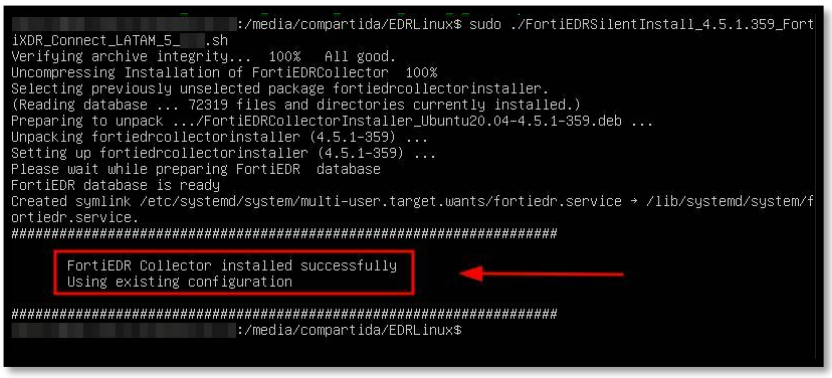
Descomprima "*sudo unzip ./FortiEDRSilentInstall_4.5.1.359_FortiXDR_Connect_LATAM_5_PFA.zip*".



Extraiga "*sudo gunzip ./FortiEDRSilentInstall_4.5.1.359_FortiXDR_Connect_LATAM_5_PFA.gz*".

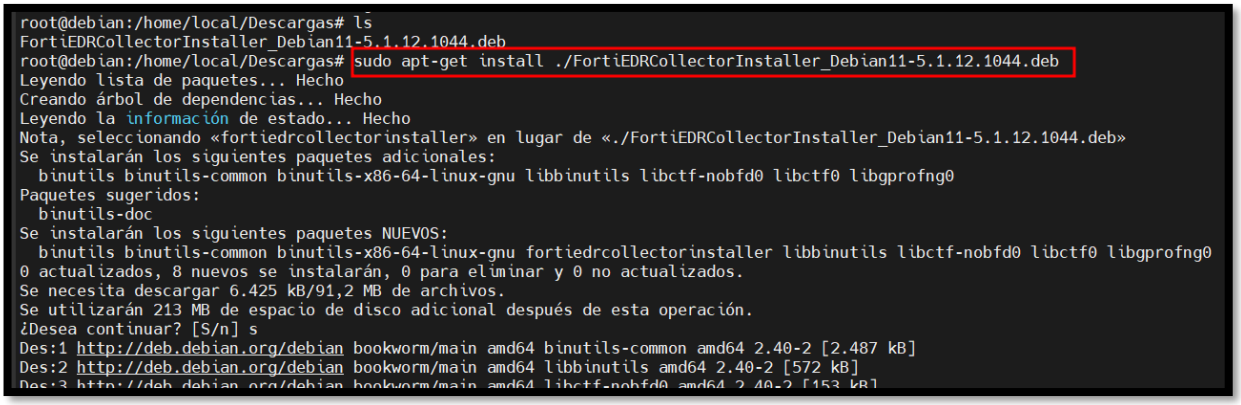


Ejecute el script de instalación "*sudo ./FortiEDRSilentInstall_4.5.1.359_FortiXDR_Connect_LATAM_5_PFA.sh*".

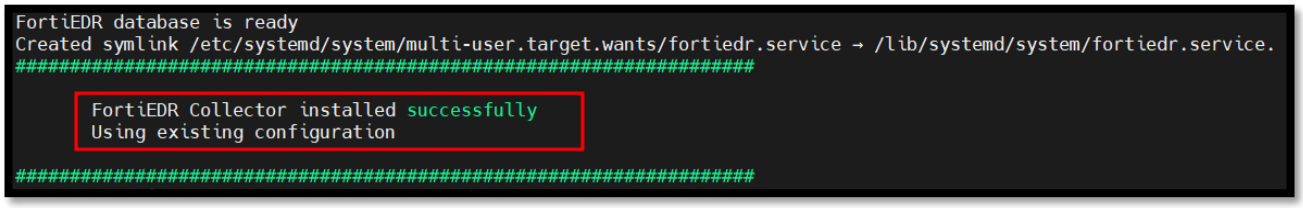


Distro Debian:

sudo apt-get install ./FortiEDRCollectorInstaller_Debian11-5.1.12.1044.deb

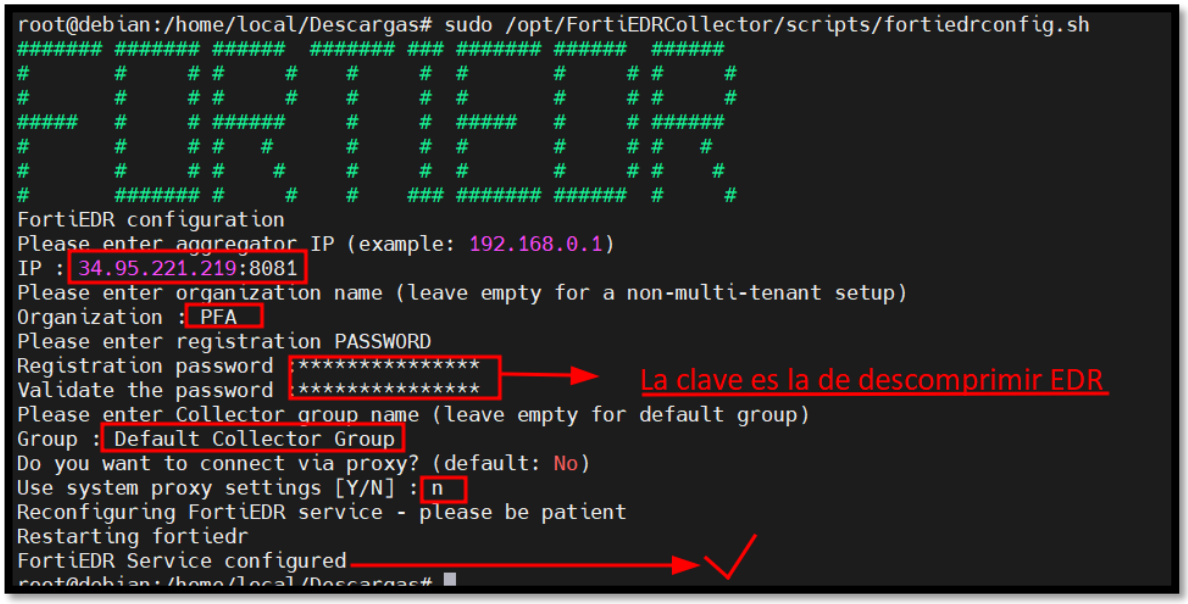


Una vez instalado.



Configurar el EDR instalado para que reporte en consola: sudo /opt/FortiEDRCollector/scripts/fortiedrconfig.sh

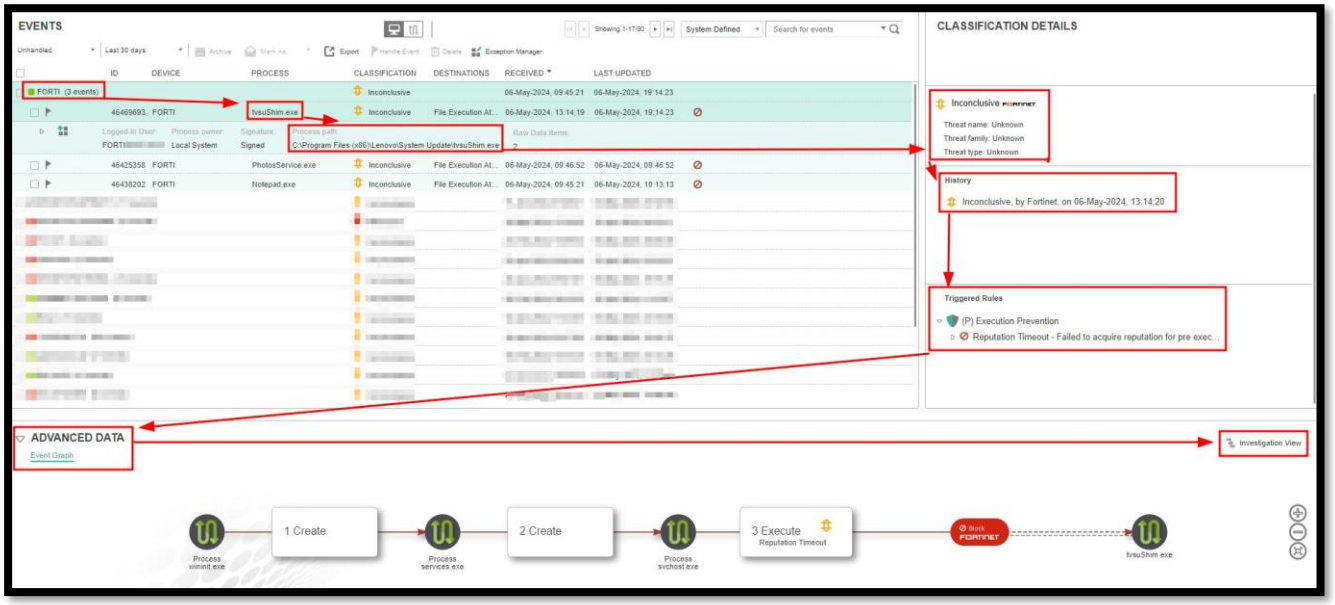
- IP/Port: 34.95.221.219:8081
- Organization: PFA
- Password: La clave es la de descomprimir en la consola EDR
- Group: Default Collector Group
- Proxy: N



Event Viewer

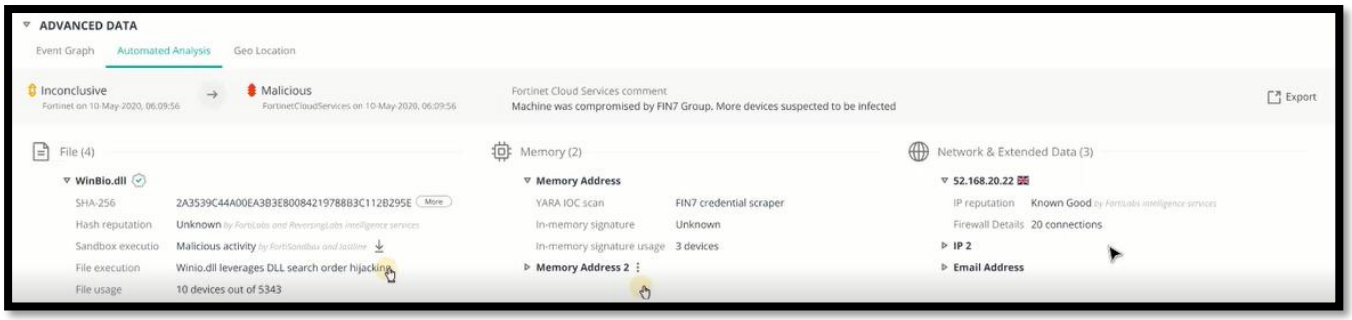
El Visor de eventos le permite ver, investigar y confirmar el control de cada uno de estos eventos de seguridad y permite mostrar dos segmentos o vistas diferentes de los datos de eventos recopilados por FortiEDR:

- Vista de dispositivo: Esta vista presenta información por dispositivo y muestra todos los eventos de seguridad detectados en un dispositivo determinado.
- Vista de proceso: Esta vista presenta información por proceso y muestra todos los eventos de seguridad detectados para un proceso determinado.



Advanced Data (Event Viewer)

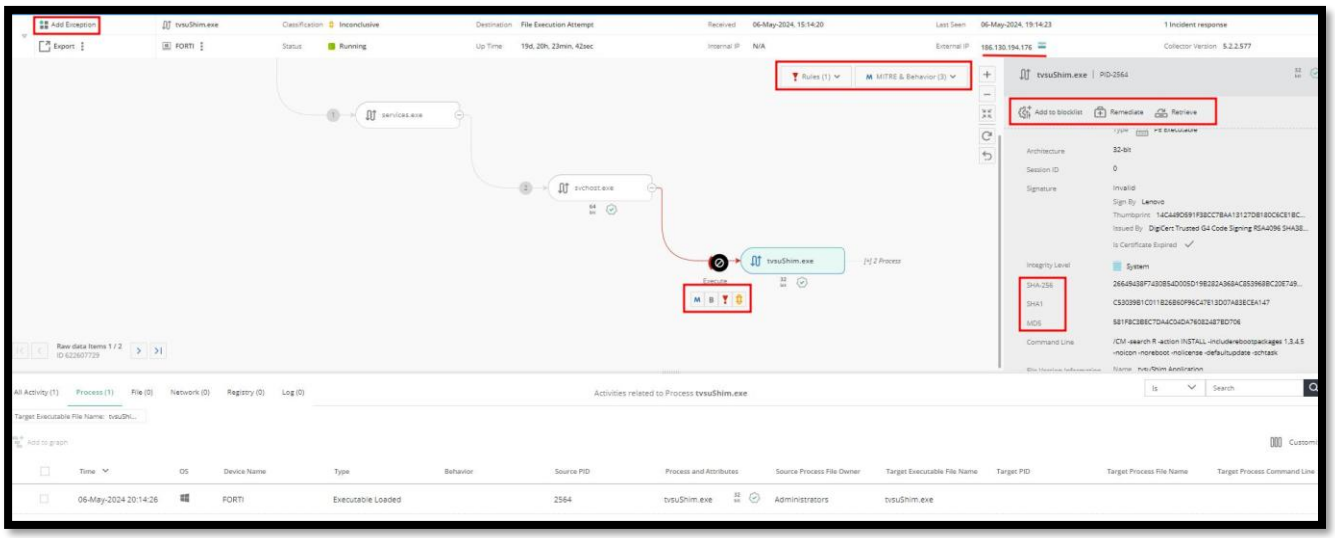
Proporciona información adicional sobre la investigación realizada automáticamente en Fortinet Cloud Services (FCS) según el evento de seguridad para ayudarlo a comprender la lógica de FortiEDR al clasificar un elemento con una clasificación específica.



Investigation View

Se puede acceder a mediante desde la pestaña **Advanced Data** en Visor de eventos. Ayuda a comprender el flujo de eventos de actividad durante la búsqueda de amenazas con una vista gráfica dinámica e interactiva de los detalles de los eventos de actividad: origen, acción y destino. La vista gráfica proporciona la capacidad de agregar más eventos de actividad al gráfico y mostrar la relación y la escala de tiempo de la ocurrencia de esas actividades, como las siguientes:

- Todas las acciones realizadas por un proceso determinado.
- Todos los archivos que el proceso ha creado o actualizado.
- Todas las direcciones IP con las que el proceso ha iniciado la comunicación.
- Navega entre los distintos procesos que intervienen en la cadena.
- Ver todos los eventos de actividad relacionados con un nodo en el gráfico de eventos de seguridad.
- Filtrar la tabla de eventos de actividad para incluir o excluir un valor específico.
- Remediar o Recuperar archivos y Aislar un equipo.
- Mover un dispositivo a un grupo de alta seguridad.



Remediate

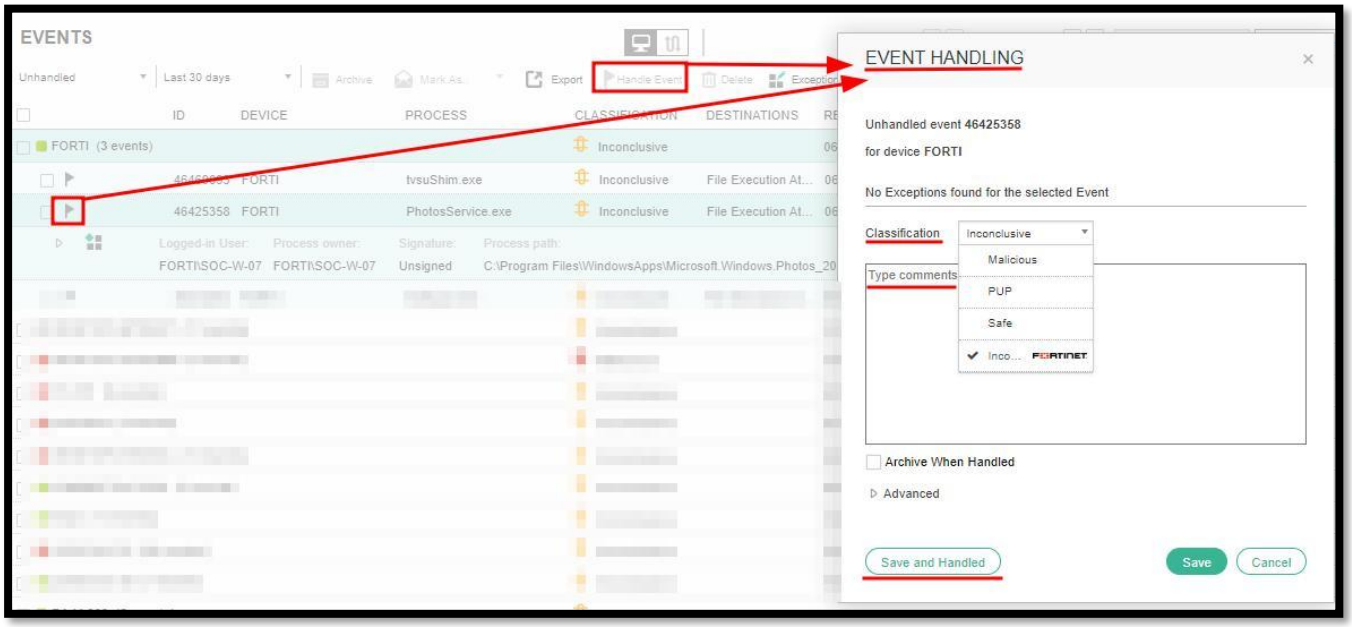
Una vez que se detecta malware en un dispositivo, puede corregir el dispositivo mediante las siguientes opciones:

Método	Descripción
Finalizar el proceso	Este método no garantiza que el proceso afectado no intente ejecutarse de nuevo.
Elimine el archivo afectado de la computadora	Este método garantiza que el archivo no intente volver a filtrar datos, ya que el archivo se elimina permanentemente del dispositivo. Al utilizar este método, tener cuidado de no eliminar archivos que sean importantes para el sistema.
Quitar o modificar la clave del Registro	Este método quita una clave del Registro o actualiza el valor de una clave del Registro. Este método cambia las modificaciones malintencionadas de la clave del Registro quitando las claves recién creadas o devolviendo los valores de clave a su forma original.

Handle Event

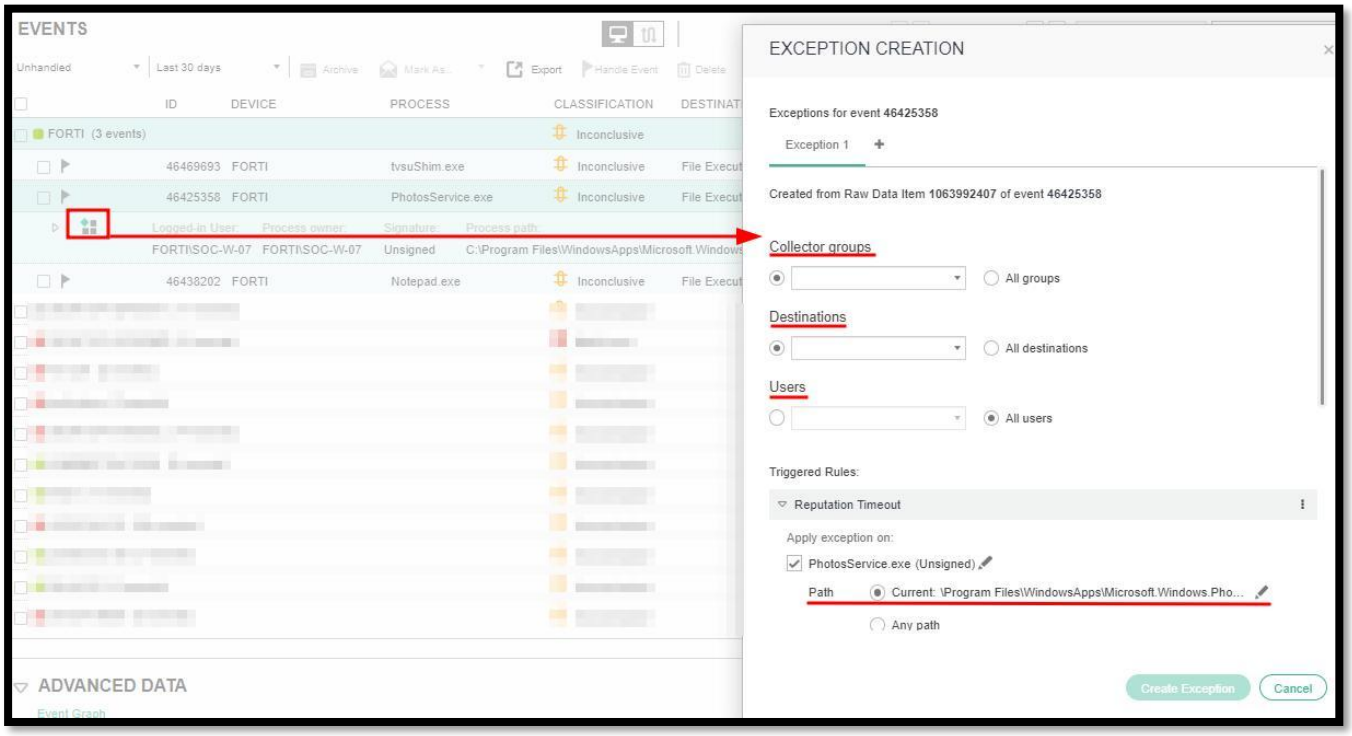
Se utiliza para marcar un evento de seguridad como “Trabajado / No trabajado”.

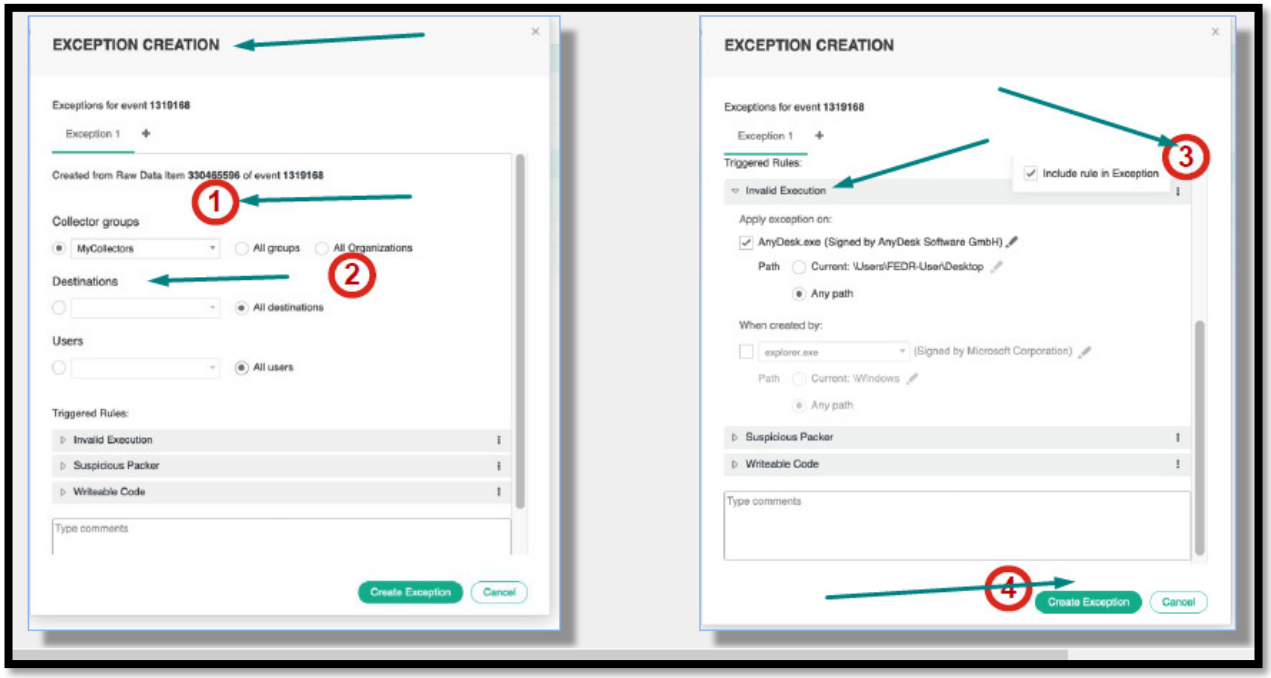
- En Clasificación, cambie la clasificación del evento de seguridad, si es necesario.
- En Comentarios, utilizar para describir cómo se controló el evento de seguridad.
- El botón Guardar o Guardar y Archivar.

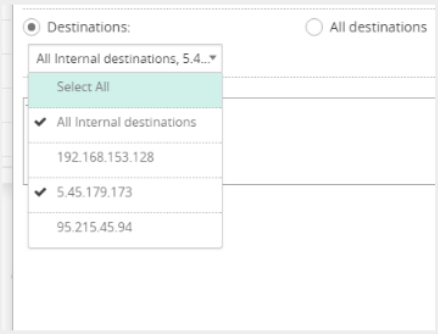
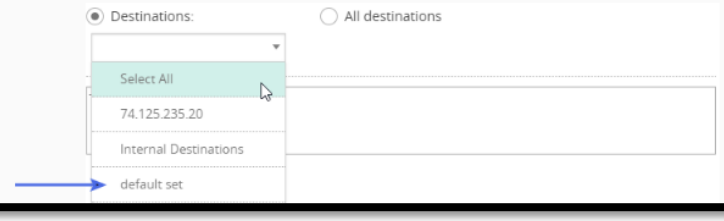


Create Exception

Las excepciones permiten limitar la aplicación de una regla, es decir, crear una lista blanca para un flujo específico de eventos de seguridad que se utilizó para establecer una solicitud de conexión o realizar una operación específica.





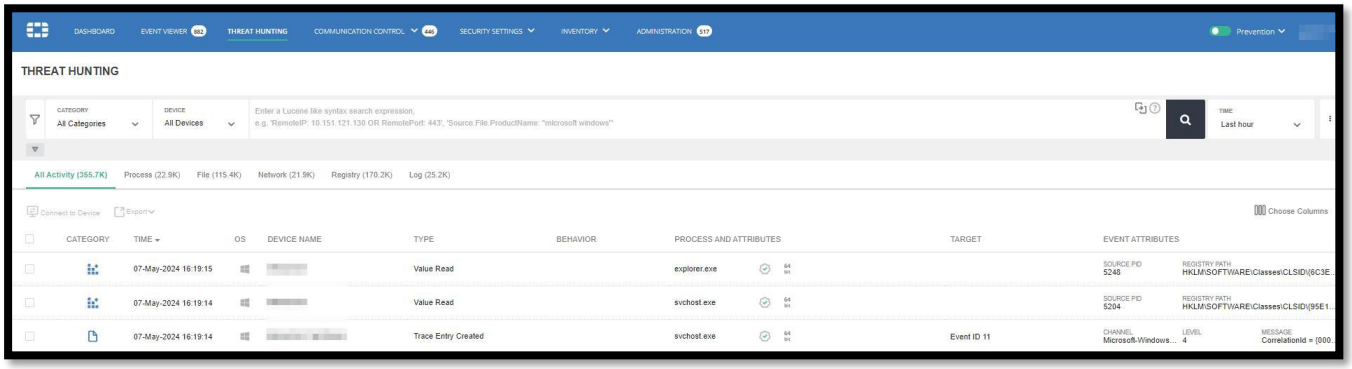
Opción	Descripción
Seleccionar todo	Aplica la excepción en todos los destinos que se vieron como parte de este evento de seguridad. Si se produce una infracción idéntica (se infringirá el mismo conjunto de reglas en este proceso) pero el intento de conexión será a una IP diferente, se activará el evento de seguridad. Para excluir por completo este evento de seguridad para que no se active en el futuro, puede seleccionar el botón de opción *Todos los destinos*.
Destinos internos	Aplica la excepción en todos los destinos internos. Los destinos internos son direcciones IP internas que se definen en las definiciones estándar TCP/IP para redes internas. Estas direcciones IP incluyen las siguientes: • Direcciones de bucle invertido: 127.X.X.X, 0:0:0:0:0:0:0:0:1 y 0:0:0:0:0:FFFF:7f • 10.0.0.0 –10.255.255.255 • 192.168.0.0–192.168.255.255 • 169.254.0.0–169.254.255.255 • 172.16.0.0 - 172.31.255.255 • IPV6: fc00:: – fd00:: :: o fe80 Esta opción es útil cuando se permite el uso de una aplicación dentro de la organización, pero no desea que se utilice para comunicaciones externas. El uso de esta opción permite que la aplicación se comunique internamente sin desencadenar alertas. Sin embargo, es posible que la aplicación siga activando alertas al intentar conectarse a una dirección IP externa.
<Dirección IP>	Aplica la excepción a la dirección IP seleccionada. Puede seleccionar varias direcciones IP. 
<Conjunto de IP>	Un conjunto de direcciones IP define un conjunto de direcciones IP que se incluirán o excluirán de un evento de seguridad. Al seleccionar un conjunto de direcciones IP aquí, significa que solo se aplica una excepción a un dispositivo que tiene una de las direcciones IP especificadas en el conjunto de direcciones IP. Los conjuntos de IP solo pueden ser definidos por un administrador, como se describe en Conjuntos de IP. 

En el caso que se requiera editar la excepción, buscar e identificar la en **Security Settings** – **Exception Manager**.

Threat Hunting

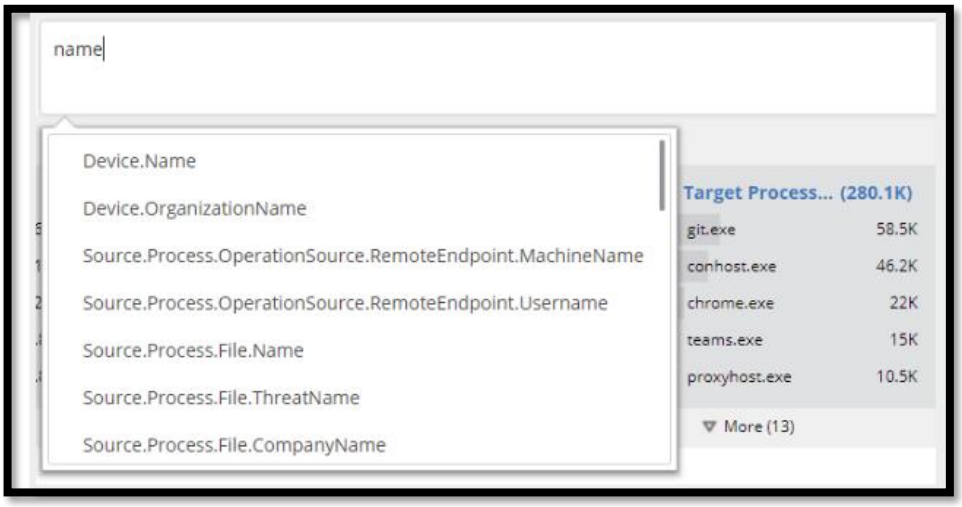
La funcionalidad de búsqueda de amenazas de FortiEDR le permite buscar muchos tipos de indicadores de compromiso (IOC) y malware. La búsqueda de amenazas es ideal en situaciones en las que se ha identificado malware y se desea buscar en toda la organización para determinar si este mismo malware existe en otro destino.

Un evento de actividad consta de un origen (normalmente un proceso), una acción (el tipo de evento de actividad) y un destino (Proceso, archivo, clave/valor del Registro, elemento de red).
Por ejemplo, cuando se ejecuta un proceso, puede realizar varias acciones en los archivos, como Abrir archivo, Lectura de archivo, Eliminar archivo, etc.



Este filtro le permite especificar una consulta de **sintaxis de Lucene** de texto libre para filtrar los resultados. También puede convertir las consultas de **sintaxis JSON y XML de STIX a la sintaxis de Lucene** mediante el botón Convertir consulta.

En el caso de las consultas de **sintaxis de Lucene**, el filtro de consulta de texto libre tiene una lista desplegable auxiliar de autocompletar que contiene todos los campos de eventos de actividad disponibles, así como los operadores de sintaxis disponibles.


name
Device.Name
Device.OrganizationName
Source.Process.OperationSource.RemoteEndpoint.MachineName
Source.Process.OperationSource.RemoteEndpoint.Username
Source.Process.File.Name
Source.Process.File.ThreatName
Source.Process.File.CompanyName
Target Process... (280.1K)
git.exe 58.5K
conhost.exe 46.2K
chrome.exe 22K
teams.exe 15K
proxyhost.exe 10.5K
More (13)

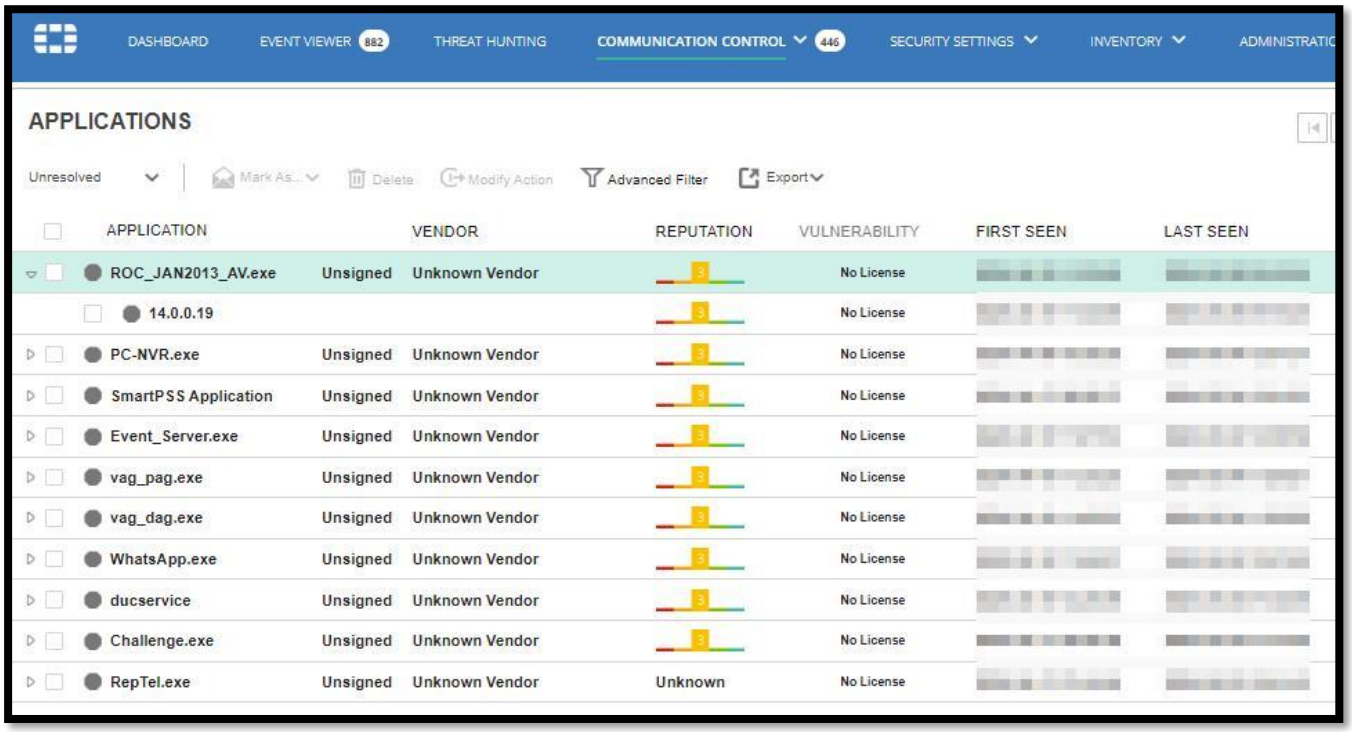
Communication Control

FortiEDR proporciona visibilidad de cualquier aplicación de comunicación en su organización, lo que le permite controlar qué aplicaciones pueden comunicarse.

Después de la instalación de FortiEDR, el sistema mapea automáticamente todas las aplicaciones de su red que se comunican externamente. Después de eso, decide cuál de estas aplicaciones permitir que se comunique externamente cuando lo use un usuario legítimo de su organización (lista de permitidos). Una vez definida la lista de aplicaciones permitidas de comunicación, solo las aplicaciones de la lista de permitidos pueden comunicarse externamente. Si un atacante abusa de una aplicación en la lista de permitidos, la tecnología patentada de FortiEDR (políticas de exfiltración y prevención de ransomware) bloquea la comunicación y muestra un evento de seguridad en la pestaña EVENTOS.

Applications

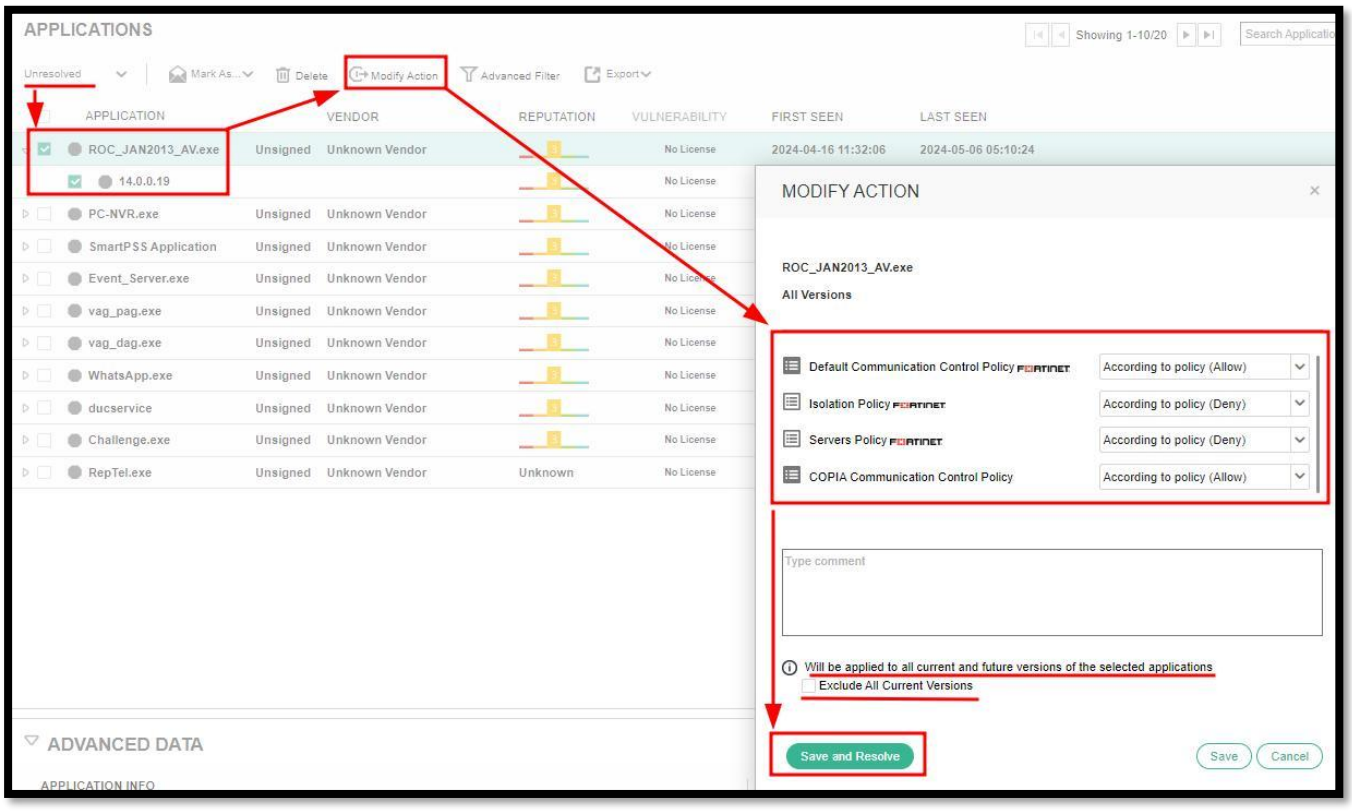
Se enumeran todas las aplicaciones de comunicación detectadas en la organización que alguna vez han intentado comunicarse.



Cada aplicación muestra un indicador de **REPUTACIÓN**, las cuales son determinadas por un servicio de terceros y se basan en el hash del archivo.

Puntuación de reputación	Descripción de la reputación
1	Conocido como malo
2	Asumido como malo
3	Poco claro, indicio de una contradicción o incapacidad para determinar la reputación
4	Se asume como bueno
5	Conocido como bueno

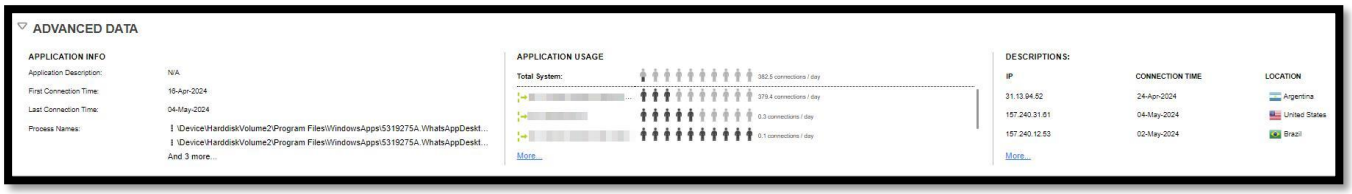
Se puede modificar la acción de una política para permitir o denegar una aplicación:



Advance Data (Communication Control – Applications)

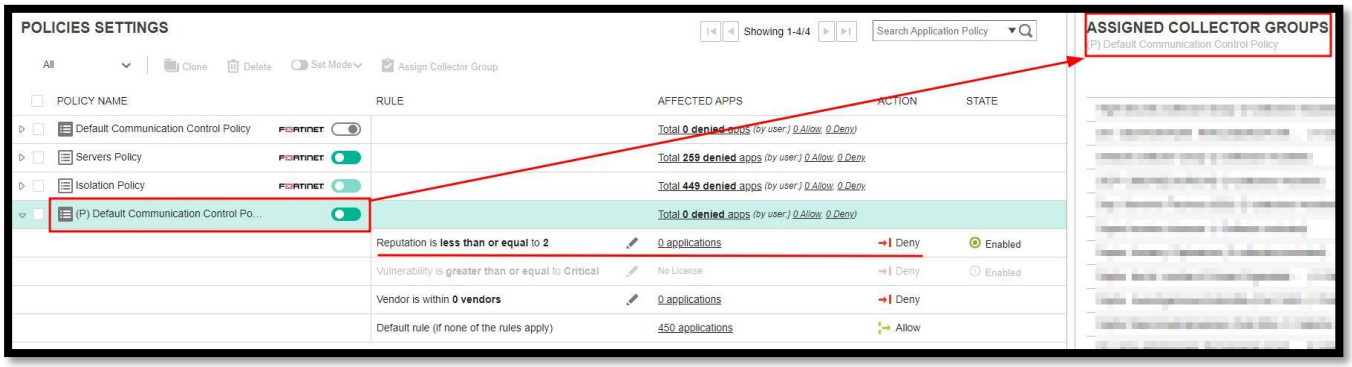
- **Application Info**: muestra información resumida sobre la aplicación seleccionada.
- **Application Usage**: muestra detalles sobre el uso de la aplicación seleccionada. Esta área muestra el número de conexiones (sesiones de comunicación) por día. La línea superior muestra el número total de dispositivos dentro de la organización en los que está instalada la aplicación seleccionada.

  Cada fila representa un grupo de dispositivos y cada icono de persona representa el 10 % del total de dispositivos de la organización. Los iconos negros representan los dispositivos que se comunican externamente mediante la aplicación seleccionada y los iconos grises representan los dispositivos que no se comunicaron externamente mediante la aplicación.
- **Descriptions**: muestra los destinos con los que la aplicación seleccionada se comunicó (Permitido) o intentó comunicarse (Denegado).



Policies

El Control de Comunicaciones tiene sus propias políticas. Las directivas definen las acciones que se deben realizar para una aplicación determinada o una versión de aplicación. Cada directiva se aplica a un grupo de colectores específicos y a todos los dispositivos que pertenecen a es o esos grupos colectores.

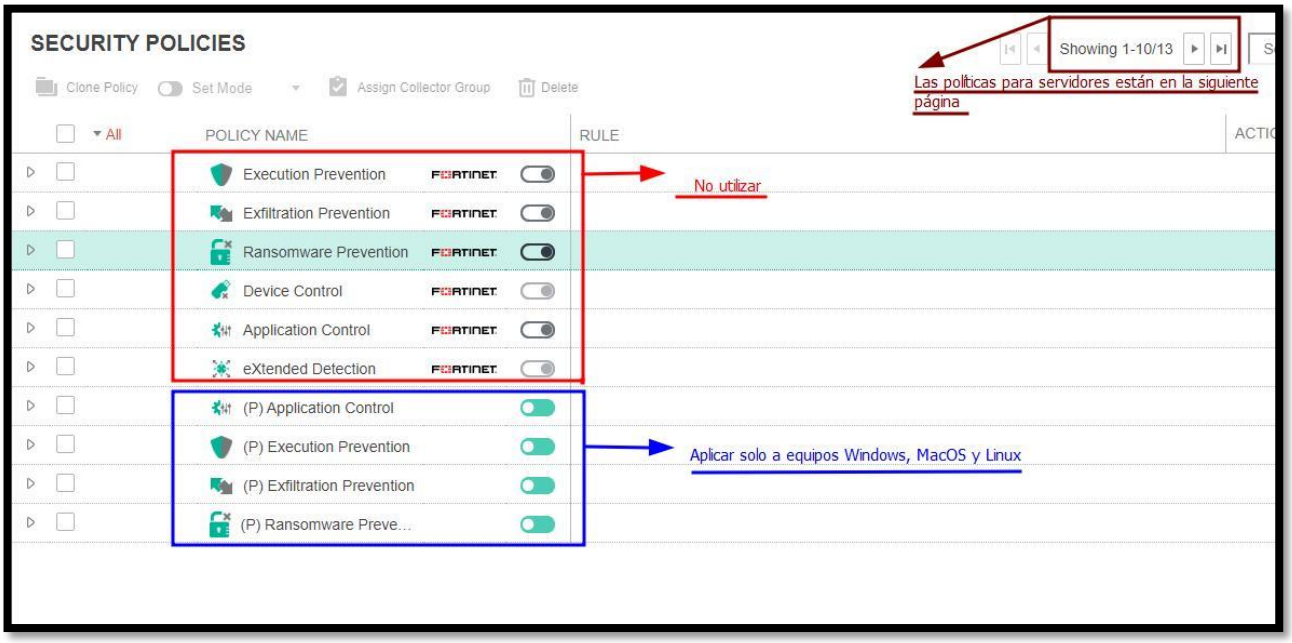


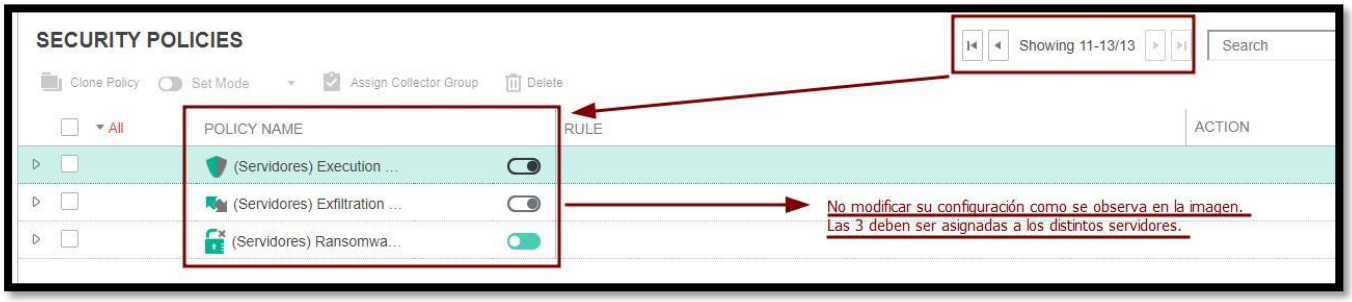
Security Settings

Security Policies

El último paso es similar al anterior, en este caso se debe asignar *SIEMPRE* de momento las siguientes políticas:

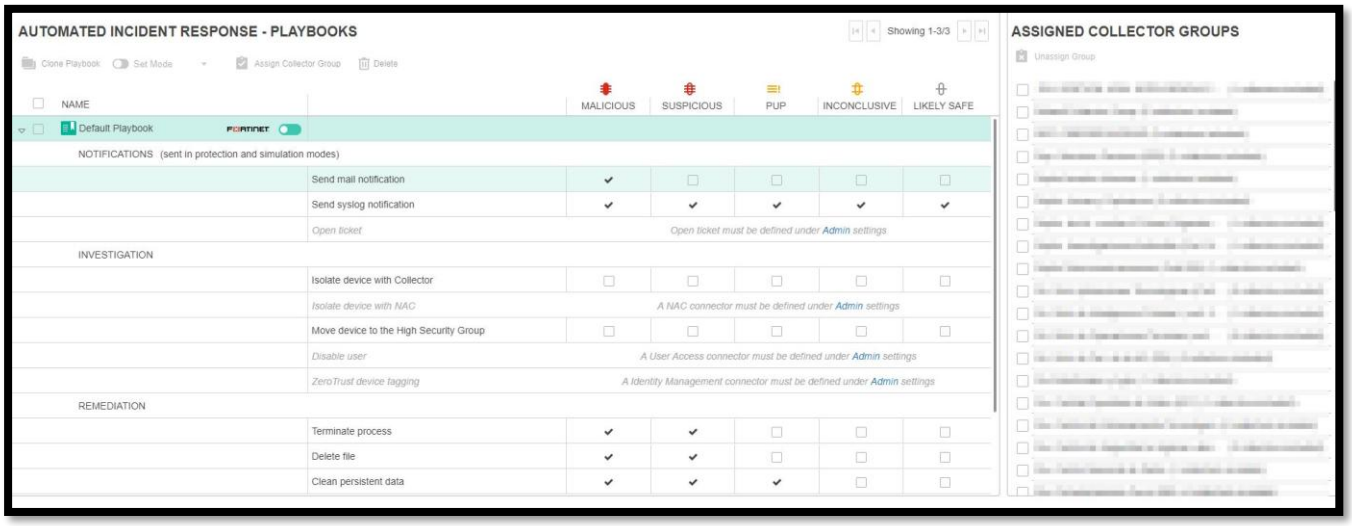
- Execution Prevention.
- Exfiltration Prevention.
- Ransomware Prevention.
- Application Control.





Playbooks

La función de las Playbooks es determina qué acciones automáticas se deben activar en función de la clasificación de un evento de seguridad, por lo cual deben ser asignadas necesariamente a los grupos colectores.



Exception Manager

Exception Manager permite crear excepciones a las reglas de seguridad. Es una lista blanca que permite que un flujo específico de eventos, que normalmente activaría una regla, se ejecute sin generar alertas. Las excepciones se aplican a todas las políticas de seguridad. Además, el servicio en la nube de Fortinet (FCS) puede generar excepciones automáticas si un análisis detallado de un evento de seguridad lo reclasifica como "Seguro". Esto evita que el evento se vuelva a activar como sospechoso. ***"Creación en la página 13-14"***

Las excepciones se pueden crear para:

- Un grupo de colector (varios específicos o todos).
- Una dirección IP de destino (una específica, un conjunto de IP o todas).
- Un usuario o todos.

Exclusion Manager

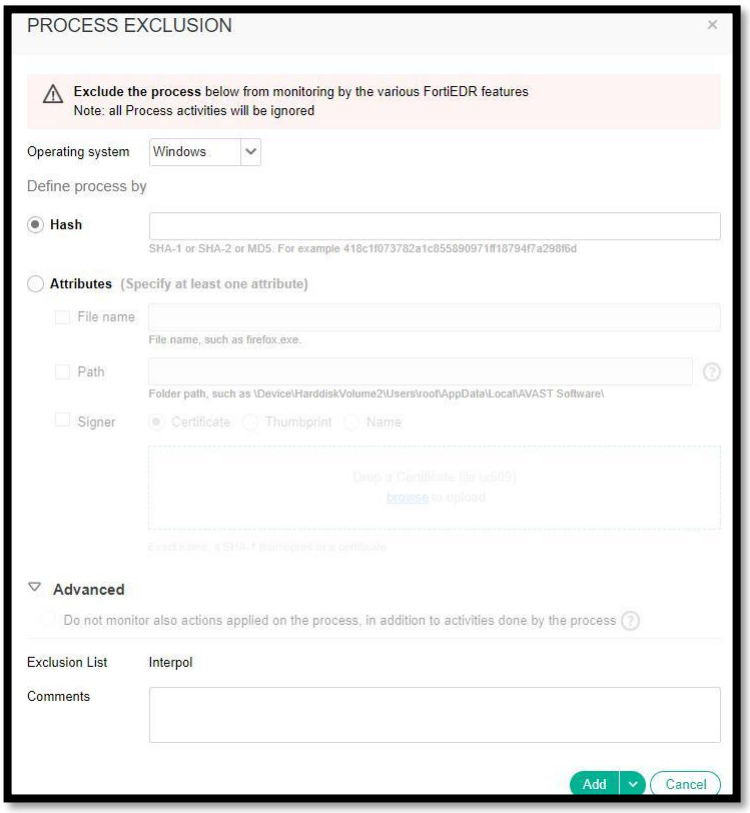
El Exclusion Manager permite definir qué procesos o archivos excluir del monitoreo de las Políticas de Seguridad de FortiEDR.

Hay dos tipos de exclusiones que puedes configurar:

- **Exclusiones de Procesos:** Este tipo de exclusión le indica a FortiEDR que no inspeccione las acciones realizadas por procesos específicos. De esta forma, dichos procesos no activarán eventos de seguridad.

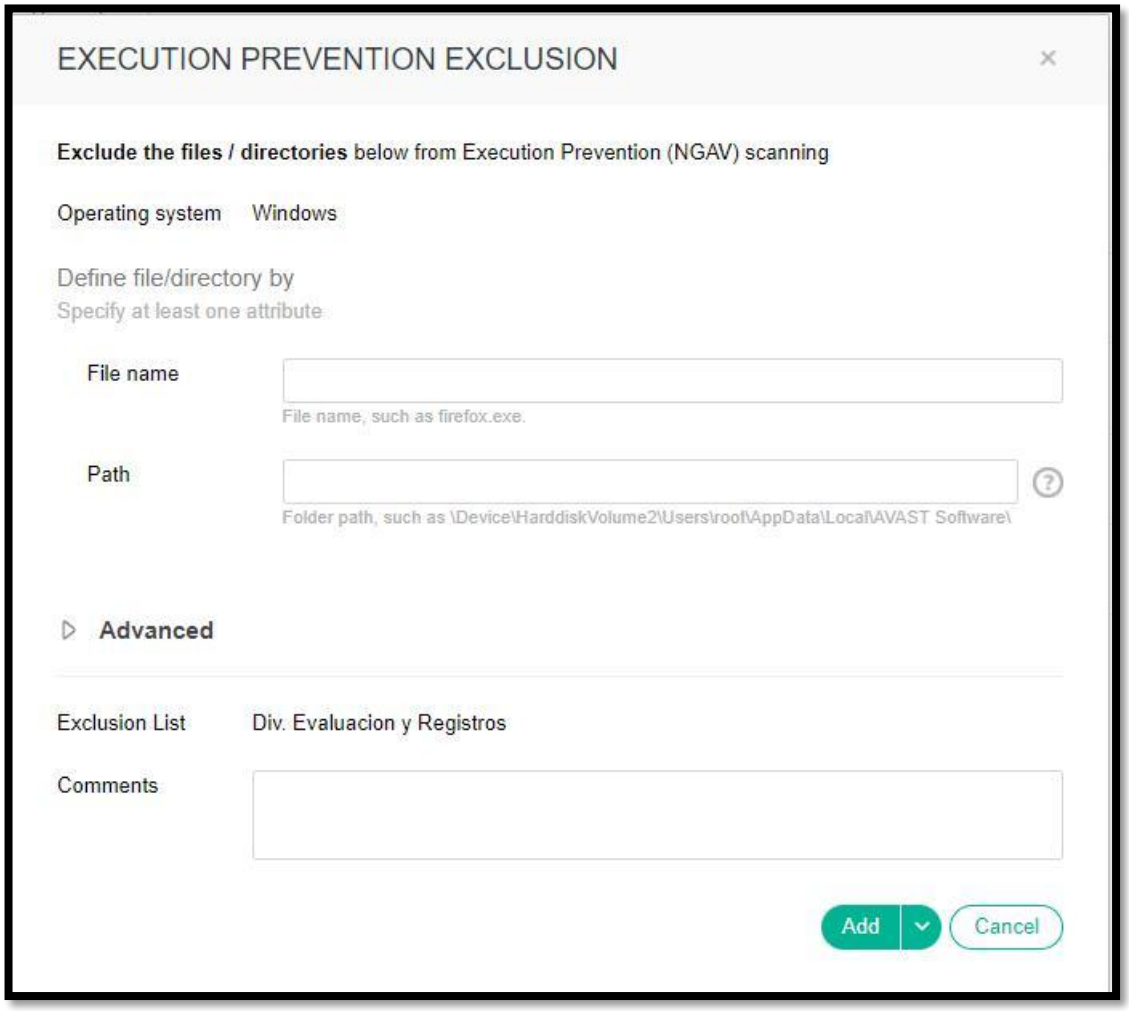
  Puede haber varias razones para excluir un proceso. Por ejemplo, si la inspección de FortiEDR afecta el rendimiento o funcionalidad de un proceso, pero sabes que es bueno y seguro (incluso si no genera eventos de seguridad). En este caso, la exclusión le dice a FortiEDR que deje de inspeccionar ese proceso en particular.

Se debe tener en cuenta que al agregar este tipo de exclusión, el proceso ya no será monitoreado por ninguna función de FortiEDR y todas sus actividades se ignorarán.



- **Exclusiones de Prevención de Ejecución**: La política de Prevención de Ejecución analiza archivos y los bloquea si se identifican como maliciosos o sospechosos.

  Las Exclusiones de Prevención de Ejecución le indican a FortiEDR que no aplique la inspección de esta política, la cual busca evidencia de actividad maliciosa en los archivos (como se describe en la Configuración de Seguridad).



Application Control Manager

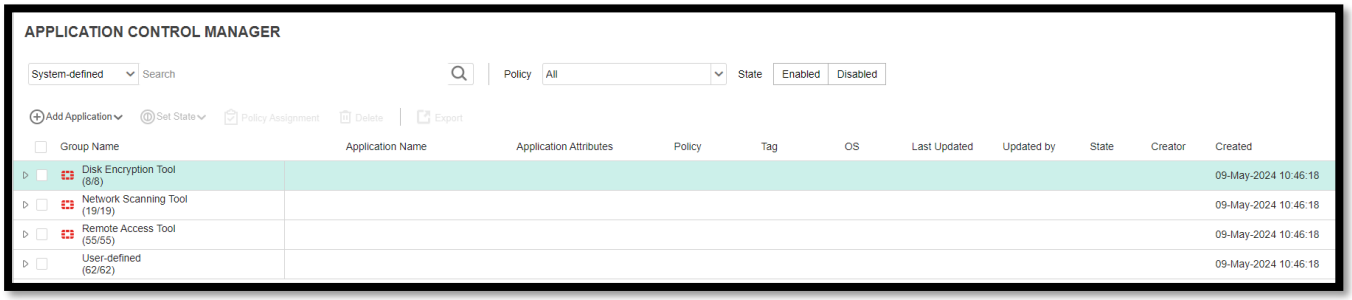
El Application Control Manager es una herramienta que permite bloquear aplicaciones no deseadas para que no se ejecuten en los dispositivos. Funciona de forma diferente al control de comunicación de aplicaciones, que solo restringe con quién se comunican las aplicaciones, pero no impide que se abran.

Para bloquear aplicaciones con Application Control Manager:

- Agregar las aplicaciones que se requiere bloquear y se puede hacer de dos formas:
  - Agregándolas manualmente
  - Seleccionándolas desde la ventana de Investigación (Investigation View)
- Asigna las aplicaciones bloqueadas a un grupo específico de dispositivos (grupos de colectores).
- Habilita la regla de lista negra (bloqueo) en la política de Control de Aplicaciones.

Asimismo, existen dos tipos de grupos de aplicaciones:

- **Grupos predefinidos de Fortinet**: Vienen configurados por defecto y aparecen en la parte superior de la lista. Solo se puede modificar la política asociada a estos grupos (Control de Aplicaciones por defecto) y no es posibles editar las aplicaciones dentro de estos grupos.
- **Grupo definido por el usuario**: Se agregan las aplicaciones que la organización haya determinado para bloquear.



Threat Hunting (Security Settings)

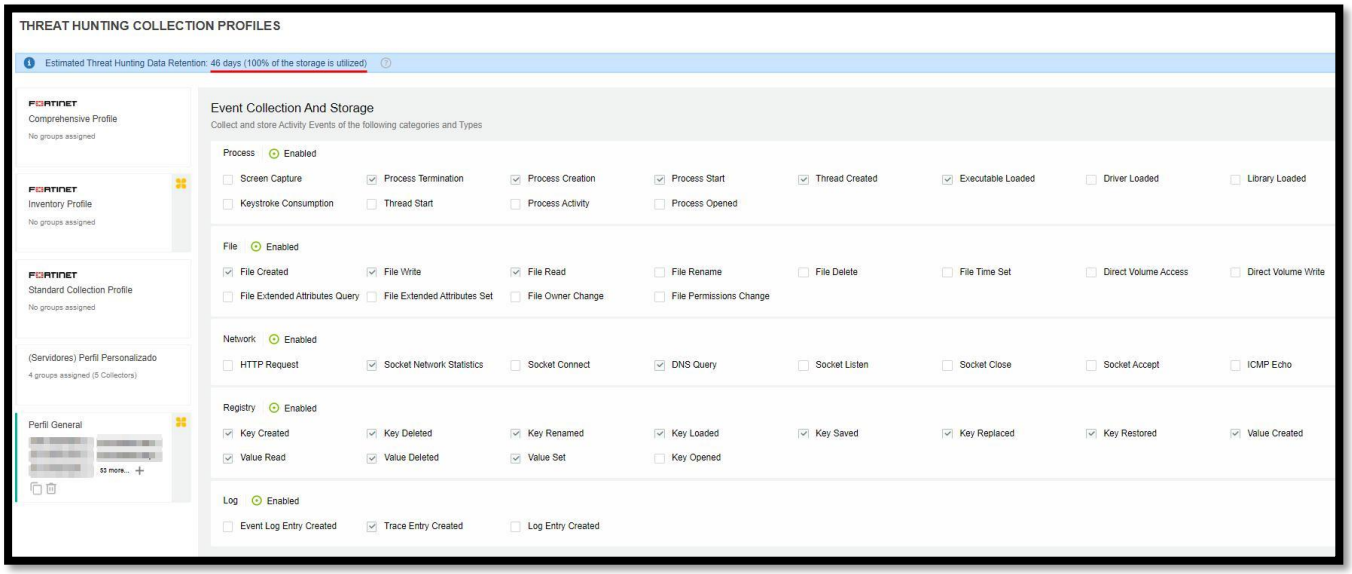
Es un conjunto de herramientas de software y fuentes de información centradas en la detección, investigación, contención y mitigación de actividades sospechosas en los dispositivos de los usuarios finales.

Collection Profiles

Los perfiles de Threat Hunting controlan el tipo de datos de actividad que se recopilan para la función de Threat Hunting y así poder tener una mayor visibilidad de los eventos de seguridad a analizar.

Actualmente se utilizan 2 perfiles configurados manualmente:

- **Perfil General**: este está dedicado a la mayoría de los dispositivos y se encuentra por default, esto quiere decir que cuando se instale un agente EDR, ese Endpoint automáticamente utilizará el perfil mencionado.
- **(Servidores) Perfil Personalizado**: es un perfil configurado exclusivamente para servidores y no generar grandes consumos de recursos en los mismos, este debe ser aplicado manualmente cada vez que se instala un agente EDR en un servidor.



Collection Exclusions

Las exclusiones permiten definir determinados tipos de eventos de actividad que se excluirán de la recopilación de datos de Threat Hunting. Por ejemplo, si sabe que un determinado proceso es legítimo, pero crea muchos eventos de actividad que no son relevantes para la investigación de Threat Hunting, puede usar las exclusiones de recopilación para definir que estas actividades no se recopilen.

Reglas y su tratamiento

Execution Prevention

Regla	Detalles	Acciones que tomar
Malicious File Detected	El motor de aprendizaje automático o por otros medios identificó el archivo como malicioso, según el análisis del archivo.	Recupere el archivo ejecutable del dispositivo de destino, según su ruta. Utilice la pestaña Forense para realizar un análisis más profundo. Verificar el origen del fichero y su uso previsto en la organización.
Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Se detectó un exploit de escalada de privilegios. Los atacantes normalmente utilizan estos exploits para obtener el control total de un dispositivo vulnerado como parte de una cadena de exploits, toma de control del servidor o movimiento lateral. Esto, a su vez, puede resultar en el robo de fichas.	Este tipo de infracción normalmente se puede inferir comprobando el contexto de la alerta. Si el proceso o uno es creado por un navegador o un documento de Office, es probable que forme parte de una cadena de explotación. Si el proceso es un intérprete de línea de comando o powershell, es probable que sea parte de un movimiento lateral o un intento de toma de control del servidor.
Sandbox Analysis - File was sent to the sandbox for analysis	Se envió un archivo sospechoso al sandbox para su análisis e inspección. Una vez finalizado el análisis, el archivo se clasificará como malicioso, en cuyo caso se bloquearán sus ejecuciones futuras, o se clasificará como benigno y su ejecución continuará.	Consulta la clasificación del evento. Si no se estableció la clasificación de la nube, el análisis del espacio aislado aún no se ha completado. Si el archivo es malicioso, el análisis de la zona de pruebas determinó que era malicioso. En este caso, su futura ejecución quedará bloqueada por las reglas de Prevención de Ejecución. Para omitir el análisis de la zona de pruebas, establezca una excepción.
Stack Pivot - Stack Pointer is Out of Bounds	Cada hilo del sistema operativo tiene una pila. La pila de cada hilo tiene asignado un espacio de direcciones bien definido. El malware puede alterar el puntero de la pila y hacer que apunte fuera de estos límites. La alteración del puntero de la pila se realiza como parte de una etapa de explotación o para eludir el software de protección que depende del seguimiento de la pila. Las pilas ejecutables son raras y existen en aplicaciones antiguas o protectores de aplicaciones agresivos.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se activaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Suspicious Driver Load - Attempt to load a suspicious driver	Se detectó un intento de cargar un controlador que contenía características de archivos sospechosos en el kernel del sistema operativo. Esta actividad suele detectarse cuando una entidad maliciosa intenta cargar un rootkit en el núcleo del sistema operativo para obtener un control total sobre el sistema.	Recupere el archivo del controlador del dispositivo de destino según su ruta. Utilice la pestaña Forense para realizar un análisis más profundo. Verificar el origen del archivo del controlador y su uso previsto en la organización.
Suspicious File Detected	Este archivo contiene características sospechosas comúnmente utilizadas por el malware y el motor de aprendizaje automático lo identificó como potencialmente malicioso.	Recupere el archivo ejecutable del dispositivo de destino, según su ruta. Utilice la pestaña Forense para realizar un análisis más profundo. Verificar el origen del fichero y su uso previsto en la organización.

Suspicious Script Execution - A script was executed in a suspicious context	Un script fue ejecutado mediante un proceso sospechoso. Los atacantes utilizan esta técnica para lograr acceso remoto al dispositivo sin dejar de ser sigilosos.	Inspeccionar los datos de la línea de comandos del proceso para comprender el contexto de la ejecución del script.
Unconfirmed File Detected	Este archivo contiene algunas características comúnmente utilizadas por el malware y nuestro motor de aprendizaje automático lo identificó como potencialmente malicioso.	Recupere el archivo ejecutable del dispositivo de destino según su ruta. Utilice la pestaña Forense para realizar un análisis más profundo. Verificar el origen del fichero y su uso previsto en la organización.

Exfiltration Prevention

Regla	Detalles	Acciones que tomar
Access to Critical System Information	Un proceso intentó acceder a credenciales, contraseñas u otra información crítica de manera sospechosa. Esta regla puede haber sido activada por un proceso malicioso o por un usuario que intenta obtener credenciales más altas para el movimiento lateral o para elevar privilegios.	Si esta es la única regla que se activó, es posible que el usuario haya intentado obtener acceso manualmente a las credenciales. También podría ser una acción realizada por un usuario malintencionado a través de una conexión RDP. Para mitigar el ataque, aísle la máquina y desactive al usuario en el dominio, si es posible. Si se violaron más reglas, siga las recomendaciones forenses de las otras reglas.
Bruteforce Attempt Detected	Se detectaron intentos sistemáticos de acceder a una cuenta. El malware puede utilizar técnicas de fuerza bruta para acceder a un servicio de red cuando se desconocen las credenciales.	Si esta es la única regla que se activó, recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Análisis forense. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.
Debugged Process - Connection from a Debugged Process	Se identificó un proceso que se está depurando. El malware puede utilizar técnicas de autodepuración para dificultar la ingeniería inversa. Esta regla también puede activarse cuando un usuario legítimo depura un proceso del sistema que se conecta externamente.	Verifique que el usuario del dispositivo no haya ejecutado un depurador cuando se desencadenó el evento.
Dynamic Code - Malicious Runtime Generated Code Detected	El origen de la mayor parte del código del proceso proviene de un archivo. Sin embargo, es posible generar código en tiempo de ejecución sin el archivo correspondiente. Es extremadamente difícil identificar el código generado en tiempo de ejecución como malicioso. Como tal, este tipo de código es comúnmente utilizado por malware y exploits para ejecutar su carga útil.	Vaya a la pestaña Análisis forense. Obtenga la dirección base y la dirección final como se especifica en la entrada de la pila correspondiente. Recupere la memoria del dispositivo objetivo de acuerdo con estas direcciones de memoria utilizando la pestaña Forense y realice un análisis más profundo.
Executable Format - Bad Executable File Format	Cada archivo ejecutable en el sistema operativo tiene un formato de archivo bien definido. Uno o más de los archivos ejecutables parecen tener una estructura sospechosa o no válida. El mal formato también puede existir en protectores de aplicaciones muy agresivos.	Si esta es la única regla que se violó, recupere el archivo ejecutable del dispositivo objetivo según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Utilice herramientas de análisis de archivos ejecutables, como CFFExplorer con la información proporcionada en la entrada de la pila

		correspondiente para comprender mejor la infracción de formato.
Executable Stack - A Stack with Executable Code	La pila de la aplicación parece contener código ejecutable. Los atacantes suelen hacer que la pila sea ejecutable durante la etapa de explotación para poder ejecutar el código desde la pila de la aplicación. Las pilas ejecutables son raras y existen en aplicaciones antiguas o protectores de aplicaciones agresivos.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se violaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Executed Program has no installer	Se ejecutó una aplicación y no tiene instalador. Los atacantes sueltan sus ejecutables sin un instalador legítimo.	Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta mediante la pestaña Forense. Verifique si es una aplicación legítima o no.
Fake Critical Program - Program Attempted to Hide as a Service	Muchos programas maliciosos intentan ocultarse aparentando ser un proceso crítico del sistema, como un servicio. Esta alerta es un indicador muy claro de actividad maliciosa, ya que es raro que un software legítimo haga esto.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Fake Packer - A Fake Known Packer Detected	Un empaquetador es un componente de software que se utiliza principalmente para reducir el tamaño de los archivos ejecutables. Los empaquetadores son comúnmente utilizados por malware, instaladores de software y aplicaciones de protección de software. Sin embargo, el malware a menudo intenta disfrazarse de empaquetador común para evitar ser detectado por el software antivirus.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si el proceso eliminó archivos, recójalos también.
Hidden Process - Connection Attempt from a Hidden Process	Se detectó un intento de conexión desde un proceso que no era visible para el sistema operativo. Este tipo de proceso lo suele crear el malware para ocultarse. Algunos productos de seguridad también utilizan estas técnicas en dispositivos de 32 bits.	Utilice herramientas forenses del kernel con la capacidad de detectar procesos ocultos como GMER.
Injected Executable - Connection Attempt from an Injected Executable	El malware suele utilizar la inyección ejecutable para ocultar o ejecutar aplicaciones benignas. Esta técnica es muy común para permitir que el malware robe información de una aplicación en ejecución y extraiga datos. Esta técnica también la utilizan algunos productos de seguridad y software potencialmente no deseado.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Injected Process - Process Created from an Injected Thread	El proceso fue creado por un hilo que previamente se inyectó en una aplicación legítima. Los atacantes suelen hacer esto para que el nuevo proceso parezca válido ejecutándolo desde una aplicación legítima.	Recupere toda la memoria del proceso de la pestaña Forense, tanto para el proceso principal como para el inyectado. Utilícelos para realizar un análisis más profundo.

Injected Thread - Connection from an Injected Thread	Un hilo que se inyectó en la aplicación intentó establecer una conexión desde la aplicación inyectada. Los atacantes suelen hacer esto para engañar al sistema haciéndole creer que una aplicación legítima está intentando conectarse cuando el iniciador real de la conexión es una aplicación completamente diferente.	Recupere toda la memoria del proceso de la pestaña Forense, tanto para el proceso principal como para el inyectado. Utilícelos para realizar un análisis más profundo.
Invalid Checksum - Connection Attempt from Application with Invalid Checksum	Cada archivo ejecutable en el sistema tiene una suma de verificación asociada. En este caso la suma de comprobación era incorrecta. Muchas veces, el malware manipula otros archivos para propagarse, como instaladores, archivos del sistema, etc. Dicha manipulación cambia la suma de comprobación del archivo y puede indicar que fue manipulado. Rara vez se produce una suma de comprobación no válida en software legítimo que no se compiló o no se actualizó correctamente.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Invalid Execution - Code Executed from an Invalid Memory Location	Cada archivo ejecutable tiene secciones ejecutables predefinidas con límites bien definidos. Sin embargo, es posible hacer que las secciones no ejecutables sean ejecutables en tiempo de ejecución, generando efectivamente código nuevo. Este tipo de modificación lo utiliza habitualmente el malware para evadir el análisis de antivirus y otros productos de seguridad. De forma predeterminada, dichos ejecutables no pueden comunicarse.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si la aplicación no es legítima o no está familiarizado con la herramienta, solucione el dispositivo.
Invalid Pointer - Invalid Stack Pointer Value	Se detectó un puntero de pila no válido. El malware puede alterar el puntero de la pila para que apunte a una memoria no válida para evitar el seguimiento de la pila o como parte de un intento de explotación.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se violaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Kernel Injection - Code Injected from Kernel to User Mode	Inyectar código desde el kernel a los procesos del usuario es una técnica avanzada comúnmente utilizada por el malware del kernel (como Rootkits, Bootkits, Bios Infectors, etc.). Básicamente, permite que el malware ejecute código en cualquier proceso del sistema. Algunos productos de seguridad, como los antivirus, también utilizan la inyección de kernel.	Si conoce el ejecutable inyectado, consígalo para un análisis más profundo. Si conoce el controlador, obtenga el controlador del dispositivo objetivo para realizar un análisis más profundo. Controlador desconocido: utilice herramientas, como Volatility, para realizar un volcado de memoria completa del sistema y analizar la rutina del kernel especificada y la rutina del usuario especificada.
Keylogging Activity Detected	Un proceso intentó registrar las pulsaciones de teclas o la actividad del mouse de manera sospechosa. El malware puede registrar las pulsaciones de teclas del usuario para adquirir credenciales u otra información crítica. Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si la aplicación no es legítima o no está familiarizado con la herramienta, solucione el dispositivo.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si la aplicación no es legítima o no está familiarizado con la herramienta, solucione el dispositivo.

Known Packer - Activity by an Application packed by a Known Packer was detected	Un empaquetador es un componente de software que se utiliza principalmente para reducir el tamaño de los archivos ejecutables. Los empaquetadores son comúnmente utilizados por malware, instaladores de software y aplicaciones de protección de software. Sin embargo, el malware a menudo intenta disfrazarse de empaquetador común para evitar ser detectado por el software antivirus.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si el proceso eliminó archivos, recójalos también.
Malicious File Detected	Nuestro motor de aprendizaje automático o por otros medios identificó el archivo como malicioso, según el análisis del archivo.	Recupere el archivo ejecutable del dispositivo de destino, según su ruta. Utilice la pestaña Forense para realizar un análisis más profundo. Verificar el origen del fichero y su uso previsto en la organización.
Malicious Process - A Process is Interfering with Collector's Operation	Un proceso intentó intervenir maliciosamente con el componente o la configuración de Collector.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Malicious Website Detected - Attempt to access a malicious website, domain or IP address	Un sitio web, dominio o dirección IP fue identificado como malicioso por el servicio de inteligencia de FortiGuard Labs u otros medios. Los sitios web maliciosos o pirateados son un vector principal para iniciar ataques y pueden provocar descargas de malware, spyware u otro contenido riesgoso.	Examine el gráfico de eventos y vuelva a rastrear el proceso que inició el acceso al sitio web para saber si es parte de un programa sospechoso, un intento de phishing o un intento de navegación web insegura. Según su conclusión, realice un seguimiento con acciones correctivas, como eliminar programas relacionados o reparar otros dispositivos específicos.
Modified Executable - Connection from an In-Memory Modified Executable	Cada ejecutable cargado en la memoria del proceso se puede modificar durante el tiempo de ejecución. Sin embargo, se espera que algunas partes del ejecutable, como el código y los datos en formato de archivo, permanezcan constantes durante toda la vida del proceso. La modificación de estas secciones puede indicar un comportamiento malicioso, como descomprimir o un parche en memoria.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si el ejecutable modificado es un ejecutable del sistema, puede indicar que el código malicioso lo modificó. Si este es el caso, recupere toda la memoria del proceso utilizando la pestaña Forense.
Network Scanning Attempt Detected	Se detectaron escaneos del servicio de red. El malware puede utilizar un escaneo de red para enumerar servicios que se ejecutan en hosts remotos, como parte del reconocimiento de red que se realiza mientras se prepara para el movimiento lateral.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si no es una herramienta de escaneo conocida, repare el dispositivo. En caso contrario, verifique que la actividad fue realizada por un usuario autorizado.
Non-standard Communication - Use of non-standard communication method detected	Se detectó el uso de un método de comunicación no estándar. Los atacantes pueden aprovechar esto para extraer datos de forma sigilosa.	Si solo se activó esta regla, recupere el archivo ejecutable del dispositivo de destino que estableció esta conexión, según su ruta. Luego, utilice la pestaña Forense para realizar un análisis más profundo. Si se activaron más reglas, actúe de acuerdo con las otras reglas.

PUP - Potentially Unwanted Program	Un programa o aplicación que se consideraría no deseado a pesar de que un usuario haya dado su consentimiento para descargarlo e instalarlo. Los programas basura incluyen spyware, adware o barras de herramientas, etc.	Si esta es la única regla que se activó, recupere el archivo ejecutable del dispositivo de destino de acuerdo con su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.
Partially Mapped - Partially Mapped Executable File on Stack	Siempre que un proceso carga un nuevo ejecutable en la memoria, el ejecutable se asigna de acuerdo con su formato de archivo. Cuando un ejecutable se asigna al proceso con la intención de ejecutarlo, se asigna completamente a la memoria del proceso. Sin embargo, sólo es posible asignar una determinada parte de un ejecutable a la memoria y ejecutarlo. Esta acción es siempre el resultado de un comportamiento malicioso. Esta alerta también puede activarse si un rootkit (o producto de seguridad invasivo) intenta ocultar sus ejecutables.	Recupere la memoria del ejecutable del dispositivo de destino de acuerdo con la dirección base y la dirección final indicadas en la entrada de pila correspondiente utilizando la pestaña Forense.
Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Se detectó un exploit de escalada de privilegios. Los atacantes normalmente utilizan estos exploits para obtener el control total de un dispositivo vulnerado como parte de una cadena de exploits, toma de control del servidor o movimiento lateral. Esto, a su vez, puede resultar en el robo de fichas.	Este tipo de infracción normalmente se puede inferir comprobando el contexto de la alerta. Si el proceso o uno de sus padres es un navegador o un documento de Office, es probable que forme parte de una cadena de explotación. Si el proceso es un intérprete de línea de comando o powershell, es probable que sea parte de un movimiento lateral o un intento de toma de control del servidor.
Process Hollowing - Process Code Was Replaced	Process Hollowing es una técnica utilizada por el malware para hacerse pasar por un proceso legítimo eliminando el proceso original de su código y reemplazándolo con una carga útil maliciosa. Los atacantes encuentran esta técnica muy eficiente ya que el proceso parecerá válido, e incluso firmado, cuando se examine.	Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta mediante la pestaña Forense. Además, recupere una memoria de archivo ejecutable completa del proceso para un análisis más profundo.
Process Injection - Entry Point Modification Detected	La inyección de procesos es una técnica utilizada por el malware para hacerse pasar por un proceso legítimo, en el que el flujo de ejecución del proceso se modifica para ejecutar código malicioso. Esta técnica es muy eficaz para los piratas informáticos, ya que el proceso parece válido e incluso está firmado cuando se examina. Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta utilizando la pestaña Forense. Además, recupere una memoria de archivo ejecutable completa del proceso para un análisis más profundo.	Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta utilizando la pestaña Forense. Además, recupere una memoria de archivo ejecutable completa del proceso para un análisis más profundo.

Protected System Configuration - Modification Attempt of Protected Configuration	Un proceso intentó modificar la configuración de registros de recopilación importantes u otras configuraciones protegidas. Dichos registros son esenciales para identificar actividades maliciosas y para proporcionar el contexto y los detalles de las acciones realizadas por los atacantes. Es posible que esta regla haya sido activada por un proceso malicioso que intentó cubrir sus huellas.	Es posible que un usuario haya intentado modificar manualmente la configuración del sistema. Utilice la pestaña Forense para recuperar el archivo ejecutable del dispositivo de destino según su ruta para examinarlo. Para solucionarlo, restaure la configuración modificada a su valor original en el dispositivo. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.
Stack Pivot - Stack Pointer is Out of Bounds	Cada hilo del sistema operativo tiene una pila. La pila de cada hilo tiene asignado un espacio de direcciones bien definido. El malware puede alterar el puntero de la pila y hacer que apunte fuera de estos límites. La alteración del puntero de la pila se realiza como parte de una etapa de explotación o para eludir el software de protección que depende del seguimiento de la pila. Las pilas ejecutables son raras y existen en aplicaciones antiguas o protectores de aplicaciones agresivos.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se activaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Stack Tampering - Stack Collection Interrupted	Cada hilo del sistema operativo tiene una pila. La pila del hilo fue manipulada. El malware puede hacer esto para impedir la recopilación de una pila completa.	Recupere toda la memoria del proceso de destino desde la pestaña Forense para un análisis más profundo.
Suspicious Application - Connection Attempt from a Suspicious Application	Algunas aplicaciones no inician conexiones a la red por sí solas, pero los actores de amenazas aún las utilizan comúnmente para filtrar datos de la red. La comunicación desde dichas aplicaciones está bloqueada de forma predeterminada.	
Suspicious Macro - A macro has performed suspicious actions	Una macro que forma parte de otra aplicación (por ejemplo, Microsoft Office) intentó establecer una conexión. Los atacantes suelen incorporar macros en documentos en un intento de incitar al usuario a activar su código malicioso.	Si los datos de la línea de comandos del proceso incluyen el tipo de archivo de la aplicación (por ejemplo, XYZ.doc), se recomienda verificar con el usuario que tenía la intención de ejecutar una macro.
Suspicious Packer - Activity by an Application packed by a Suspicious Packer was detected	Un empaquetador es un componente de software que se utiliza principalmente para reducir el tamaño de los archivos ejecutables. Los empaquetadores son comúnmente utilizados por malware, instaladores de software y aplicaciones de protección de software. Sin embargo, el malware a menudo intenta disfrazarse de empaquetador común para evitar ser detectado por el software antivirus.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si el proceso eliminó archivos, recójalos también. Nota: Algunos programas protegidos también utilizan empaquetadores sospechosos y pueden activar esta regla.
Suspicious Script Execution - A script was executed in a suspicious context	Un script fue ejecutado mediante un proceso sospechoso. Los atacantes utilizan esta técnica para lograr acceso remoto al dispositivo sin dejar de ser sigilosos.	Inspeccionar los datos de la línea de comandos del proceso para comprender el contexto de la ejecución del script.

Tampered Executable - Critical Executable was Tampered With	Un ejecutable que es fundamental para el funcionamiento de Collector o del sistema operativo fue manipulado de alguna manera. Los ejecutables críticos pueden incluir ejecutables de Collector, ejecutables relacionados con redes, etc. Este comportamiento se debe únicamente a un malware.	Recupere toda la memoria del proceso utilizando la pestaña Forense según la dirección virtual para un análisis más profundo. Generalmente es más fácil comenzar con el ejecutable manipulado.
Unconfirmed Executable - Executable File Failed Verification Test	Cada archivo ejecutable en el sistema operativo tiene un formato de archivo bien definido. Este formato de archivo tiene muchos campos que el sistema operativo no aplica, pero que el malware puede utilizar para complicar su análisis. La gravedad de esta regla es Media porque también puede indicar un programa no deseado, un protector de aplicación o simplemente una aplicación que se compiló incorrectamente.	Si esta es la única regla que se activó, recupere el archivo ejecutable del dispositivo de destino según su ruta mediante la pestaña Análisis forense. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.
Unmapped Executable - Executable File Without a Corresponding File System Reference	Un ejecutable que se ejecuta en la memoria no tiene un archivo correspondiente en el sistema de archivos. Por lo tanto, el malware puede ocultarse en la memoria de proceso sin aparecer en la lista del sistema operativo. Comúnmente, esta técnica es utilizada tanto por Advanced Persistent Threat (APT) como por Volatile Persistent Threat (VPT). También lo pueden utilizar instaladores de aplicaciones o protectores de aplicaciones muy agresivos, aunque este escenario es poco común.	Vaya a la pestaña Análisis forense. Obtenga la dirección base y la dirección final, como se especifica en la entrada de pila correspondiente. Recupere la memoria del dispositivo objetivo de acuerdo con estas direcciones de memoria utilizando la pestaña Forense y realice un análisis más profundo.
Writable Code - Identified an Executable with Writable Code	Cada archivo ejecutable tiene secciones ejecutables predefinidas. Normalmente, estas secciones son de solo lectura y no se pueden modificar a menos que los atributos de protección se modifiquen explícitamente en tiempo de ejecución. Una acción de este tipo normalmente es una indicación de manipulación del código ejecutable en tiempo de ejecución. Este tipo de acción es común en malware y exploits que intentan modificar el código de ejecutables en memoria.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si el ejecutable modificado es un ejecutable del sistema, puede indicar que el código malicioso lo modificó. Si este es el caso, recupere toda la memoria del proceso utilizando la pestaña Forense.

Ransomware Prevention

Regla	Detalles	Acciones que tomar
Debugged Process - Connection from a Debugged Process	Se identificó un proceso que se está depurando. El malware puede utilizar técnicas de autodepuración para dificultar la ingeniería inversa. Esta regla también puede activarse cuando un usuario legítimo depura un proceso del sistema que se conecta externamente.	Verifique que el usuario del dispositivo no haya ejecutado un depurador cuando se desencadenó el evento.

Disk encryption attempt detected - Suspicious full disk encryption was detected	El cifrado de disco completo está diseñado para proteger los datos cifrando volúmenes enteros de modo que los datos no se puedan leer sin una autenticación exitosa. En algunos casos, está integrado en el sistema operativo. Por ejemplo, en Windows 10 donde se le conoce como BitLocker. El ransomware puede utilizar capacidades de cifrado integradas para bloquear una unidad mientras reemplaza las claves de recuperación. Esta regla también puede activarse cuando se realiza un cifrado legítimo del disco completo.	Si el cifrado completo del disco es parte de la política de su organización, puede deshabilitar esta regla temporalmente y luego volver a habilitarla después de configurar los ajustes iniciales para evitar que un atacante altere o anule la configuración de BitLocker. También puede hacer esto si el cifrado completo del disco ya está habilitado en este dispositivo o si solo se realiza una vez en máquinas nuevas. De lo contrario, si no utiliza Bitlocker, recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Dynamic Code - Malicious Runtime Generated Code Detected	El origen de la mayor parte del código del proceso proviene de un archivo. Sin embargo, es posible generar código en tiempo de ejecución sin el archivo correspondiente. Es extremadamente difícil identificar el código generado en tiempo de ejecución como malicioso. Como tal, este tipo de código es comúnmente utilizado por malware y exploits para ejecutar su carga útil.	Vaya a la pestaña Análisis forense. Obtenga la dirección base y la dirección final como se especifica en la entrada de la pila correspondiente. Recupere la memoria del dispositivo objetivo de acuerdo con estas direcciones de memoria utilizando la pestaña Forense y realice un análisis más profundo.
Executable Format - Bad Executable File Format	Cada archivo ejecutable en el sistema operativo tiene un formato de archivo bien definido. Uno o más de los archivos ejecutables parecen tener una estructura sospechosa o no válida. El mal formato también puede existir en protectores de aplicaciones muy agresivos.	Si esta es la única regla que se violó, recupere el archivo ejecutable del dispositivo objetivo según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Utilice herramientas de análisis de archivos ejecutables, como CFFExplorer (herramienta) con la información proporcionada en la entrada de la pila correspondiente para comprender mejor la infracción de formato.
Executable Stack - A Stack with Executable Code	La pila de la aplicación (memoria dinámica) parece contener código ejecutable. Los atacantes suelen hacer que la pila sea ejecutable durante la etapa de explotación para poder ejecutar el código desde la pila de la aplicación. Las pilas ejecutables son raras y existen en aplicaciones antiguas o protectores de aplicaciones agresivos.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se violaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Executed Program has no installer	Se ejecutó una aplicación y no tiene instalador. Los atacantes sueltan sus ejecutables sin un instalador legítimo.	Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta mediante la pestaña Forense. Verifique si es una aplicación legítima o no.
Fake Critical Program - Program Attempted to Hide as a Service	Muchos programas maliciosos intentan ocultarse aparentando ser un proceso crítico del sistema, como un servicio. Esta alerta es un indicador muy claro de actividad maliciosa, ya que es raro que un software legítimo haga esto.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.

Fake Packer - A Fake Known Packer Detected	Un empaquetador es un componente de software que se utiliza principalmente para reducir el tamaño de los archivos ejecutables. Los empaquetadores son comúnmente utilizados por malware, instaladores de software y aplicaciones de protección de software. Sin embargo, el malware a menudo intenta disfrazarse de empaquetador común para evitar ser detectado por el software antivirus.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si el proceso eliminó archivos, recójalos también.
File Encryptor - Suspicious file modification	Un proceso intentó cifrar archivos o realizar modificaciones sospechosas en los archivos.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Además, recupere el archivo que estaba cifrado y verifique si debería haberse modificado. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.
Hidden Process - Connection Attempt from a Hidden Process	Se detectó un intento de conexión desde un proceso que no era visible para el sistema operativo. Este tipo de proceso lo suele crear el malware para ocultarse. Algunos productos de seguridad también utilizan estas técnicas en dispositivos de 32 bits.	Utilice herramientas forenses del kernel con la capacidad de detectar procesos ocultos como GMER (es una herramienta de rootkit y anti-forense que puede usarse para ocultar archivos, procesos y entradas del registro).
Injected Executable - Connection Attempt from an Injected Executable	El malware suele utilizar la inyección ejecutable para ocultar/ejecutar aplicaciones benignas. Esta técnica es muy común para permitir que el malware robe información de una aplicación en ejecución y extraiga datos. Esta técnica también la utilizan algunos productos de seguridad y software potencialmente no deseado.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Injected Process - Process Created from an Injected Thread	El proceso fue creado por un hilo que previamente se inyectó en una aplicación legítima. Los atacantes suelen hacer esto para que el nuevo proceso parezca válido ejecutándolo desde una aplicación legítima.	Recupere toda la memoria del proceso de la pestaña Forense, tanto para el proceso principal como para el inyectado. Utilícelos para realizar un análisis más profundo.
Injected Thread - Connection from an Injected Thread	Un hilo (ejecución de proceso) que se inyectó en la aplicación intentó establecer una conexión desde la aplicación inyectada. Los atacantes suelen hacer esto para engañar al sistema haciéndole creer que una aplicación legítima está intentando conectarse cuando el iniciador real de la conexión es una aplicación completamente diferente.	Recupere toda la memoria del proceso de la pestaña Forense, tanto para el proceso principal como para el inyectado. Utilícelos para realizar un análisis más profundo.
Invalid Checksum - Connection Attempt from Application with Invalid Checksum	Cada archivo ejecutable en el sistema tiene una suma de verificación asociada. En este caso la suma de comprobación era incorrecta. Muchas veces, el malware manipula otros archivos para propagarse, como instaladores, archivos del sistema, etc. Dicha manipulación cambia la suma de comprobación del archivo y puede indicar que fue manipulado. Rara vez se produce una suma de comprobación no válida en software legítimo que no se compiló o no se actualizó correctamente.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.

Invalid Execution - Code Executed from an Invalid Memory Location	Cada archivo ejecutable tiene secciones ejecutables predefinidas con límites bien definidos. Sin embargo, es posible hacer que las secciones no ejecutables sean ejecutables en tiempo de ejecución, generando efectivamente código nuevo. Este tipo de modificación lo utiliza habitualmente el malware para evadir el análisis de antivirus y otros productos de seguridad. De forma predeterminada, dichos ejecutables no pueden comunicarse.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si la aplicación no es legítima o no está familiarizado con la herramienta, solucione el dispositivo.
Invalid Pointer - Invalid Stack Pointer Value	Se detectó un puntero de pila no válido. El malware puede alterar el puntero de la pila para que apunte a una memoria no válida para evitar el seguimiento de la pila o como parte de un intento de explotación.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se violaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Kernel Injection - Code Injected from Kernel to User Mode	Inyectar código desde el kernel a los procesos del usuario es una técnica avanzada comúnmente utilizada por el malware del kernel (como Rootkits, Bootkits, Bios Infectors, etc.). Básicamente, permite que el malware ejecute código en cualquier proceso del sistema. Algunos productos de seguridad, como los antivirus, también utilizan la inyección de kernel.	Si conoce el ejecutable inyectado, consígalo para un análisis más profundo. Si conoce el controlador, obtenga el controlador del dispositivo objetivo para realizar un análisis más profundo. Controlador desconocido: utilice herramientas, como Volatility, para realizar un volcado de memoria completa del sistema y analizar la rutina del kernel especificada y la rutina del usuario especificada.
Known Packer - Activity by an Application packed by a Known Packer was detected	Un empaquetador es un componente de software que se utiliza principalmente para reducir el tamaño de los archivos ejecutables. Los empaquetadores son comúnmente utilizados por malware, instaladores de software y aplicaciones de protección de software. Sin embargo, el malware a menudo intenta disfrazarse de empaquetador común para evitar ser detectado por el software antivirus.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si el proceso eliminó archivos, recójalos también.
Malicious File Detected	Nuestro motor de aprendizaje automático o por otros medios identificó el archivo como malicioso, según el análisis del archivo.	Recupere el archivo ejecutable del dispositivo de destino, según su ruta. Utilice la pestaña Forense para realizar un análisis más profundo. Verificar el origen del archivo y su uso previsto en la organización.
Malicious Process - A Process is Interfering with Collector's Operation	Un proceso intentó intervenir maliciosamente con el componente o la configuración de Collector.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo.
Modified Executable - Connection from an In-Memory Modified Executable	Cada ejecutable cargado en la memoria del proceso se puede modificar durante el tiempo de ejecución. Sin embargo, se espera que algunas partes del ejecutable, como el código y los datos en formato de archivo, permanezcan constantes durante toda la vida del proceso. La modificación de estas secciones puede indicar un comportamiento malicioso, como descomprimir o un parche en memoria.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si el ejecutable modificado es un ejecutable del sistema, puede indicar que el código malicioso lo modificó. Si este es el caso, recupere toda la memoria del proceso utilizando la pestaña Forense.

PUP - Potentially Unwanted Program	Un programa o aplicación que se consideraría no deseado a pesar de que un usuario haya dado su consentimiento para descargarlo e instalarlo. Los programas basura incluyen spyware, adware o barras de herramientas, etc.	Si esta es la única regla que se activó, recupere el archivo ejecutable del dispositivo de destino de acuerdo con su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.
Partially Mapped - Partially Mapped Executable File on Stack	Siempre que un proceso carga un nuevo ejecutable en la memoria, el ejecutable se asigna de acuerdo con su formato de archivo. Cuando un ejecutable se asigna al proceso con la intención de ejecutarlo, se asigna completamente a la memoria del proceso. Sin embargo, sólo es posible asignar una determinada parte de un ejecutable a la memoria y ejecutarlo. Esta acción es siempre el resultado de un comportamiento malicioso. Esta alerta también puede activarse si un rootkit (o producto de seguridad invasivo) intenta ocultar sus ejecutables.	Recupere la memoria del ejecutable del dispositivo de destino de acuerdo con la dirección base y la dirección final indicadas en la entrada de pila correspondiente utilizando la pestaña Forense.
Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Se detectó un exploit de escalada de privilegios. Los atacantes normalmente utilizan estos exploits para obtener el control total de un dispositivo vulnerado como parte de una cadena de exploits, toma de control del servidor o movimiento lateral. Esto, a su vez, puede resultar en el robo de fichas.	Este tipo de infracción normalmente se puede inferir comprobando el contexto de la alerta. Si el proceso o uno de sus padres es un navegador o un documento de Office, es probable que forme parte de una cadena de explotación. Si el proceso es un intérprete de línea de comando o powershell, es probable que sea parte de un movimiento lateral o un intento de toma de control del servidor.
Process Hollowing - Process Code Was Replaced	Process Hollowing es una técnica utilizada por el malware para hacerse pasar por un proceso legítimo eliminando el proceso original de su código y reemplazándolo con una carga útil maliciosa. Los atacantes encuentran esta técnica muy eficiente ya que el proceso parecerá válido, e incluso firmado, cuando se examine.	Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta mediante la pestaña Forense. Además, recupere una memoria de archivo ejecutable completa del proceso para un análisis más profundo.
Process Injection - Entry Point Modification Detected	La inyección de procesos es una técnica utilizada por el malware para hacerse pasar por un proceso legítimo, en el que el flujo de ejecución del proceso se modifica para ejecutar código malicioso. Esta técnica es muy eficaz para los piratas informáticos, ya que el proceso parece válido e incluso está firmado cuando se examina. Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta utilizando la pestaña Forense. Además, recupere una memoria de archivo ejecutable completa del proceso para un análisis más profundo.	Recupere el archivo ejecutable del proceso principal del dispositivo de destino según su ruta utilizando la pestaña Forense. Además, recupere una memoria de archivo ejecutable completa del proceso para un análisis más profundo.

Stack Pivot - Stack Pointer is Out of Bounds	Cada hilo del sistema operativo tiene una pila. La pila de cada hilo tiene asignado un espacio de direcciones bien definido. El malware puede alterar el puntero de la pila y hacer que apunte fuera de estos límites. La alteración del puntero de la pila se realiza como parte de una etapa de explotación o para eludir el software de protección que depende del seguimiento de la pila. Las pilas ejecutables son raras y existen en aplicaciones antiguas o protectores de aplicaciones agresivos.	Si esta es la única regla que se violó, recupere toda la memoria del proceso de la pestaña Forense para un análisis más profundo. Si se activaron otras reglas, primero siga las recomendaciones forenses para las otras reglas.
Stack Tampering - Stack Collection Interrupted	Cada hilo del sistema operativo tiene una pila. La pila del hilo fue manipulada. El malware puede hacer esto para impedir la recopilación de una pila completa.	Recupere toda la memoria del proceso de destino desde la pestaña Forense para un análisis más profundo.
Suspicious Application - Connection Attempt from a Suspicious Application	Algunas aplicaciones no inician conexiones a la red por sí solas, pero los actores de amenazas aún las utilizan comúnmente para filtrar datos de la red. La comunicación desde dichas aplicaciones está bloqueada de forma predeterminada.	
Suspicious Packer - Activity by an Application packed by a Suspicious Packer was detected	Un empaquetador es un componente de software que se utiliza principalmente para reducir el tamaño de los archivos ejecutables. Los empaquetadores son comúnmente utilizados por malware, instaladores de software y aplicaciones de protección de software. Sin embargo, el malware a menudo intenta disfrazarse de empaquetador común para evitar ser detectado por el software antivirus.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense para realizar un análisis más profundo. Si el proceso eliminó archivos, recójalos también. Nota: Algunos programas protegidos también utilizan empaquetadores sospechosos y pueden activar esta regla.
Tampered Executable - Critical Executable was Tampered With	Un ejecutable que es fundamental para el funcionamiento de Collector o del sistema operativo fue manipulado de alguna manera. Los ejecutables críticos pueden incluir ejecutables de Collector, ejecutables relacionados con redes, etc. Este comportamiento se debe únicamente a un malware.	Recupere toda la memoria del proceso utilizando la pestaña Forense según la dirección virtual para un análisis más profundo. Generalmente es más fácil comenzar con el ejecutable manipulado.
Unconfirmed Executable - Executable File Failed Verification Test	Cada archivo ejecutable en el sistema operativo tiene un formato de archivo bien definido. Este formato de archivo tiene muchos campos que el sistema operativo no aplica, pero que el malware puede utilizar para complicar su análisis. La gravedad de esta regla es Media porque también puede indicar un programa no deseado, un protector de aplicación o simplemente una aplicación que se compiló incorrectamente.	Si esta es la única regla que se activó, recupere el archivo ejecutable del dispositivo de destino según su ruta mediante la pestaña Análisis forense. Si se violaron más reglas, primero siga las recomendaciones forenses para las otras reglas.

Unmapped Executable - Executable File Without a Corresponding File System Reference	Un ejecutable que se ejecuta en la memoria no tiene un archivo correspondiente en el sistema de archivos. Por lo tanto, el malware puede ocultarse en la memoria de proceso sin aparecer en la lista del sistema operativo. Comúnmente, esta técnica es utilizada tanto por Advanced Persistent Threat (APT) como por Volatile Persistent Threat (VPT). También lo pueden utilizar instaladores de aplicaciones o protectores de aplicaciones muy agresivos, aunque este escenario es poco común.	Vaya a la pestaña Análisis forense. Obtenga la dirección base y la dirección final, como se especifica en la entrada de pila correspondiente. Recupere la memoria del dispositivo objetivo de acuerdo con estas direcciones de memoria utilizando la pestaña Forense y realice un análisis más profundo.
Writable Code - Identified an Executable with Writable Code	Cada archivo ejecutable tiene secciones ejecutables predefinidas. Normalmente, estas secciones son de solo lectura y no se pueden modificar a menos que los atributos de protección se modifiquen explícitamente en tiempo de ejecución. Una acción de este tipo normalmente es una indicación de manipulación del código ejecutable en tiempo de ejecución. Este tipo de acción es común en malware y exploits que intentan modificar el código de ejecutables en memoria.	Recupere el archivo ejecutable del dispositivo de destino según su ruta utilizando la pestaña Forense. Si el ejecutable modificado es un ejecutable del sistema, puede indicar que el código malicioso lo modificó. Si este es el caso, recupere toda la memoria del proceso utilizando la pestaña Forense.

Revisiones y/o modificaciones

09/05/2023

04/10/2023

05/05/2024 al 09/05/2024

07/01/2025