IBM Security QRadar
Versión 7.2.6

Guía del usuario

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 269.

Información sobre el producto

Este documento se aplica a IBM QRadar Security Intelligence Platform V7.2.6 y a los releases subsiguientes a menos que se reemplace por una versión actualizada de este documento.

© Copyright IBM Corporation 2012, 2015.

Contenido

© Copyright IBM Corp. 2012, 2015

Acerca de esta guía

La Guía del usuario de IBM® Security QRadar SIEM proporciona información sobre la gestión de IBM Security QRadar SIEM , que incluye los paneles Panel de control, Delitos, Actividad de registro, Actividad de red, Activos, e Informes.

Público al que va dirigido esta guía

Esta guía está pensada para todos los usuarios de QRadar SIEM que están encargados de investigar y gestionar la seguridad de una red. Esta guía presupone que el usuario tiene acceso a QRadar SIEM y conocimientos sobre la red corporativa y las tecnologías de red.

Documentación técnica

Para obtener información sobre cómo acceder a más documentación técnica, notas técnicas y notas de release, consulte Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21612861).

Cómo ponerse en contacto con el servicio de soporte al cliente

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

Declaración de buenas prácticas de seguridad

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

Tenga en cuenta lo siguiente:

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. El cliente se compromete a utilizar este programa en conformidad con las leyes, regulaciones y políticas aplicables y asume toda la responsabilidad de su cumplimiento. El licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

© Copyright IBM Corp. 2012, 2015

Capítulo 1. Novedades para los usuarios de QRadar V7.2.6

IBM Security QRadar V7.2.6 presenta la indexación optimizada, una prueba de CRE nueva que compara propiedades, mejoras de licencias y más.

Índices optimizados que aceleran el rendimiento de búsqueda

En releases anteriores se creaban índices para cada intervalo de un minuto. Ahora, con los superíndices de QRadar V7.2.6, se optimiza la estructura de datos de índice y se crea un superíndice al final de cada hora. Para búsquedas de varias horas en particular, QRadar explora ahora el índice de forma óptima, lo que multiplica el rendimiento por 10 para las búsquedas de tipo Indicador de compromiso (IOC). Algunos ejemplos de búsquedas de tipo IOC son búsquedas sobre dirección IP, dominio y nombre de host. Todos los datos nuevos recibidos por QRadar se indexan automáticamente en el formato nuevo.

Solo se optimiza el índice de los datos nuevos recibidos. Para obtener más información sobre la mejora del rendimiento de datos históricos, consulte la nota técnica Optimizing your Ariel indexes in 7.2.6 (http://www.ibm.com/support/docview.wss?uid=swg21968002).

Pruebas de CRE nuevas

Una prueba de motor de reglas personalizadas (CRE) está disponible para comparar una propiedad con otra, incluidas las propiedades personalizadas.

Ahora puede comparar una dirección IP de origen con una dirección IP de destino.

Puede comparar un nombre de usuario con una propiedad personalizada. Más información...

Utilice una gramática de clausulas WHERE de AQL para construir comparaciones complejas en el motor de reglas personalizadas (CRE). Puede utilizar la lógica AND/OR, las búsquedas de contenedor de referencia y las consultas de modelo de activo. Solo debe teclear las condiciones cuando construye la cláusula WHERE.

Más información...

Mejoras de licencia

QRadar V7.2.6 cambia la forma en que los sucesos afectan a la licencia. En releases anteriores, todos los sucesos generados por QRadar, como por ejemplo notificaciones de EPS, notificaciones del sistema y registros generados internamente se contabilizaban contra su licencia. Ahora, los sucesos internos siguientes no se contabilizan contra su licencia:

- notificaciones del sistema
- motor de reglas personalizadas (CRE)
- auditoría
- ADE
- perfilador de activos
- resultados de búsquedas planificadas
- medidas de salud

© Copyright IBM Corp. 2012, 2015

- Preguntas, simulaciones y registro interno de QRadar Risk Manager.

Solo los sucesos que se generan en dispositivos de las instalaciones del cliente se contabilizan a favor de su licencia. Además, el 60% de los sucesos descartados mediante reglas de direccionamiento se vuelven a contabilizar a favor, hasta un máximo de 2000 sucesos por segundo (EPS).

Visualización de conjuntos de referencia en reglas y resultados de la búsqueda

Ahora tiene más acceso a datos. Anteriormente, la información del conjunto de referencia no estaba disponible si no tenía privilegios de administrador. Ahora, los administradores pueden otorgarle acceso de modo que puede ver conjuntos de referencia en resultados de búsqueda y en reglas comunes. Ahora puede incluir conjuntos de referencia en búsquedas y reglas comunes. Puede ver listas de conjuntos de referencia, el contenido de los conjuntos de referencia y pueden exportar conjuntos de referencia. Más información...

Filtro rápido en el menú que aparece al pulsar el botón derecho del ratón

Los menús que aparecen al pulsar el botón derecho del ratón incluyen ahora una opción Filtro rápido para sucesos y flujos. Utilice los criterios de Filtro rápido para encadenar datos durante las investigaciones. Puede realizar búsquedas sobre elementos que coincidan o que no coincidan con la selección. Después de añadir el filtro de coincidencia/no coincidencia, hay más criterios de búsqueda disponibles en el menú que aparece al pulsar el botón derecho del ratón. Más información...

Flujo de trabajo de consulta mejorado para proporcionar un acceso a datos más rápido

QRadar mejora la forma en que interactúa con los datos y también le permite ampliar rápidamente el tiempo antes y después de que se haya producido un delito. Utilice las opciones para gráficos de series temporales en las pestañas de Actividad de red y Actividad de registro para cambiar rápidamente el periodo de tiempo visualizado sin dejar la vista de la actividad. Por ejemplo, si está investigando un delito que se ha producido en un punto final a las 04:30 del martes, puede profundizar hacia los sucesos del delito mismo. Puede mirar lo que ocurrió unos pocos minutos antes o después del intervalo de tiempo que está mirando sin tener que abrir la página **Editar búsqueda**. Puede especificar un periodo de tiempo, hasta el minuto o ampliar un periodo de tiempo desde la lista desplegable. Más información...

Mejoras de correlación histórica

IBM Security QRadar V7.2.6 presenta una mejor visibilidad para amenazas y gestión de resultados y perfiles de correlación histórica:

Visibilidad mejorada de amenazas reales
En IBM Security QRadar V7.2.5, los delitos históricos se creaban para cualquier regla desencadenada durante la ejecución de una correlación

histórica. En V7.2.6, los delitos históricos se crean solo cuando la regla desencadenada especifica que se debe crear un delito para el suceso detectado.

Auditoría mejorada
Se crean registros de auditoría cada vez que se ejecuta o se cancela un perfil de correlación histórica. Este cambio proporciona una supervisión y una visibilidad mejoradas para ver qué usuarios están ejecutando o cancelando ejecuciones de correlaciones históricas.

Nuevas prestaciones de búsqueda de delitos
Ahora puede buscar delitos creados desde un perfil de correlación histórica seleccionado. También puede excluir resultados de correlación histórica de búsquedas guardadas. Con estos parámetros de búsqueda nuevos, puede separar delitos de correlación histórica de delitos en tiempo real para la creación de informes.

Gestión mejorada de perfiles de correlación histórica

En función del volumen de datos históricos que esté procesando y de los criterios que especifique, puede ser ocurrir que la correlación tarde mucho en realizarse. Ahora puede cancelar perfiles de correlación histórica que se estén ejecutando o que estén en cola.

Puede ordenar y filtrar columnas en la ventana Correlación histórica para buscar fácilmente la información que está buscando.

Cuando ve el historial de ejecuciones de un perfil, puede ver rápidamente el número de delitos creados por una ejecución. Con una sola pulsación, puede profundizar en los catálogos de correlación histórica para ver la lista de sucesos o flujos que coinciden con los criterios del perfil.

Más información...

Nuevas funciones estadísticas y de serie de AQL

Utilice las funciones de Ariel Query Language (AQL) siguientes en búsqueda avanzadas para buscar la posición de una serie o sustituya una serie en una expresión regular:

Función	Descripción
strpos	Devuelve la posición de una serie dentro de otra serie.
regex_replace	Sustituye una serie utilizando un regex como la condición de búsqueda.
first	Devuelve las primeras instancias de la columna especificada.
last	Devuelve las últimas instancias de la columna especificada.
stddev	Devuelve la desviación estándar de ejemplo.
stddevp	Devuelve la desviación estándar de llenado.

Para obtener más información, consulte la sección Supported Functions del documento *IBM Security QRadar Ariel Query Language Guide*.

Capítulo 2. Acerca de QRadar SIEM

QRadar SIEM es una plataforma de gestión de seguridad de red que proporciona conocimiento situacional y soporte de cumplimiento de políticas mediante la combinación del conocimiento de los flujos de red, de la correlación de sucesos de seguridad y de la evaluación de vulnerabilidades de activos.

Clave de licencia predeterminada

La clave de licencia predeterminada proporciona acceso a la interfaz de usuario durante de cinco semanas. Después de iniciar la sesión en QRadar SIEM, una ventana muestra la fecha en la que caducará la clave de licencia temporal. Para obtener más información sobre la instalación de una clave de licencia, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Excepciones y certificados de seguridad

Si está utilizando el navegador web Mozilla Firefox, debe añadir una excepción a Mozilla Firefox para iniciar una sesión en QRadar SIEM. Para obtener más información, consulte la documentación del navegador web Mozilla Firefox.

Si está utilizando el navegador web Microsoft Internet Explorer, se muestra un mensaje de certificado de seguridad de sitio web cuando accede al sistema de QRadar SIEM. Debe seleccionar la opción **Continuar en este sitio web** para iniciar una sesión en QRadar SIEM.

Navegación por la aplicación basada en la web

Cuando utilice QRadar SIEM, utilice las opciones de navegación existentes en la interfaz de usuario de QRadar SIEM en lugar del botón **Atrás** del navegador web.

Prestaciones de su producto de inteligencia y seguridad

La documentación del producto IBM Security QRadar describe funciones tales como delitos, flujos, activos y correlación histórica, que pueden no estar disponibles en todos los productos de QRadar. Dependiendo del producto que esté utilizando, algunas de las características documentadas podrían no estar disponibles en su despliegue. Revise las prestaciones de cada producto como guía para obtener la información que necesita.

IBM Security QRadar SIEM incluye la gama completa de prestaciones de inteligencia y seguridad para los despliegues locales. QRadar SIEM consolida datos de sucesos de origen de registro de aplicaciones y puntos finales de dispositivo distribuidos por la red, y realiza actividades de normalización y correlación inmediata en los datos en bruto para distinguir hebras reales de falsos positivos.

Utilice IBM Security Intelligence on Cloud para recopilar, analizar, archivar y almacenar grandes volúmenes de registros de sucesos de red y de seguridad en un entorno alojado. Analice los datos para proporcionar visibilidad en el desarrollo de hebras, y cumpla los requisitos de creación de informes y supervisión de la conformidad al tiempo que reduce el coste total de propiedad.

© Copyright IBM Corp. 2012, 2015

Utilice IBM Security QRadar Log Manager para recopilar, analizar, archivar y almacenar grandes volúmenes de registros de sucesos de red y de seguridad. QRadar Log Manager analiza datos para proporcionar visibilidad en el desarrollo de hebras, y puede ayudar al cumplimiento de los requisitos de creación de informes y supervisión.

Al buscar ayuda, utilice la tabla siguiente, que muestra las prestaciones de los productos:

Tabla 1. Comparación de prestaciones de QRadar

Prestación	QRadar SIEM	IBM Security Intelligence on Cloud	IBM Security QRadar Log Manager
Da soporte a despliegues alojados	No	Sí	No
Paneles de control personalizables	Sí	Sí	Sí
Motor de reglas personalizadas	Sí	Sí	Sí
Gestionar sucesos de red y seguridad	Sí	Sí	Sí
Gestionar registros de aplicación y host	Sí	Sí	Sí
Alertas basadas en umbral	Sí	Sí	Sí
Plantillas de conformidad	Sí	Sí	Sí
Archivado de datos	Sí	Sí	Sí
Integración de canales de información de reputación de IP de IBM Security X-Force Threat Intelligence	Sí	Sí	Sí
Despliegues autónomos de WinCollect	Sí	Sí	Sí
Despliegues gestionados de WinCollect	Sí	No	Sí
Integración de QRadar Vulnerability Manager	Sí	No	Sí
Supervisión de la actividad de red	Sí	No	No
Perfilado de activos	Sí	Sí	No [1]
Gestión de delitos	Sí	Sí	No
Captura y análisis de flujo de red	Sí	No	No
Correlación histórica	Sí	Sí	No
Integración de QRadar Risk Manager	Sí	No	No
Integración de QRadar Incident Forensics	Sí	No	No

[1] QRadar Log Manager solo hace un seguimiento de datos de activos si QRadar Vulnerability Manager está instalado.

Navegadores web soportados

Para que las características de los productos de IBM Security QRadar funcionen correctamente, debe utilizar un navegador web soportado.

Al acceder al sistema de QRadar, se le solicitará un nombre de usuario y una contraseña. El administrador debe configurar de antemano el nombre de usuario y la contraseña.

La tabla siguiente lista las versiones soportadas de navegadores web.

Tabla 2. Navegadores web soportados para productos de QRadar

Navegador web	Versiones soportadas
Mozilla Firefox	38.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, con el modo de documento y el modo de explorador habilitados.	10.0
Microsoft Internet Explorer de 32 bits y 64 bits con Microsoft Internet Explorer 10 seleccionado en modalidad de documento.	11.0
Google Chrome	Versión 46

Habilitación del modo de documento y modo de explorador en Internet Explorer

Si utiliza Microsoft Internet Explorer para acceder a productos de IBM Security QRadar, debe habilitar el modo de explorador y el modo de documento.

Procedimiento

1. En el explorador web de Internet Explorer, pulse F12 para abrir la ventana Herramientas de desarrollo.
2. Pulse **Modo de explorador** y seleccione la versión del explorador web.
3. Pulse **Modo de documento** y seleccione el **Estándar Internet Explorer** correspondiente al release de Internet Explorer.

Inicio de sesión de IBM Security QRadar

IBM Security QRadar es una aplicación basada en web. QRadar utiliza la información de inicio de sesión predeterminada para el URL, el nombre de usuario y la contraseña.

Utilice la información de la tabla siguiente cuando inicie la sesión en la consola de IBM Security QRadar.

Tabla 3. Información de inicio de sesión predeterminada para QRadar

Información de inicio de sesión	Valor predeterminado
URL	https://<Dirección IP>, donde <Dirección IP> es la dirección IP de la consola de QRadar. Para iniciar la sesión en QRadar en un entorno de IPv6 o mixto, escriba la dirección IP entre corchetes: `https://[<Dirección IP>]`
Nombre de usuario	admin
Contraseña	La contraseña que se asigna a QRadar durante el proceso de instalación.
Clave de licencia	Una clave de licencia predeterminada le proporciona acceso al sistema durante 5 semanas.

API RESTful

Utilice la API (Interfaz de programación de aplicaciones) de REST (Representational State Transfer) para realizar consultas HTTPS e integrar IBM Security QRadar con otras soluciones.

Acceso y permisos de rol de usuario

Debe tener permisos de rol de usuario administrativo en QRadar para acceder y utilizar las API RESTful. Para obtener más información sobre la gestión de los permisos del rol de usuario, consulte la publicación *Guía de administración*.

Acceso a la interfaz de usuario de documentación técnica de API REST

La interfaz de usuario API proporciona descripciones y prestaciones para las siguientes interfaces de API REST:

Tabla 4. Interfaces de API REST

API REST	Descripción
`/api/ariel`	Consultar bases de datos, búsquedas, ID de búsqueda y resultados de búsqueda.
`/api/asset_model`	Devuelve una lista de todos los activos del modelo. También puede listar todos los tipos de propiedad de activo disponibles y las búsquedas guardadas así como actualizar un activo.
`/api/auth`	Cerrar la sesión e invalidar la sesión actual.
`/api/help`	Devuelve una lista de prestaciones de API.
`/api/siem`	Devuelve una lista de todos los delitos.
`/api/qvm`	Revisar y gestionar datos de QRadar Vulnerability Manager.
`/api/reference_data`	Ver y gestionar recopilaciones de datos de referencia.
`/api/qvm`	Recupera activos, vulnerabilidades, redes, servicios abiertos y filtros. También puede crear o actualizar tíquets de remediación.
`/api/scanner`	Ver, crear o iniciar una exploración remota que esté relacionada con un perfil de exploración.

La interfaz de documentación técnica de la API REST proporciona una infraestructura que puede utilizar para recopilar el código necesario que se necesita para implementar funciones de QRadar en otros productos.

1. Especifique el URL siguiente en el navegador para acceder a la interfaz de la documentación técnica: `https://`*`dirección_IP_consola`*`/api_doc`.
2. Pulse la cabecera de la API a la que desea acceder, por ejemplo **/ariel**.
3. Pulse la subcabecera para el punto final al que desea acceder, por ejemplo **/databases**.
4. Pulse la subcabecera Experimental o Provisional.

Nota:

Los puntos finales de la API están anotados como *experimental* o *estable*.

Experimental
Indica que el punto final de la API puede no estar totalmente probado y puede cambiarse o eliminarse en el futuro sin previo aviso.

Estable
Indica que el punto final de la API se ha probado y se soporta por completo.

5. Pulse **Try it out** para recibir respuestas HTTPS formateadas correctamente.
6. Revise y recopile la información que necesita implementar en la solución de terceros.

Ejemplos de código y de foro de la API de QRadar

El foro de la API proporciona más información sobre la API REST, incluidas las respuestas a las preguntas más frecuentes y ejemplos de código anotado que puede utilizar en un entorno de prueba. Para obtener más información, consulte el foro de la API (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

Pestañas de interfaz de usuario

La funcionalidad se divide en pestañas. La pestaña **Panel de control** se visualiza cuando se inicia la sesión.

Puede desplazarse fácilmente por las pestañas para localizar los datos o la funcionalidad que necesita.

Pestaña Panel de control

La pestaña **Panel de control** es la pestaña predeterminada que se visualiza cuando se inicia la sesión.

La pestaña **Panel de control** proporciona un entorno de espacio de trabajo que soporta varios paneles de control en los que puede visualizar las vistas de seguridad de red, la actividad o los datos que QRadar recopila. Están disponibles cinco paneles de control predeterminados. Cada panel de control contiene elementos que proporcionan información detallada y de resumen sobre los delitos que se producen en la red. También puede crear un panel de control personalizado para poder centrarse en las responsabilidades de las operaciones de red o de seguridad. Para obtener más información acerca de la utilización de la pestaña Panel de control, consulte Gestión de panel de control.

Pestaña Delitos

La pestaña **Delitos** le permite ver los delitos que se producen en la red, los cuales puede localizar mediante diversas opciones de navegación o a través de búsquedas avanzadas.

Desde la pestaña **Delitos**, puede investigar un delito para determinar la causa raíz de un problema. También puede resolver el problema.

Para obtener más información sobre la pestaña **Delitos**, consulte Gestión de delitos.

Pestaña Actividad de registro

La pestaña **Actividad de registro** le permitirá investigar los registros de sucesos que se envían a QRadar en tiempo real, realizar búsquedas potentes y ver la actividad de registro utilizando gráficos de series temporales configurables.

La pestaña **Actividad de registro** le permitirá realizar investigaciones en profundidad sobre datos de suceso.

Para obtener más información, consulte Investigación de actividad de registro.

Pestaña Actividad de red

Utilice la pestaña **Actividad de red** para investigar flujos que se envían en tiempo real, realizar búsquedas avanzadas y ver actividad de red mediante gráficos de serie temporal configurables.

Un flujo es una sesión de comunicación entre dos hosts. Visualizar información de flujo le permitirá determinar cómo se transmite el tráfico, qué se transmite (si está habilitada la opción de captura de contenido) y quién está transmitiendo. Los datos de flujo también incluyen detalles tales como protocolos, valores de ASN, valores de IFIndex y prioridades.

Para obtener más información, consulte Investigación de la actividad de red.

Pestaña Activos

QRadar descubre automáticamente los activos, servidores y hosts que operan en la red.

El descubrimiento automático se basa en datos de flujo pasivos y datos de vulnerabilidad, permitiendo que QRadar cree un perfil de activo.

Los perfiles de activo proporcionan información sobre cada activo conocido de la red, incluyendo información de identidad, si está disponible, y sobre qué servicios se ejecutan en cada activo. Estos datos de perfil se utilizan para la correlación con el fin de ayudar a reducir falsos positivos.

Por ejemplo, un ataque intenta utilizar un servicio específico que se está ejecutando en un activo específico. En esta situación, QRadar puede determinar si el activo es vulnerable a este ataque correlacionando el ataque con el perfil de activo. Mediante la pestaña **Activos**, puede ver los activos aprendidos o buscar activos específicos para ver los perfiles.

Para obtener más información, consulte Gestión de activos.

Pestaña Informes

La pestaña **Informes** le permite crear, distribuir y gestionar informes para los datos en QRadar.

La característica Informes le permitirá crear informes personalizados para uso operativo y ejecutivo. Para crear un informe, puede combinar la información (por ejemplo seguridad o red) en un único informe. También puede utilizar plantillas de informe preinstaladas que se incluyen con QRadar.

La pestaña **Informes** también le permitirá marcar los informes con logotipos personalizados. Esta personalización es beneficiosa para distribuir informes a diferentes públicos.

Para obtener más información sobre informes, consulte Gestión de informes.

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager es un dispositivo instalado por separado para supervisar configuraciones de dispositivo, simular cambios en el entorno de red, y priorizar riesgos y vulnerabilidades de la red.

IBM Security QRadar Risk Manager utiliza datos recogidos por dispositivos de red y de seguridad, tales como cortafuegos, direccionadores, conmutadores, sistemas de prevención de intrusiones, canales de información de vulnerabilidades y orígenes de seguridad de proveedor. Estos datos se utilizan para determinar los riesgos de seguridad existentes dentro de la infraestructura de seguridad de la red y la probabilidad de que se exploten esos riesgos.

Nota: Para obtener más información sobre IBM Security QRadar Risk Manager, consulte al representante de ventas local.

Pestaña Admin

Los administradores utilizan la pestaña Admin para configurar y gestionar los usuarios, sistemas, redes, plug-ins y componentes. Los usuarios con privilegios de administración pueden acceder a la pestaña **Admin**.

Las herramientas de administración a las que los administradores pueden acceder en la pestaña **Admin** se describe en la Tabla 1.

Tabla 5. Herramientas de gestión de administración disponibles en QRadar

Herramienta de administración	Descripción
Configuración del sistema	Configurar opciones de gestión de sistema y usuarios.
Orígenes de datos	Configurar orígenes de registro, orígenes de flujo y opciones de vulnerabilidad.
Configuración de redes remotas y servicios	Configurar redes remotas y grupos de servicios.
Editor de despliegue	Gestionar los componentes individuales del despliegue de QRadar.

Todas las actualizaciones de configuración que realiza en la pestaña **Admin** se guardan en un área de transferencia. Cuando se hayan completado todos los cambios, puede desplegar las actualizaciones de configuración realizadas en el host gestionado en el despliegue.

Procedimientos comunes de QRadar

Varios controles de la interfaz de usuario de QRadar son comunes en la mayoría de las pestañas de interfaz de usuario.

En las secciones siguientes se describe la información sobre estos procedimientos comunes.

Visualización de mensajes

El menú **Mensajes**, que se encuentra en la esquina superior derecha de la interfaz de usuario, proporciona acceso a una ventana en la que puede leer y gestionar las notificaciones del sistema.

Antes de empezar

Para que las notificaciones del sistema se muestren en la ventana **Mensajes**, el administrador debe crear una regla que se base en cada tipo de mensaje de notificación y seleccionar el recuadro de selección **Notificar** en el **Asistente de reglas personalizadas**.

Acerca de esta tarea

El menú **Mensajes** indica cuántas notificaciones de sistema no leídas tiene en el sistema. Este indicador incrementa el número hasta que se cierran las notificaciones de sistema. Para cada notificación de sistema, la ventana **Mensajes** proporciona un resumen y la indicación de fecha y hora en que se ha creado la notificación de sistema. Puede pasar el puntero del ratón sobre una notificación para ver más detalles. Utilizando las funciones de la ventana **Mensajes**, puede gestionar las notificaciones del sistema.

Las notificaciones del sistema también están disponibles en la pestaña **Panel de control** y en una ventana emergente opcional que se puede visualizar en la esquina inferior izquierda de la interfaz de usuario. Las acciones que se realizan en la ventana **Mensajes** se propagan a la pestaña **Panel de control** y la ventana emergente. Por ejemplo, si cierra una notificación de sistema de la ventana **Mensajes**, la notificación de sistema se elimina de todas las pantallas de notificación de sistema.

Para obtener más información sobre las notificaciones de sistema del panel de control, consulte Elemento de notificaciones de sistema.

La ventana **Mensajes** proporciona las funciones siguientes:

Tabla 6. Funciones disponibles en la ventana Mensajes

Función	Descripción
Todos	Pulse **Todos** para ver todas las notificaciones del sistema. Esta opción es el valor predeterminado, por lo tanto, pulse **Todos** sólo si ha seleccionado otra opción y desea visualizar de nuevo todas las notificaciones del sistema.
Salud	Pulse **Salud** para ver solo las notificaciones de sistema que tienen un nivel de gravedad de Salud.
Errores	Pulse **Errores** para ver solo las notificaciones de sistema sólo que tienen un nivel de gravedad de Error.
Avisos	Pulse **Avisos** para ver sólo las notificaciones de sistema que tienen un nivel de gravedad de Aviso.
Información	Pulse **Información** para ver sólo las notificaciones de sistema que tienen un nivel de gravedad de información.

Tabla 6. Funciones disponibles en la ventana Mensajes (continuación)

Función	Descripción
Descartar todo	Pulse **Descartar todo** para cerrar en el sistema todas las notificaciones de sistema. Si ha filtrado la lista de notificaciones de sistema utilizando los iconos de **Salud**, **Errores**, **Avisos** o **Información**, el texto en el icono **Ver todos** cambia a una de las opciones siguientes: • **Descartar todos los errores** • **Descartar toda la salud** • **Descartar todos los avisos** • **Descartar todos los avisos** • **Descartar toda la información**
Ver todos	Pulse **Ver todos** para ver los sucesos de notificación de sistema en la pestaña **Actividad de registro**. Si ha filtrado la lista de notificaciones de sistema utilizando los iconos de **Salud**, **Errores**, **Avisos** o **Información**, el texto en el icono **Ver todos** cambia a una de las opciones siguientes: • **Ver todos los errores** • **Ver toda la salud** • **Ver todos los avisos** • **Ver toda la información**
Descartar	Pulse el icono **Descartar** junto a una notificación de sistema para cerrar en el sistema la notificación de sistema.

Procedimiento

1. Inicie la sesión en QRadar.
2. En la esquina superior derecha de la interfaz de usuario, pulse **Mensajes**.
3. En la ventana **Mensajes**, vea los detalles de la notificación de sistema.
4. Opcional. Para refinar la lista de notificaciones de sistema, pulse una de las opciones siguientes:
   - **Errores**
   - **Avisos**
   - **Información**
5. Opcional. Para cerrar las notificaciones de sistema, elija entre las opciones siguientes:

Opción	Descripción
Descartar todo	Pulse aquí para cerrar todas las notificaciones de sistema.
Descartar	Pulse el icono **Descartar** junto a la notificación de sistema que desea cerrar.

6. Opcional. Para ver los detalles de notificación de sistema, pase el puntero de ratón sobre la notificación de sistema.

Ordenación de resultados

Puede ordenar los resultados en tablas pulsando una cabecera de columna. Una flecha en la parte superior de la columna indica la dirección de la ordenación.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la cabecera de columna una vez para ordenar la tabla en orden descendente; pulse dos veces para ordenar la tabla en orden ascendente.

Renovación y pausa de la interfaz de usuario

Puede renovar, poner en pausa y reproducir manualmente los datos que se visualizan en las pestañas.

Acerca de esta tarea

Las pestañas **Panel de control** y **Delitos** se renuevan automáticamente cada 60 segundos.

Las pestañas **Actividad de registro** y **Actividad de red** se renuevan automáticamente cada 60 segundos si está viendo la pestaña en modalidad de Último intervalo (renovación automática).

El temporizador, que se encuentra en la esquina superior derecha de la interfaz, indica la cantidad de tiempo hasta que la pestaña se renueve automáticamente.

Cuando vea la pestaña **Actividad de registro** o **Actividad de red** en modalidad de Tiempo real (modalidad continua) o de Último minuto (renovación automática), puede utilizar el icono **Pausa** para poner en pausa la visualización actual.

También puede poner en pausa la visualización actual en la pestaña **Panel de control**. Al pulsar en cualquier lugar dentro de un elemento de panel de control, la pestaña se pone en pausa automáticamente. El temporizador parpadea en rojo para indicar que la visualización actual se ha puesto en pausa.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la pestaña que desea ver.
3. Elija una de las siguientes opciones:

Opción	Descripción
Renovar	Pulse **Renovar**, en la esquina derecha de la pestaña, para renovar la pestaña.
Pausa	Pulse aquí para poner en pausa la visualización de la pestaña.
Reproducir	Pulse aquí para reiniciar el temporizador después de que éste se haya puesto en pausa.

Investigación de direcciones IP

Puede utilizar varios métodos para investigar la información sobre direcciones IP en las pestañas Panel de control, Actividad de registro y Actividad de red.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la pestaña que desea ver.
3. Mueva el puntero de ratón sobre una dirección IP para ver la ubicación de la dirección IP.
4. Pulse el botón derecho del ratón en la dirección IP o el nombre de activo y seleccione una de las opciones siguientes:

Tabla 7. Información de direcciones IP

Opción	Descripción
Navegar > **Ver por red**	Muestra las redes que están asociadas con la dirección IP seleccionada.
Navegar > **Ver resumen de origen**	Muestra los delitos que están asociados con la dirección IP de origen seleccionada.
Navegar > **Ver resumen de destino**	Muestra los delitos que están asociados con la dirección IP de destino seleccionada.
Información > **Búsqueda de DNS**	Busca entradas DNS que están basados en la dirección IP.
Información > **Búsqueda de WHOIS**	Busca el propietario registrado de una dirección IP remota. El servidor WHOIS predeterminado es whois.arin.net.
Información > **Exploración de puertos**	Realiza una exploración de Network Mapper (NMAP) de la dirección IP seleccionada. Esta opción solo está disponible si NMAP está instalado en el sistema. Para obtener más información sobre la instalación de NMAP, consulte la documentación de proveedor.
Información > **Perfil de activo**	Visualiza información de perfil de activo. Esta opción se visualiza si se ha adquirido IBM Security QRadar Vulnerability Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*. Esta opción de menú está disponible si QRadar ha adquirido datos de perfil activamente a través de una exploración o pasivamente a través de orígenes de flujo. Para obtener información, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.
Información > **Sucesos de búsqueda**	Busca los sucesos que están asociados con esta dirección IP.
Información > **Buscar flujos**	Busca flujos que están asociados con esta dirección IP.

Tabla 7. Información de direcciones IP (continuación)

Opción	Descripción
Información > **Buscar en conexiones**	Busca las conexiones que están asociadas con esta dirección IP. Esta opción solo se visualiza si ha adquirido IBM Security QRadar Risk Manager y ha conectado QRadar y el dispositivo de IBM Security QRadar Risk Manager. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
Información > **Switch Port Lookup**	Determina el puerto de conmutador en un dispositivo Cisco IOS para esta dirección IP. Esta opción solo se aplica a conmutadores que se descubren utilizando la opción **Discover Devices** en la pestaña **Riesgos**. **Nota:** Esta opción de menú no está disponible en QRadar Log Manager
Información > **Ver topología**	Visualiza la pestaña **Riesgos**, que representa la topología de capa 3 de la red. Esta opción está disponible si ha adquirido IBM Security QRadar Risk Manager y ha conectado QRadar y el dispositivo de IBM Security QRadar Risk Manager.
Ejecutar Exploración de vulnerabilidad	Seleccione la opción **Ejecutar Exploración de vulnerabilidad** para realizar una exploración de IBM Security QRadar Vulnerability Manager en esta dirección IP. Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Investigar nombres de usuario

Puede pulsar el botón derecho del ratón en un nombre de usuario para acceder a más opciones de menú. Use estas opciones para ver más información sobre el nombre de usuario o la dirección IP.

Puede investigar los nombres de usuario al comprar IBM Security QRadar Vulnerability Manager y obtener la licencia del mismo. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Al pulsar el botón derecho del ratón en un nombre de usuario, puede elegir las siguientes opciones de menú.

Tabla 8. Opciones de menú para investigación de nombre de usuario

Opción	Descripción
Ver activos	Visualiza los activos actuales que están asociados con el nombre de usuario seleccionado. Para obtener más información sobre cómo ver activos, consulte Gestión de activos.

Tabla 8. Opciones de menú para investigación de nombre de usuario (continuación)

Opción	Descripción
Ver historial de usuario	Visualiza todos los activos que están asociados con el nombre de usuario seleccionado durante las 24 horas anteriores.
Ver sucesos	Visualiza los sucesos que están asociados con el nombre de usuario seleccionado. Para obtener más información sobre la ventana Lista de sucesos, consulte Supervisión de actividad de registro.

Para obtener más información sobre cómo personalizar el menú que aparece al pulsar el botón derecho del ratón, consulte la publicación *Guía de administración* correspondiente al producto.

Hora del sistema

En la esquina derecha de la interfaz de usuario de QRadar se visualiza la hora del sistema, que es la hora de la consola.

La hora de consola sincroniza los sistemas QRadar en el despliegue de QRadar. La hora de consola se utiliza para determinar qué sucesos de hora se han recibido de otros dispositivos para la correlación de sincronización de hora correcta.

En un despliegue distribuido, la consola puede estar en un huso horario diferente del correspondiente al del sistema.

Cuando se aplican filtros y búsquedas basadas en la hora en la pestaña **Actividad de registro** y la pestaña **Actividad de red**, debe utilizar la hora de sistema de la consola para especificar un intervalo de tiempo.

Cuando se aplican filtros y búsquedas basados en la hora en la pestaña **Actividad de registro**, debe utilizar la hora de sistema de la consola para especificar un intervalo de tiempo.

Actualización de preferencias de usuario

Puede establecer las preferencias de usuario, por ejemplo entorno local, en la interfaz de usuario de IBM Security QRadar SIEM principal.

Procedimiento

1. Para acceder a la información de usuario, pulse **Preferencias**.
2. Actualice las preferencias.

Opción	Descripción
Nombre de usuario	Visualiza el nombre de usuario. No puede editar este campo.

Opción	Descripción
Contraseña	Las contraseñas de usuario de QRadar se almacenan como una serie SHA-256 salada. La contraseña debe cumplir los siguientes criterios: • Un mínimo de 6 caracteres • Un máximo de 255 caracteres • Contener al menos un carácter especial • Contener un carácter en mayúsculas
Contraseña (Confirmar)	Confirmación de la contraseña
Dirección de correo electrónico	La dirección de correo electrónico debe cumplir los requisitos siguientes: • Un mínimo de 10 caracteres • Un máximo de 255 caracteres
Entorno local	QRadar está disponible en los idiomas siguientes: inglés, chino simplificado, chino tradicional, japonés, coreano, francés, alemán, italiano, español, ruso y portugués (Brasil). Si elige otro idioma, la interfaz de usuario se muestra en inglés. Se utilizan otros convenios culturales asociados, como tipo de carácter, clasificación, formato de fecha y hora, unidad de moneda.
Habilitar notificaciones emergentes	Marque este recuadro de selección si desea permitir que se visualicen notificaciones de sistema emergentes en la interfaz de usuario.

Conceptos relacionados:

"Opciones de búsqueda de Filtro rápido" en la página 181
Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

Acceder a la ayuda en línea

Puede acceder a la Ayuda en línea de QRadar a través de la interfaz de usuario principal de QRadar.

Para acceder a la Ayuda en línea, pulse **Ayuda** > **Contenido de la ayuda**.

Redimensionar columnas

Puede redimensionar las columnas en varias pestañas en QRadar.

Coloque el puntero del ratón por encima de la línea que separa las columnas y arrastre el borde de la columna a la nueva ubicación. También puede redimensionar las columnas efectuando una doble pulsación en la línea que separa las columnas para redimensionar automáticamente la columna a la anchura del campo más grande.

Nota: El redimensionamiento de columna no funciona en los navegadores web Microsoft Internet Explorer, Versión 7.0 cuando las pestañas visualizan registros en modalidad continua.

Tamaño de página

Los usuarios con privilegios administrativos pueden configurar el número máximo de resultados que se visualizan en las tablas de varios separadores de QRadar.

Capítulo 3. Gestión de panel de control

La pestaña **Panel de control** es la vista predeterminada cuando se inicia la sesión.

Proporciona un entorno de espacio de trabajo que soporta varios paneles de control en los que puede visualizar las vistas de seguridad de red, la actividad o los datos que se recopilan.

Los paneles de control le permiten organizar los elementos de panel de control en vistas funcionales, que le permiten centrarse en áreas específicas de la red.

Utilice la pestaña Panel de control para supervisar el comportamiento de sucesos de seguridad.

Puede personalizar el panel de control. El contenido que se visualiza en la pestaña **Panel de control** es específico del usuario. Los cambios que se realizan dentro de una sesión sólo afectan el sistema.

Paneles de control predeterminados

Utilice el panel de control predeterminado para personalizar elementos y crear vistas funcionales. Estas vistas funcionales están centradas en áreas determinadas de la red.

La pestaña **Panel de control** proporciona cinco paneles de control predeterminados que están centrados en la seguridad, la actividad de red, la actividad de aplicaciones, la supervisión del sistema y el cumplimiento de las normativas.

Cada panel de control muestra un conjunto predeterminado de elementos de panel de control. Los elementos de panel de control sirven de punto de partida para acceder a datos más detallados. La tabla siguiente define los paneles de control predeterminados.

Paneles de control personalizados

Puede personalizar los paneles de control. El contenido que se muestra en la pestaña **Panel de control** es específico del usuario. Los cambios realizados dentro de una sesión de QRadar sólo afectan al sistema local del usuario.

Para personalizar la pestaña **Panel de control**, puede realizar las tareas siguientes:

- Cree paneles de control personalizados que sean aplicables a las tareas que tenga asignadas. Se pueden crear un máximo de 255 paneles de control por cada usuario, pero se pueden producir problemas de rendimiento si crea más de 10 paneles de control.
- Añada y elimine elementos de los paneles de control predeterminados o personalizados.
- Mueva y sitúe los elementos de acuerdo con sus necesidades. Cuando sitúa elementos, cada elemento cambia automáticamente de tamaño en proporción al panel de control.
- Añada elementos de panel de control personalizado que están basados en cualquier dato.

© Copyright IBM Corp. 2012, 2015

Por ejemplo, puede añadir un elemento de panel de control que proporciona un gráfico de serie temporal o un gráfico de barras que representa los 10 elementos principales de actividad de red.

Para crear elementos personalizados, puede crear búsquedas guardadas en **la pestaña Actividad de red** o **la pestaña Actividad de registro** y elegir cómo desea que se representen los resultados en la pestaña de control. Cada gráfico de panel de control muestra datos actualizados en tiempo real. Los gráficos de serie temporal del panel de control se renuevan cada 5 minutos.

Personalizar el panel de control

Puede añadir elementos a paneles de control predeterminados o personalizados.

Puede personalizar los paneles de control para mostrar y organizar sus elementos de acuerdo con los requisitos de seguridad de la red.

Existen 5 paneles de control predeterminados, a los que puede acceder desde el cuadro de lista **Mostrar panel de control** de la pestaña **Panel de control**. Si previamente ha visualizado un panel de control y ha vuelto a la pestaña **Panel de control**, se muestra el último panel de control que ha visto.

Búsqueda de flujos

Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña **Actividad de red**.

Los elementos de búsqueda de flujos están listados en el menú **Añadir elemento** > **Actividad de red** > **Búsqueda de flujos**. El nombre del elemento de búsqueda de flujos coincide con el nombre de los criterios de búsqueda guardados en los que está basado el elemento.

Puede utilizar criterios de búsqueda guardados predeterminados preconfigurados para mostrar elementos de búsqueda de flujos en el menú de la pestaña **Panel de control**. Puede añadir más elementos de panel de control de la búsqueda de flujos al menú de la pestaña **Panel de control**. Para obtener más información, consulte Añadir elementos de panel de control basados en búsquedas a la lista Añadir elementos.

En un elemento de panel de control de búsqueda de flujos, los resultados de la búsqueda muestran datos actualizados en tiempo real en un gráfico. Los tipos de gráfico soportados son series temporales, de tabla, circulares y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar. Para obtener más información sobre la configuración de gráficos, consulte Configurar gráficos.

Los gráficos de serie temporal son interactivos. Mediante los gráficos de serie temporal, puede aumentar el detalle de una línea temporal para investigar actividad de la red.

Delitos

Puede añadir varios elementos relacionados con delitos al panel de control.

Nota: Los delitos ocultos o cerrados no se incluyen en los valores que se muestran en la pestaña **Panel de control**. Para obtener más información sobre delitos ocultos o cerrados, consulte Gestión de delitos.

La tabla siguiente describe los elementos de delito:

Tabla 9. Elementos de delito

Elementos de panel de control	Descripción
Delitos más recientes	Los cinco delitos más recientes se identifican con una barra de magnitudes para informarle de la importancia del delito. Coloque el puntero del ratón en el nombre del delito para ver información detallada sobre la dirección IP.
Delitos más graves	Los cinco delitos más graves se identifican con una barra de magnitudes para informarle de la importancia del delito. Coloque el puntero del ratón en el nombre del delito para ver información detallada sobre la dirección IP.
Mis delitos	El elemento **Mis delitos** muestra 5 de los delitos más recientes que tiene asignados el usuario. Los delitos se identifican con una barra de magnitudes para informarle de la importancia del delito. Coloque el puntero del ratón en la dirección IP para ver información detallada sobre la dirección IP.
Orígenes principales	El elemento **Delitos principales** muestra los orígenes de delitos principales. Cada origen se identifica con una barra de magnitudes para informarle de la importancia del origen. Coloque el puntero del ratón en la dirección IP para ver información detallada sobre la dirección IP.
Destinos locales principales	El elemento **Destinos locales principales** muestra los destinos locales principales. Cada destino se identifica con una barra de magnitudes para informarle de la importancia del destino. Coloque el puntero del ratón en la dirección IP para ver información detallada sobre la dirección IP.
Categorías	El elemento **Tipos de categorías principales** muestra las cinco categorías principales correspondientes al número mayor de delitos.

Actividad de registro

Los elementos de panel de control**Actividad de registro** le permitirán supervisar e investigar sucesos en tiempo real.

Nota: Los sucesos ocultos o cerrados no están incluidos en los valores que se visualizan en la pestaña **Panel de control** .

Tabla 10. Elementos de actividad de registro

Elemento de panel de control	Descripción
Búsquedas de suceso	Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña Actividad de registro. Los elementos de búsqueda de sucesos se listan en el menú **Añadir elemento** > **Actividad de red** > **Búsquedas de suceso**. El nombre del elemento de búsqueda de sucesos coincide con el nombre de los criterios de búsqueda guardados en los que se basa el elemento. QRadar incluye criterios de búsqueda guardados predeterminados que están preconfigurados para visualizar elementos de búsqueda de sucesos en el menú de pestaña **Panel de control**. Puede añadir más elemento de panel de control de búsqueda de sucesos en el menú de pestaña **Panel de control**. Para obtener más información, consulte Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos Añadir. En un elemento de panel de control **Actividad de registro**, los resultados de búsqueda visualizan datos de última hora en tiempo real en un gráfico. Los tipos de gráfico soportados son series de tiempo, tabla, circular y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar. Los gráficos de series temporales son interactivos. Puede ampliar y explorar en una línea temporal para investigar la actividad de registro.
Sucesos por gravedad	El elemento de panel de control **Sucesos por gravedad** visualiza el número de sucesos activos que están agrupados por gravedad. Este elemento le permitirá ver el número de sucesos que se reciben por el nivel de gravedad asignada. La gravedad indica la cantidad de amenaza que representa un origen de delito en relación al grado de preparación del destino ante el ataque. El rango de gravedad es de 0 (baja) a 10 (alta). Los tipos de gráfico soportados son tabla, circular y de barras.

Tabla 10. Elementos de actividad de registro (continuación)

Elemento de panel de control	Descripción
Orígenes de registro principales	El elemento de panel de control **Orígenes de registro principales** visualiza los 5 orígenes de registro principales que han enviado sucesos a QRadar en los últimos 5 minutos. El número de sucesos que se envían desde el origen de registro especificado se indica en el gráfico circular. Este elemento le permitirá ver los cambios potenciales en el comportamiento, por ejemplo si un origen de registro de cortafuegos que normalmente no está en la lista de 10 principales ahora contribuye en un gran porcentaje del recuento de mensajes global, debe investigar esta aparición. Los tipos de gráfico soportados son tabla, circular y de barras.

Informes más recientes

El elemento de panel de control **Informes más recientes** visualiza los informes generados más recientemente.

La pantalla proporciona el título de informe, la hora y fecha en que se ha generado el informe y el formato del informe.

Resumen del sistema

El elemento de panel de control **Resumen del sistema** proporciona un resumen de alto nivel de la actividad dentro las últimas 24 horas.

Dentro del elemento de resumen, puede ver la información siguiente:

- **Flujos actuales por segundo**: Visualiza la tasa de flujos por segundo.
- **Flujos (tras 24 horas)**: Visualiza el número total de flujos activos que se ven dentro de las últimas 24 horas.
- **Sucesos actuales por segundo**: Visualiza la tasa de sucesos por segundo.
- **Sucesos nuevos (pasadas 24 horas)**: Visualiza el número total de sucesos nuevos que se reciben dentro de las últimas 24 horas.
- **Delitos nuevos (pasadas 24 horas)**: Visualiza el número total de delitos que se han creado o modificado con evidencia nueva dentro de las últimas 24 horas.
- **Tasa de reducción de datos**: Visualiza la tasa de datos reducidos basados en el total de sucesos que se detectan dentro de las últimas 24 horas y el número de delitos modificados dentro de las últimas 24 horas.

Panel de control de supervisión de riesgos

Utilice el panel de control de **Supervisión de riesgos** para supervisar riesgos para activos, políticas y grupos de políticas.

De forma predeterminada, el panel de control **Supervisión de riesgos** muestra los elementos **Riesgo** y **Cambio de riesgo** que supervisan la puntuación de riesgo de política para activos pertenecientes a los grupos de políticas Vulnerabilidades altas, Vulnerabilidades medias y Vulnerabilidades bajas, así como las tasas de cumplimiento de políticas y cambios históricos en la puntuación de riesgo de política del grupo de políticas CIS.

Los elementos del panel de control Supervisión de riesgos no muestra ningún resultado a menos que se tenga una licencia de IBM Security QRadar Risk Manager. Para obtener más información, consulte la Guía del usuario de QRadar Risk Manager.

Para ver el panel de control predeterminado de **Supervisión de riesgos**, seleccione **Mostrar panel de control** > **Supervisión de riegos** en la pestaña **Panel de control**.

Tareas relacionadas:

"Supervisar el cumplimiento de políticas"
Puede crear un elemento de panel de control que muestra el nivel de cumplimiento de políticas y la puntuación de riesgo de política para activos, políticas y grupos de políticas seleccionados.

"Supervisar el cambio de riesgo" en la página 28
Puede crear un elemento de panel de control que muestra el cambio de riesgo de política para activos, políticas y grupos de políticas seleccionados para cada día, semana y mes.

Supervisar el cumplimiento de políticas

Puede crear un elemento de panel de control que muestra el nivel de cumplimiento de políticas y la puntuación de riesgo de política para activos, políticas y grupos de políticas seleccionados.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Panel de control nuevo**.
3. Escriba un nombre y una descripción para el panel de control de cumplimiento de políticas.
4. Pulse **Aceptar**.
5. En la barra de herramientas, seleccione **Añadir elemento** > **Gestor de riesgos** > **Riesgo**.

   Los elementos de panel de control del **Gestor de riesgos** se muestran solamente cuando IBM Security QRadar Risk Manager se utiliza con una licencia.
6. En la cabecera del elemento de panel de control nuevo, pulse el icono amarillo **Valores**.
7. Utilice las listas **Tipo de gráfico**, **Mostrar parte superior** y **Ordenar** para configurar el gráfico.
8. En la lista **Grupo**, seleccione el grupo que desee supervisar. Para obtener más información, consulte la tabla incluida en el paso 9.

   Cuando se selecciona la opción **Activo**, aparece un enlace a la página **Riesgos** > **Gestión de políticas** > **Por activo** en la parte inferior del elemento de panel de control **Riesgo**. En la página **Por activo** se muestra información más detallada sobre todos los resultados que se han devuelto para el valor de **Grupo de políticas** seleccionado. Para obtener más información sobre un activo concreto, seleccione **Tabla** en la lista **Tipo de gráfico** y pulse el enlace de la columna **Activo** para ver los detalles sobre el activo en la página **Por activo**.

   Cuando se selecciona la opción **Política**, aparece un enlace a la página **Riesgos** > **Gestión de políticas** > **Por política** en la parte inferior del elemento de panel de control **Riesgo**. En la página **Por política** se muestra información más detallada sobre todos los resultados que se han devuelto para el valor de **Grupo de políticas** seleccionado. Para obtener más información sobre una

política concreta, seleccione **Tabla** en la lista **Tipo de gráfico** y pulse el enlace de la columna **Política** para ver los detalles sobre la política en la página **Por política**.

9. En la lista **Gráfico**, seleccione el tipo de gráfico que desee utilizar. Para obtener más información, consulte la tabla siguiente:

Grupo	Porcentaje de activos aprobados	Porcentaje de controles de política aprobados	Porcentaje de grupos de políticas aprobados	Puntuación de riesgo de política
Todo	Devuelve el porcentaje promedio de cumplimiento para activos, políticas y el grupo de políticas.	Devuelve el porcentaje promedio de cumplimiento de controles de política para activos, políticas y el grupo de políticas.	Devuelve la tasa de cumplimiento promedio de grupo de políticas para todos los activos, políticas y el grupo de políticas.	Devuelve la puntuación de riesgo promedio de política para todos los activos, políticas y el grupo de políticas.
Activo	Indica si un activo ha pasado la prueba de conformidad de activo (100%=cumplimiento 0%=no cumplimiento). Utilice este valor para mostrar qué activos asociados a un grupo de políticas han pasado la prueba de conformidad.	Indica el porcentaje de controles de política que un activo ha superado. Utilice este valor para mostrar el porcentaje de controles de política que se han pasado para cada activo que está asociado al Grupo de políticas.	Muestra el porcentaje de subgrupos de políticas que están asociados al activo que ha pasado la prueba de conformidad.	Devuelve la suma de todos los valores de factor de importancia para cuestiones de política que están asociadas a cada activo. Utilice este valor para ver el riesgo de política para cada activo que está asociado a un grupo de políticas seleccionado.
Política	Indica si todos los activos asociados a cada política de un grupo de políticas han pasado la prueba de conformidad. Utilice este valor para supervisar si todos los activos asociados a cada política de un grupo de políticas pasan o no la prueba de conformidad.	Devuelve el porcentaje de controles de política superados por cada política del grupo de políticas. Utilice este valor para supervisar cuántos controles de política fallan para cada política.	Muestra el porcentaje de subgrupos de políticas de los cuales la política es una parte que pasa la prueba de conformidad.	Muestra los valores de factor de importancia para cada pregunta de política del grupo de políticas. Utilice este valor para ver el factor de importancia de cada política de un grupo de políticas.

Grupo	Porcentaje de activos aprobados	Porcentaje de controles de política aprobados	Porcentaje de grupos de políticas aprobados	Puntuación de riesgo de política
Grupo de políticas	Devuelve el porcentaje de activos que pasan la prueba de conformidad para el grupo de políticas global seleccionado.	Devuelve el porcentaje de controles de política que se pasan para cada política del grupo de políticas considerado globalmente.	Devuelve el porcentaje de subgrupos de políticas dentro del grupo de políticas que pasan la prueba de conformidad.	Devuelve la suma de todos los valores de factor de importancia para todas las preguntas de política del grupo de políticas.

10. En la lista **Grupo de políticas**, seleccione los grupos de políticas que desee supervisar.
11. Pulse **Guardar**.

Supervisar el cambio de riesgo

Puede crear un elemento de panel de control que muestra el cambio de riesgo de política para activos, políticas y grupos de políticas seleccionados para cada día, semana y mes.

Acerca de esta tarea

Utilice este elemento de panel de control para comparar los cambios en la puntuación de riesgo de política, controles de política y valores de política para un grupo de políticas a lo largo del tiempo.

El elemento de panel de control **Cambio de riesgo** utiliza flechas para indicar cuando un riesgo de política para valores seleccionados ha aumentado, disminuido o permanecido igual durante un periodo de tiempo seleccionado.

- Un número debajo de una flecha roja indica los valores que muestran un riesgo incrementado.
- Un número debajo de una flecha gris indica los valores para los que no ha habido cambio de riesgo.
- Un número debajo de una flecha verde indica los valores que muestran un riesgo decrementado.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En la barra de herramientas, pulse **Panel de control nuevo**.
3. Escriba un nombre y una descripción para el panel de control de cumplimiento de políticas histórico.
4. Pulse **Aceptar**.
5. En la barra de herramientas, seleccione **Añadir elemento** > **Gestor de riesgos** > **Cambio de riesgo**.

   Los elementos de panel de control del **Gestor de riesgos** se muestran solamente cuando IBM Security QRadar Risk Manager se utiliza con una licencia.
6. En la cabecera del elemento de panel de control nuevo, pulse el icono amarillo **Valores**.

7. En la lista **Grupo de políticas**, seleccione los grupos de políticas que desee supervisar.
8. Seleccione una opción en la lista **Valor para comparar**:
   - Si desea ver los cambios acumulativos en el factor de importancia para todas las preguntas de política dentro de los grupos de políticas seleccionados, seleccione **Puntuación de riesgo de política**.
   - Si desea ver cuántos controles de política han cambiado dentro de los grupos de políticas seleccionados, seleccione **Controles de política**.
   - Si desea ver cuántas políticas han cambiado dentro de los grupos de políticas seleccionados, seleccione **Políticas**.
9. Seleccione el período de cambio de riesgo que desee supervisar en la lista **Variación de tiempo**:
   - Si desea comparar cambios de riesgo de las 12:00 a.m. de hoy con los cambios de riesgo de ayer, seleccione **Día**.
   - Si desea comparar cambios de riesgo de las 12:00 a.m. del lunes de esta semana con los cambios de riesgo de la semana pasada, seleccione **Semana**.
   - Si desea comparar cambios de riesgo de las 12:00 a.m. del primer día del mes actual con los cambios de riesgo del mes pasado, seleccione **Mes**.
10. Pulse **Guardar**.

Elementos de Gestión de vulnerabilidades

Los elementos de panel de control Gestión de vulnerabilidades solo se visualizan cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se ha obtenido la licencia.

Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Puede visualizar un elemento de panel de control personalizado que se basa en criterios de búsqueda guardados desde la pestaña **Vulnerabilidades**. Los elementos de búsqueda se listan en el menú **Añadir elemento** > **Gestión de vulnerabilidades** > **Búsqueda de vulnerabilidades**. El nombre del elemento de búsqueda coincide con el nombre de los criterios de búsqueda guardada en los que se basa el elemento.

QRadar incluye criterios de búsqueda guardada predeterminados que se han preconfigurado para visualizar elementos de búsqueda en el menú de la **pestaña Panel de control**. Puede añadir más elementos de panel de control de búsqueda en el menú de la **pestaña Panel de control**.

Los tipos de gráfico soportados son tabla, circular y de barras. El tipo de gráfico predeterminado es el gráfico de barras. Estos gráficos se pueden configurar.

Notificación del sistema

El elemento de panel de control Notificación del sistema muestra notificaciones de sucesos recibidas por el sistema.

Para que las notificaciones se muestren en el panel de control **Notificación del sistema**, el administrador debe crear una regla que se base en cada tipo de mensaje de notificación y seleccione el recuadro de selección **Notificar** en el Asistente de reglas personalizadas.

Para obtener más información sobre cómo configurar notificaciones de sucesos y crear reglas de suceso, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

En el elemento de panel de control **Notificaciones del sistema**, puede ver la información siguiente:

- **Distintivo**: Visualiza un símbolo para indicar el nivel de gravedad de la notificación. Apunte al símbolo para ver más detalle sobre el nivel de gravedad.
  - Icono **Salud**
  - Icono **Información** (?)
  - Icono **Error** (X)
  - Icono **Aviso** (!)
- **Creado**: Visualiza la cantidad de tiempo transcurrido desde que se ha creado la notificación.
- **Descripción**: Visualiza información acerca de la notificación.
- **Icono Descartar (x)**: Le permitirá cerrar una notificación del sistema.

Puede apuntar el ratón sobre una notificación para ver más detalles:

- **IP de host**: Visualiza la dirección IP del host que ha originado la notificación.
- **Gravedad**: Visualiza el nivel de gravedad de la incidencia que ha creado esta notificación.
- **Categoría de nivel bajo**: Visualiza la categoría de bajo nivel que está asociada con el incidente que ha generado esta notificación. Por ejemplo: Interrupción de servicio.
- **Carga útil**: Visualiza el contenido de carga útil que está asociado con el incidente que ha generado esta notificación.
- **Creado**: Visualiza la cantidad de tiempo transcurrido desde que se ha creado la notificación.

Cuando se añade el elemento de panel de control **Notificaciones del sistema**, las notificaciones del sistema también se pueden visualizar como notificaciones emergentes en la interfaz de usuario de QRadar. Estas notificaciones emergentes se visualizan en la esquina inferior derecha de la interfaz de usuario, independientemente de la pestaña seleccionada.

Las notificaciones emergentes sólo están disponibles para los usuarios con permisos administrativos y están habilitadas de forma predeterminada. Para inhabilitar las notificaciones emergentes, seleccione **Preferencias de usuario** y borre el recuadro de selección **Habilitar notificaciones emergentes**.

En la ventana emergente Notificaciones del sistema, se resalta el número de notificaciones de la cola. Por ejemplo, si se visualiza (1 – 12) en la cabecera, la notificación actual es de 1 de 12 de notificaciones a visualizar.

La ventana emergente Notificación del sistema proporciona las opciones siguientes:

- **Icono Siguiente (>)**: Visualiza el siguiente mensaje de notificación. Por ejemplo, si el mensaje de notificación actual es 3 de 6, pulse el icono para ver 4 de 6.
- **Icono Cerrar (X)** : Cierra esta ventana emergente de notificación.
- **(detalles)**: Visualiza más información acerca de esta notificación del sistema.

Centro de información de amenazas de Internet

El elemento de panel de control Centro de información de amenazas de Internet es un canal de información RSS que le proporciona avisos sobre problemas de seguridad, evaluaciones diarias sobre amenazas, noticias relacionadas con la seguridad y repositorios de amenazas.

El diagrama Nivel de peligro actual indica el nivel de peligro actual y proporciona un enlace que conduce a la página Nivel de peligro actual en Internet, perteneciente al sitio web IBM Internet Security Systems.

El elemento de panel de control lista avisos actuales. Para ver un resumen del aviso, pulse el icono de **Flecha** situado junto al aviso. El aviso se expandirá para mostrar un resumen. Pulse de nuevo el icono de **Flecha** para ocultar el resumen.

Para investigar el aviso completo, pulse el enlace asociado. El sitio web IBM Internet Security Systems se abrirá en una ventana nueva del navegador para mostrar los detalles del aviso completo.

Crear un panel de control personalizado

Puede crear un panel de control personalizado para ver un grupo de elementos de panel de control que cumplen un requisito determinado.

Acerca de esta tarea

Después de crear un panel de control personalizado, el nuevo panel de control aparece en la pestaña **Panel de control** y en el cuadro de lista **Mostrar panel de control**. De forma predeterminada, un panel de control personalizado nuevo está vacío; por lo tanto, debe añadirle elementos.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. Pulse el icono **Panel de control nuevo**.
3. En el campo **Nombre**, escriba un nombre exclusivo para el panel de control. La longitud máxima es 65 caracteres.
4. En el campo **Descripción**, escriba una descripción del panel de control. La longitud máxima es de 255 caracteres. Esta descripción se muestra en la ayuda contextual para el nombre de panel de control en el cuadro de lista **Mostrar panel de control**.
5. Pulse **Aceptar**.

Utilización del panel de control para investigar actividad de registro o actividad de red

Los elementos de búsqueda de la pestaña de control proporcionan un enlace a los paneles **Actividad de registro** o **Actividad de red**, lo cual le permite investigar la actividad de registro o de red con más detalle.

Acerca de esta tarea

Para investigar flujos desde un elemento de panel de control de **Actividad de registro**:

1. Pulse el enlace **Vista en Actividad de registro**. Se abrirá la pestaña **Actividad de registro**, que muestra resultados y dos gráficos correspondientes a los parámetros del elemento de panel de control.

Para investigar flujos desde un elemento de panel de control de **Actividad de red**:

1. Pulse el enlace **Vista en Actividad de red**. Se abrirá la pestaña Actividad de red, que muestra resultados y dos gráficos correspondientes a los parámetros del elemento de panel de control.

Se abrirá la pestaña **Actividad de red**, que muestra resultados y dos gráficos correspondientes a los parámetros del elemento de panel de control. Los tipos de gráfico que aparecen en la pestaña **Actividad de registro** o **Actividad de red** dependen del gráfico que esté configurado en el elemento de panel de control:

Tipo de gráfico	Descripción
Barras, circular y de tabla	La pestaña **Actividad de registro** o **Actividad de red** muestra un gráfico de barras, un gráfico circular y una tabla de detalles de flujo.
Serie temporal	La pestaña **Actividad de registro** o **Actividad de red** muestra gráficos de acuerdo con los criterios siguientes: 1. Si el rango de tiempo que ha definido es menor o igual que 1 hora, se muestra un gráfico de serie temporal, un gráfico de barras y una tabla de detalles de suceso o de flujo. 2. Si el rango de tiempo que ha definido es mayor que 1 hora, se muestra un gráfico de serie temporal y puede pulsar Actualizar detalles. Esta acción inicia una búsqueda la cual proporciona los detalles del suceso o flujo y genera un gráfico de barras. Cuando la búsqueda finaliza, se muestran el gráfico de barras y una tabla de detalles de suceso o flujo.

Configuración de gráficos

Puede configurar elementos de los paneles de control **Actividad de registro**, **Actividad de red** y **Conexiones** para especificar el tipo de gráfico y cuántos objetos de datos desea ver.

Acerca de esta tarea

Tabla 11. Configuración de gráficos. Opciones de parámetros.

Opción	Descripción
Valor para gráfico	En el cuadro de lista, seleccione el tipo de objeto que desee representar en el gráfico. Las opciones incluyen todos los parámetros de suceso o de flujo normalizados y personalizados que se incluyen en los parámetros de búsqueda.

Tabla 11. Configuración de gráficos (continuación). Opciones de parámetros.

Opción	Descripción
Tipo de gráfico	En el cuadro de lista, seleccione el tipo de gráfico que desee ver. Las opciones son: 1. **Gráfico de barras**: muestra los datos en un gráfico de barras. Esta opción solo está disponible para sucesos o flujos agrupados. 2. **Gráfico circular**: muestra los datos en un gráfico circular. Esta opción solo está disponible para sucesos o flujos agrupados. 3. **Tabla**: muestra los datos en una tabla. Esta opción solo está disponible para sucesos o flujos agrupados. 4. **Serie temporal**: muestra un gráfico de líneas interactivo que representa los registros correspondientes a un intervalo de tiempo especificado.
Mostrar parte superior	En el cuadro de lista, seleccione el número de objetos que desee ver en el gráfico. Las opciones son **5** y **10**. El valor predeterminado es **10**.
Capturar datos de serie temporal	Seleccione esta casilla para habilitar la captura de series temporales. Cuando selecciona esta casilla, la función de representación gráfica comienza a acumular datos para gráficos de serie temporal. De forma predeterminada, esta opción está inhabilitada.
Rango de tiempo	En el cuadro de lista, seleccione el rango de tiempo que desee ver.

Las configuraciones para gráficos personalizados se conservan, por lo que se muestran como configurados cada vez que accede a la pestaña **Panel de control**.

Los datos se acumulan, por lo que cuando realiza una búsqueda guardada de serie temporal, existe una memoria caché de datos de suceso o de flujo para mostrar los datos correspondientes al periodo de tiempo anterior. Los parámetros acumulados se indican mediante un asterisco (*) en el cuadro de lista **Valor para gráfico**. Si selecciona un valor para representar gráficamente que no está acumulado (sin asterisco), no habrá datos de serie temporal disponibles.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el cuadro de lista **Mostrar panel de control**, seleccione el panel de control donde reside el elemento que desee personalizar.
3. En la cabecera del elemento de panel de control que desee configurar, pulse el icono **Valores**.
4. Configure los parámetros del gráfico.

Eliminación de elementos de panel de control

Puede eliminar elementos de un panel de control y añadir el elemento de nuevo en cualquier momento.

Acerca de esta tarea

Cuando se elimina un elemento del panel de control, el elemento no se elimina por completo.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control del que desea eliminar un elemento.
3. En la cabecera de elemento de panel de control, pulse el icono rojo [x] para eliminar el elemento del panel de control.

Desconexión de un elemento del panel de control

Puede desconectar un elemento del panel de control y visualizar el elemento en una ventana nueva en el sistema.

Acerca de esta tarea

Al desconectar un elemento de panel de control, el elemento de panel de control original permanece en la pestaña **Panel de control**, mientras que una ventana desconectada con un elemento de la pestaña de control duplicado permanece abierta y se renueva durante intervalos planificados. Si cierra la aplicación de QRadar, la ventana desconectada permanecerá abierta para supervisión y continúa renovándose hasta que se cierra manualmente la ventana o se cierra el sistema.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control del que desea desconectar un elemento.
3. En la cabecera de elemento de panel de control, pulse el icono verde para desconectar el elemento de panel de control y abrirlo en una ventana independiente.

Renombrar un panel de control

Puede renombrar un panel de control y actualizar la descripción.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control que desea editar.
3. En la barra de herramientas, pulse el icono **Renombrar panel de control** .
4. En el campo **Nombre**, escriba un nuevo nombre para el panel de control. La longitud máxima es de 65 caracteres.
5. En el campo **Descripción**, escriba una nueva descripción del panel de control. La longitud máxima es de 255 caracteres
6. Pulse **Aceptar**.

Supresión de un panel de control

Puede suprimir un panel de control.

Acerca de esta tarea

Después de suprimir un panel de control, la pestaña **Panel de control** se renueva y se visualiza el primer panel de control que se lista en el recuadro de lista **Mostrar panel de control**. El panel de control que ha suprimido ya no se visualiza en el recuadro de lista **Mostrar panel de control**.

Procedimiento

1. Pulse la pestaña **Panel de control**.
2. En el recuadro de lista **Mostrar panel de control**, seleccione el panel de control que desea suprimir.
3. En la barra de herramientas, pulse **Suprimir panel de control**.
4. Pulse **Sí**.

Gestión de notificaciones del sistema

Puede especificar el número de notificaciones que desea visualizar en el elemento de panel de control **Notificación del sistema** y cerrar las notificaciones del sistema después de leerlas.

Antes de empezar

Asegúrese de que el elemento de panel de control **Notificación del sistema** se añade al panel de control.

Procedimiento

1. En la cabecera de elemento de panel de control Notificación del sistema, pulse el icono **Valores**.
2. En el recuadro de lista **Visualizar**, seleccione el número de notificaciones de sistema que desea ver.
   - Las opciones son **5**, **10** (valor predeterminado), **20**, **50** y **Todos**.
   - Para ver todas las notificaciones del sistema que se han registrado en las últimas 24 horas, pulse **Todos**.
3. Para cerrar una notificación del sistema, pulse el icono **Suprimir**.

Adición de elementos de panel de control basados en búsqueda a la lista de adición de elementos

Puede añadir elementos de panel de control basados en búsqueda al menú **Añadir elementos**.

Antes de empezar

Para añadir un elemento de panel de control de búsqueda de sucesos y flujos al menú **Añadir elemento** en la pestaña **Panel de control**, debe acceder a la pestaña **Actividad de registro** o **Actividad de red** para crear criterios de búsqueda que especifiquen que los resultados de búsqueda se pueden visualizar en la pestaña **Panel de control**. Los criterios de búsqueda también deben especificar que los resultados se agrupen en un parámetro.

Procedimiento

1. Elija:
   - Añadir un elemento de panel de control de búsqueda de flujos, pulse la pestaña **Actividad de red**.
   - Para añadir un elemento de panel de control de búsqueda de sucesos, pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, elija una de las opciones siguientes:
   - Para crear una búsqueda, seleccione **Nueva búsqueda**.
   - Para editar una búsqueda guardada, seleccione **Editar búsqueda**.
3. Configure o edite los parámetros de búsqueda, según sea necesario.
   - En el panel Editar búsqueda, seleccione la opción **Incluir en Panel de control**.
   - En el panel Definición de columna, seleccione una columna y pulse el icono **Añadir columna** para mover la columna a la lista **Agrupar por**.
4. Pulse **Filtro**. Se visualizan los resultados de búsqueda.
5. Pulse **Guardar criterios**. Consulte Guardar criterios de búsqueda en la pestaña Delito.
6. Pulse **Aceptar**.
7. Verifique que los criterios de búsqueda guardados han añadido satisfactoriamente el elemento de panel de control de búsqueda de sucesos o flujos a la lista de **Añadir elementos**
   a. Pulse la pestaña **Panel de control**.
   b. Elija una de las siguientes opciones:
   a. Para verificar un elemento de búsqueda de sucesos, seleccione **Añadir elemento** > **Actividad de registro** > **Búsquedas de suceso** > **Añadir elemento**.
   b. Para verificar un elemento de búsqueda de flujo, seleccione **Añadir elemento** > **Actividad de red** > **Búsquedas de flujo**. El elemento de panel de control se visualiza en la lista con el mismo nombre que los criterios de búsqueda guardados.

Capítulo 4. Gestión de delitos

Se pueden establecer correlaciones entre sucesos y flujos que tienen direcciones IP de destino que están situadas en diversas redes dentro del mismo delito. Puede investigar de forma efectiva cada delito en la red.

Restricción: No puede gestionar delitos en IBM Security QRadar Log Manager. Para obtener más información sobre las diferencias entre IBM Security QRadar SIEM y IBM Security QRadar Log Manager, consulte "Prestaciones de su producto de inteligencia y seguridad" en la página 5.

Puede navegar por las distintas páginas de la pestaña **Delitos** para investigar detalles de sucesos y de flujos a fin de determinar los sucesos y flujos que han provocado el delito.

Visión general de los delitos

Desde la pestaña **Delitos**, puede investigar delitos, direcciones IP de origen y de destino, comportamientos de red y anomalías de la red.

También puede buscar delitos que están basados en diversos criterios. Para obtener más información sobre la búsqueda de delitos, consulte "Búsquedas de delitos" en la página 183.

Consideraciones sobre los permisos para delitos

Todos los usuarios pueden ver todos los delitos independientemente de qué origen de registro o qué origen de flujo esté asociado con el delito.

La pestaña **Delitos** no utiliza permisos de usuario a nivel de dispositivo para determinar qué delitos puede ver cada usuario de acuerdo con lo determinado por los permisos de red.

Para obtener más información sobre los permisos a nivel de dispositivo, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Términos clave

Desde la pestaña **Delitos**, puede acceder y analizar delitos, direcciones IP de origen y direcciones IP de destino.

Elemento	Descripción
Delitos	Un delito incluye varios sucesos o flujos que provienen de un mismo origen, tal como un host u origen de registro. La pestaña **Delitos** muestra los delitos, que incluyen el tráfico y las vulnerabilidades que trabajan conjuntamente y validan la magnitud de un delito. La magnitud de un delito está determinada por varias pruebas que se realizan en el delito cada vez que se vuelve a evaluar. La reevaluación se produce cuando se añaden sucesos al delito y a intervalos planificados.

© Copyright IBM Corp. 2012, 2015

Elemento	Descripción
Direcciones IP de origen	Una dirección IP de origen especifica el dispositivo que intenta violar la seguridad de un componente de la red. Una dirección IP de origen puede utilizar diversos métodos de ataque, tales como ataques de reconocimiento o de denegación de servicio, para intentar el acceso no autorizado.
Direcciones IP de destino	Una dirección IP de destino especifica el dispositivo de red al que intenta acceder una dirección IP de origen.

Retención de delitos

En la pestaña **Admin**, puede definir valores del sistema para el periodo de retención de delitos para eliminar delitos de la base de datos una vez transcurrido un periodo de tiempo definido.

El periodo predeterminado de retención de delitos es tres días. Debe tener permiso administrativo para acceder a la pestaña **Admin** y definir valores del sistema. Cuando define valores umbrales, se añaden cinco días al valor umbral definido.

Cuando cierra un delito, se elimina de la base de datos una vez transcurrido el periodo de retención de delitos. Si se producen más sucesos para un delito, se crea un nuevo delito. Si realiza una búsqueda que incluye delitos cerrados, el elemento se visualiza en los resultados de búsqueda si no se ha eliminado de la base de datos.

Supervisión de delitos

Mediante las diferentes vistas disponibles en la pestaña **Delitos**, puede supervisar delitos para determinar qué delitos se están produciendo actualmente en la red.

Los delitos aparecen listados con el delito de mayor magnitud en primer lugar. Puede localizar y ver los detalles de un delito determinado y luego realizar una acción sobre el delito, si es necesario.

Después de iniciar la navegación por las diversas vistas, la parte superior de la pestaña muestra la ruta de navegación que conduce hasta la vista actual. Si desea volver a una página visualizada anteriormente, pulse el nombre de la página en la ruta de navegación.

Desde el menú de navegación de la pestaña **Delitos**, puede acceder a las páginas que aparecen listadas en la tabla siguiente.

Tabla 12. Páginas a las que se puede acceder desde la pestaña **Delitos**

Página	Descripción
Mis delitos	Muestra todos los delitos que tiene asignados.
Todos los delitos	Muestra todos los delitos globales existentes en la red.
Por categoría	Muestra todos los delitos agrupados de acuerdo con las categorías de alto nivel y de bajo nivel.

Tabla 12. Páginas a las que se puede acceder desde la pestaña **Delitos** *(continuación)*

Página	Descripción
Por IP de origen	Muestra todos los delitos agrupados de acuerdo con las direcciones IP de origen que intervienen en un delito.
Por IP de destino	Muestra todos los delitos agrupados de acuerdo con las direcciones IP de destino que intervienen en un delito.
Por red	Muestra todos los delitos agrupados de acuerdo con las redes que intervienen en un delito.
Reglas	Proporciona acceso a la página Reglas, donde puede ver y crear reglas personalizadas. Esta opción sólo se muestra si tiene el permiso de rol Ver reglas personalizadas. Para obtener más información, consulte Gestión de reglas.

Supervisar delitos en las páginas Todos los delitos o Mis delitos

Puede supervisar delitos en las páginas Todos los delitos o Mis delitos

Antes de empezar

La página Todos los delitos muestra una lista de todos los delitos que se están produciendo en la red. La página Mis delitos muestra una lista de delitos que están asignados al usuario.

Acerca de esta tarea

La parte superior de la tabla muestra los detalles de los parámetros de búsqueda de delitos, si los hay, que se aplican a los resultados de la búsqueda. Para borrar esos parámetros de búsqueda, pulse **Borrar filtro**. Para obtener más información sobre la búsqueda de delitos, consulte Búsquedas de delitos.

Nota: Para ver con mayor detalle un panel en la página de resumen, pulse en la opción correspondiente de la barra de herramientas. Por ejemplo, si desea ver los detalles de las direcciones IP de origen, pulse **Orígenes**. Para obtener más información sobre las opciones de la barra de herramientas, consulte Funciones de la barra de herramientas de la pestaña Delitos.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, seleccione **Todos los delitos** o **Mis delitos**.
3. Puede refinar la lista de delitos mediante las opciones siguientes:
   - En el cuadro de lista **Ver delitos**, seleccione una opción para filtrar la lista de delitos para un intervalo de tiempo determinado.
   - Pulse el enlace **Borrar filtro** situado junto a cada filtro que aparece en el panel **Parámetros de búsqueda actuales**.
4. Efectúe una doble pulsación en el delito que desee ver.
5. En la página Resumen de delito, revise los detalles del delito. Consulte Parámetros de delito.

6. Realice las acciones necesarias sobre el delito.

Supervisar delitos agrupados por categoría

Puede supervisar delitos en la página Por detalles de categoría, que proporciona una lista de delitos que están agrupados en la categoría de nivel alto.

Acerca de esta tarea

Los campos de recuento, tales como **Recuento de sucesos**, **Recuento de flujos** y **Recuento de orígenes** no tienen en cuenta los permisos de red del usuario.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Por categoría**.
3. Para ver los grupos de categoría de nivel bajo para una categoría de nivel alto, pulse el icono de flecha situado junto al nombre de la categoría de nivel alto.
4. Para ver una lista de delitos para una categoría de nivel bajo, haga una doble pulsación en la categoría de nivel bajo.
5. Efectúe una doble pulsación en el delito que desee ver.
6. En la página Resumen de delito, revise los detalles del delito. Consulte Parámetros de delito.
7. Realice las acciones necesarias sobre el delito. Consulte Tareas de gestión de delitos.

Supervisar delitos agrupados por IP de origen

En la página Origen, puede supervisar delitos que están agrupados por dirección IP de origen.

Acerca de esta tarea

Una dirección IP de origen especifica el host que ha generado delitos como resultado de un ataque al sistema. Se listan todas las direcciones IP de origen con la magnitud más alta en primer lugar. La lista de delitos solo muestra las direcciones IP de origen con delitos activos.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Por IP de origen**.
3. Puede refinar la lista de delitos utilizando las opciones siguientes:
   - En el cuadro de lista **Ver delitos**, seleccione una opción para filtrar la lista de delitos para un intervalo de tiempo determinado.
   - Pulse el enlace **Borrar filtro** situado junto a cada filtro que aparece en el panel **Parámetros de búsqueda actuales**.
4. Efectúe una doble pulsación en el grupo que desee ver.
5. Para ver una lista de direcciones IP de destino locales para la dirección IP de origen, pulse **Destinos** en la barra de herramientas de página Origen.
6. Para ver una lista de delitos que están asociados a una dirección IP de origen, pulse **Delitos** en la barra de herramientas de la página Origen.
7. Efectúe una doble pulsación en el delito que desee ver.
8. En la página Resumen de delito, revise los detalles del delito. Consulte Parámetros de delito.

9. Realice las acciones necesarias sobre el delito. Consulte Tareas de gestión de delitos.

Supervisar delitos agrupados por IP de destino

En la página Destinos, puede supervisar delitos que están agrupados por direcciones IP de destino locales.

Acerca de esta tarea

Se listan todas las direcciones IP de destino con la magnitud más alta en primer lugar.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Por IP de destino**.
3. Puede refinar la lista de delitos utilizando las opciones siguientes:
   - En el cuadro de lista **Ver delitos**, seleccione una opción para filtrar la lista de delitos para un intervalo de tiempo determinado.
   - Pulse el enlace **Borrar filtro** situado junto a cada filtro que aparece en el panel **Parámetros de búsqueda actuales**.
4. Efectúe una doble pulsación en la dirección IP de destino que desee ver.
5. Para ver una lista de delitos que están asociados a una dirección IP de destino, pulse **Delitos** en la barra de herramientas de la página Destino.
6. Para ver una lista de direcciones IP de origen que están asociadas a una dirección IP de destino, pulse **Orígenes** en la barra de herramientas de la página Destino.
7. Efectúe una doble pulsación en el delito que desee ver.
8. En la página Resumen de delito, revise los detalles del delito. Consulte Parámetros de delito.
9. Realice las acciones necesarias sobre el delito. Consulte Tareas de gestión de delitos.

Supervisar delitos agrupados por red

En la página Redes, puede supervisar delitos que están agrupados por red.

Acerca de esta tarea

Se listan todas las redes con la magnitud más alta en primer lugar.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Por red**.
3. Efectúe una doble pulsación en la red que desee ver.
4. Para ver una lista de direcciones IP de origen que están asociadas a la red, pulse **Orígenes** en la barra de herramientas de la página Red.
5. Para ver una lista de direcciones IP de destino que están asociadas a la red, pulse **Destinos** en la barra de herramientas de la página Red.
6. Para ver una lista de delitos que están asociados a la red, pulse **Delitos** en la barra de herramientas de la página Red.
7. Efectúe una doble pulsación en el delito que desee ver.

8. En la página Resumen de delito, revise los detalles del delito. Consulte Parámetros de delito.
9. Realice las acciones necesarias sobre el delito. Consulte Tareas de gestión de delitos.

Tareas de gestión de delitos

Puede realizar acciones sobre un delito para supervisarlo.

Puede realizar las acciones siguientes:

- Añadir notas
- Eliminar delitos
- Proteger delitos
- Exportar datos de delito a XML o CSV
- Asignar delitos a otros usuarios
- Enviar notificaciones por correo electrónico
- Marcar un delito para su seguimiento
- Ocultar o cerrar un delito en una lista de delitos cualquiera

Para realizar una acción sobre varios delitos, pulse y mantenga pulsada la tecla Control mientras selecciona los delitos que desee. Para ver detalles de delito en una página nueva, mantenga pulsada la tecla Control mientras hace una doble pulsación en un delito.

Añadir notas

Puede añadir notas a cualquier delito en la pestaña **Delitos**. Las notas pueden incluir cualquier información que desee capturar para el delito, tal como un número de incidencia del servicio de soporte al cliente o información de gestión de delitos.

Acerca de esta tarea

Las notas pueden incluir un máximo de 2000 caracteres.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Navegue hasta el delito al cual desee añadir notas.
3. Efectúe una doble pulsación en el delito.
4. En el cuadro de lista **Acciones**, seleccione **Añadir nota**.
5. Escriba la nota que desee incluir para el delito.
6. Pulse **Añadir nota**.

Resultados

La nota aparecerá en el panel Últimas 5 notas del Resumen de delitos. Se mostrará un icono de **Notas** en la columna Distintivo de la lista **Delitos**. Coloque el puntero del ratón sobre el indicador de notas en la columna **Distintivo** de la lista **Delitos** para ver la nota correspondiente al delito.

Ocultar delitos

Para impedir que un delito se muestre en la pestaña **Delitos**, puede ocultar el delito.

Acerca de esta tarea

Cuando oculta un delito, deja de aparecer en todas las listas (por ejemplo, Todos los delitos) de la pestaña **Delitos**, pero si realiza una búsqueda que incluye delitos ocultos, éstos se mostrarán en los resultados de la búsqueda.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.
3. Seleccione el delito que desee ocultar.
4. En el cuadro de lista **Acciones**, seleccione **Ocultar**.
5. Pulse **Aceptar**.

Mostrar delitos ocultos

Los delitos ocultos no son visibles en la pestaña **Delitos**, pero los puede visualizar si desea verlos de nuevo.

Acerca de esta tarea

Para mostrar delitos ocultos, debe realizar una búsqueda que incluya delitos ocultos. Los resultados de la búsqueda incluyen todos los delitos, incluidos delitos ocultos y no ocultos. Los delitos se identifican como ocultos mediante el icono **Oculto** en la columna **Distintivo**.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.
3. Busque delitos ocultos:
   a. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
   b. En la lista **Excluir opción** del panel Parámetros de búsqueda, desmarque la casilla **Delitos ocultos**.
   c. Pulse **Buscar**.
4. Localice y seleccione el delito oculto que desee mostrar.
5. En el cuadro de lista **Acciones**, seleccione **Mostrar**.

Cerrar delitos

Para eliminar un delito completamente del sistema, puede cerrar el delito.

Acerca de esta tarea

Cuando cierra (suprime) un delito, deja de aparecer en todas las listas (por ejemplo, Todos los delitos) de la pestaña **Delitos**. Los delitos cerrados se eliminan de la base de datos una vez transcurrido el periodo de retención del delito. El periodo predeterminado de retención de delitos es tres días. Si se producen más sucesos para un delito, se crea un nuevo delito. Si realiza una búsqueda que incluye delitos cerrados, el elemento se visualiza en los resultados de búsqueda si no se ha eliminado de la base de datos.

Cuando cierra un delito, debe seleccionar una razón para hacerlo y puede añadir una nota. El campo **Notas** muestra la nota que se ha entrado para el cierre de delito anterior. Las notas pueden tener un máximo de 2.000 caracteres. La nota se muestra en el panel Notas del delito. Si tiene permiso para Gestionar el cierre de delitos, puede añadir nuevas razones personalizadas al cuadro de lista **Razón del cierre**.

Para obtener más información, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.
3. Elija una de las siguientes opciones:
   - Seleccione el delito que desee cerrar y seleccione **Cerrar** en el cuadro de lista **Acciones**.
   - En el cuadro de lista **Acciones**, seleccione **Cerrar listados**.
4. En el cuadro de lista **Razón del cierre**, seleccione una razón. La razón predeterminada es **Irrelevante**.
5. Opcional. En el campo **Notas**, escriba una nota para proporcionar más información sobre el cierre de la nota.
6. Pulse **Aceptar**.

Resultados

Después de cerrar los delitos, los recuentos que se muestran en la página Por categoría de la pestaña **Delitos** pueden tardar varios minutos en reflejar los delitos cerrados.

Proteger delitos

Puede impedir que se eliminen delitos de la base de datos para los que el periodo de retención ha concluido.

Acerca de esta tarea

Los delitos se retienen durante un período de retención configurable. El período de retención predeterminado es tres días, pero el administrador puede personalizar el periodo de retención. Puede haber delitos que desee conservar sin importar su periodo de retención. Puede impedir que se eliminen delitos de la base de datos para los que el periodo de retención ha concluido.

Para obtener más información sobre el período de retención de delitos, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

PRECAUCIÓN:
Cuando el modelo de datos SIM se inicializa mediante la opción Limpieza total, todos los delitos, incluidos los delitos protegido, se eliminan de la base de datos y del disco. Debe tener privilegios administrativos para inicializar el modelo de datos SIM.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.

3. Elija una de las siguientes opciones:
   - Seleccione el delito que desee proteger y luego seleccione **Proteger** en el cuadro de lista **Acciones**.
   - En el cuadro de lista **Acciones**, seleccione **Proteger listados**.
4. Pulse **Aceptar**.

Resultados

El delito protegido está indicado por un icono **Protegido** en la columna **Distintivo**.

Desproteger delitos

Puede desproteger delitos que anteriormente se habían protegido para impedir que se eliminaran una vez transcurrido su periodo de retención.

Acerca de esta tarea

Para listar solamente delitos protegidos, puede realizar una búsqueda que aplica filtros para obtener solamente delitos protegidos. Si desmarca la casilla **Protegido** y están seleccionadas todas las demás opciones de la lista **Excluye la opción** en el panel Parámetros de búsqueda, sólo se visualizan delitos protegidos.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.
3. Opcional. Realice una búsqueda que muestra solamente delitos protegidos.
4. Elija una de las siguientes opciones:
   - Seleccione el delito que desee desproteger y luego seleccione **Desproteger** en el cuadro de lista Acciones.
   - En el cuadro de lista **Acciones**, seleccione **Desproteger listados**.
5. Pulse **Aceptar**.

Exportar delitos

Puede exportar delitos en formato XML (Extensible Markup Language) o CSV (comma-separated values).

Acerca de esta tarea

Si desea reutilizar o almacenar datos de delito, puede exportar delitos. Por ejemplo, puede exportar delitos para crear informes no basados en el producto QRadar. Puede también exportar delitos como estrategia secundaria de retención a largo plazo. El servicio de soporte al cliente puede solicitarle que exporte delitos con fines de resolución de problemas.

El archivo XML o CSV resultante incluye los parámetros que están especificados en el panel Definición de columnas de los parámetros de búsqueda. El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Todos los delitos**.
3. Seleccione el delito que desee exportar.

4. Elija una de las siguientes opciones:
   - Para exportar delitos en formato XML, seleccione **Acciones** > **Exportar a XML** en el cuadro de lista Acciones.
   - Para exportar delitos en formato CSV, seleccione **Acciones** > **Exportar a CSV** en el cuadro de lista Acciones.
5. Elija una de las siguientes opciones:
   - Para abrir la lista para verla de inmediato, seleccione la opción **Abrir con** y seleccione una aplicación en el cuadro de lista.
   - Para guardar la lista, seleccione la opción **Guardar en disco**.
6. Pulse **Aceptar**.

Asignar delitos a usuarios

Desde la pestaña **Delitos**, puede asignar delitos a usuarios con fines de investigación.

Acerca de esta tarea

Cuando un delito está asignado a un usuario, el delito se muestra en la página Mis delitos perteneciente a ese usuario. Debe tener privilegios apropiados para asignar delitos a usuarios.

Puede asignar delitos a usuarios desde las páginas **Delitos** o Resumen de delitos. Este procedimiento proporciona instrucciones sobre cómo asignar delitos desde la pestaña **Delitos**.

Nota: El cuadro de lista **Nombre de usuario** sólo mostrará los usuarios que tienen privilegios para la pestaña **Delitos** .

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Todos los delitos**.
3. Seleccione el delito que desee asignar.
4. En el cuadro de lista **Acciones**, seleccione **Asignar**.
5. En el cuadro de lista **Nombre de usuario**, seleccione el usuario que desee asignar al delito.
6. Pulse **Guardar**.

Resultados

El delito se asignará al usuario seleccionado. Se mostrará el icono de **Usuario** en la columna Distintivo de la pestaña **Delitos** para indicar que el delito está asignado. El usuario designado podrá ver el delito en la página Mis delitos.

Enviar notificación de correo electrónico

Puede enviar un correo electrónico que contiene un resumen de delito a cualquier dirección de correo electrónico válida.

Acerca de esta tarea

El cuerpo del mensaje de correo electrónico incluye la información siguiente, si está disponible:

- Dirección IP origen

- Nombre de usuario de origen, nombre de host o nombre de activo
- Número total de orígenes
- Cinco primeros orígenes por magnitud
- Redes de origen
- Dirección IP destino
- Nombre de usuario de destino, nombre de host o nombre de activo
- Número total de destinos
- Cinco primeros destinos por magnitud
- Redes de destino
- Número total de sucesos
- Delito o suceso que ha provocado la activación de la regla de delito o suceso
- Descripción completa de la regla de delito o suceso
- ID de delito
- Cinco primeras categorías
- Hora de inicio del delito u hora en que se creó suceso
- Cinco primeras anotaciones
- Enlace a la interfaz de usuario del delito
- Reglas de CRE que intervienen

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Acceda al delito para el cual desee enviar una notificación de correo electrónico.
3. Efectúe una doble pulsación en el delito.
4. En el cuadro de lista **Acciones**, seleccione **Enviar por correo electrónico**.
5. Configure los parámetros siguientes:

Opción	**Descripción**
Parámetro	Descripción
Para	Escriba la dirección de correo electrónico del usuario al que desee informar si se produce un cambio en el delito seleccionado. Utilice una coma para separar las direcciones de correo electrónico.
De	Escriba la dirección de correo electrónico de origen predeterminada. La dirección predeterminada es root@localhost.com.
Asunto de correo electrónico	Escriba el asunto predeterminado para el correo electrónico. El asunto predeterminado es el ID de delito.
Mensaje de correo electrónico	Escriba el mensaje estándar que desea acompañar al correo electrónico de notificación.

6. Pulse **Enviar**.

Marcar un elemento para su seguimiento

Mediante la pestaña **Delitos**, puede marcar un delito, una dirección IP de origen, una dirección IP de destino y una red para su seguimiento. Esto le permitirá hacer un seguimiento de un elemento determinado para realizar una investigación adicional.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Acceda al delito que desee marcar para su seguimiento.
3. Efectúe una doble pulsación en el delito.
4. En el cuadro de lista **Acciones**, seleccione **Seguimiento**.

Resultados

El delito ahora mostrará un distintivo en la columna **Distintivos**, que indica el delito está marcado para su seguimiento. Si no ve el delito marcado en la lista de delitos, puede ordenar la lista para que muestre en primer lugar los delitos marcados. Para ordenar una lista de delitos de acuerdo con los delitos marcados, haga una doble pulsación en la cabecera de columna **Distintivos**.

Funciones de la barra de herramientas de la pestaña Delitos

Cada página y tabla de la pestaña **Delitos** tiene una barra de herramientas que le proporciona las funciones necesarias para realizar determinadas acciones o para investigar los factores que contribuyen a un delito.

Tabla 13. Funciones de la barra de herramientas de la pestaña Delitos

Función	Descripción
Añadir nota	Pulse **Añadir nota** para añadir una nota nueva a un delito. Esta opción sólo está disponible en los últimos 5 paneles de Notas de la página Resumen de delitos

Tabla 13. Funciones de la barra de herramientas de la pestaña Delitos (continuación)

Función	Descripción
Acciones	Las opciones disponibles en el cuadro de lista **Acciones** varían dependiendo de la página, tabla o elemento (tal como un delito o dirección IP de origen). El cuadro de lista **Acciones** pueden no aparecer exactamente tal como se indican a continuación. En el cuadro de lista **Acciones**, puede elegir una de las acciones siguientes: • **Seguimiento**: seleccione esta opción para marcar un elemento para su seguimiento posterior. Consulte Marcar un elemento para seguimiento. • **Ocultar**: seleccione esta opción para ocultar un delito. Para obtener más información sobre la ocultación de delitos, consulte Ocultar delitos. • **Mostrar**: seleccione esta opción para mostrar todos los delitos ocultos. • **Proteger delito**: seleccione esta opción para proteger un delito. Para obtener más información sobre la protección de delitos, consulte Proteger delitos. • **Cerrar**: seleccione esta opción para cerrar un delito. Para obtener más información sobre el cierre de delitos, consulte Cerrar delitos. • **Cerrar listados**: seleccione esta opción para cerrar el delito listado. Para obtener más información sobre el cierre de delitos listados, consulte Cerrar delitos. • **Correo electrónico**: seleccione esta opción para enviar por correo electrónico un resumen de delito a uno o varios destinatarios. Consulte Enviar notificación por correo electrónico. • **Añadir nota**: seleccione esta opción para añadir notas a un elemento. Consulte Añadir notas. • **Asignar**: seleccione esta opción para asignar un delito a un usuario. Consulte Asignar delitos a usuarios. • **Imprimir**: seleccione esta opción para imprimir un delito.
Anotaciones	Pulse **Anotaciones** para ver todas las anotaciones de un delito. • **Anotación**: especifica los detalles de la anotación. Las anotaciones son descripciones de texto que pueden ser añadidas automáticamente por una regla a un delito como parte de la respuesta de la regla. • **Hora**: especifica la fecha y hora en que se creó la anotación.

Tabla 13. Funciones de la barra de herramientas de la pestaña Delitos (continuación)

Función	Descripción
Anomalía	Pulse **Anomalía** para mostrar los resultados de búsqueda guardada que han hecho que la regla de detección de anomalías genere el delito. **Nota:** Este botón sólo se muestra si el delito ha sido generado por una regla de detección de anomalías.
Categorías	Pulse **Categorías** para ver información sobre categorías para el delito. Para investigar más los sucesos que están relacionados con una categoría específica, también puede pulsar el botón derecho del ratón en una categoría y seleccionar **Sucesos** o **Flujos**. Como alternativa, puede resaltar la categoría y pulsar el icono **Sucesos** o **Flujos** en la barra de herramientas de Lista de categorías de sucesos.
Conexiones	Pulse **Conexiones** para investigar más las conexiones. **Nota:** Esta opción solo está disponible si ha adquirido IBM Security QRadar Risk Manager y ha obtenido una licencia para ese producto. Para obtener más información, consulte el manual *IBM Security QRadar Risk Manager Guía del usuario*. Cuando pulsa el icono **Conexiones**, la página de criterios de búsqueda de conexiones se abre en una página nueva, y aparece rellenada con criterios de búsqueda de sucesos. Si es necesario, puede personalizar los parámetros de búsqueda. Pulse **Buscar** para ver la información de conexión.
Destino	Pulse **Destinos** para ver todas las direcciones IP de destino locales correspondientes a un delito, dirección IP de origen, o red. **Nota:** Si las direcciones IP de destino son remotas, se abre una página nueva que proporciona información sobre las direcciones IP de destino remotas.
Visualizar	La página Resumen de delitos muestra muchas tablas de información que está relacionada con un delito. Para localizar una tabla, puede desplazarse hasta a tabla que desee ver o seleccionar la opción en el cuadro de lista **Visualizar**.
Sucesos	Pulse **Sucesos** para ver todos los sucesos de un delito. Cuando pulsa **Sucesos**, se muestran los resultados de búsqueda de sucesos.

Tabla 13. Funciones de la barra de herramientas de la pestaña Delitos (continuación)

Función	Descripción
Flujos	Pulse **Flujos** para investigar los flujos que están asociados con un delito. Cuando pulsa **Flujos**, se muestran los resultados de búsqueda de Flujos.
Orígenes de registro	Pulse **Orígenes de registro** para ver todos los orígenes de registro para un delito.
Redes	Pulse **Redes** para ver todas las redes de destino para un delito.
Notas	Pulse **Notas** para ver todas las notas para un delito, dirección IP de origen, dirección IP de destino o red. Para obtener más información sobre las notas, consulte Añadir notas.
Delitos	Pulse **Delitos** para ver una lista de delitos que están asociados con una dirección IP de origen, dirección IP de destino o red.
Imprimir	Pulse **Imprimir** para imprimir un delito.
Reglas	Pulse **Reglas** para ver todas las reglas que han contribuido a un delito. La regla por la que se ha creado el delito aparece listada en primer lugar. Si tiene los permisos apropiados para editar una regla, haga una doble pulsación en la regla para abrir la página Editar reglas. Si la regla se ha suprimido, aparece un icono rojo (x) junto a la regla. Si realiza una doble pulsación en una regla suprimida, aparece un mensaje para indicar que la regla ya no existe.
Guardar criterios	Después de realizar una búsqueda de delitos, pulse **Guardar criterios** para guardar los criterios de búsqueda para su uso futuro.
Guardar diseño	De forma predeterminada, la página Por detalles por categoría se ordena de acuerdo con el parámetro Recuento de delitos. Si cambia el orden de clasificación u ordena de acuerdo con un parámetro diferente, pulse **Guardar diseño** para guardar la imagen mostrada actualmente como vista predeterminada. La próxima vez que inicie una sesión en la pestaña **Delitos**, se mostrará el diseño guardado.

Tabla 13. Funciones de la barra de herramientas de la pestaña Delitos (continuación)

Función	Descripción
Buscar	Esta opción solo está disponible en la barra de herramientas de la tabla Destinos locales. Pulse **Buscar** para filtrar la dirección IP de destino para un dirección IP de origen. Para filtrar destinos: 1. Pulse **Buscar**. 2. Escriba valores para los parámetros siguientes: • **Red de destino**: en el cuadro de lista, seleccione la red que desee filtrar. • **Magnitud**: en el cuadro de lista, seleccione si desea filtrar para una magnitud que sea Igual que, Menor que, o Mayor que el valor configurado. • **Ordenar por**: en el cuadro de lista, seleccione cómo desea ordenar los resultados del filtro. 3. Pulse **Buscar**.
Mostrar categorías inactivas	En la página de detalles Por categoría, los recuentos de cada categoría se acumulan a partir de los valores de las categorías de nivel inferior. Las categorías de nivel inferior que tienen delitos asociados se muestran con una flecha. Puede pulsar en la flecha para ver las categorías de nivel inferior asociadas. Si desea ver todas las categorías, pulse **Mostrar categorías inactivas**.
Orígenes	Pulse **Orígenes** para ver todas las direcciones IP de origen para el delito, dirección IP de destino, o red.
Resumen	Si ha pulsado en una opción desde el cuadro de lista **Visualizar**, puede pulsar **Resumen** para volver a la vista de resumen detallada.
Usuarios	Pulse **Usuarios** para ver todos los usuarios que están asociados con un delito.
Ver vía de ataque	Pulse **Ver vía de ataque** para investigar más la vía de ataque de un delito. Cuando pulsa el icono **Ver vía de ataque**, se abre el panel Topología actual en una página nueva. **Nota:** Esta opción solo está disponible si ha adquirido IBM Security QRadar Risk Manager y ha obtenido una licencia para ese producto. Para obtener más información, consulte el manual *IBM Security QRadar Risk Manager Guía del usuario*.

Tabla 13. Funciones de la barra de herramientas de la pestaña Delitos (continuación)

Función	Descripción
Ver topología	Pulse **Ver topología** para investigar más el origen de un delito. Cuando pulsa el icono **Ver topología**, se abre el panel Topología actual en una página nueva. **Nota:** Esta opción solo está disponible si ha adquirido IBM Security QRadar Risk Manager y ha obtenido una licencia para ese producto. Para obtener más información, consulte el manual *IBM Security QRadar Risk Manager Guía del usuario*.

Parámetros de delitos

Esta tabla proporciona descripciones de parámetros existentes en la pestaña Delitos.

Tabla 14. Parámetros de delitos

Parámetro	Ubicación	Descripción
Anotación	Tabla 5 primeras anotaciones	Especifica los detalles de la anotación. Las anotaciones son descripciones de texto que pueden ser añadidas automáticamente por una regla a un delito como parte de la respuesta de la regla.
Anomalía	Tabla 10 últimos sucesos (sucesos de anomalía)	Seleccione esta opción para mostrar los resultados de búsqueda guardada que han hecho que la regla de detección de anomalías genere el suceso.
Texto de anomalía	Tabla 10 últimos sucesos (sucesos de anomalía)	Proporciona una descripción del comportamiento anómalo que ha sido detectado por la regla de detección de anomalías.
Valor de anomalía	Tabla 10 últimos sucesos (sucesos de anomalía)	Especifica el valor que ha hecho que la regla de detección de anomalías genere el delito.
Aplicación	Tabla 10 últimos flujos	Especifica la aplicación que está asociada al flujo.
Nombre de aplicación	Tabla Origen de delito, si el Tipo de delito es ID de aplicación	Especifica la aplicación que está asociada al flujo por el que se creó el delito.
Índice de ASN	Tabla Origen de delito, si el Tipo de delito es ASN de origen o ASN de destino	Especifica el valor de ASN que está asociado al flujo por el que se creó el delito.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Nombre de activo	Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino	Especifica el nombre de activo que puede asignar mediante la función Perfiles de activo. Para obtener más información, consulte Gestión de activos.
Peso de activo	Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino	Especifica el peso de activo, que puede asignar mediante la función Perfil de activo. Para obtener más información, consulte Gestión de activos.
Asignado a	Tabla Delito	Especifica el usuario que está asignado al delito. Si no hay ningún usuario asignado, este campo especifica No asignado. Pulse No asignado para asignar el delito a un usuario. Para obtener más información, consulte Asignar delitos a usuarios.
Categoría	Tabla 10 últimos sucesos	Especifica la categoría del suceso.
Nombre de categoría	Página Por detalles de categoría	Especifica el nombre de categoría de nivel superior.
Encadenado	• Tabla Origen de delito, si el Tipo de delito es IP de destino • Tabla 5 primeros IP de destino	Especifica si la dirección IP de destino está encadenada. Una dirección IP de destino encadenada está asociada con otros delitos. Por ejemplo, una dirección IP de destino puede llegar a ser la dirección IP de origen de otro delito. Si la dirección IP de destino está encadenada, pulse **Sí** para ver los delitos encadenados.
Fecha de creación	Tabla 5 últimas notas	Especifica la fecha y la hora en que se creó la nota.
Credibilidad	Tabla Delito	Especifica la credibilidad del delito, tal como está determinada por la valoración de credibilidad procedente de dispositivos de origen. Por ejemplo, la credibilidad aumenta cuando varios delitos notifican el mismo suceso o flujo.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Parámetros de búsqueda actuales	• Página Por detalles de IP de origen • Página Por detalles de IP de destino	La parte superior de la tabla muestra los detalles de los parámetros de búsqueda que se aplican a los resultados de la búsqueda. Para borrar esos parámetros de búsqueda, pulse **Borrar filtro**. **Nota:** Este parámetro sólo se muestra después de aplicar un filtro.
Descripción	• Página Todos los delitos • Página Mis delitos • Tabla Delito • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos • Tabla Origen de delito, si el Tipo de delito es Origen de registro • Tabla 5 primeros orígenes de registro	Proporciona la descripción del origen de delito u origen de registro.
IP de destino	• Tabla 10 últimos sucesos • Tabla 10 últimos flujos	Especifica la dirección IP de destino del suceso o flujo.
IP de destino	• Tabla 5 primeros IP de destino • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por red – Lista de destinos locales	Especifica la dirección IP del destino. Si las búsquedas DNS están habilitadas en la pestaña Admin, puede ver el nombre de DNS colocando el puntero del ratón encima de la dirección IP.
IP de destino	Tabla Delito	Especifica las direcciones IP y el nombre de activo (si está disponible) de los destinos locales o remotos. Pulse el enlace para ver más detalles.
IP de destino	• Página Todos los delitos • Página Mis delitos	Especifica las direcciones IP y el nombre de activo (si está disponible) de los destinos locales o remotos. Si existe más de una dirección IP de destino asociada al delito, este campo especifica Múltiple y el número de direcciones IP de destino.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
IP de destino	• Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica las direcciones IP y nombres de activos (si están disponible) del destino que está asociado al delito. Si las búsquedas DNS están habilitadas en la pestaña Admin, puede ver el nombre de DNS colocando el puntero del ratón encima de la dirección IP o nombre de activo.
IP de destino	Página Por detalles de red	Especifica el número de direcciones IP de destino que están asociadas a la red.
Puerto de destino	Tabla 10 últimos flujos	Especifica el puerto de destino del flujo.
Destino(s)	• Tabla 5 primeros IP de origen • Página Por detalles de IP de origen • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes	Especifica el nombre del suceso, tal como está identificado en el mapa QID, que está asociado al suceso o flujo que creó el delito. Coloque el puntero del ratón sobre el nombre de suceso para ver el QID.
Recuento de Sucesos/flujos	Página Por detalles de categoría	Especifica el número de sucesos o flujos activos (sucesos o flujos que no están cerrados ni ocultos) que están asociados al delito en la categoría. Los delitos solo permanecen activos durante un periodo de tiempo si no se recibe ningún nuevo suceso o flujo. Los delitos se muestran todavía en la pestaña Delitos, pero no se contabilizan en este campo.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Recuento de Sucesos/flujos	Página de destino Página Red	Especifica el número de sucesos y flujos que se han producido para el delito y el número de categorías. Pulse el enlace Sucesos para investigar más los sucesos que están asociados al delito. Cuando pulsa el enlace Sucesos, se muestran los resultados de la búsqueda de sucesos. Pulse el enlace Flujos para investigar más los flujos que están asociados al delito. Cuando pulsa el enlace Flujos, se muestran los resultados de la búsqueda de flujos. **Nota:** Si el recuento de flujos muestra N/D, la fecha de inicio del delito podría ser anterior a la fecha en que actualizó a la versión 7.1.0 (MR1) del producto QRadar. Por lo tanto, los flujos no se pueden contar. Pero puede pulsar el enlace N/D para investigar los flujos asociados contenidos en los resultados de búsqueda de flujos.
Recuento de Sucesos/flujos	Página Por detalles de categoría	Especifica el número de sucesos o flujos activos (sucesos o flujos que no están cerrados ni ocultos) que están asociados al delito en la categoría. Los delitos solo permanecen activos durante un periodo de tiempo si no se recibe ningún nuevo suceso o flujo. Los delitos se muestran todavía en la pestaña Delitos, pero no se contabilizan en este campo.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Recuento de Sucesos/flujos	Página de destino Página Red	Especifica el número de sucesos y flujos que se han producido para el delito y el número de categorías. Pulse el enlace Sucesos para investigar más los sucesos que están asociados al delito. Cuando pulsa el enlace Sucesos, se muestran los resultados de la búsqueda de sucesos. Pulse el enlace Flujos para investigar más los flujos que están asociados al delito. Cuando pulsa el enlace Flujos, se muestran los resultados de la búsqueda de flujos. **Nota:** Si el recuento de flujos muestra N/D, la fecha de inicio del delito podría ser anterior a la fecha en que actualizó a la versión 7.1.0 (MR1) del producto QRadar. Por lo tanto, los flujos no se pueden contar. Pero puede pulsar el enlace N/D para investigar los flujos asociados contenidos en los resultados de búsqueda de flujos.
Sucesos	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica el número de sucesos del delito.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Sucesos/flujos	• Tabla Origen de delito, si el Tipo de delito es IP de origen, IP de destino, Nombre de host, Nombre de usuario, Puerto de origen o Puerto de destino, Nombre de suceso, Puerto, Dirección MAC de origen o Dirección MAC de destino, Origen de registro, IPv6 de origen o IPv6 de destino, ASN de origen o ASN de destino, Regla, ID de aplicación • Tabla 5 primeros IP de origen • Página Por detalles de IP de origen • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Página Detalles de origen • Tabla 5 primeros IP de destino • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por red – Lista de destinos locales • Tabla 5 primeros usuarios • Tabla 5 primeros orígenes de registro • Tabla 5 primeras categorías • Página Por detalles de red • Tabla 5 primeras categorías	Especifica el número de sucesos o flujos que están asociados con la dirección IP de origen, dirección IP de destino, nombre de suceso, nombre de usuario, dirección MAC, origen de registro, nombre de host, puerto, origen de registro, dirección de ASN, dirección de IPv6, regla, ASN, aplicación, red o categoría. Pulse el enlace para ver más detalles.
Primer suceso/flujo visto en	Página Detalles de origen	Especifica la fecha y hora en que la dirección IP de origen generó el primer suceso o flujo.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Distintivo	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Indica la acción que se realiza en el delito. Las acciones están representadas por los iconos siguientes: • Distintivo: indica que el delito está marcado para realizar su seguimiento. Esto permite seguir un elemento determinado para investigar más. Para más información sobre cómo marcar un delito para su seguimiento, consulte Marcar un elemento para seguimiento. • Usuario: indica que el delito se ha asignado a un usuario. Cuando un delito está asignado a un usuario, el delito se muestra en la página Mis delitos perteneciente a ese usuario. Para más información sobre la asignación de delitos a usuarios, consulte Asignar delitos a usuarios. • Notas: indica que un usuario añadió notas al delito. Las notas pueden incluir cualquier información que desee capturar para el delito. Por ejemplo, puede añadir una nota con información que no se incluye automáticamente en un delito, tal como un número de incidencia de soporte al cliente o información de gestión del delito. Para más información sobre la adición de notas, consulte Añadir notas. • Protegido: indica que el delito está protegido. El distintivo Proteger impide que los delitos especificados se eliminen de la base de datos una vez transcurrido el periodo de retención. Para más información sobre delitos protegidos, consulte Proteger delitos. Coloque el puntero del ratón sobre el icono para mostrar más información.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Distintivo (continuación)		• Delito inactivo: indica que el delito está inactivo. Un delito pasa a estar inactivo después de transcurrir cinco días desde que el delito recibió el último suceso. Además, todos los delitos pasan a estar inactivos después de actualizar el software del producto QRadar. Un delito inactivo no puede pasar a estar activo de nuevo. Si se detectan nuevos sucesos para el delito, se crea un nuevo delito y el delito inactivo se conserva hasta que haya transcurrido el periodo de retención del delito. Puede realizar las acciones siguientes en delitos inactivos: proteger, marcar para seguimiento, añadir notas y asignar a usuarios.
Distintivo	• Página Por detalles de IP de origen • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por detalles de red • Página Por red - Lista de orígenes • Página Por red – Lista de destinos locales	Especifica la acción que se emprende sobre la dirección IP de origen, dirección IP de destino o red. Por ejemplo, si se muestra un distintivo, el delito está marcado para su seguimiento. Coloque el puntero del ratón sobre el icono para mostrar más información.
Flujos	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica el número de flujos del delito. **Nota:** Si la columna Flujos muestra N/D, la fecha de inicio del delito podría ser anterior a la fecha en que actualizó a QRadar 7.1.0 (MR1).
Grupo	• Tabla Origen de delito, si el Tipo de delito es Origen de registro • Tabla 5 primeros orígenes de registro	Especifica a qué grupo pertenece el origen de registro.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Grupo(s)	Tabla Origen de delito, si el Tipo de delito es Regla.	Especifica a qué grupo de reglas pertenece la regla.
Categoría de nivel superior	Tabla Origen de delito, si el Tipo de delito es Nombre de suceso	Especifica la categoría de nivel superior del suceso. Para obtener más información sobre categorías de nivel superior, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
Nombre de host	Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino	Especifica el nombre de host que está asociado a la dirección IP de origen o de destino. Si no se indica ningún nombre de host, este campo especifica Desconocido.
Nombre de perfil de correlación histórica	• Resumen de delitos	Especifica el nombre del perfil de correlación histórica que ha creado el delito.
Catálogo de correlación histórico	• Resumen de delitos	Especifica el catálogo de correlación histórica que contiene los sucesos que han desencadenado el delito. Para ver todos los sucesos en el catálogo, pulse **Ver historial** en la ventana Correlación histórica.
ID de perfil de correlación histórica	• Resumen de delitos	Especifica el identificador exclusivo del perfil de correlación histórica que ha creado el delito.
Nombre de host	Tabla Origen de delito, si el Tipo de delito es Nombre de host.	Especifica el nombre de host que está asociado al flujo por el que se creó el delito.
ID	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos	Especifica el número de identificación exclusivo que QRadar asigna al delito.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
IP	• Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino • Página Detalles de origen	Especifica la dirección IP de origen que está asociada al sucesoo flujo por el que se creó el delito.
IP/nombre de DNS	Página Destino	Especifica la dirección IP del destino. Si las búsquedas DNS están habilitadas en la pestaña **Admin**, puede ver el nombre de DNS colocando el puntero del ratón encima de la dirección IP o nombre de activo. Para obtener más información, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
IPv6	Tabla Origen de delito, si el Tipo de delito es IPv6 de origen o IPv6 de destino	Especifica la dirección IPv6 que está asociada al suceso o flujo por el que se creó el delito.
Último suceso/flujo	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de destinos locales • Tabla 5 primeros IP de origen • Página Por detalles de IP de origen • Página Por red - Lista de orígenes • Tabla 5 primeros IP de destino • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por red – Lista de destinos locales • Tabla 5 primeras categorías	Especifica el tiempo transcurrido desde que se observó el último suceso o flujo para el delito, categoría, dirección IP de origen o dirección IP de destino.
Último suceso/flujo visto en	Página Detalles de origen	Especifica la fecha y hora del último suceso o flujo generado que está asociado a la dirección IP de origen.
Hora de último suceso/flujo	Tabla Origen de delito, si el Tipo de delito es Origen de registro	Especifica la fecha y hora en que se observó por última vez el origen de registro en el sistema.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Último grupo conocido	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario, Dirección MAC de origen, Dirección MAC de destino o Nombre de host	Especifica el grupo actual al que pertenece el usuario, dirección MAC o nombre de host. Si no hay ningún grupo asociado, el valor de este campo es Desconocido. **Nota:** Este campo no muestra información histórica.
Último host conocido	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario, Dirección MAC de origen o Dirección MAC de destino	Especifica el host actual al que está asociado el usuario o dirección MAC. Si no se indica ningún host, este campo especifica Desconocido. **Nota:** Este campo no muestra información histórica.
Última dirección IP conocida	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario, Dirección MAC de origen, Dirección MAC de destino o Nombre de host	Especifica la dirección IP actual del usuario, MAC o nombre de host. Si no se indica ninguna dirección IP, este campo especifica Desconocido. **Nota:** Este campo no muestra información histórica.
Última dirección MAC conocida	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario o Nombre de host	Especifica la última dirección MAC conocida del nombre de usuario o nombre de host. Si no se indica ninguna dirección MAC, este campo especifica Desconocido. **Nota:** Este campo no muestra información histórica.
Última máquina conocida	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario, Dirección MAC de origen, Dirección MAC de destino o Nombre de host	Especifica el nombre de máquina actual que está asociado al usuario, dirección MAC o nombre de host. Si no se indica ningún nombre de máquina, este campo especifica Desconocido. **Nota:** Este campo no muestra información histórica.
Último nombre de usuario conocido	Tabla Origen de delito, si el Tipo de delito es Dirección MAC de origen, Dirección MAC de destino o Nombre de host	Especifica el usuario actual de la dirección MAC o nombre de host. Si no se indica ninguna dirección MAC, este campo especifica Desconocido. **Nota:** Este campo no muestra información histórica.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Observado por última vez	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario, Dirección MAC de origen, Dirección MAC de destino o Nombre de host	Especifica la fecha y hora en que se observó por última vez el usuario, dirección MAC o nombre de host.
Hora de último paquete	Tabla 10 últimos flujos	Especifica la fecha y hora en que se envió el último paquete del flujo.
Recuento de destinos locales	Tabla 5 primeras categorías Página Por detalles de categoría	Especifica el número de direcciones IP de destino locales asociadas a la categoría.
Destinos locales	Página Detalles de origen	Especifica las direcciones IP de destino locales asociadas a la dirección IP de origen. Para ver más información sobre las direcciones IP de destino, pulse la dirección IP o término que se muestra. Si hay varias direcciones IP de destino, se muestra el término Múltiple.
Ubicación	• Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino • Tabla 5 primeros IP de origen • Página Por detalles de IP de origen • Página Detalles de origen • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes	Especifica la ubicación de red de la dirección IP de origen o dirección IP de destino. Si la ubicación es local, puede pulsar el enlace para ver las redes.
Origen de registro	Tabla 10 últimos sucesos	Especifica el origen de registro que detectó el suceso.
Identificador de origen de registro	Tabla Origen de delito, si el Tipo de delito es Origen de registro	Especifica el nombre de host del origen de registro.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Nombre de origen de registro	Tabla Origen de delito, si el Tipo de delito es Origen de registro	Especifica el nombre de origen de registro, tal como está identificado en la tabla Orígenes de registro, que está asociado al suceso que creó el delito. **Nota:** La información que se muestra para delitos de origen de registro se obtiene a partir de la página Orígenes de registro de la pestaña Admin. Debe tener acceso administrativo para acceder a la pestaña Admin y gestionar orígenes de registro. Para obtener más información sobre la gestión de orígenes de registro, consulte el manual *Managing Log Sources Guide*.
Orígenes de registro	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica los orígenes de registro que están asociados al delito. Si hay más de un origen de registro asociado al delito, este campo especifica el término Múltiple y el número de orígenes de registro.
Categoría de nivel bajo	Tabla Origen de delito, si el Tipo de delito es Nombre de suceso	Especifica la categoría de nivel bajo del suceso.
MAC	• Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino • Tabla 5 primeros IP de origen • Tabla 5 primeros IP de destino • Página Por detalles de IP de origen • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Página Por red – Lista de destinos locales	Especifica la dirección MAC de la dirección IP de origen o destino cuando se inició el delito. Si no se conoce la dirección MAC, este campo especifica Desconocido.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Dirección MAC	Tabla Origen de delito, si el Tipo de delito es Dirección MAC de origen o Dirección MAC de destino	Especifica la dirección MAC que está asociada al suceso por el que se creó el delito. Si no se indica ninguna dirección MAC, este campo especifica Desconocido.
Magnitud	• Página Todos los delitos • Página Mis delitos • Tabla Delito • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos • Tabla 5 primeras categorías • Tabla 10 últimos sucesos • Página Por detalles de red • Página Red	Especifica la importancia relativa del delito, categoría, suceso o red. La barra de magnitudes proporciona una representación visual de todas las variables correlacionadas. Las variables incluyen Importancia, Gravedad, y Credibilidad. Coloque el puntero del ratón sobre la barra de magnitudes para mostrar valores y la magnitud calculada.
Magnitud	• Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino • Tabla 5 primeros IP de origen • Tabla 5 primeros IP de destino • Página Por detalles de IP de origen • Página Detalles de origen • Página Por IP de origen - Lista de destinos locales • Página Destino • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Página Por red – Lista de destinos locales	Especifica la importancia relativa de la dirección IP de origen o destino. La barra de magnitudes proporciona una representación visual del valor de riesgo de CVSS del activo que está asociado a la dirección IP. Coloque el puntero del ratón sobre la barra de magnitudes para mostrar la magnitud calculada.
Nombre	• Tabla 5 primeros orígenes de registro • Tabla 5 primeros usuarios • Tabla 5 primeras categorías • Página Red	Especifica el nombre del origen de registro, usuario, categoría, dirección IP de red o nombre.
Red	Página Por detalles de red	Especifica el nombre de la red.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Red(es)	Tabla Delito	Especifica la red de destino del delito. Si el delito tiene una sola red de destino, este campo muestra el nodo final de red. Pulse el enlace para ver la información de red. Si el delito tiene más de una red de destino, se muestra el término Múltiple. Pulse el enlace para ver más detalles.
Notas	• Tabla Origen de delito, si el Tipo de delito es Regla. • Tabla 5 últimas notas	Especifica las notas para la regla.
Recuento de delitos	Página Por detalles de categoría	Especifica el número de delitos activos de cada categoría. Los delitos activos son delitos que no se han ocultado ni cerrado. Si la página Por Detalles de categoría incluye el filtro Excluir delitos ocultos, el valor que se muestra en el parámetro Recuento de delitos podría no ser correcto. Si desea ver el recuento total en el panel Por categoría, pulse **Borrar filtro** junto al filtro Excluir delitos ocultos en la página Por detalles de categoría.
Origen de delito	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica información sobre el origen del delito. La información que se visualiza en el campo **Origen de delito** depende del tipo de delito. Por ejemplo, si el tipo de delito es Puerto de origen, el campo **Origen de delito** muestra el puerto de origen del suceso que ha creado el delito.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Tipo de delito	• Página Mis delitos • Tabla Delito • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica el tipo de delito. El Tipo de delito está determinado por la regla que ha creado el delito. Por ejemplo, si el tipo de delito es de suceso de origen de registro, la regla que ha generado el delito correlaciona sucesos que están basados en el dispositivo que ha detectado el suceso. Los tipos de delito son los siguientes: • IP de origen • IP de destino • Nombre de suceso • Nombre de usuario • Dirección MAC de origen • Dirección MAC de destino • Origen de registro • Nombre de host • Puerto de origen • Puerto de destino • IPv6 de origen • IPv6 de destino • ASN de origen • ASN de destino • Regla • ID de aplicación El tipo de delito determina qué tipo de información se visualiza en el panel Resumen de origen de delito.
Delito(s)	• Página Detalles de origen • Página Destino	Especifica los nombres de los delitos que están asociados a la dirección IP de origen o de destino. Para ver más información sobre el delito, pulse el nombre o término que se visualiza. Si hay varios delitos, se muestra el término Múltiple.
Delitos iniciados	Página Red	Especifica los delitos que se inician desde la red. Si hay varios delitos responsables, este campo muestra el término Múltiple y el número de delitos.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Delitos elegidos como objetivo	Página Red	Especifica los delitos que se eligen como objetivo para la red. Si hay varios delitos responsables, este campo muestra el término Múltiple y el número de delitos
Delitos	• Tabla Origen de delito, si el Tipo de delito es IP de origen, IP de destino, Nombre de suceso, Nombre de usuario, Dirección MAC de origen o Dirección MAC de destino, Origen de registro, Nombre de host, Puerto de origen o Puerto de destino, IPv6 de origen o IPv6 de destino, ASN de origen o ASN de destino, Regla, ID de aplicación • Tabla 5 primeros IP de origen • Tabla 5 primeros IP de destino • Tabla 5 primeros orígenes de registro • Tabla 5 primeros usuarios • Página Por detalles de IP de origen • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Página Por red – Lista de destinos locales	Especifica el número de delitos que están asociados con la dirección IP de origen, dirección IP de destino, nombre de suceso, nombre de usuario, dirección MAC, origen de registro, nombre de host, puerto, dirección de IPv6, ASN, regla o aplicación. Pulse el enlace para ver más detalles.
Delitos iniciados	Página Por detalles de red	Especifica el número de delitos que se originaron en la red.
Delitos elegidos como objetivo	Página Por detalles de red	Especifica el número de delitos que se eligen como objetivo para la red.
Puerto	Tabla Origen de delito, si el Tipo de delito es Puerto de origen o Puerto de destino	Especifica el puerto que está asociado al suceso o flujo por el que se creó el delito.
Importancia	Tabla Delito	Especifica la importancia relativa del delito.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Respuesta	Tabla Origen de delito, si el Tipo de delito es Regla.	Especifica el tipo de respuesta de la regla.
Descripción de la regla	Tabla Origen de delito, si el Tipo de delito es Regla.	Especifica el resumen de los parámetros de regla.
Nombre de regla	Tabla Origen de delito, si el Tipo de delito es Regla.	Especifica el nombre de la regla que está asociada al suceso o flujo por el que se creó el delito. **Nota:** La información que se visualiza para delitos de regla se obtiene de la pestaña **Reglas**.
Tipo de regla	Tabla Origen de delito, si el Tipo de delito es Regla.	Especifica la red de regla del delito.
Gravedad	• Tabla Origen de delito, si el Tipo de delito es Nombre de suceso • Tabla Delito	Especifica la gravedad del suceso o delito. La gravedad indica el nivel de peligro que un delito representa en relación a cuán preparada está la dirección IP de destino para el ataque. Este valor está correlacionado directamente con la categoría de suceso que está asociada al delito. Por ejemplo, un ataque de denegación de servicio (DoS) tiene una gravedad de 10, lo que indica un caso grave.
Recuento de orígenes	Página Por detalles de categoría	Especifica el número de direcciones IP de origen que están asociadas a delitos pertenecientes a la categoría. Si una dirección IP de origen está asociada con delitos en cinco categorías diferentes de bajo nivel, la dirección IP de origen se contabiliza una sola vez.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
IP de origen	• Página Por detalles de IP de origen • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Tabla 5 primeros IP de origen • Tabla 10 últimos flujos	Especifica la dirección IP o el nombre de host del dispositivo que ha intentado violar la seguridad de un componente de la red. Si las búsquedas DNS están habilitadas en la pestaña Admin, puede ver el nombre de DNS colocando el puntero del ratón encima de la dirección IP. Para obtener más información, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
IP(s) de origen	Tabla Delito	Especifica la dirección IP o el nombre de host del dispositivo que ha intentado violar la seguridad de un componente de la red. Pulse el enlace para ver más detalles. Para obtener más información sobre direcciones IP de origen, consulte Supervisar delitos agrupados por IP de origen.
Direcciones IP de origen	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica las direcciones IP o nombre de host del dispositivo que ha intentado violar la seguridad de un componente de la red. Si existe más de una dirección IP de origen asociada al delito, este campo contiene el término Múltiple y el número de direcciones IP de origen. Si las búsquedas DNS están habilitadas en la pestaña Admin, puede ver el nombre de DNS colocando el puntero del ratón encima de la dirección IP o nombre de activo. Para obtener más información, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
Direcciones IP de origen	Página Por detalles de red	Especifica el número de direcciones IP de origen que están asociadas a la red.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Puerto de origen	Tabla 10 últimos flujos	Especifica el puerto de origen del flujo.
Origen(es)	• Tabla 5 primeros IP de destino • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino	Especifica el número de direcciones IP de origen que están asociadas a la dirección IP de destino.
Origen(es)	• Página Destino • Página Red	Especifica las direcciones IP de origen del delito que está asociado a la dirección IP de destino o red. Para ver más información sobre las direcciones IP de origen, pulse en la dirección IP, nombre de activo o término que se visualiza. Si se especifica una sola dirección IP de origen, se muestra una dirección IP y un nombre de activo (si existe). Puede pulsar en la dirección IP o nombre de activo para ver los detalles de la dirección IP de origen. Si existen varias direcciones IP de origen, este campo contiene el término Múltiple y el número de direcciones IP de origen.
Origen(es)	Página Por red – Lista de destinos locales	Especifica el número de direcciones IP de origen que están asociadas a la dirección IP de destino.
Inicio	Tabla Delito	Especifica la fecha y hora en que se produjo el primer suceso o flujo para el delito.
Fecha de inicio	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica la fecha y hora del primer suceso o flujo que está asociado al delito.
Estado	Tabla Origen de delito, si el Tipo de delito es Origen de registro	Especifica el estado del origen de registro.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Estado	Tabla Delito	Muestra iconos para indicar el estado de un delito. Los iconos de estado son los siguientes: **Delito inactivo**. Un delito pasa a estar inactivo después de transcurrir cinco días desde que el delito recibió el último suceso. Todos los delitos pasan a estar inactivos después de actualizar el software del producto QRadar. Un delito inactivo no puede pasar a estar activo de nuevo. Si se detectan nuevos sucesos para el delito, se crea un nuevo delito y el delito inactivo se conserva hasta que haya transcurrido el periodo de retención del delito. Puede proteger, marcar para seguimiento, añadir notas y asignar usuarios a un delito inactivo. El distintivo de **Delito oculto** en la página Todos los delitos indica que el delito está oculto a la vista. Si busca delitos ocultos, son sólo visibles en la página Todos los delitos, donde están marcados como delito oculto. Para obtener más información, consulte Ocultar delitos. El distintivo **Usuario** indica que el delito está asignado a un usuario. Cuando un delito está asignado a un usuario, el delito aparece en la página Mis delitos perteneciente a ese usuario. Para obtener más información, consulte Asignar delitos a usuarios. El distintivo **Proteger** impide que los delitos especificados se eliminen de la base de datos una vez transcurrido el periodo de retención. Para obtener más información, consulte Proteger delitos. El distintivo **Delito cerrado** indica que el delito está cerrado. Para obtener más información, consulte Cerrar delitos.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Hora	• Tabla 10 últimos sucesos • Tabla 10 últimos sucesos (sucesos de anomalía)	Especifica la fecha y hora en que se detectó el primer suceso en el suceso normalizado. Este fecha y hora son especificados por el dispositivo que detectó el suceso.
Hora	Tabla 5 primeras anotaciones	Especifica la fecha y la hora en que se creó la anotación.
Bytes totales	Tabla 10 últimos flujos	Especifica el número total de bytes del flujo.
Sucesos/flujos totales	• Tabla 5 primeros orígenes de registro • Tabla 5 primeros usuarios	Especifica el número total de sucesos del origen de registro o usuario.
Usuario	• Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino, o Nombre de usuario • Tabla 5 primeros IP de origen • Tabla 5 primeros IP de destino • Página Por detalles de IP de origen • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Página Por red – Lista de destinos locales	Especifica el usuario que está asociado a una dirección IP de origen o dirección IP de destino. Si no se indica ningún usuario, este campo especifica Desconocido.
Nombre de usuario	Tabla Origen de delito, si el Tipo de delito es Nombre de usuario.	Especifica el nombre de usuario que está asociado al suceso o flujo por el que se creó el delito. **Nota:** Coloque el puntero del ratón sobre el parámetro Nombre de usuario para ver el nombre de usuario más reciente de la pestaña Activos, en lugar del nombre de usuario que está asociado al suceso o flujo por el que se creó el delito.
Nombre de usuario	Tabla 5 últimas notas	Especifica el usuario que ha creado la nota.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Usuarios	• Página Todos los delitos • Página Mis delitos • Página Por IP de origen - Lista de delitos • Página Por red - Lista de delitos • Página Por IP de destino - Lista de delitos	Especifica los nombres de usuario que están asociados al delito. Si existe más de un nombre de usuario asociado al delito, este campo contiene el término Múltiple y el número de nombres de usuario. Si no se indica ningún usuario, este campo especifica Desconocido.
Ver delitos	• Página Por detalles de IP de origen • Página Por detalles de IP de destino	Seleccione una opción en este cuadro de lista para filtrar los delitos de acuerdo con los que desee ver en esta página. Puede ver todos los delitos o filtrar los delitos de acuerdo con un rango de tiempo. En el cuadro de lista, seleccione el rango de tiempo por el que desee filtrar.
Vulnerabilidades	Tabla Origen de delito, si el Tipo de delito es IP de origen o IP de destino	Especifica el número de vulnerabilidades identificadas que están asociadas a la dirección IP de origen o de destino. Este valor incluye también el número de vulnerabilidades activas y pasivas.
Vulnerabilidades	Página Por IP de destino - Lista de orígenes	Especifica si una dirección IP de origen tiene vulnerabilidades.
Vulnerabilidad	• Tabla 5 primeros IP de origen • Página Por detalles de IP de origen • Página Por red - Lista de orígenes • Tabla 5 primeros IP de destino • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de destino • Página Por red – Lista de destinos locales	Especifica si la dirección IP de origen o de destino tiene vulnerabilidades.

Tabla 14. Parámetros de delitos (continuación)

Parámetro	Ubicación	Descripción
Peso	• Tabla 5 primeros IP de origen • Tabla 5 primeros IP de destino • Página Por IP de origen - Lista de destinos locales • Página Por detalles de IP de origen • Página Por detalles de IP de destino • Página Por IP de destino - Lista de orígenes • Página Por red - Lista de orígenes • Página Por red – Lista de destinos locales • Tabla 5 primeras anotaciones	Especifica el peso de la dirección IP de origen, dirección IP de destino o anotación. El peso de una dirección IP se asigna en la pestaña **Activos**. Para obtener más información, consulte Gestión de activos.

Capítulo 5. Investigación de la actividad de registro

Puede supervisar e investigar sucesos en tiempo real o realizar búsquedas avanzadas.

Utilizando la pestaña **Actividad de registro**, puede supervisar e investigar la actividad de registro (sucesos) en tiempo real o realizar búsquedas avanzadas.

Visión general de la pestaña Actividad de registro

Un suceso es un registro de un origen de registro, como un cortafuegos o dispositivo de direccionador, que describe una acción en una red o un host.

La pestaña **Actividad de registro** especifica qué sucesos se asocian con delitos.

Debe tener permiso para ver la pestaña **Actividad de registro**.

Barra de herramientas de pestaña Actividad de registro

Puede acceder a varias opciones desde la barra de herramientas Actividad de registro

Mediante la barra de herramientas, puede acceder a las siguientes opciones:

Tabla 15. Opciones de barra de herramientas Actividad de registro

Opción	Descripción
Buscar	Pulse **Buscar** para realizar búsquedas avanzadas en sucesos. Las opciones incluyen: • **Nueva búsqueda**: Seleccione esta opción para crear una nueva búsqueda de sucesos. • **Editar búsqueda**: Seleccione esta opción para seleccionar y editar una búsqueda de sucesos. • **Gestionar resultados de búsqueda**: Seleccione esta opción para ver y gestionar los resultados de búsqueda.
Búsquedas rápidas	En este cuadro de lista, puede guardar búsquedas guardadas anteriormente. Las opciones se muestran en el recuadro de lista**Búsquedas rápidas** sólo cuando ha guardado los criterios de búsqueda que especifican la opción **Incluir en Búsquedas rápidas**.
Añadir filtro	Pulse **Añadir filtro** para añadir un filtro a los resultados de búsqueda actuales.
Guardar criterios	Pulse **Guardar criterios** para guardar los criterios de búsqueda actuales.

© Copyright IBM Corp. 2012, 2015

Tabla 15. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Guardar resultados	Pulse **Guardar criterios** para guardar los resultados de búsqueda actuales. Esta opción sólo se visualiza después de que se haya completado una búsqueda. Esta opción está inhabilitada en modalidad continua.
Cancelar	Pulse **Cancelar** para cancelar una búsqueda en curso. Esta opción está inhabilitada en modalidad continua.
Falso positivo	Pulse **Falso positivo** para abrir la ventana Ajuste de falsos positivos, que le permitirá impedir que los sucesos que se conoce que son falsos positivos creen delitos. Esta opción está inhabilitada en modalidad continua. Para obtener más información sobre el ajuste de falsos positivos, consulte Ajuste de falsos positivos.

Tabla 15. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Reglas	La opción Reglas sólo es visible si tiene permiso para ver reglas. Pulse **Reglas** para configurar reglas de suceso personalizadas. Las opciones incluyen: • **Reglas**: Seleccione esta opción para ver o crear una regla. Si solo tiene permiso para ver reglas, se visualiza la página de resumen del asistente de reglas. Si tiene permiso para mantener reglas personalizadas, se visualiza el asistente de reglas y puede editar la regla. Para habilitar las opciones de regla de detección de anomalías (Añadir regla de umbral, Añadir regla conductual y Añadir regla de anomalía), debe guardar los criterios de búsqueda agregados porque los criterios de búsqueda guardados especifican los parámetros necesarios. **Nota:** Las opciones de regla de detección de anomalías sólo están visibles si tiene el permiso **Actividad de registro** > **Mantener reglas personalizadas** . • **Añadir regla de umbral**: Seleccione esta opción para crear una regla de umbral. Una regla de umbral prueba en el tráfico de sucesos la actividad que supera un umbral configurado. Los umbrales pueden basarse en los datos que QRadar recopila. Por ejemplo, si crea una regla de umbral que indica que no pueden iniciar la sesión en el servidor más de 220 clientes entre las 08:00 y las 17:00, las reglas generan una alerta cuando el cliente número 221 intenta iniciar la sesión. Cuando se selecciona la opción **Añadir regla de umbral**, el asistente de reglas se visualiza, lleno con las opciones adecuadas para crear una regla de umbral.

Tabla 15. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Reglas (continuación)	• **Añadir regla conductual**: Seleccione esta opción para crear una regla conductual. Una regla conductual prueba en el tráfico de sucesos la actividad anormal como, por ejemplo, la existencia de tráfico nuevo o desconocido, que es tráfico que cesa de repente o un cambio de porcentaje en la cantidad de tiempo que un objeto está activo. Por ejemplo, puede crear una regla conductual para comparar el promedio de volumen de tráfico durante los últimos 5 minutos con el promedio de volumen de tráfico durante la última hora. Si el cambio es superior al 40%, la regla genera una respuesta. Cuando se selecciona la opción **Añadir regla conductual**, el asistente de reglas se visualiza, llenado previamente con las opciones adecuadas para crear una regla conductual. • **Añadir regla de anomalía**: Seleccione esta opción para crear una regla de anomalía. Una regla de anomalía prueba en el tráfico de sucesos la actividad anormal como, por ejemplo, la existencia de tráfico nuevo o desconocido, que es tráfico que cesa de repente o un cambio de porcentaje en la cantidad de tiempo que un objeto está activo. Por ejemplo, si un área de la red que nunca se comunica con Asia empieza a comunicarse con hosts de ese país, una regla de anomalía genera una alerta. Cuando se selecciona la opción **Añadir regla de anomalía**, el asistente de reglas se visualiza, llenado previamente con las opciones adecuadas para crear una regla de anomalía.

Tabla 15. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Acciones	Pulse **Acciones** para realizar las acciones siguientes: • **Mostrar todo**: Seleccione esta opción para eliminar todos los filtros en los criterios de búsqueda y visualizar todos los sucesos no filtrados. • **Imprimir**: Seleccione esta opción para imprimir los sucesos que se visualizan en la página. • **Exportar a XML** > **Columnas visibles**: Seleccione esta opción para exportar sólo las columnas que son visibles en la pestaña Actividad de registro. Esta es la opción recomendada. Vea Exportación de sucesos. • **Exportar a XML** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse. Vea Exportación de sucesos. • **Exportar a CSV** >**Columnas visibles**: Seleccione esta opción para exportar solo las columnas que están visibles en la pestaña Actividad de registro. Esta es la opción recomendada. Vea Exportación de sucesos. • **Exportar a CSV** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse. Vea Exportación de sucesos. • **Suprimir**: Seleccione esta opción para suprimir un resultado de búsqueda. Consulte Gestión de resultados de búsqueda de sucesos y flujos. • **Notificar**: Seleccione esta opción para especificar que desea que se le envíe una notificación por correo electrónico cuando terminen las búsquedas seleccionadas. Esta opción solo está habilitada para las búsquedas en curso. **Nota:** Las opciones **Imprimir**, **Exportar a XML** y **Exportar a CSV** están inhabilitadas en modalidad continua y cuando se ven resultados de búsqueda parciales.

Tabla 15. Opciones de barra de herramientas Actividad de registro (continuación)

Opción	Descripción
Barra de herramientas Buscar	**Búsqueda avanzada** Seleccione **Búsqueda avanzada** en el recuadro de lista para entrar una serie de búsqueda AQL (Ariel Query Language) para especificar los campos que desea que se devuelvan. **Filtro rápido** Seleccione Filtro rápido en el recuadro de lista para buscar cargas útiles utilizando palabras o frases simples.
Ver	La vista predeterminada de la pestaña **Actividad de registro** es una corriente de sucesos en tiempo real. La lista **Ver** contiene opciones para ver también sucesos de periodos de tiempo específicos. Después de elegir un periodo de tiempo especificado de la lista **Ver** puede modificar el periodo de tiempo visualizado cambiando los valores de fecha y hora en los campos **Hora de inicio** y **Hora de finalización**.

Opciones del menú que aparece al pulsar el botón derecho del ratón

En la pestaña **Actividad de registro**, puede pulsar el botón derecho del ratón en un suceso para acceder a más información de filtro de sucesos.

Las opciones del menú que aparece al pulsar el botón derecho del ratón son las siguientes:

Tabla 16. Opciones del menú que aparece al pulsar el botón derecho del ratón

Opción	Descripción
Filtro en	Seleccione esta opción para filtrar en el suceso seleccionado, en función del parámetro seleccionado del suceso.
Falso positivo	Seleccione esta opción para abrir la ventana Falso positivo, que le permitirá impedir que los sucesos que se conoce que son falsos positivos creen delitos. Esta opción está inhabilitada en modalidad continua. Consulte Ajustes de falsos positivos.
Más opciones:	Seleccione esta opción para investigar una dirección IP o un nombre de usuario. Para obtener más información sobre la investigación una dirección IP, consulte Investigación de direcciones IP. Para obtener más información sobre la investigación de un nombre de usuario, consulte Investigación de nombres de usuario. **Nota:** Esta opción no se visualiza en modalidad continua.

Tabla 16. Opciones del menú que aparece al pulsar el botón derecho del ratón (continuación)

Opción	Descripción
Filtro rápido	Filtrar elementos que coinciden o no coinciden con la selección.

Barra de estado

Al transmitir sucesos, la barra de estado visualiza el número promedio de resultados que se reciben por segundo.

Este es el número de resultados que la consola ha recibido satisfactoriamente de los procesadores de sucesos. Si este número supera los 40 resultados por segundo, sólo se visualizarán 40 resultados. El resto se acumula en el almacenamiento intermedio de resultados. Para ver más información de estado, mueva el puntero del ratón sobre la barra de estado.

Cuando no se transmiten sucesos, la barra de estado muestra el número de resultados de búsqueda que se visualizan actualmente en la pestaña y la cantidad de tiempo que se necesita para procesar los resultados de búsqueda.

Supervisión de actividad de registro

De forma predeterminada, la pestaña **Actividad de registro** visualiza sucesos en modalidad continua, lo que le permite ver los sucesos en tiempo real.

Para obtener más información sobre la modalidad continua, consulte Visualización de sucesos de modalidad continua. Puede especificar un rango de tiempo distinto para filtrar sucesos mediante el recuadro de lista **Ver**.

Si anteriormente ha configurado criterios de búsqueda guardados como el valor predeterminado, los resultados de dicha búsqueda se visualizan automáticamente cuando se accede a la pestaña **Actividad de registro**. Para obtener más información acerca de cómo guardar criterios de búsqueda, consulte Guardar criterios de búsqueda de sucesos y flujos.

Visualización de sucesos en modalidad continua

La modalidad continua le permitirá ver los datos de sucesos que entran en el sistema. Esta modalidad le proporciona una vista en tiempo real de la actividad actual de sucesos visualizando los últimos 50 sucesos.

Acerca de esta tarea

Si se aplican filtros en la pestaña **Actividad de registro** o en los criterios de búsqueda antes de habilitar la modalidad continua, los filtros se mantienen en modalidad continua. Sin embargo, la modalidad continua no soporta búsquedas que incluyan sucesos agrupados. Si habilita la modalidad continua en sucesos agrupados o criterios de búsqueda agrupados, la pestaña **Actividad de registro** visualiza los sucesos normalizados. Consulte Visualización de sucesos normalizados.

Cuando desea seleccionar un suceso para ver detalles o realizar una acción, debe poner en pausa la modalidad continua antes de efectuar una doble pulsación en un

suceso. Cuando la modalidad continua está en pausa, se visualizan los últimos 1.000 sucesos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Ver**, seleccione **Tiempo real (modalidad continua)**. Para obtener información sobre las opciones de la barra de herramientas, consulte la Tabla 4-1. Para obtener más información sobre los parámetros que se visualizan en modalidad continua, consulte la Tabla 4-7.
3. Opcional. Poner en pausa o reproducir los sucesos en modalidad continua. Elija una de las siguientes opciones:
   - Para seleccionar un registro de sucesos, pulse el icono de **Pausa** para poner en pausa la modalidad continua.
   - Para reiniciar la modalidad continua, pulse el icono de **Reproducir**.

Visualización de sucesos normalizados

Los sucesos se recopilan en formato en bruto y, a continuación, se normalizan para visualizarse en la pestaña **Actividad de registro**.

Acerca de esta tarea

La normalización implica analizar los datos de sucesos en bruto y preparar los datos para visualizar información legible sobre la pestaña. Cuando los sucesos se normalizan, el sistema también normaliza los nombres. Por lo tanto, el nombre que se muestra en la pestaña **Actividad de registro** puede no coincidir con el nombre que se visualiza en el suceso.

Nota: Si ha seleccionado que se visualice un intervalo de tiempo, se visualiza un gráfico de serie temporal. Para obtener más información sobre la utilización de gráficos de serie temporal, consulte Visión general de gráfico de serie temporal.

La pestaña **Actividad de registro** muestra los parámetros siguientes cuando se visualizan sucesos normalizados:

Tabla 17. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado)

Parámetro	Descripción
Filtros actuales	En la parte superior de la tabla se muestran los detalles de los filtros que se aplican a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**. **Nota:** Este parámetro sólo se muestra después de aplicar un filtro.
Ver	En este recuadro de lista, puede seleccionar el rango de tiempo por el que desea filtrar.

Tabla 17. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Estadísticas actuales	Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para visualizar u ocultar las estadísticas • **Resultados totales**: Especifica el número total de resultados que coincidían con los criterios de búsqueda. • **Archivos de datos buscados**: Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado. • **Duración**: Especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar los problemas de sucesos, es posible que se le solicite que proporcione información estadística actual.
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse **Ocultar gráficos** si desea eliminar los gráficos de la pantalla. Los gráficos sólo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. Para obtener más información sobre cómo configurar gráficos, consulte Gestión de gráficos. **Nota:** Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.

Tabla 17. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Icono de delitos	Pulse este icono para ver detalles del delito que está asociado con este suceso. Para obtener más información, consulte Gestión de gráficos. **Nota:** Dependiendo del producto, es posible que este icono no esté disponible. Debe tener IBM Security QRadar SIEM.
Hora de inicio	Especifica la hora del primer suceso, tal como lo ha indicado el origen de registro a QRadar.
Nombre de suceso	Especifica el nombre normalizado del suceso.
Origen de registro	Especifica el origen de registro que ha originado el suceso. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Recuento de sucesos	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se detectan muchos sucesos del mismo tipo para la misma dirección IP de origen y dirección en un breve periodo de tiempo.
Hora	Especifica la fecha y hora en que QRadar ha recibido el suceso.
Categoría de nivel bajo	Especifica la categoría de bajo nivel que está asociada con este suceso. Para obtener más información sobre categorías de suceso, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.
IP de origen	Especifica la dirección IP de origen del suceso.
Puerto de origen	Especifica el puerto de origen del suceso.
IP de destino	Especifica la dirección IP de destino del suceso.
Puerto de destino	Especifica el puerto de destino del suceso.
Nombre de usuario	Especifica el nombre de usuario que está asociado con este suceso. Normalmente los nombres de usuario están disponibles en sucesos relacionados con la autenticación. Para todos los demás tipos de sucesos donde el nombre de usuario no está disponible, este campo especifica N/A.

Tabla 17. Parámetros de pestaña Actividad de registro - Valor predeterminado (normalizado) (continuación)

Parámetro	Descripción
Magnitud	Especifica la magnitud de este suceso. Las variables incluyen credibilidad, pertinencia y gravedad. Apunte el ratón sobre la barra de magnitud para visualizar los valores y la magnitud calculada.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Visualizar**, seleccione **Valor predeterminado (normalizado)**.
3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Pulse el icono **Pausa** para poner en pausa la modalidad continua.
5. Efectúe una doble pulsación en el suceso que desea con más detalle. Para obtener más información, consulte Detalles de suceso.

Visualización de sucesos en bruto

Puede ver los datos de sucesos en bruto, que son los datos de sucesos sin analizar desde el origen de registro.

Acerca de esta tarea

Al ver datos de sucesos en bruto, la pestaña **Actividad de registro** proporciona los parámetros siguientes para cada suceso.

Tabla 18. Parámetros de sucesos en bruto

Parámetro	Descripción
Filtros actuales	En la parte superior de la tabla se muestran los detalles de los filtros que se aplican a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**. **Nota:** Este parámetro sólo se visualiza después de aplicar un filtro.
Ver	En este recuadro de lista, puede seleccionar el rango de tiempo por el que desea filtrar.

Tabla 18. Parámetros de sucesos en bruto (continuación)

Parámetro	Descripción
Estadísticas actuales	Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para visualizar u ocultar las estadísticas • **Resultados totales**: Especifica el número total de resultados que coincidían con los criterios de búsqueda. • **Archivos de datos buscados**: Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado. • **Duración**: Especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar los problemas de sucesos, es posible que se le solicite que proporcione información estadística actual.
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse **Ocultar gráficos** si desea eliminar los gráficos de la pantalla. Los gráficos sólo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. **Nota:** Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.
Icono de delitos	Pulse este icono para ver detalles del delito que está asociado con este suceso.
Hora de inicio	Especifica la hora del primer suceso, tal como lo ha indicado el origen de registro a QRadar.

Tabla 18. Parámetros de sucesos en bruto (continuación)

Parámetro	Descripción
Origen de registro	Especifica el origen de registro que ha originado el suceso. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Carga útil	Especifica la información de carga útil de suceso original en formato UTF-8.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Visualizar**, seleccione **Sucesos en bruto**.
3. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
4. Efectúe una doble pulsación en el suceso que desea con más detalle. Consulte Detalles del suceso.

Visualización de sucesos agrupados

Utilizando la pestaña **Actividad de registro**, puede ver sucesos que están agrupados por diversas opciones. En el recuadro de lista **Visualizar**, puede seleccionar el parámetro por el que desea agrupar los sucesos.

Acerca de esta tarea

El recuadro de lista Visualizar no aparece en modalidad continua porque la modalidad continua no soporta los sucesos agrupados. Si ha entrado en modalidad continua utilizando criterios de búsqueda no agrupados, se visualiza esta opción.

El recuadro de lista Visualizar proporciona las opciones siguientes:

Tabla 19. Opciones de sucesos agrupados

Opción de grupo	Descripción
Categoría de nivel bajo	Muestra una lista resumida de sucesos que están agrupados por la categoría de bajo nivel del suceso. Para obtener más información sobre las categorías, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.
Nombre de suceso	Muestra una lista resumida de sucesos que están agrupados por el nombre normalizado del suceso.
IP de destino	Muestra una lista resumida de sucesos que están agrupados por la dirección IP de destino del suceso.
Puerto de destino	Muestra una lista resumida de sucesos que están agrupados por la dirección de puerto de destino del suceso.

Tabla 19. Opciones de sucesos agrupados (continuación)

Opción de grupo	Descripción
IP de origen	Muestra una lista resumida de sucesos que están agrupados por la dirección IP de origen del suceso.
Regla personalizada	Muestra una lista resumida de sucesos que están agrupados por la regla personalizada asociada.
Nombre de usuario	Muestra una lista resumida de sucesos que están agrupados por el nombre de usuario que está asociado con los sucesos.
Origen de registro	Muestra una lista resumida de sucesos que están agrupados por los orígenes de registro que han enviado el suceso a QRadar.
Categoría de nivel alto	Muestra una lista resumida de sucesos que están agrupados por la categoría de nivel alto del suceso.
Red	Muestra una lista resumida de sucesos que están agrupados por la red que está asociada con el suceso.
Puerto de origen	Muestra una lista resumida de sucesos que están agrupados por la dirección de puerto de origen del suceso.

Después de seleccionar una opción en el cuadro de lista **Visualizar**, la disposición de las columnas de datos depende de la opción de agrupación elegida. Cada fila de la tabla de sucesos representa un grupo de sucesos. La pestaña **Actividad de registro** proporciona la siguiente información para cada grupo de sucesos

Tabla 20. Parámetros de sucesos agrupados

Parámetro	Descripción
Agrupando por	Especifica el parámetro para el que se agrupa la búsqueda.
Filtros actuales	En la parte superior de la tabla se muestran los detalles del filtro que se aplica a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**.
Ver	En el cuadro de lista, seleccione el rango de tiempo para el que desee aplicar el filtro.

Tabla 20. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Estadísticas actuales	Cuando no se está en modalidad de tiempo real (modalidad continua) o de último minuto (renovación automática), se visualizan las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para mostrar u ocultar las estadísticas. • **Resultados totales**: Especifica el número total de resultados que coincidían con los criterios de búsqueda. • **Archivos de datos buscados**: Especifica el número total de archivos de datos buscados durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: Especifica el número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: Especifica el número total de archivos de índice buscados durante el intervalo de tiempo especificado. • **Duración**: Especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para resolver problemas de los sucesos, es posible que se le solicite que proporcione información estadística actual.

Tabla 20. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Gráficos	Muestra gráficos configurables que representan los registros que se comparan con la opción de intervalo de tiempo y agrupación. Pulse **Ocultar gráficos** si desea eliminar el gráfico de la pantalla. Cada gráfico proporciona una leyenda, que es una referencia visual para ayudarle a asociar los objetos de gráfico con los parámetros que representan. Mediante la característica de leyenda, puede realizar las acciones siguientes: • Mueva el puntero del ratón sobre un elemento de leyenda para ver más información sobre los parámetros que representa. • Pulse el botón derecho del ratón en el elemento de leyenda para investigar el elemento adicionalmente. • Pulse en un elemento de leyenda para ocultar el elemento en el gráfico. Pulse el elemento de leyenda de nuevo para mostrar el elemento oculto. También puede pulsar el elemento de gráfico correspondiente para ocultar y mostrar el elemento. • Pulse **Leyenda** si desea eliminar la leyenda de la pantalla gráfica. **Nota:** Los gráficos sólo se visualizan después de seleccionar un intervalo de tiempo de Último intervalo (renovación automática) o superior y una opción de agrupación a visualizar. **Nota:** Si utiliza Mozilla Firefox como navegador y se instala una extensión de navegador de bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.
IP de origen (Recuento exclusivo)	Especifica la dirección IP de origen que está asociada con este suceso. Si hay varias direcciones IP que están asociados con este suceso, este campo especifica el término Múltiple y el número de direcciones IP.
IP de destino (Recuento exclusivo)	Especifica la dirección IP de destino que está asociada con este suceso. Si hay varias direcciones IP que están asociados con este suceso, este campo especifica el término Múltiple y el número de direcciones IP.

Tabla 20. Parámetros de sucesos agrupados (continuación)

Parámetro	Descripción
Puerto de destino (Recuento exclusivo)	Especifica los puertos de destino que están asociados con este suceso. Si hay varios puertos que están asociados con este suceso, este campo especifica el término Múltiple y el número de puertos.
Nombre de suceso	Especifica el nombre normalizado del suceso.
Origen de registro (Recuento exclusivo)	Especifica los orígenes de registro que han enviado el suceso a QRadar. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Categoría de nivel alto (Recuento exclusivo)	Especifica la categoría de alto nivel de este suceso. Si hay varias categorías que están asociadas con este suceso, este campo especifica el término Múltiple y el número de categorías. Para obtener más información sobre las categorías, consulte la publicación *IBM Security QRadar Log Manager Administration Guide*.
Categoría de nivel bajo (Recuento exclusivo)	Especifica la categoría de bajo nivel de este suceso. Si hay varias categorías que están asociadas con este suceso, este campo especifica el término Múltiple y el número de categorías.
Protocolo (Recuento exclusivo)	Especifica el ID de protocolo asociado con este suceso. Si hay varios protocolos que están asociados con este suceso, este campo especifica el término Múltiple y el número de ID de protocolo.
Nombre de usuario (Recuento exclusivo)	Especifica el nombre de usuario que está asociado con este suceso, si está disponible. Si hay varios nombres de usuario que están asociados con este suceso, este campo especifica el término Múltiple y el número de nombres de usuario.
Magnitud (máxima)	Especifica la magnitud máxima calculada para sucesos agrupados. Las variables que se utilizan para calcular la magnitud incluyen la credibilidad, la pertinencia y la gravedad. Para obtener más información sobre la credibilidad, el pertinencia y la gravedad, consulte el Glosario.
Recuento de sucesos (Suma)	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se ven muchos sucesos del mismo tipo para la misma dirección IP de origen y destino en un corto periodo de tiempo.
Recuento	Especifica el número total de sucesos normalizados en este grupo de sucesos.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Ver**, seleccione el intervalo de tiempo que desea visualizar.
3. En el recuadro de lista Visualizar, elija el parámetro por el que desea agrupar los sucesos. Consulte la Tabla 2.Se listan los grupos de sucesos. Para obtener más información sobre los detalles de grupo de sucesos, consulte la Tabla 1.
4. Para ver la página Lista de sucesos para un grupo, efectúe una doble pulsación en el grupo de sucesos que desea investigar. La página Lista de sucesos no conserva las configuraciones de gráfico que pueda haber definido en la pestaña **Actividad de registro**. Para obtener más información sobre los parámetros de página Lista de sucesos, consulte la Tabla 1.
5. Para ver los detalles de un suceso, efectúe una doble pulsación en el suceso que desea investigar. Para obtener más información sobre los detalles de suceso, consulte la Tabla 2.

Detalles de suceso

Puede ver una lista de sucesos en varias modalidades, incluida la modalidad continua o en grupos de sucesos. Sea cual sea la modalidad que elija para ver sucesos, puede localizar y ver los detalles de un único suceso.

La página de detalles de suceso proporciona la siguiente información:

Tabla 21. Detalles de suceso

Parámetro	Descripción
Nombre de suceso	Especifica el nombre normalizado del suceso.
Categoría de nivel bajo	Especifica la categoría de bajo nivel de este suceso. Para obtener más información sobre las categorías, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.
Descripción del suceso	Especifica una descripción del suceso, si está disponible.
Magnitud	Especifica la magnitud de este suceso. Para obtener más información sobre la magnitud, consulte el Glosario
Pertinencia	Especifica la pertinencia de este suceso. Para obtener más información sobre la pertinencia, consulte el Glosario.
Gravedad	Especifica la gravedad de este suceso. Para obtener más información sobre la gravedad, consulte el Glosario.
Credibilidad	Especifica la credibilidad de este suceso. Para obtener más información sobre credibilidad, consulte el Glosario.
Nombre de usuario	Especifica el nombre de usuario que está asociado con este suceso, si está disponible.
Hora de inicio	Especifica la hora en que se ha recibido el suceso del origen de registro.

Tabla 21. Detalles de suceso (continuación)

Parámetro	Descripción
Hora de almacenamiento	Especifica el tiempo que el suceso ha estado almacenado en la base de datos de QRadar.
Hora de origen de registro	Especifica la hora de sistema indicada por el origen de registro en la carga útil de suceso.
Información de detección de anomalía: Este panel solo se visualiza si este suceso lo ha generado una regla de detección de anomalías. Pulse el icono **Anomalía** para ver los resultados de búsqueda guardados que han hecho que la regla de detección de anomalías generara este suceso.	
Descripción de regla	Especifica la regla de detección de anomalías que ha generado este suceso.
Descripción de anomalía	Especifica una descripción del comportamiento anómalo que ha sido detectada por la regla de detección de anomalías.
Valor de alerta de anomalía	Especifica el valor de alerta de anomalía.
Información de origen y destino	
IP de origen	Especifica la dirección IP de origen del suceso.
IP de destino	Especifica la dirección IP de destino del suceso.
Nombre de activo de origen	Especifica el nombre de activo definido por el usuario del origen de suceso. Para obtener más información sobre activos, consulte Gestión de activos.
Nombre de activo de destino	Especifica el nombre de activo definido por el usuario del destino de suceso. Para obtener más información sobre activos, consulte Gestión de activos
Puerto de origen	Especifica el puerto de origen de este suceso.
Puerto de destino	Especifica el puerto de destino de este suceso.
IP de origen NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT (Network Address Translation - Conversión de direcciones de red), este parámetro especifica la dirección IP de origen antes de que se aplicaran los valores de NAT. NAT convierte una dirección IP de una red en una dirección IP diferente de otra red.
IP de destino NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de destino antes de que se aplicaran los valores de NAT.
Puerto de origen NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen antes de que se aplicaran los valores de NAT.

Tabla 21. Detalles de suceso (continuación)

Parámetro	Descripción
Puerto de destino NAT previo	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino antes de que se aplicaran los valores de NAT.
IP de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de origen después de que se aplicaran los valores de NAT.
IP de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica la dirección IP de destino después de que se aplicaran los valores de NAT.
Puerto de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen después de que se aplicaran los valores de NAT.
Puerto de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino después de que se aplicaran los valores de NAT.
Puerto de origen NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de origen después de que se aplicaran los valores de NAT.
Puerto de destino NAT posterior	Para un cortafuegos u otro dispositivo con capacidad para NAT, este parámetro especifica el puerto de destino después de que se aplicaran los valores de NAT.
Origen IPv6	Especifica la dirección IPv6 de origen del suceso.
Destino IPv6	Especifica la dirección IPv6 de destino del suceso.
MAC de origen	Especifica la dirección MAC de origen del suceso.
MAC de destino	Especifica la dirección MAC de destino del suceso.
Información de carga útil	
Carga útil	Especifica el contenido de carga útil del suceso. Este campo ofrece 3 pestañas para ver la carga útil: • Universal Transformation Format (UTF): Pulse UTF. • Hexadecimal: Pulse HEX. • Base64: Pulse Base64.
Información adicional	
Protocolo	Especifica el protocolo que está asociado con este suceso.

Tabla 21. Detalles de suceso (continuación)

Parámetro	Descripción
QID	Especifica el QID para este suceso. Cada suceso tiene un QID exclusivo. Para obtener más información sobre la correlación de un QID, consulte Modificación de correlación de sucesos.
Origen de registro	Especifica el origen de registro que ha enviado el suceso a QRadar. Si hay varios orígenes de registro que están asociados con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
Recuento de sucesos	Especifica el número total de sucesos que están empaquetados en este suceso normalizado. Los sucesos se empaquetan cuando se ven muchos sucesos del mismo tipo para la misma dirección IP de origen y destino en un corto periodo de tiempo.
Reglas personalizadas	Especifica las reglas personalizadas que coinciden con este suceso. .
Reglas personalizadas coinciden parcialmente	Especifica reglas personalizadas que coinciden parcialmente con este suceso.
Anotaciones	Especifica el anotación para este suceso. Las anotaciones son descripciones de texto que las reglas pueden añadir automáticamente a los sucesos como parte de la respuesta de regla.
Información de identidad: QRadar recopila información de identidad, si está disponible, de los mensajes de origen de registro. La información de identidad proporciona detalles adicionales acerca de los activos en la red. Los orígenes de registro sólo generan información de identidad si el mensaje de registro enviado a QRadar contiene una dirección IP y al menos uno de los elementos siguientes: Nombre de usuario o Dirección MAC. No todos los orígenes de registro generan información de identidad. Para obtener más información sobre la identidad y los activos, consulte Gestión de activos.	
Nombre de usuario de identidad	Especifica el nombre de usuario del activo que está asociado con este suceso.
IP de identidad	Especifica la dirección IP del activo que está asociado con este suceso.
Nombre de NetBios de identidad	Especifica el nombre del Sistema básico de entrada/salida de red (NetBios) del activo que está asociado con este suceso.
Campo ampliado de identidad	Especifica más información sobre el activo que está asociado con este suceso. El contenido de este campo es texto definido por el usuario y depende de los dispositivos de la red que están disponibles para proporcionar información de identidad. Los ejemplos incluyen: ubicación física de dispositivos, políticas pertinentes, conmutador de red y nombres de puerto.

Tabla 21. Detalles de suceso (continuación)

Parámetro	Descripción
Tiene identidad (distintivo)	Especifica Verdadero si QRadar ha recopilado información de identificación para el activo que está asociado con este suceso. Para obtener más información sobre qué dispositivos envían información de identidad, consulte la publicación *IBM Security QRadar DSM Configuration Guide*.
Nombre de host de identidad	Especifica el nombre de host del activo que está asociado con este suceso.
MAC de identidad	Especifica la dirección MAC del activo que está asociado con este suceso.
Nombre de grupo de identidad	Especifica el nombre de grupo del activo que está asociado con este suceso.

Barra de herramientas de detalles de suceso

La barra de herramientas de detalles de sucesos proporciona varias funciones para ver detalles de sucesos.

La barra de herramientas de **detalles de suceso** proporciona las siguientes funciones:

Tabla 22. Barra de herramientas de detalles de suceso

Volver a lista de sucesos	Pulse **Volver** a **Lista de sucesos** para volver a la lista de sucesos.
Delito	Pulse **Delito** para visualizar los delitos que están asociadas con el suceso.
Anomalía	Pulse **Anomalía** para visualizar los resultados de búsqueda guardados que han hecho que la regla de detección de anomalías generara este suceso. **Nota:** Este icono sólo se visualiza si este suceso ha sido generado por una regla de detección de anomalías.
Correlación de sucesos	Pulse **Correlación de suceso** para editar la correlación de sucesos. Para obtener más información, consulte Modificación de correlación de sucesos.
Falso positivo	Pulse **Falso positivo** para ajustar QRadar a fin de evitar que los sucesos positivos falsos generen delitos.
Extraer propiedad	Pulse **Extraer propiedad** para crear una propiedad de suceso personalizada a partir del suceso seleccionado.
Anterior	Pulse **Anterior** para ver el suceso anterior en la lista de sucesos.
Siguiente	Pulse **Siguiente** para ver el siguiente suceso en la lista de sucesos.

Tabla 22. Barra de herramientas de detalles de suceso (continuación)

Datos de PCAP	**Nota:** Esta opción sólo se visualiza si la consola de QRadar se ha configurado para integrarse con el DSM de Juniper JunOS Platform. Para obtener más información sobre cómo gestionar datos de PCAP, consulte Gestión de datos de PCAP. • **Ver información de PCAP**: Seleccione esta opción para ver la información de PCAP. Para obtener más información, consulte Visualización de información de PCAP. • **Descargar archivo de PCAP**: Seleccione esta opción para descargar el archivo de PCAP en el sistema de escritorio. Para obtener más información, consulte Descarga del archivo de PCAP en el sistema.
Imprimir	Pulse **Imprimir** para imprimir los detalles de suceso.

Visualización de delitos asociados

En la pestaña Actividad de registro, puede ver el delito que está asociado con el suceso.

Acerca de esta tarea

Si un suceso coincide con una regla, se puede generar un delito en la pestaña **Delitos**.

Para obtener más información sobre reglas, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Cuando vea un delito en la pestaña **Actividad de registro**, es posible que el delito no se visualice si el magistrado aún no se ha guardado en disco el delito que está asociado con el suceso seleccionado o si el delito se ha depurado de la base de datos. Si esto ocurre, el sistema se lo notificará.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Pulse el icono **Delito** junto al suceso que desea investigar.
4. Vea el delito asociado.

Modificación de la correlación de sucesos

Puede correlacionar manualmente un suceso normalizado o en bruto con una categoría de alto nivel y de bajo nivel (o QID).

Antes de empezar

Esta acción manual se utiliza para correlacionar sucesos de origen de registro desconocidos con sucesos de QRadar conocidos para que se puedan categorizar y procesar adecuadamente.

Acerca de esta tarea

A efectos de normalización, QRadar correlaciona automáticamente sucesos de orígenes de registro con categorías de alto y bajo nivel.

Para obtener más información sobre categorías de suceso, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Si los sucesos se reciben de orígenes de registro que el sistema no puede categorizar, los sucesos se categorizan como desconocidos. Dichos sucesos se producen por distintos motivos, incluyendo:

- **Sucesos definidos por el usuario**: Algunos orígenes de registro, como Snort, le permiten crear sucesos definidos por el usuario.
- **Sucesos nuevos o antiguos**: Los orígenes de registro de proveedor pueden actualizar el software con releases de mantenimiento para soportar sucesos nuevos que es posible que QRadar no soporte.

Nota: El icono **Correlacionar suceso** está inhabilitado para los sucesos cuando la categoría de alto nivel es Auditoría SIM o el tipo de origen de registro es Protocolo de acceso a objetos simple (SOAP).

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Efectúe una doble pulsación en el suceso que desea correlacionar.
4. Pulse **Correlación de suceso**.
5. Si conoce el QID que desea correlacionar con este suceso, escriba el QID en el campo **Especifique los QID**.
6. Si no conoce el QID que desea correlacionar con este suceso, puede buscar un QID específico:
   a. Elija una de las opciones siguientes: `Para buscar un QID por categoría, seleccione la categoría de alto nivel en el recuadro de lista Categoría de alto nivel. Para buscar un QID por categoría, seleccione la categoría de bajo nivel en el recuadro de lista Categoría de bajo nivel. Para buscar un QID por tipo de origen de registro, seleccione un tipo de origen de registro en el recuadro de lista Tipo de origen de registro. Para buscar un QID por nombre, escriba un nombre en el campo QID/Nombre.`
   b. Pulse **Buscar**.
   c. Seleccione **QID** con el que desea asociar este suceso.
7. Pulse **Aceptar**.

Ajustar falsos positivos

Puede utilizar la función Ajuste de falsos positivos para impedir que sucesos de falso positivo generen delitos.

Antes de empezar

Puede ajustar sucesos de falso positivo en la página lista de sucesos o detalles de suceso.

Acerca de esta tarea

Puede ajustar sucesos de falso positivo en la página lista de sucesos o detalles de suceso.

Debe tener permisos adecuados para crear reglas personalizadas para ajustar falsos positivos.

Para obtener más información sobre roles, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Para obtener más información sobre falsos positivos, consulte el Glosario.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. Seleccione el suceso que desee ajustar.
4. Pulse **Falso positivo**.
5. En el panel Propiedad de suceso/flujo de la ventana Falso positivo, seleccione una de las opciones siguientes:
   - Suceso/flujo(s) con un QID específico de <Suceso>
   - Cualquier suceso/flujo(s) con una categoría de bajo nivel de <Suceso>
   - Cualquier suceso/flujo(s) con una categoría de alto nivel de <Suceso>
6. En el panel Dirección de tráfico, seleccione una de las opciones siguientes:
   - <Dirección IP de origen> a <Dirección IP de destino>
   - <Dirección IP de origen> a cualquier destino
   - Cualquier origen a <Dirección IP de destino>
   - Cualquier origen a cualquier destino
7. Pulse **Ajustar**.

Datos de PCAP

Si la consola de QRadar se ha configurado para integrarse con el DSM Juniper JunOS Platform, Packet Capture (PCAP) se puede recibir, procesar y los datos se pueden almacenar de un origen de registro Juniper SRX-Series Services Gateway.

Para obtener más información sobre el DSM Juniper JunOS Platform, consulte la publicación *IBM Security QRadar DSM Configuration Guide*.

Visualización de la columna de datos de PCAP

La columna **Datos de PCAP** no se visualiza en la pestaña **Actividad de registro** de forma predeterminada. Al crear criterios de búsqueda, debe seleccionar la columna **Datos de PCAP** en el panel Definición de columna.

Antes de empezar

Para poder visualizar los datos de PCAP en la pestaña **Actividad de registro**, se debe configurar el origen de registro de Juniper SRX-Series Services Gateway con el protocolo de combinación PCAP Syslog. Para obtener más información sobre cómo configurar protocolos de origen de registro, consulte la publicación *Managing Log Sources Guide*.

Acerca de esta tarea

Cuando se realiza una búsqueda que incluye la columna **Datos de PCAP**, se visualiza un icono en la columna **Datos de PCAP** de los resultados de búsqueda si hay datos de PCAP disponibles para un suceso. Utilizando el icono de **PCAP**, puede ver los datos de PCAP o descargar el archivo **PCAP** en el sistema.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En el recuadro de lista **Buscar**, seleccione **Nueva búsqueda**.
3. Opcional. Para buscar sucesos que tienen datos de PCAP, configure los criterios de búsqueda siguientes:
   a. En el primer recuadro de lista, seleccione **Datos de PCAP**.
   b. En el segundo recuadro de lista, seleccione **Igual que**.
   c. En el tercer recuadro de lista, seleccione **Verdadero**.
   d. Pulse **Añadir filtro**.
4. Configure las definiciones de columna para incluir la columna **Datos de PCAP**:
   a. En la lista **Columnas disponibles** del panel Definición de columna, pulse **Datos de PCAP**.
   b. Pulse el icono **Añadir columna** en el conjunto inferior de iconos para mover la columna **Datos de PCAP** a la lista **Columnas**.
   c. Opcional. Pulse el icono **Añadir columna** en el conjunto superior de iconos para mover la columna **Datos de PCAP** a la lista **Agrupar por**.
5. Pulse **Filtro**.
6. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
7. Efectúe una doble pulsación en el suceso que desee investigar.

Qué hacer a continuación

Para obtener más información sobre cómo ver y descargar datos de PCAP, consulte las secciones siguientes:

- Visualización de la información de PCAP
- Descarga del archivo de PCAP en el sistema

Visualización de la información de PCAP

En el menú de barra de herramientas **Datos de PCAP**, puede ver una versión legible de los datos en el archivo de PCAP o descargar el archivo de PCAP en el sistema.

Antes de empezar

Para poder ver información de PCAP, debe realizar o seleccionar una búsqueda que visualice la columna **Datos de PCAP**.

Acerca de esta tarea

Antes de poder visualizar los datos de PCAP, se debe recuperar el archivo de PCAP para visualizarlo en la interfaz de usuario. Si el proceso de descarga tarda un período de tiempo prolongado, se visualiza la ventana Downloading PCAP Packet information. En la mayoría de los casos, el proceso de descarga es rápido y esta ventana no se visualiza.

Una vez recuperado el archivo, una ventana emergente proporciona una versión legible del archivo de PCAP. Puede leer la información que se visualiza en la ventana o descargar la información en el sistema

Procedimiento

1. Para el suceso que desea investigar, elija una de las opciones siguientes:
   - Seleccione el suceso y pulse el icono **PCAP**.
   - Pulse el botón derecho del ratón en el icono **PCAP** para el suceso y seleccione **Más opciones** > **Ver información de PCAP**.
   - Efectúe una doble pulsación en el suceso que desea investigar y, a continuación, seleccione **Datos de PCAP** > **Ver información de PCAP** en la barra de herramientas de detalles de suceso.
2. Si desea descargar la información en el sistema, seleccione una de las opciones siguientes:
   - Pulse **Descargar archivo de PCAP** para descargar el archivo de PCAP original que se debe utilizar en una aplicación externa.
   - Pulse **Descargar texto de PCAP** para descargar la información de PCAP en formato .TXT
3. Elija una de las siguientes opciones:
   - Si desea abrir el archivo para su visualización inmediata, seleccione la opción **Open with** y seleccione una aplicación en el recuadro de lista.
   - Si desea guardar la lista, seleccione la opción **Save File** .
4. Pulse **Aceptar**.

Descarga del archivo de PCAP en el sistema

Puede descargar el archivo PCAP en el sistema para almacenarlo o para utilizar en otras aplicaciones.

Antes de empezar

Antes de poder ver la información de PCAP, debe realizar o seleccionar una búsqueda que muestre la columna Datos de PCAP. consulte **Visualización de la columna de datos de PCAP**.

Procedimiento

1. Para el suceso que desea investigar, elija una de las opciones siguientes:
   - Seleccione el suceso y pulse el icono **PCAP**.
   - Pulse el botón derecho del ratón en el icono de PCAP para el evento y seleccione **Más opciones** > **Descargar archivo de PCAP**.

- Efectúe una doble pulsación en el suceso que desea investigar, y, a continuación, seleccione **Datos de PCAP** > **Descargar archivo de PCAP** en la barra de herramientas de detalles de suceso.

2. Elija una de las siguientes opciones:
   - Si desea abrir el archivo para su visualización inmediata, seleccione la opción **Open with** y seleccione una aplicación en el recuadro de lista.
   - Si desea guardar la lista, seleccione la opción **Save File** .
3. Pulse **Aceptar**.

Exportación de sucesos

Puede exportar sucesos en formato XML (Extensible Markup Language - Lenguaje de marcas extensible) o CSV (Valores separados por comas).

Antes de empezar

El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos en modalidad continua, pulse el icono de **Pausa** para detener la modalidad continua.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:
   - **Exportar a XML** > **Columnas visibles**: seleccione esta opción para exportar solo las columnas que están visibles en la pestaña Actividad de registro. Esta es la opción recomendada.
   - **Exportar a XML** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
   - **Exportar a CSV** > **Columnas visibles**: Seleccione esta opción para exportar sólo las columnas que están visibles en la pestaña **Actividad de registro**. Esta es la opción recomendada.
   - **Exportar a CSV** > **Exportación completa (Todas las columnas)**: Seleccione esta opción para exportar todos los parámetros de sucesos. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
4. Si desea reanudar las actividades mientras la exportación está en curso, pulse **Notificar cuando termine**.

Resultados

Cuando la exportación se haya completado, recibirá una notificación de que la exportación se ha completado. Si no ha seleccionado el icono **Notificar cuando termine**, se visualiza la ventana de estado.

Capítulo 6. Investigación de la actividad de red

Puede utilizar la pestaña **Actividad de red** para supervisar e investigar la actividad de red (flujos) en tiempo real o realizar búsquedas avanzadas

Visión general de la pestaña Actividad de red

Puede utilizar la pestaña **Actividad de red** para supervisar e investigar actividad de red (flujos) en tiempo real o realizar búsquedas avanzadas.

Debe tener permiso para ver la pestaña **Actividad de red**.

Para obtener más información sobre permisos y asignar roles, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Seleccione la pestaña **Actividad de red** para supervisar e investigar visualmente datos de flujo en tiempo real o realizar búsquedas avanzadas para filtrar los flujos mostrados. Un flujo es una sesión de comunicación entre dos hosts. Puede ver información de flujo para determinar cómo se transmite el tráfico y qué se ha transmitido (si está habilitada la opción de captura de contenido). La información de flujo también puede incluir detalles tales como protocolos, valores de ASN (Autonomous System Number) o valores de IFIndex (Interface Index).

Barra de herramientas de la pestaña Actividad de red

Puede acceder a varias opciones desde la barra de herramientas de la pestaña **Actividad de red**.

Puede acceder a las opciones siguientes desde la barra de herramientas de la pestaña **Actividad de red**:

Tabla 23. Opciones de la barra de herramientas de la pestaña Actividad de red

Opciones	Descripción
Buscar	Pulse **Buscar** para realizar búsquedas avanzadas de flujos. Las opciones de búsqueda incluyen: • **Búsqueda nueva**: seleccione esta opción para crear una búsqueda de flujos nueva. • **Editar búsqueda**: seleccione esta opción para seleccionar y editar una búsqueda de flujos. • **Gestionar resultados de búsqueda**: seleccione esta opción para ver y gestionar resultados de búsqueda. Para obtener más información sobre la función de búsqueda, consulte Búsquedas de datos.
Búsquedas rápidas	Desde este cuadro de lista, puede ejecutar búsquedas guardadas anteriormente. Se muestran opciones en el cuadro de lista **Búsquedas rápidas** sólo si ha guardado criterios de búsqueda que especifican la opción **Incluir en Búsquedas rápidas**.
Añadir filtro	Pulse **Añadir filtro** para añadir un filtro a los resultados de búsqueda actuales.

© Copyright IBM Corp. 2012, 2015

Tabla 23. Opciones de la barra de herramientas de la pestaña Actividad de red (continuación)

Opciones	Descripción
Guardar criterios	Pulse **Guardar criterios** para guardar los criterios de búsqueda actuales.
Guardar resultados	Pulse **Guardar resultados** para guardar los resultados de búsqueda actuales. Esta opción sólo se muestra después de realizar una búsqueda. Esta opción está inhabilitada en la modalidad continua.
Cancelar	Pulse **Cancelar** para cancelar una búsqueda que está en curso. Esta opción está inhabilitada en la modalidad continua.
Falso positivo	Pulse **Falso positivo** para abrir la ventana Ajuste de falsos positivos, que le permite descartar los flujos que se sabe que son falsos positivos en la creación de delitos. Para obtener más información sobre falsos positivos, consulte el Glosario. Esta opción está inhabilitada en la modalidad continua. Consulte Exportar flujos.

Tabla 23. Opciones de la barra de herramientas de la pestaña Actividad de red (continuación)

Opciones	Descripción
Reglas	La opción **Reglas** sólo es visible si tiene permiso para ver reglas personalizadas. Elija una de las siguientes opciones: **Reglas** para ver o crear una regla. Si tiene permiso para ver reglas, se abre la página de resumen del asistente Reglas. Si tiene permiso para mantener reglas personalizadas, puede editar la regla. **Nota:** Las opciones para reglas de detección de anomalías son visibles solamente si tiene el permiso **Actividad de red** > **Mantener reglas personalizadas**. Para habilitar las opciones para reglas de detección de anomalías, debe guardar criterios de búsqueda agregados. Los criterios de búsqueda guardados especifican los parámetros necesarios. Elija una de las siguientes opciones: **Añadir regla de umbral** para crear una regla de umbral. Una regla de umbral comprueba si la actividad del tráfico de flujo sobrepasa un valor umbral configurado. Los umbrales pueden estar basados en cualquier dato recogido. Por ejemplo, si crea una regla de umbral que indica que no más de 220 clientes pueden iniciar una sesión en el servidor entre las 08:00 y las 17:00, la regla genera una alerta cuando el cliente que hace el número 221 intenta iniciar una sesión. **Añadir regla de comportamiento** para crear una regla de comportamiento. Una regla de comportamiento comprueba si hay cambios en el volumen del tráfico de flujo que se producen según patrones estacionales regulares. Por ejemplo, si un servidor de correo normalmente se comunica con 100 hosts por segundo en la mitad de la noche y después súbitamente inicia la comunicación con 1.000 hosts por segundo, una regla de comportamiento genera una alerta. **Añadir regla de anomalía** para crear una regla de anomalía. Una regla de anomalía comprueba si hay actividad anómala en el tráfico de flujo, tal como tráfico nuevo o desconocido. Por ejemplo, puede crear una regla de anomalía para comparar el volumen promedio de tráfico existente durante los últimos 5 minutos con el volumen promedio de tráfico existente durante la última hora. Si se produce un cambio de más del 40%, la regla genera un respuesta. Para obtener más información, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Tabla 23. Opciones de la barra de herramientas de la pestaña Actividad de red (continuación)

Opciones	Descripción
Acciones	Pulse **Acciones** para realizar las acciones siguientes: • **Mostrado todos**: seleccione esta opción para eliminar todos los filtros en los criterios de búsqueda y visualizar todos los flujos sin filtrar. • **Imprimir**: seleccione esta opción para imprimir los flujos que aparecen en la página. • **Exportar a XML**: seleccione esta opción para exportar flujos en formato XML. Consulte Exportar flujos. • **Exportar a CSV**: seleccione esta opción para exportar flujos en formato CSV. Consulte Exportar flujos. • **Suprimir**: seleccione esta opción para suprimir un resultado de búsqueda. Consulte Búsquedas de datos. • **Notificar**: seleccione esta opción para especificar que desea recibir una notificación por correo electrónico cuando finalicen las búsquedas seleccionadas. Esta opción sólo está habilitada para búsquedas en curso. **Nota:** Las opciones **Imprimir**, **Exportar a XML** y **Exportar a CSV** están inhabilitadas en la modalidad continua y cuando está viendo resultados de búsqueda parciales.
Barra de herramientas de búsqueda	**Búsqueda avanzada** Seleccione **Búsqueda avanzada** en el cuadro de lista y escriba una cadena de búsqueda de Ariel Query Language (AOL) para especificar los campos que desee que se devuelvan. **Filtro rápido** Seleccione **Filtro rápido** en el cuadro de lista para buscar cargas útiles mediante palabras o frases simples.
Ver	La vista predeterminada de la pestaña **Actividad de red** es una corriente de sucesos en tiempo real. La lista **Ver** contiene opciones para ver también sucesos de periodos de tiempo específicos. Después de elegir un periodo de tiempo especificado de la lista **Ver** puede modificar el periodo de tiempo visualizado cambiando los valores de fecha y hora en los campos **Hora de inicio** y **Hora de finalización**.

Opciones de menú que aparecen al pulsar el botón derecho del ratón

En la pestaña **Actividad de red**, puede pulsar con el botón derecho del ratón en un flujo para acceder a más criterios de filtro de flujos.

Las opciones de menú que aparecen al pulsar el botón derecho del ratón son las siguientes:

Tabla 24. Opciones de menú que aparecen al pulsar el botón derecho del ratón

Opción	Descripción
Filtrar por	Seleccione esta opción para filtrar de acuerdo con el flujo seleccionado, dependiendo del parámetro seleccionado en el flujo.
Falso positivo	Seleccione esta opción para abrir la ventana Ajuste de falsos positivos, que le permite descartar los flujos que se sabe que son falsos positivos en la creación de delitos. Esta opción está inhabilitada en la modalidad continua. Consulte Exportar flujos.
Más opciones:	Seleccione esta opción para investigar una dirección IP. Consulte Investigar direcciones IP. **Nota:** Esta opción no se muestra en la modalidad continua.
Filtro rápido	Filtrar elementos que coinciden o no coinciden con la selección.

Barra de estado

Para los flujos de modalidad continua, la barra de estado muestra el número promedio de resultados que se reciben por segundo.

Esto es el número de resultados que la consola ha recibido satisfactoriamente procedentes de los procesadores de sucesos. Si este número es mayor que 40 resultados por segundo, sólo se visualizarán 40 resultados. El resto se acumula en el almacenamiento intermedio de resultados. Para ver más información de estado, coloque el puntero del ratón encima de la barra de estado.

Cuando los flujos no son de modalidad continua, la barra de estado muestra el número de resultados de búsqueda que se muestran actualmente y la cantidad de tiempo necesaria para procesar los resultados de la búsqueda.

Registros de desbordamiento

Si tiene permisos administrativos, puede especificar el número máximo de flujos que desea enviar desde QRadar QFlow Collector a los procesadores de sucesos.

Si tiene permisos administrativos, puede especificar el número máximo de flujos que desea enviar desde QRadar QFlow Collector a los procesadores de sucesos. Todos los datos que se recogen después alcanzar el límite de flujos configurado se agrupan en un solo registro de flujo. Este registro de flujo se visualiza entonces en la pestaña **Actividad de red** con una dirección IP de origen de 127.0.0.4 y una dirección IP de destino de 127.0.0.5. Este registro de flujo especifica Desbordamiento en la pestaña **Actividad de red**.

Supervisión de la actividad de red

De forma predeterminada, la pestaña **Actividad de red** muestra flujos en modalidad continua, lo que le permite ver flujos en tiempo real.

Para obtener más información sobre la modalidad continua, consulte Visualizar flujos en modalidad continua. Puede especificar un rango de tiempo diferente para filtrar los flujos mediante el cuadro de lista **Ver**.

Si previamente ha configurado una búsqueda guardada predeterminada, los resultados de esa búsqueda se muestran automáticamente cuando abre la pestaña **Actividad de red**. Para obtener más información sobre cómo guardar criterios de búsqueda, consulte Guardar criterios de búsqueda de sucesos y flujos.

Ver flujos continuos

La modalidad continua le permite ver datos de flujo a medida que entran en el sistema. Esta modalidad le proporciona una visión en tiempo real de la actividad de flujo actual al mostrar los últimos 50 flujos.

Acerca de esta tarea

Si aplica filtros en la pestaña Actividad de red o en los criterios de búsqueda antes de habilitar la modalidad continua, los filtros se conservan en la modalidad continua. Pero la modalidad continua no permite realizar búsquedas que incluyen flujos agrupados. Si habilita la modalidad continua para flujos agrupados o criterios de búsqueda agrupados, la pestaña Actividad de red muestra los flujos normalizados. Consulte Ver flujos normalizados.

Cuando desea seleccionar un flujo para ver detalles o realizar una acción, debe poner en pausa la modalidad continua antes de seleccionar un suceso. Cuando la modalidad continua está en pausa, se muestran los últimos 1.000 flujos.

Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En el cuadro de lista Ver, seleccione **Tiempo real (modalidad continua)**.

Para obtener más información sobre las opciones de la barra de herramientas, consulte la Tabla 5-1. Para obtener más información sobre los parámetros que se visualizan en la modalidad continua, consulte la Tabla 5-3.

3. Opcional. Ponga en pausa o inicie los flujos continuos. Elija una de las siguientes opciones:
   - Para seleccionar un registro de suceso, pulse el icono **Pausar** para poner en pausa la modalidad continua.
   - Para reiniciar la modalidad continua, pulse el icono **Reproducir**.

Ver flujos normalizados

El flujo de datos se captura, normaliza y luego visualiza en la pestaña **Actividad de red**.

Acerca de esta tarea

La normalización implica preparar datos de flujo para visualizar información legible en la pestaña.

Nota: Si selecciona un intervalo de tiempo para visualizar, se muestra un gráfico de serie temporal. Para obtener más información sobre el uso de gráficos de serie temporal, consulte Visión general de los gráficos de serie temporal.

La pestaña **Actividad de red** muestra los parámetros siguientes cuando visualiza flujos normalizados:

Tabla 25. Parámetros de la pestaña Actividad de red

Parámetro	Descripción
Filtros actuales	La parte superior de la tabla muestra los detalles de los filtros que se aplican a los resultados de la búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**. **Nota:** Este parámetro sólo se muestra después de aplicar un filtro.
Ver	En el cuadro de lista, seleccione el rango de tiempo para el que desee aplicar el filtro.
Estadísticas actuales	Cuando no está en la modalidad de tiempo real (modalidad continua) ni de Último minuto (renovación automática), se muestran las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto Estadísticas actuales para mostrar u ocultar las estadísticas. • **Resultados totales**: especifica el número total de resultados que coinciden con los criterios de búsqueda. • **Archivos de datos buscados**: especifica el número total de archivos de datos que se han buscado durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: especifica el número total de archivos de datos comprimidos que se han buscado dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: especifica el número total de archivos de índices que se han buscado durante el intervalo de tiempo especificado. • **Duración**: especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el servicio de atención al cliente para resolver problemas de flujos, se le puede solicitar que proporcione información estadística actual.

Tabla 25. Parámetros de la pestaña Actividad de red (continuación)

Parámetro	Descripción
Gráficos	Muestra gráficos configurables que representan los registros correspondientes al intervalo de tiempo y la opción de agrupación. Pulse **Ocultar gráficos** si no desea que aparezcan los gráficos en la pantalla. Los gráficos solo se muestran después de seleccionar un rango de tiempo de Último intervalo (renovación automática) o superior, y una opción de agrupación para visualizar. Para obtener más información sobre la configuración de gráficos, consulte Configurar gráficos. **Nota:** Si utiliza Mozilla Firefox como navegador y está instalado un bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe desinstalar el bloqueador de anuncios. Para obtener más información, consulte la documentación del navegador.
Icono **Delito**	Pulse el icono **Delitos** para ver detalles del delito que está asociado al flujo.
Tipo de flujo	Especifica el tipo de flujo. Los tipos de flujo se miden de acuerdo con la proporción entre la actividad de entrada y la actividad de salida. Los tipos de flujo son los siguientes: • **Estándar**: tráfico bidireccional • **Tipo A**: de uno a muchos (unidireccional), por ejemplo, un host que realiza una exploración de red. • **Tipo B**: de muchos a uno (unidireccional), por ejemplo, un ataque de denegación de servicio distribuido (DDoS). • **Tipo C**: de uno a uno (unidireccional), por ejemplo, una exploración de puertos de host a host.
Hora de primer paquete	Especifica la fecha y hora en que se recibió el flujo.
Hora de almacenamiento	Especifica la hora en que se almacenó el flujo en la base de datos de QRadar.
IP de origen	Especifica la dirección IP de origen del flujo.
Puerto de origen	Especifica el puerto de origen del flujo.
IP de destino	Especifica la dirección IP de destino del flujo.
Puerto de destino	Especifica el puerto de destino del flujo.
Bytes de origen	Especifica el número de bytes enviados desde el host de origen.
Bytes de destino	Especifica el número de bytes enviados desde el host de destino.
Bytes totales	Especifica el número total de bytes del flujo.

Tabla 25. Parámetros de la pestaña Actividad de red (continuación)

Parámetro	Descripción
Paquetes de origen	Especifica el número total de paquetes que se envían desde el host de origen.
Paquetes de destino	Especifica el número total de paquetes que se envían desde el host de destino.
Paquetes totales	Especifica el número total de paquetes que están asociados al flujo.
Protocolo	Especifica el protocolo que está asociado al flujo.
Aplicación	Especifica la aplicación detectada del flujo. Para obtener más información sobre la detección de aplicaciones, consulte el manual *IBM Security QRadar Application Configuration Guide*.
Tipo/código de ICMP	Especifica el tipo y código de ICMP (Internet Control Message Protocol), si es pertinente. Si el flujo tiene un tipo y código de ICMP en un formato conocido, este campo se visualiza como Tipo <A>. Código <B>, donde <A> y <B> son los valores numéricos del tipo y del código.
Distintivos de origen	Especifica los distintivos de TCP (Transmission Control Protocol) detectados en el paquete de origen, si es pertinente.
Distintivos de destino	Especifica los distintivos de TCP detectados en el paquete de destino, si es pertinente.
Calidad de servicio de origen	Especifica el nivel de calidad de servicio (QoS) del flujo. La calidad de servicio permite a una red proporcionar diversos niveles de servicio para los flujos. La calidad de servicio proporciona los niveles siguientes de servicio básico: • **Mejor esfuerzo**: este nivel de servicio no garantiza la entrega. La entrega del flujo está considerada la mejor posible. • **Servicio diferenciado**: se otorga prioridad a determinados flujos con respecto a otros. Esta prioridad se otorga de acuerdo con la clasificación del tráfico. • **Servicio garantizado**: este nivel de servicio garantiza la reserva de recursos de red para flujos determinados.
Calidad de servicio de destino	Especifica el nivel de calidad de servicio del flujo de destino.
Origen de flujo	Especifica sistema que detectó el flujo.
Interfaz de flujo	Especifica la interfaz que recibió el flujo.
IFIndex de origen	Especifica el número de índice de interfaz (IFIndex) del origen.
IFIndex de destino	Especifica el número de índice de interfaz (IFIndex) del destino.

Tabla 25. Parámetros de la pestaña Actividad de red (continuación)

Parámetro	Descripción
ASN de origen	Especifica el valor de ASN (Autonomous System Number) del origen.
ASN de destino	Especifica el valor de ASN del destino.

Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En el cuadro de lista **Visualizar**, seleccione **Valor predeterminado (normalizado)**.
3. En el cuadro de lista **Ver**, seleccione el rango de tiempo que desee ver.
4. Pulse el icono **Pausar** para detener la modalidad continua.
5. Efectúe una doble pulsación en el flujo que desee ver con mayor detalle. Consulte Detalles de flujo.

Ver flujos agrupados

En la pestaña **Actividad de red**, puede ver flujos que están agrupados según diversas opciones. En el cuadro de lista **Visualizar**, puede seleccionar el parámetro para el que desee agrupar flujos.

Acerca de esta tarea

El cuadro de lista **Visualizar** no aparece en la modalidad continua porque esta modalidad no da soporte a los flujos agrupados. Si ha entrado en la modalidad continua utilizando criterios de búsqueda no agrupados, esta opción se visualiza.

El cuadro de lista **Visualizar** proporciona las opciones siguientes:

Tabla 26. Opciones para flujos agrupados

Opción de agrupación	Descripción
IP de origen o destino	Muestra una lista resumida de flujos que están agrupados por la dirección IP del flujo.
IP de origen	Muestra una lista resumida de flujos que están agrupados por la dirección IP de origen del flujo.
IP de destino	Muestra una lista resumida de flujos que están agrupados por la dirección IP de destino del flujo.
Puerto de origen	Muestra una lista resumida de flujos que están agrupados por el puerto de origen del flujo.
Puerto de destino	Muestra una lista resumida de flujos que están agrupados por el puerto de destino del flujo.
Red de origen	Muestra una lista resumida de flujos que están agrupados por la red de origen del flujo.
Red de destino	Muestra una lista resumida de flujos que están agrupados por la red de destino del flujo.

Tabla 26. Opciones para flujos agrupados (continuación)

Opción de agrupación	Descripción
Aplicación	Muestra una lista resumida de flujos que están agrupados por la aplicación que generó el flujo.
Geográfico	Muestra una lista resumida de flujos que están agrupados por la ubicación geográfica.
Protocolo	Muestra una lista resumida de flujos que están agrupados por el protocolo del flujo.
Sesgo de flujo	Muestra una lista resumida de flujos que están agrupados por la dirección del flujo.
Tipo ICMP	Muestra una lista resumida de flujos que están agrupados por el tipo ICMP del flujo.

Después de seleccionar una opción en el cuadro de lista **Visualizar**, la disposición de las columnas de datos depende de la opción de agrupación elegida. Cada fila de la tabla de flujos representa un grupo de flujos. La pestaña **Actividad de red** proporciona la información siguiente para cada grupo de flujos.

Tabla 27. Parámetros de flujos agrupados

Cabecera	Descripción
Agrupación por	Especifica el parámetro para el que se agrupa la búsqueda.
Filtros actuales	En la parte superior de la tabla se muestran los detalles del filtro que se aplica a los resultados de búsqueda. Para borrar estos valores de filtro, pulse **Borrar filtro**.
Ver	En el cuadro de lista, seleccione el rango de tiempo para el que desee aplicar el filtro.

Tabla 27. Parámetros de flujos agrupados (continuación)

Cabecera	Descripción
Estadísticas actuales	Cuando no está en la modalidad de tiempo real (modalidad continua) ni de Último minuto (renovación automática), se muestran las estadísticas actuales, que incluyen: **Nota:** Pulse la flecha situada junto a **Estadísticas actuales** para mostrar u ocultar las estadísticas. • **Resultados totales**: especifica el número total de resultados que coinciden con los criterios de búsqueda. • **Archivos de datos buscados**: especifica el número total de archivos de datos que se han buscado durante el intervalo de tiempo especificado. • **Archivos de datos comprimidos buscados**: especifica el número total de archivos de datos comprimidos que se han buscado dentro del intervalo de tiempo especificado. • **Recuento de archivos de índices**: especifica el número total de archivos de índices que se han buscado durante el intervalo de tiempo especificado. • **Duración**: especifica la duración de la búsqueda. **Nota:** Las estadísticas actuales son útiles para la resolución de problemas. Cuando se ponga en contacto con el servicio de atención al cliente para resolver problemas de flujos, se le puede solicitar que proporcione información estadística actual.
Gráficos	Muestra gráficos configurables que representan los registros que se asocian de acuerdo con el intervalo de tiempo y la opción de agrupación. Pulse **Ocultar gráficos** si no desea que aparezcan los gráficos en la pantalla. Los gráficos solo se muestran después de seleccionar un rango de tiempo de Último intervalo (renovación automática) o superior, y una opción de agrupación para visualizar. Para obtener más información sobre la configuración de gráficos, consulte Configurar gráficos. **Nota:** Si utiliza Mozilla Firefox como navegador y está instalado un bloqueador de anuncios, los gráficos no se visualizan. Para visualizar gráficos, debe desinstalar el bloqueador de anuncios. Para obtener más información, consulte la documentación del navegador.
IP de origen (recuento exclusivo)	Especifica la dirección IP de origen del flujo.

Tabla 27. Parámetros de flujos agrupados (continuación)

Cabecera	Descripción
IP de destino (recuento exclusivo)	Especifica la dirección IP de destino del flujo. Si hay varias direcciones IP de destino asociadas al flujo, este campo especifica el término Múltiple y el número de direcciones IP.
Puerto de origen (recuento exclusivo)	Muestra el puerto de origen del flujo.
Puerto de destino (recuento exclusivo)	Especifica el puerto de destino del flujo. Si hay varios puertos de destino que están asociados al flujo, este campo contiene el término Múltiple y el número de puertos.
Red de origen (recuento exclusivo)	Especifica la red de origen del flujo. Si hay varias redes de origen que están asociadas al flujo, este campo contiene el término Múltiple y el número de redes.
Red de destino (recuento exclusivo)	Especifica la red de destino del flujo. Si hay varias redes de destino que están asociadas al flujo, este campo contiene el término Múltiple y el número de redes.
Aplicación (recuento exclusivo)	Especifica la aplicación detectada de los flujos. Si hay varias aplicaciones que están asociadas al flujo, este campo contiene el término Múltiple y el número de aplicaciones.
Bytes de origen (suma)	Especifica el número de bytes procedentes del origen.
Bytes de destino (suma)	Especifica el número de bytes procedentes del destino.
Bytes totales (suma)	Especifica el número total de bytes del flujo.
Paquetes de origen (suma)	Especifica el número de paquetes procedentes del origen.
Paquetes de origen (suma)	Especifica el número de paquetes procedentes del origen.
Paquetes de origen (suma)	Especifica el número de paquetes procedentes del origen.
Paquetes de destino (suma)	Especifica el número de paquetes procedentes del destino.
Paquetes totales (suma)	Especifica el número total de paquetes del flujo.
Recuento	Especifica el número de flujos que se han enviado o recibido.

Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En el cuadro de lista **Ver**, seleccione el rango de tiempo que desee ver.
3. En el cuadro de lista **Visualizar**, seleccione el parámetro para el que desee agrupar flujos. Consulte la Tabla 2. Los grupos de flujos aparecen listados. Para obtener más información sobre los detalles de grupos de flujos, consulte la Tabla 1.

4. Para ver la página Lista de flujos para un grupo, haga una doble pulsación en el grupo de flujos que desee investigar. La página Lista de flujos no conserva las configuraciones de gráficos que haya definido en la pestaña **Actividad de red**. Para obtener más información sobre los parámetros de la página Lista de flujos, consulte la Tabla 2.
5. Para ver los detalles de un flujo, haga una doble pulsación en el flujo que desee investigar. Para obtener más información sobre la página Detalles de flujo, consulte la Tabla 1.

Detalles de flujo

Puede ver una lista de flujos en modalidades diversas, incluida la modalidad continua o en grupos de flujos. En cualquier modalidad que elija para ver flujos, puede localizar y ver los detalles de un flujo individual.

La página Detalles de flujo proporciona la información siguiente:

Tabla 28. Detalles de flujo

Parámetro	Descripción
Información de flujo	
Protocolo	Especifica el protocolo que está asociado al flujo. Para obtener más información sobre protocolos, consulte el manual *IBM Security QRadar Application Configuration Guide*.
Aplicación	Especifica la aplicación detectada del flujo. Para obtener más información sobre la detección de aplicaciones, consulte el manual *IBM Security QRadar Application Configuration Guide*.
Magnitud	Especifica la magnitud del flujo. Para obtener más información sobre la magnitud, consulte el Glosario.
Importancia	Especifica la importancia del flujo. Para obtener más información sobre la importancia, consulte el Glosario.
Gravedad	Especifica la gravedad del flujo. Para obtener más información sobre la gravedad, consulte el Glosario.
Credibilidad	Especifica la credibilidad del flujo. Para obtener más información sobre la credibilidad, consulte el Glosario.
Hora de primer paquete	Especifica la hora de inicio del flujo, tal como ha sido notificada por el origen de flujo. Para obtener más información sobre orígenes de flujo, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
Hora de último paquete	Especifica la hora de finalización del flujo, tal como ha sido notificada por el origen de flujo.
Hora de almacenamiento	Especifica la hora en la que el flujo se ha almacenado en la base de datos de QRadar.

Tabla 28. Detalles de flujo (continuación)

Parámetro	Descripción
Nombre de suceso	Especifica el nombre normalizado del flujo.
Categoría de nivel bajo	Especifica la categoría de nivel bajo del flujo. Para obtener más información sobre categorías, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
Descripción del suceso	Especifica una descripción del flujo, si está disponible.
Información sobre origen y destino	
IP de origen	Especifica la dirección IP de origen del flujo.
IP de destino	Especifica la dirección IP de destino del flujo.
Nombre de activo de origen	Especifica el nombre de activo de origen del flujo. Para obtener más información sobre activos, consulte Gestión de activos.
Nombre de activo de destino	Especifica el nombre de activo de destino del flujo. Para obtener más información sobre activos, consulte Gestión de activos.
Origen IPv6	Especifica la dirección IPv6 de origen del flujo.
Destino IPv6	Especifica la dirección IPv6 de destino del flujo.
Puerto de origen	Especifica el puerto de origen del flujo.
Puerto de destino	Especifica el puerto de destino del flujo.
Calidad de servicio de origen	Especifica el nivel de calidad de servicio del flujo de origen.
Calidad de servicio de destino	Especifica el nivel de calidad de servicio del flujo de destino.
ASN de origen	Especifica el número ASN de origen. **Nota:** Si el flujo tiene registros duplicados de varios orígenes de flujo, se listan los correspondientes números ASN de origen.
ASN de destino	Especifica el número ASN de destino. **Nota:** Si el flujo tiene registros duplicados de varios orígenes de flujo, se listan los correspondientes números ASN de destino.
IFIndex de origen	Especifica el número IFIndex de origen. **Nota:** Si el flujo tiene registros duplicados de varios orígenes de flujo, se listan los correspondientes números IFIndex de origen.
IFIndex de destino	Especifica el número IFIndex de destino. **Nota:** Si el flujo tiene registros duplicados de varios orígenes de flujo, se listan los correspondientes números IFIndex de origen.
Carga útil de origen	Especifica el recuento de paquetes y de bytes para la carga útil de origen.

Tabla 28. Detalles de flujo (continuación)

Parámetro	Descripción
Carga útil de destino	Especifica el recuento de paquetes y de bytes para la carga útil de destino.
Información sobre la carga útil	
Carga útil de origen	Especifica el contenido de la carga útil de origen del flujo. Este campo ofrece 3 formatos para ver la carga útil: • Universal Transformation Format (UTF) - Pulse UTF. • Hexadecimal - Pulse HEX. • Base64 - Pulse Base64. **Nota:** Si el origen de flujo es Netflow v9 o IPFIX, el campo **Carga útil de origen** puede mostrar campos no analizados pertenecientes a esos orígenes. El formato del campo no analizado es <nombre>=<valor>. Por ejemplo, `MN_TTL=x`
Carga útil de destino	Especifica el contenido de la carga útil de destino del flujo. Este campo ofrece 3 formatos para ver la carga útil: • Universal Transformation Format (UTF) - Pulse **UTF**. • Hexadecimal - Pulse **HEX**. • Base64 - Pulse **Base64**.
Información adicional	
Tipo de flujo	Especifica el tipo de flujo. Los tipos de flujo se miden de acuerdo con la proporción entre la actividad de entrada y la actividad de salida. Los tipos de flujo son los siguientes: • Estándar: tráfico bidireccional • Tipo A: de uno a muchos (unidireccional) • Tipo B: de muchos a uno (unidireccional) • Tipo C: de uno a uno (unidireccional)
Dirección del flujo	Especifica la dirección del flujo. La dirección del flujo puede ser: • L2L: tráfico interno desde una red local a otra red local. • L2R: tráfico interno de una red local a una red remota. • R2L: tráfico interno desde una red remota a una red local. • R2R: tráfico interno de una red remota a otra red remota.
Reglas personalizadas	Especifica reglas personalizadas que coinciden con el flujo. Para obtener más información sobre reglas, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.
Reglas personalizadas que coinciden parcialmente	Especifica reglas personalizadas que coinciden parcialmente con el flujo.

Tabla 28. Detalles de flujo (continuación)

Parámetro	Descripción
Origen/interfaz de flujo	Especifica el nombre de origen de flujo del sistema que detectó el flujo. **Nota:** Si el flujo tiene registros duplicados de varios orígenes de flujo, se listan los correspondientes orígenes de flujo.
Anotaciones	Especifica las anotaciones o notas del flujo. Las anotaciones son descripciones de texto que pueden ser añadidas automáticamente por una regla como parte de la respuesta de la regla.

Barra de herramientas de detalles de flujo

La barra de herramientas de detalles de flujo proporciona diversas funciones.

La barra de herramientas de detalles de flujo proporciona las funciones siguientes

Tabla 29. Descripción de la barra de herramientas de detalles de flujo

Función	Descripción
Volver a resultados	Pulse **Volver a resultados** para volver a la lista de flujos.
Extraer propiedad	Pulse **Extraer propiedad** para crear una propiedad de flujo personalizada del flujo seleccionado. Para obtener más información, consulte Propiedades de suceso y de flujo personalizadas.
Falso positivo	Pulse **Falso positivo** para abrir la ventana Ajuste de falsos positivos, que le permite descartar los flujos que se sabe que son falsos positivos en la creación de delitos. Esta opción está inhabilitada en la modalidad continua. Consulte Exportar flujos.
Anterior	Pulse **Anterior** para ver el flujo anterior en la lista de flujos.
Siguiente	Pulse **Siguiente** para ver el flujo siguiente en la lista de flujos.
Imprimir	Pulse **Imprimir** para imprimir los detalles de flujo.
Delito	Si la opción **Delito** está disponible, pulse en ella para ver la página Resumen de delitos.

Ajustar falsos positivos

Puede utilizar la función Ajuste de falsos positivos para impedir que flujos de falso positivo generen delitos. Puede ajustar flujos de falso positivo en la página lista de flujos o detalles de flujo.

Acerca de esta tarea

Nota: Puede ajustar flujos de falso positivo en la página de resumen o de detalles.

Debe tener permisos adecuados para crear reglas personalizadas para ajustar falsos positivos. Para obtener más información sobre falsos positivos, consulte el Glosario.

Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. Opcional. Si está viendo flujos en la modalidad continua, pulse el icono **Pausar** para detener la modalidad continua.
3. Seleccione el flujo que desee ajustar.
4. Pulse **Falso positivo**.
5. En el panel Propiedad de suceso/flujo de la ventana Falso positivo, seleccione una de las opciones siguientes:
   - Suceso/flujo(s) con un QID específico de <Suceso>
   - Cualquier suceso/flujo(s) con una categoría de bajo nivel de <Suceso>
   - Cualquier suceso/flujo(s) con una categoría de alto nivel de <Suceso>
6. En el panel Dirección de tráfico, seleccione una de las opciones siguientes:
   - <Dirección IP de origen> a <Dirección IP de destino>
   - <Dirección IP de origen> a cualquier destino
   - Cualquier origen a <Dirección IP de destino>
   - Cualquier origen a cualquier destino
7. Pulse **Ajustar**.

Exportar flujos

Puede exportar flujos en formato XML (Extensible Markup Language) o CSV (Comma Separated Values). El periodo de tiempo necesario para exportar los datos depende del número de parámetros especificados.

Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. Opcional. Si está viendo flujos en la modalidad continua, pulse el icono **Pausar** para detener la modalidad continua.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:
   - **Exportar a XML** > **Columnas visibles**: seleccione esta opción para exportar sólo las columnas que son visibles en la pestaña Actividad de registro. Esto es la acción recomendada.
   - **Exportar a XML** > **Exportación completa (Todas las columnas)**: seleccione esta opción para exportar todos los parámetros de flujo. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
   - **Exportar a CSV** > **Columnas visibles**: seleccione esta opción para exportar sólo las columnas que son visibles en la pestaña Actividad de registro. Esto es la acción recomendada.
   - **Exportar a CSV** > **Exportación completa (Todas las columnas)**: seleccione esta opción para exportar todos los parámetros de flujo. Una exportación completa puede tardar un periodo prolongado de tiempo en completarse.
4. Si desea reanudar las actividades, pulse **Notificar al terminar**.

Resultados

Cuando la exportación se haya completado, recibirá una notificación de que la exportación se ha completado. Si no ha seleccionado el icono **Notificar al terminar**, se mostrará la ventana Estado.

Capítulo 7. Gestión de activos

La recopilación y la visualización de datos de activos le ayuda a identificar las amenazas y las vulnerabilidades. Una base de datos de activos precisa facilita la conexión de los delitos que se desencadenan en el sistema a activos físicos o virtuales en la red.

Restricción: QRadar Log Manager solo hace un seguimiento de datos de activo si QRadar Vulnerability Manager está instalado. Para obtener más información sobre las diferencias entre IBM Security QRadar SIEM y IBM Security QRadar Log Manager, consulte "Prestaciones de su producto de inteligencia y seguridad" en la página 5.

Datos de activos

Un *activo* es cualquier punto final de la red que envía o recibe datos a través de la infraestructura de la red. Por ejemplo, son activos los portátiles, los servidores, las máquinas virtuales y los dispositivos portátiles. A cada activo de la base de datos de activos se le asigna un identificador exclusivo para que pueda distinguirse de los demás registros de activos.

La detección de dispositivos también es útil para crear un conjunto de datos de información histórica sobre el activo. Hacer un seguimiento de la información de activos a medida que cambia le ayuda a supervisar el uso de los activos en la red.

Perfiles de activo

Un *perfil de activo* es una recopilación de toda la información que IBM Security QRadar SIEM ha recogido a lo largo del tiempo acerca de un activo específico. El perfil incluye información acerca de los servicios que se están ejecutando en el activo y toda la información de identidad que se conozca.

QRadar SIEM crea automáticamente perfiles de activo a partir de los sucesos de identidad y los datos de flujos bidireccionales o, si están configuradas, las exploraciones de evaluación de vulnerabilidades. Los datos se correlacionan a través de un proceso que se denomina *conciliación de activos* y el perfil se actualiza a medida que llega información nueva a QRadar. El nombre del activo se deriva de la información de la actualización del activo en el siguiente orden de prioridad:

- Nombre
- Nombre de host NETBios
- Nombre de host DNS
- Dirección IP

Recopilación de datos de activos

Los perfiles de activos se construyen dinámicamente a partir de información de identidad que se absorbe pasivamente de datos de sucesos o de flujos o de datos que QRadar busca activamente durante una exploración de vulnerabilidad. También puede importar datos de activo o editar manualmente el perfil de activo.

© Copyright IBM Corp. 2012, 2015

Orígenes de datos de activos

Se reciben datos de activos de diversos orígenes en el despliegue de IBM Security QRadar.

Los datos de activos se escriben en la base de datos de activos de forma incremental, normalmente dos o tres datos a la vez. A excepción de las actualizaciones de los exploradores de vulnerabilidades de red, cada actualización de activo contiene información sobre un solo activo.

Los datos de activos generalmente provienen de uno de los orígenes de datos de activos siguientes:

Sucesos
Las cargas útiles de sucesos, tales como las creadas por DHCP o servidores de autenticación, a menudo contienen inicios de sesión de usuario, direcciones IP, nombres de hosts, direcciones MAC y otro tipo de información de activos. Estos datos se proporcionan inmediatamente a la base de datos de activos para ayudar a determinar a qué activo se aplica la actualización de activo.

Los sucesos son la causa principal de las desviaciones de crecimiento de activos.

Flujos Las cargas útiles de flujo contienen información de comunicación, como la dirección IP, el puerto y el protocolo, que se recopila a intervalos regulares configurables. Al final de cada intervalo, los datos se proporcionan a la base de datos de activos, una dirección IP cada vez.

Puesto que los datos de activos de los flujos están emparejados con un activo según un solo identificador, la dirección IP, los datos de flujo nunca son la causa de las desviaciones de crecimiento de activos.

Exploradores de vulnerabilidades
QRadar se integra tanto con exploradores de vulnerabilidades de IBM como de terceros que puedan proporcionar datos de activos tales como el sistema operativo, el software instalado y la información de parches. El tipo de datos varía de un explorador a otro y puede variar de una exploración a otra. A medida que se descubren nuevos activos, nueva información de puertos y nuevas vulnerabilidades, los datos se llevan al perfil de activo en función de los rangos de CIDR que están definidos en la exploración.

Los exploradores pueden añadir desviaciones de crecimiento de activos, pero no es habitual.

Interfaz de usuario
Los usuarios que tienen el rol de activos pueden importar o proporcionar información de activos directamente a la base de datos de activos. Las actualizaciones de activos proporcionadas directamente por un usuario son para un activo específico y, por lo tanto, la etapa de conciliación de activos se omite.

Las actualizaciones de activos proporcionadas por los usuarios no añaden desviaciones de crecimiento de activos.

Datos de activos que tienen en cuenta el dominio

Cuando un origen de datos de activos está configurado con información de dominio, todos los datos de activos que provienen de ese origen de datos se

etiquetan automáticamente con el mismo dominio. Puesto que los datos del modelo de activos tienen en cuenta el dominio, la información de dominio se aplica a todos los componentes de QRadar, incluidos las identidades, los delitos, los perfiles de activo y el descubrimiento de servidores.

Cuando vea el perfil de activo, algunos campos podrían estar en blanco. Los campos en blanco existen cuando el sistema no ha recibido esta información en una actualización de activo o la información ha sobrepasado el periodo de retención de activos. El periodo predeterminado de retención es 120 días. Una dirección IP que aparezca como 0.0.0.0 indica que el activo no contiene información de dirección IP.

Flujo de trabajo para datos de activos entrantes

Este flujo de trabajo describe la manera en que QRadar utiliza la información de identidad en una carga útil de suceso para determinar si se crea un nuevo activo o si se actualiza un activo existente.

1. QRadar recibe el suceso. El perfilador de activos examina la carga útil del suceso para obtener la información de identidad.
2. Si la información de identidad incluye una dirección MAC, nombres de host NetBIOS o un nombre de host DNS que ya están asociados con un activo en la base de datos de activos, ese activo se actualiza con la información nueva.
3. Si la única información de identidad disponible es una dirección IP, el sistema concilia la actualización del activo existente que tenga la misma dirección IP.
4. Si una actualización de activo incluye una dirección IP que coincide con un activo existente, pero también incluye más información de identidad que no coincide con el activo existente, el sistema utiliza otra información para descartar un falso positivo en la coincidencia antes de que el activo existente se actualice.
5. Si la información de identidad no coincide con un activo existente en la base de datos, se crea un nuevo activo basado en la información de la carga útil del suceso.

Actualizaciones de los datos de activos

IBM Security QRadar utiliza la información de identidad en una carga útil de suceso para determinar si se crea un nuevo activo o si se actualiza un activo existente.

Cada actualización de activo debe contener información de confianza acerca de un único activo. Cuando QRadar recibe una actualización de activo, el sistema determina a qué activo se aplica la actualización.

La *conciliación de activos* es el proceso mediante el cual se determina la relación entre las actualizaciones de activos y el activo relacionado en la base de datos de activos. La conciliación de activos se produce después de que QRadar reciba la actualización, pero antes de que la información se escriba en la base de datos de activos.

Información de identidad

Cada activo debe contener al menos un dato de identidad. Las actualizaciones posteriores que contengan un dato o más de los mismos datos de identidad se concilian con el activo propietario de los datos. Las actualizaciones que se basan en las direcciones IP se manejan con cuidado para evitar coincidencias de activos que

sean falsos positivos. Los falsos positivos en las coincidencias de activos se producen cuando a un activo físico se le asigna la propiedad de una dirección IP que anteriormente era propiedad de otro activo del sistema.

Cuando se proporcionan varios datos de identidad, el perfilador de activos da prioridad a la información en el orden siguiente:

- Dirección MAC (más determinista)
- Nombre de host NetBIOS
- Nombre de host DNS
- Dirección IP (menos determinista)

Las direcciones MAC, los nombres de host NetBIOS y los nombres de host DNS deben ser exclusivos y, por lo tanto, se consideran datos de identidad definitivos. Las actualizaciones entrantes cuyas coincidencias con un activo existente solamente sean la dirección IP se manejan de forma diferente que las actualizaciones que coincidan con los datos de identidad más definitivos.

Conceptos relacionados:

"Reglas de exclusión de conciliación de activos"
Con cada actualización de activo que entra en IBM Security QRadar, las reglas de exclusión de conciliación de activos aplican pruebas a la dirección MAC, el nombre de host NetBIOS, el nombre de host DNS y la dirección IP en la actualización de activo.

Reglas de exclusión de conciliación de activos

Con cada actualización de activo que entra en IBM Security QRadar, las reglas de exclusión de conciliación de activos aplican pruebas a la dirección MAC, el nombre de host NetBIOS, el nombre de host DNS y la dirección IP en la actualización de activo.

De forma predeterminada, se hace un seguimiento de cada dato de activos durante un periodo de dos horas. Si algún dato de identidad de la actualización de activo muestra un comportamiento sospechoso dos o más veces en un plazo de dos horas, ese dato se añade a las listas negras de activos. Existe una lista negra por separado para cada tipo de datos de activos de identidad que se prueba.

En los entornos que tienen en cuenta el dominio, las reglas de exclusión de conciliación de activos hacen un seguimiento del comportamiento de los datos de activos por separado en cada dominio.

Las reglas de exclusión de conciliación de activos prueban los escenarios siguientes:

Tabla 30. Pruebas y respuestas de Regla

Escenario	Respuesta de regla
Cuando una dirección MAC se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos

Tabla 30. Pruebas y respuestas de Regla (continuación)

Escenario	Respuesta de regla
Cuando una dirección IPv4 se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando una dirección MAC se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando una dirección MAC se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos

Puede ver estas reglas en la pestaña **Delitos** pulsando **Reglas** y, a continuación, seleccionando el grupo **Exclusión de conciliación de activos** en la lista desplegable.

Conceptos relacionados:

"Ejemplo: Reglas de exclusión de activos que se ajustan para excluir direcciones IP de la lista negra"
Puede excluir direcciones IP de las listas negras ajustando las reglas de exclusión de activos.

Ejemplo: Reglas de exclusión de activos que se ajustan para excluir direcciones IP de la lista negra

Puede excluir direcciones IP de las listas negras ajustando las reglas de exclusión de activos.

Como administrador de seguridad de red, gestiona una red corporativa que incluye un segmento de red wifi pública en el que las cesiones de direcciones IP son generalmente breves y frecuentes. Los activos en este segmento de la red tienden a ser transitorios, principalmente sistemas portátiles y dispositivos portátiles que inician y finalizan sesión en la wifi pública con frecuencia. Normalmente, una dirección IP individual la utilizan varias veces distintos dispositivos durante un breve periodo de tiempo.

En el resto del despliegue tiene una red cuidadosamente gestionada que consta únicamente de dispositivos de la empresa con nombres correctos e inventariados. Las cesiones de direcciones IP duran mucho más tiempo en esta parte de la red y a las direcciones IP se accede únicamente a través de la autenticación. En este segmento de red, desea saber inmediatamente cuando hay desviaciones de crecimiento de activos y desea conservar los valores predeterminados para las reglas de exclusión de conciliación de activos.

Elaboración de la lista negra de direcciones IP

En este entorno, las reglas de exclusión de conciliación de activos predeterminadas incluyen inadvertidamente en una lista negra la red entera durante un breve periodo de tiempo.

Su equipo de seguridad observa que las notificaciones relacionadas con el activo generadas por el segmento de wifi son una molestia. Desea evitar que la wifi desencadene más notificaciones de desviaciones del crecimiento de activos.

Ajuste de las reglas de conciliación de activos para ignorar algunas actualizaciones de activos

Revisa el informe **Desviaciones de activo por origen de registro** en la última notificación del sistema. Determina que los datos de la lista negra proceden del servidor DHCP de la wifi.

Los valores de la columna **Recuento de sucesos**, la columna **Recuento de flujos** y la columna **Delitos** de la fila correspondiente a la regla **AssetExclusion: Excluir IP por dirección MAC** indican que el servidor DHCP de la wifi desencadena esta regla.

Añade una prueba a las reglas de conciliación de activos existentes para hacer que las reglas dejen de añadir datos de la wifi a la lista negra.

```
Aplicar AssetExclusion:Excluir IP por Dirección MAC en sucesos detectados por
el sistema Local y NO cuando los sucesos los ha detectado uno o varios
MicrosoftDHCP @ microsoft.dhcp.test.com
y NO cuando cualquiera de Dominio es la clave y cualquiera de IP de identidad
es el valor en
cualquiera de Lista blanca de IPv4 del dominio de conciliación
de activos
- Lista negra de IPv4 del dominio de conciliación de activos - IP
y cuando al menos 3 sucesos se han visto con la misma IP de identidad y
diferente MAC de identidad en 2 horas.
```

La regla actualizada prueba solamente los sucesos de los orígenes de registro que no están en el servidor DHCP de la wifi. Para evitar que los sucesos DHCP de la wifi pasen más pruebas costosas de análisis de comportamiento y conjunto de referencia, también ha movido esta prueba al principio de la pila de pruebas.

Fusión de activos

La *fusión de activos* es el proceso según el cual la información de un activo se combina con la información de otro activo bajo la premisa de que son realmente el mismo activo físico.

La fusión de activos se produce cuando una actualización de activo contiene datos de identidad que coinciden con dos perfiles de activo diferentes. Por ejemplo, una única actualización que contiene un nombre de host NetBIOS que coincide con un

perfil de activo y una dirección MAC que coincide con otro perfil de activo diferente podría desencadenar una fusión de activos.

En algunos sistemas se puede observar un gran volumen de fusión de activos porque tienen orígenes de datos de activos que inadvertidamente combinan en una misma actualización de activo información de identidad de dos activos físicos diferentes. Como ejemplos de estos sistemas cabe citar los entornos siguientes:

- Servidores syslog centrales que actúan como proxy de sucesos
- Máquinas virtuales
- Entornos de instalación automatizada
- Nombres de host no exclusivos, frecuentes con activos como iPads y iPhones.
- Redes privadas virtuales que tienen direcciones MAC compartidas
- Extensiones de origen de registro cuyo campo de identidad es `OverrideAndAlwaysSend=true`

Los activos que tienen muchas direcciones IP, direcciones MAC o nombres de host presentan desviaciones en el crecimiento de los activos y pueden desencadenar notificaciones del sistema.

Conceptos relacionados:

"Identificación de desviaciones de crecimiento de activos"
A veces los orígenes de datos de activos generan actualizaciones que IBM Security QRadar no puede manejar correctamente sin intervención manual. En función de la causa del crecimiento anormal de los activos, puede arreglar el origen de datos de activos que está causando el problema o puede bloquear las actualizaciones de activos que provienen de ese origen de datos.

Identificación de desviaciones de crecimiento de activos

A veces los orígenes de datos de activos generan actualizaciones que IBM Security QRadar no puede manejar correctamente sin intervención manual. En función de la causa del crecimiento anormal de los activos, puede arreglar el origen de datos de activos que está causando el problema o puede bloquear las actualizaciones de activos que provienen de ese origen de datos.

Las *desviaciones de crecimiento de activos* se dan cuando el número de actualizaciones de activos de un único dispositivo supera el límite establecido en el umbral de retención para un tipo concreto de información de identidad. El manejo adecuado de las desviaciones de crecimiento de activos es de vital importancia para mantener un modelo de activos preciso.

En la base de cada desviación de crecimiento de activos se encuentra un origen de datos de activos cuyos datos no son de confianza para actualizar el modelo de activos. Cuando se identifica una desviación potencial del crecimiento de los activos, debe examinar el origen de la información para determinar si hay una explicación razonable para que un activo acumule grandes cantidades de datos de identidad. La causa de una desviación de crecimiento de activos es específica de un entorno.

Ejemplo del servidor DHCP de crecimiento de activo anormal en un perfil de activo

Supongamos que hay un servidor de VPN (red privada virtual) en una red DHCP (Protocolo de configuración dinámica de hosts). El servidor de VPN está

configurado para asignar direcciones IP a los clientes de VPN entrantes enviando mediante un proxy las solicitudes DHCP en nombre del cliente al servidor DHCP de la red.

Desde la perspectiva del servidor DHCP, la misma dirección MAC solicita muchas asignaciones de direcciones IP en repetidas ocasiones. En el contexto de las operaciones de red, el servidor VPN delega las direcciones IP a los clientes, pero el servidor DHCP no puede distinguir cuándo una solicitud la realiza un activo en nombre de otro.

El registro del servidor DHCP, que está configurado como un origen de registro de QRadar, genera un suceso de acuse de recibo DHCP (DHCP ACK) que asocia la dirección MAC del servidor VPN con la dirección IP que se asigna al cliente de VPN. Cuando se produce la conciliación de activos, el sistema concilia este evento por dirección MAC, lo que da como resultado un activo existente único que crece con una dirección IP cada vez que se analiza un suceso DHCP ACK.

Finalmente, un solo perfil de activo contiene todas las direcciones IP que se han asignado al servidor de VPN. Esta desviación de crecimiento de activos está causada por las actualizaciones de activos que contienen información acerca de más de un activo.

Valores de umbral

Cuando un activo de la base de datos alcanza un número determinado de propiedades, tales como varias direcciones IP o direcciones MAC, QRadar bloquea ese activo para que no reciba más actualizaciones.

Los valores de umbral del perfilador de activos indican las condiciones bajo las cuales un activo está bloqueado frente a las actualizaciones. El activo se actualiza normalmente hasta el valor del umbral. Cuando el sistema recopila datos suficientes para superar el umbral, el activo muestra una desviación de crecimiento de activo. Las futuras actualizaciones del activo se bloquean hasta que la desviación de crecimiento se corrija.

Notificaciones del sistema que indican desviaciones de crecimiento de activos

IBM Security QRadar genera notificaciones del sistema para ayudarle a identificar y gestionar las desviaciones de crecimiento de activos en su entorno.

Los siguientes mensajes del sistema indican que QRadar ha identificado posibles desviaciones de crecimiento de activos:

- `El sistema ha detectado perfiles de activo que sobrepasan el umbral de tamaño normal`
- `Las reglas de listas negras de activos han añadido datos de activo nuevos a las listas negras de activos`

Los mensajes de notificación del sistema incluyen enlaces a los informes para que sea más fácil identificar los activos que presentan desviaciones de crecimiento.

Datos de activos que cambian con frecuencia

El crecimiento de activos puede estar causado por grandes volúmenes de datos de activos que cambian de forma correcta, como en las situaciones siguientes:

- Un dispositivo móvil que va de una oficina a otra con frecuencia al que se le asigna una dirección IP nueva cada vez que inicia sesión.
- Un dispositivo que se conecta a una wifi pública con cesiones breves de direcciones IP, como por ejemplo en un campus universitario, puede recopilar grandes volúmenes de datos de activos durante un semestre.

Ejemplo: Cómo los errores de configuración de las extensiones de origen de registro pueden provocar desviaciones de crecimiento de activos

Las extensiones de origen de registro personalizado que están configuradas incorrectamente pueden provocar desviaciones de crecimiento de activos.

Configura una extensión de origen de registro personalizado para proporcionar actualizaciones de activos a QRadar mediante el análisis de los nombres de usuario de la carga útil de suceso que se encuentra en un servidor de registro central. Configura la extensión de origen de registro para alterar temporalmente la propiedad de nombre de host de sucesos para que las actualizaciones de activos generadas por el origen de registro personalizado siempre especifiquen el nombre del host DNS del servidor de registro central.

En lugar de que QRadar reciba una actualización que tiene el nombre de host del activo en el que el usuario ha iniciado sesión, el origen de registro genera muchas actualizaciones de activos que tienen el mismo nombre de host.

En esta situación, la desviación de crecimiento de activos está causada por un solo perfil de activo que contiene muchas direcciones IP y muchos nombres de usuario.

Resolución de problemas con perfiles de activo que sobrepasan el umbral de tamaño normal

IBM Security QRadar genera la notificación del sistema siguiente cuando la acumulación de datos bajo un único activo supera los límites de umbral configurados para los datos de identidad.

```
El sistema ha detectado perfiles de activo que sobrepasan el umbral de tamaño normal
```

Explicación

La carga útil muestra una lista de los cinco activos que presentan desviaciones con más frecuencia y proporciona información sobre por qué el sistema ha marcado cada activo como una desviación de crecimiento. Tal como se muestra en el ejemplo siguiente, la carga útil también muestra el número de veces que el activo ha intentado crecer más allá del umbral del tamaño de activo.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
Los cinco activos que presentan desviaciones con más frecuencia entre
el 13 de febrero de 2015 8:10:23 PM AST y el 13 de febrero de 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Cuando los datos de activos exceden el umbral configurado, QRadar bloquea el activo frente a actualizaciones futuras. Esta intervención evita que el sistema reciba más datos dañados y mitiga el impacto en el rendimiento que podría producirse si el sistema intenta conciliar las actualizaciones de entrada con un perfil de activo anormalmente grande.

Acción del usuario necesaria

Utilice la información de la carga útil de la notificación para identificar los activos que contribuyen a la desviación de crecimiento de activo y determinar qué está provocando el crecimiento anormal. La notificación proporciona un enlace a un informe de todos los activos que han experimentado una desviación del crecimiento durante las últimas 24 horas.

Después de resolver la desviación de crecimiento de activo en su entorno, puede ejecutar el informe de nuevo.

1. Pulse la pestaña **Actividad de registro** y pulse **Buscar** > **Nueva búsqueda**.
2. Seleccione la búsqueda guardada **Desviación de crecimiento de activos: Informe de activos**.
3. Utilice el informe para identificar y reparar los datos de activos inexactos que se han creado durante la desviación.

Si los datos de activos son válidos, los administradores de QRadar pueden aumentar los límites de umbral para las direcciones IP, las direcciones MAC, los nombres de host NetBIOS y los nombres de host DNS en **Configuración del perfilador de activos** en la pestaña **Admin** de QRadar.

Los datos de activos nuevos se añaden a las listas negras de activos

IBM Security QRadar genera la notificación del sistema siguiente cuando un dato de activos concreto presenta un comportamiento que puede deberse a la desviación del crecimiento de activos.

```
Las reglas de lis. neg. act. han añadido datos de activo nuevos a las lis. neg. act.
```

Explicación

Las reglas de exclusión de activos supervisan los datos de activos para comprobar la coherencia y la integridad. Las reglas hacen un seguimiento de datos de activos concretos a lo largo del tiempo para asegurarse de que están siendo observados siempre con el mismo subconjunto de datos dentro de un plazo de tiempo razonable.

Por ejemplo, si una actualización de activo incluye una dirección MAC y un nombre de host DNS, la dirección MAC está asociada con ese nombre de host DNS durante un periodo de tiempo concreto. Las actualizaciones de activos posteriores que contengan esa dirección MAC también contienen ese nombre de host DNS si se incluye alguno en la actualización de activo. Si la dirección MAC de repente se asocia con un nombre de host DNS diferente durante un periodo breve de tiempo, el cambio se supervisa. Si la dirección MAC cambia de nuevo dentro de un periodo breve, la dirección MAC se marca para indicar que contribuye a una instancia de crecimiento de activo anormal o con desviaciones.

Acción del usuario necesaria

Utilice la información de la carga útil de la notificación para identificar las reglas que se utilizan para supervisar los datos de activos. Pulse el enlace **Desviaciones de activo por origen de registro** en la notificación para ver las desviaciones de activo que se han producido en las últimas 24 horas.

Si los datos de activos son válidos, los administradores de QRadar pueden configurar QRadar para resolver el problema.

- Si las listas negras se llenan demasiado rápido, puede ajustar las reglas de exclusión de conciliación de activos que las llenan.
- Si desea añadir los datos a la base de datos de activos, puede eliminar los datos de activos de la lista negra y añadirlos a la lista blanca de activos correspondiente. Al añadir datos de un activo a la lista blanca se impide que reaparezcan inadvertidamente en la lista negra.

Listas negras y listas blancas de activos

IBM Security QRadar utiliza un grupo de reglas de conciliación de activos para determinar si los datos de activos son de confianza. Cuando los datos de activos son cuestionables, QRadar utiliza listas negras y listas blancas de activos para determinar si deben actualizarse los perfiles de activo con los datos de activos.

Una *lista negra de activos* es un conjunto de datos que IBM Security QRadar considera no fiables. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Una *lista blanca de activos* es un conjunto de datos de activos que altera la lógica del motor de conciliación de activos con la que se añaden datos a una lista negra de activos. Cuando el sistema identifica una coincidencia en la lista negra, comprueba la lista blanca para ver si el valor existe. Si la actualización de activo coincide con datos que están en la lista blanca, el cambio se concilia y el activo se actualiza. Los datos de activos en listas blancas se aplican globalmente en todos los dominios.

El administrador de QRadar puede modificar los datos de la lista negra y la lista blanca de activos para evitar futuras desviaciones de crecimiento de activos.

Listas negras de activos

Una *lista negra de activos* es un conjunto de datos que IBM Security QRadar considera no fiables según las reglas de exclusión de conciliación de activos. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Cada actualización de activo en QRadar se compara con las listas negras de activos. Los datos de activos en listas negras se aplican globalmente en todos los dominios. Si la actualización de activo contiene información de identidad (dirección MAC, nombre de host NetBIOS, nombre de host DNS o dirección IP) que se encuentra en una lista negra, la actualización de entrada se descarta y la base de datos de activos no se actualiza.

En la tabla siguiente se muestra el nombre y el tipo de recopilación de referencia para cada tipo de datos de activos de identidad.

Tabla 31. Nombres de recopilación de referencia para los datos de las listas negras de activos

Tipo de datos de identidad	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Direcciones IP (v4)	Lista negra de IPv4 de conciliación de activos	Conjunto de referencia [Tipo de conjunto: IP]

Tabla 31. Nombres de recopilación de referencia para los datos de las listas negras de activos (continuación)

Tipo de datos de identidad	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Nombres de host DNS	Lista negra de DNS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Nombres de host NetBIOS	Lista negra de NetBIOS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Direcciones MAC	Lista negra de MAC de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
* ALNIC es un tipo alfanumérico que puede dar cabida tanto al nombre de host como a los valores de dirección MAC.		

El administrador de QRadar puede modificar las entradas de lista negra para asegurarse de que los nuevos datos de activos se manejan correctamente.

Listas blancas de activos

Puede utilizar listas blancas de activos para evitar que los datos de activos de IBM Security QRadar reaparezcan inadvertidamente en las listas negras de activos.

Una *lista blanca de activos* es un conjunto de datos de activos que altera la lógica del motor de conciliación de activos con la que se añaden datos a una lista negra de activos. Cuando el sistema identifica una coincidencia en la lista negra, comprueba la lista blanca para ver si el valor existe. Si la actualización de activo coincide con datos que están en la lista blanca, el cambio se concilia y el activo se actualiza. Los datos de activos en listas blancas se aplican globalmente en todos los dominios.

El administrador de QRadar puede modificar las entradas de lista blanca para asegurarse de que los nuevos datos de activos se manejan correctamente.

Ejemplo de caso práctico de lista blanca

La lista blanca es útil si tiene datos de activos que siguen apareciendo en las listas negras aunque se trate de una actualización de activo válido. Por ejemplo, podría tener un equilibrador de carga DNS con rotación que está configurado para rotar en un conjunto de cinco direcciones IP. Las reglas de exclusión de conciliación de activos podrían determinar que el hecho de que haya varias direcciones IP asociadas con el mismo nombre de host DNS es una indicación de que existe una desviación de crecimiento de activos, y el sistema podría añadir el equilibrador de carga DNS a la lista negra. Para resolver este problema, puede añadir el nombre de host DNS a la lista blanca de DNS de conciliación de activos.

Entradas en masa a la lista blanca de activos

Una base de datos de activos precisa facilita la conexión de los delitos que se desencadenan en el sistema a activos físicos o virtuales en la red. Pasar por alto las desviaciones de activos añadiendo entradas en masa a la lista blanca de activos no es útil para la creación de una base de datos de activos precisa. En lugar de añadir entradas en masa a la lista blanca, revise la lista negra de activos para determinar qué está contribuyendo a la desviación de crecimiento de activos y luego determine cómo solucionar el problema.

Tipos de listas blancas de activos

Cada tipo de datos de identidad se mantiene en una lista blanca por separado. En la tabla siguiente se muestra el nombre y el tipo de recopilación de referencia para cada tipo de datos de activos de identidad.

Tabla 32. Nombre de recopilación de referencia para los datos de las listas blancas de activos

Tipo de datos	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Direcciones IP	Lista blanca de IPv4 de conciliación de activos	Conjunto de referencia [Tipo de conjunto: IP]
Nombres de host DNS	Lista blanca de DNS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Nombres de host NetBIOS	Lista blanca de NetBIOS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Direcciones MAC	Lista blanca de MAC de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
* ALNIC es un tipo alfanumérico que puede dar cabida al nombre de host y a valores de dirección MAC.		

Parámetros de página de perfil de activos

Puede encontrar descripciones de parámetro de página de perfil de activo para el panel Resumen de activo, panel Interfaz de red, panel Vulnerabilidad, panel Servicios, panel Paquetes, panel Parches de Windows, panel Propiedades, panel Políticas de riesgo y panel Productos.

Esta referencia incluye tablas que describen los parámetros que se visualizan en cada pestaña del separador**Perfil de activo**.

Perfiles de activo

Los perfiles de activo proporcionan información sobre cada activo conocido en la red, incluyendo qué servicios se ejecutan en cada activo.

La información del perfil de activo se utiliza a efectos de correlación para ayudar a reducir los falsos positivos. Por ejemplo, si un origen intenta atacar un servicio específico que se ejecuta en un activo, QRadar determina si el activo es vulnerable a este ataque correlacionando el ataque con el perfil de activo.

Los perfiles de activo se descubren automáticamente si tiene exploraciones de datos de flujo o de evaluación de vulnerabilidad (VA) configuradas. Para que los datos de flujo llenen los perfiles de activo, se necesitan flujos bidireccionales. Los perfiles de activo también se pueden crear automáticamente a partir de los sucesos de identidad. Para obtener más información sobre la VA, consulte *Guía de configuración de evaluación de vulnerabilidades de IBM Security QRadar*.

Para tener más información sobre los orígenes de flujo, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Vulnerabilidades

Puede utilizar exploradores de QRadar Vulnerability Manager y de terceros para identificar vulnerabilidades.

Los exploradores de terceros identifican e informan de las vulnerabilidades descubiertas utilizando referencias externas, como Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB) y Critical Watch. Los exploradores de terceros incluyen, por ejemplo, QualysGuard y nCircle ip360. OSVDB asigna un identificador de referencia exclusiva (OSVDB ID) a cada vulnerabilidad. Las referencias externas asignan un identificador de referencia exclusiva a cada vulnerabilidad. Los ID de referencia de datos externos incluyen, por ejemplo, el ID de Common Vulnerability and Exposures (CVE) o el ID de Bugtraq. Para obtener más información sobre exploradores y evaluación de vulnerabilidad, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

QRadar Vulnerability Manager es un componente que puede comprar por separado y habilitar utilizando una clave de licencia. QRadar Vulnerability Manager es una plataforma de exploración de red que proporciona conocimiento de las vulnerabilidades que existen en las aplicaciones, sistemas o dispositivos de la red. Después de que las exploraciones identifiquen las vulnerabilidades, puede buscar y revisar datos de vulnerabilidad, remediar vulnerabilidades y volver a ejecutar exploraciones para evaluar el nuevo nivel de riesgo.

Cuando se habilita QRadar Vulnerability Manager, puede realizar tareas de evaluación de vulnerabilidades en la pestaña **Vulnerabilidades**. En la pestaña **Activos**, puede ejecutar exploraciones en los activos seleccionados.

Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*

Visión general de la pestaña Activos

La pestaña **Activos** le proporciona un espacio de trabajo desde el que puede gestionar los activos de red e investigar las vulnerabilidades de un activo, los puertos, las aplicaciones, el historial y otras asociaciones.

Mediante el uso de la pestaña **Activos**, puede:

- Ver todos los activos descubiertos.
- Añadir manualmente perfiles de activo.
- Buscar activos específicos.
- Ver información sobre activos descubiertos.
- Editar perfiles de activo para activos añadidos o descubiertos manualmente.
- Ajustar vulnerabilidades positivas falsas.
- Importar activos.
- Imprimir o exportar perfiles de activo.
- Descubrir activos.
- Configurar y gestionar exploración de volumen de terceros.
- Iniciar exploraciones de QRadar Vulnerability Manager.

Para obtener información sobre la opción de descubrimiento de servidores en el panel de navegación, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*

Para obtener más información sobre la opción de Exploración de VA en el panel de navegación, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.

Lista de pestaña Activo

La página Perfiles de activo proporciona información sobre el ID, la dirección IP, el nombre de activo, la puntuación de CVSS agregada, las vulnerabilidades y los servicios.

La página Perfiles de activo proporciona la siguiente información sobre cada activo:

Tabla 33. Parámetros de página Perfil de activo

Parámetro	Descripción
ID	Visualiza el número de ID del activo. El número de ID de activo se genera automáticamente cuando se añade un perfil de activo manualmente o cuando se descubren activos mediante sucesos, flujos o exploraciones de vulnerabilidad.
Dirección IP	Visualiza la última dirección IP conocida del activo.
Nombre de activo	Visualiza el nombre, el nombre NetBios, el nombre de DSN o la dirección MAC del activo. Si se desconoce, este campo visualiza la última dirección IP conocida. **Nota:** Estos valores se visualizan en orden de prioridad. Por ejemplo, si el activo no tiene un nombre, se visualiza el nombre de NetBios de agregado. Si el activo se descubre automáticamente, este campo se llena automáticamente, sin embargo, puede editar el nombre de activo si es necesario.

Tabla 33. Parámetros de página Perfil de activo (continuación)

Parámetro	Descripción
Puntuación de riesgo	Visualiza una de las siguientes puntuaciones de CVSS (Common Vulnerability Scoring System): • Puntuación de CVSS de entorno agregada fusionada • Puntuación de CVSS temporal agregada • Puntuación base de CVSS agregada • Estas puntuaciones se visualizan en orden de prioridad. Por ejemplo, si la puntuación de CVSS de entorno agregada fusionada no está disponible, se visualiza la puntuación de CVSS temporal agregada. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades. La puntuación de CVSS se calcula a partir de los siguientes parámetros definidos por el usuario: • Potencial de daños colaterales • Requisito de confidencialidad • Requisito de disponibilidad • Requisito de integridad Para obtener más información sobre cómo configurar estos parámetros, consulte "Adición o edición de un perfil de activo" en la página 146. Para obtener más información sobre CVSS, consulte http://www.first.org/cvss/ .
Vulnerabilidades	Visualiza el número de vulnerabilidades exclusivas que se han descubierto en este activo. Este valor incluye también el número de vulnerabilidades activas y pasivas.
Servicios	Visualiza el número de aplicaciones de capa 7 exclusivas que se ejecutan en este activo.
Último usuario	Visualiza el último usuario asociado con el activo.
Usuario visto por última vez	Visualiza la hora en que se ha visto por última vez el último usuario asociado con el activo.

Opciones del menú que aparece al pulsar el botón derecho del ratón

Al pulsar el botón derecho del ratón en un activo de la pestaña Activo se visualizan menús para obtener más información de filtro de sucesos.

En la pestaña **Activos**, puede pulsar el botón derecho del ratón en un activo para acceder a más información de filtro de sucesos.

Tabla 34. Opciones del menú que aparece al pulsar el botón derecho del ratón

Opción	Descripción
Navegar	El menú **Navegar** proporciona las opciones siguientes: • **Ver por red**: Visualiza la ventana Lista de redes, que muestra todas las redes que están asociadas con la dirección IP seleccionada. • **Ver resumen de origen**: Visualiza la ventana Lista de delitos, que muestra todos los delitos que están asociados con la dirección IP de origen seleccionada. • **Ver resumen de destino**: Visualiza la ventana Lista de delitos, que muestra todos los delitos que están asociados con la dirección IP de destino seleccionada.
Información	El menú **Información** proporciona las opciones siguientes: • **Búsqueda de DNS**: Busca entradas DNS que se basan en la dirección IP. • **Búsqueda de WHOIS**: Busca el propietario registrado de una dirección IP remota. El servidor WHOIS predeterminado es whois.arin.net. • **Exploración de puertos**: Realiza una exploración de MAP (Network Mapper - Correlacionador de red) de la dirección IP seleccionada. Esta opción solo está disponible si NMAP está instalado en el sistema. Para obtener más información sobre la instalación de NMAP, consulte la documentación de proveedor. • **Perfil de activo**: Visualiza información de perfil de activo. Esta opción de menú solo está disponible cuando los datos de un perfil los adquiere activamente una exploración o los adquieren pasivamente los orígenes de flujos. • **Sucesos de búsqueda**: Seleccione la opción **Sucesos de búsqueda** para buscar sucesos que están asociados con esta dirección IP. • **Flujos de búsqueda**: Seleccione la opción Buscar flujos para buscar flujos que están asociados con esta dirección IP.
Ejecutar Exploración de vulnerabilidad	Seleccione esta opción para ejecutar una exploración de gestor de vulnerabilidad en el activo seleccionado. Esta opción solo se visualiza después de instalar QRadar Vulnerability Manager.

Visualización de un perfil de activo

En la lista de activos de la pestaña **Activos**, puede seleccionar y ver un perfil de activo. Un perfil de activo proporciona información sobre cada perfil.

Acerca de esta tarea

La información de perfil de activo se descubre automáticamente a través del servidor de descubrimiento o se configura manualmente. Puede editar la información de perfil de activo generada automáticamente.

La página Perfil de activo proporciona la información sobre el activo que se organiza en varios paneles. Para ver un panel, puede pulsar la flecha **(>)** en el panel para ver más detalles o seleccionar el panel en el recuadro de lista **Visualizar** en la barra de herramientas.

La barra de herramientas de página Perfil de activo proporciona las funciones siguientes:

Tabla 35. Funciones de barra de herramientas de página Perfil de activo

Opciones	Descripción
Volver a lista de activos	Pulse esta opción para volver a la lista de activos.
Visualizar	En el recuadro de lista, puede seleccionar el panel que desea ver en el panel Perfil de activo. Los paneles Resumen de activo y Resumen de interfaz de red se visualizan siempre. Para obtener más información sobre los parámetros que se muestran en cada panel, consulte Parámetros de página de perfil de activos.
Editar activo	Pulse esta opción para editar el Perfil de activo. Consulte “Adición o edición de un perfil de activo” en la página 146.
Ver por red	Si este activo está asociado con un delito, esta opción le permitirá ver la lista de redes que están asociadas con este activo. Al pulsar **Ver por red**, se visualiza la ventana Lista de redes. Consulte “Supervisar delitos agrupados por red” en la página 41.
Ver resumen de origen	Si este activo es el origen de un delito, esta opción le permitirá ver la información de resumen de origen. Al pulsar **Ver resumen de origen**, se visualiza la ventana Lista de delitos. Consulte “Supervisar delitos agrupados por IP de origen” en la página 40.
Ver resumen de destino	Si este activo es el destino de un delito, esta opción le permitirá ver información de resumen de destino. Al pulsar **Ver resumen de destino**, se visualiza la ventana Lista de destinos. Consulte “Supervisar delitos agrupados por IP de destino” en la página 41.

Tabla 35. Funciones de barra de herramientas de página Perfil de activo (continuación)

Opciones	Descripción
Historial	Pulse **Historial** para ver información de historial de sucesos para este activo. Al pulsar el icono **Historial**, se visualiza la ventana Búsqueda de sucesos, previamente rellenada con los criterios de búsqueda de sucesos: Si es necesario, puede personalizar los parámetros de búsqueda. Pulse **Buscar** para ver información de historial de sucesos.
Aplicaciones	Pulse **Aplicaciones** para ver información de aplicación para este activo. Al pulsar el icono **Aplicaciones**, se visualiza la ventana Búsqueda de flujos, previamente rellenada con criterios de búsqueda de sucesos. Si es necesario, puede personalizar los parámetros de búsqueda. Pulse **Buscar** para ver la información de aplicación.
Buscar en conexiones	Pulse **Buscar en conexiones** para buscar conexiones. Se visualiza la ventana Búsqueda de conexión. Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
Ver topología	Pulse **Ver topología** para investigar el activo adicionalmente. Se visualiza la ventana Topología actual. Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
Acciones	En la lista **Acciones**, seleccione **Historial de vulnerabilidades.** Esta opción sólo se visualiza cuando se ha adquirido IBM Security QRadar Risk Manager y se ha obtenido la licencia. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**
3. Efectúe una doble pulsación en el activo que desea ver.
4. Utilice las opciones de la barra de herramientas para visualizar los diversos paneles de información de perfil de activo. Consulte Edición de un perfil de activo.
5. Para investigar las vulnerabilidades asociadas, pulse cada vulnerabilidad en el panel Vulnerabilidades. Consulte la Tabla 10-10
6. Si es necesario, edite el perfil de activo. Consulte Edición de un perfil de activo.

7. Pulse **Volver a lista de activos** para seleccionar y ver otro activo, si es necesario.

Adición o edición de un perfil de activo

Los perfiles de activo se descubren y añaden automáticamente; sin embargo, puede ser necesario añadir manualmente un perfil

Acerca de esta tarea

Cuando se descubren activos mediante la utilización de la opción Descubrimiento de servidores, algunos detalles de perfil de activo se rellenan automáticamente. Se puede añadir manualmente información al perfil de activo y se pueden editar determinados parámetros.

Sólo se pueden editar los parámetros que se han entrado manualmente. Los parámetros generados por el sistema aparecen en cursiva y no son editables. Los parámetros generados por el sistema pueden suprimirse, si es necesario.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Elija una de las siguientes opciones:
   - Para añadir un activo, pulse **Añadir activo** y escriba la dirección IP o el rango de CIDR del activo en el campo **Nueva dirección IP**.
   - Para editar un activo, efectúe una doble pulsación en el activo que desea ver y pulse **Editar activo**.
4. Configure los parámetros del panel MAC y dirección MAC. Configure una o varias de las opciones siguientes:
   - Pulse el icono **Nueva dirección MAC** y escriba una dirección MAC en el recuadro de diálogo.
   - Pulse el icono **Nueva dirección IP** y escriba una dirección IP en el recuadro de diálogo.
   - Si se lista **NIC desconocido**, puede seleccionar este elemento, pulsar el icono **Editar** y escribir una nueva dirección MAC en el recuadro de diálogo.
   - Seleccione una dirección MAC o IP en la lista, pulse el icono **Editar** y escriba una dirección MAC nueva en el recuadro de diálogo.
   - Seleccione una dirección MAC o IP en la lista y pulse el icono **Eliminar**.
5. Configure los parámetros del panel Nombres y descripción. Configure una o varias de las opciones siguientes:

Parámetro	Descripción
DNS	Elija una de las siguientes opciones: • Escriba un nombre DNS y pulse **Añadir**. • Seleccione un nombre de DNS en la lista y pulse **Editar**. • Seleccione un nombre de DNS en la lista y pulse **Eliminar**.

Parámetro	Descripción
NetBIOS	Elija una de las siguientes opciones: • Escriba un nombre NetBIOS y pulse **Añadir**. • Seleccione un nombre de NetBIOS en la lista y pulse **Editar**. • Seleccione un nombre de NetBIOS en la lista y pulse **Eliminar**.
Nombre	Escriba un nombre para este perfil de activo.
Ubicación	Escriba una ubicación para este perfil de activo.
Descripción	Escriba una descripción para este perfil de activo.
AP inalámbrico	Escriba el punto de acceso (AP) inalámbrico para este perfil de activo.
SSID inalámbrico	Escriba el identificador de conjunto de servicios (SSID) inalámbrico para este perfil de activo.
ID de conmutador	Escriba el ID de conmutador para este perfil de activo.
ID de puerto de conmutador	Escriba el ID de puerto de conmutador para este perfil de activo.

6. Configure los parámetros del panel Sistema operativo:
   a. En el recuadro de lista **Proveedor**, seleccione un proveedor de sistema operativo.
   b. En el recuadro de lista **Producto**, seleccione el sistema operativo para el perfil de activo.
   c. En el recuadro de lista **Versión**, seleccione la versión del sistema operativo seleccionado.
   d. Pulse el icono **Añadir**.
   e. En el recuadro de lista **Alterar temporalmente**, seleccione una de las opciones siguientes:
      - **Hasta próxima exploración**: Seleccione esta opción para especificar que el explorador proporciona información de sistema operativo y la información se puede editar temporalmente. Si edita los parámetros de sistema operativo, el explorador restaura la información en su próxima exploración.
      - **Siempre**: Seleccione esta opción para especificar que desea entrar manualmente la información del sistema operativo e impedir que el explorador actualice información.
   f. Seleccione un sistema operativo de la lista.
   g. Seleccione un sistema operativo y pulse en el icono **Conmutar alteración temporal**.
7. Configure los parámetros del panel CVSS y peso. Configure una o varias de las opciones siguientes:

Parámetro	Descripción
Potencial de daños colaterales	Configure este parámetro para indicar la posibilidad de pérdida de vidas humanas o activos físicos a través de daños o robo de este activo. También puede utilizar este parámetro para indicar el potencial de pérdida económica de productividad o ingresos. El mayor potencial de daños colaterales aumenta el valor calculado en el parámetro de puntuación de CVSS. En el recuadro de lista **Potencial de daños colaterales**, seleccione una de las opciones siguientes: • Ninguno • Bajo • Medio bajo • Medio alto • Alto • No definido Al configurar el parámetro **Potencial de daños colaterales**, el parámetro **Peso** se actualizar automáticamente.
Requisito de confidencialidad	Configure este parámetro para indicar el impacto en la confidencialidad de una vulnerabilidad atacada con éxito en este activo. Un mayor impacto de confidencialidad aumenta el valor calculado en el parámetro Puntuación de CVSS. En el recuadro de lista **Requisito de confidencialidad**, seleccione una de las opciones siguientes: • Bajo • Medio • Alto • No definido
Requisito de disponibilidad	Configure este parámetro para indicar el impacto en la disponibilidad del activo cuando una vulnerabilidad se ataca con éxito. Los ataques que consumen ancho de banda de red, ciclos de procesador o espacio de disco impactan la disponibilidad de un activo. Un mayor impacto de disponibilidad aumenta el valor calculado en el parámetro Puntuación de CVSS. En el recuadro de lista **Requisito de disponibilidad**, seleccione una de las opciones siguientes: • Bajo • Medio • Alto • No definido

Parámetro	Descripción
Requisito de integridad	Configure este parámetro para indicar que el impacto en la integridad del activo cuando una vulnerabilidad se ataca con éxito. La integridad hace referencia a la fiabilidad y la veracidad garantizada de la información. Un mayor impacto de integridad aumenta el valor calculado en el parámetro Puntuación de CVSS. En el recuadro de lista **Requisito de integridad**, seleccione una de las opciones siguientes: • Bajo • Medio • Alto • No definido
Peso	En el recuadro de lista **Peso** , seleccione un peso para este perfil de activo. El rango de valores es de 0 a 10. Cuando configure el parámetro **Peso**, el parámetro **Potencial de daños colaterales** se actualiza automáticamente.

8. Configure los parámetros del panel Propietario. Elija una o varias de las opciones siguientes:

Parámetro	Descripción
Propietario del negocio	Escriba el nombre del propietario del negocio del activo. Un propietario de negocio es, por ejemplo, un director de departamento. La longitud máxima es de 255 caracteres.
Contacto del propietario del negocio	Escriba la información de contacto para el propietario de negocio. La longitud máxima es de 255 caracteres.
Propietario técnico	Escriba el propietario técnico del activo. Un propietario técnico es, por ejemplo, el director o gestor de TI. La longitud máxima es de 255 caracteres.
Contacto de propietario técnico	Escriba la información de contacto para el propietario técnico. La longitud máxima es de 255 caracteres.

Parámetro	Descripción
Usuario técnico	En el recuadro de lista, seleccione el nombre de usuario que desea asociar con este perfil de activo. También puede utilizar este parámetro para habilitar la remediación de vulnerabilidad automática para IBM Security QRadar Vulnerability Manager. Para obtener más información sobre la remediación automática, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

9. Pulse **Guardar**.

Búsqueda de perfiles de activo

Puede configurar parámetros de búsqueda para mostrar sólo los perfiles de activo que desea investigar en la página Activo en la pestaña **Activos**.

Acerca de esta tarea

Al acceder a la pestaña **Activos**, se visualiza la página Activo llena con todos los activos descubiertos en la red. Para refinar esta lista, puede configurar parámetros de búsqueda para visualizar solo los perfiles de activo que desea investigar.

En la página Búsqueda de activo, puede gestionar Grupos de búsqueda de activos. Para obtener más información sobre Grupos de búsqueda de activos, consulte Grupos de búsqueda de activos.

La característica de búsqueda le permitirá buscar perfiles de host, activos e información de identidad. La información de identidad proporciona más detalles sobre los orígenes de registro en la red, incluyendo información de DNS, inicios de sesión de usuario y direcciones MAC.

Mediante la característica de búsqueda de activos, puede buscar activos por referencias de datos externas para determinar si existen vulnerabilidades conocidas en el despliegue.

Por ejemplo:

Recibe una notificación de que el ID de CVE: CVE-2010-000 está siendo utilizado activamente en el campo. Para verificar si los hosts del despliegue son vulnerables a este ataque, puede seleccionar **Referencia externa de vulnerabilidad** en la lista de parámetros de búsqueda, seleccionar **CVE** y, a continuación, escribir

```
2010-000
```

para ver una lista de todos los hosts que son vulnerables a ese ID de CVE específico.

Nota: Para obtener más información acerca de OSVDB, consulte *http://osvdb.org/*. Para obtener más información acerca de NVDB, consulte *http://nvd.nist.gov/*.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En la barra de herramientas, pulse **Buscar** > **Nueva búsqueda**.
4. Elija una de las siguientes opciones:
   - Para cargar una búsqueda guardada anteriormente, vaya al Paso 5.
   - Para crear una nueva búsqueda, vaya al Paso 6.
5. Seleccione una búsqueda guardada anteriormente:
   a. Elija una de las siguientes opciones:
      - Opcional. En el recuadro de lista **Grupo**, seleccione el grupo de búsqueda de activos que desea visualizar en la lista **Búsquedas guardadas disponibles**.
      - En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desea cargar.
      - En el campo **Escriba la búsqueda guardada o seleccione en la lista**, escriba el nombre de la búsqueda que desea cargar.
   b. Pulse **Cargar**.
6. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
   a. En el primer recuadro de lista, seleccione el parámetro de activo que desea buscar. Por ejemplo, **Nombre de host**, **Clasificación de riesgo de vulnerabilidad** o **Propietario técnico**.
   b. En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda.
   c. En el campo de entrada, escriba información específica que está relacionada con el parámetro de búsqueda.
   d. Pulse **Añadir filtro**.
   e. Repita estos pasos para cada filtro que desee añadir a los criterios de búsqueda.
7. Pulse **Buscar**.

Resultados

Puede guardar los criterios de búsqueda de activos. Consulte Guardar criterios de búsqueda de activos.

Guardar criterios de búsqueda de activos

En la pestaña **Activo**, puede guardar criterios de búsqueda configurados para poder reutilizar los criterios. Los criterios de búsqueda guardados no caducan.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Realice una búsqueda.
4. Pulse **Guardar criterios**.
5. Entre valores para los parámetros:

Parámetro	Descripción
Especifique el nombre de esta búsqueda	Escriba el nombre exclusivo que desee asignar a este criterio de búsqueda.

Parámetro	Descripción
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de búsqueda. Esta opción sólo se visualiza si tiene permisos administrativos.
Asignar búsqueda a grupo(s)	Marque el recuadro de selección para el grupo al que desea asignar esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo **Otros** de forma predeterminada.
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el recuadro de lista **Búsqueda rápida**, que se encuentra en la barra de herramientas de la pestaña **Activos**.
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada cuando accede a la pestaña **Activos**.
Compartir con todos	Marque este recuadro de selección para compartir estos requisitos de búsqueda con todos los usuarios.

Grupos de búsqueda de activos

Utilizando la ventana Grupos de búsqueda de activos, puede crear y gestionar grupos de búsqueda de activos.

Estos grupos le permiten localizar fácilmente criterios de búsqueda guardados en la pestaña **Activos**.

Visualización de grupos de búsqueda

Utilice la ventana Grupos de búsqueda de activos para ver una lista de grupos y subgrupos.

Acerca de esta tarea

En la ventana Grupos de búsqueda de activos, puede ver detalles acerca de cada grupo, incluyendo una descripción y la fecha en que se ha modificado por última vez el grupo.

Todas las búsquedas guardadas que no se asignan a un grupo están en el grupo **Otros**.

La ventana Grupos de búsqueda de activos muestra los parámetros siguientes para cada grupo:

Tabla 36. Funciones de barra de herramientas de ventanas Grupos de búsqueda de activos

Función	Descripción
Grupo nuevo	Para crear un nuevo grupo de búsqueda, puede pulsar **Grupo nuevo**. Consulte Creación de un grupo de búsqueda nuevo.
Editar	Para editar un grupo de búsqueda existente, puede pulsar en **Editar**. Consulte Edición de un grupo de búsqueda.

Tabla 36. Funciones de barra de herramientas de ventanas Grupos de búsqueda de activos (continuación)

Función	Descripción
Copiar	Para copiar una búsqueda guardada en otro grupo de búsqueda, puede pulsar en **Copiar**. Consulte Copia de una búsqueda guardada en otro grupo.
Eliminar	Para eliminar un grupo de búsqueda o una búsqueda guardada de un grupo de búsqueda, seleccione el elemento que desea eliminar y luego pulse **Eliminar**. Consulte Eliminación de un grupo o una búsqueda guardada de un grupo.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Vea los grupos de búsqueda.

Creación de un grupo de búsqueda nuevo

En la ventana Grupos de búsqueda de activos, puede crear un nuevo grupo de búsqueda.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la carpeta para el grupo donde desea crear el nuevo grupo.
6. Pulse **Grupo nuevo**.
7. En el campo **Nombre**, escriba un nombre exclusivo para el nuevo grupo.
8. Opcional. En el campo **Descripción**, escriba una descripción.
9. Pulse **Aceptar**.

Edición de un grupo de búsqueda

Puede editar los campos **Nombre** y **Descripción** de un grupo de búsqueda.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione el grupo que desea editar.
6. Pulse **Editar**.
7. Escriba un nombre nuevo en el campo **Nombre**.
8. Escriba una nueva descripción en el campo **Descripción**.
9. Pulse **Aceptar**.

Copia de una búsqueda guardada en otro grupo

Puede copiar una búsqueda guardada en otro grupo. También puede copiar la búsqueda guardada en más de un grupo.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la búsqueda guardada que desea copiar.
6. Pulse **Copiar**.
7. En la ventana Grupos de elementos, marque el recuadro de selección para el grupo en el que desea copiar la búsqueda guardada.
8. Pulse **Asignar grupos**.

Eliminación de un grupo o una búsqueda guardada de un grupo

Puede utilizar el icono **Eliminar** para eliminar una búsqueda de un grupo o eliminar un grupo de búsqueda.

Acerca de esta tarea

Cuando se elimina una búsqueda guardada de un grupo, la búsqueda guardada no se suprime del sistema. La búsqueda guardada se elimina del grupo y se mueve automáticamente al grupo **Otros**.

No puede eliminar los grupos siguientes del sistema:

- Grupos de búsqueda de activos
- Otros

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione **Buscar** > **Nueva búsqueda**.
4. Pulse **Gestionar grupos**.
5. Seleccione la búsqueda guardada que desea eliminar del grupo:
   - Seleccione la búsqueda guardada que desea eliminar del grupo.
   - Seleccione el grupo que desea eliminar.

Tareas de gestión de perfiles de activo

Puede suprimir, importar y exportar perfiles de activos utilizando la pestaña Activos.

Acerca de esta tarea

Utilizando la pestaña **Activos**, puede suprimir, importar y exportar perfiles de activos.

Supresión de activos

Puede suprimir activos específicos o todos los perfiles de activo listados.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione el activo que desea suprimir y, a continuación, seleccione **Suprimir activo** en el recuadro de lista **Acciones**.
4. Pulse **Aceptar**.

Importación de perfiles de activo

Puede importar información de perfil de activo.

Antes de empezar

El archivo importado debe ser un archivo CSV con el formato siguiente:

```
ip,nombre,peso,descripción
```

Donde:

- **IP**: Especifica cualquier dirección IP válida en formato decimal con puntos. Por ejemplo: 192.168.5.34.
- **Nombre**: Especifica el nombre de este activo con una longitud de hasta 255 caracteres. Las comas no son válidas en este campo e invalidan el proceso de importación. Por ejemplo: WebServer01 es correcto.
- **Peso**: Especifica un número de 0 a 10, que indica la importancia de este activo en la red. Un valor de 0 indica una importancia baja y 10 es muy alta.
- **Descripción**: Especifica una descripción textual para este activo con una longitud de hasta 255 caracteres. Este valor es opcional.

Por ejemplo, las siguientes entradas se pueden incluir en un archivo CSV:

-
```
192.168.5.34,WebServer01,5,Main Production Web Server
```
-
```
192.168.5.35,MailServ01,0,
```

El proceso de importación fusiona los perfiles de activo importados con la información de perfil de activo que está actualmente almacenada en el sistema.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En el recuadro de lista **Acciones**, seleccione **Importar activos**.
4. Pulse **Examinar** para localizar y seleccionar el archivo CSV que desea importar.
5. Pulse **Importar activos** para empezar el proceso de importación.

Exportación de activos

Puede exportar perfiles de activo listados a un archivo XML (Extended Markup Language - Lenguaje de marcado extensible) o CSV (Comma-Separated Value - Valor separado por comas).

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. En el cuadro de lista **Acciones**, seleccione una de las opciones siguientes:

- Exportar a XML
- Exportar a CSV

4. Vea la ventana de estado para el estado del proceso de exportación.
5. Opcional: Si desea utilizar otras pestañas y páginas mientras la exportación está en curso, pulse el enlace **Notificar cuando termine**.

   Cuando la exportación se haya completado, se visualizará la ventana Descarga de archivo.
6. En la ventana Descarga de archivo, elija una de las opciones siguientes:
   - **Abrir**: Seleccione esta opción para abrir los resultados de exportación en el navegador que haya elegido.
   - **Guardar**: Seleccione esta opción para guardar los resultados en el escritorio.
7. Pulse **Aceptar**.

Investigar vulnerabilidades de activo

El panel Vulnerabilidades en la página Perfil de activo visualiza una lista de vulnerabilidades descubiertas para el activo.

Acerca de esta tarea

Puede efectuar una doble pulsación en la vulnerabilidad a mostrar más detalles de vulnerabilidad.

La ventana Investigar detalles de vulnerabilidad proporciona los detalles siguientes:

Parámetro	Descripción
ID de vulnerabilidad	Especifica el ID de la vulnerabilidad. El ID de vulnerabilidad es un identificador exclusivo generado por VIS (Vulnerability Information System - Sistema de información de vulnerabilidad).
Fecha de publicación	Especifica la fecha en la que los detalles de vulnerabilidad se han publicado en la OSVDB.
Nombre	Especifica el nombre de la vulnerabilidad.
Activos	Especifica el número de activos de la red que tienen esta vulnerabilidad. Pulse el enlace para ver la lista de activos.
Activos, incluyendo excepciones	Especifica el número de activos de la red que tienen excepciones de vulnerabilidad. Pulse el enlace para ver la lista de activos.
CVE	Especifica el identificador de CVE para la vulnerabilidad. Los identificadores de CVE los proporciona la NVDB. Pulse el enlace para obtener más información. Al pulsar en el enlace, el sitio web NVDB se visualiza en una ventana de navegador nueva.

Parámetro	Descripción
xforce	Especifica el identificador de X-Force para la vulnerabilidad. Pulse el enlace para obtener más información. Al pulsar el enlace, el sitio web de IBM Internet Security Systems se visualiza en una ventana de navegador nueva.
OSVDB	Especifica el identificador de OSVDB para la vulnerabilidad. Pulse el enlace para obtener más información. Al pulsar el enlace, el sitio web OSVDB se visualiza en una ventana de navegador nueva.
Detalles de plug-in	Especifica el ID de QRadar Vulnerability Manager. Pulse el enlace para ver definiciones de Oval, entradas de Windows Knowledge Base o avisos de UNIX para la vulnerabilidad. Esta característica proporciona información sobre cómo QRadar Vulnerability Manager comprueba los detalles de vulnerabilidad durante una exploración de parches. Puede utilizarla para identificar por qué se ha generado una vulnerabilidad en un activo o por qué no se ha generado.
Puntuación base CVSS	Visualiza la puntuación de CVSS (Common Vulnerability Scoring System) de agregado de las vulnerabilidades en este activo. Una puntuación de CVSS es una medida de evaluación de la gravedad de una vulnerabilidad. Puede utilizar puntuaciones de CVSS para medir el grado de preocupación garantizada por una vulnerabilidad en comparación con otras vulnerabilidades. La puntuación de CVSS se calcula utilizando los siguientes parámetros definidos por el usuario: • Potencial de daños colaterales • Requisito de confidencialidad • Requisito de disponibilidad • Requisito de integridad Para obtener más información sobre cómo configurar estos parámetros, consulte “Adición o edición de un perfil de activo” en la página 146. Para obtener más información acerca de CVSS, consulte *http://www.first.org/cvss/*.

Parámetro	Descripción
Impacto	Visualiza el tipo de daño o perjuicio que se puede esperar si se aprovecha esta vulnerabilidad.
Medidas base de CVSS	Muestra las medidas que se utilizan para calcular la puntuación base de CVSS, incluyendo: • Vector de acceso • Complejidad de acceso • Autenticación • Impacto de confidencialidad • Impacto de integridad • Impacto de disponibilidad
Descripción	Especifica una descripción de la vulnerabilidad detectada. Este valor sólo está disponible cuando el sistema integra herramientas de VA.
Problema	Especifica los efectos que la vulnerabilidad puede tener en la red.
Solución	Siga las instrucciones que se proporcionan para resolver la vulnerabilidad.
Parcheo virtual	Visualiza la información de parche virtual asociada con esta vulnerabilidad, si está disponible. Un parche virtual es una solución de mitigación a corto plazo para una vulnerabilidad descubierta recientemente. Esta información se deriva de los sucesos de IPS (Intrusion Protection System - Sistema de prevención de intrusiones). Si desea instalar el parche virtual, consulte la información de proveedor de IPS.
Referencia	Visualiza una lista de referencias externas, incluyendo: • **Tipo de referencia**: Especifica el tipo de referencia que se lista, por ejemplo una lista de envío de correo o URL de advertencia. • **URL**: Especifica el URL que puede pulsar para ver la referencia. Pulse el enlace para obtener más información. Al pulsar el enlace, el recurso externo se visualiza en una ventana de navegador nueva.

Parámetro	Descripción
Productos	Visualiza una lista de productos que están asociados con esta vulnerabilidad. • **Proveedor**: Especifica el proveedor del producto. • **Producto**: Especifica el nombre de producto. • **Versión**: Especifica el número de versión del producto.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Perfiles de activo**.
3. Seleccione un perfil de activo.
4. En el panel de vulnerabilidades, pulse el valor de parámetro **ID** o **Vulnerabilidad** para la vulnerabilidad que desea investigar.

Capítulo 8. Gestión de gráficos

Puede ver los datos utilizando diversas opciones de configuración para gráficos.

Mediante los gráficos de la pestaña **Actividad de registro** y la pestaña **Actividad de red** puede ver los datos utilizando diversas opciones de configuración para gráficos.

Gestión de gráficos

Puede utilizar varias opciones de configuración de gráficos para ver los datos.

Si selecciona un intervalo de tiempo o una opción de agrupación para ver los datos, los gráficos se visualizan sobre la lista de sucesos o de flujos.

Los gráficos no se visualizan mientras se está en modalidad continua.

Puede configurar un gráfico para seleccionar los datos que desea trazar. Puede configurar gráficos independientemente el uno del otro para visualizar los resultados de búsqueda desde diferentes perspectivas.

Los tipos de gráfico incluyen:

- Gráfico de barras: Visualiza los datos en un gráfico de barras. Esta opción solo está disponible para sucesos agrupados.
- Gráfico circular: Visualiza datos en un gráfico circular. Esta opción solo está disponible para sucesos agrupados.
- Tabla: Visualiza datos en una tabla. Esta opción solo está disponible para sucesos agrupados.
- Serie temporal: Visualiza un gráfico de líneas interactivo que representa los registros que se comparan por un intervalo de tiempo especificado. Para obtener información sobre cómo configurar criterios de búsqueda de serie temporal, consulte Visión general de gráfico de serie temporal.

Después de configurar un gráfico, las configuraciones de gráfico se conservan al:

- Cambiar la vista utilizando el recuadro de lista **Visualizar**.
- Aplicar un filtro.
- Guardar criterios de búsqueda.

Las configuraciones de gráfico no se conservan al:

- Iniciar una búsqueda nueva.
- Acceder a una búsqueda rápida.
- Ver los resultados agrupados en una ventana de rama.
- Guarde los resultados de búsqueda.

Nota: Si utiliza el navegador web Mozilla Firefox y se instala una extensión de navegador de bloqueador de anuncios, no se visualizan gráficos. Para visualizar gráficos, debe eliminar la extensión de navegador de bloqueador de anuncios. Para obtener más información, consulte la documentación de navegador.

© Copyright IBM Corp. 2012, 2015

Visión general de gráfico de serie temporal

Los gráficos de serie temporal son representaciones gráficas de la actividad a lo largo del tiempo.

Los picos y valles que se visualizan en los gráficos describen la actividad de volumen alto y bajo. Los gráficos de serie temporal son útiles para las tendencias de corto plazo y largo plazo de los datos.

Mediante el uso de gráficos de serie temporal, puede acceder, navegar e investigar la actividad de registro o de red desde diversas vistas y perspectivas.

Nota: Debe tener los permisos de rol adecuados para gestionar y ver gráficos de serie temporal.

Para visualizar gráficos de serie temporal, debe crear y guardar una búsqueda que incluya opciones de agrupación y serie temporal. Puede guardar hasta 100 búsquedas de serie temporal.

Las búsquedas guardadas de serie temporal predeterminadas son accesibles desde la lista de búsquedas disponibles en la página de búsqueda de sucesos o flujos.

Puede identificar fácilmente las búsquedas de serie temporal guardadas en el menú **Búsquedas rápidas**, porque el nombre de búsqueda se añade con el rango de tiempo especificado en los criterios de búsqueda.

Si los parámetros de búsqueda coinciden con una búsqueda guardada anteriormente para las opciones de agrupación y definición de columna, es posible que se visualice automáticamente un gráfico de serie temporal para los resultados de búsqueda. Si no se visualiza automáticamente un gráfico de series temporal para los criterios de búsqueda no guardados, no existen criterios de búsqueda guardados anteriormente que coincidan con los parámetros de búsqueda. Si esto ocurre, debe habilitar la captura de datos de serie temporal y guardar los criterios de búsqueda.

Puede ampliar y explorar una línea temporal en un gráfico de series temporal para investigar la actividad. La tabla siguiente proporciona funciones que puede utilizar para ver gráficos de serie temporal.

Tabla 37. Funciones de gráficos de serie temporal

Función	Descripción
Ver datos con mayor detalle	Utilizando la característica de zoom, puede investigar segmentos de tiempo más pequeños del tráfico de sucesos. • Mueva el puntero del ratón sobre el gráfico y, a continuación, utilice la rueda del ratón para ampliar el gráfico (girar la rueda del ratón hacia arriba). • Resalte el área del gráfico que desea ampliar. Cuando suelte el botón del ratón, el gráfico muestra un segmento de tiempo más pequeño. Ahora puede pulsar y arrastrar el gráfico para explorar el gráfico. Al ampliar un gráfico de series temporal, el gráfico se renueva para mostrar un segmento de tiempo más pequeños.
Ver un intervalo de tiempo mayor de datos	Utilizando la característica de zoom, puede investigar segmentos de tiempo más grandes o volver al rango de tiempo máximo. Puede expandir un rango de tiempo utilizando una de las opciones siguientes: • Pulsar en el restablecimiento de zoom en la esquina superior izquierda del gráfico. • Mover el puntero de ratón sobre el gráfico y, a continuación, utilizar la rueda del ratón para expandir la vista (girar la rueda del ratón hacia abajo).
Explorar el gráfico	Cuando haya aumentado un gráfico de series temporal, puede pulsar y arrastrar el gráfico a la izquierda o a la derecha para explorar la línea temporal.

Leyendas de gráficos

Cada gráfico proporciona una leyenda, que es una referencia visual para ayudarle a asociar los objetos de gráfico con los parámetros que representan.

Mediante la característica de leyenda, puede realizar las acciones siguientes:

- Mueva el puntero del ratón sobre un elemento de leyenda o el bloque de color de leyenda para ver más información sobre los parámetros que representa.
- Pulse el botón derecho del ratón en el elemento de leyenda para investigar el elemento adicionalmente.
- Pulse un elemento de leyenda de gráfico circular o de barras para ocultar el elemento en el gráfico. Pulse el elemento de leyenda de nuevo para mostrar el elemento oculto. También puede pulsar el elemento de gráfico correspondiente para ocultar y mostrar el elemento.
- Pulse **Leyenda**, o la flecha que se encuentra junto a ella, si desea eliminar la leyenda de la pantalla de gráfico.

Configuración de gráficos

Puede utilizar opciones de configuración para cambiar el tipo de gráfico, el tipo de objeto del que desea crear el gráfico y el número de objetos que se representan en el gráfico. Para gráficos de serie temporal, también puede seleccionar un intervalo de tiempo y habilitar la captura de datos de serie temporal.

Antes de empezar

Los gráficos no se visualizan cuando se visualizan sucesos o flujos en modalidad de tiempo real (modalidad continua). Para visualizar gráficos, debe acceder a la pestaña **Actividad de registro** o **Actividad de red** y elija una de las opciones siguientes:

- Seleccione opciones en los recuadros de lista **Ver** y **Visualizar** y, a continuación, pulse **Guardar criterios** en la barra de herramientas. Consulte Guardar criterios de búsqueda.
- En la barra de herramientas, seleccione una búsqueda guardada en la lista **Búsqueda rápida**.
- Realice una búsqueda agrupada y, a continuación, pulse **Guardar criterios** en la barra de herramientas.

Si piensa configurar un gráfico de serie temporal, asegúrese de que los criterios de búsqueda guardada se agrupen y especifiquen un rango de tiempo.

Acerca de esta tarea

Los datos se pueden acumular para que cuando se realice una búsqueda de serie temporal, esté disponible una memoria caché de datos para visualizar datos para el periodo de tiempo anterior. Después de habilitar la captura de datos de serie temporal para un parámetro seleccionado, se visualiza un asterisco (*) junto al parámetro en el recuadro de lista Valor para gráfico.

Procedimiento

1. Pulse la pestaña **Actividad de registro** o **Actividad de red**.
2. En el panel Gráficos, pulse el icono **Configurar**.
3. Configure valores para los parámetros siguientes:

Opción	Descripción
Parámetro	Descripción
Valor para gráfico	En el recuadro de lista, seleccione el tipo de objeto que desea trazar en el eje Y del gráfico. Las opciones incluyen todos los parámetros de suceso o de flujo normalizados y personalizados que se incluyen en los parámetros de búsqueda.
Mostrar parte superior	En el cuadro de lista, seleccione el número de objetos que desee ver en el gráfico. El valor predeterminado es 10. Si se crean gráficos de más de 10 elementos es posible que los datos de gráfico no sean legibles.

Opción	Descripción
Tipo de gráfico	En el cuadro de lista, seleccione el tipo de gráfico que desee ver. Si el gráfico de barras, circular o de tabla se basa en criterios de búsqueda guardados con un rango de tiempo de más de 1 hora, debe pulsar **Actualizar detalles** para actualizar el gráfico y llenar los detalles de suceso
Capturar datos de serie temporal	Seleccione este recuadro de selección si desea habilitar la captura de datos de serie temporal. Cuando se selecciona este recuadro de selección, la característica de gráfico empieza a acumular datos para gráficos de serie temporal. De forma predeterminada, esta opción está inhabilitada. Esta opción solo está disponible en gráficos de serie temporal.
Rango de tiempo	En el cuadro de lista, seleccione el rango de tiempo que desee ver. Esta opción solo está disponible en gráficos de serie temporal.

4. Si ha seleccionado la opción de gráfico **Serie temporal** y ha habilitado la opción **Capturar datos de serie temporal**, pulse **Guardar criterios** en la barra de herramientas.
5. Para ver la lista de sucesos o flujos si el rango de tiempo es mayor que 1 hora, pulse **Actualizar detalles**.

Capítulo 9. Búsquedas de datos

En la pestaña **Actividad de registro**, **Actividad de red** y **Delitos** puede buscar sucesos, flujos y delitos utilizando criterios específicos.

Puede crear una búsqueda nueva o cargar un conjunto de criterios de búsqueda que previamente se han guardado. Puede seleccionar, organizar y agrupar las columnas de datos que se deben mostrar en los resultados de búsqueda

Búsquedas de sucesos y flujos

Puede realizar búsquedas en la pestaña **Actividad de registro** y en la pestaña **Actividad de red**.

Después de realizar una búsqueda, puede guardar los criterios de búsqueda y los resultados de la búsqueda.

Búsqueda de elementos que coinciden con los criterios

Puede buscar datos que coincidan con los criterios de búsqueda.

Acerca de esta tarea

Puesto que se busca en la base de datos entera, es posible que las búsquedas tarden un tiempo prolongado, dependiendo del tamaño de la base de datos.

Puede utilizar el parámetro de búsqueda **Filtro rápido** para buscar elementos que coinciden con la serie de búsqueda en la carga útil de suceso.

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de suceso y de flujo:

Tabla 38. Opciones de búsqueda

Opciones	Descripción
Grupo	Seleccione un grupo de búsqueda de sucesos o un grupo de búsqueda de flujos para verlo en la lista **Búsquedas guardadas disponibles**.
Escriba la búsqueda guardada o seleccione en la lista	Escriba el nombre de una búsqueda guardada o una palabra clave para filtrar la lista **Búsquedas guardadas disponibles**.
Búsquedas guardadas disponibles	Esta lista muestra todas las búsquedas disponibles, a menos que utilice las opciones **Agrupe o Escriba la búsqueda guardada** o **Seleccione en la lista** para aplicar un filtro a la lista. Puede seleccionar una búsqueda guardada en esta lista para visualizarla o editarla.
Buscar	El icono **Buscar** está disponible en varios paneles de la página de búsqueda. Puede pulsar Buscar cuando haya terminado de configurar la búsqueda y desee ver los resultados.

© Copyright IBM Corp. 2012, 2015

Tabla 38. Opciones de búsqueda (continuación)

Opciones	Descripción
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el menú **Búsqueda rápida**.
Incluir en Panel de control	Marque este recuadro de selección para incluir los datos de la búsqueda guardada en la pestaña **Panel de control**. Para obtener más información sobre la pestaña **Panel de control**, consulte Gestión de panel de control. **Nota:** Este parámetro sólo se visualiza si se agrupa la búsqueda.
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.
Compartir con todos	Marque este recuadro de selección para compartir esta búsqueda con todos los demás usuarios.
Tiempo real (modalidad continua)	Visualiza resultados en modalidad continua. Para obtener más información sobre la modalidad continua, consulte Visualización de sucesos de modalidad continua. **Nota:** Cuando se habilita Tiempo real (modalidad continua), no puede agrupar los resultados de búsqueda. Si selecciona cualquier opción de agrupación en el panel Definición de columna, se abre un mensaje de error.
Último intervalo (renovación automática)	Visualiza los resultados de búsqueda en modalidad de renovación automática. En la modalidad de renovación automática, se produce una renovación de la pestaña **Actividad de registro**y **Actividad de red** a intervalos de un minuto para visualizar la información más reciente.
Reciente	Seleccione un rango de tiempo predefinido para la búsqueda. Después de seleccionar esta opción, debe seleccionar una opción de rango de tiempo en el cuadro de lista.
Intervalo específico	Seleccione un rango de tiempo personalizado para la búsqueda. Después de seleccionar esta opción, debe seleccionar el rango de fecha y hora en los calendarios **Hora de inicio** y **Hora de finalización**.

Tabla 38. Opciones de búsqueda (continuación)

Opciones	Descripción
Acumulación de datos	Este panel sólo se visualiza cuando se carga una búsqueda guardada. La habilitación de recuentos exclusivos en datos acumulados que se comparten con muchos otros informes y búsquedas guardadas puede disminuir el rendimiento del sistema. Al cargar una búsqueda guardada, este panel muestra las opciones siguientes: • Si no se acumulan datos para esta búsqueda guardada, se visualiza el siguiente búsqueda: `No se están acumulando datos para esta búsqueda`. • Si se acumulan datos se acumulan para esta búsqueda guardada, se visualizan las opciones siguientes: – **columnas**: Al pulsar este enlace o pasar el puntero del ratón sobre él, se abre una lista de las columnas que están acumulando datos. – **Habilitar recuentos exclusivos/Inhabilitar recuentos exclusivos**: Este enlace le permite habilitar o inhabilitar los resultados de búsqueda para visualizar recuentos sucesos y flujos exclusivos en lugar de promedios de recuentos a lo largo del tiempo. Después de pulsar el enlace **Habilitar recuentos exclusivos**, se abre un recuadro de diálogo que indica qué informes y búsquedas guardadas comparten los datos acumulados.
Filtros actuales	Esta lista muestra los filtros que se aplican a esta búsqueda. Las opciones para añadir un filtro se encuentran sobre la lista **Filtros actuales**.
Guardar resultados cuando finalice la búsqueda	Marque este recuadro de selección para guardar y dar nombre a los resultados de la búsqueda.
Visualizar	Seleccione esta lista para especificar una columna predefinida que se ha establecido para visualizarse en los resultados de búsqueda.
Escriba la columna o seleccione en la lista	Puede utilizar el campo para filtrar las columnas que figuran en la lista Columnas disponibles. Escriba el nombre de la columna que desea localizar o escriba una palabra clave para visualizar una lista de nombres de columna. Por ejemplo, escriba `Device` para visualizar una lista de columnas que incluyan Device en el nombre de columna.

Tabla 38. Opciones de búsqueda (continuación)

Opciones	Descripción
Columnas disponibles	Esta lista muestra las columnas disponibles. Las columnas que se están utilizando actualmente para esta búsqueda guardada se resaltan y se visualizan en la lista de **Columnas**.
Añadir y eliminar iconos de columna (conjunto superior)	Utilice el conjunto superior de iconos para personalizar la lista **Agrupar por**. • **Añadir columna**: Seleccione una o más columnas de la lista **Columnas disponibles** y pulse el icono **Añadir columna**. • **Eliminar columna**: Seleccione una o más columnas de la lista **Agrupar por** y pulse el icono **Eliminar columna**.
Añadir y eliminar iconos de columna (conjunto inferior)	Utilice el conjunto inferior de iconos para personalizar la lista **Columnas**. • **Añadir columna**: Seleccione una o más columnas de la lista Columnas disponibles y pulse el icono **Añadir columna**. • **Eliminar columna**: Seleccione una o más columnas de la lista Columnas y pulse el icono **Eliminar columna**.
Agrupar por	Esta lista especifica las columnas en las que la búsqueda guardada agrupa los resultados. Utilice las opciones siguientes para personalizar adicionalmente la lista Agrupar por: • Subir: Seleccione una columna y muévala hacia arriba en la lista de prioridad utilizando el icono **Subir**. • Bajar: Seleccione una columna y muévala hacia abajo en la lista de prioridad utilizando el icono **Bajar**. La lista de prioridad especifica en qué orden se agrupan los resultados. Los resultados de búsqueda se agrupan por la primera columna de la lista **Agrupar por** y, a continuación, se agrupan por la columna siguiente de la lista.

Tabla 38. Opciones de búsqueda (continuación)

Opciones	Descripción
Columnas	Especifica las columnas que se han elegido para la búsqueda. Puede seleccionar más columnas de la lista **Columnas disponibles**. Puede personalizar adicionalmente la lista **Columnas** utilizando las opciones siguientes: • **Subir**: Mueve la columna seleccionada hacia arriba en la lista de prioridades. • **Bajar**: Mueve la columna seleccionada hacia abajo en la lista de prioridades. Si el tipo de columna es numérico o está basado en el tiempo y hay una entrada en la lista **Agrupar por**, la columna incluye un recuadro de lista. Utilice el recuadro de lista para elegir cómo desea agrupar la columna. Si el tipo de columna es grupo, la columna incluye un recuadro de lista para elegir cuántos niveles desea incluir para el grupo.
Ordenar por	En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda. A continuación, en el segundo recuadro de lista, seleccione el orden que desea para visualizar para los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
Límite de resultados	Puede especificar el número de filas que una búsqueda devuelve en la ventana Editar búsqueda . El campo **Límite de resultados** también aparece en la ventana Resultados . • Para una búsqueda guardada, el límite se almacena en la búsqueda guardada y se vuelve a aplicar al cargar la búsqueda. • Cuando se realiza una ordenación en una columna del resultado de búsqueda que tiene un límite de filas, la ordenación se realiza dentro de las filas limitadas que se muestran en la cuadrícula de datos. • En el caso de una búsqueda agrupada por con el gráfico de serie temporal activado, el límite de filas sólo se aplica a la cuadrícula de datos. El desplegable **N principales** del gráfico de serie temporal sigue controlando cuántas series temporales se dibujan en el gráfico.

Procedimiento

1. Elija una de las siguientes opciones:
   - Para buscar sucesos, pulse la pestaña **Actividad de registro**.
   - Para buscar flujos, pulse la pestaña **Actividad de red**.
2. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
3. Para seleccionar una búsqueda guardada anteriormente:

a. Elija una de las opciones siguientes: En la lista Búsquedas guardadas disponibles, seleccione la búsqueda guardada que desea guardar. En el campo Escriba la búsqueda guardada o seleccione en la lista, escriba el nombre de la búsqueda que desea cargar.
b. Pulse **Cargar**.
c. En el panel Editar búsqueda, seleccione las opciones que desea para esta búsqueda. Consulte la Tabla 1.

4. Para crear una búsqueda, en el panel Rango de tiempo, seleccione las opciones para el rango de tiempo que desea capturar para esta búsqueda.
5. Opcional. En el panel Acumulación de datos, habilite recuentos exclusivos:
   a. Pulse **Habilitar recuentos exclusivos**.
   b. En la ventana Aviso, lea el mensaje de aviso y pulse **Continuar**. Para obtener más información sobre cómo habilitar recuentos exclusivos, consulte la Tabla 1.
6. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
   a. En el primer recuadro de lista, seleccione un parámetro que desee buscar. Por ejemplo, Dispositivo, Puerto de origen o Nombre de suceso.
   b. En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda.
   c. En el campo de entrada, escriba información específica que está relacionada con el parámetro de búsqueda.
   d. Pulse **Añadir filtro**.
   e. Repita los pasos a hasta d para cada filtro que desea añadir a los criterios de búsqueda.
7. Opcional. Para guardar automáticamente los resultados de búsqueda cuando la búsqueda se ha completado, marque el recuadro de selección **Guarde los resultados cuando finalice la búsqueda** y, a continuación, escriba un nombre para la búsqueda guardada.
8. En el panel Definición de columna, defina las columnas y el diseño de columna que desea utilizar para ver los resultados:
   a. En el recuadro de lista **Visualizar**, seleccione la columna preconfigurada establecida para asociarse con esta búsqueda.
   b. Pulse la flecha situada junto a **Definición de vista avanzada** para visualizar parámetros de búsqueda avanzada.
   c. Personalice las columnas que se visualizarán en los resultados de búsqueda. Consulte la Tabla 1.
   d. Opcional. En el campo **Límite de resultados**, escriba el número de filas que desea que devuelva la búsqueda.
9. Pulse **Filtro**.

Resultados

Se visualiza el estado **En curso (<porcentaje>%completado)** en la esquina superior derecha.

.

Al ver resultados de búsqueda parciales, el motor de búsqueda funciona en segundo plano para completar la búsqueda y renueva los resultados parciales para actualizar la vista.

Cuando la búsqueda se ha completado, se visualiza el estado **Completado** en la esquina superior derecha.

Guardar criterios de búsqueda

Puede guardar los criterios de búsqueda configurados para poder reutilizar los criterios y utilizar los criterios de búsqueda guardados en otros componentes como, por ejemplo, informes. Los criterios de búsqueda guardados no caducan.

Acerca de esta tarea

Si se especifica un rango temporal para la búsqueda, el nombre de búsqueda se añade con el rango de tiempo especificado. Por ejemplo, una búsqueda guardada denominada Explotaciones por origen con un rango de tiempo de Últimos 5 minutos se convierte en Explotaciones por origen - Últimos 5 minutos.

Si cambia una columna establecida en una búsqueda guardada anteriormente y luego guarda los criterios de búsqueda utilizando el mismo nombre, se perderán las acumulaciones anteriores de gráficos de series temporales.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. Realice una búsqueda.
3. Pulse **Guardar criterios**.
4. Entre valores para los parámetros:

Opción	**Descripción**
Parámetro	Descripción
Nombre de búsqueda	Escriba el nombre exclusivo que desee asignar a este criterio de búsqueda.
Asignar búsqueda a grupo(s)	Marque el recuadro de selección para el grupo al que desea asignar esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo Otros de forma predeterminada. Para obtener más información, consulte Gestión de grupos de búsqueda.
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de búsqueda. Para obtener más información, consulte Gestión de grupos de búsqueda.

Opción	Descripción
Opciones de intervalo de tiempo:	Elija una de las siguientes opciones: • **Tiempo real (modalidad continua)**: Seleccione esta opción para filtrar los resultados de búsqueda mientras se está en modalidad continua. • **Último intervalo (renovación automática)**: Seleccione esta opción para filtrar los resultados de búsqueda mientras se está en modalidad de renovación automática. Se produce una renovación de la pestaña **Actividad de registro** y de la pestaña **Actividad de red** a intervalos de un minuto para visualizar la información más reciente. • **Reciente**: Seleccione esta opción y, desde este recuadro de lista, seleccione el rango de tiempo por el que desea filtrar. • **Intervalo específico**: Seleccione esta opción y, en el calendario, seleccione el rango de fecha y hora por el que desea filtrar.
Incluir en Búsquedas rápidas	Marque este recuadro de selección para incluir esta búsqueda en el recuadro de lista **Búsqueda rápida** en la barra de herramientas.
Incluir en Panel de control	Marque este recuadro de selección para incluir los datos de la búsqueda guardada en la pestaña **Panel de control**. Para obtener más información sobre la pestaña **Panel de control**, consulte Gestión de panel de control. **Nota:** Este parámetro sólo se visualiza si se agrupa la búsqueda.
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.
Compartir con todos	Marque este recuadro de selección para compartir estos requisitos de búsqueda con todos los usuarios.

5. Pulse **Aceptar**.

Búsqueda planificada

Utilice la opción de búsqueda planificada para planificar una búsqueda y ver los resultados.

Puede planificar que una búsqueda se ejecute a una hora específica del día o de la noche.

Ejemplo:
Si planifica que una búsqueda se ejecute por la noche, puede investigar por la mañana. A diferencia de los informes, tiene la opción de agrupar los resultados de búsqueda e investigar adicionalmente. Puede buscar el número de inicios de sesión anómalos en el grupo de red. Si el resultado es generalmente 10 y el resultado de

la búsqueda es 100, puede agrupar los resultados de búsqueda para facilitar la investigación. Para ver qué usuario tiene la mayoría de inicios de sesión anómalos, puede agruparlos por nombre de usuario. Puede continuar investigando adicionalmente.

Puede planificar una búsqueda en sucesos o flujos desde la pestaña **Informes**. Debe seleccionar un conjunto de criterios de búsqueda previamente guardado para la planificación.

1. Cree un informe

   Especifique la siguiente información en la ventana **Asistente de informes**:

   - El tipo de gráfico es Sucesos/Archivos de registro o Flujos.
   - El informe se basa en una búsqueda guardada.
   - Genere un delito.

     Puede elegir la opción **Crear un delito individual** o la opción **Añadir resultado a un delito existente**.

     También puede generar una búsqueda manual.
2. Vea los resultados de búsqueda

Puede ver los resultados de la búsqueda planificada desde la pestaña **Delitos**.

- Los delitos de búsqueda planificada se identifican por la columna **Tipo de delito**.

  Si crea un delito individual, se genera un delito cada vez que se ejecuta el informe. Si añade el resultado de búsqueda guardada en un delito existente, se crea un delito la primera vez que se ejecuta el informe. Las ejecuciones de informe subsiguientes se añaden a este delito. Si no se devuelven resultados, el sistema no añade o crea un delito.
- Para ver el resultado de búsqueda más reciente en la ventana Resumen de delitos, efectúe una doble pulsación en un delito de búsqueda planificada de la lista de delitos. Para ver la lista de todas las ejecuciones de búsqueda planificada, pulse **Resultados de búsqueda** en el panel **Últimos 5 resultados de búsqueda**.

Puede asignar un delito de búsqueda planificada a un usuario.

Tareas relacionadas:

"Búsqueda de elementos que coinciden con los criterios" en la página 167
Puede buscar datos que coincidan con los criterios de búsqueda.

"Asignar delitos a usuarios" en la página 46
Desde la pestaña **Delitos**, puede asignar delitos a usuarios con fines de investigación.

Opciones de búsqueda avanzada

Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

El campo **Búsqueda avanzada** tiene finalización automática y resaltado de sintaxis.

Utilice la finalización automática y el resaltado de sintaxis para ayudar a crear consultas. Para obtener información sobre los navegadores web soportados, consulte "Navegadores web soportados" en la página 6

Acceso a búsqueda avanzada

Acceda a la opción **Búsqueda avanzada** desde la barra de herramientas **Buscar** que está en las pestañas **Actividad de red** y **Actividad de registro** para escribir una consulta de AQL.

Seleccione **Búsqueda avanzada** desde el recuadro de lista de la barra de herramientas **Buscar**.

Expanda el campo **Búsqueda avanzada** siguiendo estos pasos:

1. Arrastre el icono de expansión que se encuentra a la derecha del campo.
2. Pulse Mayús + Intro para ir a la línea siguiente.
3. Pulse Intro.

Puede pulsar el botón derecho del ratón en cualquier valor del resultado de búsqueda y filtrar por ese valor.

Efectúe una doble pulsación en cualquier fila del resultado de búsqueda para ver más detalles.

Todas las búsquedas, incluidas las búsquedas de AOL, se incluyen en el registro de auditoría.

Ejemplos de serie de búsqueda de AQL

La tabla siguiente proporciona ejemplos de las series de búsqueda de AOL.

Tabla 39. Ejemplos de series de búsqueda de AOL

Descripción	Ejemplo

Seleccionar columnas predeterminadas en sucesos.
 	
Seleccionar columnas predeterminados en flujos.
	`SELECT * FROM events`
	
	`SELECT * FROM flows`

Seleccionar columnas específicas.	`SELECT sourceip, destinationip FROM events`
Seleccionar columnas específicas y ordenar los resultados.	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
Ejecutar una consulta de búsqueda agregada.	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
Ejecutar una llamada de función en una cláusula SELECT.	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
Filtrar los resultados de búsqueda utilizando una cláusula WHERE.	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
Buscar sucesos que han desencadenado una regla específica, que se basa en el nombre de regla o el texto parcial en el nombre de regla.	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
Hacer referencia a nombres de campo que contienen caracteres especiales, por ejemplo caracteres aritméticos o espacios, poniendo el nombre de campo entre comillas.	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

La tabla siguiente proporciona ejemplos de las series de búsqueda de AQL para X-Force.

Tabla 40. Ejemplos de series de búsqueda de AQL para X-Force

Descripción	Ejemplo
Comparar una dirección IP con una categoría de X-Force con un valor de confianza.	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3`
Buscar las categorías de URL de X-Force asociadas con un URL.	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
Recuperar las categorías de IP de X-Force que están asociadas con una IP.	`select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

Para obtener más información acerca de las funciones y los campos y operadores de búsqueda, consulte la publicación *Ariel Query Language guide*.

Ejemplos de cadenas de búsqueda de AQL

Utilice Ariel Query Language (AQL) para recuperar campos determinados de los sucesos, flujos y tablas simarc contenidos en la base de datos Ariel.

Nota: Cuando construye una consulta AQL, si copia texto que contiene apóstrofos de cualquier documento y lo pega en IBM Security QRadar, la consulta no se analizará. Como solución, puede pegar el texto en QRadar y volver a teclear los apóstrofos o puede copiar y pegar el texto de IBM Knowledge Center.

Informes de uso de cuenta

Comunidades de usuarios diferentes pueden tener indicadores de amenazas y de uso diferentes.

Utilice datos de referencia para informar sobre diversas propiedades de usuario, tales como departamento, ubicación o gestor.

Puede utilizar datos de referencia externos.

La consulta siguiente devuelve información de metadatos sobre el usuario a partir de sucesos de inicio de sesión.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Identificadores de cuenta múltiples

En este ejemplo, los usuarios tienen varias cuentas en la red. La empresa necesita tener una vista individual de la actividad de un usuario.

Utilice datos de referencia para correlacionar un ID de usuario local con un ID global.

La consulta siguiente devuelve las cuentas de usuario que son utilizadas por un ID global en sucesos que están marcados como sospechosos.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

La consulta siguiente muestra las actividades que se han realizado mediante un ID global.

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identificar una emisión larga de señales de baliza sospechosa

Muchas amenazas utilizan mandato y control para transmitir periódicamente durante días, semanas y meses.

Las búsquedas avanzadas pueden identificar patrones de conexión a lo largo del tiempo. Por ejemplo, puede investigar conexiones breves, constantes y de pequeño volumen que se realizan cada día/semana/mes entre direcciones IP o entre una dirección IP y una ubicación geográfica.

Utilice la API REST de IBM Security QRadar para generar un delito o para llenar un conjunto de referencia o tabla de referencia.

La consulta siguiente detecta posibles casos de emisiones de señales de baliza realizadas cada hora.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'hh')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING 'different hours' > 20
AND 'total flows' < 25
LAST 24 hours
```

Consejo: Puede modificar esta consulta para trabajar en archivos de registro de proxy y otros tipos de sucesos.

La consulta siguiente detecta posibles casos de emisiones diarias de señales de baliza.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
```

```
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING 'different days' > 4
AND 'total flows' < 14
LAST 7 days
```

La consulta siguiente detecta la emisión diaria de señales de baliza entre una dirección IP de origen y una dirección IP de destino. Las horas de emisión de señales de baliza no son las mismas cada día. El intervalo de tiempo entre emisiones es corto.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and 'total flows' < 10
LAST 7 days
```

La consulta siguiente detecta la emisión diaria de señales de baliza hacia un dominio utilizando sucesos de registro de proxy. Las horas de emisión de señales de baliza no son las mismas cada día. El intervalo de tiempo entre emisiones es corto.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

La propiedad **url_domain** es una propiedad personalizada de los archivos de registro de proxy.

Datos de inteligencia sobre amenazas externas

Los datos de uso y de seguridad que están correlacionados con datos de inteligencia sobre amenazas externas pueden proporcionar indicadores importantes sobre amenazas.

Las búsquedas avanzadas pueden asociar indicadores de amenazas externas con otros sucesos de seguridad y datos de uso.

Esta consulta muestra cómo puede analizar datos de amenazas externas durante muchos días, semanas o meses para identificar y priorizar el nivel de riesgo de activos y cuentas.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Inteligencia y configuración de activos

Los indicadores de amenazas y de uso varían según el tipo de activo, sistema operativo, vulnerabilidad, tipo de servidor, clasificación y otros parámetros.

La consulta siguiente utiliza búsquedas avanzadas y el modelo de activos para obtener conocimientos operativos respecto a una ubicación.

La función **Assetproperty** obtiene valores de propiedad de activos, lo cual permite incluir datos de activos en los resultados.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

La consulta siguiente muestra cómo puede utilizar búsquedas avanzadas y el seguimiento de identidades de usuario en el modelo de activos.

La función **AssetUser** obtiene el nombre de usuario a partir de la base de datos de activos.

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY 'Total Flows' DESC
LAST 3 HOURS
```

Función de búsqueda de red

Puede utilizar la función de **búsqueda de red** para obtener el nombre de red que está asociado a una dirección IP.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Función de búsqueda de regla

Puede utilizar la función de **búsqueda de regla** para obtener el nombre de una regla por su identificador.

```
SELECT RULENAME(123) FROM events
```

La consulta siguiente devuelve los sucesos que activaron un nombre de regla determinado.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

Búsqueda de texto completo TEXT SEARCH

Puede utilizar el operador TEXT SEARCH para realizar búsquedas de texto completo mediante la opción **Búsqueda avanzada**.

En este ejemplo, hay un número de sucesos que contienen la palabra "firewall" en la carga útil. Puede buscar estos sucesos con la opción **Filtro rápido** y la opción **Búsqueda avanzada** en la pestaña **Actividad de registro**.

- Para utilizar la opción **Filtro rápido**, escriba el texto siguiente en el cuadro **Filtro rápido**: `'firewall'`
- Para utilizar la opción **Búsqueda avanzada**, escriba la consulta siguiente en el cuadro **Búsqueda avanzada**:

```
SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
```

Propiedad personalizada

Puede acceder a las propiedades personalizadas para sucesos y flujos cuando utiliza la opción **Búsqueda avanzada**.

La consulta siguiente utiliza la propiedad personalizada "MyWebsiteUrl" para ordenar sucesos por un URL web determinada:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Conceptos relacionados:

"Opciones de búsqueda de Filtro rápido"
Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

Tareas relacionadas:

"Creación de una propiedad personalizada basada en expresión regular" en la página 204
Puede crear una propiedad personalizada basada en expresión regular para comparar cargas útiles de sucesos o flujos con una expresión regular.

Opciones de búsqueda de Filtro rápido

Buscar cargas útiles de sucesos y flujos escribiendo una serie de búsqueda de texto que utilice palabras o frases simples.

Puede filtrar las búsquedas desde estas ubicaciones:

Barra de herramientas Actividad de registro y barras de herramientas Actividad de red
Seleccione **Filtro rápido** en el recuadro de lista de la barra de herramientas **Buscar** para escribir una serie de búsqueda de texto. Pulse el icono **Filtro rápido** para aplicar el **Filtro rápido** a la lista de sucesos o flujos.

Recuadro de diálogo Añadir filtro
Pulse el icono **Añadir filtro** en la pestaña **Actividad de registro** o **Actividad de red**.

Seleccione **Filtro rápido** como parámetro de filtro y escriba una serie de búsqueda de texto.

Páginas de búsqueda de flujos
Añada un filtro rápido a la lista de filtros.

Cuando vea **flujos** en tiempo real (modalidad continua) o modalidad del último intervalo, puede escribir sólo palabras o frases simples en el campo **Filtro rápido**. Cuando vea **sucesos** o **flujos** en un rango de tiempo, siga estas directrices de sintaxis:

Tabla 41. Directrices de sintaxis de filtro rápido

Descripción	Ejemplo
Incluir cualquier texto sin formato que se espera encontrar en la carga útil.	`Firewall`
Buscar frases exactas incluyendo varios términos entre comillas.	`"Denegación de cortafuegos"`
Incluir caracteres comodín individuales y múltiples. El término de búsqueda no puede empezar con un comodín.	`F?rewall` o `F??ew*`
Agrupar términos con expresiones lógicas, por ejemplo AND, OR y NOT. Para que se reconozca como expresiones lógicas y no como términos de búsqueda, la sintaxis y los operadores deben estar en mayúsculas.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
Al crear criterios de búsqueda que incluyen la expresión lógica NOT, debe incluir al menos otro tipo de expresión lógica, de lo contrario, no se devuelven resultados.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
Preceder los siguientes caracteres por una barra inclinada invertida para indicar que el carácter es parte del término de búsqueda: `+ - && || ! () {} [] ^ " ~ * ? : \.`	`"%PIX\-5\-304001"`

Los términos de búsqueda se comparan en secuencia desde el primer carácter de la palabra o frase de carga útil. El término de búsqueda `user` coincide con `user_1` y `user_2`, pero no coincide con las frases siguientes: `ruser`, `myuser` o `anyuser`.

Las búsquedas de Filtro rápido utilizan el entorno local inglés. El *entorno local* es un valor que identifica el idioma o la geografía y determina los convenios de formato como ordenación, conversión de mayúsculas y minúsculas, clasificación de caracteres, idioma de los mensajes, representación de la fecha y la hora y representación numérica.

El entorno local lo establece el sistema operativo. Puede configurar QRadar para alterar temporalmente el valor del entorno local del sistema operativo. Por ejemplo, puede establecer el entorno local en **Inglés** y QRadar Console puede establecerse en **Italiano**.

Si utiliza caracteres Unicode en la consulta de búsqueda de Filtro rápido, podrían devolverse resultados de búsqueda inesperados.

Si elige un entorno local que no sea inglés, puede utilizar la opción Búsqueda avanzada en QRadar para realizar búsquedas en los datos de sucesos y carga útil.

Conceptos relacionados:

Capítulo 9, “Búsquedas de datos”, en la página 167
En la pestaña **Actividad de registro**, **Actividad de red** y **Delitos** puede buscar sucesos, flujos y delitos utilizando criterios específicos.

“Opciones de búsqueda avanzada” en la página 175
Utilizar el campo **Búsqueda avanzada** para entrar un lenguaje de consulta de Ariel (AQL) que especifique los campos que desea y cómo desea agruparlos para ejecutar una consulta.

“Ejemplos de cadenas de búsqueda de AQL” en la página 177
Utilice Ariel Query Language (AQL) para recuperar campos determinados de los

sucesos, flujos y tablas simarc contenidos en la base de datos Ariel.

Tareas relacionadas:

"Actualización de preferencias de usuario" en la página 17
Puede establecer las preferencias de usuario, por ejemplo entorno local, en la interfaz de usuario de IBM Security QRadar SIEM principal.

Búsquedas de delitos

Puede buscar delitos utilizando criterios específicos para visualizar, en una lista de resultados, los delitos que coinciden con los criterios de búsqueda.

Puede crear una búsqueda nueva o cargar un conjunto de criterios de búsqueda que previamente se han guardado.

Buscar delitos en las páginas Mis delitos y Todos los delitos

En las páginas Mis delitos y Todos los delitos de la pestaña **Delito**, puede buscar delitos que coinciden con los criterios de búsqueda especificados.

Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en las páginas **Mis delitos** y **Todos los delitos**.

Para obtener información sobre categorías, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Tabla 42. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos

Opciones	Descripción
Grupo	Este cuadro de lista le permite seleccionar un grupo de búsqueda de delito en la lista **Búsquedas guardadas disponibles** para su visualización.
Escriba la búsqueda guardada o seleccione en la lista	Este campo le permite escribir el nombre de una búsqueda guardada o una palabra clave para filtrar la lista **Búsquedas guardadas disponibles**.
Búsquedas guardadas disponibles	Esta lista muestra todas las búsquedas disponibles, a menos que aplique un filtro a la lista utilizando las opciones Grupo o **Escriba la búsqueda guardada o seleccione en la lista**. Puede seleccionar una búsqueda guardada en esta lista para visualizarla o editarla.
Todos los delitos	Esta opción le permite buscar todos los delitos sin importar el rango de tiempo.
Reciente	Esta opción le permite seleccionar un rango de tiempo predefinido que desee utilizar como filtro. Después de seleccionar esta opción, debe seleccionar una opción de rango de tiempo en el cuadro de lista.

Tabla 42. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos (continuación)

Opciones	Descripción
Intervalo específico	Esta opción le permite definir un rango de tiempo personalizado para la búsqueda. Después de seleccionar esta opción, debe seleccionar una de las opciones siguientes. • **Fecha de inicio entre**: seleccione esta casilla para buscar delitos que se iniciaron durante un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar. • **Último suceso/flujo entre**: seleccione esta casilla para buscar delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.
Buscar	El icono **Buscar** está disponible en varios paneles de la página de búsqueda. Puede pulsar **Buscar** cuando termine de configurar la búsqueda y desee ver los resultados.
ID de delito	En este campo, puede escribir el ID de delito que desee buscar.
Descripción	En este campo, puede escribir la descripción para la que desee buscar.
Asignado a usuario	En este cuadro de lista, puede seleccionar el nombre de usuario para el que desee buscar.
Dirección	En este cuadro de lista, puede seleccionar la dirección de delito para la que desee buscar. Las opciones son: • Local a local • Local a remoto • Remoto a local • Remoto a remoto • Local a remoto o local • Remoto a remoto o local
IP de origen	En este campo, puede escribir la dirección IP de origen o rango de CIDR para el que desee buscar.
IP de destino	En este campo, puede escribir la dirección IP de destino o rango de CIDR para el que desee buscar.
Magnitud	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.

Tabla 42. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos (continuación)

Opciones	Descripción
Gravedad	En este cuadro de lista, puede especificar un valor de gravedad y luego seleccionar que solamente se muestren los delitos cuya gravedad sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
Credibilidad	En este cuadro de lista, puede especificar un valor de credibilidad y luego seleccionar que solamente se muestren los delitos cuya credibilidad sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
Importancia	En este cuadro de lista, puede especificar un valor de importancia y luego seleccionar que solamente se muestren los delitos cuya importancia sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
Contiene nombre de usuario	En este campo, puede escribir una sentencia de expresión regular (regex) para buscar delitos que contienen un nombre de usuario determinado. Cuando defina patrones de expresión de regular personalizados, siga las reglas de expresión regular tal como están definidas por el lenguaje de programación Java™. Para obtener más información, puede consultar las guías de aprendizaje sobre expresiones regulares que encontrará en la web.
Red de origen	En este cuadro de lista, puede seleccionar la red de origen para la que desee buscar.
Red de destino	En este cuadro de lista, puede seleccionar la red de destino para la que desee buscar.
Categoría de nivel alto	En este cuadro de lista, puede seleccionar la categoría de nivel alto para la que desee buscar. .
Categoría de nivel bajo	En este cuadro de lista, puede seleccionar la categoría de nivel bajo para la que desee buscar.
Excluir	Las opciones de este panel le permiten excluir delitos en los resultados de búsqueda. Las opciones son: • Delitos activos • Delitos ocultos • Delitos cerrados • Delitos inactivos • Delitos protegidos

Tabla 42. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos (continuación)

Opciones	Descripción
Cerrado por usuario	Este parámetro sólo se muestra cuando la casilla **Delitos cerrados** está en blanco en el panel Excluir. En este cuadro de lista, puede seleccionar el nombre de usuario para el que desee buscar delitos cerrados, o seleccionar `Cualquiera` para mostrar todos los delitos cerrados.
Razón del cierre	Este parámetro sólo se muestra cuando la casilla **Delitos cerrados** está en blanco en el panel Excluir. En este cuadro de lista, puede seleccionar una razón para la que desee buscar delitos cerrados, o seleccionar **Cualquiera** para mostrar todos los delitos cerrados.
Sucesos	En este cuadro de lista, puede especificar un valor de recuento de sucesos y luego seleccionar que solamente se muestren los delitos cuyo recuento de sucesos sea igual, menor o mayor que el valor configurado.
Flujos	En este cuadro de lista, puede especificar un valor de recuento de flujos y luego seleccionar que solamente se muestren los delitos cuyo recuento de flujos sea igual, menor o mayor que el valor configurado.
Sucesos/flujos totales	En este cuadro de lista, puede especificar un valor de recuento total de sucesosy flujos y luego seleccionar que solamente se muestren los delitos cuyo recuento total de sucesosy flujos sea igual, menor o mayor que el valor configurado.
Destinos	En este cuadro de lista, puede especificar un valor de recuento de direcciones IP de destino y luego seleccionar que solamente se muestren los delitos cuyo recuento de direcciones IP de destino sea igual, menor o mayor que el valor configurado.
Grupo de origen de registro	En este cuadro de lista, puede seleccionar un grupo de origen de registro que contiene el origen de registro para el que desee buscar. El cuadro de lista **Origen de registro** muestra todos los orígenes de registro que se han asignado al grupo de origen de registro seleccionado.
Origen de registro	En este cuadro de lista, puede seleccionar el origen de registro para el que desee buscar.
Grupo de reglas	En este cuadro de lista, puede seleccionar un grupo de reglas que contiene la regla contribuyente para la que desee buscar. El cuadro de lista **Regla** muestra todas las reglas que están asignadas al grupo de reglas seleccionado.

Tabla 42. Opciones de búsqueda de las páginas Mis delitos y Todos los delitos (continuación)

Opciones	Descripción
Regla	En este cuadro de lista, puede seleccionar la regla contribuyente para la que desee buscar.
Tipo de delito	En este cuadro de lista, puede seleccionar un tipo de delito para el que desee buscar. Para obtener más información sobre las opciones del cuadro de lista **Tipo de delito**, consulte la Tabla 2.

La tabla siguiente describe las opciones disponibles en el cuadro de lista **Tipo de delito**:

Tabla 43. Opciones de tipo de delito

Tipos de delito	Descripción
Cualquiera	Esta opción busca todos los orígenes de registro.
IP de origen	Para buscar delitos con una dirección IP de origen determinada, puede seleccionar esta opción y luego escribir la dirección IP de origen para la que desee buscar.
IP de destino	Para buscar delitos con una dirección IP de destino determinada, puede seleccionar esta opción y luego escribir la dirección IP de destino para la que desee buscar.
Nombre de suceso	Para buscar delitos con un nombre de suceso determinado, puede pulsar el icono **Examinar** para abrir el Explorador de sucesos y seleccionar el nombre de suceso (QID) para el que desee buscar. Puede buscar un QID determinado utilizando una de las opciones siguientes: • Para buscar un QID por categoría, seleccione la casilla **Examinar por categoría** y seleccione la categoría de nivel alto o bajo en los cuadros de lista. • Para buscar un QID por tipo de origen de registro, seleccione la casilla **Examinar por origen de registro** y seleccione un tipo de origen de registro en el cuadro de lista **Tipo de origen de registro**. • Para buscar un QID por tipo de origen de registro, seleccione la casilla **Examinar por tipo de origen de registro** y seleccione un tipo de origen de registro en el cuadro de lista **Tipo de origen de registro**. • Para buscar un QID por nombre, seleccione la casilla **Búsqueda de QID** y escriba un nombre en el campo **QID/Nombre**.

Tabla 43. Opciones de tipo de delito (continuación)

Tipos de delito	Descripción
Nombre de usuario	Para buscar delitos con un nombre de usuario determinado, puede seleccionar esta opción y luego escribir el nombre de usuario para el que desee buscar.
Dirección MAC de origen	Para buscar delitos con una dirección MAC de origen determinada, puede seleccionar esta opción y luego escribir la dirección MAC de origen para la que desee buscar.
Dirección MAC de destino	Para buscar delitos con una dirección MAC de destino determinada, puede seleccionar esta opción y luego escribir la dirección MAC de destino para la que desee buscar.
Origen de registro	En el cuadro de lista **Grupo de origen de registro**, puede seleccionar el grupo de origen de registro que contiene el origen de registro para el que desee buscar. El cuadro de lista **Origen de registro** muestra todos los orígenes de registro que se han asignado al grupo de origen de registro seleccionado. En el cuadro de lista **Origen de registro**, seleccione el origen de registro para el que desee buscar.
Nombre de host	Para buscar delitos con un nombre de host determinado, puede seleccionar esta opción y luego escribir el nombre de host para el que desee buscar.
Puerto de origen	Para buscar delitos con un puerto de origen determinado, puede seleccionar esta opción y luego escribir el puerto de origen para el que desee buscar.
Puerto de destino	Para buscar delitos con un puerto de destino determinado, puede seleccionar esta opción y luego escribir el puerto de destino para el que desee buscar.
IPv6 de origen	Para buscar delitos con una dirección IPv6 de origen determinada, puede seleccionar esta opción y luego escribir la dirección IPv6 de origen para la que desee buscar.
IPv6 de destino	Para buscar delitos con una dirección IPv6 de destino determinada, puede seleccionar esta opción y luego escribir la dirección IPv6 de destino para la que desee buscar.
ASN de origen	Para buscar delitos con un ASN de origen determinado, puede seleccionar el ASN de origen en el cuadro de lista **ASN de origen**.
ASN de destino	Para buscar delitos con un ASN de destino determinado, puede seleccionar el ASN de destino en el cuadro de lista **ASN de destino**.

Tabla 43. Opciones de tipo de delito (continuación)

Tipos de delito	Descripción
Regla	Para buscar delitos que están asociados a una regla determinada, puede seleccionar el grupo de reglas donde reside la regla que desee buscar en el cuadro de lista **Grupo de reglas**. El cuadro de lista **Grupo de reglas** muestra todas las reglas que están asignadas al grupo de la reglas seleccionado. En el cuadro de lista **Regla**, seleccione la regla para la que desee buscar.
ID de aplicación	Para buscar delitos con un ID de aplicación, puede seleccionar el ID de aplicación en el cuadro de lista **ID de aplicación**.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
3. Elija una de las siguientes opciones:
   - Para cargar una búsqueda guardada anteriormente, vaya al Paso 4.
   - Para crear una búsqueda nueva, vaya al Paso 7.
4. Seleccione una búsqueda guardada anteriormente utilizando una de estas opciones:
   - En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desee cargar.
   - En el campo **Escriba la búsqueda guardada** o **Seleccione en la lista**, escriba el nombre de la búsqueda que desee cargar.
5. Pulse **Cargar**.
6. Opcional. Seleccione la casilla **Establecer como valor predeterminado** en el panel Editar búsqueda para establecer la búsqueda actual como búsqueda predeterminada. Si establece esta búsqueda como búsqueda predeterminada, la búsqueda se ejecutará automáticamente y mostrará resultados cada vez que acceda a la pestaña **Delitos**.
7. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desee capturar para esta búsqueda. Consulte la Tabla 1.
8. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
9. En el panel Origen de delito, especifique el tipo de delito y origen de delito que desee buscar:
   a. En el cuadro de lista, seleccione el tipo de delito para el que desee buscar.
   b. Escriba los parámetros de búsqueda. Consulte la Tabla 2.
10. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
    a. En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
    b. En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son Ascendente y Descendente.
11. Pulse **Buscar**.

Qué hacer a continuación

Guardar criterios de búsqueda en la pestaña Delito

Buscar delitos en la página Por IP de origen

Este tema describe cómo buscar delitos en la página **Por IP de origen** de la pestaña **Delito**.

Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en la página Por IP de origen:

Tabla 44. Opciones de búsqueda de la página Por IP de origen

Opciones	Descripción
Todos los delitos	Puede seleccionar esta opción para buscar todas las direcciones IP de origen sin importar el rango de tiempo.
Reciente	Puede seleccionar esta opción y, desde este cuadro de lista, seleccionar el rango de tiempo para el que desee buscar.
Intervalo específico	Para especificar un intervalo para el que buscar, puede seleccionar la opción Intervalo específico y luego seleccionar una de las opciones siguientes: • **Fecha de inicio entre**: seleccione esta casilla para buscar direcciones IP de origen asociadas a delitos que se iniciaron durante un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar. • **Último suceso/flujo entre**: seleccione esta casilla para buscar direcciones IP de origen asociadas con delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.
Buscar	El icono **Buscar** está disponible en varios paneles de la página de búsqueda. Puede pulsar **Buscar** cuando termine de configurar la búsqueda y desee ver los resultados.
IP de origen	En este campo, puede escribir la dirección IP de origen o rango de CIDR para el que desee buscar.
Magnitud	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.

Tabla 44. Opciones de búsqueda de la página Por IP de origen (continuación)

Opciones	Descripción
Riesgo de VA	En este cuadro de lista, puede especificar un valor de riesgo de VA y luego seleccionar que solamente se muestren los delitos cuyo riesgo de VA sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
Sucesos/flujos	En este cuadro de lista, puede especificar un valor de recuento de sucesos o flujos y luego seleccionar que solamente se muestren los delitos cuyo recuento de sucesos o flujos sea igual, menor o mayor que el valor configurado.
Excluir	Puede seleccionar las casillas correspondientes a los delitos que desee excluir de los resultados de búsqueda. Las opciones son: • **Delitos activos** • **Delitos ocultos** • **Delitos cerrados** • **Delitos inactivos** • **Delitos protegidos**

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Por IP de origen**.
3. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
4. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desee capturar para esta búsqueda. Consulte la Tabla 1.
5. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
6. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
   a. En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
   b. En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
7. Pulse **Buscar**.

Qué hacer a continuación

Guardar criterios de búsqueda en la pestaña Delito

Buscar delitos en la página Por IP de destino

En la página **Por IP de destino** de la pestaña **Delito**, puede buscar delitos que están agrupados por la dirección IP de destino.

Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en la página Por IP de destino:

Tabla 45. Opciones de búsqueda de la página Por IP de destino

Opciones	Descripción
Todos los delitos	Puede seleccionar esta opción para buscar todas las direcciones IP de destino sin importar el rango de tiempo.
Reciente	Puede seleccionar esta opción y, desde este cuadro de lista, seleccionar el rango de tiempo para el que desee buscar.
Intervalo específico	Para especificar un intervalo determinado para el que buscar, puede seleccionar la opción **Intervalo específico** y luego seleccionar una de las opciones siguientes: • Para especificar un intervalo determinado para el que buscar, puede seleccionar la opción **Intervalo específico** y luego seleccionar una de las opciones siguientes: • **Último suceso/flujo entre**: seleccione esta casilla para buscar direcciones IP de destino asociadas con delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar
Buscar	El icono **Buscar** está disponible en varios paneles de la página de búsqueda. Puede pulsar **Buscar** cuando termine de configurar la búsqueda y desee ver los resultados.
IP de destino	Puede escribir la dirección IP de destino o rango de CIDR para el que desee buscar.
Magnitud	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado.
Riesgo de VA	En este cuadro de lista, puede especificar un valor de riesgo de VA y luego seleccionar que solamente se muestren los delitos cuyo riesgo de VA sea igual, menor o mayor que el valor configurado. El rango de valores es 0 - 10.
Sucesos/flujos	En este cuadro de lista puede especificar una magnitud de recuento de suceso o flujo y seleccionar que solamente se visualicen los delitos cuyo recuento de sucesos o flujos sea igual, menor o mayor que el valor configurado.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Por IP de destino**.
3. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
4. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desee capturar para esta búsqueda. Consulte la Tabla 1.
5. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
6. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
   a. En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
   b. En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
7. Pulse **Buscar**.

Qué hacer a continuación

Guardar criterios de búsqueda en la pestaña Delito

Buscar delitos en la página Por red

En la página **Por red** de la pestaña **Delito**, puede buscar delitos que están agrupados por la red asociada.

Acerca de esta tarea

La tabla siguiente describe las opciones de búsqueda que puede utilizar para buscar datos de delito en la página Por Red:

Tabla 46. Opciones de búsqueda para buscar datos de delito en la página Por red

Opción	Descripción
Red	En este cuadro de lista, puede seleccionar la red para la que desee buscar.
Magnitud	En este cuadro de lista, puede especificar un valor de magnitud y luego seleccionar que solamente se muestren los delitos cuya magnitud sea igual, menor o mayor que el valor configurado.
Riesgo de VA	En este cuadro de lista, puede especificar un valor de riesgo de VA y luego seleccionar que solamente se muestren los delitos cuyo riesgo de VA sea igual, menor o mayor que el valor configurado.
Suceso/flujo	En este cuadro de lista puede especificar un recuento de suceso o flujo y seleccionar que solamente se visualicen los delitos cuyo recuento de sucesos o flujos sea igual, menor o mayor que el valor configurado.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Pulse **Por red**.

3. En el cuadro de lista **Buscar**, seleccione **Búsqueda nueva**.
4. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos. Consulte la Tabla 1.
5. En el panel Definición de columna, defina el orden en el que desee ordenar los resultados:
   a. En el primer cuadro de lista, seleccione la columna por la que desee ordenar los resultados de búsqueda.
   b. En el segundo cuadro de lista, seleccione el orden en el que desee mostrar los resultados de búsqueda. Las opciones son **Descendente** y **Ascendente**.
6. Pulse **Buscar**.

Qué hacer a continuación

Guardar criterios de búsqueda en la pestaña Delito

Guardar criterios de búsqueda en la pestaña Delitos

En la pestaña **Delitos**, puede guardar criterios de búsqueda configurados para reutilizarlos en búsquedas futuras. Los criterios de búsqueda guardados no caducan.

Procedimiento

1. Procedimiento
2. Realice una búsqueda. Consulte Búsquedas de delitos.
3. Pulse **Guardar criterios**.
4. Escriba valores para los parámetros siguientes:

Opción	**Descripción**
Parámetro	Descripción
Nombre de búsqueda	Escriba un nombre que desee asignar a los criterios de búsqueda.
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de búsqueda. Consulte Gestionar grupos de búsqueda.

Opción	Descripción
Opciones de rango de tiempo:	Elija una de las siguientes opciones: • **Todos los delitos**: seleccione esta opción para buscar todos los delitos sin importar el rango de tiempo. • **Reciente**: seleccione esta opción y, desde este cuadro de lista, seleccione el rango de tiempo para el que desee buscar. • **Intervalo específico**: para especificar un intervalo determinado para el que buscar, seleccione la opción **Intervalo específico** y luego seleccione una de las opciones siguientes: `Fecha de inicio entre: seleccione esta casilla para buscar delitos que se iniciaron durante un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar. Último suceso/flujo entre: seleccione esta casilla para buscar delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de marcar este recuadro de selección, utilice los cuadros de lista para seleccionar las fechas en las que desea buscar.Último suceso entre: marque este recuadro de selección para buscar delitos para los que el último suceso detectado se produjo dentro de un periodo de tiempo determinado. Después de seleccionar esta casilla, utilice los cuadros de lista para seleccionar las fechas para las que desee buscar.`
Establecer como valor predeterminado	Marque este recuadro de selección para establecer esta búsqueda como búsqueda predeterminada.

5. Pulse **Aceptar**.

Supresión de criterios de búsqueda

Puede suprimir criterios de búsqueda.

Acerca de esta tarea

Al suprimir una búsqueda guardada, es posible que los objetos que están asociados con la búsqueda guardada no funcionen. Los informes y las reglas de detección de anomalías son objetos de QRadar que utilizan criterios de búsqueda guardada. Después de suprimir una búsqueda guardada, edite los objetos asociados para asegurarse de que siguen funcionando.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.

- Pulse la pestaña **Actividad de red**.

2. En el recuadro de lista **Buscar**, seleccione **Nueva búsqueda** o **Editar búsqueda**.
3. En el panel Búsquedas guardadas, seleccione una búsqueda guardada en el recuadro de lista **Búsquedas guardadas disponibles**.
4. Pulse **Suprimir**.
   - Si los criterios de búsqueda guardada no están asociado con otros objetos de QRadar, se visualiza una ventana de confirmación.
   - Si los criterios de búsqueda guardada están asociado con otros objetos, se visualiza la ventana Suprimir búsqueda guardada. La ventana lista objetos que están asociados con la búsqueda guardada que desea suprimir. Tome nota de los objetos asociados.
5. Pulse **Aceptar**.
6. Elija una de las siguientes opciones:
   - Pulse **Aceptar** para continuar.
   - Pulse **Cancelar** para cerrar la ventana Suprimir búsqueda guardada.

Qué hacer a continuación

Si los criterios de búsqueda guardada estaban asociados con otros objetos de QRadar, acceda a los objetos asociados que ha anotado y edite los objetos para eliminar o sustituir la asociación con la búsqueda guardada suprimida.

Utilización de una sub-búsqueda para refinar los resultados de búsqueda

Puede utilizar una sub-búsqueda para buscar en un conjunto de resultados de búsqueda completada. La sub-búsqueda se utiliza para refinar los resultados de búsqueda, sin buscar de nuevo en la base de datos.

Antes de empezar

Al definir una búsqueda que desea utilizar como base para realizar una sub-búsqueda, asegúrese de que la opción Tiempo real (modalidad continua) está inhabilitada y la búsqueda no se ha agrupado.

Acerca de esta tarea

Esta característica no está disponible para búsquedas agrupados, búsquedas en curso o en modalidad continua.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. Realice una búsqueda.
3. Cuando la búsqueda se haya completado, añada otro filtro:
   a. Pulse **Añadir filtro**.
   b. En el primer recuadro de lista, seleccione un parámetro que desee buscar.
   c. En el segundo recuadro de lista, seleccione el modificador que desea utilizar para la búsqueda. La lista de modificadores que están disponibles depende del atributo que se ha seleccionado en la primera lista.

d. En el campo de entrada, escriba información específica que esté relacionada con la búsqueda.
e. Pulse **Añadir filtro**.

Resultados

El panel Filtros originales especifica los filtros originales que se aplican a la búsqueda de base. El panel Filtros actuales especifica los filtros que se aplican a la sub-búsqueda. Puede borrar filtros de sub-búsqueda sin reiniciar la búsqueda de base. Pulse el enlace **Borrar filtro** junto al filtro que desea borrar. Si borra un filtro en el panel Filtros originales, se reinicia la búsqueda de base.

Si suprime los criterios de búsqueda de base para los criterios de sub-búsqueda guardados, seguirá teniendo acceso a los criterios de sub-búsqueda guardados. Si añade un filtro, la sub-búsqueda busca en la base de datos entera porque la función de búsqueda ya no basa la búsqueda en un conjunto de datos buscado previamente.

Qué hacer a continuación

Guardar criterios de búsqueda

Gestión de resultados de búsqueda

Puede iniciar varias búsquedas y, a continuación, ir a otras pestañas para realizar otras tareas mientras las búsquedas se completan en segundo plano.

Puede configurar una búsqueda para que, al finalizarse, envíe una notificación por correo electrónico.

En cualquier momento mientras una búsqueda está en curso, puede volver a la pestaña **Actividad de registro** o la pestaña **Actividad de red** para ver resultados de búsqueda parciales o completos.

Cancelación de una búsqueda

Mientras una búsqueda está en cola o en curso, puede cancelar la búsqueda en la página Gestionar resultados de búsqueda.

Acerca de esta tarea

Si la búsqueda está en curso cuando se cancela, se mantienen los resultados que se han acumulado hasta que la cancelación.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.
3. Seleccione el resultado de búsqueda en cola o en curso que desea cancelar.
4. Pulse **Cancelar**.
5. Pulse **Sí**.

Supresión de una búsqueda

Si un resultado de búsqueda ya no es necesario, puede suprimir el resultado de búsqueda de la página Gestionar resultados de búsqueda.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. En el menú **Buscar**, seleccione **Gestionar resultados de búsqueda**.
3. Seleccione el resultado de búsqueda que desea suprimir.
4. Pulse **Suprimir**.
5. Pulse **Sí**.

Gestión de grupos de búsqueda

Utilizando la ventana Grupos de búsqueda, puede crear y gestionar grupos de búsqueda de sucesos, flujos y delitos.

Estos grupos le permiten localizar fácilmente criterios de búsqueda guardados en las pestañas**Actividad de registro**, **Actividad de red** y **Delitos** y en el asistente de informes.

Visualización de grupos de búsqueda

Está disponible un conjunto predeterminado de grupos y subgrupos.

Acerca de esta tarea

Puede ver grupos de búsqueda en las ventanas Grupos de búsqueda de sucesos, Grupos de búsqueda de flujos o Grupos de búsqueda de delitos.

Todas las búsquedas guardadas que no se asignan a un grupo están en el grupo **Otros**.

Las ventanas Grupos de búsqueda de sucesos, Grupos de búsqueda de flujos y Grupos de búsqueda de delitos muestran los parámetros siguientes para cada grupo.

Tabla 47. Parámetros de ventanas de grupos de búsqueda

Parámetro	Descripción
Nombre	Especifica el nombre del grupo de búsqueda.
Usuario	Especifica el nombre del usuario que ha creado el grupo de búsqueda.
Descripción	Especifica la descripción del grupo de búsqueda.
Fecha de modificación	Especifica la fecha en que se ha modificado el grupo de búsqueda.

Las barras de herramienta de las ventanas Grupos de búsqueda de sucesos, Grupos de búsqueda de flujos y Grupos de búsqueda de delitos proporcionan las funciones siguientes.

Tabla 48. Funciones de barra de herramientas de ventanas de grupos de búsqueda

Función	Descripción
Grupo nuevo	Para crear un nuevo grupo de búsqueda, puede pulsar **Grupo nuevo**. Consulte Creación de un grupo de búsqueda nuevo.
Editar	Para editar un grupo de búsqueda existente, puede pulsar en **Editar**. Consulte Edición de un grupo de búsqueda.
Copiar	Para copiar una búsqueda guardada en otro grupo de búsqueda, puede pulsar en **Copiar**. Consulte Copia de una búsqueda guardada en otro grupo.
Eliminar	Para eliminar un grupo de búsqueda o una búsqueda guardada de un grupo de búsqueda, seleccione el elemento que desea eliminar y luego pulse **Eliminar**. Consulte Eliminación de un grupo o una búsqueda guardada de un grupo.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. **Seleccionar búsqueda** >**Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Vea los grupos de búsqueda.

Creación de un grupo de búsqueda nuevo

Puede crear un grupo de búsqueda nuevo.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. **Seleccionar búsqueda Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione la carpeta para el grupo donde desea crear el nuevo grupo.
5. Pulse **Grupo nuevo**.
6. En el campo **Nombre**, escriba un nombre exclusivo para el nuevo grupo.
7. Opcional. En el campo **Descripción**, escriba una descripción.
8. Pulse **Aceptar**.

Edición de un grupo de búsqueda

Puede editar los campos **Nombre** y **Descripción** de un grupo de búsqueda.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.

2. Seleccione **Buscar** > **Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione el grupo que desea editar.
5. Pulse **Editar**.
6. Edite los parámetros:
   - Escriba un nombre nuevo en el campo **Nombre**.
   - Escriba una nueva descripción en el campo **Descripción**.
7. Pulse **Aceptar**.

Copia de una búsqueda guardada en otro grupo

Puede copiar una búsqueda guardada en uno o varios grupos.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. Seleccione **Buscar** > **Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Seleccione la búsqueda guardada que desea copiar.
5. Pulse **Copiar**.
6. En la ventana Grupos de elementos, marque el recuadro de selección para el grupo en el que desea copiar la búsqueda guardada.
7. Pulse **Asignar grupos**.

Eliminación de un grupo o una búsqueda guardada de un grupo

Puede utilizar el icono **Eliminar** para eliminar una búsqueda de un grupo o eliminar un grupo de búsqueda.

Acerca de esta tarea

Cuando se elimina una búsqueda guardada de un grupo, la búsqueda guardada no se suprime del sistema. La búsqueda guardada se elimina del grupo y se mueve automáticamente al grupo **Otros**.

No puede eliminar los grupos siguientes del sistema:

- Grupos de búsqueda de sucesos
- Grupos de búsqueda de flujos
- Grupos de búsqueda de delitos
- Otros

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. Seleccione **Buscar** > **Editar búsqueda**.
3. Pulse **Gestionar grupos**.
4. Elija una de las siguientes opciones:

- Seleccione la búsqueda guardada que desea eliminar del grupo.
- Seleccione el grupo que desea eliminar.

5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Capítulo 10. Propiedades de suceso y flujo personalizadas

Utilice Propiedades de suceso y de flujo personalizadas para buscar, ver y informar sobre la información contenida en archivos de registro que QRadar generalmente no normaliza y visualiza.

Puede crear propiedades de suceso y flujo personalizadas desde varias ubicaciones en la pestaña **Actividad de registro** o la pestaña **Actividad de red**:

- En la pestaña **Actividad de registro**, haga una doble pulsación en un suceso y seleccione **Extraer propiedad**.
- En la pestaña **Actividad de red**, haga una doble pulsación en un flujo y seleccione **Extraer propiedad**.
- Puede crear o editar una propiedad de suceso o de flujopersonalizada desde la página Buscar. Cuando crea una propiedad personalizada en la página Buscar, la propiedad no deriva de ningún suceso ni flujo determinado; por lo tanto, la ventana Propiedades de suceso personalizadas no se llena de antemano. Puede copiar y pegar información de carga útil procedente de otro origen.

Permisos necesarios

Crear propiedades personalizadas si tiene el permiso correcto.

Debe tener el permiso de Propiedades de suceso definidas por el usuario o de Propiedades de flujo definidas por el usuario.

Si tiene permisos administrativos, también puede crear y modificar las propiedades personalizadas de la pestaña Admin.

Pulse **Admin** > **Orígenes de datos** > **Propiedades de sucesos personalizadas** > o **Admin** > **Orígenes de datos** > **Propiedades de flujos personalizadas**.

Consulte con el administrador para asegurarse de que tiene los permisos correctos.

Para obtener más información, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Tipos de propiedad personalizada

Puede crear un tipo de propiedad personalizada.

Cuando se crea una propiedad personalizada, puede optar por crear una expresión regular o un tipo de propiedad calculado.

Utilizando sentencias de expresión regular (Regex), puede extraer datos no normalizados de cargas útiles de sucesos o flujos.

Por ejemplo, un informe se crea para informar a todos los usuarios que realizan cambios de permiso de usuario en un servidor Oracle. Se informa de una lista de usuarios y del número de veces que realizan un cambio en el permiso de otra cuenta. Sin embargo, normalmente el permiso o la cuenta de usuario real que se ha cambiado no se puede visualizar. Puede crear una propiedad personalizada para extraer esta información de los registros y, a continuación, utilizar la propiedad en

© Copyright IBM Corp. 2012, 2015

las búsquedas y los informes. El uso de esta característica requiere conocimientos avanzados de expresiones regulares (regex).

La expresión regular define el campo que desea que se convierta en la propiedad personalizada. Después de entrar una sentencia de expresión regular, puede validarla para la carga útil. Cuando defina patrones de expresión regular personalizados, respete las reglas de expresión regular definidas por el lenguaje de programación Java.

Para obtener más información, puede consultar las guías de aprendizaje de expresión regular disponibles en la web. Una propiedad personalizada puede asociarse con varias expresiones regulares.

Cuando se analiza un suceso o flujo, se prueba cada patrón de expresión regular en el suceso o flujo hasta que un patrón de expresión regular coincide con la carga útil. El primer patrón de expresión regular que coincide con la carga útil de suceso o flujo determina los datos que se deben extraer.

Utilizando propiedades personalizadas basadas en cálculo, puede realizar cálculos en las propiedades de suceso numérico o flujo existentes para producir una propiedad calculada.

Por ejemplo, puede crear una propiedad que visualice un porcentaje dividiendo una propiedad numérica por otra propiedad numérica.

Creación de una propiedad personalizada basada en expresión regular

Puede crear una propiedad personalizada basada en expresión regular para comparar cargas útiles de sucesos o flujos con una expresión regular.

Acerca de esta tarea

Cuando se configura una propiedad personalizada basada en expresión regular, la ventana Propiedad de suceso personalizada o la ventana Propiedad de flujo personalizada proporcionan parámetros. La tabla siguiente proporciona información de referencia para algunos parámetros.

Tabla 49. Parámetros de ventana Propiedades de sucesos personalizadas (expresión regular)

Parámetro	Descripción
Campo de prueba	
Propiedad nueva	El nombre de propiedad nueva no puede ser el nombre de una propiedad normalizada, por ejemplo `nombre de usuario`, `IP de origen` o `IP de destino`.
Optimizar el análisis de reglas, informes y búsquedas	Analiza y almacena la propiedad la primera vez que se recibe el suceso o flujo. Al marcar el recuadro de selección, la propiedad no necesita más análisis para el informe, la búsqueda y la prueba de regla. Si se elimina la marca de este recuadro de selección, la propiedad se analiza cada vez que se aplica un informe, una búsqueda o una prueba de regla.

Tabla 49. Parámetros de ventana Propiedades de sucesos personalizadas (expresión regular) (continuación)

Parámetro	Descripción
Origen de registro	Si se asocian varios orígenes de registro con este suceso, este campo especifica el término Múltiple y el número de orígenes de registro.
RegEx	La expresión regular que desea utilizar para extraer los datos de la carga útil. Las expresiones regulares son sensibles a las mayúsculas y minúsculas. A continuación, se muestran expresiones regulares de ejemplo: • Correo electrónico: `(.+@[^\.].*\.[a-z]{2,}$)` • URL: `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • Nombre de dominio: `(http[s]?://(.+?)["/?:])` • Número de coma flotante: `([-+]?\d*\.?\d*$)` • Entero: `([-+]?\d*$)` • Dirección IP: `(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` Los grupos de capturas deben estar entre paréntesis.
Grupo de capturas	Los grupos de capturas tratan varios caracteres como una sola unidad. En un grupo de capturas, los caracteres se agrupan en un conjunto de paréntesis.
Habilitado	Si quita la marca del recuadro de selección, esta propiedad personalizada no se visualiza en los filtros de búsqueda o las listas de columna y la propiedad no se analiza desde las cargas útiles.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. Si está viendo sucesos o flujos en modalidad continua, pulse el icono **Pausa** para poner en pausa la modalidad continua.
3. Efectúe una doble pulsación en el suceso o flujo en el que desea basar la propiedad personalizada.
4. Efectúe una doble pulsación en el suceso en el que desea basar la propiedad personalizada
5. Pulse **Extraer propiedad**.
6. En el panel **Selección de tipo de propiedad**, seleccione la opción **Basado en expresión regular**.
7. Configure los parámetros de propiedad personalizada.

8. Pulse **Probar** para probar la expresión regular en la carga útil.
9. Pulse **Guardar**.

Resultados

La propiedad personalizada se visualiza como una opción en la lista de columnas disponibles de la página de búsqueda. Para incluir una propiedad personalizada en una lista de sucesos o flujos, debe seleccionar la propiedad personalizada en la lista de columnas disponibles cuando cree una búsqueda.

Conceptos relacionados:

"Ejemplos de cadenas de búsqueda de AQL" en la página 177
Utilice Ariel Query Language (AQL) para recuperar campos determinados de los sucesos, flujos y tablas simarc contenidos en la base de datos Ariel.

Creación de una propiedad personalizada basada en el cálculo

Puede crear una propiedad de cliente basada en cálculo para comparar las cargas útiles con una expresión regular.

Acerca de esta tarea

Cuando configure una propiedad personalizada basada en cálculo, en la ventana Propiedad de suceso personalizada o en la ventana Propiedad de flujo personalizada se proporcionan los parámetros siguientes:

Tabla 50. Parámetros de ventana de definición de propiedad personalizada (cálculo)

Parámetro	Descripción
Definición de propiedad	
Nombre de propiedad	Escriba un nombre exclusivo para esta propiedad personalizada. El nuevo nombre de propiedad no puede ser el nombre de una propiedad normalizada, por ejemplo Nombre de usuario, IP de origen o IP de destino.
Descripción	Escriba una descripción de esta propiedad personalizada.
Definición de cálculo de propiedad	
Propiedad 1	En el recuadro de lista, seleccione la primera propiedad que desee utilizar en el cálculo. Las opciones incluyen todas las propiedades personalizadas numéricas y normalizadas numéricas. También puede especificar un valor numérico específico. En el recuadro de lista **Propiedad 1**, seleccione la opción **Definido por el usuario**. Se visualiza el parámetro **Propiedad numérica**. Escriba un valor numérico específico.

Tabla 50. Parámetros de ventana de definición de propiedad personalizada (cálculo) (continuación)

Parámetro	Descripción
Operador	En el recuadro de lista, seleccione el operador que desea aplicar a las propiedades seleccionadas en el cálculo. Las opciones incluyen: • Sumar • Restar • Multiplicar • Dividir
Propiedad 2	En el recuadro de lista, seleccione la segunda propiedad que desee utilizar en el cálculo. Las opciones incluyen todas las propiedades personalizadas numéricas y normalizadas numéricas. También puede especificar un valor numérico específico. En el recuadro de lista **Propiedad 1**, seleccione la opción **Definido por el usuario**. Se visualiza el parámetro **Propiedad numérica**. Escriba un valor numérico específico.
Habilitado	Seleccione este recuadro de selección para habilitar esta propiedad personalizada. Si quita la marca del recuadro de selección, esta propiedad personalizada no se visualiza en los filtros de búsqueda de sucesos o flujos o las listas de columna y la propiedad de suceso o flujo no se analiza en las cargas útiles.

Procedimiento

1. Elija una de las opciones siguientes: Pulse la pestaña **Actividad de registro**.
2. Opcional. Si está viendo sucesos o flujos en modalidad continua, pulse el icono **Pausa** para poner en pausa la modalidad continua.
3. Efectúe una doble pulsación en el suceso o flujo en el que desea basar la propiedad personalizada.
4. Pulse **Extraer propiedad**.
5. En el panel Selección de tipo de propiedad, seleccione la opción **Basado en cálculo**.
6. Configure los parámetros de propiedad personalizada.
7. Pulse **Probar** para probar la expresión regular en la carga útil.
8. Pulse **Guardar**.

Resultados

Ahora la propiedad personalizada se visualiza como una opción en la lista de columnas disponibles en la página de búsqueda. Para incluir una propiedad personalizada en una lista de sucesos o flujos, debe seleccionar la propiedad

personalizada en la lista de columnas disponibles cuando cree una búsqueda.

Modificación de una propiedad personalizada

Puede modificar una propiedad personalizada.

Acerca de esta tarea

Puede utilizar la ventana Propiedades de sucesos personalizadas o Propiedades de flujos personalizadas para modificar una propiedad personalizada.

Las propiedades personalizadas se describen en la tabla siguiente.

Tabla 51. Columnas de ventana de propiedades personalizadas

Columna	Descripción
Nombre de propiedad	Especifica un nombre exclusivo para esta propiedad personalizada.
Tipo	Especifica el tipo para esta propiedad personalizada.
Descripción de propiedad	Especifica una descripción para esta propiedad personalizada.
Tipo de origen de registro	Especifica el nombre del tipo de origen de registro al que se aplica esta propiedad personalizada. Esta columna sólo se visualiza en la ventana Propiedades de sucesos personalizadas.
Origen de registro	Especifica el origen de registro al que se aplica esta propiedad personalizada. Si hay varios orígenes de registro que están asociados con este suceso o flujo, este campo especifica el término Múltiple y el número de orígenes de registro. Esta columna sólo se visualiza en la ventana Propiedades de sucesos personalizadas.
Expresión	Especifica la expresión para esta propiedad personalizada. La expresión depende del tipo de propiedad personalizada: Para una propiedad personalizada basada en expresión regular, este parámetro especifica la expresión regular que desea utilizar para extraer los datos de la carga útil. Para una propiedad personalizada basada en cálculo, este parámetro especifica el cálculo que desea utilizar para crear el valor de propiedad personalizada.
Nombre de usuario	Especifica el nombre del usuario que ha creado esta propiedad personalizada.

Tabla 51. Columnas de ventana de propiedades personalizadas (continuación)

Columna	Descripción
Habilitado	Especifica si esta propiedad personalizada está habilitada. Este campo especifica Verdadero o Falso.
Fecha de creación	Especifica la fecha en que se ha creado esta propiedad personalizada.
Fecha de modificación	Especifica la hora en que se ha modificado por última vez esta propiedad personalizada.

En la barra de herramientas Propiedades de sucesos personalizadas y Propiedades de flujos personalizadas se proporcionan las funciones siguientes:

Tabla 52. Opciones de barra de herramientas de propiedades personalizadas

Opción	Descripción
Añadir	Pulse **Añadir** para añadir una nueva propiedad personalizada.
Editar	Pulse **Editar** para editar la propiedad personalizada seleccionada.
Copiar	Pulse **Copiar** para copiar propiedades personalizadas seleccionadas.
Suprimir	Pulse **Suprimir** para suprimir propiedades personalizadas seleccionadas.
Habilitar/Inhabilitar	Pulse **Habilitar/Inhabilitar** para habilitar o inhabilitar las propiedades personalizadas seleccionadas para el análisis y la visualización en los filtros de búsqueda o las listas de columna.

Procedimiento

1. Elija una de las opciones siguientes:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
3. Pulse **Gestionar propiedades personalizadas**.
4. Seleccione la propiedad personalizada que desea editar y pulse **Editar**.
5. Edite los parámetros necesarios.
6. Opcional. Si ha editado la expresión regular, pulse **Probar** para probar la expresión regular en la carga útil.
7. Pulse **Guardar**.

Copia de una propiedad personalizada

Para crear una nueva propiedad personalizada que esté basada en una propiedad personalizada existente, puede copiar la propiedad personalizada existente y, a continuación, modificar los parámetros.

Procedimiento

1. Elija una de las opciones siguientes:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
3. Pulse **Gestionar propiedades personalizadas**.
4. Seleccione la propiedad personalizada que desea copiar y pulse **Copiar**.
5. Edite los parámetros necesarios.
6. Opcional. Si ha editado la expresión regular, pulse **Probar** para probar la expresión regular en la carga útil.
7. Pulse **Guardar**.

Supresión de una propiedad personalizada

Puede suprimir cualquier propiedad personalizada, a condición que la propiedad personalizada no esté asociada con otra propiedad personalizada.

Procedimiento

1. Elija una de las opciones siguientes:
   - Pulse la pestaña **Actividad de registro**.
   - Pulse la pestaña **Actividad de red**.
2. Pulse la pestaña **Actividad de registro**.
3. En el recuadro de lista **Buscar**, seleccione **Editar búsqueda**.
4. Pulse **Gestionar propiedades personalizadas**.
5. Seleccione la propiedad personalizada que desea suprimir y pulse **Suprimir**.
6. Pulse **Sí**.

Capítulo 11. Gestión de reglas

Desde la pestaña **Actividad de registro**, la pestaña **Actividad de red** y la pestaña **Delitos** puede ver y mantener reglas.

Este tema es aplicable a los usuarios que tienen permisos de rol de usuario para **Ver reglas personalizadas** o **Mantener reglas personalizadas**.

Consideraciones sobre el permiso de regla

Puede ver y gestionar reglas para las áreas de la red a la que puede acceder si tiene los permisos de rol de usuario Ver reglas personalizadas y Mantener reglas personalizadas.

Para crear reglas de detección de anomalía, debe tener el permiso **Mantener reglas personalizadas** adecuado para la pestaña en la que desea crear la regla. Por ejemplo, para poder crear una regla de detección de anomalía en la pestaña Actividad de registro, debe tener el permiso **Actividad de registro** > **Mantener reglas personalizadas**.

Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Visión general de las reglas

Las reglas realizan pruebas sobre sucesos, flujos o delitos, y generan una respuesta si se cumplen todas las condiciones de una prueba.

Las pruebas de una regla pueden también hacer referencia a otros componentes y reglas. No es necesario crear las reglas en un orden determinado, pues el sistema comprueba si existen dependencias cada vez que se añade, edita o suprime una regla. Si se intenta suprimir o inhabilitar una regla a la que hace referencia otra regla, se muestra un aviso y no se emprende ninguna acción.

Para obtener una lista completa de reglas predeterminadas, consulte el manual *Guía del administrador de IBM Security QRadar SIEM*.

Categorías de reglas

Existen dos categorías de reglas: las reglas personalizadas y las reglas de anomalías.

Las reglas personalizadas realizan pruebas sobre sucesos, flujos y delitos para detectar actividad inusual en la red.

La reglas de detección de anomalías realizan pruebas sobre los resultados de búsquedas guardadas de flujos o de sucesos para detectar patrones de tráfico inusuales en la red.

La reglas de detección de anomalías realizan pruebas sobre los resultados de búsquedas guardadas de flujos o de sucesos para detectar patrones de tráfico inusuales en la red. Esta categoría de reglas incluye los tipos de reglas siguientes: de anomalía, de umbral y de comportamiento.

© Copyright IBM Corp. 2012, 2015

Una regla de anomalía realiza pruebas sobre el tráfico de sucesos y de flujospara detectar tráfico nuevo o desconocido, que es tráfico que cesa repentinamente, o un cambio porcentual en la cantidad de tiempo que un objeto está activo. Por ejemplo, puede crear una regla de anomalía para comparar el volumen promedio de tráfico existente durante los últimos 5 minutos con el volumen promedio de tráfico existente durante la última hora. Si se produce un cambio de más del 40%, la regla genera un respuesta.

Una regla de umbral realiza pruebas sobre el tráfico de sucesos y de flujospara detectar actividad que es menor, igual o mayor que un valor umbral configurado, o que está dentro de un rango especificado. Los umbrales pueden estar basados en cualquier dato recogido. Por ejemplo, puede crear una regla de umbral que especifique que no más de 220 clientes pueden iniciar una sesión en el servidor entre las 08:00 y las 17:00. La regla de umbral genera una alerta cuando el cliente 221 intenta iniciar una sesión.

Una regla de comportamiento realiza pruebas sobre el tráfico de sucesos y de flujos para detectar cambios de volumen en el comportamiento que se produce en patrones estacionales regulares. Por ejemplo, si un servidor de correo normalmente se comunica con 100 hosts por segundo en la mitad de la noche y después súbitamente inicia la comunicación con 1.000 hosts por segundo, una regla de comportamiento genera una alerta.

Tipos de reglas

Existen cuatro tipos diferentes de reglas: reglas de suceso, flujo, comunes y de delito.

Regla de suceso

Una regla de suceso realiza pruebas sobre sucesos a medida que son procesados en tiempo real por el procesador de sucesos. Puede crear una regla de suceso para detectar un suceso individual (dentro de propiedades determinadas) o secuencias de sucesos. Por ejemplo, si desea supervisar la red para detectar intentos fallidos de inicio de sesión, el acceso a varios hosts o un suceso de reconocimiento seguido de una explotación, puede crear una regla de suceso. Es habitual que las reglas de suceso creen delitos como respuesta.

Regla de flujo

Una regla de flujo realiza pruebas sobre flujos a medida que son procesados en tiempo real por QFlow Collector. Puede crear una regla de flujo para detectar un flujo individual (dentro de propiedades determinadas) o secuencias de flujos. Es habitual que las reglas de flujo creen delitos como respuesta.

Regla común

Una regla común realiza pruebas sobre campos que son comunes a registros de suceso y de flujo. Por ejemplo, puede crear una regla común para detectar sucesos y flujos que tienen una dirección IP de origen determinada. Es habitual que las reglas comunes creen delitos como respuesta.

Regla de delito

Una regla de delito procesa delitos sólo cuando se realizan cambios en el delito, por ejemplo, cuando se añaden nuevos sucesos o el sistema ha planificado la

reevaluación del delito. Es habitual que las reglas de delito envíen una notificación de correo electrónico como respuesta.

Condiciones de regla

Cada regla puede contener funciones, componentes básicos o pruebas.

Con las funciones, puede utilizar componentes básicos y otras reglas para crear una función de varios sucesos, varios flujos o varios delitos. Puede conectar reglas utilizando funciones que soportan operadores booleanos, por ejemplo OR y AND. Por ejemplo, si desea conectar reglas de suceso, puede utilizar la función cuando un suceso coincide con alguna | todas las reglas siguientes.

Un componente básico es una regla sin una respuesta y se utiliza como una variable común en varias reglas o crear reglas complejas o lógica que desea utilizar en otras reglas. Puede guardar un grupo de pruebas como componentes básicos para utilizarlas con otras funciones. Los componentes básicos le permitirán reutilizar pruebas de regla específicas en otras reglas. Por ejemplo, puede guardar un componente básico que incluye las direcciones IP de todos los servidores de correo en la red y, a continuación, utilizar ese componente básico para excluir esos servidores de correo de otra regla. Los componentes básicos predeterminados se proporcionan como directrices, que deben revisarse y editarse en función de las necesidades de la red.

Nota: De forma predeterminada, los componentes básicos no se cargan. Defina una regla para crear componentes básicos.

Para obtener una lista completa de componentes básicos, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Puede ejecutar pruebas en la propiedad de un suceso, flujo o delito, por ejemplo dirección IP de origen, gravedad de suceso o análisis de ritmo.

Respuestas de regla

Cuando se cumplen las condiciones de regla, una regla puede generar una o más respuestas.

Las reglas pueden generar una o varias de las respuestas siguientes:

- Crear un delito.
- Enviar un correo electrónico.
- Generar notificaciones de sistema en la característica de panel de control.
- Añadir datos a conjuntos de referencia.
- Añadir datos a colecciones de datos de referencia.
- Generar una respuesta a un sistema externo.
- Añadir datos a recopilaciones de datos de referencia que se pueden utilizar en pruebas de regla.
- Ejecutar un script de acción personalizada en respuesta a un suceso.

Tipos de recopilación de datos de referencia

Antes de poder configurar una respuesta de regla para enviar datos a una recopilación de datos de referencia, debe crear la recopilación de datos de referencia utilizando la interfaz de línea de mandatos (CLI). QRadar soporta los siguientes tipos de recopilación de datos:

Conjunto de referencia
Un conjunto de elementos, por ejemplo una lista de direcciones IP o nombres de usuario, que se derivan de los sucesos y flujos que se producen en la red.

Correlación de referencia
Los datos se almacenan en registros que correlacionan una clave con un valor. Por ejemplo, para correlacionar la actividad de usuario en la red, puede crear una correlación de referencia que utiliza el parámetro **Nombre de usuario** como clave y el **ID global** del usuario como valor.

Correlación de referencia de conjuntos
Los datos se almacenan en registros que correlacionan una clave con varios valores. Por ejemplo, para probar el acceso autorizado a una patente, utilice una propiedad de suceso personalizada para **ID de patente** como clave y el parámetro **Nombre de usuario** como valor. Utilice una correlación de conjuntos para llenar una lista de usuarios autorizados.

Correlación de referencia de correlaciones
Los datos se almacenan en registros que correlacionan una clave a otra clave, que a continuación se correlaciona con un valor único. Por ejemplo, para probar las violaciones de ancho de banda de red, puede crear una correlación de correlaciones. Utilice el parámetro **IP de origen** como la primera clave, el parámetro **Aplicación** como segunda clave y el parámetro **Bytes totales** como valor.

Tabla de referencia
En una tabla de referencia, los datos se almacenan en una tabla que correlaciona una clave con otra clave, que a continuación se correlaciona con un valor único. La segunda clave tiene un tipo asignado. Esta correlación es similar a una tabla de base de datos donde cada columna de la tabla está asociada con un tipo. Por ejemplo, puede crear una tabla de referencia que almacena el parámetro **Nombre de usuario** como primera clave y tiene varias claves secundarias que tienen un tipo asignado definido por el usuario como **Tipo de IP** con el parámetro **IP de origen** o **Puerto de origen** como valor. Puede configurar una respuesta de regla para añadir una o más claves definidas en la tabla. También puede añadir valores personalizados a la respuesta de regla. El valor personalizado debe ser válido para el tipo de la clave secundaria.

Nota: Para obtener información sobre los conjuntos de referencia y las recopilaciones de datos de referencia, consulte la *Guía de administración* correspondiente al producto.

Visualización de reglas

Puede ver los detalles de una regla, incluyendo las pruebas, los componentes básicos y las respuestas.

Antes de empezar

En función de los permisos de rol de usuario, puede acceder a la página de reglas de la pestaña **Delitos**, **Actividad de registro**o **Actividad de red**.

Para obtener más información sobre los permisos de rol de usuario, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Acerca de esta tarea

La página Reglas visualiza una lista de reglas con sus parámetros asociados. Para localizar la regla que desea abrir y cuyos detalles desea ver, puede utilizar el recuadro de lista Grupo o el campo **Buscar en reglas** en la barra de herramientas.

Procedimiento

1. Elija una de las siguientes opciones:
   - Pulse la pestaña **Delitos** y, a continuación, pulse **Reglas** en el menú de navegación.
   - Pulse la pestaña **Actividad de registro** y, a continuación, seleccione **Reglas** en el recuadro de lista **Reglas** de la barra de herramientas.
   - Pulse la pestaña **Actividad de red** y, a continuación, seleccione **Reglas** en el recuadro de lista **Reglas** de la barra de herramientas.
2. En el recuadro de lista **Visualizar**, seleccione **Reglas**.
3. Efectúe una doble pulsación en la regla que desea ver.
4. Revise los detalles de regla.

Resultados

Si tiene el permiso **Ver reglas personalizadas**, pero no tiene el permiso **Mantener reglas personalizadas**, se visualiza la página **Resumen de regla** y la regla no se puede editar. Si tiene el permiso **Mantener reglas personalizadas**, se visualiza la página **Editor de pila de prueba de regla**. Puede revisar y editar los detalles de regla.

Creación de una regla

Las reglas evalúan los datos entrantes con condiciones de prueba de regla para generar una respuesta del sistema. Cuando las condiciones de una regla se cumplen, se pueden llevar a cabo varias acciones. Por ejemplo, puede configurar la respuesta del sistema a la regla, que puede ser la generación de delitos, el envío de correos electrónicos, el inicio de exploraciones, la adición de datos de referencia o el aumento o la disminución de valores como la gravedad.

Antes de empezar

Para crear una regla nueva, debe tener el permiso **Delitos** > **Mantener reglas personalizadas**.

Acerca de esta tarea

Cuando defina pruebas de regla, trate las reglas igual que trata las búsquedas y realice pruebas con el volumen de datos más pequeño posible. Al realizar las pruebas de esta manera, se obtiene un mejor rendimiento de las pruebas de regla y se asegura de no crear reglas costosas. Para optimizar el rendimiento, empiece con categorías amplias que restrinjan los datos que evalúa una prueba de regla. Por ejemplo, empiece con una prueba de regla para un tipo de origen de registro, una ubicación de red, un origen de flujo o un contexto (R2L, L2R, L2L) específico. Las pruebas de nivel medio que realice serán direcciones IP, tráfico de puerto u otras pruebas asociadas. Deje las pruebas de carga útil y regex como la última prueba de regla.

La mayoría de las pruebas de regla evalúan una sola condición, como por ejemplo la existencia de un elemento en una recopilación de datos de consulta o la prueba de un valor contra una propiedad de un suceso. Para comparaciones complejas, puede probar reglas de suceso construyendo una consulta de Ariel Query Language (AQL) con condiciones de cláusula WHERE. Puede utilizar todas las funciones de cláusula WHERE para escribir criterios complejos que pueden eliminar la necesidad de ejecutar numerosas pruebas individuales. Por ejemplo, utilice una clausula WHERE de AQL para comprobar si se está realizando un seguimiento del tráfico web o SSL entrante en un conjunto de referencia.

Procedimiento

1. En **Delitos**, pestañas **Actividad de registro** o **Actividad de red**, pulse **Reglas**.
2. En la lista **Acciones**, seleccione un tipo de regla.

   Cada tipo de regla se prueba contra los datos entrantes de diferentes orígenes en tiempo real. Por ejemplo, las reglas de suceso prueban datos de origen de registro entrante y las reglas de delito prueban los parámetros de un delito para desencadenar más respuestas.
3. En la página Editor de pila de prueba de regla, en el panel Regla, teclee un nombre exclusivo que desee para asignar a esta regla en el cuadro de texto **Aplicar**.
4. En el recuadro de lista, seleccione **Local** o **Global**.

   Las reglas locales envían sucesos y flujos al procesador de sucesos local para desencadenar la regla. Esta es la acción predeterminada.

   Las reglas globales envían sucesos y flujos al procesador de sucesos central, lo que puede disminuir el rendimiento de la Consola. El motor de reglas personalizadas (CRE) de la Consola hace un seguimiento de las coincidencias de suceso tal como las proporciona cada host gestionado en el despliegue. Conforme se realizan las coincidencias parciales o se deben actualizar los contadores, cada host gestionado envía una actualización al CRE en la Consola. Cuando la regla general es verdadera, la Consola desencadena la respuesta de regla.

   Para obtener más información sobre las pruebas de regla locales y globales, consulte *Guía del administrador de IBM Security QRadar SIEM*
5. En la lista **Grupo de pruebas**, seleccione una o varias pruebas que desea añadir a esta regla. El CRE evalúa las pruebas de regla en orden, línea por línea. La primera prueba se evalúa y cuando es verdadera, se evalúa la línea siguiente hasta que se alcanza la prueba final.

   Si selecciona la prueba **cuando el suceso coincide con esta consulta de filtro de AQL** para una regla de suceso nueva, especifique una consulta de cláusula WHERE de AQL en el cuadro de texto **Especifique una consulta de filtro de AQL**.

   Obtenga más información sobre la utilización de reglas para sucesos que no se detectan:

   Las pruebas de regla siguiente se pueden desencadenar individualmente pero no se actúa sobre las pruebas de regla subsiguientes de la misma pila de pruebas de reglas.

   - **cuando uno o varios de estos tipos de origen de registro no han detectado los sucesos durante este número de segundos**
   - **cuando uno o varios de estos orígenes de registro no han detectado los sucesos durante este número de segundos**

- **cuando uno o varios de estos grupos de origen de registro no han detectado los sucesos durante este número de segundos**

  Estas pruebas de regla no se ven activadas por un suceso entrante, sino que se activan cuando no se ve un suceso específico durante un intervalo de tiempo específico configurado. QRadar utiliza una *tarea observadora* que consulta periódicamente la última vez que se vio un suceso (hora de última visualización) y almacena esta hora del suceso para cada origen de registro. La regla se desencadena cuando la diferencia entre la hora de última visualización y la hora actual sobrepasa el número de segundos configurado en la regla.

6. Para exportar la regla configurada como un bloque básico a utilizar con otras reglas, pulse **Exportar como componente básico**.

   Un componente básico es un subconjunto de pruebas de regla que no tienen respuestas. Piense en los bloques básicos como un conjunto de pruebas de regla que puede utilizar dentro de otras reglas. Un ejemplo habitual es llenar los bloques básicos de BB:Definición de host con las direcciones de servidores. Los administradores pueden excluir o incluir pruebas de regla por tipos de servidor específicos, como por ejemplo servidores VPN, servidores de correo o servidores LDAP.

7. En la página Respuestas de regla, configure las respuestas que desea que genere esta regla.

   Las respuestas de regla son la acción que el dispositivo de QRadar lleva a cabo cuando todas las pruebas de regla son verdaderas. Las se respuestas de regla, como por ejemplo correos electrónicos, mensajes de syslog y sucesos de reenvío se producen para reglas locales en el procesador y para reglas globales en la Consola, donde la regla se convierte en verdadera.

Conceptos relacionados:

"Parámetros de página Rule Response" en la página 227
Configure los parámetros de la página Respuesta de regla para especificar cómo desea que IBM Security QRadar responda cuando se desencadena una regla.

Creación de una regla de detección de anomalías

Utilice el asistente de Regla de detección de anomalías para crear reglas que apliquen criterios de rango de tiempo utilizando pruebas de datos y hora.

Antes de empezar

Para crear una regla de detección de anomalías nueva, debe cumplir con los siguientes requisitos:

- Tener el permiso para Mantener reglas personalizadas.
- Realizar una búsqueda agrupada.

Las opciones de detección de anomalías se visualizan después de realizar una búsqueda agrupada y guardar los criterios de búsqueda.

Acerca de esta tarea

Debe tener el permiso de rol apropiado para poder crear una regla de detección de anomalías.

Para crear reglas de detección de anomalías en la pestaña **Actividad de registro**, debe tener el permiso de rol de **Actividad de registro Mantener reglas personalizadas**.

Para crear reglas de detección de anomalías en la pestaña **Actividad de red**, debe tener el permiso de rol de **Red Mantener reglas personalizadas**.

Las reglas de detección de anomalías utilizan todos los criterios de agrupación y filtro de los criterios de búsqueda guardados en los que se basa la regla, pero no utilizan rangos de tiempo de los criterios de búsqueda.

Cuando se crea una regla de detección de anomalías, la regla se rellena con una pila de prueba predeterminada. Puede editar las pruebas predeterminadas o añadir pruebas a la pila de prueba. Al menos se debe incluir una prueba de Propiedad acumulada en la pila de prueba.

De forma predeterminada, la opción **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado** está seleccionada en la página Editor de pila de prueba de regla.

Esto hace que una regla de detección de anomalías pruebe la propiedad acumulada seleccionada para cada grupo de sucesos o flujos por separado. Por ejemplo, si el valor acumulado seleccionado es **UniqueCount(sourceIP)**, la regla prueba cada dirección IP de origen exclusiva para cada grupo de sucesos o flujos.

Esta opción **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado** es dinámica. El valor **[Propiedad acumulada seleccionada]** depende de la opción que seleccione para el campo **esta prueba de propiedad acumulada** de la pila de prueba predeterminada. El valor **[grupo]** depende de las opciones de agrupación que se han especificado en los criterios de búsqueda guardados. Si se incluyen varias opciones de agrupación, es posible que el texto se trunque. Mueva el puntero del ratón sobre el texto para ver todos los grupos.

Procedimiento

1. Pulse la pestaña **Actividad de registro** o **Actividad de red**.
2. Realice una búsqueda.
3. En el menú **Reglas**, seleccione el tipo de regla que desea crear. Las opciones incluyen:
   - Añadir regla de anomalía
   - Añadir regla de umbral
   - Añadir regla conductual
4. Lea el texto de introducción del asistente de reglas. Pulse **Siguiente**. Se selecciona la regla que ha elegido anteriormente.
5. Pulse **Siguiente** para ver la página Editor de pila de prueba de regla.
6. En el campo **especifique aquí el nombre de la regla**, escriba un nombre exclusivo que desee asignar a esta regla.
7. Para añadir una prueba a una regla:
   a. Opcional. Para filtrar las opciones en el recuadro de lista Grupo de pruebas, escriba el texto por el que desea filtrar en el campo Tipo por filtrar.
   b. En el recuadro de lista Grupo de pruebas, seleccione el tipo de prueba que desea añadir a esta regla.
   c. Para cada prueba que desee añadir a la regla, seleccione el signo + junto a la prueba.

d. Opcional. Para identificar una prueba como prueba excluida, pulse "and" al principio de la prueba en el panel Regla. "and" se visualiza como "and not".

e. Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.

f. En el recuadro de diálogo, seleccione valores para la variable y, a continuación, pulse **Enviar**.

8. Opcional. Para probar las propiedades acumuladas seleccionadas totales para cada grupo de sucesos o flujos, borre la marca del recuadro de selección **Probar el valor [Propiedad acumulada seleccionada] de cada [grupo] por separado**.
9. En el panel Grupos, seleccione los recuadros de selección de los grupos a los que desea asignar esta regla. Para obtener más información, consulte Gestión de grupos de reglas.
10. En el campo **Notas**, escriba las notas que desea incluir para esta regla. Pulse **Siguiente**.
11. En la página Respuestas de regla, configure las respuestas que desea que genere esta regla. “Parámetros de página Rule Response” en la página 227
12. Pulse **Siguiente**.
13. Revise la regla configurada. Pulse **Finalizar**.

Tareas de gestión de reglas

Puede gestionar reglas personalizadas y de anomalía.

Puede habilitar e inhabilitar reglas, según sea necesario. También puede editar, copiar o suprimir una regla.

Solo puede crear reglas de detección de anomalías en las pestañas **Actividad de registro** y **Actividad de red**.

Para gestionar reglas de detección de anomalías predeterminadas y creadas anteriormente, debe utilizar la página Reglas en la pestaña **Delitos**.

Habilitación e inhabilitación de reglas

Al ajustar el sistema, puede habilitar o inhabilitar las reglas adecuadas para asegurarse de que el sistema genera delitos significativos para el entorno.

Acerca de esta tarea

Debe tener el permiso de rol **Delitos** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Visualizar** de la página **Reglas**, seleccione **Reglas**.
4. Seleccione la regla que desea habilitar o inhabilitar.
5. En el recuadro de lista **Acciones**, seleccione **Habilitar/Inhabilitar**.

Edición de una regla

Puede editar una regla para cambiar el nombre de regla, el tipo de regla, las pruebas o las respuestas.

Acerca de esta tarea

Debe tener el permiso de rol **Delitos** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Visualizar** de la página **Reglas**, seleccione **Reglas**.
4. Efectúe una doble pulsación en la regla que desea editar.
5. En el recuadro de lista **Acciones**, seleccione **Abrir**.
6. Opcional. Si desea cambiar el tipo de regla, pulse **Anterior** y seleccione un nuevo tipo de regla.
7. En la página Editor de pila de prueba de regla, edite los parámetros.
8. Pulse **Siguiente**.
9. En la página Respuesta de regla, edite los parámetros.
10. Pulse **Siguiente**.
11. Revise la regla editada. Pulse **Finalizar**.

Copia de una regla

Puede copiar una regla existente, entrar un nombre nuevo para la regla y, a continuación, personalizar los parámetros en la nueva regla según sea necesario.

Acerca de esta tarea

Debe tener el permiso de rol **Delitos** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Visualizar**, seleccione **Reglas**.
4. Seleccione la regla que desea duplicar.
5. En el recuadro de lista **Acciones**, seleccione **Duplicar**.
6. En el campo Escriba un nombre para la regla copiada:, escriba un nombre para la regla nueva. Pulse **Aceptar**.

Supresión de una regla

Puede suprimir una regla del sistema.

Acerca de esta tarea

Debe tener el permiso de rol **Delitos** > **Mantener reglas personalizadas** para poder habilitar o inhabilitar una regla.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Visualizar**, seleccione **Reglas**.
4. Seleccione la regla que desea suprimir.
5. En el recuadro de lista **Acciones**, seleccione **Suprimir**.

Gestión de grupo de reglas

Si el usuario es administrador, puede crear, editar y suprimir grupos de reglas. La categorización de reglas y componentes básicos en grupos le permite ver las reglas y realizar su seguimiento de forma eficiente.

Por ejemplo, puede ver todas las reglas que están relacionados con la conformidad.

Al crear nuevas reglas, puede asignar la regla a un grupo existente. Para obtener información sobre la asignación de un grupo utilizando el asistente de reglas, consulte Creación de una regla personalizada o Creación de una regla de detección de anomalías.

Visualización de un grupo de reglas

En la página Reglas, puede filtrar las reglas o componentes básicos para ver sólo las reglas o componentes básicos que pertenecen a un grupo específico.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Visualizar**, seleccione si desea ver reglas o componentes básicos.
4. En el recuadro de lista **Filtro**, seleccione la categoría de grupo que desea ver.

Creación de un grupo

Aunque la página Reglas proporciona grupos de reglas predeterminados, puede crear un grupo nuevo.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Pulse **Grupos**.
4. En el árbol de navegación, seleccione el grupo bajo el que desea crear un grupo nuevo.
5. Pulse **Grupo nuevo**.
6. Escriba valores para los parámetros siguientes:
   - **Nombre**: Escriba un nombre exclusivo para asignarlo al nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Escriba una descripción que desee asignar a este grupo. La descripción puede tener un máximo 255 caracteres de longitud.
7. Pulse **Aceptar**.
8. Opcional. Para cambiar la ubicación del grupo nuevo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.

Asignación de un elemento a un grupo

Puede asignar una regla o un componente básico seleccionados a un grupo.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Seleccione la regla o el componente básico que desea asignar a un grupo.
4. En el recuadro de lista **Acciones**, seleccione **Asignar grupos**.
5. Seleccione el grupo al que desea asignar la regla o el componente básico.
6. Pulse **Asignar grupos**.
7. Cierre la ventana **Elegir grupo**.

Edición de un grupo

Puede editar un grupo para cambiar el nombre o la descripción.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Pulse **Grupos**.
4. En el árbol de navegación, seleccione el grupo que desea editar.
5. Pulse **Editar**.
6. Actualice los valores para los parámetros siguientes:
   - **Nombre**: Escriba un nombre exclusivo para asignarlo al nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Escriba una descripción que desee asignar a este grupo. La descripción puede tener un máximo 255 caracteres de longitud.
7. Pulse **Aceptar**.
8. Opcional. Para cambiar la ubicación del grupo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.

Copia de un elemento en otro grupo

Puede copiar una regla o un componente básico de un grupo a otros grupos.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Pulse **Grupos**.
4. En el árbol de navegación, seleccione la regla o el componente básico que desea copiar en otro grupo.
5. Pulse **Copiar**.
6. Marque el recuadro de selección para el grupo en el que desea copiar la regla o el componente básico.
7. Pulse **Copiar**.

Supresión de un elemento de un grupo

Puede suprimir un elemento de un grupo. Cuando suprime un elemento de un grupo, la regla o el componente básico sólo se suprime del grupo; sigue estando disponible en la página Reglas.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Pulse **Grupos**.
4. Utilizando el árbol de navegación, vaya al elemento que desea suprimir y selecciónelo.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Supresión de un grupo

Puede suprimir un grupo. Cuando se suprime un grupo, las reglas o los componentes básicos de ese grupo permanecen disponibles en la página Reglas.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. Pulse **Grupos**.
4. Utilizando el árbol de navegación, vaya al grupo que desea suprimir y selecciónelo.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Edición de componentes básicos

Puede editar cualquiera de los componentes básicos predeterminados para que coincidan con las necesidades del despliegue.

Acerca de esta tarea

Un componente básico es una pila de prueba de regla reutilizable que puede incluir como componente en otras reglas.

Por ejemplo, puede editar el componente básico BB:HostDefinition: Servidores de correo para identificar todos los servidores de correo del despliegue. A continuación, puede configurar cualquier regla para excluir los servidores de correo de las pruebas de regla.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Visualiza**, seleccione **Componentes básicos**.
4. Efectúe una doble pulsación en el componente básico que desea editar.
5. Actualice el componente básico, como sea necesario.
6. Pulse **Siguiente**.
7. Continúe con el asistente. Para obtener más información, consulte Creación de una regla personalizada.
8. Pulse **Finalizar**.

Parámetros de página Reglas

Descripción de los parámetros de la página Reglas.

La lista de reglas desplegadas proporciona la siguiente información para cada regla:

Tabla 53. Parámetros de página Reglas

Parámetro	Descripción
Nombre de regla	Visualiza el nombre de la regla.
Grupo	Visualiza el grupo al que está asignada esta regla. Para obtener más información sobre grupos, consulte Gestión de grupo de reglas.
Categoría de reglas	Visualiza la categoría de la regla. Las opciones incluyen Regla personalizada y Regla de detección de anomalías.
Tipo de regla	Visualiza el tipo de regla. Los tipos de regla incluyen: • Suceso • Flujo • Común • Delito • Anomalía • Umbral • Conductual Para obtener más información sobre los tipos de reglas, consulte Tipos de regla.
Habilitado	Indica si la regla está habilitada o inhabilitada. Para obtener más información sobre cómo habilitar e inhabilitar reglas, consulte Habilitación e inhabilitación de reglas.
Respuesta	Visualiza la respuesta de regla, si existe. Las respuestas de regla incluyen: • Asignar suceso nuevo • Correo electrónico • Notificación de registro • SNMP • Conjunto de referencia • Datos de referencia • Respuesta de IF-MAP Para obtener más información sobre las respuestas de regla, consulte Respuestas de regla.
Recuento de Sucesos/flujos	Visualiza el número de sucesos o flujos que están asociados con esta regla cuando la regla contribuye a un delito.
Recuento de delitos	Visualiza el número de delitos generados por esta regla.

Tabla 53. Parámetros de página Reglas (continuación)

Parámetro	Descripción
Origen	Visualiza si esta regla es una regla predeterminada (Sistema) o una regla personalizada (Usuario).
Fecha de creación	Especifica la fecha y hora en que se ha creado esta regla.
Fecha de modificación	Especifica la fecha y hora en que se ha modificado esta regla.

Barra de herramientas de página Reglas

Utilice barra de herramientas de la página Reglas para visualizar reglas, componentes básicos o grupos. Puede gestionar grupos de reglas y trabajar con reglas.

La barra de herramientas de página Reglas proporciona las funciones siguientes:

Tabla 54. Función de barra de herramientas de página Reglas

Función	Descripción
Visualizar	En el recuadro de lista, seleccione si desea visualizar reglas o componentes básicos en la lista de reglas.
Grupo	En el recuadro de lista, seleccione qué grupo de reglas desea que se visualice en la lista de reglas.
Grupos	Pulse **Grupos** para gestionar grupos de reglas.

Tabla 54. Función de barra de herramientas de página Reglas (continuación)

Función	Descripción
Acciones	Pulse **Acciones** y seleccione una de las opciones siguientes: • **Nueva regla de sucesos**: Seleccione esta opción para crear una regla de suceso nueva. • **Nueva regla de flujos**: Seleccione esta opción para crear una nueva regla de flujos. • **Nueva regla común**: Seleccione esta opción para crear una nueva regla común. • **Nueva regla de delito**: Seleccione esta opción para crear una nueva regla de delito. • **Habilitar/Inhabilitar**: Seleccione esta opción para habilitar o inhabilitar reglas seleccionadas. • **Duplicar**: Seleccione esta opción para copiar una regla seleccionada. • **Editar**: Seleccione esta opción para editar una regla seleccionada. • **Suprimir**: Seleccione esta opción para suprimir una regla seleccionada. • **Asignar grupos**: Seleccione esta opción para asignar reglas seleccionadas a grupos de reglas.
Revertir regla	Pulse **Revertir regla** para revertir una regla de sistema modificada al valor predeterminado. Al pulsar **Revertir regla**, se visualiza una ventana de confirmación. Al revertir una regla, las modificaciones anteriores se eliminan de forma permanente. Para revertir la regla y mantener una versión modificada, duplique la regla y utilice la opción **Revertir regla** en la regla modificada.

Tabla 54. Función de barra de herramientas de página Reglas (continuación)

Función	Descripción
Buscar en reglas	Escriba los criterios de búsqueda en el campo **Buscar en reglas** y pulse el icono **Buscar en reglas** o pulse Intro en el teclado. Todas las reglas que coinciden con los criterios de búsqueda se muestran en la lista de reglas. En los parámetros siguientes se busca una coincidencia con los criterios de búsqueda: • Nombre de regla • Regla (descripción) • Notas • Respuesta La característica Buscar en reglas intenta localizar una coincidencia de serie de texto directa. Si no se encuentra ninguna coincidencia, la característica Buscar en reglas intenta una coincidencia de expresión regular (regex).

Parámetros de página Rule Response

Configure los parámetros de la página Respuesta de regla para especificar cómo desea que IBM Security QRadar responda cuando se desencadena una regla.

Nota: Cuando construye una consulta AQL, si copia texto que contiene apóstrofos de cualquier documento y lo pega en IBM Security QRadar, la consulta no se analizará. Como solución, puede pegar el texto en QRadar y volver a teclear los apóstrofos o puede copiar y pegar el texto de IBM Knowledge Center.

La tabla siguiente proporciona los parámetros de la página Rule Response.

Tabla 55. Parámetros de página Respuesta de regla de suceso, de flujo y común

Parámetro	Descripción
Anotar suceso	Marque este recuadro de selección si desea añadir una anotación a este suceso y escriba la anotación que desea añadir al suceso.
Descartar el suceso detectado	Marque este recuadro de selección para forzar que un suceso, que normalmente se envía al componente Magistrado, se envíe a la base de datos de Ariel para la creación de informes o la realización de búsquedas. El suceso descartado se graba en el almacenamiento e ignora las pruebas de reglas. Este suceso no se visualiza en la pestaña **Delitos**.

Tabla 55. Parámetros de página Respuesta de regla de suceso, de flujo y común (continuación)

Parámetro	Descripción
Asignar suceso nuevo	Marque este recuadro de selección para asignar un suceso nuevo además del suceso o flujo original, que se procesa igual que todos los demás sucesos en el sistema. Marque este recuadro de selección para asignar un suceso nuevo además del suceso original, que se procesa igual que todos los demás sucesos del sistema. Los parámetros **Asignar suceso nuevo** se visualizan cuando se marca este recuadro de selección. De forma predeterminada, el recuadro de selección no está marcado.
Nombre de suceso	Escriba un nombre exclusivo para el suceso que desea que se visualice en la pestaña **Delitos**.
Descripción del suceso	Escriba una descripción para el suceso. La descripción se visualiza en el panel Anotaciones de los detalles de suceso.
Gravedad	En el recuadro de lista, seleccione la gravedad para el suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 0. La Gravedad se visualiza en el panel Anotación de los detalle de suceso.
Credibilidad	En el recuadro de lista, seleccione la credibilidad del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 10. La credibilidad se visualiza en el panel Anotación de los detalles de suceso.
Pertinencia	En el recuadro de lista, seleccione la pertinencia del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 10. La pertinencia se visualiza en el panel Anotación de los detalles de suceso.
Categoría de alto nivel	En el recuadro de lista, seleccione la categoría de sucesos de alto nivel que desea que esta regla utilice al procesar sucesos.
Categoría de bajo nivel	En el recuadro de lista, seleccione la categoría de sucesos de bajo nivel que desea que esta regla utilice al procesar sucesos.
Anotar este delito	Marque este recuadro de selección para añadir una anotación a este delito y escriba la anotación.
Correo electrónico	Seleccione este recuadro de selección para visualizar las opciones de correo electrónico. **Nota:** Para cambiar el valor **Entorno local del correo electrónico**, seleccione **Valores del sistema** en la pestaña **Admin**.
Especifique las direcciones de correo electrónico que se deben notificar:	Escriba la dirección de correo electrónico a la que hay que enviar una notificación si se genera esta regla. Utilice una coma para separar varias direcciones de correo electrónico.
Seleccione la plantilla de correo electrónico de suceso/flujo	Seleccione la plantilla de correo electrónico para correos electrónicos asociados a esta regla. Para obtener más información sobre las notificaciones de correo electrónico personalizadas, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Tabla 55. Parámetros de página Respuesta de regla de suceso, de flujo y común (continuación)

Parámetro	Descripción
Condición de excepción de SNMP	Este parámetro sólo se visualiza cuando los parámetros Valores de SNMP se han configurado en los valores del sistema. Marque este recuadro de selección para permitir que esta regla envíe una notificación de SNMP (condición de excepción). La salida de condición de excepción SNMP incluye la hora del sistema, el OID de condición de excepción y los datos de notificación, como los define el MIB.
Enviar a SysLog Local	Marque este recuadro de selección si desea registrar el suceso o flujo localmente. De forma predeterminada, este recuadro de selección no está marcado. **Nota:** Sólo los sucesos normalizados se pueden registrar localmente en un dispositivo. Si desea enviar datos de sucesos en bruto, debe utilizar la opción Enviar a destinos de reenvío para enviar los datos a un host de syslog remoto.
Enviar a destinos de reenvío	Marque este recuadro de selección si desea registrar el suceso o flujo en un destino de reenvío. Un destino de reenvío es un sistema de proveedor, por ejemplo SIEM, tíquets o sistemas de alerta. Al marcar este recuadro de selección, se visualiza una lista de destinos de reenvío. Marque este recuadro de selección para el destino de reenvío al que desea enviar este suceso o flujo. Para añadir, editar o suprimir un destino de reenvío, pulse el enlace **Gestionar destinos**.
Notificar	Marque este recuadro de selección si desea que, los sucesos que se generan como resultado de esta regla se visualicen en el elemento Notificaciones del sistema en la pestaña Panel de control. Si habilita las notificaciones, configure el parámetro **Limitador de respuestas**.

Tabla 55. Parámetros de página Respuesta de regla de suceso, de flujo y común (continuación)

Parámetro	Descripción
Añadir a un conjunto de referencia	Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla añadan datos a un conjunto de referencia. Para añadir datos a un conjunto de referencia: 1. En el primer recuadro de lista, seleccione los datos que desea añadir. Las opciones incluyen todos los datos normalizados o personalizados. 2. En el segundo recuadro de lista, seleccione la referencia que está establecida en la que desea añadir los datos especificados. La respuesta de la regla **Añadir a un conjunto de referencia** proporciona las funciones siguientes: **Renovar** Pulse **Renovar** para renovar el primer recuadro de lista para asegurarse de que la lista es actual. **Configurar conjuntos de referencia** Pulse **Configurar conjuntos de referencia** para configurar el conjunto de referencia. Esta opción sólo está disponible si tiene permisos administrativos.

Tabla 55. Parámetros de página Respuesta de regla de suceso, de flujo y común (continuación)

Parámetro	Descripción
Añadir a datos de referencia	Antes de poder utilizar esta respuesta de regla, debe crear la recopilación de datos de referencia utilizando la interfaz de línea de mandatos (CLI). Para obtener más información sobre cómo crear y utilizar recopilaciones de datos de referencia, consulte la *Guía de administración* correspondiente al producto. Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla se añadan a una recopilación de datos de referencia. Después de marcar el recuadro de selección, seleccione una de las opciones siguientes: **Añadir a una correlación de referencia** Seleccione esta opción para enviar datos a una recopilación de pares de clave única/múltiples valores. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccione la correlación de referencia a la que desea añadir el registro de datos. **Añadir a una correlación de referencia de conjuntos** Seleccione esta opción para enviar datos a una recopilación de pares de clave/valor único. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccionar la correlación de referencia de conjuntos a los que desea añadir el registro de datos. **Añadir a una correlación de referencia de correlaciones** Seleccione esta opción para enviar datos a una recopilación de pares de varias claves/valor único. Debe seleccionar una clave para la primera correlación, una clave para la segunda correlación y, a continuación, el valor para el registro de datos. También debe seleccionar la correlación de referencia de correlaciones a la que desea añadir el registro de datos. **Añadir a una tabla de referencia** Seleccione esta opción para enviar datos a una recopilación de pares de múltiples claves/valor único, donde se ha asignado un tipo a las claves secundarios. Seleccione la tabla de referencia a la que desea añadir datos y, a continuación, seleccione una clave primaria. Seleccione las claves internas (claves secundarias) y sus valores para los registros de datos.

Tabla 55. Parámetros de página Respuesta de regla de suceso, de flujo y común (continuación)

Parámetro	Descripción
Ejecutar una acción personalizada	Puede escribir scripts que realizan acciones específicas en respuesta a los sucesos de red. Por ejemplo, puede escribir un script para crear una regla de cortafuegos que bloquea una dirección IP de origen concreta de la red en respuesta a repetidos intentos fallidos de inicio de sesión. Marque este recuadro de selección y seleccione una acción personalizada de la lista **Acción personalizada a ejecutar**. Puede añadir y configurar acciones personalizadas utilizando el icono **Definir acciones** en la pestaña **Admin**.
Publicar en el servidor IF-MAP	Si los parámetros IF-MAP están configurados y desplegados en los valores del sistema, seleccione esta opción para publicar la información de suceso sobre el servidor IF-MAP.
Limitador de respuestas	Marque este recuadro de selección y utilice los recuadros de lista para configurar la frecuencia con la que desea que responda esta regla.
Habilitar regla	Marque este recuadro de selección para habilitar esta regla.

La tabla siguiente proporciona los parámetros de página Respuesta de regla si el tipo de regla es Delito.

Tabla 56. Parámetros de página de respuesta de regla de delito

Parámetro	Descripción
Nombrar / Anotar el delito detectado	Marque este recuadro de selección para visualizar las opciones de Nombre.
Nombre de delito nuevo	Escriba el nombre que desea asignar al delito.
Anotación de delito	Escriba la anotación de delito que desea que se visualice en la pestaña Delitos.
Nombre del delito	Seleccione una de las opciones siguientes: **Esta información debe contribuir al nombre del delito** Seleccione esta opción si desea que la información de Nombre de suceso contribuya en el nombre del delito. **Esta información debe establecer o sustituir el nombre del delito** Seleccione esta opción si desea que el nombre de suceso configurado sea el nombre del delito.
Correo electrónico	Seleccione este recuadro de selección para visualizar las opciones de correo electrónico. **Nota:** Para cambiar el valor **Entorno local del correo electrónico**, seleccione **Valores del sistema** en la pestaña **Admin**.
Especifique las direcciones de correo electrónico que se deben notificar	Escriba la dirección de correo electrónico para enviar la notificación si se genera el suceso. Utilice una coma para separar varias direcciones de correo electrónico.

Tabla 56. Parámetros de página de respuesta de regla de delito (continuación)

Parámetro	Descripción
Condición de excepción de SNMP	Este parámetro sólo se visualiza cuando los parámetros Valores de SNMP se han configurado en los valores del sistema. Marque este recuadro de selección para permitir que esta regla envíe una notificación de SNMP (condición de excepción). En el caso de una regla de delito, la salida de condición de excepción SNMP incluye la hora del sistema, el OID condición de excepción y los datos de notificación, tal como los define el MIB.
Enviar a SysLog Local	Marque este recuadro de selección si desea registrar el suceso o flujo localmente.
Enviar a destinos de reenvío	Marque este recuadro de selección si desea registrar el suceso o flujo en un destino de reenvío. Un destino de reenvío es un sistema de proveedor, por ejemplo SIEM, tíquets o sistemas de alerta. Al marcar este recuadro de selección, se visualiza una lista de destinos de reenvío. Marque este recuadro de selección para el destino de reenvío al que desea enviar este suceso o flujo. Para añadir, editar o suprimir un destino de reenvío, pulse el enlace **Gestionar destinos**.
Publicar en el servidor IF-MAP	Si los parámetros IF-MAP están configurados y desplegados en los valores del sistema, seleccione esta opción para publicar la información de delito sobre el servidor IF-MAP.
Limitador de respuestas	Marque este recuadro de selección y utilice los recuadros de lista para configurar la frecuencia con la que desea que responda esta regla.
Habilitar regla	Marque este recuadro de selección para habilitar esta regla. De manera predeterminada, el recuadro de selección aparece seleccionado.

La tabla siguiente proporciona los parámetros de página Respuesta de regla si el tipo de regla es Anomalía.

Tabla 57. Parámetros de página de respuesta de regla de detección de anomalías

Parámetro	Descripción
Asignar suceso nuevo	Especifica que esta regla asigna un suceso nuevo además del suceso o flujo original, que se procesa como todos los demás sucesos del sistema. De forma predeterminada, este recuadro de selección está seleccionado y no se puede borrar.
Nombre de suceso	Escriba el nombre exclusivo del suceso que desea que se visualice en la pestaña Delitos.
Descripción del suceso	Escriba una descripción para el suceso. La descripción se visualiza en el panel Anotaciones de los detalles de suceso.

Tabla 57. Parámetros de página de respuesta de regla de detección de anomalías (continuación)

Parámetro	Descripción
Denominación de delito	Seleccione una de las opciones siguientes: **Esta información debe contribuir al nombre de los delitos asociados** Seleccione esta opción si desea que la información de Nombre de suceso contribuya en el nombre del delito. **Esta información debe establecer o sustituir el nombre de los delitos asociados** Seleccione esta opción si desea que el nombre de suceso configurado sea el nombre del delito. **Nota:** Una vez sustituido el nombre del delito, éste no cambiará hasta que se cierre el delito. Por ejemplo, si un delito está asociado a más de una regla y el último suceso no desencadena la regla configurada para sustituir temporalmente el nombre del delito, el último suceso no actualizará el nombre del delito. En lugar de esto, el nombre del delito sigue siendo el nombre establecido por la regla de alteración temporal. **Esta información no debe contribuir a la denominación de los delitos asociados** Seleccione esta opción si no desea que la información de Nombre de suceso contribuya en el nombre del delito.
Gravedad	El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 5. La Gravedad se visualiza en el panel Anotaciones de los detalles de suceso.
Credibilidad	Utilizando los recuadros de lista, seleccione la credibilidad del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 5. La Credibilidad se visualiza en el panel Anotaciones de los detalles de suceso.
Pertinencia	Utilizando los recuadros de lista, seleccione la pertinencia del suceso. El rango es de 0 (el más bajo) a 10 (el más alto) y el valor predeterminado es 5. La Pertinencia se visualiza en el panel Anotaciones de los detalles de suceso.
Categoría de nivel alto	En el recuadro de lista, seleccione la categoría de sucesos de alto nivel que desea que esta regla utilice al procesar sucesos.
Categoría de nivel bajo	En el recuadro de lista, seleccione la categoría de sucesos de bajo nivel que desea que esta regla utilice al procesar sucesos.
Anotar este delito	Marque este recuadro de selección para añadir una anotación a este delito y escriba la anotación.

Tabla 57. Parámetros de página de respuesta de regla de detección de anomalías (continuación)

Parámetro	Descripción
Asegúrese de que el suceso asignado forma parte de un delito	Como resultado de esta regla, el suceso se reenvía al componente Magistrado. Si existe un delito, se añade este suceso. Si no se ha creado ningún delito en la pestaña Delitos, se crea un delito nuevo. Se visualizan las opciones siguientes: **Indexar delito según** Especifica que el delito nuevo se base en el nombre de suceso. Este parámetro está habilitado de forma predeterminada. **Incluir sucesos detectados por Nombre de suceso de este punto en adelante, durante segundo(s), en el delito** Marque este recuadro de selección y escriba el número de segundos que desea incluir sucesos o flujos detectados desde el origen en la pestaña **Delitos**.
Correo electrónico	Seleccione este recuadro de selección para visualizar las opciones de correo electrónico. **Nota:** Para cambiar el valor **Entorno local del correo electrónico**, seleccione **Valores del sistema** en la pestaña **Admin**.
Especifique las direcciones de correo electrónico que se deben notificar	Escriba la dirección de correo electrónico a la que hay que enviar una notificación si se genera esta regla. Utilice una coma para separar varias direcciones de correo electrónico.
Seleccione la plantilla de correo electrónico de suceso	Seleccione la plantilla de correo electrónico para correos electrónicos asociados a esta regla. Para obtener información sobre la configuración de notificaciones de correo electrónico, consulte la *Guía de administración de IBM Security QRadar*.
Notificar	Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla se visualicen en el elemento Notificaciones del sistema en la pestaña **Panel de control**. Si habilita las notificaciones, configure el parámetro **Limitador de respuestas**.
Enviar a SysLog Local	Marque este recuadro de selección si desea registrar el suceso o flujo localmente. De forma predeterminada, el recuadro de selección no está marcado. **Nota:** Solo los sucesos normalizados se pueden registrar localmente en un dispositivo de QRadar. Si desea enviar datos de sucesos en bruto, debe utilizar la opción Enviar a destinos de reenvío para enviar los datos a un host de syslog remoto.

Tabla 57. Parámetros de página de respuesta de regla de detección de anomalías (continuación)

Parámetro	Descripción
Añadir a un conjunto de referencia	Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla añadan datos a un conjunto de referencia. Para añadir datos a un conjunto de referencia: 1. En el primer recuadro de lista, seleccione los datos que desea añadir. Las opciones incluyen todos los datos normalizados o personalizados. 2. Utilizando el segundo recuadro de lista, seleccione el conjunto de referencia al que desea añadir los datos especificados. La respuesta de la regla **Añadir a un conjunto de referencia** proporciona las funciones siguientes: **Renovar** Pulse **Renovar** para renovar el primer recuadro de lista para asegurarse de que la lista es actual. **Configurar conjuntos de referencia** Pulse **Configurar conjuntos de referencia** para configurar el conjunto de referencia. Esta opción sólo está disponible si tiene permisos administrativos.

Tabla 57. Parámetros de página de respuesta de regla de detección de anomalías (continuación)

Parámetro	Descripción
Añadir a datos de referencia	Antes de poder utilizar esta respuesta de regla, debe crear la recopilación de datos de referencia utilizando la interfaz de línea de mandatos (CLI). Para obtener más información sobre cómo crear y utilizar recopilaciones de datos de referencia, consulte la *Guía de administración* correspondiente al producto. Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta regla se añadan a una recopilación de datos de referencia. Después de marcar el recuadro de selección, seleccione una de las opciones siguientes: **Añadir a una correlación de referencia** Seleccione esta opción para enviar datos a una recopilación de pares de clave única/múltiples valores. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccione la correlación de referencia a la que desea añadir el registro de datos. **Añadir a una correlación de referencia de conjuntos** Seleccione esta opción para enviar datos a una recopilación de pares de clave/valor único. Debe seleccionar la clave y el valor para el registro de datos y, a continuación, seleccionar la correlación de referencia de conjuntos a los que desea añadir el registro de datos. **Añadir a una correlación de referencia de correlaciones** Seleccione esta opción para enviar datos a una recopilación de pares de varias claves/valor único. Debe seleccionar una clave para la primera correlación, una clave para la segunda correlación y, a continuación, el valor para el registro de datos. También debe seleccionar la correlación de referencia de correlaciones a la que desea añadir el registro de datos. **Añadir a una tabla de referencia** Seleccione esta opción para enviar datos a una recopilación de pares de múltiples claves/valor único, donde se ha asignado un tipo a las claves secundarios. Seleccione la tabla de referencia a la que desea añadir datos y, a continuación, seleccione una clave primaria. Seleccione las claves internas (claves secundarias) y sus valores para los registros de datos.

Tabla 57. Parámetros de página de respuesta de regla de detección de anomalías (continuación)

Parámetro	Descripción
Ejecutar una acción personalizada	Puede escribir scripts que realizan acciones específicas en respuesta a los sucesos de red. Por ejemplo, puede escribir un script para crear una regla de cortafuegos que bloquea una dirección IP de origen concreta de la red en respuesta a repetidos intentos fallidos de inicio de sesión. Marque este recuadro de selección y seleccione una acción personalizada de la lista **Acción personalizada a ejecutar**. Puede añadir y configurar acciones personalizadas utilizando el icono **Definir acciones** en la pestaña **Admin**.
Publicar en el servidor IF-MAP	Si los parámetros IF-MAP están configurados y desplegados en los valores del sistema, seleccione esta opción para publicar la información de delito sobre el servidor IF-MAP.
Limitador de respuestas	Marque este recuadro de selección y utilice los recuadros de lista para configurar la frecuencia con la que desea que responda esta regla
Habilitar regla	Marque este recuadro de selección para habilitar esta regla. De manera predeterminada, el recuadro de selección aparece seleccionado.

Una notificación SNMP puede tener el aspecto siguiente:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

Una salida de syslog puede tener este aspecto:

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

Tareas relacionadas:

"Creación de una regla" en la página 215
Las reglas evalúan los datos entrantes con condiciones de prueba de regla para generar una respuesta del sistema. Cuando las condiciones de una regla se cumplen, se pueden llevar a cabo varias acciones. Por ejemplo, puede configurar la respuesta del sistema a la regla, que puede ser la generación de delitos, el envío de correos electrónicos, el inicio de exploraciones, la adición de datos de referencia o el aumento o la disminución de valores como la gravedad.

Capítulo 12. Correlación histórica

Utilice la correlación histórica para ejecutar sucesos y flujos pasados a través del motor de reglas personalizadas (CRE) para identificar amenazas o incidentes de seguridad que ya se han producido.

Restricción: No puede utilizar la correlación histórica en IBM Security QRadar Log Manager. Para obtener más información sobre las diferencias entre IBM Security QRadar SIEM y IBM Security QRadar Log Manager, consulte "Prestaciones de su producto de inteligencia y seguridad" en la página 5.

De forma predeterminada, un despliegue de IBM Security QRadar SIEM analiza la información que se recopila de los orígenes de registro y los orígenes de flujo en tiempo casi real. Con la correlación histórica, puede crear correlaciones por la hora de inicio o por la hora de dispositivo. La *hora de inicio* es la hora a la que el suceso se ha recibido en QRadar. La *hora de dispositivo* es la hora a la que se produjo el suceso en el dispositivo.

La correlación histórica puede resultar útil en las situaciones siguientes:

Análisis de datos en masa
Si carga datos en masa en el despliegue de QRadar, puede utilizar la correlación histórica para correlacionar los datos contra los datos que se recopilaron en tiempo real. Por ejemplo, para evitar la degradación del rendimiento durante las horas de negocio normales, puede cargar sucesos de varios orígenes de registro cada día a media noche. Puede utilizar la correlación histórica para correlacionar los datos por hora de dispositivo para ver la secuencia de sucesos de red conforme se han producido en las últimas 24 horas.

Probar reglas nuevas
Puede ejecutar la correlación histórica para probar reglas nuevas. Por ejemplo, uno de sus servidores ha sufrido recientemente un ataque de un programa malicioso nuevo para el cual no tiene reglas implementadas. Puede crear una regla para comprobar la existencia de ese programa malicioso. Después, puede utilizar la correlación histórica para comprobar la regla con datos históricos para ver si la regla desencadenaría una respuesta si estuviese implementada en el momento del ataque. De forma similar, puede utilizar la correlación histórica para determinar cuándo se ha producido el ataque o la frecuencia del ataque. Puede seguir ajustando la regla y después pasarla a un entorno de producción.

Volver a crear delitos que se habían perdido o depurado
Si el sistema ha perdido delitos debido a un interrupción en la actividad o a cualquier otro motivo, puede volver a crear los delitos ejecutando la correlación histórica sobre los sucesos y los flujos que se recibieron durante ese tiempo.

Identificar hebras ocultas anteriormente
Conforme se conoce información sobre las amenazas de seguridad más recientes, puede utilizar la correlación histórica para identificar sucesos de red que ya se han producido paro que no han desencadenando un suceso. Puede realizar pruebas rápidamente para amenazas que ya hayan comprometido el sistema o los datos de su organización.

© Copyright IBM Corp. 2012, 2015

Visión general de la correlación histórica

Puede configurar un perfil de correlación histórica para especificar los datos históricos que desea analizar y el conjunto de reglas contra el que desea probar. Cuando se desencadena una regla, se crea un delito. Debe asignar el delito para la investigación y la corrección.

Selección de datos

El perfil utiliza una búsqueda guardada para recopilar los datos históricos de sucesos y flujos a utilizar en la ejecución. Asegúrese de que el perfil de seguridad otorga permiso para ver los sucesos y los flujos que desea incluir en la correlación histórica ejecutada.

Selección y manejo de reglas

La consola de QRadar procesa datos solo contra las reglas especificadas en el perfil de correlación.

Las reglas comunes prueban datos en sucesos y flujos. Debe tener permiso para ver sucesos y flujos para poder añadir reglas comunes al perfil. Cuando un usuario que carece de permiso para ver sucesos y flujos edita un perfil, las reglas comunes se eliminan automáticamente del perfil.

Puede incluir reglas inhabilitadas en un perfil de correlación histórica. Cuando se ejecuta el perfil, la regla inhabilitada se evalúa contra los sucesos y flujos entrantes. Si la regla se desencadena y la acción de regla es generar un delito, el delito se crea incluso aunque la regla esté inhabilitada. Para evitar la generación de distracciones innecesarias, las respuestas de regla, como por ejemplo la generación de informes y las notificaciones de correo se ignoran durante la correlación histórica.

Puesto que el proceso de correlación histórica se produce en una sola ubicación, las reglas que están incluidas en el perfil se tratan como reglas globales. El proceso no hace que una regla local se convierta en global, pero maneja la regla como si fuera global durante la ejecución de la correlación histórica. Algunas reglas, como por ejemplo las reglas con estados, podrían no desencadenar la misma respuesta que en una correlación normal que se ejecuta en un procesador de sucesos local. Por ejemplo, una regla con estados local que hace el seguimiento de cinco inicios de sesión fallidos en un periodo de cinco minutos con el mismo nombre de usuario se comporta de forma diferente en las ejecuciones de correlación normal e histórica. En una correlación normal, esta regla local mantiene un contador para el número de inicios de sesión fallidos que recibe cada procesador de sucesos local. En la correlación histórica, esta regla mantiene un solo contador para todo el sistema QRadar. En esta situación, se pueden crear delitos de forma diferente en comparación con una ejecución de correlación normal.

Creación de delitos

Las ejecuciones de correlación histórica crean delitos solo cuando se desencadena una regla y la acción de regla especifica que se debe crear un delito. Una correlación histórica no contribuye a un delito en tiempo real ni a un delito creado a partir de una correlación histórica anterior ejecutada, incluso cuando se utiliza el mismo perfil.

El número máximo de delitos que se pueden crear mediante una ejecución de correlación histórica es 100. La ejecución de correlación histórica se detiene cuando se alcanza el límite.

Puede ver delitos históricos en el panel de control Supervisión de amenazas y seguridad y en la pestaña **Delitos** al mismo tiempo que revisa los delitos en tiempo real.

Creación de un perfil de correlación histórica

Puede crear un perfil de correlación histórica para volver a ejecutar sucesos y flujos pasados a través del motor de reglas personalizadas (CRE). El perfil incluye información sobre el conjunto de datos y las reglas a utilizar durante la ejecución.

Restricción: Puede crear perfiles históricos solamente en IBM Security QRadar SIEM. No puede crear perfiles históricos en IBM Security QRadar Log Manager.

Antes de empezar

Las reglas comunes prueban datos en sucesos y flujos. Debe tener permiso para ver sucesos y flujos para poder añadir reglas comunes al perfil. Cuando un usuario que carece de permiso para ver sucesos y flujos edita un perfil, las reglas comunes se eliminan automáticamente del perfil.

Acerca de esta tarea

Puede configurar un perfil para correlacionar por hora de inicio u hora de dispositivo. La *hora de inicio* es la hora a la que los sucesos llegan al recopilador de sucesos. La *hora de dispositivo* es la hora a la que se produjo el suceso en el dispositivo. Los sucesos se pueden correlacionar por hora de inicio o por hora de dispositivo. Los flujos se pueden correlacionar por hora de inicio únicamente.

Puede incluir reglas inhabilitadas en el perfil. Las reglas inhabilitadas se indican en la lista de reglas con **(Inhabilitado)** después del nombre de regla.

Una correlación histórica no contribuye a un delito en tiempo real ni a un delito creado a partir de una correlación histórica anterior ejecutada, incluso cuando se utiliza el mismo perfil.

Procedimiento

1. Abra el cuadro de diálogo Correlación histórica.
   - En la pestaña **Actividad de registro**, pulse **Acciones** > **Correlación histórica**.
   - En la pestaña **Actividad de red**, pulse **Acciones** > **Correlación histórica**.
   - En la pestaña **Delitos**, pulse **Reglas** > **Acciones** > **Correlación histórica**.
2. Pulse **Añadir** y seleccione **Perfil de suceso** o **Perfil de flujo**.
3. Teclee un nombre para el perfil y seleccione una búsqueda guardada. Solo puede utilizar búsquedas guardadas no agregadas.
4. En la pestaña **Reglas**, seleccione las reglas a ejecutar contra los datos históricos y elija la hora de correlación.

   Si marca el recuadro de selección **Utilizar todas las reglas habilitadas**, no puede incluir reglas inhabilitadas en el perfil. Si desea incluir reglas habilitadas e inhabilitadas en el perfil, debe seleccionarlas individualmente de la lista de reglas y pulsar **Añadir seleccionado**.

5. En la pestaña **Planificar**, especifique el rango de horas para la búsqueda guardada y establezca los valores de planificación de perfil.
6. En la pestaña **Resumen**, revise la configuración y elija si desea ejecutar el perfil inmediatamente.
7. Pulse **Guardar**.

   El perfil se pone en cola para su proceso. Los perfiles en cola basados en una planificación tienen prioridad sobre las ejecuciones manuales.

Visualización de la información sobre ejecuciones de correlación histórica

Puede ver el historial de un perfil de correlación histórica para ver información sobre ejecuciones pasadas del perfil. Puede ver la lista de delitos creados durante la ejecución y el catálogo de sucesos o flujos que coinciden con las reglas desencadenadas del perfil. Puede ver el historial de ejecuciones de correlaciones históricas en cola, en ejecución, completadas, completadas con errores y canceladas.

Acerca de esta tarea

Se crea un catálogo de correlación histórica para cada regla desencadenada para cada dirección IP de origen exclusiva durante la ejecución, incluso si no se creó un delito. El catálogo contiene todos los sucesos o flujos que coinciden parcial o totalmente con la regla desencadenada.

No puede crear informes sobre datos de correlación histórica directamente desde QRadar. Si desea utilizar programas de terceros para crear informes, puede exportar los datos desde QRadar.

Procedimiento

1. Abra el cuadro de diálogo Correlación histórica.
   - En la pestaña **Actividad de registro**, pulse **Acciones** > **Correlación histórica**.
   - En la pestaña **Actividad de red**, pulse **Acciones** > **Correlación histórica**.
   - En la pestaña **Delitos**, pulse **Reglas** > **Acciones** > **Correlación histórica**.
2. Seleccione un perfil y pulse **Ver historial**.
   a. Si el estado de ejecución de correlación histórica es **Completado** y **Recuento de delitos** es 0, las reglas de perfil no han desencadenado delitos.
   b. Si la ejecución de la correlación histórica ha creado delitos, en la columna **Recuento de delitos** pulse el enlace para ver una lista de los delitos que se han creado. Si solo se ha creado un delito, se muestra el resumen de delitos.
3. En la columna **Catálogos**, pulse los enlaces para ver la lista de sucesos que coinciden completa o parcialmente con las reglas de perfil.

   La columna **StartTime** en la lista de sucesos representa la hora en que QRadar ha recibido el suceso.
4. Pulse **Cerrar**.

Capítulo 13. Integración de canal de información de X-Force Threat Intelligence

El canal de información de IBM Security X-Force Threat Intelligence proporciona una lista al minuto de direcciones IP y URL potencialmente maliciosas. Esta información se puede incorporar a reglas, delitos y sucesos y se puede utilizar para identificar una actividad indeseada en su entorno de red antes de que amenace la estabilidad de la red.

Debe tener una ampliación de licencia de QRadar para utilizar el canal de información X-Force Threat Intelligence con QRadar.

Al contenido del canal de información de X-Force Threat Intelligence se le proporciona una puntuación de amenaza que puede utilizar para ayudarle a priorizar incidentes y delitos generados a través de ese contenido. Los datos procedentes de estas fuentes de inteligencia se incorporan automáticamente a las funciones de correlación y análisis de QRadar, lo cual enriquece sus capacidades de detección de amenazas con datos sobre amenazas procedentes de Internet. Los datos de suceso de seguridad o de actividad de red que impliquen estas direcciones se señalan automáticamente y, por consiguiente, añaden contexto valiosos a las investigaciones y los análisis de incidentes de seguridad

Para priorizar la amenaza e identificar los incidentes de seguridad que requieren más análisis, puede elegir qué canales de información de X-Force se deben incorporar en las reglas, los delitos y los sucesos de QRadar. Por ejemplo, puede utilizar los canales de información para identificar estos tipos de incidentes:

- Una serie de inicios de sesión intentados para un rango dinámico de direcciones IP
- Una conexión proxy anónima a un portal de Business Partner
- Una conexión entre un punto final interno y un mandato y control de botnet conocido
- Comunicación entre un punto final y un sitio distribución de programas maliciosos conocido

El canal de información de X-Force Threat Intelligence categoriza las direcciones IP y asigna un valor de calificación de confianza a esta categorización. Un valor de factor de confianza de 0 a 100 se asigna a la categorización de los datos de reputación de IP. Este valor de confianza representa la confianza que X-Force tiene en que los datos de esta dirección IP se hayan categorizado adecuadamente. Una categorización de reputación de IP de correo no deseado con un valor de factor de confianza de 0 indica que el tráfico de IP de origen definitivamente no es correo no deseado, mientras que un valor de 100 indica un origen de correo no deseado definitivo. Cuando ajusta las reglas, puede utilizar el valor de factor de confianza para ajustar la sensibilidad de los desencadenantes de reglas. Al ajustar este valor de factor de confianza, puede ajustar el número de delitos generados.

Las direcciones IP se agrupan en las categorías siguientes:

- Hosts de programas maliciosos
- Orígenes de SPAM
- Direcciones IP dinámicas

© Copyright IBM Corp. 2012, 2015

- Proxies anónimos
- Mandato y control de Botnet
- Exploración de direcciones IP

El canal de información de X-Force Threat Intelligence también categoriza direcciones URL. Por ejemplo, las direcciones URL pueden categorizarse como sitios de citas, apuestas o pornografía. Para ver la lista completa de categorías para la clasificación de URL, consulte el sitio web IBM X-Force Exchange (https://exchange.xforce.ibmcloud.com/faq).

Antes de poder utilizar reglas basadas en URL, debe crear una propiedad de suceso personalizada para extraer el URL de la carga útil. La propiedad personalizada de URL ya está definida para sucesos de diversos orígenes como Blue Coat SG y Juniper Networks Secure Access.

Para obtener más información sobre cómo crear propiedades de suceso personalizadas, consulte Propiedades de sucesos y flujos personalizadas.

Actualizaciones y servidores de X-Force Threat Intelligence

Después de añadir el canal de información de IBM Security X-Force Threat Intelligence a QRadar, puede recibir inmediatamente datos de amenaza avanzados.

En general, el conjunto de datos de X-Force se actualiza cada 3 minutos y QRadar Console es responsable de todas las comunicaciones externas.

Para actualizaciones de datos, licencias y canales de información de widget de panel de control de X-Force y actualizaciones automáticas de QRadar se consultan los servidores siguientes:

Tabla 58. Servidores de X-Force

Servidor consultado	Descripción del servidor
www.iss.net	Widget de panel de control de X-Force Threat Intelligence para QRadar (AlertCon / canal de información RSS)
update.xforce-security.com	Servidor de actualización de canal de información de X-Force Threat Intelligence para datos de URL y reputación de IP
license.xforce-security.com	Servidor de licencias de X-Force Threat Intelligence
qmmunity.q1labs.com	Actualizaciones automáticas de QRadar. Para obtener más información sobre servidores de actualizaciones automáticas, consulte www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).

Habilitación de reglas de X-Force en IBM Security QRadar

Al añadir la licencia de X-Force IP Reputation Intelligence Feed a su sistema QRadar, se añaden reglas de X-Force mejoradas.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Reglas** > **Reglas**.
3. En el menú **Grupo**, pulse **XForce Premium**.

   La columna **Grupo** puede mostrar las reglas de legado y mejoradas. De forma predeterminada, las reglas de legado de X-Force están inhabilitadas. Sin

embargo, puede ver las reglas de legado que están habilitadas. Utilice las reglas mejoradas más recientes y no las reglas de legado que utilizan las redes remotas. Se elimina la opción de redes remotas.

4. Inhabilite las Reglas de legado, las reglas de X-Force Premium, seleccionando la fila de regla y pulsando **Acciones** > **Habilitar/inhabilitar**.

Reglas de X-Force Threat Intelligence mejoradas

Después e añadir el canal de alimentación de X-Force Threat Intelligence a QRadar, puede empezar a utilizar reglas del grupo de reglas de X-Force mejorado.

Las reglas siguientes forman parte del grupo de **Reglas de X-Force mejoradas**. Se pueden utilizar tal cual o se pueden personalizar.

Las reglas siguientes están basadas en IP:

X-Force Premium: Conexión interna a posible host de programa malicioso
Esta comunicación indica una fuerte posibilidad de que se haya realizado un intento de infectar el sistema cliente o de que se haya descargado un programa malicioso.

X-Force Premium: Hosts internos comunicándose con proxies anónimos
Los *proxies anónimos* son direcciones que son conocidas por enmascarar la identidad. Las utilizan con frecuencia los programas maliciosos o se utilizan durante las amenazas persistentes avanzadas de ocultar el origen de las comunicaciones con los orígenes externos. Estas direcciones pueden estar relacionadas con actividades tales como la comunicación de programas maliciosos o la exfiltración de datos.

X-Force Premium: Servidor de correo interno que envía correo a posible host de correo no deseado
Normalmente, los servidores de correo que se comunican con hosts de correo no deseado se están utilizando incorrectamente.

X-Force Premium: Servidores no de correo que se comunican con hosts de envío de correo no deseado conocidos
Este comportamiento es un fuerte indicador de que el servidor se ha comprometido y está siendo utilizado como una retransmisión de correo no deseado.

X-Force Premium: No servidores que se comunican con IP dinámica externa
Las direcciones IP asignadas dinámicamente no están normalmente asociadas con servidores legítimos en Internet. Las estaciones de trabajo internas que se están comunicando con direcciones dinámicas pueden indicar actividad interna sospechosa o actividad de botnet o programas maliciosos.

X-Force Premium: El servidor ha iniciado la conexión con hosts dinámicos
Generalmente, los servidores se comunican con hosts que tienen una identidad fija y no direcciones IP dinámicas.

Dado que el URL es un indicador más específico de los datos que se transfieren, las reglas basadas en URL pueden ser más precisas que las reglas basadas en IP.

Las reglas siguientes están basadas en URL:

X-Force Premium: Host interno que se comunica con URL de mandato y control de Botnet

A veces los servidores legítimos pueden utilizarse para proporcionar conectividad de botnet en direcciones de URL específicas.

X-Force Premium: Comunicación de host interno con URL de programa malicioso

A veces los servidores legítimos pueden utilizarse para proporcionar programas maliciosos para direcciones de URL específicas.

Creación de una regla utilizando la categorización de URL para supervisar el acceso a determinados tipos de sitios web

Puede crear una regla que envíe una notificación de correo electrónico si los usuarios de la red interna acceden a direcciones de URL que están categorizadas como sitios web de apuestas.

Antes de empezar

Para utilizar reglas de categorización de URL, debe tener una suscripción al canal de información de X-Force Threat Intelligence.

Para crear una regla nueva, debe tener el permiso **Delitos** > **Mantener reglas personalizadas**.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el menú de navegación, pulse **Reglas**.
3. En el recuadro de lista **Acciones**, seleccione **Nueva regla de sucesos**.
4. Lea el texto introductorio en el asistente de reglas y pulse **Siguiente**.
5. Pulse **Sucesos** y pulse **Siguiente**.
6. En el recuadro de lista **Grupo de pruebas**, seleccione **X-Force Tests**.
7. Pulse el signo más (+) signo junto a la prueba **when this URL property is categorized by X-Force as one of the following categories**.
8. En el campo **especifique aquí el nombre de la regla** en el panel Regla, escriba un nombre exclusivo que desee asignar a esta regla.
9. En el recuadro de lista, seleccione **Local** o **Global**.
10. Pulse los parámetros configurables subrayados para personalizar las variables de la prueba.
    a. Pulse **URL (personalizado)**.
    b. Seleccione la propiedad de URL que contiene el URL que se ha extraído de la carga útil y pulse **Enviar**.
    c. Pulse **una de las siguientes categorías**.
    d. Seleccione **Gambling / Lottery** en las categorías de URL de X-Force, pulse **Añadir +** y pulse **Enviar**.
11. Para exportar la regla configurada como un componente básico para utilizarlo con otras reglas:
    a. Pulse **Exportar como componente básico**.
    b. Escriba un nombre exclusivo para este componente básico.
    c. Pulse **Guardar**.

12. En el panel Grupos, seleccione los recuadros de selección de los grupos a los que desea asignar esta regla.
13. En el campo **Notas**, escriba una nota que desee incluir para esta regla y pulse **Siguiente**.
14. En la página Respuestas de regla, pulse **Correo electrónico** y escriba las direcciones de correo electrónico que recibirán la notificación. Para obtener información sobre otros parámetros de respuesta para una regla de suceso, consulte Parámetros de página de respuesta de regla común, flujo y suceso.
15. Pulse **Siguiente**.
16. Si la regla es precisa, pulse **Finalizar**.

Búsqueda de información de direcciones IP y URL en X-Force Exchange

Utilice las opciones del menú contextual de IBM Security QRadar para buscar información sobre las direcciones IP y URL que se encuentra en IBM Security X-Force Exchange. Puede utilizar la información de las búsquedas, los delitos y las reglas de QRadar para investigar más o para añadir información sobre direcciones IP o URL a una recopilación de X-Force Exchange.

Acerca de esta tarea

Puede proporcionar información pública o privada para hacer un seguimiento de los datos de las recopilaciones cuando investigue problemas de seguridad.

Una *recopilación* es un repositorio donde se almacena la información que se encuentra durante una investigación. Puede utilizar una recopilación para guardar informes, comentarios o cualquier otro contenido de X-Force Exchange. Un informe de X-Force Exchange contiene una versión del informe del momento en que se guardó y un enlace a la versión actual del informe. La recopilación también contiene una sección (línea temporal) que tiene un área de notas con estilo wiki en la que puede añadir comentarios que son relevantes para la recopilación.

Para obtener más información acerca de X-Force Exchange, consulte X-Force Exchange (https://exchange.xforce.ibmcloud.com/).

Procedimiento

1. Para buscar una dirección IP en X-Force Exchange desde QRadar, siga estos pasos:
   a. Seleccione la pestaña **Actividad de registro** o **Actividad de red**.
   b. Pulse el botón derecho del ratón en la dirección IP que desea ver en X-Force Exchange y seleccione **Más opciones** > **Opciones de plugin** > **Búsqueda de X-Force Exchange** para abrir la interfaz de X-Force Exchange.
2. Para buscar un URL en X-Force Exchange desde QRadar, siga estos pasos:
   a. Seleccione la pestaña **Delitos** o las ventanas de detalles de sucesos disponibles en **Delitos**.
   b. Pulse el botón derecho del ratón en el URL que desea ver en X-Force Exchange y seleccione **Opciones de plugin > Búsqueda de X-Force Exchange** para abrir la interfaz de X-Force Exchange.

Gestión de falsos positivos

Puede utilizar X-Force Threat Intelligence para gestionar la sensibilidad de sus desencadenantes de reglas para poder reducir el número de falsos positivos de la red. Utilice el ajuste de falsos positivos para impedir que los sucesos y los flujos se correlacionen con delitos.

Factor de confianza

X-Force categoriza los datos de reputación de IP y asigna un factor de confianza de 0 a 100 a esa categorización, donde 0 representa ninguna confianza y 100 representa la certeza. Por ejemplo, X-Force puede categorizar una dirección IP de origen como una IP de exploración con un factor de confianza de 75, que es un nivel de confianza moderadamente elevado.

¿Cómo especifico un valor de confianza?

Especifique un valor de confianza en la prueba de regla de X-Force siguiente en QRadar: **cuando esta propiedad de host está categorizada por X-Force como esta categoría con un valor de confianza igual a esta cantidad**

Directrices para establecer el valor de confianza

El factor de confianza es una de las herramientas principales que puede utilizar para ayudar a limitar el número de delitos creados por reglas desencadenadas. En función del nivel de protección que desea, puede ajustar los valores de confianza al nivel que mejor se ajuste a su entorno de red.

En una zona DMZ, puede elegir un valor de confianza más elevado, por ejemplo, 95% o superior porque no necesita investigar muchos delitos en ese área. Con este nivel de confianza, las direcciones IP se ajustarán con mucha probabilidad a la categoría listada. Si hay un 95% de certidumbre de que un host esté proporcionando malware, debe saberlo.

Puede bajar el valor de confianza para áreas más seguras de la red como por ejemplo una agrupación de servidores. Al bajar el nivel de confianza, hay mayor posibilidad de identificar amenazas y dedica menos esfuerzo a investigar porque la amenaza pertenece a un segmento de red específico.

Para un ajuste de falso positivo, gestione sus desencadenantes de regla por segmento. Busque en su infraestructura de red y decida qué activos necesitan un alto nivel de protección y qué activos no. Puede aplicar diferentes valores de confianza para los diferentes segmentos de red. Utilice los bloques básicos para agrupar las pruebas utilizada más habitualmente de modo que se puedan utilizar en reglas.

Reglas basadas en URL

Puede ver falsos positivos de sitios de hosts virtuales compartidos porque un sitio puede proporcionar contenido legítimo mientras que otro sitio de la misma dirección IP puede proporcionar malware. En una configuración de hospedaje virtual compartido, la información de URL es útil porque el URL es un indicador más específico de los datos transferidos. Las reglas basadas en URL pueden ser más precisas que las reglas basadas en IP.

Para las reglas basadas en URL, debe crear una propiedad de suceso personalizada para extraer el URL de la carga útil.

Para obtener más información sobre el ajuste de falsos positivos, consulte la *Guía de ajuste*.

Capítulo 14. Gestión de informes

Puede utilizar la pestaña **Informes** para crear, editar, distribuir y gestionar informes.

Unas opciones de creación de informes detalladas y flexibles satisfacen diversos estándares normativos como, por ejemplo, la conformidad con PCI.

Puede crear sus propios informes personalizados o utilizar informes predeterminados. Puede personalizar y cambiar el nombre de informes predeterminados y distribuirlos a otros usuarios.

La pestaña **Informes** puede necesitar un largo periodo de tiempo para renovarse si el sistema incluye muchos informes.

Nota: Si ejecuta Microsoft Exchange Server 5.5, es posible que aparezcan caracteres de tipos no disponibles en la línea del asunto de los informes enviados por correo electrónico. Para resolver este problema, descargue e instale el Service Pack 4 de Microsoft Exchange Server 5.5. Para obtener más información, póngase en contacto con el soporte de Microsoft.

Consideraciones sobre el huso horario

Para asegurarse de que la característica de creación de informes utiliza la fecha y hora correctas para crear informes de datos, la sesión debe estar sincronizada con el huso horario.

Durante la instalación y configuración de los productos de QRadar, se configura el huso horario. Consulte con el administrador para asegurarse de que la sesión de QRadar está sincronizada con el huso horario.

Permisos de la pestaña de informes

Los usuarios administrativos pueden ver todos los informes creados por otros usuarios.

Los usuarios no administrativos solo pueden ver los informes que ellos han creado o los informes compartidos por otros usuarios.

Parámetros de la pestaña de informes

La pestaña **Informes** muestra una lista de informes personalizados y predeterminados.

En la pestaña **Informes**, puede ver información estadística acerca de la plantilla de informes, realizar acciones en las plantillas de informes, ver los informes generados y suprimir el contenido generado.

Si un informe no especifica una planificación de intervalo, debe generar manualmente el informe.

Puede pasar el puntero del ratón sobre cualquier informe para previsualizar un resumen de informe en una ayuda contextual. El resumen especifica la

© Copyright IBM Corp. 2012, 2015

configuración del informe y el tipo de contenido que genera el informe.

Diseño de informe

Un informe puede constar de varios elementos de datos y puede representar datos de red y de seguridad en diversos estilos, tales como tablas, gráficos de línea, gráficos circulares y gráficos de barras.

Al seleccionar el diseño de un informe, tenga en cuenta el tipo de informe que desea crear. Por ejemplo, no elija un contenedor de gráfico pequeño para un contenido de gráfico que muestra muchos objetos. Cada gráfico incluye una leyenda y una lista de redes de las que se deriva el contenido; elija un contenedor suficientemente grande para contener los datos. Para ver previamente cómo visualiza cada gráfico los datos, consulte Tipos de gráfico.

Tipos de gráfico

Cuando se crea un informe, debe elegir un tipo de gráfico para cada gráfico que desea incluir en el informe.

El tipo de gráfico determina cómo presenta el informe generado los datos y objetos de red. Puede crear un gráfico de datos con varias características y crear los gráficos en un único informe generado.

Puede utilizar cualquiera de los tipos de gráficos siguientes:

- **Ninguno**: Utilice esta opción para visualizar un contenedor vacío en el informe. Esta opción puede ser útil para crear espacio en blanco en el informe. Si selecciona la opción **Ninguno** para cualquier contenedor, no es necesario realizar ninguna configuración adicional para dicho contenedor.
- **Vulnerabilidades de activos**: Utilice este gráfico para ver los datos de vulnerabilidad para cada activo definido en el despliegue. Puede generar gráficos de vulnerabilidad de activos cuando una exploración de VA ha detectado vulnerabilidades. Este gráfico está disponible después de instalar IBM Security QRadar Vulnerability Manager.
- **Conexiones**: Esta opción de gráfico sólo se visualiza si ha adquirido IBM Security QRadar Risk Manager y tiene licencia para el mismo. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
- **Reglas de dispositivo**: Esta opción de gráfico sólo se visualiza si ha adquirido IBM Security QRadar Risk Manager y tiene licencia para el mismo. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
- **Objetos no utilizados de dispositivo**: Esta opción de gráfico sólo se visualiza si ha adquirido IBM Security QRadar Risk Manager y tiene licencia para el mismo. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Guía del usuario*.
- **Sucesos/Registros**: Utilice este gráfico para ver información de suceso. Puede basar los gráficos en datos de búsquedas guardadas de la pestaña **Actividad de registro**. Puede personalizar los datos que desea visualizar en el informe generado. Puede configurar el gráfico para trazar datos durante un periodo de tiempo configurable. Esta funcionalidad le ayuda a detectar tendencias de sucesos. Para obtener más información sobre las búsquedas guardadas, consulte Búsquedas de datos.

- **Orígenes de registro**: Utilice este gráfico para exportar o informe sobre los orígenes de registro. Seleccione los orígenes de registro y los grupos de orígenes de registro que desea que aparezcan en el informe. Ordene los orígenes de registro por columnas de informe. Incluya orígenes de registro de los que no se ha informado durante un periodo de tiempo definido. Incluya orígenes de registro que se han creado en un tiempo especificado.
- **Flujos**: Utilice este gráfico para ver información de flujo. Puede basar los gráficos en datos de las búsquedas guardadas de la pestaña Actividad de red. Esto le permite personalizar los datos que desea visualizar en el informe generado. Puede utilizar las búsquedas guardadas para configurar el gráfico para trazar datos de flujo a lo largo de un periodo de tiempo configurable. Esta funcionalidad le ayuda a detectar tendencias de flujo. Para obtener más información sobre las búsquedas guardadas, consulte Búsquedas de datos.
- **Direcciones IP de destino principales**: Utilice este gráfico para visualizar las direcciones IP de destino principales en las ubicaciones de red que seleccione.
- **Delitos principales**: Utilice este gráfico para visualizar los delitos principales que se producen en el momento actual para las ubicaciones de red que seleccione.
- **Direcciones IP de origen principales**: Utilice este gráfico para visualizar y ordenar los principales orígenes de delito (direcciones IP) que atacan la red o los activos de la empresa.
- **Vulnerabilidades**: La opción Vulnerabilidades sólo se visualiza cuando se ha adquirido IBM Security QRadar Vulnerability Manager y se dispone de licencia para el mismo. Para obtener más información, consulte la publicación *Guía del usuario de IBM Security QRadar Vulnerability Manager*.

Barra de herramientas de la pestaña de informes

Puede utilizar la barra de herramientas para realizar una serie de acciones en los informes.

La tabla siguiente identifica y describe las opciones de la barra de herramientas de Informes.

Tabla 59. Opciones de barra de herramientas de Informes

Opción	Descripción
Grupo	
Gestionar grupos	Pulse **Gestionar grupos** para gestionar grupos de informes. Mediante el uso de la característica Gestionar grupos, puede organizar los informes en grupos funcionales. Puede compartir los grupos de informes con otros usuarios.

Tabla 59. Opciones de barra de herramientas de Informes (continuación)

Opción	Descripción
Acciones	Pulse **Acciones** para realizar las acciones siguientes: • **Crear**: Seleccione esta opción para crear un informe nuevo. • **Editar**: Seleccione esta opción para editar el informe seleccionado. También puede efectuar una doble pulsación en un informe para editar el contenido. • **Duplicar**: Seleccione esta opción para duplicar o renombrar el informe seleccionado. • **Asignar grupos**: Seleccione esta opción para asignar el informe seleccionado a un grupo de informes. • **Compartir**: Seleccione esta opción para compartir el informe seleccionado con otros usuarios. Debe tener privilegios administrativos para compartir informes. • **Conmutar planificación**: Seleccione esta opción para conmutar el informe seleccionado al estado Activo o Inactivo. • **Ejecutar informe**: Seleccione esta opción para generar el informe seleccionado. Para generar varios informes, mantenga pulsada la tecla Control y pulse los informes que desea generar. • **Ejecutar informe para datos en bruto**: Seleccione esta opción para generar el informe seleccionado utilizando datos en bruto. Esta opción es útil si desea generar un informe antes de que estén disponibles los datos acumulados necesarios. Por ejemplo, si desea ejecutar un informe semanal antes de que haya transcurrido una semana completa desde que creó el informe, puede generar el informe utilizando esta opción. • **Suprimir informe**: Seleccione esta opción para suprimir el informe seleccionado. Para suprimir varios informes, mantenga pulsada la tecla Control y pulse los informes que desea suprimir. • **Suprimir contenido generado**: Seleccione esta opción para suprimir todo el contenido generado para las filas seleccionadas. Para suprimir varios informes generados, mantenga pulsada la tecla Control y pulse los informes generados que desea suprimir.

Tabla 59. Opciones de barra de herramientas de Informes (continuación)

Opción	Descripción
Ocultar informes inactivos	Seleccione este recuadro de selección para ocultar las plantillas de informes inactivos. La pestaña **Informes** se renueva automáticamente y muestra sólo los informes de activos. Quite la marca del recuadro de selección para mostrar los informes inactivos ocultos.
Buscar en informes	Escriba los criterios de búsqueda en el campo **Buscar en informes** y pulse el icono **Buscar en informes**. Se ejecuta una búsqueda en los parámetros siguientes para determinar cuáles coinciden con los criterios especificados: • Título de informe • Descripción de informe • Grupo de informes • Grupos de informes • Nombre de usuario de autor de informes

Tipos de gráfico

Cada tipo de diagrama soporta varios tipos de gráfico que puede utilizar para visualizar datos.

Los archivos de configuración de red determinan los colores que los diagramas utilizan para representar el tráfico de red. Cada dirección IP se representa mediante un color exclusivo. La tabla siguiente proporciona ejemplos de cómo se utilizan los datos de red y de seguridad en los diagramas. La tabla describe los tipos de diagrama que están disponibles para cada tipo de gráfico.

Tabla 60. Tipos de gráfico

Tipo de gráfico	Tipos de diagrama disponibles
Línea	• Sucesos/Registros • Flujos • Conexiones • Vulnerabilidades
Línea apilada	• Sucesos/Registros • Flujos • Conexiones • Vulnerabilidades
Barra	• Sucesos/Registros • Flujos • Conexiones de vulnerabilidades de activos • Conexiones • Vulnerabilidades

Tabla 60. Tipos de gráfico (continuación)

Tipo de gráfico	Tipos de diagrama disponibles
Barra horizontal	• IP de origen principales • Delitos principales • IP de destino principales
Barra apilada	• Sucesos/Registros • Flujos • Conexiones
Circular	• Sucesos/Registros • Flujos • Vulnerabilidades de activos • Conexiones • Vulnerabilidades
Tabla	• Sucesos/Registros • Flujos • IP de origen principales • Delitos principales • IP de destino principales • Conexiones • Vulnerabilidades Para visualizar el contenido en una tabla, debe diseñar el informe con un contenedor de ancho de página completa.
Tabla de agregación	Disponible con el diagrama de Vulnerabilidades de activos. Para visualizar el contenido en una tabla, debe diseñar el informe con un contenedor de ancho de página completa.

Están disponibles los siguientes tipos de gráfico para informes de QRadar Log Manager:

- Gráfico de líneas
- Gráfico de líneas apiladas
- Gráfico de barras
- Gráfico de barras apiladas
- Gráfico circular
- Gráfico de tabla

Nota: Cuando crea informes de gráficos de barras y barras apiladas, la leyenda se presenta en formato fijo, donde las barras o las secciones de barras se representan por etiquetes codificadas por colores en la mayoría de los casos. Si selecciona el tiempo como el valor del eje x, puede crear intervalos de tiempo en el eje x.

Creación de informes personalizados

Utilice el Asistente de informes para crear un nuevo informe y personalizarlo.

Antes de empezar

Debe tener los permisos de red apropiados para compartir un informe generado con otros usuarios.

Para obtener más información sobre los permisos, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Acerca de esta tarea

El Asistente de informes proporciona una guía paso a paso sobre cómo diseñar, planificar y generar informes.

El asistente utiliza los siguientes elementos clave para ayudarle a crear un informe:

- **Diseño**: Posición y tamaño de cada contenedor
- **Contenedor**: Marcador para el contenido presentado
- **Contenido**: Definición del gráfico que se coloca en el contenedor

Después de crear un informe que se genera semanal o mensualmente, debe transcurrir el tiempo planificado antes de que el informe generado devuelva resultados. Para un informe planificado, debe esperar el periodo de tiempo planificado para que se creen los resultados. Por ejemplo, una búsqueda semanal necesita siete días para crear los datos. Esta búsqueda devolverá resultados tras siete días.

Cuando especifique el formato de salida para el informe, tenga en cuenta que el tamaño de archivo de los informes generados puede tener de uno a dos megabytes, dependiendo del formato de salida seleccionado. El formato PDF es menor de tamaño y no utiliza una gran cantidad de espacio de almacenamiento de disco.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el cuadro de lista **Acciones**, seleccione **Crear**.
3. En la ventana Bienvenido al Asistente de informes, pulse **Siguiente**.
4. Seleccione una de las opciones siguientes:

Opción	Descripción
Manualmente	De forma predeterminada, el informe se genera una vez. Puede generar el informe con la frecuencia que desee.
Cada hora	Planifica que el informe se genere al final de cada hora. Se utilizan los datos de la hora anterior. En los recuadros de lista, seleccione un intervalo de tiempo para empezar y finalizar el ciclo del informe. Se genera un informe para cada hora dentro de este intervalo de tiempo. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m. para los campos **Desde** y **Hasta**.

Opción	Descripción
Semanalmente	Planifica que el informe se genere semanalmente utilizando los datos de la semana anterior. Seleccione el día que desea generar el informe. El valor predeterminado es Lunes. En el recuadro de lista, seleccione una hora para empezar el ciclo del informe. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.
Mensualmente	Planifica el informe para generar mensualmente utilizando los datos del mes anterior. En el recuadro de lista, seleccione la fecha en la que desea generar el informe. El valor predeterminado es el primer día del mes. Seleccione una hora para empezar el ciclo del informe. El tiempo está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.

5. En el panel **Permitir que este informe se genere manualmente**, seleccione **Sí** o **No**.
6. Configure el diseño del informe:
   a. En el recuadro de lista **Orientación**, seleccione **Vertical** u **Horizontal** para la orientación de página.
   b. Seleccione una de las seis opciones de diseño que se muestran en el asistente de informes.
   c. Pulse **Siguiente**.
7. Especifique valores para los parámetros siguientes:

Parámetro	Valores
Título de informe	El título puede tener una longitud máxima de 100 caracteres. No utilice caracteres especiales.
Logotipo	En el recuadro de lista, seleccione un logotipo.
Opciones de paginación	En el recuadro de lista, seleccione la ubicación en el informe en la que se aparecerán los números de página. Puede optar por no mostrar números de página.
Clasificación de informe	Escriba una clasificación para este informe. Puede escribir un máximo de 75 caracteres. Puede utilizar espacios iniciales, caracteres especiales y caracteres de doble byte. La clasificación del informe se muestra en la cabecera y el pie de página del informe. Si lo desea, puede clasificar el informe como `confidencial`, `muy confidencial`, `sensible` o `interno`.

8. Configure cada contenedor en el informe:
   a. En el recuadro de lista **Tipo de gráfico**, seleccione un tipo de gráfico.

b. En la ventana Detalles de contenedor, configure los parámetros de gráfico.

   Nota: También puede crear búsquedas guardadas de activos. En el cuadro de lista **Buscar para utilizar**, seleccione la búsqueda guardada.

c. Pulse **Guardar detalles de contenedor**.

d. Si ha seleccionado más de un contenedor, repita los pasos del a al c.

e. Pulse **Siguiente**.

9. Vea previamente la página Vista previa del diseño y, a continuación, pulse **Siguiente**.

10. Marque los recuadros de selección para los formatos de informe que desea generar y pulse **Siguiente**.

    Importante: Extensible Markup Language sólo está disponible para tablas.

11. Seleccione los canales de distribución para el informe y, a continuación, pulse **Siguiente**. Las opciones incluyen los siguientes canales de distribución:

Opción	Descripción
Consola de informes	Marque este recuadro de selección para enviar el informe generado a la pestaña **Informes**. **Consola de informes** es el canal de distribución predeterminado.
Seleccione los usuarios que deben poder ver el informe generado.	Esta opción se muestra después de seleccionar el recuadro de selección **Consola de informes**. En la lista de usuarios, seleccione los usuarios a los que desea otorgar permiso para ver los informes generados.
Seleccionar todos los usuarios	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Consola de informes**. Marque este recuadro de selección si desea otorgar permiso a todos los usuarios para ver los informes generados. Debe tener permisos de red apropiados para compartir el informe generado con otros usuarios.
Correo electrónico	Marque este recuadro de selección si desea distribuir el informe generado por correo electrónico.
Escriba la dirección o direcciones de correo electrónico de destino del informe:	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Correo electrónico**. Escriba la dirección de correo electrónico para cada destinatario de informe generado; separe una lista de direcciones de correo electrónico con comas. El máximo de caracteres para este parámetro es de 255. Los destinatarios de correo electrónico reciben este correo electrónico desde no_reply_reports@qradar.

Opción	Descripción
Incluir informe como archivo adjunto (sólo no HTML)	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Correo electrónico**. Marque este recuadro de selección para enviar el informe generado como un archivo adjunto.
Incluir enlace a consola de informes	Esta opción sólo se visualiza después de seleccionar el recuadro de selección **Correo electrónico**. Marque este recuadro de selección para incluir un enlace a la Consola de informes en el correo electrónico.

12. En la página Se está terminando, entre valores para los parámetros siguientes.

Opción	Descripción
Descripción de informe	Escriba una descripción para este informe. La descripción se visualiza en la página Resumen de informe y en el correo electrónico de distribución de informes generados.
Seleccione los grupos a los que deba pertenecer este informe	Seleccione los grupos a los que desea asignar este informe. Para obtener más información sobre grupos, consulte Grupos de informes.
¿Desea ejecutar el informe ahora?	Marque este recuadro de selección si desea generar el informe cuando se complete el asistente. De manera predeterminada, el recuadro de selección aparece seleccionado.

13. Pulse **Siguiente** para ver el resumen de informe.
14. En la página Resumen de informe, seleccione las pestañas disponibles en el informe de resumen para previsualizar la configuración de informe.

Resultados

El informe se genera inmediatamente. Si ha borrado el recuadro de selección **¿Desea ejecutar el informe ahora?** en la página final del asistente, el informe se guarda y se genera a la hora planificada. El título de informe es el título predeterminado para el informe generado. Si reconfigura un informe para entrar título de informe nuevo, el informe se guarda como un informe nuevo con el nombre nuevo; sin embargo, el informe original sigue siendo el mismo.

Edición de un informe

Utilizando el asistente de informes, puede editar cualquier informe personalizado o predeterminado para cambiarlo.

Acerca de esta tarea

Puede utilizar o personalizar un número significativo de informes predeterminados. La pestaña **Informes** predeterminada visualiza la lista de informes. Cada informe captura y visualiza los datos existentes.

Nota: Cuando personaliza un informe planificado para que se genere manualmente, seleccione el intervalo de tiempo **Fecha de finalización** antes de seleccionar el valor de **Fecha de inicio**.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Efectúe una doble pulsación en el informe que desea personalizar.
3. En el asistente de informes, cambie los parámetros para personalizar el informe para generar el contenido que necesita.

Resultados

Si reconfigura un informe para entrar título de informe nuevo, el informe se guarda como un informe nuevo con el nombre nuevo; sin embargo, el informe original sigue siendo el mismo.

Visualización de informes generados

En la pestaña **Informes**, se visualiza un icono en la columna **Formatos** si un informe ha generado contenido. Puede pulsar el icono para ver el informe.

Acerca de esta tarea

Cuando un informe ha generado contenido, la columna **Informes generados** visualiza un recuadro de lista. El recuadro de lista muestra todo el contenido generado, que se organiza por la indicación de fecha y hora del informe. Los informes más recientes se muestran en la parte superior de la lista. Si un informe no tiene ningún contenido generado, se visualiza el valor **Ninguno** en la columna **Informes generados**.

Los iconos que representan el formato del informe generado se visualizan en la columna **Formatos**.

Los informes pueden generarse en los formatos PDF, HTML, RTF, XML y XLS.

Nota: Los formatos XML y XLS sólo están disponibles para los informes que utilizan un formato de tabla de un solo gráfico (vertical u horizontal).

Puede ver sólo los informes a los que se le ha dado acceso desde el administrador. Los usuarios administrativos pueden acceder a todos los informes.

Si utiliza el navegador web Mozilla Firefox y selecciona el formato de informe RTF, el navegador web Mozilla Firefox inicia una nueva ventana de navegador. Este nuevo inicio de ventana es el resultado de la configuración de navegador web Mozilla Firefox y no afecta a QRadar. Puede cerrar la ventana y continuar con la sesión de QRadar.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el recuadro de lista de la columna **Informes generados**, seleccione la indicación de fecha y hora del informe desea ver.
3. Pulse el icono correspondiente al formato que desea ver.

Supresión de contenido generado

Cuando suprime el contenido generado, todos los informes que se han generado a partir de la plantilla de informe se suprimen, pero la plantilla de informe se conserva.

Procedimiento

1. Pulse la pestaña **Informe**.
2. Seleccione los informes para los que desea suprimir el contenido generado.
3. En el recuadro de lista **Acciones**, pulse **Suprimir contenido generado**.

Generación manual de un informe

Un informe puede configurarse para que se genere automáticamente, sin embargo, el usuario puede generar manualmente un informe en cualquier momento.

Acerca de esta tarea

Mientras se genera un informe, la columna Próxima hora de ejecución visualiza uno de los tres mensajes siguientes:

- **Generando**: El informe se está generando.
- **En cola (posición en la cola)**: El informe se pone en cola para generarse. El mensaje indica la posición en la que está el informe en la cola. Por ejemplo, 1 de 3.
- **(x hora(s) x min(s) y seg(s))**: Está planificado que el informe se ejecute. El mensaje es un temporizador de cuenta atrás que especifica cuándo se ejecutará el informe la próxima vez.

Puede seleccionar el icono **Renovar** para renovar la vista, incluida la información de la columna **Próxima hora de ejecución**.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea generar.
3. Pulse **Ejecutar informe**.

Qué hacer a continuación

Una vez que se ha generado el informe, puede ver el informe generado desde la columna Informes generados.

Duplicación de un informe

Para crear un informe que se parezca detenidamente a un informe existente, puede duplicar el informe que desea modelar y, a continuación, personalizarlo.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea duplicar.
3. En el recuadro de lista **Acciones**, pulse **Duplicar**.
4. Escriba un nuevo nombre, sin espacios, para el informe.

Qué hacer a continuación

Puede personalizar el informe duplicado.

Compartición de un informe

Puede compartir informes con otros usuarios. Cuando se comparte un informe, se proporciona una copia del informe seleccionado a otro usuario para editarlo o planificarlo.

Acerca de esta tarea

Las actualizaciones que el usuario realiza en un informe compartido no afectan a la versión original del informe.

Debe tener privilegios administrativos para compartir informes. Además, para que un usuario nuevo vea y acceda a los informes, un usuario administrativo debe compartir todos los informes necesarios con el nuevo usuario.

Sólo puede compartir el informe con los usuarios que tienen el acceso adecuado.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione los informes que desea compartir.
3. En el recuadro de lista **Acciones**, pulse **Compartir**.
4. En la lista de usuarios, seleccione los usuarios con los que desea compartir este informe.

Creación de marca de informes

Para marcar de informes, puede importar logotipos e imágenes específicas. Para marcar informes con logotipos personalizados, debe cargar y configurar los logotipos antes de empezar a utilizar el asistente de informes.

Antes de empezar

Asegúrese de que el gráfico que desea utilizar tiene 144 x 50 píxeles con un fondo en blanco.

Para asegurarse de que el navegador visualice el nuevo logotipo, borre la caché de navegador.

Acerca de esta tarea

La creación de marcas de informe es beneficiosa para la empresa cuando se soporta más de un logotipo. Cuando se carga una imagen, esta imagen se guarda de forma automática en formato PNG (Portable Network Graphic).

Cuando se carga una nueva imagen y se establece la imagen como valor predeterminado, la nueva imagen predeterminada no se aplica a los informes que se han generado anteriormente. Para actualizar el logotipo en informes generados previamente es necesario generar manualmente contenido nuevo desde el informe.

Si carga una imagen que tiene una longitud mayor que la que puede soportar la cabecera del informe, la imagen se redimensiona automáticamente para ajustarse a

la cabecera; esto tiene aproximadamente una altura de 50 píxeles.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En el menú de navegación, pulse **Creación de una identidad visual**.
3. Pulse **Examinar** para examinar los archivos que están ubicados en el sistema.
4. Seleccione el archivo que contiene el logotipo que desea cargar. Pulse **Abrir**.
5. Pulse **Cargar imagen**.
6. Seleccione el logotipo que desea utilizar como valor predeterminado y pulse **Establecer imagen predeterminada**.

Grupos de informes

Los informes pueden ordenarse en grupos funcionales. Si se categorizan los informes por grupos, puede organizar y buscar informes de forma eficiente.

Por ejemplo, puede ver todos los informes relacionados con la conformidad con el estándar PCIDSS (Payment Card Industry Data Security Standard).

De forma predeterminada, la pestaña **Informes** muestra la lista de todos los informes, sin embargo, puede categorizar los informes en grupos tales como:

- Conformidad
- Ejecutivo
- Orígenes de registro
- Gestión de red
- Seguridad
- VoIP
- Otros

Cuando se crea un informe nuevo, se puede asignar el informe a un grupo existente o crear un grupo nuevo. Debe tener acceso administrativo para crear, editar o suprimir grupos.

Para obtener más información sobre los roles de usuario, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Creación de un grupo de informes

Puede crear grupos nuevos.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. Utilizando el árbol de navegación, seleccione el grupo en el que desea crear un nuevo grupo.
4. Pulse **Grupo nuevo**.
5. Escriba valores para los parámetros siguientes:
   - **Nombre**: Escriba el nombre del nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Opcional. Escriba una descripción para este grupo. La descripción puede tener un máximo 255 caracteres de longitud.

6. Pulse **Aceptar**.
7. Para cambiar la ubicación del nuevo grupo, pulse el nuevo grupo y arrastre la carpeta a la nueva ubicación en el árbol de navegación.
8. Cierre la ventana Grupos de informes.

Edición de un grupo

Puede editar un grupo de informes para cambiar el nombre o la descripción.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, seleccione el grupo que desea editar.
4. Pulse **Editar**.
5. Actualice los valores de los parámetros, según sea necesario:
   - **Nombre**: Escriba el nombre del nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
   - **Descripción**: Opcional. Escriba una descripción para este grupo. La descripción puede tener un máximo 255 caracteres de longitud. Este campo es opcional.
6. Pulse **Aceptar**.
7. Cierre la ventana Grupos de informes.

Compartición de grupos de informes

Puede compartir los grupos de informes con otros usuarios.

Antes de empezar

Debe tener permisos administrativos para compartir un grupo de informes con otros usuarios.

Para obtener más información sobre los permisos, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

No puede utilizar la herramienta de gestión de contenido (CMT) para compartir grupos de informes.

Para obtener más información sobre la herramienta CMT, consulte la publicación *Guía del administrador de IBM Security QRadar SIEM*.

Acerca de esta tarea

En la ventana Grupos de informes, los usuarios compartidos pueden ver el grupo de informes en la lista de informes.

Las actualizaciones que el usuario realiza en un grupo de informes compartido no afectan a la versión original del informe. Solamente el propietario puede realizar operaciones de supresión o modificación.

Se crea una copia del informe cuando un usuario duplica o ejecuta el informe compartido. El usuario puede editar o planificar informes en el grupo de informes copiado.

La opción de compartición de grupo altera temporalmente las opciones de compartición de informe anteriores que se configuraron para los informes del grupo.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. En la ventana **Informes**, pulse **Gestionar grupos**.
3. En la ventana **Grupos de informes**, seleccione el grupo de informes que desea compartir y pulse **Compartir**.
4. En la ventana **Opciones para compartir**, seleccione una de las opciones siguientes.

Opción	Descripción
Valor predeterminado (heredar del padre)	El grupo de informes no está compartido. Todos los grupos de informes copiados o todos los informes generados permanecen en la lista de informes del usuario. A cada informe del grupo se le asignan todas las opciones de compartición de informe padre que se hayan configurado.
Compartir con todos	El grupo de informes se comparte con todos los usuarios.
Compartir con usuarios que coinciden con los criterios siguientes...	El grupo de informes se comparte con usuarios determinados. **Roles de usuario** Efectúe una selección de la lista de roles de usuario y pulse el icono añadir (+). **Perfiles de seguridad** Efectúe una selección de la lista de perfiles de seguridad y pulse el icono añadir (+).

5. Pulse **Guardar**.

Resultados

En la ventana Grupos de informes, los usuarios compartidos ven el grupo de informes en la lista de informes. Los informes generados muestran el contenido en función del valor del perfil de seguridad.

Asignar un informe a un grupo

Puede utilizar la opción **Asignar grupos** para asignar un informe a otro grupo.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Seleccione el informe que desea asignar a un grupo.
3. En el recuadro de lista **Acciones**, seleccione **Asignar grupos**.
4. En la lista **Grupos de elementos**, seleccione el recuadro de selección del grupo que desee asignar a este informe.

5. Pulse **Asignar grupos**.

Copia de un informe en otro grupo

Utilice el icono **Copiar** para copiar un informe en uno o más grupos de informes.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, seleccione el informe que desea copiar.
4. Pulse **Copiar**.
5. Seleccione el grupo o los grupos en los que desea copiar el informe.
6. Pulse **Asignar grupos**.
7. Cierre la ventana Grupos de informes.

Eliminación de un informe

Utilice el icono **Eliminar** para eliminar un informe de un grupo.

Acerca de esta tarea

Cuando se elimina un informe de un grupo, el informe sigue existiendo en la pestaña **Informes**. El informe no se elimina del sistema.

Procedimiento

1. Pulse en la pestaña **Informes**.
2. Pulse **Gestionar grupos**.
3. En el árbol de navegación, vaya a la carpeta que contiene el informe que desea eliminar.
4. En la lista de grupos, seleccione el informe que desea eliminar.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.
7. Cierre la ventana Grupos de informes.

Avisos

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

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

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

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

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

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

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país donde tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no permiten la exclusión de garantías explícitas ni implícitas en determinadas transacciones, por lo que es posible que esta declaración no sea aplicable en su caso.

Esta información puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se realizan cambios en la información incluida en este documento; estos cambios se incorporarán en las nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

© Copyright IBM Corp. 2012, 2015

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

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

Los licenciatarios de este programa que deseen obtener información sobre él con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, se deben poner en contacto con:

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

Esta información puede estar disponible, de acuerdo con los términos y condiciones apropiados, incluido en algunos casos el pago de una tarifa.

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

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones se pueden haber realizado en sistemas en fase de desarrollo y no es seguro que esas mediciones serán las mismas en los sistemas disponibles habitualmente. Además, algunas mediciones se pueden haber calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para el entorno específico que utilicen.

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

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y sólo representan metas y objetivos.

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

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es totalmente casual.

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

Marcas registradas

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

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

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

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

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicio de terceros.

Consideraciones sobre la política de privacidad

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

Dependiendo de las configuraciones desplegadas, esta oferta de software puede utilizar cookies de sesión que recogen el ID de sesión de cada usuario con fines de gestión y autenticación de sesiones. Estos cookies se pueden inhabilitar, pero si se inhabilitan también se pierde la función que los cookies hacen posible.

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

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

Glosario

Este glosario proporciona términos y definiciones para el software de [nombre de producto] y los productos.

En este glosario se utilizan las siguientes referencias cruzadas:

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

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

A

activo Objeto gestionable que se despliega o se tiene previsto desplegar en un entorno operativo.

acumulador
Registro en el que un operando de una operación se puede almacenar y posteriormente sustituir por el resultado de esa operación.

agregación de enlaces
Agrupación de tarjetas de interfaz de red física, como cables o puertos, en una única interfaz de red lógica. La agregación de enlaces se utiliza para aumentar el ancho de banda y la disponibilidad de red.

alta disponibilidad (HA)
Relativo a un sistema en clúster que se vuelve a configurar cuando se producen anomalías de nodo o daemon para que las cargas de trabajo se puedan redistribuir en los nodos restantes del clúster.

anomalía
Desviación del comportamiento esperado de la red.

archivo de almacén de confianza
Archivo de base de datos de claves que contiene las claves públicas para una entidad de confianza.

archivo de claves
En seguridad de sistemas, archivo que contiene claves públicas, claves privadas, raíces de confianza y certificados.

ARP Véase Protocolo de resolución de direcciones.

ASN Véase número de sistema autónomo.

C

capa de red
En la arquitectura OSI, capa que proporciona servicios para establecer una vía de acceso entre sistemas abiertos con una calidad de servicio predecible.

captura de contenido
Proceso que captura una cantidad configurable de carga útil y, a continuación, almacena los datos en un registro de flujo.

CIDR Véase Classless Inter-Domain Routing.

cifrado
En seguridad de sistemas, proceso de transformación de datos a un formato ininteligible de manera que los datos originales no se puedan obtener o sólo se puedan obtener utilizando un proceso de decodificación.

Classless Inter-Domain Routing (CIDR)
Método para añadir direcciones de Protocolo Internet (IP) de clase C. Las direcciones se proporcionan a los proveedores de servicios de Internet (ISP) para que las utilicen sus clientes. Las direcciones CIDR reducen el tamaño de las tablas de direccionamiento y hacen que haya más direcciones IP disponibles en las organizaciones.

© Copyright IBM Corp. 2012, 2015

cliente
Programa de software o sistema que solicita servicios de un servidor.

clúster de alta disponibilidad
Configuración de alta disponibilidad que consta de un servidor primario y un servidor secundario.

código de autenticación de mensaje basado en hash (HMAC)
Código criptográfico que utiliza una función hash críptica y una clave secreta.

Common Vulnerability Scoring System (CVSS)
Sistema de puntuación mediante el cual se mide la gravedad de una vulnerabilidad.

compartimiento administrativo
Recurso de red que se oculta a los usuarios sin privilegios administrativos. Los compartimientos administrativos proporcionan a los administradores acceso a todos los recursos en un sistema de red.

comportamiento
Efectos observables de una operación o suceso, incluidos los resultados.

conjunto de referencia
Lista de elementos únicos que se derivan de sucesos o flujos en una red. Por ejemplo, una lista de direcciones IP o una lista de nombres de usuario.

consola
Estación de pantalla en la que un operador puede controlar y observar el funcionamiento del sistema.

contexto de host
Servicio que supervisa los componentes para asegurarse de que cada componente está funcionando como se esperaba.

conversión de direcciones de red (NAT)
En un cortafuegos, conversión de las direcciones seguras del protocolo de Internet (IP) en direcciones registradas externas. Esto permite las comunicaciones con redes externas pero enmascara las direcciones IP que se utilizan dentro del cortafuegos.

Correlación de QID
Taxonomía que identifica cada suceso exclusivo y correlaciona los sucesos con categorías de bajo nivel y alto nivel para determinar cómo se debe correlacionar y organizar un suceso.

correlación de referencia
Registro de datos de la correlación directa de una clave con un valor, por ejemplo un nombre de usuario con un ID global.

correlación de referencia de conjuntos
Registro de datos de una clave correlacionada con muchos valores. Por ejemplo, la correlación de una lista de usuarios privilegiados con un host.

correlación de referencia de correlaciones
Registro de datos de dos claves correlacionadas con muchos valores. Por ejemplo, la correlación de los bytes totales de una aplicación con una IP de origen.

credencial
Conjunto de información que otorga a un usuario o proceso determinados derechos de acceso.

credibilidad
Calificación numérica entre 0 y 10 que se utiliza para determinar la integridad de un suceso o un delito. La credibilidad aumenta a medida que varios orígenes informan el mismo suceso o delito.

CVSS Véase Common Vulnerability Scoring System.

D

datos de carga útil
Datos de aplicación contenidos en un flujo de IP, excluyendo la cabecera y la información administrativa.

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

destino de reenvío
Uno o varios sistemas de proveedores que reciben datos en bruto y normalizados de orígenes de registro y orígenes de flujo.

destino externo
Dispositivo que está fuera del sitio primario que recibe los datos de sucesos o flujos de un recopilador de sucesos.

DHCP Véase Protocolo de configuración dinámica de hosts.

dirección IP virtual de clúster
Dirección IP que se comparte entre el host primario o secundario y el clúster de alta disponibilidad.

dispositivo de exploración externa
Máquina que está conectada a la red para recopilar información de vulnerabilidad sobre los activos de la red.

DNS Véase Sistema de nombres de dominio.

DSM Véase Módulo de soporte de dispositivos.

E

exploración en tiempo real
Exploración de vulnerabilidad que genera datos de informe a partir de los resultados de exploración basándose en el nombre de sesión.

explorador
Programa de seguridad automático que busca vulnerabilidades de software dentro de las aplicaciones web.

extensión de origen de registro
Archivo XML que incluye todos los patrones de expresión regular necesarios para identificar y categorizar sucesos de la carga útil de sucesos.

F

falso positivo
Resultado de prueba clasificado como positivo (indicando que el sitio es vulnerable a ataques), que el usuario decide que en realidad es negativo (no una vulnerabilidad).

firma de aplicación
Conjunto exclusivo de características que se derivan mediante el examen de la carga útil de paquete y, a continuación, se utilizan para identificar una aplicación específica.

flujo Transmisión única de datos que pasan a través de un enlace durante una conversación.

flujo duplicado
Varias instancias de la misma transmisión de datos recibida de orígenes de flujo diferentes.

FQDN
Véase nombre de dominio completo.

FQNN
Véase nombre de red completo.

G

gravedad
Medida de la amenaza relativa que un origen plantea en un destino.

H

HA Véase alta disponibilidad.

HMAC
Véase Código de autenticación de mensaje basado en hash.

hoja En un árbol, entrada o nodo que no tiene hijos.

host primario de alta disponibilidad
Sistema principal que está conectado al clúster de alta disponibilidad.

host secundario de alta disponibilidad
Sistema en espera que está conectado al clúster de alta disponibilidad. El host secundario de alta disponibilidad asume la responsabilidad del host primario de alta disponibilidad si el host primario de alta disponibilidad falla.

I

ICMP Véase protocolo de mensajes de control de Internet.

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

IDS Véase sistema de detección de intrusiones.

informe
En gestión de consultas, datos formateados que se obtienen al ejecutar una consulta y aplicarle un formato.

interconexión de sistemas abiertos (OSI)
Interconexión de sistemas abiertos de acuerdo con los estándares de la ISO (International Organization for Standardization) para el intercambio de información.

interfaz enlazada
Véase agregación de enlaces.

intervalo de fusión
Intervalo en el que se empaquetan los sucesos. El empaquetado de sucesos se produce a intervalos de 10 segundos y empieza con el primer suceso que no coincide con ningún suceso de fusión simultánea. En el intervalo de fusión, los tres primeros sucesos coincidentes se empaquetan y envían al procesador de sucesos.

intervalo de informe
Intervalo de tiempo configurable al final del cual el procesador de sucesos debe enviar todos los datos de sucesos y flujos capturados a la consola.

IP Véase Protocolo Internet.

IPS Véase sistema de prevención de intrusiones.

ISP Véase proveedor de servicios de Internet.

J

jerarquía de red
Tipo de contenedor que es una colección jerárquica de objetos de red.

L

LAN Véase red de área local.

LDAP Véase Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)
Protocolo abierto que utiliza TCP/IP para proporcionar acceso a directorios que soportan un modelo X.500, y que no está sujeto a los requisitos de recursos del protocolo de acceso a directorios (DAP) X.500 más complejo. Por ejemplo, se puede utilizar LDAP para localizar personas, organizaciones y otros recursos en un directorio de Internet o de intranet.

Local a local (L2L)
Relativo al tráfico interno de una red local a otra red local.

Local a remoto (L2R)
Relativo al tráfico interno de una red local a otra red remota.

L2R Véase Local a remoto.

L2L Véase Local a local.

M

magistrado
Componente interno que analiza el tráfico de red y los sucesos de seguridad respecto a las reglas personalizadas definidas.

magnitud
Medida de la importancia relativa de un determinado delito. Magnitud es un valor ponderado calculado a partir de pertinencia, gravedad y credibilidad.

máscara de subred
Para la gestión de subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred de la parte de host de una dirección IP.

Módulo de soporte de dispositivo (DSM)
Archivo de configuración que analiza los sucesos recibidos de varios orígenes de registro y los convierte a un formato de taxonomía estándar que puede visualizarse como salida.

multidifusión IP
Transmisión de un datagrama de Protocolo Internet (IP) para establecer un conjunto de sistemas que forman un grupo de multidifusión único.

N

NAT Véase conversión de direcciones de red.

NetFlow
Protocolo de red Cisco que supervisa datos de flujo de tráfico de red. Los datos de NetFlow incluyen la información de cliente y servidor, los puertos que se utilizan y el número de bytes y paquetes que fluyen a través de los conmutadores y direccionadores conectados a una red. Los datos se envían a recopiladores de NetFlow donde se realiza el análisis de datos.

nombre de dominio completo (FQDN)
En comunicaciones de Internet, nombre de un sistema host que incluye todos los subnombres del nombre de dominio. Un ejemplo de nombre de dominio completo es rchland.vnet.ibm.com.

nombre de red completo (FQNN)
En una jerarquía de red, nombre de un objeto que incluye todos los

departamentos. Un ejemplo de un nombre de red completo es CompanyA.Department.Marketing.

número de sistema autónomo (ASN)
En TCP/IP, número asignado a un sistema autónomo por la misma autoridad central que asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automáticos distingan los sistemas autónomos.

O

objeto de hoja de base de datos
Nodo u objeto de terminal en una jerarquía de base de datos.

objeto de red
Componente de una jerarquía de red.

Open Source Vulnerability Database (OSVDB)
Creado por la comunidad de seguridad de red para la comunidad de seguridad de red, base de datos de código abierto que proporciona información técnica sobre las vulnerabilidades de seguridad de la red.

orden de análisis
Una definición de origen de registro en la que el usuario puede definir el orden de importancia para los orígenes de registro que comparten una dirección IP o un nombre de host comunes.

origen de registro
Equipo de seguridad o equipo de red desde el que se origina une registro de sucesos.

orígenes de flujo
Origen del que se captura el flujo. Un origen de flujo se clasifica como interno cuando el flujo procede del hardware instalado en un host gestionado o se clasifica como externo cuando el flujo se envía a un recopilador de flujo.

origen externo
Dispositivo que está fuera del sitio primario que reenvía datos normalizados a un recopilador de sucesos.

OSI Véase interconexión de sistemas abiertos.

OSVDB
Véase Open Source Vulnerability Database.

P

pasarela
Dispositivo o programa utilizado para conectar redes o sistemas con diferentes arquitecturas de red.

pertinencia
Medida de impacto relativo de un suceso, una categoría o un delito en la red.

protocolo
Conjunto de reglas que controlan la comunicación y la transferencia de datos entre dos o varios dispositivos o sistemas en una red de comunicaciones.

Protocolo de configuración dinámica de hosts (DHCP)
Protocolo de comunicación que se utiliza para gestionar de forma central información de configuración. Por ejemplo, DHCP asigna automáticamente direcciones IP a sistemas de una red.

Protocolo de control de transmisiones (TCP)
Protocolo de comunicación utilizado en Internet y en cualquier red que cumple los estándares de IETF (Internet Engineering Task Force) para el protocolo entre redes. TCP proporciona un protocolo fiable de host a host en las redes de comunicaciones de conmutación de paquetes y en los sistemas interconectados de dichas redes. Véase también Protocolo Internet.

Protocolo de Internet (IP)
Protocolo que direcciona los datos a través de una red o de redes interconectadas. Este protocolo actúa como intermediario entre las capas de protocolo más altas y la red física. Véase también Protocolo de control de transmisiones.

Protocolo de mensajes de control de Internet (ICMP)
Protocolo de Internet utilizado por una pasarela para comunicarse con un host de origen, por ejemplo, para informar de un error en un datagrama.

Protocolo de resolución de direcciones (ARP)
Protocolo que correlaciona dinámicamente una dirección IP con una dirección de adaptador de red en una red de área local.

Protocolo simple de gestión de red (SNMP)
Conjunto de protocolos para supervisar sistemas y dispositivos en redes complejas. La información sobre dispositivos gestionados se define y almacena en una MIB (Management Information Base - Base de información de gestión).

proveedor de servicios de Internet (ISP)
Organización que proporciona acceso a Internet.

punto de datos
Valor calculado de una medida en un punto en el tiempo.

punto final
Dirección de una API o un servicio en un entorno. Una API expone un punto final y al mismo tiempo invoca los puntos finales de otros servicios.

R

ráfaga Incremento brusco repentino en la tasa de sucesos o flujos entrantes de modo que se supera el límite de la tasa de sucesos o flujos con licencia.

recon Véase reconocimiento.

reconocimiento (recon)
Método mediante el cual se recopila información que pertenece a la identidad de los recursos de red. Se utilizan técnicas de exploración de red y otras para compilar una lista de sucesos de recursos de red a los que entonces se les asigna un nivel de gravedad.

red de área local (LAN)
Red que conecta varios dispositivos en un área limitada (como un único edificio o campus) y que se puede conectar a una red más grande.

Redirección de ARP
Método ARP para notificar al host si existe un problema en una red.

registro de flujo
Colección de registros de flujo.

regla Conjunto de sentencias condicionales que permiten a los sistemas identificar relaciones y ejecutar respuestas automáticas como corresponda.

regla de direccionamiento
Condición en la que, cuando los datos de sucesos satisfacen sus criterios, se ejecutan un conjunto de condiciones y el direccionamiento consecuente.

Remoto a local (R2L)
Tráfico externo desde una red remota a una red local.

Remoto a remoto (R2R)
Tráfico externo desde una red remota a otra red remota.

R2L Véase Remoto a local.

R2R Véase Remoto a remoto.

S

servidor whois
Servidor que se utiliza para recuperar información sobre un recurso de Internet registrado, por ejemplo nombres de dominio y asignaciones de dirección IP.

sistema activo
En un clúster de alta disponibilidad (HA), sistema que tiene todos los servicios en ejecución.

sistema de detección de intrusiones (IDS)
Software que detecta los intentos o los ataques satisfactorios en los recursos supervisados que forman parte de una red o un sistema host.

Sistema de nombres de dominio (DNS)
Sistema de base de datos distribuida que correlaciona nombres de dominio con direcciones IP.

sistema de prevención de intrusiones (IPS)
Sistema que intenta denegar la actividad potencialmente maliciosa. Los mecanismos de denegación pueden implicar el filtrado, seguimiento o establecimiento de límites de velocidad.

sistema en espera
Sistema que se activa automáticamente cuando el sistema activo falla. Si se ha habilitado la replicación de disco, replica los datos del sistema activo.

SNMP
Véase Protocolo simple de gestión de red.

SOAP Protocolo ligero basado en XML para intercambiar información en un entorno distribuido descentralizado. Se puede

utilizar SOAP para consultar y devolver información e invocar servicios en Internet.

sub-búsqueda
Función que permite realizar una consulta de búsqueda en un conjunto de resultados de búsqueda completada.

subred
Red que se divide en subgrupos independientes más pequeños, que siguen estando interconectados.

subred
Véase subred.

superflujo
Flujo único que consta de varios flujos con propiedades similares con el fin de aumentar la capacidad de proceso reduciendo las restricciones de almacenamiento.

T

tabla de referencia
Tabla donde el registro de datos correlaciona claves que tienen un tipo asignado con otras claves, que a continuación se correlacionan con un único valor.

TCP Véase Protocolo de control de transmisiones.

temporizador de renovación
Dispositivo interno que se desencadena manual o automáticamente a intervalos temporizados que actualiza los datos de actividad de red actuales.

V

violación
Acto que ignora o contraviene la política corporativa.

vista de sistema
Representación visual de hosts primarios y gestionados que componen un sistema.

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

Índice

© Copyright IBM Corp. 2012, 2015

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

X

Impreso en España