IBM Security QRadar Incident Forensics
Versión 7.2.6

Guía de administración

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 21.

Información sobre el producto

Este documento corresponde a IBM QRadar Security Intelligence Platform V7.2.6 y a todos los releases subsiguientes a menos sea reemplazado por una versión actualizada de este documento.

Contenido

Introducción a la administración de IBM Security QRadar Incident Forensics

Información sobre la administración de IBM® Security QRadar Incident Forensics.

Público al que se dirige

Los administradores crean, mantienen y utilizan una prestación de análisis forense activo para que los usuarios, denominados investigadores, puedan concentrarse en investigar los incidentes de seguridad, o casos, y explorar los datos.

Documentación técnica

Para buscar documentación del producto IBM Security QRadar en la web, incluida toda la documentación traducida, acceda al Knowledge Center de IBM (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obtener información sobre el acceso a más documentación técnica en la biblioteca de productos de QRadar, consulte Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Cómo ponerse en contacto con el servicio de soporte al cliente

Para obtener información acerca de cómo ponerse en contacto con el servicio de soporte al cliente, consulte la nota técnica sobre soporte y descarga (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de TI implica la protección de sistemas e información mediante la prevención, la detección y la respuesta a accesos indebidos desde dentro o fuera de la empresa. Un acceso indebido puede alterar, destruir o dar un uso inapropiado de la información o puede ocasionar daños o un uso erróneo de sus sistemas, incluidos los ataques a terceros. Ningún producto ni sistema de TI debe considerarse completamente seguro, y ningún producto, servicio o medida de seguridad por sí solo debe considerarse totalmente eficaz para evitar el acceso o el uso indebidos. Los sistemas, productos y servicios de IBM están diseñados como parte de un procedimiento global de seguridad de acuerdo con la legalidad vigente, lo que implica necesariamente procedimientos operativos adicionales, y pueden requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALICIOSAS O ILEGALES DE TERCEROS.

Tenga en cuenta lo siguiente:

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. El Cliente se compromete a utilizar este Programa de acuerdo con, y asume toda la responsabilidad en lo que

se refiere al cumplimiento de, las leyes, normativas y políticas aplicables. El licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

Nota

IBM Security QRadar Incident Forensics se ha diseñado para ayudar a las compañías a mejorar su entorno de seguridad y sus datos. Más concretamente, IBM Security QRadar Incident Forensics se ha diseñado para ayudar a las compañías a investigar y comprender mejor lo ocurrido en los incidentes de seguridad de red. La herramienta permite a las compañías indexar los datos de paquetes de red capturados (PCAP) y hacer búsquedas en ellos, e incluye una característica que puede reconstruir esos datos con su formato original. Esta característica de reconstrucción puede reconstruir datos y archivos, incluidos los mensajes de correo electrónico, los adjuntos de tipo archivo e imagen, las llamadas telefónicas de VoIP y los sitios web. En los manuales y otra documentación que se adjunta con el programa encontrará más información acerca de las funciones y características del programa y la manera de configurarlo. El uso de este programa puede involucrar diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar Incident Forensics solamente se puede utilizar para fines que respeten la legalidad de una forma que también respete la legalidad. El Cliente se compromete a utilizar este Programa de acuerdo con, y asume toda la responsabilidad en lo que se refiere al cumplimiento de, las leyes, normativas y políticas aplicables. El licenciatario afirma que obtendrá o que ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso de forma legal de IBM Security QRadar Incident Forensics.

Capítulo 1. Novedades para administradores en QRadar Incident Forensics V7.2.6

IBM Security QRadar Incident Forensics V7.2.6 presenta inspectores nuevos que identifican más protocolos, dominios web y tipos de archivo. Los administradores también pueden auditar el uso del sistema y de usuario.

QRadar Incident Forensics puede procesar más protocolos, dominios web y tipos de archivo

Ahora se da soporte a más inspectores que pueden identificar varios protocolos, dominios web y tipos de archivo en archivos de captura de paquetes (PCAP) y cargar documentos.

SPDY Un protocolo de red abierto que se utiliza para transportar contenido web desarrollado para reducir el tiempo que se tarda en cargar páginas web y en mejorar la seguridad web.

Samba (SMB)
Bloque de mensajes de servidor (SMB) es un protocolo para compartir archivos, impresoras, puertos serial y comunicaciones, como por ejemplo comunicaciones por conducto y buzones entre sistemas. Se da soporte a la versión 1.

Clasificación de aplicación web (WAC)
QRadar Incident Forensics inspecciona un URL y puede identificar el tipo de aplicación web y operación. Utiliza la información para clasificar el tráfico en clases, según la aplicación web y la operación.

Detección de aplicación de QFlow
Detección de aplicación de QFlow se utiliza cuando ningún otro inspector puede detectar una aplicación, sesión o un protocolo. La detección de aplicación QFlow inspecciona los primeros 64 bytes de un paquete para una firma e intenta identificar la aplicación desde la firma y el puerto.

 Conocer más...

Registros de auditoría para hacer un seguimiento y registrar la actividad de aplicación y de usuario

Los registros de auditoría hacen visible lo que están haciendo los analistas de seguridad, incluidas las acciones que realizan, los datos a los que acceden y la información que están viendo. La evidencia documental registra la secuencia de actividades que se han realizado durante una investigación.

Las actividades siguientes generan sucesos de registro de auditoría:

- Crear caso
- Suprimir caso
- Suprimir colección
- Todas las consultas de usuario
- Vista de documento
- Exportar documento

 Conocer más...

Capítulo 2. Flujo de trabajo de administración y acceso de usuario a prestaciones de análisis forense

Después de instalar y configurar IBM Security QRadar Incident Forensics, un administrador puede resolver problemas, realizar el mantenimiento y supervisar el sistema y sus operaciones, y gestionar el acceso del usuario a casos.

Debe tener privilegios administrativos para ver las herramientas de administración de QRadar Incident Forensics.

Ejemplo: flujo de trabajo de administración

El diagrama siguiente muestra un flujo de trabajo de ejemplo para la administración de QRadar Incident Forensics.

1. Utilice la herramienta Gestión de casos para descartar por filtración las categorías y tráfico web que no desee supervisar.
2. Utilice Permisos de usuario de análisis forense para asignar casos a investigadores.
3. Utilice Gestión de casos para crear y suprimir casos e importar contenido externo al sistema.
4. Utilice Acciones planificadas para planificar tareas de mantenimiento, tales como suprimir documentos antiguos, ajustar la base de datos y restablecer el servidor de QRadar Incident Forensics.

Roles de usuario

Para añadir cuentas de usuario, debe primero crear perfiles de seguridad para cumplir los requisitos de acceso específicos de los usuarios. Para obtener más información sobre cómo crear perfiles de seguridad, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

En la herramienta Roles de usuario del panel **Admin** de QRadar, puede asignar los roles de usuario siguientes:

Admin
: Los usuarios pueden ver y acceder a todos los casos que están asignados a los usuarios e incidentes, y se les otorga automáticamente acceso total a QRadar Incident Forensics.

Análisis forense
: Los usuarios pueden ver y acceder al panel **Análisis forense**, pero no pueden crear casos.

Crear casos en Incident Forensics
: Los usuarios pueden crear automáticamente casos forenses.

Capítulo 3. Gestión de servidor

Los administradores pueden resolver problemas, realizar el mantenimiento y supervisar el sistema IBM Security QRadar Incident Forensics y sus operaciones.

Para supervisar o cambiar valores de servidor o ver los usuarios que están conectados al sistema, abra la herramienta Gestión de servidores:

1. Inicie una sesión en QRadar como administrador.
2. Pulse la pestaña **Admin**.
3. En la sección **Análisis forense** del panel principal, pulse **Gestión de servidores**.

Valores de configuración del servidor

Utilice los valores del servidor de la herramienta Gestión de servidor de IBM Security QRadar Incident Forensics para configurar los valores de servidor que afectan a todos los hosts gestionados. Después de cambiar un valor, debe desplegar los cambios utilizando el menú **Desplegar cambios** en la pestaña **Admin**.

Borrar historial de búsqueda al salir
El historial de búsqueda se borra cuando el usuario cierra la sesión. Las búsquedas borradas se aplican a la lista de historial de consulta en Query Helper y al último usuario del campo **Search Criteria Input** de la página Search and Results.

Número predeterminado de nodos para visualizar
Número máximo de nodos que muestra la herramienta Visualizar. Puede definir el número de nodos que se muestran después de ser mostrados por primera vez. El ajuste del número de nodos que se muestran afecta solamente a esa instancia de la herramienta Visualizar.

Filtros del inspector de protocolos y dominios

Puede excluir determinados tipos de tráfico en las investigaciones desactivando inspectores de protocolos o dominios en la herramienta Gestión de servidores. Utilice la opción **Filtro de inspector**.

Los inspectores de protocolos y dominios procesan datos de tráfico de red absorbidos e intentan identificar e indexar los datos de una forma útil. La identificación e indexación de esos datos proporciona a los investigadores un mayor control para encontrar la información.

A medida que se absorben los datos de tráfico de red y se identifican los protocolos, el inspector de protocolos adecuado inspecciona más a fondo los datos. Los datos de tráfico de red identificados por el inspector del protocolo HTTP son inspeccionados e indexados adicionalmente por los inspectores de dominios.

Inspectores de protocolos
Los inspectores de protocolos pueden identificar protocolos tales como HTTP, POP3, FTP y telnet. Puede excluir inspectores de protocolos. Cuando excluye inspectores de protocolos, se siguen absorbiendo los datos de tráfico de red asociados al inspector, pero el tráfico se identifica e indexa solamente a nivel genérico.

Inspectores de dominios

Los inspectores de dominios inspeccionan sitios web determinados. Puede excluir inspectores de dominios. Cuando excluye inspectores de dominios, se siguen absorbiendo los datos de tráfico de red HTTP asociados al inspector, pero el tráfico se identifica e indexa solamente a nivel HTTP. Para que los inspectores de dominios estén activos, el inspector del protocolo HTTP también debe estar activo.

De forma predeterminada, todos los filtros están activados y puede ver el tráfico de todos los protocolos. La única excepción es el tráfico SIP (Protocolo de inicio de sesiones). Este protocolo de configuración de llamadas, que funciona en la capa de aplicación, está desactivado de forma predeterminada.

Recuerde: Cuando cambia la configuración de los filtros de inspector, la configuración nueva se aplica a cada caso nuevo creado. Los inspectores activados influyen en los documentos creados para un caso y los investigadores pierden la capacidad de buscar determinados inspectores. Los usuarios no saben qué inspectores de aplican a un caso.

Cualquier protocolo no procesado por un inspector está categorizado como desconocido.

Filtro de categoría web

Puede elegir los tipos de páginas web y servidores web reconocidos mediante filtros de categoría web.

Por ejemplo, puede excluir tipos determinados de tráfico de red HTTP en las investigaciones. Cuando se absorben datos de tráfico de red HTTP, se clasifican los datos y se agrupan los documentos resultantes.

Los administradores pueden filtrar los datos de tráfico de red HTTP para evitar su absorción.

Para excluir o filtrar tráfico para una categoría o grupo, desactive la categoría o grupo en la herramienta Gestión de servidor.

La categorización, la agrupación y el filtrado web afectan a los datos de tráfico de red HTTP mientras se están absorbiendo y no tienen ningún efecto en los datos que ya están en el sistema.

Cuando un filtro de grupo está establecido para excluir datos, los datos de tráfico de red HTTP que están asociados a categorías de ese grupo se descartan por filtración durante el consumo, sin importar los valores de filtro de categoría asociados.

Ejemplo: ¿Qué ocurre cuando utiliza un filtro de categoría web para excluir tráfico?

Ha decidido excluir el tráfico que contiene datos de los sitios de noticias o revistas.

1. En la pestaña **Admin**, en QRadar, pulse **Gestión de servidor**.
2. Pulse **Filtro de categoría web** y pulse **Desactivado** junto al filtro **Noticias / Revistas**.
3. Pulse el filtro **Webmail / Mensaje unificado** y pulse **Activado**.

Ahora, cuando un usuario investiga el tráfico ingerido en la pestaña **Análisis forense**, verá que el tráfico contiene datos de **Noticias / Revistas** y que **Webmail / Mensaje unificado** no se absorbe aunque el filtro **Webmail / Mensaje unificado** está activado.

Protocolos y tipos de documentos soportados

IBM Security QRadar Incident Forensics captura el contenido de los paquetes del flujo de red e indexa y procesa la carga útil y los metadatos.

La lista siguiente indica los protocolos soportados que QRadar Incident Forensics puede procesar:

- AIM
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- IMAP
- IRC
- Jabber
- Myspace
- NFS
- SIP
- NetBIOS
- Oracle
- POP3
- SMB
- SMTP
- SPDY
- TLS (SSL)
- SSH
- Telnet
- Yahoo Messenger
- MySQL

La lista siguiente indica los dominios soportados (sitios web) y los idiomas soportados para el dominio que QRadar Incident Forensics puede procesar:

- AOL (Accessible, Basic, Standard) (EN)
- Charter (EN)
- Facebook (Mobile, Desktop) (AR,CN,DE,EN,ES,FR,RU)
- Gmail (Classic, Standard) (AR,CN,DE,EN,ES,FR,RU)
- Hotmail (AR,CN,DE,EN,ES,FR,RU)
- LinkedIn (DE,EN,ES,FR,RU)
- MailCom (CN,EN,ES,FR,RU)
- MailRu (RU)
- Maktoob (AR,EN)
- Myspace (EN)

- QQMail (EN,CN)
- Twitter (EN)
- YAHOO Mail (Standard, Classic) (EN)
- YAHOO Note (EN)
- YouTube (AR,CN,DE,EN,ES,FR,RU)
- Comcast (Zimbra) (EN)

La lista siguiente indica los formatos de documento soportados que QRadar Incident Forensics puede procesar:

- HyperText Markup Language
- XML y formatos derivados
- Formatos de documento de Microsoft Office
- OpenDocument Format
- Portable Document Format
- Electronic Publication Format
- Rich Text Format
- Formatos de compresión y empaquetado
- Formatos de texto
- Formatos de audio
- Formatos de imagen
- Formatos de vídeo
- Archivos de clase y archivos Java™
- Formato mbox

Detección de aplicación de QFlow

Detección de aplicación de QFlow se utiliza cuando ningún otro inspector puede detectar una aplicación, sesión o un protocolo. La detección de aplicación QFlow inspecciona los primeros 64 bytes de un paquete para una firma e intenta identificar la aplicación desde la firma y el puerto. A continuación de proporciona una lista no exclusiva de algunos ejemplos de aplicaciones, sesiones o protocolos que la detección de aplicación de QFlow puede ser capaz de identificar:

- BitTorrent
- Blubster
- CitrixICA
- Google Talk
- Gnucleuslan
- Gnutella
- GSS-SPNEGO
- NTLMMSSP
- OpenNap
- PeerEnabler
- Piolet
- UpdateDaemon
- VNC

Capítulo 4. Gestión de casos

Como administrador puede gestionar casos y colecciones mediante Gestión de casos. Puede crear casos para colecciones de documentos o archivos de captura de paquetes (pcap) y también puede importar archivos externos al sistema IBM Security QRadar Incident Forensics.

Ajuste de la gestión de casos

Para ayudarle a ajustar la gestión de casos, puede utilizar la opción **Vaciar**. Para un *flujo de datos pcap*, que es una serie de archivos pcap que están relacionados entre sí desde un punto de vista lógico y forman un solo archivo pcap grande, puede obligar a que los datos puestos en almacenamiento intermedio se escriban en disco. La opción **Vaciar** obliga a los hosts de QRadar Incident Forensics a grabar en el disco flujos indeterminados, lo que a su vez ayuda a realizar búsquedas en estos flujos en una fase anterior.

Gráficos de distribución

Si piensa suprimir un caso, puede utilizar gráficos para revisar rápidamente el contenido del caso. Puede revisar el tipo de archivos, los protocolos y los dominios que están en el caso.

Carga de archivos pcap en hosts gestionados

Puede cargar manualmente datos de pcap de orígenes externos. Puede especifica en qué host gestionado de QRadar Incident Forensics desea cargar los datos para procesar. Por ejemplo, si tiene tres hosts gestionados y tres archivos pcap, puede cargar cada uno en un host gestionado diferente. Para archivos pcap más grandes, utilice FTP.

Creación de casos

Los casos son contenedores lógicos para recopilar los documentos y archivos de pcap importados. Puede utilizar un caso individual para todos los archivos pcap o crear varios casos. Los casos puede estar restringidos a usuarios específicos.

Procedimiento

1. En la pestaña **Admin**, seleccione **Gestión de casos**.
2. Pulse **Añadir nuevo**.
3. En el campo **Nombre de caso**, escriba un nombre exclusivo.

   Restricción: Los nombres de caso no pueden contener espacios.
4. Pulse **Guardar**.

Resultados

Se creará un directorio nuevo que está basado en el nombre del caso: `/case_input/<nombre_caso>`. Este directorio se utiliza para importar los archivos pcap.

Cargar archivos en casos

Como administrador puede cargar archivos de captura de paquetes (pcap) y documentos externos, como por ejemplo hojas de cálculo, archivos de texto y archivos de imagen en la Gestión de casos de IBM Security QRadar Incident Forensics.

Se da soporte a los tipos de archivo siguientes:

- HyperText Markup Language
- XML y formatos derivados
- Formatos de documento de Microsoft Office
- Formato OpenDocument
- Portable Document Format
- Electronic Publication Format
- Rich Text Format
- Formatos de compresión y empaquetado
- Formatos de texto
- Formatos de audio
- Formatos de imagen
- Formatos de vídeo
- Archivos y archivos de archivado de clase Java
- El formato mbox

Gestión de casos limita tanto el número de archivos que puede añadir a un caso como el tamaño máximo de archivo.

Procedimiento

1. En la sección **Análisis forense** del panel **Admin**, pulse **Gestión de casos**.
2. Seleccione un caso.
   - Para añadir archivos externos a un caso existente, seleccione el caso en la lista **Casos**.
   - Para añadir archivos a un caso nuevo, pulse **Añadir nuevo**.

     Restricción: Los nombres de caso no pueden contener espacios.
3. En la lista **Cargar en host**, seleccione el host gestionado que desea que procese los archivos.
4. Para añadir archivos pcap y otros tipos de documento, elija uno de los métodos siguientes:
   - Pulse **Añadir pcaps**, seleccione los archivos y pulse **Iniciar carga**.
   - Arrastre los archivos al cuadro de carga.

   Una vez completada la carga, los archivos aparecerán listados en la lista **Colecciones**.

Capítulo 5. Asignar casos a usuarios

Como administrador puede otorgar acceso a datos forenses a los usuarios, asignar casos a los usuarios y definir permisos de usuario tales como el acceso FTP. Los usuarios no pueden ver datos hasta que se les asigna un caso y sólo pueden ver los datos de los casos a los que están asignados.

Tenga cuidado cuando asigne casos a usuarios no administrativos que tengan acceso restringido a las redes. Pueden ver documentos de direcciones IP a las que normalmente no tengan acceso. Por ejemplo, si asigna a un usuario no administrativo un caso que contiene información financiera o de recursos humanos, pueden ver los datos cuando investigan el caso.

Acerca de esta tarea

Los administradores pueden realizar las tareas siguientes:

- Asignar varios usuarios a un caso.
- Retirar un caso respecto de un usuario.
- Ver y acceder a todos los casos que están asignados a un usuario.

Los usuarios solamente pueden ver los casos que están asignados explícitamente a ellos.

Procedimiento

1. En el panel **Admin**, pulse **Permisos de usuario de análisis forense**.
2. En la lista **Usuarios**, seleccione un usuario.
3. En la lista de casos **Disponible**, seleccione uno o varios casos y pulse la flecha (>) para trasladar casos a la lista **Asignado**.

   Consejo: De forma predeterminada, un usuario con privilegios administrativos tiene asignados todos los casos. Las fechas a izquierda (<) y derecha (>) no se visualizan.

Importar manualmente archivos a un caso forense

A diferencia de la herramienta Gestión de casos, no existen restricciones respecto al tamaño o número de archivos cuando importa manualmente archivos. Puede crear manualmente un caso y copiar archivos en él o copiar manualmente archivos en un caso existente.

Por ejemplo, puede utilizar el mandato **scp** para copiar de forma segura archivos desde otro host al directorio `/opt/ibm/forensics/case_input/case_input/` del host de IBM Security QRadar Incident Forensics.

Antes de empezar

Haga una copia de seguridad de los archivos importados. Una vez que el archivo se ha importado y procesado, se suprime el archivo original.

Procedimiento

1. Utilice SSH para iniciar una sesión en QRadar Incident Forensics como usuario root.
2. Para crear un caso nuevo, acceda al directorio `/opt/ibm/forensics/case_input` y escriba el mandato siguiente:

   `mkdir /opt/ibm/forensics/case_input/<nombre_caso>`
3. Para copiar archivos en un caso, utilice el mandato **scp** u otro programa de transferencia de archivos para copiar los archivos en el directorio correspondiente al tipo de archivo.

   La tabla siguiente se indica la estructura de directorios para los archivos importados.

Tabla 1. Estructura de directorios para archivos de caso

Directorio	Descripción
`/opt/ibm/forensics/case_input/<nombre_caso>`	Directorio que se utiliza para importar un flujo de archivos pcap.
`/opt/ibm/forensics/case_input/<nombre_caso>/singles`	Directorio que se utiliza para importar archivos pcap individuales.
`/opt/ibm/forensics/case_input/case_input/<nombre_caso>/import`	Directorio que se utiliza para importar un archivo individual que no sea de tipo pcap, por ejemplo, documentos Microsoft Word, documentos PDF de Adobe Acrobat, archivos de texto e imágenes.

Importante: Si se utiliza un guión en un nombre de archivo, el guión se cambia por un carácter de subrayado cuando se importa el archivo.

Resultados

Una vez realizada satisfactoriamente la importación, el nombre del archivo aparece automáticamente en la ventana Colecciones del caso que ha creado.

Permitir que los usuarios transfieran mediante FTP archivos pcap y documentos desde sistemas externos a casos forenses

Para cargar datos externos para incluirlos en casos específicos, los administradores pueden otorgar permisos FTP seguros a los usuarios y gestionar el caso al que están asociados los datos. Los usuarios pueden elegir qué host de IBM Security QRadar Incident Forensics procesa la solicitud FTP.

Para cambiar una contraseña una vez habilitado el acceso de FTP, debe inhabilitar el acceso FTP y guardar el usuario y después volver a habilitar el acceso FTP y especificar la contraseña nueva.

Antes de empezar

Asegúrese de crear o asignar roles para investigadores forenses en la herramienta Roles de usuario de la pestaña **Admin**.

De forma predeterminada, el archivo `/etc/vsftpd/vsftpd.conf` está configurado de modo que hay cinco puertos abiertos: 55100-55104. Puede cambiar el rango de

puertos editando el archivo `/etc/vsftpd/vsftpd.conf` y cambiando los valores de `pasv_min_port` y `pasv_max_port` según el rano de puertos que desea. Debe desplegar los cambios de configuración pulsando **Desplegar cambios** en la pestaña **Admin**.

Acerca de esta tarea

IBM Security QRadar Incident Forensics puede importar datos de cualquier directorio accesible que esté situado en la red. Los datos pueden estar en varios formatos, tales como los siguientes:

- Archivos de formato PCAP estándar pertenecientes a orígenes externos
- Documentos tales como archivos de texto, hojas de cálculo y presentaciones
- Archivos de imagen
- Datos continuos de aplicaciones
- Datos continuos de orígenes CAP externos

Los usuarios pueden cargar varios archivos en un caso y un administrador puede otorgar acceso al caso a varios usuarios.

Restricción: El nombre del caso debe ser exclusivo. Un caso está asociado un solo usuario, por lo que dos usuarios no pueden crear un caso que tenga el mismo nombre.

Procedimiento

1. En el panel **Admin**, pulse **Permisos de usuario de análisis forense**.
2. En la lista **Usuarios**, seleccione un usuario.
3. En el panel **Editar usuario**, seleccione la casilla **Habilitar acceso FTP**.
4. Escriba y confirme la contraseña FTP del usuario.
5. Para guardar los cambios realizados en los permisos, pulse **Guardar usuario**.
6. En el cliente FTP, siga estos pasos:
   a. Asegúrese de que Transport Layer Security (TLS) esté seleccionado como protocolo.
   b. Añada la dirección IP del host de QRadar Incident Forensics.
   c. Cree un inicio de sesión que utilice el nombre de usuario y contraseña de QRadar Incident Forensics que se han creado.
7. Conecte con el servidor de QRadar Incident Forensics y cree un directorio nuevo.
8. Para enviar por FTP y almacenar archivos pcap, en el directorio que ha creado para el caso, cree un directorio denominado `singles` y arrastre los archivos pcap hasta ese directorio.
9. Para enviar por FTP y almacenar otros tipos de archivos que no sean archivos pcap, en el directorio que ha creado para el caso, cree un directorio denominado `import` y arrastre los archivos hasta ese directorio.
10. Para reiniciar el servidor FTP, escriba el mandato siguiente:
    ```
    etc/init.d/vsftpd restart
    ```
11. Para reiniciar el servidor que traslada los archivos desde el área de carga hasta el directorio de QRadar Incident Forensics, escriba el mandato siguiente:
    ```
    /etc/init.d/ftpmonitor restart
    ```

Resultados

En Gestión de casos, un administrador puede ver los datos que se cargan. Un usuario puede ver su caso en una de las herramientas del panel **Análisis forense**.

Descifrado de tráfico SSL y TLS en QRadar Incident Forensics

Para encontrar amenazad ocultas, IBM Security QRadar Incident Forensics puede descifrar tráfico SSL. Si proporciona la clave privada y dirección IP del servidor o una clave de sesión de navegador y alguna otra información de sesión, el inspector de protocolos puede descifrar tráfico SSL.

Si la clave de sesión se genera a partir de sitios web externos o mediante otro navegador, el inspector de protocolos no puede descifrar tráfico SSL de una sesión de navegador.

Restricción: El mecanismo de intercambio de claves `Diffie Hellman` no está soportado cuando el tráfico cifrado se descifra mediante una clave privada. Cuando utiliza una clave privada, se pueden utilizar otros métodos de intercambio de claves, tales como RSA.

La restricción referente a `Diffie Hellman` no es aplicable cuando el tráfico se descifra con información que reside en un registro de claves.

Acerca de esta tarea

El descifrado está soportado para los protocolos siguientes:

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

Los archivos de registro de claves son generados por los navegadores Chrome, Firefox y Opera mediante la variable de entorno SSLKEYLOGFILE. La clave de sesión SSLKEYLOGFILE es compatible con los formatos de clave siguientes:

- RSA
- DH

Procedimiento

1. Utilice SSH para iniciar una sesión en el host primario de QRadar Incident Forensics como usuario root.
2. Revise la ubicación de las claves en el archivo `/opt/qradar/forensics.conf`.

   ```
   <sslkeys
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

3. Copie las claves en el directorio que está especificado en el archivo `/opt/qradar/forensics.conf`.
   - Para las claves privadas, copie la clave en el directorio `/opt/ibm/forensics/decapper/keys`.

     Ejemplo:

     ```
     <keys>
     ```

```
 <key file="
/opt/ibm/forensics/decapper/keys/nombre_clave">
    <address> 1.2.3.4</address>
    <range> 1.2.3.0-1.2.3.255</range>
  </key></keys>
```

- Para los archivos de registro de claves que son generados por el navegador, copie esos archivos en el directorio `/opt/ibm/forensics/decapper/keylogs/default`.

Si cambia los subdirectorios contenidos en los directorios `/opt/ibm/forensics/decapper/keys` o `/opt/ibm/forensics/decapper/keylogs`, debe reiniciar el servicio decapper.

Para reiniciar el servicio decapper, escriba el mandato siguiente: `service decapper restart`

Capítulo 6. Acciones planificadas en QRadar Incident Forensics

Puede planificar tareas de mantenimiento, tales como suprimir documentos antiguos, ajustar la base de datos y restablecer el servidor de IBM Security QRadar Incident Forensics.

Si existen muchos documentos, las acciones planificadas, tales como suprimir documentos antiguos, pueden tardar mucho tiempo en realizarse. Si desea suprimir un caso completo, utilice la herramienta Gestión de casos.

Suprimir documentos

Los administradores pueden suprimir los documentos obsoletos que están basados en las indicaciones de fecha y hora de la red de documentos.

Puede suprimir documentos, tales como archivos pcap y otros tipos de archivos, de un caso o del servidor. La supresión de documentos obsoletos ayuda a mantener la velocidad cuando busca documentos.

Vaciar caso

Para ayudarle a ajustar la gestión de casos, puede utilizar la opción **Vaciar caso**. Para un *flujo de datos pcap*, que es una serie de archivos pcap que están relacionados entre sí desde un punto de vista lógico y forman un solo archivo pcap grande, puede obligar a que los datos puestos en almacenamiento intermedio se escriban en disco. La opción **Vaciar caso** obliga a los hosts de QRadar Incident Forensics a grabar en el disco flujos indeterminados, lo que a su vez ayuda a realizar búsquedas en estos flujos en una fase anterior.

Optimizar la base de datos

Los administradores pueden optimizar la base de datos para reorganizar el índice del motor de búsqueda en segmentos y eliminar los documentos suprimidos.

La acción planificada **Optimizar base de datos** es similar a un mandato **`defrag`**.

Cuando optimiza la base de datos, se crea un índice nuevo, el cual sustituye al antiguo. Debido a que existen dos índices hasta que se sustituye el índice antiguo, el mandato para automatizar el índice necesita el doble de espacio de disco duro.

Antes de optimizar la base de datos, asegúrese de que el tamaño del índice no sea mayor que el 50 por ciento del espacio disponible en el disco duro.

Planificación de acciones para hosts de QRadar Incident Forensics

Puede planificar tareas de mantenimiento en los hosts de IBM Security QRadar Incident Forensics.

Puede planificar estas tareas:

- Construir un índice nuevo para los casos disponibles actualmente.

- Eliminar (*caducar*) documentos que no desea retener después de un periodo de tiempo especificado.
- Forzar la grabación de datos en disco.

Procedimiento

1. En la pestaña **Admin**, en la sección **Análisis forense**, pulse **Planificar acciones**.
2. Pulse **Añadir nueva acción**.
3. En la lista **Seleccionar acción**, seleccione una acción y especifique los valores.
   - Para construir un índice nuevo para los casos actuales, seleccione **Optimizar índice**.

     El índice nuevo necesita dos veces más espacio que el índice existente. Asegúrese de tener el espacio adecuado.
   - Para suprimir documentos cuya indicación de la hora de red es mayor que una edad especificada, seleccione **Caducar documentos**.

     Los índices también se eliminan cuando suprime los documentos.
   - Para grabar flujos indeterminados en disco, seleccione **Variar caso**.
4. Pulse **Guardar**.
5. Para ejecutar, editar o suprimir la acción, seleccione la acción de la lista **Acciones** y pulse **ejecutar**, **editar** o **suprimir**.

Capítulo 7. Auditoría del uso del sistema y de usuario en QRadar Incident Forensics

Los registros de auditoría son registros cronológicos que identifican cuentas de usuario asociadas con el acceso a datos. Estos registros pueden detectar un acceso inusual o no autorizado y pueden identificar problemas como por ejemplo trabajos que han fallado.

Las actividades siguientes generan sucesos de registro de auditoría:

- Crear caso
- Suprimir caso
- Suprimir colección
- Todas las consultas de usuario
- Vista de documento
- Exportar documento

Restricción: El registro de sucesos de creación de recopilación no está soportado.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar Console o QRadar Incident Forensics Standalone como administrador.
2. Vaya al directorio `/var/log/audit`.
3. Abra el archivo `audit.log` en un editor, como por ejemplo vi, para revisar el contenido o utilice el mandato **`grep`** para buscar una entrada específica.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que solo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785, EE. UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japón

El párrafo siguiente no es aplicable en el Reino Unido ni en ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de estos sitios web. El contenido de esos sitios web no forma parte del contenido de este producto de IBM, por lo que la utilización de dichos sitios es responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir:(i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se haya intercambiado, deberán ponerse en contacto con:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, EE. UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluyendo, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del contrato de cliente IBM, el contrato internacional de licencia de programa de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas en nivel de desarrollo y no existe garantía alguna de que estas mediciones sean iguales en los sistemas de disponibilidad general. Además, es posible que algunas mediciones se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, compatibilidad o cualquier otra declaración relacionada con los productos que no son de IBM. Las preguntas relativas a las prestaciones de los productos que no son de IBM deberán dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la orientación o intención futura de IBM están sujetas a cambio o anulación sin previo aviso y representan solamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales cotidianas. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos

esos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por empresas reales es mera coincidencia.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de servicios y productos pueden ser marcas registradas de IBM o de otras empresas. Encontrará una lista actualizada de marcas registradas de IBM en la sección "Copyright and trademark information" del sitio web www.ibm.com/legal/copytrade.shtml.

Los términos siguientes son marcas registradas de otras empresas:

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Java y todas las marcas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o de sus filiales.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio (Ofertas de software), pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia del usuario final, ajustar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se define información sobre el uso de cookies de esta oferta.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilan el ID de sesión de cada usuario para la gestión y autenticación de sesiones. Estas cookies se pueden inhabilitar, pero si se inhabilitan también se elimina la función que estas cookies habilitan.

Si las configuraciones desplegadas para esta oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, que incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de diversas tecnologías, incluidos los cookies, para estos fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, la sección titulada “Cookies, Web Beacons and Other Technologies” y la declaración “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.