IBM Security QRadar Incident Forensics
Versión 7.2.6

Guía del usuario

Nota

Antes de utilizar esta información y el producto al que sirve de complemento, lea la información contenida en la sección "Avisos" en la página 39.

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 al uso de IBM Security QRadar Incident Forensics

Esta guía contiene información sobre cómo investigar incidentes de seguridad mediante IBM® Security QRadar Incident Forensics.

Público al que va dirigida esta guía

Los investigadores extraen información del tráfico de red y de los documentos del repositorio de análisis forense. Esta información se utiliza en la investigación de incidentes de seguridad.

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 implicar varias leyes o regulaciones, incluyendo aquellas 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 conformidad con las leyes, disposiciones y políticas aplicables, y asume la responsabilidad de su cumplimiento. 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 las leyes, disposiciones y políticas aplicables, y asume la responsabilidad de su cumplimiento. 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 los usuarios de QRadar Incident Forensics V7.2.6

IBM Security QRadar Incident Forensics V7.2.6 introduce nuevas herramientas de investigación que facilitan el análisis de archivos e imágenes con respecto a contenido o comportamiento sospechoso. También puede analizar enlaces que muestran las relaciones o conexiones entre páginas web y colaboradores.

Análisis de artefactos con respecto a contenido sospechoso o malicioso

Puede utilizar el análisis de artefactos para investigar incidentes tales como el modo en que se han infectado los sistemas y si hay otros activos comprometidos de forma similar.

Por ejemplo, puede utilizar las prestaciones de análisis de archivos en datos de paquete recuperados para ver una lista de todos los archivos y si contienen archivos o scripts incluidos.

Puede observar archivos de imagen que están marcados como contenedores de contenido sospechoso y scripts incluidos.

La distribución y puntuación de entropía de archivo puede ayudar a distinguir anomalías de archivo y suministrar pruebas de que este archivo contiene un programa malicioso que ha burlado la detección y es responsable de infectar sistemas.

Para determinar qué otros sistemas pueden estar afectados, puede utilizar el análisis de enlaces para visualizar rápidamente todos los sitios web que se han visitado y el subconjunto de accesos al host web infectado.

 Más información...

Capítulo 2. Investigaciones de seguridad

Mediante IBM Security QRadar Incident Forensics, puede detectar amenazas emergentes, determinar la causa raíz e impedir recurrencias. Mediante herramientas de análisis forense, puede rápidamente centrar su análisis en quién inició la amenaza, cómo se llevó a cabo y qué se ha puesto en peligro.

Como investigador de análisis forense, puede hacer un seguimiento paso a paso de las acciones de los delincuentes cibernéticos y reconstruir los datos de red en bruto que están relacionados con un incidente de seguridad.

Una vez que la empresa conoce la existencia de una amenaza, un riesgo de seguridad potencial o una vulneración de normas, define objetivos para determinar el alcance del ataque, identificar las entidades involucradas y conocer las motivaciones.

Puede utilizar las herramientas incluidas en IBM Security QRadar Incident Forensics para casos determinados en los diferentes tipos de investigaciones, tales como seguridad de red, análisis de personas con información privilegiada, fraude y abuso, y recogida de pruebas.

1. Recuperar y reconstruir sesiones de red hacia y desde una dirección IP.
2. A partir de los incidentes creados, puede consultar categorías de atributos para recoger pruebas.

   Cuando se crea una recuperación, se crea un incidente.
3. Utilizar filtros de búsqueda para recuperar sólo la información en la que se está interesado.
4. Dependiendo del tipo de investigación, elegir la herramienta forense que suministre las pruebas necesarias.

Contenido sospechoso

Puede buscar cualquier elemento contextual o identificador que conozca sobre el atacante o incidente. Si utiliza la palabra clave en la búsqueda, obtendrá resultados sospechosos. Parte del contenido sospechoso puede ser significativo para la investigación.

Encadenamiento de datos

El encadenamiento de datos se consigue haciendo que el contenido devuelto por el resultado de una búsqueda adopte la forma de enlace activo. Por ejemplo, si busca `"Tom"`, los resultados pueden incluir correos electrónicos que Tom escribió, conversaciones de Tom en redes sociales, y más información contextual. Cuando pulsa en un correo electrónico para visualizarlo, cada activo o entidad, tales como archivos adjuntos o identificadores del sistema que Tom utilizó, aparecen en forma de enlaces. Un investigador puede utilizar estos enlaces para investigar rápidamente.

Impresión digital

Utilice la impresión digital para buscar en los datos y correlacionar la relación entre entidades, tales como direcciones IP, nombre y direcciones MAC, de acuerdo

con la frecuencia. Puede seleccionar uno o varios resultados para ver la frecuencia y dirección de la relación.

Herramienta de supervisión

Utilice la herramienta de supervisión para ver un calendario de actividades que le permita hacer un seguimiento de un ataque. La herramienta de supervisión reconstruye la sesión y ordena los documentos por orden de hora.

Filtrado de contenido

Utilice el filtrado de contenido para examinar un subconjunto de categorías de contenido, tales como WebMail, y eliminar la información irrelevante cuando realiza una búsqueda.

Investigaciones de la seguridad de red

Puede utilizar QRadar Incident Forensics para detectar e investigar actividades maliciosas que están dirigidas a activos críticos. Puede utilizar las herramientas incorporadas de análisis forense para ayudar a corregir un error de seguridad de red e impedir que ocurra de nuevo.

Utilice las herramientas de investigación de QRadar Incident Forensics como ayuda para determinar cómo se produjo el suceso, minimizar su efecto y hacer todo lo posible para impedir otro error de seguridad.

Sistema inicial infectado: identificar el origen de un ataque

En este caso de ejemplo, una empresa recibe aviso sobre un posible error de seguridad. La empresa desea encontrar el punto inicial de un ataque para determinar el origen. La empresa debe poner en cuarentena las entidades en peligro para impedir la difusión del ataque a otras partes de la empresa.

Objetivos

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar el tipo de ataque.
- Identificar el punto de entrada inicial de la amenaza.
- Obtener detalles sobre los datos maliciosos.
- Conocer cómo los datos maliciosos se difundieron desde el punto de entrada.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para encontrar atributos sintomáticos que están asociados a datos maliciosos.
2. Utilice categorías de contenido para descartar por filtración contenido que no es significativo para la investigación.
3. Examine el contenido sospechoso que está señalizado por el producto.
4. Utilice las impresiones digitales y visualizaciones para explorar las relaciones ampliadas de los datos maliciosos, el delincuente o sistema atacado.
5. Utilice el encadenamiento de datos y siga enlaces de datos para identificar el sistema inicial infectado.

6. Utilice la herramienta de supervisión para ver un calendario de actividades que le permita hacer un seguimiento de un ataque.

Sistemas en peligro

En este caso de ejemplo, una empresa recibe aviso de que un ataque cibernético, tal como espionaje de empresas, suplantación de identidad, fuerza bruta o inyección SQL, ha puesto en peligro uno o varios sistemas de la empresa.

Objetivos

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar el alcance del riesgo dentro de la empresa.
- Conocer el tipo de riesgo operativo existente en cada sistema.
- Descubrir las acciones periféricas que el ataque inicial realizó para eludir las actividades de limpieza y detección.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar datos maliciosos o activos en riesgo.
2. Examine el contenido sospechoso que está señalizado por el producto.
3. Utilice las impresiones digitales y visualizaciones para explorar las relaciones de entidad que resultan de los sistemas en peligro.
4. Utilice la herramienta de supervisión para ver un calendario de actividades que le permita hacer un seguimiento de un ataque.
5. Descubra incoherencias o interacciones sospechosas entre las categorías de datos mediante la búsqueda de formato libre, el encadenamiento de datos y el examen de contenido sospechoso.

Datos filtrados a entidades no autorizadas

En este caso de ejemplo, una empresa recibe aviso de que se han filtrado datos confidenciales a entidades no autorizadas dentro de la empresa o a entidades externas.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar la naturaleza y el volumen de datos filtrados.
- Conocer las técnicas que se han empleado.
- Descubrir a los autores.
- Identificar el origen de la filtración de datos.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar identificadores de los que se han filtrado.
2. Examine el contenido sospechoso que está señalizado por el producto.

3. Revise la reconstrucción de datos para ver el alcance total de los datos filtrados.
4. Utilice la impresión digital y visualizaciones para explorar todas las relaciones de entidades que intervienen.
5. Utilice la herramienta de supervisión para ver un calendario de actividades que le permita hacer un seguimiento de un ataque.
6. Utilice la búsqueda de formato libre para descubrir las motivaciones de la filtración de datos.
7. Utilice el encadenamiento de datos para encontrar enlaces a otros datos que posiblemente se filtraron.

Investigaciones de análisis de personas con información privilegiada

Utilice QRadar Incident Forensics para detectar confabulaciones, sabotajes y el uso indebido del acceso. Identifique el delincuente, los colaboradores y los sistemas en peligro, y documente las pérdidas de datos.

Uso indebido del acceso

En este caso de ejemplo, una empresa recibe aviso de que uno o varios de sus empleados utilizan credenciales de forma indebida o se utilizan como sustituto para acceder a sistemas y datos confidenciales a fin de realizar actividades no autorizadas.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar la identidad del usuario.
- Determinar quién o qué está utilizando la identidad para realizar actividades no autorizadas.
- Conocer el objetivo del uso indebido del acceso.
- Evaluar si la entidad tiene más identidades que también podrían ser objeto de uso indebido.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar identidades que están accediendo a sistemas o datos confidenciales.
2. Mediante el examen de contenido sospechoso, búsquedas de formato libre, encadenamiento de datos y filtrado de contenido determine cuáles de esos intentos de acceso son sospechosos.
3. Examine la reconstrucción de datos para el contenido que es objeto de acceso.
4. Haga un seguimiento de los patrones de acceso y determine la frecuencia en la herramienta de supervisión.
5. Utilice la impresión digital para descubrir los alias utilizados por una misma entidad.

Confabulación

En este caso de ejemplo, una empresa recibe aviso de que una o más partes interesadas están confabulando entre ellos o con terceros para realizar actividades en perjuicio de la empresa.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar las entidades que están en confabulación.
- Conocer la naturaleza y los patrones de las interacciones entre los colaboradores.
- Descubrir el contenido que subyace en la confabulación.
- Determinar la duración de la confabulación para conocer el alcance del riesgo.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar identificadores de entidades que están implicadas.
2. Examine el contenido sospechoso que está señalizado por el producto.
3. Utilice la impresión digital, visualizaciones y el filtrado de contenido para identificar relaciones que podrían ser sospechosas.
4. Utilice la herramienta de supervisión para rastrear las actividades de las entidades implicadas para obtener el contenido de las interacciones.
5. Descubra las motivaciones de la confabulación mediante la revisión de documentos reconstruidos.
6. Utilice la búsqueda de formato libre y el encadenamiento de datos para encontrar el inicio de las actividades de confabulación.

Sabotaje

En este caso de ejemplo, una empresa recibe aviso de que una o más partes implicadas están intentando perturbar operaciones. La parte interesada se podría estar utilizando como agente.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Identificar el saboteador.
- Conocer las técnicas que el saboteador ha empleado.
- Evaluar el efecto y ámbito de la perturbación.
- Identificar las vulnerabilidades que han sido explotadas por el saboteador.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar síntomas del sabotaje.
2. Examine el contenido sospechoso que está señalizado por el producto.
3. Utilice la navegación visual, la impresión digital y el filtrado de contenido para explorar los síntomas y detectar identificadores del saboteador.
4. Utilice la herramienta de supervisión para hacer un seguimiento de las actividades del saboteador.
5. Utilice la reconstrucción de datos para descubrir los roles y las motivaciones del saboteador.

6. Utilice la reconstrucción de datos para revisar el contenido que el saboteador ha utilizado.
7. Utilice la búsqueda de formato libre, la herramienta de supervisión y el contenido sospechoso para descubrir los sistemas en peligro y los procedimientos que permitieron el sabotaje.

Investigaciones de fraudes y abusos

Utilice QRadar Incident Forensics para localizar transacciones no autorizadas, asignaciones indebidas de recursos, desviaciones de protocolo y la evasión de controles legales.

Transacciones no autorizadas

En este caso de ejemplo, una empresa recibe aviso de que transacciones no autorizadas están produciendo un efecto financiero negativo en las operaciones de negocio.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Localizar las transacciones no autorizadas.
- Identificar las entidades que están implicadas y son responsables de las transacciones no autorizadas.
- Conocer la frecuencia y las tendencias de las transacciones no autorizadas.
- Evaluar el ámbito de riesgo de las transacciones no autorizadas.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar transacciones incoherentes o sospechosas.
2. Utilice la búsqueda de formato libre y el encadenamiento de datos para buscar repeticiones de esas transacciones.
3. Utilice el encadenamiento de datos y la impresión digital para descubrir las entidades que están asociadas con las transacciones sospechosas.
4. Descubra el contenido de las transacciones para revelar el valor cuantitativo mediante la revisión de documentos reconstruidos.

Asignación no autorizada de recursos

En este caso de ejemplo, una empresa sospecha de que existe una asignación no autorizada de recursos, lo cual produce un efecto financiero negativo en las operaciones comerciales.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Localizar la asignación indebida de recursos.
- Identificar las entidades que están implicadas y son responsables de la asignación indebida de recursos.
- Conocer las motivaciones de la asignación no autorizada de recursos.
- Evaluar el tamaño y la magnitud de los recursos asignados indebidamente.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para las comunicaciones que están asociadas con recursos asignados.
2. Utilice la búsqueda de formato libre, el encadenamiento de datos y la impresión digital para encontrar identificadores de entidades que están realizando una asignación no autorizada de recursos.
3. Procese el contenido de las interacciones implicadas para evaluar los motivos de la asignación no autorizada. Para ello revise documentos reconstruidos y utilice visualizaciones.
4. Utilice la herramienta de supervisión para hacer un seguimiento de las actividades de asignación y conocer la cantidad de recursos asignados indebidamente.

Desviaciones de protocolo y evasión de controles legales

En este caso de ejemplo, una empresa recibe aviso sobre una evasión de controles legales y protocolos que puede tener un efecto financiero negativo.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar qué protocolos o controles legales se han evadido.
- Identificar las entidades que han participado en este comportamiento.
- Conocer las motivaciones de estas entidades.
- Determinar el grado de difusión de este comportamiento indebido.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar procesos de la empresa que están gobernados por protocolos o controles.
2. Utilice la búsqueda de formato libre, el encadenamiento de datos y la reconstrucción de datos para establecer correspondencias con documentación que describe los protocolos y controles legales.
3. Utilice el filtrado de contenido y la búsqueda de formato libre para descubrir casos específicos en donde se han evadido controles o protocolos.
4. Utilice la impresión digital, las visualizaciones, el encadenamiento de datos y el filtrado de contenido para encontrar los identificadores de entidades asociados.
5. Utilice la herramienta de supervisión para hacer un seguimiento de las actividades de entidades a fin de explorar las posibles motivaciones.

Investigaciones para la recogida de indicios

Utilice QRadar Incident Forensics para evaluar el riesgo de vulnerabilidades en la empresa, medir el nivel de confianza en la identificación de amenazas o delincuentes, y refinar las prácticas de seguridad.

Nivel de confianza en la identificación de amenazas

En este caso de ejemplo, una empresa recibe aviso sobre una determinada amenaza, software malicioso o vulnerabilidad. Para justificar las acciones correctivas que de otro modo podrían interrumpir las operaciones comerciales normales, la empresa desea medir el intervalo de confianza de los riesgos.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Validar la susceptibilidad al riesgo de seguridad.
- Determinar si existen indicios del riesgo de seguridad.
- Evaluar la amplitud y el efecto monetario del riesgo de seguridad.
- Conocer la naturaleza del riesgo de seguridad

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre, el contenido sospechoso y el encadenamiento de datos para buscar la amenaza, software malicioso o vulnerabilidad utilizando como punto de partida posibles entidades susceptibles de ataque.
2. Utilice la búsqueda de formato libre y el encadenamiento de datos para recopilar apariciones del ataque.
3. Utilice la búsqueda de formato libre para establecer correspondencias con documentos que pueden proporcionar referencias al impacto.
4. Utilice la impresión digital y visualizaciones para identificar las entidades afectadas.
5. Utilice la herramienta de supervisión para analizar las actividades que están asociadas con la amenaza o el delincuente.

Refinar las prácticas de seguridad

La detección de comportamientos nuevos y peligrosos hace que una empresa evalúe si las prácticas de seguridad existentes son suficientes. En este caso de ejemplo, una empresa desea evaluar la efectividad de sus reglas de seguridad para los riesgos a los que tiene hacer frente.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Reconocer comportamientos nuevos o peligrosos.
- Evaluar la eficacia de las reglas de seguridad existentes.
- Conocer los déficits de seguridad que surgen debido a operaciones dinámicas.
- Evaluar la efectividad de prácticas de seguridad propuestas.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar comportamientos nuevos o peligrosos, tales como los asociados a usuarios de dispositivos móviles y servicios en la nube, utilizando conocimiento de dominio y de la organización.
2. Examine contenido sospechoso y utilice la herramienta de supervisión para establecer correspondencias entre estos comportamientos y reglas o prácticas de seguridad existentes.
3. Utilice la búsqueda de formato libre, la herramienta de supervisión, la reconstrucción de contenido y la visualización para analizar las alertas resultantes de reglas de seguridad para determinar la frecuencia de falsos positivos.
4. Utilice la búsqueda de formato libre, la herramienta de supervisión, la reconstrucción de contenido, el encadenamiento de datos y la visualización para descubrir falsos negativos que no son detectados por las reglas o prácticas de seguridad existentes.

Evaluaciones de riesgos

En este caso de ejemplo, una empresa realiza una evaluación de riesgos como consecuencia de un boletín de seguridad que describe determinadas vulnerabilidades, software malicioso o comportamiento malicioso. La evaluación de riesgos determina si la empresa es susceptible al ataque o ya está en peligro.

Objetivo

Para resolver el problema en estas investigaciones, la empresa tiene estos objetivos:

- Determinar la presencia de vulnerabilidades identificadas en la empresa.
- Detectar la presencia maliciosa de terceros.
- Descubrir indicios de cualquier riesgo.
- Determinar si la empresa es una víctima de software malicioso.
- Determinar la identidad del usuario.

Investigación

Utilice las herramientas del panel **Análisis forense** como ayuda para la investigación.

1. Utilice la búsqueda de formato libre para buscar rasgos de vulnerabilidades, software malicioso o comportamiento malicioso que están descritos en el boletín de seguridad.
2. Utilice la búsqueda de formato libre para establecer correspondencias con otros datos o investigaciones a fin de obtener indicadores.
3. Utilice la herramienta de supervisión para investigar interacciones que posiblemente han explotado vulnerabilidades identificadas.
4. Examine el contenido sospechoso que está señalizado por el producto.
5. Revise el contenido que subyace en las interacciones potencialmente peligrosas mediante la reconstrucción de datos.
6. Utilice la herramienta de supervisión para hacer un seguimiento de las actividades de entidades potencialmente peligrosas.

Capítulo 3. Cómo empezar con las investigaciones de análisis forense

Para iniciar las investigaciones de análisis forense en IBM Security QRadar Incident Forensics, utilice el menú **Inicio rápido** para navegar y filtrar datos que están en el repositorio de análisis forense. Este launchpad contiene consultas de resumen predefinidas que puede utilizar para iniciar una búsqueda u obtener relaciones para una entidad.

Para empezar, siga estas directrices:

1. Inicie una recuperación o una búsqueda forense desde un delito en la pestaña **Delitos**.
   - Si pulsa con el botón derecho sobre un delito o cualquier dirección IP y ejecuta una recuperación forense, el análisis forense recupera los datos de captura en bruto para los intervalos de tiempo especificados del dispositivo de captura, extrae y reconstruye los documentos y a continuación añade los resultados al repositorio de análisis forense.
   - Si pulsa con el botón derecho sobre una ofensa o cualquier dirección IP y ejecuta una búsqueda forense, el repositorio de análisis forense se aplica un filtro y realiza una búsqueda en el repositorio de análisis forense para esa dirección IP. Los resultados se muestran en la cuadrícula principal de la pestaña **Análisis forense**. Puede refinar la búsqueda construyendo consultas.

   Cuando QRadar Incident Forensics recibe una solicitud de búsqueda, procesa los datos de captura de paquetes y los vuelve a poner en el formato enviado al destinatario deseado. Los documentos de Microsoft Word, por ejemplo, se recuperan como archivos Word. Las llamadas de teléfono de voz a través de IP se recuperan como archivos de audio. Los archivos recuperados se indexan mediante contenido de archivo y metadatos para que sea posible realizar búsquedas dentro de ellos.
2. En la pestaña **Análisis forense**, pulse **Inicio rápido**.

   Después de ejecutar una recuperación o una búsqueda, en lugar de realizar búsquedas de formato libre y construir sus propias consultas, puede iniciar rápidamente la investigación mediante las consultas predefinidas del menú **Inicio rápido** en la pestaña **Análisis forense**. Por ejemplo, puede mirar en la categoría **Contenido sospechoso** y ejecutar una de las consultas como por ejemplo **alerta de entidad**. *Contenido sospechoso* está basada en un conjunto de reglas definido sobre el contenido que significa una actividad sospechosa. Una *alerta de entidad* marca una posible entidad maliciosa implicada en la infracción de una política de seguridad.

   Las prestaciones de filtrado y categorización de contenido ayudan a reducir el volumen de datos devuelto
3. En la **Cuadrícula**, seleccione los documentos a buscar.

   QRadar Incident Forensics devuelve resultados de la búsqueda priorizados. Al igual que la optimización del motor de búsqueda prioriza los sitios en una búsqueda en Internet, las apariciones más frecuentes se sitúan en la parte superior de la lista.

   Puede empezar a encadenar los datos pulsando enlaces y buscando los metadatos asociados al documento. Las prestaciones de encadenamiento de datos proporcionan varias vistas de búsqueda resúmenes de datos.

4. Para investigar las relaciones entre todas las acciones y el incidente de seguridad, en la vista de documento, seleccione un enlace y pulse con el botón derecho **Obtener relaciones para**.

   Después de investigar atributos, filtre la información que recopile conectando entidades.

5. Pulse **Impresiones digitales** para seguir la pista de identidad y obtener un conjunto de asociaciones compilado.

   Una impresión digital es un índice de metadatos que puede ayudar a identificar atacantes sospechosos o personas con información privilegiada malintencionadas haciendo un seguimiento de pistas de usuarios maliciosos. Al construir estas relaciones, QRadar Incident Forensics utiliza datos de orígenes de red como por ejemplo direcciones IP, direcciones MAC y puertos y protocolos TCP. Puede buscar información como por ejemplo IDs de chat y puede leer información como por ejemplo la identificación del autor de aplicaciones de proceso de textos u hoja de cálculo. Una impresión digital puede ayudar a descubrir asociaciones enlazando la identidad de la entidad para identificar información para otros usos o entidades.

Búsquedas y marcadores de QRadar Incident Forensics

Los investigadores utilizan IBM Security QRadar Incident Forensics para extraer datos significativos del tráfico de red y de documentos.

Búsqueda y marcaje de registros

Para permitir una actividad de análisis forense intuitiva, QRadar Incident Forensics recupera datos de paquetes y absorbe otro contenido. Esta tecnología proporciona exploración de datos basada en búsquedas, reconstrucción de sesiones e inteligencia de análisis forense para ayudar en las investigaciones de incidentes de seguridad.

Los investigadores centran inicialmente su investigación en acciones generales y después refinan los hallazgos para obtener un conjunto de resultados final significativo. Un método simple general consiste es buscar y marcar muchos registros inicialmente. A continuación, se centra el interés en los registros marcados para identificar un conjunto final de registros. Determine qué información es significativa y modifique las consultas para incluir o excluir determinados elementos. Utilice esta información para probar una hipótesis.

A medida que desarrolla nuevas pistas, puede hacer un seguimiento de ellas utilizando otros métodos. Puede utilizar herramientas de visualización y análisis para evaluar manual y automáticamente el grado de pertinencia de los resultados. También puede utilizar consultas variadas para obtener un aspecto diferente del mismo problema.

Proceso de resultados marcados

Cuando encuentra resultados que son significativos para la investigación, puede marcar los resultados para realizar un examen más profundo y llegar a una determinación final. Marque más información que la que cree que necesita. En caso de duda, marque la información. El objetivo es eliminar la información irrelevante y centrarse en lo que cree que es significativo.

Después de marcar un conjunto de resultados que piensa que son significativos, puede afinar el examen.

1. Examine cada documento marcado utilizando las herramientas de visualización y análisis.
2. Adjunte notas de caso a los documentos y tome una decisión final sobre la importancia de cada documento para el caso.
3. Si un registro no es importante, elimine la marca.

   En el proceso de investigación, ha identificado la información importante del repositorio y ahora tiene un conjunto de registros marcados significativos.
4. Imprima, exporte o procese los registros significativos.

Búsqueda de documentos e investigación

Los investigadores buscan documentos que sean relevantes para una línea de investigación o una hipótesis sobre cómo se produjo un incidente de seguridad.

Búsquedas

En lugar de bucear en cantidades ingentes de documentos, la mayoría de los cuales no están relacionados con el caso, los investigadores utilizan el repositorio de análisis forense para extraer los documentos que cumplen ciertas características de interés. Por ejemplo, un documento que ha aparecido dentro de un periodo de tiempo determinado, que se refiere a un tema que interesa o que ha sido enviado o recibido por un presunto atacante.

Las búsquedas pueden ser específicas. Por ejemplo, "encontrar la serie de caracteres “Mission Alpha”" es específico. Las búsquedas también pueden ser generales. Por ejemplo, "encontrar todos los números de la seguridad social que existen en el repositorio" es más general.

Las búsquedas pueden ser simples y estar basadas en un solo criterio. Los resultados de las búsquedas complejas deben satisfacer varias condiciones. Un ejemplo de búsqueda compleja sería encontrar todo el correo electrónico intercambiado entre dos atacantes sospechosos acerca de un tema y excluir los correos electrónicos que contienen archivos adjuntos. La finalidad de una búsqueda es reducir de forma rápida y precisa los registros a un conjunto de trabajo manejable. Cuando el investigador tiene un conjunto de documentos menor para examinar, es más probable que los documentos sean significativos para el caso.

Ejecución de una recuperación en una dirección IP o un puerto

Puede ejecutar una recuperación en una o varias direcciones IP o puertos. Si no especifica una dirección IP o puerto, se recupera todo el tráfico TCP y UDP. Si especifica varias direcciones IP o puertos, debe utilizar una coma para separarlos.

Restricción: Como regla, puede especificar alrededor de 7 direcciones IPv4 y 7 puertos o 255 caracteres como máximo a la vez. Los campos **Dirección IP** y **Puerto** se combinan con otras frases para crear una serie de filtro. La serie de filtro no puede tener más de 255 caracteres

Casos de análisis forense

Los casos son contenedores lógicos para la recopilación de archivos de captura de paquetes y documentos importados.

Los casos los crean los administradores o los investigadores que disponen de privilegios para crear casos. Los administradores crean y asignan casos a los

investigadores. Los investigadores pueden crear un nuevo caso cuando recuperan datos de captura de paquetes de una dirección IP en IBM Security QRadar.

Tareas relacionadas:

"Cargar archivos y documentos pcap desde sistemas externos a casos de análisis forense"
Puede cargar datos externos en casos específicos.

Recopilaciones

Utilice las recopilaciones para agrupar datos relacionados de un origen específico, como, por ejemplo, un archivo de datos de captura de paquetes (pcap), PDF o la corriente de red.

Las recopilaciones se utilizan para identificar y gestionar grupos de datos relacionados. Puede suprimir rápidamente los datos de grupo en la recopilación cuando la investigación finalice.

Las recopilaciones las crean los administradores o los investigadores. Los administradores crean recopilaciones para cargar datos manualmente en IBM Security QRadar Incident Forensics. Los administradores también añaden recopilaciones a los casos. Los investigadores pueden crear una nueva recopilación cuando inicien la recuperación de datos de captura de paquetes desde una dirección IP en IBM Security QRadar.

Tenga en cuenta las reglas siguientes para las recopilaciones y los nombres de las recopilaciones:

- Los nombres de las recopilaciones deben ser exclusivos.
- Los casos incluyen una o varias recopilaciones.
- Se pueden añadir recopilaciones a varios casos.
- Los resultados de búsqueda devuelven datos duplicados si un investigador tiene dos casos con la misma recopilación.
- Si un nombre de recopilación no es exclusivo cuando se carga un nuevo pcap, la recopilación original se suprime antes de cargar el pcap nuevo.

Cargar archivos y documentos pcap desde sistemas externos a casos de análisis forense

Puede cargar datos externos en casos específicos.

Antes de empezar

Un administrador debe habilitar permisos de FTP seguro para el usuario que desee cargar archivos externos.

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

Puede cargar varios archivos en un caso.

Restricción: El nombre del caso debe ser exclusivo. No puede crear un caso que tenga el mismo nombre que un caso existente.

Procedimiento

1. 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.
2. Conecte con el servidor de QRadar Incident Forensics y cree un directorio nuevo.
3. 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.
4. 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.
5. Para reiniciar el servidor FTP, escriba el mandato siguiente:

   ```
   etc/init.d/vsftpd restart
   ```
6. Para reiniciar el servidor que traslada los archivos desde el área de carga hasta el directorio de QRadar Incident Forensics, escriba el mandato siguiente:

Resultados

El caso aparecerá en una de las herramientas del panel **Análisis forense**.

Consultas al repositorio de análisis forense

Los investigadores especifican las características de los documentos que les interesa recuperar de la base de datos de análisis forense. Se utilizan varias consultas para encontrar un conjunto de documentos para una investigación.

La realización de varias consultas y una inspección manual de un pequeño conjunto de documentos es mejor que estudiar todo el repositorio. A menudo, las ideas para consultas posteriores y consultas afinadas aparecen durante la inspección de un documento que no es relevante.

Una mayor cantidad de términos de consulta más específicos se traduce en conjuntos de resultados de mayor relevancia. Su objetivo es definir todo lo que se sabe acerca de los resultados que desea y ser muy específico siempre que sea posible. En los criterios de búsqueda se puede especificar un número cualesquiera de términos de consulta. Separe los términos con un espacio o con un operador booleano. Los términos que están separados únicamente con un espacio implican un operador lógico OR booleano. Un operador OR significa que es igual de importante encontrar un término u otro de los especificados. Los resultados que satisfacen más términos de búsqueda se colocan en la parte superior de la lista para indicar la fortaleza de la coincidencia respecto a los términos de consulta.

Un solo criterio de búsqueda se conoce también como término de consulta. Las búsquedas normalmente implican más de un término de consulta. El conjunto de términos de consulta para una sola búsqueda también se conoce como serie de consulta. La formulación de consultas requiere práctica, pero no es difícil. Implica únicamente unos cuantos términos de búsqueda y aprender a crear y negar los términos creando las combinaciones que ofrecerán los resultados que desea. Puesto que las series de consulta se guardan en QRadar Incident Forensics, puede ir ajustando las búsquedas a medida que conozca mejor los datos.

Tareas relacionadas:

"Visualización de relaciones y asociaciones" en la página 30
Utilice la ventana Visualize para ver las relaciones entre los atributos en los documentos recuperados. Por ejemplo, puede inspeccionar las direcciones de correo electrónico que se han comunicado con una dirección de correo electrónico concreta.

Términos de consulta de formato libre

Para buscar coincidencias exactas de series de caracteres, los investigadores escriben los términos de consulta directamente en el campo de criterios de búsqueda en la pestaña **Análisis forense**. Puede utilizar consultas de una sola palabra o de varias.

En la tabla siguiente se describe el tipo de consultas de búsqueda que se pueden utilizar.

Tabla 1. Tipos de consultas de formato libre

Tipo de consulta de búsqueda	Descripción	Ejemplo
Consulta de una sola palabra	Busca un solo término en los documentos.	cachorros
Consulta simple con comodín	Busca una coincidencia de uno o varios caracteres en el medio o al final de un término de consulta. **Restricción:** Los caracteres comodín no se pueden utilizar como primer carácter en una búsqueda.	te?t test* te*t
Consulta de varias palabras	Especifica que los resultados de la búsqueda se devuelven ordenados según la relevancia del término de consulta. Los documentos que contienen ambos términos aparecen en la parte superior de la lista, seguidos de los documentos que contienen solamente uno de los términos de búsqueda. Los documentos que contienen solamente un término de consulta se clasifican según el número de apariciones de ese término de consulta.	regalar cachorros

Tabla 1. Tipos de consultas de formato libre (continuación)

Tipo de consulta de búsqueda	Descripción	Ejemplo
Consulta de varias palabras con comillas dobles	Coincide con la serie exacta. Los documentos que contienen ambas palabras, pero no en este orden y con esta proximidad, no se devuelven como resultado. Las comillas dobles hacen que estas dos palabras se consideren una sola serie o término de consulta. Para el motor de búsqueda, dejan de considerarse dos palabras por separado.	"regalar cachorros"
Consulta de varias palabras que utiliza el operador AND	Especifica que ambos términos de consulta deben estar presentes en el documento para dar como resultado una coincidencia. Los términos de consulta pueden estar en cualquier orden y no es necesario para que estén próximos entre sí.	regalar AND cachorros

Etiquetas de metadatos

Las entidades habituales se etiquetan para permitir a los investigadores recuperar rápidamente conjuntos de resultados exactos a partir de los documentos relevantes.

Muchos campos de metadatos se pueden utilizar en el índice de Incident Forensics, según el tipo de sesión, documento o protocolo.

Cuando especifique un nombre de etiqueta de metadatos, debe ser exacto y existir en el repositorio de análisis forense.

En la tabla siguiente se enumeran los tipos de búsquedas de etiquetas de metadatos.

Tabla 2. Búsquedas de etiquetas de metadatos

Tipo de búsqueda de etiquetas de metadatos	Formato	Ejemplo
Estándar	`MetadataTag:<valor>`	`ApplicationProtocol:http`
Con comodines	`MetadataTag:*`	`CreditCardNumber:*`
Rango	`MetadataTag:[<valor inicial> TO <valor final>`	`Duration:[30 TO 56]`

Conceptos relacionados:

"Anotaciones de documentos" en la página 23
Los investigadores marcan documentos y les añaden notas para realizar un seguimiento de ideas y motivaciones relacionadas con los documentos del caso.

Combinaciones booleanas

Se pueden unir varios términos de consulta mediante operadores booleanos simples para crear cadenas de consulta muy específicas. Si se crean correctamente, estas series de consulta pueden devolver resultados que se correspondan exactamente con lo que el investigador está buscando.

Los operadores booleanos básicos son AND, OR, NOT y (). El operador AND especifica que los dos términos de consulta deben coincidir en el documento. El operador OR especifica que uno de los dos términos se puede encontrar en un documento. El operador NOT niega, o elimina los resultados, que coinciden con los términos de la consulta que están negados. El operador () agrupa los términos de consulta y los valores para aplicar funciones a un conjunto, aplicar varios valores a una sola función o para proporcionar mayor claridad en la sintaxis.

Los operadores booleanos deben escribirse en mayúsculas.

En la tabla siguiente se enumeran los operadores booleanos y se proporciona un ejemplo de una serie de consulta.

Tabla 3. Operadores booleanos para las series de consulta

Operador booleano	Serie de consulta de ejemplo	Explicación del ejemplo
AND	`TcpPort:80 AND Protocol:http`	Se utilizan dos términos de consulta para buscar todo el tráfico web estándar. Si se realizan pruebas de la Web en el puerto 8080, no se trataría de un resultado coincidente, ya que no se darían ambos términos de consulta.
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	Se utilizan tres términos de consulta para limitar los resultados a las colecciones de documentos de Yahoo, CNN y MSN del repositorio de análisis forense.
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	Busca tráfico que utiliza puertos no estándares. El primer término de consulta busca tráfico HTTP estándar y el segundo término de consulta excluye todo el tráfico que está utilizando puertos HTTP aceptados.

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		Estas consultas utilizan paréntesis para lograr objetivos complejos. Sin los paréntesis, estas consultas tardan más tiempo y son más difíciles de crear y depurar.

Herramienta de creador de consultas

Utilizar la herramienta de creador de consultas para crear búsquedas o gestionar las búsquedas guardadas.

La herramienta de creador de consultas guía gráficamente a los investigadores a través del proceso de creación de búsquedas potentes que utilizan listas categorizadas de términos de consulta con ejemplos.

Tabla 4. Parámetros para la herramienta de creador de consultas

Parámetro	Descripción
Select Category	Filtra la lista de etiquetas de metadatos disponibles en la lista **Select Field**.

Tabla 4. Parámetros para la herramienta de creador de consultas (continuación)

Parámetro	Descripción
Select Field	Etiquetas de metadatos utilizadas para etiquetar la información en el repositorio de análisis forense.
Query Example	Ejecuta la consulta que se encuentra en el campo **Query Input** e indica el número de resultados.
New	Sustituye una consulta existente por la consulta nueva cuando se pulsa **Insert Query**.
AND	Combina una consulta nueva con la consulta existente cuando se pulsa **Insert Query**. Los documentos deben contener ambos términos de consulta.
OR	Combina la consulta nueva con la consulta existente cuando se pulsa **Insert Query**. Los documentos deben contener uno de los términos.

Los investigadores puede guardar y organizar las búsquedas en carpetas en el sistema de archivos, lo que permite que los investigadores las compartan. Los investigadores utilizan descripciones o nombres para las consultas guardadas con fines de consulta, gestión y comprensión.

La función **Use Query** de la pestaña **Query** se utiliza para enviar una consulta guardada al campo **Search Criteria Input** para su ejecución.

Los investigadores utilizan la lista de consultas anterior para buscar las consultas ejecutadas anteriormente y volver a ejecutarlas; para ello, seleccionan la consulta que desean ejecutar y pulsan **Insert Query**.

Herramienta de filtro de consultas

La herramienta de filtro de consultas utiliza los datos activos para proporcionar pistas visuales para la creación de filtros persistentes.

El filtro de consultas es un filtro persistente en segundo plano que reduce el conjunto de documentos activos que es objeto de interrogación por parte de la cadena de consulta. Mediante el uso de un filtro, puede reducir el conjunto de documentos disponibles sin sobrecargar la cadena de consulta con términos de consulta estáticos. Como resultado, tiene más control sobre la cadena de consulta.

El filtro de consultas es un buen lugar para iniciar una investigación debido a las listas de tipos de filtro que dependen del caso, la actualización dinámica y el resumen de resultados en tiempo real. Las listas de tipos de filtro se llenan con todos los valores que se encuentran en los casos que están disponibles para el usuario. El usuario puede ver rápidamente qué datos se encuentran dentro de los casos que son propiedad del usuario. Cuando selecciona o deselecciona elementos de la lista de tipos de filtro, el resumen de resultados se actualiza automáticamente. Puede ver rápidamente la eficacia del filtro y qué volumen del conjunto de documentos permanece cuando se utiliza el filtro.

No es recomendable ajustar el filtro de consultas predeterminado para las consultas que desee reutilizar. Para las consultas que desee conservar, cree un filtro de consultas nuevo. Si ha modificado el filtro de consultas predeterminado, debe restablecerlo cuando haya finalizado para evitar la exclusión errónea de documentos en las consultas de búsqueda futuras.

Resultados de los filtros activos

Los investigadores ven los resultados de los filtros activos en la sección de resumen de resultados de la herramienta de filtro de consultas.

A medida que el filtro se cambia, el resumen se actualiza para mostrar el número total de documentos y el número de documentos disponibles. El número total de documentos es el número de documentos disponibles para el investigador antes de aplicar el filtro. El número de documentos disponibles es el número de documentos disponibles después de aplicar el filtro. Los investigadores utilizan estos números para juzgar la eficacia del filtro y ajustarlo correctamente a medida que lo crean.

Filtros de búsqueda de la herramienta de filtro de consultas

Los investigadores filtran los datos de los casos que tienen asignados. Los datos se dividen en grupos por tipo de filtro; por ejemplo, dirección IP o dirección MAC.

Mediante el conmutador de acción de lógica, el investigador puede incluir o excluir elementos que están seleccionados en la lista.

Cada grupo de filtros de búsqueda tiene un conmutador de acción de lógica que se puede establecer de manera que se incluyan o se excluyan los elementos que están seleccionados en la lista. Cuando está establecido en incluir, los elementos de la lista se unen con un operador AND lógico, lo que significa que cada documento disponible contiene todos los elementos seleccionados. Cuando está establecido en excluir, se utiliza un operador OR lógico, lo que significa que los documentos disponibles no contienen ninguno de los elementos seleccionados.

Los investigadores pueden utilizar el grupo **UserQuery** para crear sus propias cadenas de consulta y añadirlas al filtro.

Limitación del número de documentos devueltos en una búsqueda

Puede añadir filtros a las consultas de IBM Security QRadar Incident Forensics para limitar el número o el tipo de documentos que ve en la página de resultados de la búsqueda.

Procedimiento

1. En la pestaña **Análisis forense**, pulse el icono de **Filtros de consulta**.
   Los datos se separan en grupos por tipo de filtro.
2. En la ventana Filtros de búsqueda, para cada tipo de filtro, elija si desea incluir los documentos en los resultados de la búsqueda pulsando **Incluir** o **Excluir**.
3. Para buscar un elemento en un grupo de filtros, siga estos pasos:
   a. En la columna **Tipo de filtro**, expanda un grupo de filtros.
   b. En la ventana Buscar, seleccione los criterios y pulse **Buscar**.
      Cuando busca un registro en el grupo de filtros**Categoría web**, se visualizan todos los campos de categoría coincidentes. Por ejemplo, cuando busca **Categoría web equal chat**, se visualiza **Chat** y las categoría relacionadas,

como por ejemplo **Mensajería instantánea**, **Webmail/Mensaje unificado**, **Motores de búsqueda/catálogos web/portales** y **Cloud**.

Anotaciones de documentos

Los investigadores marcan documentos y les añaden notas para realizar un seguimiento de ideas y motivaciones relacionadas con los documentos del caso.

Los marcadores se pueden añadir a los documentos en la pantalla de resultados principal y también en la herramienta de supervisión en la cuadrícula cronológica que muestra la secuencia de documentos que se intercambian durante una interacción. Puesto que la consultas y las investigaciones pueden ser complejas, los investigadores añaden marcadores a todos los registros, incluidos los documentos de escaso interés. El uso de un marcador evita tener que volver a crear consultas y líneas de investigación complejas. Se pueden crear anotaciones después de marcar un registro.

Durante una investigación, habrá ocasiones en las que deseará seguir dos o más rutas de actuación. Utilice la función de navegador para duplicar el panel actual en el que se encuentra. De este modo no tendrá que recordar que debe retroceder y seguir las demás rutas ni recordar cómo llegar al punto de bifurcación. Puede duplicar el panel actual tantas veces como sea necesario. Siga cada ruta diferente en un panel diferente y marque los documentos pertinentes sobre la marcha. Puede añadir una nota que indique la ruta que condujo a cada documento marcado.

Las notas son una forma de anotar pensamientos mientras investiga. Solamente un administrador puede eliminar las notas. Las notas se etiquetan con el ID de usuario del investigador y la indicación de fecha y hora en la que se crearon. Cuando se exportan documentos, las notas se incluyen con el documento reconstruido y sus atributos.

Conceptos relacionados:

"Etiquetas de metadatos" en la página 19
Las entidades habituales se etiquetan para permitir a los investigadores recuperar rápidamente conjuntos de resultados exactos a partir de los documentos relevantes.

Capítulo 4. Herramientas de investigación

Los investigadores utilizan las herramientas de supervisión, impresiones digitales, exportación y visualización para gestionar los datos de distintas formas.

La página de resultados de la búsqueda es la página predeterminada en la pestaña **Análisis forense**. Los resultados de la búsqueda se muestran en el panel **Cuadrícula**. Los investigadores utilizan los resultados de la búsqueda en la cuadrícula para buscar rápidamente los documentos y acceder a ellos. En el panel **Cuadrícula**, utilice las herramientas de supervisión, impresiones digitales, exportación y visualización para proseguir la investigación.

Indicador de fila

El indicador de fila proporciona un identificador exclusivo para cada documento que se devuelve en un conjunto de resultados. Utilice el indicador de fila para enviar un documento y todos los documentos relacionados necesarios a la herramienta de visualización de vista reconstruida.

Ordenación de filas

Puede ordenar las filas que se muestran en la cuadrícula. Debido a que el número total de resultados puede ser mayor que el número de resultados que se muestran en la cuadrícula, el conjunto de resultados completo no se puede ordenar.

Indicador de documentos vistos

El indicador de documentos vistos es un pequeño círculo que alterna entre los colores rojo y verde para indicar si un investigador ha visto un documento.

Selección de documentos

Los investigadores utilizan el selector de documentos visualizados para elegir el número de documentos que se muestran en la cuadrícula de resultados. Puede utilizar SELECT ALL para enviar documentos a una función subsiguiente y enviar muchos documentos para su proceso o visualización. Cuando selecciona documentos con el selector de documentos visualizados, está seleccionando todos los documentos, no solo los que aparecen en la cuadrícula.

Visualización de documentos y la red

Los investigadores utilizan la herramienta de visualización para detectar patrones, saber dónde se produce más tráfico de red y mayor congestión de documentos durante un periodo de tiempo especificado y ver contenido sospechoso. Por ejemplo, los investigadores pueden visualizar los patrones de tráfico de red, como, por ejemplo,servidores a los que se accede después del horario de oficina.

La herramienta VGrid se divide en bloques de tiempo. El contenido sospechoso, como el tráfico de red o los documentos, se representa mediante un rectángulo rojo en la cuadrícula. Un rectángulo verde representa contenido normal. Un bloque de color brillante indica más tráfico. Cuanto mayor sea la saturación del color, mayor será la cantidad de tráfico. El brillo de un bloque de tiempo se refiere a los datos

actuales visualizados en la herramienta VGrid. Por ejemplo, un bloque de tiempo de color brillante adquiere un color más oscuro a medida que se cargan diferentes bloques de tiempo con más datos.

Los investigadores pueden ver los tipos de tráfico de red y el número de documentos de cada bloque de tiempo que tiene contenido.

Inspección del tráfico de red y los documentos en un bloque de tiempo

Puede que a los investigadores les interese inspeccionar documentos individuales, los sitios explorados o los mensajes de correo electrónico enviados en un bloque de tiempo específico.

Procedimiento

1. En el panel **Análisis forense**, seleccione la pestaña **VGrid**.
2. Utilice una de las opciones siguientes para inspeccionar el contenido en un bloque de tiempo:
   - Para ver los tipos de tráfico de red y el número de documentos, pase el ratón sobre el bloque de tiempo.
   - Para realizar búsquedas en el contenido en el bloque de tiempo, seleccione uno o varios bloques de tiempo. Pulse el botón derecho del ratón y seleccione **Search selected time blocks**.
   - Para ver la secuencia de sucesos, seleccione el bloque de tiempo y, a continuación, seleccione **Surveyor**.
   - Para visualizar el contenido, seleccione un bloque de tiempo y, a continuación, seleccione **Visualize**.

Herramienta de supervisión

Utilice la herramienta de supervisión para visualizar una secuencia de sucesos en un incidente de seguridad según se han producido.

Esta herramienta la utilizan los investigadores para saber qué han visto los presuntos atacantes y qué acciones han realizado. La herramienta de supervisión muestra la secuencia cronológica de actividades en un incidente de seguridad en un visualizador como si fuese una película. Puesto que la herramienta de supervisión está orientada al tiempo, la selección de un único documento en la pantalla de resultado no proporciona demasiada información. Si se han seleccionado demasiados pocos documentos, amplíe el radio de tiempo en torno a los documentos seleccionados en el panel **Atributos**. Para ello, pulse el enlace **Mostrar contexto**.

Los investigadores pueden filtrar las consultas de acuerdo con la hora del caso, protocolo y dirección IP.

En el panel **Lista** puede ver una lista cronológica de documentos que se han enviado y recibido. La herramienta de supervisión muestra una recreación paso a paso de la interacción.

Los identificadores de documento de color verde indican que un investigador ha revisado el documento, mientras que los documentos cuyos identificadores son de color rojo no se han revisado.

Vista de documentos reconstruidos

En la pestaña **Ver** se muestra una vista reconstruida del documento que está seleccionado en la parte izquierda de la pantalla en la vista de lista.

Esta potente combinación de secuencia en la parte izquierda y reconstrucción en la parte derecha hace posible ver lo que los atacantes sospechosos han visto y han hecho en la red. Además de los documentos visibles que han pasado por la red, la herramienta de supervisión también muestra los reconocimientos de sistema a sistema subyacentes y los intercambios de certificados que han tenido lugar.

Tareas relacionadas:

Capítulo 5, "Investigación del tráfico de red de una dirección IP", en la página 37
Para obtener visibilidad del contenido relevante en las conversaciones que se han producido durante un incidente de seguridad, puede recuperar y reconstruir el tráfico de red que está asociado con una dirección IP. También puede buscar entre los casos existentes relacionados con una dirección IP.

Contenido extraído del documento

El panel **Texto** muestra el contenido que se extrae del documento. El contenido del documento no tiene formato.

Este texto es del indexador del motor de búsqueda.

Exportación de documentos en QRadar Incident Forensics

En IBM Security QRadar Incident Forensics, todos los documentos exportados, excepto los documentos pcap exportados, incluyen el documento reconstruido, el texto en bruto del documento, los atributos y las notas que se hayan adjuntado al documento.

Cuando se exportan documentos pcap, no se realiza ninguna reconstrucción. Por ejemplo, cuando exporta una página web, se descarga cualquier cosa que el navegador haya descargado durante la conexión principal. Normalmente, la mayor parte del contenido de texto se descarga durante la conexión principal. Sin embargo, la mayoría de navegadores modernos utilizan varias conexiones para descargar más elementos, como por ejemplo las hojas de cálculo y las imágenes que no forman parte de la exportación. Cuando exporta, el contenido de pcap no se reconstruye primero.

Otro ejemplo son los protocolos complejos, como por ejemplo FTP y VOIP, donde hay una conexión de control y mandato principal y una conexión de datos aparte. Si exporta los archivos pcap para una llamada VOIP o una descarga FTP, los datos no se reconstruyen y puede obtener resultados inesperados.

Exportación de documentos como archivos pcap

Puede exportar documentos como archivos pcap de varios dispositivos IBM Security QRadar Incident Forensics y IBM Security QRadar Packet Capture.

Restricción: El contenido que exporta al formato pcap no se reconstruye.

Procedimiento

1. Para exportar datos de documentos seleccionados, en esta cuadrícula de recuperación en la pestaña **Análisis forense**, marque los recuadros de selección situados junto a los documentos, y a continuación pulse **Exportar**.

Puede seleccionar un máximo de 25 documentos a exportar al formato pcap.

2. En la lista **Seleccionar tipo de exportación**, pulse **PCAP**.
3. Una vez exportados todos los documentos para un host de QRadar Incident Forensics, puede pulsar **Descargar**.
4. Si la exportación de un documento falla, vuelva a exportar el documento pulsando el mensaje **FAIL**.

Resultados

Si exporta un solo archivo pcap, se descarga el archivo pcap. Si exporta más de un archivo pcap, los archivos pcap se ensamblan en un archivo comprimido (.zip) que se descarga.

Cada documento almacena la dirección IP del host de QRadar Incident Forensics y la dirección IP del dispositivo QRadar Packet Capture del que proviene originalmente el documento. Si elimina un host de QRadar Incident Forensics o mueve un QRadar Packet Capture, no podrá realizar una exportación.

Impresión digital

Una *impresión digital* es un conjunto compilado de asociaciones y relaciones que identifican un seguimiento de pista de identidad. Las impresiones digitales reconstruyen las relaciones de red para ayudar a descubrir la identidad de una entidad atacante, cómo se comunica y con qué se comunica.

Utilice la herramienta de impresión digital para responder rápidamente a estas cuestiones importantes:

- ¿Qué se conoce sobre este atacante, sistema o dirección IP sospechoso?
- ¿Con quién se ha comunicado este atacante sospechoso?
- ¿Quién forma parte de la red de contactos del atacante?
- ¿Está el atacante intentando disfrazar su identidad?

Identificadores en línea

Los identificadores en línea, tales como direcciones de correo electrónico, direcciones de Skype, direcciones MAC, identificadores de conversación, identificadores de medios sociales o identificadores de Twitter, se utilizan para identificar entidades o personas. Las entidades o personas conocidas que se encuentran en el tráfico de red y en los documentos se etiquetan automáticamente.

IBM Security QRadar Incident Forensics correlaciona los identificadores etiquetados que han interactuado entre sí para generar una impresión digital.

Las relaciones de recopilación de los informes de impresión digital representan una presencia electrónica recopilada continuamente que está asociada con un atacante, una entidad relacionada con la red o cualquier término de metadatos de impresión digital. Los investigadores pueden pulsar cualquier identificador de impresión digital etiquetado que esté asociado con un documento. El informe de impresión digital resultante se lista en formato tabular y está ordenado por tipo de identificador.

Obtención de información sobre relaciones

Un informe de impresión digital muestra las interacciones entre un *identificador de centrado* y todos los otros identificadores. Un *identificador de centrado* es el identificador en línea que es la fuente de interés en un incidente de seguridad.

El identificador de nivel más alto en muchas categorías suele ser la identidad del identificador de centrado perteneciente a esa categoría o tipo de identificador. Por ejemplo, si el identificador es una dirección MAC, la dirección de correo electrónico que tiene más interacciones probablemente pertenece al presunto atacante que tiene la propiedad del sistema. Sin embargo, si las direcciones IP se asignan de forma dinámica, también debe investigar las direcciones IP que se han asignado durante un intervalo de tiempo determinado.

Las correlaciones entre otras categorías y el identificador de centrado suelen ser menos fuertes. Antes de decidir actuar de acuerdo con la impresión digital, valide los datos con fuentes independientes. Utilice la impresión digital para ampliar el ámbito de una investigación e incluir a más atacantes y entidades sospechosos.

Investigación de relaciones para realizar seguimientos de pistas de identidad

La función de impresión digital reconstruye las relaciones de red para ayudarle a identificar una entidad atacante y otras entidades con las que esta se comunica.

La herramienta de impresión digital muestra la distribución de frecuencias de sucesos correlacionados. La herramienta muestra las relaciones existentes entre entidades y contabiliza el número de relaciones. Cuanto mayor es el número, más fuerte es la relación. Por ejemplo, si examina las relaciones entre una dirección de correo electrónico y otras entidades, puede ver quién se comunica con quién. Puede ver las direcciones IP que están asociadas con la dirección de correo electrónico, las direcciones IP que el sospechoso visitó, y los demás nombres que están asociados con la dirección de correo electrónico.

En los despliegues distribuidos, puede elegir ver las relaciones correspondientes a un solo nodo de la empresa.

Procedimiento

1. Seleccione un resultado de la lista de documentos en la cuadrícula de recuperación y pulse la pestaña **Impresión digital**.
2. En la lista, seleccione un elemento que desee explorar.

   De forma predeterminada, el informe de impresión digital se lista en formato tabular y está ordenado por tipo de identificador. Se muestran todos los identificadores que han interactuado con el identificador de centrado. Los identificadores de las interacciones están organizados por tipo de identificador y se ordenan por frecuencia de interacción.
3. Si ve un identificador de interés, seleccione el identificador.

   Los identificadores son hiperenlaces y puede utilizarlos como el identificador de centrado de otro informe. Se crea otra pestaña y se visualiza el nuevo identificador de centrado. Puede ver con quién interactúa un presunto atacante y luego con quién interactúan las interacciones del sospechoso. Puede ampliar el radio de una investigación a más atacantes y entidades sospechosos con los que interactúan.
4. Para ver otro host, seleccione la dirección IP en la lista **Seleccionar host remoto**.

En las instalaciones distribuidas, puede elegir el host de QRadar Incident Forensics y luego ver la impresión digital. La vista predeterminada es el host primario, pero puede seleccionar cualquier host secundario que esté asociado con el host de QRadar Incident Forensics.

5. Para ver una visualización de las asociaciones y relaciones de las interacciones del identificador de centrado con otros identificadores, pulse la pestaña **Visualizar datos**.

Herramienta de visualización

Puede explorar las asociaciones y las relaciones visualmente entre varios atributos y categorías de datos.

Utilice la ventana Visualize para ver la correlación relacional de metadatos de uno, dos o más documentos. Cuando se utiliza una amplia selección de documentos, el investigador obtiene una vista completa de las relaciones de metadatos y la frecuencia relativa. A continuación, los investigadores pueden seguir estas rutas para profundizar en la investigación de un incidente de seguridad.

La visualización de los documentos seleccionados se puede reconstruir fácilmente con una relación diferente cambiando una o ambas relaciones.

La visualización muestra cada relación que está contenida dentro de los documentos seleccionados, así como la frecuencia de relación. Cada nodo representa un metadato diferenciado que se está relacionando desde los documentos seleccionados. El tamaño indica la frecuencia relativa cuando se compara con otros nodos. Los enlaces muestran las conexiones existentes entre los distintos metadatos e indican la frecuencia a través del tamaño. Los investigadores pueden utilizar los nodos para identificar posibles vías para una investigación más detallada.

Visualización de relaciones y asociaciones

Utilice la ventana Visualize para ver las relaciones entre los atributos en los documentos recuperados. Por ejemplo, puede inspeccionar las direcciones de correo electrónico que se han comunicado con una dirección de correo electrónico concreta.

Procedimiento

1. En la cuadrícula de recuperación, seleccione las casillas de verificación correspondientes a los documentos que desee investigar y pulse **Visualize**.
2. Seleccione el diseño, el número de documentos que se visualizarán y las relaciones entre los atributos que desea ver; a continuación, pulse Renovar.
3. Utilice los controles de zoom para ver más o menos detalles de la imagen.
4. Para realizar una búsqueda nueva o modificar el filtro activo, pulse el botón derecho del ratón en un nodo.

   En el menú contextual, puede recuperar un metadato para realizar una búsqueda nueva. También puede modificar el filtro activo para incluir o excluir los metadatos.

   Restricción: Puede ver hasta 9999 documentos cada vez en una ventana Visualizar.

Análisis de artefactos con respecto a contenido sospechoso o malicioso

Como analista de seguridad, puede buscar amenazas que han escapado a la detección analizando artefactos reconstruidos, como por ejemplo archivos e imágenes. Para entender las conexiones entre los colaboradores y los artefactos, también puede investigar los enlaces hacia y desde estos archivos e imágenes.

Ejemplo - Utilizar el análisis de artefactos para buscar el origen de un ataque (paciente cero)

John es un analista de seguridad en Replay Industries. Varios sistemas están infectados a pesar de todas las medidas de seguridad implementadas. Después de identificar y colocar en cuarentena estos sistemas, John necesita averiguar el modo en que se han infectado y si hay otros activos comprometidos de forma similar.

Recuperación de paquetes desde una dirección IP

A partir de las direcciones IP y el marco de tiempo aproximado implicado, John puede utilizar QRadar Incident Forensics para recuperar los datos de paquete relevantes.

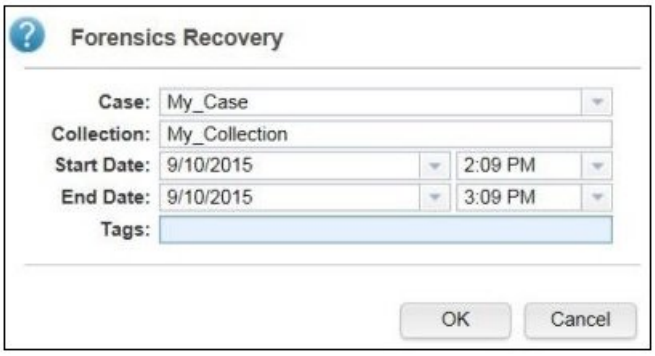


Figura 1. Recuperación desde una dirección IP

Análisis de archivos

En busca de contenido ejecutable, John empieza por utilizar las prestaciones de análisis de archivos incluidas en QRadar Incident Forensics. Ahora puede ver una lista de todos los archivos, la frecuencia con la que se han enviado si contenían archivos o scripts incluidos y sus puntuaciones de entropía. John observa rápidamente un archivo de imagen que QRadar Incident Forensics ha marcado como contenido sospechoso y con un script incluido.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

Figura 2. Atributos de análisis de archivos

La *puntuación de entropía de archivo*, que mide la aleatoriedad de los datos y se utiliza para buscar programas maliciosos cifrados, y la distribución de entropía también muestran claramente que una parte del archivo no es como debería. Un análisis más detallado prueba que este archivo contiene una nueva forma de programa malicioso que ha burlado las medidas de seguridad existentes y que es el responsable de los sistemas infectados.

En el diagrama siguiente, la entropía se utiliza como indicador de la variabilidad de bits por byte. Dado que cada carácter de una unidad de datos consta de 1 byte, el valor de entropía indica la variación de los caracteres y la compresibilidad de la unidad de datos. Las variaciones en los valores de entropía del archivo pueden indicar que hay contenido sospechoso oculto en los archivos. Por ejemplo, valores de entropía elevados pueden ser una indicación de que los datos se almacenan cifrados y comprimidos, y valores inferiores pueden indicar que, en tiempo de ejecución, la carga útil se descifra y almacena en secciones diferentes,

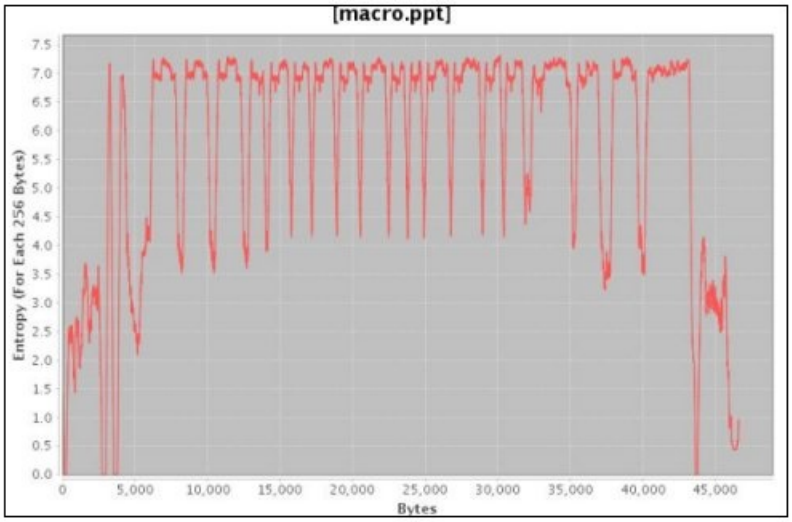


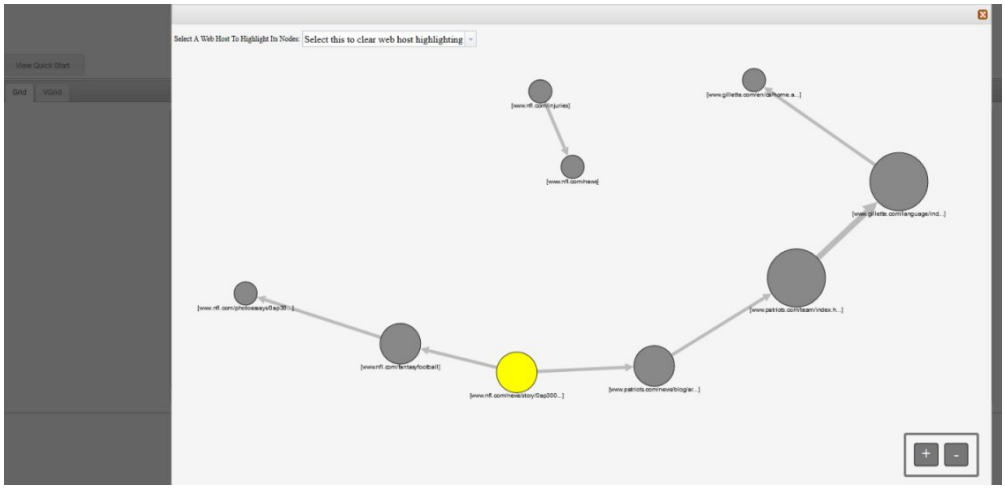
Figura 3. Ejemplo de gráfico de entropía de archivo que muestra scripts incluidos

Ahora, John necesita entender de dónde procede este archivo y quien más puede tenerlo. John utiliza QRadar Incident Forensics para buscar con rapidez el servidor web que ha suministrado el archivo de imagen infectado. La página web en cuestión es popular por difundir las noticias más actuales del equipo de la NFL favorito de todo el mundo y está comprometida. Aunque el sitio web contiene muchas imágenes, sólo la que John ha encontrado anteriormente mediante el análisis de archivos contenía el programa malicioso incluido.

Análisis de enlaces para visualizar la comunicación del sitio web

Para determinar qué otros sistemas pueden estar afectados, John utiliza el análisis de enlaces para visualizar rápidamente todos los sitios web que se han visitado y, a pesar de la gran cantidad de tráfico a través de los sitios web de empresas con las que Replay ha hecho negocios, puede observarse claramente un pequeño subconjunto de accesos al host web infectado. John analiza estos enlaces para averiguar qué otros servidores de su red se han utilizado para acceder a este host web.

En su investigación, John utiliza los nodos del gráfico, que representan páginas web, y las flechas entre los nodos, que representan las relaciones o transacciones entre las páginas web, para evaluar con rapidez patrones de tráfico y ver cómo se han cruzado documentos. Cuanto mayor es el nodo, más enlaces tiene el documento en su vía de acceso, y, cuanto más ancha es la flecha de enlace, más veces se ha utilizado el enlace.



Siendo un popular sitio de noticias de la NFL, no resulta sorprendente observar que otros diversos servidores han estado en contacto con ese host web y, posiblemente, habrán resultado afectados.

Análisis de imágenes

Para reducir el número de servidores que han descargado el archivo de imagen malicioso, John pasa al análisis de imágenes y puede ver rápidamente todos los archivos de imagen que se han enviado o recibido.

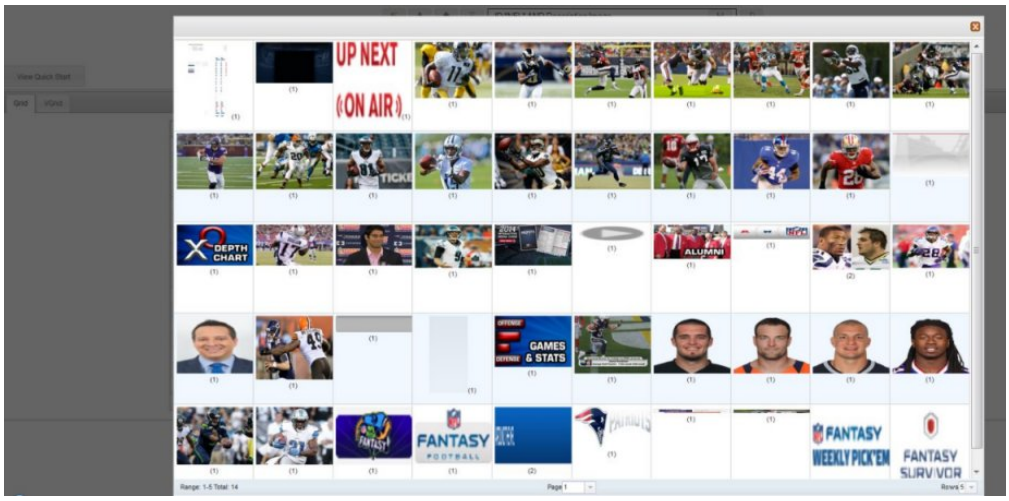


Figura 4. Ejemplo de análisis de imágenes

John confirma rápidamente que todos sus servidores infectados y 2 servidores de los que no tenía conocimiento tenían acceso al archivo de imagen comprometido.

John también determina que varios de los demás servidores que habían accedido al mismo sitio web no descargaron el archivo infectado. John tiene ahora la información necesaria para situar en cuarentena estos 2 servidores adicionales y crear un del archivo infectado que Replay Industries puede cargar y compartir con otros en IBM X-Force Exchange.

Analizar archivos con respecto a contenido incluido y actividad maliciosa

Para investigar amenazas ocultas en los archivos, puede observar valores de entropía de archivo, descargar archivos y scripts incluidos para un análisis más detallado y visualizar el documento y sus atributos.

Dado que los intrusos pueden enmascarar el contenido de los archivos binarios dentro de archivos contenedores, puede utilizar el análisis de archivos de IBM Security QRadar Incident Forensics para examinar si los archivos contienen scripts incluidos u otro contenido binario.

La *entropía de archivo* mide la aleatoriedad de los datos de un archivo y se utiliza para determinar si un archivo contiene datos ocultos o scripts sospechosos. La escala de aleatoriedad va de 0, no aleatorio, a 8, totalmente aleatorio, como por ejemplo un archivo cifrado. Cuanto más pueda comprimirse una unidad, menor será el valor de entropía; cuando menos pueda comprimirse una unidad, mayor será el valor de entropía.

En el diagrama siguiente, la entropía se utiliza como indicador de la variabilidad de bits por byte. Dado que cada carácter de una unidad de datos consta de 1 byte, el valor de entropía indica la variación de los caracteres y la compresibilidad de la unidad de datos. Las variaciones en los valores de entropía del archivo pueden indicar que hay contenido sospechoso oculto en los archivos. Por ejemplo, valores de entropía elevados pueden ser una indicación de que los datos se almacenan cifrados y comprimidos, y valores inferiores pueden indicar que, en tiempo de ejecución, la carga útil se descifra y almacena en secciones diferentes,

Procedimiento

1. En la pestaña **Análisis forense**, seleccione uno o más archivos recuperados en la vista **Cuadrícula**.
2. En el menú de herramientas de investigación de la parte superior de la cuadrícula, pulse **Análisis de archivos**.

   En los resultados, cada fila de la cuadrícula contiene un dato de análisis de un documento, por ejemplo, el nombre de archivo, la descripción, si se ha detectado contenido sospechoso y valores de entropía.
3. Para ordenar los archivos según un atributo específico, como por ejemplo la entropía, pulse la cabecera de columna correspondiente.
4. En la lista de archivos, pulse un archivo con el botón derecho del ratón para investigar con mayor detalle.
   - Para revisar el documento y sus atributos, pulse **Visualizar documento**.
   - Para revisar un gráfico de entropía y comprobar si un archivo o script incluido puede contener un programa malicioso, pulse **Visualizar entropía**.

     Puede utilizar los valores de entropía como indicación de si el archivo puede incluir contenido malicioso. Por ejemplo, los archivos de texto ASCII son por lo general altamente comprimibles y tienen bajos valores de entropía. Los datos cifrados no son generalmente comprimibles, y habitualmente tienen un valor de entropía elevado. Los programas maliciosos están a menudo empaquetados y ocultos tanto en archivos como en imágenes.
   - Para descargar archivos incluidos, pulse **Extraer archivos incluidos** y seleccione los archivos a descargar.

Esta opción sólo está disponible para documentos con archivos o scripts incluidos. Los archivos se descargan en la ubicación de descargas del navegador web. Tenga cuidado de no abrir scripts potencialmente peligrosos en un entorno desprotegido.

Analizar imágenes con respecto a amenazas ocultas o actividad sospechosa

Las imágenes visualizadas se ordenan por tamaño y relevancia con un número de frecuencia entre paréntesis. Este análisis puede ser de utilidad si un empleado está utilizando recursos de la empresa para consultar imágenes inapropiadas, restringidas o prohibidas. Por ejemplo, las imágenes podrían estar relacionadas con aviones, determinados edificios o ubicaciones objetivos de brechas de seguridad.

Con el análisis de imágenes, puede ver las imágenes más relevantes de uno o más documentos de uno o más archivos de captura de paquete en una sola pantalla en lugar de tener que abrir cada documento y visualizar las imágenes.

Procedimiento

1. En la pestaña **Análisis forense**, seleccione en la vista **Cuadrícula** uno o más documentos que contengan image en la descripción.
2. En el menú de herramientas de investigación de la parte superior de la cuadrícula, pulse **Análisis de imágenes**.

   En los resultados, se visualizan por versiones en miniatura de todas las imágenes contenidas en los documentos por orden de relevancia. El número entre paréntesis situado junto a la imagen indica el número de instancias de la imagen en el documento. Si sitúa el cursor encima de una imagen en miniatura, la imagen se ampliará.
3. Pulse una imagen con el botón derecho del ratón para investigarla con mayor detalle.
   - Para revisar la imagen y sus atributos, pulse **Visualizar documento**.
   - Para revisar un gráfico de entropía y comprobar si la imagen puede contener un programa malicioso, pulse **Visualizar entropía**.

     Puede utilizar los valores de entropía como indicación de si el archivo puede incluir contenido malicioso. Por ejemplo, los archivos de imagen de mapa de bits y los archivos de texto ASCII son por lo general altamente comprimibles y tienen bajos valores de entropía. Los datos cifrados no son generalmente comprimibles, y habitualmente tienen un valor de entropía elevado. Los programas maliciosos están a menudo empaquetados y ocultos tanto en archivos como en imágenes.

Analizar enlaces con respecto a conexiones y relaciones

En el análisis de enlaces, los enlaces muestran los elementos en común entre los sitios web visitados. Durante las investigaciones de incidentes de seguridad, puede ver rápidamente dónde hay solapamiento y cómo se comunican los usuarios.

Por ejemplo, si cree que un grupo de infractores está colaborando pero no está seguro de cómo, puede observar un conjunto de documentos de diversos usuarios y utilizar el análisis de enlaces para visualizar páginas web comunes. A continuación, puede investigar sitios web específicos.

Procedimiento

1. En la pestaña **Análisis forense**, seleccione una o más páginas web en la vista **Cuadrícula**.

2. En el menú de herramientas de investigación de la parte superior de la cuadrícula, pulse **Análisis de enlaces**.

   Si existe una relación entre sitios web, un gráfico cytoscape muestra las páginas web en forma de círculos (nodos), y enlaces hacia y desde las páginas web en forma de flechas. Cuanto mayor es el nodo, más enlaces tiene el documento en su vía de acceso, y, cuanto más ancha es la flecha de enlace, más veces se ha utilizado el enlace. Los nodos seleccionados aparecen en amarillo.
3. Para investigar la comunicación desde un host web específico, selecciónelo en la lista **Seleccionar host web**.

   Los nodos que representan las páginas web del host web seleccionado se resaltan en forma de círculos de color gris oscuro.
4. Para aumentar o disminuir el tamaño de los círculos (nodos) y flechas, utilice los controles de acercamiento (+) o alejamiento (-).

   Puede desplazar hacia adelante y hacia atrás la ruedecilla del ratón para aumentar o disminuir el tamaño de los nodos y flechas.
5. Para mover uno o más nodos, pulse y arrastre los nodos.

   Puede mover todo el gráfico pulsando en cualquier lugar del fondo, manteniendo la pulsación y arrastrando.

Ejecución de una recuperación desde la página Atributos de un documento

Cuando ve la pestaña **Atributos** para un documento, puede ejecutar una recuperación para una dirección IP o un puerto.

Procedimiento

1. En la página Buscar, en la pestaña **Análisis forense**, realice una búsqueda.
2. En la lista de documentos devueltos, pulse uno para abrirlo.
3. Pulse la pestaña **Atributos**.
4. Pulse una dirección IP o un puerto.
5. En el menú, pulse **Ejecutar recuperación para**.

Capítulo 5. Investigación del tráfico de red de una dirección IP

Para obtener visibilidad del contenido relevante en las conversaciones que se han producido durante un incidente de seguridad, puede recuperar y reconstruir el tráfico de red que está asociado con una dirección IP. También puede buscar entre los casos existentes relacionados con una dirección IP.

Cuando el tráfico de red se reconstruye a partir de una dirección IP, se crea un incidente. Los investigadores pueden visualizar una secuencia de sucesos del incidente de seguridad o ver los documentos del incidente.

IBM Security QRadar Incident Forensics indexa todos los datos de red, datos de archivos, metadatos y caracteres de texto disponibles que se encuentran en cada uno de los archivos recuperados.

En los despliegues distribuidos, varios dispositivos de captura y hosts de QRadar Incident Forensics capturan y procesan los datos. Puede ver los resultados totales de la recuperación de incidentes o los resultados por host y dispositivo de captura.

Procedimiento

1. Para crear un caso y obtener datos de los dispositivos de captura de paquetes, en QRadar, pulse una dirección IP con el botón derecho del ratón y después seleccione **Ejecutar recuperación forense**.
   a. En la tabla siguiente se proporciona una guía de los parámetros de recuperación de datos:

Tabla 5. Parámetros de recuperación de datos

Parámetro	Descripción
Caso	Caso que se utiliza para la investigación. **Restricción:** El nombre del caso debe ser exclusivo.
Colección	Los datos recuperados se agrupan para formar una colección y se asocian al caso. **Restricción:** El nombre de la recopilación debe ser exclusivo. Si el nombre de la recopilación existe en el caso, la recopilación original se suprime.
Fecha de inicio	Fecha y hora de inicio de la captura de paquetes de datos.
Fecha de finalización	Fecha y hora de finalización de la captura de paquetes de datos.
Etiquetas	Etiquetas de metadatos que se utilizan para recuperar rápidamente conjuntos de resultados exactos a partir de los documentos relevantes. **Restricción:** El símbolo # no está permitido. Puede utilizar otros caracteres especiales, tales como $, %, *.

   b. Pulse **Aceptar** y luego pulse la pestaña **Análisis forense**.

      Resolución de problemas: Si aparece un mensaje para indicarle que no tiene permiso para recuperar datos, compruebe que su perfil de seguridad tiene acceso a la dirección IP. En algunos casos, si ha utilizado un carácter # en el campo **Etiquetas**, puede aparecer ese mensaje.
   c. Pulse el icono en forma de triángulo para ver los incidentes.

d. Para ver una secuencia de sucesos del incidente, pulse **Saltar a página de resultados de la herramienta de supervisión**.

e. Para ver los documentos del incidente, pulse **Saltar a página de resultados de búsqueda**.

2. Para buscar en casos existentes de la dirección IP, en QRadar, pulse una dirección IP con el botón derecho del ratón y pulse **Ejecutar búsqueda forense**.

   a. En la pestaña **Análisis forense**, pulse el icono de incidentes (triángulo).

   b. Para investigar todas las actividades que están asociadas con un incidente, coloque el ratón sobre un caso para resaltarlo y, a continuación, pulse el icono de búsqueda.

   c. Para investigar las actividades por host de QRadar Incident Forensics y dispositivo de captura en los despliegues distribuidos, expanda la entrada **Caso** y, a continuación, expanda la entrada **Recopilación**.

   d. Para ver una lista cronológica de las interacciones en un incidente, coloque el ratón sobre la recopilación para resaltarla y, a continuación, pulse el icono del supervisor.

Conceptos relacionados:

"Vista de documentos reconstruidos" en la página 27
En la pestaña **Ver** se muestra una vista reconstruida del documento que está seleccionado en la parte izquierda de la pantalla en la vista de lista.

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 o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de www.ibm.com/legal/copytrade.shtml.

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.

Glosario

Este glosario proporciona términos y definiciones para el software y los productos de IBM Security QRadar Incident Forensics.

En este glosario se utilizan las referencias cruzadas siguientes:

- *Véase* le remite desde un término no preferido al término preferido o desde una abreviatura a la forma completa.
- *Véase también* le remite a un término relacionado u opuesto.

Para otros términos y definiciones, consulte el sitio web de terminología de IBM (se abre en una ventana nueva).

"A" "C" "D" "H" en la página 44 "I" en la página 44 "M" en la página 44 "O" en la página 44 "P" en la página 44 "R" en la página 44 "S" en la página 44 "T" en la página 45 "V" en la página 45

A

anomalía
Desviación del comportamiento esperado de la red.

atacante
Usuario (persona o programa de software) que intenta causar daño a un sistema de información o acceder a información no pensada para el acceso general. Véase también ataque.

ataque
Cualquier intento por parte de una persona no autorizada de poner en peligro el funcionamiento de un programa de software o sistema en red. Véase también atacante.

C

caso Información situada en una base de datos que pertenece a una investigación determinada.

categoría
Conjunto de elementos que se agrupan de acuerdo con una clasificación o descripción determinada. Las categorías pueden ser niveles diferentes de información dentro de una dimensión.

cifrado
En seguridad informática, proceso que transforma datos a un formato ininteligible de manera que los datos originales no se pueden obtener o sólo se pueden obtener utilizando un proceso de descifrado.

colección
Un conjunto diferenciado de datos, con nombre, que está asociado a un caso. Por ejemplo, un conjunto ordenado de paquetes de red capturados.

conversación
Flujo de datos reconstruido por análisis forense entre dos o más puntos finales de red. Por ejemplo, una conversación de red social.

correlación relacional de metadatos
Correlación que muestra metadatos relacionados de documentos de casos.

D

delito Mensaje enviado o suceso generado en respuesta a una condición supervisada. Por ejemplo, un delito proporcionará información sobre si se ha vulnerado una política o si la red está bajo ataque.

descompilación
Proceso por el cual se descompilan los datos de captura de paquetes para que todos los datos absorbidos se generen como informe de resultados.

dispositivo de captura
Véase dispositivo de captura de paquetes.

dispositivo de captura de paquetes
Dispositivo autónomo que intercepta y registra datos de tráfico.

H

herramienta de supervisión
Herramienta que muestra la secuencia cronológica de actividades de un incidente de seguridad en un visualizador.

hipótesis
Explicación propuesta para un incidente que está basada en los datos disponibles que se han recopilado en un caso. Una hipótesis se debe poder probar y falsificar.

I

identidad
Colección de atributos procedentes de un origen de datos que representan una persona, organización, lugar o elemento.

identificador de centrado
Elemento de categoría con el que han interactuado todos los demás identificadores. El identificador de centrado es el elemento central en una investigación.

impresión digital
Informe que consta de identificadores etiquetados que están relacionados entre sí dentro de un caso individual.

incidente
Véase incidente de seguridad.

incidente de seguridad
Suceso en el que se violan, ponen en peligro o atacan operaciones de red normales.

información de captura de paquetes
Información sobre datos de tráfico que se recopila mediante un dispositivo de captura.

inspector de dominios
Inspector especializado que está diseñado para deconstruir y extraer datos forenses de sitios web de dominio determinados, tales como Facebook o Gmail.

inspector de protocolos
Inspector especializado que está diseñado para extraer datos forenses a partir de protocolos de red, tales como HTTP o FTP.

investigador forense
Usuario que extrae datos significativos del tráfico de red y documentos del repositorio de análisis forense.

M

metadatos
Datos que describen las características de datos; datos descriptivos.

O

Operador booleano
Función incorporada que especifica una operación lógica AND, OR o NOT cuando se evalúan conjuntos de operaciones. Los operadores booleanos son &&, || y !.

P

presencia electrónica recopilada continuamente
Identidad en línea de un atacante en forma de colección de impresiones digitales que están enlazadas.

R

registro de flujo
Registro de la conversación entre dos hosts.

relación de impresión digital
Relación entre identificadores etiquetados relacionados con un caso.

ruta de navegación
Elemento de interfaz web que muestra la posición del usuario dentro de un sitio web. Normalmente es una serie de hiperenlaces que aparecen a lo largo de la parte superior o inferior de la página. Estos enlaces indican páginas que se han visitado y permiten que el usuario regrese a la ubicación inicial.

S

seguimiento
Impresiones digitales que asocian personas involucradas en un caso con personas ajenas al caso.

superflujo
Flujo que consta de varios flujos con propiedades similares a fin de aumentar la capacidad de proceso mediante la reducción de las restricciones de almacenamiento.

T

trabajo de recuperación
Proceso que recupera datos de captura consultados y los reenvía al dispositivo de descompilación para su absorción.

tráfico En comunicación de datos, volumen de datos transmitidos a partir de un punto determinado de una ruta.

tráfico de red absorbido
Tráfico de red capturado que ha sido procesado por el proceso de descompilación forense.

V

vulnerabilidad
Riesgo de seguridad en un sistema operativo, software del sistema o componente de software de aplicación.

Índice