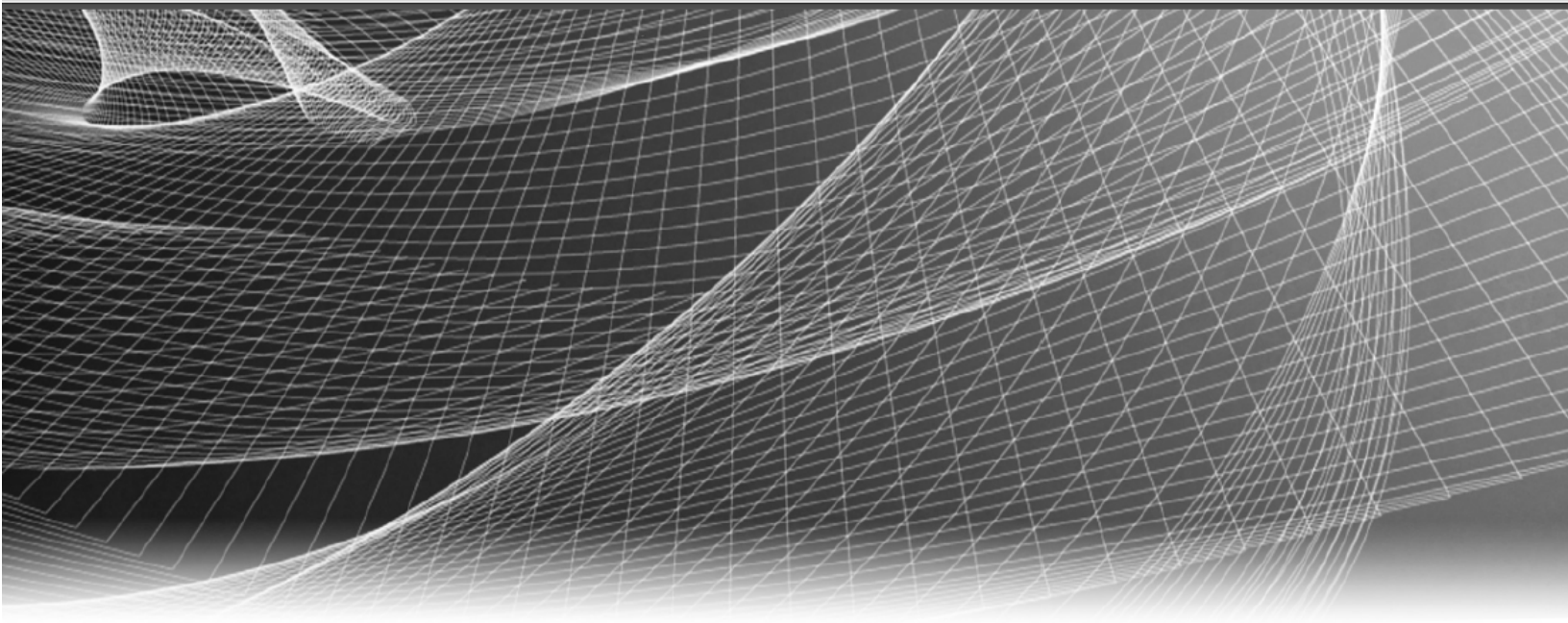


RSA Security Analytics

Guía de Investigation y Malware Analysis

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Cómo funciona Investigation

El módulo Investigation ofrece funcionalidades de análisis de datos en Security Analytics de modo que los analistas puedan analizar datos e identificar posibles amenazas internas o externas a la seguridad y la infraestructura de IP.

Datos y metadatos para Investigation

Security Analytics audita y monitorea todo el tráfico en una red. En la red de RSA, los Decoders recopilan, analizan y almacenan los paquetes y los registros que recorren la red. Los Concentrators almacenan los metadatos que generan los analizadores y los feeds a medida que los Decoders recopilan paquetes y registros. En la mayoría de los ambientes, todas las consultas de Investigation, Event Stream Analysis (ESA), Malware Analysis (MA) y Reporting Engine (RE) se procesan en el Concentrator. La primera interacción del analista es con los metadatos, y el Concentrator maneja la mayoría de las consultas, las cuales solo se dirigen al Decoder cuando se requiere una reconstrucción completa de sesiones o registros crudos. ESA, Malware Analysis y Reporting Engine también consultan al Concentrator, donde pueden obtener rápidamente todos los metadatos pertinentes asociados a un evento y generar información sobre este sin tener que dirigirse a cada Decoder.

Nota: Aunque un dispositivo híbrido puede desempeñar la función del Concentrator, cualquier ambiente grande que necesite un mayor nivel de ancho de banda o de eventos por segundo (EPS) requiere un dispositivo Concentrator por separado. El dispositivo Concentrator cuenta con diseño de almacenamiento que usa unidades de estado sólido para el índice, lo cual aumenta el rendimiento de lectura.

Métodos de análisis

Los analistas pueden investigar los datos capturados, abrir resultados de consultas de otros módulos de Security Analytics en una investigación e importar datos de otros orígenes de recopilación. Durante el curso de una investigación, los analistas pueden desplazarse sin inconvenientes entre las tres vistas de Investigation: vista Navegar, vista Eventos y vista Malware Analysis.

Nota: Se requieren funciones de usuario y permisos específicos para que un usuario realice investigaciones y análisis de malware en Security Analytics. Si no puede realizar una tarea de análisis o abrir una vista, es posible que el administrador necesite ajustar las funciones y los permisos configurados para usted.

Los analistas usan Investigation para buscar incidentes con el fin de impulsar su flujo de trabajo o para realizar análisis estratégico después de que otra herramienta ha generado un evento. En ambos casos, el analista desglosa o cambia a los metadatos para filtrar la cantidad de registros y paquetes y ver eventos sospechosos, a la vez que se centra en ciertas combinaciones de metadatos que llevan al incidente.

Vista Navegar

La vista Navegar proporciona la funcionalidad de desglosar y consultar datos sobre un servicio de Security Analytics. Cada situación es única en términos de los tipos de información que el analista intenta encontrar. Investigation presenta el contenido de los paquetes o los registros capturados como una recopilación en la vista Navegar. Se consultan las claves de metadatos definidas y se devuelven los valores junto con la cantidad de sesiones. Si se hace clic en un valor en cualquier nivel determinado, se revelan los resultados en detalle.

Por ejemplo, si hay alguna preocupación respecto de tráfico sospechoso con otros países, la clave de metadatos País de destino revela todos los destinos y la frecuencia del contacto. El desglose a estos valores genera los datos específicos del tráfico, como la dirección IP del originador y el destinatario. La comprobación de otros metadatos puede exponer la naturaleza los archivos adjuntos intercambiados entre las dos direcciones IP. La reconstrucción de evento puede revelar el contenido de cualquier conversación.

Vista Eventos

La vista Eventos proporciona una vista de eventos en formato de lista que permite ver eventos y reconstruirlos con seguridad. Puede abrir la vista Eventos para un valor de metadatos en un punto de desglose actual desde la vista Navegar. Para aquellos analistas que no tienen los privilegios suficientes para navegar a un servicio, la vista Eventos es una vista de investigación independiente en la cual pueden acceder a una lista de eventos de la red y de registro desde un servicio Security Analytics Core sin necesidad de desglosar primero a través de los metadatos.

La vista Eventos presenta información de eventos en tres formatos estándar: una lista de eventos en cuadrícula simple, una lista de eventos detallada y una vista de registros. Además de los formatos estándar, puede crear un grupo de columnas personalizado de claves de metadatos seleccionadas y, a continuación, asignarlo a un perfil personalizado para ver la lista de eventos. Una vez creados, los grupos de columnas personalizados y los perfiles se pueden seleccionar en una lista desplegable.

La vista Eventos permite:

- Reconstruir un evento desde la lista de eventos.
- Usar perfiles de investigación para vincular varias configuraciones de Investigation en conjuntos seleccionables, importar y exportar grupos de metadatos de Investigator e importar

y exportar grupos de columnas de Investigator.

- Exportar eventos y archivos asociados.

Vista Malware Analysis

La vista Malware Analysis proporciona una forma de analizar determinados tipos de objetos de archivos (como Windows PE, PDF y MS Office) para evaluar la probabilidad de que un archivo sea malicioso. El analista de malware puede aprovechar los módulos de puntaje de múltiples niveles para establecer prioridades entre la enorme cantidad de archivos capturados, con el fin de concentrar los esfuerzos de análisis en los archivos que tienen más probabilidad de ser maliciosos.

Funciones de Malware Analysis

Security Analytics Malware Analysis es un procesador de análisis de malware automatizado que analiza determinados tipos de objetos de archivos (como Windows PE, PDF y MS Office) para evaluar la probabilidad de que un archivo sea malicioso. Mediante el uso de Malware Analysis, el analista de malware puede establecer prioridades entre la enorme cantidad de archivos capturados, con el fin de concentrar los esfuerzos de análisis en los archivos que tienen más probabilidad de ser maliciosos.

Security Analytics Malware Analysis detecta indicadores de riesgo mediante el uso de cuatro metodologías de análisis distintas:

- Análisis de sesión de red (red)
- Análisis de archivo estático (estático)
- Análisis de archivo dinámico (Sandbox)
- Análisis de seguridad comunitario (comunidad)

Cada una de las cuatro metodologías de análisis está diseñada para compensar las debilidades inherentes de las demás. Por ejemplo, el análisis de archivo dinámico puede compensar los ataques de día cero que no se detectan durante la fase de análisis de seguridad comunitario. Al evitar análisis de malware que se concentran estrictamente en una metodología, el analista tiene más probabilidades de protegerse contra falsos negativos en los resultados.

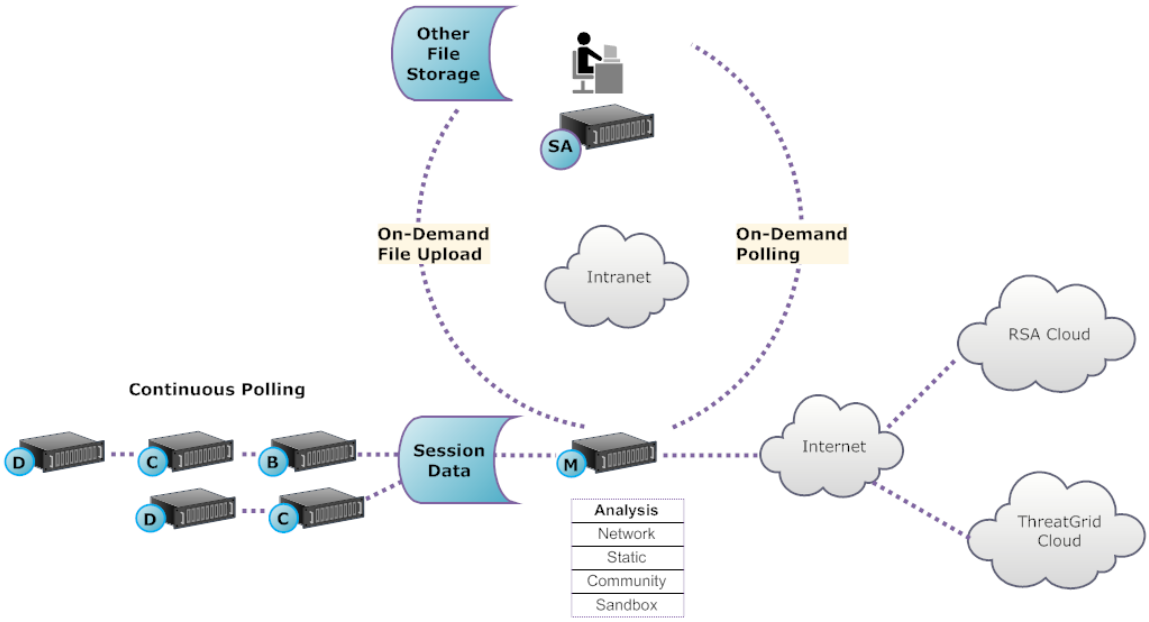
Además de los indicadores de riesgo incorporados, a partir de Security Analytics 10.3, Malware Analysis también es compatible con indicadores de riesgo escritos en YARA. YARA es un lenguaje de reglas que permite a los investigadores de malware identificar y clasificar muestras de malware. Esto permite que los autores de IOC agreguen funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live. Estos IOC basados en YARA en RSA Live se descargarán y se habilitarán automáticamente en el host suscrito con el fin de complementar el análisis existente que se ejecuta en cada archivo analizado.

A partir de Security Analytics 10.4, Malware Analysis incluye funciones compatibles con alertas para Incident Management.

Descripción funcional

En esta figura se ilustra la relación funcional entre los servicios Security Analytics Core (Decoder, Concentrator y Broker), el servicio Security Analytics Malware Analysis y el servidor de Security Analytics.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



El servicio Malware Analysis analiza objetos de archivos mediante cualquier combinación de los siguientes métodos:

- **Sondeo automático continuo de un Concentrator o un Broker** para extraer sesiones que identificó un analizador como posibles portadoras de contenido de malware.
- **Sondeo según demanda de un Concentrator o un Broker** para extraer sesiones que identificó un analista de malware como posibles portadoras de contenido de malware.
- **Carga según demanda de archivos** de una carpeta especificada por el usuario.

Cuando se habilita el sondeo automático de un Concentrator o un Broker, el servicio Malware Analysis extrae y prioriza continuamente contenido ejecutable, documentos PDF y documentos de Microsoft Office en su red, directamente de los datos que capturó y analizó el servicio Security Analytics Core. Dado que el servicio Malware Analysis se conecta a un Concentrator o un Broker para extraer solo los archivos ejecutables que están marcados como posible malware, el proceso es rápido y eficiente. Este proceso es continuo y no requiere monitoreo.

Si selecciona el sondeo según demanda de un Concentrator o un Broker, el analista de malware utiliza Security Analytics Investigation para desglosar a los datos capturados y seleccionar las sesiones que se analizarán. El servicio Malware Analysis utiliza esta información para sondear automáticamente el Concentrator o el Broker y descargar las sesiones especificadas para el análisis.

La carga según demanda de archivos proporciona un método para que el analista revise los archivos capturados de manera externa a la infraestructura de Core. El analista de malware utiliza Security Analytics para seleccionar una ubicación de carpeta e identificar uno o más archivos con el fin de cargarlos y someterlos al análisis de Security Analytics Malware Analysis. Estos archivos se analizan con el uso de la misma metodología que los archivos que se extraen automáticamente de las sesiones de red.

Método de análisis

Para el análisis de red, el servicio Malware Analysis busca características que parezcan desviarse de la norma, de manera muy similar a lo que hace un analista. Al observar cientos de miles de funciones y combinar los resultados en un sistema de puntaje ponderado, las sesiones legítimas que por coincidencia tienen algunos rasgos anormales se omiten, mientras que las sesiones realmente maliciosas se destacan. Un usuario puede aprender patrones que indican actividad anómala en las sesiones, como indicadores que requieren una investigación más detallada o indicadores de riesgo.

El servicio Malware Analysis puede ejecutar el análisis estático de objetos sospechosos que detecte en la red y determinar si esos objetos contienen código malicioso. En el caso del análisis comunitario, el nuevo malware detectado en la red se envía a RSA Cloud para compararlo con los análisis de malware propios de RSA y feeds de SANS Internet Storm Center, SRI International, el Departamento del tesoro y VeriSign. En el caso del análisis de Sandbox, los servicios también pueden enviar datos a importantes hosts de información de seguridad y administración de eventos (SIEM) (ThreatGrid Cloud).

Security Analytics Malware Analysis cuenta con un método de análisis exclusivo que se basa en asociaciones con líderes y expertos del sector, de modo que sus tecnologías puedan enriquecer el sistema de puntaje de Security Analytics Malware Analysis.

Acceso del servidor de Security Analytics al servicio Malware Analysis

El servidor de Security Analytics está configurado para conectarse al servicio Security Analytics Malware Analysis e importar datos etiquetados para un análisis más profundo en Security Analytics Investigation. El acceso se basa en tres niveles de suscripción.

- Suscripción gratuita: Todos los clientes de Security Analytics tienen una suscripción gratuita con una clave de prueba gratuita para análisis de ThreatGrid. El servicio Malware Analysis tiene un límite de 100 muestras de archivo por día. La cantidad de muestras (dentro del conjunto de archivos anterior) enviadas a la nube de ThreatGrid para el análisis de Sandbox se limita a cinco por día. Si una sesión de red tuviera 100 archivos, los clientes alcanzarían el

límite después de procesar esa sesión de red. Si los 100 archivos se cargaran manualmente, se alcanzaría el límite.

- Nivel de suscripción estándar: La cantidad de envíos al servicio Malware Analysis es ilimitada. La cantidad de muestras enviadas a la nube de ThreatGrid para el análisis de Sandbox es de 1,000 por día.
- Nivel de suscripción empresarial: La cantidad de envíos al servicio Malware Analysis es ilimitada. El número de muestras enviadas a ThreatGrid Cloud para el análisis de Sandbox es de 5,000 por día.

Método de puntaje

De manera predeterminada, los indicadores de riesgo (IOC) se ajustan para reflejar las mejores prácticas del sector. A cada IOC se le asigna un puntaje que va desde -100 (bueno) a +100 (malo). Durante el análisis, los IOC que se activan hacen que el puntaje aumente o disminuya para indicar la probabilidad de que la muestra sea maliciosa. El ajuste de los IOC se expone en Security Analytics para que el analista de malware pueda elegir si desea reemplazar el puntaje asignado o deshabilitar la evaluación de un IOC. El analista tiene la flexibilidad de usar el ajuste predeterminado o de personalizarlo completamente de acuerdo con necesidades específicas.

Los IOC basados en YARA se entrelazan con los IOC incorporados dentro de cada categoría incorporada y no se distinguen de los IOC nativos. Cuando los IOC se muestran en la vista Configuración de servicio, los administradores pueden seleccionar YARA en la lista de selección Módulo para ver una lista de reglas YARA.

Después de que se importa una sesión a Security Analytics, todas las funcionalidades de visualización y análisis de Security Analytics Investigation quedan disponibles para realizar un análisis más detallado de los indicadores de riesgo. Cuando se muestran en Investigation, los IOC de YARA se diferencian de los IOC nativos incorporados por la etiqueta `Yara rule.`.

Implementación

El servicio Security Analytics Malware Analysis se implementa como un servicio que comparte ubicación en un servidor de Security Analytics o con un host de RSA Malware Analysis exclusivo.

El host de Malware Analysis exclusivo cuenta con un Broker incorporado que se conecta a la infraestructura de Security Analytics Core (que puede ser otro Broker o un Concentrator). Antes de esta conexión, se debe agregar un conjunto de analizadores y feeds a los Decoders que están conectados a los Concentrators y los Brokers desde los cuales extrae datos el servicio Malware Analysis. Esto permite que los archivos de datos sospechosos se marquen para extracción. Estos archivos son contenido etiquetado como `malware analysis` que está disponible a través del sistema de administración de contenido de RSA Live.

Módulos de puntaje de malware

RSA Security Analytics Malware Analysis analiza y asigna puntajes a las sesiones y a los archivos incorporados dentro de estas según cuatro categorías de puntaje: Red, Análisis estático, Comunidad y Sandbox. Cada categoría comprende muchas reglas y comprobaciones individuales que se usan para calcular un puntaje entre 1 y 100. Cuanto más alto es el puntaje, más probable es que la sesión sea maliciosa y que amerite una investigación de seguimiento más profunda.

Security Analytics Malware Analysis puede facilitar una investigación histórica de los eventos que conducen a una alarma o incidente en la red. Si sabe que cierto tipo de actividad está ocurriendo en su red, puede seleccionar solo los informes de interés para examinar el contenido de recopilaciones de datos. También puede modificar el comportamiento de cada categoría de puntaje de acuerdo con la categoría de puntaje o el tipo de archivo (Windows PE, PDF y Microsoft Office).

Una vez que se haya familiarizado con los métodos de navegación de datos, podrá explorar los datos de manera más completa con:

- Búsqueda de tipos de información específicos
- Revisión de contenido específico en detalle.

Los puntajes de categoría de Red, Análisis estático, Comunidad y Sandbox se mantienen y se informan de manera independiente. Cuando los eventos se visualizan según los puntajes independientes, siempre que una categoría detecte malware, es evidente en la sección Análisis.

Red

La primera categoría examina cada sesión de red principal de Security Analytics Core para determinar si la distribución de los candidatos de malware fue sospechosa. Por ejemplo, software benigno que se descarga desde un sitio seguro conocido, utilizando puertos y protocolos adecuados, se considera menos sospechoso que descargar software que se sabe que es malicioso desde un sitio de descarga dudoso. Los factores de muestra que se usan en el puntaje de este conjunto de criterios pueden incluir sesiones que:

- Contienen información de feed de amenazas
- Se conectan a sitios maliciosos bien conocidos
- Se conectan a dominios/países de alto riesgo (por ejemplo, el dominio .cc)
- Usan protocolos bien conocidos en puertos no estándar
- Contienen JavaScript oculto

Análisis estático

La segunda categoría analiza cada archivo de la sesión en busca de señales de ocultamiento para predecir la probabilidad de que el archivo se comporte de manera maliciosa si se ejecuta. Por ejemplo, software que se vincula con bibliotecas en red tiene más probabilidades de ejecutar actividades sospechosas en la red. Los factores de muestra que se usan en el puntaje de este conjunto de criterios pueden incluir:

- Archivos codificados con XOR
- Archivos detectados incorporados dentro de formatos que no son .EXE (por ejemplo, si se encuentra un archivo PE incorporado dentro de un formato GIF)
- Archivos que se vinculan a bibliotecas de importación de alto riesgo
- Archivos que se desvían considerablemente del formato PE

Comunidad

La tercera categoría asigna puntaje a la sesión y los archivos de acuerdo con el conocimiento colectivo de la comunidad de seguridad. Por ejemplo, los archivos cuya huella digital/hash ya se ha identificado como buena o maliciosa por proveedores de antivirus (AV) respetables reciben el puntaje que corresponde según eso. Los archivos también reciben puntaje según el conocimiento de que un archivo provenga de un sitio conocido como bueno o malicioso por la comunidad de seguridad.

El puntaje de la comunidad también indica si el antivirus de su red marcó los archivos como maliciosos. No indica que el producto antivirus residente actuara para proteger su sistema.

Sandbox

La cuarta categoría examina el comportamiento del software ejecutándolo en un ambiente de Sandbox. Al ejecutar el software para observar su comportamiento, se puede calcular un puntaje según la identificación de actividad maliciosa bien conocida. Por ejemplo, software que se configura a sí mismo para iniciarse automáticamente en cada reinicio y establecer conexiones IRC tendría un puntaje más alto que un archivo que no presente un comportamiento malicioso conocido.

Funciones y permisos para analistas de malware

En este tema se identifican las funciones y los permisos que se necesitan para que un usuario realice análisis de malware en Security Analytics. Si no puede realizar una tarea de análisis o abrir una vista, es posible que el administrador necesite ajustar las funciones y los permisos configurados para usted.

Funciones y permisos requeridos

RSA Security Analytics administra la seguridad mediante el acceso a las vistas y las funciones con el uso de permisos del sistema y permisos de servicios individuales.

En el nivel del sistema, es necesario que se asigne al usuario una función del sistema, en la vista Administration > Sistema, que proporcione acceso a vistas y funciones específicas. A la función predeterminada `Malware_Analysts` en Security Analytics 10.5 se asignan todos los permisos que se enumeran a continuación. Si es necesario, un administrador puede crear una función personalizada con alguna combinación de los siguientes permisos:

- Acceder al módulo Investigation (requerido)
- Investigation: navegar por los eventos
- Investigation: navegar por los valores
- Acceder al módulo Incident
- Ver y administrar incidentes
- Ver eventos de malware (para ver eventos)
- Descarga de archivos (para descargar archivos desde el servicio Malware Analysis)
- Iniciar escaneo de malware (para iniciar un escaneo de servicio de una sola vez o una carga de archivos de una sola vez)
- Permisos de dashlet para mayor comodidad: Dashlet - Investigar dashlet de valores principales, Dashlet - Investigar dashlet de lista de servicios, Dashlet - Investigar dashlet de trabajos, Dashlet - Investigar dashlet de accesos directos.

Nota: Cuando se actualiza de Security Analytics 10.4 a Security Analytics 10.5, el nombre de la función predeterminada `MalwareAnalysts` de Security Analytics 10.4 se cambia a `Malware_Analysts` y los permisos asignados no se modifican.
Cuando se actualiza de Security Analytics 10.3 y anteriores, la función `Malware Analyst` incluye un subconjunto de estos permisos. El nombre de la función `Malware Analyst` predeterminada se cambia a `MalwareAnalysts`, si existe, y se agregan los nuevos permisos. Si la función `Malware Analyst` no existía, se crea la función `MalwareAnalysts` nueva.

Un caso de uso para la creación de una función personalizada sería una función Analista de malware junior, con permisos limitados que no incluyen el permiso de descarga de archivos.

En servicios específicos, un analista de malware debe ser miembro del grupo **Analistas** o de un grupo que tenga los dos permisos predeterminados asignados al grupo Analista: **sdk.meta** y **sdk.content**. Los usuarios que tienen estos permisos pueden utilizar aplicaciones específicas, ejecutar consultas y ver el contenido para fines de análisis del servicio.

Configurar las vistas y las preferencias de Investigation

Los analistas pueden configurar algunos aspectos de las vistas y el comportamiento de Security Analytics Investigation. Puede personalizar la forma en que aparecen las vistas de Investigation, los tipos de información que se muestran y los factores que afectan el rendimiento en la devolución de resultados y la reconstrucción de eventos. Todos los ajustes configurables tienen valores predeterminados que son eficaces en la mayoría de las implementaciones; sin embargo, los analistas tienen la opción de ajustarlos si es necesario.

Las cuentas de usuario de los analistas que realizan análisis mediante Security Analytics Investigation deben tener configuradas las funciones y los permisos correspondientes del sistema. Un administrador debe configurar las funciones y los permisos, como se describe en Funciones y permisos para los analistas.

Se proporciona información detallada en los siguientes temas:

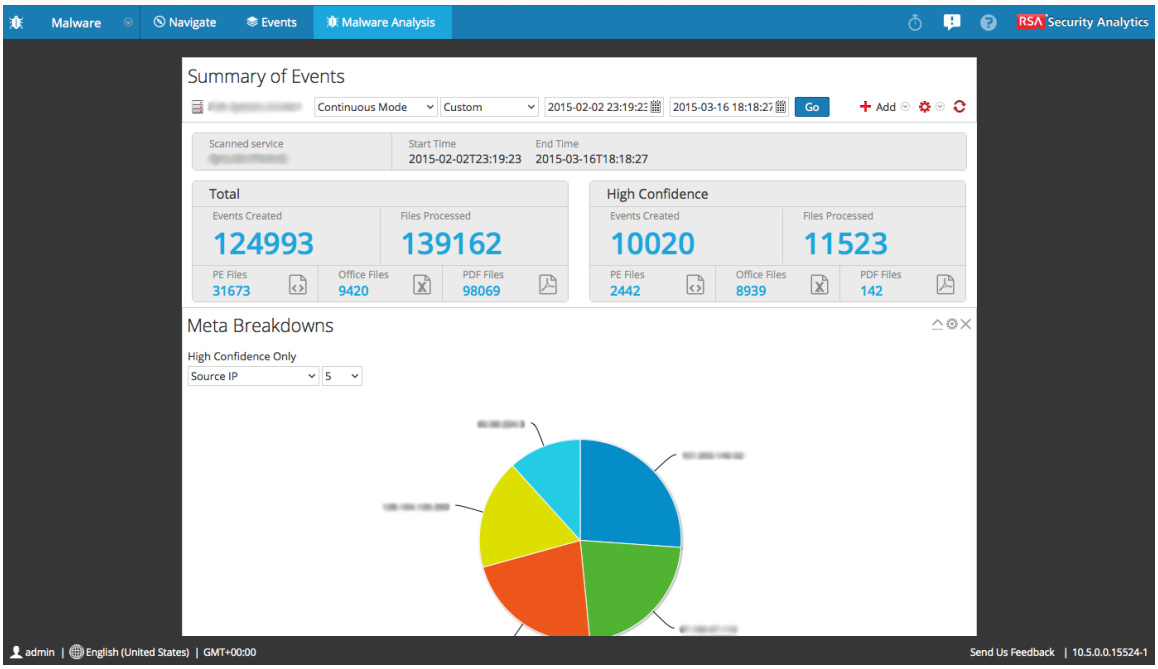
- Configurar la vista Navegar y la vista Eventos
- Configurar la vista Resumen de eventos de malware

Configurar la vista Resumen de eventos de malware

En el Resumen de eventos se ofrece un resumen del escaneo que se investiga, y bajo el resumen se presentan dashlets configurables, como gráficos de visualización y listas. De forma predeterminada, se abre el Resumen de eventos para un escaneo, el cual muestra los dashlets predeterminados. Puede personalizar la vista mediante la adición, la modificación y la eliminación de dashlets predeterminados. La personalización de dashlets configurada persiste en distintas investigaciones de escaneos y los dashlets predeterminados se pueden restaurar en cualquier momento. Los dashlets predeterminados son:

- Resumen de eventos (fijo)
- Cronograma de evento
- Lista del malware altamente sospechoso principal
- Mapa de árbol de metadatos
- Rueda de puntaje
- Desgloses de metadatos

En la siguiente figura se muestra un ejemplo del Resumen de eventos predeterminado.



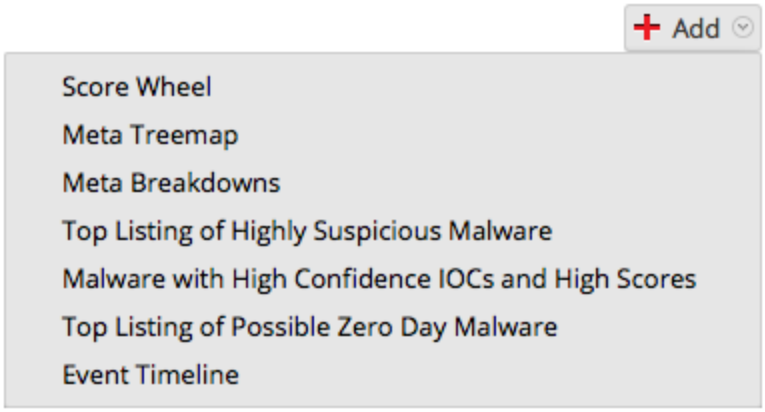
El resto de este tema proporciona instrucciones para administrar y configurar los dashlets.

Agregar un dashlet

Puede agregar múltiples copias de dashlets en el Resumen de eventos de Malware Analysis. Para agregar un dashlet:

1. En la barra de herramientas, seleccione **Agregar**.

   Se muestra la lista desplegable de dashlets. Hay cuatro opciones de visualización: Rueda de puntaje, Mapa de árbol de metadatos, Desgloses de metadatos y Cronograma de evento. Los otros tres dashlets son los mismos dashlets disponibles en el tablero Unified: Malware con IOC de alta confianza y altos puntajes, Lista del malware altamente sospechoso principal y Lista del posible malware de día cero principal.



2. Seleccione un dashlet.

   El nuevo dashlet se agrega como el último debajo de los dashlets existentes.

3. Si el dashlet es un duplicado de otro existente, cambie el nombre del nuevo dashlet para que sea único.

Modificar o eliminar un dashlet mediante opciones de la barra de herramientas

Cada dashlet tiene una barra de herramientas que ofrece opciones para modificarlo. Los gráficos de visualización tienen los mismos ajustes de configuración, aunque algunos de los otros dashlets tienen distintos ajustes adicionales.

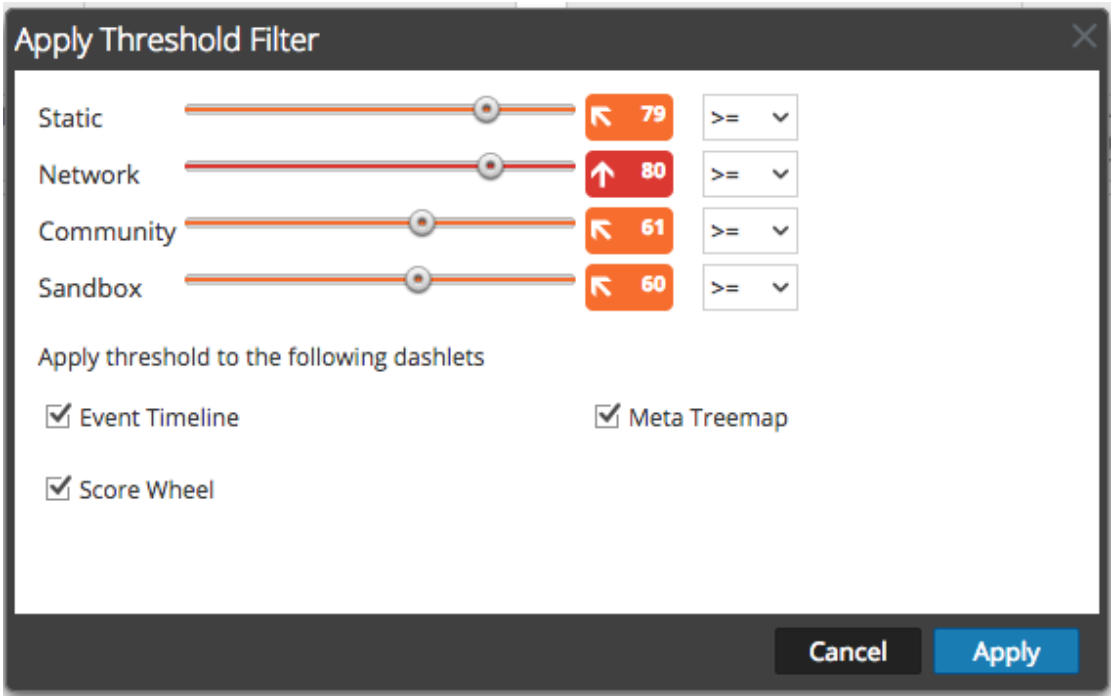
Para usar las opciones de la barra de herramientas:

- Para cerrar un dashlet de modo que solo se muestre la barra de título, haga clic en .
- Para abrir un dashlet que está cerrado, haga clic en .
- Para mostrar los ajustes configurables de un dashlet, haga clic en .
  Se muestra el cuadro de diálogo de configuración del dashlet.
- Para eliminar un dashlet, haga clic en .

Aplicar un filtro de umbral a múltiples dashlets

Dentro de los dashlets, puede configurar un umbral para mostrar únicamente eventos iguales a, por sobre o por debajo de cierto puntaje en las cuatro categorías (Estático, Red, Community y Sandbox). Este procedimiento configura los umbrales por tipo de dashlet para estos dashlets: Cronograma de evento, Rueda de puntaje y Mapa de árbol de metadatos. También puede configurar el umbral para dashlets individuales.

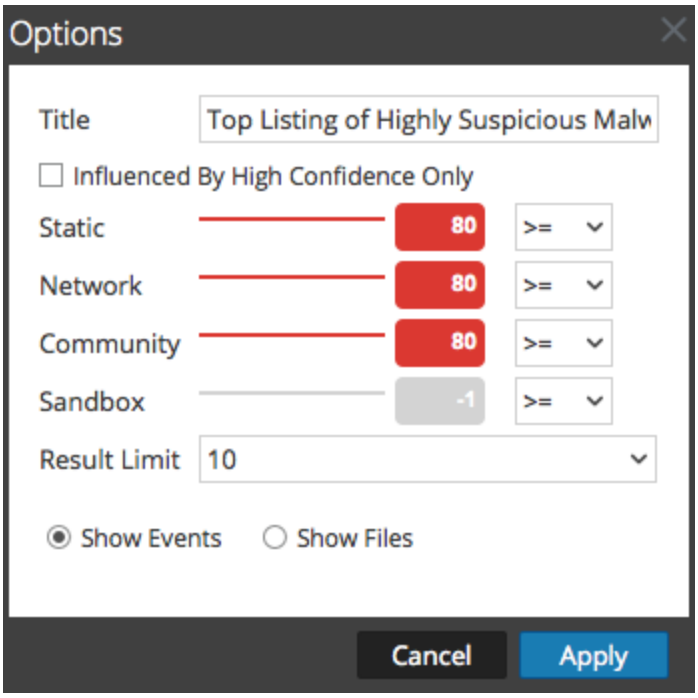
1. En la barra de herramientas, seleccione > **Aplicar filtro de umbral**.
   Se muestra el cuadro de diálogo Aplicar filtro de umbral.



2. Seleccione uno o más tipos de dashlets: Cronograma de evento, Rueda de puntaje y Mapa de árbol de metadatos.
3. Arrastre el control deslizante correspondiente o ingrese un valor numérico y, a continuación, seleccione un operador en la lista desplegable: =, >= o <=.
4. Haga clic en **Aplicar**.
   Los filtros de umbral se aplican a los tipos de dashlets seleccionados en el Resumen de eventos.

Establecer opciones de título y categoría para un dashlet

1. Para mostrar los ajustes configurables de un dashlet, haga clic en .
   Se muestra el cuadro de diálogo Opciones del dashlet.

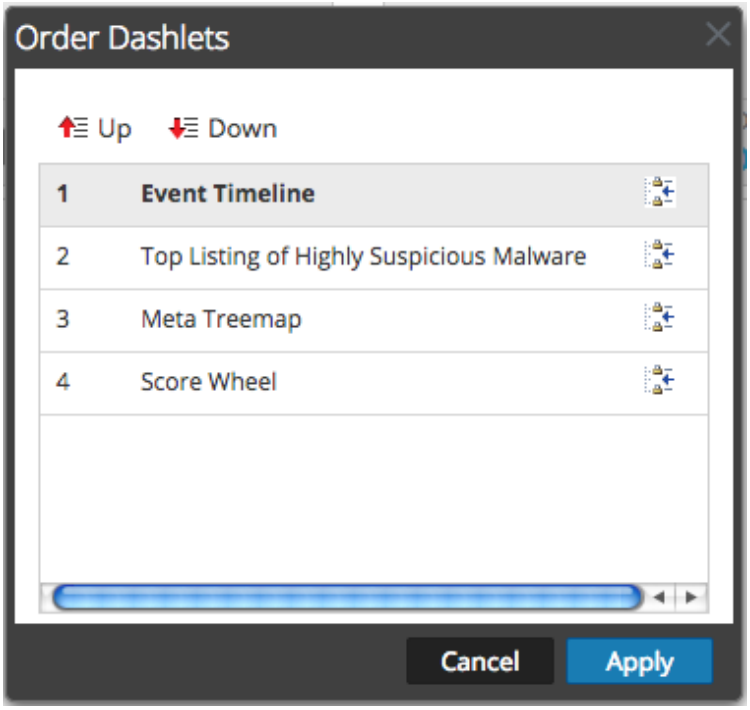


2. Escriba un nuevo título para el dashlet en el campo **Título**.
3. Si solo desea ver eventos con influencia de una etiqueta Alta confianza, lo cual significa que existe alta confianza de que el evento contiene código dañino, seleccione la opción **Solo con influencia de alta confianza**.
4. Si solo desea ver eventos que obtuvieron un puntaje por sobre determinado valor en las cuatro categorías (Estático, Red, Comunidad y Sandbox), arrastre el control deslizante correspondiente o ingrese un valor numérico y, a continuación, seleccione un operador en la lista desplegable: =, >= o <=.
5. Haga clic en **Aplicar**.
   El título y los filtros se aplican al dashlet.

Ordenar dashlets

Para cambiar el orden de los dashlets que aparecen debajo del Resumen de eventos:

1. En la barra de herramientas, seleccione > **Ordenar dashlets**.
   Se muestra el cuadro de diálogo Ordenar dashlets.



2. Seleccione un dashlet que desee subir o bajar y haga clic en Up o en Down.
3. Cuando esté conforme con el orden, haga clic en **Aplicar**.
   El cuadro de diálogo se cierra y el orden de los dashlets debajo del Resumen de eventos cambia de acuerdo con sus opciones.

Restaurar dashlets predeterminados

Cuando haya agregado, modificado y ordenado los dashlets, puede volver a la configuración predeterminada de presentación de los dashlets. Para restaurar los dashlets predeterminados:

1. En la barra de herramientas, seleccione > **Restaurar configuración predeterminada**.
   En un cuadro de diálogo se solicita confirmar la intención de restaurar la configuración.
2. Realice una de las siguientes acciones
   a. Si decide mantener el orden de los dashlets que configuró, haga clic en **No**.
   b. Si está seguro de que desea restaurar los valores predeterminados, haga clic en **Sí**.
      La presentación de los dashlets vuelve al valor predeterminado.

Configurar la vista Navegar y la vista Eventos

Los analistas pueden configurar las preferencias que afectan el rendimiento y el comportamiento de Security Analytics cuando se analizan datos en Investigation > vistas Navegar y Eventos.

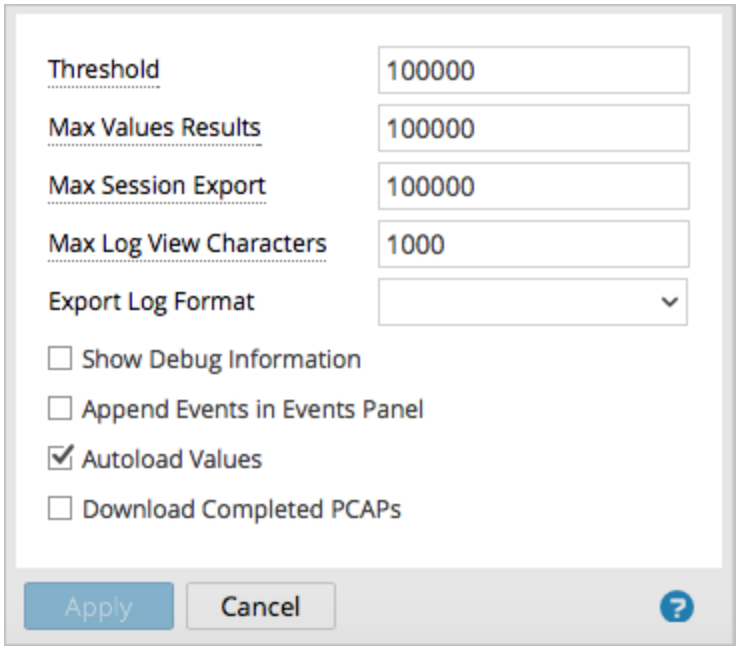
Estas configuraciones están disponibles en dos lugares de Security Analytics y los cambios realizados en cualquiera de las ubicaciones se aplican en la otra vista:

- Vista Investigation > cuadro de diálogo Ajustes de configuración y campo Buscar de la vista Navegar y de la vista Eventos.
- En Perfiles > panel Preferencias > pestaña Investigaciones.

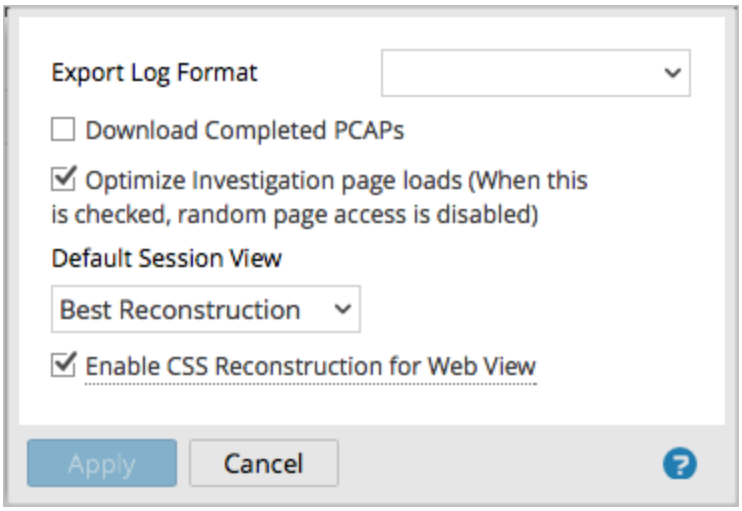
Acceder a la configuración de Investigation

Para acceder a la configuración, realice una de las siguientes acciones:

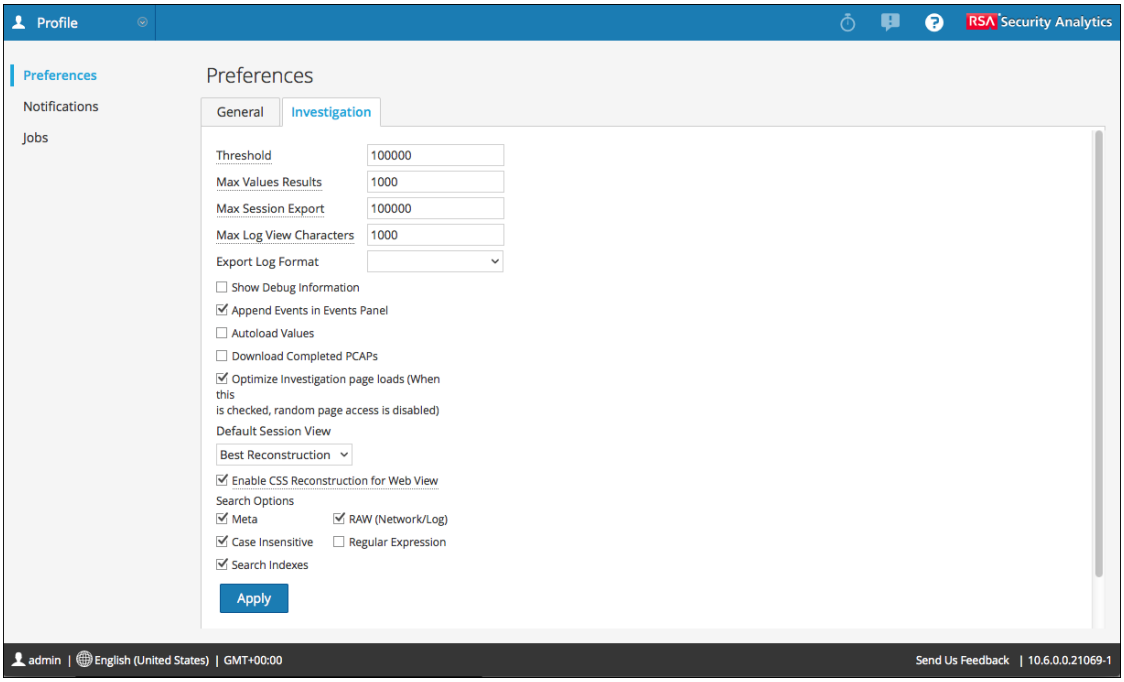
- En la barra de herramientas de la vista **Navegar**, seleccione la opción **Configuración**.
  Se muestra el cuadro de diálogo Configuración de la vista Navegar.



- En la barra de herramientas de la vista **Eventos**, seleccione la opción **Configuración**.
  Se muestra el cuadro de diálogo Configuración de la vista Eventos.



- En el menú de **Security Analytics**, seleccione **Perfil**. En el panel de **navegación izquierdo**, seleccione **Preferencias.** Haga clic en la pestaña **Investigaciones**.
  Se muestra la pestaña Investigation.



Calibrar los parámetros de carga de valor de la vista Navegar

Varios ajustes de Investigation influyen en el rendimiento de Security Analytics cuando se realiza la carga de valores en el panel Valores. Los valores predeterminados se configuran en función del uso común, y los analistas individuales pueden ajustar estas configuraciones para sus propias investigaciones.

Para ajustar estas configuraciones:

1. Navegue a la pestaña **Investigation** o al cuadro de diálogo **Configuración** de la vista Navegar.
2. Ajuste los siguientes parámetros:

- Umbral: Ajuste el umbral para la cantidad máxima de sesiones cargadas de un valor clave de metadatos en el panel Valores. Un umbral más alto permite conteos precisos de un valor y también produce tiempos de carga mayores. El valor predeterminado es **100000**.
- Número máximo de resultados de valores: Ajuste la cantidad máximo de valores para cargar en la vista Navegar cuando la opción Resultados máximos está seleccionada en el menú Clave de metadatos para una Clave de metadatos abierta. El valor predeterminado es **1,000**.
- Máximo de exportación de sesiones: Especifique la cantidad de eventos que se pueden exportar en una única PCAP o archivo de registro.
- Caracteres de vista de registro máximos: Configure el número máximo de caracteres que desea mostrar en **Investigation > Eventos > Texto del registro**. El valor predeterminado es **1,000**.
- Mostrar información de depuración: Si desea que Security Analytics muestre la cláusula `where` debajo de la ruta de navegación en la vista Navegar y el tiempo de carga transcurrido para cada servicio agregado en un Broker, seleccione esta opción. El valor predeterminado es **Desactivado**.
- Cargar valores automáticamente: Si desea que Security Analytics cargue valores automáticamente para el servicio seleccionado en la vista Navegar, seleccione esta opción. Cuando no está seleccionada, Security Analytics muestra un botón **Cargar valores**, el cual da la oportunidad de modificar las opciones. El valor predeterminado es **Desactivado**.

3. Haga clic en **Aplicar**.

Estos ajustes se aplican de inmediato y los podrá ver la próxima vez que cargue valores.

Configurar el comportamiento de descarga de PCAP en Investigation

Puede automatizar la descarga de las PCAP extraídas en el módulo Investigation a fin de que el navegador descargue la PCAP extraída y la abra en la aplicación predeterminada para abrir archivos PCAP, como por ejemplo Wireshark.

Para configurar esto:

1. Asegúrese de que el sistema de archivos local tenga instalada una aplicación para abrir PCAP y que la aplicación esté establecida como la predeterminada para manejar formatos de archivos PCAP.

2. Navegue a la pestaña **Investigation** o al cuadro de diálogo **Configuración** de la vista Navegar o la vista Eventos.
3. Seleccione la opción **Descargar PCAP finalizadas**.
4. Haga clic en **Aplicar**.
   La configuración se aplica de inmediato.

Configurar el formato predeterminado de exportación de registros en Investigation

Puede exportar registros de Investigation en diferentes formatos. Las opciones disponibles son Texto, XML, CSV, JSON. No hay valor predeterminado incorporado para el formato de exportación de registro. Si no selecciona un formato aquí, Security Analytics muestra un cuadro de diálogo de selección cuando invoca la exportación de registros.

Para seleccionar el formato de los registros exportados:

1. Navegue a la pestaña **Investigation** o al cuadro de diálogo **Configuración** de la vista Navegar.
2. Seleccione una de las opciones del menú desplegable **Formato de registro de exportación**.
3. Haga clic en **Aplicar**.
   El ajuste se aplica de inmediato.

Calibrar la recuperación de la vista Eventos y la reconstrucción predeterminada

Puede configurar varios parámetros que controlan la manera en que Security Analytics recupera y reconstruye eventos en la vista Eventos. Para esto:

1. Navegue a la pestaña **Investigation** o al cuadro de diálogo **Configuración** de la vista Eventos.
2. Configure los siguientes parámetros.

Optimizar las cargas de páginas de Investigation	Establezca una opción de paginación. Cuando está optimizada, los resultados se devuelven lo más rápidamente posible, pero se renuncia a la capacidad original de ir a una página específica de la lista de eventos. La deselección de esta casilla cambia la paginación en la Lista de eventos y permite ir a una página específica de la lista (o a la última página). El valor predeterminado es **habilitado**.

Agregar eventos en el panel de eventos	Cuando se selecciona esta opción, los eventos que se muestran en el **Panel de eventos** se agregan de manera incremental. Por ejemplo, cada vez que hace clic en el ícono de la página siguiente, se agrega el siguiente incremento de eventos; en primer lugar, verá 1 a 25, a continuación, 1 a 50, después, 1 a 75 y así sucesivamente. **Nota:** Esta opción está disponible solo si la opción Optimizar cargas de la página Investigation está habilitada.
Vista de sesión predeterminada	Selecciona el tipo de reconstrucción predeterminado para la reconstrucción inicial en la vista Eventos. El valor predeterminado es **Mejor reconstrucción**, con el cual los eventos se reconstruyen mediante el método de reconstrucción más apropiado para el evento.

3. Para activar los cambios de inmediato, haga clic en **Aplicar**.

Habilitar o inhabilitar la generación de hojas de estilo en cascada en reconstrucciones de contenido web

Los analistas pueden habilitar el uso de hojas de estilo en cascada (CSS) cuando reconstruyen contenido web. Si está habilitada, la reconstrucción web incluye imágenes y estilos de hoja de estilo en cascada (CSS), de modo que su aspecto coincide con la vista original en un navegador web. Esto incluye el escaneo y la reconstrucción de eventos relacionados y la búsqueda de hojas de estilo e imágenes que se usan en el evento objetivo. Esta opción está habilitada de manera predeterminada. Deshabilítela si hay problemas para ver sitios web específicos.

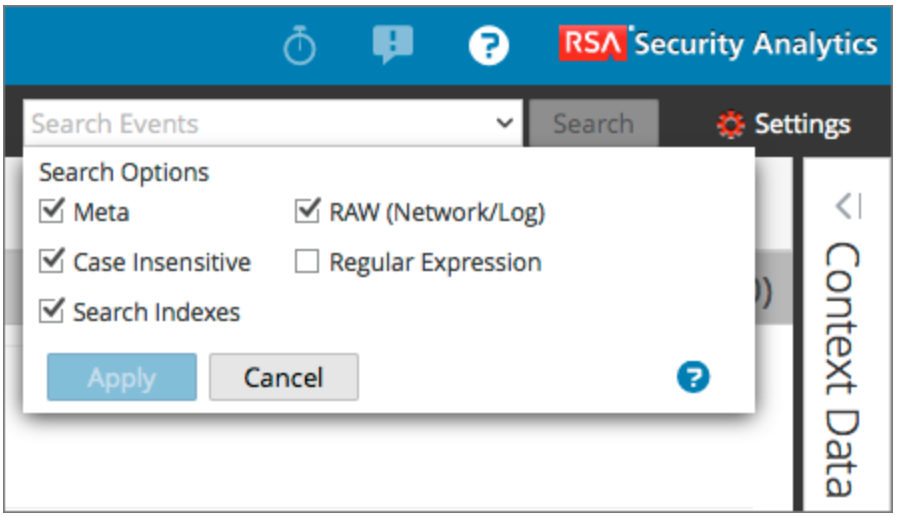
Nota: Es posible que el aspecto del contenido reconstruido no coincida perfectamente con la página web original si no se pudo encontrar imágenes y hojas de estilo relacionadas o si estas se cargaron desde la caché del navegador web. Además, el diseño o el estilo que se ejecuta dinámicamente a través de JavaScript en el lado del cliente no se generarán en la reconstrucción debido a que todo el JavaScript del lado de cliente se elimina por motivos de seguridad.

Para habilitar o inhabilitar esta opción:

1. Navegue a la pestaña **Investigation**.
2. Haga clic en la casilla de verificación **Habilitar reconstrucción de CSS para vista web**.
3. Haga clic en **Aplicar**.
   La configuración se aplica de inmediato y se puede ver en la siguiente reconstrucción de contenido web.

(Opcional) Configurar opciones de búsqueda

1. Haga clic en el campo **Buscar** para mostrar el menú desplegable Buscar eventos.



2. Seleccione una o más opciones de búsqueda que desee aplicar a la búsqueda. Investigation: Opciones de búsqueda ofrece información detallada sobre cada opción.
3. Para guardar la configuración de la búsqueda, haga clic en **Aplicar**.
   Las preferencias se guardan y se aplican de inmediato.

Realizar una investigación

Puede comenzar una investigación de varias maneras en Security Analytics. Una vez que se inicia una investigación, no hay un orden específico en el cual se deba desarrollar. En cambio, Security Analytics ofrece varios métodos para mostrar, filtrar y consultar los datos, actuar conforme a un punto de desglose y examinar eventos específicos.

- Las cuentas de usuario de los analistas que realizan análisis mediante Security Analytics Investigation deben tener configuradas las funciones y los permisos correspondientes del sistema. Consulte Funciones y permisos para los analistas. Un administrador debe configurar las funciones y los permisos.

  Los procedimientos detallados son los siguientes:

  Comenzar una investigación de un servicio o una recopilación

  Filtrar información en la vista Navegar

  Consultar datos en la vista Navegar

  Actuar conforme a un punto de desglose en la vista Navegar

  Examinar eventos

Comenzar una investigación de un servicio o una recopilación

Los analistas pueden comenzar una investigación de datos en un servicio o una recopilación de Security Analytics, lo cual da lugar a la carga de valores.

Para comenzar una investigación en Security Analytics, se debe especificar un servicio.

- Security Analytics abre la vista Navegar con el servicio predeterminado especificado por el usuario seleccionado.
- Si actualmente no se ha especificado ningún servicio predeterminado y el ID del servicio no se encuentra en la URL, Security Analytics presenta un cuadro de diálogo que permite seleccionar el servicio o la recopilación que se investigarán.
- Cuando un servicio se seleccionó de forma manual o predeterminada en la vista Navegar, puede cambiar el servicio o la recopilación que se investigará mediante la selección del nombre del servicio en la barra de herramientas. Security Analytics presenta el cuadro de diálogo para seleccionar el servicio que se investigará.

Nota: El servicio Archiver no aparece en la vista Navegar para minimizar la experiencia del usuario de bajo rendimiento cuando se realizan investigaciones. Archiver está disponible en la vista Eventos para exportaciones de registros y mejora de funcionalidades de búsqueda.

Con un servicio o una recopilación seleccionados, Security Analytics está listo para cargar datos para el servicio o la recopilación. Varios ajustes en el cuadro de diálogo Configuración de la vista Navegar y de la vista Eventos o en Perfiles > panel Preferencias > pestaña Investigaciones afectan el proceso de carga: Umbral, Número máximo de resultados de valores, Mostrar información de depuración, Cargar valores automáticamente y Optimizar cargas de la página Investigation (consulte Configurar las vistas y las preferencias de Investigation).

Nota: Si especificó Cargar valores automáticamente, Security Analytics completa los datos de forma automática. De lo contrario, debe seleccionar el botón Cargar. Security Analytics completa los metadatos en el panel Valores de la vista Navegar y los resultados se pueden ver casi de inmediato.

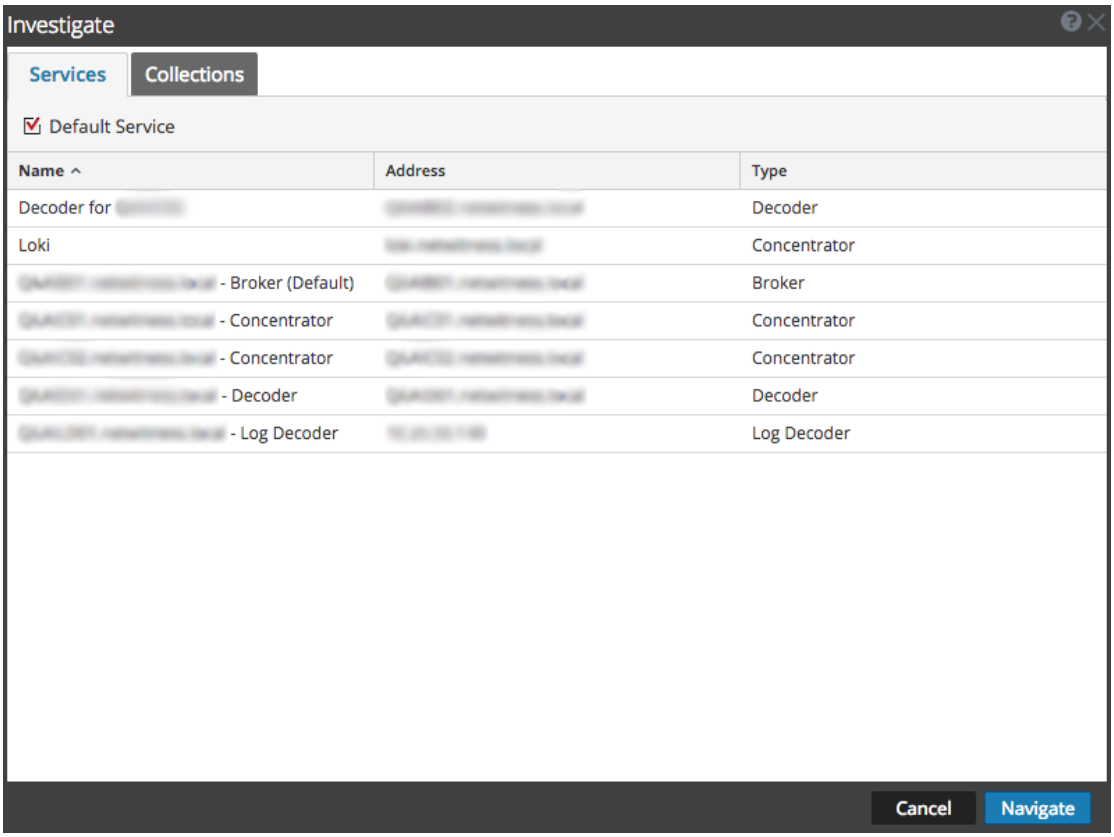
En el resto de este tema se proporcionan instrucciones para comenzar la investigación de datos de un servicio.

Nota: Solo los usuarios a los cuales se asignó la función de administrador pueden crear una recopilación y solo el creador de la recopilación puede investigarla.

Procedimientos

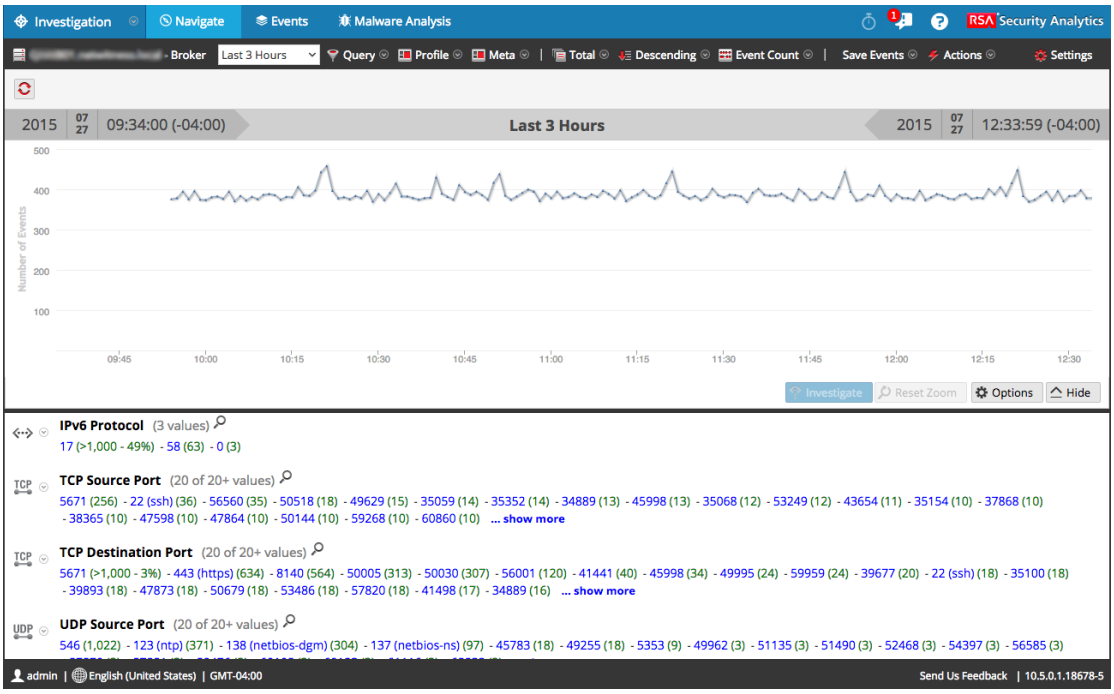
Comenzar una investigación (sin servicio predeterminado)

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar**.
   Se muestra el cuadro de diálogo Investigar.



2. Haga doble clic en un servicio o seleccione uno y haga clic en **Navegar**.
   El panel resultante muestra la actividad del servicio seleccionado.
3. Si desea modificar opciones de la investigación antes de realizar la carga, puede crear o modificar un perfil personalizado, aplicar otro rango de tiempo, crear o aplicar un grupo de metadatos y realizar una consulta personalizada, como se describe en Filtrar información en la vista Navegar.
4. Cuando esté listo, haga clic en 

   .
   Comienza la carga de los datos del servicio seleccionado.

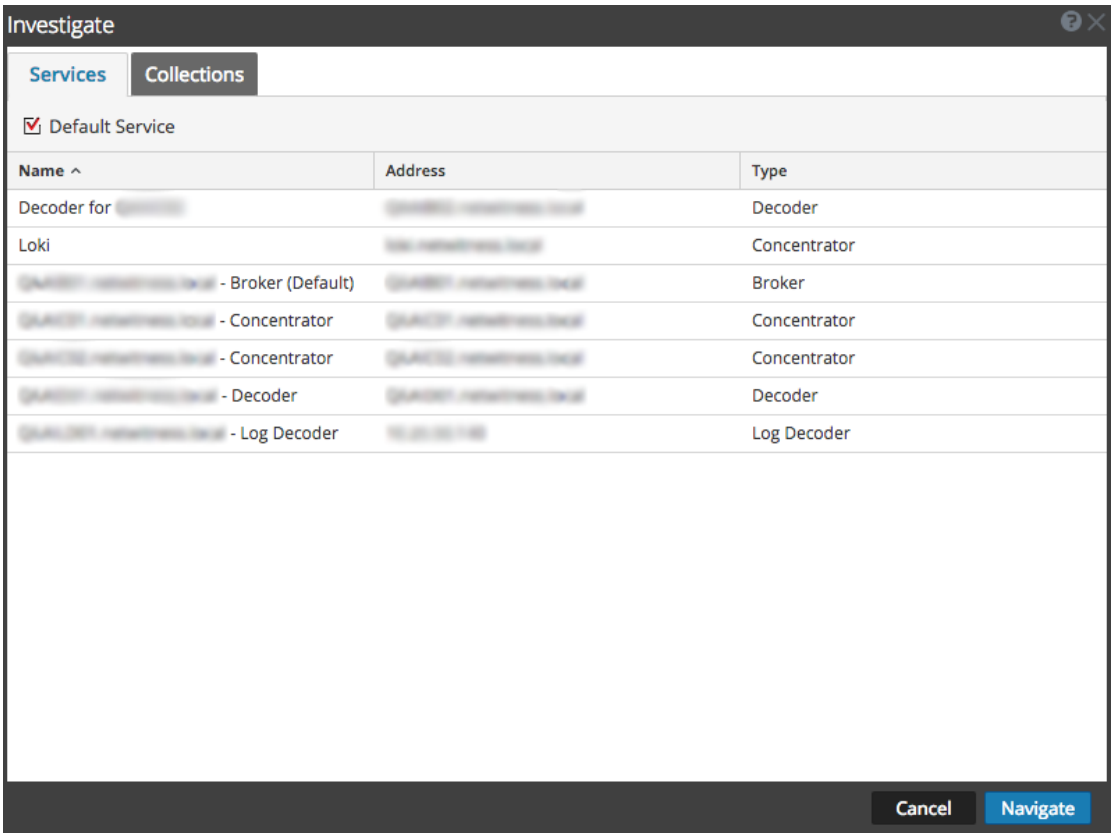


Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos.

Configurar o borrar el servicio predeterminado

Puede configurar o borrar el servicio predeterminado en el cuadro de diálogo Investigar un servicio.

1. Haga clic en el nombre del servicio en la barra de herramientas.
   Se muestra el cuadro de diálogo Investigar.



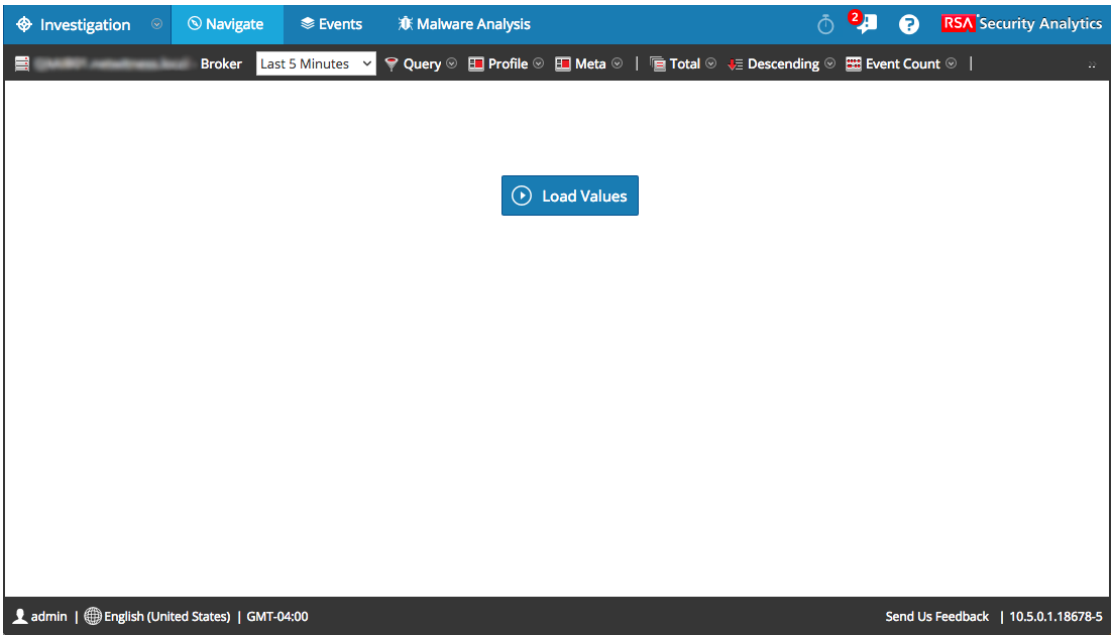
2. Seleccione un servicio en la cuadrícula **Servicios** y haga clic en Default Service.
   El servicio se convierte en el valor predeterminado (lo indica **Predeterminado** entre paréntesis después del nombre del servicio).
3. Para borrar el servicio predeterminado, selecciónelo en la cuadrícula y haga clic en Default Service y, a continuación, haga clic en **Cancelar** para cerrar el cuadro de diálogo.
   No se configura un servicio predeterminado.

> **Nota:** El botón Cancelar no cancela la selección del servicio predeterminado. Simplemente cierra el cuadro de diálogo sin tener que navegar al servicio seleccionado actualmente en la cuadrícula. La configuración de un servicio predeterminado que es diferente del servicio que se investiga en la actualidad, no actualiza la vista Navegar. Debe seleccionar explícitamente y navegar a un servicio diferente.

Comenzar una investigación (se especifica el servicio predeterminado)

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar**.
   Si el ajuste de Cargar valores automáticamente está desactivado, la vista Navegar se muestra con el servicio predeterminado seleccionado y listo para cargar datos. Si el ajuste

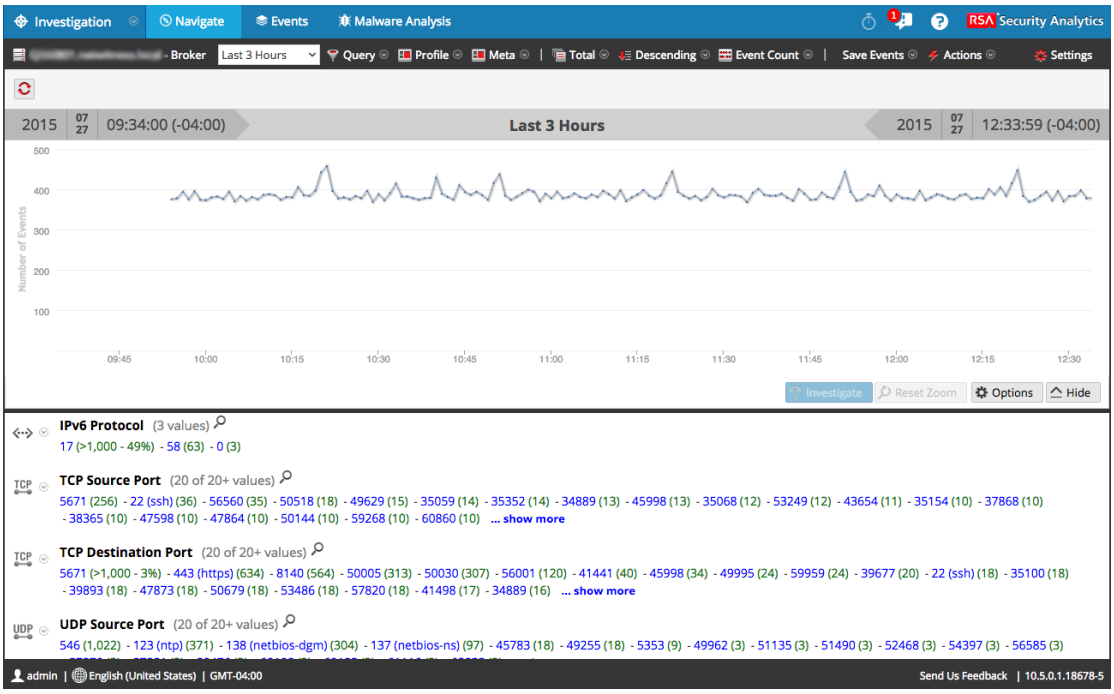
Cargar valores automáticamente está activado, se cargan los valores, como se muestra en el paso 3.



2. Si desea modificar opciones de la investigación antes de realizar la carga, puede crear o modificar un perfil personalizado, aplicar otro rango de tiempo, crear o aplicar un grupo de metadatos y realizar una consulta personalizada.
3. Cuando esté listo, haga clic en 

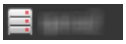
.

   Los valores del servicio se cargan de acuerdo con las opciones seleccionadas.

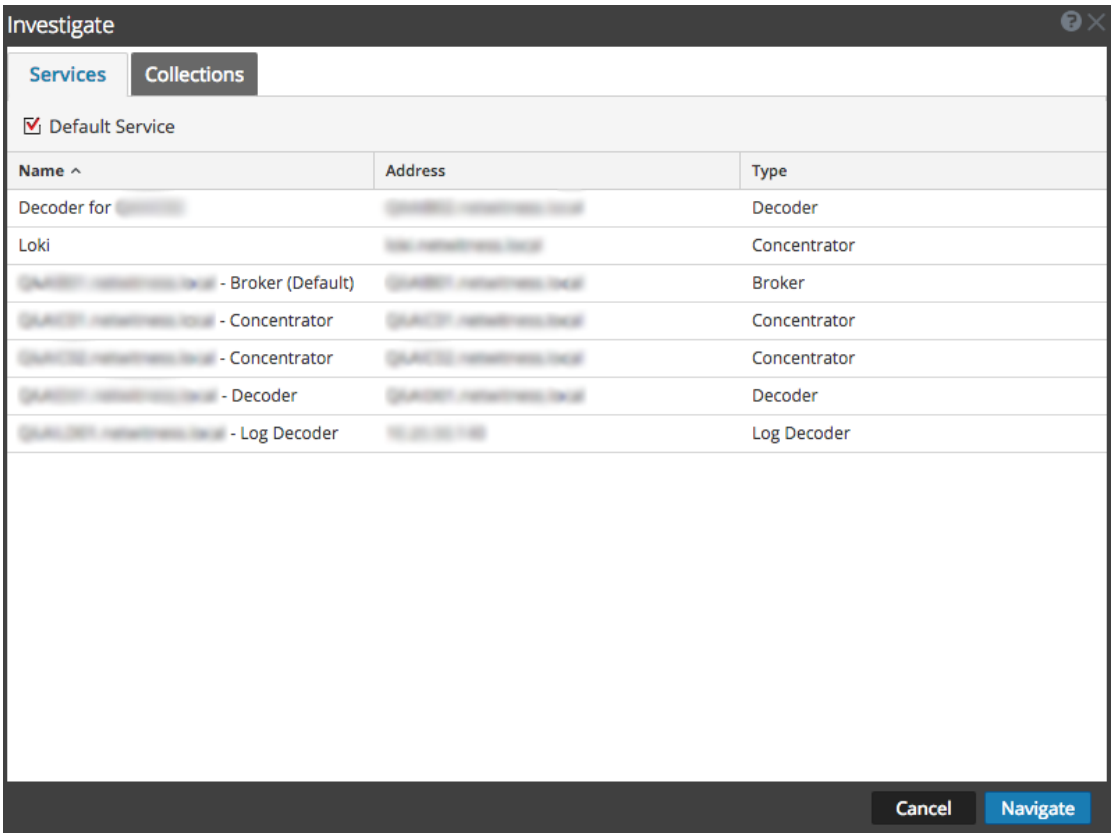


Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos.

Cambiar el servicio o la recopilación que se investigará

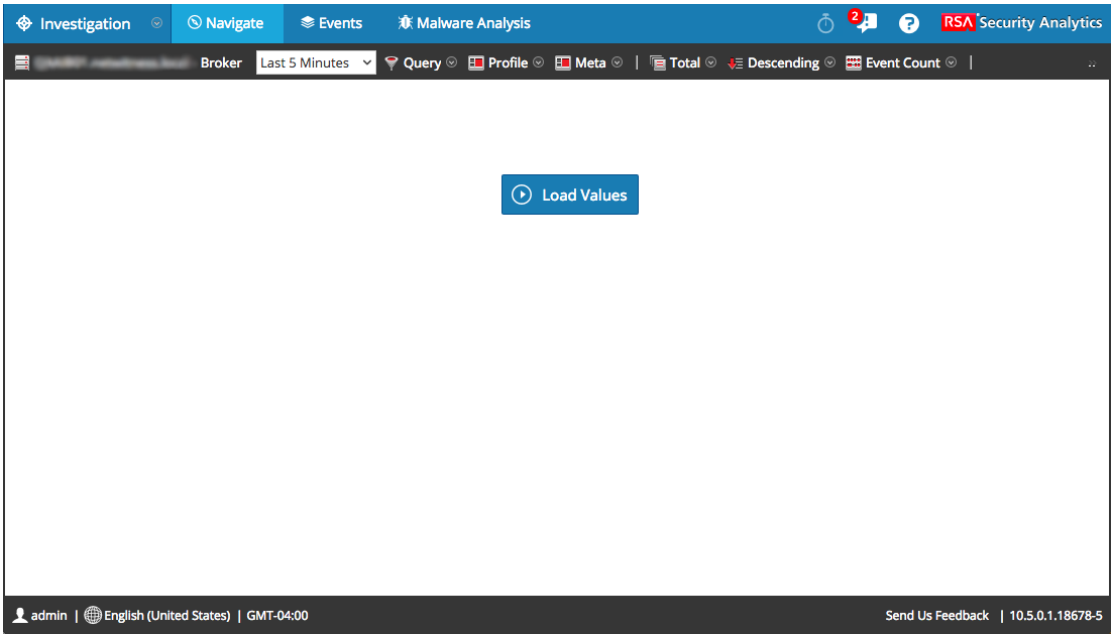
1. En la vista Navegar, haga clic en  (el nombre del servicio) en la parte superior del panel de opciones.

   Se muestra el cuadro de diálogo Investigar.



2. Haga doble clic en un servicio o seleccione uno y haga clic en **Navegar**. El panel resultante muestra la actividad del servicio seleccionado.

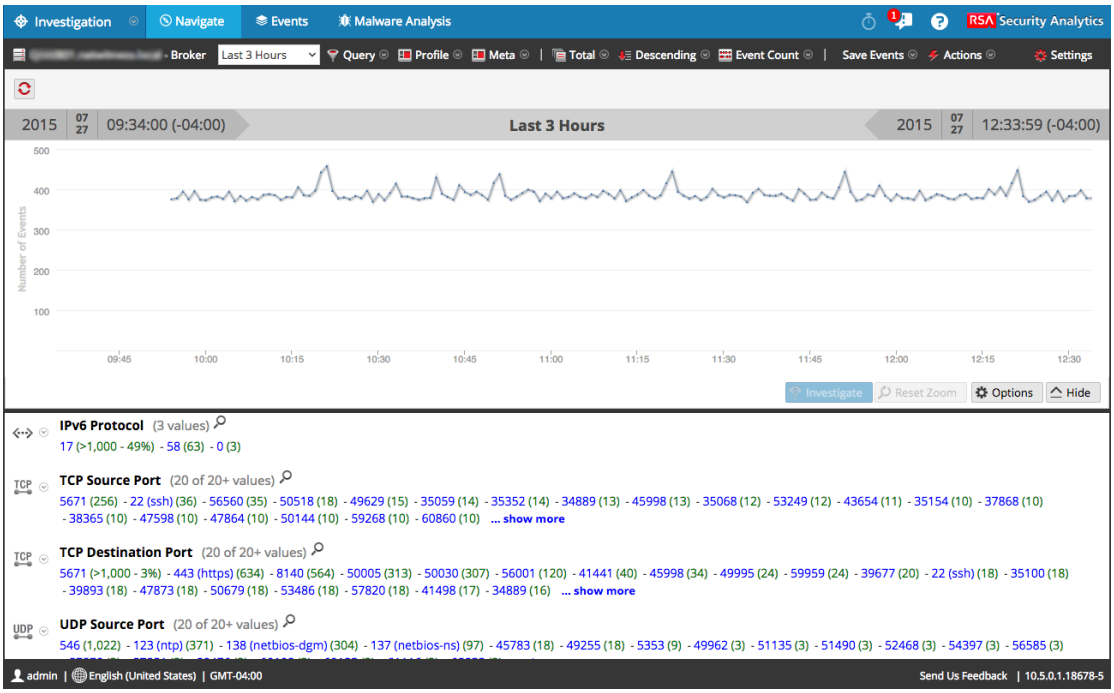
   Si el ajuste Cargar valores automáticamente está activado, se cargan los valores, como se muestra en el paso 3. De lo contrario, se muestra la vista Navegar con el servicio predeterminado seleccionado y los datos listos para cargarse.



3. Cuando esté listo, haga clic en 

.

Los valores del servicio comienzan a cargarse de acuerdo con las opciones seleccionadas.



Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos.

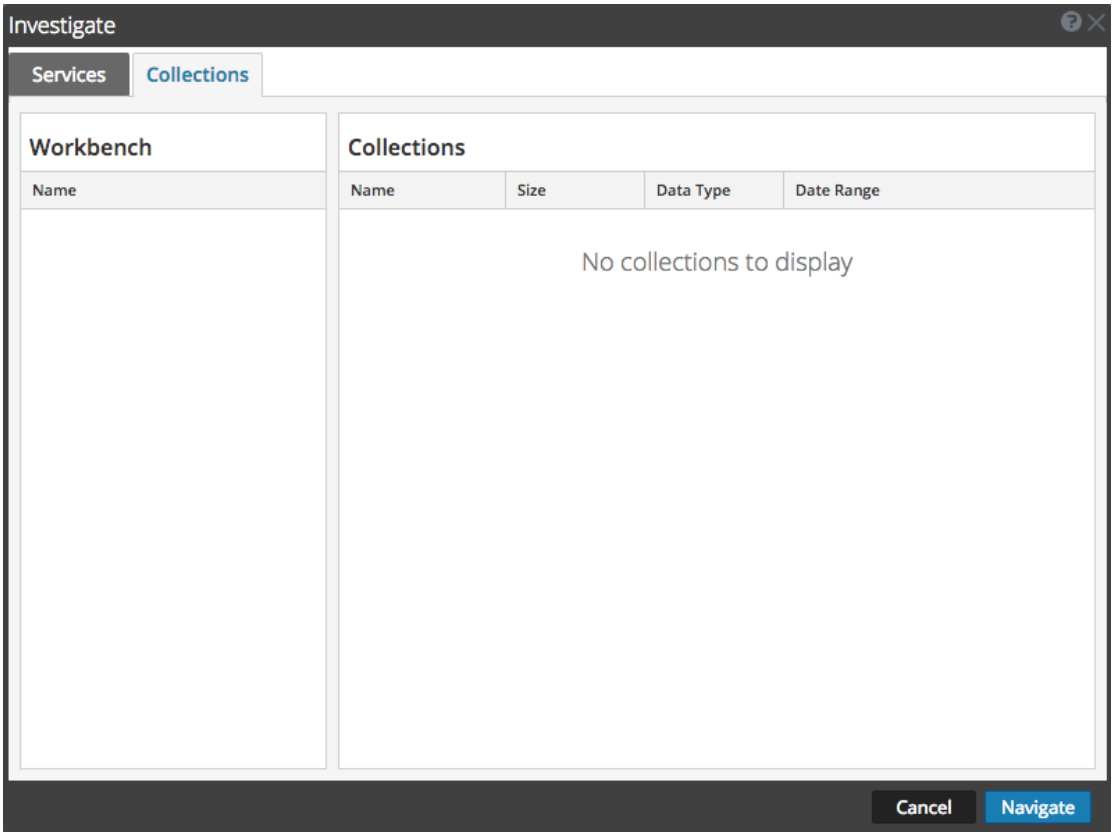
Investigar recopilaciones de restauración de Workbench

Este procedimiento permite que los administradores seleccionen contenido de una recopilación existente que se volverá a procesar para realizar una investigación más detallada.

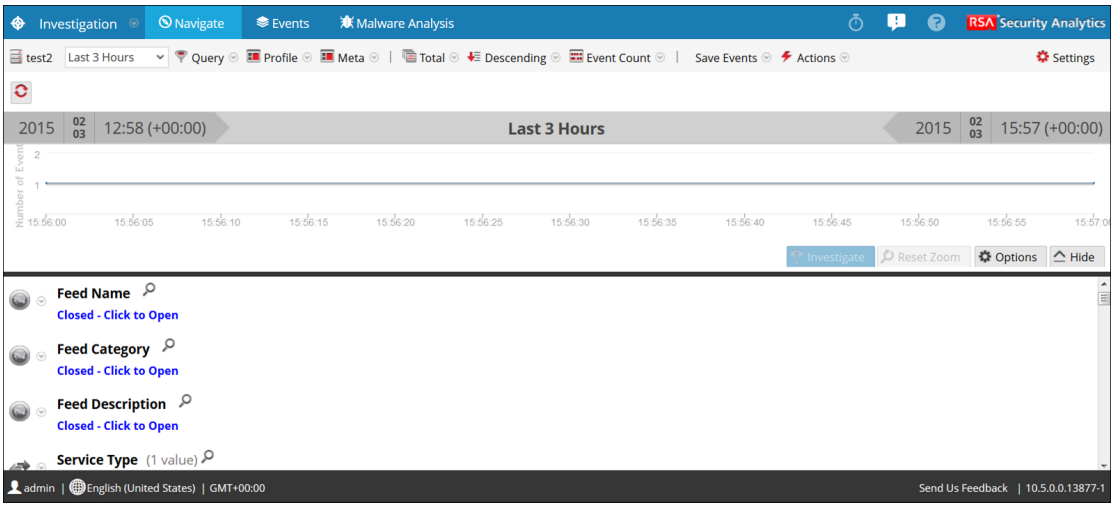
Nota: Solo un usuario con privilegios administrativos puede crear una recopilación y usted solo puede ver las recopilaciones que creó.

Para volver a procesar los datos con el fin de realizar una investigación más detallada:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar**.
   Se muestra el cuadro de diálogo Investigar.



2. Seleccione un servicio de Workbench y un nombre de Workbench que desee investigar.
3. Haga clic en **Navegar** para realizar una investigación sobre el servicio de Workbench que seleccionó.
   Haga clic en **Cancelar** para seleccionar otro servicio de Workbench que se investigará.
   Se muestra la vista Investigación.



Con la recopilación seleccionada y los datos cargados, está listo para comenzar a analizar los datos.

Filtrar información en la vista Navegar

En este tema se describen los métodos disponibles para filtrar resultados en la vista Investigation > Navegar.

Cuando se realiza una investigación en Security Analytics, están disponibles varios métodos para refinar los resultados que se muestran cuando se cargan valores de claves de metadatos en la vista Navegar. Los analistas pueden:

- Establecer el rango de tiempo para una investigación
- Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos.
- Administrar y aplicar claves de metadatos predeterminadas en una investigación.
- Administrar grupos de metadatos definidos por el usuario
- Visualizar metadatos como coordenadas paralelas
- Usar perfiles de Investigation para encapsular vistas personalizadas.

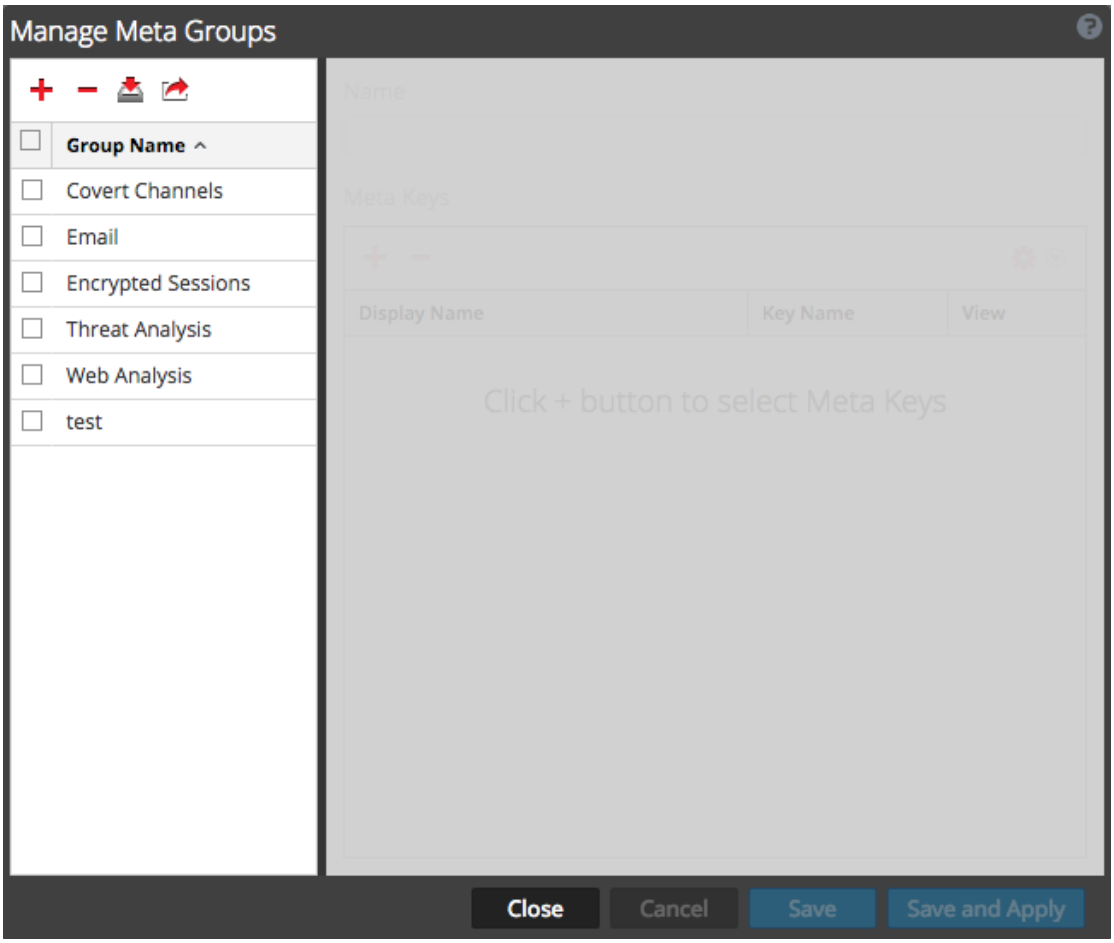
Administrar grupos de metadatos definidos por el usuario

En la vista Investigation > Navegar, puede definir grupos de metadatos para filtrar los datos que se muestran en una investigación. En esta sección se describe cómo agregar, editar, importar, exportar y eliminar los grupos de metadatos personalizados que se utilizarán durante la navegación en un servicio específico. En una visualización de coordenadas paralelas, las claves de metadatos en un grupo aparecen como ejes de izquierda a derecha. Los grupos de metadatos personalizados están visibles para todos los usuarios de un servicio y se pueden exportar para importarlos en cualquier servicio, con la limitación de las claves de metadatos disponibles para ese servicio.

Nota: cuando un administrador agrega manualmente grupos de metadatos personalizados mediante la edición del archivo de índice personalizado para un servicio, los grupos nuevos quedan disponibles para Investigation después del reinicio del servicio.

Crear un grupo de metadatos y agregar claves de metadatos

1. Mientras investiga un servicio en la vista **Investigation > Navegar**, seleccione **Metadatos > Administrar grupos de metadatos** en la barra de herramientas.
   Se muestra el cuadro de diálogo Administrar grupos de metadatos. Inicialmente no hay ningún grupo configurado para un servicio. Si ya se configuraron grupos, estos se enumeran bajo Nombre del grupo.

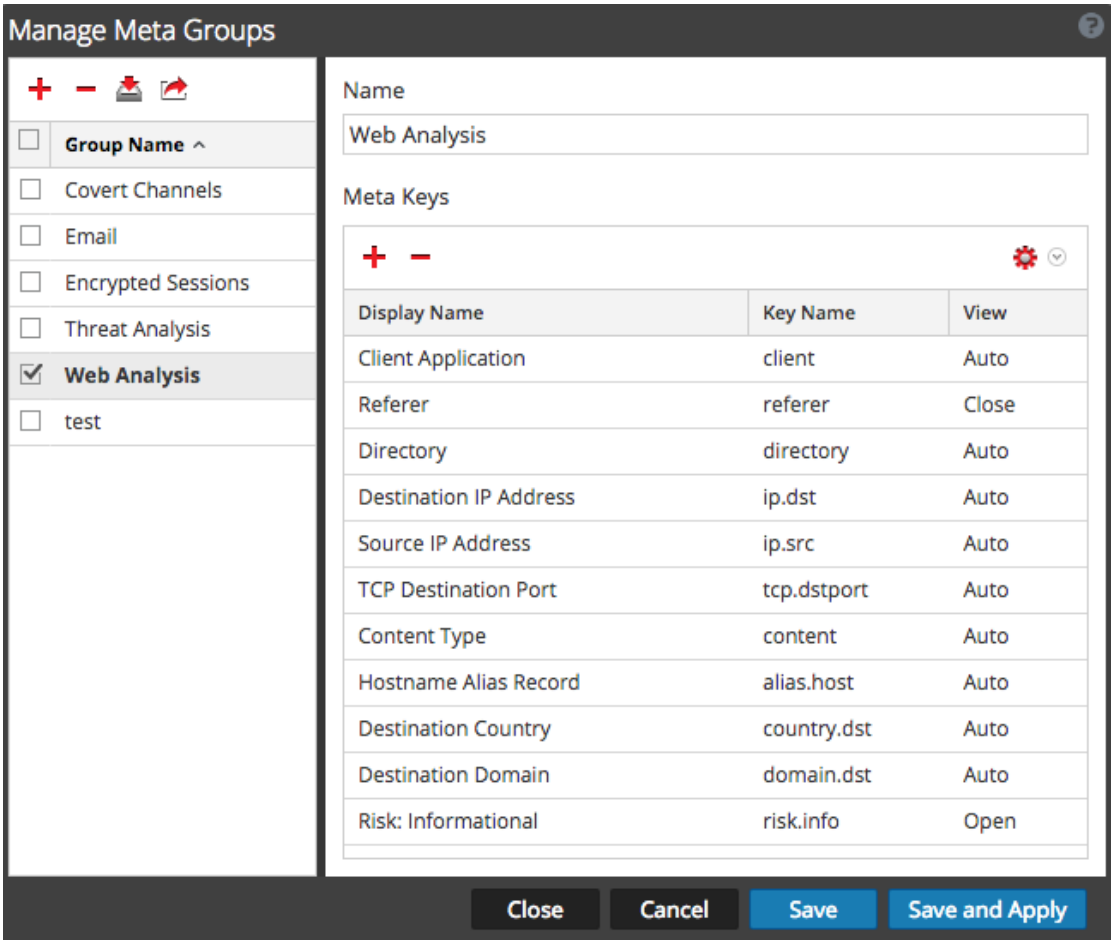


2. En la barra de herramientas de la cuadrícula, haga clic en +.

   Se inserta una nueva fila en la parte superior de la cuadrícula Grupos de metadatos.

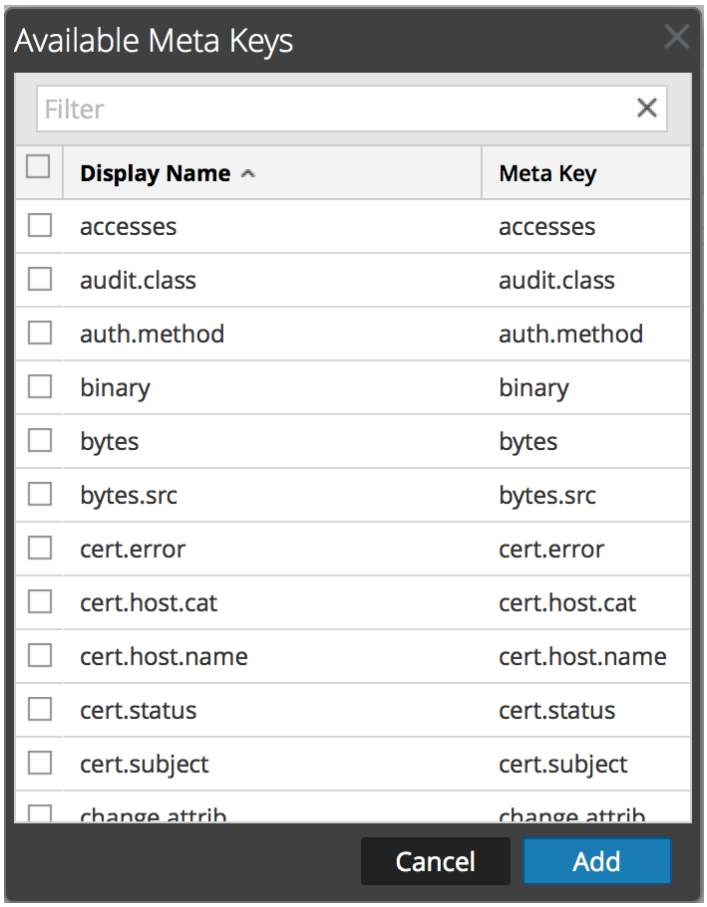
3. Escriba un nombre para el nuevo grupo de metadatos y presione **Intro**.

   El formulario de la derecha se abre para edición.



4. (Opcional) Si desea cambiar el nombre del grupo de metadatos, escriba un nuevo valor en el campo **Nombre** .
5. En la barra de herramientas **Claves de metadatos**, haga clic en +.

   Se muestra el cuadro de diálogo Claves de metadatos disponibles con las claves en orden alfabético.



6. Para filtrar la lista de claves de metadatos, escriba una palabra o una frase en el campo **Filtrar** y seleccione **Intro**.
   La lista muestra claves de metadatos coincidentes de acuerdo con una búsqueda que no distingue mayúsculas de minúsculas. Elimine el texto del filtro y presione **Intro** para extraer el filtro.
7. Para seleccionar claves de metadatos para incluir en el grupo de metadatos, haga clic en las casillas de verificación. Para seleccionar todas las claves de metadatos, haga clic en la casilla de verificación en la barra de título y luego en **Agregar**.
   Las claves de metadatos seleccionadas se agregan a la lista Claves de metadatos.
8. (Opcional) Si desea cambiar el orden en que las claves de metadatos se cargan y enumeran en una investigación, haga clic y arrastre una o más claves de metadatos a una nueva posición.
9. Para terminar de crear el grupo de metadatos, realice una de estas acciones:
   a. Para guardar el grupo de metadatos, haga clic en **Guardar**.
      Se crea el grupo y está disponible para utilizar.

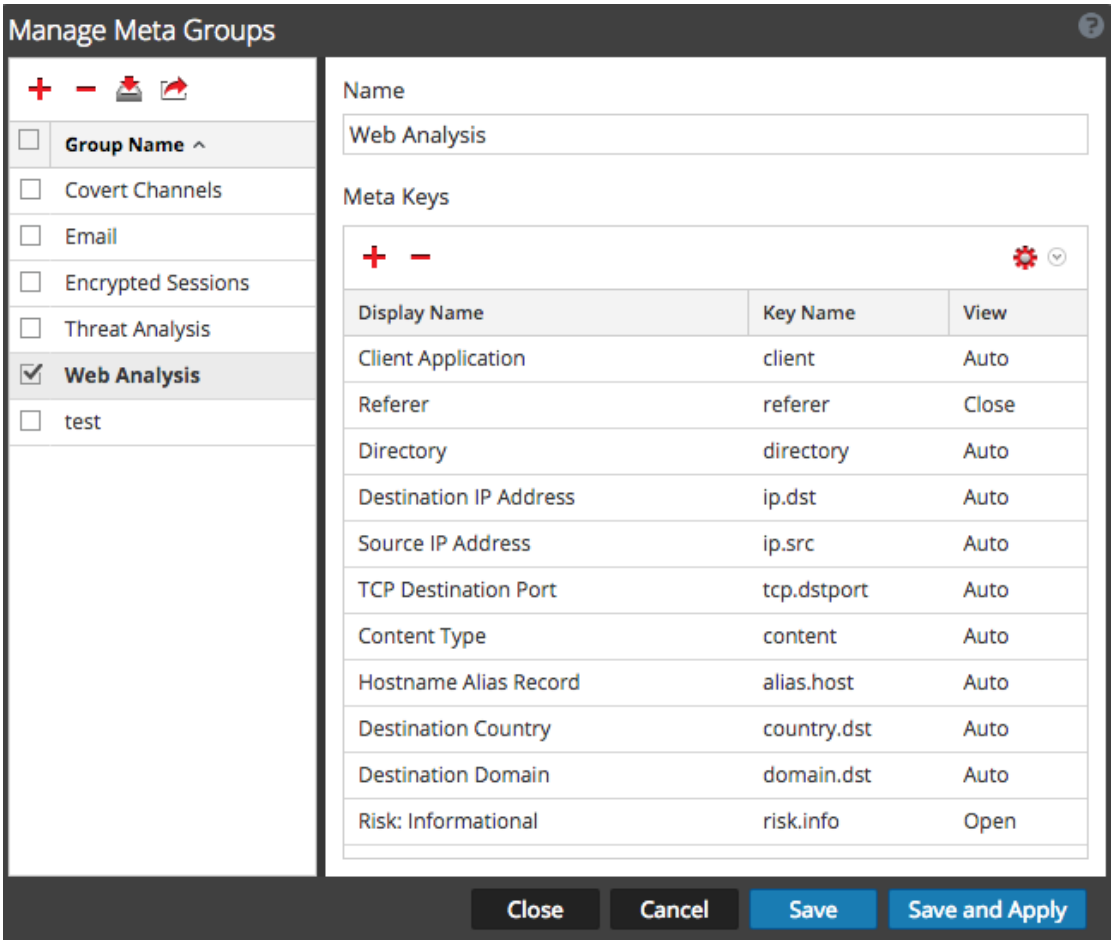
b. Para guardar y aplicar el grupo de metadatos a la vista Investigation actual, haga clic en **Guardar y aplicar**.

El grupo se crea y se aplica de inmediato a la vista Investigation actual.

10. Haga clic en **Close**.

Editar un grupo de metadatos

1. Seleccione un grupo en la cuadrícula **Grupos de metadatos**.
   El formulario de la derecha se abre para edición.



2. (Opcional) Editar el nombre del grupo.
3. (Opcional) Agregar nuevas claves de metadatos, como se describe más arriba en Crear un grupo de metadatos y agregar claves de metadatos.
4. (Opcional) Para establecer el orden de las claves, arrastre y suelte una o más claves.
5. (Opcional) Para cambiar la vista inicial de una clave de metadatos, haga clic en y seleccione una de las posibles vistas.
   Cuando modifica el grupo de metadatos, no puede establecer la clave en ABIERTO. Si cambia a ABIERTO la vista predeterminada para un grupo de claves de metadatos y algunas de las claves de metadatos no están indexadas, estas claves vuelven a AUTOMÁTICO. En consecuencia, la clave de metadatos se carga automáticamente solo si está indexada, y las

claves de metadatos no indexadas se CIERRAN hasta que se abren de forma manual.
El valor de la vista inicial se muestra en la columna Vista.

6. Para guardar los cambios, haga clic en **Guardar**.
7. Para aplicar los cambios a la actual vista Navegación, haga clic en **Guardar y aplicar**.

Eliminar un grupo de metadatos

1. En la cuadrícula **Grupos de metadatos**, seleccione el grupo de que desea eliminar.
2. Haga clic en .
   Un cuadro de diálogo de confirmación brinda la oportunidad para cancelar o finalizar la solicitud.
3. Haga clic en **Aceptar**.
   Se elimina el grupo de metadatos. Cuando cierra la ventana, si el grupo eliminado era el grupo de metadatos que se aplicaba actualmente, se elimina y las claves de metadatos predeterminadas se utilizan para crear la vista.

Exportar un grupo de metadatos

Los grupos de metadatos definidos por el usuario se crean en servicios individuales. Para que los grupos de metadatos estén disponibles para otro servicio, debe exportarlos a su sistema de archivos local. Para exportar uno o más grupos de metadatos:

1. En la cuadrícula **Grupos de metadatos**, seleccione uno o más grupos para exportar.
2. Haga clic en  .
   Los grupos seleccionados se descargan en el sistema local de archivos como **archivo MetaGroups.jsn**. Todas las descargas de grupos de metadatos tienen el mismo nombre con un número anexado para evitar sobrescribir las descargas anteriores.

Importar un grupo de metadatos

Para hacer que los grupos de metadatos definidos por el usuario desde otro servicio estén disponibles para el servicio que se investiga actualmente, debe importar el **archivo MetaGroups.jsn** desde el sistema de archivos local. Para importar grupos de metadatos:

1. En la cuadrícula **Grupos de metadatos**, seleccione un archivo para exportar y haga clic en  .
   Se muestra el cuadro de diálogo de selección.

2. Haga clic en **Navegar** y navegue al directorio del sistema local de archivos donde se almacenan los archivos MetaGroups.jsn descargados. Seleccione un archivo y haga clic en **Abrir**.
   El nombre de archivo se muestra en el campo Cargar archivo.
3. Haga clic en **Cargar**.
   El proceso de carga comienza y un mensaje indica que la carga se ha realizado correctamente. Los grupos de metadatos se agregan a la cuadrícula Grupo de metadatos. Si el archivo es un duplicado de un grupo de metadatos existente, un cuadro de diálogo le indica que ya existe el grupo de metadatos.

Administrar y aplicar claves de metadatos predeterminadas en una investigación

Cuando los analistas realizan una investigación de datos capturados en Investigation, se carga un conjunto de claves de metadatos predeterminado, el cual se muestra en una secuencia predeterminada en la vista Navegar > panel Valores. La secuencia y el contenido predeterminados se basan en las claves de metadatos del servicio que se investiga. Los analistas pueden especificar las claves de metadatos para mostrar durante la navegación mediante la selección de las claves de metadatos predeterminadas o de un grupo de claves de metadatos definido por el usuario, que proporciona una gran flexibilidad para definir claves de metadatos. Esto puede ayudar a desglosar más directamente los datos deseados y reducir el tiempo de carga mediante la prevención de la carga de metadatos que no es de interés en la investigación actual.

Si ningún grupo de metadatos personalizado está vigente, la vista Navegar se muestra con la visibilidad de claves de metadatos especificada en el cuadro de diálogo Claves de metadatos predeterminadas. Para optimizar la carga de claves de metadatos en la vista Navegar > panel Valores, Security Analytics no abre claves de metadatos no indexadas de forma predeterminada. Cuando abre una clave de metadatos no indexada en la vista Valores, Security Analytics comienza a cargar valores para esa clave de metadatos. Si el tiempo de carga es excesivo, el tiempo de espera de la carga de las claves de metadatos se agota con un mensaje. El título, los valores y los conteos de las claves de metadatos no indexadas no se pueden desglosar en el panel Valores. El etiquetado adicional en Investigation identifica las claves de metadatos no indexadas, que también estaban presentes en versiones anteriores.

Para seleccionar las claves de metadatos a aplicar en su investigación, puede:

- Seleccionar las claves de metadatos predeterminadas.
- Seleccione un conjunto de claves de metadatos definido por el usuario, denominado grupo de metadatos.

Nota: Security Analytics no tiene grupos de metadatos incorporados además del grupo predeterminado. Se deben definir grupos de metadatos adicionales antes de que aparezcan en el menú Usar grupo de metadatos. Una vez creados, los grupos de metadatos definidos por el usuario se pueden editar, eliminar, exportar para su uso en otros servicios e importar al servicio que se está investigando. Todos estos procedimientos están dentro de un tema aparte: Administrar grupos de metadatos definidos por el usuario.

El cuadro de diálogo Claves de metadatos predeterminadas permite especificar la vista predeterminada y mostrar la secuencia de claves de metadatos durante la navegación en la vista Investigation > Navegar para un servicio específico. En el caso de cada clave o de todas las claves, puede establecer la vista predeterminada en:

- Oculta: Los resultados de la clave de metadatos predeterminada se ocultan y no están disponibles para carga.
- Abierto: Los resultados de la clave de metadatos predeterminada son abiertos y se muestran todos los valores y conteos.
- Cerrada: Los resultados de la clave de metadatos predeterminada son cerrados, solamente se puede ver el nombre de los metadatos.
- Automática: La carga de claves de metadatos predeterminadas se controla mediante el nivel de índice, el cual debe indexarse según valor.

Cuando use las claves de metadatos predeterminadas, tenga presente que se pueden modificar para distintos servicios y que es posible que no vea el mismo conjunto de claves de metadatos predeterminadas cuando navegue a un punto de desglose en diferentes servicios. Si no ve los datos que espera, puede ser necesario cambiar la vista inicial de las claves de metadatos predeterminadas.

Cuando cambia el estado inicial de las claves de metadatos predeterminadas en la vista Navegar, el cambio persiste para ese servicio. Cuando se agregan nuevas claves al archivo de índice personalizado para un servicio Core (por ejemplo, `broker-custom-index.xml` y `decoder-custom-index.xml`), las nuevas claves se agregan a la lista de claves de metadatos predeterminadas. Los cambios que hace en la vista Navegar se aplican solo al servicio actual.

Usar claves de metadatos predeterminadas

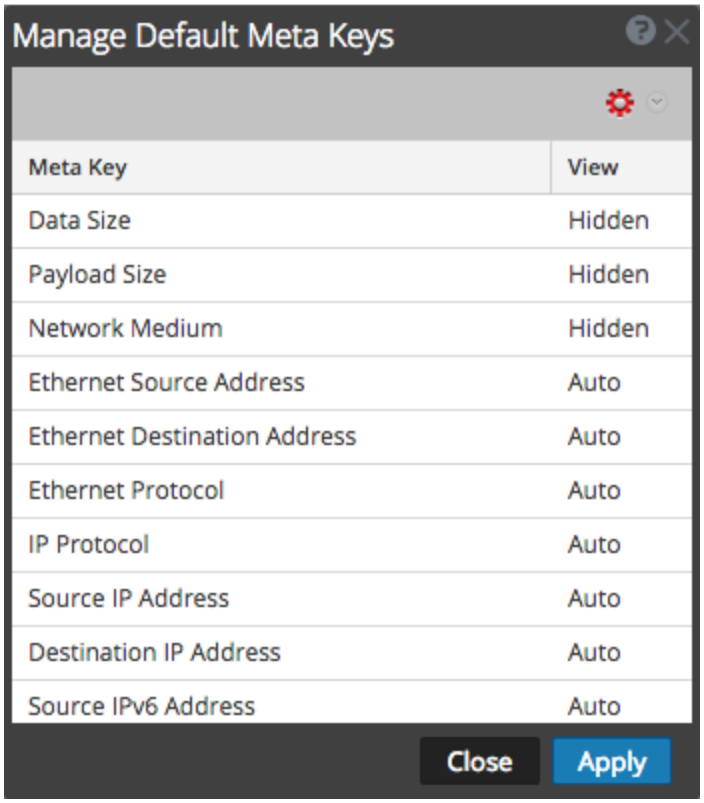
Para especificar que la vista Navegar inicial se abra con las claves de metadatos predeterminadas:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar.**
2. Seleccione un servicio y elija **Navegar**.
3. En el menú **Metadatos**, seleccione **Usar claves de metadatos predeterminadas**.
   Si hay una investigación en curso, los datos se vuelven a cargar en la vista actual y un ícono resalta la opción seleccionada. Si aún no se cargan datos, las claves de metadatos predeterminadas se usan para la carga siguiente.

Configurar claves de metadatos predeterminadas

Para configurar la vista predeterminada de claves de metadatos predeterminadas en la vista Investigation > Navegar:

1. En la barra de herramientas de la vista **Navegar**, seleccione **Metadatos > Administrar claves de metadatos predeterminadas**.
   El cuadro de diálogo Administrar claves de metadatos predeterminadas se muestra con la lista de claves de metadatos disponibles para el servicio.



2. (Opcional) Para cambiar el orden de las claves, seleccione una o más claves y arrastre los valores hacia arriba o hacia abajo por la lista de claves.

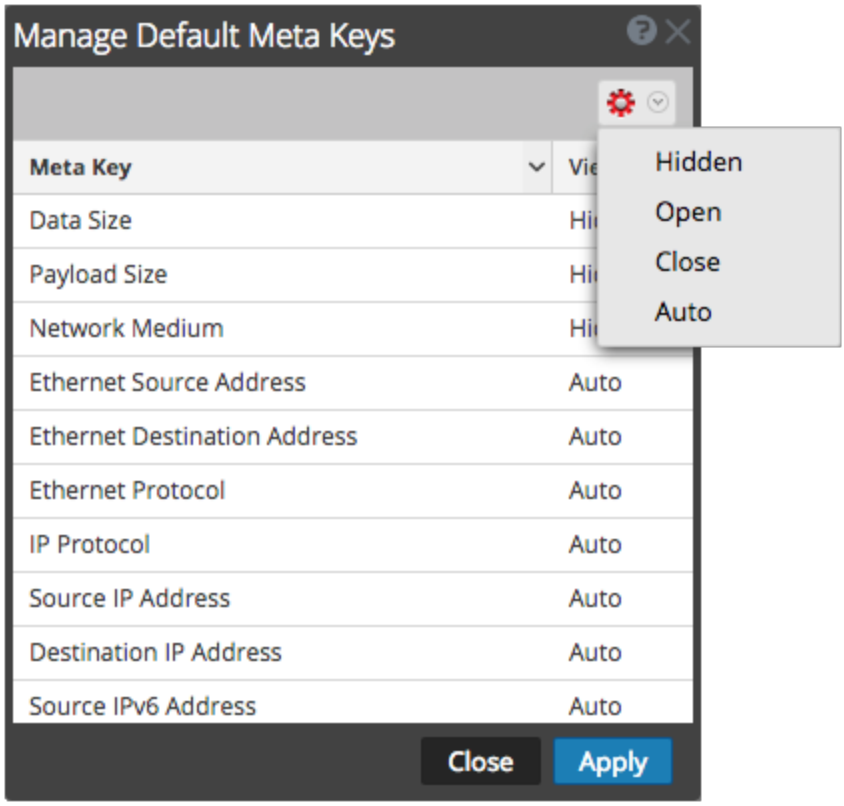
3. Realice una de las siguientes acciones

   a. (Opcional) Para cambiar la vista predeterminada de todas las claves de metadatos, asegúrese de que no se ha seleccionado ninguna clave y en la barra de herramientas, seleccione .

   b. (Opcional)Para cambiar la vista predeterminada de una o más claves, seleccione las claves y en la barra de herramientas, seleccione .

      Se muestra una lista desplegable de las posibles vistas iniciales de todas las claves de metadatos predeterminadas.

   c. (Opcional) Para volver a la vista predeterminada de claves de metadatos como se especifica en el archivo de índice del servicio, asegúrese de que no esté seleccionada ninguna clave y, en la barra de herramientas, seleccione > **Automático**.



   Cuando modifica las claves de metadatos predeterminadas para una clave de metadatos no indexada, no puede configurar la clave en ABIERTO. Si cambia a ABIERTO la vista predeterminada para un grupo de claves de metadatos y algunas de las claves de metadatos no están indexadas, estas claves vuelven a AUTOMÁTICO. En consecuencia, la clave de metadatos se carga automáticamente solo si está indexada, y las claves de metadatos no indexadas se CIERRAN hasta que se abren de forma manual.

4. Seleccione una de las vistas.
5. Para guardar los cambios, haga clic en **Aplicar**.
   Las claves de metadatos que se muestran en la vista Navegar están ajustadas a sus especificaciones. Si las claves de metadatos predeterminadas están ocultas, los valores de las claves de metadatos no se muestran en la investigación en absoluto. Si las claves de metadatos predeterminadas están cerradas, los valores de las claves de metadatos no se cargan de forma predeterminada, pero puede cargar las claves de metadatos individuales de forma manual en la vista Navegar.

Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos

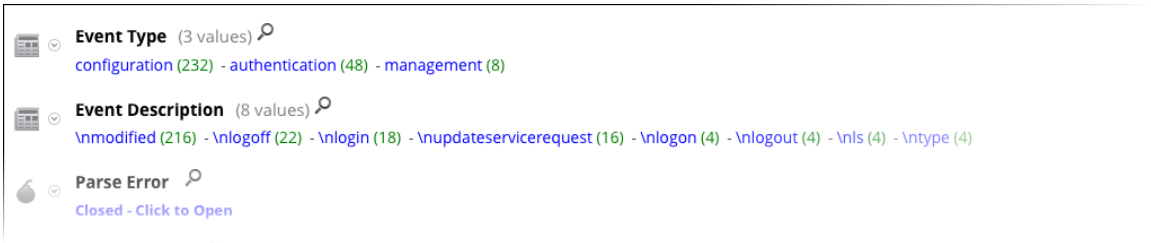
En este tema se proporciona un procedimiento para seleccionar la forma en que se cuantifican y se secuencian los resultados de cada clave de metadatos en la vista Investigation > Navegar.

Cada sección Clave de metadatos en la vista Investigation > Navegar contiene una lista de valores ordenada que muestra cada valor de clave de metadatos (Valor) y su conteo (Total). Puede especificar si:

- Los resultados de cada sección Clave de metadatos se clasifican según Valor o Total.
- Los resultados se clasifican en orden ascendente o descendente.
- Los valores que se muestran para cada clave de metadatos se cuantifican por cantidad de paquetes (Conteo de paquetes), cantidad de sesiones o registros (Cuantificar por conteo de eventos) o tamaño de los eventos (Cuantificar por tamaño de evento).

Nota: Si tiene un Log Decoder y un Packet Decoder cuyos metadatos observa, el cálculo de lo que se cuenta realmente depende del tipo de clave. Si opta por Cuantificar por conteo de paquetes y observa los registros, la salida de la vista Navegar es la misma que si hubiera seleccionado Cuantificar por conteo de eventos (consulte Investigation: Vista Navegar para obtener detalles).

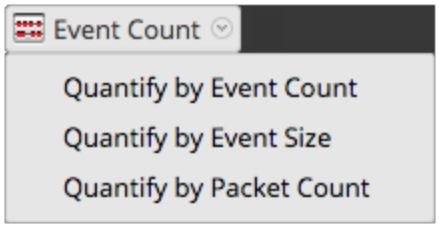
En esta imagen se muestra la clave de metadatos `Event Type` clasificada por **Total** en orden **Descendente**. El valor con el mayor conteo de coincidencias se presenta primero. El valor `configuration` tiene 232 coincidencias y se enumera primero. El valor `management` solo tiene ocho coincidencias y se presenta al final. El método de cuantificación es **Conteo de eventos**.



En esta imagen se muestran las claves de metadatos `Event Type` clasificadas por **Valor** en orden **Descendente**. Los nombres de los valores se presentan en orden alfabético a partir del final del alfabeto. El valor `management` se enumera primero. El valor `authentication` se presenta al final. El método de cuantificación es **Conteo de eventos**.

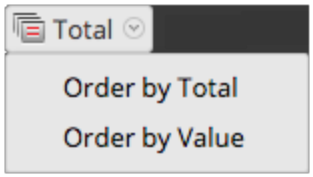
Para seleccionar el método de cuantificación de conteo de claves de metadatos y el orden de los resultados de claves de metadatos que se muestran en la vista Navegar:

1. En la barra de herramientas, seleccione **Conteo de eventos, Tamaño de evento** o **Conteo de paquetes** y elija una de las opciones de cuantificación del menú desplegable. La etiqueta del menú muestra la opción seleccionada.

   La vista actual se vuelve a cargar de acuerdo con la selección.

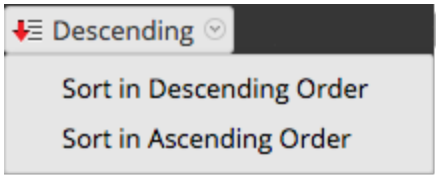
2. En la barra de herramientas, seleccione **Total** o **Valor** y elija uno de los métodos de orden del menú desplegable. La etiqueta del menú muestra la opción seleccionada.

   La vista actual se vuelve a cargar de acuerdo con la selección.

3. En la barra de herramientas, seleccione **Ascendente** o **Descendente** y elija una de las opciones de orden de clasificación del menú desplegable. La etiqueta del menú muestra la opción seleccionada.

La vista actual se vuelve a cargar de acuerdo con la selección.



Establecer el rango de tiempo para una investigación

Cuando realiza una investigación en la vista Investigation > Navegar, las opciones de rango de tiempo limitan los resultados devueltos. Puede seleccionar:

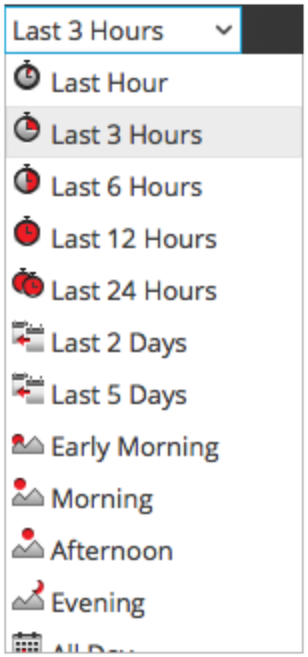
- Un rango de tiempo relativo a la recopilación. Los rangos relativos a la recopilación se basan en la última hora de recopilación de datos.
- Un rango de tiempo relativo al calendario.
- Un rango de fechas personalizado.
- Todos los datos.

El rango de fechas seleccionado (tipo) se muestra en el panel de opciones como la etiqueta Rango de tiempo; de forma predeterminada la etiqueta es **Últimas 3 horas**. La pantalla Rango de tiempo muestra el primer y el último registro de fecha y hora del rango de fechas que se está utilizando para los metadatos.

Nota: El rango de tiempo se basa en la zona horaria configurada en el panel Preferencias de perfil, como se describe en "Configurar las preferencias de usuario" en la *Guía de introducción de Security Analytics*.

Seleccione un rango de tiempo incorporado para la investigación

1. En el panel de opciones, haga clic en la opción **Rango de tiempo** de la barra de herramientas de la vista Navegar. (El rango de tiempo predeterminado es para las **Últimas 3 horas**, pero es posible que ya esté seleccionado un valor distinto en la lista de selección, por ejemplo, **Todos los datos** o **Última hora**, y que se utilice como etiqueta en el panel de opciones).
   Se muestra la lista de selección Rango de tiempo.



2. Realice una de las siguientes acciones

   a. Si desea ver todos los datos, seleccione **Todos los datos**.

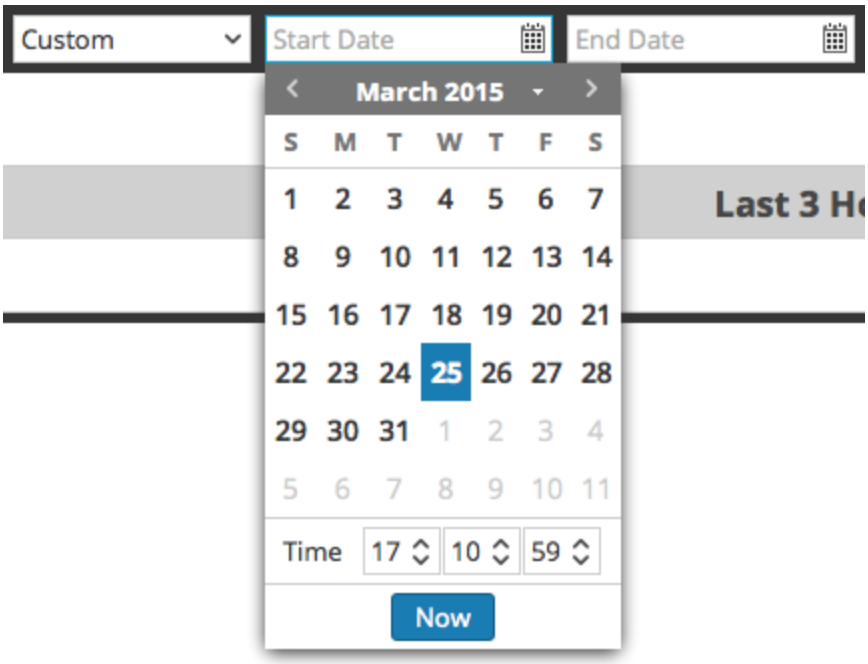
   b. Si desea establecer un rango de tiempo relativo a la recopilación en minutos, horas o días, seleccione un valor como **Últimos 10 minutos**, **Últimas 3 horas** o **Últimos 5 días**.

   c. Si desea establecer un rango de tiempo relativo a hoy, seleccione **Ayer**, **Todo el día** o una parte del día, como **Primera hora**, **Mañana**, **Tarde** o **Noche**.

   d. Si desea establecer un rango de fechas único, seleccione **Personalizado** en el menú **Rango de tiempo** y siga el procedimiento a continuación.
   El rango de tiempo seleccionado se aplica a los resultados actuales del panel Valores.

Especificar un rango de tiempo personalizado para una investigación

1. Seleccione **Personalizado** en el menú **Rango de tiempo**.
   Las opciones de selección de fecha se muestran en la barra de herramientas.



2. Dentro de los campos de tiempo **Fecha inicial** y **Fecha de finalización**, realice lo siguiente para especificar la fecha y la hora:
   a. Haga clic en una fecha del calendario.
   b. (Opcional) Seleccione la hora en los campos Hora, Minuto, Segundo o haga clic en **Ahora**. La selección de la hora se configura de manera predeterminada en la hora actual.

Nota: Si se especifican horas de inicio o finalización personalizadas en segundos, siempre el valor de la hora de inicio en segundos se configura de manera predeterminada en :00 y siempre el valor de la hora de finalización en segundos se configura de manera predeterminada en :59. Por ejemplo, si está usando la hora para desglosar a un problema, la hora de desglose se interpreta como “HH:MM:00 - HH:MM:59”. Los segundos se muestran en este formato en las funciones de **Investigation > Navegar**.

3. Para aplicar el rango, haga clic en **Ir**.
   El rango de tiempo seleccionado se aplica a los resultados actuales del panel Valores.

Usar perfiles de Investigation para encapsular vistas personalizadas

En este tema se indica a los analistas cómo usar perfiles que definen un conjunto de preferencias de Investigation para las vistas Navegar y Eventos.

El uso de perfiles es una manera rápida y fácil de personalizar los datos que se muestran en Investigation. En el cuadro de diálogo Administrar perfiles, puede usar un perfil para especificar los grupos de metadatos y los grupos de columnas que se muestran de forma predeterminada, para agregar consultas a una investigación y para importar o exportar perfiles.

Nota: Los perfiles se comparten entre usuarios en la misma red de Security Analytics. Si un usuario modifica o elimina un perfil, esto afecta lo que está disponible para los demás usuarios.

Si tiene múltiples perfiles, puede alternar entre ellos para cambiar rápidamente a las preferencias del perfil seleccionado. Si un perfil está activo actualmente, el título del menú Perfil se reemplaza por el nombre del perfil.

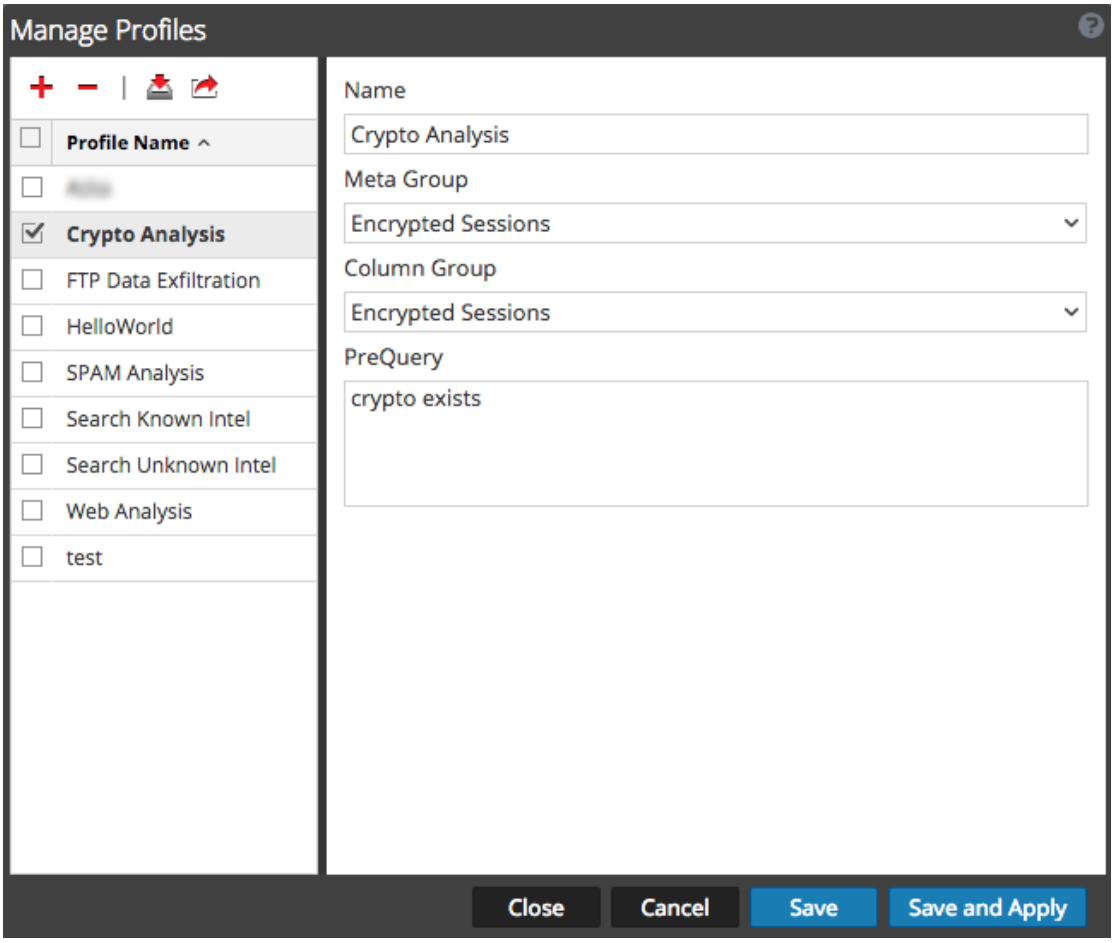
En la siguiente figura, esto se ilustra en la vista Navegar. El nombre del perfil se muestra entre Consulta y Metadatos.

En la siguiente figura, esto se ilustra en la vista Eventos. El nombre del perfil se muestra entre Consulta y Vista de lista.

Navegar al cuadro de diálogo Administrar perfiles

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Investigation > Eventos**.
2. Si se muestra el cuadro de diálogo **Investigar**, seleccione un servicio y haga clic en **Navegar**.

3. En la barra de herramientas, seleccione **Perfil > Administrar perfiles**.
   Se muestra el cuadro de diálogo Administrar perfiles.



Crear y editar perfiles

1. En el cuadro de diálogo **Administrar perfiles**, seleccione un perfil existente mediante un clic en la casilla de verificación junto al nombre o haga clic en + para crear un nuevo perfil.
   El panel derecho está disponible.
2. Edite o ingrese el nombre del perfil. Para esto, escríbalo en el campo **Nombre**. El nombre debe tener entre dos y 80 caracteres.
3. Seleccione un grupo de metadatos en la lista desplegable **Grupo de metadatos**. Puede agregar grupos de metadatos personalizados como se describe en Administrar grupos de metadatos definidos por el usuario.

4. Seleccione un grupo de columnas para la lista desplegable **Grupo de columnas**. Puede agregar grupos de columnas personalizados como se describe en Administrar grupos de columnas en la vista Eventos.
5. Escriba consultas para filtrar los resultados en el campo **Consulta previa**. Consulta previa sigue la misma sintaxis que el generador de consultas. La consulta previa en la figura usa un grupo de metadatos llamado **crypto exists**.
6. Haga clic en **Guardar** para guardar el perfil sin usarlo o haga clic en **Guardar y aplicar** para guardar el perfil y usarlo de inmediato.
   Si hace clic en **Guardar y aplicar**, se muestra un cuadro de diálogo de confirmación antes de que el perfil seleccionado se configure como activo.

Cambiar el perfil activo

Si no ve resultados suficientes o los resultados correctos en las vistas Navegar o Eventos, es posible que haya un perfil activo. Si no desea usar ningún perfil, puede hacer clic en **Desactivar perfiles** en el menú desplegable **Perfiles**.

Para usar otro perfil:

1. En la barra de herramientas de las vistas **Navegar** o **Eventos**, abra el menú desplegable **Perfiles**.
2. Mantenga el mouse sobre la opción **Perfil** para mostrar una lista desplegable de perfiles disponibles.
3. Seleccione el perfil que desea usar.
   La configuración del perfil se aplica de inmediato.

Si desea cambiar el perfil activo en el cuadro de diálogo Administrar perfil:

1. En la barra de herramientas de las vistas **Navegar** o **Eventos**, seleccione **Perfiles > Administrar perfiles**.
   Se muestra el cuadro de diálogo Administrar perfiles.
2. Seleccione un perfil en el panel de la izquierda y haga clic en **Guardar y aplicar**.
   Se muestra un cuadro de diálogo de confirmación.
3. Haga clic en **Sí**.
   La configuración del perfil se aplica de inmediato.

Importar perfiles

Puede cargar o importar archivos .jsn que se descargaron de otro servicio.

1. En el cuadro de diálogo **Administrar perfiles**, haga clic en  en la barra de herramientas del panel de la izquierda.
2. Se muestra el cuadro de diálogo Importación de perfil.
3. Haga clic en **Navegar** o en el campo **Cargar archivo** para seleccionar un archivo de la computadora.
4. Cuando se haya seleccionado el archivo, haga clic en **Cargar**.
   El perfil se muestra en el panel de la izquierda.

Descargar perfiles

Los perfiles se descargan como archivos .jsn.

1. En el cuadro de diálogo **Administrar perfiles**, seleccione uno o más perfiles en el panel de la izquierda.
2. En la barra de herramientas del panel de la izquierda, haga clic en  .
   La descarga comienza de inmediato.

Visualizar metadatos como coordenadas paralelas

En este tema se indica a los analistas cómo usar la visualización de coordenadas paralelas de la vista Navegar para centrar la investigación en combinaciones de valores y claves de metadatos que pueden indicar que los eventos son anormales y que ameritan una investigación.

El gráfico de coordenadas paralelas es una manera de visualizar el punto de desglose actual en Investigation para examinar más de dos claves de metadatos simultáneamente. La visualización simultánea de varias claves de metadatos puede ayudar a identificar problemas de seguridad asociados a comparaciones y patrones multivariantes, como cuando los valores y las claves de metadatos individuales no causan preocupación, pero si se combinan, pueden revelar un patrón o una relación anormales.

Mejores prácticas para obtener gráficos de coordenadas paralelas eficaces

Para crear gráficos de coordenadas paralelas eficaces, siga estas recomendaciones:

- Comience desde un punto de desglose en la vista Navegar en lugar de intentar visualizar todos los datos.
- Limite el rango de tiempo si es necesario.
- Elija el conjunto útil de claves de metadatos más pequeño para mostrar como ejes.
- Especifique la secuencia de ejes para resaltar las anomalías entre los valores de metadatos a medida que sigue una línea que cruza el gráfico.

- Cuando pueda identificar un conjunto de claves de metadatos útil y una secuencia, cree un grupo de metadatos personalizado para usarlo en investigaciones futuras. Por ejemplo, puede crear un grupo de metadatos personalizado para tipos de archivos ejecutables de Windows.
- Importe los grupos de metadatos personalizados que RSA distribuyó a través de la comunidad de RSA.
- Vuelva a utilizar y comparta los grupos de metadatos personalizados mediante su importación y exportación como archivos .jsn.
- Puede ser útil crear dos versiones de cada grupo de metadatos personalizado. Una para el análisis de valores de metadatos y otra para crear un gráfico de coordenadas paralelas que se centre en un subconjunto más pequeño del mismo caso de uso.

Nota: Cuando se importan grupos de metadatos en el servidor de Security Analytics, Security Analytics muestra un mensaje de error si alguno de los grupos ya está presente en la aplicación. Para importar un grupo que es un duplicado, primero debe eliminar el grupo existente. Si desea eliminar un grupo de metadatos, un perfil no puede estar usándolo.

Como ayuda para optimizar la creación de gráficos de coordenadas paralelas, en Security Analytics 10.5 y superior se incluyen varias optimizaciones.

- Los analistas pueden especificar que en el gráfico solo se representen las sesiones en las cuales existen todas las claves de metadatos.
- El administrador puede aumentar la cantidad de valores de metadatos que se representan en Configuración de coordenadas paralelas de la vista Sistema de Administration.

Casos de uso de grupos de metadatos de RSA para coordenadas paralelas

En la comunidad de RSA, un conjunto de grupos de metadatos personalizados predefinidos está disponible como un archivo jsn: MetaGroups_ootb_w_query.jsn. Para comenzar a utilizar algunos grupos de metadatos que RSA configuró con el fin de resaltar ciertas actividades, puede importar este archivo .jsn en el cuadro de diálogo Administrar grupos de metadatos. Algunas de las actividades dirigidas que se prestan para las visualizaciones de coordenadas paralelas son:

- Señalización por botnet
- Canales encubiertos
- Correo electrónico
- Sesiones cifradas
- Análisis de archivos
- Malware Analysis

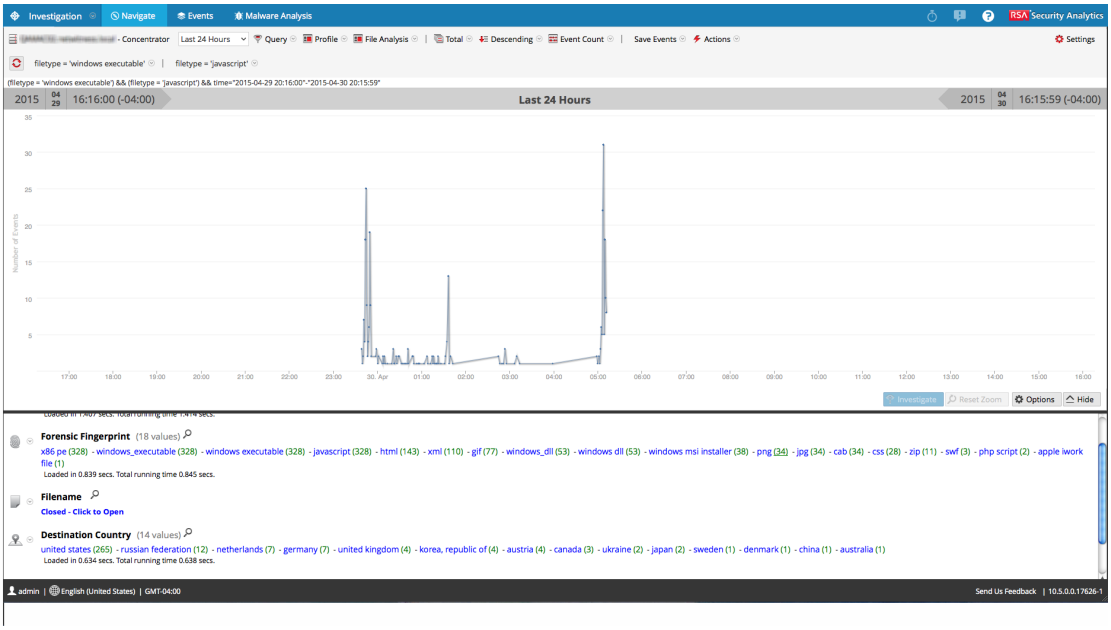
- Consultar archivos
- Consultar hosts
- Consultar direcciones IP
- Consultar correo
- Consultar usuarios
- Consultar web
- Ataques de inyección SQL
- Análisis de amenazas
- Análisis web

Ver una visualización de coordenadas paralelas

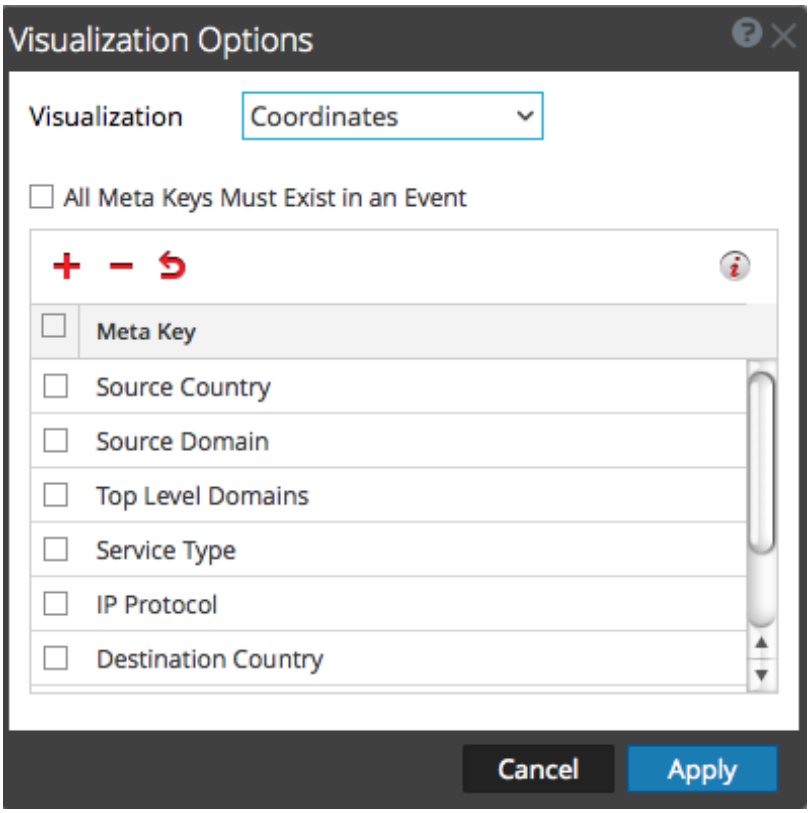
Desde una investigación en la vista Investigation > Navegar:

1. Si el panel Visualización sobre el panel Valores está cerrado, seleccione **Visualización**.
2. En la barra de herramientas, seleccione **Usar grupo de metadatos > Análisis de archivos**.
3. En el panel **Valores**, en la clave de metadatos **Huella digital forense**, haga clic en `windows_executable` y en `javascript`, de modo que la ruta de navegación indique `filetype = 'windows_executable' | filetype = 'javascript'`.

4. Una visualización predeterminada para el punto de desglose actual se muestra como un cronograma.

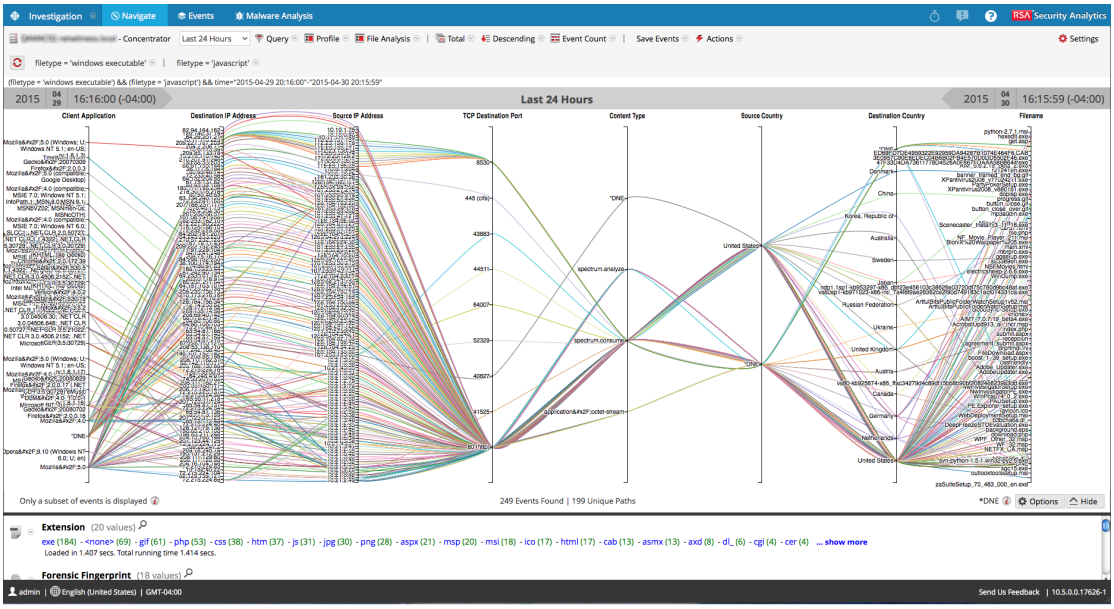


5. En el panel **Visualización**, seleccione **Opciones**.
   Se muestra el cuadro de diálogo Opciones de visualización.
6. En la lista desplegable **Visualización**, seleccione **Coordenadas** y haga clic en **Aplicar**.



La visualización se carga. En este ejemplo, se encuentran 249 eventos y se visualizan 199

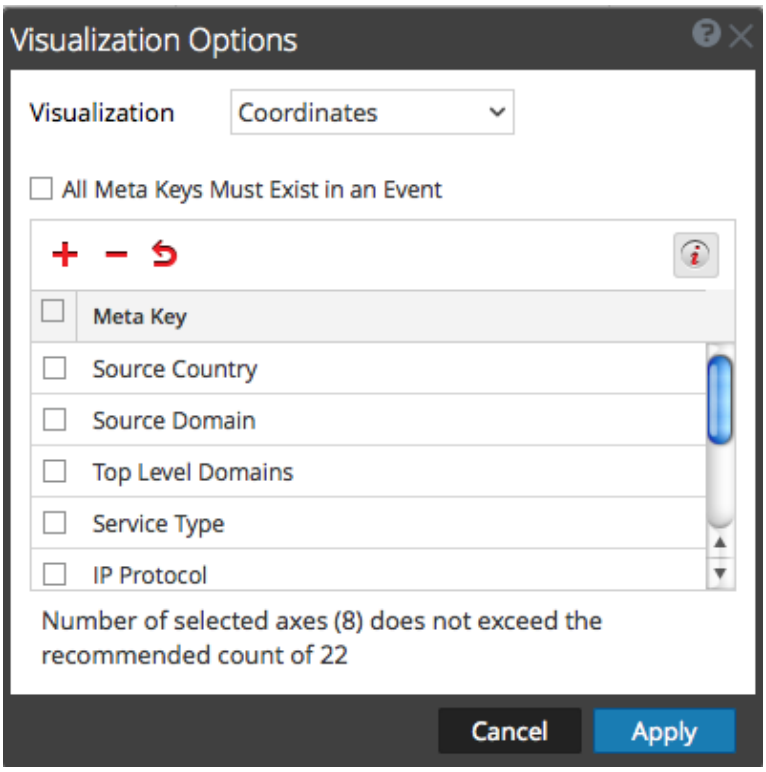
rutas únicas.



Seleccionar claves de metadatos para una visualización de coordenadas paralelas

Con una visualización de coordenadas paralelas abierta, realice lo siguiente:

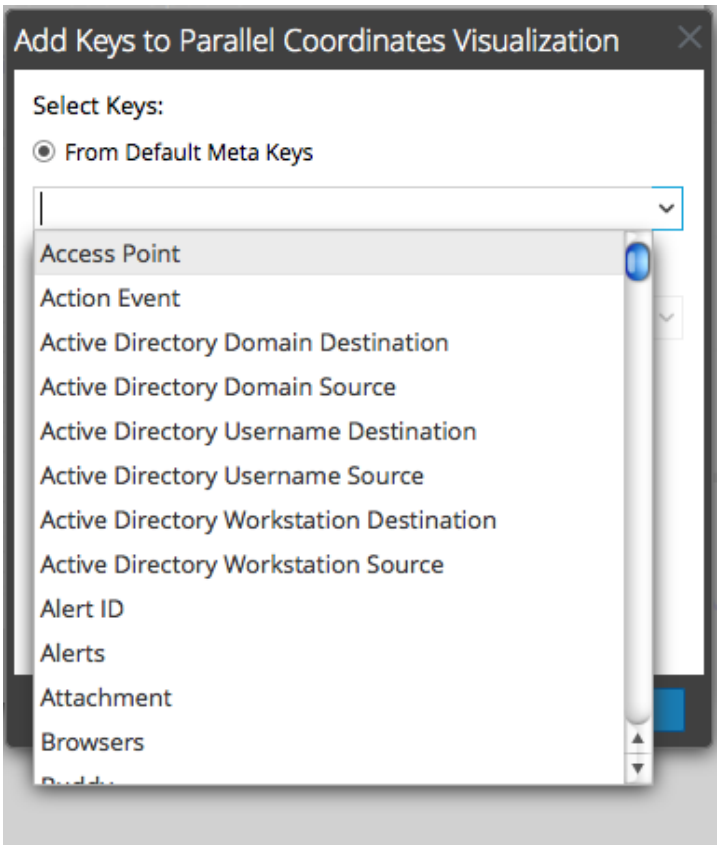
1. En el panel Visualización, seleccione **Opciones**.
   Se muestra el cuadro de diálogo Opciones de visualización. En la barra de herramientas, haga clic en con el fin de mostrar la cantidad recomendada de ejes para una visualización legible. Cuando se muestra un conteo de claves recomendado, el conteo cambia en función del tamaño del navegador. Si agranda la ventana del navegador, el conteo recomendado aumenta.



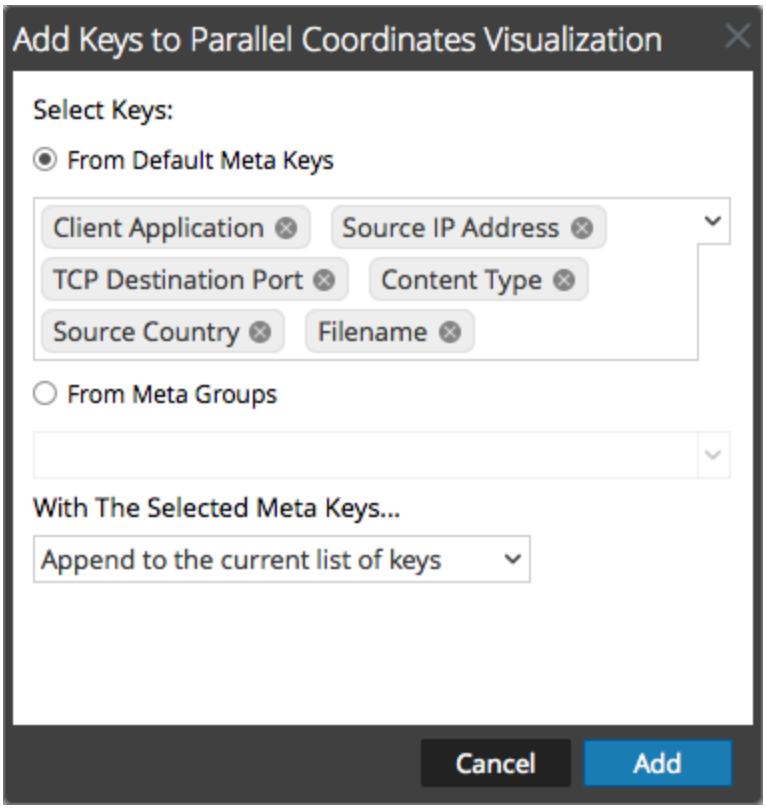
2. Si desea cambiar la secuencia de claves de metadatos, arrastre las claves de metadatos hacia arriba o hacia abajo para disponerlas en la secuencia deseada.
3. Si desea eliminar las claves de metadatos, haga clic en el cuadro de selección y, a continuación, en —.

   Las claves de metadatos se eliminan, pero el cambio aún no se aplica.
4. Si desea revertir al estado anterior, haga clic en ↩.

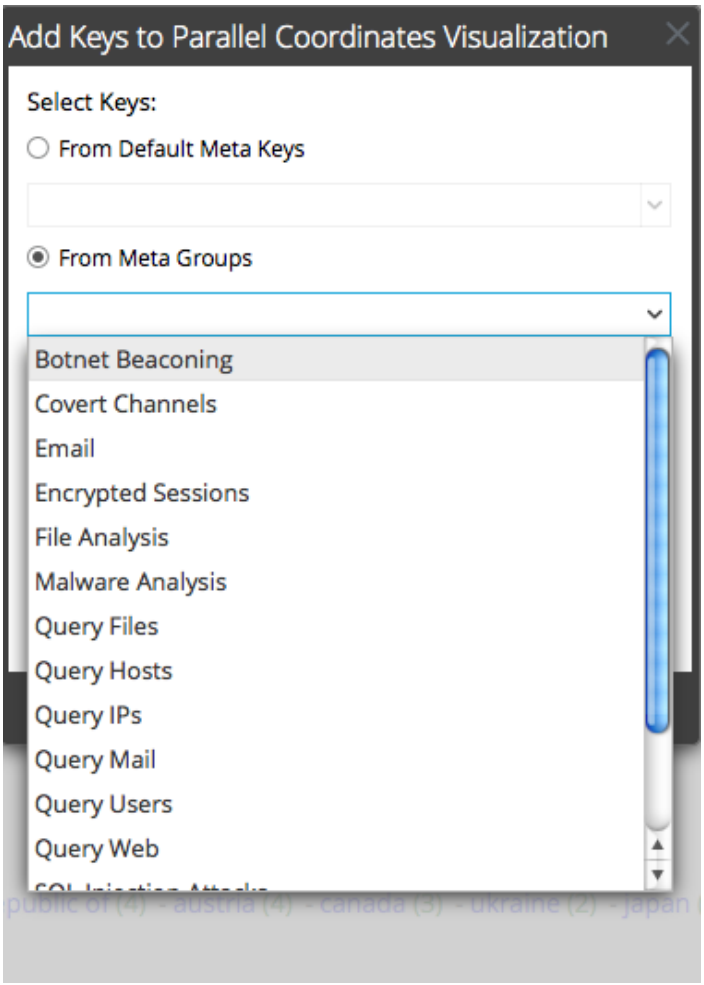
   Las claves de metadatos que eliminó se restauran y los cambios que hizo se eliminan.
5. Si desea seleccionar claves de metadatos individuales, haga clic en +, seleccione **Desde claves predeterminadas** y, en la lista desplegable, seleccione las claves de metadatos.



Las claves seleccionadas se enumeran.

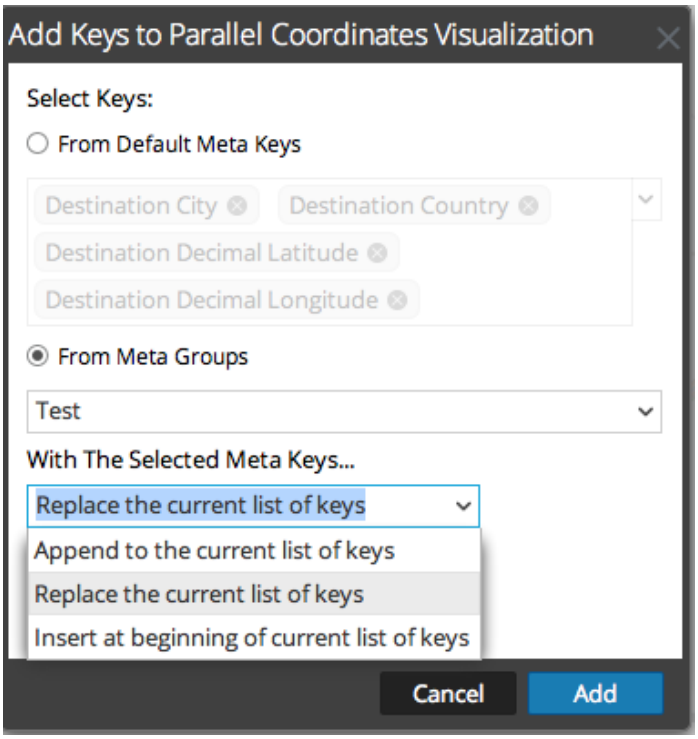


6. Si desea agregar todas las claves de un grupo de metadatos, no puede agregar claves de metadatos individuales. Seleccione **Desde grupos de metadatos** y elija un grupo en la lista desplegable.

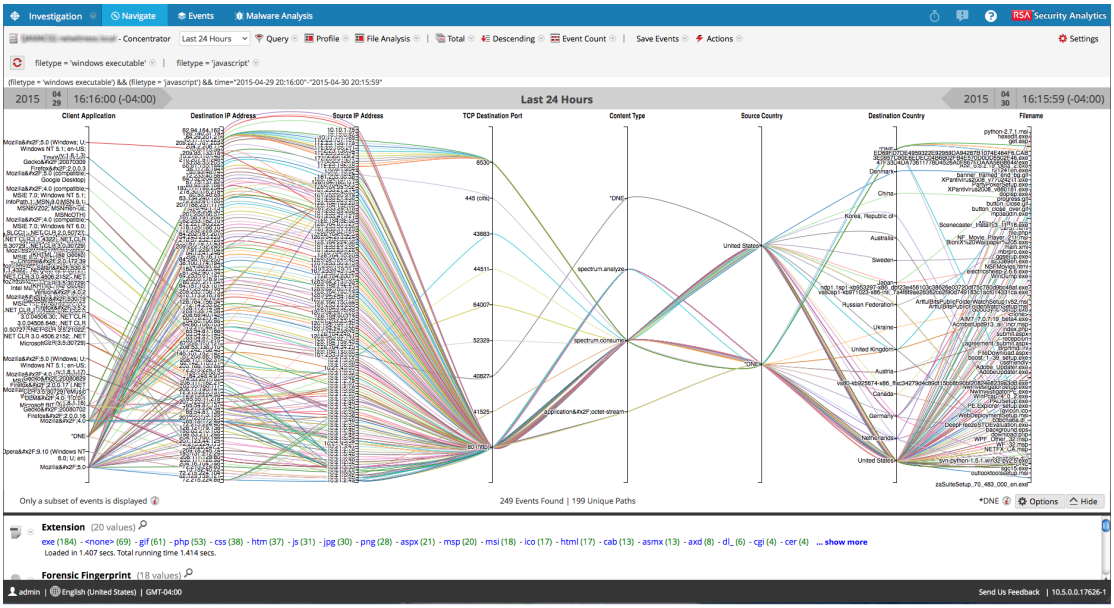


Los grupos de metadatos seleccionados se enumeran en el campo.

7. Seleccione el método para agregar las claves o los grupos: **Reemplazar la lista actual de claves**, **Agregar a la lista actual de claves** (al final) o **Insertar al comienzo de la lista actual de claves.**

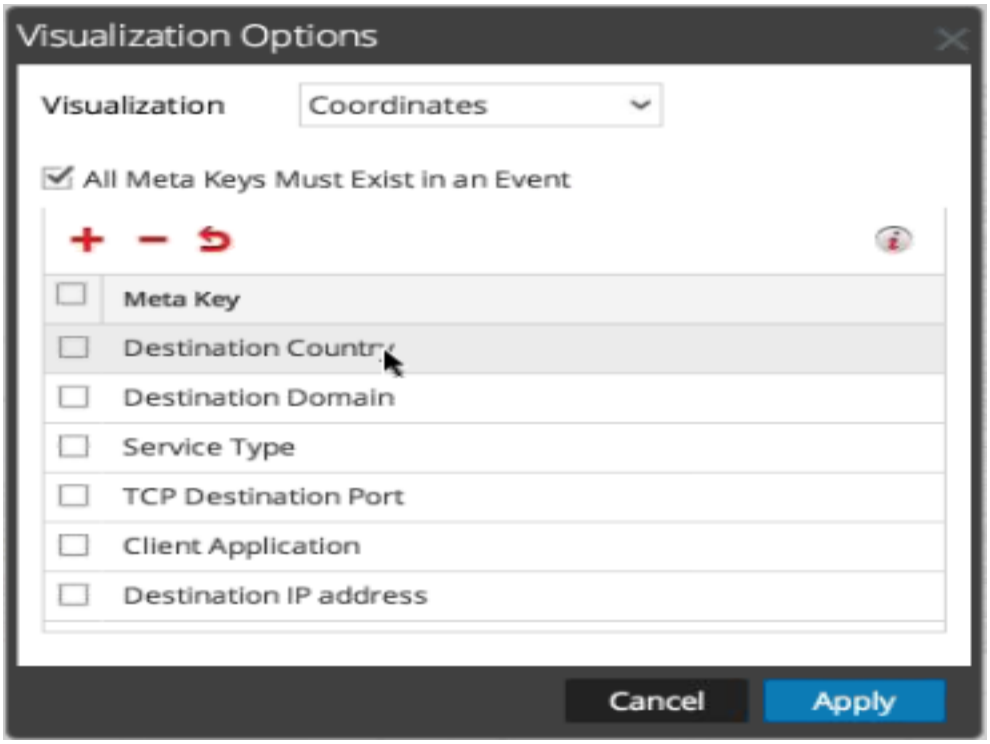


8. Para completar el procedimiento, haga clic en **Agregar**.
   El cuadro de diálogo Opciones de visualización se muestra con los grupos o las claves de metadatos que seleccionó.
9. Para mostrar el nuevo gráfico de visualización, haga clic en **Aplicar**.

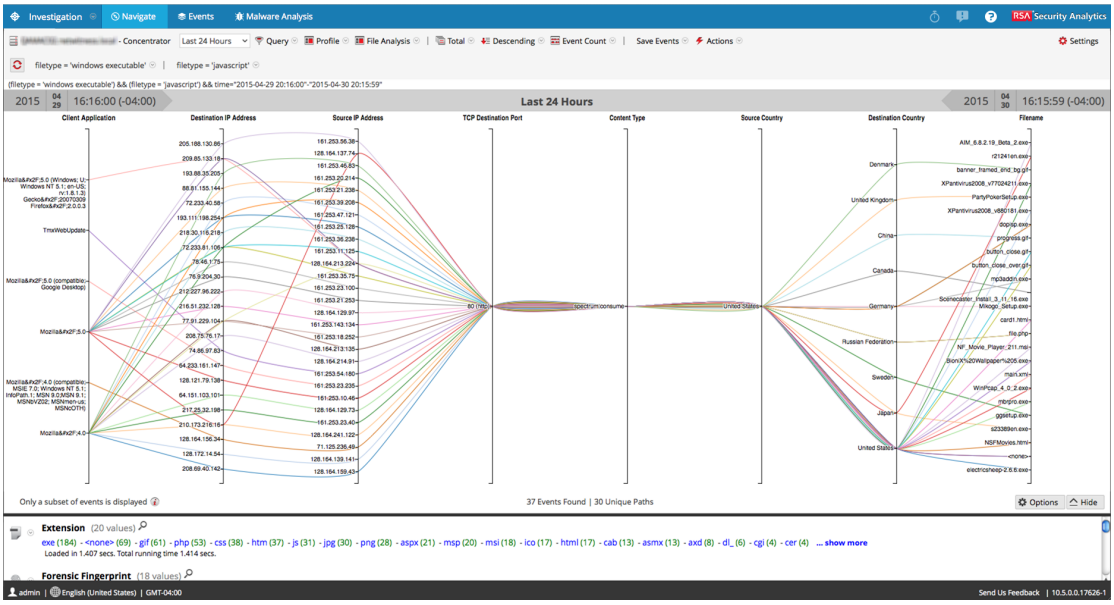


Optimizar una visualización de coordenadas paralelas

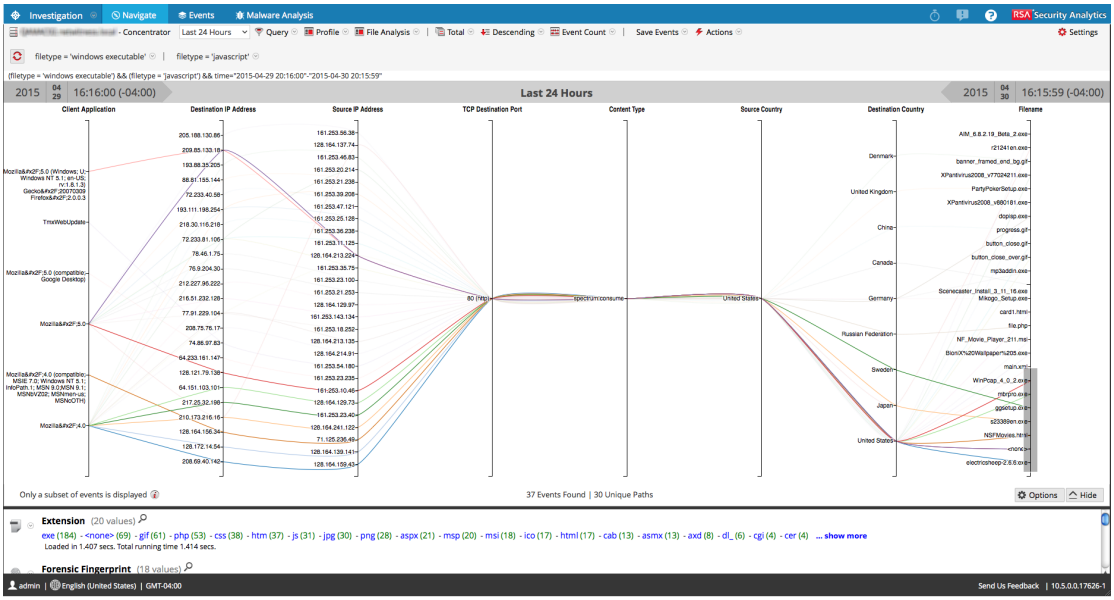
1. Para optimizar la visualización mediante la eliminación de eventos en los cuales no existen todas las claves de metadatos, seleccione **Opciones**.



2. En el cuadro de diálogo Opciones de visualización, seleccione **Todas las claves de metadatos deben existir en un evento**. Haga clic en **Aplicar**.
   El gráfico resultante es más legible y útil, y generalmente tiene menos rutas únicas.



3. Si desea resaltar un conjunto de puntos pequeño para ver la ruta de la línea de derecha a izquierda, haga clic en un eje. El cursor cambia a una mira, la cual puede arrastrar para seleccionar uno o más valores. Cuando suelta el mouse, las líneas se resaltan. En el siguiente ejemplo, el tipo de servicio SSL se resalta con un cuadro de colorgris.



4. Si desea ampliar la visualización, arrastre hacia abajo el borde inferior del panel y ensanche la ventana del navegador desde el borde derecho.

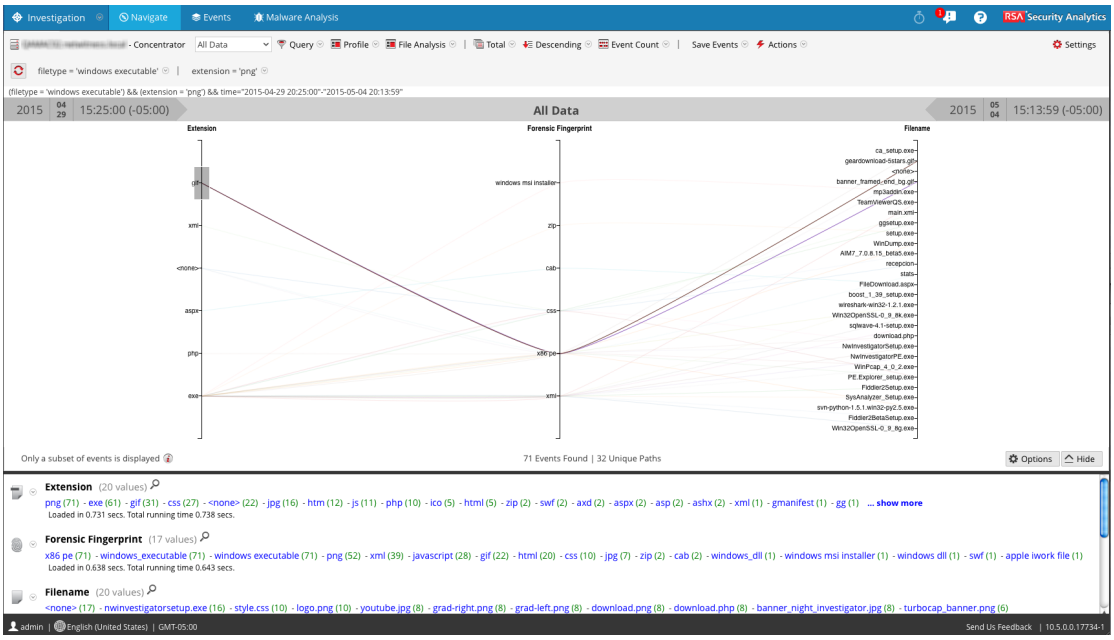
Ejemplo de caso de uso

El siguiente es un ejemplo de una visualización de coordenadas paralelas de claves de metadatos que representa metadatos de archivo en una sesión. Hay tres claves de metadatos o ejes de izquierda a derecha: Extensiones, Huella digital forense y Nombre de archivo con valores que se enumeran a lo largo de cada eje. Los valores del eje Extensión muestran la extensión de archivo y los valores del eje Huella digital forense son archivos ejecutables de Windows. Normalmente, el tipo de archivo coincide con la huella digital forense prevista; sin embargo, es anormal que un tipo de archivo gif esté en combinación con la huella digital de archivo ejecutable de Windows. Se selecciona el tipo de archivo gif para resaltar las correlaciones de ese tipo de archivo, x86pe, y dos nombres de archivo en el tercer eje, de modo que un analista pueda identificar rápidamente los archivos que ameritan una investigación.

Para llegar a esta vista:

1. Ordene por valor y clasifique en orden ascendente.
2. Aplique dos filtros (file type = 'windows executable' y extension = 'gif') en la vista Navegar para limitar la cantidad de datos.

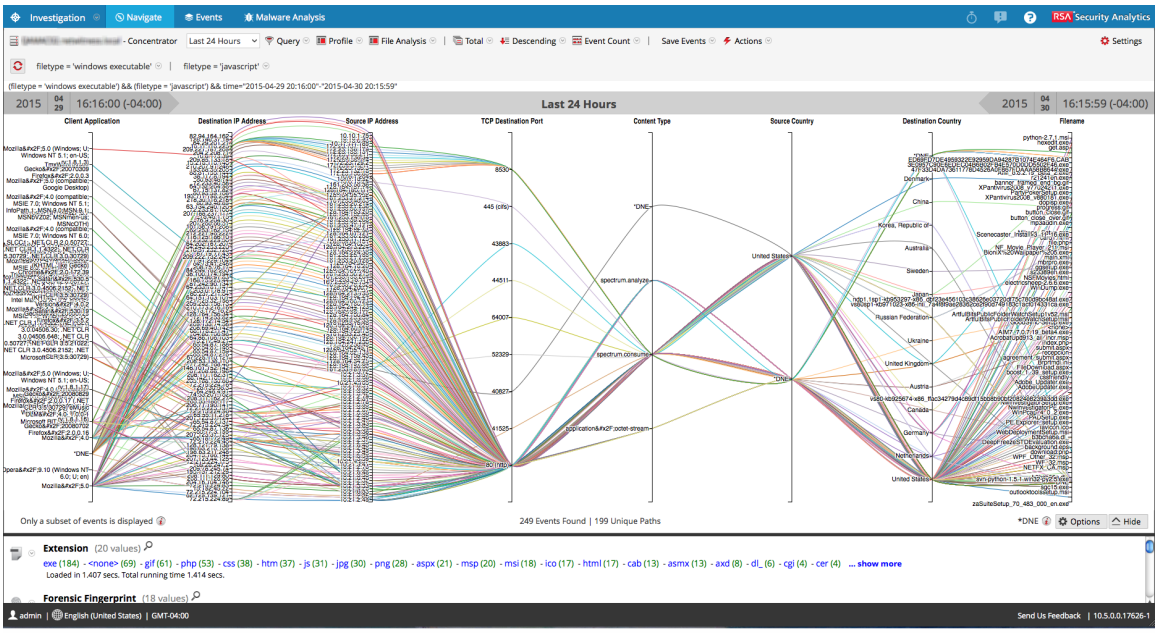
3. Configure un gráfico de coordenadas paralelas con la selección de tres ejes: extensión de archivo, huella digital forense y nombre de archivo.



Ejemplo de la visualización de un conjunto de datos grande

En este ejemplo de una visualización de coordenadas paralelas aplicada a un conjunto de datos más grande se ilustran varios mensajes que ayudan a los analistas a comprender lo que se graficó.

- Para crear un gráfico, Security Analytics comienza a escanear valores de metadatos y a devolver los resultados. Un rango de tiempo típico podría tener hasta 10,000,000 valores de metadatos. Cuando la cantidad de valores de metadatos devueltos alcanza el Límite de resultados de valores de metadatos, el gráfico se genera incluso si Security Analytics no ha escaneado una cantidad de valores de metadatos equivalente al Límite de escaneo de valores de metadatos.
- Hay un límite fijo en la cantidad de datos que se pueden representar como un gráfico de coordenadas paralelas. En Security Analytics 10.4 y anteriores, el límite se basa en la cantidad de ejes por valores de datos: 1,000 x la cantidad de ejes para proteger el rendimiento, pero en Security Analytics 10.5 y superior, el administrador configura límites de coordenadas paralelas como parte de los ajustes de Investigation en la vista Administration > Sistema.



Con un conjunto de datos más grande, el procesamiento del gráfico de coordenadas paralelas tarda más que con un conjunto de datos y claves de metadatos más pequeño. Para preservar el rendimiento, Security Analytics representa los valores de metadatos del panel Valores de abajo hasta que se alcanzan los límites que estableció el administrador. Un mensaje informativo indica: **Solo se muestra un subconjunto de eventos.**

De todos los datos visualizados para 249 eventos, solo hubo 199 rutas de coordenadas paralelas únicas. Ciertos eventos se incluyen aunque no contienen algunas de las claves de metadatos; estos se etiquetan **DNE** debido a que los metadatos no existen en el evento.

Consultar datos en la vista Navegar

En este tema se describen los métodos disponibles para consultar datos en la vista Investigation > Navegar.

Cuando se realiza una investigación en Security Analytics, están disponibles varios métodos para consultar los resultados y desglosar a un área de interés en la vista Navegar. Los analistas pueden:

- Crear una consulta personalizada, en lugar de hacer clic a través de claves y valores de metadatos.
- Desglosar a datos en Gráfico de tiempo de la vista Navegar.
- Desglosar a datos en el panel Valores
- Ver y modificar consultas mediante la integración de URL

Crear una consulta personalizada

En el panel de opciones de la vista Investigation > Navegar, puede crear una consulta en lugar de hacer clic en las claves y los valores de metadatos para desglosar a los metadatos. Los cuadros de diálogo para la creación de una consulta ofrecen ayuda de sintaxis con listas desplegables de las claves y los operadores de metadatos aplicables. Cuando observa la lista desplegable, puede expandir y contraer cada grupo de metadatos para ver u ocultar las claves de metadatos individuales en ese grupo.

Cuando selecciona un grupo de metadatos, Security Analytics genera la consulta compleja igual a una consulta con todas las claves de metadatos en ese grupo reunidas mediante OR. Entonces, si un grupo de metadatos contiene `ip.src` y `ip.dst`, la consulta generada es `ip.src = <value> OR ip.dst = <value>`. Si el grupo de metadatos contiene claves de metadatos que tienen diferentes tipos de valores de metadatos, el valor de entrada se deshabilita y la consulta utiliza declaraciones `exists`. Por ejemplo, un grupo de metadatos que contiene `ip.src`, `ip.dst` y `alias.host` incluye claves de metadatos que tienen diferentes tipos de valores; `ip.src` e `ip.dst` son las direcciones IP y `alias.host` es el texto. La consulta generada es `ip.src exists OR ip.dst exists OR alias.host exists`.

Una consulta básica tiene el siguiente formato:

`<metakey> <operator> [<metavalue>]`

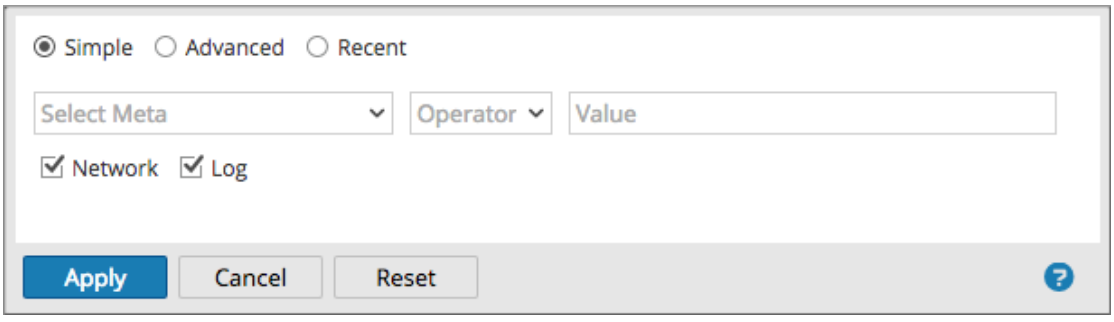
Estos son algunos ejemplos:

```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Crear una consulta con el método básico

Cuando crea una consulta con el método básico, Security Analytics proporciona listas desplegables de metadatos y operadores.

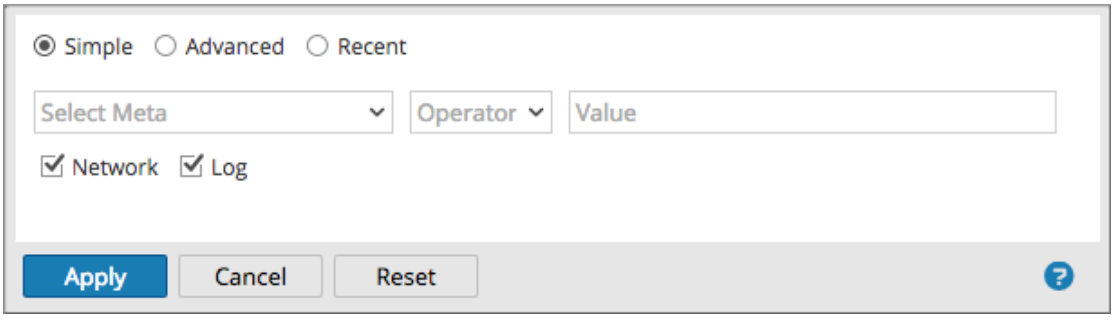
1. En la barra de herramientas de la **vista Navegación**, seleccione **Consulta**.
   El cuadro de diálogo Consulta se muestra con la opción Simple seleccionada.



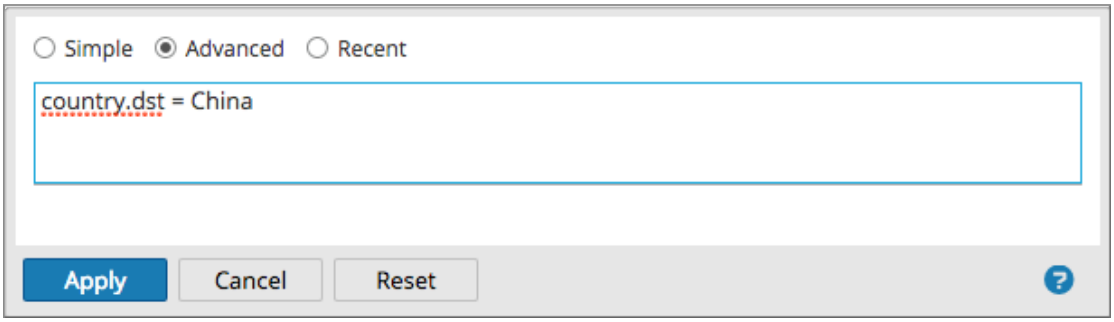
2. En el campo **Seleccionar metadatos**, haga clic para mostrar la lista desplegable. La lista desplegable tiene dos secciones: Grupos de metadatos y Todos los metadatos.
3. Seleccione una única clave de metadatos bajo **Todos los metadatos** o seleccione un grupo de metadatos bajo **Grupos de metadatos**. También puede ingresar en el campo una clave de metadatos o un grupo de metadatos.
4. En el campo **Operador**, escriba un operador o haga clic en la lista desplegable para seleccionar un operador válido.
5. (Opcional) Si ha seleccionado un operador que requiere un valor, por ejemplo, comienza, en el tercer campo escriba el valor de la clave de metadatos.
6. En las casillas de verificación Red y Log, seleccione el tipo de datos para consultar. Realice una de las siguientes acciones
   a. Para limitar la consulta a paquetes, seleccione **Red** y deseleccione **Log**. En la consulta, medium 1 = paquete.
   b. Para limitar la consulta a registros, seleccione **Log** y deseleccione **Red**. En la consulta, medium 32 = registros.
   c. Para aplicar la consulta a los paquetes y los registros, seleccione **Red** y **Log**.
7. Realice una de las siguientes acciones
   a. Haga clic en **Aceptar**.
      La ventana se cierra y la vista se actualiza con los resultados de la nueva consulta.
      La consulta se muestra en la ruta de navegación.
   b. Haga clic en **Cancelar**.
      La ventana se cierra y no se realizan cambios en la vista ni en la consulta actual.

Crear una consulta con el método avanzado

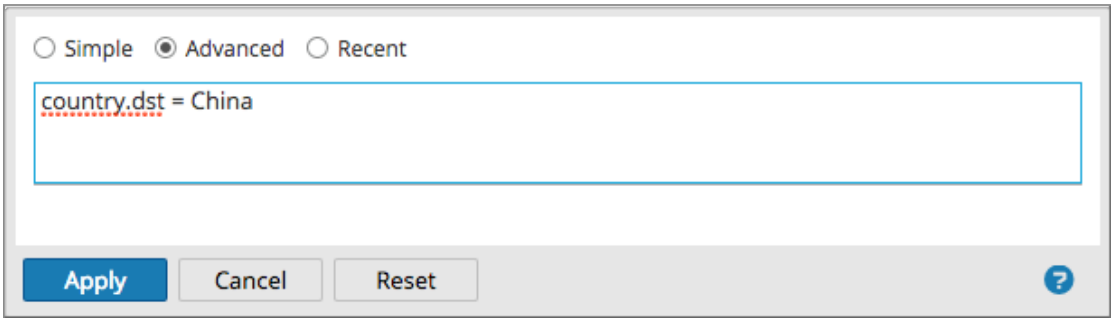
1. En la barra de herramientas de la **vista Navegar**, seleccione **Consulta**.
   Se mostrará el cuadro de diálogo Consulta.



2. Seleccione **Avanzado**.
   Se muestra el campo de consulta avanzada.



3. En el campo, cree una consulta que pueda incluir la clave de metadatos, el operador y un valor. Cuando comienza a escribir una clave de metadatos en el campo, se muestra una lista desplegable de las claves de metadatos disponibles para el servicio seleccionado.
4. Seleccione la clave de metadatos para la consulta.
   Se actualiza la pantalla. Si la expresión no se ha completado, el estado indica que la consulta no es válida.
5. Continúe con un operador, de la lista desplegable y, a continuación un valor si es necesario. La pantalla se actualiza a medida que sigue ingresando la consulta. Si ingresa un operador, como **exists** o **!exists**, que no utiliza el campo de valor, el campo de valor se desactiva y el estado no válido se borra. Si ingresa un operador, como =, que requiere el campo de valor, el estado no válido permanece hasta que se ingresa un valor. Cuando la consulta es válida ya no se muestra el estado no válido.



6. Realice una de las siguientes acciones
   a. Haga clic en **Aceptar**.
      La ventana se cierra y la vista se actualiza con los resultados de la nueva consulta.
      La consulta se muestra en la ruta de navegación.

b. Haga clic en **Cancelar**.

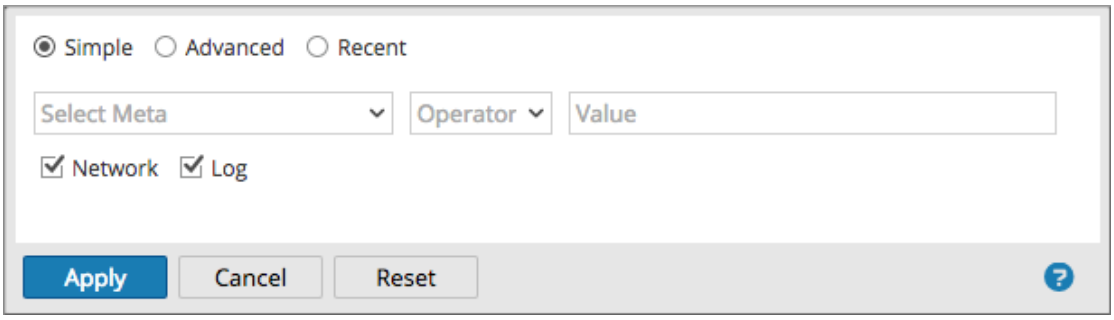
La ventana se cierra y no se realizan cambios en la vista ni en la consulta actual.

Aplicar una consulta reciente

Puede ver consultas recientes y seleccionar una para aplicar al servicio actual que se investiga. Para seleccionar una consulta reciente:

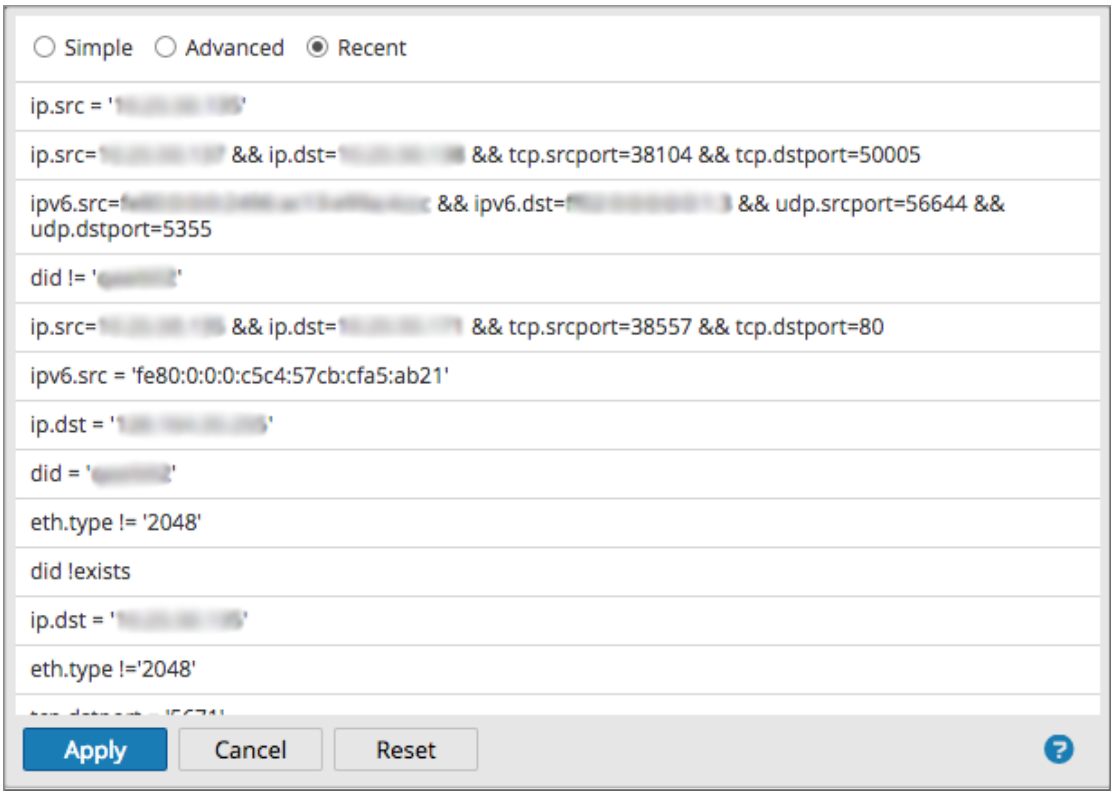
1. En la barra de herramientas de la **vista Navegar**, seleccione **Consulta**.

   El cuadro de diálogo Consulta se muestra con la opción Simple seleccionada.



2. Seleccione la opción **Reciente**.

   La lista de consultas recientes se muestra en la parte inferior del cuadro de diálogo.

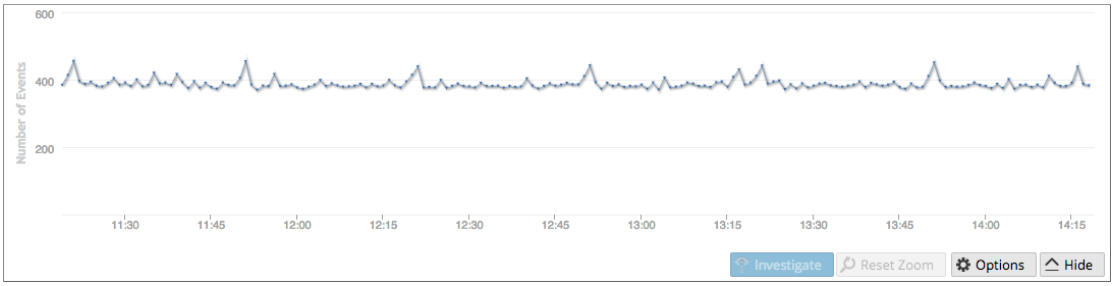


3. En la lista de consultas recientes, haga clic para seleccionar una consulta.
4. Realice una de las siguientes acciones
   a. Haga doble clic en una consulta.
   b. Seleccione una consulta y haga clic en **Aceptar**.
      La ventana se cierra y la vista se actualiza con los resultados de la nueva consulta.
      La consulta se muestra en la ruta de navegación.
   c. Haga clic en **Cancelar**.
      La ventana se cierra y no se realizan cambios en la vista ni en la consulta actual.

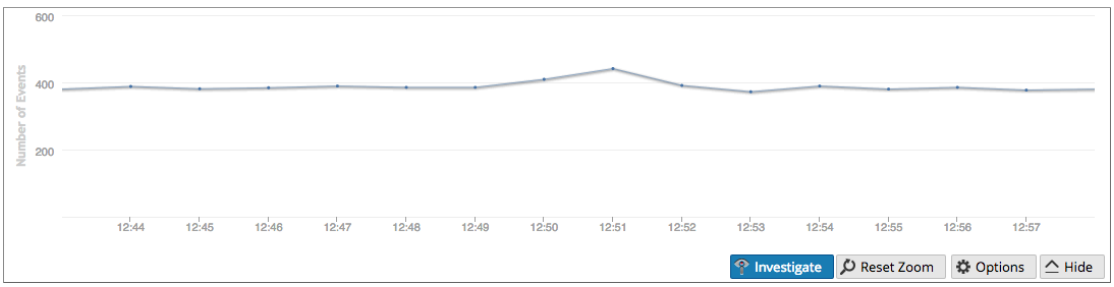
Desglosar a datos en Gráfico de tiempo de la vista Navegar

La visualización Gráfico de tiempo permite a los analistas visualizar actividades en el transcurso del tiempo. Puede acercar la vista a los datos mediante la selección de una ventana de tiempo y la opción Investigar. A continuación, puede restablecer la navegación al rango de tiempo que esta aplicado antes de acercar la vista.

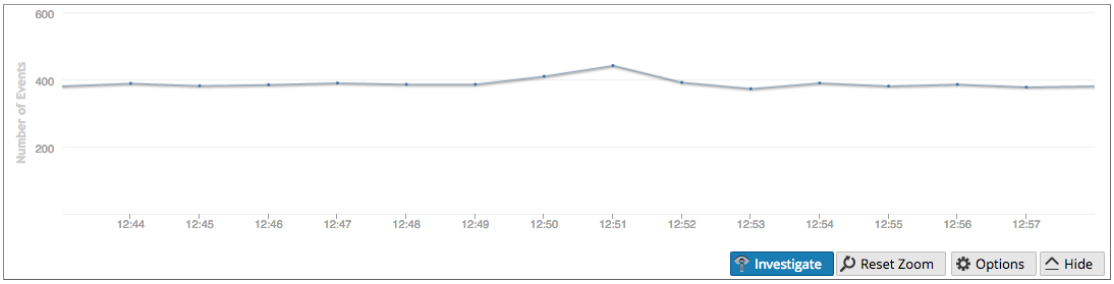
1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar**.
   Se muestran el gráfico de tiempo para el punto de desglose actual y el rango de tiempo seleccionado.



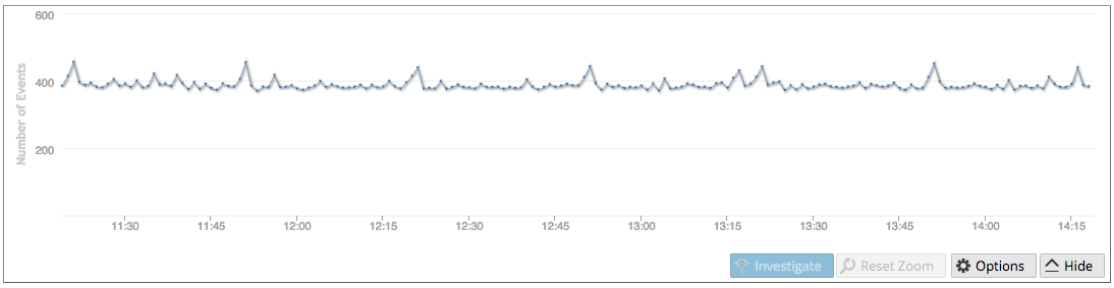
2. Para destacar un período de tiempo en el gráfico de tiempo, haga clic en el período de tiempo deseado y arrastre el mouse.
   Se vuelve a crear el gráfico de tiempo para el rango de tiempo seleccionado, sin embargo, no se alteran los valores de metadatos.



3. Para desglosar a datos en el rango de tiempo seleccionado, haga clic en **Investigar**.
   La URL se actualiza para reflejar el reemplazo del rango de tiempo, al igual que el panel de opciones de Investigation para reflejar el rango de tiempo personalizado. Se vuelve a crear el gráfico de tiempo y se cargan los valores de metadatos para el rango de tiempo seleccionado.



4. Para restablecer el gráfico de tiempo al rango de tiempo original, haga clic en **Restablecer zoom**.
   La URL se actualiza para reflejar la URL original antes de acercar la vista a los datos, al igual que el panel de opciones de Investigation para reflejar el rango de tiempo seleccionado antes del acercamiento. Se vuelve a crear el gráfico de tiempo para el rango de tiempo seleccionado y se cargan los valores de metadatos para ese rango de tiempo.

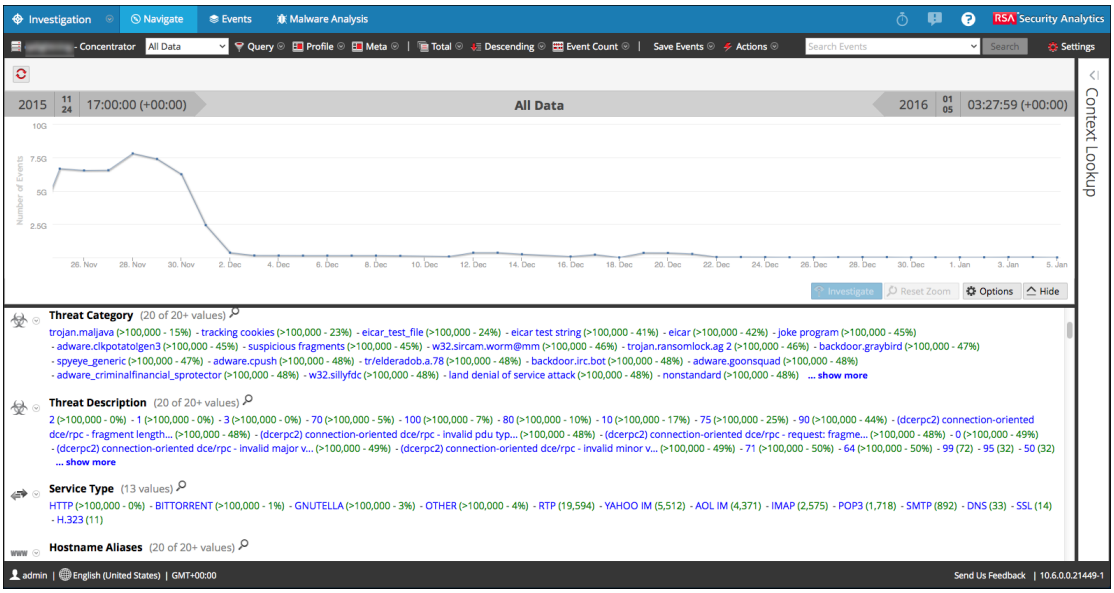


Desglosar a datos en el panel Valores

Security Analytics muestra la actividad y los valores del servicio seleccionado en la vista Investigation > Navegar. Para investigar los datos, los analistas desglosan a estos, para lo cual hacen clic en una clave de metadatos o en un valor de metadatos, lo que se trata como una consulta. En el panel Valores, cada consulta se agrega a los datos de la ruta de navegación. Esto da como resultado una ruta de navegación en la parte superior, con una ruta de navegación para cada consulta. Puede editar la ruta de navegación para insertar o quitar una consulta.

Desglosar a un subconjunto de metadatos

1. Inicie una investigación para mostrar los metadatos en la vista Navegar.

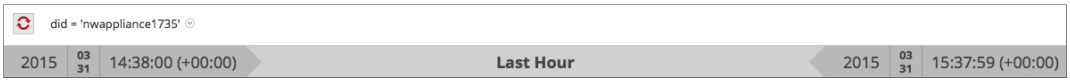


2. Para desglosar a los metadatos, realice cualquier combinación de las siguientes acciones:

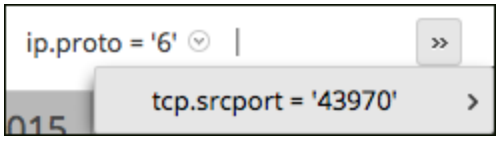
   a. Haga clic en una **clave de metadatos**, por ejemplo, País de origen o País de destino.

   b. Haga clic en un **valor de metadatos**, el texto de color azul en los resultados. Por ejemplo, Italia.

      Cada vez que hace clic en una clave de metadatos o en un valor de metadatos, la consulta de investigación cambia a un punto focal restringido, o punto de desglose, en los datos. En cada punto de desglose, el panel Valores se actualiza y el nuevo punto de desglose se muestra en la ruta de navegación. El siguiente es un ejemplo de la primera ruta de navegación.



      Este es un ejemplo de una ruta de navegación larga que no cabe en la barra de herramientas. A la última consulta que cabe le sigue un menú desplegable que muestra consultas adicionales. Para seleccionar un punto de desglose dentro del desbordamiento, haga clic en el ícono de desbordamiento y en una consulta de la lista desplegable.

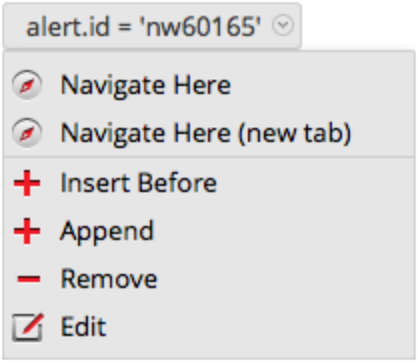


Agregar una consulta en la ruta de navegación

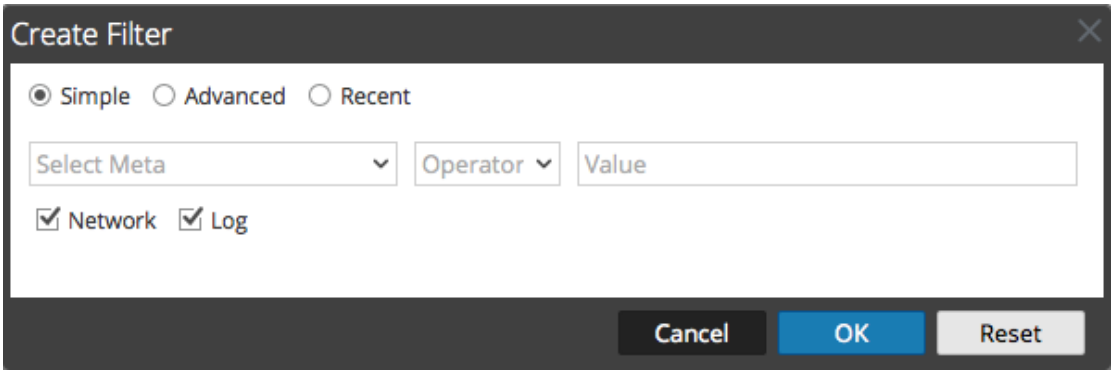
En la ruta de navegación, puede hacer clic en cualquiera de las rutas para mostrar el menú Consulta. Puede insertar una nueva consulta antes de una ruta de navegación y agregar una nueva consulta al final de la ruta. Después de cada edición en la ruta de navegación, Security Analytics actualiza los resultados.

Para agregar una consulta en la ruta de navegación:

1. Haga clic en una ruta de navegación.
   Se muestra el menú Ruta de navegación.



2. Para agregar una consulta en la ruta de navegación, seleccione **Agregar** o **Insertar antes**.
   Se muestra el cuadro de diálogo Crear filtro.



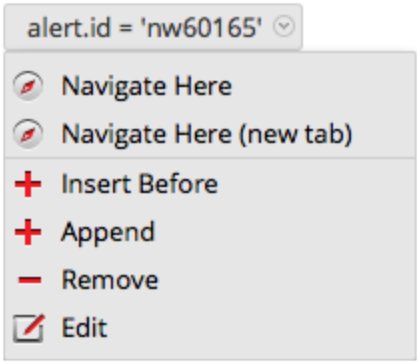
3. Cree la consulta como se describe en Crear una consulta personalizada.

Editar una consulta en la ruta de navegación

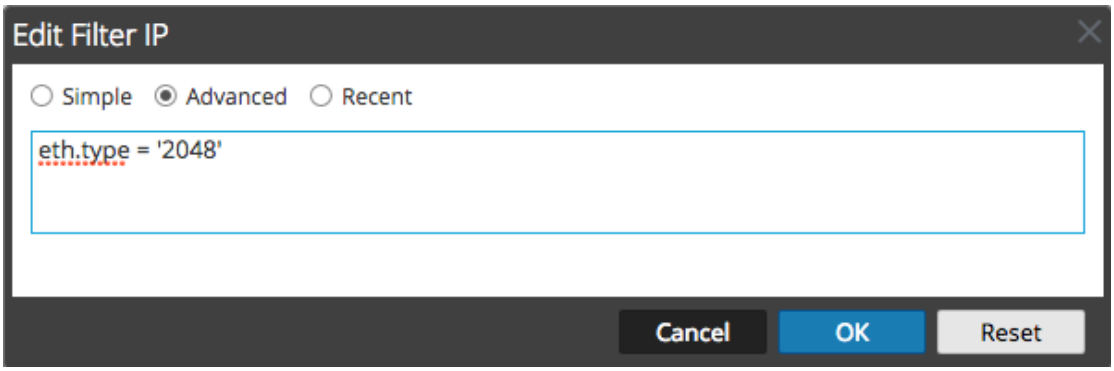
En la ruta de navegación, puede hacer clic en cualquiera de las rutas para mostrar el menú Consulta. Puede eliminar una ruta de navegación y editar una consulta en una ruta de navegación. Después de cada edición en la ruta de navegación, Security Analytics actualiza los resultados.

Para trabajar con consultas en la ruta de navegación:

1. Haga clic en una ruta de navegación.
   Se muestra el menú Ruta de navegación.



2. Para editar una consulta en la ruta de navegación, seleccione **Editar**.
   El cuadro de diálogo Crear se muestra con la consulta seleccionada abierta para edición.



3. Edite los campos como se describe en Crear una consulta personalizada.

Búsqueda rápida dentro de una clave de metadatos

1. Mantenga el mouse sobre una sección de clave de metadatos y haga clic en la lupa.
   Se muestra el formulario Búsqueda rápida, el cual contiene un comparador y un operando opcional para la búsqueda.

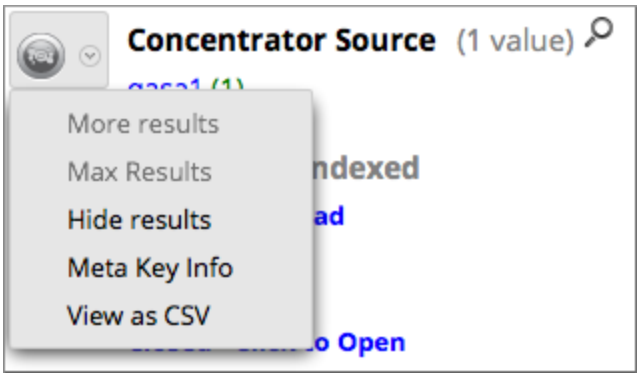
2. (Opcional) Si desea cerrar el formulario de búsqueda, vuelva a hacer clic en la lupa.

3. Seleccione la operación en la lista desplegable de la izquierda y escriba el valor de texto que desea buscar. A continuación, haga clic en **Desglosar** para realizar la ejecución.
   Los metadatos de esa clave de metadatos se utilizan para desglosar a los metadatos actuales.

Ver información de clave de metadatos en la vista Navegar

Para ver detalles sobre una clave de metadatos, específicamente el nombre de la clave, el nivel de índice configurado para mostrar la clave de metadatos y la vista predeterminada configurada para la clave de metadatos:

1. Haga clic en el menú desplegable junto a la clave de metadatos.



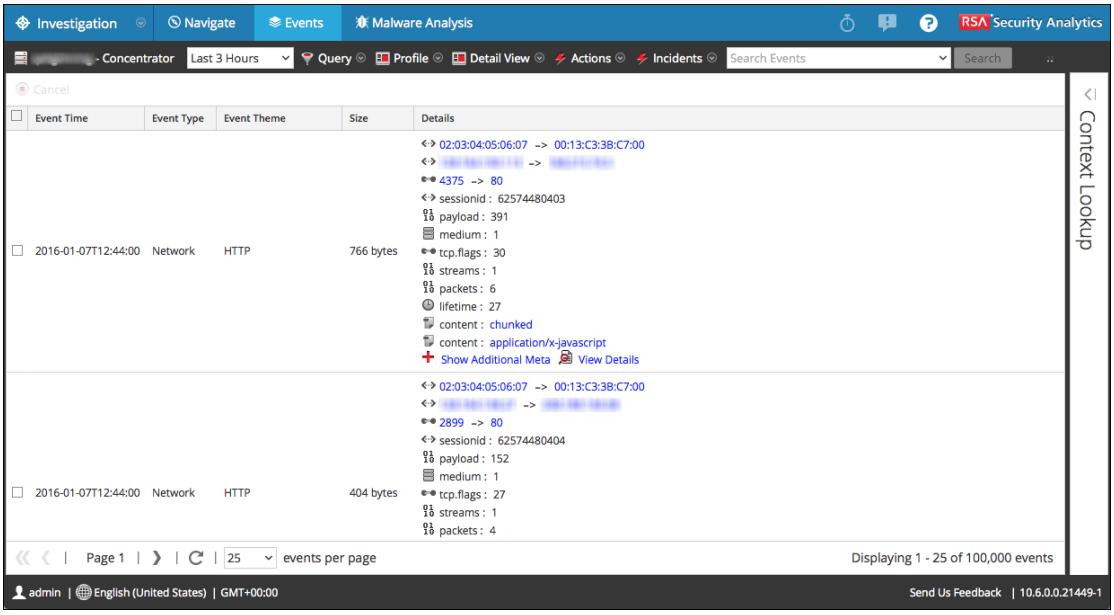
2. Seleccione **Información de clave de metadatos**.
   Se muestra el cuadro de diálogo Información de clave de metadatos.
3. Una vez que haya finalizado la visualización, haga clic en .
4. (Opcional) Para ver nombres de metadatos encontrados para la clave de metadatos como una lista de valores separados por coma, haga clic en el menú desplegable junto a la clave de metadatos y seleccione **Ver como CSV**.
   Se muestra el cuadro de diálogo Mostrando valores en formato CSV.
5. Una vez que haya finalizado la visualización, haga clic en **Cerrar**.
6. (Opcional) Si desea ocultar los resultados de la clave de metadatos en el punto de desglose actual, haga clic en el menú desplegable junto a la clave de metadatos y, a continuación, haga clic en **Ocultar resultados**.

Mostrar eventos asociados a un valor de metadatos

La vista Eventos proporciona detalles adicionales para un evento en dos vistas distintas: Lista Eventos y Vista detallada.

1. En la vista Navegar, desglose a los metadatos que sean el centro de la investigación.
2. Haga clic en el conteo (el número de color verde) junto a un valor de metadatos de color azul.

   Se muestra la vista Eventos correspondiente al punto de desglose actual.

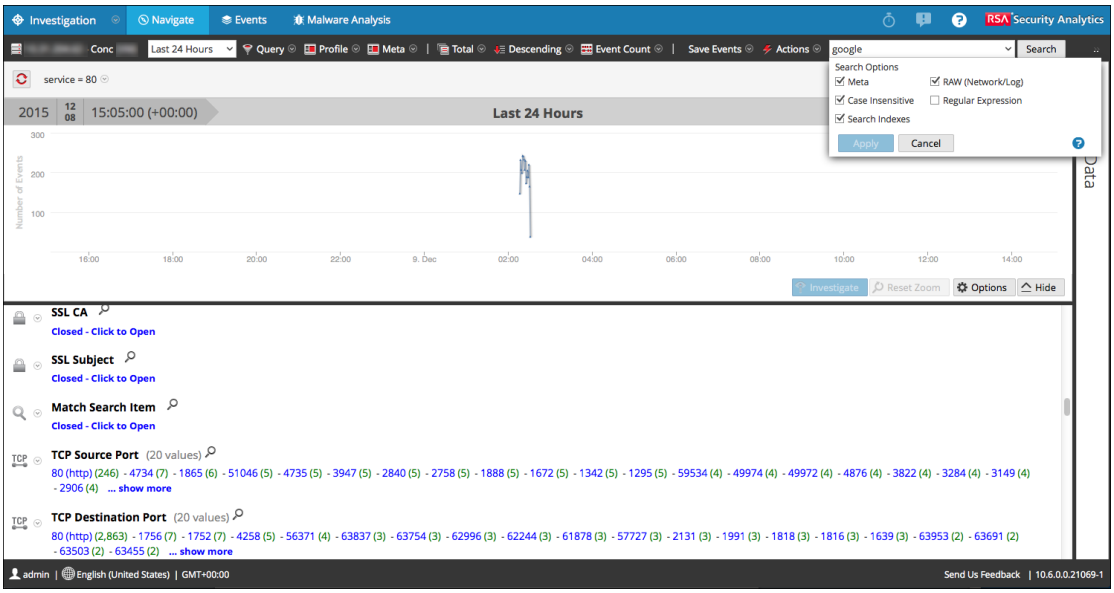


Las operaciones que puede realizar en la vista Eventos se describen en Examinar eventos.

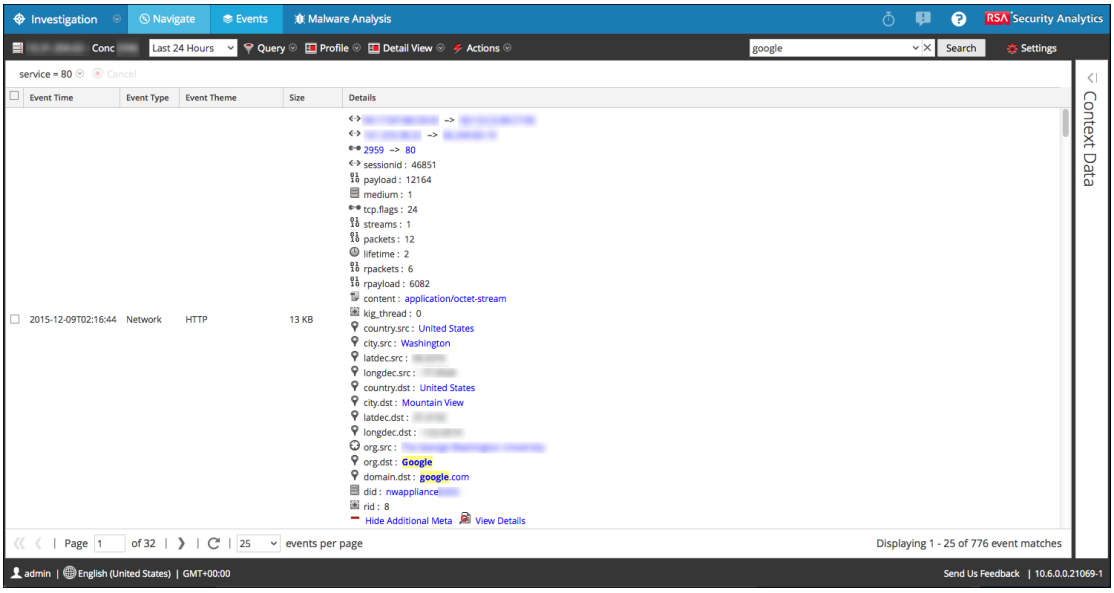
Búsqueda de eventos específicos asociados con un valor de metadatos

1. En la vista Navegar, desglose a los metadatos que sean el centro de la investigación (haga clic en el valor de metadatos o agregue una consulta).
2. Escriba una cadena de búsqueda en el cuadro de búsqueda y presione **Intro** o haga clic en **Buscar**.

   También puede seleccionar y configurar preferencias de modo de búsqueda para sus búsquedas. Consulte Investigation: Opciones de búsqueda para obtener información detallada acerca de la búsqueda.

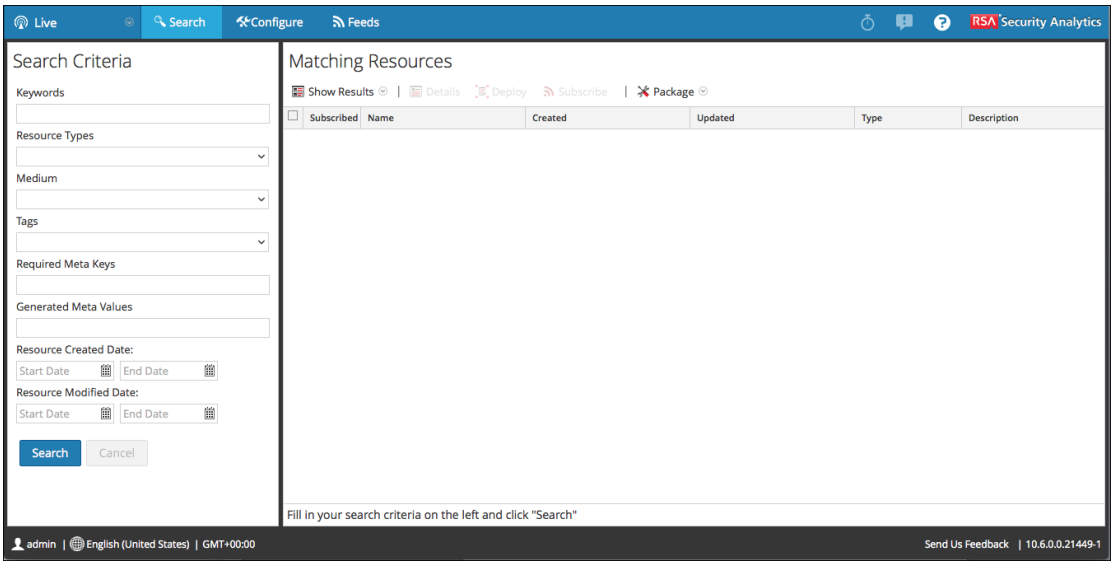


La vista Eventos se abre en una nueva pestaña y muestra los resultados de la búsqueda. Su selección de rango de tiempo y los desgloses (consultas) se transfieren a la vista Eventos.



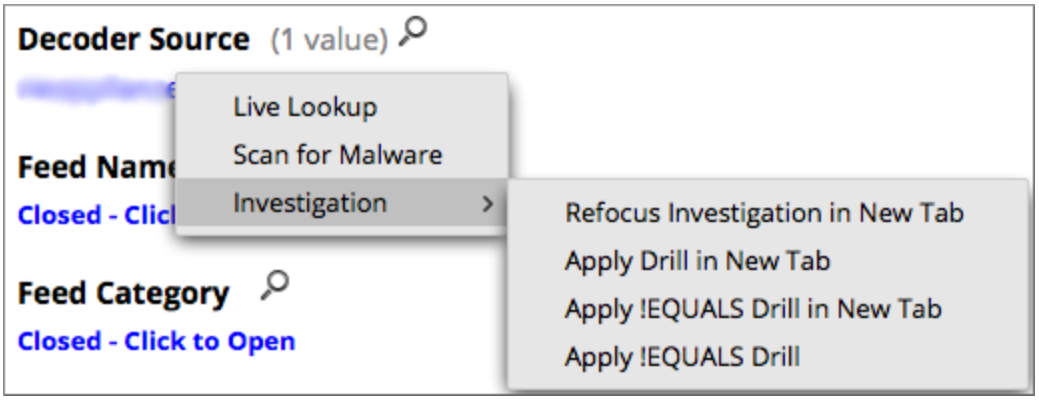
Ver un valor de metadatos seleccionado en Live

1. En la vista Navegar, desglose a los metadatos que sean el centro de la investigación.
2. Haga clic con el botón secundario en un valor de metadatos (el texto en azul).
   Se muestra el menú desplegable Valor de metadatos.
3. Para buscar el valor de metadatos en Security Analytics Live, seleccione **Búsqueda en Live**.
   La vista Búsqueda en Live se muestra con el valor de metadatos ingresado en el campo Valores de metadatos generados, el cual está listo para realizar una búsqueda.



Volver a enfocar la investigación en un punto de desglose

1. Haga clic con el botón secundario en un valor de metadatos (el texto en azul).
   Se muestra el menú desplegable Valor de metadatos.



2. Elija una de las opciones cambio de enfoque:
   El desglose se vuelve a enfocar según la opción elegida.

Observar un conteo específico en una nueva pestaña

Para ver un conteo de un valor de metadatos en una nueva pestaña o ver un geomap de las ubicaciones para el valor de metadatos seleccionado:

1. Haga clic con el botón secundario en el conteo de un valor de metadatos (el número de color verde después del valor de metadatos de color azul).
   Se muestra el menú contextual.
2. (Opcional) Para abrir una investigación por separado para el valor de metadatos específico, seleccione **Abrir en una nueva pestaña**.
3. (Opcional) Para abrir un geomap que muestra las ubicaciones donde se originó el valor de metadatos seleccionado, elija **Ubicaciones de Geomap en pestaña nueva**.

Ver y modificar consultas mediante la integración de URL

Investigation incluye una integración de URL externa que facilita la integración con productos de otros fabricantes, ya que permite una búsqueda contra la arquitectura de Security Analytics. Cuando utiliza una consulta en un URI, puede ir directamente desde cualquier producto que permita vínculos personalizados a un punto de desglose específico en la vista Investigation en Security Analytics. Esta integración proporciona una presentación interna de la consulta del usuario.

La integración de URL permite al usuario identificar el servicio, ya sea por el ID de host o por el servicio y el puerto, como se define en Security Analytics. Si Security Analytics no puede resolver el servicio, se redirige al analista a la vista Navegación, la cual muestra el cuadro de diálogo Selección de servicios. Una vez seleccionado el servicio, la vista Navegación se carga con el punto de desglose, definido por la consulta.

ID de servicio conocido

Cuando se conoce el ID del servicio que se usará para la investigación, el formato para ingresar un URI mediante una consulta con codificación URL es:

http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>

where

- <sa host: port> es la dirección IP o DNS, con o sin un puerto, según corresponda (SSL o no). Esta designación solo se necesita si el acceso está configurado sobre un puerto no estándar a través de un proxy.
- <deviceId> es el ID de servicio interno en la instancia de Security Analytics para el servicio que se consultará. El ID de servicio solo se puede representar como un entero. Puede

ver el ID de servicio pertinente en la URL cuando accede a la vista Investigation en Security Analytics. Este valor cambia según el servicio al cual se conecta para el análisis.

- <encoded query> es la consulta de Security Analytics con codificación de URL. El largo de la consulta está restringido por las limitaciones de HTML URL.
- <start date> y <end date> definen el rango de fechas para la consulta. El formato es <aaaa-mm-dd>T<hh:mm:ss>Z. Se requieren las fechas de inicio y finalización. Si no se proporciona ninguna fecha, se usan los valores predeterminados del usuario para ese servicio. Los rangos relativos (por ejemplo, última hora) no son compatibles con esta versión. Todas las horas se ejecutan como UTC.
  Por ejemplo:
  `http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Host y puerto conocidos

Cuando se conoce el host y el puerto del servicio que se usará para la investigación, el formato para ingresar un URI mediante una consulta con codificación URL es:

`http://<sa host:port>/investigation/<device host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>`

donde

- <sa host: port> es la dirección IP o DNS, con o sin un puerto, según corresponda (SSL o no). Esta designación solo se necesita si el acceso está configurado sobre un puerto no estándar a través de un proxy.
- **<device host:port>** es el host y el puerto de un servicio definido en la instancia de Security Analytics para el servicio que se consultará. Security Analytics intenta resolver el host y el puerto como un ID de servicio definido en Security Analytics.
- <encoded query> es la consulta de Security Analytics con codificación de URL. El largo de la consulta está restringido por las limitaciones de HTML URL.
- <start date> y <end date> definen el rango de fechas para la consulta. El formato es <aaaa-mm-dd>T<hh:mm:ss>Z. Se requieren las fechas de inicio y finalización. Si no se proporciona ninguna fecha, se usan los valores predeterminados del usuario para ese servicio. Los rangos relativos (por ejemplo, última hora) no están soportado en esta versión. Todas las horas se ejecutan como UTC.
  Por ejemplo:

```
http://localhost:9191/investigation/concentrator:50105/navigate/query
/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z
```

Ejemplos

Estos son ejemplos de consultas donde el servidor de SA es 192.168.1.10 y el ID de dispositivo está identificado como 2.

Toda actividad realizada el 12/03/13 entre las 5:00 y 06:00 a.m. con un nombre host registrado

- Tabla dinámica personalizada: `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

Toda actividad realizada el 3/12/2013 entre las 5:00 y 05:10 p.m. con tráfico http hacia y desde la dirección IP 10.10.10.3

- Tabla dinámica personalizada: `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Dirección con codificación diseccionada:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z`

Notas adicionales

Es posible que algunos valores no necesiten codificarse como parte de la consulta. Por ejemplo, normalmente se utiliza la IP src y dst para este punto de integración. Si aprovecha una aplicación de otros fabricantes para la integración de esta funcionalidad, es posible hacer referencia a ella sin aplicar la codificación.

Actuar conforme a un punto de desglose en la vista Navegar

En este tema se describen las acciones disponibles para los analistas que desean enviar un punto de desglose a una determinada forma de salida o que desean verlo desde otra perspectiva en la vista Investigation > Navegar.

Cuando se realiza una investigación en Security Analytics, hay varias acciones disponibles una vez que se obtiene un punto de desglose en la vista Navegar. Los analistas pueden:

- Exportar un punto de desglose.
- Imprimir el punto de desglose actual.
- Abrir la lista de eventos para un valor de metadatos.
- Iniciar una búsqueda externa de una clave de metadatos
- Iniciar un escaneo de Malware Analysis desde la vista Navegar.
- Ver el contexto adicional de un punto de datos
- Administrar listas y valores de lista de Context Hub en Investigation
- Visualizar el punto de desglose actual en Informer

Exportar un punto de desglose

En Security Analytics Investigation, cuando se muestran los datos para un punto de desglose en la vista Navegar, puede:

- Extraer archivos desde una sesión y escoger el tipo de archivos que desea extraer: archivos, BitTorrent de audio, documentos, archivos ejecutables, imágenes, otros, videos y archivos web.
- Exportar el punto de desglose como archivo de captura de paquete (PCAP) o archivo de registro.

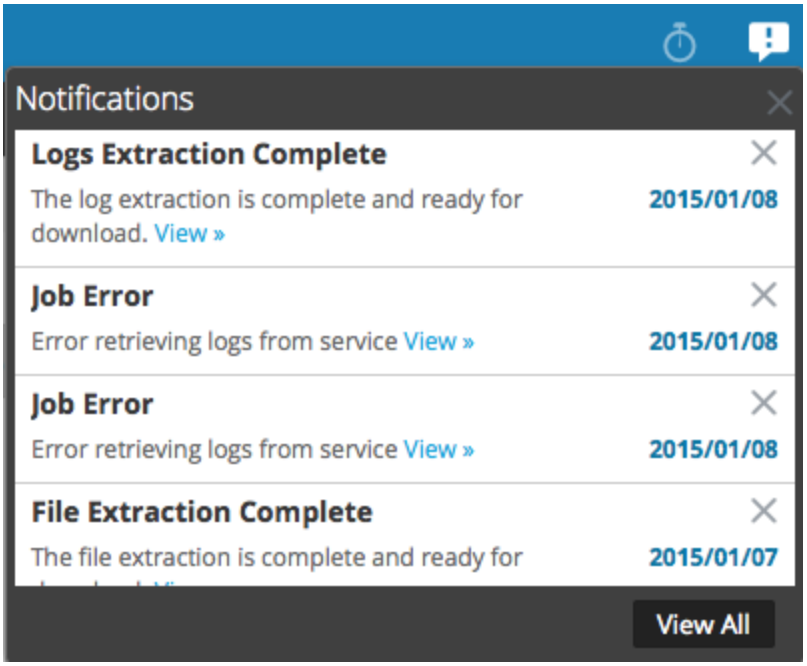
Los detalles que se exporten se verán afectados por el rango de tiempo y el punto de desglose en el momento de la exportación.

Nota: cuando exporta el punto de desglose como un archivo de registro, solo se exportan las sesiones de registro. El mensaje de la línea de espera de trabajos se refiere a la cantidad total de sesiones en el punto de desglose y no a la cantidad de registros. Por ejemplo, si el punto de desglose tiene 505 sesiones y solo cinco sesiones de registro, el mensaje de la línea de espera de trabajos indica que Security Analytics está extrayendo registros para 505 sesiones.

Para exportar un punto de desglose desde la vista Navegar:

1. Realice una investigación hasta llegar al punto de desglose deseado.
2. En la **barra de herramientas**, seleccione **Acciones > Exportar** y seleccione una de las opciones de exportación: Extraer archivos, Exportación de PCAP y Exportación de registros. Se extrae el punto de desglose y un mensaje aconseja calendarizar el trabajo. Puede revisar la página de trabajos para el estado.

3. Cuando se completa la extracción de archivos calendarizada, se muestra en la bandeja Notificaciones de trabajos.



4. Haga clic en el vínculo **Ver** para ver la Bandeja de trabajos y descargar el archivo de extracción específico solicitado.

Iniciar una búsqueda externa de una clave de metadatos

En este tema se proporcionan instrucciones para usar plug-ins de Investigation de manera inmediata con el fin de iniciar una búsqueda externa de claves de metadatos específicas mediante herramientas externas a Security Analytics durante la investigación de datos en las vistas Navegar o Eventos.

Los analistas pueden usar búsquedas externas de Security Analytics Investigation de manera inmediata para ahorrar tiempo durante las investigaciones. Las búsquedas de uso inmediato están disponibles cuando se hace clic con el botón secundario en una de estas claves de metadatos: Dirección IP (`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`), `host (alias-host, domain.dst)`, `client`, y `file-hash`.

En el caso de todas las claves de metadatos `IP` y `host`, las siguientes búsquedas están incorporadas en Security Analytics:

- Google Malware: abre una búsqueda en Google Malware en una nueva pestaña.
- McAfee SiteAdvisor: abre una búsqueda en McAfee SiteAdvisor en una nueva pestaña.
- Recopilación de DNS pasivo de BFK: abre una búsqueda en una recopilación de DNS pasivo de BFK en una nueva pestaña

- CentralOps Whois para direcciones IP y nombres de host: abre una búsqueda en CentralOps Whois de direcciones IP y nombres de host
- Búsqueda en Malwaredomainlist.com: abre una búsqueda en Malwaredomainlist.com en una nueva pestaña
- Búsqueda en Malwaredomains.com: abre una búsqueda en Malwaredomains.com en una nueva pestaña
- Búsqueda de dirección IP en Robtex: abre una búsqueda de dirección IP en Robtex en una nueva pestaña
- Búsqueda en SamSpade: abre una búsqueda en SamSpade en una nueva pestaña
- Búsqueda en ThreatExpert: abre una búsqueda en ThreatExpert en una nueva pestaña
- Búsqueda en UrlVoid: abre una búsqueda en UrlVoid en una nueva pestaña

Para las claves de metadatos `file-hash` y `alias-host`, la búsqueda en Google abre una búsqueda en Google en una nueva pestaña.

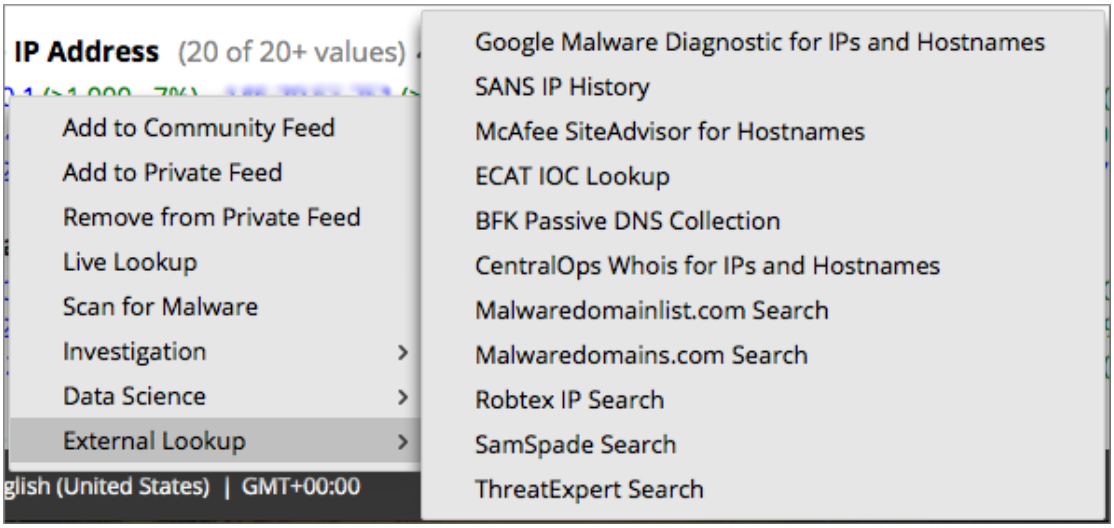
Para la clave de metadatos `client`, la opción Búsqueda en ECAT abre un cliente de ECAT en una nueva pestaña si este cliente está instalado en el mismo sistema en el cual se usa el navegador.

Los administradores pueden agregar búsquedas externas adicionales y otras acciones personalizadas, como se describe en "Agregar acciones de menú contextual personalizadas" en la *Guía de configuración del sistema*.

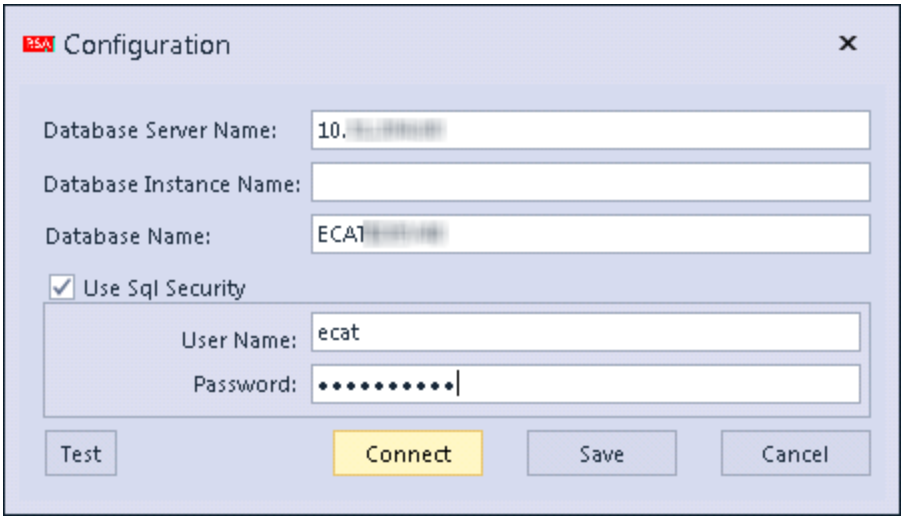
Iniciar una búsqueda de IOC en ECAT

Para iniciar una búsqueda de datos de ECAT en la vista Investigation > Navegar:

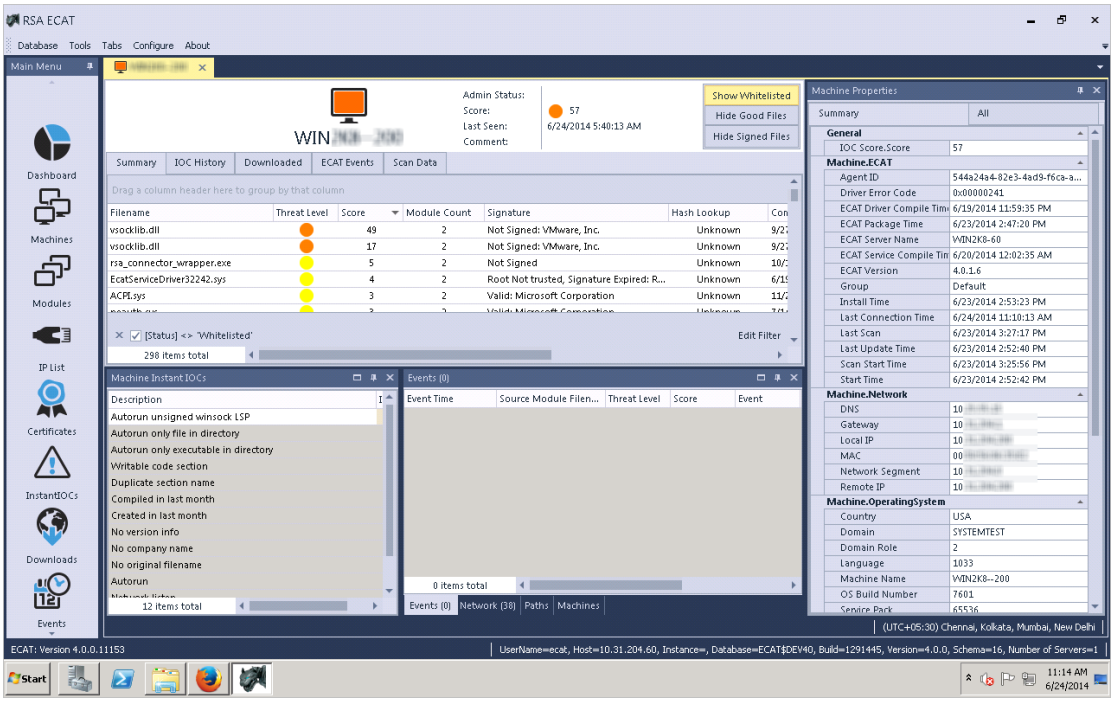
1. Haga clic con el botón secundario en un valor de metadatos para una de las siguientes claves de metadatos: `ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`, `alias-host`, `domain.dst`, `client`.
2. Seleccione **Búsqueda externa** en el menú contextual.
   Se muestra un submenú de opciones de la búsqueda externa.



3. Seleccione **Búsqueda de IOC en ECAT**.
   Un cuadro de diálogo solicita elegir una aplicación.
4. Seleccione ECAT y haga clic en **Aceptar**.
   Se muestra el cuadro de diálogo Configuración de RSA ECAT.



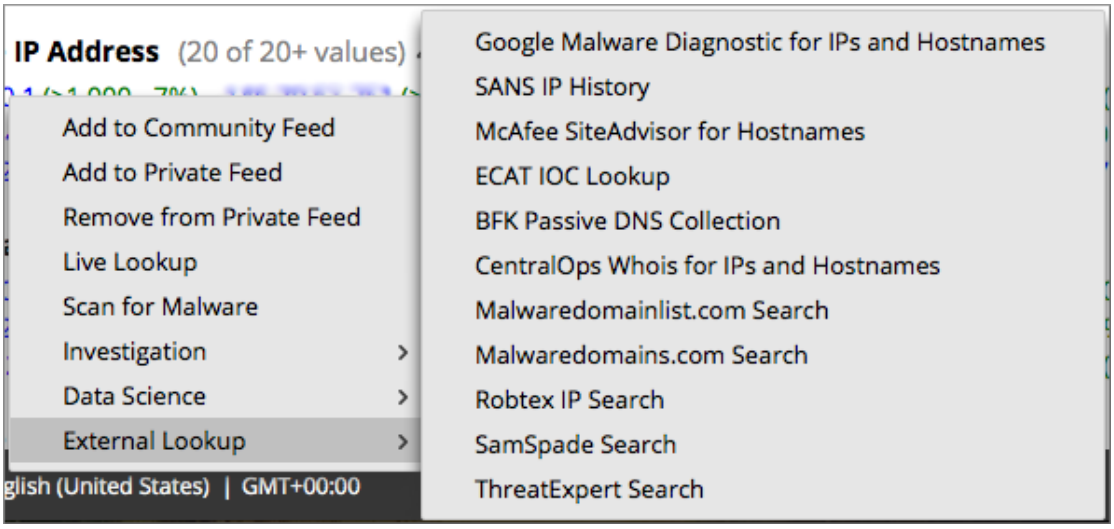
5. Ingrese el nombre de usuario y la contraseña que se requieren para iniciar sesión en el cliente de ECAT y haga clic en **Conectar**.
   El punto de desglose se abre en RSA ECAT.



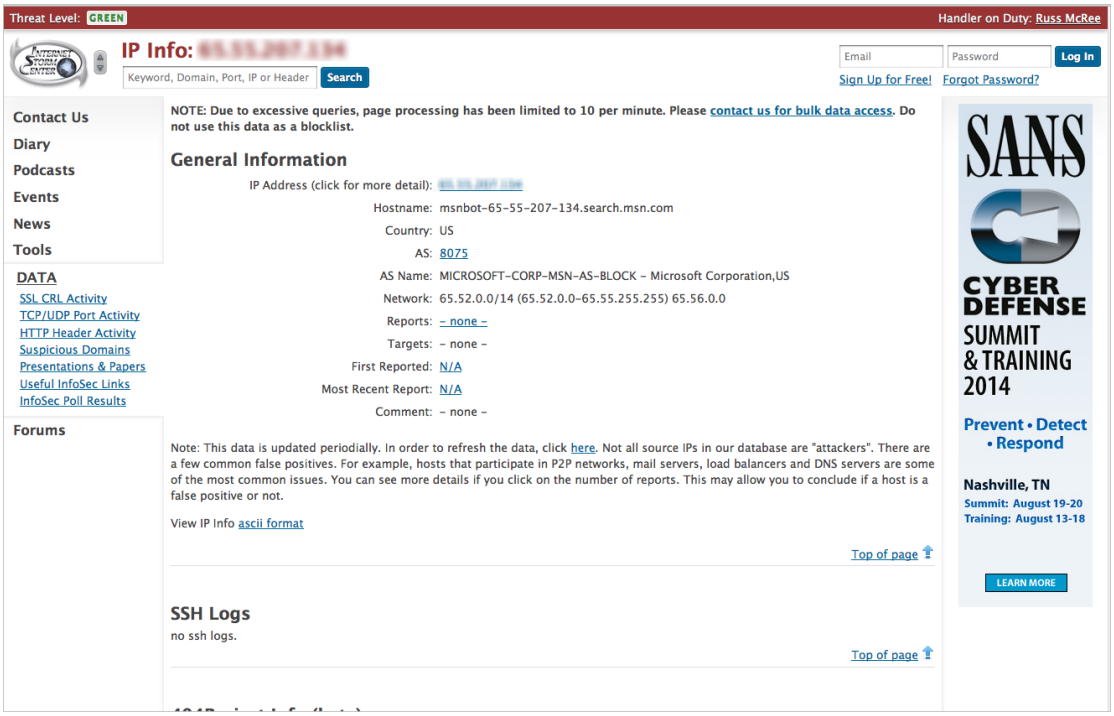
Iniciar otras búsquedas externas

Para iniciar una búsqueda externa de datos (distinta de IOC de ECAT) en la vista Investigation > Navegar:

1. Haga clic con el botón secundario en un valor de metadatos para una de las siguientes claves de metadatos: `ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`, `alias-host`, `domain.dst`, `client`.
2. Seleccione **Búsqueda externa** en el menú contextual.
   Se muestra un submenú de opciones de la búsqueda externa.



3. Seleccione una de las opciones de búsqueda.
   El valor de metadatos seleccionado se abre en la búsqueda seleccionada. Por ejemplo, si seleccionó Historial de IP SANS, la información del punto de desglose se muestra en SANS Internet Storm Center.

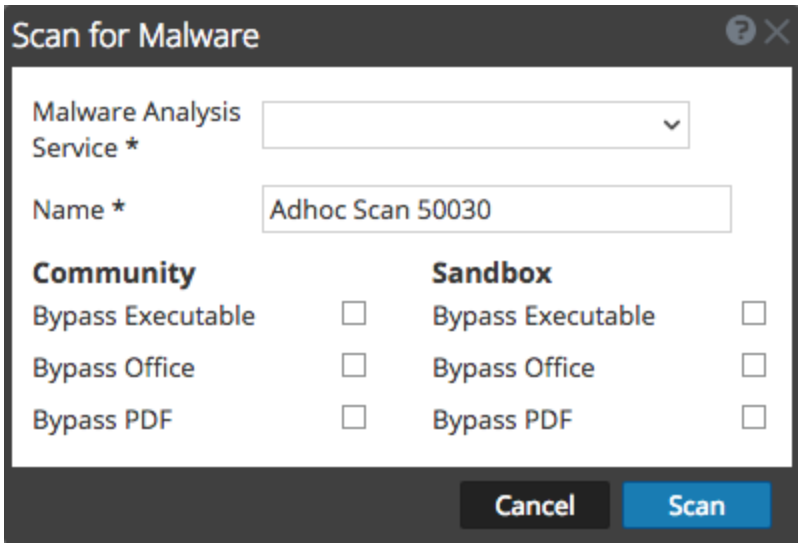


Iniciar un escaneo de Malware Analysis desde la vista Navegar

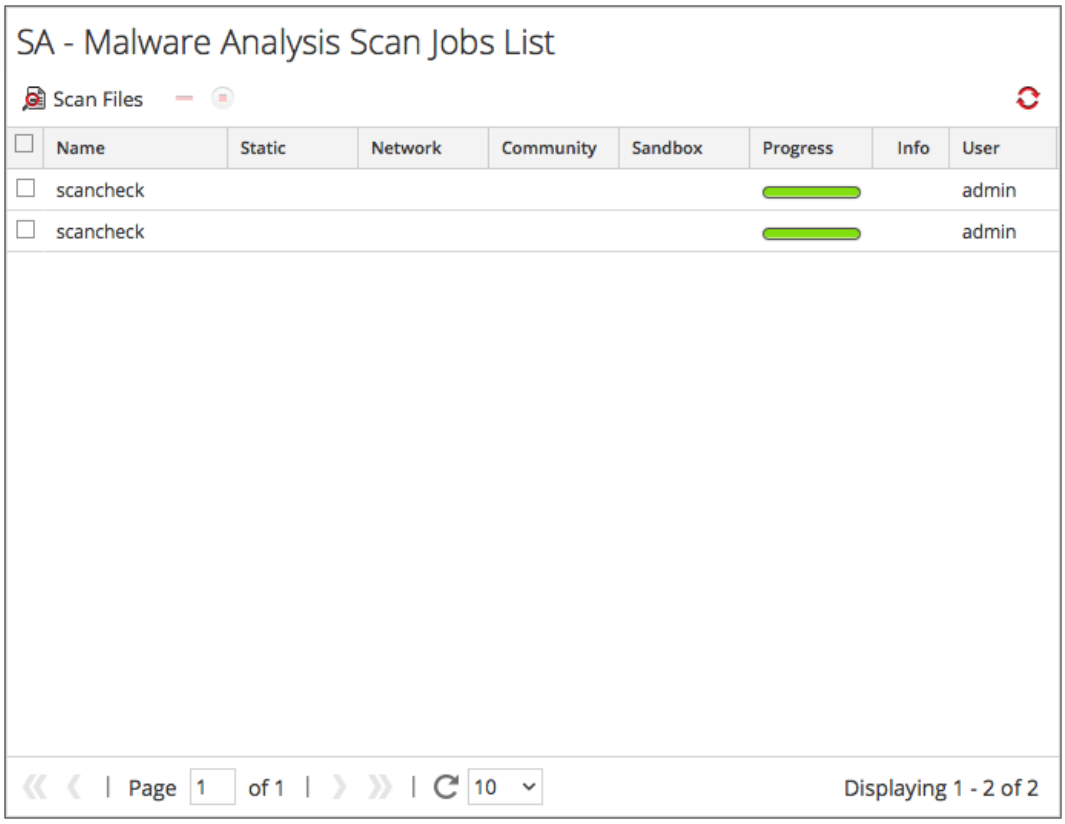
Desde Investigation, los analistas pueden iniciar un escaneo de Malware Analysis según demanda mediante la selección de un servicio y un valor de metadatos, así como de una opción del menú contextual. Cuando finaliza el sondeo, los datos escaneados están disponibles para Malware Analysis.

Para iniciar un escaneo de datos de Malware Analysis en la vista Investigation > Navegar:

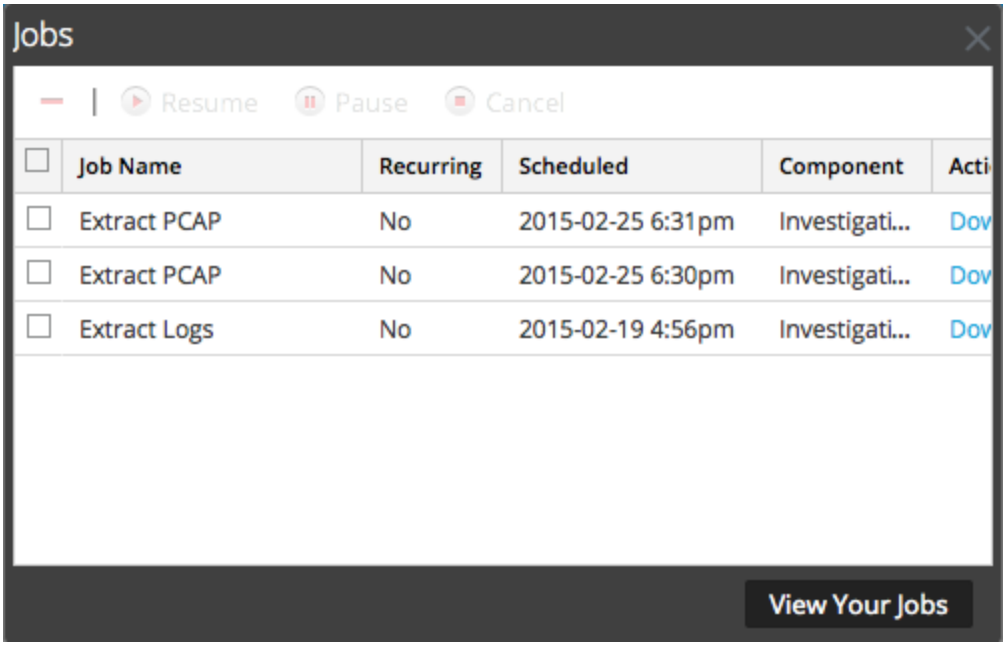
1. Haga clic con el botón secundario en un valor de metadatos (por ejemplo, OTHER, DNS o FTP) y seleccione **Escanear para encontrar malware** en el menú contextual.
   Se muestra el cuadro de diálogo Escanear para encontrar malware con un nombre sugerido para el escaneo según demanda y ningún servicio seleccionado.
2. En el cuadro de diálogo Escanear para encontrar malware, seleccione un servicio para ejecutar el escaneo, edite el nombre y seleccione los tipos de archivos que desea omitir en Community y Sandbox.



3. Haga clic en **Escanear**.
   La solicitud de escaneo se agrega al dashlet Lista de trabajos de escaneo y a la bandeja de trabajos. La configuración de omisión en este cuadro de diálogo reemplaza a la configuración predeterminada definida en los ajustes de configuración básicos de Malware Analysis.
4. Para ver los trabajos, realice una de las siguientes acciones:
   a. Navegue a la Lista de trabajos de escaneo en la vista Malware Analysis o en el tablero Unified. Haga doble clic en un escaneo para verlo.



b. Para ver el trabajo en la bandeja de trabajos, haga clic en en la barra de herramientas de Security Analytics. Cuando el trabajo finalice, desplácese a la izquierda y haga clic en **Ver**.



Se muestra el Resumen de eventos de malware del escaneo seleccionado. El escaneo

también se agrega a la lista de escaneos disponibles en el cuadro de diálogo para seleccionar escaneos en la pestaña Investigation > Malware.

Administrar listas y valores de lista de Context Hub en Investigation

Los analistas pueden agregar listas y valores de lista para el enriquecimiento de Context Hub en las vistas de Investigation. El servicio Context Hub se incluye en RSA Security Analytics 10.6 y versiones superiores.

Cuando el servicio Context Hub está habilitado y configurado, Security Analytics proporciona datos de enriquecimiento desde Incident Management, listas personalizadas y ECAT directamente en las vistas Navegar y Eventos. Una indicación visual destaca los valores de metadatos para los cuales los datos de enriquecimiento están disponibles en las vistas de Investigation y puede hacer clic en el valor destacado para buscar la información contextual e inteligencia.

Además, desde el panel Valores en las vistas Navegar y Eventos, puede ver listas, editar valores de metadatos en una lista existente o crear una nueva lista. Cuando agrega valores de metadatos a una lista, puede investigar los valores de metadatos con la opción de búsqueda de contexto.

Requisitos previos

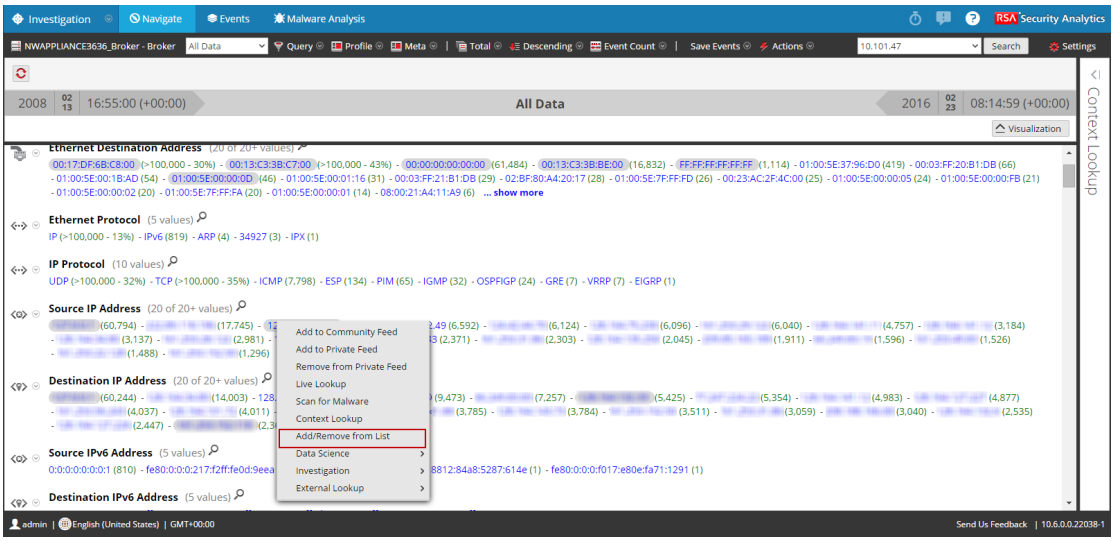
Para que un analista administre listas en Investigation, el administrador debe:

- Habilitar el servicio Context Hub.
- Asignar una función de analista con permiso `Manage List from Investigation` al usuario que llevará a cabo la búsqueda de contexto en las vistas de Investigation.
- Configurar funciones y permisos adecuados, como se describe en "Permisos de funciones" y "Administrar usuarios con funciones y permisos" en la *Guía de administración de usuarios y seguridad del sistema*.

Agregar valores de metadatos a una lista existente

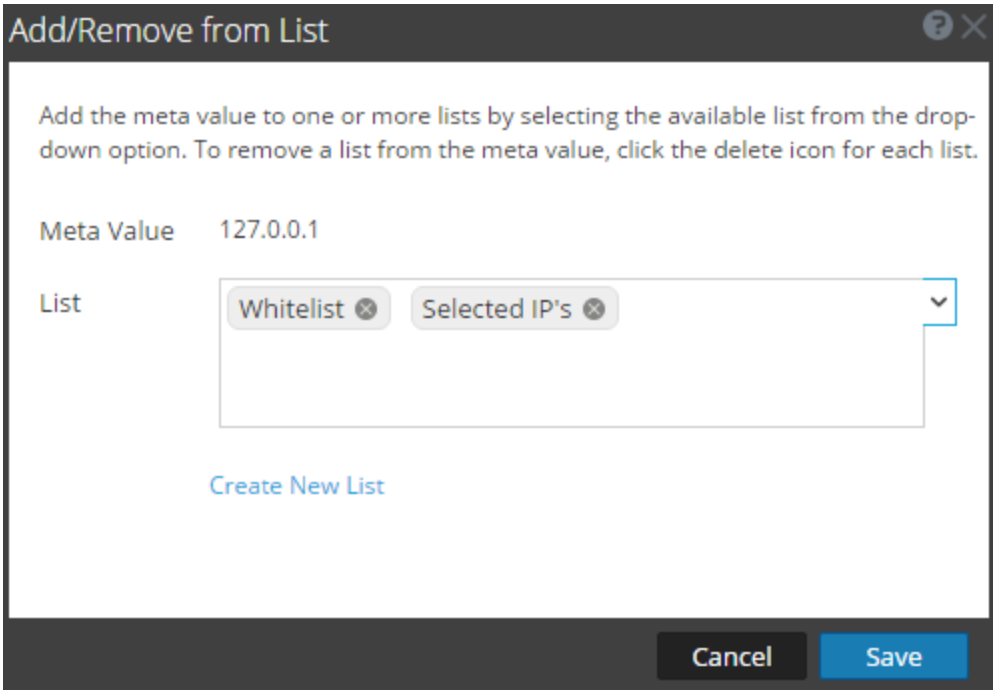
Para agregar valores de metadatos a una lista existente en Context Hub:

1. Mientras investiga un servicio en la vista **Navegar**, haga clic con el botón secundario en un valor de metadatos (por ejemplo, valores bajo Dirección IP de origen, Dirección IP de destino o Nombre de usuario) y seleccione **Agregar/eliminar de la lista** en el menú contextual.



Se muestra el cuadro de diálogo Agregar/eliminar de la lista.

2. En el campo **Lista**, seleccione una o más listas de la opción de menú desplegable al cual se debe agregar el valor de metadatos.



3. Haga clic en **Guardar**.
   El valor de metadatos se agrega a las listas seleccionadas.

Quitar un valor de metadatos de una lista de Context Hub en Investigation

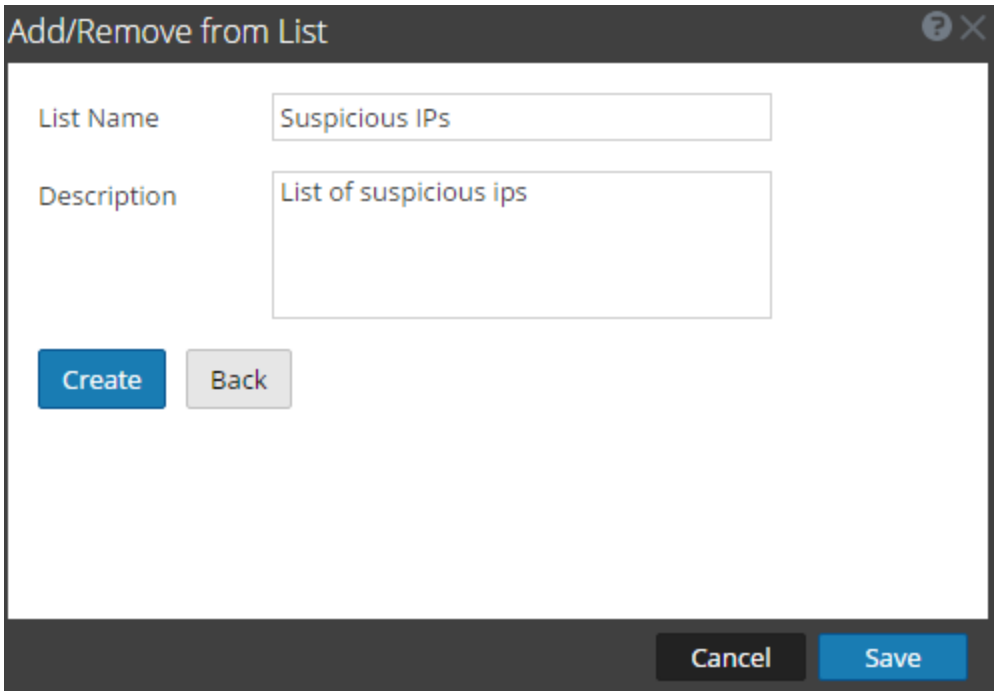
Para quitar un valor de metadatos de la lista:

1. En el cuadro de diálogo **Agregar/eliminar de la lista**, en el campo **Lista**, vea las listas que incluyen el valor de metadatos.
2. Haga clic en el icono Eliminar (x) de cada lista que no debe incluir el valor de metadatos.
3. Haga clic en **Guardar**.
   El valor de metadatos se elimina de la lista eliminada.

Crear una nueva lista en Investigation

Para crear una lista de Context Hub en Investigation:

1. En el cuadro de diálogo **Agregar/eliminar de la lista**, haga clic en **Crear lista nueva**.



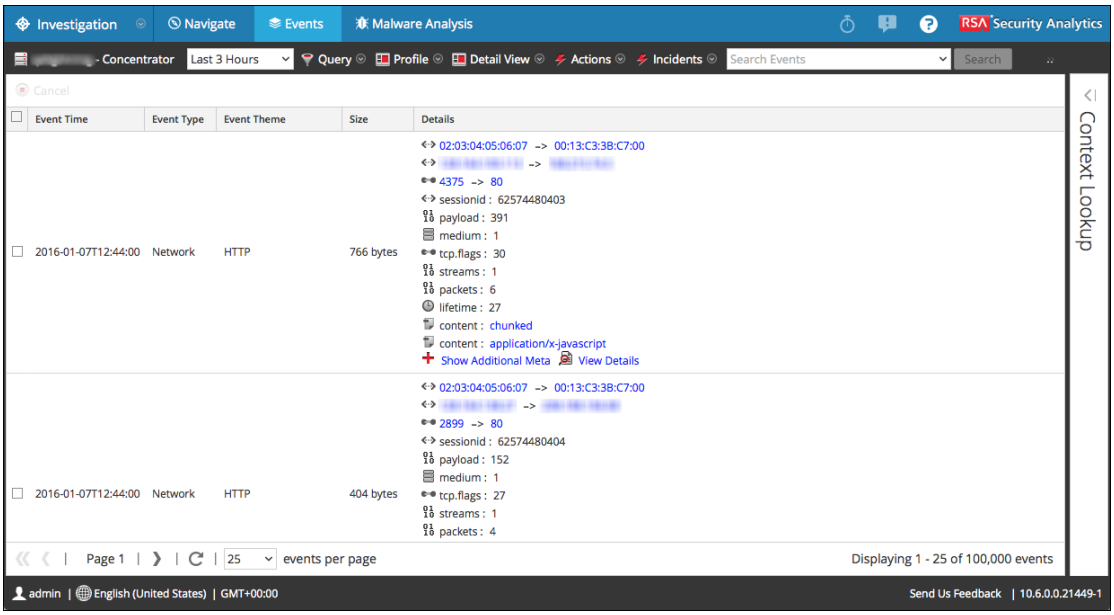
2. En el campo **Nombre de lista**, ingrese un nombre único para la lista.
3. En el campo **Descripción**, ingrese una descripción de la lista.
4. Haga clic en **Crear** para crear la lista.
5. Haga clic en **Guardar** para agregar el valor de metadatos a la lista creada.
   Estas listas se consideran orígenes de datos para la recuperación de información de contexto.

Abrir la lista de eventos

Los analistas pueden ver una lista de eventos asociada a una sesión en Investigation > vista Eventos.

Existen dos maneras de mostrar la vista Eventos:

1. Seleccione **Investigación > Eventos** en el menú de **Security Analytics**. Security Analytics ejecuta una consulta predeterminada acerca de las últimas tres horas para el servicio predeterminado (si hay uno configurado) o muestra un cuadro de diálogo en el cual puede seleccionar un servicio y, a continuación, ejecuta la consulta predeterminada. La consulta predeterminada selecciona todos los eventos y la vista Eventos muestra los pertinentes al servicio seleccionado, con los más antiguos en primer lugar.
2. En la vista **Navegar**, haga clic en un valor de metadatos que represente un evento. La vista Eventos muestra los eventos en el servicio seleccionado según el punto de desglose en la vista Navegar. La vista Eventos proporciona tres presentaciones incorporadas de datos de eventos: la Vista detallada, la Vista de lista y la Vista de registro.



Puede utilizar consultas, la configuración del rango de tiempo y perfiles para filtrar los eventos mostrados en la vista Eventos. Desde cualquier tipo de vista de la vista Eventos, puede extraer archivos, exportar eventos, exportar registros y abrir el panel Reconstrucción de evento si hace doble clic en un evento. Consulte Examinar eventos para ver información detallada acerca de estas capacidades.

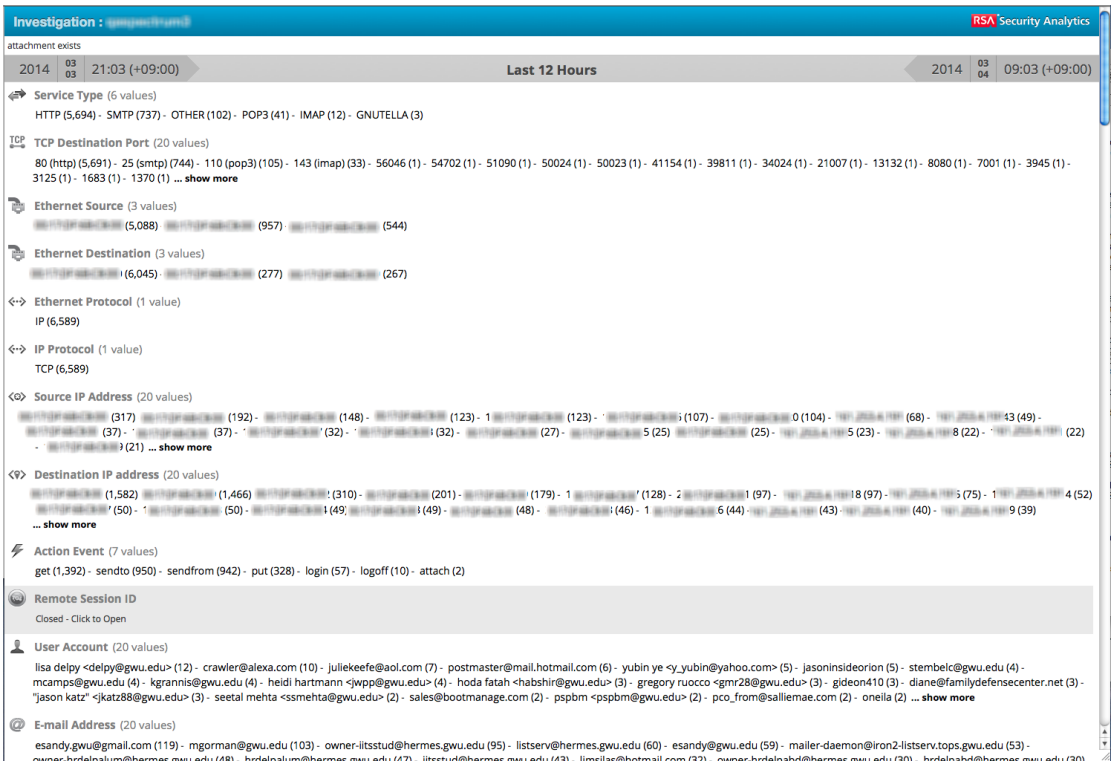
Imprimir el punto de desglose actual

La vista Investigation > Navegar permite mostrar el contenido del punto de desglose actual en formato para impresión en la ventana del navegador.

Para mostrar el punto de desglose en una vista de impresión:

1. Con un punto de desglose abierto en la vista **Investigation >Navegar,** seleccione **Acciones > Imprimir** en la barra de herramientas.

   Se crea una nueva pestaña con la vista de impresión del punto de desglose actual.



2. Use la opción de impresión en el navegador para enviar la vista imprimible a la impresora.

Visualizar el punto de desglose actual en Informer

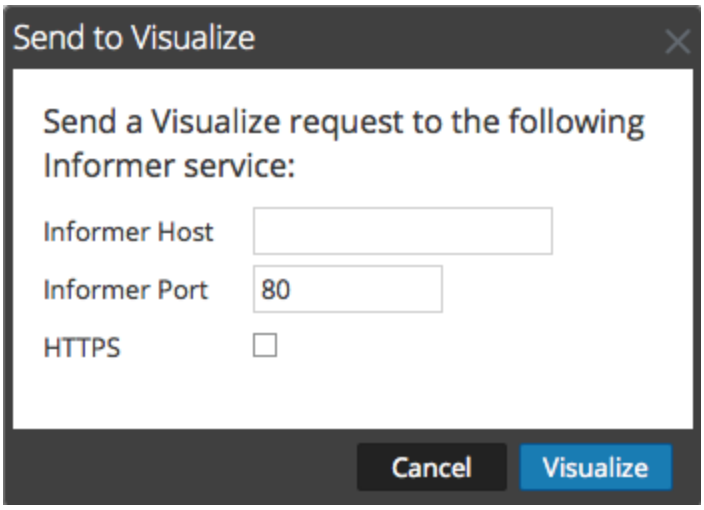
En este tema se proporcionan instrucciones para enviar un punto de desglose en la vista Investigation > Navegar a una visualización de Informer.

Informer debe estar instalado en la red y el servicio que se está investigado debe poder acceder a él. Debe proporcionar el nombre de host y el puerto utilizado en el host de Informer para comunicarse con Security Analytics.

Para mostrar una visualización en Informer del punto de desglose actual:

1. Con un punto de desglose abierto en la vista Investigation > Navegar, haga clic en **Acciones > Visualizar**.

   Se muestra el cuadro de diálogo Enviar a visualización.



2. Escriba el nombre de host o la dirección IP de Informer y verifique el puerto del servidor de Security Analytics que se utiliza para comunicarse con el host de Informer.
3. (Opcional) Seleccione la opción HTTPS si el host de Informer utiliza comunicaciones seguras.
4. Haga clic en **Visualizar**.
   La visualización se muestra en una pestaña nueva.

Ver el contexto adicional de un punto de datos

Cuando se realiza una investigación en la vista Navegar o en la vista Eventos, los analistas pueden buscar información de contexto adicional e inteligencia para un punto de datos o un valor de metadatos en diversos orígenes configurados como, por ejemplo, ESA.

Un analista con permiso `Context Lookup` puede realizar la búsqueda de contexto en las vistas de Investigation. Un administrador debe configurar funciones y permisos como se describe en "Permisos de funciones" y "Administrar usuarios con funciones y permisos" en la *Guía de administración de usuarios y seguridad del sistema*.

Para realizar la búsqueda de contexto, el administrador debe:

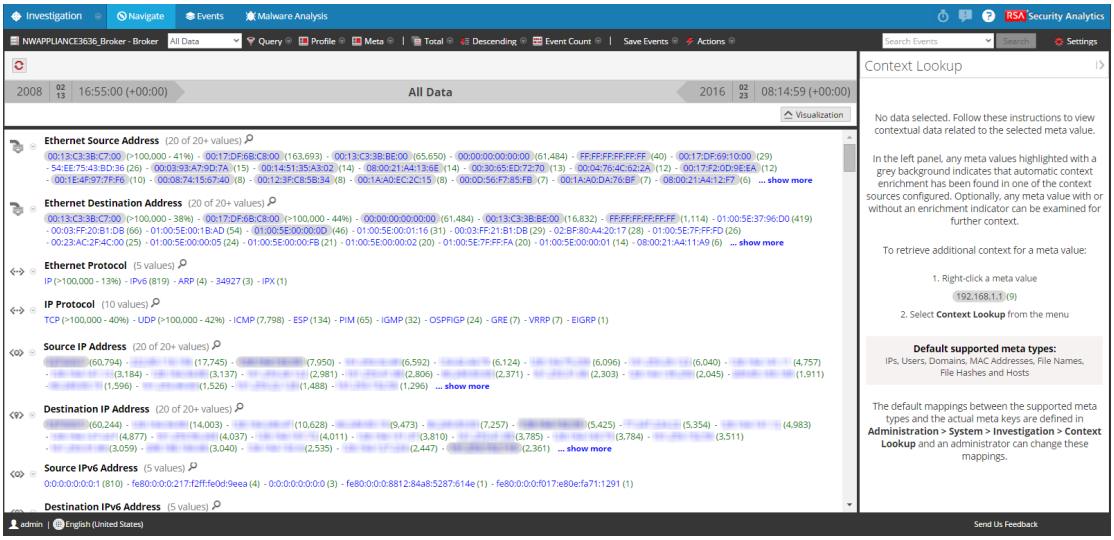
- Agregar el servicio Context Hub en Security Analytics. (El servicio Context Hub se incluye en Security Analytics 10.6 y superior).
- Configurar orígenes de datos para el servicio Context Hub como se describe en la *Guía de configuración de Context Hub*.

Ver el contexto adicional mediante búsqueda de contexto

Para ver el contexto adicional de un punto de datos en las vistas de Investigation:

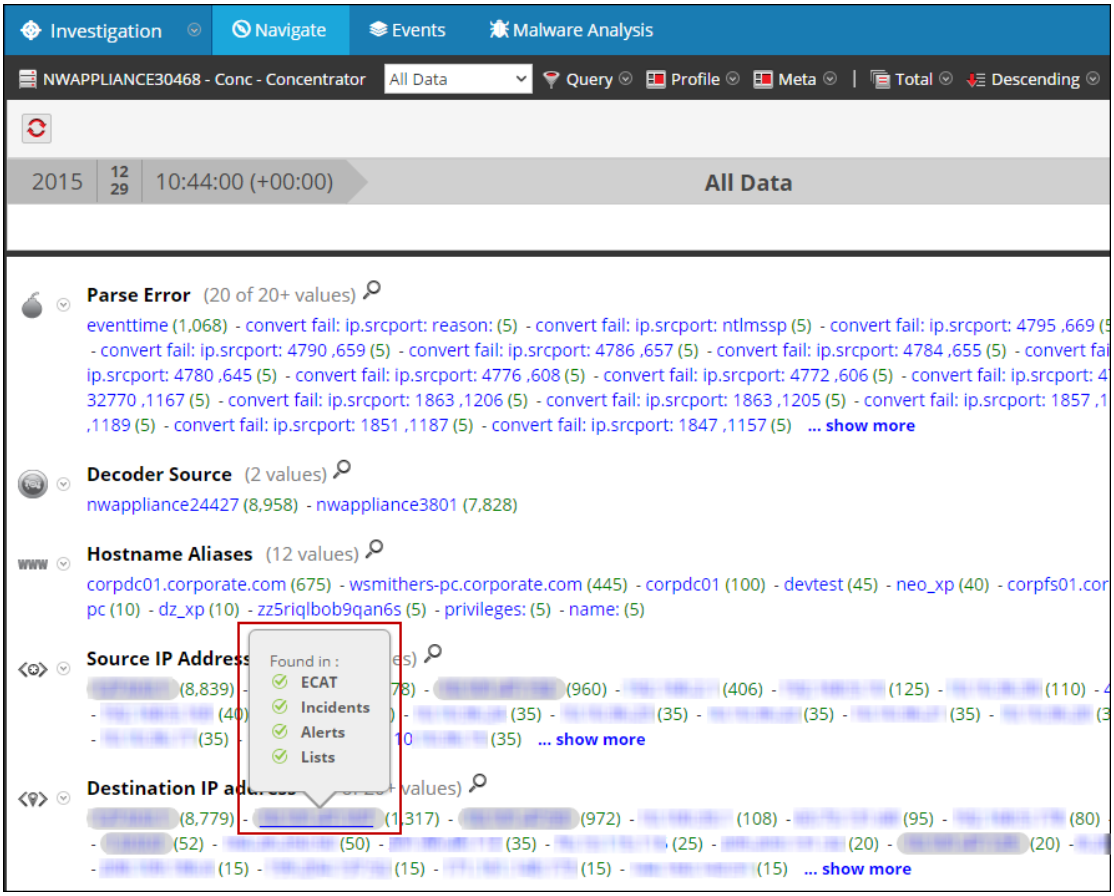
1. Mientras realiza una investigación o un análisis de eventos en el menú de **Security Analytics**, vaya a la vista Navegar.

   La vista Navegar tiene el panel Valores a la izquierda y el panel Búsqueda de contexto a la derecha, como se muestra a continuación. El panel Búsqueda de contexto no muestra ningún dato hasta que se realiza una búsqueda de contexto. Los valores de metadatos que tienen información de contexto asociada se resaltan con un fondo de color gris.

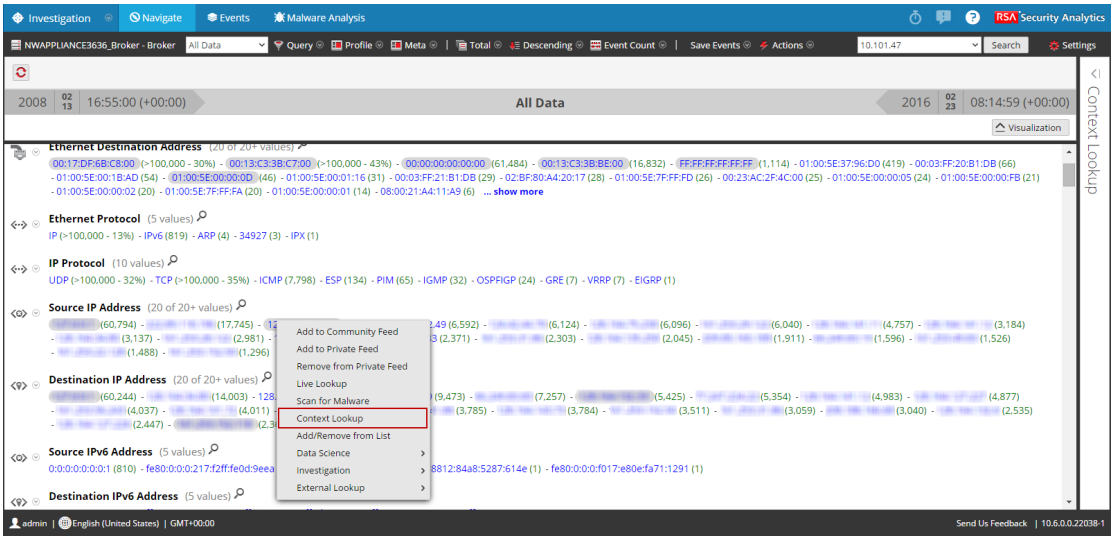


2. Para ver el tipo de datos de contexto que está disponible para un valor de metadatos resaltado, mantenga el mouse sobre un valor de metadatos resaltado.

   Un indicador de en línea muestra qué tipo de datos de contexto están disponibles para los metadatos: ECAT, incidentes, alertas o listas.



3. Para ver los datos de búsqueda de contexto del panel Valores, haga clic con el botón secundario en un valor de metadatos resaltado y seleccione **Búsqueda de contexto** en el menú contextual.



El panel Búsqueda de contexto muestra los resultados de búsqueda en función de los datos disponibles en los orígenes configurados.

Nota: El indicador de en línea para los valores de metadatos solo es compatible en la vista Navegar. Para la vista Eventos, debe realizar una búsqueda según demanda con respecto a los valores de metadatos.

Ver los resultados del panel Búsqueda de contexto

En el panel Búsqueda de contexto, puede ver los resultados de búsqueda y explorar datos individuales para una investigación más profunda. Por ejemplo, cuando hace clic en un determinado valor de incidentes, los detalles de los incidentes se muestran en la vista Incident Management.

Para obtener una descripción detallada de la información que se muestra en el panel Búsqueda de contexto, consulte Investigation: Panel Búsqueda de contexto.

Examinar eventos

Los analistas que investigan datos en Investigation pueden ver y reconstruir eventos asociados con una sesión.

- Los analistas que realizan análisis con Security Analytics Investigation y que tienen configuradas las funciones y los permisos del sistema adecuados para sus cuentas de usuario, pueden ir desde el punto de desglose de la vista Navegar a la vista Eventos.
- Los analistas que no tienen acceso a la vista Navegar o que desean ir directamente a la vista Eventos, pueden abrir sesiones y examinar los eventos que componen la sesión en Investigation > pestaña Eventos.

Cada tema describe los métodos de trabajo en la vista Eventos.

- Combinar eventos desde sesiones divididas
- Exportar eventos y extraer archivos
- Filtrar y buscar resultados en la vista Eventos
- Administrar grupos de columnas en la vista Eventos
- Reconstruir un evento

Combinar eventos desde sesiones divididas

Los analistas pueden identificar sesiones que se dividieron debido a su tamaño en la vista Eventos, y combinar las sesiones fragmentadas de modo que se pueda ver la sesión completa como un único resultado de consulta en la vista Eventos. Cuando las sesiones divididas se vuelven a combinar, una única exportación de paquete de la sesión en la vista Eventos incluye todos los fragmentos de la sesión.

La versión 10.4 y los Decoders anteriores están configurados con un tamaño de sesión predeterminado de 32 MB. Cuando una sesión supera el límite de 32 MB, el Decoder la divide y todos los paquetes subsiguientes pasan a ser parte de una nueva sesión, lo cual fragmenta la sesión de red real en varias sesiones de Decoder. Las sesiones divididas se analizan sin el contexto de que es un fragmento de la sesión de red más grande, lo cual a veces da como resultado fragmentos de sesiones con direcciones y puertos de origen y destino invertidos y con protocolos de aplicación no identificados. Otro resultado de las sesiones divididas puede ser la dificultad de ver todos los fragmentos de una sesión como un único resultado de consulta o de crear la exportación de un paquete de todos los fragmentos de la sesión.

Las mejoras de Decoder en Security Analytics 10.5 brindan un procesamiento mejorado de las sesiones fragmentadas:

- Análisis contextual de fragmentos.
- Resaltado de fragmentos de sesión.
- Búsqueda de fragmentos de sesiones.
- Exportación de todos los paquetes a una única PCAP.

Análisis contextual de fragmentos

En Security Analytics 10.5 y superior, el Decoder completa el análisis de sesiones antes de dividir la sesión según el tamaño máximo de sesión configurado (32 MB) o el tiempo de espera configurado (60 segundos). Cuando se completa el análisis, los resultados analizados incluyen la direccionalidad y el protocolo de aplicación correctos, los cuales se propagan a cada fragmento de sesión subsiguiente para garantizar la coherencia con la sesión de red lógica que representan.

Nota: Todos los cambios en la configuración de Decoder necesarios se realizan cuando se actualiza a 10.5. Sin embargo, Buscar fragmentos de sesión requiere que las claves de metadatos de los puertos de origen tcp y udp (tcp.srcport y udp.srcport) estén totalmente indexadas, lo cual no era la configuración predeterminada antes de 10.5. Esto limita funcionalmente la capacidad de buscar fragmentos de sesión en sesiones capturadas después de la actualización de Decoder a 10.5.

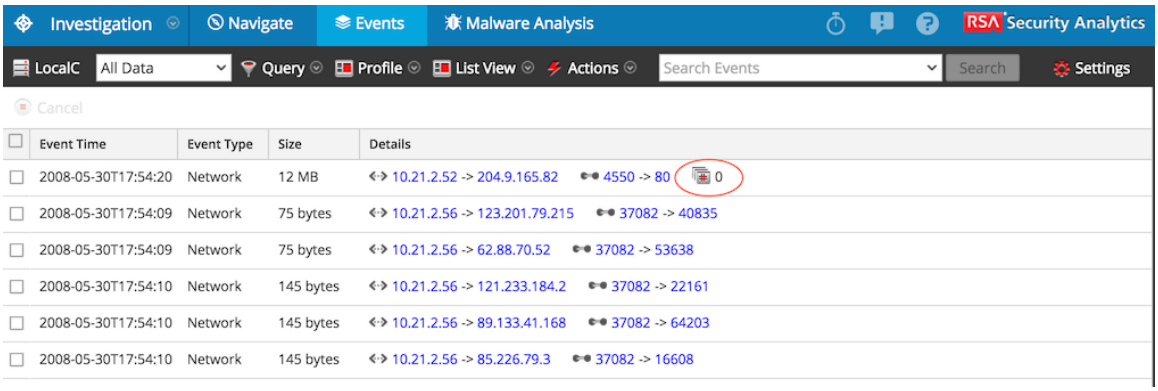
Resaltado de fragmentos de sesión

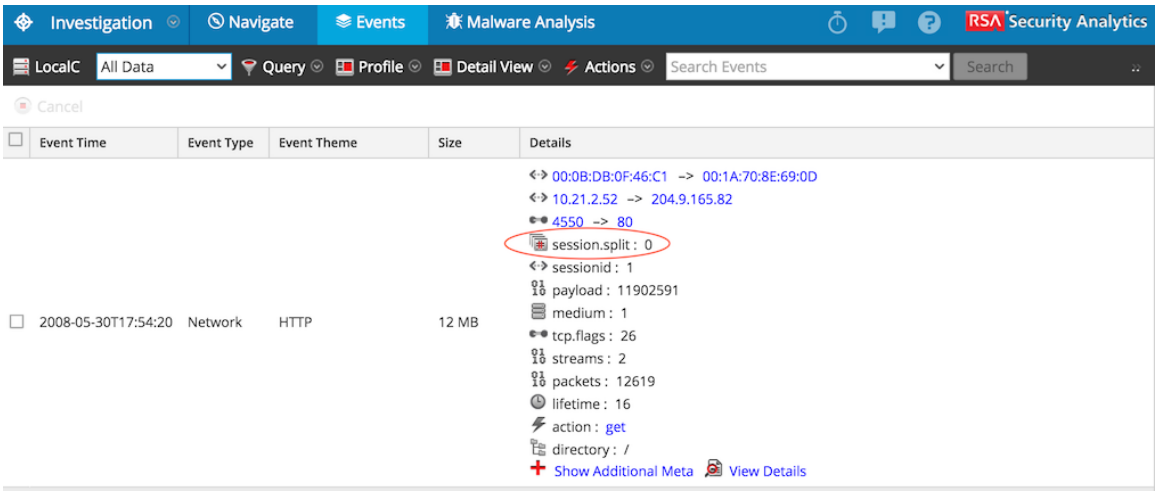
Cada fragmento de sesión tiene metadatos adicionales, `session.split`. El valor de los metadatos `session.split` para un fragmento de sesión específico indica cuántos fragmentos preceden a ese fragmento. Cuando se ven sesiones en la vista Eventos, los metadatos `session.split` identifican claramente las sesiones que son fragmentos en la vista Lista de eventos y en la vista Detalles de eventos.

La división de la sesión se produce cuando se alcanzan los valores de `assembler.size.max` o `assembler.timeout.session` (latencia entre sesiones) configurados del Decoder. El primer fragmento es la sesión 0 y las sesiones con un registro de fecha y hora posterior se numeran incrementalmente 1, 2, 3, etc. Los metadatos `session.split` indican la cantidad de fragmentos de sesión precedentes; sin embargo, no siempre indican que hay fragmentos de sesión subsiguientes, incluso con un valor de 0. También es posible que el primer fragmento de la sesión no tenga los metadatos `session.split` si la sesión se analiza antes de que se supere su tamaño máximo.

Después de ver los fragmentos de la sesión, puede determinar el tamaño máximo o el tiempo de espera agotado de la sesión necesarios para el análisis con el fin de volver combinar las sesiones divididas en una sola. Por ejemplo, si tiene cuatro fragmentos de 32 MB, debe configurar el Decoder de prueba (generalmente una máquina virtual configurada por separado del servicio de producción principal) con un tamaño máximo de sesión mayor que 128 MB. Los pasos son los mismos para todos los fragmentos en función de un tiempo de espera agotado de sesión. En las siguientes figuras se muestra la vista Lista de eventos y la vista Detalles de eventos con la información de sesión fragmentada resaltada.

Nota: cuando se crearon las siguientes capturas de pantalla, estaba configurado un tamaño máximo de sesión de 12 MB.





Los metadatos `session.split` se muestran siempre inmediatamente después de los metadatos de dirección y puerto en la vista de detalles. Nunca se ocultan como metadatos adicionales.

Estas mejoras permiten hacer lo siguiente de manera rápida:

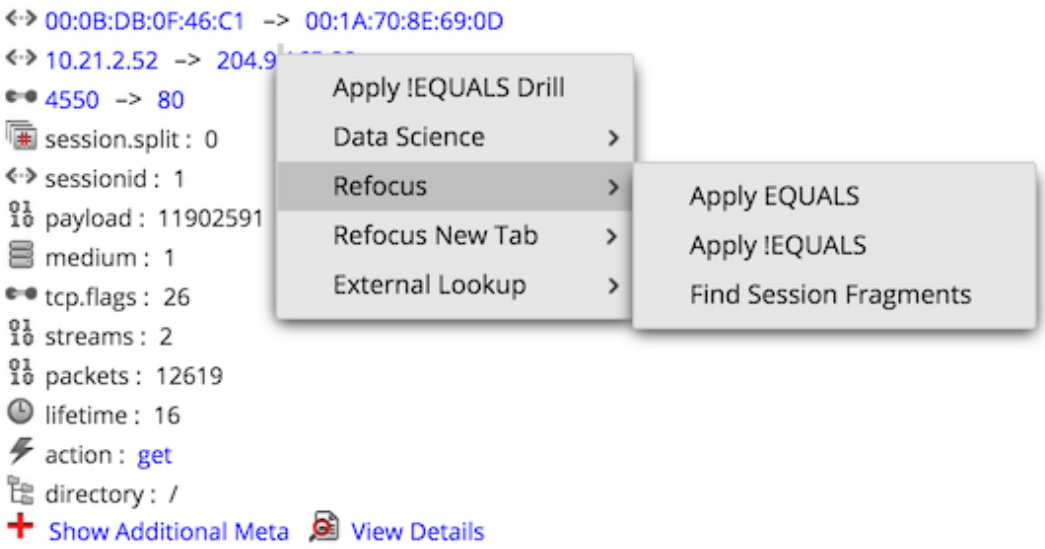
1. Identificar sesiones que son fragmentos de sesiones de red.
2. Ver todos los fragmentos de una sesión de red o un único fragmento de sesión.
3. Exportar los paquetes de la sesión de red completa como un único archivo PCAP.

Buscar y combinar fragmentos

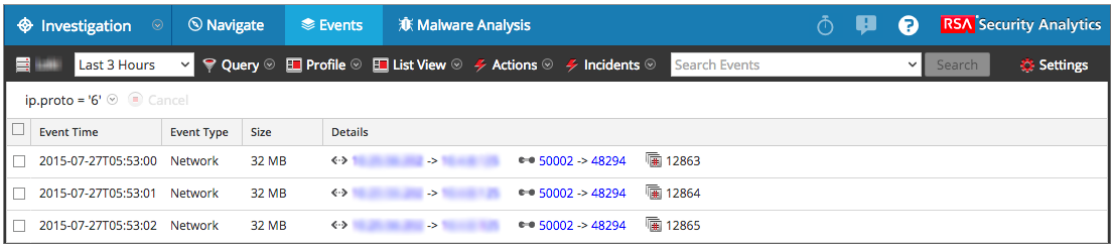
Dentro de la vista Eventos, puede buscar fragmentos de una sesión mediante la opción del menú contextual Reenfocar > Buscar fragmentos de sesión. Security Analytics crea una consulta con el uso de las direcciones y los puertos de origen y destino de la sesión seleccionada y muestra todas las sesiones que coinciden con esa consulta en la ventana de tiempo actual.

Para buscar fragmentos de sesión:

1. En **Investigation > vista Eventos**, haga clic con el botón secundario en cualquiera de los valores de dirección y puerto de origen y destino: (`ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport` y `udp.dstport`), así como en valores `session.split`.
   Se muestra el menú contextual.



2. Seleccione **Reenfocar > Buscar fragmentos de sesión** o **Reenfocar pestaña nueva > Buscar fragmentos de sesión**.
   Security Analytics vuelve a llenar la lista de eventos con fragmentos de sesión para una única sesión dentro del rango de tiempo actual. Según la opción que seleccionó, el reenfoque reemplaza a la vista actual o se abre en una nueva pestaña. (En estos ejemplos se usan todos los datos, pero esto no se recomienda en sistemas de producción).



3. Si es necesario, ajuste el rango de tiempo para incluir los fragmentos de sesión que pueden preceder o seguir a la ventana de tiempo actual. Puede determinar que es necesario ampliar el rango de tiempo si los fragmentos ocurren cerca del límite de tiempo, en especial si el primer fragmento visible no tiene un valor de división de 0 (o ninguno). Como alternativa, la inspección de los paquetes de la última sesión visible puede hacerlo pensar que la sesión continúa. El siguiente es un ejemplo:

   a. Si observa fragmentos que obviamente no corresponden al primero, por ejemplo, 1, 2, 3 y 4 en el rango de tiempo entre las 10:30 y las 10:35 h, debe haber un fragmento 0. Puede aumentar el rango de tiempo de modo que comience más temprano (en este ejemplo, 10:25 h) con el fin de buscar el fragmento adicional.

b. Si el tamaño de la sesión del último fragmento se acerca al tamaño máximo (12 MB en este ejemplo), busque fragmentos adicionales mediante el aumento de la ventana de tiempo para incluir una hora posterior (en este ejemplo, 10:40 h).
Cuando todos los fragmentos de una sesión de red se incluyen en una única lista Eventos, la lista puede abarcar varias páginas.

4. (Opcional) Para exportar los paquetes de cada fragmento de la sesión a un único archivo PCAP, seleccione **Acciones > Exportar todas las PCAP**.
Un mensaje le informa que el PCAP se está descargando. Cuando se completa la descarga, el archivo PCAP incluye la sesión de red completa que se fragmentó.

Exportar eventos y extraer archivos

Cuando los analistas están viendo una reconstrucción de evento en Security Analytics Investigation, el menú Acciones tiene una opción para extraer archivos del evento que se está visualizando y exportarlos a un archivo.

Nota: solo puede exportar archivos de sesión a los cuales puede acceder o que tiene permiso para ver.

La función de exportación de archivos consulta al servicio todas las sesiones dentro del rango de tiempo y el punto de desglose seleccionados para extraer el contenido de cada sesión. El rango de tiempo y el punto de desglose en el momento de la exportación afectan los detalles que se exportan. En el cuadro de diálogo Extracción de archivo, puede seleccionar:

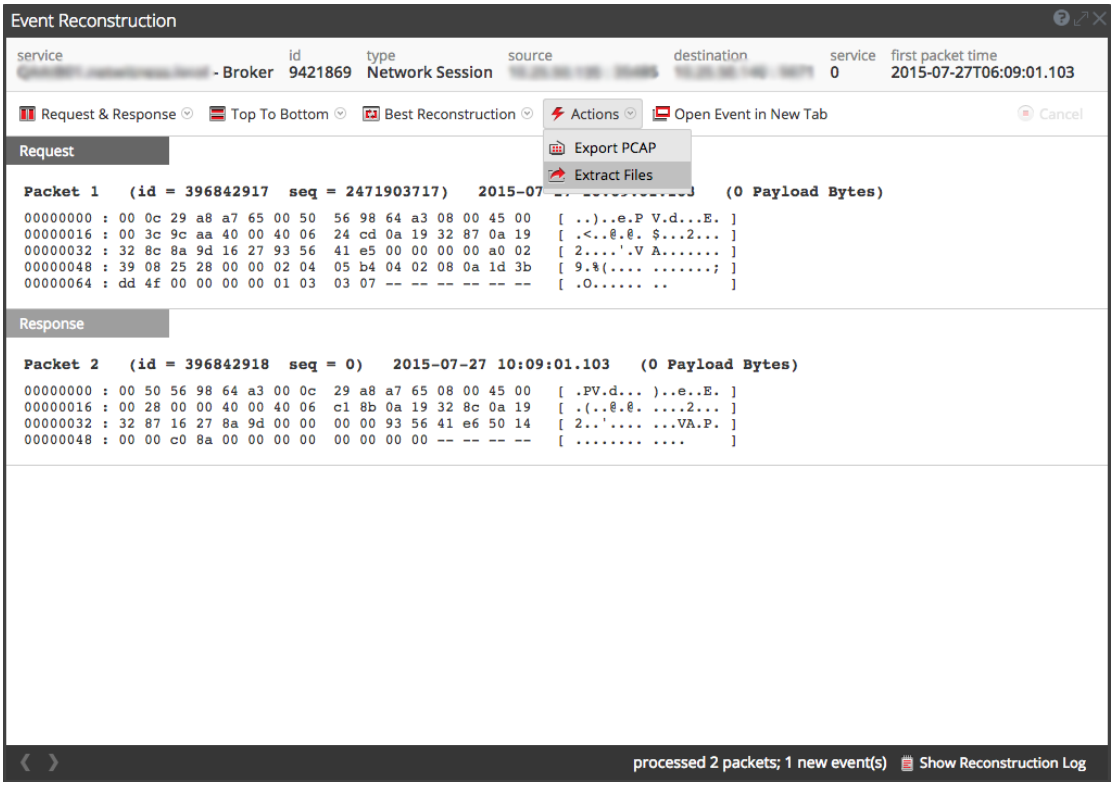
- Tipo de contenido que se exporta: archivos, BitTorrent de audio, documentos, archivos ejecutables, imágenes, otros, video y web.
- El formato del archivo exportado: Archivo ZIP o GZIP.

Una vez que se envía la solicitud, se calendariza un trabajo, el cual se puede rastrear en la bandeja de trabajos. Si hay un error cuando se recupera el registro o la PCAP del servicio, Security Analytics muestra una notificación de error.

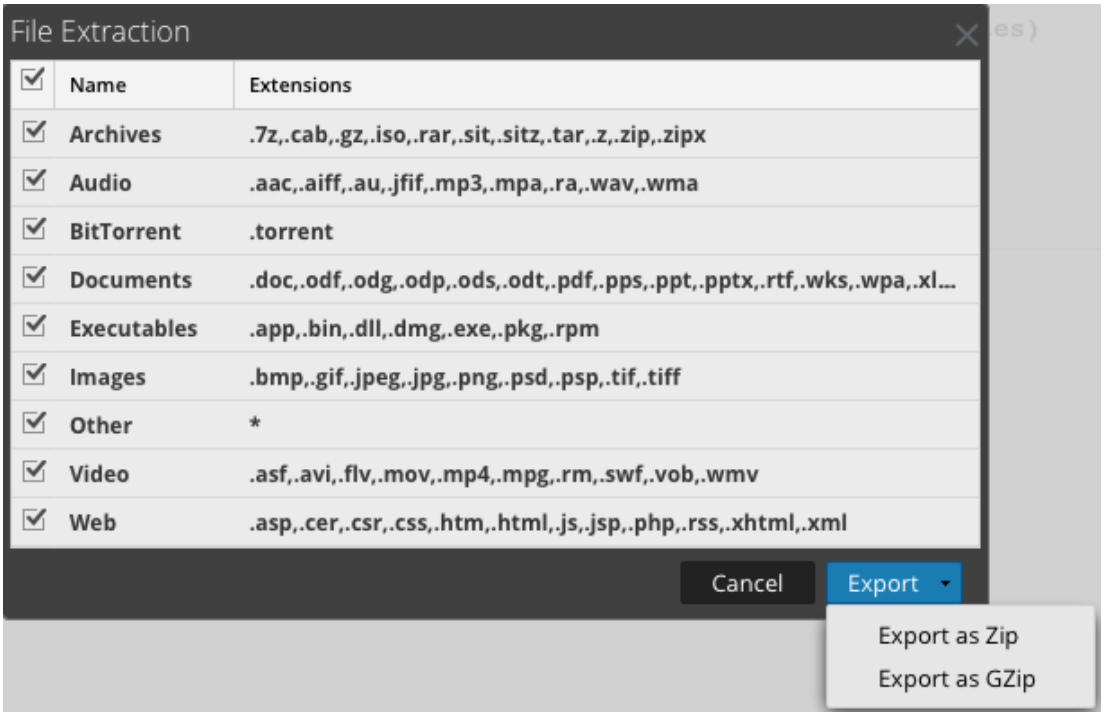
Para extraer archivos de un evento:

1. Mientras está en la **Vista detallada** o en la **Vista de lista** de una reconstrucción de evento, haga clic en un evento.
2. Haga clic en el menú **Acciones** de la barra de herramientas Reconstrucción de evento.
3. Si desea exportar el evento, seleccione **Exportar PCAP** en el menú desplegable.
Un mensaje le informa que el PCAP se está descargando.

4. Si desea extraer archivos, seleccione **Extraer archivos**.



5. Aparece el cuadro de diálogo **Extracción de archivo**.



6. En la columna **Nombre**, seleccione los tipos de contenido que desea extraer.
7. Para generar un archivo de los tipos de archivo seleccionados que contiene el evento, haga clic en **Exportar**.
   Se muestra una lista desplegable de los tipos de archivo que se exportarán.
8. Seleccione **Exportar como Zip** o **Exportar como GZip**.
   El contenido que especificó se extrae a un archivo y se descarga al sistema de archivos local.

Filtrar y buscar resultados en la vista Eventos

Los analistas pueden filtrar los resultados en la vista Investigation > Eventos mediante la búsqueda de eventos o la selección del servicio en el cual se verán, la configuración del rango de tiempo y la consulta de metadatos.

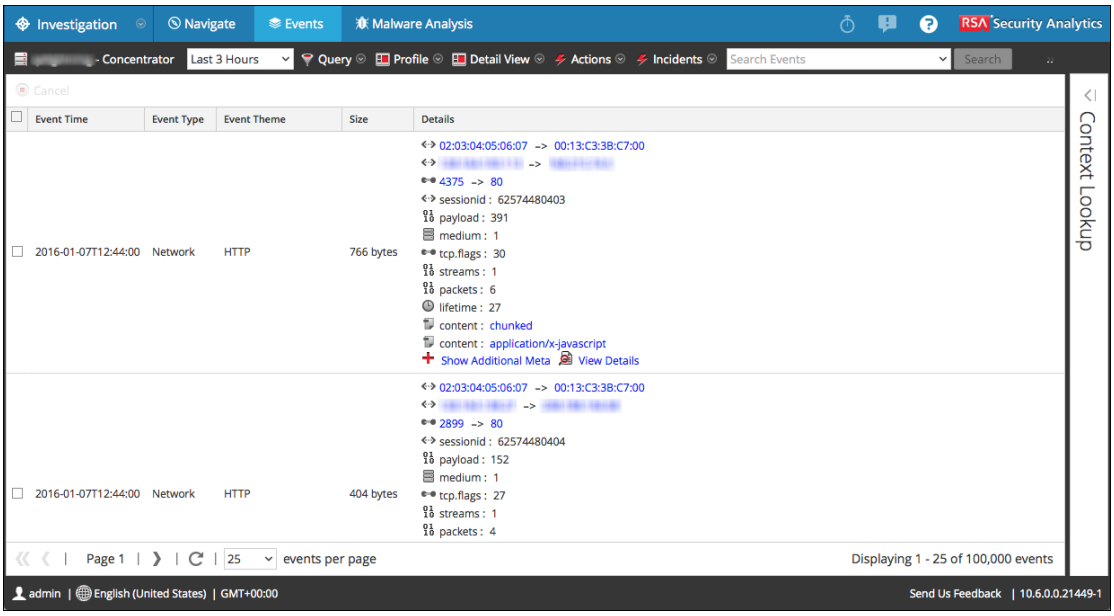
Si abrió la vista Eventos desde un punto de desglose de la vista Navegar, de forma predeterminada la vista se abre en la Vista detallada de eventos. Los analistas que no tienen permisos para utilizar la vista Navegar pueden consultar servicios directamente en la vista Eventos. Hay varias opciones de configuración para filtrar la información que se muestra en la vista Eventos.

Nota: Cuando un Archiver es el servicio seleccionado actualmente en la vista Eventos y se busca contra un Broker o un Concentrator, la búsqueda es más lenta que si se busca contra un Broker o un Concentrator porque los datos del Archiver están comprimidos y normalmente son más.

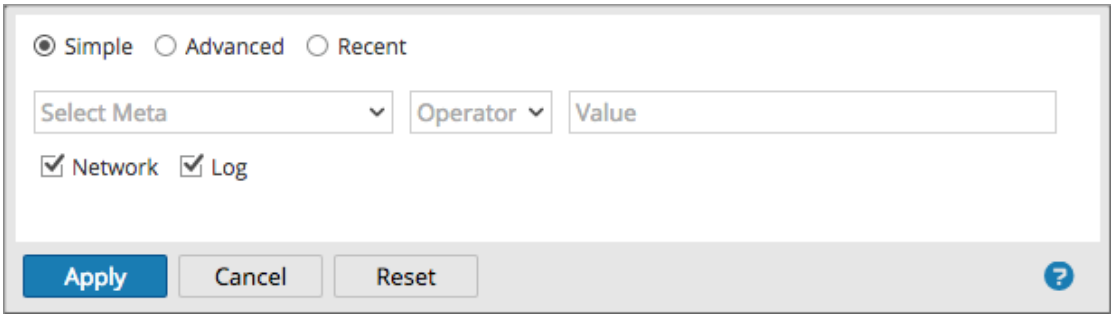
Filtrar los eventos que se muestran en la vista Eventos

Para filtrar los datos que se muestran en la vista Eventos:

1. En el menú de **Security Analytics**, seleccione **Investigar > Eventos**.
   Se muestra la vista Eventos.



2. Para seleccionar un rango de tiempo distinto del predeterminado (**Últimas 3 horas**), haga clic en el campo de rango de tiempo de la barra de herramientas y seleccione un valor. Por ejemplo, **Última hora**.
   La vista Eventos se actualiza con el rango de tiempo seleccionado.
3. Para ingresar una consulta para el servicio y el rango de tiempo seleccionados, haga clic en **Consulta** en la barra de herramientas.
   Se muestra el cuadro de diálogo Consulta simple.

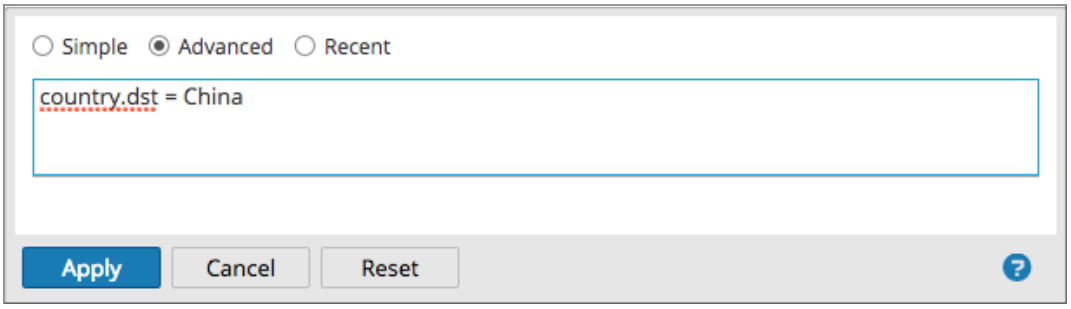


4. Si desea ingresar una consulta simple con la función de autocompletado para seleccionar metadatos y operadores, realice una de las siguientes acciones:
   a. Haga clic en el campo **Seleccionar metadatos** y seleccione una clave de metadatos de la lista desplegable.
   b. En el campo **Operador**, seleccione un operador de la lista desplegable.
   c. Escriba un valor que coincida en el campo **Valor**.

d. Seleccione datos de **Red** o **Registro** y haga clic en **Aplicar**.
Los datos coincidentes se muestran en la vista Eventos.

5. Si desea ingresar una consulta más compleja en función de su conocimiento de los metadatos y operadores:

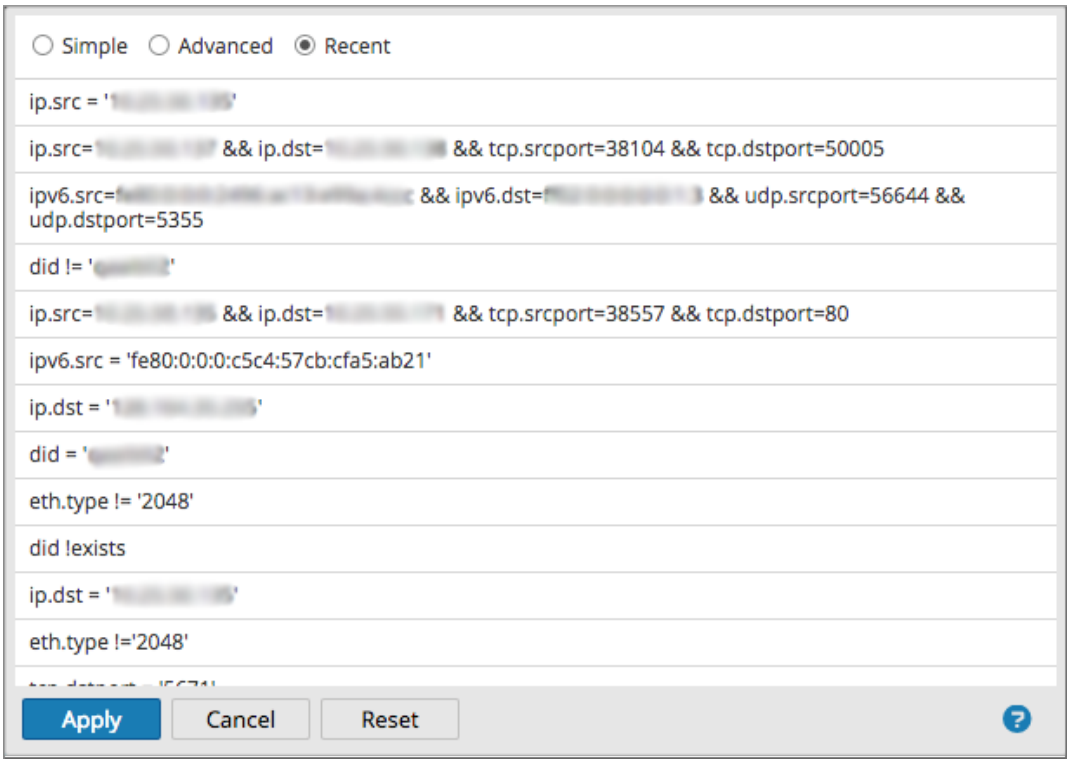
a. Haga clic en **Avanzado**.
Se muestra el cuadro de diálogo Consulta avanzada.



b. Escriba una consulta. A medida que escribe la consulta, a partir de la clave de metadatos, se muestran listas desplegables de claves de metadatos y operadores disponibles. Cuando termine, haga clic en **Aplicar**.

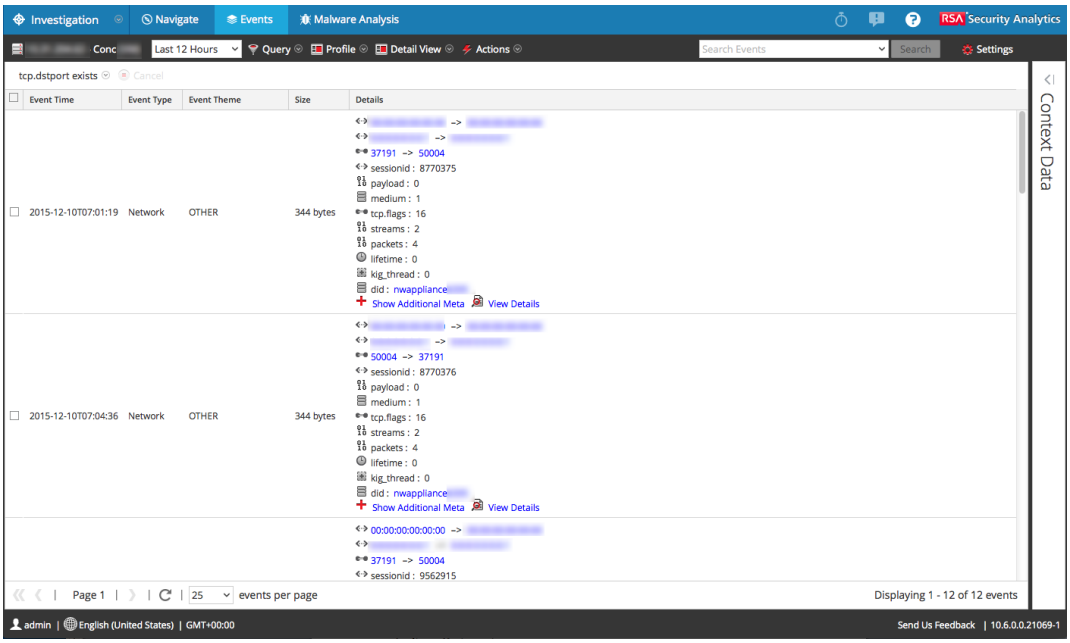
6. Si desea seleccionar una consulta en una lista de consultas recientes:

a. Seleccione **Reciente**.
Se muestra el cuadro de diálogo Consulta reciente.



b. Seleccione una consulta y haga clic en **Aplicar**.

Los resultados coincidentes de la consulta se muestran en la Vista detallada de la vista Eventos. Observe que la ruta de navegación refleja la consulta (tcp.dstport exists, en el ejemplo).



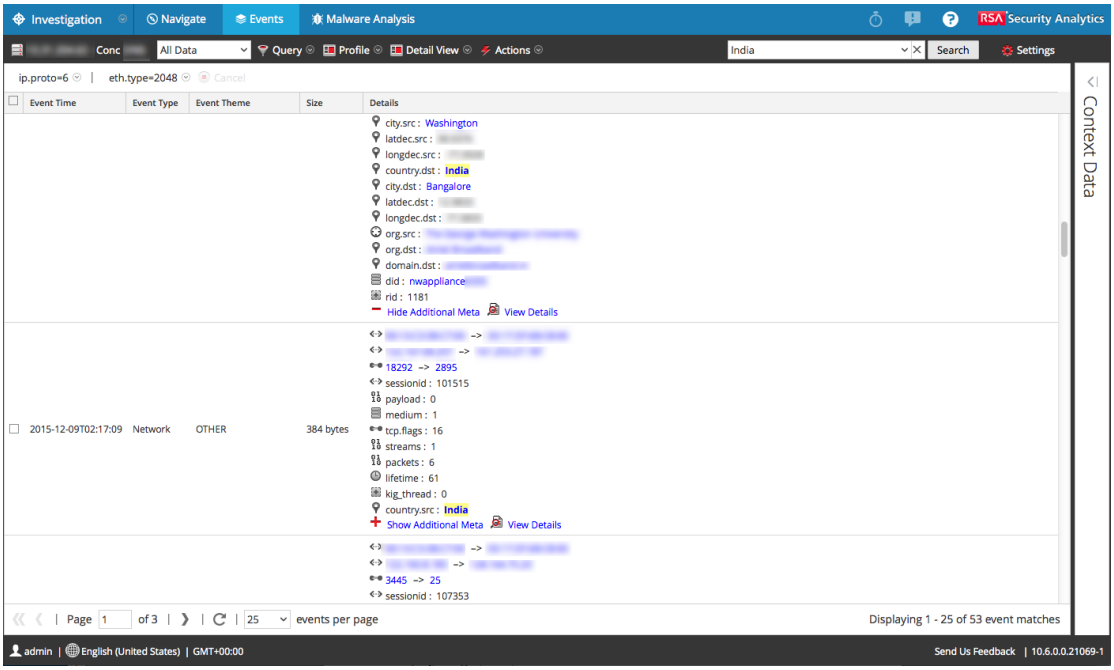
c. En la ruta de navegación, puede hacer clic en cualquiera de las rutas para mostrar el menú Consulta. Puede insertar una nueva consulta antes de una ruta de navegación y agregar una nueva consulta al final de la ruta. Después de cada edición en la ruta de navegación, Security Analytics actualiza los resultados.

Buscar eventos en la vista Eventos

Puede buscar los datos que se muestran actualmente en la vista Eventos mediante el ingreso de una cadena de búsqueda en el campo Buscar. La cadena de búsqueda puede ser Regex (expresión regular) o puede ser una búsqueda de texto simple. Investigation: Opciones de búsqueda proporciona información detallada acerca de estos tipos de búsqueda.

Para buscar en los datos que se muestran actualmente en la vista Eventos:

1. Para ejecutar la búsqueda, coloque el cursor en el cuadro Buscar, escriba una cadena de búsqueda y presione **Intro** o haga clic en **Buscar**.
   Los resultados de búsqueda se muestran en la vista Eventos. Los eventos que coinciden con los criterios de búsqueda se muestran en la cuadrícula de la vista Eventos. En la vista Detalles y en la vista Lista, las coincidencias se resaltan en la columna Detalles. Además, cuando busca RAW, las coincidencias se resaltan en el columna Registros de la vista Registro. A continuación se muestra un ejemplo de los resultados de búsqueda para el término **India** en la vista Detalles de eventos. Observe que las coincidencias de la búsqueda no se resaltan en ninguna reconstrucción de evento.



2. Si desea limitar la búsqueda, cambie la consulta y la hora como se describe en Filtrar los eventos que se muestran en la vista Eventos.
3. Si desea detener la búsqueda y volver a la vista Eventos, haga clic en **Cancelar**.
   Se conserva cualquier resultado que se muestre.
4. Para borrar el cuadro de búsqueda y volver a la vista Eventos normal, haga clic en **X** en el cuadro de búsqueda.

Administrar grupos de columnas en la vista Eventos

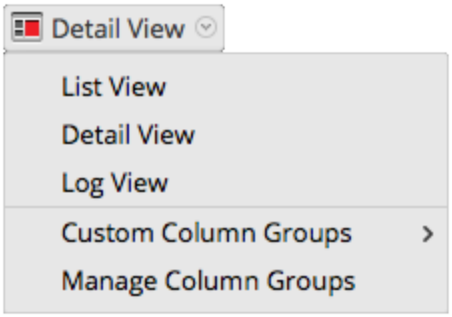
En este tema se proporcionan instrucciones para que un analista cree y administre grupos de columnas personalizados con el objetivo de mostrar datos en la vista Navegación > Eventos.

Cuando observa una lista de eventos en Security Analytics Investigation > vista Eventos, puede personalizar la manera en que se muestran los datos mediante la definición de los metadatos que se muestran en una columna, la posición de la columna en la cuadrícula y el ancho predeterminado de la columna.

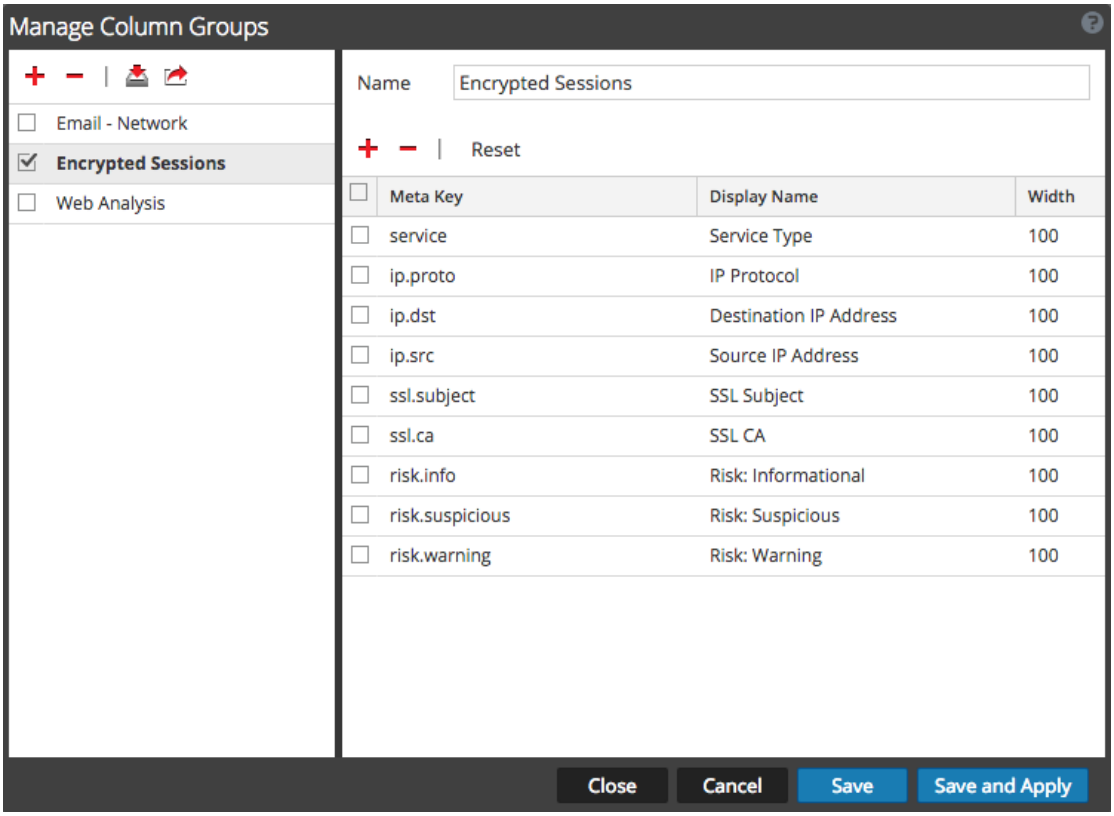
Nota: Los perfiles de Investigation pueden incluir grupos de columnas personalizados. Si se utiliza un grupo de columnas personalizado en un perfil y se observan eventos en la vista Eventos con el uso de un grupo de columnas personalizado, no se puede cambiar el tipo de vista (Detalle, Lista o Registro).

Crear un grupo de columnas personalizado

1. En el menú de **Security Analytics**, seleccione **Investigation > Eventos.**
   Se muestra la vista Eventos.
2. Seleccione **Administrar grupos de columnas** en la barra de herramientas (el nombre de la opción es el valor predeterminado Vista detallada o el valor actual).



   Se muestra el cuadro de diálogo Administrar grupos de columnas. En este ejemplo ya está definido un grupo de columnas.

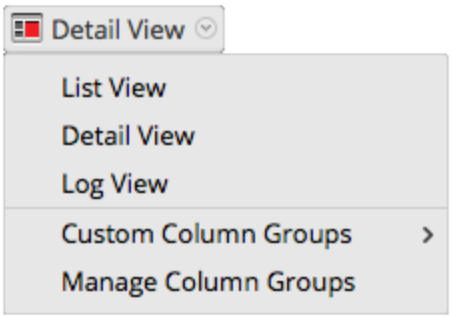


3. Para agregar un nuevo grupo de columnas en el panel de grupos de columnas, haga clic en + e ingrese el nombre del nuevo grupo en el campo resultante.
4. El panel de definición de columnas se abre en el lado derecho y el nombre del grupo aparece completado. Puede editar el nombre del grupo.
5. Para agregar una columna al grupo, haga clic en + y, a continuación, haga clic en el campo vacío **Clave de metadatos** para mostrar la lista desplegable **Clave de metadatos**.
6. Seleccione un campo de clave de metadatos en la lista y repita este paso hasta que el conjunto de columnas esté completo.
7. (Opcional) Para eliminar una clave de metadatos del grupo de columnas, haga clic en −.
8. (Opcional) Para volver a ordenar la secuencia en la cual aparecen las columnas en la lista Eventos, arrastre claves de metadatos a la posición que desee.
9. (Opcional) Para configurar el ancho predeterminado de una columna, haga clic en el valor correspondiente en la columna **Ancho** e ingrese un nuevo ancho de columna.
10. (Opcional) Para volver a la configuración anterior del grupo de columnas y deshacer todos los cambios, haga clic en **Restablecer**.

11. Cuando esté listo para guardar, realice una de las siguientes acciones:
    a. Para guardar el grupo de columnas editado y actualizar la vista Eventos con los ajustes del grupo de columnas, haga clic en **Guardar y aplicar**.
    b. Para guardar el grupo de columnas editado sin actualizar la vista Eventos, haga clic en **Guardar**.

Seleccionar un grupo de columnas personalizado

1. Con la vista Eventos abierta, seleccione **Grupos de columnas personalizados** en la barra de herramientas (el nombre de la opción es el valor predeterminado Vista detallada o el valor actual).



2. Seleccione uno de los grupos personalizados en el submenú.
   La vista Eventos se actualiza para reflejar el grupo de columnas personalizado.

Reconstruir un evento

Cuando visualiza una lista de eventos en la vista Security Analytics Investigation > Eventos, puede crear con seguridad una reconstrucción del evento en un formato legible que coincide con el original. De forma predeterminada, la vista inicial de un evento reconstruido es el formato más adecuado (Mejor reconstrucción); por ejemplo, el contenido web se reconstruye como una página web; una conversación por IM se muestra con ambas partes de la conversación. Cada usuario puede seleccionar una reconstrucción predeterminada distinta en la vista Perfil > Preferencias.

En la reconstrucción, puede:

- Seleccionar la información del evento que desea ver. Los valores posibles son: datos de solicitud, datos de respuesta, datos de solicitud y de respuesta.
- Seleccione el tipo de reconstrucción: detalles, texto, hexadecimal, paquetes, web, correo o IM.
- Exportar registros crudos.

- Exportar el evento como un archivo PCAP.
- Extraer los archivos disponibles en el evento.

> **Precaución:** tenga cuidado cuando haga clic en un vínculo a un archivo en la reconstrucción. Si el sistema tiene una aplicación asociada al archivo o el navegador puede abrirlo y los archivos adjuntos son maliciosos, estos pueden afectar negativamente al sistema.

- Mostrar el evento en una ventana o pestaña independiente (dependiendo de la configuración del navegador).
- Si visualiza la reconstrucción como una vista previa en la vista actual, puede avanzar al próximo evento y retroceder al evento anterior mediante los botones de navegación en la esquina inferior izquierda.

Nota: Las opciones Configuración de la reconstrucción y Configuración de caché de reconstrucción de Security Analytics permiten que un administrador administre el rendimiento de la aplicación para Investigation. A medida que los analistas reconstruyen sesiones que están investigando, dos situaciones pueden afectar el rendimiento y a los resultados.
- Algunos eventos pueden ser muy grandes e incluir muchos miles de paquetes de origen. La reconstrucción de estos tipos de sesiones puede degradar el rendimiento de las aplicaciones.
- En algunos casos, la caché de reconstrucción puede presentar contenido incorrecto; por esta razón, Security Analytics limpia cada 24 horas la caché que tiene más de un día. Entre las limpiezas diarias de la caché, ciertas acciones pueden dejar obsoleta la caché que se usa en una reconstrucción y, si es necesario, los administradores pueden limpiar manualmente la caché para uno o más servicios que están conectados al servidor de Security Analytics actual.

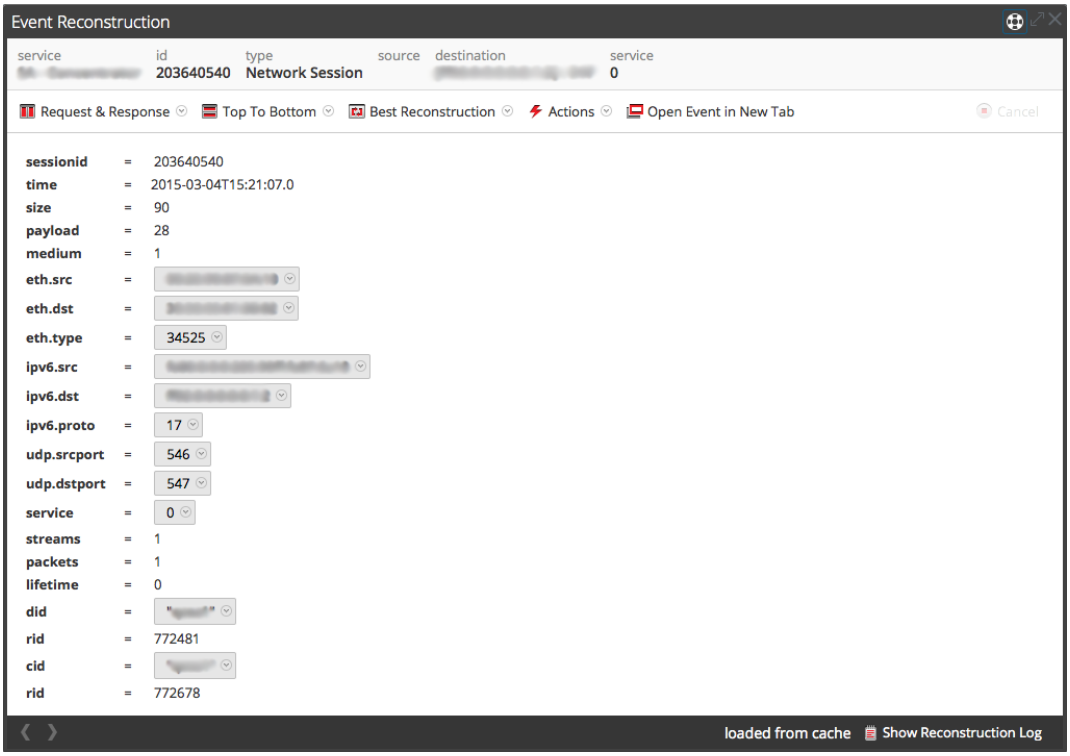
Reconstruir un evento

1. Abrir un punto de desglose en la vista **Eventos**.
2. Para mostrar todos los metadatos, haga clic en 

.
3. Para abrir una reconstrucción de evento en la vista actual, realice una de las siguientes acciones:
   a. Al final del evento, seleccione 

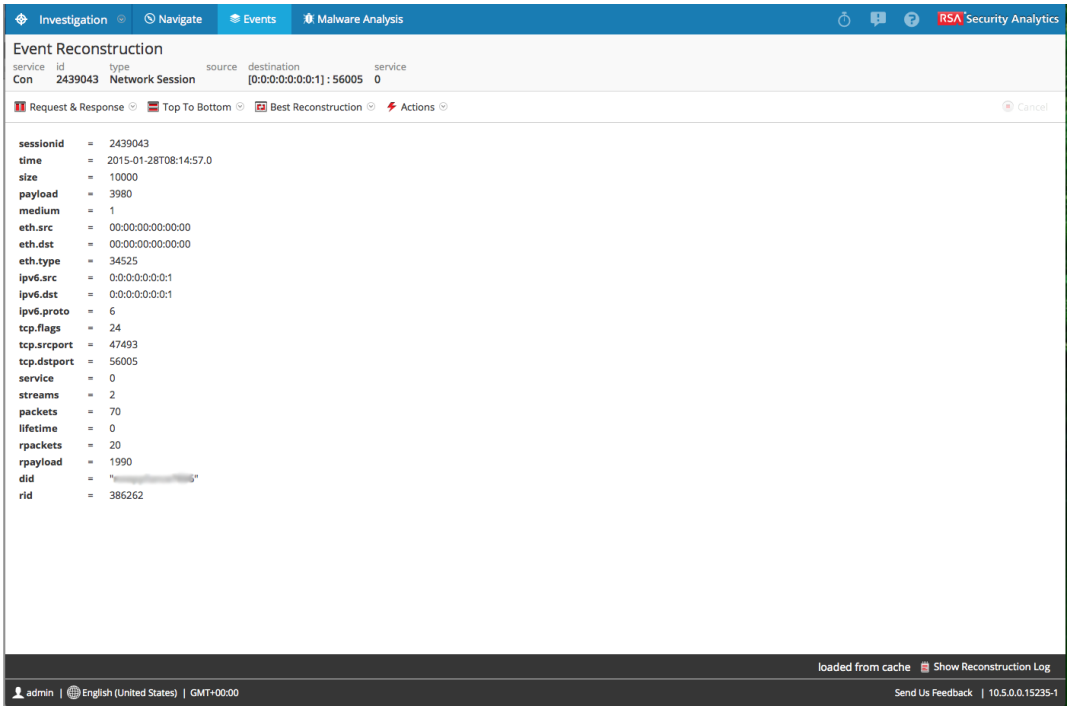
.
   b. Seleccione un evento para reconstruir y elija **Acciones > Ver evento > Vista previa en línea**.
   La Reconstrucción de evento se abre en una ventana emergente en la misma vista. De forma predeterminada, Security Analytics muestra la mejor reconstrucción para el evento, según lo determina el contenido del evento o la reconstrucción que seleccionó en la configuración Vista de sesión predeterminada para Investigation. Puede utilizar las opciones de la barra de herramientas Reconstrucción de evento para cambiar el método

de reconstrucción, ver los resultados en paralelo, exportar un evento, abrir archivos adjuntos del correo electrónico, extraer archivos y abrir el evento en una nueva pestaña.



4. Para tener una vista previa de una reconstrucción del siguiente evento, haga clic en ❯ o para una vista previa de una reconstrucción del evento anterior, haga clic en ❮.
5. Para abrir una reconstrucción de evento en una nueva pestaña, realice una de las siguientes acciones:

   a. En la vista **Eventos**, seleccione un evento para reconstruir y elija **Acciones > Ver evento> Abrir en una nueva pestaña**.
   b. En la barra de herramientas **Reconstrucción de evento** de la reconstrucción con vista previa, haga clic en **Abrir evento en nueva pestaña** en la barra de herramientas.
   La Reconstrucción de evento se abre en una pestaña nueva.

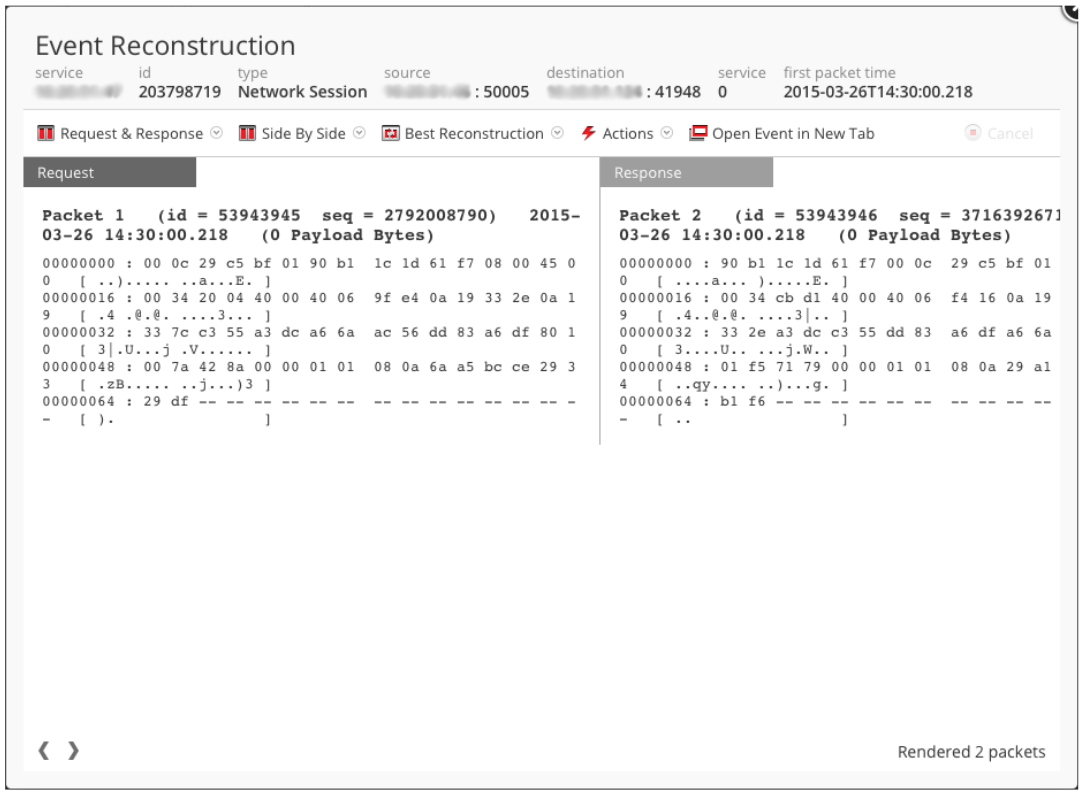


Ver en paralelo o de arriba abajo

Para seleccionar la forma en que se muestran las solicitudes y respuestas para un evento:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **De arriba abajo** o **En paralelo**.
2. En el menú desplegable, seleccione la información que desea ver en el evento: **En paralelo** o **De arriba abajo.**

   La reconstrucción se actualiza con la información seleccionada.



Seleccione la información del evento que desea ver

Para seleccionar la información de evento que desea ver:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **Solicitud y respuesta**.
2. En el menú desplegable, seleccione la información que desea ver en el evento: **Solicitud y respuesta**, **Solicitud** o **Respuesta**.
   La reconstrucción se actualiza con la información seleccionada.

Seleccionar el tipo de reconstrucción de evento

Para seleccionar el tipo de reconstrucción de un evento:

1. En la barra de herramientas de la sección **Reconstrucción de evento**, haga clic en **Mejor reconstrucción**.
2. En el menú desplegable, seleccione el tipo de reconstrucción que desea ver: **metadatos**, **texto**, **formato hexadecimal**, **paquetes**, **web**, **correo** o **archivos**.
   La reconstrucción se actualiza con el tipo de reconstrucción seleccionado.

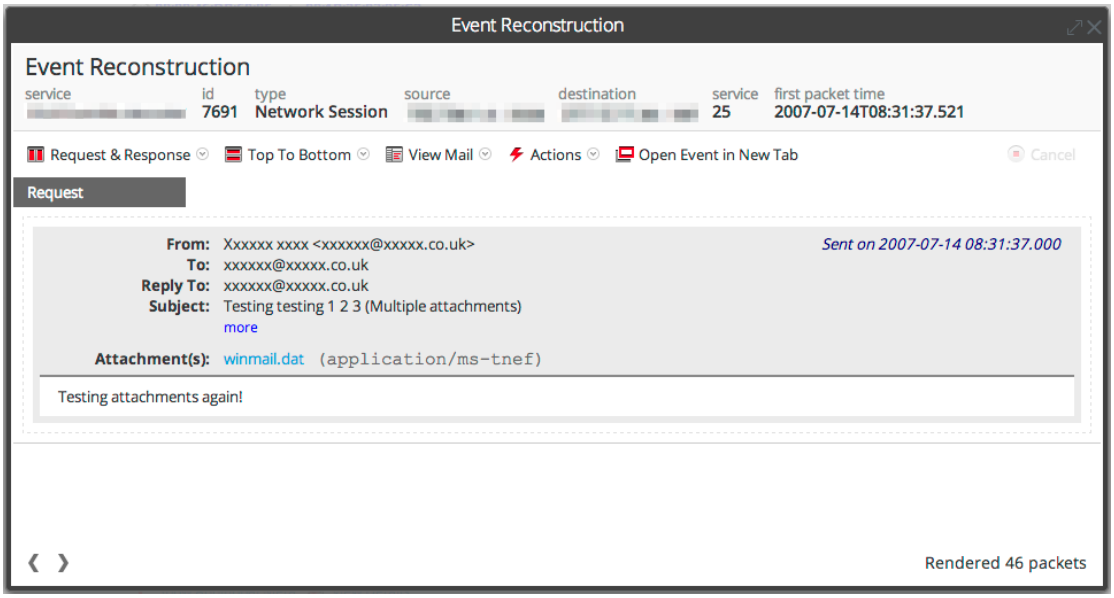
Abrir o descargar archivos adjuntos del correo electrónico

Cuando observa una reconstrucción de un correo electrónico que tiene archivos adjuntos, puede abrir tipos de archivos compatibles o descargarlos al sistema local.

Precaución: tenga cuidado cuando seleccione los archivos adjuntos. Si el sistema tiene una aplicación asociada a los archivos adjuntos o el navegador puede abrirlos y son maliciosos, estos pueden afectar negativamente al sistema.

Para abrir o descargar archivos adjuntos del correo electrónico:

1. En la barra de herramientas de la sección **Reconstrucción de evento**, seleccione el menú desplegable Ver y elija **Ver correo**.
   Se muestra la sección Reconstrucción de evento.



2. En la sección **Reconstrucción de evento** del correo electrónico, haga clic en Archivo adjunto.
   Si el tipo de archivo es compatible con el navegador, el archivo adjunto se abre en una nueva pestaña.
   Si no lo es, se muestra el cuadro de diálogo Descargar que permite descargar el archivo adjunto.

Exportar un evento como un archivo PCAP

La opción Exportar PCAP descarga las sesiones del rango de tiempo actual y del punto de desglose a un archivo PCAP. Para exportar un evento como un archivo pcap:

1. En la barra de herramientas de la sección **Reconstrucción de evento**, haga clic en **Acciones**.
2. Haga clic en **Exportar PCAP**.
3. Se muestra un cuadro de diálogo de confirmación.
4. Haga clic en **Aceptar**.
   El trabajo se calendariza y cuando finaliza el PCAP se descarga al sistema de archivo local. En la pestaña Perfil > Trabajos, puede descargar el PCAP.

Extraer archivos de un evento reconstruido

La opción Extraer archivos extrae y descarga los archivos asociados con el evento. Para extraer archivos:

1. En la barra de herramientas de la sección **Reconstrucción de evento**, haga clic en **Acciones**.
2. Haga clic en **Extraer archivos**.
   Aparece el cuadro de diálogo Extracción de archivo.
3. Seleccione los tipos de archivos que desea extraer y haga clic en **Aceptar**.
4. El trabajo se calendariza y cuando finaliza los tipos de archivo seleccionados se descargan al sistema de archivo local. En la pestaña Perfil > Trabajos, puede descargar los archivos.

Realizar un análisis de malware

Los analistas pueden usar el servicio RSA Security Analytics Malware Analysis para detectar malware.

Una vez iniciada una investigación de Malware Analysis, no hay un orden específico para llevarla a cabo. En cambio, Security Analytics ofrece varios métodos para mostrar, filtrar y consultar los datos, actuar conforme a un punto de desglose y examinar eventos específicos. En este tema se proporciona información y procedimientos para los analistas que utilizan el servicio RSA Security Analytics Malware Analysis para detectar malware en datos y archivos seleccionados.

Las cuentas de usuario de los analistas que realizan análisis mediante Security Analytics Malware Analysis deben tener configuradas las funciones y los permisos correspondientes del sistema. Consulte Funciones y permisos para los analistas. Un administrador debe configurar las funciones y los permisos.

Este documento agrupa las tareas de investigación de acuerdo con las funciones generales de una investigación:

- Iniciar una investigación de Malware Analysis.
- Cargar archivos para escaneo de Malware Analysis.
- Implementar contenido personalizado de YARA.
- Filtrar datos de dashlets en la vista Resumen de eventos.
- Examinar archivos y eventos de escaneo en formato de lista
- Ver detalles de Malware Analysis de un evento.

Iniciar una investigación de Malware Analysis

En este tema se proporcionan instrucciones para investigar los datos escaneados por Malware Analysis en Security Analytics Investigation.

Puede investigar datos que Security Analytics Malware Analysis haya escaneado, marcado y clasificado por su contenido de indicadores de riesgo. Esto incluye todos los tipos de escaneos de Malware Analysis: sondeo en modo continuo, sondeo según demanda y archivos cargados según demanda. El sondeo en modo continuo se debe habilitar cuando el administrador configura ajustes básicos para el servicio Malware Analysis.

Security Analytics proporciona varios métodos para iniciar una investigación de Malware Analysis.

Más veloz: Inicio inmediato desde dashlets de Malware Analysis

La manera más rápida de comenzar una investigación de Malware Analysis es un inicio inmediato desde el tablero Security Analytics mediante uno de los dashlets de Malware Analysis que enumera eventos o archivos que probablemente contienen malware. Desde uno de estos dashlets, puede ir directamente a los resultados de análisis de un evento específico que se ha enumerado como digno de investigación:

- Lista del malware altamente sospechoso principal
- Lista del posible malware de día cero principal
- Dashlet Malware con IOC de alta confianza y altos puntajes

Sondeo según demanda desde un valor de metadatos en la vista Navegar

Puede iniciar un sondeo según demanda en una investigación si hace clic con el botón secundario en un valor de metadatos en la vista Navegar y selecciona una opción en el menú contextual. Cuando se completa el sondeo, los datos escaneados están disponibles para Malware Analysis (consulte Iniciar un escaneo de Malware Analysis desde la vista Navegar).

Investigar un servicio de RSA específico

También puede iniciar una investigación de Malware Analysis de un servicio en la vista Investigation > Malware Analysis. Para una investigación de Malware Analysis por servicio, se debe especificar un servicio en la vista Investigation > Malware Analysis:

1. Security Analytics abre la vista Malware Analysis, en la cual está seleccionado el servicio predeterminado especificado por el usuario.
2. Si no se especifica ningún servicio predeterminado, Security Analytics presenta un cuadro de diálogo que permite seleccionar el servicio de Malware Analysis que se investigará.
3. Cuando un servicio se selecciona manualmente o de manera predeterminada en la vista Malware Analysis, Security Analytics abre el Resumen de eventos para el servicio seleccionado y sus datos de escaneo continuo.

En este tema se proporcionan instrucciones para todos los métodos de inicio de una investigación de Malware Analysis.

Iniciar una investigación de malware desde un dashlet de Malware Analysis

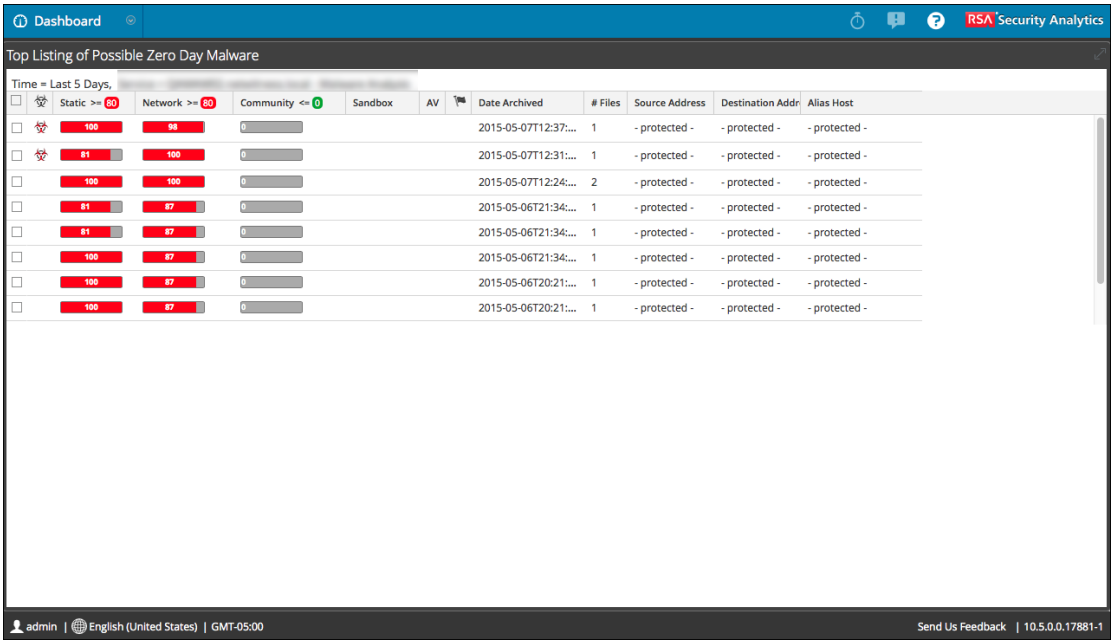
Este procedimiento tiene el requisito previo de que uno de los siguientes dashlets debe estar visible en el tablero Unified o en la vista Malware Analysis y se debe completar con eventos o archivos enumerados. Si no ve los dashlets, agréguelos y configúrelos.

- Lista del malware altamente sospechoso principal
- Lista del posible malware de día cero principal

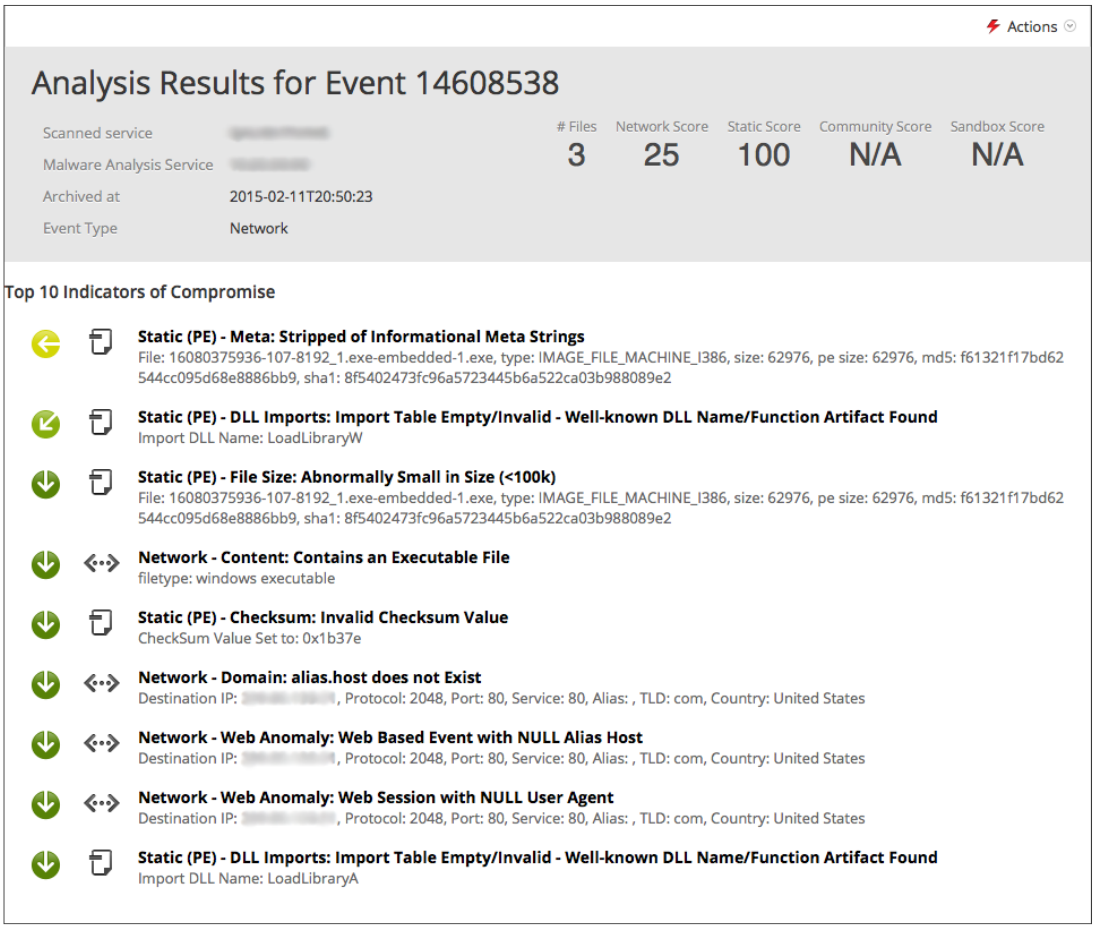
- Dashlet Malware con IOC de alta confianza y altos puntajes

Para iniciar una investigación de Malware Analysis desde un dashlet:

1. Inicie sesión en Security Analytics y busque uno de los dashlets mencionados anteriormente en el tablero principal o en la vista Malware Analysis. El siguiente es un ejemplo del dashlet Lista del posible malware de día cero principal configurado para mostrar archivos.



2. En el dashlet, haga doble clic en un evento o un archivo para realizar un análisis más profundo. La vista Malware Analysis presenta un análisis detallado del evento en la Lista de eventos o el evento con el cual está asociado el archivo en la Lista de archivos.



Para obtener más información sobre cómo configurar los dashlets de Malware Analysis en el tablero Unified, consulte “Dashlets” en la *Guía de introducción de Security Analytics*.

Para conocer los métodos para configurar y filtrar la información de los dashlets en la vista Malware Analysis, consulte Filtrar datos de dashlets en la vista Resumen de eventos.

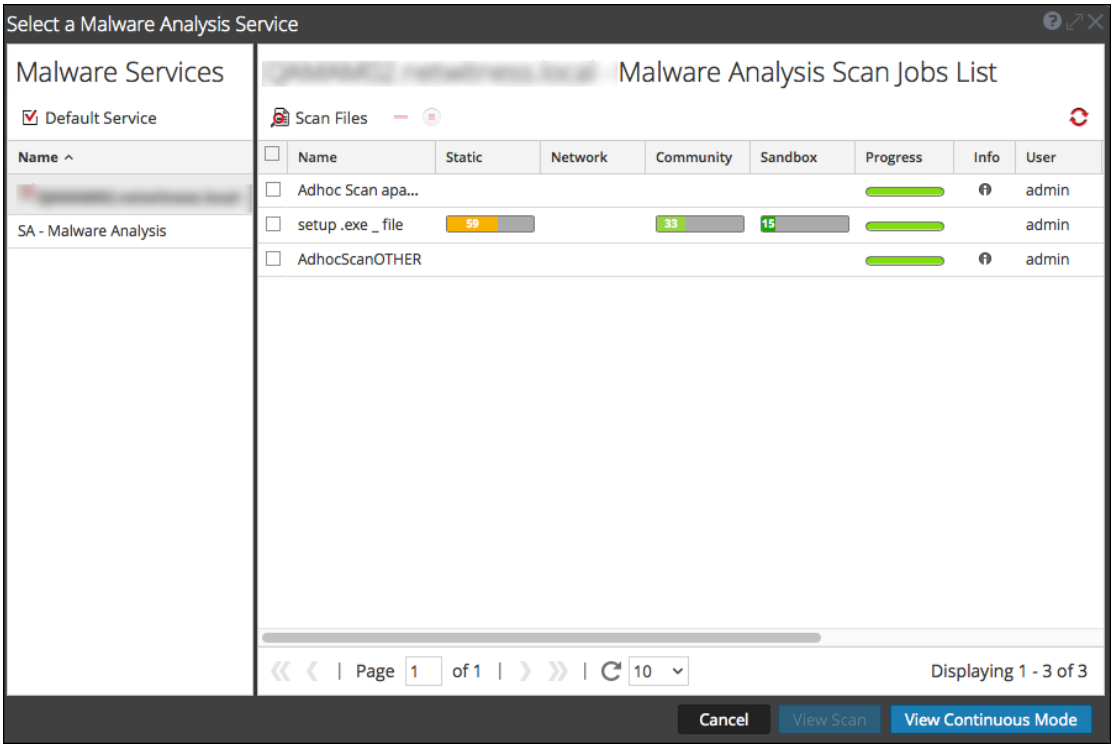
Para obtener información sobre las acciones que puede realizar en los resultados del análisis, consulte Ver detalles de Malware Analysis de un evento.

Comenzar una investigación de Malware Analysis (sin servicio predeterminado)

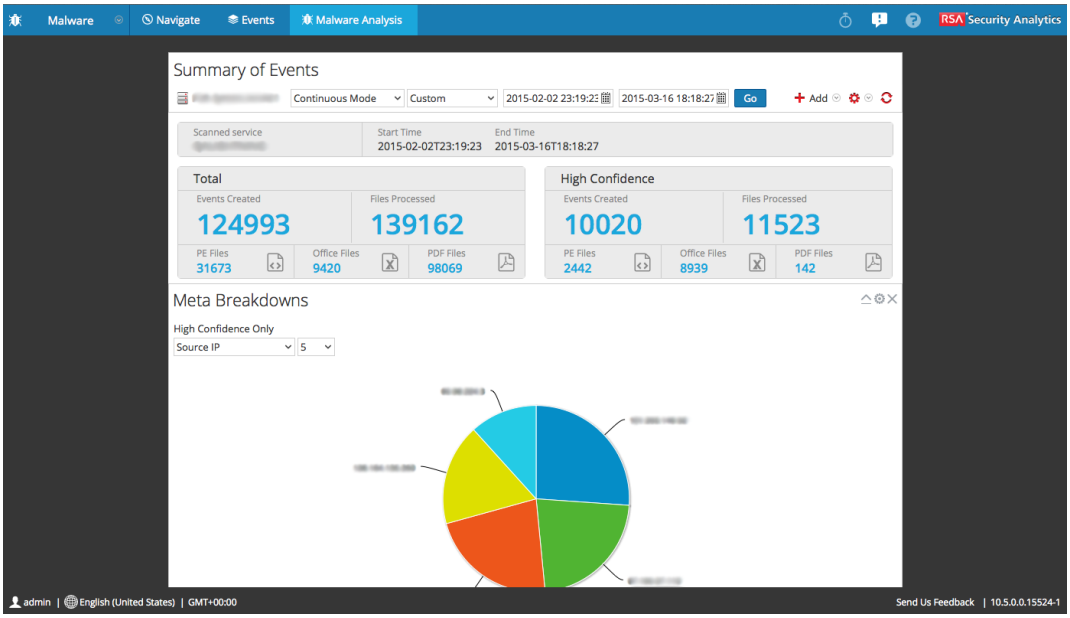
Para comenzar una investigación sin especificar algún servicio predeterminado:

1. En el menú de **Security Analytics**, seleccione **Investigation > Malware Analysis**.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis con los hosts y los servicios de Malware Analysis disponibles para el usuario actual en el panel de la izquierda y los trabajos de escaneo disponibles en el panel de la derecha. Este panel de

trabajos de escaneo contiene las mismas columnas que el dashlet Trabajos de escaneo de malware en el tablero Unified. Además, tiene una barra de herramientas y opciones de visualización, las cuales se describen en Investigation: Cuadro de diálogo Seleccionar un servicio Malware Analysis.



2. En la lista de hosts de Malware Analysis, seleccione un host. Se muestra una lista de trabajos de escaneo en el panel de la derecha.
3. Para comenzar a analizar un escaneo, realice lo siguiente:
   a. Seleccione un escaneo y haga clic en **Ver escaneo**.
   b. Haga clic en **Ver modo continuo**.
      El Resumen de eventos para el escaneo seleccionado se muestra con los dashlets predeterminados abiertos. Cada usuario puede agregar, modificar y eliminar dashlets predeterminados, lo cual persiste en las distintas investigaciones de escaneos. Los usuarios también pueden restaurar los dashlets predeterminados, como se describe en Filtrar datos de dashlets en la vista Resumen de eventos.

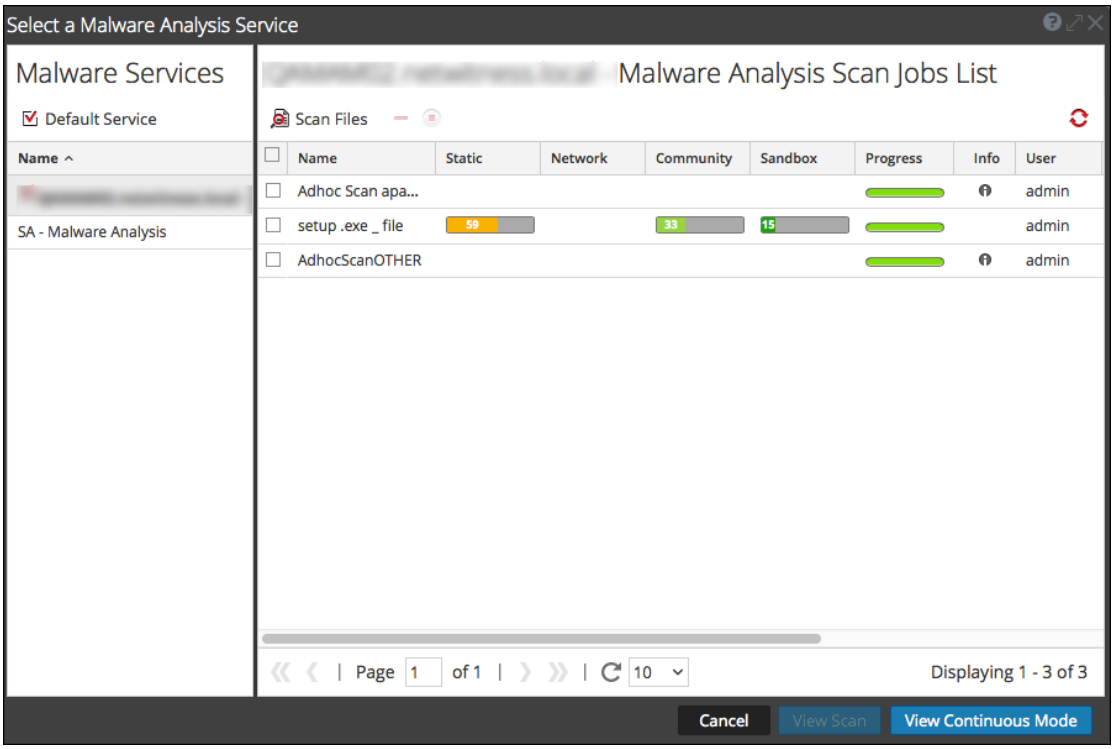


Configurar o borrar el servicio predeterminado

Puede configurar y borrar el servicio predeterminado en el cuadro de diálogo Seleccionar un servicio Malware Analysis.

Para configurar un servicio predeterminado:

1. Haga clic en el nombre del servicio en la barra de herramientas Resumen de eventos.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis.



2. Seleccione un servicio en la lista de servicios de malware disponibles y haga clic en Default Service.

   El servicio se convierte en el valor predeterminado (lo cual se indica con ☑ frente al nombre de host).

3. Para borrar el servicio predeterminado, selecciónelo en la cuadrícula y haga clic en Default Service.

   No se configura un servicio predeterminado.

Cargar y escanear archivos

Un analista de malware con permiso para `Iniciar escaneo de Malware Analysis` puede cargar archivos para escanear mediante la opción Escanear archivos del cuadro de diálogo Seleccionar un servicio Malware Analysis (consulte Cargar archivos para escaneo de Malware Analysis. Un administrador puede cargar archivos de captura de paquete en un Decoder para Malware Analysis en la vista Sistema de servicios, como se describe en "Cargar archivo de captura de paquetes" en la *Guía de configuración de Decoder y Log Decoder*.

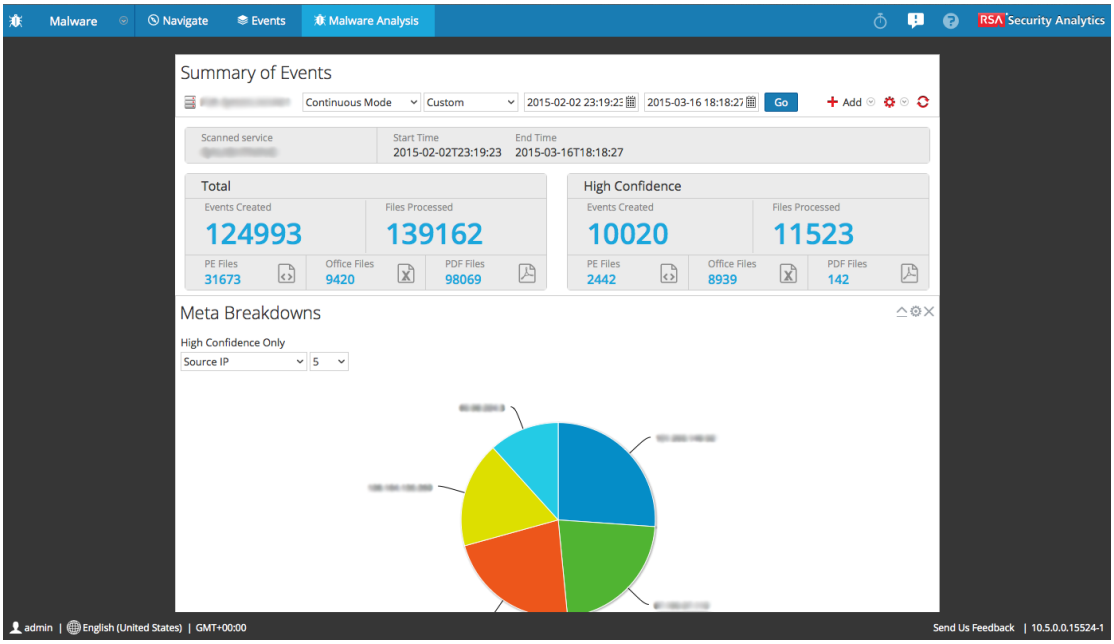
Comenzar una investigación (se especifica el servicio predeterminado)

Para comenzar una investigación con un servicio predeterminado especificado:

1. En el menú de **Security Analytics**, seleccione **Investigation > Malware Analysis**.

   El Resumen de eventos para un escaneo continuo del servicio seleccionado se muestra con

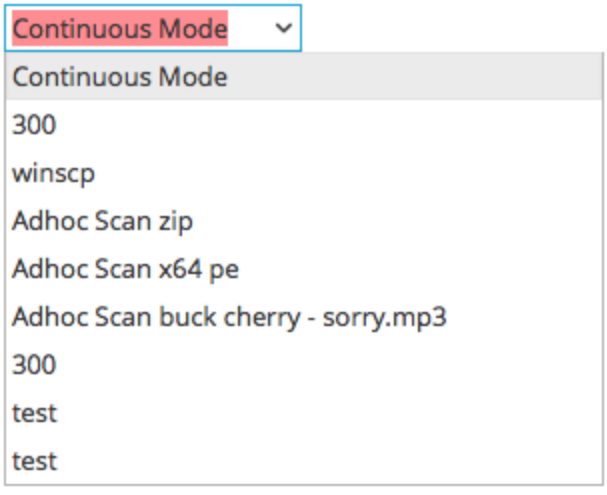
los dashlets predeterminados abiertos. Cada usuario puede agregar, modificar y eliminar dashlets predeterminados, lo cual persiste en las distintas investigaciones de escaneos. Los usuarios también pueden restaurar los dashlets predeterminados, como se describe en Filtrar datos de dashlets en la vista Resumen de eventos.



Aplicar un filtro de parámetros de tiempo a los resultados

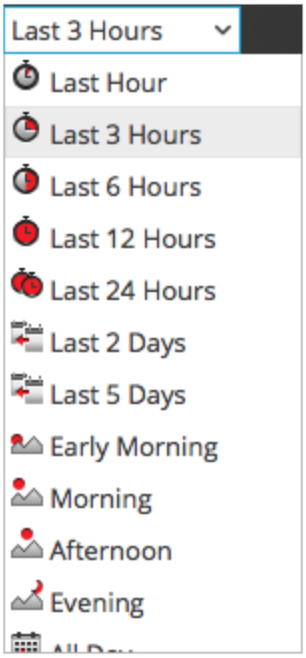
Puede aplicar un filtro de umbral para actualizar los resultados de los dashlets seleccionados.

1. Para seleccionar un rango de tiempo distinto, seleccione **Modo continuo** u otro escaneo en la barra de herramientas.



Se muestra el Resumen de eventos de malware del escaneo seleccionado.

2. Para seleccionar un nuevo rango de tiempo para el escaneo, haga clic en la lista de selección de rangos en la barra de herramientas. Los rangos disponibles son: Últimos 5 minutos, Últimos 10 minutos, Últimos 15 minutos, Últimos 30 minutos, Última hora, Últimas 3 horas, Últimas 6 horas, Últimas 12 horas, Últimas 24 horas, Últimos 2 días, Últimos 5 días, Primera hora, Mañana, Tarde, Noche, Todo el día, Ayer, Esta semana, La semana pasada o Personalizado.



   Los resultados se actualizan de inmediato.

3. Para actualizar un escaneo en modo continuo con nuevos datos, haga clic en .

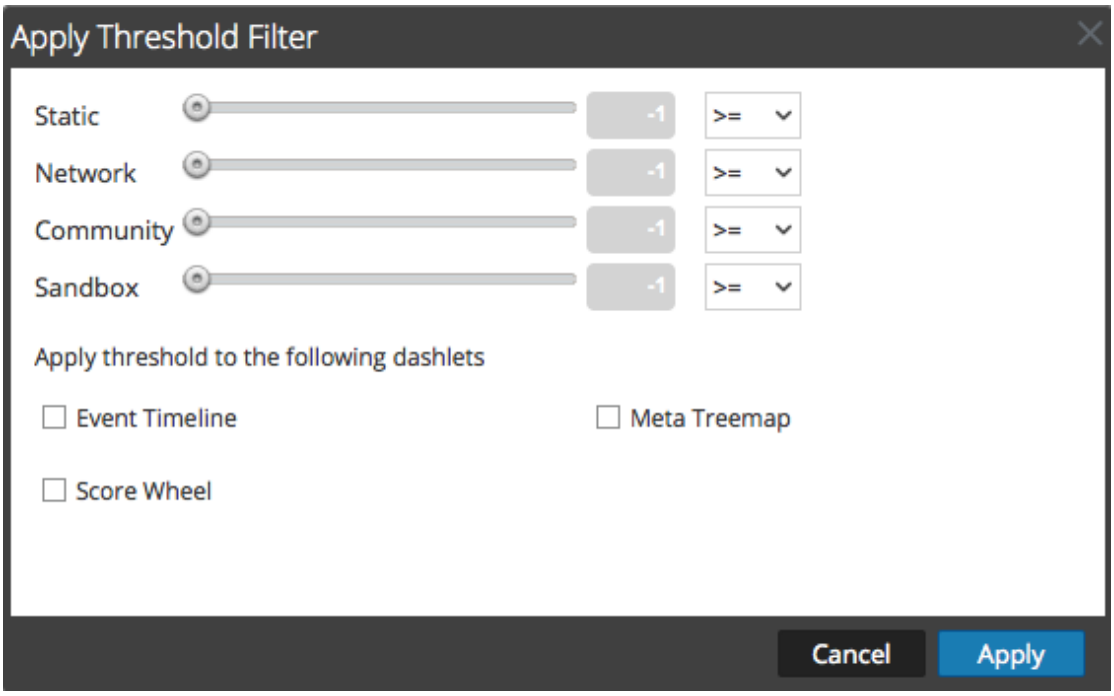
Aplicar un filtro de umbral a los resultados del modo continuo

Puede aplicar un nuevo filtro de umbral a una instancia de los dashlets Malware con IOC de alta confianza y altos puntajes, Mapa de árbol de metadatos, Rueda de puntaje y Cronograma de evento.

Para personalizar el puntaje que se aplica al escaneo, realice lo siguiente en la barra de herramientas:

1. Seleccione **Configuración > Aplicar filtro de umbral.**

   Se muestra el cuadro de diálogo Aplicar filtro de umbral.



2. Si desea limitar la cantidad de eventos que se muestran a aquellos que obtuvieron un puntaje superior a un determinado número, realice lo siguiente:
   a. Arrastre el control deslizante en las barras Static, Red, Comunidad y Sandbox.
   b. Para seleccionar los dashlets a los cuales se aplican los umbrales, seleccione las casillas de verificación apropiadas.
   c. Haga clic en **Aplicar**.

Eliminar o volver a enviar un escaneo según demanda con una nueva configuración de omisión

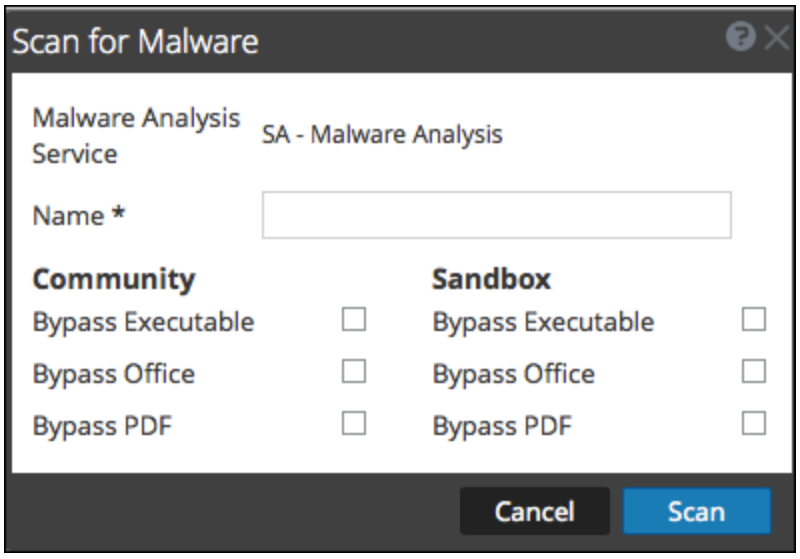
Puede eliminar o volver a enviar un escaneo según demanda con una configuración de omisión distinta a la que se especificó en la vista Configuración del servicio para un servicio Malware Analysis.

Para eliminar un escaneo mientras observa un escaneo según demanda, realice lo siguiente:

1. Seleccione **Acciones > Eliminar escaneo**.
   Security Analytics solicita confirmar la intención de eliminar el escaneo.
2. Haga clic en **Sí**.
   El escaneo seleccionado se elimina.

Para aplicar una configuración de omisión distinta al escaneo actual:

1. Seleccione **Acciones > Volver a enviar escaneo**.
   Se muestra el cuadro de diálogo Escanear para encontrar malware.



2. Seleccione la configuración de omisión que desea utilizar en el nuevo escaneo y haga clic en **Escanear**.
   Malware Analysis restablece la caché y vuelve a enviar el archivo para un nuevo escaneo, y Security Analytics lo agrega a la línea de espera de trabajos.
3. Cuando el trabajo finalice, desplácese a la izquierda y seleccione **Ver**.
   Se muestra el Resumen de eventos de malware del escaneo seleccionado.

Ver la lista de archivos

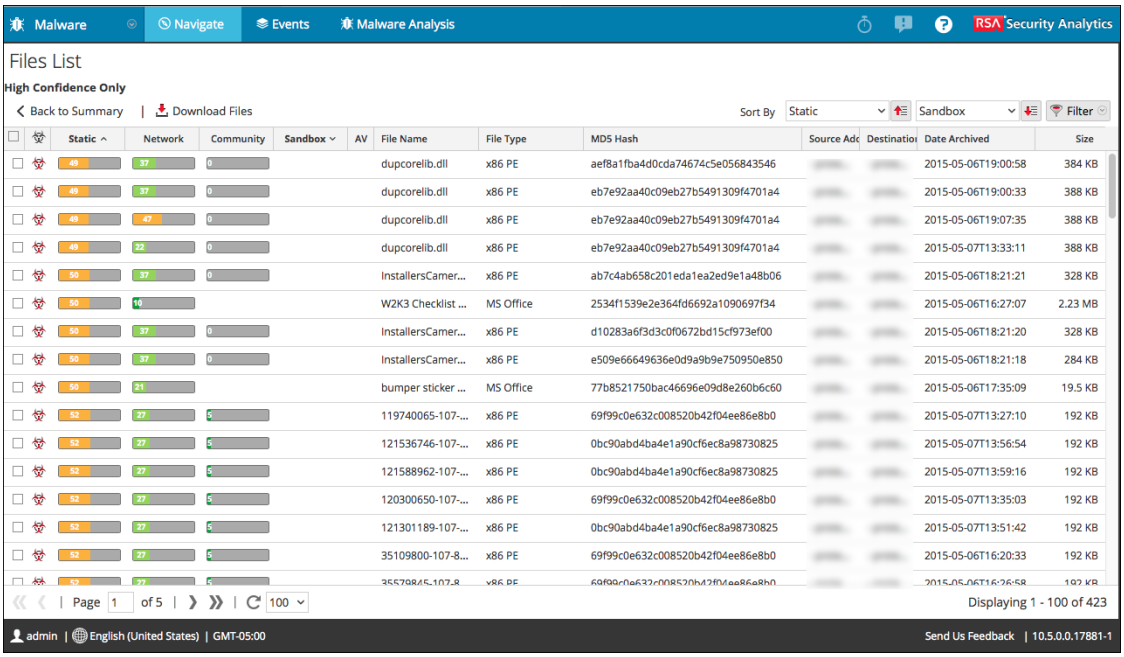
Puede ver una lista de archivos para un evento desde el Resumen de eventos de Malware Analysis y desde cada uno de los gráficos de visualización: Cronograma de evento, Desgloses de metadatos, Mapa de árbol de metadatos y Rueda de puntaje.

Para ver la Lista de archivos, realice una de las siguientes acciones:

- En el Resumen de eventos, haga clic en la cantidad de archivos en la fila **Total** o en la fila **Alta confianza** bajo **Archivos procesados**, **Archivos de PE**, **Archivos de Office** o **Archivos PDF**. Se muestra la Lista de archivos.

- En cualquier dashlet de visualización, haga clic en el número junto al campo **Archivos** en la esquina superior derecha del dashlet.

Se muestra la Lista de archivos para el punto de desglose seleccionado.



En la lista de archivos, puede buscar un archivo por nombre de archivo o hash de archivo MD5, clasificar la lista según dos criterios y orden ascendente o descendente y descargar archivos, como se describe en Examinar archivos y eventos de escaneo en formato de lista.

Para volver al Resumen de eventos, haga clic en **Volver al resumen**.

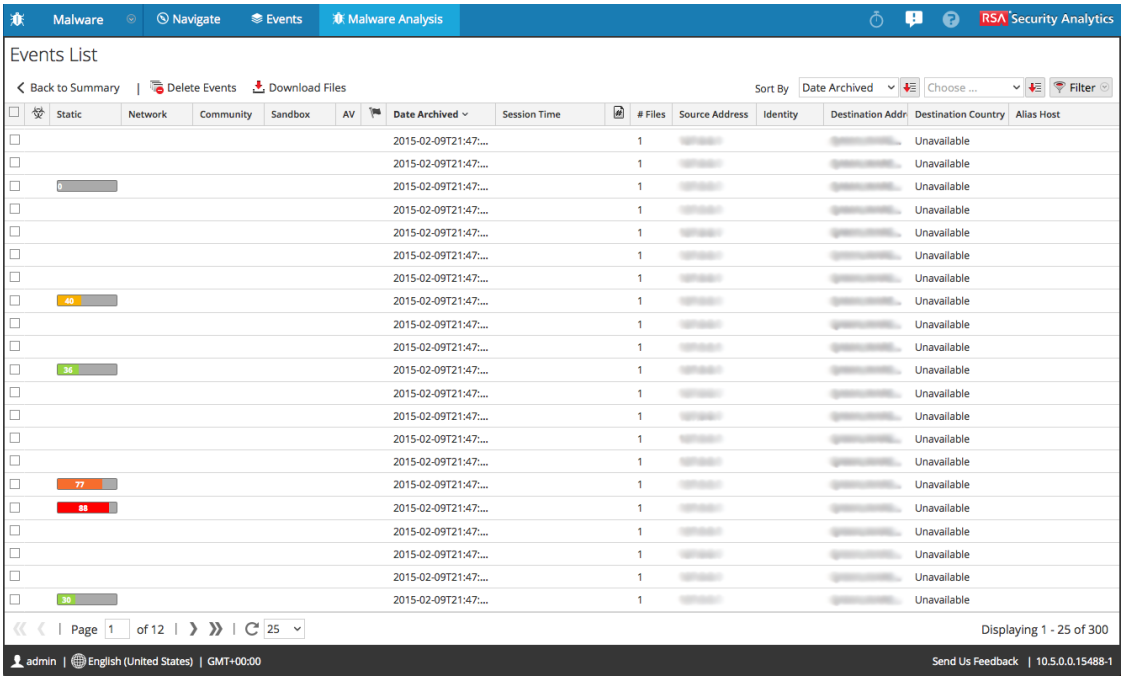
Ver la lista de eventos

En el Resumen de eventos de Malware Analysis y desde cada uno de los gráficos de visualización (Cronograma de evento, Desgloses de metadatos, Mapa de árbol de metadatos y Rueda de puntaje), puede seleccionar eventos para ver en la cuadrícula Eventos.

Para ver la Lista de eventos, realice una de las siguientes acciones:

- En el Resumen de eventos, haga clic en la cantidad de Eventos creados en la fila **Total** o en la fila **Alta confianza**. Se muestra la Lista de eventos.
- En cualquier dashlet de visualización, haga clic en el número junto al campo Eventos en la esquina superior derecha del dashlet.

Se muestra la Lista de eventos para la hora seleccionada.



Implementar contenido personalizado de YARA

En este tema se proporcionan instrucciones para implementar contenido personalizado de YARA en Security Analytics Malware Analysis.

Además de los indicadores de riesgo incorporados, Security Analytics Malware Analysis es compatible con indicadores de riesgo escritos en YARA. YARA es un lenguaje de reglas que permite a los investigadores de malware identificar y clasificar muestras de malware. En RSA Live están disponibles indicadores de riesgo (IOC) basados en YARA incorporados; estos se descargan y se habilitan automáticamente en hosts suscritos.

Los clientes con habilidades y conocimientos avanzados pueden agregar funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live o la colocación de estas reglas en una carpeta inspeccionada para consumo del host.

A medida que el malware y el panorama de amenazas evolucionan, es importante revisar y examinar las reglas personalizadas existentes. A menudo se requieren actualizaciones para incorporar nuevos métodos de detección. RSA también actualiza ocasionalmente las reglas YARA en Live. Para recibir actualizaciones, puede suscribirse al blog de RSA y a RSA Live en http://blogs.rsa.com/feed.

En este documento se proporciona información para ayudar a los clientes a implementar reglas personalizadas de YARA en Malware Analysis.

Requisitos previos

El host en el cual está agregando reglas personalizadas debe estar configurado para ser compatible con la creación de reglas YARA, como se describe en "Habilitar contenido personalizado de YARA" en la *Guía de configuración de Malware Analysis*.

Versión y recursos de YARA

RSA Malware Analysis viene empaquetado con YARA versión 1.7 (rev.: 167). Para descubrir la versión exacta, puede ejecutar `yara -v` en el host de Malware Analysis, como se muestra en este ejemplo:

```
[root@TESTHOST yara] # yara -v
 yara 1.7 (rev:167)
```

Claves de metadatos en las reglas YARA

Malware Analysis es compatible con otros orígenes de reglas YARA y también consume claves de metadatos adicionales que son específicas de Malware Analysis. Cada regla YARA es equivalente a un indicador de riesgo (IOC) dentro de Malware Analysis. En el siguiente ejemplo se ilustran las definiciones de metadatos en una regla:

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Clave de metadatos	Descripción
iocName	(Requerido) Este es el nombre que usa MA como nombre de la regla. Es específico de Malware Analysis y se requiere para agregar la regla a la lista de IOC.
fileType	Especifica el tipo de archivo. Los valores posibles son: WINDOWS_PE, MS_OFFICE y PDF. Si no se especifica, el valor predeterminado es WINDOWS_PE.
puntaje	Este valor se agrega al puntaje estático si se activa la regla YARA. Si no se especifica, el valor predeterminado es 10.

Clave de metadatos	Descripción
ceiling	Esta es la cantidad máxima que se agrega a los puntajes estáticos cuando una regla se activa varias veces en una sesión. Por ejemplo, si cada vez que se activa una regla se agregan 20 puntos al puntaje estático y no se desea que se agreguen más de 40 puntos cuando la regla se activa más de dos veces, se puede especificar un límite de 40. Si no se especifica, el valor predeterminado es 100.
highConfidence	Esto configura el indicador de Alta confianza, el cual se establece en IOC cuando hay indicadores de alta confianza que delatan la presencia de malware. Si no se especifica, el valor de archivo predeterminado es false.

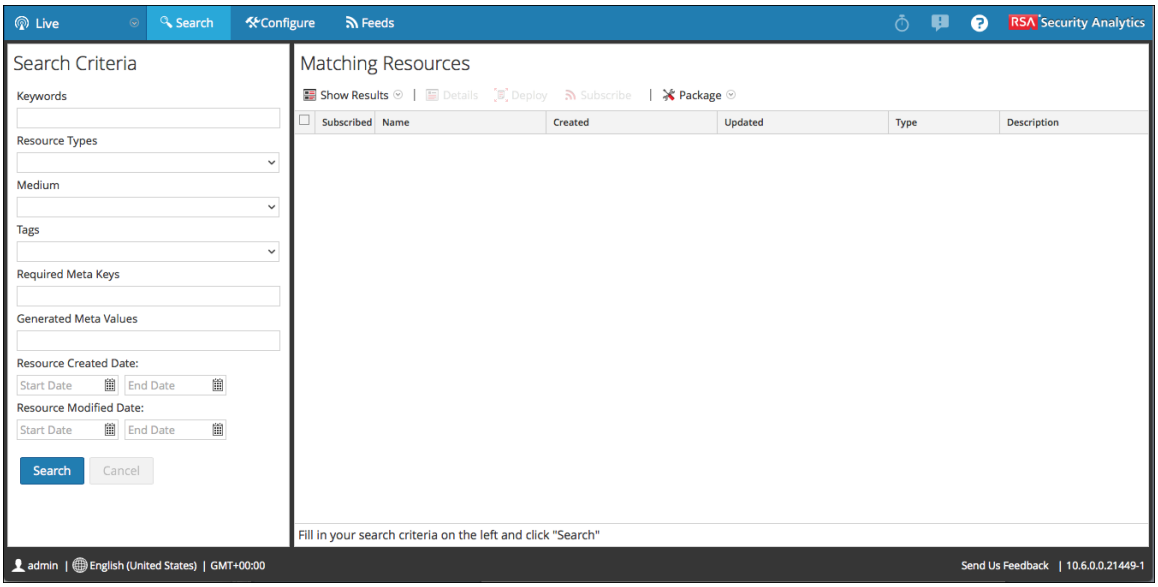
Nota: Consulte la siguiente URL para acceder a los recursos de YARA: https://code.google.com/p/yara-project/downloads/list. Security Analytics usa YARA 1.7, no YARA 2.0.

Contenido de YARA

RSA Live incluye tres conjuntos de reglas Yara:

- PE Packers
- PDF Artifacts
- PE Artifacts

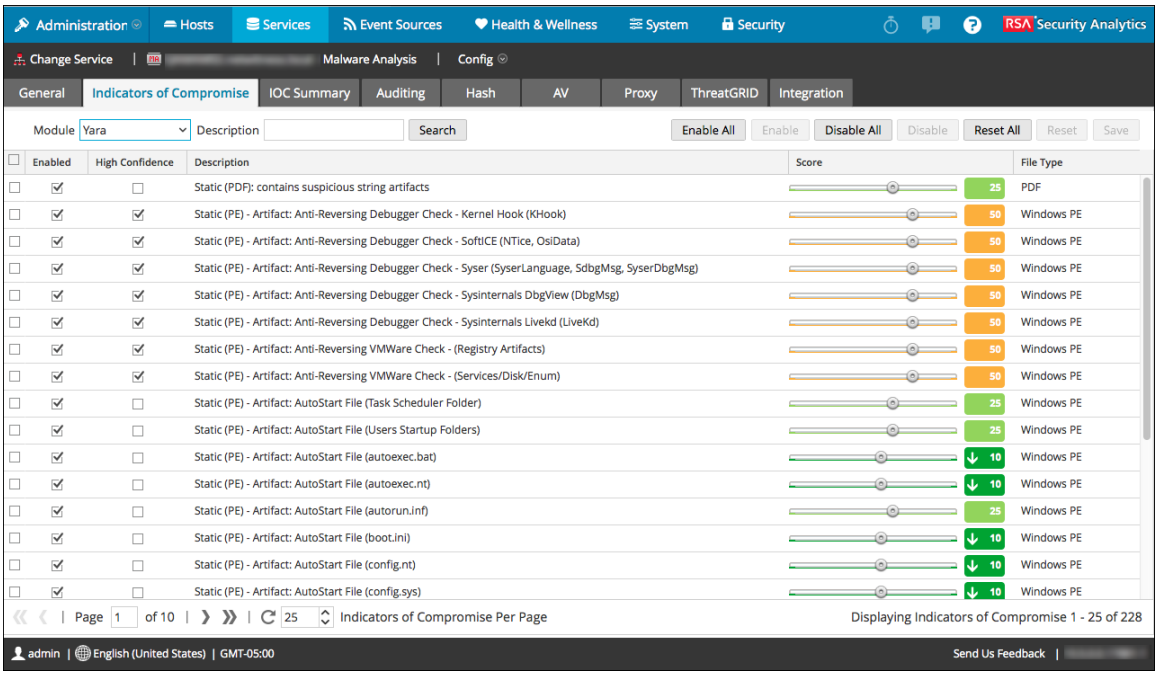
En la siguiente figura se ilustra el contenido de YARA disponible como reglas YARA en Security Analytics Live.



En el host de Malware Analysis, las reglas YARA residen en `/var/lib/rsamalware/spectrum/yara`, como se muestra en el siguiente ejemplo.

```
[root@TESTHOST yara]# pwd
 /var/lib/rsamalware/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_
packers.yara
```

Las reglas individuales se muestran como IOC en la vista Configuración del servicio Malware Analysis > pestaña Indicadores de riesgo. Para verlas, use el módulo Yara como filtro. Puede ajustar la configuración de una regla de la misma manera que configura otros IOC.



Agregar reglas YARA personalizadas

Para presentar reglas YARA personalizadas desde otros orígenes:

1. Para asegurarse de que las reglas YARA sigan la sintaxis y el formato correctos, use el comando YARA con el fin de compilar la regla YARA como se muestra en el siguiente ejemplo. Si la regla YARA se compila sin errores, esto indica que tiene la sintaxis correcta.

   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
   [root@TESTHOST yara]#
   ```

2. Asegúrese de que las reglas personalizadas no dupliquen reglas YARA existentes de RSA o de otros orígenes. Todas las reglas YARA se encuentran en `/var/lib/rsamalware/spectrum/yara`.

3. Asegúrese de que se incluyan las claves de metadatos compatibles con RSA para organizar las reglas YARA como parte de los IOC configurables y dé al archivo un nombre con la extensión yara (<filename>.yara). Para una mejor organización, asegúrese de que los metadatos `iocName` se incluyan en la sección de metadatos, como se muestra en el siguiente ejemplo.

   Ejemplo:

   ```
   rule HEX_EXAMPLE
   {
       meta:
           author = "RSA"
           info = "HEX Detection"
          iocName = "Hex Example"
        strings:
           $hex1 = { E2 34 A1 C8 23 FB }
           $wide_string = "Ausov" wide ascii
        condition:
           $hex1 or $wide_string
   }
   ```

4. Cuando esté listo, coloque el archivo de YARA personalizado en la carpeta que inspecciona el servicio Malware Analysis:

   `/var/lib/rsamalware/spectrum/yara/watch`

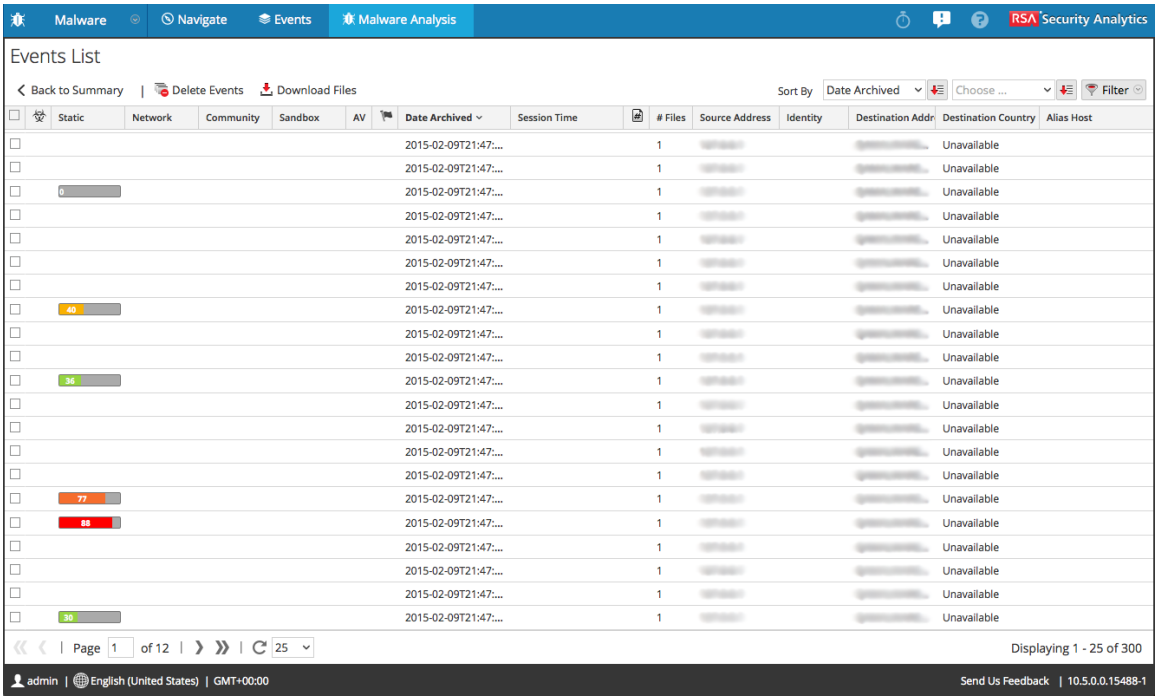
   El archivo se consume en un minuto.

   Cuando se consume, Security Analytics lo transfiere a la carpeta `processed` y la nueva regla se agrega a la vista Configuración de servicios > pestaña Indicadores de riesgo de Malware Analysis.

Examinar archivos y eventos de escaneo en formato de lista

En este tema se proporcionan instrucciones para ver archivos asociados con un evento en la Lista de archivos de Security Analytics Malware Analysis.

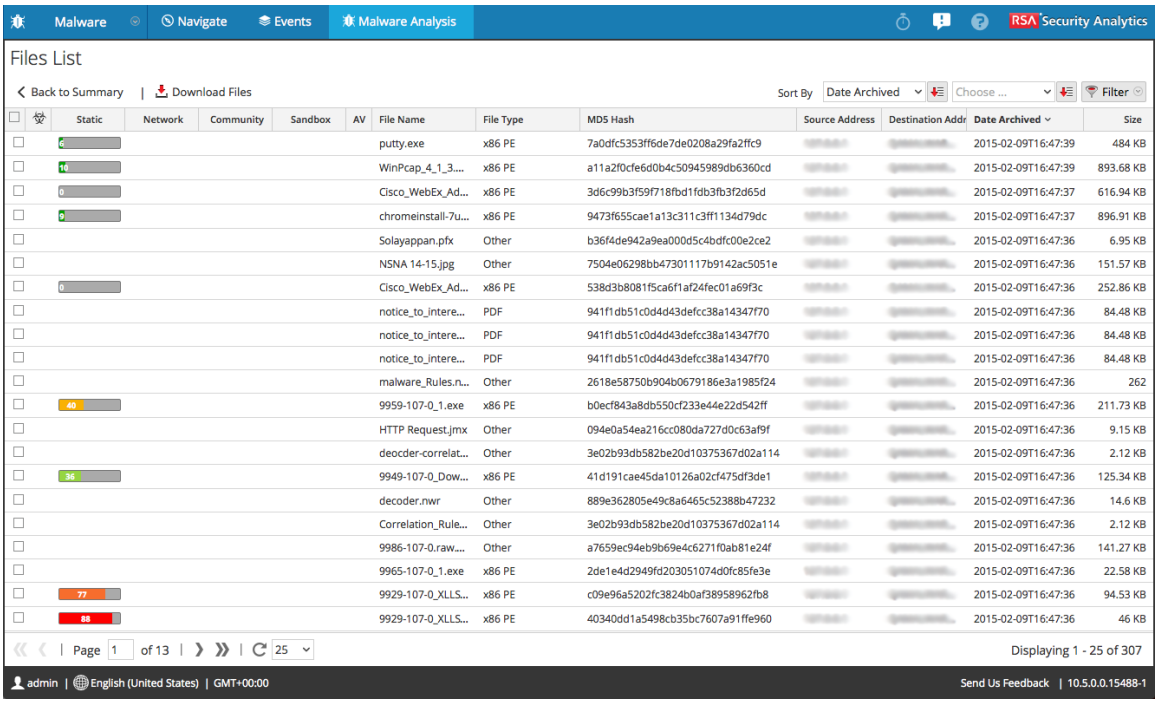
Cuando ve el Resumen de eventos en un escaneo de Security Analytics Malware Analysis, puede hacer clic en un conteo de archivos o en un conteo de eventos para ver la Lista de archivos o la Lista de eventos del escaneo (consulte Iniciar una investigación de Malware Analysis). En la Lista de archivos y la Lista de eventos, puede buscar un archivo por nombre de archivo o hash de archivo MD5, clasificar la lista mediante dos criterios y orden ascendente o descendente, y descargar archivos. Cuando encuentra un evento o archivo que el interesa en la Lista de eventos o Lista de archivos, puede ver muchos detalles sobre el evento en la vista Detalles de eventos.



Para cada evento de la Lista de eventos, Security Analytics proporciona la siguiente información:

- Marcado como un evento de alta confianza, que probablemente contenga indicadores de riesgo.
- El puntaje numérico de cada módulo de puntaje: Estático, Red, Community y Sandbox.
- Puntajes del proveedor de antivirus.
- El indicador Influido por regla personalizada.
- La fecha en que se archivó el evento.

- La hora de sesión.
- El filtro de hash de MD5.
- Cantidad de archivos en el evento.
- La dirección IP de origen del evento.
- La identidad.
- La dirección IP de destino.
- El país de destino.
- El nombre del host de alias.
- El tipo de evento, por ejemplo, Network.
- El servicio que utiliza el evento.
- La organización de destino



Para cada archivo en la Lista de archivos, Security Analytics proporciona la siguiente información:

- Marcado como un evento de alta confianza, que probablemente contenga indicadores de riesgo.
- El puntaje numérico de cada módulo de puntaje: Estático, Red, Community y Sandbox.

- Puntajes del proveedor de antivirus.
- El nombre de archivo.
- El tipo de archivo.
- El filtro de hash de MD5.
- La dirección IP de origen del evento que contenía el archivo.
- La dirección IP de destino.
- La fecha en que se archivó el evento que contenía el archivo.
- El tamaño del archivo.

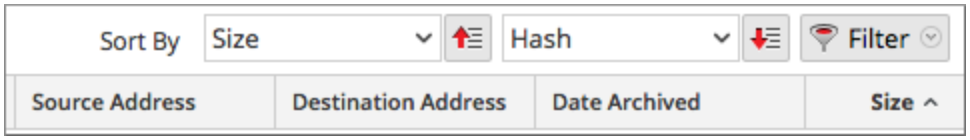
Clasificar la Lista de archivos o la Lista de eventos

Puede clasificar la Lista de archivos y la Lista de eventos por nombre de columna en orden ascendente y descendente. Puede elegir una o dos columnas.

Para clasificar la lista:

1. En la primera lista desplegable **Ordenar por**, elija un nombre de columna y una dirección de clasificación: para el orden descendente o para el orden ascendente.
2. (Opcional) En la segunda lista desplegable **Ordenar por**, elija un nombre de columna y una dirección de clasificación, para el orden descendente o para el orden ascendente.

   Los títulos de las columnas reflejan el orden de clasificación seleccionado. En el siguiente ejemplo, la columna Hash se clasifica en orden ascendente y la columna Tamaño se clasifica en orden descendente.



Filtrar la lista por nombre de archivo o hash de archivo MD5

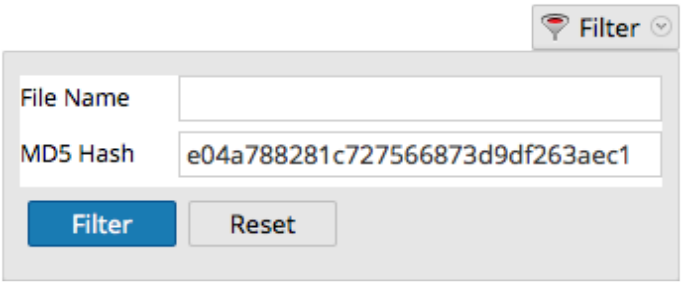
Puede filtrar la Lista de archivos y la Lista de eventos por nombre de archivo o hash de archivo. Con esta función, puede especificar un subconjunto limitado de los datos originales en función de los criterios de búsqueda.

Nota: Cuando realiza una búsqueda, se busca el escaneo que está visualizando actualmente, no todos los escaneos.

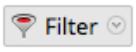
1. Haga clic en Filter.

   Se muestra el cuadro de diálogo Filtrar.

2. Ingrese un valor en **Nombre de archivo** o **Hash de MD5** y haga clic en **Filtrar**. Los campos Nombre de archivo y Hash de archivo no distinguen mayúsculas de minúsculas. No se admiten comodines o expresiones regulares. El filtro se basa en coincidencias exactas. Puede arrastrar un nombre de archivo o hash que desee seleccionar desde la Lista de archivos o la Lista de eventos y, a continuación, copiarlo y pegarlo en el cuadro de diálogo.



3. Haga clic en **Filtrar**.
   Malware Analysis filtra la lista para mostrar solo archivos o eventos con el hash seleccionado.

4. Para revertir a la lista no filtrada, haga clic en 

. Cuando aparezca el cuadro de diálogo Filtrar, haga clic en **Restablecer**.

Descargar archivos de la Lista de archivos

Security Analytics permite seleccionar y descargar archivos de la Lista de archivos o la Lista de eventos.

Precaución: Sea precavido cuando descargue archivos desde Malware Analysis; algunos archivos pueden contener código dañino. La descarga de archivos es un permiso específico que se puede configurar. Consulte "Definir funciones y permisos para analistas de malware" en la *Guía de configuración de Malware Analysis* para obtener más detalles.

Para descargar archivos de la Lista de archivos o la Lista de eventos:

1. En la **Lista de archivos** o la **Lista de eventos**, seleccione la casilla de verificación junto a una o más filas.
2. En la barra de herramientas, seleccione 

.
   Se muestra el cuadro de diálogo Descarga de archivo de malware.
3. Realice una de las siguientes acciones
   a. Si decide no descargar el archivo, haga clic en **Cancelar**.

b. Si desea descargar el archivo, haga clic en el botón **Descargar**.
El archivo o los archivos seleccionados se descargar en un archivo zip con el nombre `Malware_Files.zip`.

Eliminar eventos del escaneo

En la Lista de eventos, seleccione uno o más eventos y elimínelos del escaneo. Esto es útil para eliminar eventos que no le interesan.

Para eliminar un evento del escaneo que se visualiza:

1. En la **Lista de eventos**, seleccione uno o más eventos.
2. En la barra de herramientas, haga clic en 

.
Security Analytics solicita confirmar la intención de eliminar los eventos.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.
Se eliminan los eventos seleccionados.

Volver al resumen de eventos

Para salir de la Lista de archivos o la Lista de eventos y volver al Resumen de eventos, haga clic en **Volver al resumen**.

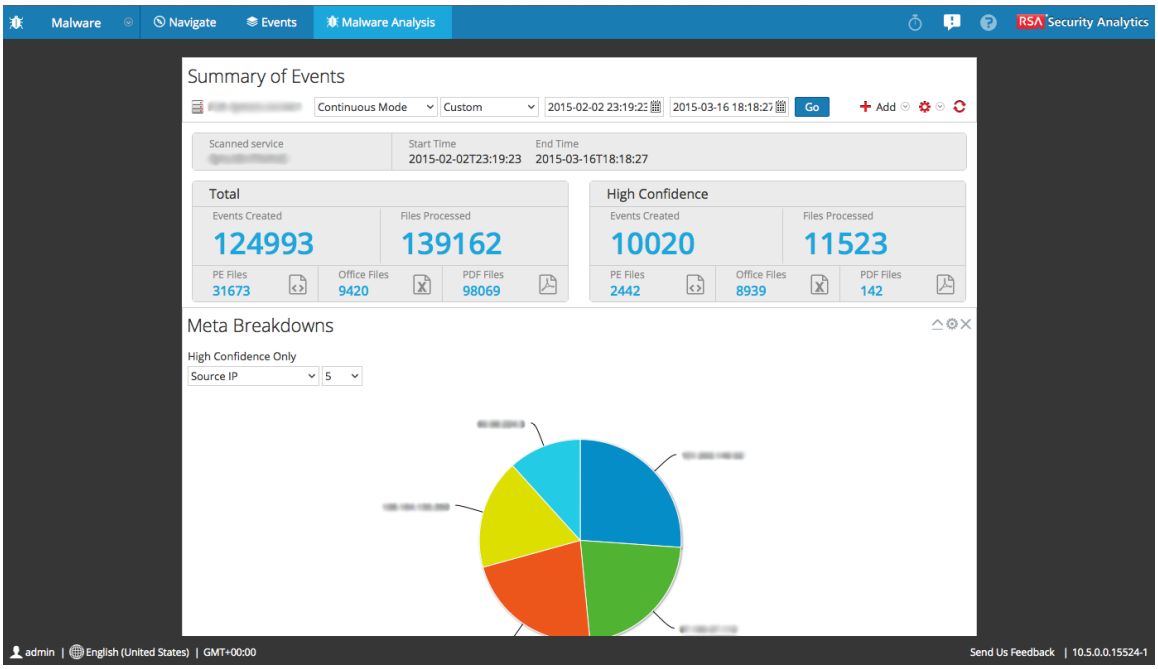
Abra el análisis detallado de un evento

Mientras examina eventos o archivos en la Lista de archivos o la Lista de eventos, puede hacer doble clic en cualquier evento o archivo para abrir un análisis detallado del evento en la Lista de eventos o el evento con el cual está asociado el archivo en la Lista de archivos (consulte Ver detalles de Malware Analysis de un evento).

Filtrar datos de dashlets en la vista Resumen de eventos

En este tema se proporcionan instrucciones para que los analistas filtren datos en los dashlets que se ven en la vista Resumen de eventos de Security Analytics Malware.

La vista Resumen de eventos ofrece un resumen del escaneo que se investiga e incluye dashlets seleccionables. El Resumen de eventos es fijo, pero los analistas pueden configurar cada dashlet para filtrar la información y desglosar los datos.



El resto de este tema proporciona instrucciones para administrar y configurar los dashlets.

Configurar el dashlet Rueda de puntaje

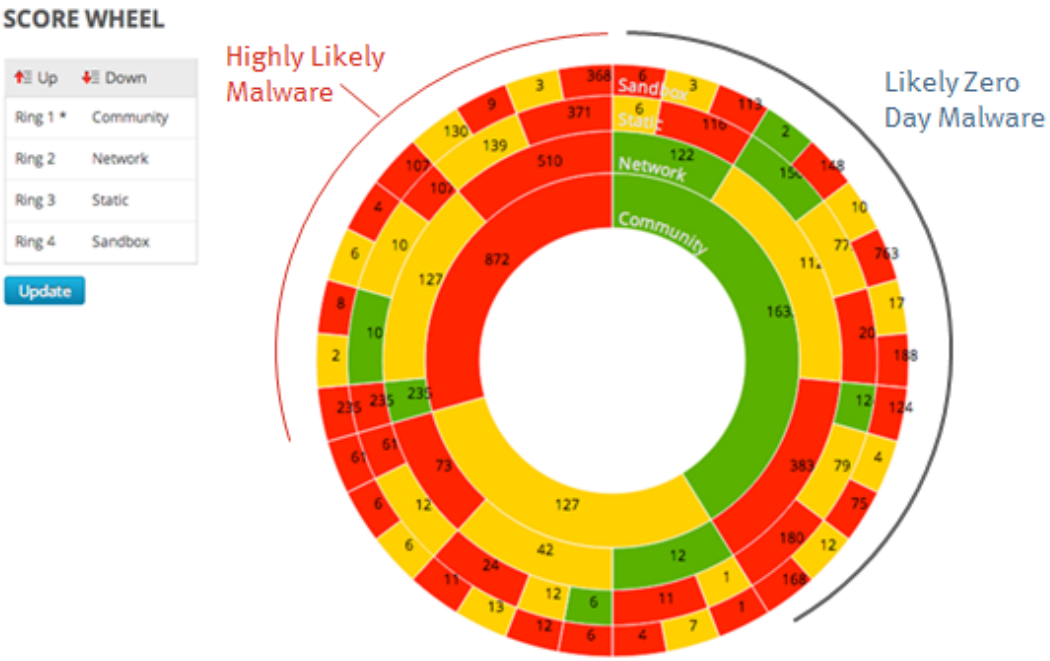
La Rueda de puntaje es una visualización general de las sesiones analizadas que puntuaron alto, medio o bajo en cada una de las categorías de puntaje: Estático, Red, Community y Sandbox. La Rueda de puntaje es una forma rápida de desglosar las sesiones para revisarlas. Cada anillo representa una categoría de puntaje diferente, de modo que pueda comparar visualmente los resultados por categoría.

Puede cambiar el orden de los anillos para resaltar los indicadores de riesgo que se marcaron en una categoría, pero no en otra. La comparación de los mismos resultados en una secuencia de anillos diferente proporciona visibilidad de las vulnerabilidades adicionales en una sesión y se permite desglosar a sesiones de interés. En los siguientes ejemplos se muestran dos posibles casos de uso.

Ejemplo de candidatos de día cero

En este ejemplo se muestra cómo desglosar sesiones que Community no marcó como maliciosas, pero que todas las demás categorías de puntaje marcaron como maliciosas. La lista de sesiones resultante resalta los candidatos de día cero.

1. Configure los anillos de la rueda de puntaje en la siguiente secuencia:
   Community (más interior) > **Estático** > **Red** > **Sandbox** (más exterior)
2. Haga clic en el segmento rojo del anillo más exterior (Sandbox) que se alinea con un segmento verde del anillo más interior (Comunidad): verde (más interior) -> **Estático**: rojo -> **Red**: rojo -> **Sandbox**: rojo (más exterior).



Ejemplo de sesiones maliciosas

En este ejemplo se muestra cómo desglosar sesiones en las que todas las categorías de puntaje identifican la lista de sesiones resultante como maliciosa, lo cual indica que Malware Analysis tiene la máxima confianza de que corresponden a malware.

1. Configure los anillos de la rueda de puntaje en la siguiente secuencia:
   Community (más interior) > **Estático** > **Red** > **Sandbox** (más exterior)
2. Haga clic en el segmento rojo del anillo más exterior (Sandbox) que se alinea con un segmento rojo del anillo más interior (Comunidad): rojo (más interior) -> Estático: rojo -> Red: rojo -> Sandbox: Red (más exterior).

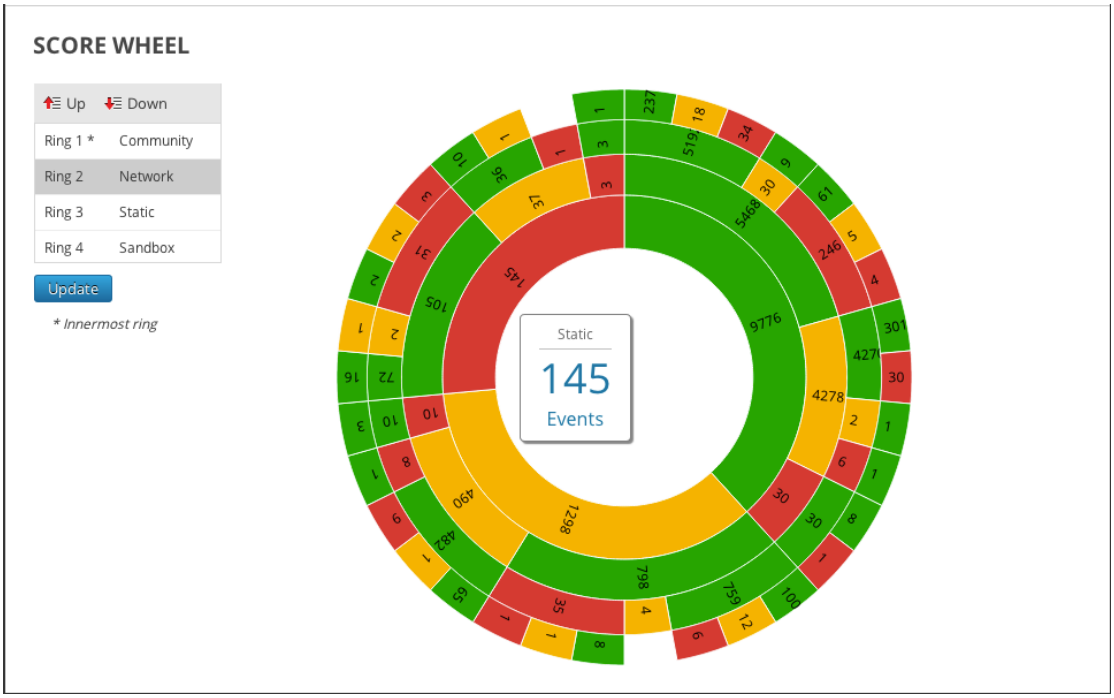
Organizar la secuencia de los anillos por módulo de puntaje

En la Rueda de puntaje, puede organizar la secuencia de los anillos por módulo de puntaje. Inicialmente, la secuencia de anillos del interior al exterior es Estático, Red, Community y Sandbox.

Para cambiar la secuencia de los anillos:

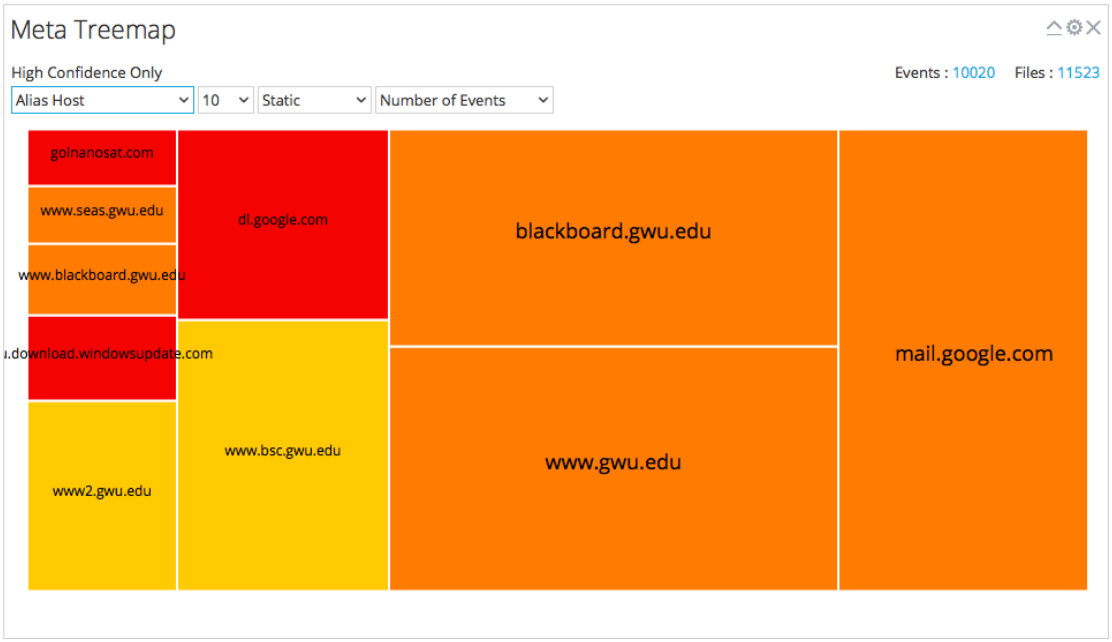
1. Realice una de las siguientes acciones
   a. Haga clic y arrastre cada módulo de puntaje hacia arriba o abajo.
   b. Seleccione cada módulo de puntaje y utilice los botones Arriba y Abajo para transferirlo.

2. Cuando esté conforme con la secuencia de anillos, haga clic en el botón **Actualizar**.
   La Rueda de puntaje se actualiza con la nueva secuencia.



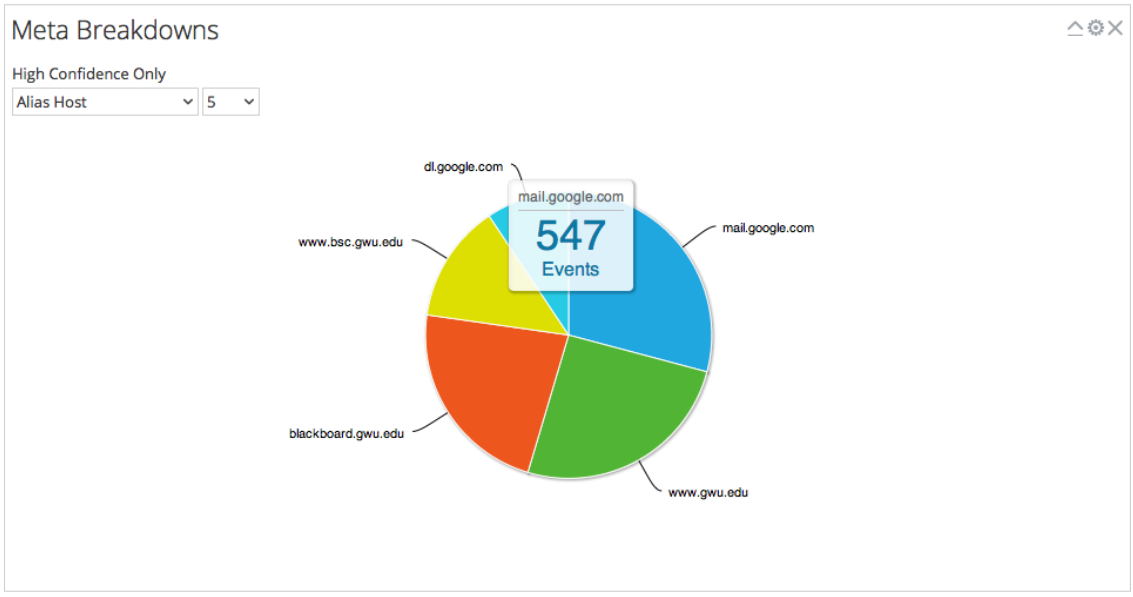
Configurar el dashlet Mapa de árbol de metadatos

En el gráfico Mapa de árbol de metadatos, puede visualizar y filtrar desgloses de metadatos por tipo, conteo y tipo de análisis de metadatos. Utilice las tres listas de selección para definir el filtro y el gráfico Mapa de árbol de metadatos se actualiza inmediatamente.



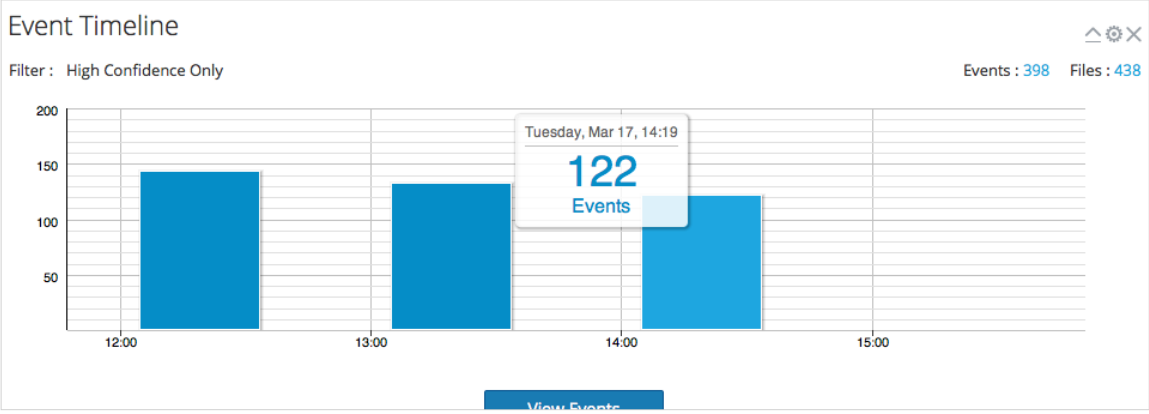
Configurar el dashlet Desgloses de metadatos

El dashlet Desgloses de metadatos es una visualización de valores para una clave de metadatos específica en un gráfico circular. En el gráfico Desgloses de metadatos, puede filtrar desgloses de metadatos por tipo y conteo de metadatos. Utilice las dos listas de selección para definir el filtro y el gráfico Desgloses de metadatos se actualiza inmediatamente.



Configurar el dashlet Cronograma de eventos

El dashlet Cronograma de eventos es una visualización de los eventos en un cronograma. No hay filtros adicionales disponibles para el Cronograma de evento.

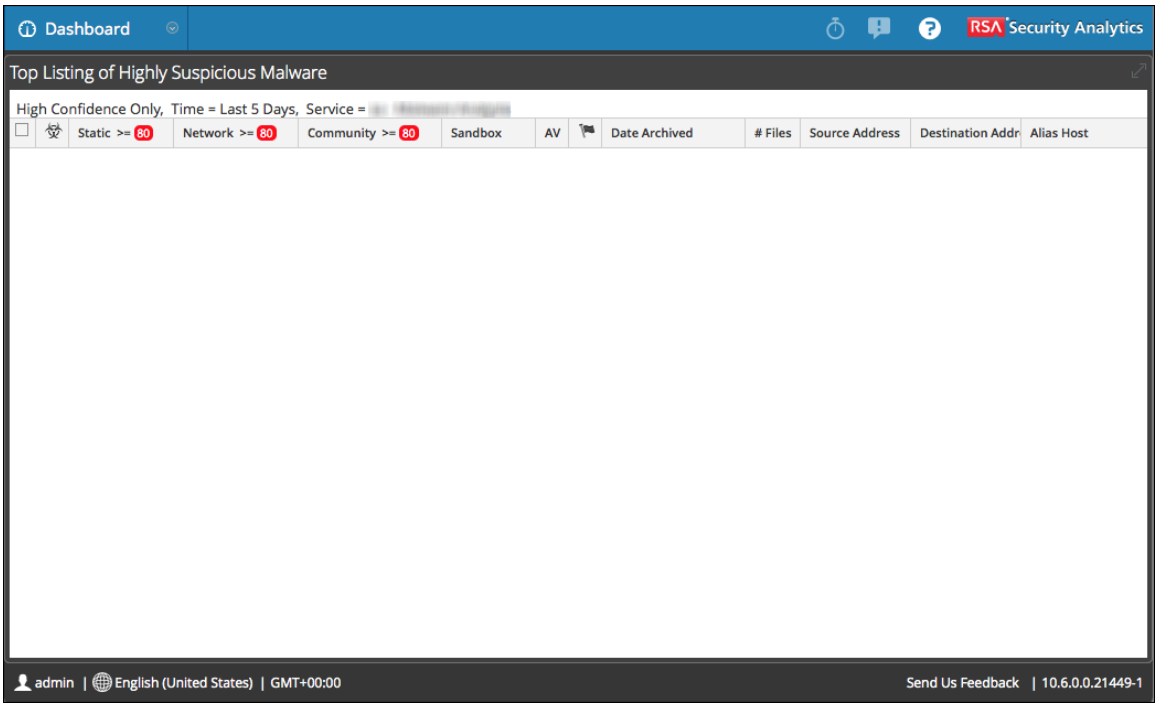


Abrir todos los eventos en la lista de eventos

Desde el interior del Cronograma de evento, puede abrir toda la lista de eventos en la Lista de eventos. Para hacerlo, haga clic en View Events. Esta opción no es igual que hacer clic en el conteo junto a Eventos, que es el mismo para todos los gráficos de visualización y abre el punto de desglose actual en la Lista de eventos.

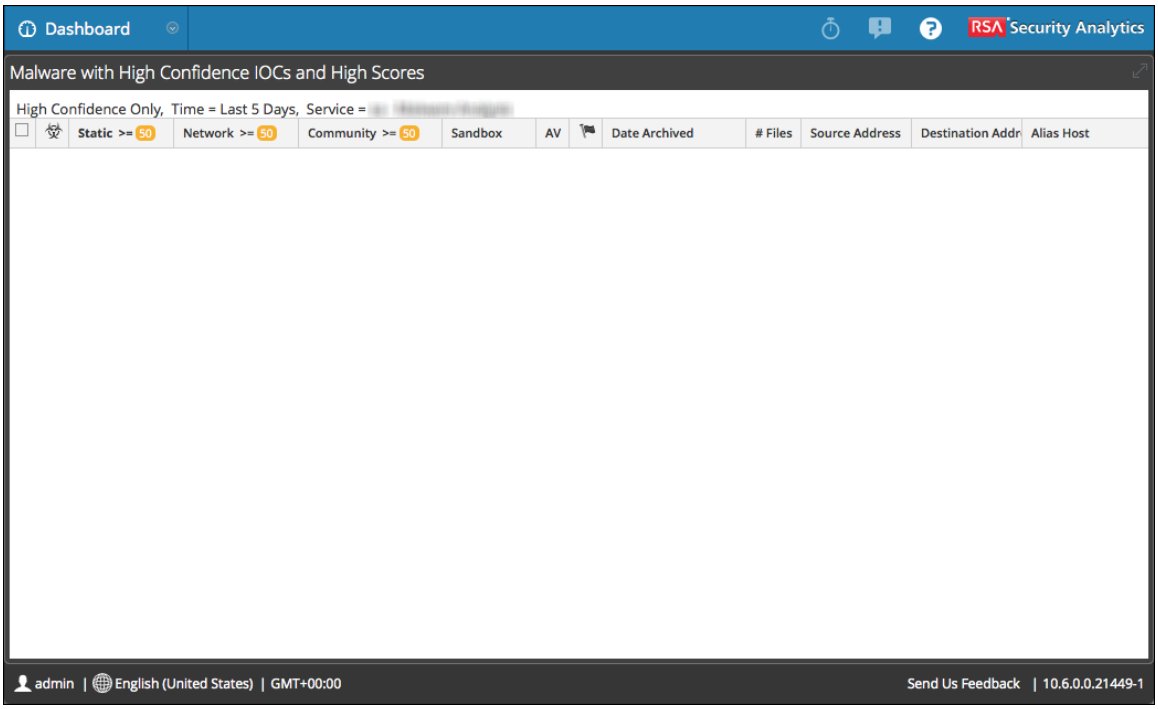
Configure el dashlet Lista del malware altamente sospechoso principal

El dashlet Lista del malware altamente sospechoso principal presenta los 10 eventos más sospechosos en la Lista de eventos o en la Lista de archivos. Este dashlet también está disponible en el tablero Unified y las opciones de configuración se describen en la *Guía de introducción de Security Analytics*.


Dashboard
RSA Security Analytics
Top Listing of Highly Suspicious Malware
High Confidence Only, Time = Last 5 Days, Service =
Static >= 80
Network >= 80
Community >= 80
Sandbox
AV
Date Archived
Files
Source Address
Destination Addr
Alias Host
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.21449-1

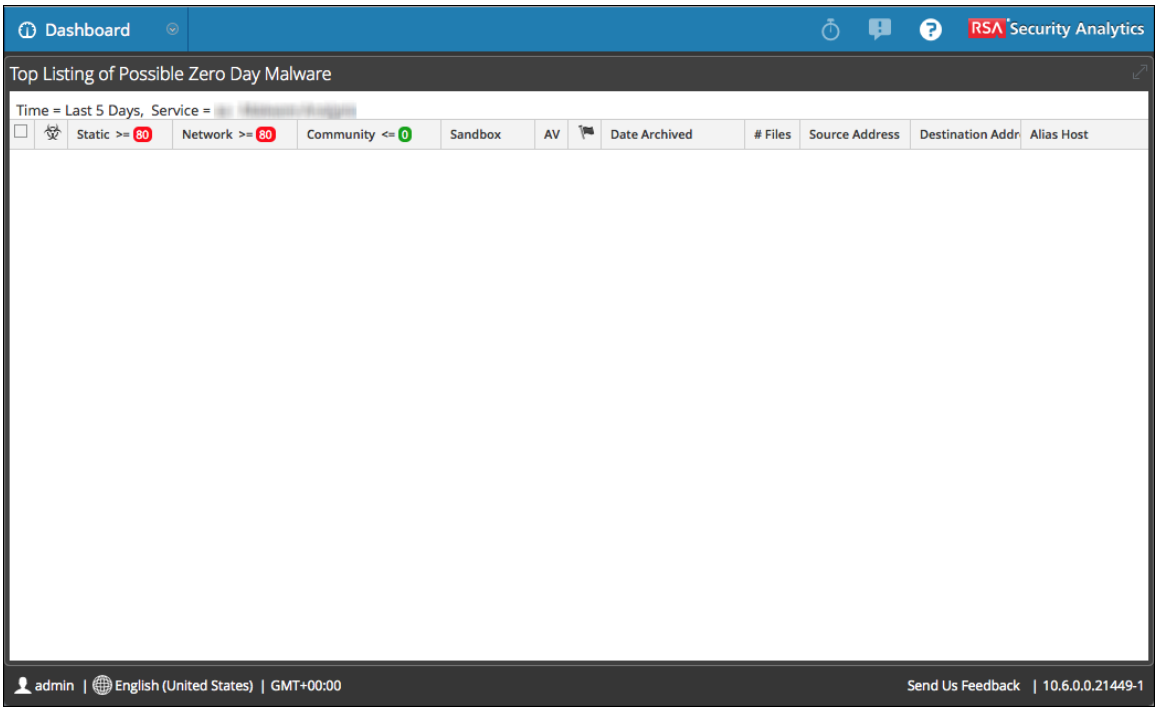
Configurar el dashlet Malware con IOC de alta confianza y altos puntajes

El dashlet Malware con IOC de alta confianza y altos puntajes presenta indicadores de riesgo que tienen puntajes altos y confianza alta de que es probable que los eventos contengan malware. El dashlet también está disponible en el tablero Unified y las opciones de configuración se describen en Dashlet Malware con IOC de alta confianza y altos puntajes en la *Guía de introducción de Security Analytics*.



Configurar el dashlet Lista del posible malware de día cero principal

El dashlet Lista del posible malware de día cero principal presenta posibles eventos de día cero en la Lista de eventos o la Lista de archivos. El dashlet también está disponible en el tablero Unified y las opciones de configuración se describen en la *Guía de introducción de Security Analytics*.



Cargar archivos para escaneo de Malware Analysis

Existen dos métodos para que los analistas carguen archivos para su escaneo en Malware Analysis.

Un analista de malware con permiso para **Iniciar escaneo de Malware Analysis** puede cargar archivos para escanear mediante la opción Escanear archivos del cuadro de diálogo Seleccionar un servicio Malware Analysis.

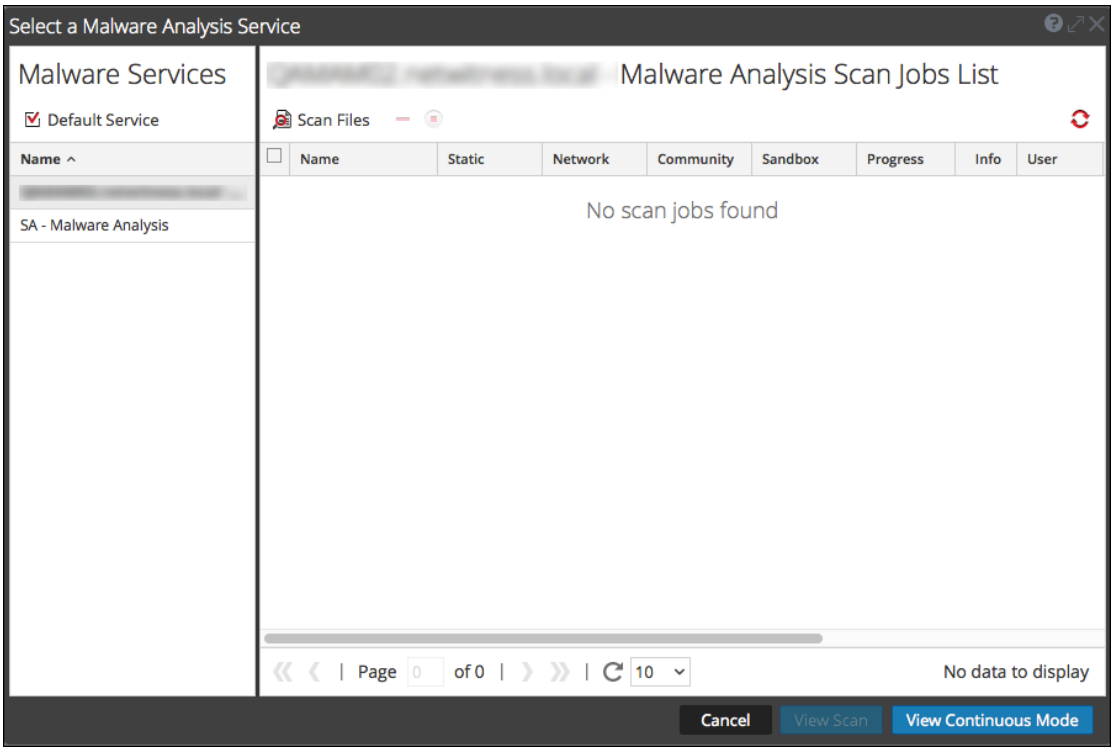
También es posible cargar un archivo para su escaneo mediante un recurso compartido de archivos inspeccionados.

Cargar archivos manualmente

En este tema se proporcionan instrucciones para iniciar un escaneo por demanda de un archivo cargado. Cuando se carga un archivo para su escaneo, Security Analytics inicia el trabajo de carga y lo agrega a la línea de espera de trabajos. Cuando el trabajo ha finalizado, puede ver el escaneo en la pestaña **Investigation** > **Malware Analysis**.

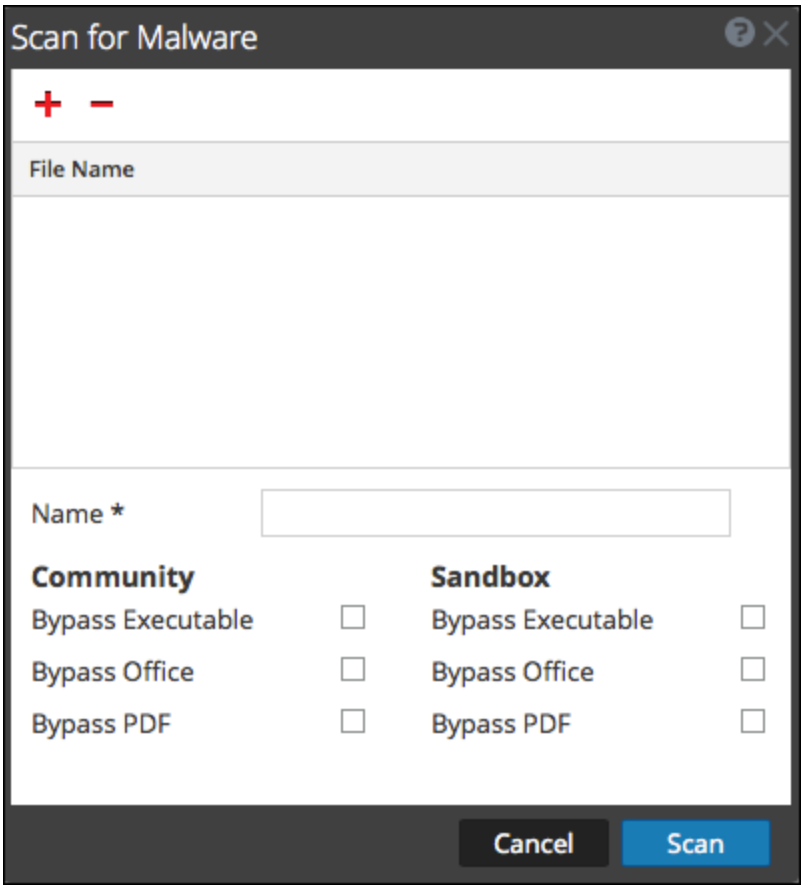
Para cargar un archivo para escanear:

1. En el menú de **Security Analytics**, seleccione **Investigation > Malware Analysis**.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis con hosts y servicios de Malware Analysis disponibles para el usuario actual en el panel de la izquierda.



2. Haga clic en **Ver escaneo**.

   Aparece el dashlet Escanear para encontrar malware.



3. Haga clic en +

   Se muestra una vista del sistema de archivos que permite elegir los archivos que se cargarán.

4. Seleccione uno o más archivos de la lista y haga clic en **Abrir**.

   Se agregan los nombres de archivo.

5. Continúe agregando y eliminando archivos hasta que tenga una lista de los archivos que desea cargar.

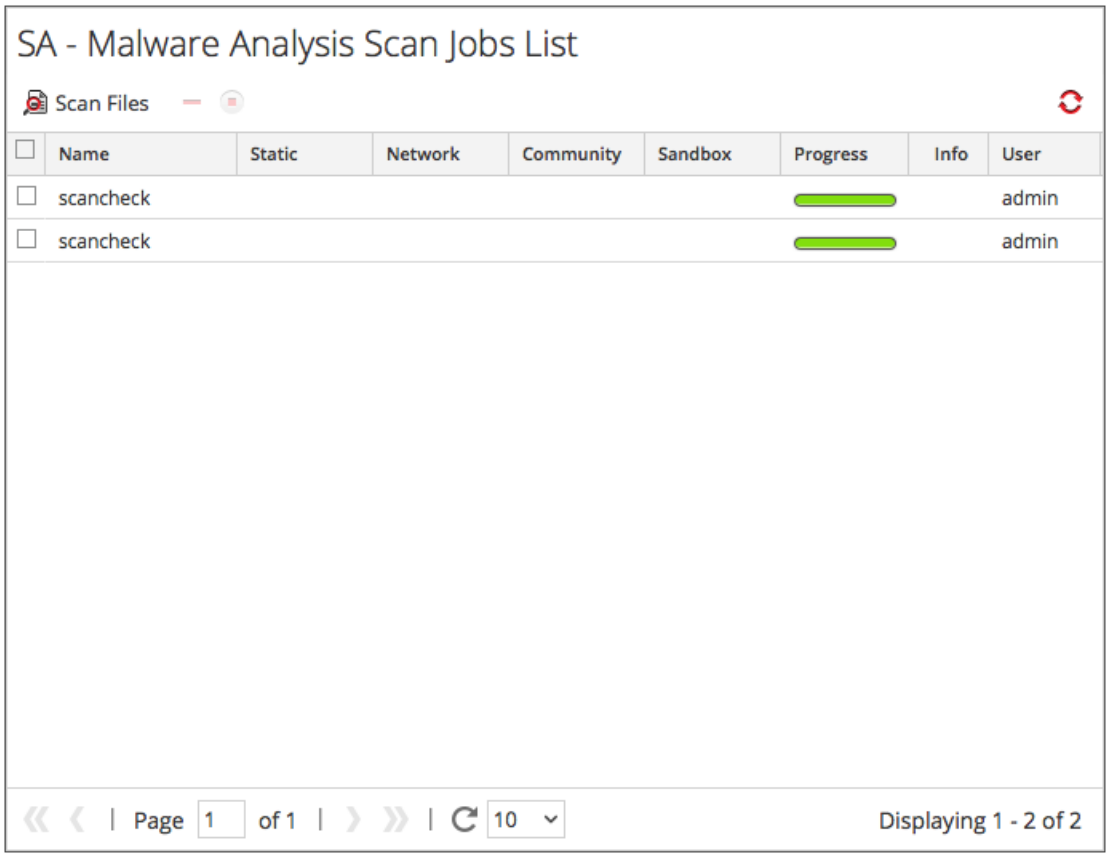
6. Nombre el escaneo y seleccione los tipos de archivos que desea omitir. Esto es útil para un archivo .zip que contenga tipos de archivos diferentes y sobrescribe la configuración de omisión predeterminada.

7. Haga clic en **Escanear**.

   El trabajo de escaneo se envía y Security Analytics muestra un mensaje de confirmación que indica que el envío se realizó correctamente. La solicitud de escaneo se agrega al dashlet Lista de trabajos de escaneo. La configuración de omisión en este cuadro de diálogo

reemplaza a la configuración predeterminada definida en los ajustes de configuración básicos de Malware Analysis.

8. El trabajo se agrega a la Lista de trabajos de escaneo del cuadro de diálogo Seleccionar un servicio Malware Analysis y del dashlet Lista de trabajos de escaneo del tablero Unified.



9. Para ver el escaneo cuando finalice, haga doble clic en el escaneo.
   Se muestra el Resumen de eventos de malware del escaneo seleccionado.

Cargar archivos desde una carpeta inspeccionada

Para cargar archivos desde una carpeta inspeccionada, puede soltarlos en un recurso compartido de archivo inspeccionado para Malware Analysis. Los analistas pueden compartir reglas YARA, archivos de hash y archivos zip infectados con Malware Analysis.

Security Analytics Malware Analysis inspecciona un recurso compartido de archivo y consume automáticamente los archivos que se colocan en carpetas específicas de dicho recurso compartido. Esta función es útil para:

- La importación en masa de archivos de hash desde `/var/lib/rsamalware/spectrum/hashWatch`.

- La adición de reglas YARA personalizadas a la lista de indicadores de riesgo (IOC) en el host desde `/var/lib/rsamalware/spectrum/yara/watch`.
- La creación de trabajos de escaneo según demanda a partir de un archivo Zip de archivos Zip infectados desde `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Los analistas deben preparar los archivos para el consumo de acuerdo con los requisitos, la extensión del archivo debe estar correcta y el archivo debe copiarse a la carpeta inspeccionada correcta en el recurso compartido de archivo.

Importar una lista de hash

Para importar una lista de hash desde el directorio inspeccionado, la lista debe tener el formato especificado y estar clasificada por md5. Puede soltar un archivo con formato en una carpeta (/var/lib/rsamalware/spectrum/hashWatch) del host de Malware Analysis y se importará automáticamente a la base de datos de hash local. Esto se describe en "Configurar el filtro de hash" en la *Guía de configuración de Malware Analysis*.

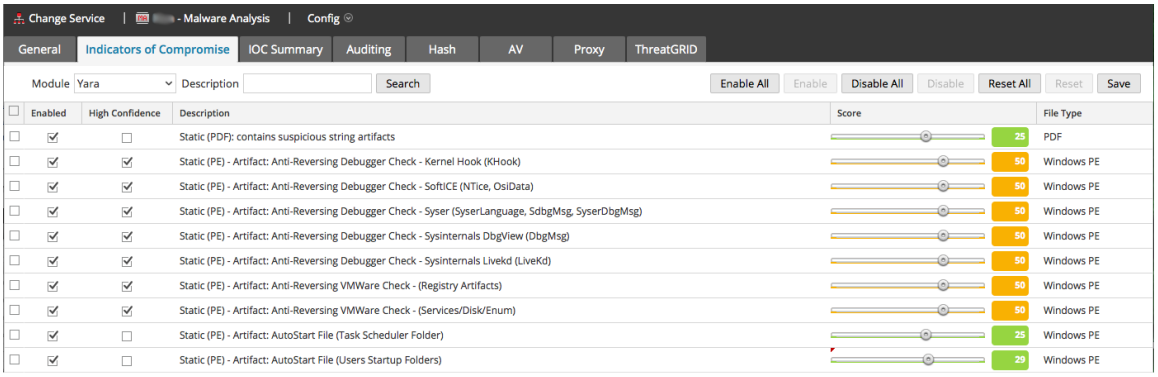
Para importar una lista de hash mediante el método de carpeta inspeccionada:

1. Copie las listas de hash que desea importar al directorio **/var/lib/rsamalware/spectrum/hashWatch**.
   Security Analytics Malware Analysis inspecciona automáticamente esta carpeta y procesa los archivos que contiene.
   a. Security Analytics Malware Analysis agrega cada hash encontrado en las listas de hash al filtro de hash.
   b. Si se producen errores de procesamiento, estos se registran en: **/var/lib/rsamalware/spectrum/hashWatch/error**
   c. Los archivos procesados se catalogan aquí: **/var/lib/rsamalware/spectrum/hashWatch/processed**
   d. Los archivos procesados no se eliminan del directorio hashWatch.
2. Después de importar hashes de forma masiva, el administrador del sistema puede usar un cronjob para limpiar archivos procesados antiguos.

Importar reglas YARA a la lista de IOC

Los clientes con habilidades y conocimientos avanzados pueden agregar funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live o la colocación de estas reglas en una carpeta inspeccionada para consumo del host. En Implementar contenido personalizado de YARA se proporciona información completa sobre los requisitos previos para el uso de contenido personalizado de YARA y la creación de reglas.

Cuando las reglas estén listas, coloque los archivos de YARA personalizados en la carpeta que inspecciona el servicio Malware Analysis:
`/var/lib/rsamalware/spectrum/yara/watch`
El archivo se consume en un minuto.
Cuando se consume, Security Analytics lo transfiere a la carpeta `processed` y la nueva regla se agrega a la vista Configuración del servicio Malware Analysis > pestaña Indicadores de riesgo.



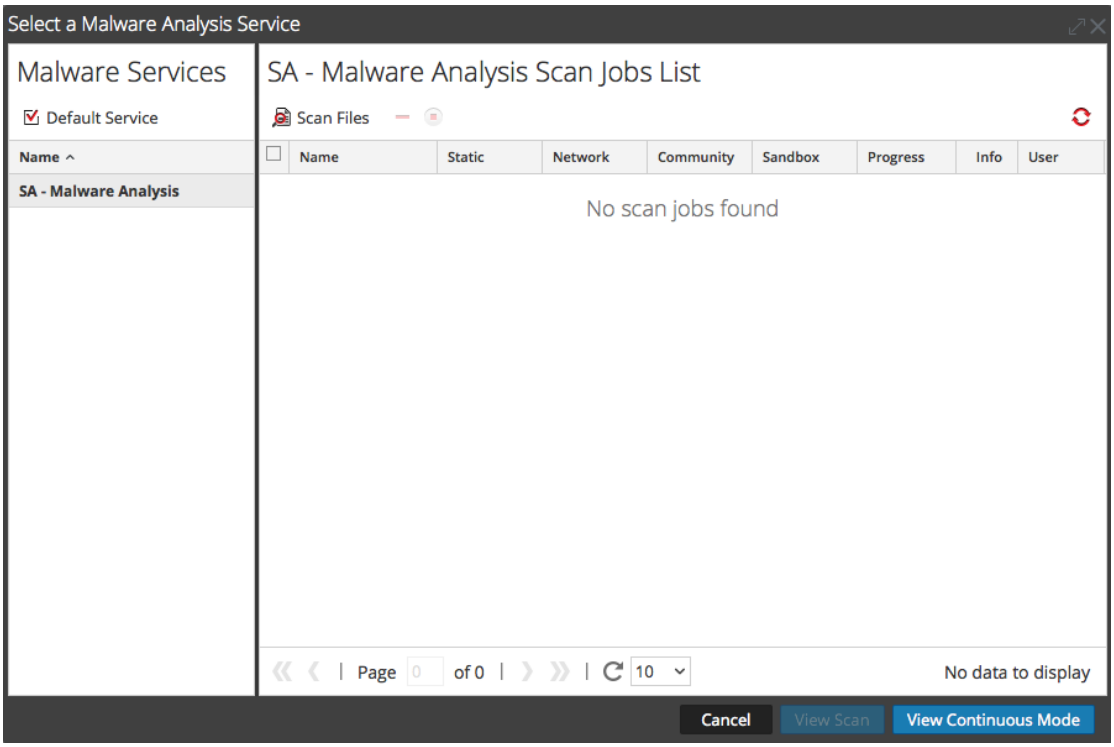
Importar archivos a la Lista de trabajos de escaneo

Cuando obtiene muestras de soluciones de seguridad perimetral y desea realizar un análisis adicional de los archivos, puede comprimirlos y proteger el archivo con `infected` y, a continuación, agregarlo a la carpeta inspeccionada para que Malware Analysis lo consuma. Este archivo comprimido se puede colocar en la carpeta inspeccionada:
`/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Nota: El tamaño máximo del archivo es 100 MB.

Para analizar archivos zip protegidos con contraseña que están infectados, Malware Analysis consume los archivos que se colocan en una carpeta inspeccionada y crea un trabajo según demanda que se agrega a la Lista de trabajos de escaneo.

1. Cuando haya iniciado sesión como administrador, coloque los archivos que se procesarán en un archivo zip con la contraseña `infected` en
   `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   En uno o dos minutos, Malware Analysis consumirá el archivo y creará un trabajo según demanda en la Lista de trabajos de escaneo. El nombre del trabajo de escaneo es el nombre del archivo, el usuario es **file share**, y el tipo de evento es 1. El archivo se transfiere a
   `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`



2. Cuando el trabajo se haya agregado a la Lista de trabajos de escaneo, ejecute un script o un cronjob para limpiar el archivo Zip en `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`.

Ver detalles de Malware Analysis de un evento

En este tema se proporcionan instrucciones para ver detalles de un evento en la cuadrícula Eventos de Security Analytics Malware Analysis.

Al ver la lista de eventos individuales en un escaneo de Security Analytics Malware Analysis en la cuadrícula Eventos de Malware Analysis, puede hacer doble clic en un evento para ver los resultados de análisis detallados para el evento.

Ver detalles de Malware Analysis para un evento

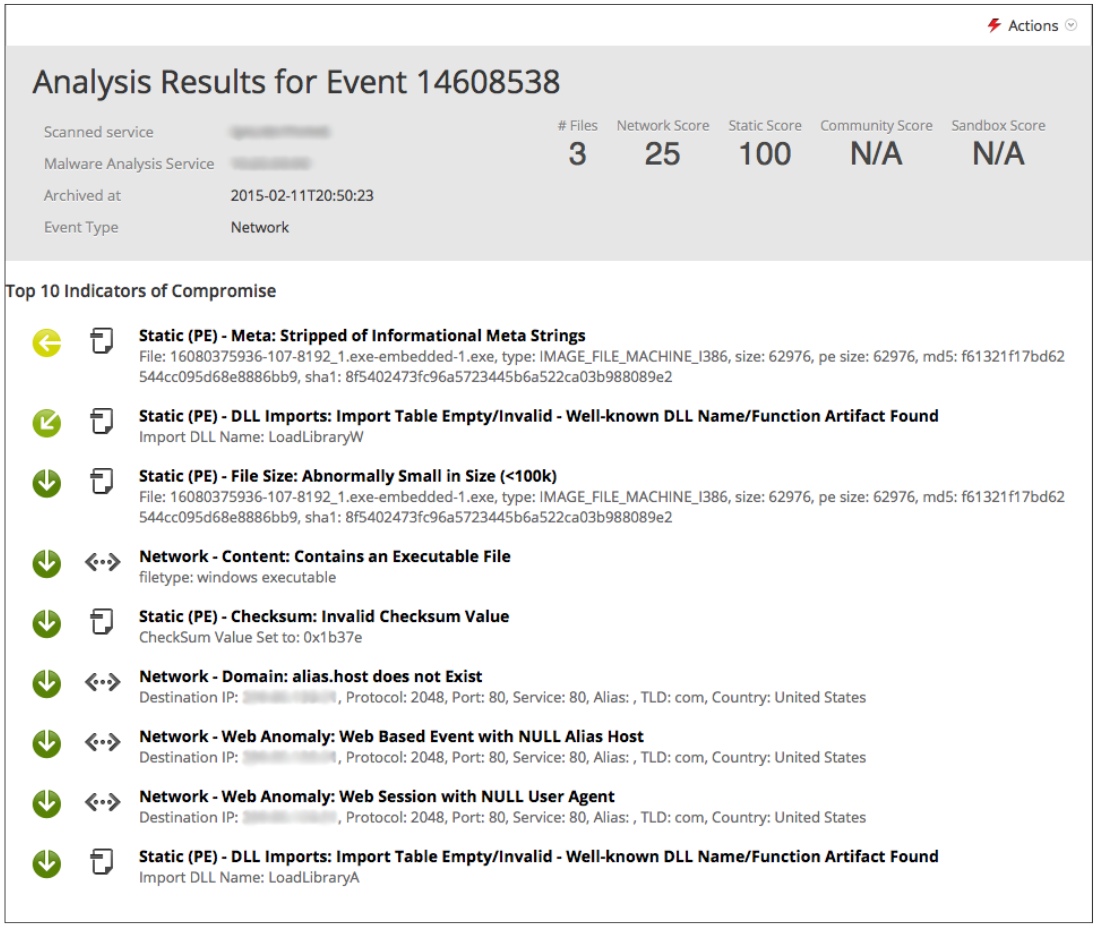
1. Inicie una investigación en la pestaña **Investigation > Malware Analysis**.
   Se muestra el Resumen de eventos de malware, el cual incluye cuatro gráficos, entre ellos, el Cronograma de evento.
2. Realice una de las siguientes acciones
   a. Para ver todos los eventos en el Cronograma de evento, haga clic en el botón **Ver eventos**. .

b. Haga doble clic en **Desglose de metadatos**, **Gráfico de mapa de árbol de metadatos** o **Rueda de puntaje**.

Se muestra la Lista de eventos.

3. Haga doble clic en un evento.

Se muestran los resultados del análisis para el evento.



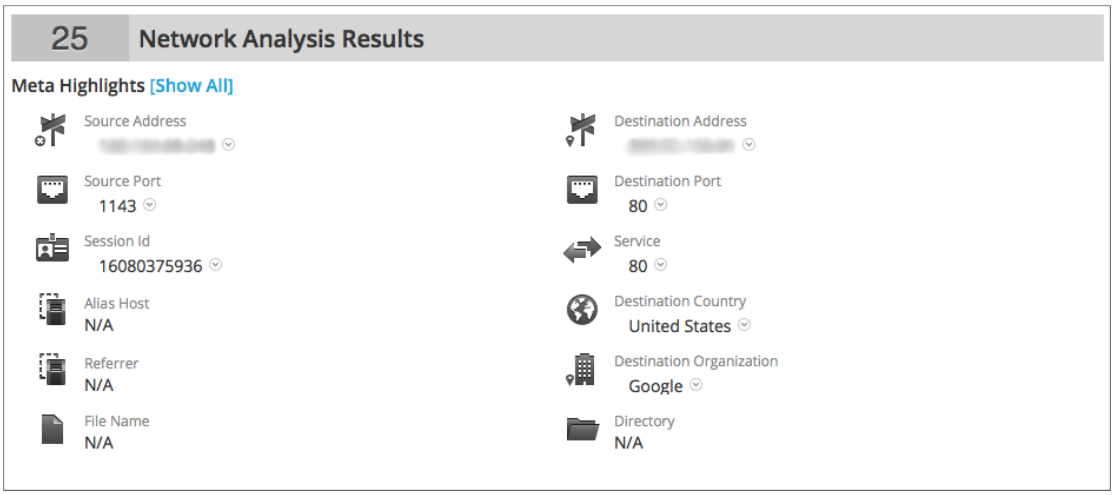
4. (Opcional) Si desea eliminar un evento, seleccione **Acciones > Eliminar evento**.
5. Si desea ver una reconstrucción de la sesión de red, seleccione **Acciones > Ver sesión de red**.

La sesión se abre en la vista Navegar > Reconstrucción de evento.

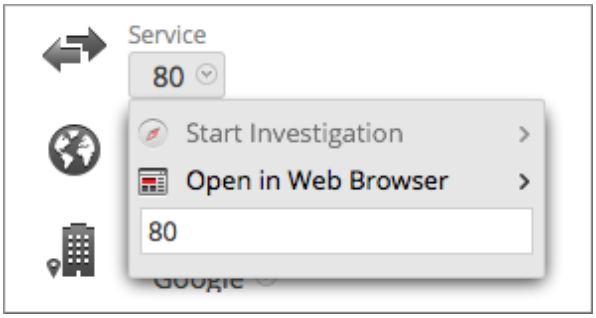
Agilizar resultados de análisis de la red

Puede agilizar los resultados de análisis de la red de varias formas:

1. Desplácese hacia abajo hasta Resultados de análisis de la red.



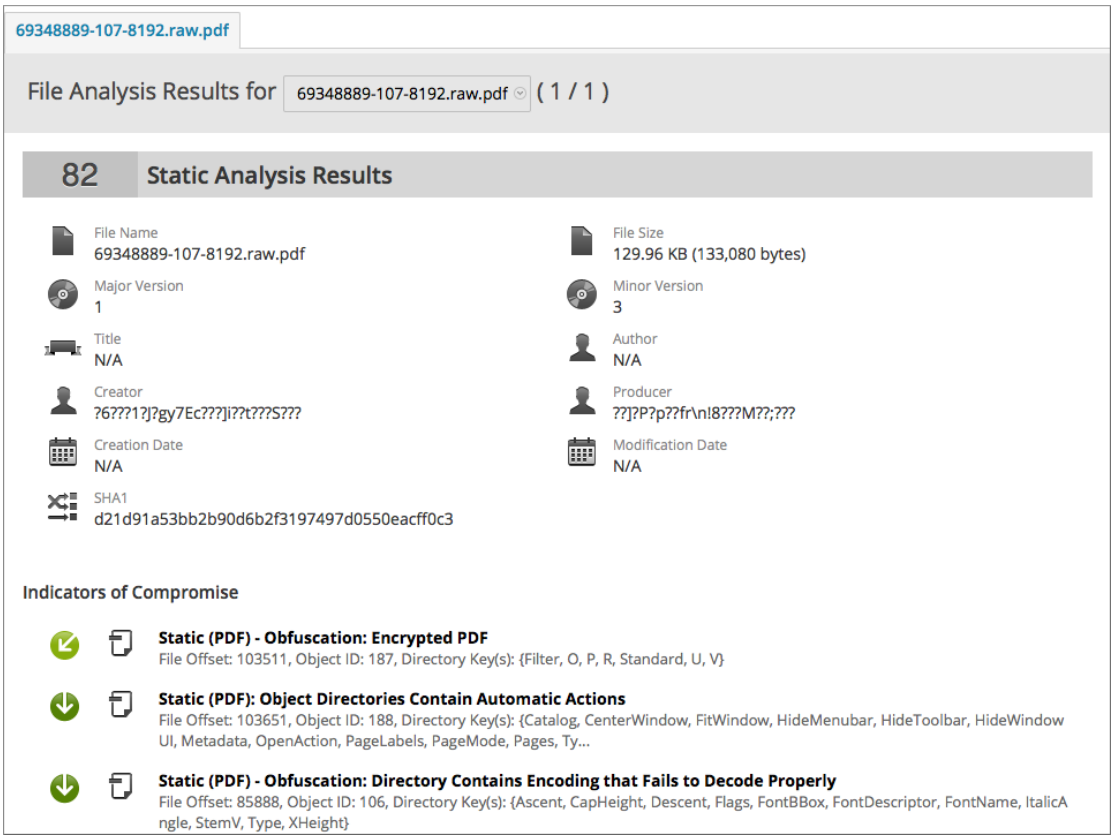
2. Mantenga el mouse sobre un valor de metadatos y haga clic con el botón primario.
   Se muestra el menú contextual.



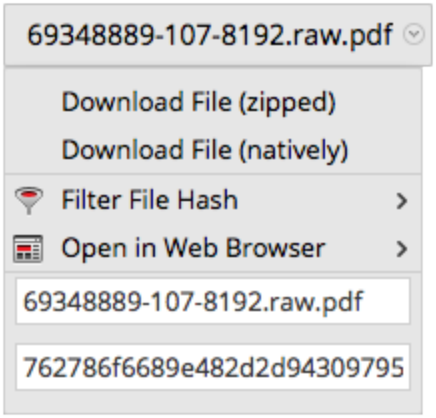
3. Para ver el valor de metadatos seleccionado en la vista **Navegar**, seleccione **Iniciar investigación** y una opción de tiempo.
4. Para ver el valor de metadatos seleccionado en un navegador, seleccione **Abrir en el navegador web > Abrir en Google**.

Utilizar acciones de archivo en los resultados de análisis estático.

1. Desplácese hacia abajo hasta Resultados del análisis estático.



2. Si desea descargar un archivo, seleccione el nombre de archivo y **Descargar archivo (comprimido)** o **Descargar archivo (nativamente)** en el menú desplegable. Es más seguro descargar un archivo en formato comprimido.



3. Si desea marcar el archivo como seguro o no seguro en la lista de hash, seleccione **Filtrar hash de archivo** y **Marcar hash como correcto** o **Marcar hash como incorrecto**.

Ver detalles de Resultados de análisis de Community

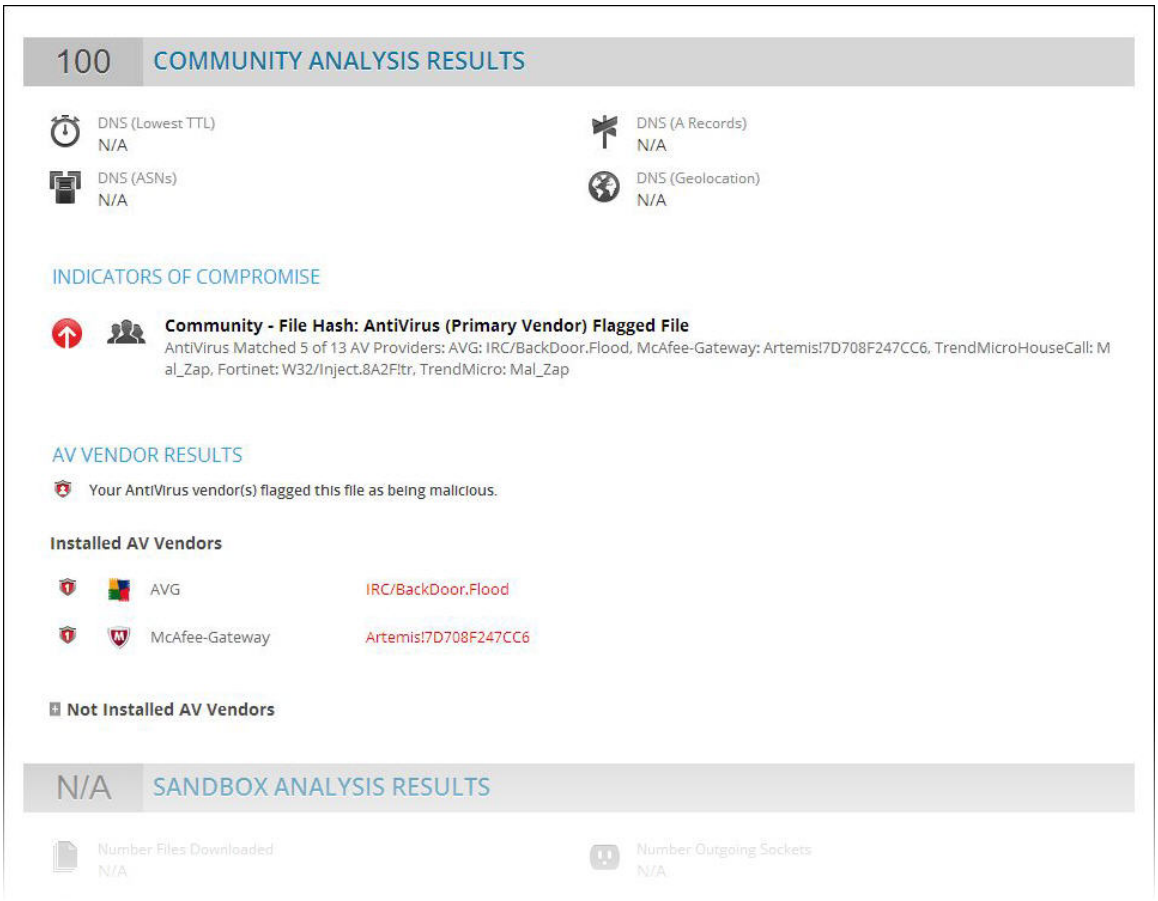
Los Resultados de análisis de Community resumen los resultados de la comunidad y muestran indicadores de riesgo que se señalaron como un riesgo o se identificaron como seguros.

Además, en esta vista se indican los resultados de los proveedores de antivirus instalados y no instalados. Puede comparar los resultados de los proveedores de antivirus instalados que se configuraron para el servicio Malware Analysis actual con los de la Comunidad. También puede ver los resultados de una lista de proveedores de antivirus que no están configurados como instalados para el servicio Malware Analysis actual.

Cada fila de los resultados de los proveedores de antivirus incluye el ícono de escudo para mostrar si al IOC lo descubrió un proveedor de antivirus primario () o uno secundario () en la comunidad, el nombre del proveedor instalado o no instalado y el nombre del malware o del riesgo que detectó la comunidad y el proveedor de antivirus. Si el proveedor de antivirus no detectó un riesgo, se muestra **-- No detectado --** en lugar del nombre del riesgo.

La sección Proveedores de antivirus no instalados se puede expandir para ver todas las entradas, pero está contraída de manera predeterminada para minimizar la necesidad de desplazamiento. Para expandir la lista, haga clic en el signo +.

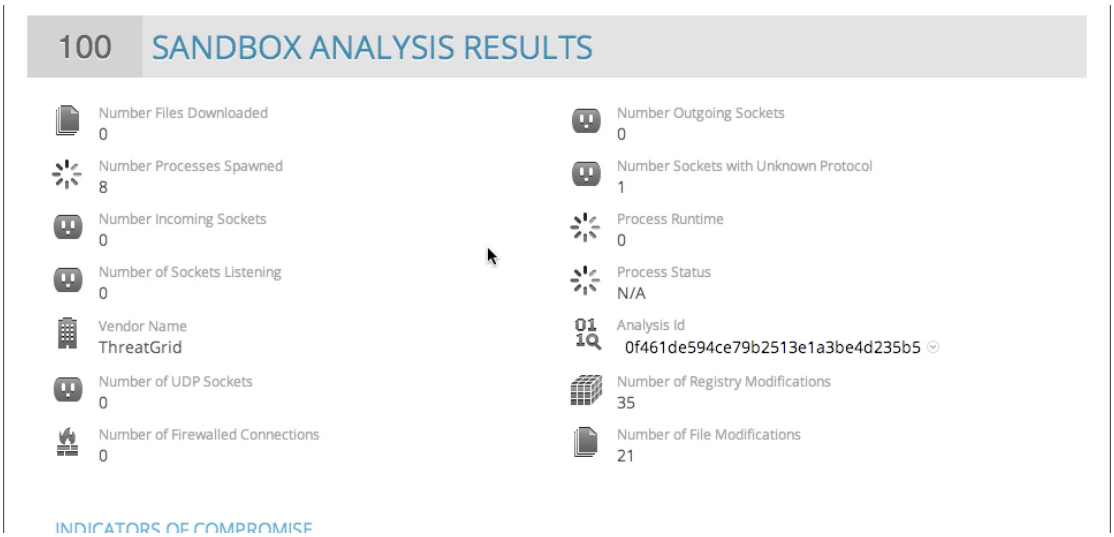
Si no se configuraron proveedores de antivirus instalados para el servicio de Malware Analysis actual, se muestra el siguiente mensaje: Ningún proveedor de antivirus se marcó como instalado. Vaya a la página Configuración del servicio Malware Analysis para identificar a los proveedores de antivirus instalados.



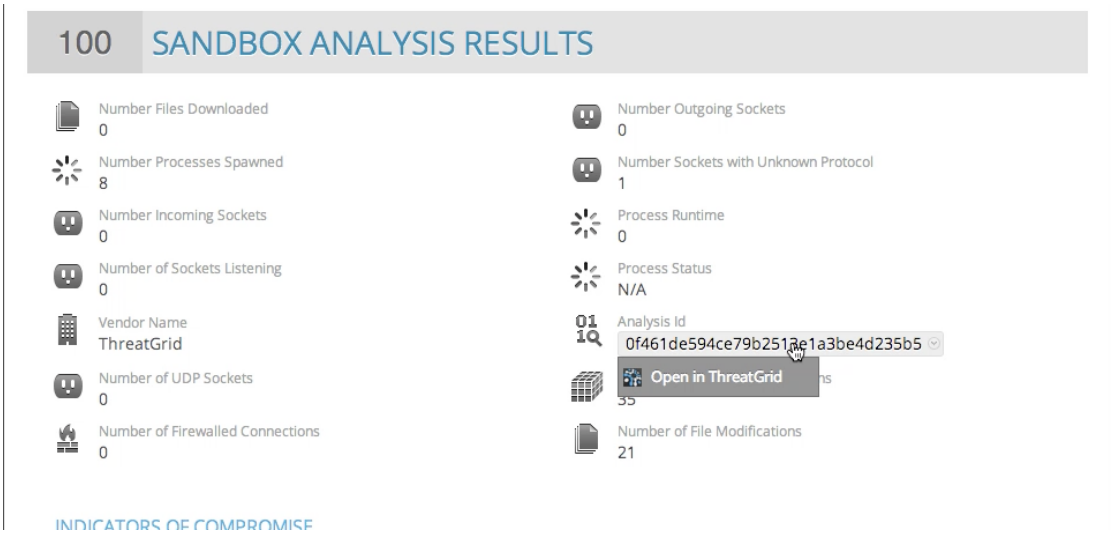
Ver resultados de análisis de Sandbox en la interfaz del usuario de ThreatGrid

Si se registró en ThreatGrid, puede ver los resultados de Sandbox directamente en ThreatGrid.

1. Desplácese hacia abajo hasta Resultados de análisis de Sandbox.

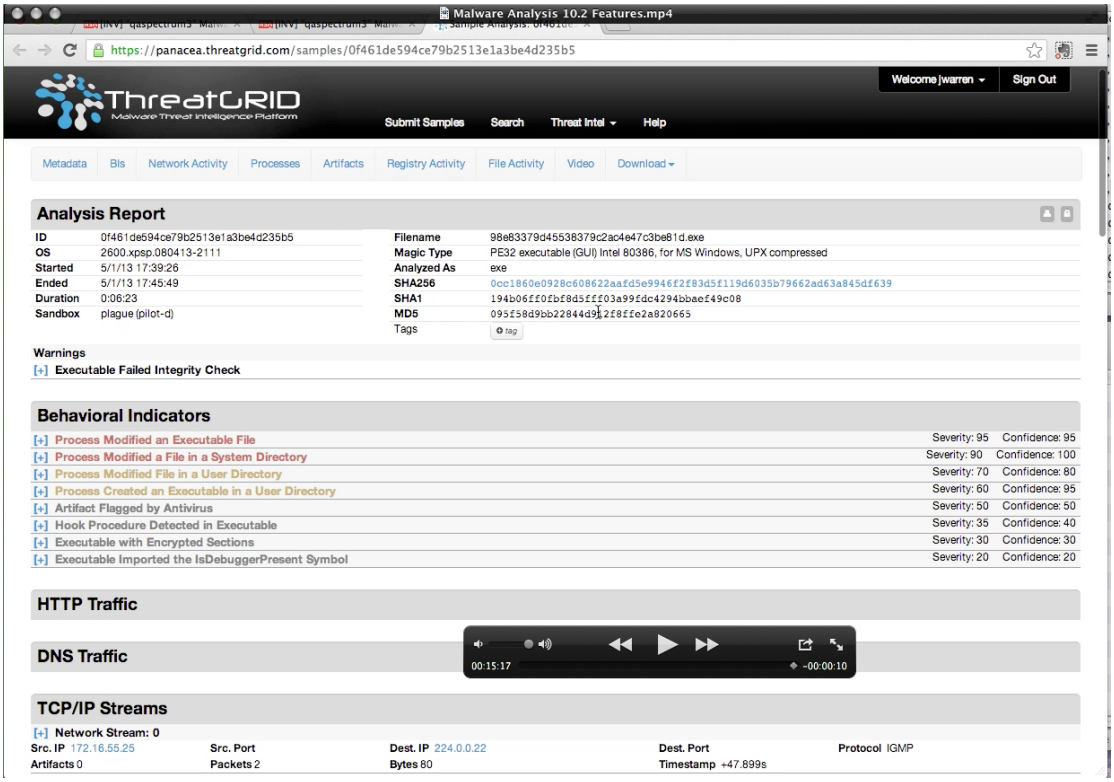


2. Mantenga el mouse sobre el **ID de análisis** y haga clic con el botón secundario.



3. Seleccione **Abrir en ThreatGrid**.

   Se muestra el informe de análisis en ThreatGrid.


Malware Analysis 10.2 Features.mp4
https://panacea.threatgrid.com/samples/0f461de594ce79b2513e1a3be4d235b5
ThreatGRID
Malware Threat Intelligence Platform
Submit Samples
Search
Threat Intel
Help
Welcome jwarren
Sign Out
Metadata
Bls
Network Activity
Processes
Artifacts
Registry Activity
File Activity
Video
Download
Analysis Report
ID 0f461de594ce79b2513e1a3be4d235b5
OS 2600.xpsp.080413-2111
Started 5/1/13 17:39:26
Ended 5/1/13 17:45:49
Duration 0:06:23
Sandbox plague (pilot-d)
Filename 98e83379d45538379c2ac4e47c3be81d.exe
Magic Type PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Analyzed As exe
SHA256 0cc1860e0928c608622aafd5e9946f2f83d5f119d6035b79662ad63a845df639
SHA1 194b06ff0fbf8d5fff03a99fdc4294bbaef49c08
MD5 095f58d9bb22844d912f8ffe2a820665
Tags
tag
Warnings
[+] Executable Failed Integrity Check
Behavioral Indicators
[+] Process Modified an Executable File Severity: 95 Confidence: 95
[+] Process Modified a File in a System Directory Severity: 90 Confidence: 100
[+] Process Modified File in a User Directory Severity: 70 Confidence: 80
[+] Process Created an Executable in a User Directory Severity: 60 Confidence: 95
[+] Artifact Flagged by Antivirus Severity: 50 Confidence: 50
[+] Hook Procedure Detected in Executable Severity: 35 Confidence: 40
[+] Executable with Encrypted Sections Severity: 30 Confidence: 30
[+] Executable Imported the IsDebuggerPresent Symbol Severity: 20 Confidence: 20
HTTP Traffic
DNS Traffic
00:15:17
-00:00:10
TCP/IP Streams
[+] Network Stream: 0
Src. IP 172.16.55.25
Src. Port
Dest. IP 224.0.0.22
Dest. Port
Protocol IGMP
Artifacts 0
Packets 2
Bytes 80
Timestamp +47.899s

Materiales de referencia de Investigation

Security Analytics ofrece varias vistas de los datos cuando se realiza una investigación. En esta sección se proporciona información detallada acerca de las herramientas y las opciones de la interfaz de usuario en Security Analytics Investigation.

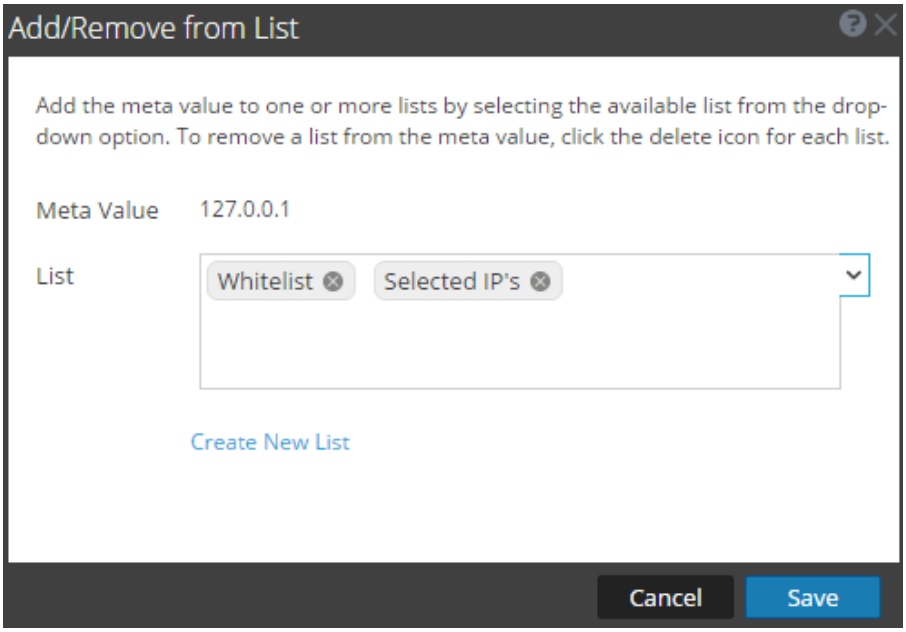
Investigation: Cuadro de diálogo Agregar/eliminar de la lista

En Investigation > vistas Navegar o Eventos, puede agregar valores de metadatos a una lista existente o crear una lista mediante la opción Agregar/eliminar de la lista. Los procedimientos relacionados están disponibles en Administrar listas y valores de lista de Context Hub en Investigation.

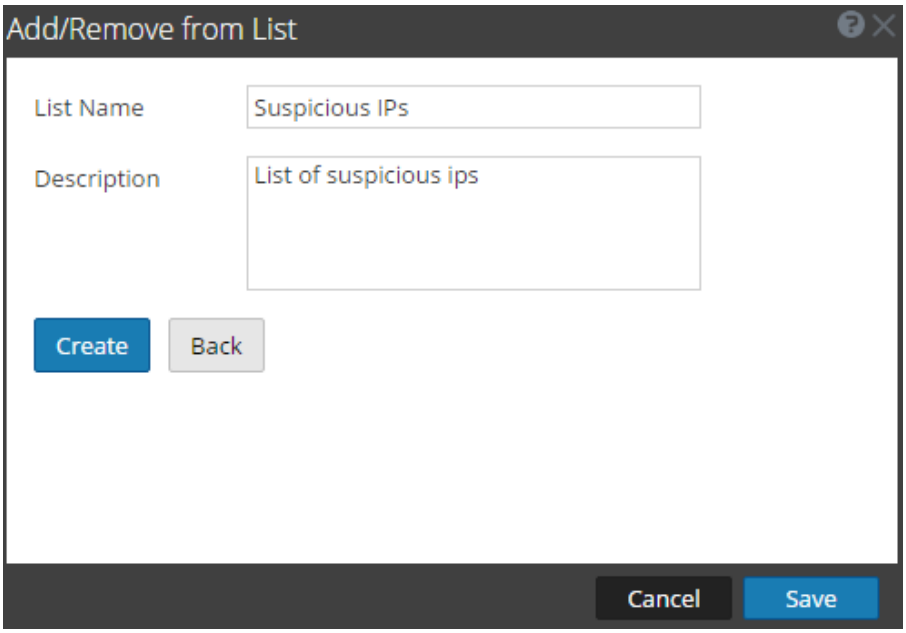
Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Eventos**. Ambas vistas proporcionan acceso al cuadro de diálogo Agregar/eliminar de la lista.
2. Haga clic con el botón secundario en un valor de metadatos (por ejemplo, valores bajo Dirección IP de origen, Dirección IP de destino o Nombre de usuario) y seleccione **Agregar/eliminar de la lista** en el menú contextual.

La siguiente figura es un ejemplo del cuadro de diálogo cuando se abre inicialmente.



En la siguiente figura se muestra el cuadro de diálogo Crear lista nueva.



Características

En la siguiente tabla se describen las características de los cuadros de diálogo Agregar/eliminar de la lista y Crear lista nueva.

Característica	Descripción
Valor de metadatos	El valor de metadatos seleccionado que se agregará a la lista nueva o existente.
Lista	La lista a la cual se debe agregar el valor de metadatos seleccionado. Un menú desplegable proporciona una lista de las listas disponibles a las cuales puede agregar el valor de metadatos.
Crear lista nueva	Se abre un cuadro de diálogo nuevo en el que puede crear una nueva lista para el valor de metadatos seleccionado.
Nombre de lista	El nombre de la lista.
Descripción	La descripción de la nueva lista.
Crear	Crear una nueva lista después de ingresar los campos obligatorios.

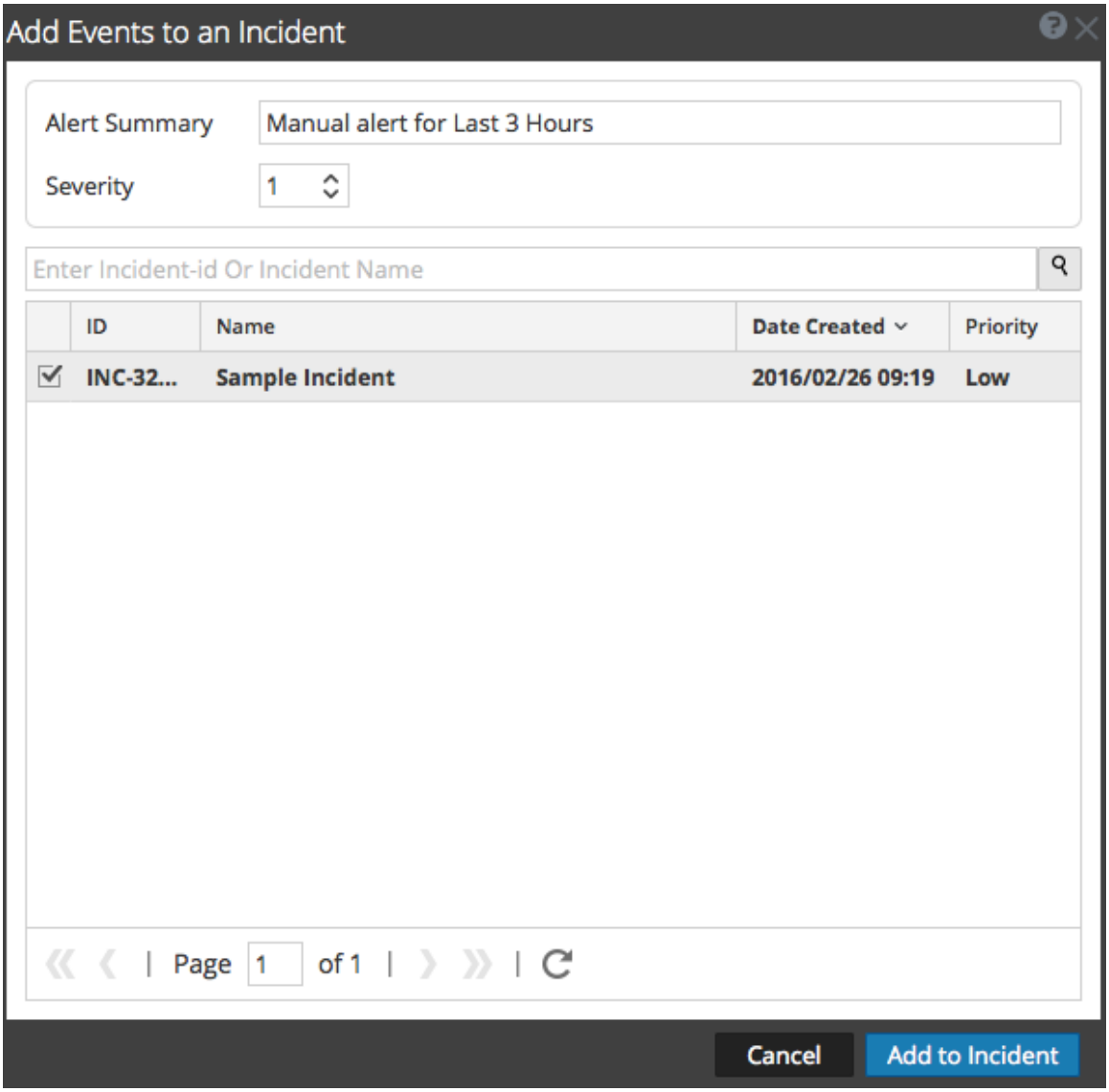
Característica	Descripción
Atrás	En el nuevo modo de lista, cancela la nueva creación de listas y regresa al cuadro de diálogo original.
Cancelar	Cancela la adición del valor de metadatos a una lista y cierra el cuadro de diálogo.
Guardar	Guarda los cambios realizados en las listas y cierra el cuadro de diálogo.

Investigation: Cuadro de diálogo Agregar eventos a un incidente

En el cuadro de diálogo Agregar eventos a un incidente, los analistas pueden agregar alertas a un incidente existente para que los encargados de responder ante incidentes busquen en los eventos asociados como parte de una respuesta ante incidentes. Los procedimientos relacionados están disponibles en Administrar listas y valores de lista de Context Hub en Investigation.

Para acceder a este cuadro de diálogo mientras investiga un servicio en Investigation > vista Eventos, seleccione **Incidentes > Agregar a incidente existente** en la barra de herramientas.

La siguiente figura es un ejemplo del cuadro de diálogo Agregar eventos a un incidente.



Características

El cuadro de diálogo Agregar alertas a un incidente tiene características que se muestran en la siguiente tabla.

Característica	Descripción
Resumen de alerta	El campo Resumen de alerta se rellena con la consulta que produjo las alertas seleccionadas, las cuales seleccionó para crear este incidente. El campo Severidad refleja la severidad de la alerta seleccionada, un número entero entre 1 y 100.
Buscar	Le permite buscar un evento existente.
ID	El ID del incidente. Puede ordenar los ID en orden ascendente o descendente.
Nombre	El nombre del incidente. Puede ordenar el nombre en orden ascendente o descendente.
Fecha de creación	Muestra la fecha y la hora de creación del incidente. Puede ordenar las fechas en orden ascendente o descendente.
Prioridad	Muestra la prioridad del incidente: baja o crítica.
Cancelar	Cierra el cuadro de diálogo sin guardar los cambios.
Agregar a un incidente	Agrega las alertas al incidente. Un cuadro de diálogo confirma que las alertas se agregaron correctamente

Investigation: Panel Búsqueda de contexto

Después de configurar el servicio Context Hub, puede ver el panel Búsqueda de contexto en la vista Navegar y en la vista Eventos del módulo Investigation. Cuando se ve este panel por primera vez, muestra las instrucciones para ejecutar la búsqueda de contexto. Más adelante este panel se minimiza y, si es necesario, puede ampliarse.

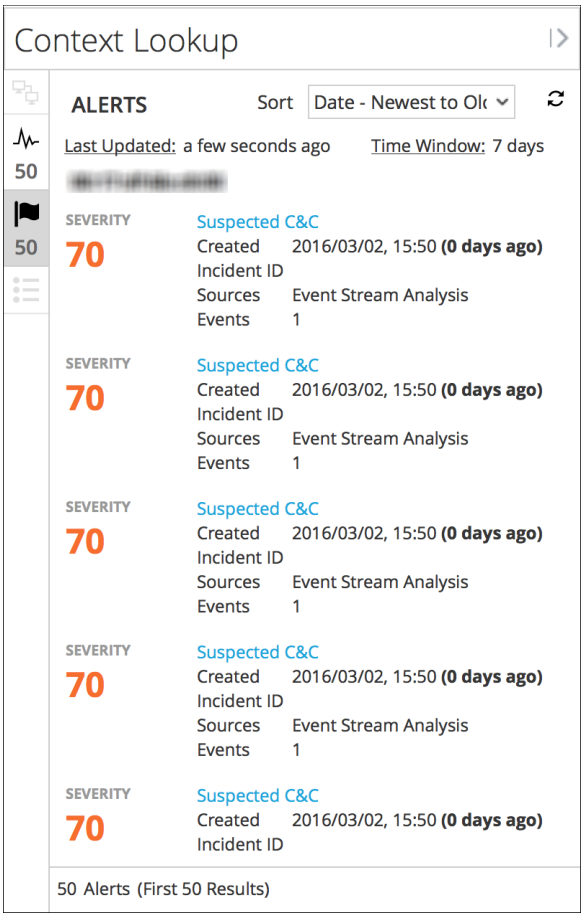
El panel Búsqueda de contexto no muestra ningún dato hasta que se realiza una búsqueda de contexto en un valor de metadatos. Los valores de metadatos que tienen información de contexto asociada se resaltan con un fondo de color gris. Los resultados de la búsqueda se muestran en el panel Búsqueda de contexto para diferentes orígenes configurados del valor de metadatos seleccionado. Los procedimientos relacionados con este panel se describen en Ver el contexto adicional de un punto de datos.

Para acceder a este panel:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Eventos**.
2. Haga clic con el botón secundario en un valor de metadatos y seleccione **Búsqueda de contexto** en el menú contextual.

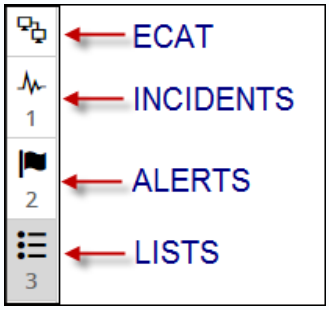
   El panel Búsqueda de contexto muestra la información contextual.
3. En la barra de íconos, seleccione el origen para el cual desea ver la información contextual; para ello, haga clic en el ícono correspondiente.

En la siguiente figura se muestra un ejemplo del panel Búsqueda.



Características

En el panel Búsqueda de contexto se encuentran los siguientes controles y características:

Característica	Descripción
Barra de opciones de origen 	Muestra los íconos de los orígenes disponibles: ECAT, incidentes, alertas y listas.

Característica	Descripción
Nombre de origen	Muestra el nombre de origen según el ícono seleccionado: • ECAT • INCIDENTES • ALERTAS • LISTAS
Clasificar	Proporciona una lista desplegable de opciones de clasificación para la información de contexto detallada. Las opciones de clasificación posibles son Severidad: alta a baja, Severidad: baja a alta, Fecha: más antiguo a más reciente y Fecha: más reciente a más antiguo. Las opciones de clasificación varían según el tipo de origen.
	Actualiza los resultados de búsqueda.
n elementos (primeros n resultados)	El pie de página proporciona un conteo de la cantidad total de resultados y el conteo de resultados que se muestra actualmente. Por ejemplo, 50 alertas (primeras 50 alertas).

Resultados de búsqueda

En el panel Búsqueda de contexto se muestra la siguiente información cuando se recuperan los datos de contexto de diferentes orígenes configurados:

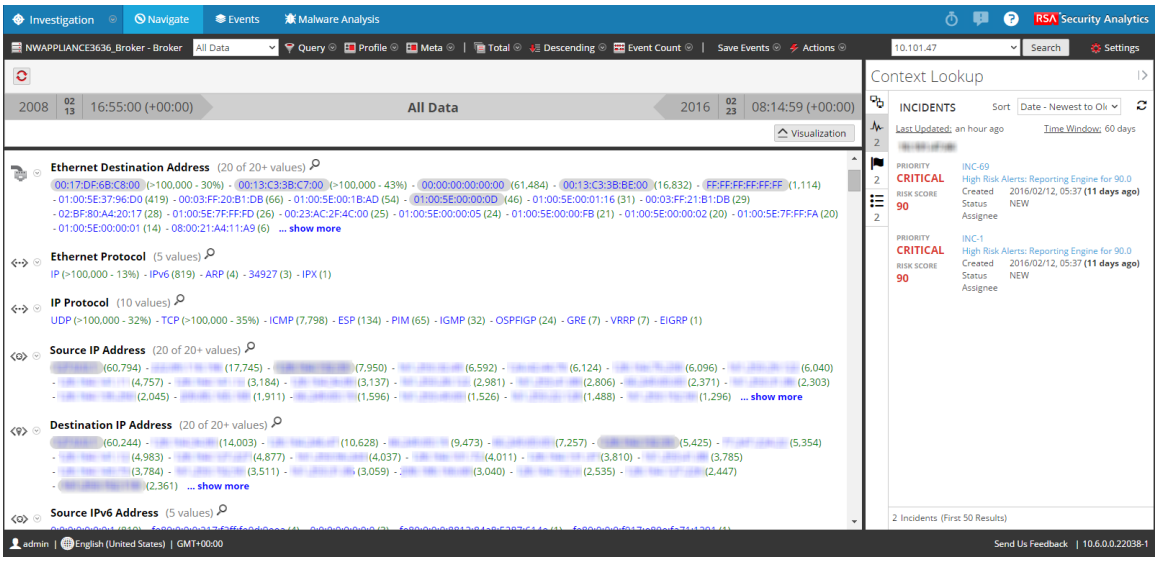
Incidentes

Se muestran los incidentes, en primer lugar según la hora (más recientes a más antiguos) y, a continuación, según el estado de prioridad. Se muestra la siguiente información para las búsquedas de incidentes:

- ID y nombre del incidente
- Estado de prioridad de los incidentes
- Valor de puntaje de riesgo de los incidentes
- La fecha de creación del incidente
- Estado del incidente

- Usuario asignado al incidente
- Última actualización: Indica la última vez en que se recuperaron datos contextuales del origen de datos y se actualizaron en la caché.
- Ventana de tiempo: Se basa en el valor que se configura para el campo "Consultar últimos" de la ventana **Configurar respuestas de Incident Management**. Para obtener detalles, consulte el tema **Configurar respuestas de Incident Management** de la *Guía de configuración de Context Hub*.
- Clasificar: Este campo desplegable proporciona la opción para cambiar el orden de los resultados según la hora o la prioridad.

La siguiente figura es un ejemplo de los resultados de búsqueda de incidentes.



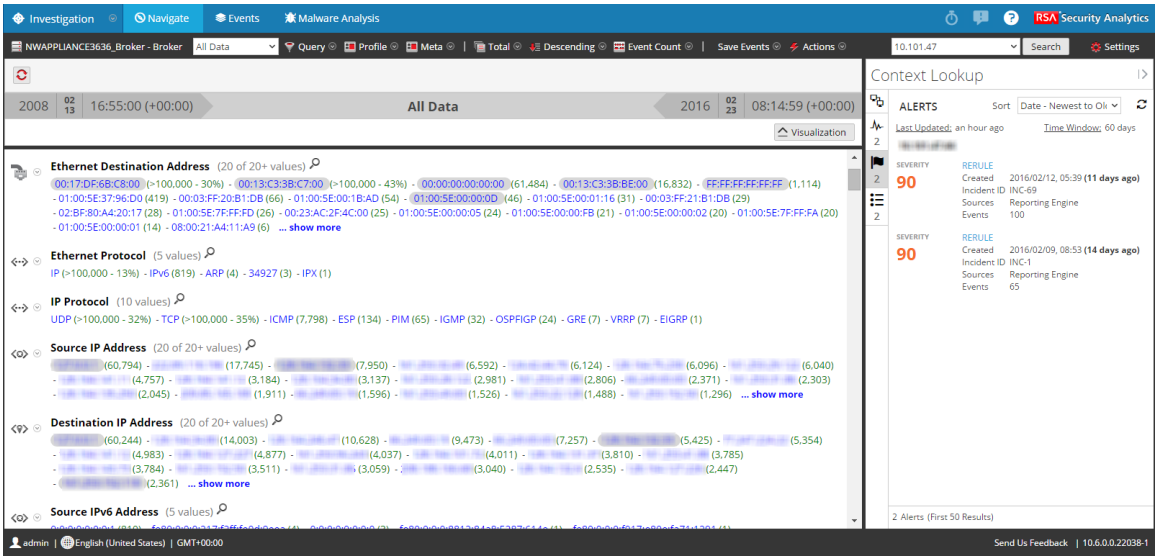
Alertas

Las alertas se muestran en función de la gravedad. Se muestra la siguiente información para búsquedas de alertas:

- Nombre de la alerta
- Valor de severidad de las alertas
- Fecha en que se creó la alerta
- ID del incidente: Este es el ID del incidente con el cual está asociada la alerta (si corresponde).
- Orígenes: Nombre del origen de eventos

- Número de eventos asociados con la alerta.
- Última actualización: Indica la última vez en que se recuperaron datos contextuales del origen de datos y se actualizaron en la caché.
- Ventana de tiempo: Se basa en el valor que se configura para el campo “Consultar últimos” de la ventana Configurar respuestas de Incident Management, la cual se describe en la *Guía de configuración de Context Hub*.
- Clasificar: Este campo desplegable proporciona la opción para cambiar el orden de los resultados según la hora o la prioridad.

La siguiente figura es un ejemplo de los resultados de búsqueda de alertas.

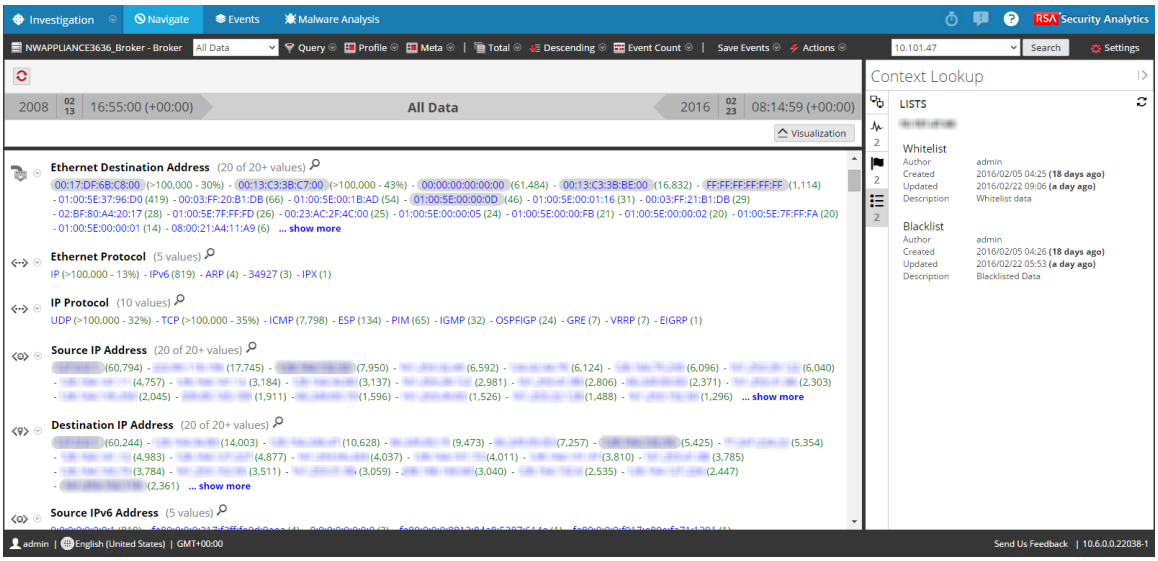


Listas

Se muestra la siguiente información para búsquedas de listas.

- Nombre de lista
- Propietario que creó la lista
- Fecha de creación
- Fecha de la última actualización
- Descripción de la lista

La siguiente figura es un ejemplo de los resultados de búsqueda del origen de datos Listas.



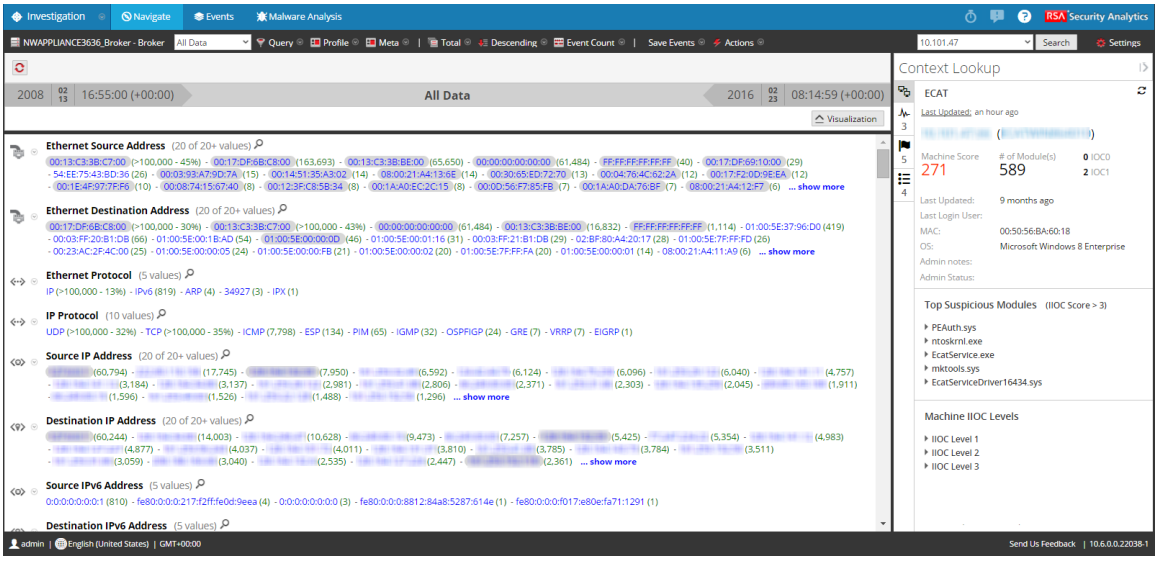
ECAT

Se muestra la siguiente información para búsquedas de ECAT.

- Nombre y dirección IP de la máquina.
  Si hace clic en la dirección IP o en el nombre de la máquina de ECAT, se desplazará hasta la interfaz del usuario de ECAT para ejecutar una investigación más profunda.
- Última actualización: Indica la última vez en que se recuperaron datos contextuales del origen de datos y se actualizaron en la caché.
- Puntaje de la máquina: Un puntaje de IIOC de la máquina se agrega en función de los puntajes del módulo.
- Cantidad de módulos: Cantidad de archivos activos para la máquina seleccionada.
- Última actualización: Indica cuándo se actualizaron por última vez los resultados del escaneo en la base de datos ECAT.
- Último usuario de inicio de sesión
- Dirección MAC de la máquina
- Versión del sistema operativo
- Notas administrativas (si corresponde)
- Estado administrativo (si corresponde)

- Principales módulos sospechosos (módulos cuyo puntaje de IIOC > 500). Se basa en el valor configurado para el campo “Puntaje de IIOC mínimo” en la ventana Configurar respuestas de Incident Management. El valor predeterminado para “Puntaje de IIOC mínimo” es 500.
- Niveles de IIOC de la máquina

La siguiente figura es un ejemplo de los resultados de búsqueda del origen de datos ECAT.

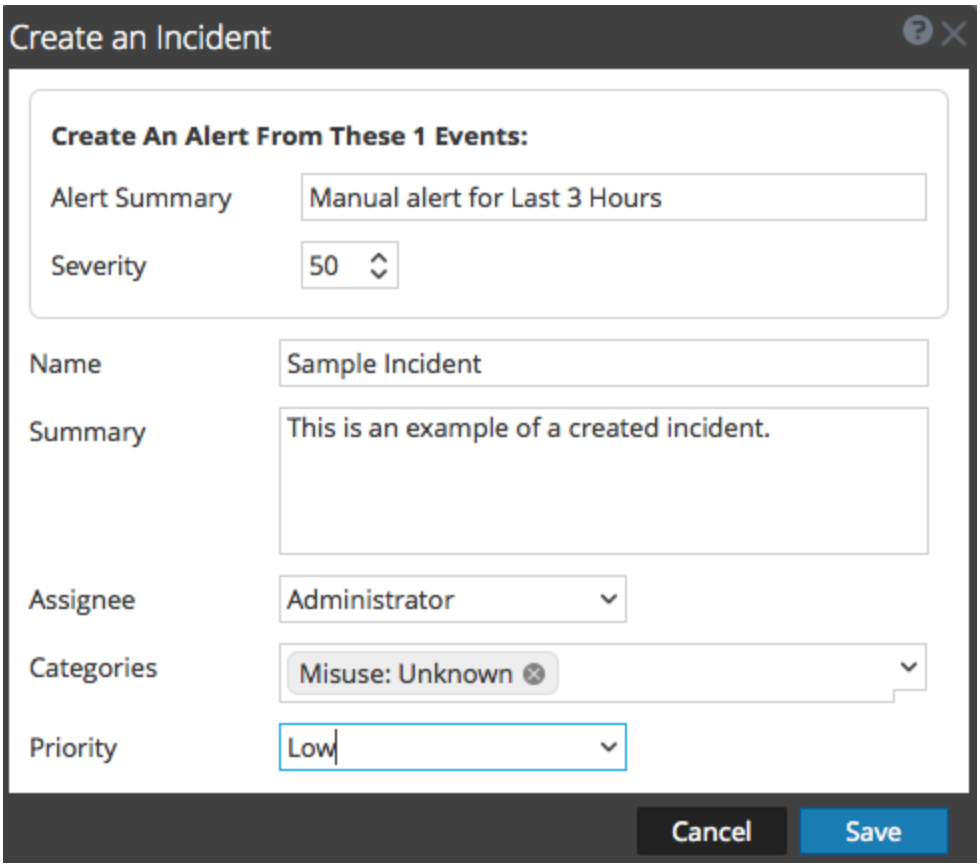


Investigation: Cuadro de diálogo Crear un incidente

En el cuadro de diálogo Crear un incidente, los analistas pueden crear un incidente a partir de eventos seleccionados en la vista Eventos. Cuando se crea el incidente, los analistas pueden identificar la categoría y la prioridad del incidente y pueden asignar su manejo a un analista del SOC.

Para acceder a este cuadro de diálogo mientras investiga un servicio en Investigation > vista Eventos, seleccione **Incidentes > Crear nuevo incidente** en la barra de herramientas.

La siguiente figura es un ejemplo del cuadro de diálogo Crear un incidente.



Características

El cuadro de diálogo Crear un incidente tiene las características que se muestran en la siguiente tabla.

Característica	Descripción
Crear una alerta de estos eventos	El campo Resumen de alerta se rellena con la consulta que produjo las alertas seleccionadas, las cuales seleccionó para crear este incidente. El campo Severidad refleja la severidad de la alerta seleccionada, un número entero entre 1 y 100.
Nombre	(Obligatorio) Especifica un nombre para identificar el incidente. En el ejemplo, el nombre es Incidente de muestra. Puede proporcionar un nombre que identifique claramente la naturaleza de los eventos que se agregarán a este incidente
Resumen	(Opcional) Especifica una descripción del incidente. Un buen resumen identifica claramente el incidente para otros analistas y encargados de responder.
Usuario asignado	(Opcional) Asigna el incidente a un usuario en el SOC. Si hace clic en Usuario asignado, se abre una lista desplegable que muestra los nombres de usuario del personal del SOC que responden ante incidentes.
Categorías	(Opcional) Identifica las categorías de incidentes. Si hace clic en Categorías, se abre una lista desplegable de categorías y subcategorías de incidentes. Puede seleccionar una o más categorías a las cuales pertenece el incidente. Las categorías se dividen en estos grupos principales: Ambiental, error, hacking, malware, uso indebido y redes sociales.
Prioridad	Identifica la prioridad del incidente. Si hace clic en Prioridad, se abre una lista desplegable de prioridades: En la lista desplegable, se muestra crítica, alta, media o baja.
Cancelar	Cierra el cuadro de diálogo sin guardar los cambios.
Guardar	Guarda el incidente y cierra el cuadro de diálogo. Un mensaje confirma que el incidente se creó correctamente.

Investigation: Panel Reconstrucción de evento

En este tema se describen las funciones disponibles en Investigation > vista Eventos > panel Reconstrucción de evento.

De forma predeterminada, Security Analytics muestra la mejor reconstrucción para el evento, según lo determina el contenido del evento o la reconstrucción que seleccionó en la configuración Vista de sesión predeterminada para Investigation. Puede utilizar las opciones de la barra de herramientas Reconstrucción de evento para cambiar el método de reconstrucción, ver los resultados en paralelo, exportar un evento, abrir archivos adjuntos del correo electrónico, extraer archivos y abrir el evento en una nueva pestaña.

Para acceder a este panel en una nueva pestaña, realice una de las siguientes acciones:

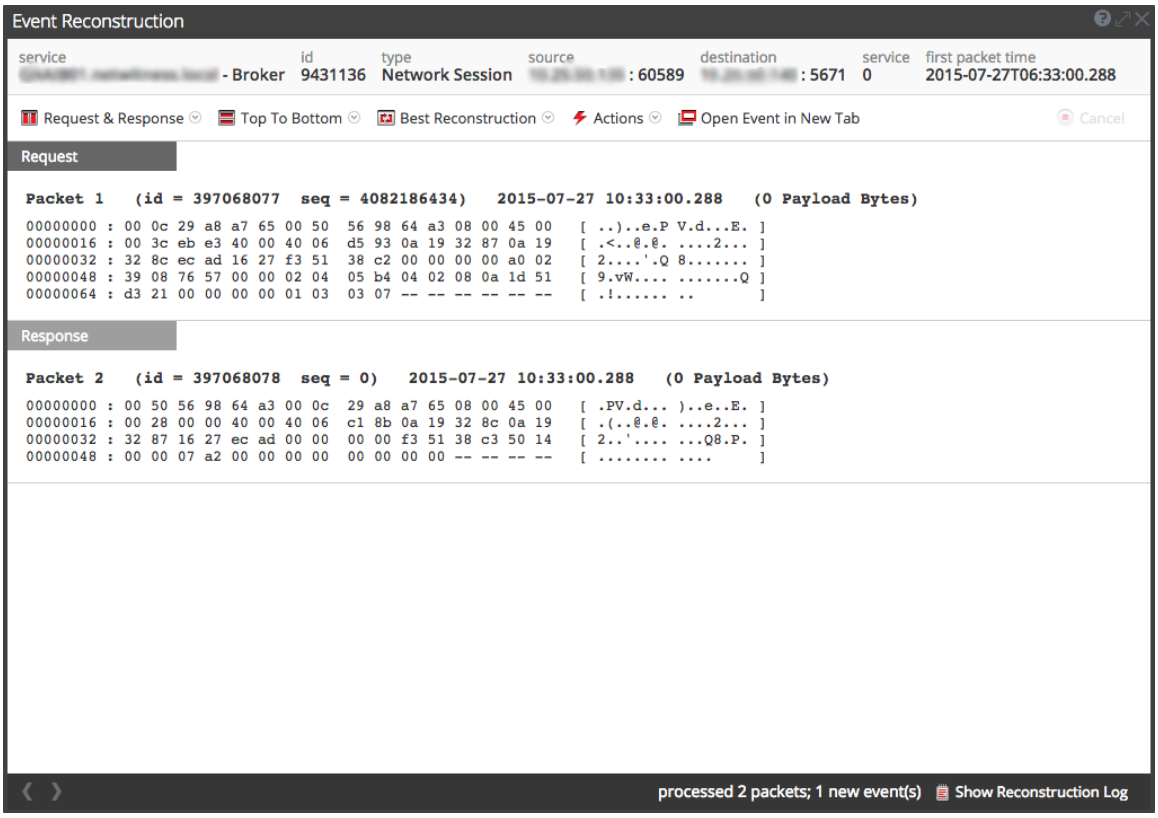
- En la vista Eventos, seleccione un evento para reconstruir y elija **Acciones > Ver evento> Abrir en una nueva pestaña**.
- En la barra de herramientas Reconstrucción de evento de la reconstrucción con vista previa, haga clic en **Abrir evento en nueva pestaña** en la barra de herramientas.
  La Reconstrucción de evento se muestra en una nueva pestaña.

Para acceder a este panel en la pestaña actual, realice una de las siguientes acciones:

- Al final del evento, seleccione 

- Seleccione un evento para reconstruir y elija **Acciones > Ver evento > Vista previa en línea**.

El panel Reconstrucción de evento se abre en una ventana emergente en la misma vista.



Características

El panel Reconstrucción de evento tiene una barra de herramientas en la parte superior, la cual incluye las siguientes opciones.

Característica	Descripción
Solicitud y respuesta	Muestra un menú desplegable que permite seleccionar si el panel muestra: • Solicitud y respuesta • Solicitud • Respuesta
Organización	Muestra un menú desplegable que permite seleccionar si la información se presenta de arriba abajo o en paralelo.

Característica	Descripción
Ver	Muestra un menú desplegable que permite seleccionar la información que se presenta. De forma predeterminada, la opción Mejor reconstrucción está seleccionada. Otras opciones son: • Ver metadatos • Ver texto • Ver valor hexadecimal • Ver paquetes • Ver web • Ver correo • Ver archivos
Acciones	Muestra un menú desplegable con las acciones disponibles en el panel Reconstrucción de evento.
Abrir evento en nueva pestaña	Abre el evento en una nueva pestaña del navegador.

Debajo de la barra de herramientas hay una lista de claves de metadatos y valores. Algunas de las claves ofrecen un menú desplegable con acciones disponibles.

La barra de la parte inferior del panel ofrece varias opciones.

Característica	Descripción
	Muestra el evento anterior.
	Muestra el evento siguiente.
Mostrar registro de reconstrucción	Muestra el registro de reconstrucción en la parte inferior del panel. Cuando hace clic en el botón, este cambia a Ocultar registro de reconstrucción.

Investigation: Vista Eventos

En este tema se describen las funciones disponibles en Investigation > vista Eventos.

En Investigation > vista Eventos está disponible una lista de eventos asociada con una sesión. Existen dos maneras de mostrar la vista Eventos:

- Seleccione **Investigación > Eventos** en el menú de **Security Analytics**. Security Analytics ejecuta una consulta predeterminada acerca de las últimas tres horas para el servicio predeterminado (si hay uno configurado) o muestra un cuadro de diálogo en el cual puede seleccionar un servicio y, a continuación, ejecuta la consulta predeterminada. La consulta predeterminada selecciona todos los eventos y la vista Eventos muestra los pertinentes al servicio seleccionado, con los más antiguos en primer lugar.
- En la vista Navegar, haga clic en un evento. La vista Eventos muestra los eventos en el servicio seleccionado según el punto de desglose en la vista Navegar.

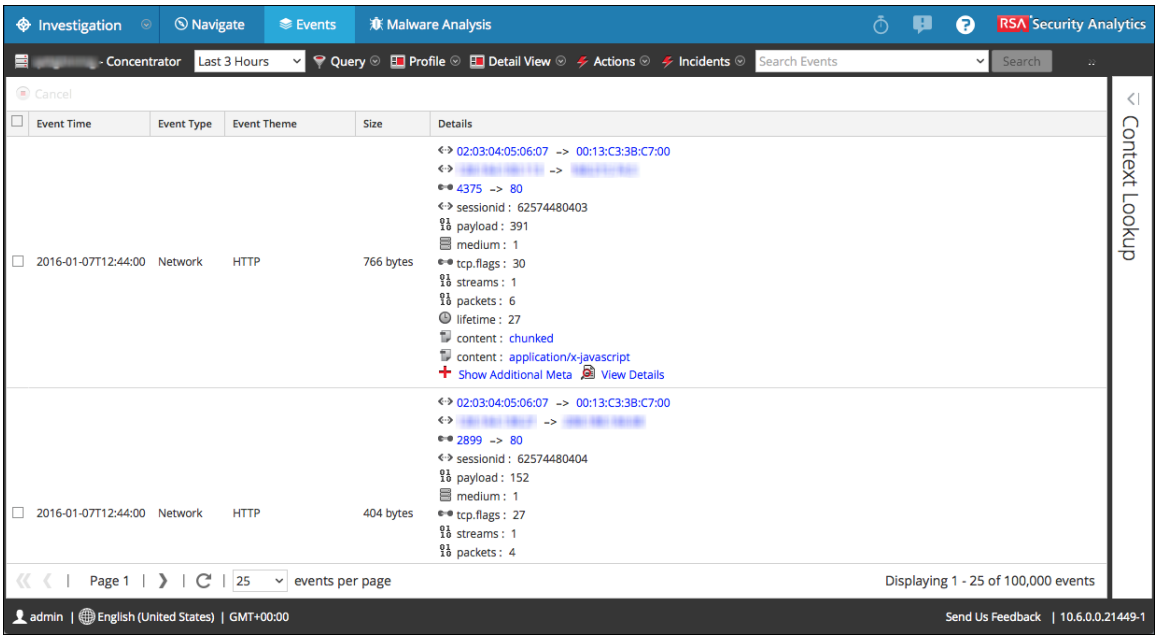
Esta vista proporciona tres presentaciones incorporadas de datos de eventos: la vista detallada, la vista de lista y la vista de registro. La vista Lista y la Vista detallada están destinadas a la visualización de eventos de paquetes de datos y proporcionan más información para cada evento, que incluye registro de fecha y hora, tipo de evento, tema del evento y tamaño.

- La vista Lista muestra la información de las direcciones y los puertos de origen y destino correspondientes de los eventos en forma de resumen en un grid.
- La Vista detallada muestra todos los metadatos recopilados del evento en una vista paginada.

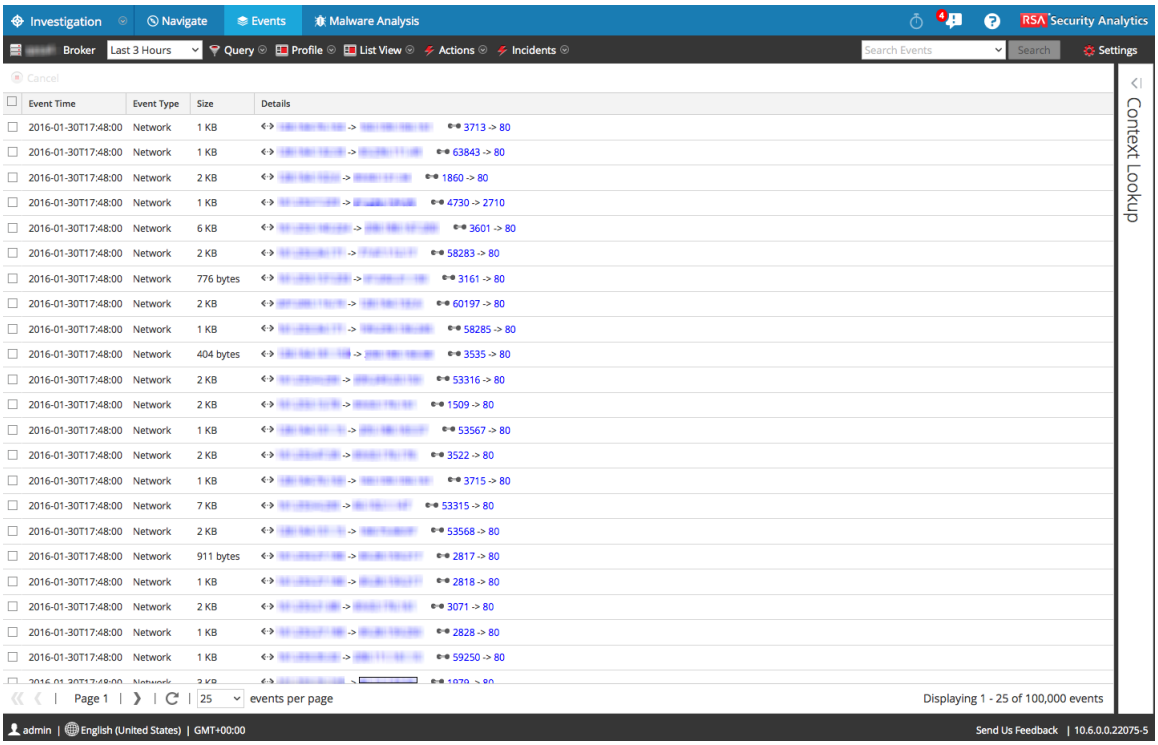
La vista Registro está optimizada para mostrar información de registro y proporciona más información para cada registro, incluido el registro de fecha y hora, el tipo de evento, el tipo de servicio, la clase de servicio y los registros.

Puede utilizar consultas, la configuración del rango de tiempo y perfiles para filtrar los eventos mostrados en la vista Eventos. Desde cualquier tipo de vista de la vista Eventos, puede extraer archivos, exportar eventos, exportar registros y abrir el panel Reconstrucción de evento si hace doble clic en un evento.

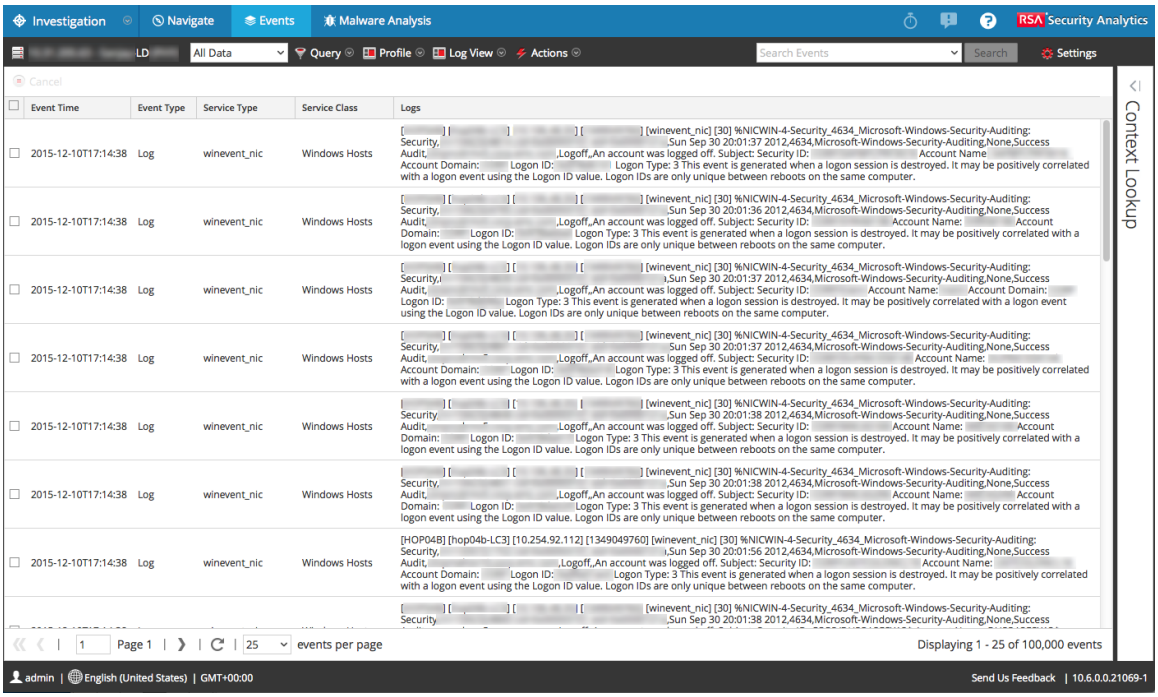
En la siguiente figura se muestra un ejemplo de eventos en la vista detallada. El panel Búsqueda de contexto es visible solo si está configurado el servicio Context Hub.



La siguiente figura es un ejemplo de eventos en la Vista de lista.



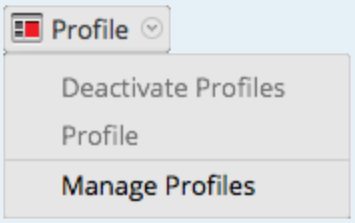
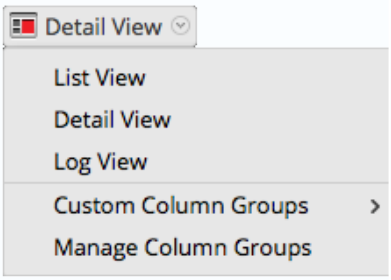
La siguiente figura es un ejemplo de la vista de registro.

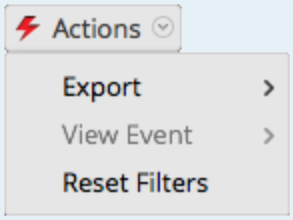


Características

La vista Eventos tiene una barra de herramientas en la parte superior con las siguientes opciones.

Característica	Descripción
Seleccionar servicio	Muestra el nombre del servicio seleccionado junto al ícono. Abre el cuadro de diálogo Seleccionar un servicio, donde puede seleccionar un servicio para el cual se muestra la lista de eventos.
Rango de tiempo	Muestra un menú desplegable para seleccionar el rango de tiempo para aplicar a la lista de eventos. Puede elegir una de las opciones estándar o especificar un rango de tiempo personalizado.
Consulta 	Se muestra el cuadro de diálogo Crear filtro, en el cual puede ingresar directamente una consulta personalizada en lugar de desglosar a los datos (consulte Crear una consulta personalizada)

Característica	Descripción
Usar perfil 	Muestra el menú Usar perfil; el perfil seleccionado se muestra en la barra de herramientas. Un perfil permite administrar y usar perfiles que pueden incluir grupos de metadatos personalizados, un grupo de columnas predeterminado y una consulta inicial. Los perfiles se aplican a la vista Navegar (consultas y grupos de metadatos) y a la vista Eventos (consultas y grupos de columnas).
Ver el menú despegable de tipo 	Muestra un menú desplegable para seleccionar el tipo de vista de evento. • La Vista detallada muestra los eventos en un formato paginado con información detallada de cada evento. • La vista Lista muestra los eventos en formato de cuadrícula con un resumen de cada evento en una fila por separado. • La Vista de registro muestra una cuadrícula de eventos orientados a registros con un resumen de cada registro en una fila por separado. • Grupos de columnas personalizados muestra la lista de eventos mediante el uso de un grupo de columnas seleccionado en una lista desplegable de grupos de columnas personalizados. • Administrar grupos de columnas muestra el cuadro de diálogo para crear y editar grupos de columnas personalizados.

Característica	Descripción
Acciones 	Muestra un menú desplegable con acciones en la vista Eventos: • Extraer archivos, exportar eventos como un archivo PCAP o exportar registros. • Ver una reconstrucción de evento en una ventana emergente o en una pestaña nueva. • Restablecer todos los filtros en la ventana Eventos.
Incidentes	Muestra un menú desplegable en el cual puede crear un nuevo incidente o agregar información a un incidente existente.
Buscar eventos	Le permite buscar patrones de texto en el conjunto actual de eventos que se muestran. Si hace clic en el campo de búsqueda, se muestra un menú desplegable con opciones de búsqueda. Si hace clic en Aplicar, guarda las opciones seleccionadas y también actualiza las opciones de búsqueda en la vista Navegar y el perfil de investigaciones (consulte Investigation: Opciones de búsqueda).
Configuración 	Muestra los ajustes de Investigation para la vista Eventos (los cuales también se pueden editar en la vista Perfil), de modo que puede cambiarlos sin salir de la vista Eventos. Cuando cambia un ajuste en la vista Eventos, este también se cambia en la vista Perfil (consulte Configurar la vista Navegar y la vista Eventos).

La barra de paginación de la vista Eventos en la parte inferior de la página cuenta con opciones para paginación a través de la lista Eventos.

Característica	Descripción
	Muestra la primera página.

Característica	Descripción
‹	Muestra la página anterior.
Page 25 of 4000	Si no habilitó la opción **Paginación en lista de eventos de Investigation optimizada para velocidad** en el cuadro de diálogo Preferencias de Investigation, se habilita la paginación mediante el ingreso de un número de página específico.
›	Muestra la página siguiente.
»	Muestra la última página.
↻	Actualiza la lista de eventos.
Elementos por página	Muestra una lista de selección para la cantidad de elementos a mostrar en una página.

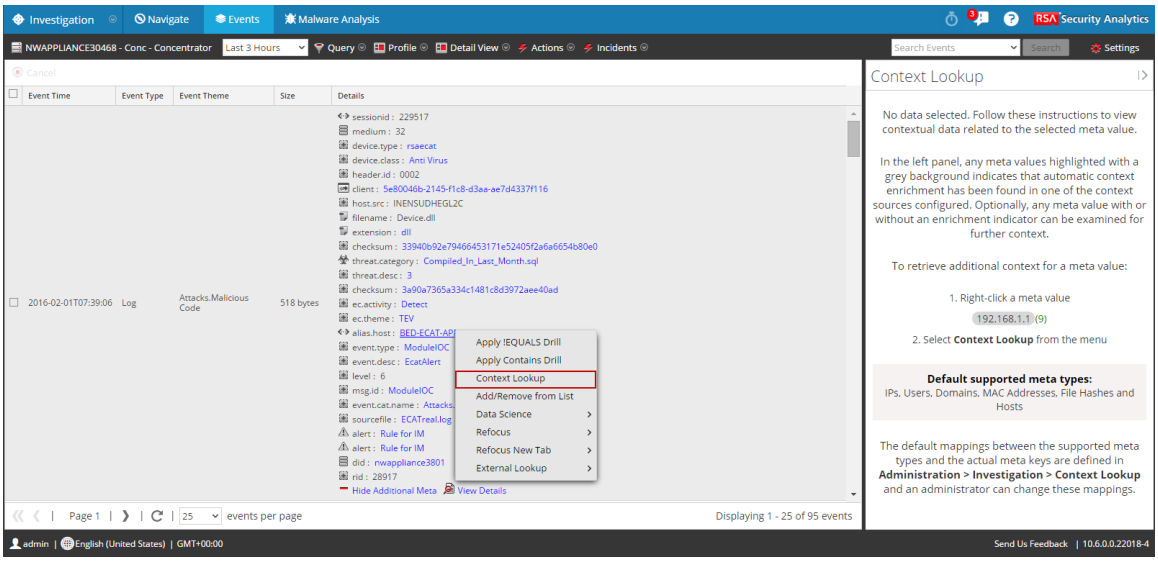
Panel Búsqueda de contexto

Después de configurar el servicio Context Hub, puede ver la información contextual para los valores de metadatos en la vista **Navegar** y en la vista **Eventos** del módulo Investigation. Para obtener más información sobre cómo configurar el servicio Context Hub, consulte *Guía de configuración de Context Hub*.

Para obtener información acerca de cómo realizar la búsqueda de contexto de valores de metadatos, consulte Ver el contexto adicional de un punto de datos.

El servicio Context Hub está preconfigurado con un mapeo predeterminado de tipos de metadatos y claves de metadatos. Para obtener información sobre el mapeo del valor de metadatos de Context Hub con clave de metadatos de Investigation, consulte "Administrar el mapeo de tipos de metadatos y claves de metadatos" en la *Guía de configuración de Context Hub*.

En la siguiente figura se muestra la opción Búsqueda de contexto cuando hace clic con el botón secundario en un valor de metadatos.

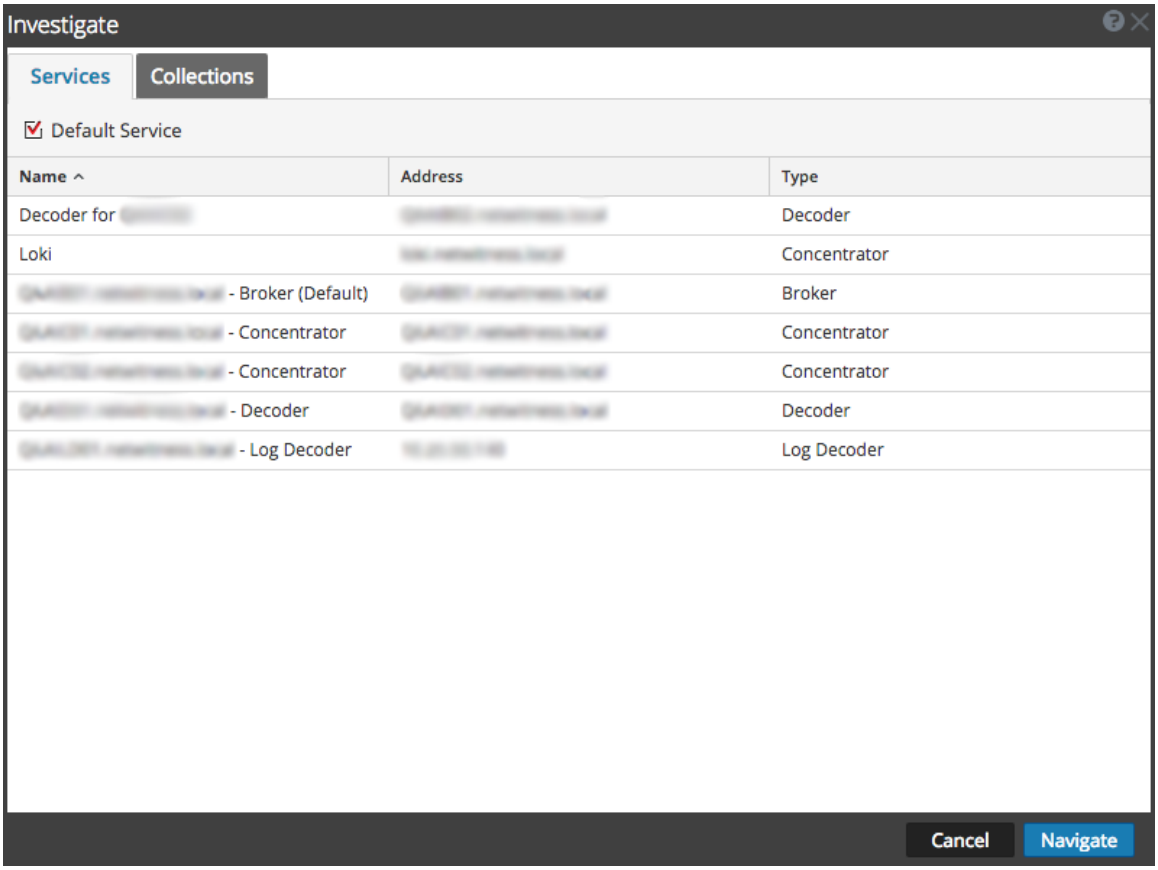


Para obtener más información sobre los resultados de búsqueda y la información contextual de distintos orígenes de datos, consulte “Panel Búsqueda de contexto” en la *Guía de configuración de Context Hub*.

Investigation: Cuadro de diálogo Investigar

El cuadro de diálogo Investigar permite a los analistas seleccionar un servicio o una recopilación para investigar.

El cuadro de diálogo se muestra automáticamente cuando se dirige en primer lugar a la vista Navegar o Eventos y no ha seleccionado un servicio predeterminado para investigar. Para acceder al cuadro de diálogo desde una investigación actual, seleccione el nombre actual del servicio en la barra de herramientas.



Características

El cuadro de diálogo Investigar tiene dos pestañas: Servicios y Recopilaciones.

Nota: Las recopilaciones también se conocen como recopilaciones de Workbench. Solo puede ver recopilaciones de Workbench que ha creado y solo los administradores pueden crear una recopilación de Workbench.

Pestaña Servicios

La pestaña Servicios incluye una lista de servicios disponibles para investigación y tres botones. En la siguiente tabla se describen todas las funciones.

Característica	Descripción
Servicio pre-determinado	Si se hace clic en este botón, se establece o se borra el servicio pre-determinado para investigar. Cuando un servicio se configura como el pre-determinado, la palabra (Predeterminado) se añade al nombre del servicio.
Nombre	El nombre del servicio.
Dirección	La dirección IP del servicio.
Tipo	Tipo de servicio.
Cancelar	Cierra el cuadro de diálogo.
Navegar	Abre el servicio seleccionado en la vista Navegar o Eventos.

Pestaña Recopilaciones

La pestaña Recopilaciones incluye dos botones y dos paneles: Workbench y Recopilaciones.

En el panel Workbench se muestran los servicios Workbench disponibles. Una vez que se selecciona un servicio Workbench, se puede seleccionar una recopilación en el panel Recopilaciones. El nombre es el nombre del servicio Workbench.

En el panel Recopilaciones se muestran las recopilaciones disponibles para investigar. Una vez que se selecciona una recopilación, se puede hacer clic en Navegar para ver la recopilación.

En la siguiente tabla se describen las funciones del panel Recopilaciones.

Característica	Descripción
Nombre	El nombre de la recopilación.
Tipo	El tipo de recopilación.
Tamaño	El tamaño de la recopilación.
Tipo de datos	El tipo de datos dentro de la recopilación.
Fecha de creación	La fecha en que se creó la recopilación.

Pestaña Investigation: Panel Preferencias de usuario

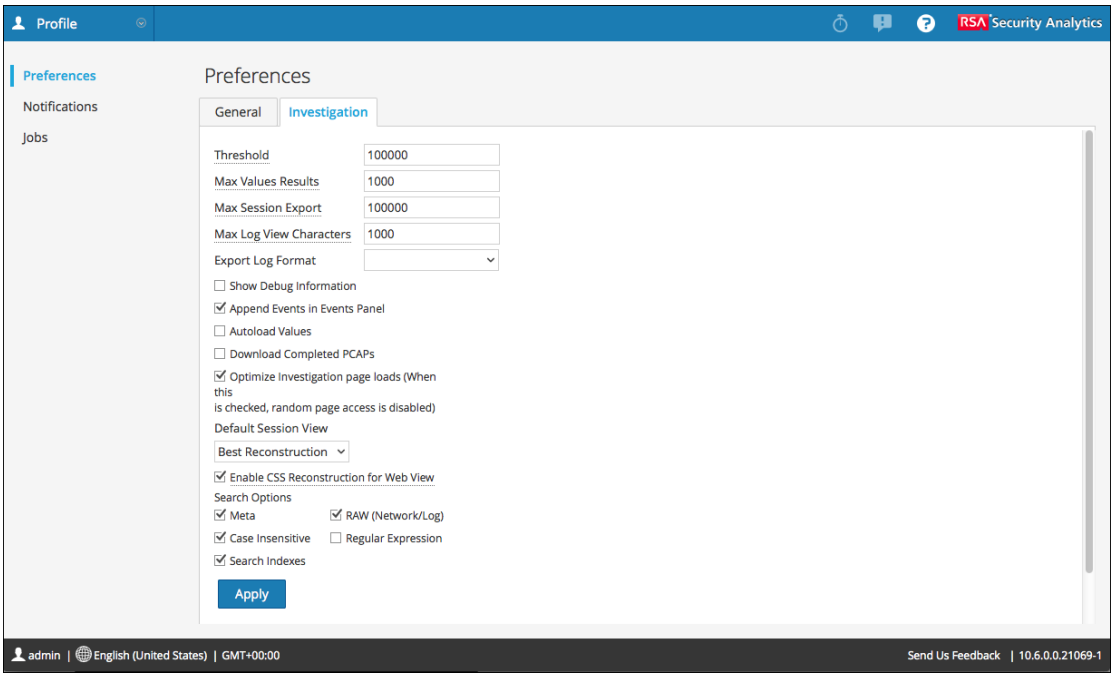
En este tema se presentan las funciones de la vista Perfil >panel Preferencias > pestaña Investigation.

En la vista Perfil > panel Preferencias > pestaña Investigation, los usuarios pueden configurar varias preferencias que afectan el rendimiento y el comportamiento de Security Analytics cuando se analizan datos, se ven eventos y se reconstruyen eventos en Investigation.

Los procedimientos relacionados con esta pestaña se describen en Configurar la vista Navegar y la vista Eventos.

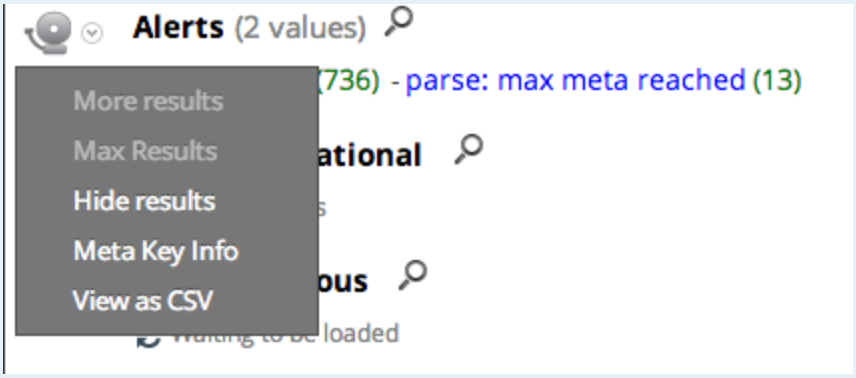
Para acceder a esta pestaña:

1. En el menú de **Security Analytics**, seleccione **Perfil**.
2. En el **panel de navegación izquierdo**, seleccione **Preferencias**.
3. En el panel **Preferencias**, seleccione la pestaña **Investigation**.



Características

En la siguiente tabla se describen las preferencias de Investigation.

Característica	Descripción
Umbral	Esta configuración controla el conteo que se muestra para un valor de clave de metadatos en la vista Navegar durante la carga. Un umbral mayor permite conteos más precisos para un valor. Sin embargo, un umbral mayor provoca que los tiempos de carga sean más extensos. Cuando se alcanza el umbral, Security Analytics muestra el conteo y el porcentaje de tiempo usado para alcanzar el conteo en comparación con el tiempo necesario para cargar todas las sesiones con ese valor. Por ejemplo, **(>100,000 - 18 %)** indica que el umbral se estableció en 100,000 y que esta carga tardó solamente el 18 % del tiempo que hubiese tardado sin un umbral definido. El valor predeterminado es **100000**.
Número máximo de resultados de valores	Esta configuración controla el número máximo de valores para cargar en la vista Navegar cuando la opción Resultados máximos está seleccionada en el menú Clave de metadatos para una Clave de metadatos abierta. El valor predeterminado es **1,000**. 
Máximo de exportación de sesiones	Esta configuración controla la cantidad máxima de sesiones que se pueden exportar. El valor predeterminado es **100000**.
Caracteres de vista de registro máximos	Este ajuste controla la cantidad máxima de caracteres que se mostrarán en **Investigation > Eventos > Texto del registro**. El valor predeterminado es **1,000**.

Característica	Descripción
Formato de registro de exportación	Este ajuste especifica el formato predeterminado para exportar registros desde Investigation. Las opciones disponibles son **Texto**, **XML**, **CSV** y **JSON**. No hay valor predeterminado incorporado para el formato de exportación de registro. Si no selecciona un formato aquí, Security Analytics muestra un cuadro de diálogo de selección cuando invoca la exportación de registros. Cuando selecciona una de las opciones del menú desplegable Formato de registro de exportación y hace clic en Aplicar, el ajuste se aplica de inmediato.
Mostrar información de depuración	Cuando se selecciona esta opción, Security Analytics muestra la cláusula where debajo de la ruta de navegación en la vista Navegar. Para cada carga de valor de metadatos se muestra el tiempo de carga. Si el servicio es un Broker, se informa el tiempo transcurrido para cada servicio agregado. El valor predeterminado es **Desactivado**.
Agregar eventos en el panel de eventos	Cuando se selecciona esta opción, los eventos que se muestran en el **Panel de eventos** se agregan de manera incremental, en lugar de sobrescribir los eventos visualizados actualmente. Por ejemplo, cada vez que hace clic en el ícono de la página siguiente, los eventos se muestran incrementalmente, como 1 -25, 1 -50, 1 -75 y así sucesivamente. **Nota:** Esta opción está disponible solo si la opción Optimizar cargas de la página Investigation está habilitada.
Cargar valores automáticamente	Cuando se selecciona esta opción, los valores del servicio se cargan automáticamente en la vista Navegar. Cuando no está seleccionada, Security Analytics muestra un botón **Cargar valores** que da al usuario la oportunidad de modificar las opciones. El valor predeterminado es **Desactivado**.

Característica	Descripción
Descargar PCAP finalizadas	Este ajuste automatiza la descarga de PCAP extraídas del módulo Investigation de modo que no sea necesario descargar ni abrir manualmente estos archivos en una aplicación que permite la visualización de datos en formato PCAP, como Wireshark.
Optimizar las cargas de páginas de Investigation	Esta opción está habilitada de forma predeterminada (marcada) y controla la forma en que la vista Eventos recupera eventos. Una vez optimizados, los resultados se devuelven lo más rápidamente posible. Esto dificulta la capacidad original de ir a una página específica en la lista de eventos. La deselección de esta casilla cambia la paginación en la lista de eventos y permite ir a una página específica de la lista (o a la última página). La capacidad de ir a cualquier página de la lista hace que se pierda velocidad en la entrega de resultados debido a la sobrecarga adicional para determinar los eventos por adelantado.
Vista de sesión predeterminada	Este ajuste selecciona el tipo de reconstrucción predeterminado para la vista de reconstrucción inicial. Los eventos predeterminados se construyen con el método de reconstrucción más apropiado para el evento.

Característica	Descripción
Habilitar reconstrucción de CSS para vista web	Esta configuración controla la forma en que se ejecuta la reconstrucción del contenido web. Si está habilitada, la reconstrucción web incluye imágenes y estilos de hoja de estilo en cascada (CSS), de modo que su aspecto coincide con la vista original en un navegador web. Esto incluye el escaneo y la reconstrucción de eventos relacionados y la búsqueda de hojasde estilo e imágenes que se usan en el evento objetivo. Esta opción está habilitada de manera predeterminada. Deseleccione esta opción si hay problemas para ver sitios web específicos. **Nota:** Es posible que el aspecto del contenido reconstruido no coincida perfectamente con la página web original si no se pudo encontrar imágenes y hojas de estilo relacionadas o si estas se cargaron desde la caché del navegador web. Además, el diseño o el estilo que se ejecuta dinámicamente a través de JavaScript en el lado del cliente no se generarán en la reconstrucción debido a que todo el JavaScript del lado de cliente se elimina por motivos de seguridad.
Opciones de búsqueda	Esta configuración establece las opciones de búsqueda predeterminadas que se aplicarán a una búsqueda en las vistas Navegar y Eventos. Investigation: Opciones de búsqueda proporciona información detallada.
Aplicar	Guarda las preferencias y las aplica de inmediato.

Investigation: Cuadro de diálogo Administrar claves de metadatos predeterminadas

En este tema se proporciona una descripción del cuadro de diálogo Administrar claves de metadatos predeterminadas.

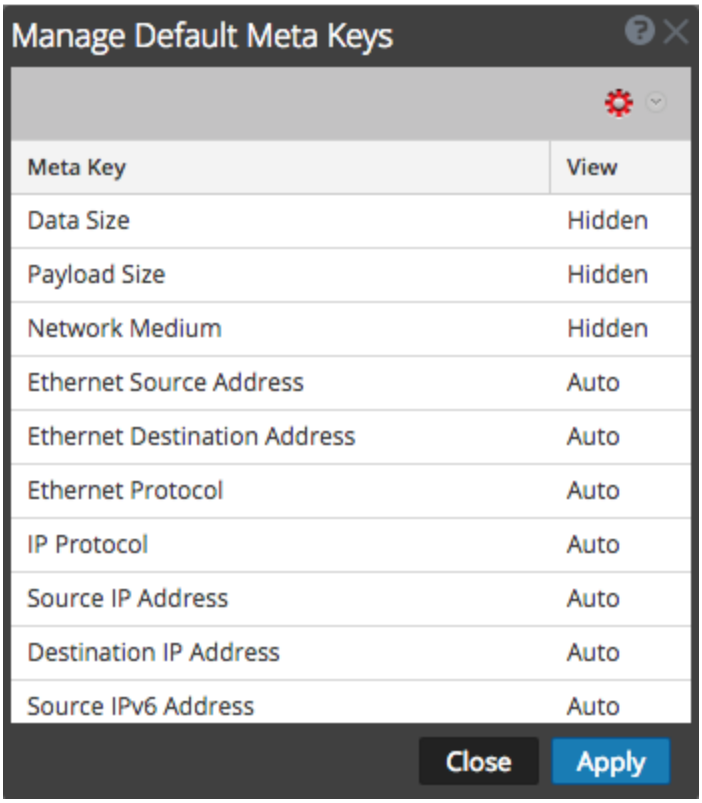
En el cuadro de diálogo Administrar claves de metadatos predeterminadas, los analistas pueden especificar las claves de metadatos que se mostrarán durante la navegación para un servicio específico. Esto puede ayudarlo a encontrar los datos que desea con mayor rapidez e impide la carga de metadatos que no son de interés.

Cuando modifica las claves de metadatos predeterminadas para una clave de metadatos no indexada, no puede configurar la clave en **Abierto**. Si cambia a **Abierto** la vista predeterminada para un grupo de claves de metadatos y algunas de las claves de metadatos no están indexadas, estas claves vuelven a **Automático**. En consecuencia, la clave de metadatos se carga automáticamente solo si está indexada, y las claves de metadatos no indexadas se **Cierran** hasta que se abren de forma manual.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar**.
   Se muestra el cuadro de diálogo Investigar.
2. Para seleccionar un servicio, realice una de las siguientes acciones:
   - Haga doble clic en un servicio.
   - Seleccione un servicio y haga clic en **Navegar**.
     Se muestra la vista Navegar del servicio seleccionado.
3. En la barra de herramientas de la **vista Navegar**, seleccione **Metadatos > Administrar claves de metadatos predeterminadas**.

Se muestra el cuadro de diálogo Administrar claves de metadatos predeterminadas.



Los procedimientos relacionados están disponibles en Administrar y aplicar claves de metadatos predeterminadas en una investigación.

Características

El cuadro de diálogo Administrar claves de metadatos predeterminadas tiene una cuadrícula, una barra de herramientas, el botón Cerrar y el botón Aplicar.

Cuadrícula

En la cuadrícula, puede ver, ordenar y administrar las claves de metadatos predeterminadas. Si hace clic y arrastra las claves de metadatos, puede cambiar su orden. En la tabla siguiente se proporcionan descripciones de las funciones de la cuadrícula.

Característica	Descripción
Clave de metadatos	En esta columna se muestran las claves de metadatos disponibles para el servicio.

Característica	Descripción
Ver	En esta columna se muestra el tipo de vista asignado a cada clave de metadatos. Si hace clic en la vista en cada fila, puede asignar otra vista predeterminada a la clave de metadatos. Hay cuatro vistas: • Automática: revierte a la vista predeterminada para las claves de metadatos según se especifica en el archivo de índice del servicio. • Cerrada: los valores de esta clave de metadatos están cerrados de manera predeterminada y se pueden abrir manualmente. • Oculta: estas claves de metadatos están ocultas de manera predeterminada y no se muestran en absoluto en Investigation. • Abierto: los valores de esta clave de metadatos se muestran de manera predeterminada.

Barra de herramientas y botones

En la siguiente tabla se describen las funciones de la barra de herramientas y de los botones.

Característica	Descripción
	Si hace clic en el menú Acciones, puede cambiar la vista predeterminada de todas las claves de metadatos. Hay cuatro vistas: • Automática: revierte a la vista predeterminada para las claves de metadatos según se especifica en el archivo de índice del servicio. • Cerrada: los valores de esta clave de metadatos están cerrados de manera predeterminada. • Oculta: los valores de esta clave de metadatos están ocultos de manera predeterminada. • Abierto: los valores de esta clave de metadatos se muestran de manera predeterminada.
Cerrar	Cierra el cuadro de diálogo. Los cambios sin guardar se pierden.

Característica	Descripción
Aplicar	Aplica los cambios y estos se implementan de inmediato.

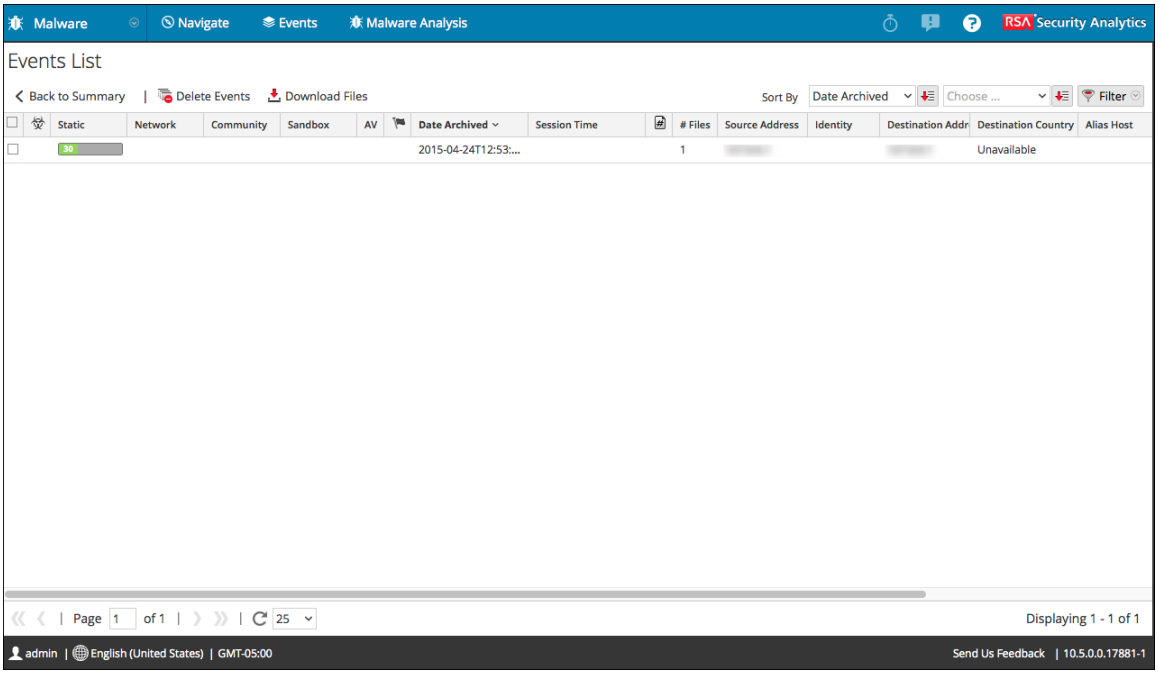
Investigation: Lista de eventos y Lista de archivos de Malware Analysis

La Lista de eventos y la Lista de archivos de Malware Analysis proporcionan una vista detallada de eventos o archivos. Puede hacer doble clic en un evento o archivo en cualquiera de las listas para mostrar la vista Resultados de análisis en una nueva pestaña del navegador.

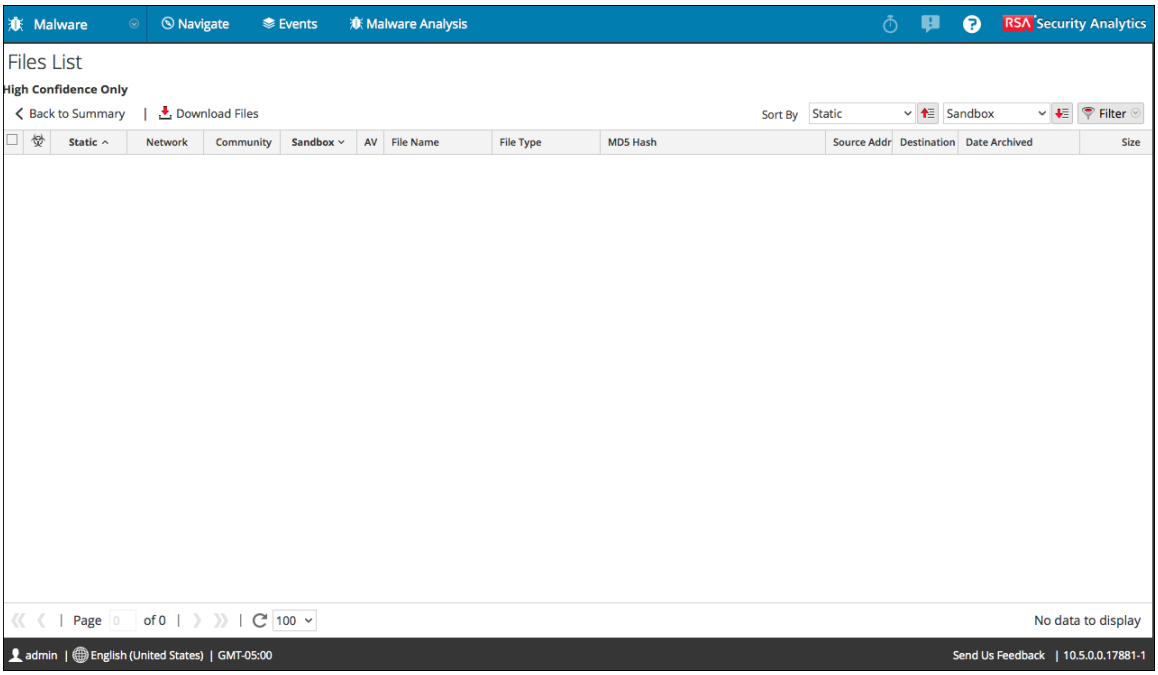
Para acceder a esta vista:

1. En el menú de **Security Analytics**, seleccione **Investigation > Malware Analysis**.
2. En el cuadro de diálogo **Seleccionar un servicio Malware Analysis**, seleccione un servicio en el panel de la izquierda y elija un trabajo en el panel de la derecha.
3. Haga clic en **Ver escaneo**.
   Se muestra la vista Resumen de eventos.
4. En el panel **Total** o en el panel **Alta confianza**, haga clic en el número de la sección **Eventos creados**.
   Si desea ver la Lista de archivos, haga clic en el número de la sección **Archivos procesados**.
5. De acuerdo con la opción elegida, se muestra la Lista de eventos o la Lista de archivos.

Este es un ejemplo de la vista Lista de eventos.



Este es un ejemplo de la vista Lista de archivos.



Los procedimientos relacionados están disponibles en Examinar archivos y eventos de escaneo en formato de lista.

Características

La **Lista de eventos** y la **Lista de archivos** tienen una cuadrícula y una barra de herramientas.

Barra de herramientas de la Lista de eventos

Estas son las funciones de la barra de herramientas de la Lista de eventos.

Cuadrícula de la Lista de eventos

Estas son las funciones de la cuadrícula de la Lista de eventos.

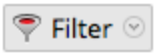
Característica	Descripción
	Indica si el evento tiene influencia de la marca de alta confianza.
Estático, Red, Comunidad y Sandbox	Muestra los puntajes de cada módulo de puntaje.
AV	Indica si el antivirus marcó este evento como sospechoso.

Característica	Descripción
	Indica si el evento tiene influencia de una regla personalizada.
Date Archived	Muestra la fecha y la hora en que se archivó el evento.
Tiempo de sesión	Muestra el tiempo de la sesión del evento.
	Indica si el valor de hash está marcado como de confianza.
Número de archivos	Muestra la cantidad de archivos que se incluyen en el evento.
Dirección de origen	Muestra la dirección del origen de eventos.
Identidad	Muestra la identidad del origen de eventos.
Dirección de destino	Muestra la dirección del destino del evento.
País de destino	Muestra el país del destino del evento.
Host de alias	Muestra el nombre de host del alias.
Tipo de evento	Muestra el tipo de evento. Por ejemplo, Carga manual.
Servicio	Muestra el servicio en el cual se produjo el evento.
Organización de destino	Muestra la organización del destino.

Barra de herramientas de la Lista de archivos

Estas son las funciones de la barra de herramientas de la Lista de archivos.

Característica	Descripción
Volver al resumen	Regresa a la vista Resumen de eventos.

Característica	Descripción
Download Files	Muestra el cuadro de diálogo Descarga de archivo de malware, el cual permite descargar los archivos disponibles.
	Muestra un menú desplegable desde el cual puede decidir cómo ordenar la lista. Estas son las opciones disponibles para ordenar la lista: • Alta confianza • Estático • Red • Comunidad • Sandbox • AV • Nombre de archivo • Tipo de archivo • Hash • Date Archived • Tamaño El botón directamente a la derecha de esta lista desplegable indica si la lista se ordenará por valores ascendentes o descendentes.
	Muestra un menú desplegable desde el cual puede seleccionar un orden de clasificación secundario. Este menú incluye una opción **Ninguno** que hace innecesaria la selección de un orden de clasificación secundario.
	Muestra una ventana desplegable en la cual puede filtrar la lista por nombre de archivo o hash de MD5.

Cuadrícula de la Lista de archivos

Estas son las funciones de la cuadrícula de la Lista de archivos.

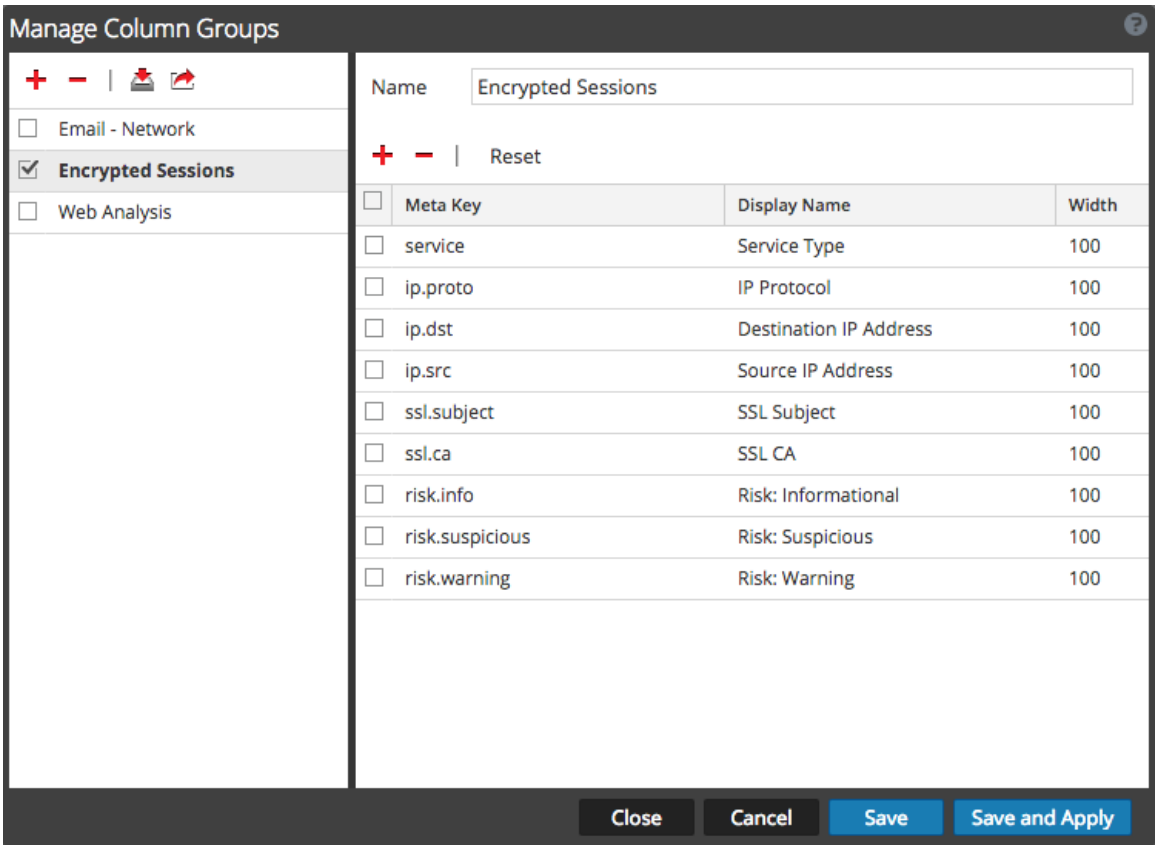
Característica	Descripción
	Indica si el evento tiene influencia de la marca de alta confianza.
Estático, Red, Comunidad y Sandbox	Muestra los puntajes de cada módulo de puntaje.
AV	Indica si el antivirus marcó este evento como sospechoso.
Nombre de archivo	Muestra el nombre del archivo.
Tipo de archivo	Muestra el tipo del archivo (por ejemplo, PDF o x86 PE)
Hash de MD5	Muestra el hash de MD5.
Dirección de origen	Muestra la dirección del origen del archivo.
Dirección de destino	Muestra la dirección del destino del archivo.
Date Archived	Muestra la fecha y la hora en que se archivó el archivo.
Tamaño	Indica el tamaño del archivo.

Investigation: Cuadro de diálogo Administrar grupos de columnas

El cuadro de diálogo Administrar grupos de columnas permite agregar, eliminar, importar, exportar y editar grupos de columnas para mostrar claves de metadatos específicas.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Investigation > Eventos**.
   Se muestra el cuadro de diálogo Investigar.
2. Seleccione un servicio y haga clic en **Navegar**.
3. En la barra de herramientas, seleccione **Vista detallada > Administrar grupos de columnas**.
   Se muestra el cuadro de diálogo Administrar grupos de columnas.



Los procedimientos relacionados están disponibles en Administrar grupos de columnas en la vista Eventos.

Características

El cuadro de diálogo Administrar grupos de columnas tiene dos paneles: Grupos y Configuración.

En la parte inferior de este cuadro diálogo hay cuatro botones: Cerrar, Cancelar, Guardar y Guardar y aplicar. En la siguiente tabla se proporcionan descripciones de estos botones.

Característica	Descripción
Cerrar	Cierra el cuadro de diálogo sin guardar.
Cancelar	Cancela todos los cambios no guardados.
Guardar	Guarda todos los cambios sin cerrar el cuadro de diálogo.
Guardar y aplicar	Guarda y aplica todos los cambios de inmediato y cierra el cuadro de diálogo.

Panel Grupos

El panel izquierdo es el panel Grupos. Este panel permite agregar, eliminar, importar o exportar grupos de columnas. En la parte superior del panel hay una barra de herramientas que proporciona acciones. Debajo de la barra de herramientas encontrará una lista de grupos de columnas agregados que permite seleccionar uno o más grupos.

En la siguiente tabla se indican las acciones de la barra de herramientas.

Acción	Descripción
	Agrega un grupo de columnas. Si se hace clic en este botón, se resalta el panel Configuración de la derecha que permite dar un nombre al grupo de columnas y agregar o eliminar claves de metadatos. Para agregar un grupo, se requiere por lo menos una clave de metadatos.
	Elimina un grupo de columnas. Se muestra un cuadro de diálogo de confirmación antes de la eliminación del grupo seleccionado.
	Muestra el cuadro de diálogo Importar grupos de columnas que permite seleccionar un archivo para cargar.
	Exporta uno o más grupos seleccionados a la computadora.

Panel Configuración

El panel de la derecha es el panel Configuración. Aquí puede crear y editar grupos de columnas. Este panel incluye el campo Nombre, una barra de herramientas y una cuadrícula.

En la siguiente tabla se describen las funciones del panel Configuración.

Característica	Descripción
Nombre	El nombre del grupo de columnas seleccionado.
	Agrega una nueva fila a la lista de claves de metadatos, donde puede abrir un menú desplegable para seleccionar una nueva clave de metadatos.
	Elimina una o más claves de metadatos seleccionadas. Muestra un cuadro de diálogo de confirmación antes de la eliminación.
Restablecer	Devuelve el grupo de columnas a la configuración guardada más reciente.
Clave de metadatos	Indica las claves de metadatos agregadas al grupo de columnas seleccionado.
Display Name	Indica los nombres de las claves de metadatos como se mostrarán en la vista Eventos.
Ancho	Especifica el ancho de la columna de cada clave de metadatos. El ancho se puede configurar entre **10** y **1000**. El ancho predeterminado es **100**.

Investigation: Cuadro de diálogo Administrar grupos de metadatos

En este tema se describen las características y las funciones del cuadro de diálogo Administrar grupos de metadatos.

El cuadro de diálogo Administrar grupos de metadatos permite agregar, eliminar, importar y exportar grupos de metadatos.

Para acceder a este cuadro de diálogo:

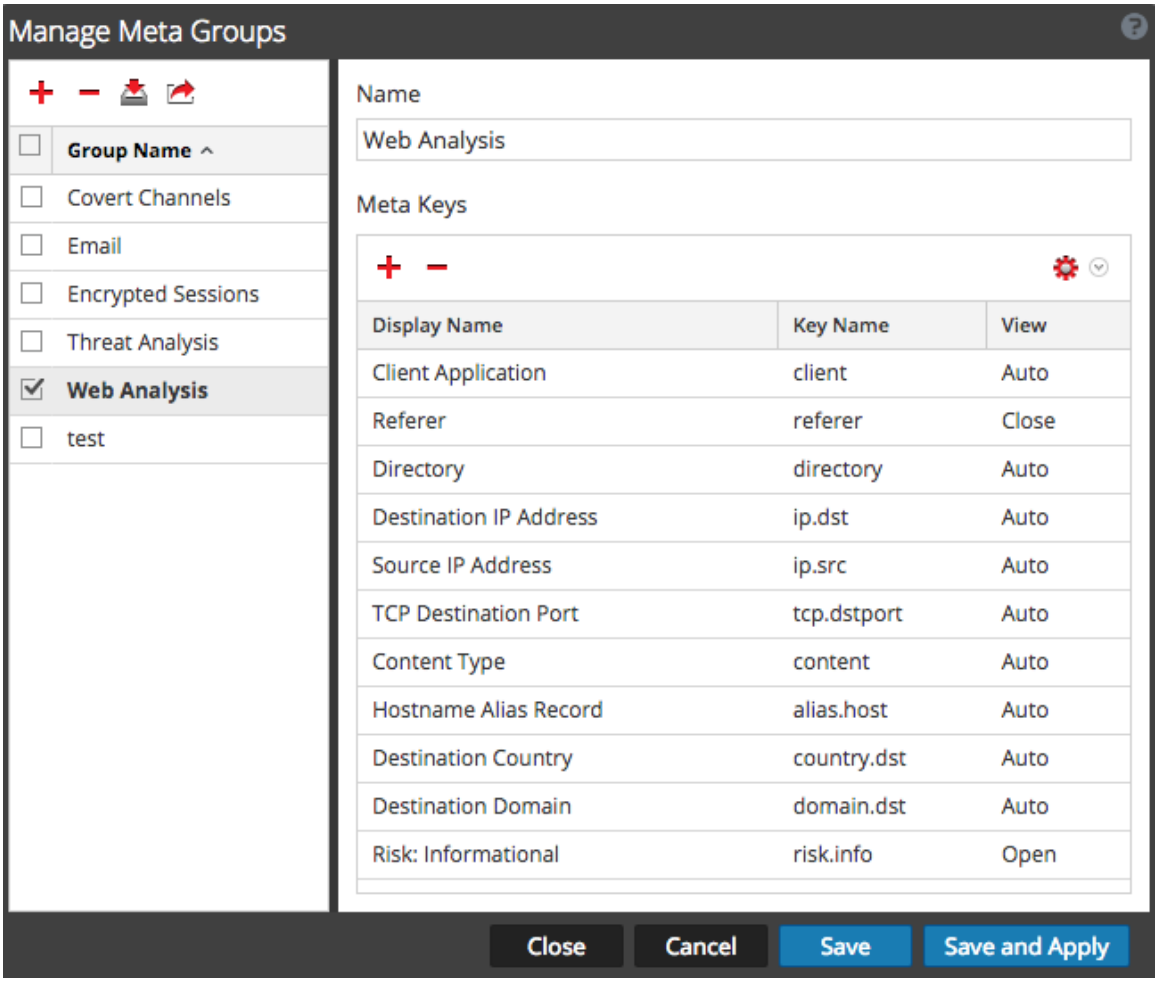
1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar**.

   Se muestra el cuadro de diálogo Investigar.

2. Seleccione un servicio y haga clic en **Navegar**.

3. En la barra de herramientas de la **vista Navegar**, seleccione **Metadatos > Administrar grupos de metadatos**.

   Se muestra el cuadro de diálogo Administrar grupos de metadatos.



Los procedimientos que puede realizar en este cuadro de diálogo se describen en Administrar grupos de metadatos definidos por el usuario.

Características

El cuadro de diálogo Administrar grupos de metadatos tiene dos paneles. En la siguiente tabla se describen los botones de la parte inferior del cuadro de diálogo.

Característica	Descripción
Cerrar	Cierra el cuadro de diálogo.
Cancelar	Cancela todos los cambios.
Guardar	Guarda todos los cambios.
Guardar y aplicar	Guarda todos los cambios y los aplica de inmediato.

Panel Grupos de metadatos

El panel Grupos de metadatos está en el lado izquierdo del cuadro de diálogo Administrar grupos de metadatos. Aquí puede agregar, eliminar, importar y exportar grupos de metadatos.

En la siguiente tabla se describen las funciones del panel Grupos de metadatos.

Característica	Descripción
	Agrega un grupo de metadatos mediante el panel Configuración del lado derecho del cuadro de diálogo Administrar grupos de metadatos.
	Elimina los grupos de metadatos seleccionados. Se muestra un cuadro de diálogo de confirmación antes de la eliminación del grupo de metadatos.
	Muestra el cuadro de diálogo Importación de grupo de metadatos, en el cual puede cargar un archivo.
	Exporta el grupo de metadatos seleccionado a la computadora.
Group Name	Enumera todos los nombres de grupos de metadatos.

Panel Configuración

El panel Configuración está en el lado derecho del cuadro de diálogo Administrar grupos de metadatos. Aquí puede crear y editar grupos de metadatos. Debajo del campo Nombre se encuentra la cuadrícula Claves de metadatos.

En la siguiente tabla se describen las funciones del panel Configuración.

Característica	Descripción
Nombre	Muestra el nombre del grupo de metadatos seleccionado.
	Muestra el cuadro de diálogo Claves de metadatos disponibles, en el cual puede seleccionar las claves de metadatos que agregará al grupo.
	Elimina las claves de metadatos seleccionadas.
	Muestra un menú desplegable que permite seleccionar la vista para todas las claves de metadatos. Hay cuatro opciones de acuerdo con los posibles valores de la propiedad `defaultAction` que se usa para definir una clave en el archivo de índice personalizado para el servicio: • Oculto: Estas claves de metadatos están ocultas de manera predeterminada y no se muestran en absoluto en Investigation. • Abierto: Los valores de esta clave de metadatos se muestran de manera predeterminada. • Cerrado: Los valores de esta clave de metadatos están cerrados de manera predeterminada y se pueden abrir manualmente. • Automático: Revierte a la vista predeterminada para las claves de metadatos según se especifica en el archivo de índice del servicio.
Display Name	Indica el nombre que se muestra para la clave en las vistas de Investigation y se define mediante la propiedad `description` para la clave en el archivo de índice personalizado del servicio.
Nombre de clave	Indica el valor `name` de la clave de metadatos según se define en el archivo de índice personalizado del servicio.

Característica	Descripción
Ver	Indica en qué vista está configurada la clave de metadatos. Para cambiar esto: • Haga clic en  y seleccione una vista para cambiar todas las vistas de la clave de metadatos. • Haga clic en una única clave de metadatos en la columna Vista y abra el menú desplegable en el cual se muestran todas las vistas disponibles para cambiar una vista de clave de metadatos individual.

Investigation: Cuadro de diálogo Administrar perfiles

El cuadro de diálogo Administrar perfiles permite configurar, agregar, eliminar, importar y exportar perfiles.

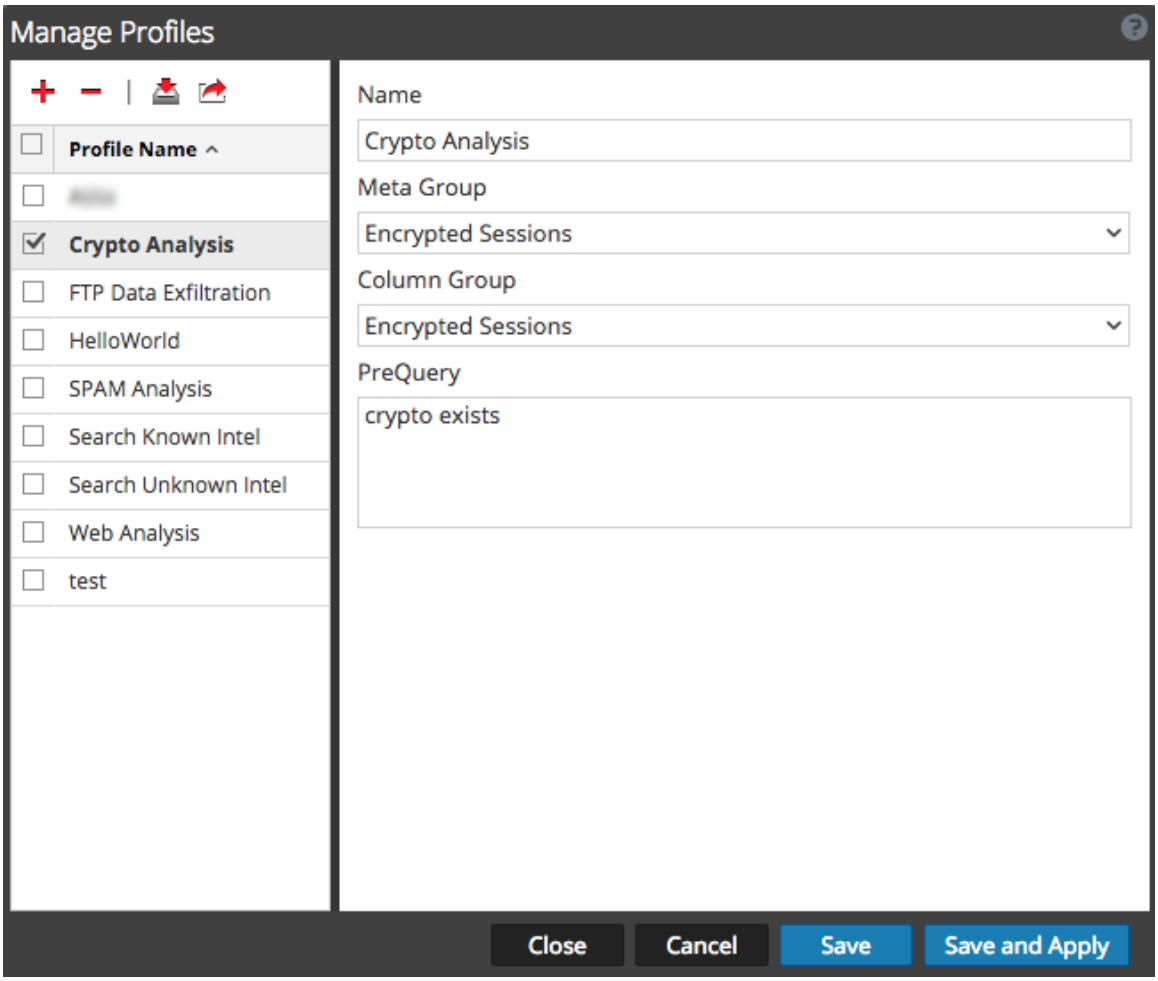
Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Eventos**. Ambas vistas proporcionan acceso al cuadro de diálogo Administrar perfiles.

   Se muestra el cuadro de diálogo Investigar.

2. Seleccione un servicio y haga clic en **Navegar**.
3. En la barra de herramientas, seleccione **Perfil > Administrar perfiles**.

   Se muestra el cuadro de diálogo Administrar perfiles.



Los procedimientos relacionados están disponibles en Usar perfiles de Investigation para encapsular vistas personalizadas.

El cuadro de diálogo Administrar perfiles tiene dos paneles. En la parte inferior del cuadro de diálogo se incluye una fila de botones.

Botones

En la siguiente tabla se describen los botones.

Campo	Descripción
Cerrar	Cierra el cuadro de diálogo.
Cancelar	Cancela todos los cambios.
Guardar	Guarda todos los cambios.
Guardar y aplicar	Guarda y aplica todos los cambios de inmediato.

Panel Perfil

El panel Perfil del lado izquierdo del cuadro de diálogo muestra los perfiles disponibles y permite agregar, eliminar, importar y exportar perfiles.

En la siguiente tabla se describen los campos del panel Perfil.

Campo	Descripción
	Agrega un nuevo perfil mediante el panel Configuración del lado derecho del cuadro de diálogo Administrar perfiles.
	Elimina el perfil seleccionado. Antes de que se elimine el perfil, se muestra un cuadro de diálogo de confirmación.
	Muestra el cuadro de diálogo Importación de perfil, el cual permite cargar un archivo.
	Exporta el perfil seleccionado a una computadora.
Profile Name	Enumera todos los nombres de perfil.

Panel Configuración

El panel Configuración del lado derecho del cuadro de diálogo ofrece opciones para configurar perfiles. Solo se puede usar cuando hay un perfil seleccionado.

En la siguiente tabla se describen los campos del panel Configuración.

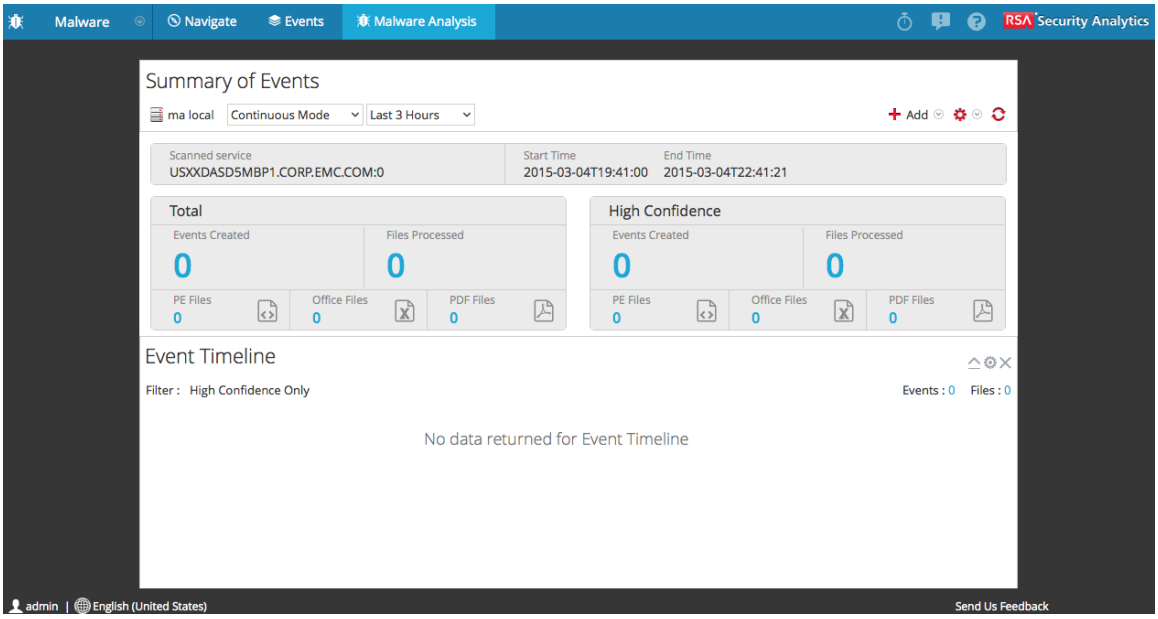
Característica	Descripción
Nombre	Muestra el nombre del perfil.
Grupo de metadatos	Muestra un menú desplegable que enumera los grupos de metadatos disponibles.
Grupo de columnas	Muestra un menú desplegable que enumera los grupos de columnas disponibles. De manera predeterminada, hay tres grupos disponibles: • Vista de lista • Vista detallada • Vista de registro
Consulta previa	Define una consulta restrictiva para filtrar los resultados de Investigation. Esta consulta se usa cuando el perfil asociado está habilitado y la consulta previa se aplica a cualquier consulta utilizada en las vistas Navegar y Eventos de Investigation. Este es un ejemplo de una consulta previa: `'service=80,25,110'.`

Investigation: Vista Malware Analysis

En Security Analytics Investigation, la vista Malware Analysis proporciona la interfaz del usuario para realizar un análisis de malware. Esta vista tiene un formato de tablero personalizable, en el cual los dashlets predeterminados de la vista inicial se basan en la función del usuario (Administración o Analista) y en sus personalizaciones. Inicialmente, en la vista Malware Analysis se muestra el dashlet Resumen de eventos. Los dashlets adicionales presentan distintas visualizaciones de los eventos que se ven, y cada representación se puede configurar para refinar aún más la vista a medida que usted busca indicadores de riesgo. Los dashlets de Malware Analysis disponibles en el tablero de Security Analytics también están disponibles en la vista Malware.

Para acceder a esta vista:

1. En el menú de **Security Analytics**, seleccione **Investigation > Malware Analysis**.
   Si no se seleccionó un servicio predeterminado, se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis.
2. Seleccione un servicio y haga clic en **Ver modo continuo**.
   Se muestra la vista Malware Analysis.



Características

La vista Malware Analysis consta del panel Resumen de eventos y de cuatro dashlets exclusivos. Cada uno de los dashlets únicos tiene cuadros de diálogo Opciones idénticos. Los dashlets de Malware Analysis en el tablero de Security Analytics también están disponibles y se describen en Dashlets de Security Analytics.

Panel Resumen de eventos

El panel Resumen de eventos permite seleccionar el servicio, el modo de escaneo y el rango de tiempo. Además, puede seleccionar un punto de datos y ver los eventos asociados al evento.

En la siguiente tabla se describen todas las funciones del panel Resumen de eventos.

Característica	Descripción
	Selecciona un servicio para mostrar.
Modo de escaneo	Muestra una lista desplegable de modos de escaneo disponibles.
Rango de tiempo	Muestra una lista desplegable de rangos de tiempo para ver eventos.
Fecha de inicio	Cuando Rango de tiempo se configura en personalizado, ofrece un calendario que permite elegir la fecha inicial del rango de tiempo.
Fecha final	Cuando Rango de tiempo se configura en personalizado, ofrece un calendario que permite elegir la fecha final del rango de tiempo.
	Muestra una lista desplegable de dashlets que puede agregar a la vista.
	Muestra una lista desplegable de acciones que puede realizar en esta vista: • Restaurar configuración predeterminada • Ordenar dashlets • Aplicar filtro de umbral
	Actualiza la vista Malware Analysis.

Cuadro de diálogo Opciones

El cuadro de diálogo Opciones permite personalizar los resultados que se muestran en el dashlet.

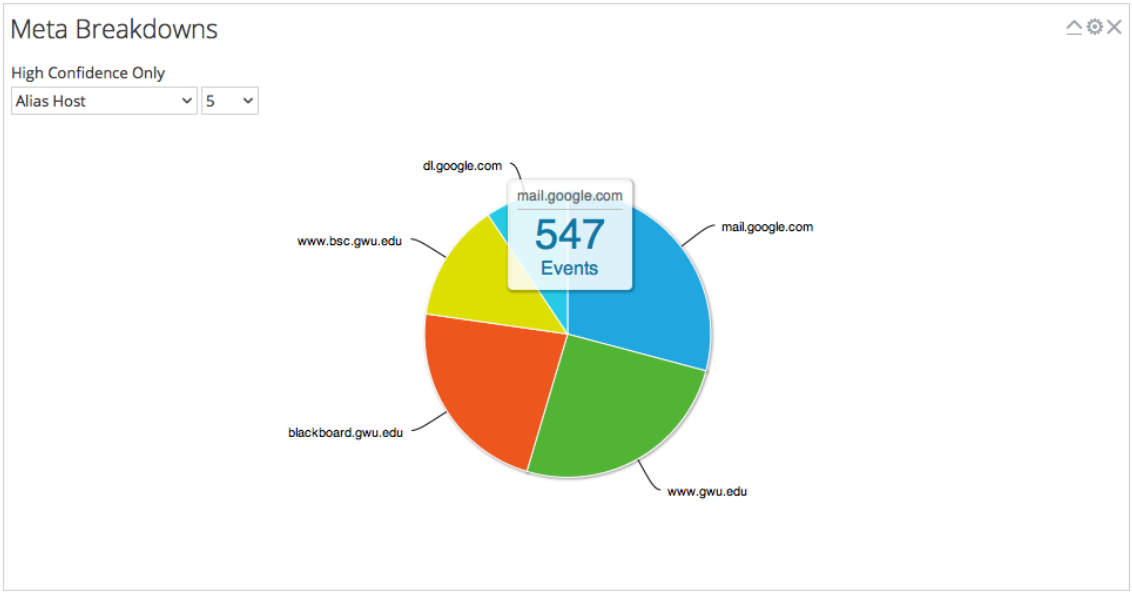
Para acceder a este cuadro de diálogo, haga clic en el ícono  en la esquina superior derecha de cada dashlet. En la siguiente tabla se describen las funciones del cuadro de diálogo Opciones.

Característica	Descripción

Característica	Descripción
Título	Indica si los datos mostrados se restringen o no a eventos marcados como de alta confianza. Si los datos no están restringidos, esta línea no se muestra.
Solo con influencia de alta confianza	Indica si los datos mostrados se restringen a eventos marcados como de alta confianza.
Estático, Red, Comunidad y Sandbox	Permite filtrar los resultados en función de los puntajes de los módulos de puntaje.
Cancelar	Cierra el cuadro de diálogo sin guardar los cambios.
Aplicar	Aplica los cambios al dashlet de inmediato y cierra el cuadro de diálogo.

Desgloses de metadatos

Desgloses de metadatos presenta eventos en forma de un gráfico circular, en el cual cada segmento representa un valor de metadatos para la clave de metadatos especificada. Puede seleccionar la clave de metadatos y el conteo de valores de metadatos para esa clave que se generará en el gráfico, comenzando por el valor de metadatos que tiene más eventos. Si mantiene el mouse sobre un evento se muestra el conteo.

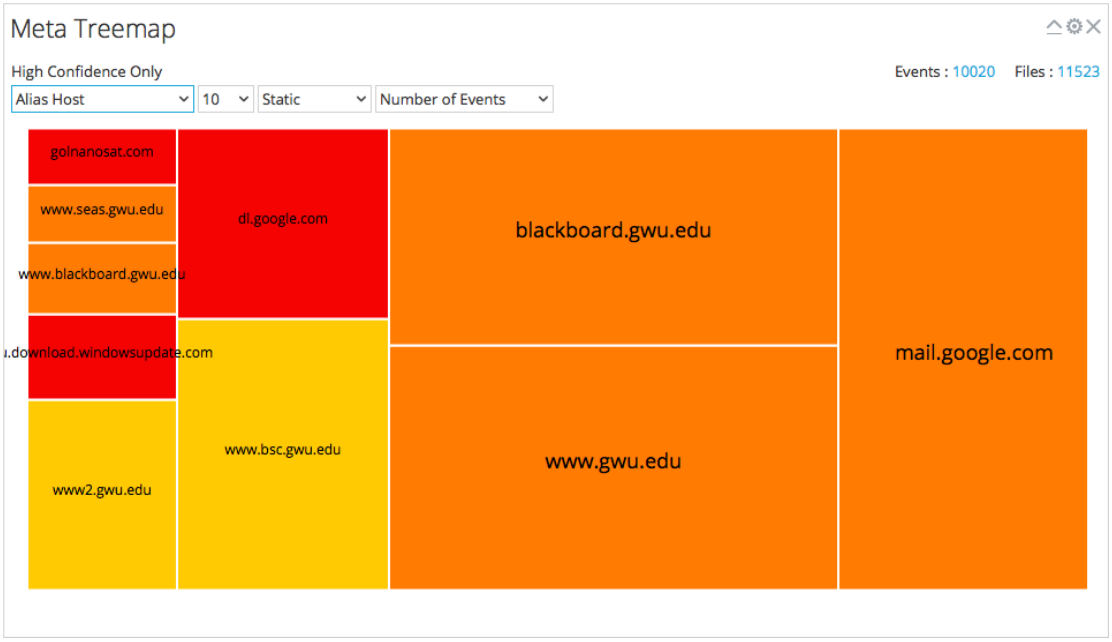


En la siguiente tabla se describen las opciones del dashlet Desgloses de metadatos.

Característica	Descripción
Solo alta confianza	Indica si los datos mostrados se restringen o no a eventos marcados como de alta confianza. Si los datos no están restringidos, esta línea no se muestra.
Clave de metadatos	Lista desplegable de claves de metadatos disponibles.
Count	Lista desplegable que especifica cuántos de los resultados principales se muestran.

Mapa de árbol de metadatos

El Mapa de árbol de metadatos presenta eventos en forma de un mapa de riesgos. Puede seleccionar la clave de metadatos y el conteo de valores de metadatos para esa clave que se generará en el gráfico, comenzando por los valores de metadatos que tienen más eventos. Además, puede seleccionar el módulo que detectó el valor de metadatos en los eventos: estático, red, Community o Sandbox.



En la siguiente tabla se describen las opciones del dashlet Mapa de árbol de metadatos.

Característica	Descripción
Solo alta confianza	Indica si los resultados se restringen o no a eventos marcados como de alta confianza. Si los resultados no están restringidos, esta línea no se muestra.
Clave de metadatos	Lista desplegable de claves de metadatos disponibles para seleccionar como filtro.
Count	Lista desplegable que especifica cuántos de los resultados principales se muestran.
Módulo	Lista desplegable que especifica de qué módulo se extraerán resultados.
Valor	Lista desplegable que especifica la información que se mostrará cuando se mantenga el mouse sobre un resultado (por ejemplo, Puntaje promedio).

Rueda de puntaje

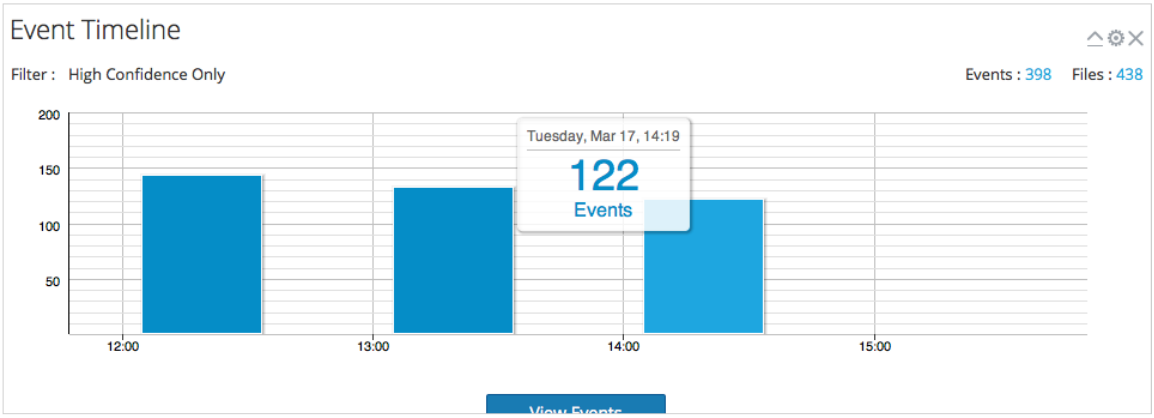
La rueda de puntaje ofrece una vista de eventos como anillos concéntricos con colores que representan los puntajes de los eventos de acuerdo con indicadores de riesgo y el módulo de puntaje. Puede cambiar la posición de los anillos mediante las flechas hacia arriba y hacia abajo para obtener una vista que resalta los eventos que detectó un módulo de puntaje (rojo) y que no detectaron otros módulos de puntaje.

En la siguiente tabla se describen las funciones del dashlet Rueda de puntaje.

Característica	Descripción
Solo alta confianza	Indica si los resultados se restringen o no a eventos marcados como de alta confianza. Si los resultados no están restringidos, esta línea no se muestra.
Cuadrícula Orden de módulos	Muestra el orden de los anillos en la rueda de puntaje. Anillo 1 es el anillo interior y Anillo 4, el exterior. Puede hacer clic en los botones **Arriba** y **Abajo** para reordenar los módulos y, a continuación, hacer clic en **Actualizar** para aplicar los cambios.

Cronograma de evento

El Cronograma de evento ofrece una vista de eventos organizados por el momento de la aparición en un gráfico de barras. Si se hace clic y se arrastra para seleccionar un rango de tiempo dentro del gráfico, se realiza un acercamiento al tiempo seleccionado.



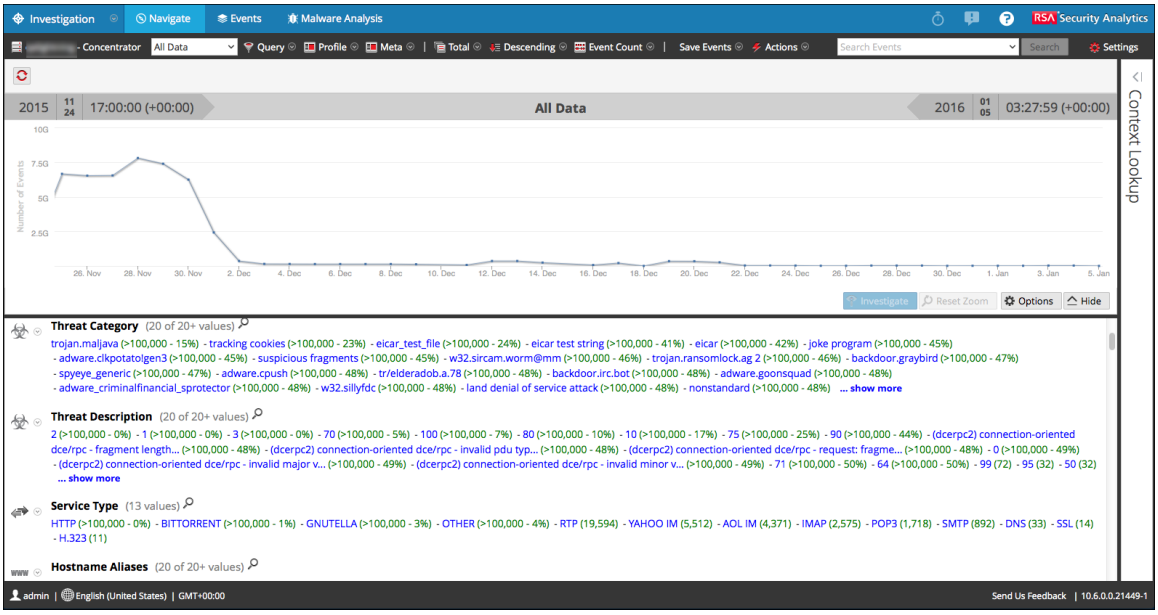
En la siguiente tabla se describen las funciones del dashlet Cronograma de evento.

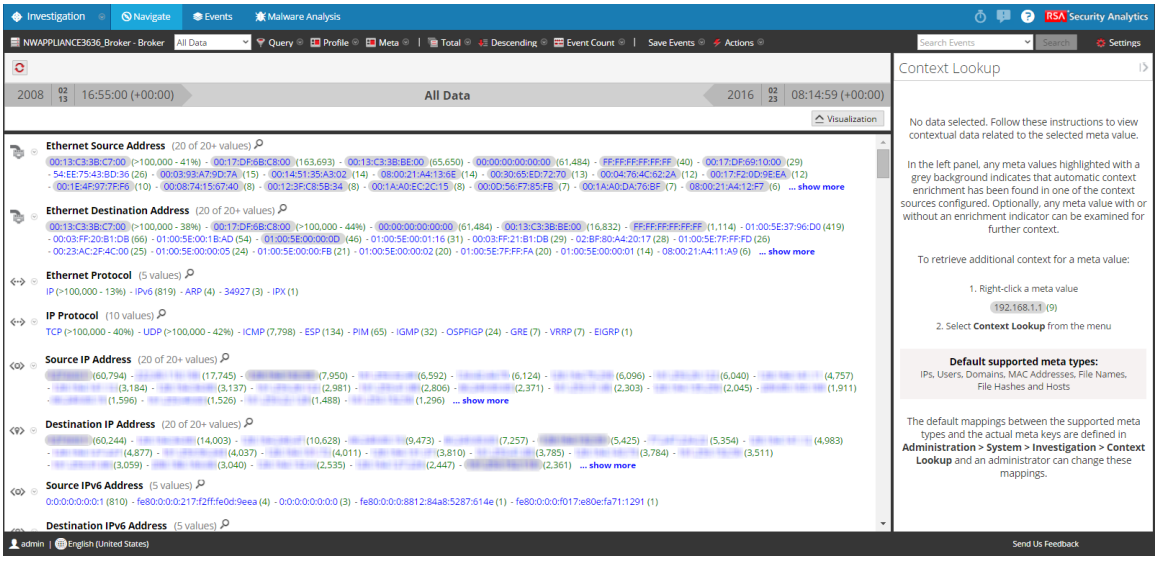
Característica	Descripción
Solo alta con-fianza	Indica si los resultados se restringen o no a eventos marcados como de alta confianza. Si los resultados no están restringidos, esta línea no se muestra.
Ver eventos	Muestra Investigation > vista Eventos.

Investigation: Vista Navegar

La vista Navegar muestra la actividad y los valores del servicio seleccionado de acuerdo con las opciones de Investigation en el panel Opciones: perfil, rango de tiempo, grupo de metadatos y consulta. A medida que investiga eventos de interés, se muestran las claves de metadatos y los valores.

Para acceder a la vista Navegar, seleccione **Investigation > Navegar** en el menú de **Security Analytics**. Cuando hay una investigación de servicio abierta, la vista es similar a la figura que se muestra a continuación.





La vista Navegar consta de las siguientes características:

- Barra de herramientas
- Botón Pausa/Recarga y ruta de navegación
- Anuncio de tiempo
- Información de depuración opcional.
- Panel Visualización contraíble
- Panel Valores
- Panel Búsqueda de contexto

Barra de herramientas

La barra de herramientas proporciona una manera de:

- Cambiar el servicio que se investiga.
- Controlar el rango de datos que se muestra: puede seleccionar perfiles de uso, establecer un rango de tiempo, usar grupos de metadatos y crear consultas para aplicar a los datos.
- Establecer el método de cuantificación y el método de clasificación de los datos en el panel Valores.
- Realizar acciones en función de los resultados. Puede exportar e imprimir resultados, navegar a un evento para el cual tiene un ID de evento y transmitir una consulta a Informer.
- Configurar ajustes de Investigation sin salir de las vistas de Investigation.

Algunas de las opciones de la barra de herramientas están etiquetadas con el valor predeterminado o el valor seleccionado en lugar de mostrar el nombre de la opción. Por ejemplo, la opción de rango de tiempo del ejemplo anterior está etiquetada **Todos los datos** para reflejar el valor seleccionado actualmente. Las opciones de la barra de herramientas son las siguientes.

Opción	Descripción
	Muestra el nombre del servicio seleccionado junto al ícono. Si hace clic en el ícono, se abre un cuadro de diálogo Investigar un servicio, en el cual puede seleccionar un servicio para investigar y establecer el servicio predeterminado que se investigará (consulte Comenzar una investigación de un servicio o una recopilación). El cambio del servicio no hace que se vuelvan a cargar los datos.

Opción	Descripción
Rango de tiempo	Muestra las opciones de Rango de tiempo; la opción seleccionada actualmente aparece en la barra de herramientas (consulte Establecer el rango de tiempo para una investigación). Las posibles opciones son las siguientes: • Todos los datos • Últimos 5, 10, 15 o 30 minutos • Última hora, últimas 3, 6, 12 o 24 horas • Últimos 2 o 5 días • Primera hora • Mañana • Tarde • Noche • Todo el día • Ayer • Esta semana • La semana pasada • Personalizado **Nota:** Si se especifican horas de inicio o finalización personalizadas en segundos, siempre el valor de la hora de inicio en segundos se configura de manera predeterminada en :00 y siempre el valor de la hora de finalización en segundos se configura de manera predeterminada en :59. Por ejemplo, si está usando la hora para desglosar un problema, la hora de desglose se interpreta como `HH:MM:00 - HH:MM:59`. Los segundos se muestran en este formato en las funciones de Investigation > Navegar.
Consulta	Se muestra el cuadro de diálogo Consulta, en el cual puede ingresar directamente una consulta personalizada, en lugar de desglosar los datos. Consulte Investigation: Cuadro de diálogo Consulta para obtener una descripción del cuadro de diálogo.

Opción	Descripción
Perfil	Muestra el menú Perfil; el perfil seleccionado se muestra en la barra de herramientas. Un perfil permite administrar y usar perfiles que pueden incluir grupos de metadatos personalizados, un grupo de columnas predeterminado y una consulta inicial. Los perfiles se aplican a la vista Navegar (consultas y grupos de metadatos) y a la vista Eventos (consultas y grupos de columnas). Consulte Usar perfiles de Investigation para encapsular vistas personalizadas para obtener más información.
Metadatos	Muestra el menú Grupo de metadatos. Puede usar claves de metadatos predeterminadas o un grupo de metadatos personalizado. También tiene la opción de realizar cambios en ambos tipos de grupos (consulte Administrar grupos de metadatos definidos por el usuario).
Campo de clasificación	Muestra el menú Campo de clasificación; la opción actualmente seleccionada se muestra en la barra de herramientas. Este menú tiene dos opciones: Ordenar por total y Ordenar por valor. El Campo de clasificación es un complemento de la opción Orden de clasificación; los datos de cada clave de metadatos se ordenan de acuerdo con el total (número verde) o con el valor de metadatos (texto azul) (consulte Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos).
Orden de clasificación	Muestra el menú Orden de clasificación; la opción actualmente seleccionada se muestra en la barra de herramientas. Este menú tiene dos opciones: Clasificar en orden ascendente y Clasificar en orden descendente. El Orden de clasificación es un complemento de la opción Campo de clasificación; el campo seleccionado de cada clave de metadatos se clasifica en orden descendente o ascendente (consulte Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos)).

Opción	Descripción
Método de cuantificación	Muestra el menú Método de cuantificación; la opción actualmente seleccionada se muestra en la barra de herramientas. El menú desplegable contiene tres opciones para calcular la cantidad (el número verde entre paréntesis) para un valor de metadatos: Cuantificar por conteo de eventos, Cuantificar por tamaño de evento y Cuantificar por conteo de paquetes (consulte Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos)). Estas opciones se aplican de manera diferente según el tipo de datos de la vista. Para datos de paquetes: • Cuantificar por conteo de eventos muestra la cantidad de sesiones. • Cuantificar por tamaño de evento muestra el tamaño en bytes. • Cuantificar por conteo de paquetes muestra la cantidad de paquetes. Para datos de registros: • Cuantificar por conteo de eventos muestra la cantidad de registros. • Cuantificar por tamaño de evento muestra el tamaño en bytes. • Cuantificar por conteo de paquetes muestra la cantidad de registros.
Acciones	En el menú Acciones se incluyen varias acciones (Visualizar, Ir a evento e Imprimir) que puede realizar en la vista Navegar (consulte Actuar conforme a un punto de desglose en la vista Navegar).
Guardar eventos	Muestra el menú Guardar eventos, en el cual pude utilizar opciones para:extraer archivos asociados con un evento, exportar el punto de desglose actual como un archivo PCAP y exportar el punto de desglose actual como un archivo de registro (consulte Exportar un punto de desglose).
Buscar eventos	Le permite buscar patrones de texto en el conjunto actual de eventos. Si hace clic en el campo de búsqueda, se muestra un menú desplegable con opciones de búsqueda. Si hace clic en Aplicar, guarda las opciones seleccionadas y también actualiza las opciones de búsqueda en la vista Eventos y el perfil de investigaciones (consulte Investigation: Opciones de búsqueda).

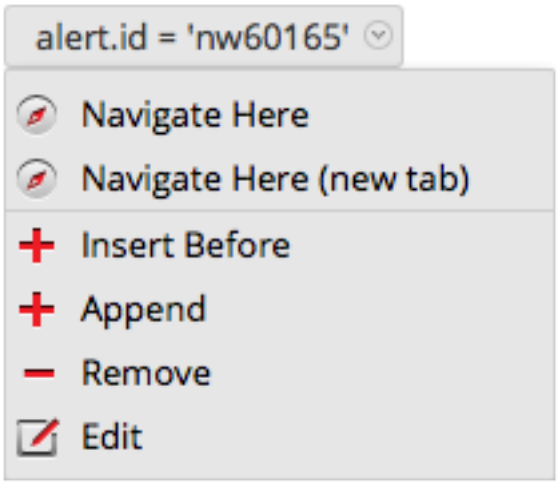
Opción	Descripción
Configuración	Muestra los ajustes de Investigation para la vista Navegar (los cuales también se pueden editar en la vista Perfil), de modo que puede cambiarlos sin salir de la vista Navegar. Cuando cambia un ajuste en la vista Navegar, este también se cambia en la vista Perfil (consulte Configurar la vista Navegar y la vista Eventos).

Botón Pausa/Volver a cargar y ruta de navegación

La ruta de navegación rastrea cada consulta a medida que se desglosa a través de los metadatos del servicio. Cada consulta se enumera con un menú desplegable en una cadena separada por barras verticales. El último punto es el punto actual, que también se llama punta. El ícono frente a la ruta de navegación permite poner en pausa la carga de valores de metadatos y volver a cargarlos.

La ruta de navegación no incluye el nombre del servicio y solo se muestra si hay una consulta vigente. Si existen demasiados puntos de desglose para mostrar, el desbordamiento se indica como paréntesis angulares dobles, >>, al final de la ruta de navegación.

Cada menú desplegable en la ruta de navegación es igual, pero presenta una leve variación en función de la posición en la ruta de navegación.

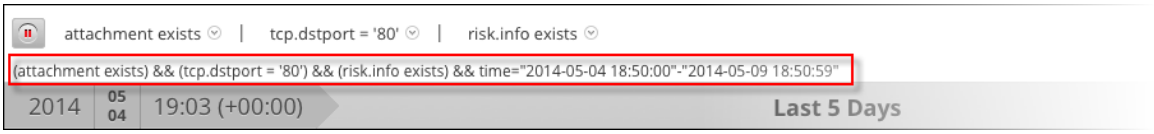


En la siguiente tabla se describen los controles y las opciones de menú en la ruta de navegación.

Característica	Descripción
	Botón Pausa y Recarga. Controla la carga de datos en la vista. Tiene tres funciones posibles: pausar carga, continuar carga y volver a cargar.
Navegar aquí	Abre el punto de desglose seleccionado en el panel Valores actual.
Navegar aquí (nueva pestaña)	Abre el punto de desglose seleccionado en una nueva pestaña.
Insertar antes	Inserta una consulta antes del punto de desglose actual. Se abre el cuadro de diálogo Crear filtro, en el cual puede definir una consulta personalizada para insertar en la ruta de navegación (consulte Crear una consulta personalizada).
Anexar	Agrega una consulta después del punto de desglose actual. Se abre el cuadro de diálogo Crear filtro, en el cual puede definir una consulta personalizada para anexar al final de la ruta de navegación (consulte Crear una consulta personalizada).
Quitar	Elimina el punto de desglose seleccionado de la ruta de navegación.
Editar	Abre el punto de desglose seleccionado en el cuadro de diálogo Crear filtro, lo cual le permite editar la consulta.
>>	Si hace clic en los paréntesis angulares, se muestra un menú desplegable del desbordamiento de la ruta de navegación.

(Opcional) Información de depuración

Si activó el ajuste Mostrar información de depuración y el servicio en el cual está navegando es un Broker 10.4 o superior, Security Analytics muestra la información de depuración debajo de la ruta de navegación.



La información de depuración es la cláusula `where` de la consulta actual. La única vez que no hay una cláusula `where` es cuando el rango de tiempo corresponde a todos los datos y no hay puntos de desglose. Si el Broker tiene por lo menos un servicio agregado que está offline, la información de depuración también incluye el servicio offline.

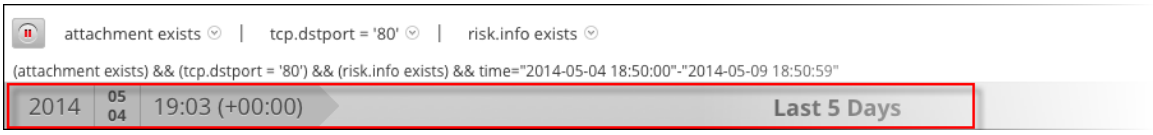
Por ejemplo:

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)
$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment exists) &&
(tcp.dstport = '80') && (risk.info exists) && time="2014-05-04
18:50:00"-"2014-05-09 18:50:59"
```

Además, el tiempo de carga se muestra al final de cada clave de metadatos en el panel Valores.

Anuncio de tiempo

Inmediatamente debajo de la ruta de navegación y de la información de depuración (si está presente), el anuncio de tiempo muestra el rango de tiempo que se usó para crear el gráfico.

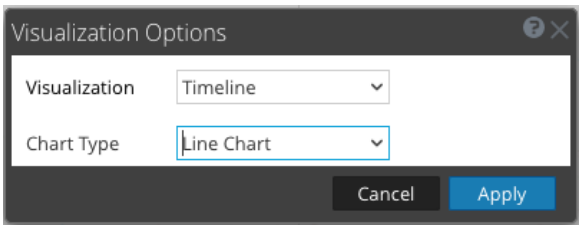


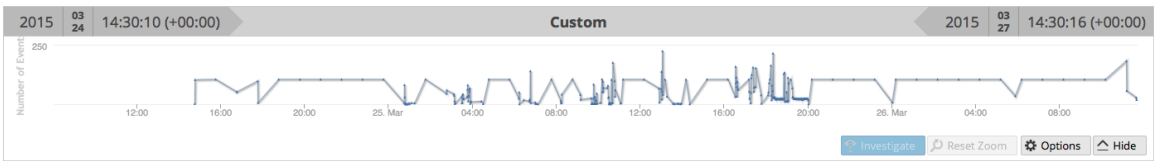
Visualizaciones

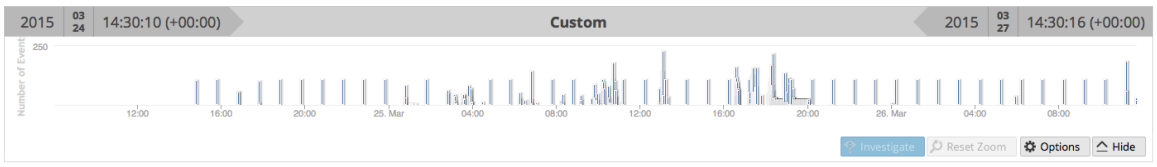
En la parte superior de la vista Navegar hay una visualización del punto de desglose actual. Puede usarla para desglosar a datos desde el panel Visualización (consulte Desglosar a datos en Gráfico de tiempo de la vista Navegar). Puede mostrar u ocultar la visualización y elegir una de las opciones de visualización: Cronograma o Coordenadas. La visualización se abre inicialmente en la última visualización guardada.

Gráfico de cronograma

El cronograma muestra actividad del servicio y el rango de tiempo especificados como un gráfico de líneas o un gráfico de barras, de acuerdo con la selección en el menú Opciones. En la segunda figura se ilustra un gráfico de líneas y en la tercera, un gráfico de barras.



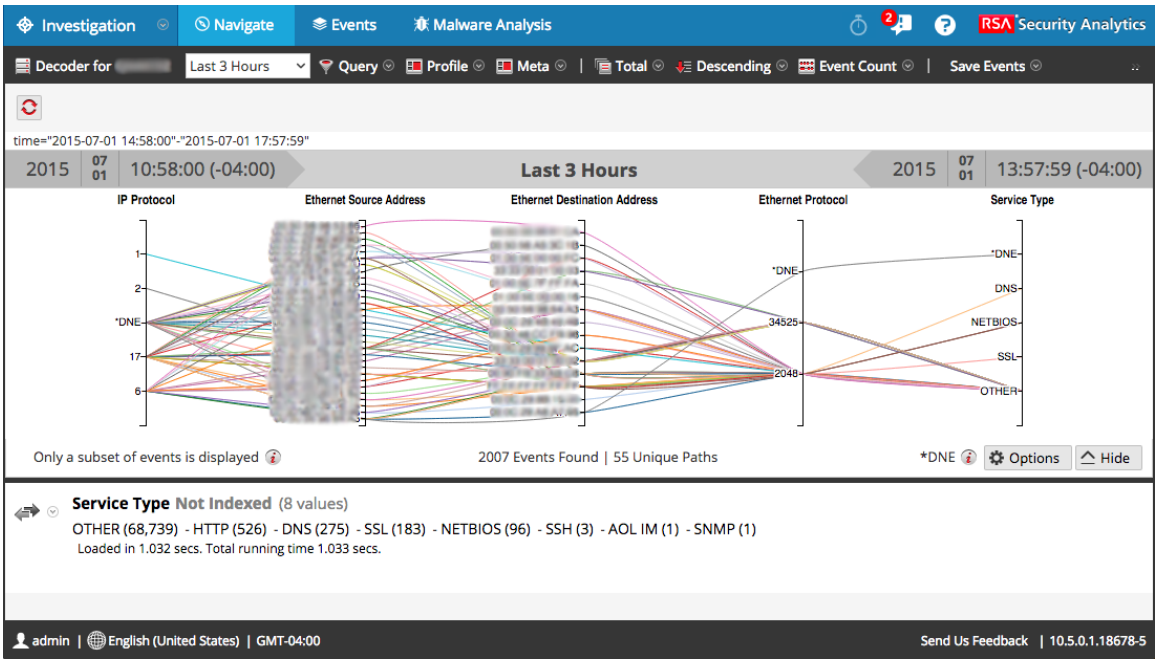




Característica	Descripción
Número de eventos (Cronograma)	El eje Y del gráfico, basado en miles de eventos.
Cronograma (Cronograma)	El eje X del gráfico, basado en la hora en que ocurrieron los eventos.
Punto de evento (Cronograma)	Si desea explorar una sección específica, seleccione simplemente el rango en el gráfico. El nuevo rango de tiempo se reflejará en el gráfico.
Investigar (Cronograma)	Muestra los valores de metadatos del subconjunto seleccionado.
Restablecer zoom (Cronograma)	Para volver al rango de tiempo original, haga clic en Restablecer zoom.
Opciones	Muestra el cuadro de diálogo Opciones de visualización. Los puntos de datos se pueden mostrar como un gráfico de líneas (predeterminado), un gráfico de barras o un gráfico de coordenadas. Cuando se selecciona un tipo de gráfico, se muestran las opciones pertinentes.
Ocultar	Contrae el gráfico.

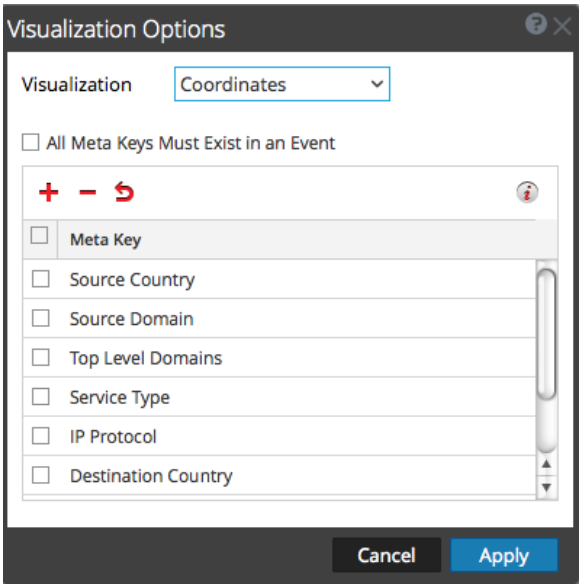
Gráfico de coordenadas paralelas

El gráfico de coordenadas paralelas es una de las alternativas del menú Opciones para visualizar el punto de desglose actual. Si se selecciona Coordenadas en el cuadro de diálogo Opciones de visualización, puede elegir los metadatos que se mostrarán (consulte Visualizar metadatos como coordenadas paralelas).



Característica	Descripción
Ejes	Cada eje es una clave de metadatos. La cantidad de claves de metadatos afecta el tiempo de carga del gráfico. Se cargan todas las claves de metadatos, pero la cantidad de eventos por clave de metadatos es limitada.
Líneas	Las líneas representan eventos y conectan valores en los ejes para mostrar la correlación entre varias claves de metadatos.
Opciones	Muestra el cuadro de diálogo Opciones de visualización. Los puntos de datos se pueden mostrar como un gráfico de líneas (predeterminado), un gráfico de barras o un gráfico de coordenadas. Cuando se selecciona un tipo de gráfico, se muestran las opciones pertinentes.
Solo se muestra un subconjunto de eventos.	Este mensaje es una notificación que indica que en el gráfico no se representan todos los eventos del panel Valores. La eliminación de ejes o el filtrado de los datos en el panel Valores pueden ayudar a mostrar todos los eventos.
Eventos encontrados | Rutas únicas	Muestra la cantidad total de eventos graficados en comparación con la cantidad de rutas únicas graficadas. La configuración de la opción Todas las claves de metadatos deben existir en un evento vuelve a generar el gráfico en una versión más dirigida y legible.
DNE	Indica que no hay valores para esta clave de metadatos en el evento.

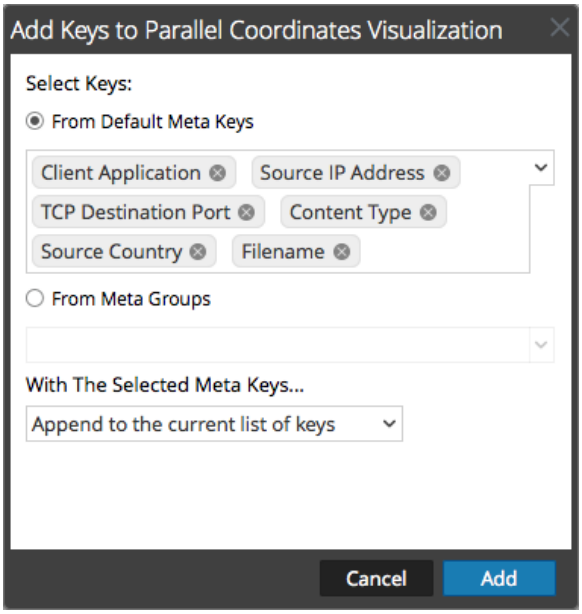
El cuadro de diálogo Opciones de visualización para Coordenadas permite seleccionar las claves de metadatos que se graficarán.



Característica	Descripción
Selección de visualización	Muestra una lista desplegable de tipos de visualización: Cronograma y Coordenadas
Todas las claves de metadatos deben existir en un evento	Limita los datos representados en la visualización solo a aquellos eventos que incluyen todas las claves de metadatos seleccionadas. Esto puede dar lugar a una visualización más clara y dirigida.
+	Muestra el cuadro de diálogo Agregar claves a visualización de coordenadas paralelas, el cual permite agregar ejes a la visualización. Esto es útil si busca relaciones entre las claves de metadatos predeterminadas y otras adicionales.
−	Elimina las claves seleccionadas de modo que no aparezcan como ejes en la visualización. Esto puede contribuir a que la visualización sea menos desordenada y permitir que incluya más puntos de datos.
	Revierte a las claves de metadatos predeterminadas para visualización, lo cual representa todas las claves de metadatos en el punto de desglose actual.
	Controla la presentación de información adicional sobre la cantidad de ejes seleccionados en comparación con el conteo recomendado. Esto contribuye a que tenga en cuenta posibles mejoras en el rendimiento debido a la eliminación de ejes.

Característica	Descripción
Ejes	Enumera las claves de metadatos seleccionadas como ejes en la visualización.
Cancelar	Cancela los cambios hechos en las opciones de visualización.
Aplicar	Guarda los cambios hechos en las opciones de visualización y los aplica a la visualización actual.

En el cuadro de diálogo Agregar claves a visualización de coordenadas paralelas, puede seleccionar las claves de metadatos o los grupos de metadatos que se usarán como ejes en la visualización de coordenadas paralelas.

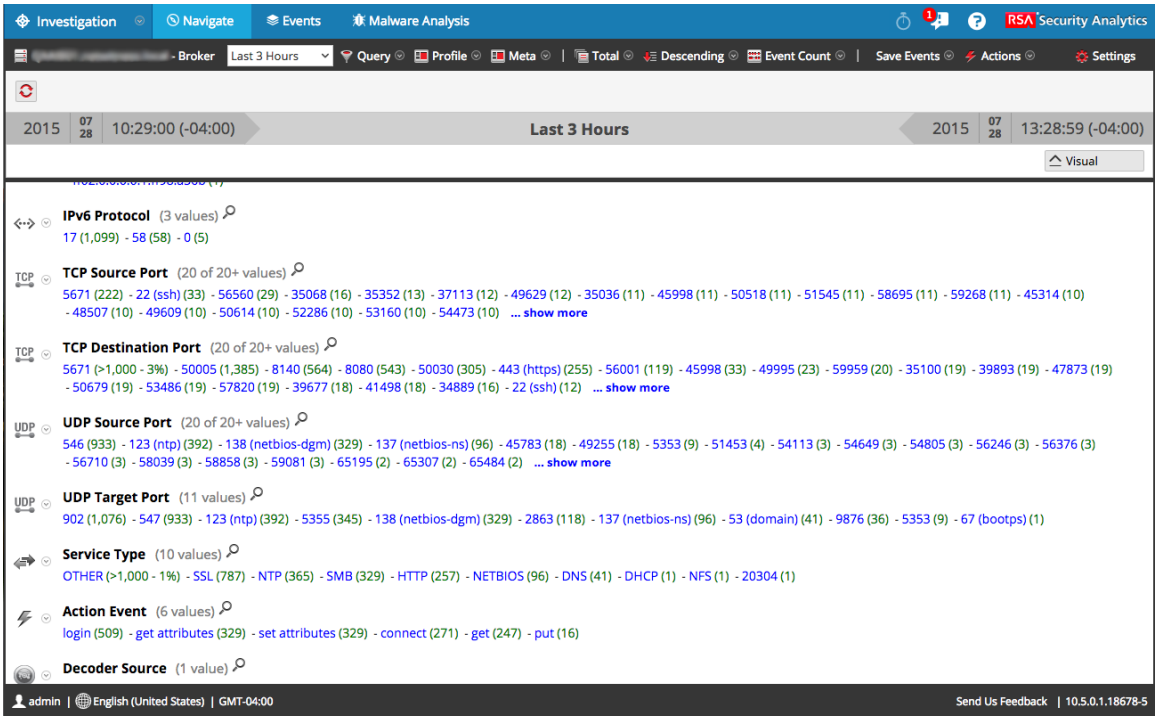


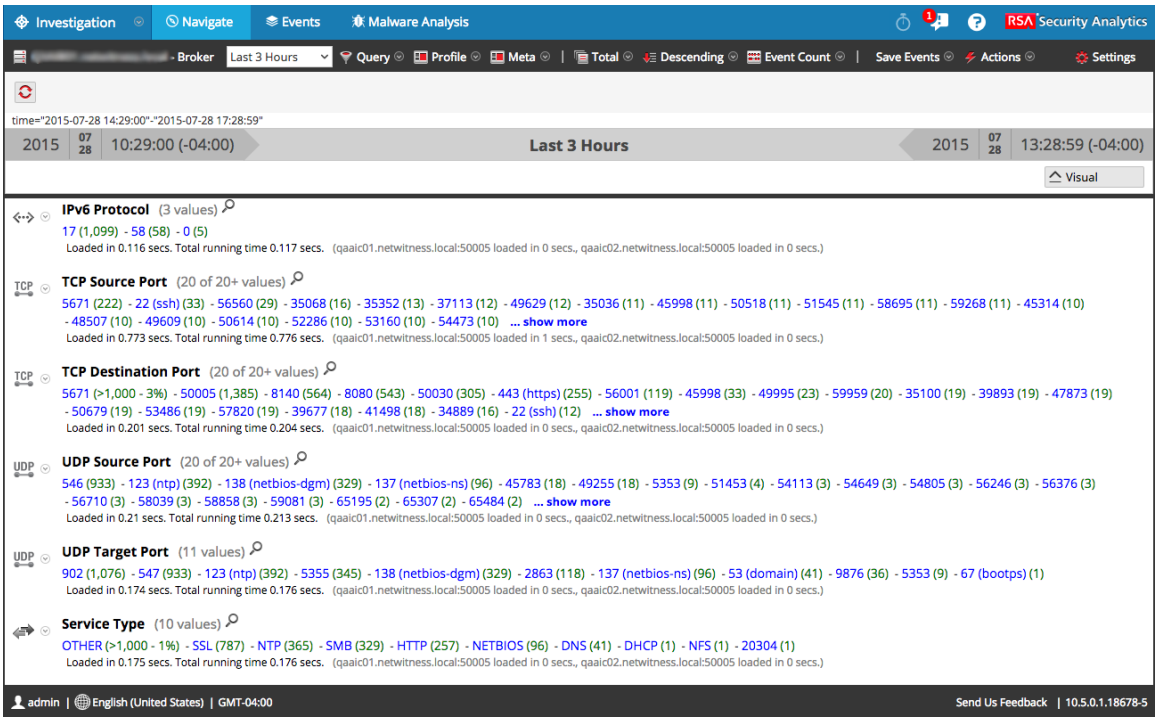
Característica	Descripción
Selección de visualización	Seleccionar claves: Las dos opciones para seleccionar claves de metadatos son: • Desde claves de metadatos predeterminadas • Desde grupos de metadatos Cada opción ofrece una lista desplegable en la cual se hace una selección.

Característica	Descripción
Con las claves de metadatos selec-cionadas…	Las opciones del método de adición de claves de metadatos permiten: • Reemplazar la lista actual de claves • Agregar a la lista actual de claves • Insertar en el comienzo de la lista actual de claves
Cancelar	Cierra el cuadro de diálogo y no agrega ninguna clave.
Agregar	Cierra el cuadro de diálogo y agrega las claves seleccionadas según lo especificado.

Panel Valores

La función principal de la vista Navegar es el panel Valores, el cual se puede usar para analizar datos (consulte Desglosar a datos en el panel Valores). En la primera figura que se muestra a continuación se ilustra el panel Valores en modo normal; en la segunda figura se ilustra la información que se agrega cuando está activo el ajuste Mostrar información de depuración.





La vista predeterminada corresponde a las últimas tres horas de recopilación, con uso de las claves de metadatos predeterminadas y las claves de metadatos no indexadas cerradas. Las claves de metadatos dentro de los grupos de metadatos se muestran en el orden en que Security Analytics las consulta. A medida que los datos se cargan en el panel Valores, Security Analytics se optimiza para mostrar resultados parciales, el progreso de la carga y el estado de los servicios durante la carga de datos.

El comportamiento de la carga lo determinan varios ajustes de configuración. Los ajustes de nivel más alto los configura el administrador para cada usuario. Son los siguientes:

- La cantidad máxima de tiempo que se permite ejecutar una consulta a este usuario (Tiempo de espera agotado de consulta).
- El límite en el cual Security Analytics deja de contar la cantidad de valores de metadatos en una sesión (Umbral de sesión). Si se establece un umbral para una sesión, la vista Navegación muestra que el umbral se alcanzó y el porcentaje del tiempo de consulta utilizado para alcanzarlo.

Nota: los valores de las claves de metadatos no indexadas tardan más en cargarse en el panel Valores. Para optimizar la carga, Security Analytics no abre las claves de metadatos no indexadas de manera predeterminada. Consulte Administrar y aplicar claves de metadatos predeterminadas en una investigación para obtener una descripción detallada de las claves de metadatos no indexadas en Investigation.

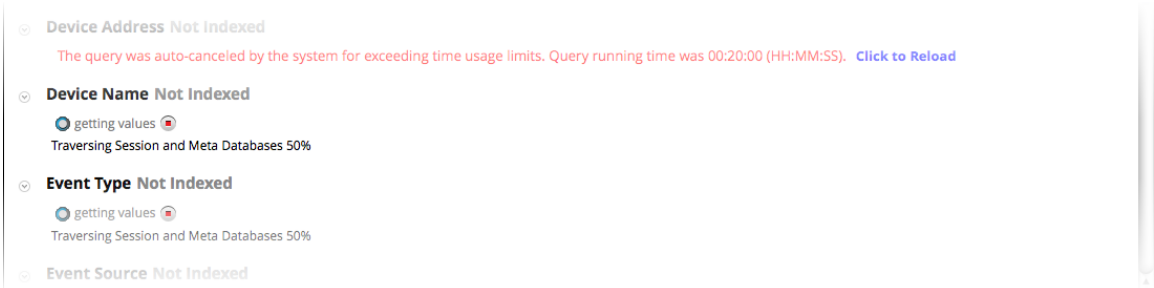
Cuando ha iniciado la investigación de un servicio, Security Analytics muestra los resultados en el panel Valores.

1. Security Analytics carga claves de metadatos y valores de metadatos en el panel Valores. Para cada carga de clave de metadatos, las etapas de carga son:
   a. **En espera de carga** o **Cerrado**. En el caso de Cerrado, no se cargan datos para esa clave.
   b. **Cargando**
      i. **Progreso de carga**: Security Analytics recibe y muestra mensajes de progreso.
      ii. **Resultados parciales**: Security Analytics recibe mensajes de valores y se muestran resultados parciales en el panel Valores.
   c. **Carga finalizada**: terminó la carga de todos los resultados.
2. A medida que termina la carga de cada clave de metadatos y que se muestran los valores finales, se inicia la clave de metadatos siguiente. El valor Procesos de generación en la configuración Preferencias de Investigation especifica la cantidad o los valores que se generan para cada clave de metadatos. La carga continúa hasta que finalizan todas las claves que se cargarán.
3. Si la opción **Mostrar información de depuración** está activa y el servicio en el cual está navegando es un Broker 10.4 o superior, Security Analytics muestra la información del tiempo de carga debajo de los valores para cada clave de metadatos y muestra detalles de carga adicionales para los servicios agregados. Security Analytics también muestra la información de depuración debajo de la ruta de navegación.

Resultados iterativos

Los resultados iterativos proporcionan retroalimentación sobre el estado de consultas dentro de las interfaces para ofrecer contexto adicional en cuanto a la duración de la carga de datos y si faltan datos de servicios. Por ejemplo, si está consultando un Broker que realiza la agregación desde dos Concentrators, Security Analytics comienza a mostrar los resultados del primer Concentrator tan pronto están disponibles, incluso si el segundo Concentrator continúa en espera de resultados.

Los resultados iterativos también incluyen una notificación que informa que faltan datos del servicio porque no está accesible.

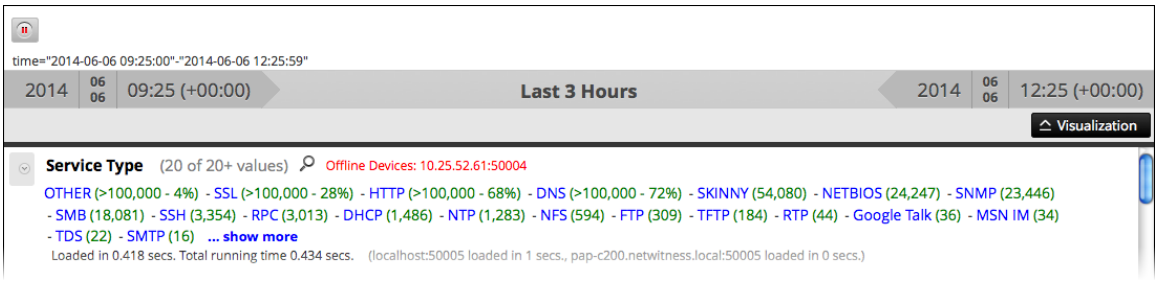


Resultados parciales

Cuando se devuelven valores parciales del servicio Principal, sin que haya finalizado, un mensaje al final de la lista de claves de metadatos muestra el progreso de los valores cargados. En el siguiente ejemplo, Currently looking at 38 ip.src values 71% indica que la carga de valores para la clave de metadatos lleva un 71 %.

Información de depuración

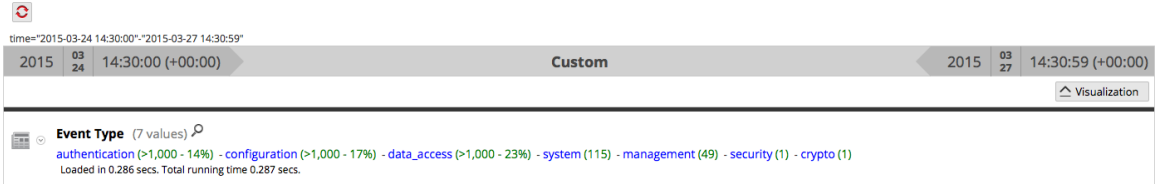
Si el ajuste Mostrar información de depuración está activo, un campo al final de los valores muestra el estado de los diversos sistemas contra los cuales realiza la consulta dentro de Security Analytics. Por ejemplo, cuando realiza una consulta contra un Broker 10.4 que extrae datos de múltiples Concentrators, Security Analytics muestra el estado de la consulta en cada uno de los Concentrators, lo cual proporciona información sobre la velocidad relativa de carga de datos desde cada Concentrator. Cada servicio que participó en la consulta se muestra con el tiempo total transcurrido para la consulta.



Cada servicio que participó en la consulta se muestra con el tiempo total transcurrido para la consulta. En el ejemplo anterior, dos servicios devolvieron resultados en 3.207 segundos; localhost:50005 tardó dos segundos en devolver los resultados. Además, la cláusula Where de la consulta se muestra debajo de la ruta de navegación. Puede copiar esta sintaxis directamente en una regla de aplicación o en la cláusula Where de Informes de una regla.

Carga finalizada

Este es un ejemplo de valores que terminaron de cargarse.



Para cada clave de metadatos, hay una lista de valores (texto azul) y conteos (texto verde) en el punto de desglose actual. Cuando hace clic en un valor para desglosar a un subconjunto de los datos seleccionados actualmente, la pantalla se actualiza y el nuevo punto de desglose se registra en la ruta de navegación. Puede especificar los métodos de clasificación y cuantificación de la lista de valores mediante la opción de la barra de herramientas.

Nota: el título, los valores y los conteos de claves de metadatos no indexadas no se pueden desglosar; los valores y los conteos se muestran en negro. Consulte Administrar y aplicar claves de metadatos predeterminadas en una investigación para obtener una descripción detallada de las claves de metadatos no indexadas en Investigation.

Característica	Descripción
Clave de metadatos	El nombre de los metadatos que se enumeran; por ejemplo, **Tipo de servicio** es una clave de metadatos.
Cantidad de valores generados frente a cantidad de valores disponibles para cargar	El valor Procesos de generación en la configuración Preferencias de Investigation especifica la cantidad o los valores que se generan. En el ejemplo anterior, la clave de metadatos es **Tipo de servicio** y se muestran 20 de más de 20 valores. Puede mostrar valores adicionales si hace clic en **...mostrar más**.

Característica	Descripción
	Si hace clic en  en una clave de metadatos indexada, se abre el cuadro de diálogo Buscar, en el cual puede ingresar un filtro para la clave de metadatos actual. La función de búsqueda no está disponible para claves de metadatos no indexadas y se basa en el valor de metadatos real, no en el alias. El desglose mediante alias en el cuadro de diálogo Buscar no es compatible. NOTA: consulte al administrador para obtener una lista de los alias que se usan para una clave de metadatos en Investigation. Cuando se usa un alias, este cuadro de diálogo de búsqueda no proporciona resultados. En lugar de esto, debe consultar la clave de metadatos mediante la funcionalidad de consulta de clic con el botón secundario o el cuadro de diálogo Consulta. 
Servicios offline: xxx.-xxx.xxx.xxx:50004	Enumera los servicios offline que consulta un Broker 10.4.
Conteo de metadatos, por ejemplo 	La cantidad de instancias que se encuentran para un metadato específico en la sesión.
Valor de metadatos, por ejemplo 	El nombre específico asociado con los metadatos encontrados.
...mostrar más	Si se limitó la cantidad de valores de metadatos (por ejemplo, 20) y se hace clic en esta opción, se muestran valores de metadatos adicionales para la clave de metadatos seleccionada.

Característica	Descripción
Se cargó en 0.418 s Tiempo de ejecución total 0.434 s (localhost:50005 se cargó en 1 s…	Las estadísticas de depuración muestran los tiempos de carga de acuerdo con la configuración Mostrar información de depuración.

Menús contextuales de claves de metadatos

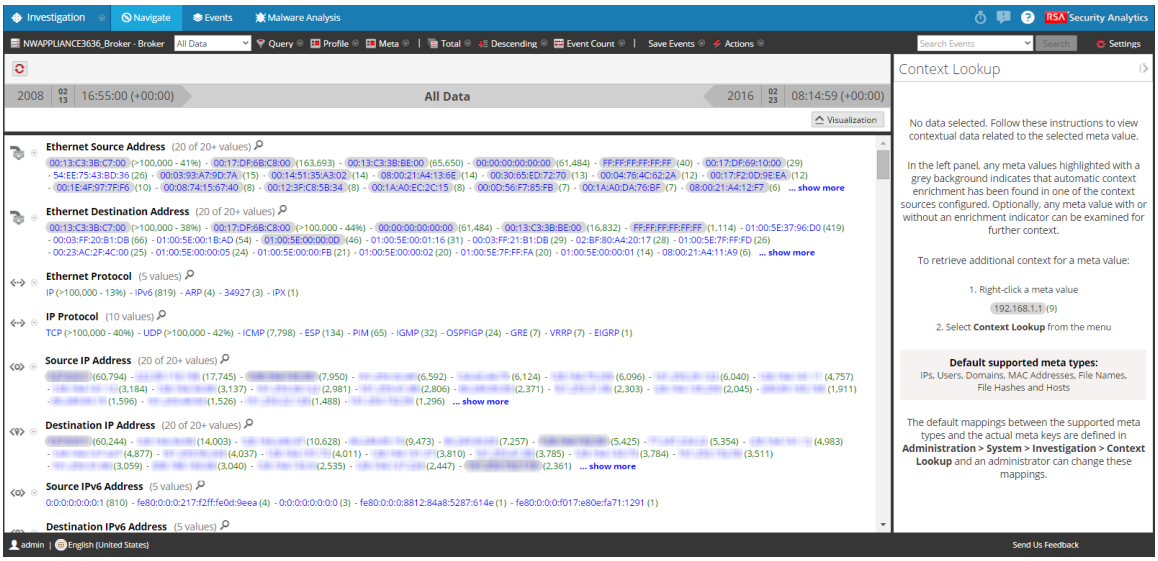
Las claves de metadatos en el panel Valores tienen menús contextuales. Al lado de cada etiqueta de metadatos, una flecha desplegable muestra las opciones que se pueden aplicar a ese elemento. Puede usar esto para cambiar la manera en que se muestran los resultados de la clave de metadatos en la vista actual. Los cambios que se hacen en las claves de metadatos se muestran en la vista actual durante los puntos de desglose y persisten hasta que se actualiza la página o se selecciona un nuevo servicio en la barra de herramientas de la vista Navegar. UnaAdministrar y aplicar claves de metadatos predeterminadas en una investigación actualización revierte la vista actual de claves de metadatos según lo definido en el cuadro de diálogo Administrar claves de metadatos predeterminadas (consulte Administrar y aplicar claves de metadatos predeterminadas en una investigación). Si nunca ha hecho modificaciones en el cuadro de diálogo Administrar claves de metadatos predeterminadas, Security Analytics restaura las claves de metadatos predeterminadas desde el servicio Core.

- Más resultados
- Resultados máximos
- Ocultar resultados
- Información de clave de metadatos

Panel Búsqueda de contexto

Con la adición de un nuevo servicio Context Hub, la vista Navegar tiene un panel en el lado derecho denominado panel Búsqueda de contexto. El panel Búsqueda de contexto es visible solo si ha instalado el servicio Context Hub, el cual debe estar configurado. Para obtener más información sobre cómo configurar el servicio Context Hub, consulte la *Guía de configuración de Context Hub*.

En el panel Búsqueda de contexto se muestran los datos pertinentes cuando un analista busca datos contextuales para un valor de metadatos en el panel Valores.

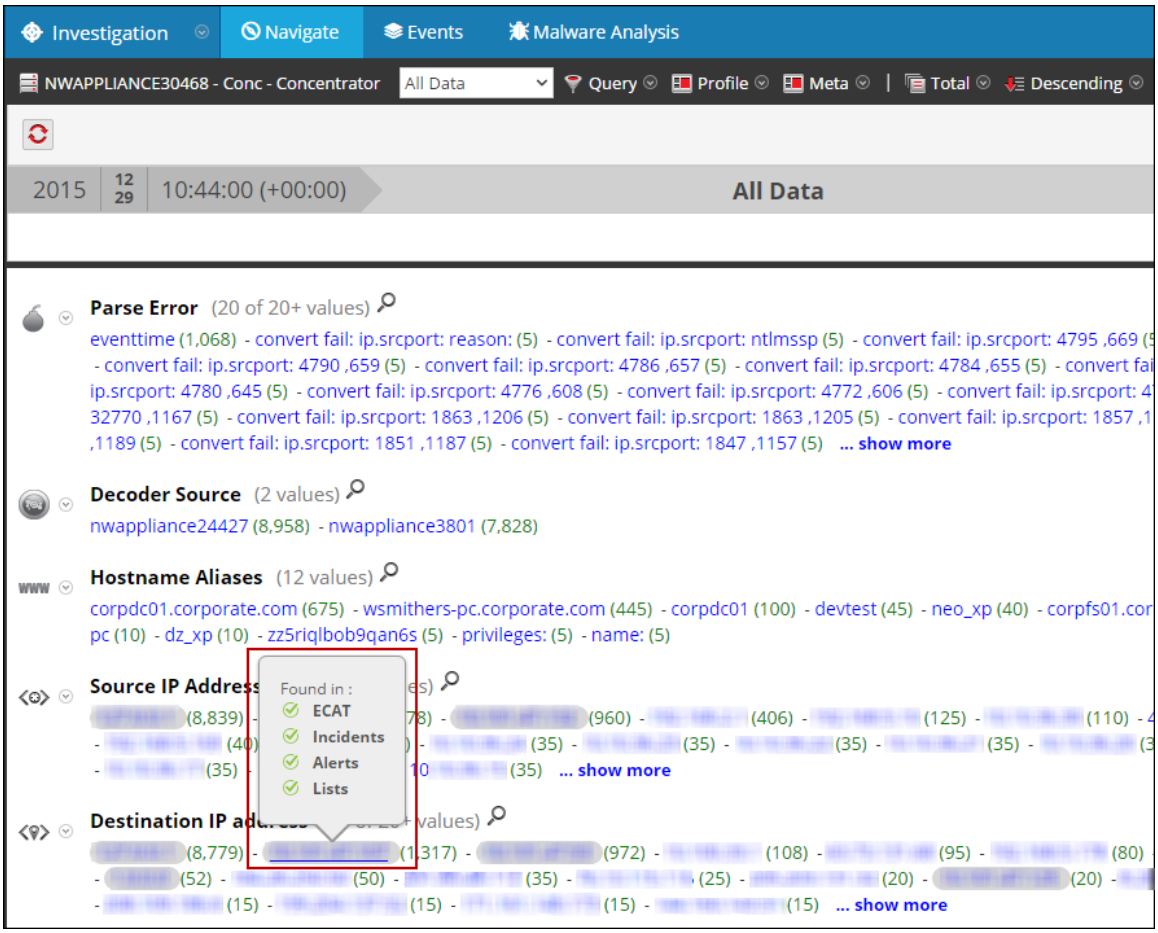


Después de que el administrador configura el servicio Context Hub, puede ver la información contextual para los valores de metadatos en la vista Navegar y en la vista Eventos. Para obtener más información sobre cómo configurar el servicio Context Hub, consulte la *Guía de configuración de Context Hub*.

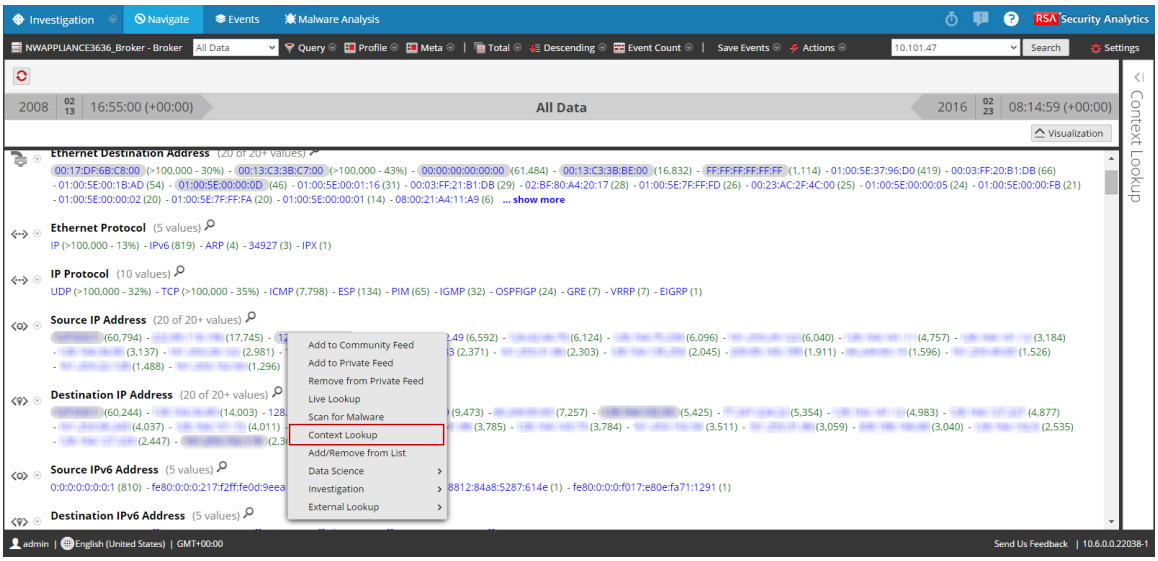
Para obtener información acerca de cómo realizar la búsqueda de contexto de valores de metadatos, consulte Ver el contexto adicional de un punto de datos.

El servicio Context Hub está preconfigurado con un mapeo predeterminado de tipos de metadatos y claves de metadatos. Para obtener información sobre el mapeo del valor de metadatos de Context Hub con clave de metadatos de Investigation, consulte “Administrar el mapeo de tipos de metadatos y claves de metadatos” en la *Guía de configuración de Context Hub*.

Puede ver el tipo de datos de contexto que está disponible para un valor de metadatos resaltado si mantiene el mouse sobre un valor de metadatos resaltado. Un indicador de en línea muestra qué tipo de datos de contexto están disponibles para los metadatos: ECAT, incidentes, alertas o listas.



Cuando se hace clic con el botón secundario en un valor de metadatos, se abre un menú con la opción de búsqueda de contexto. En la siguiente figura se muestra la opción Búsqueda de contexto cuando hace clic con el botón secundario en un valor de metadatos.



Para obtener más información sobre los resultados de búsqueda y la información contextual de distintos orígenes de datos, consulte Investigation: Panel Búsqueda de contexto.

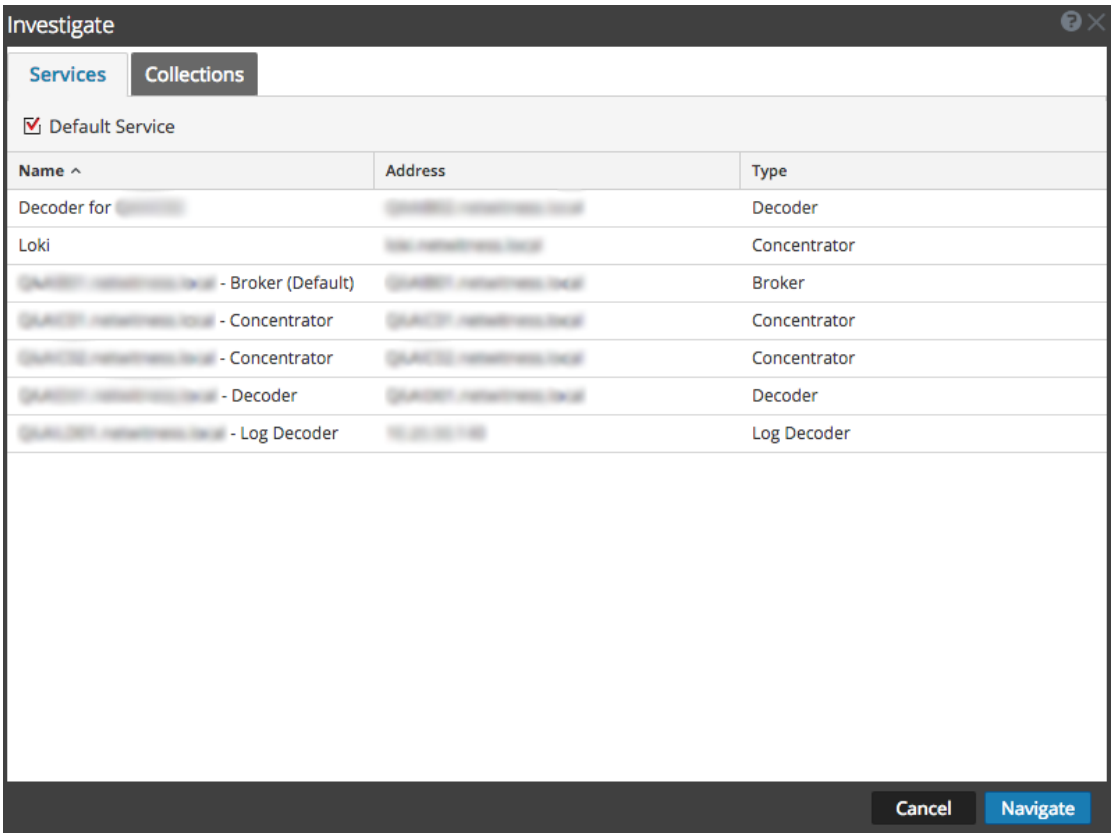
Investigation: Cuadro de diálogo Consulta

En Investigation > vista Navegar o vista Eventos, puede crear una consulta en lugar de hacer clic en las claves y los valores de metadatos para desglosar a los metadatos. Los cuadros de diálogo para la creación de una consulta ofrecen ayuda de sintaxis con listas desplegables de las claves y los operadores de metadatos aplicables. Los procedimientos relacionados están disponibles en Consultar datos en la vista Navegar.

Para acceder a este cuadro de diálogo:

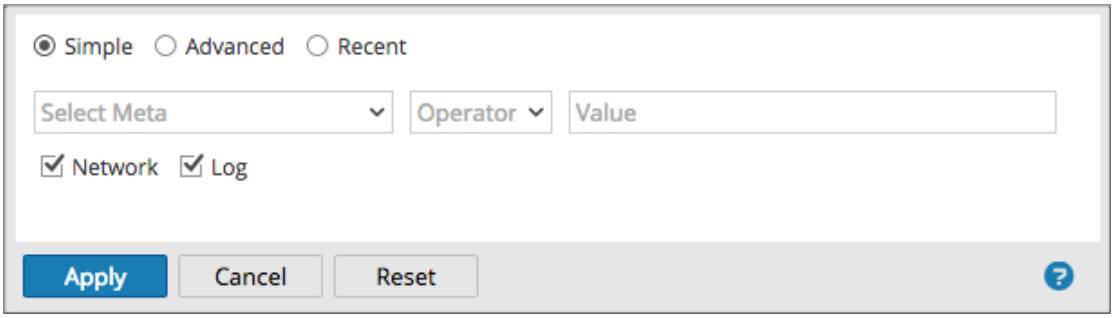
1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Eventos**. Ambas vistas proporcionan acceso al cuadro de diálogo Consulta.

   Se muestra el cuadro de diálogo Investigar.



2. Seleccione un servicio y haga clic en **Navegar**.
3. En la barra de herramientas, seleccione **Consulta**.

   Se mostrará el cuadro de diálogo Consulta.



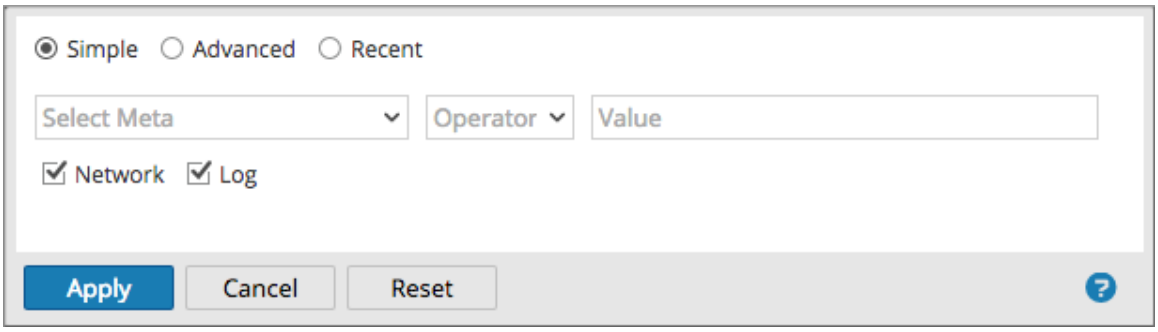
Características

El cuadro de diálogo Consulta tiene tres vistas:

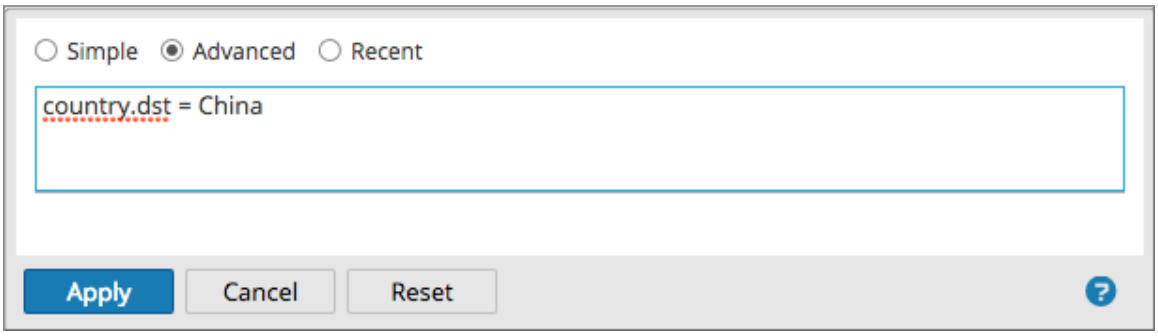
- Simple
- Avanzado
- Recientes

En la vista Simple, puede crear una consulta a partir de las opciones que se muestran en el cuadro de diálogo. En la vista Opciones avanzadas, puede crear una consulta sin orientación. En la vista Reciente, puede seleccionar una consulta en una lista desplegable de consultas recientes.

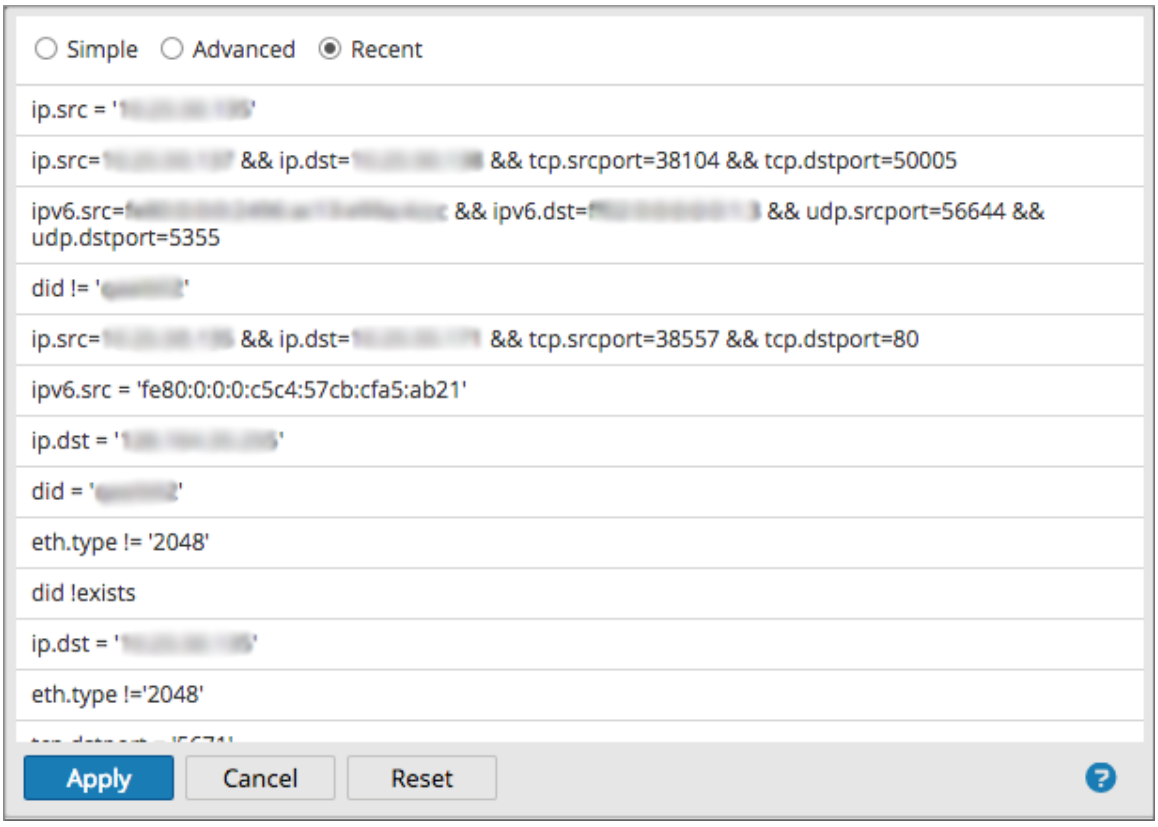
Vista Simple



Vista Opciones avanzadas



Vista Reciente



En la siguiente tabla se describe el cuadro de diálogo Consulta.

Característica	Descripción
Seleccionar meta-datos	Muestra una lista desplegable de grupos de metadatos.

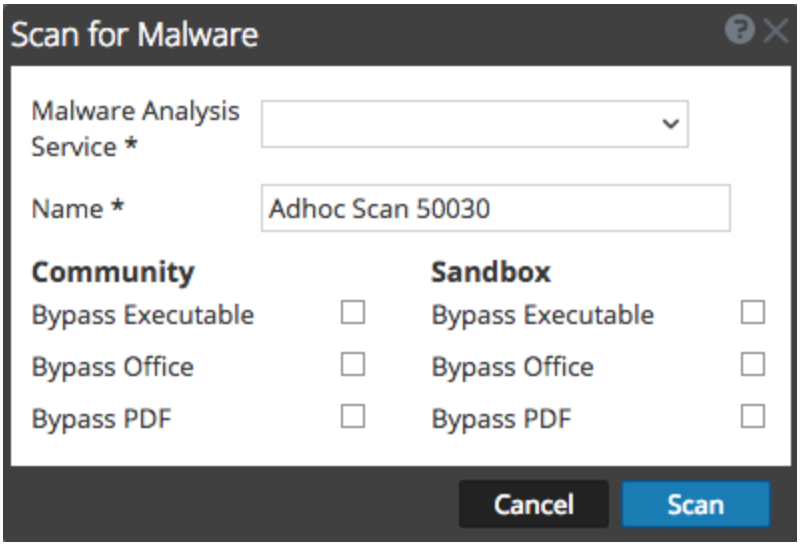
Característica	Descripción
Operador	Muestra una lista desplegable de operadores `(=, !=, exists, !exists)`
Valor	Permite ingresar un valor para completar la consulta.
Red	Limita la consulta a paquetes si no se selecciona la opción Registro.
Log	Limita la consulta a registros si no se selecciona la opción Red.
Cuadro Consulta	Permite ingresar una consulta en la vista Opciones avanzadas. Cuando comienza a escribir, se muestra una lista desplegable de claves de metadatos disponibles para el servicio y, a medida que escribe, se muestra una lista desplegable de operadores. Si la expresión ingresada actualmente en el cuadro Consulta no es válida, aparece una advertencia junto al cuadro. Cuando la consulta es válida, la advertencia se elimina.
Lista Consulta	Permite seleccionar una consulta en una lista de consultas recientes de la vista Reciente. Si se hace doble clic en una consulta, esta se aplica automáticamente.
Aplicar	Aplica la nueva consulta a la vista actual de Investigation.
Cancelar	Cierra el cuadro de diálogo sin aplicar cambios.
Restablecer	Restablece todos los campos.

Investigation: Cuadro de diálogo Escanear para encontrar malware

En el cuadro de diálogo Escanear para encontrar malware, los analistas de Malware Analysis pueden cargar archivos para investigar en Malware Analysis.

Para acceder a este cuadro de diálogo:

1. En el menú de **Security Analytics**, seleccione **Investigation > Malware Analysis**.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis.
2. Seleccione un servicio en el panel de la izquierda y haga clic en Scan Files en el panel de la derecha.
   Se muestra el cuadro de diálogo Escanear para encontrar malware.



Los procedimientos relacionados están disponibles en Realizar un análisis de malware.

Características

En la siguiente tabla se describen las funciones disponibles en el cuadro de diálogo Escanear para encontrar malware.

Característica	Descripción
+	Carga un archivo desde la computadora.
−	Elimina un archivo de la lista.

Característica	Descripción
Nombre de archivo	Muestra los nombres de los archivos agregados a la lista.
Nombre	Permite asignar un nombre al trabajo de escaneo.
Comunidad	Muestra opciones de Comunidad con el fin de saltar u omitir ciertos tipos de archivos: • Omitir archivo ejecutable • Omitir Office • Omitir PDF
Sandbox	Muestra opciones de Sandbox con el fin de saltar u omitir ciertos tipos de archivos: • Omitir archivo ejecutable • Omitir Office • Omitir PDF
Cancelar	Cierra el cuadro de diálogo sin realizar ninguna acción.
Analizar	Escanea los archivos cargados.

Investigation: Opciones de búsqueda

Puede buscar eventos en la vista Navegar y en la vista Eventos de Investigation. En la vista Navegar, puede hacer clic en un valor de metadatos, como HTTP, para desglosar a los datos y, a continuación, ingresar una cadena de búsqueda en el campo Buscar para buscar eventos en ese subconjunto de datos. La búsqueda abre una pestaña en la vista Eventos, presenta el desglose y el rango de tiempo hacia delante y muestra los resultados de búsqueda. También puede desglosar a los datos mediante consultas antes de iniciar una búsqueda.

Los procedimientos relacionados con la búsqueda en las vistas de Investigation se describen en Configurar la vista Navegar y la vista Eventos, Filtrar y buscar resultados en la vista Eventosy Desglosar a datos en el panel Valores.

Las vistas Navegar y Eventos de Investigation le permiten buscar patrones de texto en el conjunto actual de eventos. Puede ejecutar una búsqueda de texto por palabra clave o una coincidencia de regex (expresión regular).

Búsqueda por palabra clave

La búsqueda de texto proporciona estas funcionalidades:

- A cada palabra delimitada por un espacio en blanco se le agrega Y para que se encuentren todas las palabras, pero el orden o la ubicación con relación a las otras palabras es irrelevante. Por ejemplo, si busca `Mark Albert`, tanto Mark como Albert se deben encontrar en la sesión, pero no es necesario que estén juntas o en un orden específico.
- La palabra O es especial. Si busca `Mark OR Albert`, se debe encontrar Mark o Albert como coincidencia en la sesión, pero no se requieren ambos.
- Puede combinar o hacer coincidir Y y O implícitos juntos en la cadena de búsqueda. Un O explícito tiene mayor prioridad que Y implícito (espacio en blanco). En los siguientes ejemplos se hace la misma declaración lógica, que requiere que los términos queso y albóndigas estén presentes en una coincidencia, además de tostada o pan:

  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```

- Puede excluir palabras de los resultados de la búsqueda con el operador `-`. Por ejemplo, la búsqueda de `cheese -toast` arrojará cualquier resultado que tenga la palabra queso, a menos que la palabra tostada también esté presente.
- La búsqueda por palabra clave puede coincidir con los metadatos almacenados en los siguientes patrones:

- **Direcciones IPv4 e IPv6**. Cualquier término que se puedan reconocer como una dirección IP se convertirán al formato nativo de metadatos, de modo que puede encontrarse en los metadatos indexados.
- **Rangos de IPv4 CIDR**. Puede usar la notación CIDR para localizar las direcciones IPv4 dentro de un rango.
- **Registros de fecha y hora**. Los registros de fecha y hora se comparan con los metadatos de tiempo nativo y cualquier campo de metadatos de tiempo adicional se almacena con el tipo de tiempo.
- **Números**. La función de búsqueda intentará automáticamente identificar los términos de búsqueda decimal y hacerlos coincidir con campos numéricos de datos de metadatos.

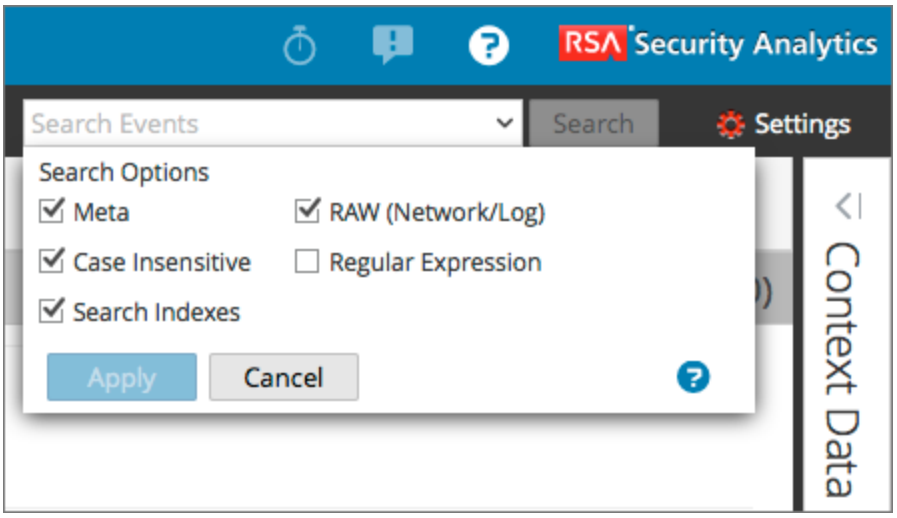
Opciones para controlar el comportamiento de la búsqueda

Para acceder al cuadro de búsqueda y a las opciones de búsqueda en las vistas Navegar o Eventos:

1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Eventos**.
2. En el cuadro de diálogo Investigar, seleccione un servicio y haga clic en **Navegar**.
   Puede ver el campo Buscar eventos en la barra de herramientas.

   Solución de problemas: Si no puede ver el campo Buscar eventos en la barra de herramientas, haga clic en  a la derecha de la barra de herramientas.
3. Haga clic en el campo Buscar para ver el menú desplegable Buscar eventos.

Las opciones seleccionadas en este cuadro cambiarán la forma en que se ejecuta la búsqueda. El modo de búsqueda predeterminado es usar los índices de búsqueda de palabras clave en metadatos y datos crudos.

En la siguiente tabla se describen las opciones de búsqueda de Investigation.

Característica	Descripción
Índices de búsqueda	En primer lugar, busca en los índices antes de escanear los metadatos o los datos crudos. Buscar en el índice es la manera más rápida de buscar palabras clave en un conjunto de datos de gran tamaño. La búsqueda de índice utiliza cualquier índice pertinente presente en la recopilación de datos. **Precaución:** - La búsqueda de índice solamente arroja resultados de los datos indexados. - Las búsquedas de índice no encontrarán coincidencias de subcadena. Si necesita coincidencias de subcadena, desactive esta casilla de verificación y utilice un modo de búsqueda sin índice.
Metadatos	Busca los metadatos. Su patrón de palabra clave o regex se comparará con los metadatos analizados.
RAW (red/-registro)	Busca el texto del registro. Cada evento se decodifica y se busca en el contenido coincidencias con el patrón de palabra clave o regex. Si selecciona todos los datos sin filtros en un Archiver, el tiempo de ejecución puede ser excesivo y se puede mostrar una advertencia. **Precaución:** La búsqueda cruda de sesiones de red hace que las sesiones se decodifiquen, lo cual requiere mucho tiempo. Es posible que desee deshabilitar las búsquedas crudas cuando busca recopilaciones solo de red.
No distingue mayúsculas de minúsculas	Omite mayúsculas y minúsculas en la búsqueda.

Característica	Descripción
Expresión regular	Realiza las búsquedas mediante una expresión regular de Perl, en lugar de texto. De forma predeterminada, Security Analytics ejecuta una búsqueda de texto. Para ejecutar una búsqueda de expresión regular, seleccione la opción Expresión regular. **Precaución:** - Las búsquedas de expresión regular pueden ser muy lentas. - Al combinar las expresiones regulares y las opciones de índice de búsqueda, el patrón de expresión regular se compara con valores de índice únicos en lugar de valores de metadatos. Esto genera resultados con mayor rapidez, pero no es una búsqueda exhaustiva de todos los metadatos o datos crudos.
Aplicar	Configura las opciones de búsqueda predeterminadas que se aplicarán a una búsqueda en la vista Navegar y en la vista Eventos. Esto también actualiza las preferencias de Investigation en su perfil (Perfil > Preferencias > pestaña Investigation). Las preferencias se guardan y se aplican de inmediato. Puede seleccionar opciones de búsqueda para una determinada búsqueda sin cambiar las preferencias de búsqueda predeterminadas.

Sintaxis de búsqueda de expresiones regulares

La búsqueda de una expresión regular utiliza sintaxis de expresión regular de Perl, que se documenta detalladamente en http://perldoc.perl.org/perlre.html.

Búsqueda de palabras clave de texto crudo (nuevo en la versión 10.6)

El Log Decoder tiene la capacidad de crear un índice de texto crudo para eventos de registro sin analizar. Esta funcionalidad crea elementos de metadatos que forman una indexación de texto completo en los servicios descendentes como Concentrators y Archivers. Cuando se habilita la opción de índices de búsqueda en las preferencias de búsqueda, la búsqueda utiliza automáticamente el índice de texto. Tenga en cuenta que el índice de texto genera elementos de metadatos que tienen una granularidad gruesa. Por ejemplo, la configuración predeterminada del indexador de texto trunca los términos de texto. Al comparar las coincidencias de índice con datos crudos, el motor de búsqueda encontrará resultados precisos para la búsqueda. Sin embargo, puede mejorar los tiempos de búsqueda si deshabilita la casilla de verificación de la búsqueda cruda. Si lo hace, se devolverá resultados con mayor rapidez, pero es posible que vea falsos positivos en los resultados de la búsqueda.

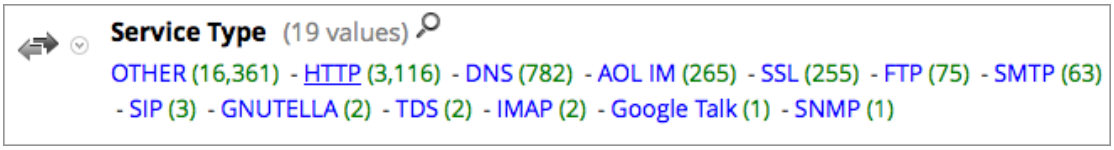
Ejemplos de búsqueda

Los siguientes ejemplos muestran búsquedas en las vistas Navegar y Eventos.

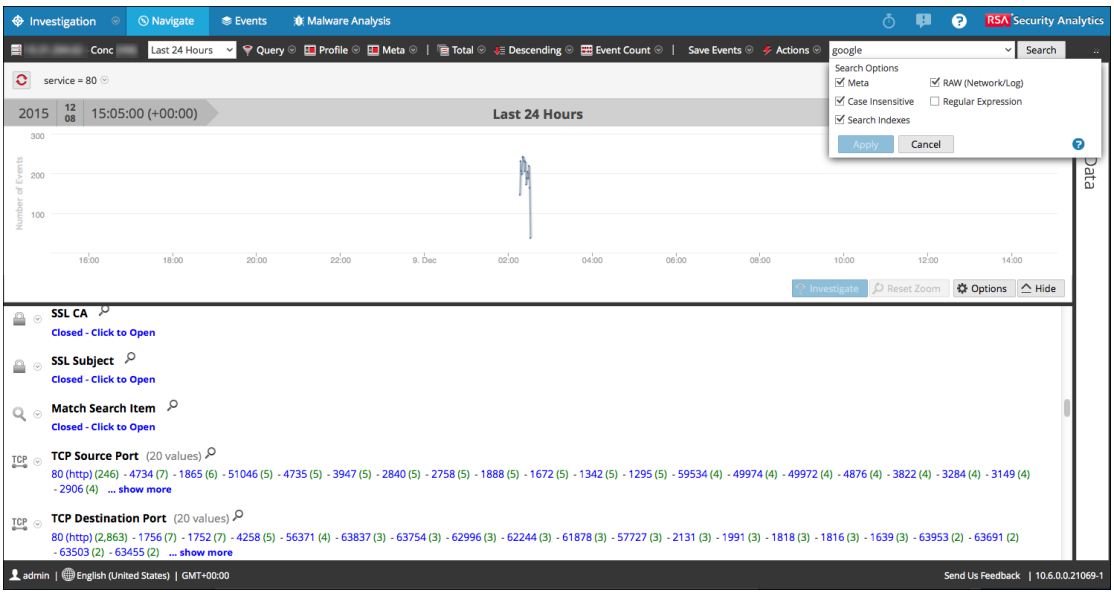
Búsqueda en la vista Navegar

Para buscar en los datos que se muestran actualmente en la vista Navegar:

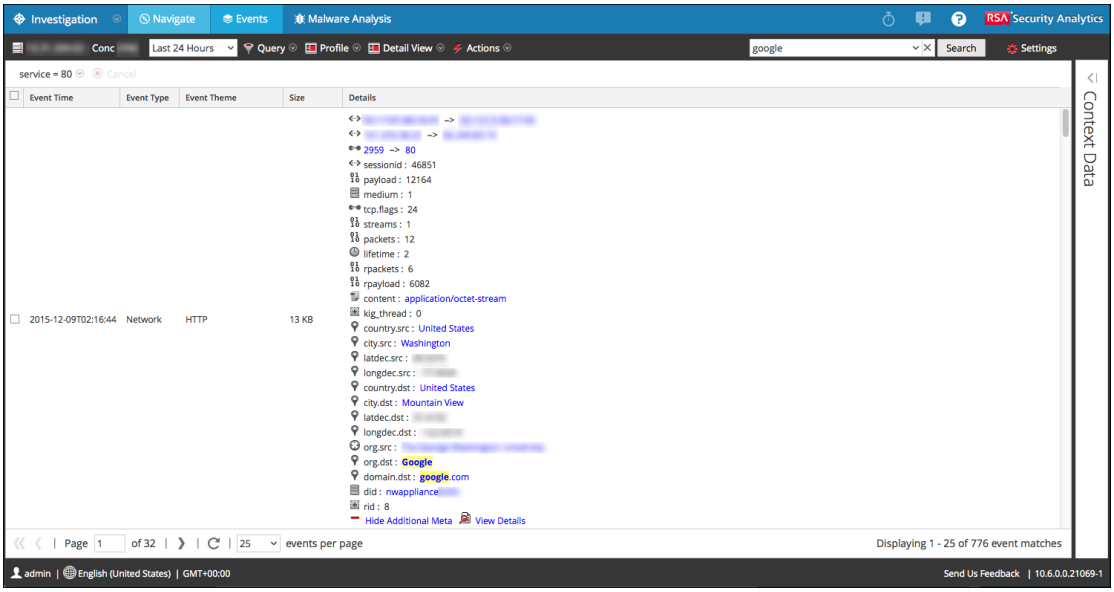
1. Para desglosar los datos, haga clic en un valor de metadatos, como HTTP, en el panel Navegar.



2. Escriba una cadena de búsqueda en el campo Buscar y presione **Intro** o haga clic en **Buscar**.



En el siguiente ejemplo se muestran los resultados de búsqueda de la cadena de búsqueda **google** en una nueva pestaña en la vista Eventos. El desglose (consulta) y el rango de tiempo en la vista Navegar se presentan en la vista Eventos (**servicio=80** y **Últimas 24 horas** en este ejemplo).



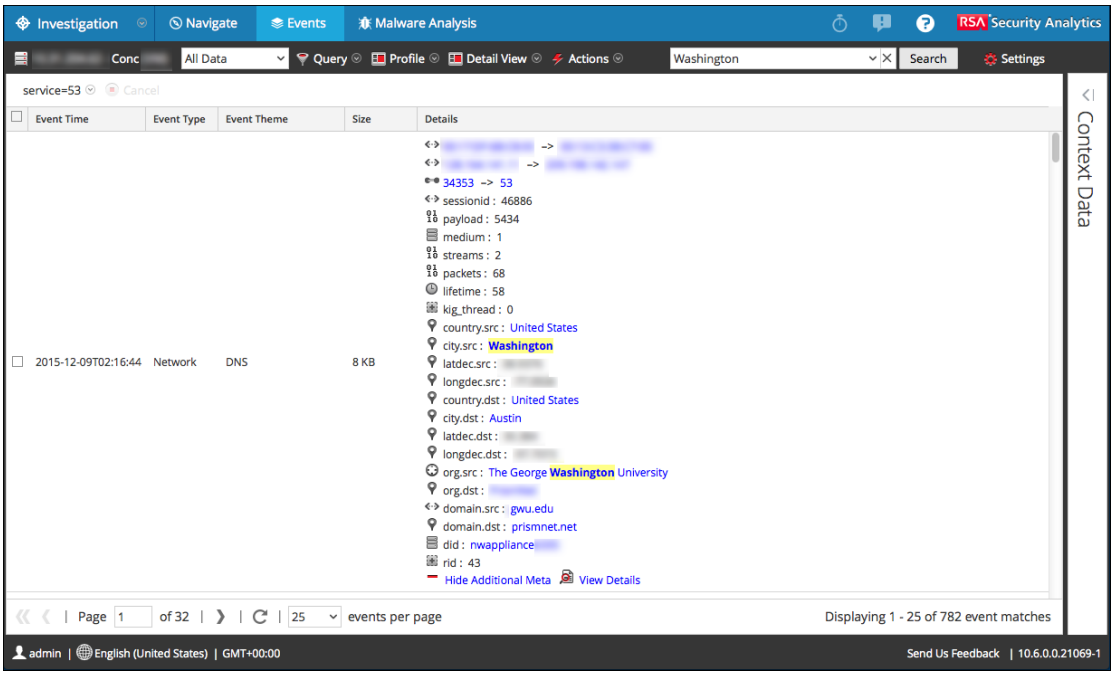
3. Para borrar el cuadro de búsqueda y volver a la vista Eventos normal, haga clic en **X** en el cuadro de búsqueda.

Buscar en la vista Eventos

Para buscar en los datos que se muestran actualmente en la vista Eventos:

1. Escriba una cadena de búsqueda en el cuadro Buscar y presione **Intro** o haga clic en **Buscar**.

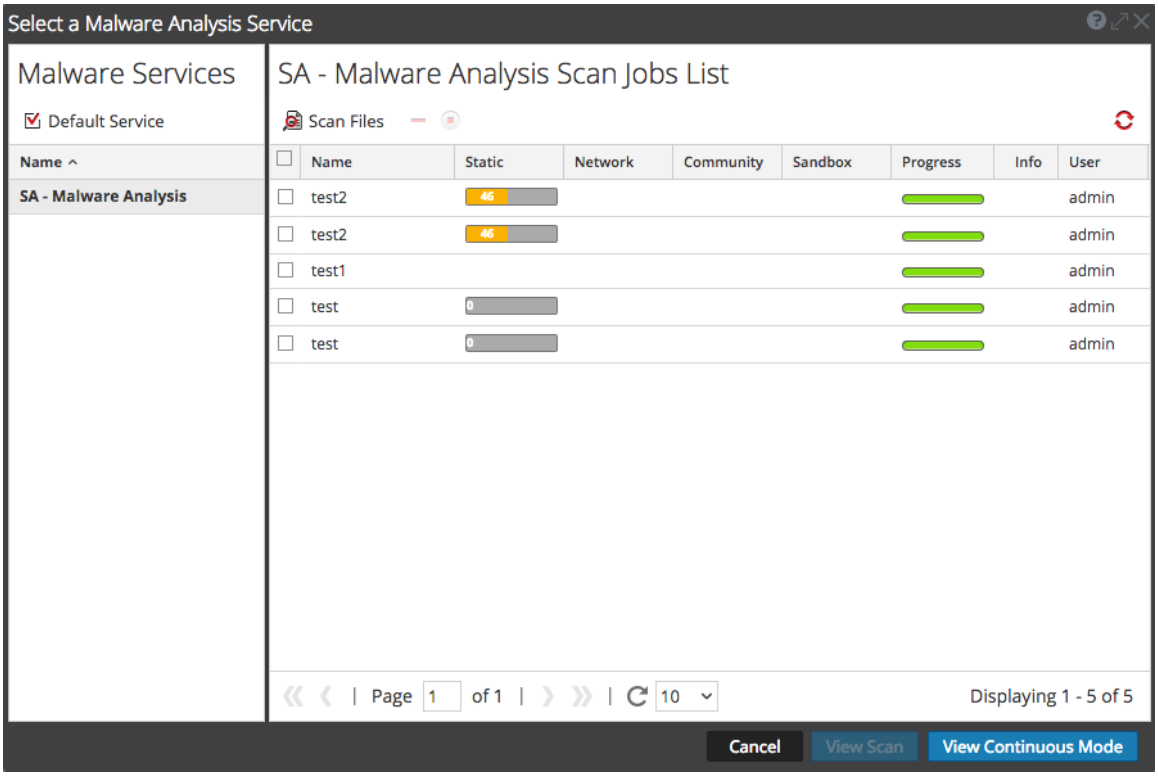
   Los resultados de búsqueda se muestran en la vista Eventos. Los eventos que coinciden con los criterios de búsqueda se muestran en la cuadrícula de la vista Eventos. En la vista Detalles y en la vista Lista, las coincidencias se resaltan en la columna Detalles. Además, cuando busca RAW, las coincidencias se resaltan en el columna Registros de la vista Registro. A continuación se muestra un ejemplo de los resultados de búsqueda del término **Washington** en la vista Detalles de eventos. Observe que las coincidencias de la búsqueda no se resaltan en ninguna reconstrucción de evento.



2. Si desea limitar la búsqueda, cambie la consulta y la hora.
3. Si desea detener la búsqueda y volver a la vista Eventos, haga clic en **Cancelar**.
   Se conserva cualquier resultado que se muestre.
4. Para borrar el cuadro de búsqueda y volver a la vista Eventos normal, haga clic en **X** en el cuadro de búsqueda.

Investigation: Cuadro de diálogo Seleccionar un servicio Malware Analysis

Se puede acceder al cuadro de diálogo Seleccionar un servicio Malware Analysis en la vista Malware Analysis. En este cuadro de diálogo, los analistas de Malware Analysis pueden seleccionar un servicio para investigar, elegir un escaneo en ese servicio y cargar un archivo para investigar en Malware Analysis.



Características

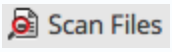
El cuadro de diálogo Seleccionar un servicio Malware Analysis consta de un panel Servicios de malware en el lado izquierdo y de una Lista de trabajos de escaneo en el lado derecho. El panel Lista de trabajos de escaneo tiene una barra de herramientas, una lista y botones para ver escaneos.

Panel Servicios de malware

El panel Servicios de malware es una lista de servicios disponibles para análisis de malware. En este panel, puede seleccionar el servicio que desea investigar y establecer un servicio predeterminado mediante el ícono Servicio predeterminado. Cuando selecciona un servicio, los trabajos de escaneo disponibles para ese servicio se muestran en la Lista de trabajos de escaneo.

Barra de herramientas Lista de trabajos de escaneo

Estas son las funciones de la barra de herramientas.

Característica	Descripción
	Muestra el cuadro de diálogo Escanear para encontrar malware, en el cual puede cargar un archivo en el servicio para su escaneo.
Eliminar trabajo de escaneo ()	Elimina uno o más trabajos de escaneo seleccionados. Security Analytics muestra un cuadro de diálogo de confirmación antes de eliminar los trabajos de escaneo.
Cancelar trabajo de escaneo ()	Pausa o continúa una o más trabajos de escaneo.
Actualizar ()	Actualiza la lista de trabajos de escaneo.

Lista de trabajos de escaneo

Estas son las columnas de la Lista de trabajos de escaneo. Esta lista también está disponible en el dashlet Trabajos de escaneo de malware.

Característica	Descripción
Nombre	Muestra el nombre del trabajo.
Estático, Red, Comunidad y Sandbox	Filtra los resultados en función de los puntajes para cada módulo de puntaje.
Progreso	Muestra el progreso actual del trabajo. • Verde: El trabajo está finalizado. • Negro: El trabajo está en curso. • Rojo: Se produjo un error.

Característica	Descripción
Información	Proporciona información adicional. Muestra la consulta del trabajo. Si el trabajo no está completo, también muestra una descripción más detallada del estado.
Usuario	Muestra el nombre del usuario que creó el trabajo.
Activity	Realiza un conteo de la cantidad de eventos del trabajo.
Descartados	Realiza un conteo de la cantidad de archivos/eventos en el el trabajo que se descartaron debido a que los puntajes estaban por debajo del umbral configurado.
Tipo de evento	Muestra el tipo de trabajo: Carga manual, A pedido o Volver a enviar.
Programado	Muestra la fecha y hora en que se ejecutó el trabajo.

Acciones

Estas son las acciones disponibles en el cuadro de diálogo.

Característica	Descripción
Botón Cancelar	Cancela el trabajo de escaneo seleccionado.
Botón Ver escaneo	Muestra el Resumen de eventos del escaneo seleccionado con los dashlets predeterminados abiertos.
Botón Ver modo continuo	Muestra el Resumen de eventos del escaneo seleccionado con los dashlets predeterminados abiertos.

Investigation: Cuadro de diálogo Configuración de la vista Navegar y la vista Eventos

La configuración en los cuadros de diálogo Ajustes de configuración de las vistas Navegar y Eventos es un subconjunto de la configuración de Investigation que se establece en Perfiles > panel Preferencias > pestaña Investigaciones. Si la configuración se proporciona en la vista Investigation, Security Analytics permite ahorrar tiempo a los analistas. Si cambia una configuración aquí, la misma configuración se cambia en la vista Perfiles, y si cambia una configuración en la vista Perfiles, la misma configuración se cambia aquí.

Para acceder a este cuadro de diálogo:

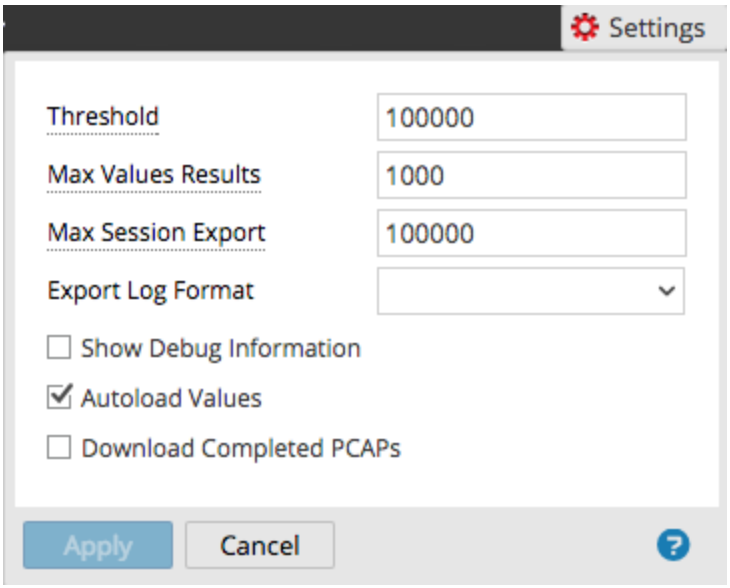
1. En el menú de **Security Analytics**, seleccione **Investigation > Navegar** o **Eventos**.
   Se muestra el cuadro de diálogo Investigar.
2. Seleccione un servicio y haga clic en **Navegar**.
3. En la barra de herramientas, seleccione la opción **Configuración**.
   Se muestra el cuadro de diálogo Configuración.

Características

Los cuadros de diálogo Configuración de las vistas Navegar y Eventos tienen varias funciones en común.

Cuadro de diálogo Configuración de la vista Navegar

Varios ajustes de Investigation influyen en el rendimiento de Security Analytics cuando se realiza la carga de valores en el panel Valores. Los valores predeterminados se configuran en función del uso común, y los analistas individuales pueden ajustar estas configuraciones para sus propias investigaciones.



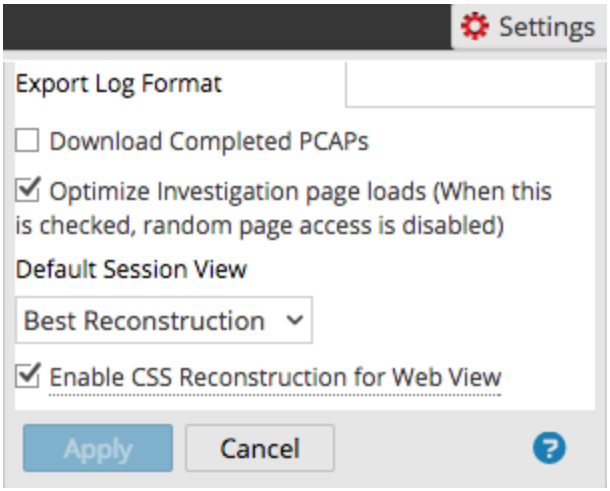
En la siguiente tabla se describen las funciones.

Característica	Descripción
Umbral	Ajusta el umbral de la cantidad máxima de sesiones cargadas para un valor clave de metadatos en el panel Valores. Un umbral más alto permite conteos precisos de un valor y también produce tiempos de carga mayores. El valor predeterminado es **100000**.
Número máximo de resultados de valores	Ajusta la cantidad máxima de valores para cargar en la vista Navegar cuando la opción Resultados máximos está seleccionada en el menú Clave de metadatos para una Clave de metadatos abierta. El valor predeterminado es **1,000**.
Máximo de exportación de sesiones	Ajusta la cantidad máxima de sesiones que se pueden exportar. El valor predeterminado es **100000**.

Característica	Descripción
Formato de registro de exportación	Ajusta el formato de archivo de los registros exportados. Hay cuatro formatos disponibles: • Texto • SML • CSV • JSON
Mostrar información de depuración	Si desea que Security Analytics muestre la cláusula `where` debajo de la ruta de navegación en la vista Navegar y el tiempo de carga transcurrido para cada servicio agregado en un Broker, seleccione esta opción. El valor predeterminado es **Desactivado**.
Cargar valores automáticamente	Si desea que Security Analytics cargue valores automáticamente para el servicio seleccionado en la vista Navegar, seleccione esta opción. Cuando no está seleccionada, Security Analytics muestra un botón **Cargar valores**, el cual da la oportunidad de modificar las opciones. El valor predeterminado es **Desactivado**.
Descargar PCAP finalizadas	Este ajuste automatiza la descarga de PCAP extraídas del módulo Investigation de modo que no sea necesario descargar ni abrir manualmente estos archivos en una aplicación que permite la visualización de datos en formato PCAP, como Wireshark.
Aplicar	La configuración se aplica de inmediato y estará visible la próxima vez que cargue valores. Los mismos cambios también se aplican en la vista Perfiles.
Cancelar	Cancela la operación de edición y cierra el cuadro de diálogo. La configuración permanece sin cambios.

Cuadro de diálogo Configuración de la vista Eventos

Varios ajustes de Investigation influyen en el rendimiento de Security Analytics cuando se ven y se reconstruyen sesiones en el panel Eventos. Los valores predeterminados se configuran en función del uso común, y los analistas individuales pueden ajustar estas configuraciones para sus propias investigaciones.



En la siguiente tabla se describen las funciones.

Característica	Descripción
Formato de registro de exportación	Ajusta el formato de archivo de los registros exportados. Hay cuatro formatos disponibles: • Texto • SML • CSV • JSON
Descargar PCAP finalizadas	Este ajuste automatiza la descarga de PCAP extraídas del módulo Investigation de modo que no sea necesario descargar ni abrir manualmente estos archivos en una aplicación que permite la visualización de datos en formato PCAP, como Wireshark.

Característica	Descripción
Optimizar las cargas de páginas de Investigation	Establece una opción de paginación. Cuando está optimizada, los resultados se devuelven lo más rápidamente posible, pero se renuncia a la capacidad original de ir a una página específica de la lista de eventos. La deselección de esta casilla cambia la paginación en la Lista de eventos y permite ir a una página específica de la lista (o a la última página). El valor predeterminado es **habilitado**.
Vista de sesión predeterminada	Selecciona el tipo de reconstrucción predeterminado para la reconstrucción inicial en la vista Eventos. El valor predeterminado es **Mejor reconstrucción**, con el cual los eventos se reconstruyen mediante el método de reconstrucción más apropiado para el evento.
Habilitar reconstrucción de CSS para vista web	Esta configuración controla la forma en que se ejecuta la reconstrucción del contenido web. Si está habilitada, la reconstrucción web incluye imágenes y estilos de hoja de estilo en cascada (CSS), de modo que su aspecto coincide con la vista original en un navegador web. Esto incluye el escaneo y la reconstrucción de eventos relacionados y la búsqueda de hojas de estilo e imágenes que se usan en el evento objetivo. Esta opción está habilitada de manera predeterminada. Deseleccione esta opción si hay problemas para ver sitios web específicos.
Aplicar	La configuración se aplica de inmediato y estará visible la próxima vez que vea eventos. Los mismos cambios también se aplican en la vista Perfiles.
Cancelar	Cancela la operación de edición y cierra el cuadro de diálogo. La configuración permanece sin cambios.