IBM Security QRadar SIEM
Versión 7.2.4

Guía de inicio

Nota

Antes de utilizar esta información y el producto al que sirve de complemento, lea la información contenida en la sección "Avisos" en la página 25.

Información sobre el producto

Este documento corresponde a IBM QRadar Security Intelligence Platform V7.2.4 y a todos los releases subsiguientes a menos sea reemplazado por una versión actualizada de este documento.

Contenido

Iniciación a QRadar SIEM

La Guía de iniciación de IBM Security QRadar SIEM describe conceptos básicos, el proceso de instalación y las tareas básicas que el usuario realiza en la interfaz de usuario.

A quién va dirigido este manual

Esta información está pensada para ser utilizada por los administradores de seguridad encargados de investigar y gestionar la seguridad de red. Para utilizar esta guía, debe tener conocimientos sobre la infraestructura de su red corporativa y tecnologías de gestión de redes.

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).

Contactar 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 Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de tecnologías de la información supone proteger sistemas e información mediante la prevención, detección y respuesta al acceso no autorizado realizado desde dentro o fuera de la empresa. El acceso no autorizado puede dar como resultado la alteración, destrucción, apropiación indebida o uso indebido de información, o puede producir daños o maltrato en los sistemas, incluida su utilización para atacar a otros sistemas. Ningún sistema o producto de tecnologías de la información se debe considerar completamente seguro ni ningún producto, servicio o medida de seguridad individual puede ser completamente efectivo para impedir el uso o acceso indebido. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un sistema de seguridad completo, que necesariamente abarca procedimientos operativos adicionales y que puede necesitar otros sistemas, productos o servicios para que sea el máximo de efectivo. IBM NO GARANTIZA QUE NINGÚN SISTEMA, PRODUCTO O SERVICIO SEA INMUNE O QUE CONFIERA INMUNIDAD A LA EMPRESA DEL USUARIO RESPECTO AL COMPORTAMIENTO MALICIOSO O ILEGAL DE TERCEROS.

Tenga en cuenta lo siguiente:

El uso de este Programa puede implicar a diversas leyes o normativas, incluidas las referentes a la privacidad, protección de datos, empleo, y comunicaciones y almacenamiento por medios electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. Cliente se compromete a utilizar este Programa de acuerdo con las leyes, normativas 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.

Capítulo 1. visión general de QRadar SIEM

IBM Security QRadar SIEM es una plataforma de gestión de seguridad de la red que proporciona conocimiento situacional y soporte de conformidad. QRadar SIEM utiliza una combinación de conocimiento de la red basado en flujos, correlación de sucesos de seguridad y evaluación de vulnerabilidades basada en activos.

Para comenzar, configure una instalación básica de QRadar SIEM, recopile datos de sucesos y de flujos, y cree informes.

Actividad de registro

En IBM Security QRadar SIEM, puede supervisar y mostrar sucesos de red en tiempo real o realizar búsquedas avanzadas.

El panel **Actividad de registro** muestra información de sucesos en forma de registros de un origen de registro, tal como un dispositivo cortafuegos o direccionador. En el panel **Actividad de registro**, puede realizar las tareas siguientes:

- Investigar datos de sucesos.
- Investigar en tiempo real registros de sucesos que se envían a QRadar SIEM.
- Buscar sucesos.
- Supervisar la actividad de registro mediante gráficos de serie temporal configurables.
- Identificar falsos positivos para ajustar QRadar SIEM.

Actividad de red

En IBM Security QRadar SIEM, puede investigar las sesiones de comunicación establecidas entre dos hosts.

El panel **Actividad de red** muestra información sobre cómo se transmite el tráfico de red, y qué se transmite, si la captura de contenido está habilitada. En el panel **Actividad de red**, puede realizar las tareas siguientes:

- Investigar en tiempo real los flujos que se envían a QRadar SIEM.
- Buscar flujos de red.
- Supervisar la actividad de red utilizando gráficos de serie temporal configurables.

Activos

QRadar SIEM crea automáticamente perfiles de activo mediante datos de flujo pasivo y datos de vulnerabilidad para descubrir servidores de red y hosts.

Los perfiles de activo proporcionan información sobre cada activo conocido existente en la red, incluidos los servicios que se están ejecutando. La información de perfil de activo se utiliza con fines de correlación, lo cual ayuda a reducir los falsos positivos.

En el panel Activos, puede realizar las tareas siguientes:

- Buscar activos.
- Ver todos los activos aprendidos.
- Ver información de identidad para activos aprendidos.
- Ajustar vulnerabilidades de falsos positivos.

Delitos

En IBM Security QRadar SIEM, puede investigar delitos para determinar la causa raíz de un problema de red.

En el panel **Delitos**, puede ver todos los delitos que se producen en la red y realizar las tareas siguientes:

- Investigar delitos, direcciones IP de origen y destino, comportamientos de red y anomalías de la red.
- Asociar sucesos y flujos procedentes de varias redes con una misma dirección IP de destino.
- Navegar por las diversas páginas del panel **Delitos** para investigar detalles de sucesos y flujos.
- Determinar los sucesos exclusivos que han provocado un delito.

Informes

En IBM Security QRadar SIEM, puede crear informes personalizados o utilizar informes predeterminados.

QRadar SIEM proporciona plantillas de informe predeterminadas que puede personalizar, cambiar de nombre y distribuir a los usuarios de QRadar SIEM.

Las plantillas de informe se agrupan en tipos de informe, tales como informes de conformidad, de dispositivo, ejecutivo y de red. Utilice el panel **Informes** para realizar las tareas siguientes:

- Crear, distribuir y gestionar informes para datos de QRadar SIEM.
- Crear informes personalizados para uso operativo y ejecutivo.
- Combinar información de seguridad y de red en un solo informe.
- Utilizar o editar plantillas de informe preinstaladas.
- Etiquetar informes con logotipos personalizados. El etiquetaje es beneficioso para distribuir informes a destinatarios diferentes.
- Establecer una planificación para crear informes personalizados y predeterminados.
- Publicar informes en diversos formatos.

Recopilación de datos

QRadar SIEM acepta información en diversos formatos procedente de una gran variedad de dispositivos, tal como sucesos de seguridad, tráfico de red y resultados de exploración.

Los datos recopilados se agrupan en tres secciones principales: información de suceso, de flujo y de evaluación de vulnerabilidades.

Recopilación de datos de suceso

Los orígenes de registro, tales como cortafuegos, direccionadores, servidores, y sistemas de detección de intrusiones o de prevención de intrusiones, generan sucesos.

La mayoría de los orígenes de registro envían información a QRadar SIEM mediante el protocolo syslog. QRadar SIEM también permite utilizar los protocolos siguientes:

- Protocolo simple de gestión de red (SNMP)
- Java™ Database Connectivity (JDBC)
- Security Device Event Exchange (SDEE)

De forma predeterminada, QRadar SIEM detecta automáticamente orígenes de registro después de haberse recibido un número determinado de archivos de registro identificables dentro de un intervalo de tiempo determinado. Una vez que se han detectado satisfactoriamente los orígenes de registro, QRadar SIEM añade el módulo DSM (Device Support Module) adecuado a la ventana Orígenes de registro del panel **Admin**.

Aunque la mayoría de los DSM incluyen la capacidad nativa para enviar archivos de registro, algunos DSM necesitan una configuración adicional, o un agente o ambas cosas para enviar archivos de registro. La configuración varía de un tipo a otro de DSM. Debe asegurarse de que los DSM están configurados para enviar archivos de registro en un formato que sea compatible con QRadar SIEM. Para obtener más información sobre la configuración de los DSM, consulte la *Guía de configuración de DSM*.

Determinados tipos de orígenes de registro, tales como direccionadores y conmutadores, no envían archivos de registro suficientes para que QRadar SIEM los detecte rápidamente y los añada a la lista Origen de registro. Puede añadir manualmente estos orígenes de registro. Para obtener más información sobre la adición manual de orígenes de registro, consulte el manual *Orígenes de registro, Guía del usuario*.

Los datos recopilados se agrupan en tres secciones principales: información de suceso, de flujo y de evaluación de vulnerabilidades.

Recopilación de datos de flujo

Los flujos proporcionan información sobre el tráfico de red y se pueden enviar a QRadar SIEM en diversos formatos, tales como archivos flowlog, NetFlow, J-Flow, sFlow y Packeteer.

QRadar SIEM puede aceptar varios formatos de flujo al mismo tiempo, lo cual le permite detectar amenazas y actividades que de otra forma no se detectarían si se dependiera estrictamente de sucesos para obtener información.

Los QRadar QFlow Collectors proporcionan detección completa del tráfico de red mediante aplicación sin importar el puerto en el que está trabajando la aplicación. Por ejemplo, si el protocolo Internet Relay Chat (IRC) se comunica en el puerto 7500/TCP, un QRadar QFlow Collector identifica el tráfico como IRC y proporciona captura de paquetes al comienzo de la conversación. NetFlow y J-Flow solamente le notifican de que existe tráfico en el puerto 7500/TCP, sin proporcionar ningún contexto respecto al protocolo utilizado.

Las ubicaciones de puerto duplicado habituales incluyen conmutadores core, DMZ, de servidor y de aplicación, y NetFlow proporciona información complementaria procedente de direccionadores y conmutadores.

Los QRadar QFlow Collectors están habilitados de forma predeterminada y necesitan que se conecte un puerto duplicado, SPAN o TAP a una interfaz disponible del dispositivo QRadar SIEM. El análisis de flujo comienza automáticamente cuando el puerto duplicado se conecta a una de las interfaces de red del dispositivo QRadar SIEM. De forma predeterminada, QRadar SIEM supervisa en la interfaz de gestión para detectar tráfico de NetFlow en el puerto 2055/UDP. Puede asignar puertos de NetFlow adicionales, si es necesario.

Información de evaluación de vulnerabilidades

QRadar SIEM puede importar información de evaluación de vulnerabilidades procedente de diversos exploradores externos.

La información de evaluación de vulnerabilidades ayuda a QRadar Risk Manager a identificar hosts activos, puertos abiertos y posibles vulnerabilidades.

QRadar Risk Manager utiliza información de evaluación de vulnerabilidades para clasificar la magnitud de los delitos producidos en la red.

Dependiendo del tipo de explorador de evaluación de vulnerabilidades, QRadar Risk Manager puede importar resultados de exploración procedentes del servidor de exploración o iniciar una exploración de forma remota.

Reglas de QRadar SIEM

Las reglas ejecutan pruebas para sucesos, flujos o delitos, y cuando se cumplen todas las condiciones de una prueba, la regla genera una respuesta.

QRadar SIEM incluye reglas que detectan una amplia gama de actividades, tales como denegaciones de cortafuegos excesivas, múltiples intentos fallidos de inicio de sesión y una posible actividad de red de robots. Para obtener más información sobre reglas, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

La lista siguiente describe las dos categorías de reglas:

- Las reglas personalizadas ejecutan pruebas para sucesos, flujos y ataques para detectar actividad inusual en la red.
- Las reglas de detección de anomalías ejecutan pruebas sobre los resultados de búsquedas guardadas de flujos o sucesos para detectar patrones de tráfico inusuales en la red.

Importante: Un usuario con acceso no administrativo puede crear reglas para áreas de la red a las que tenga acceso. Es necesario tener permisos de rol apropiados para gestionar reglas. Para obtener información sobre permisos de rol de usuario , consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Navegadores web soportados

Para que las funciones de los productos IBM Security QRadar trabajen debidamente, debe utilizar un navegador web soportado.

Cuando accede al sistema de QRadar, se le solicita 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 1. Navegadores web soportados para productos QRadar

Navegador web	**Versión soportada**
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, con la modalidad de documento y la modalidad de navegador habilitadas	9.0 10
Google Chrome	La versión actual de los productos IBM Security QRadar V7.2.4 de acuerdo con la fecha de publicación

Capítulo 2. Inicio del despliegue de QRadar SIEM

Antes de poder evaluar las capacidades clave de IBM Security QRadar SIEM, un administrador debe desplegar QRadar SIEM.

Para desplegar QRadar SIEM, los administradores deben realizar las tareas siguientes:

- Instalar el dispositivo QRadar SIEM.
- Configurar la instalación de QRadar SIEM.
- Recopilar datos de suceso, de flujo y de evaluación de vulnerabilidades.
- Ajustar la instalación de QRadar SIEM.

Instalar el dispositivo QRadar SIEM

Los administradores deben instalar el dispositivo QRadar SIEM para habilitar el acceso a la interfaz de usuario.

Antes de empezar

Antes de instalar el dispositivo de evaluación QRadar SIEM, compruebe que tiene lo siguiente:

- Espacio para un dispositivo de dos unidades.
- Rieles y estanterías de bastidor (montado).
- Opcional. Un teclado USB y un monitor VGA estándar para acceder a la consola.

Procedimiento

1. Conecte la interfaz de red de gestión al puerto etiquetado como Ethernet 1.
2. Enchufe las conexiones de alimentación dedicadas a la parte posterior del dispositivo.
3. Si necesita acceder a la consola, conecte el teclado USB y el monitor VGA estándar.
4. Si existe un panel frontal en el dispositivo, extraiga el panel presionando en las pestañas situadas a ambos lados para separar el panel del dispositivo.
5. Encienda el dispositivo.

El dispositivo QRadar SIEM

El dispositivo de evaluación QRadar SIEM es un servidor de montaje en bastidor que consta de dos unidades. No se proporcionan rieles ni estanterías de bastidor con el equipo de evaluación.

El dispositivo QRadar SIEM incluye cuatro interfaces de red. Para esta evaluación, utilice como interfaz de gestión la interfaz que está etiquetada como Ethernet 1.

Puede utilizar las tres interfaces de supervisión restantes para la recopilación de flujo. QRadar QFlow Collector proporciona análisis completo de la aplicación de la red y puede realizar capturas de paquetes al comienzo de cada conversación. Dependiendo del dispositivo QRadar SIEM, el análisis de flujo comienza automáticamente cuando un puerto SPAN (Switch Port Analyzer) o TAP (Test

Access Point) se conecta a una interfaz cualquiera que no sea Ethernet 1. Pueden ser necesarios pasos adicionales para habilitar el componente QRadar QFlow Collector contenido en QRadar SIEM.

Para obtener más información, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Restricción: El dispositivo de evaluación QRadar SIEM tiene un límite de 50 Mbps para el análisis de flujo. Asegúrese de que el tráfico total en las interfaces de supervisión para la recopilación de flujo no sobrepase los 50 Mbps.

Configuración de QRadar SIEM

Configure QRadar SIEM para revisar la jerarquía de la red y personalizar las actualizaciones automáticas.

Procedimiento

1. Compruebe que las aplicaciones siguientes están instaladas en todos los sistemas que utiliza para acceder a la interfaz de usuario del producto QRadar
   - Java Runtime Environment (JRE) versión 1.7 o IBM 64-bit Runtime Environment for Java V7.0
   - Adobe Flash versión 10.x
2. Asegúrese de que está utilizando un navegador web soportado. Consulte "Navegadores web soportados" en la página 4.
3. Si utiliza Internet Explorer, habilite la modalidad de documento y la modalidad de navegador.
   a. En su navegador web de Internet Explorer, pulse F12 para abrir la ventana Herramientas de desarrollador.
   b. Pulse **Modalidad de navegador** y seleccione la versión de su navegador web.
   c. Pulse **Modalidad de documento** y seleccione **Internet Explorer 7.0 Standards**.
4. Inicie una sesión en la interfaz de usuario de QRadar SIEM escribiendo el URL siguiente:

   https://<dirección IP>

   Donde <dirección IP> es la dirección IP de la QRadar SIEM Console.

Jerarquía de red

Puede ver áreas diferentes de la red que está organizada por función de negocio y priorizar la información de amenazas y política de acuerdo con el riesgo del valor de negocio.

QRadar SIEM utiliza la jerarquía de red para realizar las tareas siguientes:

- Conocer el tráfico de red y ver la actividad de red.
- Supervisar grupos lógicos o servicios determinados de la red, tales como marketing, DMZ o VoIP.
- Supervisar el tráfico y analizar el comportamiento de cada grupo y host existente en el grupo.
- Determinar e identificar hosts locales y remotos.

Para fines de evaluación, se incluye una jerarquía de red predeterminada que contiene grupos lógicos predefinidos. Revise la jerarquía de red para comprobar su

exactitud e integridad. Si su entorno operativo incluye rangos de red que no aparecen en la jerarquía de red preconfigurada, debe añadirlos manualmente.

No es necesario que los objetos que están definidos en la jerarquía de red estén físicamente en el entorno. Todos los rangos de red lógica pertenecientes a la infraestructura se deben definir como objetos de red.

Nota: Si el sistema no incluye una jerarquía de red completa, utilice el panel **Admin** para crear una jerarquía que sea específica del entorno.

Para obtener más información, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Revisar la jerarquía de la red

Puede revisar la jerarquía de la red.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Jerarquía de red**.
4. En la lista **Gestionar grupo: Superior**, pulse **Servidores de conformidad con la normativa**.

   Si la jerarquía de la red no incluye un servidor de conformidad con la normativa, puede utilizar el componente Correo para el resto de este procedimiento.
5. Pulse el icono **Editar este objeto**.
6. Para añadir servidores de conformidad:
   a. En el campo **IP/CIDR(s)**, escriba la dirección IP o rango de CIDR de los servidores de conformidad.
   b. Pulse **Añadir**.
   c. Repita los pasos anteriores para todos los servidores de conformidad.
   d. Pulse **Guardar**.
   e. Repita este proceso para cualquier otra red que desee editar.
7. En el menú del panel **Admin**, pulse **Desplegar cambios**.

   Puede actualizar automáticamente o manualmente los archivos de configuración con la información de seguridad de red más reciente. QRadar SIEM utiliza archivos de configuración del sistema para proporcionar caracterizaciones útiles de los flujos de datos de red.

Actualizaciones automáticas

La consola de QRadar SIEM debe estar conectada a Internet para recibir actualizaciones. Si la consola no está conectada a Internet, debe configurar un servidor de actualización interno.

Para obtener información sobre la configuración de un servidor de actualización automática, consulte el manual *IBM Security QRadar SIEM Users Guide*.

Mediante QRadar SIEM, puede sustituir los archivos de configuración existentes o integrar los archivos actualizados en los archivos existentes.

Puede descargar actualizaciones de software desde el sitio web siguiente:

http://www.ibm.com/support/fixcentral/

Los archivos de actualización pueden incluir las actualizaciones siguientes:

- Actualizaciones de configuración, que incluyen cambios en el archivo de configuración, vulnerabilidad, correlación QID, y actualizaciones de información sobre amenazas de seguridad.
- Actualizaciones de DSM, que incluyen correcciones para problemas de análisis, cambios de escáner y actualizaciones de protocolo.
- Actualizaciones importantes, que incluyen elementos tales como archivos JAR actualizados.
- Actualizaciones secundarias, que incluyen elementos tales como contenido adicional de la ayuda en línea o scripts actualizados.

Configurar valores de actualización automática

Puede personalizar la frecuencia de las actualizaciones de QRadar SIEM, los tipos de actualización, la configuración del servidor y valores de copia de seguridad.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Actualización automática**.
4. En el panel de navegación, pulse **Cambiar valores**.
5. En el panel **Planificación de actualizaciones automáticas**, acepte los parámetros predeterminados.
6. En el panel **Tipos de actualización**, defina los parámetros siguientes:
   a. En el cuadro de lista **Actualizaciones de configuración**, seleccione **Actualización automática**.
   b. Acepte los valores predeterminados para los parámetros siguientes:
      - Actualizaciones de DSM, Explorador, Protocolo.
      - Actualizaciones principales.
      - Actualizaciones secundarias.
7. Deseleccione la casilla **Despliegue automático**.

   De forma predeterminada, la casilla está seleccionada. Cuando la casilla no está seleccionada, el panel **Panel de control** muestra una notificación del sistema para indicar que el usuario debe desplegar los cambios una vez instaladas las actualizaciones.
8. Pulse la pestaña **Avanzado**.
9. En el panel **Configuración de servidor**, acepte los parámetros predeterminados.
10. En el panel **Otros valores**, acepte los parámetros predeterminados.
11. Pulse **Guardar** y cierre la ventana Actualizaciones.
12. En la barra de herramientas, pulse **Desplegar cambios**.

Recopilar sucesos

Puede recopilar sucesos para investigar los archivos de registro que se envían en tiempo real a QRadar SIEM.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Orígenes de datos**.
3. Pulse el icono **Orígenes de registro**.
4. Repase la lista de orígenes de registro y haga los cambios necesarios en ellos.

   Para obtener información sobre cómo configurar orígenes de registro, consulte el manual *Orígenes de registro, Guía del usuario*.
5. Cierre la ventana Orígenes de registro.
6. En el menú del panel **Admin**, pulse **Desplegar cambios**.

Recopilar flujos

Puede recopilar flujos para investigar las sesiones de comunicación de red entre hosts.

Para obtener más información sobre cómo habilitar flujos en dispositivos de red externos, tales como conmutadores y direccionadores, consulte la documentación del proveedor.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos** > **Flujos**.
3. Pulse el icono **Orígenes de flujos**.
4. Repase la lista de orígenes de flujos y haga los cambios necesarios en ellos.

   Para obtener más información sobre cómo configurar orígenes de flujos, consulte el manual *IBM Security QRadar SIEM Administration Guide*.
5. Cierre la ventana Orígenes de flujos.
6. En el menú del panel **Admin**, pulse **Desplegar cambios**.

Importar información de evaluación de vulnerabilidades

Puede importar información de evaluación de vulnerabilidades para identificar hosts activos, puertos abiertos y posibles vulnerabilidades.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos** > **Vulnerabilidad**.
3. Pulse el icono **Exploradores de evaluación de vulnerabilidades**.
4. En la barra de herramientas, pulse **Añadir**.
5. Escriba valores para los parámetros.

   Los parámetros dependen del tipo de explorador que desee añadir. Para obtener más información, consulte el manual *Evaluación de vulnerabilidades, Guía de configuración*.

   Importante: El rango de CIDR especifica qué redes QRadar SIEM integra en los resultados de la exploración. Por ejemplo, si desea realizar una exploración para la red 192.168.0.0/16 y especifica 192.168.1.0/24 como rango de CIDR, solamente se integran los resultados del rango 192.168.1.0/24.
6. Pulse **Guardar**.
7. En el menú del panel **Admin**, pulse **Desplegar cambios**.
8. Pulse el icono **Planificar exploradores de evaluación de vulnerabilidades**.

9. Pulse **Añadir**.
10. Especifique los criterios para la frecuencia con la que desee que se realice la exploración.

    Dependiendo del tipo de exploración, esto incluye la frecuencia con la que QRadar SIEM importa resultados de exploración o inicia una nueva exploración. También debe especificar los puertos que se deben incluir en los resultados de la exploración.
11. Pulse **Guardar**.

Ajuste de QRadar SIEM

Puede ajustar QRadar SIEM de acuerdo con las necesidades del entorno de trabajo.

Antes de ajustar QRadar SIEM, espere un día para permitir que QRadar SIEM detecte los servidores de la red, almacene sucesos y flujos, y cree delitos basados en reglas existentes.

Los administradores pueden realizar las tareas de ajuste siguientes:

- Optimizar las búsquedas de sucesos y de carga útil de flujo habilitando un índice de carga útil en la propiedad **Filtro rápido** de **Actividad de registro** y **Actividad de red**.
- Añadir automáticamente o manualmente servidores a componentes básicos para proporcionar un despliegue inicial más rápido y un ajuste más fácil.
- Crear o modificar reglas personalizadas y reglas de detección de anomalías para configurar respuestas a condiciones de suceso, flujo o delito.
- Asegurarse de que cada host de la red crea delitos de acuerdo con las reglas más actuales, servidores descubiertos y jerarquía de la red.

Indexación de carga útil

Utilice la función **Filtro rápido**, existente en los paneles **Actividad de registro** y **Actividad de red**, para buscar cargas útiles de suceso y de flujo.

Para optimizar el **Filtro rápido**, puede habilitar la indexación de carga útil en la propiedad **Filtro rápido**.

El habilitar la indexación de carga útil puede disminuir el rendimiento del sistema. Supervise las estadísticas de índice después de habilitar la indexación de carga útil en la propiedad **Filtro rápido**.

Para obtener más información sobre la gestión y las estadísticas de índice, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Habilitar la indexación de carga útil

Puede optimizar las búsquedas de sucesos y de carga útil de flujo habilitando un índice de carga útil en la propiedad **Filtro rápido** de **Actividad de registro** y **Actividad de red**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión de índices**.
4. En el campo **Búsqueda rápida**, escriba **Filtro rápido**.

5. Pulse la propiedad de **Filtro rápido** que desee indexar.
6. Pulse **Habilitar índice**.
7. Pulse **Guardar**.
8. Pulse **Aceptar**.
9. Opcional: Para inhabilitar un índice de carga útil, seleccione una de las opciones siguientes:
   - Pulse **Inhabilitar índice**.
   - Pulse con el botón derecho en una propiedad y seleccione **Inhabilitar índice** en el menú.

Qué hacer a continuación

Para obtener información detallada sobre los parámetros que se muestran en la ventana Gestión de índices, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Servidores y componentes básicos

QRadar SIEM descubre y clasifica automáticamente servidores existentes en la red, lo cual permite un despliegue inicial más rápido y un ajuste más fácil cuando se producen cambios en la red.

Para asegurarse de que se aplican las reglas apropiadas al tipo de servidor, puede añadir dispositivos individuales o rangos completos de direcciones de dispositivos. Puede añadir manualmente tipos de servidor, que no se ajustan a protocolos exclusivos, a su correspondiente componente básico de definición de host. Por ejemplo, añadir los tipos de servidor siguientes a componentes básicos reduce la necesidad de realizar ajustes adicionales por falsos positivos:

- Añada servidores de gestión de red al componente básico **BB:HostDefinition: Servidores de gestión de red**.
- Añada servidores proxy al componente básico **BB:HostDefinition: Servidores proxy**.
- Añada servidores de definición de virus y de actualización de Windows al componente básico **BB:HostDefinition: Servidores de definición de virus y otros servidores de actualización**.
- Añada exploradores de evaluación de vulnerabilidades al componente básico **BB-HostDefinition: IP de origen de explorador de evaluación de vulnerabilidades**.

La función Descubrimiento de servidores utiliza la base de datos de perfiles de activo para descubrir varios tipos de servidores en la red. La función Descubrimiento de servidores lista automáticamente servidores descubiertos y el usuario puede seleccionar qué servidores desea incluir en componentes básicos.

Para obtener más información sobre el descubrimiento de servidores, consulte el manual *IBM Security QRadar SIEM Administration Guide*.

Mediante la utilización de componentes básicos, puede reutilizar pruebas de regla determinadas en otras reglas. Puede reducir el número de falsos positivos utilizando componentes básicos para ajustar QRadar SIEM y habilitar reglas de correlación adicionales.

Añadir servidores a componentes básicos automáticamente

Puede añadir automáticamente servidores a componentes básicos.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Descubrimiento de servidores**.
3. En la lista **Tipo de servidor**, seleccione el tipo de servidor que desee descubrir.

   Deje los parámetros restantes como valor predeterminado.
4. Pulse **Descubrir servidores**.
5. En el panel Servidores coincidentes, seleccione la casilla correspondiente a los servidores que desee asignar el rol de servidor.
6. Pulse **Aprobar servidores seleccionados**.

   Recuerde: Puede pulsar con el botón derecho del ratón en una dirección IP o nombre de host cualquiera para ver información de resolución de DNS.

Añadir servidores manualmente a componentes básicos

Si un servidor no se detecta automáticamente, puede añadir manualmente el servidor a su componente correspondiente de Definición de host.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. En el panel de navegación, pulse **Reglas**.
3. En la lista **Visualizar**, seleccione **Componentes básicos**.
4. En la lista **Grupo**, seleccione **Definiciones de host**.

   El nombre del componente básico corresponde al tipo de servidor. Por ejemplo, **BB:HostDefinition: Servidores proxy** corresponde a todos los servidores proxy del entorno.
5. Para añadir manualmente un host o red, haga una doble pulsación en el correspondiente componente básico de definición de host que sea apropiado para el entorno utilizado.
6. En el campo **Componente básico**, pulse el valor subrayado que aparece a continuación de la frase **cuando el IP de origen o destino es uno de los siguientes**.
7. En el campo **Escriba una dirección IP o CIDR**, escriba los nombres de host o rangos de direcciones IP que desee asignar al componente básico.
8. Pulse **Añadir**.
9. Pulse **Enviar**.
10. Pulse **Finalizar**.
11. Repita estos pasos para cada tipo de servidor que desee añadir.

Configurar reglas

En el panel **Actividad de registro**, **Actividad de red** y **Delitos**, puede configurar reglas o componentes básicos.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Haga una doble pulsación en el delito que desee investigar.
3. Pulse **Visualizar** > **Reglas**.

4. Haga una doble pulsación en una regla.

   Puede ajustar más las reglas. Para obtener más información sobre el ajuste de reglas, consulte el manual *IBM Security QRadar SIEM Administration Guide*
5. Cierre el asistente Reglas.
6. En la página Reglas, pulse **Acciones**.
7. Opcional: Si desea impedir que el delito se elimine de la base de datos una vez transcurrido el período de retención de delito, seleccione **Proteger delito**.
8. Opcional: Si desea asignar el delito a un usuario de QRadar SIEM, seleccione **Asignar**.

Conceptos relacionados:

"Reglas de QRadar SIEM" en la página 4
Las reglas ejecutan pruebas para sucesos, flujos o delitos, y cuando se cumplen todas las condiciones de una prueba, la regla genera una respuesta.

Limpieza del modelo SIM

Depure el modelo SIEM para asegurarse de que cada host crea delitos de acuerdo con las reglas más actuales, servidores descubiertos y jerarquía de la red.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En la barra de herramientas, seleccione **Avanzado** > **Limpiar modelo SIM**.
3. Pulse la opción necesaria:

   `Limpieza parcial` para establecer los delitos en inactivos.

   `Limpieza parcial` con la opción `Desactivar todos los delitos` para cerrar todos los delitos.

   `Limpieza total` para borrar todas las entradas.
4. Pulse **¿Está seguro de que desea restablecer el modelo de datos?**.
5. Pulse **Continuar**.
6. Después de que finalice el proceso de restablecimiento de SIM, renueve el navegador.

Resultados

Cuando limpia el modelo SIM, se cierran todos los delitos existentes. La limpieza del modelo SIM no afecta a los sucesos y flujos existentes.

Capítulo 3. Iniciación a QRadar SIEM

Para comenzar a utilizar IBM Security QRadar SIEM, debe obtener conocimientos sobre la búsqueda de sucesos, flujos y activos. También debe aprender a investigar delitos y crear informes.

Por ejemplo, puede buscar información utilizando búsquedas guardadas predeterminadas en los paneles **Actividad de registro** y **Actividad de red**. También puede crear y guardar sus propias búsquedas personalizadas.

Los administradores pueden realizar las tareas siguientes:

- Buscar datos de suceso utilizando criterios específicos y mostrar los sucesos que coinciden con los criterios de búsqueda en una lista de resultados. Seleccionar, organizar y agrupar las columnas de datos de suceso.
- Supervisar e investigar de forma gráfica datos de flujo en tiempo real, o realizar búsquedas avanzadas para filtrar los flujos visualizados. Ver información de flujo para determinar cómo se transmite el tráfico de red y qué tráfico se transmite.
- Ver todos los activos aprendidos o buscar activos específicos en el entorno.
- Investigar delitos, direcciones IP de origen y destino, comportamientos de red y anomalías de la red.
- Editar, crear, planificar y distribuir informes predeterminados o personalizados.

Buscar sucesos

Puede buscar todos los sucesos de autenticación que QRadar SIEM ha recibido durante las últimas 6 horas.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
3. En el panel Rango de tiempo, defina el rango de tiempo para la búsqueda de sucesos:
   a. Pulse **Reciente**.
   b. En la lista **Reciente**, seleccione **Últimas 6 horas**.
4. En el panel Parámetros de búsqueda, defina los parámetros de búsqueda:
   a. En la primera lista, seleccione **Categoría**.
   b. En la segunda lista, seleccione **Igual que**.
   c. En la lista **Categoría de nivel superior**, seleccione **Autenticación**.
   d. En la lista **Categoría de nivel inferior**, acepte el valor predeterminado, **Cualquiera**.
   e. Pulse **Añadir filtro**.
5. En el panel Definición de columna, seleccione **Nombre de suceso** en la lista **Visualizar**.
6. Pulse **Buscar**.

Guardar criterios de búsqueda de sucesos

Puede guardar criterios especificados de búsqueda de sucesos para utilizarlos más adelante.

Procedimiento

1. Pulse la pestaña **Actividad de registro**.
2. En la barra de herramientas, pulse **Guardar criterios**.
3. En el campo **Nombre de búsqueda**, escriba **Búsqueda de ejemplo 1**.
4. En el panel Opciones de intervalo de tiempo, pulse **Reciente**.
5. En la lista **Reciente**, seleccione **Últimas 6 horas**.
6. Pulse **Incluir en Búsquedas rápidas**.
7. Pulse **Incluir en Panel de control**.

   Si **Incluir en Panel de control** no aparece, pulse **Buscar** > **Editar búsqueda** para verificar que ha seleccionado **Nombre de suceso** en el panel Definición de columna.
8. Pulse **Aceptar**.

Qué hacer a continuación

Configure un gráfico de serie temporal. Para obtener más información, consulte "Configurar un gráfico de serie temporal".

Configurar un gráfico de serie temporal

Puede visualizar gráficos interactivos de serie temporal para representar los registros que coinciden con una búsqueda de intervalo de tiempo determinado.

Procedimiento

1. En la barra de título del gráfico, pulse el icono **Configurar**.
2. En la lista **Valor para gráfico**, seleccione **IP de destino (recuento exclusivo)**.
3. En la lista **Tipo de gráfico**, seleccione **Serie temporal**.
4. Pulse **Capturar datos de serie temporal**.
5. Pulse **Guardar**.
6. Pulse **Actualizar detalles**.
7. Filtre los resultados de la búsqueda:
   a. Pulse con el botón derecho en el suceso que desee filtrar.
   b. Pulse **Filtrar por nombre de suceso es <Nombre de suceso>**.
8. Para visualizar la lista de sucesos que está agrupada por el nombre de usuario, seleccione **Nombre de usuario** en la lista **Visualizar**.
9. Verifique que la búsqueda es visible en el panel **Panel de control**:
   a. Pulse la pestaña **Panel de control**.
   b. Pulse el icono **Panel de control nuevo**.
   c. En el campo **Nombre**, escriba **Panel de control personalizado de ejemplo**.
   d. Pulse **Aceptar**.
   e. En la lista **Añadir elemento**, seleccione **Actividad de registro** > **Búsquedas de sucesos** > **Búsqueda de ejemplo 1**.

Resultados

El Panel de control mostrará los resultados de la búsqueda de sucesos guardada.

Buscar flujos

Puede buscar, supervisar e investigar datos de flujo en tiempo real.

También puede realizar búsquedas avanzadas para filtrar los flujos visualizados. Examine información de flujo para determinar cómo se transmite el tráfico de red y qué tráfico se transmite.

Procedimiento

1. Pulse la pestaña **Actividad de red**.
2. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
3. En el panel Rango de tiempo, defina el rango de tiempo para la búsqueda de flujos.
   a. Pulse **Reciente**.
   b. En la lista **Reciente**, seleccione **Últimas 6 horas**.
4. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
   a. En la primera lista, seleccione **Dirección de flujo**.
   b. En la segunda lista, seleccione **Igual que**.
   c. En la tercera lista, seleccione **R2L**.
   d. Pulse **Añadir filtro**.
5. En la lista **Visualizar** del panel Definición de columna, seleccione **Aplicación**.
6. Pulse **Buscar**.

Resultados

Se mostrarán todos los flujos cuya dirección de flujo sea de remoto a local (R2L) correspondientes a las 6 últimas horas y ordenados de acuerdo con el campo **Nombre de aplicación**.

Guardar criterios de búsqueda de flujos

Puede guardar criterios especificados de búsqueda de flujos para utilizarlos más adelante.

Procedimiento

1. En la barra de herramientas del panel **Actividad de red**, pulse **Guardar criterios**.
2. En el campo **Nombre de búsqueda**, escriba el nombre **Búsqueda de ejemplo 2**.
3. En la lista **Reciente**, seleccione **Últimas 6 horas**.
4. Pulse **Incluir en Panel de control** e **Incluir en Búsquedas rápidas**.
5. Pulse **Aceptar**.

Qué hacer a continuación

Cree un elemento de panel de control. Para obtener más información, consulte “Crear un elemento de panel de control” en la página 20.

Crear un elemento de panel de control

Puede crear un elemento de panel de control utilizando criterios guardados de búsqueda de flujos.

Procedimiento

1. En la barra de herramientas de **Actividad de red**, seleccione **Búsquedas rápidas** > **Búsqueda de ejemplo 2**.
2. Verifique que la búsqueda seleccionada está incluida en el Panel de control:
   a. Pulse la pestaña **Panel de control**.
   b. En la lista **Mostrar panel de control**, seleccione **Panel de control personalizado de ejemplo**.
   c. En la lista **Añadir elemento**, seleccione **Búsquedas de flujos** > **Búsqueda de ejemplo 2**.
3. Configure el gráfico del panel de control:
   a. Pulse el icono **Valores**.
   b. Mediante las opciones de configuración, puede cambiar el valor que aparece representado en el gráfico, cuántos objetos se muestran, el tipo de gráfico o el rango de tiempo mostrado en el gráfico.
4. Para investigar flujos que se muestran actualmente en el gráfico, pulse **Ver en actividad de red**.

Resultados

La página Actividad de red mostrará los resultados que coinciden con los parámetros del gráfico de serie temporal. Para obtener más información sobre los gráficos de serie temporal, consulte el manual *IBM Security QRadar SIEM Users Guide*.

Buscar activos

Cuando accede al panel **Activos**, aparece la página Activo, que muestra todos los activos descubiertos en la red. Para refinar esta lista, puede definir parámetros de búsqueda para mostrar sólo los perfiles de activo que desee investigar.

Acerca de esta tarea

Utilice la función de búsqueda para buscar perfiles de host, activos e información de identidad. La información de identidad proporciona más detalles, tales como información de DNS, inicios de sesión de usuario y direcciones MAC de la red.

Por ejemplo:

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el panel de navegación, pulse **Perfiles de activo**.
3. En la barra de herramientas, seleccione **Buscar** > **Búsqueda nueva**.
4. Si desea cargar una búsqueda guardada, siga los pasos siguientes:
   a. Opcional: En la lista **Grupo**, seleccione el grupo de búsqueda de activos que desee mostrar en la lista **Búsquedas guardadas disponibles**.
   b. Elija una de las opciones siguientes:

- En el campo **Escriba la búsqueda guardada o seleccione en la lista**, escriba el nombre de la búsqueda que desee cargar.
- En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desee cargar.

c. Pulse **Cargar**.

5. En el panel Parámetros de búsqueda, defina los criterios de búsqueda:
   a. En la primera lista, seleccione el parámetro de activo para el que desee buscar. Por ejemplo, **Nombre de host**, **Clasificación de riesgo de vulnerabilidad** o **Propietario técnico**.
   b. En la segunda lista, seleccione el modificador que desee utilizar para la búsqueda.
   c. En el campo **Entrada**, escriba información específica que esté 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.
6. Pulse **Buscar**.

Ejemplo

Ha recibido una notificación de que el ID de CVE: CVE-2010-000 es objeto de un ataque. Para determinar si algún host desplegado es vulnerable a este ataque, siga los pasos siguientes:

1. En la lista de parámetros de búsqueda, seleccione **Referencia externa de vulnerabilidad**.
2. Seleccione **CVE**.
3. Escriba 2010-000 para ver una lista de todos los hosts que son vulnerables a ese ID de CVE específico.

Para obtener más información, consulte el sitio web de Open Source Vulnerability Database (*http://osvdb.org/*) y el sitio web de National Vulnerability Database (*http://nvd.nist.gov/*).

Investigaciones de delitos

En el panel **Delitos**, puede investigar delitos, direcciones IP de origen y destino, comportamientos de red, y anomalías en la red.

QRadar SIEM puede asociar sucesos y flujos con direcciones IP de destino situadas en varias redes del mismo delito, y finalmente el mismo incidente de red. Esto le permite investigar de forma efectiva cada delito en la red.

Ver delitos

Puede investigar cada delito producido en la red.

Por ejemplo, puede investigar delitos, direcciones IP de origen y de destino, comportamientos de red y anomalías de la red.

Procedimiento

1. Pulse la pestaña **Delitos**.
2. Haga una doble pulsación en el delito que desee investigar.
3. En la barra de herramientas, seleccione **Visualizar** > **Destinos**.

Puede investigar cada destino para determinar si la seguridad del destino está comprometida o muestra un comportamiento sospechoso.

4. En la barra de herramientas, pulse **Sucesos**.

Resultados

La ventana Lista de sucesos mostrará todos los sucesos que están asociados al delito. Puede buscar, ordenar y filtrar los sucesos.

Ejemplo: habilitar las plantillas de informe PCI

Utilice el panel **Informes** para habilitar, inhabilitar y editar las plantillas de informe.

En esta tarea de iniciación habilitará las plantillas de informe PCI (Payment Card Industry).

Procedimiento

1. Pulse la pestaña **Informes**.
2. Deseleccione la casilla **Ocultar informes inactivos**.
3. En la lista **Grupo**, seleccione **Conformidad** > **PCI**.
4. Seleccione todas las plantillas de informe contenidas en la lista:
   a. Pulse en el primero informe de la lista.
   b. Para seleccionar todas las plantillas de informe, pulse y mantenga pulsada la tecla Mayúsculas y luego pulse en el último informe de la lista.
5. En la lista **Acciones**, seleccione **Conmutar planificación**.
6. Acceda a los informes generados:
   a. En la lista contenida en la columna **Informes generados**, seleccione la indicación de fecha y hora del informe que desee ver.
   b. En la columna **Formato**, pulse el icono correspondiente al formato de informe que desee ver.

Ejemplo: crear un informe personalizado basado en una búsqueda guardada

Puede crear un informe importando una búsqueda o creando criterios personalizados.

Acerca de esta tarea

En esta tarea de iniciación creará un informe que está basado en las búsquedas de sucesos y de flujos que creó en “Buscar sucesos” en la página 17.

Procedimiento

1. Pulse la pestaña **Informes**.
2. En la lista **Acciones**, seleccione **Crear**.
3. Pulse **Siguiente**.
4. Defina la planificación del informe.
   a. Seleccione la opción **Diario**.
   b. Seleccione las opciones **Lunes, Martes, Miércoles, Jueves y Viernes**.
   c. Utilizando las listas, seleccione **8:00** y **AM**.

d. Asegúrese de que esté seleccionada la opción **Sí - Generar manualmente el informe**.
e. Pulse **Siguiente**.

5. Defina el diseño del informe:
   a. En la lista **Orientación**, seleccione **Horizontal**.
   b. Seleccione el diseño con dos contenedores de gráfico.
   c. Pulse **Siguiente**.
6. En el campo **Título de informe**, escriba **Informe de ejemplo**.
7. Defina el contenedor de gráfico superior:
   a. En la lista **Tipo de gráfico**, seleccione **Sucesos/registros**.
   b. En el campo **Título de gráfico**, escriba **Búsqueda de sucesos de ejemplo**.
   c. En la lista **Limitar sucesos/registros a primeros**, seleccione **10**.
   d. En la lista **Tipo de gráfico**, seleccione **Barra apilada**.
   e. Pulse **Todos los datos de 24 horas anteriores**.
   f. En la lista **Basar este informe de suceso en**, seleccione **Búsqueda de ejemplo 1**.

      Los parámetros restantes se llenan automáticamente utilizando los valores de la búsqueda guardada Búsqueda de ejemplo 1.
   g. Pulse **Guardar detalles de contenedor**.
8. Defina el contenedor de gráfico inferior:
   a. En la lista **Tipo de gráfico**, seleccione **Flujos**.
   b. En el campo **Título de gráfico**, escriba **Búsqueda de flujos de ejemplo**.
   c. En la lista **Limitar flujos a primeros**, seleccione **10**.
   d. En la lista **Tipo de gráfico**, seleccione **Barra apilada**.
   e. Pulse **Todos los datos de 24 horas anteriores**.
   f. En la lista **Búsquedas guardadas disponibles**, seleccione **Búsqueda de ejemplo 2**.

      Los parámetros restantes se llenan automáticamente utilizando los valores de la búsqueda guardada Búsqueda de ejemplo 2.
   g. Pulse **Guardar detalles de contenedor**.
9. Pulse **Siguiente**.
10. Pulse **Siguiente**.
11. Elija el formato de informe:
    a. Pulse las casillas **PDF y HTML**.
    b. Pulse **Siguiente**.
12. Elija los canales de distribución del informe:
    a. Pulse **Consola de informes**.
    b. Pulse **Correo electrónico**.
    c. En el campo **Escriba la dirección o direcciones de correo electrónico de destino**, escriba su dirección de correo electrónico.
    d. Pulse **Incluir informe como archivo adjunto**.
    e. Pulse **Siguiente**.
13. Complete los detalles finales del Asistente de informes:
    a. En el campo **Descripción del informe**, escriba una descripción de la plantilla.
    b. Pulse **Sí - Ejecutar este informe cuando finalice el asistente**.

c. Pulse **Finalizar**.

14. Mediante el cuadro de lista de la columna **Informes generados**, seleccione la indicación de fecha y hora del informe.

Avisos

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

Es posible que IBM no comercialice en otros países los productos, servicios o características que se describen en este documento. Consulte al representante local de IBM para obtener información sobre los productos y servicios que están disponibles actualmente en su zona geográfica. Cualquier referencia a un producto, programa o servicio de IBM no indica ni implica que únicamente se pueda utilizar ese producto, programa o servicio de IBM. En su lugar se puede utilizar 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 cubran el tema descrito en este documento. El suministro de este documento no le otorga ninguna licencia sobre estas 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 referentes a información sobre el juego de caracteres de doble byte (DBCS), consulte al departamento de propiedad intelectual de IBM de su país o envíe 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 se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no permiten la renuncia a garantías implícitas o explícitas en determinadas transacciones, por lo que puede que esta declaración no sea aplicable a su caso.

Esta información puede incluir inexactitudes técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán a 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.

Cualquier referencia en esta publicación a sitios web que no sean de IBM se proporciona sólo para su comodidad y no constituye un aval de esos sitios web. Los materiales de esos sitios web no forma parte de los materiales de este producto de IBM, por lo que la utilización de esos sitios web se realiza bajo la propia responsabilidad del usuario.

IBM puede utilizar o distribuir cualquier información que el usuario le proporcione en la forma que considere adecuada, sin incurrir por ello en ninguna obligación con el usuario.

Los licenciatarios de este programa que deseen obtener información sobre él con el fin de habilitar: (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, deben ponerse en contacto con:

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

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido, en algunos casos, el pago de una tarifa.

El programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para él son proporcionados por IBM bajo los términos del Acuerdo de cliente de IBM, el Acuerdo internacional de programas bajo licencia de IBM o cualquier acuerdo equivalente establecido entre las partes.

Los datos de rendimiento contenidos aquí se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Algunas mediciones pueden haberse realizado en sistemas a nivel de desarrollo y no es seguro de que estas mediciones sean las mismas en los sistemas de uso general. Además, algunas mediciones se pueden haber calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables al entorno operativo utilizado.

La información referente a productos que no son de IBM se ha obtenido de los proveedores de esos productos, sus anuncios publicados u otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad ni otras declaraciones referentes a productos que no son de IBM. Las preguntas sobre las prestaciones de los 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 representan únicamente metas y objetivos.

Todos los precios de IBM que se muestran son precios de venta al detalle recomendados de IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de distribuidor pueden variar.

Este documento contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos

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

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

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas en Estados Unidos o en otros países. Si estos y otros términos de marca registrada de IBM están marcados con un símbolo de marca registrada (® o ™) cuando aparecen por primera vez en este documento, estos símbolos indican marcas registradas en los EE.UU. o marcas registradas de derecho común que son propiedad de IBM en el momento de publicar el presente documento. Estas marcas registradas también pueden ser marcas registradas o marcas registradas de derecho común en otros países. Encontrará una lista de marcas registradas de IBM en la página web Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos o en otros países.

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

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas 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 sobre la utilización del producto a fin de mejorar la experiencia final del usuario, personalizar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recogen ninguna 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, más adelante se proporciona información específica sobre el uso de cookies por parte de la oferta de software.

Dependiendo de las configuraciones desplegadas, esta oferta de software puede utilizar cookies de sesión que obtienen el ID de sesión de cada usuario para la gestión y autenticación de las sesiones. Estos cookies se pueden inhabilitar, pero inhabilitarlos también eliminará la funcionalidad que es posible gracias a ellos.

Si las configuraciones desplegadas para esta oferta de software le ofrecen 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" e "IBM Software Products and Software-as-a-Service Privacy Statement" en http://www.ibm.com/software/info/product-privacy.

Glosario

Este glosario incluye términos y definiciones para productos y software de IBM Security QRadar SIEM.

En este glosario se utilizan las referencias cruzadas siguientes:

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

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

A

activo Objeto gestionable que se despliega o se piensa desplegar en un entorno operativo.

acumulador
Registro en el que se puede almacenar un operando de una operación y luego ser sustituido por el resultado de esa operación.

alta disponibilidad (HA)
Relativo a un sistema en clúster que se reconfigura cuando se producen errores de nodo o de daemon de manera que las cargas de trabajo se pueden redistribuir hacia los nodos restantes del clúster.

anomalía
Desviación respecto del comportamiento esperado de la red.

archivo de almacén de confianza
Archivo de base de datos de claves que contiene las claves públicas de 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 ruta entre sistemas abiertos con una calidad de servicio predecible.

captura de contenido
Proceso que captura una cantidad configurable de carga útil y luego almacena los datos en un registro de flujo.

CIDR Véase Direccionamiento entre dominios sin uso de clases.

cifrado
En la seguridad de sistemas, proceso que transforma datos a una forma no inteligible de manera que no se pueden obtener los datos originales o solamente se pueden obtener utilizando un proceso de descifrado.

cliente
Programa de software o sistema que solicita servicios a un servidor.

clúster de alta disponibilidad
Configuración de alta disponibilidad que consta de un servidor primario y un servidor secundario.

Common Vulnerability Scoring System (CVSS)
Sistema de puntuación para medir la gravedad de una vulnerabilidad.

comportamiento
Efectos observables de una operación o suceso, incluidos sus resultados.

conjunto de referencia
Lista de elementos individuales que 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 desde la que un operador puede controlar y observar el funcionamiento del sistema.

contexto de host
Servicio que supervisa componentes para asegurar el funcionamiento correcto de cada componente.

Conversión de direcciones de red (NAT)
En un cortafuegos, conversión de direcciones seguras del Protocolo 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 alto y bajo 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 identificador 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 del número total de bytes de una aplicación con un IP de origen.

credencial
Conjunto de información que otorga determinados derechos de acceso a un usuario o proceso.

credibilidad
Puntuación numérica dentro del rango 0-10 que se utiliza para determinar la integridad de un suceso o delito. La credibilidad aumenta a medida que varias fuentes notifican el mismo suceso o delito.

CVSS Véase Common Vulnerability Scoring System.

D

datos de carga útil
Datos de aplicación contenidos en un flujo de datos IP, excluida la cabecera y la información administrativa.

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

destino de reenvío
Uno o varios sistemas de proveedor que reciben datos en bruto y normalizados procedentes de orígenes de registro y orígenes de flujo.

destino externo
Dispositivo que está separado del sitio primario que recibe flujos de sucesos o de datos de un recopilador de sucesos.

DHCP Véase Protocolo de configuración dinámica de hosts.

Direccionamiento entre dominios sin uso de clases (CIDR)
Método para añadir direcciones de Protocolo Internet de clase C. Las direcciones se proporcionan a los proveedor de servicios de Internet (ISP) para que las utilicen sus clientes. Las direcciones CIDR reducen el tamaño de las tablas de direccionamiento y habilitan más direcciones IP dentro de las empresas.

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 se conecta a la red para recopilar información de vulnerabilidades sobre 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 vulnerabilidades que genera datos de informe a partir de los resultados de exploración de acuerdo con el nombre de la sesión.

explorador
Programa de seguridad automatizado que busca vulnerabilidades de software dentro de aplicaciones web.

extensión de origen de registro
Archivo XML que incluye todos los patrones de expresión regular necesarios para identificar y clasificar sucesos de la carga útil de sucesos.

F

falso positivo
Resultado de una prueba clasificado como positivo (lo que indica que el sitio web es vulnerable al ataque) que el usuario considera que en realidad es un resultado negativo (ausencia de vulnerabilidad).

firma de aplicación
Conjunto exclusivo de características que derivan del examen de la carga útil de los paquetes y luego se utilizan para identificar una aplicación determinada.

flujo Transmisión de datos a través de un enlace durante una conversación.

flujo duplicado
Varias instancias de la misma transmisión de datos recibidas desde 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 representa para un destino.

H

HA Véase alta disponibilidad.

Hash-Based Message Authentication Code (HMAC)
Código criptográfico que utiliza una función hash críptica y una clave secreta.

HMAC
Véase Hash-Based Message Authentication Code.

hoja En un árbol, entrada o nodo que carece de nodos hijos.

host de alta disponibilidad primario
Sistema principal que está conectado al clúster de alta disponibilidad.

host de alta disponibilidad secundario
Sistema en espera que está conectado al clúster de alta disponibilidad. El host de alta disponibilidad secundario toma el control del host de alta disponibilidad primario si éste falla.

I

ICMP Véase Protocolo de mensajes de control de Internet.

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

IDS Véase sistema de detección de intrusiones.

informe
En la gestión de consultas, datos formateados que resultan de ejecutar una consulta y aplicarles un formato.

interconexión de sistemas abiertos (OSI)
Interconexión de sistemas abiertos de acuerdo con las normas ISO (International Organization for Standardization) para el intercambio de información.

intervalo de fusión
Intervalo de frecuencia con que se agrupan los sucesos. La agrupación de sucesos se produce a intervalos de 10 segundos y comienza con el primer suceso que no coincide con ningún suceso de fusión actual. Dentro del intervalo de fusión, los tres primeros sucesos coincidentes se agrupan y se envían al procesador de sucesos.

intervalo de informe
Intervalo de tiempo configurable al final de cual el procesador de sucesos debe enviar todos los datos capturados de sucesos y flujos 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 permitir el acceso a directorios que son compatibles con un modelo X.500, y que no tiene las necesidades de recursos del protocolo DAP (Directory Access Protocol) de X.500, más complejo. Por ejemplo, LDAP se puede utilizar para localizar personas, organizaciones y otros recursos en un directorio de Internet o intranet.

Local a local (L2L)
Relativo al tráfico interno desde una red local a otra red local.

Local a remoto (L2R)
Relativo al tráfico interno desde una red local a otra red remota.

L2R Véase Local a remoto.

L2L Véase Local a local.

M

magistrado
Componente interno que analiza tráfico de red y sucesos de seguridad por comparación con reglas personalizadas definidas.

magnitud
Medida de la importancia relativa de un delito determinado. La magnitud es un valor ponderado que se calcula a partir de los valores de pertinencia, gravedad y credibilidad.

máscara de subred
En las subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred en la porción de una dirección IP correspondiente al host.

Módulo de soporte de dispositivos (DSM)
Archivo de configuración que analiza sucesos recibidos de varios orígenes de registro y los convierte a un formato de taxonomía estándar que se puede visualizar como datos de salida.

multidifusión IP
Transmisión de un datagrama de IP (Protocolo Internet) a un conjunto de sistemas que forman un grupo de multidifusión individual.

N

NAT Véase Conversión de direcciones de red.

NetFlow
Protocolo de red Cisco que supervisa datos de flujo del tráfico de red. Los datos de NetFlow incluyen la información del cliente y servidor, los puertos utilizados, y el número de bytes y paquetes que circulan por los conmutadores y direccionadores conectados a la red. Los datos se envían a los recopiladores de datos de NetFlow, donde se analizan.

nombre de dominio completo (FQDN)
En las 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 nombre de red completo es CompanyA.Department.Marketing.

número de sistema autónomo (ASN)
En TCP/IP, número que es asignado a un sistema autónomo por la misma autoridad central que asigna direcciones IP. El número de sistema autónomo permite que los algoritmos de direccionamiento automatizado distingan sistemas autónomos.

O

objeto de red
Componente de una jerarquía de red.

objeto terminal de base de datos
Objeto o nodo terminal dentro de una jerarquía de base de datos.

Open Source Vulnerability Database (OSVDB)
Base de datos de código abierto, creada por y para la comunidad de seguridad de red, que proporciona información técnica sobre vulnerabilidades de seguridad de red.

orden de análisis
Definición de origen de registro en la que el usuario puede definir el orden de importancia de los orígenes de registro que comparten una misma dirección IP o nombre de host.

origen de registro
Equipo de seguridad o equipo de red desde el que se crea un registro de sucesos.

orígenes de flujo
Origen desde el cual se captura flujo. Un origen de flujo se clasifica como interno cuando el flujo procede de hardware instalado en un host gestionado, y se clasifica como externo cuando el flujo se envía a un recopilador de flujos.

origen externo
Dispositivo que está separado del sitio primario que envía datos normalizados a un recopilador de sucesos.

OSI Véase interconexión de sistemas abiertos.

OSVDB
Véase Open Source Vulnerability Database.

P

pasarela
Dispositivo o programa que se utiliza para conectar redes o sistemas que tienen arquitecturas de red diferentes.

pertinencia
Medida del efecto relativo de un suceso, categoría o delito sobre la red.

peso de red
Valor numérico que se asigna a cada red para representar la importancia de la red. El peso de la red está definido por el usuario.

protocolo
Conjunto de reglas que controlan la comunicación y transferencia de datos entre dos o más dispositivos o sistemas en una red de comunicaciones.

Protocolo de configuración dinámica de hosts (DHCP)
Protocolo de comunicaciones que se utiliza para gestionar centralmente información de configuración. Por ejemplo, DHCP asigna automáticamente direcciones IP a los sistemas de una red.

Protocolo de control de transmisiones (TCP)
Protocolo de comunicación utilizado en Internet y en todas las redes que siguen las normas de IETF (Internet Engineering Task Force) para el protocolo de interconexión de redes. TCP proporciona un protocolo fiable de host a host en redes de comunicaciones de paquetes conmutados y en sistemas interconectados de esas redes. Véase también Protocolo Internet.

Protocolo de mensajes de control de Internet (ICMP)
Protocolo de Internet que es utilizado por una pasarela para comunicarse con un host de origen, por ejemplo, para notificar la existencia 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 Internet (IP)
Protocolo que direcciona datos a través de una red o redes interconectadas. Este protocolo actúa como intermediario entre las capas superiores del protocolo y la red física. Véase también Protocolo de control de transmisiones.

Protocolo simple de gestión de red (SNMP)
Conjunto de protocolos para supervisar sistemas y dispositivos en redes complejas. Se define información sobre dispositivos gestionados y se almacena en una base de información de gestión (Management Information Base).

Proveedor de servicios de Internet (ISP)
Organización que proporciona acceso a Internet.

punto de datos
Valor calculado de una medida en un momento específico.

punto final
Dirección de una API o servicio en un

entorno. Una API expone un punto final y al mismo tiempo invoca los puntos finales de otros servicios.

R

recon Véase reconocimiento.

reconocimiento (recon)
Método para recoger información relativa a la identidad de recursos de red. Se utiliza la exploración de red y otras técnicas para crear una lista de sucesos de recursos de red, a los cuales se les asigna un nivel de gravedad.

recurso compartido administrativo
Recurso de red que está oculto respecto de los usuarios sin privilegios administrativos. Los recursos compartidos administrativos proporcionan a los administradores acceso a todos los recursos de un sistema de red.

red de área local (LAN)
Red que conecta varios dispositivos situados en un área limitada (tal como un edificio o campus) y que se puede conectar a una red mayor.

redirección de ARP
Método de 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 que los sistemas identifiquen relaciones y ejecuten respuestas automatizadas de acuerdo con ello.

regla de direccionamiento
Condición que cuando sus criterios son satisfechos por datos de suceso, se realiza una recogida de condiciones y el direccionamiento subsiguiente.

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 recursos de Internet registrados, tales como nombres de dominio y asignaciones de direcciones IP.

sistema activo
En un clúster de alta disponibilidad, sistema que tiene todos sus servicios en ejecución.

sistema de detección de intrusiones (IDS)
Software que detecta intentos de ataque o ataques consumados sobre recursos supervisados que forman parte de una red o 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 rechazar actividad potencialmente maliciosa. Los mecanismos de rechazo pueden comprender filtrado, seguimiento o el establecimiento de límites de frecuencia.

sistema en espera
Sistema que pasa a estar activo automáticamente cuando falla el sistema activo. Si la replicación de disco está habilitada, el sistema en espera replica 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. SOAP se puede utilizar para consultar y devolver información, e invocar servicios en Internet.

subbúsqueda
Función que permite realizar una consulta de búsqueda dentro de los resultados de una búsqueda completada.

subred
Véase subred.

subred
Red que está dividida en subgrupos independientes menores, que siguen estando interconectados.

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

T

tabla de referencia
Tabla en la que el registro de datos correlaciona claves que tienen un tipo asignado con otras claves, las cuales se correlacionan entonces con un valor individual.

TCP Véase Protocolo de control de transmisiones.

temporizador de renovación
Dispositivo interno, activado manualmente o automáticamente a intervalos regulares, que actualiza los datos actuales sobre la actividad de red.

V

violación
Acto que paso por alto o contraviene una política corporativa.

vista de sistema
Representación visual del host primario y hosts gestionados que componen un sistema.

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

Índice