

IBM Security QRadar Risk Manager
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 163.

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

Introducción a IBM Security QRadar Risk Manager.	vii
Capítulo 1. Novedades para los usuarios de QRadar Risk Manager V7.2.6	1
Capítulo 2. IBM Security QRadar Risk Manager	3
Conexiones	3
Configuration Monitor	3
Topología	4
Policy Monitor.	4
Simulaciones	5
Informes de IBM Security QRadar Risk Manager	5
Navegadores web soportados.	6
Habilitación de la modalidad de documento y la modalidad de navegador en Internet Explorer	6
Acceso a la interfaz de usuario de IBM Security QRadar Risk Manager	6
Características no soportadas en IBM Security QRadar Risk Manager	7
Capítulo 3. Configurar acceso a QRadar Risk Manager	9
Configuración del acceso de cortafuegos	9
Adición del servidor de correo electrónico para alertas y notificaciones.	9
Configuración de interfaces de red	10
Cambio de la contraseña de root	10
Actualización de la hora del sistema	11
Capítulo 4. Configuration Source Management	13
Credenciales	13
Conjunto de credenciales	14
Grupo de red.	14
Conjunto de direcciones	14
Configuración de credenciales para IBM Security QRadar Risk Manager	14
Descubrimiento de dispositivos.	16
Descubrimiento de dispositivos.	16
Importar dispositivos	17
Importación de un archivo CSV	18
Gestionar dispositivos	18
Visualización de dispositivos	18
Adición de un dispositivo	19
Edición de dispositivos	19
Supresión de un dispositivo	20
Filtrado de la lista de dispositivos	20
Obtención de la configuración de dispositivo	22
Recopilación de datos de vecino	23
Recopilación de datos de un repositorio de archivos.	23
Gestionar trabajos de copia de seguridad	24
Ver trabajos de copia de seguridad	25
Visualización del estado y los registros de los trabajos de copia de seguridad	25
Adición de un trabajo de copia de seguridad	26
Edición de un trabajo de copia de seguridad	28
Renombrar un trabajo de copia de seguridad	29
Supresión de un trabajo de copia de seguridad	29
Configurar protocolos	30
Configuración de protocolos.	30
Configuración de la planificación de descubrimiento	33

Capítulo 5. Gráfico de topología de red.	35
Búsquedas de gráfico de topología	35
Búsqueda de aplicaciones.	36
Búsqueda de vulnerabilidades	37
Indicadores NAT en resultados de búsqueda	37
Añadir un sistema de prevención de intrusiones (IPS)	38
Eliminar un Sistema de prevención de intrusiones (IPS)	38
Grupos de dispositivos de topología	39
Diseño de gráfico de topología	39
Capítulo 6. Policy Monitor	41
Preguntas de Policy Monitor.	41
Factor de importancia	42
Ver información de preguntas	43
Creación de una pregunta de activo	43
Creación de una pregunta que pruebe las reglas en los dispositivos	44
Envío de una pregunta	45
Creación de una pregunta de conformidad de activo	46
Edición de una prueba de referencia de conformidad	47
Supervisión de preguntas de conformidad de activos	47
Exportar e importar preguntas de Policy Monitor.	48
Exportación de preguntas de Policy Monitor	48
Importación de preguntas de Policy Monitor	49
Resultados de activos	50
Resultados de dispositivo/regla	53
Evaluar resultados de preguntas de Policy Monitor	55
Aprobación de resultados.	56
Preguntas de supervisor	56
Creación de un suceso para supervisar los resultados	57
Agrupar preguntas	58
Visualización de grupos	58
Creación de un grupo	58
Edición de un grupo	59
Copia de un elemento en otro grupo	59
Supresión de un elemento de un grupo	59
Asignación de un elemento a un grupo	60
Integración de IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager	60
Casos de uso de Policy Monitor	61
Prueba de activos para la comunicación posible en los activos protegidos	61
Comunicación de prueba de dispositivos/reglas en el acceso a Internet	62
Prioridad de las vulnerabilidades de alto riesgo aplicando políticas de riesgo	63
Comunicación real para protocolos permitidos de DMZ	64
Exploraciones de prueba de referencia CIS	65
Supervisión de recuentos de sucesos de reglas de cortafuegos de dispositivos de Check Point.	75
Preguntas de Policy Monitor.	82
Preguntas contribuyentes para pruebas de comunicación reales	83
Preguntas contribuyentes para posibles pruebas de comunicación	89
Parámetros de preguntas restrictivas para pruebas de comunicación posibles	93
Preguntas de prueba de dispositivo/reglas	94
Capítulo 7. Investigar conexiones	97
Visualización de conexiones	97
Utilizar gráficos para ver datos de conexión	99
Utilización del gráfico de serie temporal	100
Utilizar gráfico de conexión para ver conexiones de red	102
Utilización de los gráficos circular, de barras y de tabla	103
Búsqueda de conexiones.	104
Guardar criterios de búsqueda	106
Realización de una sub-búsqueda	108
Gestionar resultados de búsqueda	109

Cancelación de una búsqueda	110
Supresión de una búsqueda	110
Exportación de conexiones	111
Capítulo 8. Correlación de origen de registro	113
Creación o edición de una correlación de origen de registro	113
Capítulo 9. Investigación de las configuraciones de dispositivo de red	115
Búsqueda de dispositivos de regla	116
Comparación de la configuración de los dispositivos de red	116
Capítulo 10. Filtrado de reglas de dispositivo por usuario o grupo	119
Capítulo 11. Gestión de informes de IBM Security QRadar Risk Manager.	121
Generación manual de un informe	121
Utilizar el asistente de informes	122
Creación de un informe	122
Edición de un informe	125
Duplicación de un informe	126
Compartición de un informe	126
Configuración de gráficos	127
Gráficos de conexiones	127
Gráficos de reglas de dispositivo	130
Gráficos de objetos no utilizados de dispositivo	135
Capítulo 12. Gestión de políticas	137
Capítulo 13. Utilizar simulaciones en IBM Security QRadar Risk Manager	139
Simulaciones	139
Creación de una simulación	140
Edición de una simulación	144
Duplicación de una simulación	144
Supresión de una simulación	144
Ejecución manual de una simulación	144
Gestión de resultados de simulación.	145
Visualización de resultados de simulación	145
Aprobación de resultados de simulación	147
Revocación de aprobación de simulación	147
Supervisión de simulaciones	148
Agrupación de simulaciones	149
Edición de un grupo	150
Copia de un elemento en otro grupo	150
Supresión de un elemento de un grupo.	150
Asignación de un elemento a un grupo.	150
Capítulo 14. Modelos de topología	153
Creación de un modelo de topología	153
Edición de un modelo de topología	156
Duplicación de un modelo de topología	156
Supresión de un modelo de topología	156
Agrupar modelos de topología	157
Visualización de grupos	157
Creación de un grupo	157
Edición de un grupo	157
Copia de un elemento en otro grupo	158
Supresión de un elemento de un grupo.	158
Asignar una topología a un grupo	158

Capítulo 15. Datos de registro de auditoría.	159
Acciones registradas	159
Visualización de actividad de usuario	161
Visualización del archivo de registro.	161
Detalles de archivo de registro	162
Avisos	163
Marca registradas	165
Consideraciones sobre la política de privacidad	165
Glosario	167
A	167
C	167
D	167
G	167
I.	167
L	167
M	168
N	168
P	168
R	168
S	168
V	168
Índice.	169

Introducción a IBM Security QRadar Risk Manager

Esta información está destinada a utilizarse con IBM® Security QRadar Risk Manager. QRadar Risk Manager es un dispositivo que se utiliza para supervisar configuraciones de dispositivo, simular cambios de red y priorizar los riesgos y las vulnerabilidades de la red.

Esta guía contiene instrucciones para configurar y utilizar IBM Security QRadar Risk Manager en una consola de IBM Security QRadar SIEM.

A quién va dirigido este manual

Los administradores del sistema responsables de configurar y utilizar QRadar Risk Manager deben tener acceso administrativo a IBM Security QRadar SIEM y a los dispositivos de red y los cortafuegos. El administrador del sistema debe tener conocimientos de la red corporativa y de las tecnologías de red.

Documentación técnica

Para obtener información sobre cómo acceder a documentación más técnica, notas técnicas y notas del 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 soporte al cliente

Para obtener información sobre cómo ponerse en contacto con soporte al cliente, consulte 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 TI implica la protección de sistemas e información mediante la prevención, la detección y la respuesta a accesos indebidos desde dentro o fuera de la empresa. Un acceso indebido puede alterar, destruir o dar un uso inapropiado de la información o puede ocasionar daños o un uso erróneo de los sistemas, incluidos los ataques a terceros. Ningún producto o sistema de TI debe considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo en la prevención de un uso o acceso indebidos. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un sistema de seguridad completo, que necesariamente incluye procedimientos operativos adicionales y puede necesitar otros sistemas, productos o servicios para lograr la máxima efectividad. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALICIOSAS O ILEGALES DE CUALQUIERA DE LAS PARTES.

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

IBM Security QRadar Risk Manager V7.2.6 presenta mejoras para ayudarle a organizar y gestionar la topología de red, filtrar reglas de dispositivos por usuarios y grupos e integraciones de dispositivos nuevas.


Mejoras de la pantalla Topología

Gestione y organice el gráfico de topología agrupando y renombrando dispositivos, filtrando el número de subredes visualizados para el dispositivo, mostrando u ocultando dispositivos no clasificados. Puede gestionar la densidad de nodos de red visualizados filtrando dispositivos y redes para formar un gráfico no

desordenado.  Más información...

Filtrado de reglas de dispositivo por usuario o grupo

Para ayudarle a gestionar y optimizar las políticas de regla de red, puede ver,

filtrar y buscar las reglas de dispositivo por usuario o grupo.  Más información...

Integraciones de adaptador

QRadar Risk Manager presenta dos integraciones de adaptador nuevas que amplían los dispositivos de red soportados, como por ejemplo cortafuegos, direccionadores y conmutadores a los que se puede preguntar.

Adaptador de Sidewinder

El adaptador QRadar Risk Manager para Sidewinder da soporte a dispositivos de McAfee Enterprise Firewall (Sidewinder) que ejecutan SecureOS.

Adaptador de TippingPoint

El adaptador de QRadar Risk Manager para TippingPoint da soporte a dispositivos de TippingPoint que ejecutan TOS y están bajo el control de SMS.

Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

Capítulo 2. IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager es un dispositivo que se instala de forma independiente para supervisar configuraciones de dispositivo, simulando cambios en el entorno de red y priorizando los riesgos y las vulnerabilidades de la red.

Se accede a QRadar Risk Manager utilizando la pestaña **Risks** en IBM Security QRadar SIEM Console.

QRadar Risk Manager utiliza los datos recopilados por QRadar. Por ejemplo, los datos de configuración de cortafuegos, direccionadores, conmutadores o sistemas de prevención de intrusiones (IPS), canales de información de vulnerabilidad y orígenes de seguridad de terceros. Los orígenes de datos permiten a QRadar Risk Manager identificar los riesgos de seguridad, política y conformidad en la red y calcular la probabilidad de explotación de riesgo.

QRadar Risk Manager le advierte de los riesgos descubiertos visualizando delitos en la pestaña **Delitos**. Los datos de riesgo se analizan y notifican en el contexto de todos los demás datos que QRadar procesa. En QRadar Risk Manager puede evaluar y gestionar el riesgo a un nivel aceptable que se basa en la tolerancia de riesgo en la empresa.

También puede utilizar QRadar Risk Manager para consultar todas las conexiones de red, comparar las configuraciones de dispositivo, filtrar la topología de red y simular los posibles efectos de actualizar las configuraciones de dispositivos.

Puede utilizar QRadar Risk Manager para definir un conjunto de políticas (o preguntas) sobre la red y supervisar los cambios en las políticas. Por ejemplo, si desea denegar protocolos cifrados en la DMZ desde Internet, puede definir una pregunta de supervisor de política para detectar los protocolos sin cifrar. Al enviar la pregunta se devuelve una lista de protocolos no cifrados que se comunican desde internet a la DMZ y puede determinar qué protocolos no cifrados son riesgos de seguridad.

Conexiones

Utilice la página Conexiones para supervisar las conexiones de red de los hosts locales.

Puede ejecutar consultas e informes sobre las conexiones de red de los hosts locales que se basen en las aplicaciones, los puertos, los protocolos y los sitios web con los que los hosts locales se pueden comunicar.

Para obtener más información sobre conexiones, consulte Investigación de conexiones.

Configuration Monitor

Utilice Configuration Monitor para revisar y comparar la configuración de dispositivos, lo que le permite aplicar políticas de seguridad y supervisar las modificaciones de dispositivo en la red.

Las configuraciones de dispositivo pueden incluir conmutadores, direccionadores, cortafuegos y dispositivos IPS en la red. Para cada dispositivo, puede ver el historial de configuración de dispositivo, las interfaces y las reglas. También puede comparar configuraciones dentro de un dispositivo y entre dispositivos.

La información de configuración de dispositivo también se utiliza para crear la representación de toda la empresa de la topología de red, lo que le permite determinar actividad permitida y denegada en la red. La configuración de dispositivo le permite identificar incoherencias y cambios de configuración que presentan riesgo en la red.

Topología

La topología es una representación gráfica que ilustra la capa de red de la red, basándose en los dispositivos añadidos de Configuration Source Management.

La capa de red es la capa 3 del modelo OSI (Interconexión de sistemas abiertos).

La capa de aplicación es la capa 7 del modelo OSI.

Utilice el gráfico interactivo de la topología para ver las conexiones entre dispositivos, los dispositivos de seguridad de red virtualizados con varios contextos, los activos, los dispositivos NAT (Conversión de direcciones de red), los indicadores de NAT y la información sobre correlaciones NAT.

Puede buscar sucesos, dispositivos, vías de acceso y guardar los diseños de red.

Puede agrupar dispositivos y renombrar dispositivos y grupos.

En la topología, puede consultar la capa de transporte (capa 4) y filtrar las vías de acceso de red basándose en el puerto y el protocolo. La información de gráfico y conexión se crea a partir de la información de configuración detallada obtenida de los dispositivos de red, por ejemplo cortafuegos, direccionadores y sistemas IPS.

Para obtener más información, consulte Topología.

Policy Monitor

Utilice Policy Monitor para definir preguntas específicas sobre el riesgo de la red y enviar la pregunta a IBM Security QRadar Risk Manager.

QRadar Risk Manager evalúa los parámetros que ha definido en la pregunta y devuelve activos de la red para ayudarle a evaluar el riesgo. Las preguntas se basan en una serie de pruebas que se pueden combinar y configurar como sea necesario. QRadar Risk Manager proporciona un gran número de preguntas de Policy Monitor predefinidas y permite la creación de preguntas personalizadas. Se pueden crear preguntas de Policy Monitor para las siguientes situaciones:

- Comunicaciones que se han producido
- Comunicaciones posibles basadas en la configuración de cortafuegos y direccionadores
- Reglas de cortafuegos reales (pruebas de dispositivo)

Policy Monitor utiliza los datos obtenidos de los datos de configuración, los datos de actividad de red, los sucesos de red y seguridad y los datos de exploración de vulnerabilidad para determinar la respuesta apropiada. QRadar Risk Manager

proporciona plantillas de políticas para ayudarle a determinar el riesgo en varios mandatos normativos y mejores prácticas de seguridad de la información, como por ejemplo PCI, HIPPA e ISO 27001. Puede actualizar las plantillas para alinearse con las políticas de seguridad de información corporativas definidas. Si la respuesta es completa, puede aceptar la respuesta a la pregunta y definir cómo desea que el sistema responda a resultados no aceptados.

Policy Monitor permite que se supervise activamente un número ilimitado de preguntas. Cuando se supervisa una pregunta, QRadar Risk Manager evalúa continuamente la pregunta para los resultados no aprobados. A medida que se descubren resultados no aprobados, QRadar Risk Manager tiene la capacidad de enviar correo electrónico, visualizar notificaciones, generar un suceso syslog o crear un delito en IBM Security QRadar SIEM.

Para obtener más información sobre Policy Monitor, consulte Policy Monitor.

Simulaciones

Utilice simulaciones para definir, planificar y realizar simulaciones de explotación en la red.

Puede crear un ataque simulado en la topología basándose en una serie de parámetros que están configurados de una forma similar en Policy Monitor. Puede crear un ataque simulado en la topología de red actual o crear un modelo de topología. Un modelo de topología es una topología virtual que le permite realizar modificaciones en la topología virtual y simular un ataque. Esto le permite simular cómo las modificaciones en las reglas de red, los puertos, los protocolos o las conexiones permitidas o denegadas pueden afectar a la red. Simulation es una herramienta potente para determinar el impacto de riesgo de los cambios propuestos en la configuración de red antes de que se implementen los cambios.

Después de que se haya completado una simulación, puede revisar los resultados. Si desea aceptar los resultados, puede configurar la modalidad de simulación, que le permite definir cómo desea responder a resultados no aceptados.

IBM Security QRadar Risk Manager permite supervisar activamente un máximo de 10 simulaciones. Cuando se supervisa una simulación, QRadar Risk Manager analiza continuamente en la topología los resultados no aprobados. A medida que se descubren resultados no aprobados, QRadar Risk Manager tiene la capacidad de enviar correo electrónico, visualizar notificaciones, generar un suceso syslog o crear un delito en QRadar SIEM.

Para obtener más información sobre las simulaciones, consulte Utilización de simulaciones.

Informes de IBM Security QRadar Risk Manager

Utilice la pestaña **Informes** para ver informes específicos, basándose en los datos disponibles en QRadar Risk Manager, como por ejemplo conexiones, reglas de dispositivos y objetos no utilizados de dispositivo.

Están disponibles los siguientes informes detallados adicionales:

- conexiones entre dispositivos
- reglas de cortafuegos en un dispositivo
- objetos no utilizados en un dispositivo

Para obtener más información sobre informes, consulte Gestión de informes de IBM Security QRadar Risk Manager.

Navegadores web soportados

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

Cuando se accede al sistema 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 de QRadar

Navegador web	Versiones soportadas
Mozilla Firefox	38.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, con modalidad de documento y modalidad de navegador habilitadas	10.0 11.0
Google Chrome	Versión 43 y anteriores.

Habilitación de la modalidad de documento y la modalidad de navegador en Internet Explorer

Si utiliza Microsoft Internet Explorer para acceder a los productos de IBM Security QRadar, debe habilitar la modalidad de navegador y modalidad de documento.

Procedimiento

1. En el navegador 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 los **Estándares de Internet Explorer** para su release de Internet Explorer.

Acceso a la interfaz de usuario de IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager utiliza la información de inicio de sesión predeterminada para el URL, el nombre de usuario y la contraseña.

A QRadar Risk Manager se accede a través de IBM Security QRadar SIEM Console. Utilice la información de la tabla siguiente cuando inicie la sesión en QRadar Console.

Tabla 2. Información de inicio de sesión predeterminada para QRadar Risk Manager

Información de inicio de sesión	Valor predeterminado
URL	https://<dirección IP>, donde <dirección IP> es la dirección IP de QRadar Console.
Nombre de usuario	admin

Tabla 2. Información de inicio de sesión predeterminada para QRadar Risk Manager (continuación)

Información de inicio de sesión	Valor predeterminado
Contraseña	La contraseña que se asigna a QRadar Risk Manager durante el proceso de instalación.
Clave de licencia	Una clave de licencia predeterminada proporciona acceso al sistema durante 5 semanas.

Características no soportadas en IBM Security QRadar Risk Manager

Es importante tener en cuenta las características no soportadas por QRadar Risk Manager.

Las siguientes características no se soportan en QRadar Risk Manager:

- Alta disponibilidad (HA)
- Direccionamiento dinámico para BGP (Border Gateway Protocol - Protocolo de pasarela fronteriza), OSPF (Open Shortest Path First) o RIP (Routing Information Protocol - Protocolo de información de direccionamiento)
- IPv6
- Máscaras de red no contiguas
- Rutas con equilibrio de carga
- Correlaciones de referencia
- Almacenar y reenviar

Capítulo 3. Configurar acceso a QRadar Risk Manager

Puede configurar valores de acceso para QRadar Risk Manager desde la pestaña **Admin** de IBM Security QRadar SIEM. Cuando añada QRadar Risk Manager al despliegue, debe configurar valores, como por ejemplo el cortafuegos local, las interfaces de red y el servidor de correo electrónico y añadir la licencia adecuada.

Si tiene permisos de administrador, puede configurar varios valores de dispositivo para QRadar Risk Manager.

Los administradores pueden realizar las tareas siguientes:

- En la ventana **Gestión del sistema y licencias** puede gestionar licencias, configurar el cortafuegos local, añadir un servidor de correo electrónico y configurar interfaces de red para QRadar Risk Manager.
- Cambiar la contraseña para un host.
- Actualizar la hora del sistema.

Configuración del acceso de cortafuegos

Configure el cortafuegos local de IBM Security QRadar Risk Manager para permitir el acceso desde dispositivos especificados fuera de este despliegue que necesitan acceder a este host. Por ejemplo, puede conectarse a este host desde un sistema que no forme parte de la configuración de QRadar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione el host para el que desea configurar los valores de acceso de cortafuegos.
6. En el menú **Acciones**, pulse **Ver y gestionar el sistema**.
Puede pulsar con el botón derecho sobre el host seleccionado para acceder a esta opción de menú o puede efectuar una doble pulsación sobre el host para abrir la ventana **Información del sistema**.
7. Pulse la pestaña **Cortafuegos**.
8. Configure acceso para dispositivos que están fuera del despliegue y que deben conectarse a este host.
9. Añada esta regla de acceso pulsando la flecha.
10. Pulse **Guardar**.

Adición del servidor de correo electrónico para alertas y notificaciones

Puede configurar el servidor de correo electrónico utilizado por QRadar Risk Manager. Esto se utiliza para distribuir alertas y mensajes de suceso.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.

3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione el host para el que desea añadir una dirección de servidor de correo electrónico.
6. En el menú **Acciones**, seleccione **Ver y gestionar el sistema**.

Nota: También puede pulsar con el botón derecho sobre el host para acceder a este menú o puede efectuar una doble pulsación sobre el host para abrir la ventana Información del sistema.

7. Pulse la pestaña **Servidor de correo electrónico**.
8. En el campo **Dirección de servidor de correo electrónico**, teclee el nombre host o la dirección IP del servidor de correo electrónico que desea utilizar.
Conecte el servidor de correo electrónico a través del puerto 25.
Si no tiene un servidor de correo electrónico y desea utilizar el servidor de correo electrónico proporcionado por QRadar, teclee localhost.
9. Pulse **Guardar**.

Configuración de interfaces de red

Configuración de información de direcciones IP y roles para interfaces de red de QRadar Risk Manager.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione el host en el que desea editar los valores de interfaz de red.
6. Pulse **Acciones > Ver y gestionar el sistema** o pulse con el botón derecho sobre el dispositivo seleccionado para acceder a esta opción de menú. También puede efectuar una doble pulsación sobre el host para abrir la ventana Información del sistema.
7. Pulse la pestaña **Interfaces de red**.
8. Seleccione una interfaz de red en la columna **Dispositivo**.
9. Pulse **Editar**.
No puede editar una interfaz de red con un rol de gestión, cruce de alta disponibilidad o esclavo.
10. Configure los siguientes parámetros:
 - El **Rol**.
 - Atributos de dirección IP.
 - Opción **Mover esta configuración con alta disponibilidad activa**.
11. Pulse **Guardar** para actualizar los valores.

Cambio de la contraseña de root

Puede cambiar la contraseña de root en el host de IBM Security QRadar Risk Manager a intervalos regulares o cada 90 días como mínimo.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar Console como usuario root.
2. Escriba el nombre de usuario y la contraseña para el usuario root.
El nombre de usuario y la contraseña son sensibles a las mayúsculas y minúsculas.
3. En QRadar Console, utilice SSH para iniciar la sesión en QRadar Risk Manager como usuario root.
4. Utilice el mandato `passwd` para cambiar la contraseña.
La contraseña de root no acepta los siguientes caracteres especiales: apóstrofo ('), signo de dólar (\$), signo de exclamación (!)

Actualización de la hora del sistema

Todos los cambios de hora del sistema se deben establecer en QRadar Console. Habilite los servicios de sincronización en QRadar Console y sincronice la hora con los hosts gestionados.

Acerca de esta tarea

Para obtener más configuración sobre la configuración de la hora del sistema en la Consola y sincronizar la hora con hosts gestionados en el despliegue, consulte la Guía de administración de IBM Security QRadar SIEM.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar Console como usuario root.
 2. Edite el archivo `ntp.conf`.

```
vi /etc/ntp.conf
```
 3. En la sección `server` del archivo `ntp.conf`, puede dejar las entradas de servidor existentes o sustituirlas por su propio servidor NTP (Network Time Protocol) interno. Las entradas de servidor del archivo `ntp.conf` empiezan por `'server'`. Puede utilizar servidores públicos de Proyecto NTP en (<http://www.ntp.org/>).
- ```
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst
server 3.rhel.pool.ntp.org iburst
```
- Si utiliza servidores NTP públicos, compruebe que el cortafuegos permite las solicitudes NTP salientes.
4. Guarde los cambios y cierre el archivo.
  5. Habilite el servicio `ntpd` para ejecutar en el nivel de ejecución 3.  

```
chkconfig --level 3 ntpd on
```
  6. Verifique que el servicio `ntpd` está habilitado para ejecutarse durante el reinicio.  

```
chkconfig --list ntpd
```

Verifique que `3:on` se visualice en la salida. Esto confirma que el servicio está habilitado.

```
ntpd 0:off 1:off 2:off 3:on 4:off 5:off 6:off
```

Debe concluir servicios antes de sincronizar manualmente la hora con el servidor NTP.
  7. Para evitar que se produzcan errores de recopilación de datos cuando cambie la hora del sistema, concluya los servicios de QRadar.

- ```
service hostcontext stop
service tomcat stop
service hostservices stop
```
8. Sincronice la hora con su servidor NTP.
`ntpdate <ntp.server.address>`
 9. Inicie el servicio ntpd.
`service ntpd start`
 10. Reinicie los servicios de QRadar.
`service hostservices start`
`service tomcat start`
`service hostcontext start`
 11. Sincronice la hora en todos los hosts gestionados con su QRadar Console
tecleando el mandato siguiente.
`/opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh`
 12. En la pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**,
para reiniciar servicios en todos los hosts gestionados de QRadar.
La hora queda sincronizada entre QRadar Console y los hosts gestionados.

Capítulo 4. Configuration Source Management

Utilice Configuration Source Management para configurar credenciales, añadir o descubrir dispositivos, ver configuraciones de dispositivo y realizar copia de seguridad de configuraciones de dispositivo en IBM Security QRadar Risk Manager.

Los datos que se obtienen de los dispositivos de la red se utilizan para llenar la topología. Debe tener privilegios administrativos para acceder a las funciones de Configuration Source Management desde la pestaña **Admin** de IBM Security QRadar SIEM.

Para configurar los orígenes de configuración, debe:

1. Configurar las credenciales de dispositivo.
2. Descubrir o importar dispositivos. Hay dos maneras de añadir dispositivos de red a QRadar Risk Manager; descubrir dispositivos utilizando Configuration Source Management o importar una lista de dispositivos de un archivo CSV utilizando la importación de dispositivo.
3. Obtener la configuración de dispositivo de cada uno de los dispositivos.
4. Gestionar trabajos de copia de seguridad para asegurar que se capturan todas las actualizaciones de las configuraciones de dispositivo.
5. Configurar la planificación de descubrimiento para asegurar que se descubren automáticamente los dispositivos nuevos.

Utilice Configuration Source Management para:

- Añadir, editar, buscar y suprimir los orígenes de configuración. Para obtener más información, consulte Gestionar dispositivos.
- Configurar o gestionar protocolos de comunicación para los dispositivos. Para obtener más información, consulte Configurar protocolos.

Si está utilizando el dispositivo NSM de Juniper, también debe obtener información de configuración.

Para obtener información detallada acerca de los adaptadores utilizados para comunicarse con dispositivos de fabricantes específicos, consulte la publicación *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

Credenciales

En IBM Security QRadar Risk Manager, las credenciales se utilizan para acceder a la configuración de dispositivos como cortafuegos, direccionadores, conmutadores o IPS y descargar dicha configuración.

Los administradores utilizan Configuration Source Management para entrar credenciales de dispositivo. Esto proporciona a QRadar Risk Manager acceso a un dispositivo específico. Las credenciales de dispositivo individuales se pueden guardar para un dispositivo de red específico. Si varios dispositivos de red utilizan las mismas credenciales, puede asignar las credenciales a un grupo.

Por ejemplo, si todos los cortafuegos de la organización tienen los mismos nombre de usuario y contraseña, las credenciales se asocian con los conjuntos de

direcciones para todos los cortafuegos y se utilizan para realizar la copia de seguridad de las configuraciones de dispositivo para todos los cortafuegos de la organización.

Si una credencial de red no es necesaria para un dispositivo específico, el parámetro se puede dejar en blanco en la configuración de orígenes de gestión. Para ver una lista de credenciales de adaptador necesarias, consulte la publicación *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

Puede asignar distintos dispositivos de la red a grupos de red, lo que le permite agrupar conjuntos de credenciales y direcciones para los dispositivos.

Conjunto de credenciales

Un conjunto de credenciales contiene información como los valores de nombre de usuario y contraseña para un conjunto de dispositivos.

Grupo de red

Cada grupo de red puede incluir varios conjuntos de credenciales y de direcciones. Puede configurar IBM Security QRadar Risk Manager para priorizar cómo se evalúa cada grupo de red.

El grupo de red en la parte superior de la lista tiene la prioridad más alta. El primer grupo de red que coincide con la dirección IP configurada se incluye como candidato cuando se realiza una copia de seguridad de un dispositivo. Se tiene en cuenta un máximo de tres conjuntos de credenciales de un grupo de red.

Por ejemplo, si la configuración incluye estos dos grupos de red:

- El Grupo de red 1 incluye dos conjuntos de credenciales
- El Grupo de red 2 incluye dos conjuntos de credenciales

QRadar Risk Manager intenta compilar una lista de un máximo de tres conjuntos de credenciales. Dado que el Grupo de red 1 está más alto en la lista, se añaden ambos conjuntos de credenciales del Grupo de red 1 a la lista de candidatos. Puesto que se necesitan tres conjuntos de credenciales, se añade a la lista el primer conjunto de credenciales del Grupo de red 2.

Cuando un conjunto de credenciales accede satisfactoriamente a un dispositivo, QRadar Risk Manager utiliza ese conjunto de credenciales para los posteriores intentos de acceso al dispositivo. Si cambian las credenciales de ese dispositivo, la autenticación falla cuando se intenta acceder al dispositivo. A continuación, en el intento de autenticación siguiente, QRadar Risk Manager reconcilia las credenciales de nuevo para garantizar el éxito.

Conjunto de direcciones

Un conjunto de direcciones es una lista de direcciones IP que definen un grupo de dispositivos que comparten el mismo conjunto de credenciales.

Configuración de credenciales para IBM Security QRadar Risk Manager

Los administradores deben configurar credenciales para permitir que IBM Security QRadar Risk Manager se conecte a los dispositivos de la red.

Acerca de esta tarea

Puede escribir un rango de direcciones IP utilizando un guión o un comodín (*) para indicar un rango, por ejemplo, 10.100.20.0-10.100.20.240 o 1.1.1*. Si escribe 1.1.1.*, se incluyen todas las direcciones IP que cumplen ese requisito.

Al configurar el conjunto de direcciones con Juniper Networks NSM o un adaptador XML genérico, debe escribir el rango de direcciones IP o el rango de direcciones CIDR para todos los dispositivos gestionados por Juniper Networks NSM o los archivos para los dispositivos del repositorio.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. En el menú de navegación, pulse **Credentials**.
5. En el panel **Network Groups**, pulse el icono **Add (+)**.
6. Escriba un nombre para un grupo de red y, a continuación, pulse **OK**.
7. Mueva el grupo de red que desea que tenga la primera prioridad a la parte superior de la lista. Puede utilizar los iconos de flecha **Move Up** y **Move Down** para priorizar un grupo de red.
8. En el campo **Add Address**, escriba la dirección IP o el rango CIDR que desea aplicar al grupo de red y, a continuación, pulse el icono **Add (+)**.
Repita para todas las direcciones IP que desea añadir al conjunto de direcciones para este grupo de red.
9. En el panel **Credentials**, pulse el icono **Add (+)**.
10. Escriba un nombre para el nuevo conjunto de credenciales y, a continuación, pulse **OK**.
11. Escriba valores para los parámetros:

Opción	Descripción
Username	<p>Escriba el nombre de usuario para el conjunto de credenciales.</p> <p>Si está utilizando un Juniper Networks NSM o un adaptador XML genérico, escriba un nombre de usuario que pueda acceder al servidor Juniper NSM o un nombre de usuario que pueda acceder al repositorio de archivos que contiene los archivos SED (documento de elemento estándar).</p>
Password	<p>Escriba la contraseña para el conjunto de credenciales.</p> <p>Si está utilizando Juniper Networks NSM o un adaptador XML genérico, escriba la contraseña para el servidor Juniper NSM o la contraseña para iniciar la sesión en el repositorio de archivos que contiene los archivos SED (documento de elemento estándar).</p>

Opción	Descripción
Enable Username	Escriba el nombre de usuario para la autenticación de segundo nivel para el conjunto de credenciales.
Enable Password	Escriba la contraseña para la autenticación de segundo nivel para el conjunto de credenciales.
SNMP Get Community	Escriba la comunidad SNMP Get.
SNMPv3 Authentication Username	Escriba el nombre de usuario que desea utilizar para autenticar SNMPv3.
SNMPv3 Authentication Password	Escriba la contraseña que desea utilizar para autenticar SNMPv3.
SNMPv3 Privacy Password	Escriba el protocolo que desea utilizar para descifrar interrupciones SNMPv3.

12. Mueva el conjunto de credenciales que desea que tenga la primera prioridad a la parte superior de la lista. Utilice los iconos de flecha **Move Up** y **Move Down** para priorizar un conjunto de credenciales.
13. Repítalo para cada conjunto de credenciales que desea añadir.
14. Pulse **OK**.

Descubrimiento de dispositivos

El proceso de descubrimiento utiliza el SNMP (Protocolo simple de gestión de redes) y la CLI (interfaz de línea de mandatos) para descubrir dispositivos de red.

Después de configurar una dirección IP o un rango de CIDR, el motor de descubrimiento realiza una exploración de TCP en la dirección IP para determinar si el puerto 22, 23 o 443 están supervisando conexiones. Si la exploración de TCP es satisfactoria y la consulta SNMP está configurada para determinar el tipo de dispositivo, la serie de SNMP de obtención de comunidad se utiliza basándose en la dirección IP.

Esta información se utiliza para determinar con qué adaptador se debe correlacionar el dispositivo cuando se añade. IBM Security QRadar Risk Manager se conecta al dispositivo y recopila una lista de interfaces e información de vecinos, como tablas CDP, NDP o ARP. Entonces el dispositivo se añade al inventario.

Es posible que a la dirección IP configurada que se utiliza para iniciar el proceso de descubrimiento no se le asigne la dirección IP asignada para el nuevo dispositivo. QRadar Risk Manager añade un dispositivo utilizando la dirección IP para la interfaz de numeración más baja en el dispositivo (o dirección de bucle más baja, si existe).

Si utiliza la casilla de verificación **Crawl the network from the addresses defined above**, la dirección IP de los vecinos recopilados del dispositivo se vuelven a incorporar en el proceso de descubrimiento y el proceso se repite para cada dirección IP.

Descubrimiento de dispositivos

Los administradores utilizan el descubrimiento de dispositivos para determinar el tipo de dispositivo.

Acerca de esta tarea

Al realizar un descubrimiento de dispositivo, cualquier dispositivo que no está soportado pero responde a SNMP se añade con el adaptador de SNMP genérico. Si desea ejecutar un filtro de vía de acceso mediante el dispositivo con rutas simuladas, debe eliminar manualmente el dispositivo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. En el menú de navegación, pulse **Discover Devices**.
5. Escriba una dirección IP o un rango de CIDR.
Esta dirección IP o rango de CIDR indica la ubicación de los dispositivos que desea descubrir.
6. Pulse el icono **Add (+)**.
7. Si desea buscar también dispositivos en la red desde la dirección IP o el rango de CIDR definidos, marque el recuadro de selección **Crawl the network from the addresses defined above**.
8. Pulse **Run**.

Importar dispositivos

Utilizar la importación de dispositivos para añadir una lista de adaptadores y las direcciones IP de red al Gestor de origen de configuración utilizando un archivo de valor separado por coma (.CSV).

La lista de importación de dispositivos puede contener hasta 5000 dispositivos, pero la lista debe contener una línea para cada adaptador y la dirección IP asociada en el archivo de importación.

Por ejemplo,

```
<Adaptador::Nombre 1>,<Dirección IP>  
<Adaptador::Nombre 2>,<Dirección IP>  
<Adaptador::Nombre 3>,<Dirección IP>
```

Donde:

<Adaptador::Nombre> contiene el fabricante y nombre de dispositivo, por ejemplo Cisco::IOS.

<Dirección IP> contiene la dirección IP del dispositivo, por ejemplo 191.168.1.1.

Tabla 3. Ejemplos de importación de dispositivos

Fabricante	Nombre	Ejemplo <Adaptador::Nombre>,<Dirección IP>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8

Tabla 3. Ejemplos de importación de dispositivos (continuación)

Fabricante	Nombre	Ejemplo <Adaptador::Nombre>,<Dirección IP>
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importación de un archivo CSV

Puede importar una lista de dispositivos maestros a Configuration Source Management utilizando un archivo CSV (valores separados por comas).

Antes de empezar

Si importa una lista de dispositivos y, a continuación, realiza un cambio en una dirección IP en el archivo CSV, es posible que duplique accidentalmente un dispositivo en la lista de Configuration Source Management. Por este motivo, suprima un dispositivo de Configuration Source Management antes de volver a importar la lista de dispositivos maestros.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Plug-Ins**, pulse **Device Import**.
4. Pulse **Browse**.
5. Localice el archivo CSV, pulse **Open**.
6. Pulse **Import Devices**.

Resultados

Si se visualiza un error, debe revisar el archivo CSV para corregir los errores y volver a importar el archivo. Una importación del archivo CSV puede fallar si la lista de dispositivos está estructurada incorrectamente o si la lista de dispositivos contiene información incorrecta. Por ejemplo, es posible que en el archivo CSV falten dos puntos o un mandato, que haya varios dispositivos en una sola línea o que un nombre de adaptador tenga un error tipográfico.

Si se anula la importación de dispositivos, no se añaden dispositivos del archivo CSV a Configuration Source Management.

Gestionar dispositivos

Mediante el uso de la pestaña **Devices** de la ventana de Configuration Source Management, puede gestionar los dispositivos de la red.

En la pestaña de dispositivos, puede ver, añadir, editar y suprimir dispositivos. También puede filtrar la lista de dispositivos, obtener información de configuración de dispositivo, recopilar datos de vecinos y descubrir dispositivos que se encuentran en el despliegue.

Visualización de dispositivos

Puede ver todos los dispositivos del despliegue en la pestaña **Devices**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Devices**.
5. Para ver información detallada para una configuración de dispositivo, seleccione el dispositivo que desee ver y pulse **Abrir**.

Adición de un dispositivo

Puede añadir dispositivos de red y adaptadores individuales utilizando Configuration Source Management.

Acerca de esta tarea

Puede añadir un dispositivo individual a la lista de dispositivos en Configuration Source Management o puede añadir varios dispositivos utilizando un archivo CSV.

Para obtener información acerca de la adición de varios dispositivos, consulte Importar dispositivos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. En el panel de navegación, pulse **Add Device**.
5. Configure los valores de los parámetros siguientes:

Opción	Descripción
IP Address	Escriba la dirección IP de gestión del dispositivo.
Adapter	En la lista desplegable Adapter , seleccione el adaptador que desea asignar a este dispositivo.

6. Pulse **Add**.
Si es necesario, pulse **Go** para renovar la lista de adaptadores.

Edición de dispositivos

Puede editar un dispositivo para corregir la dirección IP o el tipo de adaptador si se produce un error o si la red ha cambiado y necesita reasignar una dirección IP.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Seleccione el dispositivo que desea editar.
5. Pulse **Edit**.
6. Configure los valores de los parámetros siguientes:

Opción	Descripción
IP Address	Escriba la dirección IP de gestión del dispositivo.
Adapter	En la lista desplegable Adapter , seleccione el adaptador que desea asignar a este dispositivo.

7. Pulse **Save**.

Supresión de un dispositivo

Puede suprimir un dispositivo de IBM Security QRadar Risk Manager. Un dispositivo suprimido se elimina de Configuration Source Management, de Configuration Monitor y de la topología.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Devices**.
5. Seleccione el dispositivo que desea suprimir.
6. Pulse **Remove**.
7. Pulse **Yes** para suprimir el dispositivo.

Resultados

Después de suprimir un dispositivo, el proceso para eliminar el dispositivo de la topología puede necesitar varios minutos.

Filtrado de la lista de dispositivos

Puede utilizar filtros para encontrar rápidamente dispositivos en la lista de dispositivos.

Acerca de esta tarea

IBM Security QRadar Risk Manager puede manejar un máximo de 5000 dispositivos de red en Configuration Source Management. Un gran número de dispositivos de red puede hacer que el desplazamiento por la lista de dispositivos sea una tarea tediosa.

La tabla siguiente describe los tipos de filtros que se pueden aplicar a la lista de dispositivos para ayudarle a encontrar dispositivos más rápidamente.

Tabla 4. Tipos de filtro para la lista de dispositivos

Opción de búsqueda	Descripción
Interface IP Address	<p>Filtra para dispositivos que tienen una interfaz que coincide con una dirección IP o el rango de CIDR.</p> <p>Escriba la dirección IP o el rango de CIDR que desea buscar en el campo IP/CIDR.</p> <p>Por ejemplo, si escribe un criterio de búsqueda de 10.100.22.6, los resultados de la búsqueda devuelven un dispositivo con una dirección IP de 10.100.22.6. Si escribe un rango de CIDR de 10.100.22.0/24, se devuelven todos los dispositivos de 10.100.22.*.</p>
Admin IP Address	<p>Filtra la lista de dispositivos basándose en la dirección IP de interfaz administrativa. Una dirección IP administrativa es la dirección IP que identifica de forma exclusiva un dispositivo.</p> <p>Escriba la dirección IP o el rango de CIDR donde desea buscar en el campo IP/CIDR .</p>
OS Version	<p>Filtra la lista de dispositivos basándose en los dispositivos de versión de sistema operativo que se están ejecutando.</p> <p>Seleccione valores para los parámetros siguientes:</p> <ul style="list-style-type: none"> • Adapter: Utilizando la lista desplegable, seleccione el tipo de adaptador que desea buscar. • Version: Utilizando la lista desplegable, seleccione los criterios de búsqueda para la versión. Por ejemplo, mayor que, menor que o igual al valor especificado. Escriba el número de versión en el campo en el que desea buscar. Si no selecciona una opción de búsqueda para la versión, los resultados incluyen todos los dispositivos que están configurados con el adaptador seleccionado, independientemente de la versión.
Model	<p>Filtra la lista de dispositivos basándose en el proveedor y el número de modelo.</p> <p>Configure valores para los parámetros siguientes:</p> <ul style="list-style-type: none"> • Vendor: Utilizando la lista desplegable, seleccione el proveedor que desea buscar. • Model: Escriba el modelo que desea buscar.

Tabla 4. Tipos de filtro para la lista de dispositivos (continuación)

Opción de búsqueda	Descripción
Hostname	Filtra la lista de dispositivo basándose en el nombre de host. Escriba el nombre de host en el que desea buscar en el campo Hostname .

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel de Risk Manager, pulse **Configuration Source Management**.
4. Pulse la pestaña **Devices**.
5. Utilizando la lista desplegable en el lado izquierdo de la lista de dispositivos, seleccione un filtro.
6. Pulse **Go**.

Resultados

Todos los resultados de búsqueda que coincidan con los criterios se visualizarán en la tabla.

Qué hacer a continuación

Para restablecer un filtro, seleccione **Interface IP Address**, borre la dirección IP/CIDR y, a continuación, pulse **Go**.

Obtención de la configuración de dispositivo

El proceso de copia de seguridad de un dispositivo para obtener una configuración de dispositivo se puede completar para un solo dispositivo de la lista de dispositivos o bien puede realizar una copia de seguridad de todos los dispositivos de la pestaña **Dispositivos**.

Acerca de esta tarea

Después de configurar los conjuntos de credenciales y conjuntos de direcciones para acceder a los dispositivos de red, debe realizar una copia de seguridad de los dispositivos para descargar la configuración de dispositivo a fin de que la información de dispositivo se incluya en la topología.

Para obtener más información sobre la planificación de las copias de seguridad automáticas de las configuraciones de dispositivo de la pestaña **Jobs**, consulte Gestionar trabajos de copia de seguridad.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Devices**.

5. Para obtener la configuración para todos los dispositivos, pulse **Backup All** en el panel de navegación y, a continuación, pulse **Yes** para continuar.
6. Para obtener la configuración de un dispositivo, seleccione el dispositivo. Para seleccionar varios dispositivos, mantenga pulsada la tecla CONTROL y seleccione todos los dispositivos necesarios. Pulse **Backup**.
7. Si es necesario, pulse **View Error** para ver los detalles de un error. Después de corregir el error, pulse **Backup All** en el panel de navegación.

Recopilación de datos de vecino

Utilice el proceso de descubrimiento para obtener datos de vecino de un dispositivo utilizando SNMP y una interfaz de línea de mandatos (CLI).

Acerca de esta tarea

Los datos de vecino se utilizan en la topología para trazar las líneas de conexión para visualizar el mapa de topología gráfica de los dispositivos de red. El botón de descubrimiento le permite seleccionar dispositivos individuales o múltiples y actualizar los datos de vecino para un dispositivo. Esta información se utiliza para actualizar las líneas de conexión para uno o varios dispositivos de la topología.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Devices**.
5. Seleccione el dispositivo para el que desea obtener datos. Para seleccionar varios dispositivos, mantenga pulsada la tecla CONTROL y seleccione todos los dispositivos necesarios.
6. Pulse **Discover**.
7. Pulse **Yes** para continuar.

Resultados

Si selecciona varios dispositivos, el proceso de descubrimiento puede tardar varios minutos en completarse.

Qué hacer a continuación

Seleccione **Run in Background** para trabajar en otras tareas.

Recopilación de datos de un repositorio de archivos

Puede obtener archivos SED (documento de elemento estándar) XML de dispositivo o archivos de entrada que contienen la configuración de dispositivo básica de un repositorio de archivos de red.

Acerca de esta tarea

El repositorio de archivos que aloja los archivos debe soportar el protocolo FTP o SFTP. IBM Security QRadar Risk Manager obtiene información de dispositivo de todos los archivos SED (documento de elemento estándar) XML ubicados en el directorio de archivo remoto del repositorio de archivos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Devices**.
5. Seleccione **Discover from Repository**.
6. Configure los valores de los parámetros siguientes:

Opción	Descripción
Protocol	En la lista desplegable Protocol , seleccione FTP o SFTP como el protocolo de comunicaciones para acceder al repositorio de archivos de configuración.
IP Address	Escriba la dirección IP del repositorio de archivos de configuración.
Remote Path	Escriba la vía de acceso de archivo remoto al directorio que contiene los archivos SED (documento de elemento estándar) XML. La vía de acceso de archivo predeterminada para archivos SED (documento de elemento estándar) es <directorio de instalación>/output. El <directorio de instalación> es la ubicación de archivo ziptie-adapter.<fecha>-<build>.zip.
Username	Escriba el nombre de usuario para iniciar la sesión en el sistema que aloja el repositorio de archivos de configuración.
Password	Escriba la contraseña para iniciar la sesión en el sistema que aloja el repositorio de archivos de configuración.

7. Pulse **OK** para descubrir un dispositivo de un repositorio.
8. Pulse **Go** para renovar la lista de dispositivos.

Gestionar trabajos de copia de seguridad

Un trabajo hace referencia a un trabajo de copia de seguridad, lo que permite realizar automáticamente una copia de seguridad de la información de configuración para todos los dispositivos de la pestaña **Devices** en una planificación.

Mediante el uso de la pestaña **Jobs** de Configuration Source Management, puede crear trabajos de copia de seguridad para todos los dispositivos o grupos individuales de dispositivos en Configuration Source Management.

Cualquier trabajo de copia de seguridad que se define en la página Configuration Source Management no afecta a la configuración de copia de seguridad de IBM Security QRadar SIEM utilizando el icono de **Copia de seguridad y recuperación** de la pestaña **Admin**. La funcionalidad de copia de seguridad y recuperación obtiene información de configuración y datos para QRadar SIEM. El trabajo de copia de seguridad sólo obtiene información para dispositivos externos.

Ver trabajos de copia de seguridad

Los trabajos y los detalles de trabajo se visualizan en la pestaña **Jobs**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Jobs**.
5. Efectúe una doble pulsación en cualquier trabajo que desee ver con mayor detalle.

Visualización del estado y los registros de los trabajos de copia de seguridad

Puede resolver los problemas de los trabajo de copia de seguridad utilizando la información de archivo de registro y estado de copia de seguridad que se proporciona en la página **Configuration Monitor**.

Acerca de esta tarea

Para ver el estado y el progreso de los trabajos de copia de seguridad, utilice la página **Configuration Monitor**. Para ver el archivo de registro de trabajos de copia de seguridad, utilice **Backup Log Viewer**.

Procedimiento

Vaya a **Riesgos > Configuration Monitor**. En las columnas siguientes de la tabla **Lista de dispositivos** se proporciona información sobre el estado de los trabajos de copia de seguridad:

Columna	Descripción
Backup Status	Indica el estado de finalización del trabajo de copia de seguridad: <ul style="list-style-type: none">• COLLECTED. El trabajo de copia de seguridad está en espera de ser procesado.• RUNNING. El trabajo de copia de seguridad está en curso.• SUCCESS. El trabajo de copia de seguridad ha finalizado satisfactoriamente.• FAILURE. El trabajo de copia de seguridad no se ha completado.
Progress	Muestra una barra de progreso que realiza un seguimiento del porcentaje de finalización del trabajo de copia de seguridad. Para actualizar la barra de progreso, pulse el icono Renovar en la página Configuration Monitor .
Backup Log	Para abrir la ventana Backup Log Viewer correspondiente al trabajo de copia de seguridad, pulse el enlace See Log de esta columna. Para actualizar la barra de progreso, pulse Renovar en la página Backup Log Viewer .

Adición de un trabajo de copia de seguridad

Puede crear trabajos de copia de seguridad para todos los dispositivos o grupos de dispositivos individuales en Configuration Source Management.

Acerca de esta tarea

Después de definir los criterios de búsqueda, defina la planificación de trabajos. La configuración de planificación se visualiza en la columna Triggers. Los desencadenantes de un trabajo representan la planificación de trabajo. Puede tener varias planificaciones que se han configurado. Por ejemplo, puede configurar dos opciones de planificación para que un trabajo se ejecuta cada lunes y el primero de cada mes.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Jobs**.
5. Seleccione **New Job > Backup**.
6. Configure los valores de los parámetros siguientes:

Opción	Descripción
Job Name	Escriba el nombre que desea aplicar a este trabajo.
Group	En la lista Group, seleccione el grupo al que desea asignar este trabajo. Si no se lista ningún grupo, puede escribir un nombre de grupo. Puede ordenar trabajos después de que se hayan asignado a un grupo.
Comment	Escriba cualquier comentario que desee asociar con este trabajo de copia de seguridad. Puede escribir hasta 255 caracteres en la descripción del trabajo de copia de seguridad.

7. Pulse **OK**.
8. Seleccione uno de los métodos de búsqueda siguientes:

Opción	Descripción
Static list	Puede utilizar una lista estática para buscar dispositivos utilizando varias opciones. Mediante el uso de la opción de lista estática, puede definir los dispositivos específicos en los que desea ejecutar el trabajo.

Opción	Descripción
Search	Escriba una dirección IP o un rango CIDR que desee incluir en el trabajo. Al definir los criterios de búsqueda, la búsqueda de dispositivos se realiza después de que el trabajo se ejecute. De este modo se asegura de que los dispositivos nuevos se incluyan en el trabajo.

9. Si elige la lista estática, defina los criterios de búsqueda:
 - a. Pulse la pestaña **Devices**.
 - b. En la lista de la pestaña **Devices**, seleccione los criterios de búsqueda. Para obtener más información, consulte Criterios de búsqueda para obtener una lista estática o búsqueda.
 - c. Pulse **Go**.
 - d. En la pestaña **Devices**, seleccione los dispositivos que desea incluir en el trabajo.
 - e. En el panel Job Details, pulse **Add selected from device view search**.
10. Si elige Search, defina los criterios de búsqueda:
 - a. Pulse la pestaña **Devices**.
 - b. Mediante la lista de la pestaña **Devices**, seleccione los criterios de búsqueda. Para obtener más información, consulte Criterios de búsqueda para una lista estática o búsqueda.
 - c. Pulse **Go**.
 - d. En el panel Job Details, pulse **Use search from devices view**. Estos criterios de búsqueda se utilizan para determinar los dispositivos que están asociados con este trabajo.
11. Pulse **Schedule** y configure valores para los parámetros siguientes:

Opción	Descripción
Name	Escriba un nombre para la configuración de planificación.
Start time	Seleccione una hora y fecha en que desea iniciar el proceso de copia de seguridad. La hora debe especificarse en hora militar.
Frequency	Seleccione la frecuencia que desea asociar a esta planificación.
Cron	Escriba una expresión cron, que se interpreta en hora media de Greenwich (GMT). Para obtener ayuda, póngase en contacto con el administrador.
Specify End Date	Opcional. Seleccione una fecha para finalizar el trabajo de planificación.

12. Pulse **Guardar** en el panel Trigger.
13. Repita los pasos 11 y 12 para crear varias planificaciones.
14. Si desea ejecutar el trabajo inmediatamente, pulse **Run Now**.
15. Pulse **Yes** para continuar.

Edición de un trabajo de copia de seguridad

Puede editar trabajos de copia de seguridad.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Jobs**.
5. Efectúe una doble pulsación en el trabajo que desea editar.
6. Elija una de las opciones de búsqueda siguientes en el parámetro **Selection Type**:

Opción	Descripción
Static list	Una lista estática le permite buscar dispositivos utilizando varias opciones. Mediante el uso de la opción de lista estática, puede definir los dispositivos específicos en los que desea ejecutar el trabajo.
Search	Escriba una dirección IP o un rango CIDR que desee incluir en el trabajo. Al definir los criterios de búsqueda, la búsqueda de dispositivos se produce después de que se haya ejecutado el trabajo. De este modo se asegura de que los dispositivos nuevos se incluyan en el trabajo.

7. Si elige **Static List**, defina los criterios de búsqueda:
 - a. Pulse la pestaña **Devices**.
 - b. En la lista de la pestaña **Devices**, seleccione los criterios de búsqueda.
 - c. Pulse **Go**.
 - d. En la pestaña **Devices**, seleccione los dispositivos que desea incluir en el trabajo.
 - e. En el panel **Job Details**, pulse **Add selected from device view search**.
8. Si elige **Search**, defina los criterios:
 - a. Pulse la pestaña **Devices**.
 - b. Mediante la lista de la pestaña **Devices**, seleccione los criterios de búsqueda.
 - c. Pulse **Go**.
 - d. En el panel **Job Details**, pulse **Use search from devices view**. Estos criterios de búsqueda se utilizan para determinar los dispositivos que están asociados con este trabajo.
9. Pulse **Schedule** y configure valores para los parámetros siguientes:

Opción	Descripción
Name	Escriba un nombre para la configuración de planificación.
Start time	Seleccione una hora y fecha en que desea iniciar el proceso de copia de seguridad. La hora debe especificarse en hora militar.

Opción	Descripción
Frequency	Seleccione la frecuencia que desea asociar a esta planificación.
Cron	Escriba una expresión cron, que se interpreta en hora media de Greenwich (GMT). Para obtener ayuda, póngase en contacto con el administrador.
Specify End Date	Opcional. Seleccione una fecha para finalizar el trabajo de planificación.

10. Pulse **Save**.
11. Pulse **Ejecutar ahora**.
12. Repita los pasos 9 y 10, según sea necesario.
13. Pulse **Yes** para continuar.

Renombrar un trabajo de copia de seguridad

Puede renombrar un trabajo de copia de seguridad

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Jobs**.
5. Seleccione el trabajo de copia de seguridad de que desea renombrar.
6. Pulse **Rename**.
7. Configure los valores de los parámetros siguientes:

Opción	Descripción
Job Name	Escriba el nombre que desea aplicar a este trabajo.
Group	En la lista Group , seleccione el grupo al que desea asignar este trabajo. También puede especificar un nombre de grupo nuevo.
Comment	Opcional. Escriba cualquier comentario que desee asociar con este trabajo de copia de seguridad. Puede escribir hasta 255 caracteres en la descripción del trabajo de copia de seguridad.

8. Pulse **OK**.

Supresión de un trabajo de copia de seguridad

Puede suprimir un trabajo de copia de seguridad.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. Pulse la pestaña **Jobs**.

5. Seleccione el trabajo de copia de seguridad que desea suprimir.
6. Pulse **Suprimir**.

Configurar protocolos

Para que IBM Security QRadar Risk Manager se comunice con los dispositivos, debe definir el método de comunicación (protocolo) necesario para la comunicación con los dispositivos de red.

QRadar Risk Manager proporciona la configuración de protocolo predeterminada para el sistema. Si necesita definir protocolos, puede definir protocolos para permitir que QRadar Risk Manager obtenga y actualice la configuración de dispositivo. Muchos entornos de red tienen diferentes protocolos de comunicación de tipos o funciones diferentes del dispositivo. Por ejemplo, es posible que un direccionador utilice un protocolo distinto de los cortafuegos de la red. Para obtener una lista de protocolos soportados por fabricante de dispositivo, consulte la publicación *IBM Security QRadar Risk Manager Adapter Configuration Guide*.

QRadar Risk Manager utiliza conjuntos de protocolo para definir grupos de protocolos para un conjunto de dispositivos que requieren un protocolo de comunicaciones específico. Puede asignar dispositivos a grupos de red, lo que le permite agrupar conjuntos de protocolos y conjuntos de direcciones para los dispositivos.

Los conjuntos de protocolos son un conjunto con nombre de protocolos para un conjunto de dispositivos que requieren credenciales de protocolo específicas.

Los conjuntos de direcciones son direcciones IP que definen el grupo de red.

Configuración de protocolos

Puede definir protocolos para obtener y actualizar la configuración de dispositivo.

Acerca de esta tarea

Puede configurar los siguientes valores para los parámetros de protocolo.

Tabla 5. Parámetros de protocolo

Protocolo	Parámetro
SSH	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • Port: Escriba el puerto en el que desea que se utilice el protocolo SSH al comunicarse con los dispositivos de red y realizar copia de seguridad de dichos dispositivos. <p>El puerto de protocolo SSH predeterminado es el 22.</p> <ul style="list-style-type: none"> • Version: Seleccione la versión de SSH que desea que este grupo de red utilice al comunicarse con los dispositivos de red. Las opciones disponibles son las siguientes: <p>Auto: Esta opción detecta automáticamente la versión de SSH que se debe utilizar al comunicarse con dispositivos de red.</p> <p>1: Utilice SSH-1 al comunicarse con dispositivos de red.</p> <p>2: Utilice SSH-2 al comunicarse con dispositivos de red.</p>
Telnet	<p>Escriba el número de puerto que desea que el protocolo Telnet utilice al comunicarse con los dispositivos de red y realizar la copia de seguridad de dichos dispositivos.</p> <p>El puerto de protocolo Telnet predeterminado es el 23.</p>
HTTPS	<p>Escriba el número de puerto que desea que el protocolo HTTPS utilice al comunicarse con los dispositivos de red y realizar la copia de seguridad de dichos dispositivos.</p> <p>El puerto de protocolo HTTPS predeterminado es el 443.</p>
HTTP	<p>Escriba el número de puerto que desea que el protocolo HTTP utilice al comunicarse con los dispositivos de red y realizar la copia de seguridad de dichos dispositivos.</p> <p>El puerto de protocolo HTTP predeterminado es el 80.</p>
SCP	<p>Escriba el número de puerto que desea que el protocolo SCP utilice al comunicarse con los dispositivos de red y realizar la copia de seguridad de dichos dispositivos.</p> <p>El puerto de protocolo SCP predeterminado es el 22.</p>

Tabla 5. Parámetros de protocolo (continuación)

Protocolo	Parámetro
SFTP	<p>Escriba el número de puerto que desea que el protocolo SFTP utilice al comunicarse con los dispositivos de red y realizar la copia de seguridad de dichos dispositivos.</p> <p>El puerto de protocolo SFTP predeterminado es el 22.</p>
FTP	<p>Escriba el número de puerto que desea que el protocolo FTP utilice al comunicarse con los dispositivos de red y realizar la copia de seguridad de dichos dispositivos.</p> <p>El puerto de protocolo SFTP predeterminado es el 22.</p>
TFTP	<p>El protocolo TFTP no tiene ninguna opción configurable.</p>
SNMP	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • Port: Escriba el número de puerto que desea que el protocolo SNMP utilice al comunicarse con los dispositivos de red y realizar copia de seguridad de dichos dispositivos. • Timeout(ms): Seleccione la cantidad de tiempo, en milisegundos, que desea utilizar para determinar un tiempo de espera de comunicación. • Retries: Seleccione el número de veces que desea volver a intentar las comunicaciones con un dispositivo. • Version: Seleccione la versión de SNMP que desea utilizar para las comunicaciones. Las opciones son v1, v2 o v3. • V3 Authentication: Seleccione el algoritmo que desea utilizar para autenticar condiciones de excepción SNMP. • V3 Encryption: Seleccione el protocolo que desea utilizar para descifrar condiciones de excepción SNMP.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. En el menú de navegación, pulse **Protocols**.
5. Configure un grupo de red nuevo:
 - a. En el panel **Network Groups**, pulse el icono **Add (+)**.
 - b. Escriba un nombre para un grupo de red.
 - c. Pulse **OK**.

- d. Utilice los iconos **Move Up** y **Move Down** para priorizar los grupos de red. Mueva el grupo de red que desea que tenga la primera prioridad a la parte superior de la lista.
6. Configure el conjunto de direcciones:
 - a. En el campo **Add Address**, escriba la dirección IP o el rango CIDR que desea aplicar al grupo de red y, a continuación, pulse el icono **Add (+)**. Por ejemplo, escriba un rango de direcciones IP utilizando un guión o comodín (*) para indicar un rango, por ejemplo 10.100.20.0-10.100.20.240 o 1.1.1*. Si escribe 1.1.1.*, se incluyen todas las direcciones IP que cumplen ese requisito.
 - b. Repita para todas las direcciones IP que desea añadir al conjunto de direcciones para este grupo de red.
7. Configure el conjunto de protocolos:
 - a. En el panel **Network Groups**, asegúrese de que se ha seleccionado el grupo de red para el que desea configurar protocolos.
 - b. Marque los recuadros de selección para aplicar un protocolo para el rango de direcciones IP asignadas al grupo de red que ha creado. Al borrar el recuadro de selección se desactiva la opción de comunicaciones para el protocolo al intentar realizar una copia de seguridad de un dispositivo de red.
 - c. Para cada protocolo que ha seleccionado, configure los valores de los parámetros.
 - d. Utilice los iconos **Move Up** y **Move Down** para priorizar los protocolos. Mueva a la parte superior de la lista el protocolo que desea que tenga la primera prioridad.
8. Pulse **OK**.

Configuración de la planificación de descubrimiento

Puede configurar una planificación de descubrimiento para llenar ARP, tablas MAC e información de vecinos para los dispositivos. La planificación de descubrimiento también permite que se añadan dispositivos nuevos automáticamente al inventario.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Plug-ins**.
3. En el panel **Risk Manager**, pulse **Configuration Source Management**.
4. En el menú de navegación, pulse **Schedule Discovery**.
5. Seleccione el recuadro de selección **Enable periodic discovery** para habilitar el descubrimiento de planificación.
6. Configure los valores de los parámetros siguientes:

Opción	Descripción
Name	Escriba un nombre para la configuración de planificación.
Start time	Seleccione una hora y fecha en que desea iniciar el proceso de copia de seguridad. La hora debe especificarse en hora militar.
Frequency	Seleccione la frecuencia que desee asociar con esta planificación.

Opción	Descripción
Cron	Escriba una expresión cron, que se interpreta en hora media de Greenwich (GMT). Para obtener ayuda, póngase en contacto con el administrador.
Specify End Date	Opcional. Seleccione una fecha para finalizar el trabajo de planificación.
Crawl and discover new devices	Marque el recuadro de selección si desea que el proceso de descubrimiento descubra dispositivos nuevos. Quite la marca del recuadro de selección si no desea añadir dispositivos nuevos al inventario.

7. Pulse **OK**.

Capítulo 5. Gráfico de topología de red

En IBM Security QRadar Risk Manager, puede utilizar el gráfico del modelo de topología para ver, filtrar e investigar la conectividad física de su red.

El gráfico de topología de red se genera a partir de la información de configuración que se obtiene de dispositivos como por ejemplo cortafuegos, direccionadores, conmutadores y sistemas IPS (Sistema de prevención de intrusiones). Puede pasar el cursor por encima de las líneas de conexión para visualizar la información de conexión de red. Puede filtrar la topología buscando vías de acceso de ataque potenciales en protocolos, puertos o vulnerabilidades permitidos. Puede ver el flujo de tráfico entre dispositivos o subredes y puede ver reglas de dispositivo.

Puede utilizar el gráfico de topología para completar las tareas siguientes:

- Visualizar vías de acceso de red específicas y la dirección de tráfico para el análisis avanzado de amenazas.
- Incorporar correlaciones de seguridad IPS pasivas al gráfico de topología.
- Agrupar dispositivos para organizar y simplificar la vista.
- Añadir dispositivos a grupos y eliminar dispositivos de grupos.
- Recolocar iconos en el gráfico mediante el ratón.
- Guardar diseños de gráfico de topología.
- Redenominar dispositivos y grupos.
- Cree y guardar filtros de búsqueda para la topología de red que se basen en protocolos, puertos o vulnerabilidades.
- Ver información detallada de conexión entre dispositivos y subredes.
- Ver reglas de dispositivo en conexiones de nodo de topología con los puertos y protocolos permitidos.
- Ver dispositivos NAT (Conversión de direcciones de red), indicadores NAT e información sobre correlaciones NAT.
- Ver dispositivos de seguridad de red virtual que tienen múltiples contextos.

Cuando busca y ve los puertos y los protocolos permitidos entre dispositivos, solo puede ver conexiones que utilizan protocolos TCP, UDP e ICMP en el gráfico de topología.

Búsquedas de gráfico de topología

Utilice la característica de búsqueda de topología para ver e investigar diversos elementos de la infraestructura de la red.

Puede utilizar la característica de búsqueda para filtrar la vista de topología y centrarse en vías de acceso de red, hosts, subredes y otros elementos de la red. Puede refinar la búsqueda hasta el nivel de puerto o protocolo, por ejemplo para buscar vías de ataque potenciales en protocolos o puertos permitidos.

Puede buscar sucesos pulsando con el botón derecho del ratón sobre dispositivos y subredes o buscar flujos pulsando con el botón derecho del ratón sobre subredes.

Pulse **Acciones** para acceder al menú **Buscar**. Especifique los criterios de búsqueda en el panel Criterios de búsqueda. A continuación se muestran algunas de las opciones de búsqueda que puede utilizar:

Búsqueda de hosts

Si busca un host, se visualizan todos los dispositivos que comunican con ese host. Si el host no coincide con una interfaz en un dispositivo pero se incluye en la subred, se muestra esa subred y todos los dispositivos conectados.

Búsqueda de redes

Búsqueda de un CIDR concreto, por ejemplo, 10.3.51.200/24.

Si está buscando varios CIDRs, asegúrese de que los CIDRs son válidos y están separados por comas, por ejemplo, 10.51.0.0/24,10.51.01/24.

Búsqueda de vías de acceso

Una búsqueda de vía de acceso visualiza la dirección de tráfico, los protocolos total o parcialmente permitidos y las reglas de dispositivo. Si existen conexiones de puerto entre redes, se visualizan los puertos permitidos en un resumen de vía de acceso.

Un **cuadrado rojo** en una conexión puede indicar que el tráfico de red está bloqueado. Si el tráfico de red se mueve del nodo A al nodo B, entonces un **cuadrado rojo** en la conexión entre el nodo y el nodo B puede indicar lo siguiente:

- Las reglas de cortafuegos en el nodo B están bloqueando el tráfico.
- No hay ninguna ruta en el nodo B para reenviar paquetes.

Pase el puntero del ratón sobre el **cuadrado rojo** para obtener más información.

Puede buscar aplicaciones cuando selecciona una vía de acceso en la topología; consulte Búsqueda de aplicaciones. El indicador NAT es un **punto verde**. Esto se muestra en el gráfico de topología cuando la búsqueda devuelve una vía de acceso que contiene conversiones de origen o destino.

En el menú **Acciones** puede acceder al menú **Buscar**.

Búsqueda de aplicaciones

Buscar aplicaciones en la topología de IBM Security QRadar Risk Manager desde la pestaña **Risks** o cuando se selecciona una vía de acceso en la topología, para ver detalles de aplicación.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Topology**.
3. Pulse **Search > New Search**.
4. Seleccione la opción **Path**.
5. Pulse **Select Applications**.
6. En el menú desplegable **Device Adaptador**, seleccione el tipo de adaptador de dispositivo necesario.
7. En el campo **Application Name**, entre el descriptor para la aplicación.

8. Pulse **Search**.
9. Pulse cada aplicación en la que desea buscar en el campo **Search Results** y pulse **Add**.
10. Pulse **OK**.

Búsqueda de vulnerabilidades

Puede buscar vulnerabilidades en el menú **Buscar** si tiene un sistema prevención de intrusiones (IPS) en el gráfico de Topología.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Topología**.
3. Pulse **Buscar > Nueva búsqueda**.
4. Seleccione la opción **Vía de acceso**.
5. Pulse **Seleccionar vulnerabilidad**.
6. En el menú **Buscar por**, seleccione la categoría de vulnerabilidad.
7. En el **Campo** junto al menú **Buscar por**, especifique el número de ID de la vulnerabilidad.
8. Pulse **Buscar**.
9. Pulse cada vulnerabilidad en la que desea buscar en el campo **Resultados de búsqueda** y pulse **Añadir**.
10. Pulse **Guardar**.
11. Pulse **Buscar** para ver los resultados.

Consulte **Añadir** un sistema de prevención de intrusiones (IPS) si no ve las opciones de búsqueda de vulnerabilidades.

Indicadores NAT en resultados de búsqueda

Un indicador NAT, que es un punto verde sólido, aparece en el gráfico de topología si la búsqueda encuentra una vía de acceso que contiene conversiones de origen o de destino.

Acerca de esta tarea

Un indicador NAT indica que la dirección IP de destino que se ha especificado en el filtro de vía de acceso puede no ser el destino final. Pase el cursor por encima del indicador para ver la información siguiente sobre las conversiones.

Tabla 6. Información disponible del indicador NAT

Parámetro	Descripción
Source	IP o CIDR de origen convertidos.
Source Port(s)	Puertos de origen convertidos, si es aplicable.
Translated Source	Resultado de la conversión que se ha aplicado al origen.
Translated Source Port(s)	Resultado de la conversión que se ha aplicado al puerto o los puertos de origen, si es aplicable.
Destination	IP o CIDR de destino convertidos.
Destination Port(s)	Puertos de destino convertidos, si es aplicable.

Tabla 6. Información disponible del indicador NAT (continuación)

Parámetro	Descripción
Translated Destination	Resultado de la conversión que se ha aplicado al destino.
Translated Destination Port(s)	Resultado de la conversión que se ha aplicado al puerto o los puertos de destino, si es aplicable.
Phase	Fase de direccionamiento cuando se ha aplicado la conversión. Las conversiones se aplican antes o después del direccionamiento.

Añadir un sistema de prevención de intrusiones (IPS)

Si la lista **Configuration Source Management** incluye un dispositivo de sistema de prevención de intrusiones (IPS) puede añadir un IPS a las conexiones entre nodos de dispositivo a subred y entre nodos de dispositivo a dispositivo.

Acerca de esta tarea

La adición de una conexión IPS es útil para determinar la ubicación del IPS si el dispositivo es pasivo.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Topología**.
3. Mueva el puntero del ratón sobre la línea de conexión que enlaza un nodo de dispositivo y un nodo de subred.
4. Pulse el botón derecho del ratón en línea de conexión y seleccione **Añadir IPS**.
5. Seleccione el dispositivo y las interfaces a añadir en las listas siguientes:

Opción	Descripción
Place IPS	Seleccione una ubicación de la lista.
Connect IPS interface to device	Seleccione una interfaz para conectarla al dispositivo. Si hay varias opciones de dispositivos, debe seleccionar un dispositivo (consulte la opción siguiente).
	Seleccione el dispositivo que desea conectar al IPS. Esta opción está disponible si hay varios dispositivos.
Connect IPS interface	Seleccione una interfaz para conectarla a la subred.

6. Utilizando las listas, seleccione el dispositivo y las interfaces para añadir la conexión IPS a la topología.
7. Pulse **OK**. Si desea añadir un IPS a un dispositivo que está en un grupo, expanda el grupo para añadir el IPS.

Eliminar un Sistema de prevención de intrusiones (IPS)

Puede eliminar una conexión IPS.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Topology**.
3. Mueva el puntero del ratón sobre la línea de conexión que enlaza un nodo de dispositivo y un nodo de subred.
4. Efectúe una doble pulsación en la línea de conexión y seleccione la opción para eliminar idp IPS.
5. Pulse **OK**.

Grupos de dispositivos de topología

Agrupe dispositivos en una página de Topología para organizar y simplificar gráficos de topología complicados.

Seleccione un dispositivo en la ventana Topología actual y pulse el menú **Acciones** de la barra de herramientas o utilice el menú contextual para acceder a la característica **Grupos** de dispositivos.

Diseño de gráfico de topología

Guarde el diseño de topología como la vista actual. Cuando guarda el diseño, está guardando la representación gráfica de la topología.

El diseño guardado queda como la pantalla de topología predefinida hasta que lo restablece pulsando **Acciones > Diseño > Restablecer diseño**.

Cuando restablece un diseño, seleccione **Guardar diseño** si desea retenerlo.

Descargue la topología actual como imagen PNG o un dibujo VDX (Visio XML), pulsando **Acciones > Descargar**.

Capítulo 6. Policy Monitor

Las organizaciones utilizan Policy Monitor para definir preguntas de riesgo específicas sobre la red a fin de evaluar o supervisar el riesgo que se basa en el análisis de los indicadores de riesgo.

En Policy Monitor, puede definir políticas, evaluar el cumplimiento de una política, evaluar los resultados de las preguntas y supervisar riesgos nuevos.

Se proporcionan plantillas de pregunta predeterminadas para que evalúe y supervise el riesgo en la red. Puede utilizar una de las plantillas de pregunta predeterminadas como base para sus propias preguntas o puede crear una pregunta nueva. Puede encontrar las plantillas de pregunta predeterminadas en el menú **Grupo** en la página Policy Monitor.

Puede elegir en la lista siguiente de indicadores de riesgo:

- La actividad de red mide el riesgo basándose en las comunicaciones de red que se han producido en el pasado.
- La configuración y la topología miden el riesgo que se basa en posibles conexiones de red y comunicación.
- Las vulnerabilidades miden el riesgo que se basa en los datos de exploración de vulnerabilidades y configuración de red que se recopilan de los activos de red.
- Las reglas de cortafuegos miden el riesgo basándose en la obligatoriedad o la ausencia de reglas de cortafuegos que se aplican en la red.

Puede definir pruebas que se basen en los indicadores de riesgo y, a continuación, restringir los resultados de prueba para filtrar la consulta para obtener resultados específicos o infracciones.

Los profesionales de seguridad crean preguntas para los activos o dispositivos/reglas para señalar los riesgos en las redes. El nivel de riesgo para un activo o un dispositivo/regla se indica después de que envía una pregunta a Policy Monitor. Puede aprobar resultados devueltos de activos o definir cómo desea que el sistema responda a resultados no aprobados.

Puede utilizar los resultados para evaluar los casos de riesgo para muchos escenarios de seguridad diversos, por ejemplo:

- Evaluar si los usuarios han utilizado protocolos prohibidos para comunicarse.
- Evaluar si los usuarios, en redes específicas, puede comunicarse con redes o activos prohibidos.
- Evaluar las reglas de cortafuegos satisfacen la política corporativa.
- Priorizar vulnerabilidades evaluando qué sistemas pueden estar comprometidos como resultados de una configuración de red.

Preguntas de Policy Monitor

Puede definir preguntas en Policy Monitor para evaluar y supervisar el riesgo basándose en la actividad de red, las vulnerabilidades y las reglas de cortafuegos.

Al enviar una pregunta, la búsqueda de topología se basa en el tipo de datos que ha seleccionado:

- Para preguntas basadas en activos, la búsqueda se basa en los activos de red que han violado una política definida o activos que han introducido un riesgo en la red.
- Para preguntas basadas en dispositivos/reglas, la búsqueda identifica las reglas de un dispositivo que han violado una política definida o han introducido un riesgo en la red.
- Si una pregunta se basa en la conformidad de activo, la búsqueda identifica si un activo está en conformidad con una prueba de referencia CIS.

Nota: Si ha configurado IBM Security QRadar para varios dominios, las preguntas de activo solamente supervisan los activos del dominio predeterminado. Las preguntas de conformidad de activo supervisan los activos del dominio predeterminado a menos que haya configurado otro dominio en la ventana **Admin > Gestión de dominios**. Para obtener más información sobre la gestión de los dominios, consulte la publicación *IBM Security QRadar SIEM Administration Guide*.

Las preguntas de dispositivos/reglas buscan violaciones en las reglas y la política y no tienen componentes de prueba restrictivos. También puede hacer preguntas de dispositivos/reglas para aplicaciones.

Las pruebas de activos se dividen en estas categorías:

- Una *prueba contribuyente* utiliza los parámetros de pregunta para examinar los indicadores de riesgo que son específicos en la pregunta. Se generan resultados de datos de riesgo, que se pueden filtrar adicionalmente utilizando una *prueba restrictiva*. Las pruebas contribuyentes se muestran en el área **Which tests do you want to include in your question**. Las pruebas contribuyentes devuelven datos basándose en los activos detectados que coinciden con la pregunta de prueba.
- Un *prueba restrictiva* limita los resultados devueltos por una pregunta de *prueba contribuyente*. Las pruebas restrictivas sólo se visualizan en el área **Which tests do you want to include in your question** después de añadir una prueba contribuyente. Solo puede añadir pruebas restrictivas después de incluir una prueba contribuyente en la pregunta. Si elimina o suprime una pregunta de prueba contribuyente, la pregunta de prueba restrictiva no se puede guardar.

Las preguntas de conformidad de activo buscan los activos que no están en conformidad con las pruebas de referencia CIS. Las pruebas que se incluyen en la prueba de referencia CEI se configuran con Compliance Benchmark Editor.

Tareas relacionadas:

“Envío de una pregunta” en la página 45

Envíe una pregunta para determinar el riesgo asociado. También puede determinar el tiempo que se necesita para ejecutar una pregunta y la cantidad de datos que se están consultando.

“Edición de una prueba de referencia de conformidad” en la página 47

Utilice el Compliance Benchmark Editor en IBM Security QRadar Risk Manager para añadir o eliminar pruebas de las pruebas de referencia CIS predeterminadas.

Factor de importancia

El Factor de importancia se utiliza para calcular la puntuación de riesgo y definir el número de resultados devueltos para una pregunta.

El rango es de 1 (importancia baja) a 10 (alta importancia). El valor predeterminado es 5.

Tabla 7. Matriz de resultados de factor de importancia

Factor de importancia	Resultados devueltos para pruebas de activos	Resultados devueltos para pruebas de dispositivo/regla
1 (importancia baja)	10.000	1.000
10 (alta importancia)	1	1

Por ejemplo, una pregunta de política que indica **have accepted communication from the internet and include only the following networks (DMZ)** necesitará un factor de importancia alta de 10 porque los resultados de la pregunta son inaceptables debido a la naturaleza de alto riesgo de la pregunta. Sin embargo, una pregunta de política que indica que se ha aceptado la comunicación de internet y sólo se incluyen las siguientes aplicaciones de entrada (P2P) puede necesitar un factor de importancia más baja porque los resultados de la pregunta no indican riesgo alto, pero puede supervisar esta comunicación con fines informativos.

Ver información de preguntas

Puede ver información sobre preguntas y parámetros de Policy Monitor en la página Policy Monitor.

Si desea ver más información sobre cualquier pregunta, puede seleccionar la pregunta para ver la descripción.

Si la pregunta está en modalidad de supervisión cuando la selecciona, puede ver los sucesos y delitos que se generan como resultado de la pregunta seleccionada.

Creación de una pregunta de activo

Buscar activos en la red que infrinjan una política definida o activos que presenten riesgos.

Acerca de esta tarea

Las preguntas de Policy Monitor se evalúan de arriba a abajo. El orden de las preguntas de Policy Monitor afecta a los resultados.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, seleccione **New Asset Question**.
4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.
5. En la lista **Evaluate On**, seleccione una de las opciones siguientes:

Opción	Descripción
Actual Communication	Incluye activos en los que se han detectado comunicaciones que utilizan conexiones.

Opción	Descripción
Possible Communication	Incluye activos en los que se permiten las comunicaciones a través de la topología de red, por ejemplo cortafuegos. Utilice estas preguntas para investigar si son posibles comunicaciones específicas, independientemente de que se haya detectado una comunicación.

6. En la lista **Importance Factor**, seleccione el nivel de importancia que desea asociar a esta pregunta. El Factor de importancia se utiliza para calcular la puntuación de riesgo y definir el número de resultados devueltos para una pregunta.
7. Especifique el rango de tiempo para la pregunta.
8. En el campo **Which tests do you want to include in your question**, seleccione el icono de suma (+) junto a las pruebas que desea incluir.
9. Configure los parámetros para las pruebas en el campo **Find Assets that**. Los parámetros configurables están en negrita y subrayados. Pulse cada parámetro para ver las opciones disponibles para la pregunta.
10. En el área de grupos, pulse los recuadros de selección pertinentes para asignar la pertenencia a grupos a esta pregunta.
11. Pulse **Save Question**.

Qué hacer a continuación

Envíe una pregunta para determinar el factor de riesgo. Consulte “Envío de una pregunta” en la página 45.

Conceptos relacionados:

“Factor de importancia” en la página 42

El Factor de importancia se utiliza para calcular la puntuación de riesgo y definir el número de resultados devueltos para una pregunta.

“Agrupar preguntas” en la página 58

Puede agrupar y ver las preguntas basándose en los criterios elegidos

Creación de una pregunta que pruebe las reglas en los dispositivos

Crear una pregunta de dispositivos/reglas en Policy Monitor para identificar las reglas de un dispositivo que han violado una política definida o han presentado riesgos en la red.

Acerca de esta tarea

Las preguntas de Policy Monitor se evalúan de arriba a abajo. El orden de las preguntas de Policy Monitor afecta a los resultados.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, pulse **New Device/Rules Question**.
4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.

5. En la lista **Importance Factor**, seleccione el nivel de importancia que desea asociar a esta pregunta.
6. En el campo **Which tests do you want to include in your question**, seleccione el icono + junto a las pruebas que desea incluir.
7. En el campo **Find Devices/Rules that**, configure los parámetros para las pruebas.
Los parámetros configurables están en negrita y subrayados. Pulse cada parámetro para ver las opciones disponibles para la pregunta.
8. En el área de grupos, pulse los recuadros de selección pertinentes para asignar la pertenencia a grupos a esta pregunta.
9. Pulse **Save Question**.

Qué hacer a continuación

Envíe una pregunta para determinar el factor de riesgo.

Conceptos relacionados:

“Factor de importancia” en la página 42

El Factor de importancia se utiliza para calcular la puntuación de riesgo y definir el número de resultados devueltos para una pregunta.

“Agrupar preguntas” en la página 58

Puede agrupar y ver las preguntas basándose en los criterios elegidos

Tareas relacionadas:

“Envío de una pregunta”

Envíe una pregunta para determinar el riesgo asociado. También puede determinar el tiempo que se necesita para ejecutar una pregunta y la cantidad de datos que se están consultando.

Envío de una pregunta

Envíe una pregunta para determinar el riesgo asociado. También puede determinar el tiempo que se necesita para ejecutar una pregunta y la cantidad de datos que se están consultando.

Acerca de esta tarea

Al enviar una pregunta, la información resultante depende de los datos que se consultan; activos o dispositivos y reglas.

Después de enviar una pregunta de Policy Monitor, puede ver cuánto tiempo tarda la pregunta en ejecutarse. El tiempo que se necesita para ejecutar la política también indica la cantidad de datos que se consultan. Por ejemplo, si el tiempo de ejecución es de 3 horas, hay 3 horas de datos. Puede ver la hora en la columna **Policy Execution Time** para determinar una frecuencia intervalo eficiente a definir para las preguntas que desea supervisar. Por ejemplo, si el tiempo de ejecución política es de 3 horas, el intervalo de evaluación de política debe ser mayor que 3 horas.

Nota: Cuando se edita una pregunta después de haberla enviado y la edición afecta las pruebas asociadas, es posible que se tarde hasta una hora para ver esos cambios.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. Seleccione la pregunta que desea enviar.
4. Pulse **Submit Question**.

Creación de una pregunta de conformidad de activo

Crear una pregunta de conformidad de activo en Policy Monitor para buscar activos en la red que fallan las pruebas de referencia CEI.

Antes de empezar

Las preguntas de Policy Monitor se evalúan de arriba a abajo. El orden de las preguntas de Policy Monitor afecta a los resultados.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, seleccione **New Asset Compliance Question**.
4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.
5. Seleccione el nivel de importancia que desea asociar con esta pregunta de la lista **Importance Factor**.
6. En el campo **Which tests do you want to include in your question**, seleccione el icono de suma (+) junto a la prueba **test compliance of assets in asset saved searches with CIS benchmarks**.
Seleccione esta prueba varias veces, si es necesario.
7. Configure los parámetros para las pruebas en el campo **Find Assets that**.
Pulse cada parámetro para ver las opciones disponibles para la pregunta. Especifique varias búsquedas guardadas de activos y varias listas de comprobación en esta prueba, si es necesario.
8. En el área de grupo, pulse los recuadros de selección pertinentes para asignar la pertenencia a grupos a esta pregunta.
Las preguntas de conformidad de activos se deben asignar a un grupo para incluirlas en paneles de control o informes de conformidad.
9. Pulse **Save Question**.

Qué hacer a continuación

Asocie un perfil de prueba de referencia con la pregunta que ha creado y supervise los resultados de dicha pregunta.

Conceptos relacionados:

“Factor de importancia” en la página 42

El Factor de importancia se utiliza para calcular la puntuación de riesgo y definir el número de resultados devueltos para una pregunta.

“Agrupar preguntas” en la página 58

Puede agrupar y ver las preguntas basándose en los criterios elegidos

Tareas relacionadas:

“Supervisión de preguntas de conformidad de activos”

Supervisar preguntas de conformidad de activos seleccionando perfiles de exploración de CIS. Se ejecutan exploraciones de prueba de referencia CIS en los activos.

Edición de una prueba de referencia de conformidad

Utilice el Compliance Benchmark Editor en IBM Security QRadar Risk Manager para añadir o eliminar pruebas de las pruebas de referencia CIS predeterminadas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. Pulse **Policy Monitor**.
3. Pulse **Compliance** para abrir la ventana Compliance Benchmark Editor.
4. En el menú de navegación, pulse la prueba de referencia CIS predeterminada que desea editar.
5. En el panel **Compliance**, pulse el recuadro de selección **Enabled** en la fila que se ha asignado a la prueba que desea incluir.

Pulse en cualquier lugar de una fila para ver una descripción de la prueba de referencia, una lógica de despliegue e información sobre elementos a comprobar antes de habilitar la prueba.

Cuando cree una lista de comprobación de CIS personalizada, tenga en cuenta que algunas pruebas de referencia que no están incluidas de forma predeterminada pueden tardar mucho tiempo en ejecutarse. Para obtener más información, consulte la documentación de CIS.

Qué hacer a continuación

Cree una pregunta de conformidad de activo para probar activos en la prueba de referencia que ha editado.

Tareas relacionadas:

“Creación de una pregunta de conformidad de activo” en la página 46

Crear una pregunta de conformidad de activo en Policy Monitor para buscar activos en la red que fallan las pruebas de referencia CEI.

Supervisión de preguntas de conformidad de activos

Supervisar preguntas de conformidad de activos seleccionando perfiles de exploración de CIS. Se ejecutan exploraciones de prueba de referencia CIS en los activos.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Supervisor de políticas**.
3. En el panel **Preguntas**, seleccione la pregunta de conformidad de activos que desea supervisar.
4. Pulse **Supervisor** para abrir la ventana Resultados de supervisor.
5. Seleccione un perfil de prueba de referencia en la lista **Which benchmark profile to associate with this question?**

El perfil de exploración de referencia seleccionado utiliza un explorador QRadar Vulnerability Manager que está asociado con un dominio. El nombre del dominio se muestra en el área **Benchmark Profile Details**. Para obtener

más información sobre la gestión de los dominios, consulte la publicación *IBM Security QRadar SIEM Administration Guide*.

6. Seleccione el recuadro de selección **Enable the monitor results function for this question/simulation**.

7. Pulse **Guardar supervisor**.

La supervisión empieza a la hora de inicio de exploración establecida en la pestaña **Cuándo explorar** al crear el perfil de exploración de prueba de referencia.

Tareas relacionadas:

“Edición de una prueba de referencia de conformidad” en la página 47

Utilice el Compliance Benchmark Editor en IBM Security QRadar Risk Manager para añadir o eliminar pruebas de las pruebas de referencia CIS predeterminadas.

“Creación de una pregunta de conformidad de activo” en la página 46

Crear una pregunta de conformidad de activo en Policy Monitor para buscar activos en la red que fallan las pruebas de referencia CEI.

Exportar e importar preguntas de Policy Monitor

Los usuarios con privilegios administrativos pueden exportar e importar preguntas de Policy Monitor.

La exportación e importación de preguntas proporcionan un método para realizar la copia de seguridad de las preguntas y compartirlas con otros usuarios de IBM Security QRadar Risk Manager.

Restricciones para la información confidencial

Es posible que la información confidencial de políticas o de empresa se incluya en dependencias. Al exportar o importar preguntas de Policy Monitor, no se incluyen los datos confidenciales contenidos en las dependencias.

Las preguntas de Policy Monitor pueden contener los tipos siguientes de dependencias:

- Componentes básicos de activo
- Búsquedas guardadas de activo
- Redes
- Ubicaciones de red remota
- Ubicaciones de red geográfica
- Conjuntos de referencia

Antes de exportar preguntas que tienen dependencias, puede optar por proporcionar más contexto sobre el tipo de información que está contenido en la dependencia. Al proporcionar esta información se permite que otros usuarios sepan a qué tipo de información deben hacer referencia cuando importan la pregunta a Policy Monitor.

Exportación de preguntas de Policy Monitor

Puede exportar una o varias de las preguntas de Policy Monitor a un archivo XML. La exportación de preguntas de Policy Monitor es útil para realizar la copia de seguridad de las preguntas o para compartir las preguntas con otros usuarios.

Acerca de esta tarea

Si alguna pregunta de Policy Monitor contiene dependencias, puede proporcionar más contexto sobre el tipo de información que está contenida en la dependencia.

El nombre de archivo XML predeterminado para las preguntas exportadas es `policy_monitor_questions_export.xml`.

Procedimiento

1. En la pestaña **Risks**, pulse **Policy Monitor**.
2. Elija una de las opciones siguientes:
 - Para exportar todas las preguntas, en el menú **Actions**, seleccione **Export All**.
 - Para exportar preguntas seleccionadas, pulse la tecla Control para seleccionar cada pregunta que desea exportar y, a continuación, en el menú **Actions**, seleccione **Export Selected**.
3. Opcional. Si alguna pregunta contiene dependencias, pulse el enlace de parámetro para escribir información más específica. La longitud máxima de caracteres para este campo es de 255.
4. Pulse **Export Questions**.

Resultados

Se exporta al directorio de descarga un archivo predeterminado, denominado `policy_monitor_questions_export.xml`.

Importación de preguntas de Policy Monitor

Puede importar una o más preguntas de Policy Monitor a IBM Security QRadar Risk Manager.

Acerca de esta tarea

El proceso de importación no actualiza las preguntas existentes; cada pregunta aparece como una nueva pregunta en Policy Monitor. Se añade una indicación de fecha y hora, como un sufijo, a todas las preguntas importadas.

Después de importar preguntas de Policy Monitor, se visualiza un aviso en la columna **Status** si una pregunta importada contiene una dependencia. Las preguntas importadas con dependencias contienen parámetros sin valores. Para asegurarse de que las preguntas de Policy Monitor importadas funcionan como se esperaba, debe asignar valores a parámetros vacíos.

Procedimiento

1. En la pestaña **Risks**, pulse **Policy Monitor**.
2. En el menú **Actions**, seleccione **Import**.
3. Pulse **Choose File** y, a continuación, explore para seleccionar el archivo XML que desea importar.
4. Pulse **Open**.
5. Seleccione uno o más grupos para asignar la pregunta a un grupo.
6. Pulse **Import Question**.

7. Seleccione la columna **Status** para avisos. Si una pregunta contiene un aviso, abra la pregunta y edite los parámetros dependientes. Puede guardar la pregunta después de que se hayan completado los parámetros.

Qué hacer a continuación

Se inhabilita la supervisión para las preguntas importadas. Puede crear un suceso para supervisar los resultados de las preguntas que se han importado.

Resultados de activos

Los resultados de activos se visualizan después de enviar una pregunta de Policy Monitor.

La **Puntuación de riesgo** indica el nivel de riesgo que está asociado a la pregunta. El cálculo de **Puntuación de riesgo** está basado en el factor de importancia asignado a la pregunta y al número de resultados devueltos para la pregunta.

En la tabla siguiente se describen los parámetros para los resultados de activos.

Tabla 8. Resultados de activos

Parámetro	Descripción
IP	Dirección IP del activo.
Nombre	Nombre del activo, tal como se obtiene el perfil de activo. Para obtener más información sobre los perfiles de activo, consulte la publicación <i>IBM Security QRadar SIEM Users Guide</i> .
Vlan	El nombre la VLAN asociada al activo.
Peso	Peso del activo, tal como se obtiene del perfil de activo.
Puerto(s) de destino	Lista de puertos de destino asociados con este activo, en el contexto de las pruebas de pregunta. Si hay varios puertos asociados con este activo y esta pregunta, este campo indica Múltiple y el número de puertos múltiples. La lista de puertos se obtiene filtrando las conexiones asociadas con esta pregunta para obtener todos los puertos exclusivos donde el activo ha sido el origen, el destino o la conexión. Pulse Múltiple (N) para ver las conexiones. Esta pantalla proporciona las conexiones agregadas por puerto, filtradas por la dirección IP de activo y basadas en el intervalo de tiempo especificado en la pregunta.

Tabla 8. Resultados de activos (continuación)

Parámetro	Descripción
Protocolo(s)	<p>Lista de protocolos asociados con este activo, en el contexto de las pruebas de pregunta. Si hay varios protocolos asociados con este activo y pregunta, este campo indica Múltiple y el número de protocolos. La lista de protocolos se obtiene filtrando las conexiones asociadas con esta pregunta para obtener todos los protocolos exclusivos donde el activo ha sido el origen, el destino o la conexión.</p> <p>Pulse Múltiple (N) para ver las conexiones. Esta pantalla proporciona las conexiones agregadas por protocolo, filtradas por la dirección IP de activo y basadas en el intervalo de tiempo especificado en la pregunta.</p>
Aplicación (Aplicaciones) de flujo	<p>Lista de aplicaciones asociadas con este activo, en el contexto de las pruebas de pregunta. Si hay varias aplicaciones asociadas con este activo y pregunta, este campo indica Múltiple y el número de aplicaciones. La lista de aplicaciones se obtiene filtrando las conexiones asociadas con esta pregunta para obtener todas las aplicaciones exclusivas donde el activo ha sido el origen, el destino o la conexión.</p> <p>Pulse Múltiple (N) para ver las conexiones. Esta pantalla proporciona las conexiones agregadas por aplicación, filtradas por la dirección IP de activo y basadas en el intervalo de tiempo especificado en la pregunta.</p>
Vulnerabilidad(es)	<p>Lista de vulnerabilidades asociadas con este activo, en el contexto de las pruebas de pregunta. Si hay varias vulnerabilidades asociadas con este activo y pregunta, este campo indica Múltiple y el número de vulnerabilidades.</p> <p>La lista de vulnerabilidades se obtiene utilizando una lista de todas las vulnerabilidades compiladas de pruebas relevantes y utilizando esta lista para filtrar las vulnerabilidades detectadas en este activo. Si no se especifica ninguna vulnerabilidad para esta pregunta, se utilizan todas las vulnerabilidades del activo para compilar la lista.</p> <p>Pulse Múltiple (N) para ver los activos. Esta pantalla proporciona las conexiones agregadas por vulnerabilidad, filtradas por la dirección IP de activo y basadas en el intervalo de tiempo especificado en la pregunta.</p>

Tabla 8. Resultados de activos (continuación)

Parámetro	Descripción
Recuento de flujos	<p>Recuento de flujos total asociado con este activo, en el contexto de las pruebas de pregunta.</p> <p>El recuento de flujos se determina filtrando las conexiones asociadas con esta pregunta para obtener el total de recuento de flujos, donde el activo ha sido el origen, el destino o la conexión.</p>
Origen (Orígenes)	<p>Lista de direcciones IP de origen asociadas con este activo, en el contexto de las pruebas de pregunta. Si hay varias direcciones IP de origen asociadas con este activo y pregunta, este campo indica Múltiple y el número de direcciones IP de origen. La lista de direcciones IP de origen se obtiene filtrando las conexiones asociadas con esta pregunta para obtener todas las direcciones IP de origen exclusivas donde el activo es el destino de la conexión.</p> <p>Pulse Múltiple (N) para ver las conexiones. Esta pantalla proporciona las conexiones agregadas por dirección IP de origen filtradas por la dirección IP de activo basándose en el intervalo de tiempo especificado en la pregunta.</p>
Destino(s)	<p>Lista de direcciones IP de destino asociadas con este activo, en el contexto de las pruebas de pregunta. Si hay varias direcciones IP de destino asociadas con este activo y pregunta, este campo indica Múltiple y el número de pruebas de pregunta. La lista de direcciones IP de destino se obtiene filtrando las conexiones asociadas con esta pregunta para obtener todas las direcciones IP de destino exclusivas donde el activo es el origen de la conexión.</p> <p>Pulse Múltiple (N) para ver las conexiones. Esta pantalla proporciona las conexiones agregadas por dirección IP de destino filtradas por la dirección IP de activo basándose en el intervalo de tiempo especificado en la pregunta.</p>
Bytes de origen de flujo	<p>El total de bytes de origen asociados a este activo, en el contexto de la prueba de pregunta.</p> <p>Los bytes de origen se determinan filtrando las conexiones asociadas con esta pregunta para obtener el total de bytes de origen donde el activo es el origen de la conexión.</p>

Tabla 8. Resultados de activos (continuación)

Parámetro	Descripción
Bytes de destino de flujo	Total de bytes de destino asociados con este activo, en el contexto de la prueba de pregunta. Los bytes de destino se determinan filtrando las conexiones asociadas con esta pregunta para obtener el total de bytes de destino donde el activo es el destino de la conexión.

Resultados de dispositivo/regla

Los resultados de dispositivo/regla se visualizan después de enviar una pregunta de supervisor de políticas.

La **Puntuación de riesgo** visualizada indica el nivel de riesgo que está asociado a la pregunta. El cálculo de **Puntuación de riesgo** está basado en el factor de importancia asignado a la pregunta y al número de resultados devueltos para la pregunta.

Los parámetros para los resultados de dispositivos y reglas se describen en la tabla siguiente.

Tabla 9. Resultados de dispositivos y reglas

Parámetro	Descripción
IP de dispositivo	Dirección IP del dispositivo.
Nombre de dispositivo	Nombre del dispositivo, tal como se obtiene de Configuration Monitor.
Tipo de dispositivo	Tipo de dispositivo, tal como se obtiene del perfil de activo. Para obtener más información sobre los perfiles de activo, consulte la publicación <i>IBM Security QRadar SIEM Users Guide</i> .
Lista	Nombre de la regla del dispositivo.
Entrada	Número de entrada de la regla.
Acción	Acción asociada con la regla relevante del dispositivo. Las opciones son: permit, deny o NA.
Origen (Orígenes)	Red de origen asociada con este activo. Los orígenes con un hiperenlace indican una referencia de grupo de objetos. Pulse el enlace para ver información detallada sobre la(s) referencia(s) de grupo de objetos.

Tabla 9. Resultados de dispositivos y reglas (continuación)

Parámetro	Descripción
Servicio(s) de origen	<p>Puertos de origen y comparación asociada con la regla relevante del dispositivo en el formato siguiente:</p> <p><comparación>:<puerto></p> <p>Donde</p> <p><comparación></p> <p>puede incluir una de las opciones siguientes:</p> <ul style="list-style-type: none"> • eq - Igual • ne - No igual • lt - Menor que • gt - Mayor que <p>Por ejemplo, si el parámetro indica ne:80, cualquier puerto distinto de 80 se aplica a este servicio de origen. Si el parámetro indica lt:80, el rango de puertos aplicables es de 0 a 79.</p> <p>Este parámetro visualiza puerto de origen para la regla de dispositivo. Si no existe ningún puerto para esta regla de dispositivo, se visualiza el término NA.</p> <p>Los servicios de origen con un hipervínculo indican una referencia de grupo de objetos. Pulse el enlace para ver información detallada sobre la(s) referencia(s) de grupo de objetos.</p>
Destino(s)	<p>Red de destino asociada con la regla relevante del dispositivo.</p> <p>Los destinos con un hipervínculo indican una referencia de grupo de objetos. Pulse el enlace para ver información detallada sobre la(s) referencia(s) de grupo de objetos.</p>

Tabla 9. Resultados de dispositivos y reglas (continuación)

Parámetro	Descripción
Servicio(s) de destino	<p>Los puertos de destino y comparación asociada con la regla relevante del dispositivo se visualizan en el formato siguiente: <comparación>:<puerto></p> <p>Donde <comparación></p> <p>puede incluir una de las opciones siguientes:</p> <ul style="list-style-type: none"> • eq - Igual • ne - No igual • lt - Menor que • gt - Mayor que <p>Por ejemplo, si el parámetro indica ne:80, cualquier puerto distinto de 80 se aplica a este servicio de destino. Si el parámetro indica lt:80, el rango de puertos aplicables es de 0 a 79.</p> <p>Este parámetro visualiza el puerto de destino para la regla de dispositivo. Si no existe ningún puerto para esta regla de dispositivo, se visualiza el término NA.</p> <p>Los servicios de destino con un hipervínculo indican una referencia de grupo de objetos. Pulse el enlace para ver información detallada sobre la(s) referencia(s) de grupo de objetos.</p>
Usuario(s)Grupo(s)	Los usuarios o los grupos asociados a la regla relevante del dispositivo.
Protocolo(s)	Protocolo o grupo de protocolos asociados con la regla relevante del dispositivo.
Firma(s)	Firma de este dispositivo, que sólo se visualiza para una regla de dispositivo en un dispositivo de IP.
Aplicaciones	Las aplicaciones asociadas a la regla relevante del dispositivo.

Evaluar resultados de preguntas de Policy Monitor

Puede evaluar los resultados que se devuelven de una pregunta de Policy Monitor.

Aprobar un resultado de una pregunta es similar a ajustar el sistema para informar a IBM Security QRadar Risk Manager de que el activo asociado con el resultado de la pregunta es seguro o se puede ignorar en el futuro.

Cuando un usuario aprueba un resultado de activo, Policy Monitor ve ese resultado de activo como aprobado, y cuando la pregunta de Policy Monitor se envía o supervisa en el futuro, el activo no se lista en los resultados de la pregunta. El activo aprobado no se visualiza en la lista de resultados de la pregunta a menos que se revoque la aprobación. Policy Monitor registra el usuario, la dirección IP del dispositivo, la razón de la aprobación, el dispositivo o la regla aplicable y la fecha y la hora para los administradores de seguridad de la red.

Aprobación de resultados

Puede evaluar la lista de activos o reglas de dispositivo devueltas para determinar el nivel de riesgo involucrado. Después de evaluar, puede aprobar todos los resultados o resultados específicos.

Procedimiento

1. En la tabla de resultados, seleccione el recuadro de selección junto a los resultados que desea aceptar.
2. Elija una de las opciones siguientes:

Opción	Descripción
Approve All	Seleccione esta opción para aprobar todos los resultados.
Approve Selected	Marque el recuadro de selección situado junto a los resultados que desea aprobar y, a continuación, pulse Approve Selected .

3. Escriba la razón de la aprobación.
4. Pulse **OK**.
5. Pulse **OK**.
6. Para ver los resultados aprobados para la pregunta, pulse **View Approved**.

Resultados

La ventana **Approved Question Results** proporciona la información siguiente:

Tabla 10. Parámetros de *Approved question results*

Parámetro	Descripción
Device/Rule	Para un resultado de pregunta de dispositivo/regla, esto indica el dispositivo asociado con este resultado.
IP	Para un resultado de pregunta de activo, esto indica la dirección IP asociada con el activo.
Approved By	Usuario que ha aprobado los resultados.
Approved On	Fecha y hora en que los resultados se han aprobado.
Notes	Muestra el texto de las notas asociadas con este resultado y la razón por la que se ha aprobado la pregunta.

Si desea eliminar aprobaciones para cualquier resultado, marque el recuadro de selección para cada resultado para el que desea eliminar la aprobación y pulse **Revoke Selected**. Para eliminar todas las aprobaciones, pulse **Revoke All**.

Preguntas de supervisor

Si desea generar un suceso cuando cambian los resultados de una pregunta, puede configurar que se supervise una pregunta.

Cuando se selecciona que se supervise una pregunta, IBM Security QRadar Risk Manager analiza continuamente la pregunta para determinar si cambian los

resultados de una pregunta. Si QRadar Risk Manager detecta un cambio de resultado, se puede generar un delito para avisarle de una desviación en la política definida.

Una pregunta en modalidad de supervisor toma de forma predeterminada un intervalo de tiempo de 1 hora. Este valor altera temporalmente el valor de tiempo que se ha establecido cuando se ha creado la pregunta.

Creación de un suceso para supervisar los resultados

Puede crear un suceso para supervisar los resultados de las preguntas que se han creado en Policy Monitor.

Acerca de esta tarea

Los parámetros que configure para un suceso se describen en la tabla siguiente.

Tabla 11. Parámetros de supervisión de resultados de preguntas

Parámetro	Descripción
Policy evaluation interval	Frecuencia con la que se debe ejecutar el suceso.
Event Name	Nombre del suceso que desea visualizar en las pestañas Log Activity y Offenses .
Event Description	Descripción del suceso. La descripción se visualiza en las anotaciones de los detalles de suceso.
High-Level Category	Categoría de suceso de alto nivel que desea que esta regla utilice al procesar sucesos.
Low-Level Category	Categoría de suceso de bajo nivel que desea que esta regla utilice al procesar los sucesos.
Ensure the dispatched event is part of an offense	<p>Reenvía los sucesos al componente magistrado. Si no se ha generado ningún delito, se crea un delito nuevo. Si existe un delito, se añade el suceso.</p> <p>Si correlaciona por pregunta o simulación, todos los sucesos de una pregunta se asocian a un delito único.</p> <p>Si correlaciona por activo, se crea o actualiza un delito exclusivo para cada activo exclusivo.</p>
Dispatch question passed events	Reenvía sucesos que pasan la pregunta de Policy Monitor al componente magistrado.
Vulnerability Score Adjustments	Ajusta la puntuación de riesgo de vulnerabilidad de un activo, dependiendo de si la pregunta falla o pasa. Las puntuaciones de riesgo de vulnerabilidad se ajustan en IBM Security QRadar Vulnerability Manager.

Tabla 11. Parámetros de supervisión de resultados de preguntas (continuación)

Parámetro	Descripción
Additional Actions	<p>Acciones adicionales que se deben llevar a cabo cuando se recibe un suceso.</p> <p>Separe varias direcciones de correo electrónico utilizando una coma.</p> <p>Seleccione Notificar si desea que los sucesos que se generan como resultado de esta pregunta supervisada visualicen sucesos en el elemento de notificaciones del sistema en el panel de control.</p> <p>La salida de syslog puede parecerse a la siguiente: 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</p>
Enable Monitor	Supervisar la pregunta.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. Seleccione la pregunta que desea supervisar.
4. Pulse **Monitor**.
5. Configure los valores de los parámetros.
6. Pulse **Save Monitor**.

Agrupar preguntas

Puede agrupar y ver las preguntas basándose en los criterios elegidos

La categorización de las preguntas le permite ver las preguntas y realizar el seguimiento de las mismas de forma eficiente. Por ejemplo, puede ver todas las preguntas relacionadas con el cumplimiento.

Al crear preguntas nuevas, puede asignar la pregunta a un grupo existente.

Visualización de grupos

Puede ver un grupo de preguntas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En la lista **Group**, seleccione el grupo que desea ver.

Creación de un grupo

Puede crear un nuevo grupo para las preguntas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo en el que desea crear un nuevo grupo.
5. Pulse **New**.
6. En el campo **Name**, especifique el nombre que desea asignar al nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
7. En el campo **Description**, especifique una descripción que desee asignar a este grupo. La descripción puede tener un máximo de 255 caracteres de longitud.
8. Pulse **OK**.
9. Si desea cambiar la ubicación del grupo nuevo, pulse el nuevo grupo y arrastre la carpeta a la ubicación elegida en el árbol de menús.

Edición de un grupo

Puede editar un grupo de preguntas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo que desea editar.
5. Pulse **Edit**.
6. Edite **Name** y **Description**, según sea necesario.
Los campos de nombre y descripción pueden tener un máximo de 255 caracteres.
7. Pulse **OK**.
8. Si desea cambiar la ubicación del grupo, seleccione el grupo y arrastre la carpeta a la ubicación preferida en el árbol de menús.
9. Cerrar la ventana **Groups**.

Copia de un elemento en otro grupo

Mediante el uso de la funcionalidad de grupos, puede copiar una simulación en uno o muchos grupos.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione la pregunta que desea copiar en otro grupo.
5. Pulse **Copy**.
6. Marque este recuadro de selección para el grupo en el que desea copiar la simulación.
7. Pulse **Copy**.

Supresión de un elemento de un grupo

Puede suprimir un elemento de un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo de nivel superior.
5. En la lista de grupos, seleccione el elemento o grupo que desea suprimir.
6. Pulse **Remove**.
7. Pulse **OK**.

Asignación de un elemento a un grupo

Puede asignar una pregunta a un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. Seleccione la pregunta que desea asignar a un grupo.
4. Mediante el uso del menú **Actions**, seleccione **Assign Groups**.
5. Seleccione el grupo al que desea que se asigne la pregunta.
6. Pulse **Assign Groups**.

Integración de IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager se integra con QRadar Risk Manager para ayudarle a priorizar los riesgos y las vulnerabilidades de la red.

Políticas de riesgo y priorización de vulnerabilidades

Puede integrar QRadar Vulnerability Manager con QRadar Risk Manager definiendo y supervisando las políticas de riesgo de vulnerabilidad o activo.

Cuando las políticas de riesgo que define en QRadar Risk Manager pasan o fallan, se ajustan las puntuaciones de riesgo de vulnerabilidad en QRadar Vulnerability Manager. Los niveles de ajuste dependen de las políticas de riesgo de la organización.

Cuando las puntuaciones de riesgo de vulnerabilidad se ajustan en QRadar Vulnerability Manager, los administradores pueden realizar las tareas siguientes:

- Obtener visibilidad inmediata de las vulnerabilidades que han fallado en una política de riesgo.

Por ejemplo, es posible que la información nueva se visualice en el panel de control de QRadar o se envíe utilizando el correo electrónico.

- Volver a priorizar las vulnerabilidades que necesitan atención inmediata.

Por ejemplo, un administrador puede utilizar la **Puntuación de riesgo** para identificar rápidamente las vulnerabilidades de alto riesgo.

Si se aplican políticas de riesgo a un nivel de activo en QRadar Risk Manager, se ajustan las puntuaciones de riesgo de todas las vulnerabilidades de dicho activo.

Casos de uso de Policy Monitor

Están disponibles muchas opciones al crear preguntas para analizar el riesgo en la red.

Los siguientes ejemplos de Policy Monitor describen casos de uso comunes que puede utilizar en el entorno de red.

Prueba de activos para la comunicación posible en los activos protegidos

Este caso de uso muestra cómo crear una pregunta de Policy Monitor basándose en la dirección IP. Todas las organizaciones tienen redes que contienen servidores críticos donde se supervisa el tráfico y a los que solo pueden acceder los empleados de confianza.

Acerca de esta tarea

Desde una perspectiva de riesgo, es importante saber qué usuarios de la organización pueden comunicarse con activos de red críticos. IBM Security QRadar Risk Manager lleva a cabo esta tarea creando una pregunta de Policy Monitor basándose en una prueba de activo para las comunicaciones posibles.

Hay varias maneras de generar una pregunta de Policy Monitor para este objetivo de caso de uso. Puede examinar todas las conexiones con el servidor crítico a lo largo del tiempo, pero puede que le preocupe más que los empleados regionales no estén accediendo a estos servidores críticos. Para ello, puede crear una pregunta de Policy Monitor que examine la topología de la red mediante la dirección IP.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, seleccione **New**.
4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.
5. En la lista desplegable **What type of data do you want to return** seleccione **Assets**.
6. En la lista desplegable **Evaluate On**, seleccione **Possible Communication**.
7. En la lista desplegable **Importance Factor**, especifique un nivel de importancia a asociar con la pregunta.
8. En la sección **Time Range**, especifique un rango de tiempo para la pregunta.
9. En la sección **Which tests do you want to include in your question**, efectúe una doble pulsación para seleccionar **have accepted communication to destination asset building blocks**.
10. En la sección **Buscar activos**, pulse **asset building blocks** para configurar adicionalmente esta prueba y especifique **Protected Assets**.

Nota: Para definir los activos remotos de red, debe haber definido anteriormente el componente básico de activos remotos.

11. En la sección **Which tests do you want to include in your question**, efectúe una doble pulsación para seleccionar la prueba restrictiva **and include only the following IP addresses**.
12. En la sección **Find Assets that**, pulse **IP Addresses**.

13. Especifique el rango de direcciones IP o la dirección CIDR de la red remota.
14. Pulse **Save Question**.
15. Seleccione la pregunta de Policy Monitor que ha creado para los activos protegidos.
16. Pulse **Submit Question**.
17. Revise los resultados para ver si algún activo protegido ha aceptado la comunicación desde una dirección IP o rango CIDR desconocidos.
18. Opcional. Después de que los resultados se hayan ajustado correctamente, puede supervisar los activos protegidos poniendo la pregunta en modalidad de supervisión. Si un activo protegido se ha conectado mediante una dirección IP no reconocida, QRadar Risk Manager puede generar una alerta.

Qué hacer a continuación

Puede supervisar las preguntas.

Comunicación de prueba de dispositivos/reglas en el acceso a Internet

Este caso de uso muestra cómo crear una pregunta de Policy Monitor basada en dispositivos/reglas. Las pruebas de dispositivos identifican las reglas de un dispositivo que infringen una política definida o los cambios que han presentado riesgos en el entorno.

Acerca de esta tarea

Las pruebas de dispositivos identifican las reglas de un dispositivo que infringen una política definida o los cambios que han presentado riesgos en el entorno. Desde una perspectiva de red, es importante saber qué reglas de dispositivo podían haber cambiado y alertarle sobre la regla para que ésta se pueda corregir. Sucede muy a menudo cuando, debido a un cambio de cortafuegos en la red, se otorga acceso a Internet a servidores que anteriormente no lo tenían. IBM Security QRadar Risk Manager puede supervisar los cambios de regla en los dispositivos de red creando una pregunta de Policy Monitor basada en las reglas de dispositivo.

Hay varias maneras de generar una pregunta de Policy Monitor para este objetivo de caso de uso. En este ejemplo, creará una pregunta de Policy Monitor para ver qué dispositivos tienen acceso a Internet.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, seleccione **New**.
4. En la lista desplegable **What type of data do you want to return** seleccione **Devices/Rules**.
5. En la lista desplegable **Importance Factor**, especifique un nivel de importancia a asociar con la pregunta.
6. En la sección **Which tests do you want to include in your question**, efectúe una doble pulsación para seleccionar **allow connection to the internet**.
7. Pulse **Save Question**.
8. Seleccione la pregunta de Policy Monitor que ha creado para supervisar las reglas de dispositivos.
9. Pulse **Submit Question**.

10. Revise los resultados para ver si las reglas permiten el acceso a Internet.
11. Opcional. Después de que los resultados se hayan ajustado correctamente, puede supervisar los activos protegidos poniendo la pregunta en modalidad de supervisión.

Qué hacer a continuación

Puede supervisar las preguntas.

Prioridad de las vulnerabilidades de alto riesgo aplicando políticas de riesgo

En IBM Security QRadar Vulnerability Manager, puede alertar a los administradores de las vulnerabilidades de riesgo más alto aplicando políticas de riesgo a las vulnerabilidades.

Al aplicar una política de riesgo, se ajusta la puntuación de riesgo de vulnerabilidad, permitiendo a los administradores priorizar de forma más precisa las vulnerabilidades que requieren atención inmediata.

En este ejemplo, la puntuación de riesgo de vulnerabilidad aumenta automáticamente en un factor de porcentaje para cualquier vulnerabilidad que permanezca activa en la red después de 40 días.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
 2. En el panel de navegación, pulse **Gestionar vulnerabilidades**.
 3. En la barra de herramientas, pulse **Buscar > Nueva búsqueda**.
 4. En el panel Parámetros de búsqueda, configure los filtros siguientes:
 - a. **Risk Equals High**
 - b. **Days since vulnerabilities discovered Greater than or equal to 40**
 5. Pulse **Search** y, a continuación, en la barra de herramientas, pulse **Save Search Criteria**.

Escriba un nombre de búsqueda guardada que sea identificable en QRadar Risk Manager.
 6. Pulse la pestaña **Risks**.
 7. En el panel de navegación, pulse **Policy Monitor**.
 8. En la barra de herramientas, pulse **Actions > New**.
 9. En el campo **What do you want to name this question**, escriba un nombre.
 10. En el campo **Which tests do you want to include in your question**, pulse **are susceptible to vulnerabilities contained in vulnerability saved searches**.
 11. En el campo **Find Assets that**, pulse el parámetro subrayado en **are susceptible to vulnerabilities contained in vulnerability saved searches**.
 12. Identifique la búsqueda guardada de vulnerabilidad de riesgo alto de QRadar Vulnerability Manager, pulse **Añadir** y, a continuación, pulse **Aceptar**.
 13. Pulse **Save Question**.
 14. En el panel Questions, seleccione la pregunta en la lista y en la barra de herramientas pulse **Monitor**.
- Restricción:** El campo **Event Description** es obligatorio.
15. Pulse **Dispatch question passed events**.

16. En el campo **Vulnerability Score Adjustments**, escriba un valor de porcentaje de ajuste de riesgo en el campo **Percentage vulnerability score adjustment on question fail**.
17. Pulse **Apply adjustment to all vulnerabilities on an asset** y, a continuación, pulse **Save Monitor**.

Qué hacer a continuación

En la pestaña **Vulnerabilidades**, puede buscar las vulnerabilidades de riesgo alto y priorizar las vulnerabilidades

Comunicación real para protocolos permitidos de DMZ

Este caso de uso muestra cómo crear una pregunta de Policy Monitor basada en la lista conocida de protocolos de confianza para la DMZ. En la mayoría de organizaciones, el tráfico de red que cruza la DMZ está restringido a protocolos conocidos y de confianza, como HTTP o HTTPS en puertos especificados.

Acerca de esta tarea

Desde una perspectiva de riesgo, es importante supervisar continuamente el tráfico en la DMZ para asegurarse de que sólo estén presentes los protocolos de confianza. IBM Security QRadar Risk Manager lleva a cabo esto creando una pregunta de Policy Monitor basándose en una prueba de activo para las comunicaciones reales.

Hay varias maneras de generar una pregunta de Policy Monitor para este objetivo de caso de uso. Puesto que sabemos que la política de red solo permite unos pocos protocolos de confianza, seleccionamos una opción para crear nuestra pregunta de Policy Monitor basándonos en la lista conocida de protocolos de confianza para la DMZ.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, seleccione **New**.
4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.
5. En la lista desplegable **What type of data do you want to return** seleccione **Assets**.
6. En la lista desplegable **Evaluate On**, seleccione **Actual Communication**.
7. En la lista desplegable **Importance Factor**, especifique un nivel de importancia a asociar con la pregunta.
8. En la sección **Time Range**, especifique un rango de tiempo para la pregunta.
9. En la sección **Which tests do you want to include in your question**, seleccione **have accepted communication to destination networks**.
10. En la sección **Find Assets that**, pulse **destination networks** para configurar adicionalmente esta prueba y especificar la DMZ como red de destino.
11. Seleccione **and include the following inbound ports**.
12. En la sección **Find Assets that**, pulse el parámetro "include only" para que cambie a "exclude". Ahora el parámetro visualiza "and exclude the following inbound ports".
13. Pulse **ports**.

14. Añada el puerto 80 y 443 y, a continuación, pulse **OK**.
15. Pulse **Save Question**.
16. Seleccione la pregunta DMZ de Policy Monitor que ha creado.
17. Pulse **Submit Question**.
18. Revise los resultados para ver si los protocolos distintos del puerto 80 y puerto 443 se están comunicando en la red.
19. Opcional. Después de que los resultados se hayan ajustado correctamente, puede supervisar la pregunta DMZ poniendo la pregunta en modalidad de supervisión

Qué hacer a continuación

Puede supervisar las preguntas.

Exploraciones de prueba de referencia CIS

Para configurar una exploración de prueba de referencia CIS, debe realizar varias tareas de configuración en las pestañas Admin, Activos, Vulnerabilidades y Riesgos en QRadar.

Para configurar la exploración de prueba de referencia CIS, se necesitan los requisitos previos siguientes:

Licencias válidas de IBM Security QRadar Vulnerability Manager y IBM Security QRadar Risk Manager

Si ha aplicado un parche en una versión anterior de IBM Security QRadar, debe realizar una actualización automática antes de realizar una exploración de prueba de referencia CIS.

Hay 8 pasos implicados en la configuración de una exploración de prueba de referencia CIS:

1. Adición de activos.
2. Configuración de un conjunto de credenciales.
Lo más fácil es añadir credenciales centralizadas en la pestaña Admin de IBM Security QRadar pero también puede añadir credenciales cuando crea un perfil de prueba de referencia.
3. Creación de una búsqueda guardada de activo.
Puede utilizar las búsquedas guardadas de activo cuando configure las preguntas de conformidad de activos.
4. Modificación de comprobaciones de prueba de referencia CIS en QRadar Vulnerability Manager.
Puede crea una lista de comprobación de pruebas de referencia mediante el Editor de pruebas de referencia de conformidad.
5. Configuración de un perfil de exploración de prueba de referencia CIS en QRadar Vulnerability Manager.
6. Creación de una pregunta de conformidad de activo en IBM Security QRadar Risk Manager.
7. Supervisión de la pregunta de conformidad de activo creada.
8. Visualización de los resultados de exploración de prueba de referencia CIS.

Adición o edición de un perfil de activo

Para poder realizar una exploración de prueba de referencia CIS, debe añadir los activos de red que pretende explorar a IBM Security QRadar. Los perfiles de activo se descubren y se añaden automáticamente, sin embargo se le solicitará que añada manualmente un perfil.

Acerca de esta tarea

Puede especificar manualmente información sobre cada activo creando un Perfil de activo en la pestaña **Activos**. También puede configurar un perfil de exploración en la pestaña **Vulnerabilidades** para ejecutar una exploración de descubrimiento. La exploración de descubrimiento permite que QRadar® identifique las características de activo clave, como por ejemplo el sistema operativo, el tipo de dispositivo y los servicios.

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 opciones siguientes:
 - Para añadir un activo, pulse **Añadir activo** y teclee la dirección IP o el rango de CIDR del activo en el campo **Nueva dirección IP**.
 - Para editar un activo, efectúe una doble pulsación sobre 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 cuadro de diálogo.
 - Pulse el icono **Nueva dirección IP** y teclee una dirección IP en el cuadro de diálogo.
 - Si en la lista aparece **NIC desconocido**, puede seleccionar este elemento, pulsar el icono **Editar** y teclear una dirección MAC nueva en el cuadro de diálogo.
 - Seleccione una dirección MAC o IP de la lista, pulse el icono **Editar** y teclee una dirección MAC nueva en el cuadro 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 opciones siguientes: <ul style="list-style-type: none"> • Escriba un nombre de DNS y pulse Añadir. • Seleccione un nombre de DNS de la lista y pulse Editar. • Seleccione un nombre de DNS de la lista y pulse Eliminar.
NetBIOS	Elija una de las opciones siguientes: <ul style="list-style-type: none"> • Escriba un nombre de NetBIOS y pulse Añadir. • Seleccione un nombre de NetBIOS de la lista y pulse Editar. • Seleccione un nombre de NetBIOS de 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 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	<p>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.</p> <p>En el cuadro de lista Potencial de daños colaterales, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Ninguno • Bajo • Medio bajo • Medio alto • Alto • No definido <p>Cuando configura el parámetro Potencial de daños colaterales, el parámetro Peso se actualiza automáticamente.</p>
Requisito de confidencialidad	<p>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.</p> <p>En el recuadro de lista Requisito de confidencialidad, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Bajo • Medio • Alto • No definido

Parámetro	Descripción
Requisito de disponibilidad	<p>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.</p> <p>En el cuadro de lista Requisito de disponibilidad, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Bajo • Medio • Alto • No definido
Requisito de integridad	<p>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.</p> <p>En el cuadro de lista Requisito de integridad, seleccione una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Bajo • Medio • Alto • No definido
Peso	<p>El cuadro de lista Peso, seleccione un peso para este perfil de activo. El rango de valores es 0 - 10.</p> <p>Cuando configura el parámetro Peso, el parámetro Potencial de daños colaterales se actualiza automáticamente.</p>

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

Parámetro	Descripción
Propietario del negocio	<p>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.</p>
Contacto del propietario del negocio	<p>Escriba la información de contacto para el propietario de negocio. La longitud máxima es de 255 caracteres.</p>

Parámetro	Descripción
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.
Usuario técnico	<p>En el recuadro de lista, seleccione el nombre de usuario que desea asociar con este perfil de activo.</p> <p>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 <i>Guía del usuario de IBM Security QRadar Vulnerability Manager</i>.</p>

9. Pulse **Guardar**.

Configurar un conjunto de credenciales

En IBM Security QRadar Vulnerability Manager, puede crear un conjunto de credenciales para los activos de la red. Durante una exploración, si una herramienta de exploración necesita las credenciales de un sistema operativo Linux, UNIX o Windows, las credenciales se pasan automáticamente a la herramienta de exploración desde el conjunto de credenciales.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel **Configuración del sistema**, pulse **Credenciales centralizadas**.
3. En la barra de herramientas de la ventana Credenciales centralizadas, pulse **Añadir**.

Para configurar un conjunto de credenciales, el único campo obligatorio de la ventana Conjunto de credenciales es el campo **Nombre**.

4. En la ventana Conjunto de credenciales, pulse la pestaña **Activos**.
5. Escriba un rango de CIDR para los activos para los que desee especificar credenciales y pulse **Añadir**.
6. Opcional: Pulse las pestañas **Linux/Unix**, **Windows**, o **Dispositivos de red (SNMP)** cuando escriba las credenciales.
7. Pulse **Guardar**.

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.
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.

Edición de una prueba de referencia de conformidad

Utilice el Compliance Benchmark Editor en IBM Security QRadar Risk Manager para añadir o eliminar pruebas de las pruebas de referencia CIS predeterminadas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. Pulse **Policy Monitor**.
3. Pulse **Compliance** para abrir la ventana Compliance Benchmark Editor.
4. En el menú de navegación, pulse la prueba de referencia CIS predeterminada que desea editar.
5. En el panel **Compliance**, pulse el recuadro de selección **Enabled** en la fila que se ha asignado a la prueba que desea incluir.
 Pulse en cualquier lugar de una fila para ver una descripción de la prueba de referencia, una lógica de despliegue e información sobre elementos a comprobar antes de habilitar la prueba.
 Cuando cree una lista de comprobación de CIS personalizada, tenga en cuenta que algunas pruebas de referencia que no están incluidas de forma predeterminada pueden tardar mucho tiempo en ejecutarse. Para obtener más información, consulte la documentación de CIS.

Qué hacer a continuación

Cree una pregunta de conformidad de activo para probar activos en la prueba de referencia que ha editado.

Tareas relacionadas:

“Creación de una pregunta de conformidad de activo” en la página 46
 Crear una pregunta de conformidad de activo en Policy Monitor para buscar

activos en la red que fallan las pruebas de referencia CEI.

Creación de un perfil de prueba de referencia

Para crear exploraciones de conformidad de Center for Internet Security, debe configurar perfiles de prueba de referencia. Utilice las exploraciones de conformidad de CIS para verificar la conformidad de referencia de CIS para Windows y Red Hat Enterprise Linux.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Administrativo > Perfiles de exploración**.
3. En la barra de herramientas, pulse **Añadir prueba de referencia**.
4. Si desea utilizar credenciales centralizadas predefinidas, seleccione la casilla **Utilizar credenciales centralizadas**.

Las credenciales que se utilizan para explorar sistemas operativos Linux deben tener privilegios de usuario root. Las credenciales que se utilizan para explorar sistemas operativos Windows deben tener privilegios de administrador.

5. Si no utiliza la exploración dinámica, seleccione un explorador de QRadar Vulnerability Manager en la lista **Servidor de exploración**.
6. Para habilitar la exploración dinámica, pulse el recuadro de selección **Selección de servidor dinámica**.

Si ha configurado dominios en la ventana **Admin > Gestión de dominios**, puede seleccionar un dominio de la lista **Dominio**. Solamente se exploran los activos incluidos en los rangos de CIDR y los dominios que están configurados para los exploradores.

7. En el panel **Cuándo explorar**, establezca la planificación de ejecución, la hora de inicio de la exploración y los intervalos operativos que haya predefinidos.
8. En el panel **Correo electrónico**, defina qué información se debe enviar referente a la exploración y a quién se debe enviar.
9. Si no utiliza credenciales centralizadas, añada las credenciales que la exploración necesite en el panel **Credenciales adicionales**.

Las credenciales que se utilizan para explorar sistemas operativos Linux deben tener privilegios de usuario root. Las credenciales que se utilizan para explorar sistemas operativos Windows deben tener privilegios de administrador.

10. Pulse **Guardar**.

Creación de una pregunta de conformidad de activo

Crear una pregunta de conformidad de activo en Policy Monitor para buscar activos en la red que fallan las pruebas de referencia CEI.

Antes de empezar

Las preguntas de Policy Monitor se evalúan de arriba a abajo. El orden de las preguntas de Policy Monitor afecta a los resultados.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Policy Monitor**.
3. En el menú **Actions**, seleccione **New Asset Compliance Question**.

4. En el campo **What do you want to name this question**, escriba un nombre para la pregunta.
5. Seleccione el nivel de importancia que desea asociar con esta pregunta de la lista **Importance Factor**.
6. En el campo **Which tests do you want to include in your question**, seleccione el icono de suma (+) junto a la prueba **test compliance of assets in asset saved searches with CIS benchmarks**.
Seleccione esta prueba varias veces, si es necesario.
7. Configure los parámetros para las pruebas en el campo **Find Assets that**.
Pulse cada parámetro para ver las opciones disponibles para la pregunta. Especifique varias búsquedas guardadas de activos y varias listas de comprobación en esta prueba, si es necesario.
8. En el área de grupo, pulse los recuadros de selección pertinentes para asignar la pertenencia a grupos a esta pregunta.
Las preguntas de conformidad de activos se deben asignar a un grupo para incluirlas en paneles de control o informes de conformidad.
9. Pulse **Save Question**.

Qué hacer a continuación

Asocie un perfil de prueba de referencia con la pregunta que ha creado y supervise los resultados de dicha pregunta.

Conceptos relacionados:

“Factor de importancia” en la página 42

El Factor de importancia se utiliza para calcular la puntuación de riesgo y definir el número de resultados devueltos para una pregunta.

“Agrupar preguntas” en la página 58

Puede agrupar y ver las preguntas basándose en los criterios elegidos

Tareas relacionadas:

“Supervisión de preguntas de conformidad de activos” en la página 47

Supervisar preguntas de conformidad de activos seleccionando perfiles de exploración de CIS. Se ejecutan exploraciones de prueba de referencia CIS en los activos.

Supervisión de preguntas de conformidad de activos

Supervisar preguntas de conformidad de activos seleccionando perfiles de exploración de CIS. Se ejecutan exploraciones de prueba de referencia CIS en los activos.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Supervisor de políticas**.
3. En el panel **Preguntas**, seleccione la pregunta de conformidad de activos que desea supervisar.
4. Pulse **Supervisor** para abrir la ventana Resultados de supervisor.
5. Seleccione un perfil de prueba de referencia en la lista **Which benchmark profile to associate with this question?**

El perfil de exploración de referencia seleccionado utiliza un explorador QRadar Vulnerability Manager que está asociado con un dominio. El nombre del dominio se muestra en el área **Benchmark Profile Details**. Para obtener

más información sobre la gestión de los dominios, consulte la publicación *IBM Security QRadar SIEM Administration Guide*.

6. Seleccione el recuadro de selección **Enable the monitor results function for this question/simulation**.
7. Pulse **Guardar supervisor**.

La supervisión empieza a la hora de inicio de exploración establecida en la pestaña **Cuándo explorar** al crear el perfil de exploración de prueba de referencia.

Tareas relacionadas:

“Edición de una prueba de referencia de conformidad” en la página 47
 Utilice el Compliance Benchmark Editor en IBM Security QRadar Risk Manager para añadir o eliminar pruebas de las pruebas de referencia CIS predeterminadas.
 “Creación de una pregunta de conformidad de activo” en la página 46
 Crear una pregunta de conformidad de activo en Policy Monitor para buscar activos en la red que fallan las pruebas de referencia CEI.

Visualización de los resultados de la exploración

La página Resultados de la exploración visualiza una lista de resumen de los resultados generados al ejecutar un perfil de exploración.

Acerca de esta tarea

La página Resultados de la exploración proporciona la información siguiente:

Tabla 12. Parámetros de la lista de resultados de la exploración

Parámetro	Descripción
Perfil	El nombre del perfil de exploración. Pase el puntero del ratón sobre el Perfil para visualizar información sobre el perfil de exploración y el estado de la exploración.
Planificar	La planificación de ejecución aplicada al perfil de exploración. Si inició una exploración manual, se visualiza Manual .
Puntuación	La puntuación de Common Vulnerability Scoring System (CVSS) promedio de la exploración. Esta puntuación le ayuda a priorizar las vulnerabilidades.
Hosts	El número de hosts encontrado y explorado cuando se ejecutó el perfil de exploración. Pulse el enlace de columna Host para visualizar datos de vulnerabilidad para los hosts explorados.
Vulnerabilidades	El número de tipos diferentes de vulnerabilidades encontrado por una exploración. Pulse el enlace de la columna Vulnerabilidades para ver todas las vulnerabilidades exclusivas.
Instancias de vulnerabilidad	El número de vulnerabilidades encontrado por la exploración.

Tabla 12. Parámetros de la lista de resultados de la exploración (continuación)

Parámetro	Descripción
Servicios abiertos	El número de servicios abiertos exclusivos encontrado por la exploración. Un servicio abierto exclusivo se cuenta como un solo servicio abierto. Pulse el enlace de la columna Servicios abiertos para ver las vulnerabilidades categorizadas por servicio abierto.
Estado	El estado del Perfil de exploración. Las opciones son: <ul style="list-style-type: none"> • Detenido: este estado se visualiza si la exploración se ha completado satisfactoriamente o si la exploración se ha cancelado. • En ejecución: la exploración se está ejecutando • En pausa: la exploración está en pausa. • No iniciado: la exploración no está iniciada.
Progreso	Especifica el progreso de la exploración. Pase el puntero del ratón sobre la barra de progreso, mientras se está ejecutando la exploración, para visualizar información sobre el estado de una exploración.
Fecha/hora de inicio	La fecha y la hora en la que el perfil de exploración ha empezado a ejecutarse.
Duración	Visualiza el tiempo que ha tardado la exploración en completarse.

Procedimiento

1. Pulse la pestaña **Vulnerabilidades**.
2. En el panel de navegación, pulse **Resultados de exploración**.

Supervisión de recuentos de sucesos de reglas de cortafuegos de dispositivos de Check Point

En IBM Security QRadar Risk Manager puede supervisar los recuentos de sucesos de reglas de cortafuegos de los dispositivos de Check Point mediante la integración con Check Point SMS. Puede ver estas interacciones de regla en QRadar Risk Manager y utilizar informes de regla para gestionar la efectividad de política de la red.

En la imagen siguiente QRadar recibe y procesa registros de sucesos de regla desde dispositivos de cortafuegos de Check Point a través del SMS.

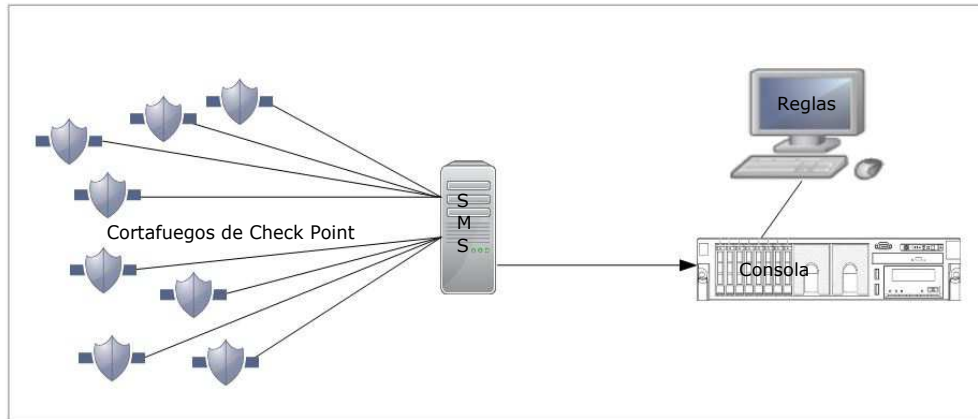


Figura 1. Recuento de reglas de Check Point

Escenario: implementación de la supervisión de reglas de cortafuegos de Check Point en QRadar

Usted es un administrador de sistemas de red responsable de la seguridad de red en una organización que utiliza Check Point para implementar sus políticas de seguridad de red. La red incluye varios cortafuegos de Check Point gestionados desde un servidor Check Point Security Management Server (SMS).

Desea ver informes diarios sobre el uso de las reglas para tener más visibilidad sobre la implementación de las reglas.

Debe configurar una conexión entre Check Point SMS y QRadar, de modo que QRadar reciba registros de sucesos de regla de dispositivos de cortafuegos de Check Point. QRadar procesa esta información de registro de sucesos de regla y visualiza la información de sucesos de regla para todos los dispositivos gestionados por cortafuegos de Check Point. En la tabla de reglas de QRadar puede analizar el uso y la efectividad de las reglas de cortafuegos supervisando recuentos de sucesos y ajustando las reglas para obtener un rendimiento óptimo.

Utilice la información de reglas para realizar las tareas siguientes:

- Ver las reglas más y menos utilizadas.
- Evaluar la viabilidad de reglas que se desencadenan con poca frecuencia.
- Ver reglas que pueden estar bloqueando el acceso a la red de forma innecesaria.
- Ver reglas que se desencadenan excesivamente y sobrecargan el ancho de banda de red.
- Ver sucesos detallados.
- Planificar informes.

Antes de empezar, descargue el paquete de adaptador más reciente de FixCentral e instálelo en su host gestionado de QRadar.

Siga estos pasos para configurar el recuento de reglas:

1. Configure las aplicaciones de OPSEC en Check Point SmartDashboard.
2. Cree un origen de registro en QRadar.
3. Configure Configuration Source Management (CSM) en QRadar Risk Manager. Descubra y haga una copia de seguridad de dispositivos en Configuration Source Management.

4. Realice las configuraciones para ver el recuento de reglas.

Configuración de aplicaciones de OPSEC en SmartDashboard

Crear y configurar 2 aplicaciones de OPSEC en Check Point SmartDashboard. Esto facilita la transferencia de archivos de registro entre Check Point y IBM Security QRadar.

Acerca de esta tarea

Cree 2 aplicaciones de OPSEC (Open Platform for Security), una con una propiedad de entidad de cliente CPMI (Check Point Management Interface) para QRadar Risk Manager y la otra con una propiedad de entidad de cliente LEA (Log Export API) para el origen de registro de QRadar Risk Manager.

Procedimiento

1. En el menú **Manage** de la barra de herramientas, pulse **Servers and OPSEC Applications**.
2. Pulse **New > OPSEC Application**.
3. En el campo **Name**, teclee un nombre para la aplicación.
4. En la lista **Host**, seleccione un host o pulse **New** para añadir uno.
5. Bajo **Client Entities**, marque el recuadro de selección **CPMI**.
Esta opción es necesaria para QRadar Risk Manager Configuration Source Management (CSM).
6. Pulse **Communication**.
7. En el campo **One-time password**, escriba una contraseña y confírmela.
La contraseña se utiliza varias veces durante la configuración y debe reutilizarla para que QRadar pueda utilizar un certificado de seguridad de Check Point.
8. Pulse **Inititalize**.
Trust state cambia a **Initialized but trust not established**.
9. Pulse **Cerrar**.
10. Para llenar el campo **DN** en la sección Secure Internal Communication, pulse **OK**.
11. Para ver el campo **DN** lleno, seleccione la OPSEC Application y pulse **Edit**.
El campo **DN** aparece ahora lleno. Esta información se utiliza para el **Application Object SIC Attribute (SIC Name)** y el **SIC Attribute (SIC Name)** cuando configura el origen de registro y Configuration Source Management en QRadar.
12. Cree la segunda aplicación OPSEC para utilizarla con el origen de registro.
Siga los pasos 1-11 para crear la primera aplicación de OPSEC con dos excepciones:
 - En el campo **Name** del paso 3, utilice un nombre diferente de la primera aplicación de OPSEC.
 - Para **Client Entities**, en el paso 5, marque el recuadro de selección **LEA**.
Asegúrese de que **Trust state** visualiza **Initialized but trust not established**.
13. En SmartDashboard, cierre todas las ventanas hasta que vuelva a la ventana de SmartDashboard principal.

Consejo: Utilice la misma contraseña única para esta aplicación de OPSEC para evitar la confusión de contraseñas.

14. En el menú **Policy** de la barra de herramientas, pulse **Install**.
15. Pulse **Install on all selected gateways, if it fails do not install on gateways of the same version**.

Qué hacer a continuación

El siguiente paso consiste en configurar el origen de registro en QRadar.

Configuración del origen de registro

Configure el origen de registro en IBM Security QRadar para obtener un certificado de Check Point y recibir información de registro.

Procedimiento

1. Inicie la sesión en QRadar.
2. Pulse la pestaña **Admin**.
3. En el menú de navegación, pulse **Orígenes de datos**.
Se visualiza el panel Orígenes de datos.
4. Pulse el icono **Orígenes de registro**.
5. Pulse **Añadir**.
6. Configure los valores siguientes:

Tabla 13. Parámetros de origen de registro de Check Point

Parámetro	Descripción
Nombre de origen de registro	El identificador del origen de registro.
Descripción del origen de registro	La descripción es opcional.
Tipo de origen de registro	Seleccione Check Point FireWall-1 .
Configuración de protocolo	Seleccione OPSEC/LEA .
Identificador de origen de registro	Dirección IP del SMS
IP de servidor	Escriba la dirección IP del SMS
Puerto de servidor	Utilice el puerto 18184.
Utilizar IP de servidor para origen de registro	No marque este recuadro de selección.
Intervalo de informe estadístico	El valor predeterminado es 600.
Tipo de autenticación	En la lista, seleccione sslca .
Atributo SIC de objeto de aplicación OPSEC (nombre SIC)	En Check Point SmartDashboard, pulse Manage > Servers and OPSEC Applications y seleccione la aplicación OPSEC cuya propiedad de entidad de cliente es LEA. Pulse Edit y copie la entrada del campo DN y péguela en el campo OPSEC Application Object SIC Attribute (SIC Name) .

Tabla 13. Parámetros de origen de registro de Check Point (continuación)

Parámetro	Descripción
Atributo SIC de origen de registro (Nombre de SIC de entidad)	<p>Utilice la entrada pegada en el campo Atributo SIC de objeto de aplicación OPSEC (nombre SIC), elimine el texto de CN= valor de propiedad y edite lo siguiente:</p> <p>Para el valor de propiedad CN=, utilice cp_mgmt_ <nombre_de_host > donde <nombre_de_host> es el nombre de Host de la ventana Propiedades de aplicación OPSEC.</p> <p>Consulte los ejemplos siguientes de un DN de aplicación OPSEC y un Host de aplicación OPSEC que se utilizan para crear el Nombre SIC de entidad:</p> <p>DN de aplicación OPSEC: CN=cpsmsxxx,0=svxxx-CPSMS..bsaobx</p> <p>Host de aplicación OPSEC: Srvxxx-SMS</p> <p>Utilice texto del DN de aplicación OPSEC y del Host de aplicación OPSEC para formar el Nombre SIC de entidad:</p> <p>CN=cp_mgmt_Srvxxx-SMS,0=svxxx-CPSMS..bsaobx</p> <p>El Nombre SIC de entidad de esta configuración está basado en una configuración de Pasarela a servidor de gestión. Si su dirección SMS no se utiliza como pasarela, utilice la configuración de servidor de gestión para el Nombre SIC de entidad que está representado por el texto siguiente:</p> <p>CN=cp_mgmt,0=<tomar_valor_0_de_campo_DN></p>
Especificar certificado	No marque este recuadro.
IP de entidad emisora de certificados	Escriba la dirección IP de SMS.
Recuperar contraseña de certificado	La contraseña especificada para las Propiedades de aplicaciones OPSEC en el campo Contraseña única de la ventana Comunicación.
Aplicación OPSEC	El nombre especificado en el campo Nombre de las Propiedades de aplicaciones OPSEC.
Habilitado	Marque este recuadro de selección para habilitar el origen de registro. De forma predeterminada, el recuadro de selección está marcado.
Credibilidad	El rango va de 0 a 10. La credibilidad indica la integridad de un suceso o un delito según viene determinada por la valoración de credibilidad de los dispositivos de origen. La credibilidad aumenta cuando varios orígenes informan del mismo suceso. El valor predeterminado es 5.
Recopilador de sucesos de destino	En la lista, seleccione el Recopilador de sucesos de destino para utilizarlo como destino para el origen de registro.
Fusionar sucesos	Habilita el origen de registro para fusionar (empaquetar) sucesos. De forma predeterminada, los orígenes de registro descubiertos automáticamente heredan el valor de la lista Fusionar sucesos de las propiedades Valores del sistema en QRadar. Cuando crea un origen de registro o edita una configuración existente, puede alterar temporalmente el valor predeterminado configurando esta opción para cada origen de registro.

Tabla 13. Parámetros de origen de registro de Check Point (continuación)

Parámetro	Descripción
Almacenar carga útil de suceso	Habilita el origen de registro para almacenar información de carga útil de suceso. De forma predeterminada, los orígenes de registro descubiertos automáticamente heredan el valor de la lista Almacenar carga útil de suceso de las propiedades Valores del sistema en QRadar. Cuando crea un origen de registro o edita una configuración existente, puede alterar temporalmente el valor predeterminado configurando esta opción para cada origen de registro.

7. Pulse **Guardar**.
8. En la pestaña **Admin**, pulse **Desplegar cambios**.
Aunque los cambios se implementen automáticamente, sigue siendo recomendable pulsar **Desplegar cambios**.
Compruebe que se establece la confianza para la aplicación OPSEC que tiene la propiedad de entidad de cliente de LEA, viendo el **Estado de confianza** en la ventana Comunicación de Propiedades de aplicación OPSEC.
La configuración del origen de registro se ha completado.
Para obtener más información sobre cómo configurar los orígenes de registro, consulte la publicación *IBM Security QRadar Managing Log Sources Guide*.

Establecimiento de una comunicación segura entre Check Point y IBM Security QRadar

Configure Configuration Source Management en IBM Security QRadar para conectar con Check Point SMS. Añada los detalles de la aplicación OPSEC de SmartDashboard y solicite un certificado de seguridad de Check Point.

Acerca de esta tarea

Configure los detalles de la aplicación OPSEC en Configuration Source Management y configure el intercambio de certificado. Una vez completada la configuración, utilice Configuration Source Management para descubrir la entrada nueva.

Procedimiento

1. Inicie sesión en QRadar como administrador.
2. Pulse la pestaña **Admin**.
3. En el menú de navegación, pulse **Plug-ins** o desplácese hasta encontrar el icono de **Configuration Source Management**.
4. Pulse el icono de **Configuration Source Management**.
5. En el menú de navegación, pulse **Credentials**.
6. En el panel Network Groups, pulse el símbolo (+).
7. Escriba un nombre para el grupo de red.
8. En el campo **Add address (IP, CIDR, Wildcard, or Range)**, escriba la dirección IP del SMS.
9. Pulse (+) para añadir la dirección IP.
10. Escriba el nombre de usuario y la contraseña de SMS SmartDashboard.
Para configurar los campos de OPSEC, utilice la información de la ventana OPSEC Application Properties del SmartDashboard donde marcó el recuadro de selección **CPMI** para la entidad de cliente.

11. En el campo **DN**, copie y pegue esta información en el campo **OPSEC Entity SIC Name**.
12. Edite la entrada pegada en **OPSEC Entity SIC Name** sustituyendo el valor de propiedad de CN= por: `cp_mgmt_<nombre_de_host>`
 donde `<nombre_de_host>` es el nombre de **Host** utilizado para el campo **Host** de la aplicación OPSEC.
 Consulte los ejemplos siguientes de una DN y un Host de aplicación OPSEC que se utilizan para crear el nombre SIC de entidad:
 - DN de aplicación OPSEC: `CN=cpsmsxxx,0=svxxx-CPSMS..bsaobx`
 - Host de aplicación OPSEC: `Srvxxx-SMS`
 Utilice texto del DN de aplicación OPSEC y el Host de aplicación OPSEC para formar el **Entity SIC Name**:
 El **Entity SIC Name** es `CN=cp_mgmt_Srvxxx-SMS,0=svxxx-CPSMS..bsaobx`
 El **Entity SIC Name** de esta configuración está basado en una configuración de Pasarela a servidor de gestión. Si la dirección IP de SMS no se utiliza como pasarela, utilice la configuración del Servidor de gestión de la tabla:

Tabla 14. Formatos de nombre SIC de entidad

Tipo	Nombre
Servidor de gestión	<code>CN=cp_mgmt,0=<tomar_valor_0_de_campo_DN></code>
Pasarela a servidor de gestión	<code>CN=cp_mgmt_<nombre_de_host_de_pasarela>,0=<tomar_valor_0_de_campo_DN></code>

13. Copie la entrada del campo **DN** y pegue esta información en el campo **OPSEC Application Object SIC Name**.
14. Pulse **Get Certificate**.
15. Especifique la dirección IP de SMS en el campo **Certificate Authority IP**.
16. Especifique la contraseña única en el campo **Pull Certificate Password**. La contraseña única viene de la ventana Communication de OPSEC Application Properties del SmartDashboard, donde marcó el recuadro de selección **CPMI** para la entidad de cliente.
17. Pulse **Aceptar**.
 Si la operación ha sido satisfactoria, el campo **OPSEC SSL Certificate** se llena y queda desactivado.
 Verifique que la propiedad **Trust State** de la ventana Communication de OPSEC Application Properties cambia a **Trust established**.
 Las credenciales están configuradas y ahora puede ejecutar un descubrimiento.
18. En el menú de navegación, pulse **Discover From Check Point SMS**.
19. En el campo **CPSMS IP Address**, escriba la dirección IP de SMS.

Inicialización del recuento de reglas para Check Point

Complete las configuraciones finales de IBM Security QRadar y Check Point para unir las configuraciones y poner utilizar el recuento de reglas en QRadar.

Acerca de esta tarea

Una vez establecida la confianza y actualizadas las políticas, puede ver el recuento de reglas en QRadar. QRadar Risk Manager necesita aproximadamente 1 hora para procesar los recuentos.

Procedimiento

1. En QRadar, pulse **Riesgos > Configuration Monitor**
2. Efectúe una doble pulsación sobre un dispositivo de Check Point para ver el recuento de reglas.
 - Verifique que el origen de registro es de correlación automática mirando en la columna **Orígenes de registro**.
 - Busque la columna **Recuento de sucesos** en la tabla de reglas.

Preguntas de Policy Monitor

Puede definir preguntas de prueba para identificar el riesgo en los dispositivos de red o las reglas en los dispositivos de red.

Parámetros genéricos y específicos de prueba para las pruebas de Policy Monitor

Configure parámetros para cada prueba de Policy Monitor. Los parámetros configurables están en negrita y subrayados. Pulse un parámetro para ver las opciones disponibles para la pregunta.

Las pruebas de Policy Monitor utilizan dos tipos de parámetros; genéricos y específicos de prueba. Los parámetros genéricos proporcionan 2 o más opciones para personalizar una prueba. Al pulsar un parámetro genérico se conmutan las opciones que están disponibles. Los parámetros específicos de prueba necesitan entrada de usuario. Pulse los parámetros específicos de prueba para especificar información.

Por ejemplo, la prueba de activos denominada **have accepted communication to destination remote network locations** contiene dos parámetros genéricos y un parámetro específico de prueba. Pulse el parámetro genérico, **have accepted**, para seleccionar **have accepted** o **have rejected**. Pulse el parámetro genérico, **to destination**, para seleccionar **to destination** o **from source**. Pulse el parámetro específico de prueba, **remote network locations**, para añadir una ubicación remota para la prueba de activos.

Preguntas de prueba de activos

Las preguntas de activos se utilizan para identificar los activos de la red que infringen una política definida o que presentan riesgos en el entorno.

Las preguntas de prueba de activos se categorizan por tipo de comunicación; real o posible. Ambos tipos de comunicación utilizan pruebas contribuyentes y restrictivas.

La comunicación real incluye los activos en los que se han detectado comunicaciones utilizando conexiones. Las posibles preguntas de comunicación le permiten revisar si son posibles comunicaciones específicas en activos, independientemente de si se ha detectado o no una comunicación.

Una pregunta de prueba contribuyente es la pregunta de prueba base que define qué tipo de comunicación real está intentando probar.

Una pregunta prueba restrictiva restringe los resultados de prueba de la prueba contribuyente para filtrar adicionalmente en la comunicación real violaciones específicas.

Cuando se utiliza una prueba restrictiva, la dirección de la prueba restrictiva debe seguir la misma dirección que la prueba contribuyente. Se pueden utilizar pruebas restrictivas que utilizan una mezcla de direcciones de entrada y salida en situaciones donde se está intentando localizar activos entre dos puntos, por ejemplo dos redes o direcciones IP.

De entrada se refiere a un prueba que filtra las conexiones para las que el activo en cuestión es un destino. De salida se refiere a una prueba que filtra conexiones para las que el activo en cuestión es un origen.

Preguntas de prueba de dispositivos/reglas

Se utilizan dispositivos y reglas para identificar las reglas en un dispositivo que infringen una política definida que puede presentar riesgos en el entorno.

Para obtener una lista detallada de preguntas de regla y de dispositivo, consulte Preguntas de prueba de dispositivos/reglas.

Preguntas contribuyentes para pruebas de comunicación reales

Las pruebas de comunicaciones reales para activos incluyen preguntas contribuyentes y parámetros que se eligen al crear una prueba de Policy Monitor.

Cuando se aplica la condición "have not" a una prueba, la condición "not" se asocia con el parámetro que se está probando.

Por ejemplo, si configura una prueba como **have not accepted communication to destination networks**, la prueba detecta los activos que han aceptado comunicaciones con redes distintas de la red configurada. Otro ejemplo, si configura una prueba como no se ha aceptado la comunicación a Internet, la prueba detecta los activos que han aceptado las comunicaciones desde o hacia áreas distintas de Internet.

La siguiente tabla lista y describe los parámetros de preguntas contribuyentes para pruebas de comunicación reales.

Tabla 15. Parámetros de preguntas contribuyentes para pruebas de comunicación reales

Nombre de prueba	Descripción
have accepted communication to any destination	<p>Detecta activos que tienen comunicaciones hacia o desde cualquier red configurada.</p> <p>Esta prueba le permite definir un punto de inicio o finalización para la pregunta.</p> <p>Por ejemplo, para identificar los activos que han aceptado la comunicación de la DMZ, configure la prueba de la siguiente manera:</p> <p>have accepted communication from any source</p> <p>Puede utilizar esta prueba para detectar las comunicaciones fuera de política.</p>

Tabla 15. Parámetros de preguntas contribuyentes para pruebas de comunicación reales (continuación)

Nombre de prueba	Descripción
have accepted communication to destination networks	<p>Detecta activos que tienen comunicaciones hacia o desde las redes que especifique.</p> <p>Esta prueba le permite definir un punto de inicio o finalización para la pregunta.</p> <p>Por ejemplo, para identificar los activos que se han comunicado con la DMZ, configure la prueba de la siguiente manera:</p> <p>have accepted communication from source <networks></p> <p>Puede utilizar esta prueba para detectar las comunicaciones fuera de política.</p>
have accepted communication to destination IP addresses	<p>Detecta activos que tienen comunicaciones hacia o desde la dirección IP que especifique.</p> <p>Esta prueba le permite especificar la dirección IP o CIDR.</p> <p>Por ejemplo, si desea identificar todos los activos que se han comunicado con un servidor de conformidad específico, configure la prueba de la siguiente manera:</p> <p>se han aceptado las comunicaciones hacia la <dirección IP de servidor de conformidad> de destino</p>
have accepted communication to destination asset building blocks	<p>Detecta activos que tienen comunicaciones hacia o desde los componentes básicos de activo que especifique. Esta prueba le permite reutilizar componentes básicos definidos en el Asistente de reglas de QRadar en la consulta.</p> <p>Para obtener más información sobre reglas, activos y componentes básicos, consulte la publicación <i>IBM Security QRadar SIEM Administration Guide</i>.</p>
have accepted communication to destination asset saved searches	<p>Detecta activos que tienen comunicaciones hacia o desde los activos devueltos por la búsqueda guardada que especifique.</p> <p>Para obtener información sobre cómo crear y guardar una búsqueda de activos, consulte la publicación <i>IBM Security QRadar SIEM Users Guide</i>.</p>
have accepted communication to destination reference sets	<p>Detecta activos que se han comunicado hacia o desde los conjuntos de referencia definidos.</p>

Tabla 15. Parámetros de preguntas contribuyentes para pruebas de comunicación reales (continuación)

Nombre de prueba	Descripción
have accepted communication to destination remote network locations	<p>Detecta activos que se han comunicado con redes definidas como una red remota.</p> <p>Por ejemplo, esta prueba puede identificar hosts que se han comunicado con botnets u otro espacio de direcciones de Internet sospechoso.</p>
have accepted communication to destination geographic network locations	<p>Detecta los activos que se han comunicado con redes definidas como redes geográficas.</p> <p>Por ejemplo, esta prueba puede detectar los activos que han intentado comunicaciones con países en los que no se tienen operaciones de negocio.</p>
have accepted communication to the Internet	<p>Detecta comunicaciones de origen o destino hacia o desde Internet.</p>
are susceptible to one of the following vulnerabilities	<p>Detecta vulnerabilidades específicas.</p> <p>Si desea detectar vulnerabilidades de un tipo determinado, utilice la prueba, are susceptible to vulnerabilities with one of the following classifications.</p> <p>Puede buscar vulnerabilidades utilizando el ID de OSVDB, ID de CVE, ID de Bugtraq o el título.</p>
are susceptible to vulnerabilities with one of the following classifications	<p>Una vulnerabilidad se puede asociar con una o más clasificaciones de vulnerabilidad. Esta prueba filtra todos los activos que incluyen vulnerabilidades con las clasificaciones especificadas.</p> <p>Configure el parámetro classifications para identificar las clasificaciones de vulnerabilidad que desea que aplique esta prueba.</p> <p>Por ejemplo, una clasificación de vulnerabilidad puede ser manipulación de entrada o denegación de servicio.</p>
are susceptible to vulnerabilities with CVSS score greater than 5	<p>Un valor de CVSS (Common Vulnerability Scoring System) es un estándar del sector para evaluar la gravedad de las vulnerabilidades. CVSS se compone de 3 grupos de medidas: base, temporal y ambiental. Estas medidas permiten a CVSS definir y comunicar las características fundamentales de una vulnerabilidad.</p> <p>Esta prueba filtra los activos de la red que incluyen vulnerabilidades con la puntuación CVSS que especifique.</p>
are susceptible to vulnerabilities disclosed after specified date	<p>Detecta activos en la red con una vulnerabilidad que se revela después, antes o en la fecha configurada.</p>

Tabla 15. Parámetros de preguntas contribuyentes para pruebas de comunicación reales (continuación)

Nombre de prueba	Descripción
are susceptible to vulnerabilities on one of the following ports	<p>Detecta activos en la red con una vulnerabilidad que está asociada con los puertos configurados.</p> <p>Configure el parámetro ports para identificar los puertos que desea que esta prueba tenga en cuenta.</p>
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	<p>Detecta activos en la red con una vulnerabilidad que coincide con el nombre de activo, el proveedor, la versión o el servicio basándose en una o más entradas de texto.</p> <p>Configure el parámetro entradas de texto para identificar el nombre de activo, el proveedor, la versión o el servicio que desea que esta prueba tenga en cuenta.</p>
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	<p>Detecta activos en la red con una vulnerabilidad que coincide con el nombre de activo, el proveedor, la versión o el servicio basándose en una o más expresiones regulares.</p> <p>Configure el parámetro expresiones regulares para identificar el nombre de activo, el proveedor, la versión o el servicio que desea que esta prueba tenga en cuenta.</p>
are susceptible to vulnerabilities contained in vulnerability saved searches	<p>Detecta los riesgos que están asociadas con las búsquedas guardadas que se han creado en IBM Security QRadar Vulnerability Manager.</p>

Preguntas de prueba contribuyentes en desuso

Las preguntas contribuyentes que se sustituyen por otra prueba se ocultan en Policy Monitor.

Las pruebas siguientes se ocultan en Policy Monitor:

- assets that are susceptible to vulnerabilities
- assets that are susceptible to vulnerabilities from the following services

Estas pruebas contribuyentes se han sustituido por otras pruebas.

Preguntas restrictivas para pruebas de comunicación reales

Las pruebas de comunicaciones reales de activos incluyen preguntas restrictivas y parámetros que puede elegir al crear una prueba de Policy Monitor.

Cuando aplique la condición de exclusión a una prueba, la condición de exclusión se aplica al parámetro de protocolos.

Por ejemplo, si configura esta prueba como **excluir los siguientes protocolos**, la prueba excluye todos los resultados de activos devueltos que excluyen los protocolos especificados distintos de los protocolos configurados.

La siguiente tabla lista y describe los parámetros de preguntas restrictivas para pruebas de comunicación reales.

Tabla 16. Parámetros de preguntas restrictivas para pruebas de comunicación reales

Nombre de prueba	Descripción
include only the following protocols	<p>Filtra activos de la prueba de contribución que incluyen o excluyen los protocolos especificados.</p> <p>Esta prueba sólo se puede seleccionar cuando se añade una prueba de activo contribuyente a esta pregunta.</p>
include only the following inbound ports	<p>Filtra activos de la prueba contribuyente que solo incluyen o excluyen los puertos especificados.</p> <p>Esta prueba sólo se puede seleccionar cuando se añade una prueba de activo contribuyente a esta pregunta.</p>
include only the following inbound applications	<p>Filtra los activos de la pregunta de prueba contribuyente que solo incluyen o excluyen las aplicaciones de entrada o salida.</p> <p>Esta prueba filtra conexiones que solo incluyen datos de flujo.</p>
include only if the source inbound and destination outbound bytes have a percentage difference less than 10	<p>Filtra activos de la pregunta de prueba contribuyente que se basa en las comunicaciones con una proporción específica de bytes de entrada a salida (o de salida a entrada)</p> <p>Esta prueba es útil para detectar los hosts que pueden estar mostrando un comportamiento de tipo proxy (entrada igual a salida).</p>

Tabla 16. Parámetros de preguntas restrictivas para pruebas de comunicación reales (continuación)

Nombre de prueba	Descripción
include only if the inbound and outbound flow count has a percentage difference less than 10	<p>Filtra activos de la pregunta de pruebas contribuyente se basa en las comunicaciones con una proporción específica de flujos de entrada a salida (o de salida a entrada).</p> <p>Esta prueba filtra conexiones que incluyen datos de flujo cuando se selecciona el recuento de flujo.</p> <p>Esta prueba restrictiva requiere dos pruebas contribuyentes que especifiquen un origen y destino. La prueba siguiente describe un conjunto de preguntas que intentan determinar qué activos entre dos puntos tienen una diferencia de porcentaje de entrada y de salida mayor que el 40%. Por ejemplo,</p> <ul style="list-style-type: none"> • Prueba contribuyente: se ha aceptado la comunicación hacia internet. • Prueba contribuyente: y se ha aceptado la comunicación desde internet. • Prueba restrictiva: e incluir sólo si el recuento de flujo de entrada y de salida tiene una diferencia de porcentaje mayor que 40.
include only if the time is between start time and end time inclusive	<p>Filtra las comunicaciones en la red que se han producido dentro de un rango de tiempo específico. Esto le permite detectar comunicaciones fuera de política. Por ejemplo, si la política corporativa permite comunicaciones FTP entre la 1 y las 3 AM, esta prueba puede detectar cualquier intento de utilizar FTP para comunicarse fuera de dicho rango de tiempo.</p>
include only if the day of week is between start day and end day inclusive	<p>Filtra activos de la pregunta de prueba contribuyente basándose en las comunicaciones de red que se han producido dentro de un rango de tiempo específico. Esto le permite detectar comunicaciones fuera de política.</p>
include only if susceptible to vulnerabilities that are exploitable.	<p>Filtra activos de una pregunta de prueba contribuyente en busca de vulnerabilidades específicas y restringe los resultados a los activos aprovechables.</p> <p>Esta prueba restrictiva no contiene parámetros configurables, pero se utiliza conjuntamente con la prueba contribuyente, are susceptible to one of the following vulnerabilities. Esta regla contribuyente que contiene un parámetro de vulnerabilidades es necesaria.</p>

Tabla 16. Parámetros de preguntas restrictivas para pruebas de comunicación reales (continuación)

Nombre de prueba	Descripción
include only the following networks	Filtra activos de una pregunta de prueba contribuyente que incluye o excluye las redes configuradas.
include only the following asset building blocks	Filtra activos de una pregunta de prueba contribuyente que están o no están asociados con los componentes básicos de activo configurados.
include only the following asset saved searches	Filtra activos de una pregunta de prueba contribuyente que están o no están asociados con la búsqueda guardada de activo.
include only the following reference sets	Filtra activos de una pregunta de prueba contribuyente que incluye o excluye los conjuntos de referencia configurados.
include only the following IP addresses	Filtra activos que están o no están asociados con las direcciones IP configuradas.
include only if the Microsoft Windows service pack for operating systems is below 0	Filtra activos para determinar si un nivel de Service Pack de Microsoft Windows para un sistema operativo está por debajo del nivel que especifica la política de empresa.
include only if the Microsoft Windows security setting is less than 0	Filtra activos para determinar si un valor de seguridad de Microsoft Windows está por debajo del nivel que especifica la política de empresa.
include only if the Microsoft Windows service equals status	Filtra activos para determinar si un servicio de Microsoft Windows es desconocido, arranque, kernel, automático, petición o inhabilitado.
include only if the Microsoft Windows setting equals regular expressions	Filtra activos para determinar si un valor de Microsoft Windows es la expresión regular especificada.

Preguntas contribuyentes para posibles pruebas de comunicación

Las pruebas de comunicación posibles para activos incluyen preguntas contribuyentes y parámetros que puede elegir al crear una prueba de Policy Monitor.

La tabla siguiente lista y describe los parámetros de preguntas contribuyentes para las posibles pruebas de comunicación.

Tabla 17. Parámetros de preguntas de comunicación posibles para pruebas contribuyentes

Nombre de prueba	Descripción
<p>have accepted communication to any destination</p>	<p>Detecta activos que tienen comunicaciones posibles hacia o desde cualquier origen o destino especificado. Por ejemplo, para determinar si un servidor crítico puede recibir posiblemente comunicaciones desde cualquier origen, configure la prueba de la siguiente manera:</p> <p>have accepted communication from any source.</p> <p>A continuación, puede aplicar la devolución de una prueba restrictiva si dicho servidor ha recibido comunicaciones en el puerto 21. Esto le permite detectar comunicaciones fuera de política para dicho servidor crítico.</p>
<p>have accepted communication to destination networks</p>	<p>Detecta activos que tienen comunicaciones posibles hacia o desde la red configurada.</p> <p>Esta prueba le permite definir un punto de inicio o finalización para la pregunta.</p> <p>Por ejemplo, para identificar los activos que tiene la posibilidad de comunicarse con la DMZ, configure la prueba de la siguiente manera:</p> <p>have accepted communication from source <networks></p> <p>Puede utilizar esta prueba para detectar las comunicaciones fuera de política.</p>
<p>have accepted communication to destination IP addresses</p>	<p>Detecta activos que tienen comunicaciones posibles hacia o desde la dirección IP configurada. Esta prueba le permite especificar una dirección IP única como foco para posibles comunicaciones. Por ejemplo, si desea identificar todos los activos que se pueden comunicar con un servidor de conformidad específico, configure la prueba de la manera siguiente:</p> <p>se han aceptado las comunicaciones hacia la <dirección IP de servidor de conformidad> de destino</p>

Tabla 17. Parámetros de preguntas de comunicación posibles para pruebas contribuyentes (continuación)

Nombre de prueba	Descripción
have accepted communication to destination asset building blocks	<p>Detecta activos que tienen comunicaciones posibles hacia o desde el activo configurado utilizando componentes básicos. Esta prueba le permite reutilizar componentes básicos definidos en el Asistente de reglas de QRadar en la consulta. Por ejemplo, si desea identificar todos los activos que pueden comunicarse con activos protegidos, configure la prueba de la siguiente manera:</p> <p>se han aceptado comunicaciones hacia <BB:HostDefinition:Protected Assets> de destino</p> <p>Para obtener más información sobre las reglas y los componentes básicos, consulte la publicación <i>IBM Security QRadar SIEM Administration Guide</i>.</p>
have accepted communication to destination asset saved searches	<p>Detecta los activos que han aceptado las comunicaciones hacia o desde los activos devueltos por la búsqueda guardada que especifique.</p> <p>Una búsqueda de activos guardada debe existir antes de utilizar esta prueba. Para obtener información sobre cómo crear y guardar una búsqueda de activos, consulte la publicación <i>IBM Security QRadar SIEM Users Guide</i>.</p>
have accepted communication to destination reference sets	<p>Detecta si la comunicación de origen o destino es posible hacia o desde los conjuntos de referencia.</p>
have accepted communication to the Internet	<p>Detecta si las comunicaciones de origen o destino son posibles hacia o desde Internet.</p> <p>Especifique el parámetro hasta o desde, para considerar el tráfico de comunicación hacia o desde Internet.</p>
are susceptible to one of the following vulnerabilities	<p>Detecta vulnerabilidades específicas posibles.</p> <p>Si desea detectar vulnerabilidades de un tipo determinado, utilice la prueba, are susceptible to vulnerabilities with one of the following classifications.</p> <p>Especifique las vulnerabilidades a las que desea que se aplique esta prueba. Puede buscar vulnerabilidades utilizando el ID de OSVDB, ID de CVE, ID de Bugtraq o el título</p>

Tabla 17. Parámetros de preguntas de comunicación posibles para pruebas contribuyentes (continuación)

Nombre de prueba	Descripción
are susceptible to vulnerabilities with one of the following classifications	<p>Una vulnerabilidad se puede asociar con una o varias clasificaciones de vulnerabilidad. Esta prueba filtra todos los activos que tienen vulnerabilidades posibles con una puntuación de CVSS (Common Vulnerability Scoring System - Sistema de puntuación de vulnerabilidad común), tal como se ha especificado.</p> <p>Configure el parámetro de clasificaciones para identificar las clasificaciones de vulnerabilidad que desea que aplique esta prueba.</p>
are susceptible to vulnerabilities with CVSS score greater than 5	<p>Un valor de CVSS (Common Vulnerability Scoring System) es un estándar del sector para evaluar la gravedad de las posibles vulnerabilidades. CVSS está formado por tres grupos de medidas: base, temporal y ambiental. Estas medidas permiten a CVSS definir y comunicar las características fundamentales de una vulnerabilidad.</p> <p>Esta prueba filtra los activos de la red que incluyen el valor de CVSS configurado.</p>
are susceptible to vulnerabilities disclosed after specified date	<p>Filtra los activos de la red con una posible vulnerabilidad que se revela después, antes o en la fecha configurada.</p>
are susceptible to vulnerabilities on one of the following ports	<p>Filtra los activos de la red con una posible vulnerabilidad que está asociada con los puertos configurados.</p> <p>Configure el parámetro de puertos para identificar los activos que tienen vulnerabilidades posibles basándose en el número de puerto especificado.</p>
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	<p>Detecta activos en la red con una vulnerabilidad que coincide con el nombre de activo, el proveedor, la versión o el servicio basándose en una o más entradas de texto.</p> <p>Configure el parámetro entradas de texto para identificar el nombre de activo, el proveedor, la versión o el servicio que desea que esta prueba tenga en cuenta.</p>
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	<p>Detecta activos en la red con una vulnerabilidad que coincide con el nombre de activo, el proveedor, la versión o el servicio basándose en una o más expresiones regulares.</p> <p>Configure el parámetro expresiones regulares para identificar el nombre de activo, el proveedor, la versión o el servicio que desea que esta prueba tenga en cuenta.</p>

Tabla 17. Parámetros de preguntas de comunicación posibles para pruebas contribuyentes (continuación)

Nombre de prueba	Descripción
are susceptible to vulnerabilities contained in vulnerability saved searches	Detecta los riesgos que están asociadas con las búsquedas guardadas que se han creado en IBM Security QRadar Vulnerability Manager.

Preguntas de prueba contribuyentes en desuso

Si se sustituye una prueba por otra prueba, ésta se oculta en Policy Monitor.

Las pruebas siguientes se ocultan en Policy Monitor:

- assets that are susceptible to vulnerabilities from the following vendors
- assets that are susceptible to vulnerabilities from the following services

Estas pruebas contribuyentes se han sustituido por otras pruebas.

Parámetros de preguntas restrictivas para pruebas de comunicación posibles

Las pruebas de comunicación posibles para activos incluyen parámetros de preguntas restrictivas.

La siguiente tabla lista y describe los parámetros de preguntas restrictivas para pruebas de comunicación posibles.

Tabla 18. Pruebas restrictivas para pruebas de comunicación posibles

Nombre de prueba	Descripción
include only the following protocols	Filtra activos que se han o no se han comunicado posiblemente con los protocolos configurados, conjuntamente con las demás pruebas añadidas a esta pregunta.
include only the following inbound ports	Filtra activos que se han o no se han comunicado posiblemente con los puertos configurados, conjuntamente con las demás pruebas añadidas a esta pregunta.
include only ports other than the following inbound ports	Filtra activos de una pregunta de prueba contribuyente que se han o no se han comunicado posiblemente con puertos distintos de los puertos configurados, conjuntamente con las demás pruebas añadidas a esta pregunta.
include only if susceptible to vulnerabilities that are exploitable.	Filtra activos de una pregunta de prueba contribuyente en busca de posibles vulnerabilidades específicas y restringe los resultados a los activos aprovechables. Esta prueba restrictiva no contiene parámetros configurables, pero se utiliza conjuntamente con la prueba contribuyente, are susceptible to one of the following vulnerabilities . Esta regla contribuyente que contiene un parámetro de vulnerabilidades es necesaria.

Tabla 18. Pruebas restrictivas para pruebas de comunicación posibles (continuación)

Nombre de prueba	Descripción
include only the following networks	Filtra activos de una pregunta de prueba contribuyente que sólo incluyen o excluyen las redes configuradas.
include only the following asset building blocks	Filtra activos de una pregunta de prueba contribuyente que sólo incluyen o excluyen los componentes básicos de activos configurados.
include only the following asset saved searches	Filtra activos de una pregunta de prueba contribuyente que sólo incluyen o excluyen la búsqueda guardada de activos asociados.
include only the following reference sets	Filtra activos de una pregunta de prueba contribuyente que sólo incluyen o excluyen los conjuntos de referencia configurados.
include only the following IP addresses	Filtra activos de una pregunta de prueba contribuyente que sólo incluyen o excluyen las direcciones IP configuradas.
include only if the Microsoft Windows service pack for operating systems is below 0	Filtra activos para determinar si un nivel de Service Pack de Microsoft Windows para un sistema operativo está por debajo del nivel que especifica la política de empresa.
include only if the Microsoft Windows security setting is less than 0	Filtra activos para determinar si un valor de seguridad de Microsoft Windows está por debajo del nivel que especifica la política de empresa.
include only if the Microsoft Windows service equals status	Filtra activos para determinar si un servicio de Microsoft Windows es desconocido, arranque, kernel, automático, petición o inhabilitado.
include only if the Microsoft Windows setting equals regular expressions	Filtra activos para determinar si un valor de Microsoft Windows es la expresión regular especificada.

Preguntas de prueba de dispositivo/reglas

Las preguntas de prueba de dispositivo/reglas se utilizan para identificar las reglas de un dispositivo que infringen una política definida que pueden presentar riesgos en el entorno.

Las preguntas de prueba de dispositivo/reglas se describen en la tabla siguiente.

Tabla 19. Pruebas de dispositivo/reglas

Nombre de prueba	Descripción
permitir conexiones a las redes siguientes	Filtra reglas y conexiones de dispositivo hacia o desde las redes configuradas. Por ejemplo, si configura la prueba para permitir las comunicaciones a una red, la prueba filtra todas las reglas y conexiones que permiten las conexiones con la red configurada.

Tabla 19. Pruebas de dispositivo/reglas (continuación)

Nombre de prueba	Descripción
permitir conexiones con las siguientes direcciones IP	Filtra reglas y conexiones de dispositivo hacia o desde las direcciones IP configuradas. Por ejemplo, si configura la prueba para permitir las comunicaciones con una dirección IP, la prueba filtra todas las reglas y conexiones que permiten las conexiones con la dirección IP configurada.
permitir las conexiones con los siguientes componentes básicos de activo	Filtra reglas y conexiones de dispositivo hacia o desde el componente básico de activo configurado.
permitir las conexiones con los siguientes conjuntos de referencia	Filtra reglas y conexiones de dispositivo hacia o desde los conjuntos de referencia configurados.
permitir conexiones utilizando los siguientes puertos de destino y protocolos	Filtra reglas y conexiones de dispositivo hacia o desde los puertos y protocolos configurados
permitir conexiones utilizando los protocolos siguientes	Filtra reglas y conexiones de dispositivo hacia o desde los protocolos configurados.
permitir conexiones a Internet	Filtra reglas y conexiones de dispositivo hacia y desde Internet.
son uno de los dispositivos siguientes	Filtra todos los dispositivos de red a los dispositivos configurados. Esta prueba puede filtrar basándose en dispositivos que están o no están en la lista configurada.
son uno de los conjuntos de referencia siguientes	Filtra reglas de dispositivo basándose en los conjuntos de referencia que especifique.
son una de las siguientes redes	Filtra reglas de dispositivo basándose en las redes que especifique.
están utilizando uno de los siguientes adaptadores	Filtra reglas de dispositivo basándose en los adaptadores que especifique.

Capítulo 7. Investigar conexiones

Una conexión es una grabación de una comunicación, incluidas las comunicaciones denegadas, entre dos direcciones IP exclusivas a través de un puerto de destino específico, tal como se detecta durante un intervalo de tiempo específico.

Si dos direcciones IP se comunican muchas veces durante el mismo intervalo en un puerto, sólo se registra una comunicación, pero los bytes comunicados y el número de flujos se suman con la conexión. Al final del intervalo, la información de conexión se acumula durante el intervalo y se almacenan en la base de datos.

Las conexiones le permiten supervisar e investigar conexiones de dispositivos de red o realizar búsquedas avanzadas. Puede:

- Buscar conexiones
- Buscar un subconjunto de conexiones
- Marcar resultados de búsqueda como un falso positivo para desconectar los sucesos positivos falsos de las infracciones creadas.
- Ver información de conexión agrupada por diversas opciones
- Exportar conexiones en formato XML o CSV
- Utilizar el gráfico interactivo para ver las conexiones en la red

Visualización de conexiones

Ver información de conexión que se agrupa por diversas opciones.

Acerca de esta tarea

De forma predeterminada, la ventana Conexiones visualiza los gráficos siguientes:

- El gráfico **Registros coincidentes a lo largo del tiempo** proporciona información de serie temporal que muestra el número de conexiones basado en el tiempo.
- **Gráfico de conexión** que proporciona una representación visual de las conexiones recuperadas.

Nota: Si una búsqueda guardada es el valor predeterminado, se visualizan los resultados de dicha búsqueda guardada.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Conexiones**.
3. Seleccione un marco temporal seleccionando los parámetros **Hora de inicio** y **Hora de finalización** o utilice la lista **Ver**.

En la tabla, pulse con el botón derecho sobre cualquier casilla, (excepto las casillas de la columna **Hora de último paquete**) para un menú, para aplicar más filtrado o para **Ver sucesos de conexión**.

Ejemplo

La ventana Conexiones visualiza la información siguiente:

Tabla 20. Ventana Conexiones - valor predeterminado

Parámetro	Descripción
Filtros actuales	<p>Este parámetro solo se visualiza después de aplicar un filtro.</p> <p>Los detalles del filtro que se aplica al resultado de la búsqueda se visualizan en la parte superior. Para borrar estos valores de filtro, pulse Borrar filtro.</p>
Ver	<p>En la lista, seleccione el rango de tiempo que desea filtrar. Utilice la opción Expandir para ajustar el rango de tiempo.</p>
Estadísticas actuales	<p>Las estadísticas actuales incluyen los parámetros siguientes:</p> <p>Resultados totales: Número total de resultados que coinciden con los criterios de búsqueda.</p> <p>Archivos de datos buscados: Número total de archivos de datos buscados durante el intervalo de tiempo especificado.</p> <p>Archivos de datos comprimidos buscados: Número total de archivos de datos comprimidos buscados dentro del intervalo de tiempo especificado.</p> <p>Recuento de archivos de índice: Número total de archivos de índice buscados durante el intervalo de tiempo especificado.</p> <p>Duración: Duración de la búsqueda.</p> <p>Estadísticas actuales útiles para la resolución de problemas. Cuando se ponga en contacto con el soporte al cliente para solucionar un problema, puede que se le solicite que proporcione información estadística actual. Pulse la flecha situada junto a Estadísticas actuales para visualizar u ocultar las estadísticas.</p>
Gráficos	<p>Visualiza gráficos que representan la opción de registros coincidentes por el tiempo de intervalo y/o agrupación. Pulse (Ocultar gráficos) si desea eliminar el gráfico de la visualización.</p> <p>Nota: Elimine Firefox <i>Adblock Plus</i> si impide que los gráficos se visualicen en Firefox.</p>
Hora de último paquete	<p>La fecha y hora del último paquete procesado para esta conexión.</p>
Tipo de origen	<p>El Tipo de origen para esta conexión, que puede ser: Host o Remoto.</p>

Tabla 20. Ventana Conexiones - valor predeterminado (continuación)

Parámetro	Descripción
Origen	A continuación se proporcionan las opciones de Origen : Dirección IP : Dirección IP para el origen de esta conexión. Si el Tipo de origen es Host , se visualiza la dirección IP. País : País de origen (con el distintivo de país) para esta conexión. El distintivo de país sólo se visualiza si el tipo de origen es remoto.
Tipo de destino	Las opciones para Tipo de destino son Host o Remoto .
Destino	Las opciones para Destino son: Dirección IP : Si el tipo de destino es host, se visualiza la dirección IP. País : País de destino (con el distintivo de país) para esta conexión. El distintivo de país sólo se visualiza si el Tipo de destino es remoto.
Protocolo	Protocolo que se utiliza para esta conexión.
Puerto de destino	Puerto de destino para esta conexión.
Aplicación de flujo	Aplicación de flujo que ha generado la conexión.
Origen de flujo	Origen de flujos asociados con esta conexión. Este parámetro sólo se aplica a las conexiones aceptadas.
Recuento de flujos	Número total de flujos asociados con esta conexión.
Bytes de origen de flujo	Número total de bytes de origen de flujo asociados con esta conexión.
Bytes de destino de flujo	Número total de bytes de destino asociados con esta conexión.
Origen de registro	Origen de sucesos que contribuyen a esta conexión.
Recuento de sucesos	Número total de sucesos detectados para la conexión.
Tipo de conexión	Las opciones para tipo de conexión son: Permitir o Denegar .

Utilizar gráficos para ver datos de conexión

Puede ver los datos de conexión utilizando diversas opciones de gráfico. De forma predeterminada, puede ver los datos utilizando registros coincidentes a lo largo del tiempo y el gráfico de conexión.

Los registros coincidentes a lo largo del tiempo es una opción que indica el número de conexiones basadas en el tiempo.

Un gráfico de conexión proporciona una representación visual de la conexión recuperada. Si desea investigar adicionalmente conexiones utilizando el gráfico de conexión, consulte Utilización del gráfico de conexión.

Las opciones de gráfico disponibles para las conexiones agrupadas son tabla, barra y circular. Para obtener más información sobre la búsqueda de conexiones, consulte Buscar conexiones.

Si utiliza una extensión de navegador Adblock Plus con un navegador web Mozilla Firefox, es posible que los gráficos no se visualicen correctamente. Para que se visualicen los gráficos, debe eliminar la extensión de navegador Adblock Plus. Para obtener más información sobre cómo eliminar complementos, consulte la documentación de navegador web.

Utilización del gráfico de serie temporal

Los gráficos de serie temporal son representaciones gráficas de las conexiones a lo largo del tiempo; los puntos más altos y más bajos que se visualizan representan la actividad de conexión alta y baja.

Antes de empezar

Si ha guardado previamente una búsqueda para que sea la predeterminada, los resultados de dicha búsqueda guardada se visualizan en la página Connections. Si dicha búsqueda incluía opciones Group By seleccionadas en el recuadro Advanced View Definitions, el gráfico de serie temporal no está disponible. Debe borrar los criterios de búsqueda antes de continuar.

Acerca de esta tarea

Los gráficos de serie temporal son útiles para la tendencia de datos a corto plazo y a largo plazo. Utilizando gráficos de serie temporal, puede acceder, navegar e investigar conexiones de diversas vistas y perspectivas.

La tabla siguiente proporciona funciones que puede utilizar para ver gráficos de serie temporal.

Tabla 21. Funciones de gráfico de serie temporal

Si desea	Entonces
Ver conexiones con mayor detalle	<p>El aumento de los datos en un gráfico de serie temporal le permite investigar segmentos de tiempo más pequeños de las conexiones. Puede ampliar el gráfico de serie temporal utilizando una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Pulse la tecla Mayús y pulse el gráfico en el momento que desea investigar. • Pulse las teclas Control y Mayús mientras pulsa y arrastra el puntero del ratón sobre el rango de tiempo que desea ver. • Mueva el puntero de ratón sobre el gráfico y pulse la flecha Arriba en el teclado. • Mueva el puntero de ratón sobre el gráfico y, a continuación, utilice la rueda del ratón para acercar (girar la rueda del ratón hacia arriba). <p>Después de ampliar un gráfico de serie de tiempo, el gráfico se renueva para mostrar un segmento de tiempo menor.</p>
Ver un intervalo de tiempo mayor de conexiones	<p>La inclusión de rangos de tiempo adicionales en el gráfico de serie temporal le permite investigar segmentos de tiempo mayores o volver al rango de tiempo máximo. Puede ver un rango de tiempo utilizando una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Pulse Max en la esquina superior izquierda del gráfico o pulse la tecla Inicio para volver al rango de tiempo máximo. • Mueva el puntero de ratón sobre el gráfico y pulse la flecha hacia abajo en el teclado. • Mueva el puntero de ratón sobre el gráfico de trazos y, a continuación, utilice la rueda del ratón para alejar (girar la rueda del ratón hacia abajo).
Explorar el gráfico	<p>Para ver el gráfico para determinar la información en cada punto de datos:</p> <ul style="list-style-type: none"> • Pulse y arrastre el gráfico para explorar la línea temporal. • Pulse la tecla RePág para mover la línea temporal una página completa a la izquierda. • Pulse la tecla de flecha izquierda para mover la línea temporal media página a la izquierda. • Pulse la tecla AvPág para mover la línea temporal una página completa a la derecha. • Pulse la tecla de flecha derecha para mover la línea temporal media página a la derecha

Procedimiento

Procedimiento

1. Pulse la pestaña Risks.
2. En el menú de navegación, pulse **Connections**.
3. En el panel de gráficos, pulse en el icono **Configure**.
4. Utilizando la lista desplegable **Chart Type**, seleccione Time Series.
5. Utilizando los gráficos de serie temporal interactivos, puede navegar por una línea temporal para investigar las conexiones.
6. Para renovar la información del gráfico, pulse Update Details.

Utilizar gráfico de conexión para ver conexiones de red

El gráfico de conexión proporciona una representación visual de las conexiones de la red.

El gráfico que se visualiza en la ventana Conexiones no es interactivo. Si pulsa el gráfico, se visualiza la ventana Visor de datos radial. La ventana Visor de datos radial le permite manipular el gráfico, según sea necesario.

De forma predeterminada, el gráfico muestra las conexiones de red de la siguiente manera:

- Sólo se visualizan las conexiones permitidas.
- Todas las direcciones IP locales se contraen para mostrar sólo las redes de hoja.
- Todos los nodos de país se contraen en un nodo denominado Países remotos.
- Todos los nodos de red remota se contraen en un nodo denominado Redes remotas.
- La vista previa de la vista miniatura del gráfico visualiza una parte del gráfico principal. Esto es útil para gráficos grandes.

El Visor de datos radial contiene varias opciones de menú, que incluyen:

Tabla 22. Opciones de menú de Visor de datos radial

Opción de menú	Descripción
Tipo de conexión	De forma predeterminada, el gráfico radial visualiza las conexiones aceptadas. Si desea ver las conexiones denegadas, seleccione Denegar en la lista desplegable Tipo de conexión .
Deshacer	Contrae la última expansión de nodo. Si desea deshacer varias expansiones, pulse el botón Deshacer para cada expansión.
Descargar	Pulse Descargar para guardar la topología actual como un archivo de imagen JPEG o un archivo de dibujo Visio (VDX). Para descargar y guardar la topología actual como un archivo de dibujo Visio (VDX), la versión de software mínima que necesita es Microsoft Visio Standard 2010.

En la tabla siguiente se proporcionan funciones adicionales para ver las conexiones, que incluyen:

Tabla 23. Funciones de Visor de datos radial

Si desea	Entonces
Acercarse o alejarse	Utilice el graduador del lado superior derecho del gráfico para cambiar la escala.
Distribuir nodos en el gráfico para ver detalles adicionales	Arrastre el nodo a la ubicación preferida para distribuir los nodos en el gráfico.
Expandir un nodo de red	Efectúe una doble pulsación en el nodo para expandir y ver activos para ese nodo. El nodo se expande para incluir los activos específicos con los que ese nodo se estaba comunicando. De forma predeterminada, esta expansión está limitada a los primeros 100 activos de la red.
Ver detalles adicionales relacionados con una conexión	<p>Apunte el ratón sobre la línea de conexión para ver detalles adicionales.</p> <p>Si la conexión es entre un nodo de red y una red remota o país remoto, pulse el botón derecho del ratón para visualizar los siguientes menú Origen y Ver flujos:</p> <p>Si la conexión es entre dos direcciones IP, se visualiza la información de origen, destino y puerto al pulsar la línea de conexión.</p>
Determinar la cantidad de datos implicados en la conexión	El grosor de la línea del gráfico indica la cantidad de datos implicados en la conexión. Una línea más gruesa indica una mayor cantidad de datos. Esta información se basa en la cantidad de bytes implicados en la comunicación
Resaltar una vía de acceso de conexión	Apunte el ratón sobre la línea de conexión. Si se permite la conexión, la vía de acceso queda resaltada en verde. Si se deniega la conexión, la vía de acceso queda resaltada en rojo.
Determinar la vía de acceso de conexión para un nodo en particular	Apunte el ratón sobre el nodo. Si el nodo está permitido, la vía de acceso al nodo y el nodo quedan resaltados en verde. Si se deniega el nodo, la vía de acceso al nodo y el nodo quedan resaltados en rojo.
Cambiar la vista gráfica	Utilizando la vista previa de miniatura, mueva la miniatura a la parte del gráfico que desea visualizar.

Utilización de los gráficos circular, de barras y de tabla

Puede ver datos de conexiones utilizando un gráfico circular, de barras o de tabla.

Acerca de esta tarea

Las opciones de gráfico circular, de barras y de tabla sólo se visualizan si la búsqueda incluye opciones Agrupar por seleccionadas en las opciones de Definición de vista avanzada.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Conexiones**.

Nota: Se visualizan los resultados de la búsqueda guardados predeterminados.

3. Realice una búsqueda.
4. En el panel de gráficos, pulse el icono **Configuración**.
5. Configure los parámetros:

Opción	Descripción
Valor para gráfico	En la lista Valor para gráfico , seleccione el tipo de objeto que desea trazar en el gráfico. Las opciones incluyen todos los parámetros de flujo normalizados y personalizados incluidos en los parámetros de búsqueda.
Tipo de gráfico	En la lista Tipo de gráfico , seleccione el tipo de gráfico que desea ver. Las opciones incluyen: <ul style="list-style-type: none">• Tabla: Visualiza los datos en una tabla.• Barra: Visualiza los datos en un diagrama de barras.• Circular: Visualiza los datos en un gráfico circular.

6. Pulse **Guardar**.

Los datos no se renuevan automáticamente, a menos que los criterios de búsqueda se muestren para visualizar detalles automáticamente.
7. Para renovar los datos, pulse **Actualizar detalles**.

Búsqueda de conexiones

Puede buscar conexiones utilizando criterios específicos y visualizar conexiones que coinciden con los criterios de búsqueda en una lista de resultados. Puede crear una nueva búsqueda o cargar un conjunto de criterios de búsqueda guardado previamente.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Conexiones**.

Si es aplicable, se visualizan los resultados de búsqueda guardada predeterminados.
3. Mediante el uso de la lista **Buscar**, seleccione **Nueva búsqueda**.
4. Si desea cargar una búsqueda guardada anteriormente, utilice una de las opciones siguientes:
 - a. En la lista **Grupo**, seleccione el grupo al que está asociada la búsqueda guardada.
 - b. En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desea cargar.
 - c. En el campo **Escriba la búsqueda guardada o seleccione en la lista**, escriba el nombre de la búsqueda que desea guardar. En la lista **Búsquedas guardadas disponibles**, seleccione la búsqueda guardada que desea cargar.

- d. Pulse **Cargar**.
- e. En el panel **Editar búsqueda**, seleccione las opciones que desea para esta búsqueda.

Opción	Descripción
Incluir en Búsquedas rápidas	Incluir esta búsqueda en los elementos de búsqueda rápida.
Incluir en Panel de control	Incluir los datos de la búsqueda guardada en el panel de control. Este parámetro sólo está disponible si la búsqueda está agrupada.
Establecer como valor predeterminado	Establezca esta búsqueda como búsqueda predeterminada.
Compartir con todos	Compartir estos requisitos de búsqueda con todos los demás usuarios de IBM Security QRadar Risk Manager.

5. En el panel Rango de tiempo, seleccione una opción para el rango de tiempo que desea capturar para esta búsqueda.

Opción	Descripción
Reciente	Utilizando la lista, especifique el rango de tiempo que desea filtrar.
Intervalo específico	Utilizando el calendario, especifique el rango de fecha y hora que desea filtrar.

6. Si ha terminado de configurar la búsqueda y desea ver los resultados, pulse **Buscar**.
7. En el panel Parámetros de búsqueda, defina los criterios de búsqueda específicos:
 - a. Utilizando la primera lista, seleccione un atributo en el que desea buscar. Por ejemplo, Tipo de conexión, Red de origen o Dirección.
 - b. Utilizando la segunda lista, seleccione el modificador que desea utilizar para la búsqueda. La lista de modificadores que se visualizan depende del atributo seleccionado en la primera lista.
 - c. En el campo de texto, escriba información específica relacionada con la búsqueda.
 - d. Pulse **Añadir filtro**.
 - e. Repita los pasos a hasta e para cada filtro que desea añadir a los criterios de búsqueda.
 - f. Si ha terminado de configurar la búsqueda y desea ver los resultados, pulse **Buscar**. De lo contrario, continúe en el paso siguiente.
8. Si desea guardar automáticamente los resultados de búsqueda cuando se haya completado la búsqueda, seleccione el recuadro de selección **Guarde los resultados** cuando finalice la búsqueda y especifique un nombre.
9. Si ha terminado de configurar la búsqueda y desea ver los resultados, pulse **Buscar**. De lo contrario, continúe en el paso siguiente.
10. Utilizando el panel de definición de columna, defina las columnas y el diseño de columna que desea utilizar para ver los resultados:
 - a. En la lista **Visualizar**, seleccione la vista que desea asociar con esta búsqueda.

- b. Pulse la flecha situada junto a **Definición de vista avanzada** para visualizar los parámetros de búsqueda avanzada. Pulse la flecha de nuevo para ocultar los parámetros.

11. Pulse **Buscar**.

Guardar criterios de búsqueda

Puede crear una búsqueda especificando criterios de búsqueda y puede guardar la búsqueda para su uso futuro.

Acerca de esta tarea

Puede personalizar las columnas que aparecen en los resultados de búsqueda. Estas opciones están disponibles en la sección Column Definition y se denominan opciones de Advanced View Definition.

Tabla 24. Opciones de Advanced View Definition

Parámetro	Descripción
Escriba la columna o seleccione en la lista	<p>Filtra las columnas de a la lista de columnas disponibles.</p> <p>Escriba el nombre de la columna que desea localizar o escriba una palabra clave para visualizar una lista de nombres de columna que incluyan dicha palabra clave.</p> <p>Por ejemplo, escriba Source para visualizar una lista de columnas que incluyan Source en el nombre de columna.</p>
Available Columns	<p>Lista las columnas disponibles asociadas a la vista seleccionada. Las columnas que se están utilizando actualmente para esta búsqueda guardada se resaltan y se muestran en la lista Columns .</p>
Añada o elimine botones de columna (conjunto superior)	<p>El conjunto superior de botones le permite personalizar la lista Group By.</p> <ul style="list-style-type: none"> • Add Column: Seleccione una o más columnas de la lista Available Columns y pulse el botón Add Column. • Remove Column: Seleccione una o más columnas en la lista Group By y pulse el botón Remove Column.
Añada o elimine botones de columna (conjunto inferior)	<p>El conjunto inferior de botones le permite personalizar la lista Columns.</p> <ul style="list-style-type: none"> • Add Column: Seleccione una o más columnas de la lista Available Columns y pulse el botón Add Column. • Remove Column: Seleccione una o más columnas en la lista Columns y pulse el botón Remove Column.

Tabla 24. Opciones de Advanced View Definition (continuación)

Parámetro	Descripción
Group By	<p>Especifica las columnas de las que la búsqueda guardada agrupa los resultados. Puede personalizar adicionalmente la lista Group By utilizando las opciones siguientes:</p> <ul style="list-style-type: none"> • Move Up: Seleccione una columna y súbala en la lista de prioridad utilizando el icono Move Up. • Move Down: Seleccione una columna y bájela en la lista de prioridad utilizando el icono Move Down. <p>La lista de prioridad especifica en qué orden se agrupan los resultados. Los resultados de búsqueda se agruparán por la primera columna de la lista Group By y luego se agruparán por la siguiente columna de la lista.</p>
Columns	<p>Especifica columnas elegidas para la búsqueda. Las columnas se cargan de una búsqueda guardada. Puede personalizar la lista Columns seleccionando las columnas de la lista Available Columns. Puede más personalizar adicionalmente la lista Columns utilizando las opciones siguientes:</p> <ul style="list-style-type: none"> • Move Up: Seleccione una columna y súbala en la lista de prioridad utilizando el botón de subida. • Move Down: Seleccione una columna y bájela en la lista de prioridad utilizando el botón de bajada. <p>Si el tipo de columna es numérico o de tiempo y hay una entrada en la lista Group By, la columna incluye una lista desplegable para que pueda elegir cómo desea agrupar la columna.</p>
Order By	<p>Utilizando la primera lista, especifique la columna por la que desea ordenar los resultados de búsqueda. A continuación, utilizando la segunda lista, especifique el orden que desea visualizar para los resultados de búsqueda: Descending o Ascending.</p>

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Connections**.
3. Realice una búsqueda.
4. Pulse **Save Criteria**.
5. Configure los valores de los parámetros siguientes:

Opción	Descripción
Nombre de búsqueda	Escriba un nombre que desee asignar a este criterio de búsqueda.
Asignar búsqueda a grupo(s)	Grupo que desea asignar a esta búsqueda guardada. Si no selecciona un grupo, esta búsqueda guardada se asigna al grupo Otros de forma predeterminada.
Opciones de intervalo tiempo	Elija una de las opciones siguientes: <ul style="list-style-type: none"> Recent: Utilizando la lista desplegable, especifique el rango de tiempo que desea filtrar. Specific Interval: Utilizando el calendario, especifique el rango de fecha y hora que desea filtrar.
Include in my Quick Searches	Marque este recuadro de selección si desea incluir esta búsqueda en los elementos de búsqueda rápida, que está disponible en la lista desplegable Search .
Include in my Dashboard	Marque este recuadro de selección si desea incluir los datos de la búsqueda guardada en el panel de control. Este parámetro sólo se visualiza si se agrupa la búsqueda.
Set as Default	Marque este recuadro de selección si desea establecer esta búsqueda como búsqueda predeterminada.
Compartir con todos	Marque este recuadro de selección si desea compartir estos requisitos de búsqueda con todos los demás usuarios de IBM Security QRadar Risk Manager.

6. Pulse **OK**.

Realización de una sub-búsqueda

Cada vez que se realiza una búsqueda, se consultan en toda la base de datos las conexiones que coinciden con los criterios. Este proceso puede tardar un periodo prolongado de tiempo, según el tamaño de la base de datos.

Acerca de esta tarea

Una sub-búsqueda le permite buscar en un conjunto de resultados de búsqueda completados. Puede refinar los resultados de búsqueda sin buscar de nuevo en la base de datos. Una sub-búsqueda no está disponible para búsquedas agrupados o búsquedas en curso.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Connections**.
3. Realice una búsqueda. Se visualizan los resultados de búsqueda. Las búsquedas adicionales utilizan el conjunto de datos de la búsqueda anterior cuando se realizan sub-búsquedas.
4. Para añadir un filtro, realice los pasos siguientes:

- a. Pulse **Add Filter**.
- b. Utilizando la primera lista, seleccione un atributo en el que desea buscar.
- c. Utilizando la segunda lista, seleccione el modificador que desea utilizar para la búsqueda. La lista de modificadores que se visualizan depende del atributo seleccionado en la primera lista.
- d. En el campo de texto, escriba información específica relacionada con la búsqueda.
- e. Pulse **Add Filter**.

Nota: Si la búsqueda sigue en curso, se visualizan resultados parciales. El panel Original Filter indica el filtro en el que se ha basado la búsqueda original. El panel Current Filter indica el filtro aplicado a la sub-búsqueda.

Consejo: Puede borrar filtros de sub-búsqueda sin reiniciar la búsqueda original. Pulse el enlace Clear Filter junto al filtro que desea borrar. Si borra un filtro del panel Original Filter, se reinicia la búsqueda original.

5. Pulse **Guardar criterios** para guardar la sub-búsqueda.

Resultados

Si suprime la búsqueda original, puede acceder a la sub-búsqueda guardada. Si añade un filtro, la sub-búsqueda busca en la base de datos entera ya que la función de búsqueda ya no basa la búsqueda en un conjunto de datos buscado previamente.

Gestionar resultados de búsqueda

Puede realizar varias búsquedas de conexiones mientras navega a otras interfaces.

Acerca de esta tarea

Puede configurar la característica de búsqueda para que le envíe una notificación por correo electrónico cuando se complete una búsqueda. En cualquier momento mientras está en curso una búsqueda, puede ver los resultados parciales de una búsqueda en curso.

La barra de herramientas de resultados de búsqueda proporciona las opciones siguientes:

Parámetro	Descripción
New Search	Pulse New Search para crear una búsqueda nueva. Al pulsar este botón, se visualiza la ventana de búsqueda.
Save Results	Pulse Save Results para guardar resultados de búsqueda. Esta opción solo está habilitada cuando se ha seleccionado una fila en la lista de Manage Search Results.
Cancel	Pulse Cancel para cancelar las búsquedas que están en curso o están en cola para iniciarse.
Delete	Pulse Delete para suprimir un resultado de búsqueda.

Parámetro	Descripción
Notify	Seleccione la búsqueda o búsquedas para las que desea recibir la notificación y, a continuación, pulse Notify para habilitar la notificación de correo electrónico cuando la búsqueda se haya completado.
Ver	En la lista desplegable, especifique qué resultados de búsqueda desea listar en la ventana de resultados de búsqueda. Las opciones son: <ul style="list-style-type: none"> • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Connections**.
3. En el menú, seleccione **Search > Manage Search Results**.

Guardar resultados de búsqueda

Puede guardar los resultados de la búsqueda.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Connections**.
3. Realice una búsqueda de conexión o sub-búsqueda.
4. En la ventana Search Results, seleccione **Search > Manage Search Results** y seleccione un resultado de búsqueda.
5. Pulse **Save Results**.
6. Escriba un nombre para los resultados de búsqueda.
7. Pulse **OK**.

Cancelación de una búsqueda

Puede cancelar uno o más búsquedas.

Acerca de esta tarea

Si una búsqueda está en curso cuando se cancela, se mantienen los resultados acumulados hasta la cancelación de la búsqueda.

Procedimiento

1. En la ventana Gestionar resultados de búsqueda, seleccione el resultado de búsqueda en progreso o en cola que desea cancelar. Puede seleccionar varias búsquedas para cancelarlas.
2. Pulse **Cancelar búsqueda**.
3. Pulse **Sí**.

Supresión de una búsqueda

Puede suprimir una búsqueda.

Procedimiento

1. En la ventana Gestionar resultados de búsqueda, seleccione el resultado de búsqueda que desea suprimir.
2. Pulse **Suprimir**.
3. Pulse **Sí**.

Exportación de conexiones

Puede exportar conexiones en formato XML (Extensible Markup Language - Lenguaje de marcado extensible) o CSV (Comma Separated Values - Valores separados por coma).

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Connections**.
3. Si desea exportar la conexión en formato XML, seleccione **Actions > Export to XML**.
4. Si desea exportar la conexión en formato CSV, seleccione **Actions>Export to CSV**.
5. Si desea reanudar las actividades, pulse **Notify When Done**.

Capítulo 8. Correlación de origen de registro

Para supervisar la frecuencia de desencadenante de reglas de cortafuegos y habilitar las búsquedas de sucesos de topología, IBM Security QRadar Risk Manager identifica los orígenes de registro de QRadar.

Si se conocen las reglas de cortafuegos se puede mantener la eficiencia del cortafuegos y evitar riesgos de seguridad.

Se puede correlacionar un máximo de 255 dispositivos con un origen de registro en QRadar Risk Manager, los dispositivos pueden tener varios orígenes de registro.

Opciones de visualización de correlación de origen de registro

Si ha configurado el dispositivo de red como un origen de registro de QRadar, la página Configuration Monitor visualiza una de las entradas siguientes en la columna **Origen de registro**:

- **Auto-Mapped**: Si QRadar Risk Manager identifica y correlaciona el origen de registro con el dispositivo automáticamente.
- **Username**: Si un administrador añade o edita manualmente un origen de registro.
- **Blank**: Si QRadar Risk Manager no puede identificar un origen de registro para el dispositivo, la columna **Origen de registro** no muestra ningún valor. Puede crear manualmente una correlación de origen de registro.

Para obtener más información sobre cómo configurar los orígenes de registro, consulte la publicación *Guía del usuario de orígenes de registro de IBM Security QRadar*.

Creación o edición de una correlación de origen de registro

Si IBM Security QRadar Risk Manager no puede identificar un origen de registro en QRadar, puede configurar una correlación de origen de registro.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el panel de navegación, pulse **Configuration Monitor**.
3. Pulse el dispositivo sin una correlación de origen de registro.
4. En la barra de herramientas, pulse **Action > Log Source Mapping > Create/Edit Log Source Mapping**.
5. En la lista **Log Source Groups**, seleccione un grupo.
6. En la lista **Log Sources**, seleccione un origen de registro y pulse (>).
7. Pulse **OK**.

Capítulo 9. Investigación de las configuraciones de dispositivo de red

En IBM Security QRadar Risk Manager, puede gestionar la eficiencia de los dispositivos de red, investigar reglas de cortafuegos e identificar riesgos de seguridad creados por reglas de cortafuegos no válidas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el panel de navegación, pulse **Configuration Monitor**.
3. Para buscar los dispositivos de red, escriba una dirección IP o un nombre de host en el campo **Input IP Address or Host Name**.
4. Efectúe una doble pulsación en el dispositivo que desea investigar.

La columna **Event Count** de regla visualiza la frecuencia de desencadenante de regla de cortafuegos. Se visualiza una regla de recuento de suceso de cero por una de las razones siguientes:

- Una regla no se desencadena y puede causar un riesgo de seguridad. Puede investigar el dispositivo de cortafuegos y eliminar las reglas que no se desencadenan.
 - Una correlación de origen de registro de QRadar no se ha configurado.
5. Para buscar las reglas, en la barra de herramientas **Rules**, pulse **Search > New Search**.
Si se visualiza un icono en la columna **Status**, puede pasar el ratón sobre el icono de estado para visualizar más información.
 6. Para investigar las interfaces de dispositivo, en la barra de herramientas, pulse **Interfaces**.
 7. Para investigar las reglas de dispositivo de lista de control de acceso (ACL), en la barra de herramientas, pulse **ACLs**.

Cada lista de control de acceso define las interfaces a través de las que se están comunicando los dispositivos de la red. Cuando se cumplen las condiciones de una ACL, se desencadenan las reglas que están asociadas con una ACL. Cada regla se prueba para permitir o denegar la comunicación entre los dispositivos.

8. Para investigar las reglas de dispositivo de conversión de direcciones de red (NAT), en la barra de herramientas, pulse **NAT**.

La columna **Phase** especifica cuándo se debe desencadenar la regla NAT, por ejemplo, antes o después del direccionamiento.

9. Para investigar el historial o comparar las configuraciones de dispositivo, en la barra de herramientas, pulse **History**.

Puede ver las reglas de dispositivo en una vista de comparación normalizada o la configuración de dispositivo en bruto. La configuración de dispositivo normalizada es una comparación gráfica que muestra reglas añadidas, suprimidas o modificadas entre dispositivos. La configuración de dispositivo en bruto es una vista de texto sin formato o XML del archivo de dispositivo.

Búsqueda de dispositivos de regla

En IBM Security QRadar Risk Manager, puede buscar reglas que han cambiado en los dispositivos de la topología. También puede descubrir los cambios de regla que se producen entre las copias de seguridad de configuración de dispositivo.

Los resultados que se devuelven para una búsqueda de reglas se basan en la copia de seguridad de gestión de origen de configuración del dispositivo. Para asegurarse de que las búsquedas de reglas proporcionan información actualizada, puede planificar copias de seguridad de dispositivo en la página de actualización de política de cortafuegos.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el panel de navegación, pulse **Configuration Monitor**.
3. Efectúe una doble pulsación en un dispositivo en la página Configuration Monitor.
4. En la barra de herramientas de panel Rules, pulse **Search > New Search**.
5. En el área **Search Criteria**, pulse un rango de tiempo.
6. Para buscar las reglas de dispositivo, elija entre las opciones siguientes:
 - Para buscar reglas **Shadowed**, **Deleted** u **Other**, pulse una opción de estado. De forma predeterminada todas las opciones de estado están habilitadas. Para buscar solo reglas de duplicación, borre las opciones **Deleted** y **Other**.
 - Para buscar una lista de control de acceso (ACL), escriba en el campo **List**.
 - Para buscar el número de pedido de la entrada de regla, escriba un valor numérico en el campo **Entry**.
 - Para buscar un origen o destino, escriba una dirección IP, una dirección de CIDR, un nombre de host o una referencia de grupo de objetos.
 - Para buscar puertos o referencias de grupo de objetos, escriba en el campo **Service**.
El servicio puede incluir rangos de puerto, como 100-200, o expresiones de puerto, como 80(TCP). Si el puerto se deniega, la información de puerto también incluye un signo de exclamación y puede estar entre paréntesis, por ejemplo !(100-200) o !80(TCP).
 - Para buscar información de regla de vulnerabilidad tal como está definida por el dispositivo IPS, escriba en el campo **Signature**.
 - Para buscar aplicaciones por adaptador, pulse **Select Applications** y, a continuación, escriba un nombre de adaptador o aplicación.
7. Pulse **Search**.

Comparación de la configuración de los dispositivos de red

En IBM Security QRadar Risk Manager, las configuraciones de dispositivo se pueden comparar entre sí mediante la comparación de varias copias de seguridad en un solo dispositivo o mediante la comparación de una copia de seguridad de dispositivo de red con otra.

Los tipos de configuración comunes pueden incluir los elementos siguientes:

- **Standard Element Document:** Los archivos SED (Standard Element Document - Documento de elemento estándar) son archivos de datos XML que contienen información sobre el dispositivo de red. Los archivos SED (documento de elemento estándar) individuales se ven en el formato XML en bruto. Si se

compara un archivo SED (documento de elemento estándar) con otro archivo SED (documento de elemento estándar), la vista se normaliza para visualizar las diferencias de regla.

- **Config:** Determinados dispositivos de red proporcionan archivos de configuración, en función del fabricante de dispositivo. Puede ver un archivo de configuración efectuando una doble pulsación en el mismo.

En función de la información que el adaptador recopile para el dispositivo, es posible que se visualicen otros tipos diversos de configuración. Estos archivos se visualizan en la vista de texto sin formato se efectúa una doble pulsación en ellos.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, pulse **Configuration Monitor**.
3. Efectúe una doble pulsación en cualquier dispositivo para ver la información de configuración detallada.
4. Pulse **History** para ver el historial de este dispositivo.
5. Para comparar dos configuraciones en un dispositivo único:
 - a. Seleccione una configuración primaria.
 - b. Pulse la tecla Control y seleccione una segunda configuración para la comparación.
 - c. En el panel History , pulse **Compare Selected**.

Si los archivos de comparación son documentos de elementos estándares (SED), la ventana Normalized Device Configuration Comparison muestra diferencias de regla entre las copias de seguridad.

Al comparar configuraciones normalizada, el color del texto muestra las actualizaciones de dispositivo siguientes:

- Un esquema de puntos verde muestra una regla o configuración que se ha añadido al dispositivo.
 - Un esquema de puntos rojo muestra una regla o configuración que se ha suprimido del dispositivo.
 - Un esquema sólido amarillo muestra una regla o configuración que se ha modificado en el dispositivo.
- d. Para ver las diferencias de configuración en bruto, pulse **View Raw Comparison**.

Si la comparación es un archivo de configuración u otro tipo de copia de seguridad, se visualizas la comparación en bruto.
6. Para comparar dos configuraciones en distintos dispositivos:
 - a. Seleccione una configuración primaria en un dispositivo.
 - b. Pulse **Mark for Comparison**.
 - c. En el menú de navegación, seleccione **All Devices** para volver a la lista de dispositivos.
 - d. Efectúe una doble pulsación en el dispositivo para comparar y pulse **History**.
 - e. Seleccione una configuración que desee comparar con la configuración marcada.
 - f. Pulse **Compare with Marked**.
 - g. Para ver las diferencias de configuración en bruto, pulse **View Raw Comparison**.

Capítulo 10. Filtrado de reglas de dispositivo por usuario o grupo

En QRadar Risk Manager, puede ver y filtrar las reglas de dispositivo por usuario o grupo.

Acerca de esta tarea

Busque por interacción de regla de usuario o grupo y obtenga una idea de cómo interacciona en la red el usuario o el grupo típico. Conocer las interacciones de regla de los usuarios de la red es útil para descubrir comportamientos erráticos y ayuda a formular políticas de regla eficientes en la red.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, pulse **Configuration Monitor**.
3. En la tabla **Lista de dispositivos**, efectúe una doble pulsación sobre la fila de la tabla correspondiente a su dispositivo.

En la columna **Usuario(s)/Grupo(s)** de la tabla de reglas, puede ver los usuarios y los grupos.

4. En el panel Reglas, pulse **Buscar > Nueva búsqueda**.
5. Teclee el nombre de usuario o de grupo en el campo **Usuario o grupo**.
6. Pulse **Buscar**.

Si la serie de búsqueda coincide con cualquier parte de un nombre de usuario o de grupo, se visualizan las reglas enlazadas con el nombre de usuario o de grupo.

Utilice la información de regla para establecer pruebas de referencia o perfiles para la interacción de regla de usuario que se pueden utilizar para optimizar políticas de regla en su entorno.

Capítulo 11. Gestión de informes de IBM Security QRadar Risk Manager

Puede crear, editar, distribuir y gestionar informes para los dispositivos de red. Normalmente se necesitan informes detallados sobre las reglas de cortafuegos y las conexiones entre dispositivos para satisfacer diversos estándares normativos como, por ejemplo, la conformidad PCI.

Las siguientes opciones de informe son específicas de QRadar Risk Manager:

Tabla 25. Opciones de informe de QRadar Risk Manager

Opción de informe	Descripción
Conexiones	Los diagramas de conexión para los dispositivos de red que se han producido durante el intervalo de tiempo especificado.
Reglas de dispositivo	Las reglas configuradas en el dispositivo de red durante el intervalo de tiempo especificado. Puede ver los tipos de reglas siguientes para uno o varios dispositivos de red utilizando esta opción de informe: <ul style="list-style-type: none">• Reglas de aceptación más utilizadas• Reglas de denegación más utilizadas• Reglas de aceptación menos utilizadas• Reglas de denegación menos utilizadas• Reglas enmascaradas• Reglas de objeto no utilizado
Objetos no utilizados de dispositivo	Produce una tabla con el nombre, la fecha/hora de configuración y una definición para los grupos de referencia de objeto que no se estén utilizando en el dispositivo. Un grupo de referencia de objeto es un término genérico utilizado para describir una colección de direcciones IP, direcciones CIDR, nombres de host, puertos u otros parámetros de dispositivo que se agrupan y se asignan a reglas en el dispositivo.

Generación manual de un informe

Los informes se pueden iniciar manualmente. Si inicia varios informes manualmente, los informes se añaden a una cola y se etiquetan con la posición de cola.

Acerca de esta tarea

Al generar manualmente un informe, no se restablece la planificación de informe existente. Por ejemplo, si genera un informe semanal para las denegaciones de cortafuegos más activas y, a continuación, genera manualmente el informe, el informe semanal se sigue generando en la planificación configurada inicialmente.

Cuando 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 generación. 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)):** Se ha planificado que el informe se ejecute. El mensaje es un temporizador de cuenta atrás que especifica la siguiente vez que se ejecutará el informe.

Procedimiento

1. Pulse la pestaña **Informes**.
2. Seleccione el informe que desea generar.
3. Pulse **Ejecutar informe**.
4. Opcional. Pulse **Renovar** para renovar la vista, incluida la información en la columna **Próxima hora de ejecución**.

Qué hacer a continuación

Después de que se genere el informe, puede ver el informe generado en la columna **Informes generados**.

Utilizar el asistente de informes

Puede utilizar el asistente de informes para crear un informe nuevo. 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 de posición y ubicación para el contenido en el informe
- **Contenido:** Define los datos de informe que IBM Security QRadar Risk Manager incluye en el gráfico para el contenedor

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 visualiza un gran número de objetos. Cada gráfico incluye una descripción y una lista de redes de la cual se deriva el contenido; elija un contenedor suficientemente grande para contener los datos.

Debe transcurrir el tiempo planificado para informes que se generan semanal o mensualmente 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 7 días para crear los datos. Esta búsqueda devuelve resultados una vez transcurridos 7 días.

Creación de un informe

Puede crear informes durante un intervalo específico y puede elegir un tipo de gráfico.

Acerca de esta tarea

Un informe puede constar de varios elementos de datos y puede representar datos de red y de seguridad en una gran variedad de estilos, tales como tablas, gráficos de línea, gráficos circulares y gráficos de barras.

Puede especificar la consola de informes o el correo electrónico para las opciones de distribución de informes. La tabla siguiente describe los parámetros de estas opciones de distribución.

Tabla 26. Opciones de distribución de informes generados

Opción	Descripción
Report Console	Marque este recuadro de selección para enviar el informe generado a la pestaña Reports . Este es el canal de distribución predeterminado.
Select the users that should be able to view the generated report.	<p>Esta opción solo se visualiza después de seleccionar el recuadro de selección Report Console.</p> <p>En la lista de usuarios, seleccione los usuarios de IBM Security QRadar Risk Manager a los que desea otorgar permiso para ver los informes generados.</p> <p>Debe tener los permisos de red apropiados para compartir el informe generado con otros usuarios. Para obtener más información sobre los permisos, consulte la publicación <i>IBM Security QRadar SIEM Administration Guide</i>.</p>
Select all users	<p>Esta opción solo se visualiza después de seleccionar el recuadro de selección Report Console.</p> <p>Marque este recuadro de selección si desea otorgar permiso a todos los usuarios de QRadar Risk Manager para ver los informes generados.</p> <p>Debe tener los permisos de red apropiados para compartir el informe generado con otros usuarios. Para obtener más información sobre los permisos, consulte la publicación <i>IBM Security QRadar SIEM Administration Guide</i>.</p>
Email	Marque este recuadro de selección si desea distribuir el informe generado utilizando el correo electrónico.

Tabla 26. Opciones de distribución de informes generados (continuación)

Opción	Descripción
Enter the report distribution email address(es)	<p>Esta opción sólo se visualiza después de seleccionar el recuadro de selección Email.</p> <p>Escriba la dirección de correo electrónico para cada destinatario de informe generado; separe una lista de direcciones de correo electrónico con comas. El número máximo de caracteres para este parámetro es de 255.</p> <p>Los destinatarios de correo electrónico reciben este correo electrónico de no_reply_reports@qradar.</p>
Include Report as attachment (non-HTML only)	<p>Esta opción sólo se visualiza después de seleccionar el recuadro de selección Email.</p> <p>Marque este recuadro de selección para enviar el informe generado como un archivo adjunto.</p>
Include link to Report Console	<p>Esta opción sólo se visualiza después de seleccionar el recuadro de selección Email.</p> <p>Marque este recuadro de selección para incluir un enlace a la Consola de informes en el correo electrónico.</p>

Procedimiento

1. Pulse la pestaña **Reports**.
2. En la lista **Actions**, seleccione **Create**.
3. Pulse **Next** para pasar a la página siguiente del asistente de informes.
4. Seleccione la frecuencia de la planificación de informes.
5. En el panel Allow this report to generate manually, seleccione **Yes** para habilitar o **No** para inhabilitar la generación manual de este informe. Esta opción no está disponible para informes generados manualmente.
6. Pulse **Next**.
7. Elija un diseño del informe y, a continuación, pulse **Next**.
8. Entre un título de informe. El título puede tener hasta 100 caracteres de longitud. No utilice caracteres especiales.
9. Elija un logotipo. El logotipo de QRadar es el logotipo predeterminado. Para obtener más información sobre la creación de marcas de informes, consulte la publicación *IBM Security QRadar SIEM Administration Guide*.
10. En la lista **Chart Type**, seleccione uno de los informes específicos de QRadar Risk Manager.
11. Configure los datos de informe para el gráfico.
12. Pulse **Save Container Details**.
13. Pulse **Next**.
14. Seleccione formatos de informe. Puede seleccionar varias opciones.

Nota: Los informes de reglas de dispositivo y reglas de objetos no utilizados sólo soportan los formatos de informe PDF, HTML y RTF.

15. Pulse **Next**.
16. Seleccione los canales de distribución que desea para el informe.
17. Pulse **Next**.
18. Escriba una descripción para este informe. La descripción se visualiza en la página de resumen de informe y en el correo electrónico de distribución de informe generado.
19. Seleccione los grupos a los que desea asignar este informe. Para obtener más información sobre grupos, consulte la gestión de informes en la publicación *IBM Security QRadar SIEM Administration Guide*.
20. Opcional. Seleccione yes para ejecutar este informe cuando se haya completado la configuración de asistente. Pulse **Next** para ver el resumen de informe. Puede seleccionar las pestañas disponibles en el informe de resumen para obtener una vista previa de las selecciones de informe.
21. Pulse **Finish**.

Resultados

El informe se genera inmediatamente. Si ha borrado el recuadro de selección **>Would you like to run the report now** en la página final del asistente, el informe se guarda y se genera como estaba previsto.

El título de informe es el título predeterminado para el informe generado. Si reconfigura un informe para entrar un 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

Puede editar un informe para ajustar una planificación de informe, el diseño, la configuración, el título, el formato y método de entrega. Puede editar informes existentes o editar un informe predeterminado.

Procedimiento

1. Pulse la pestaña **Reports**.
2. Seleccione el informe que desea editar.
3. En la lista **Actions**, seleccione **Edit**.
4. Seleccione la frecuencia para la nueva planificación de informes.
5. En el panel Allow this report to generate manually, seleccione una de las opciones siguientes:
 - **Yes:** Habilita la generación manual de este informe.
 - **No:** Inhabilita la generación manual de este informe.
6. Pulse **Next** para pasar a la página siguiente del asistente de informes.
7. Configure el diseño del informe:
 - a. En la lista **Orientation**, seleccione la orientación de la página.
 - b. Seleccione una opción de diseño para el informe de IBM Security QRadar Risk Manager.
 - c. Pulse **Next**.
8. Especifique los valores de los parámetros siguientes:

- **Report Title:** Escriba un título de informe. El título puede tener hasta 100 caracteres de longitud. No utilice caracteres especiales.
 - **Logo:** En la lista, seleccione un logotipo. El logotipo de QRadar es el logotipo predeterminado. Para obtener más información sobre la creación de marcas de informes, consulte la publicación *IBM Security QRadar SIEM Administration Guide*.
9. Configure el contenedor para los datos de informe:
 - a. Pulse **Define**.
 - b. Configure los datos de informe para el gráfico.
 - c. Pulse **Save Container Details**.
 - d. Si es necesario, repita estos pasos para editar contenedores adicionales.
 - e. Pulse **Next** para ir a la página siguiente del asistente de informes.
 10. Pulse **Next** para ir al paso siguiente del asistente de informes.
 11. Marque los recuadros de selección para los formatos de informe. Puede seleccionar más de una opción.

Nota: Los informes específicos de QRadar Risk Manager, por ejemplo informes de Regla de dispositivo y Objeto no utilizado de dispositivo solo soportan los formatos PDF, HTML y RTF.

12. Pulse **Next** para ir a la página siguiente del asistente de informes.
13. Seleccione los canales de distribución para el informe.
14. Pulse **Next** para ir al paso final del asistente de informes.
15. Escriba una descripción para este informe. La descripción se visualiza en la página Report Summary y en el correo electrónico de distribución de informe generado.
16. Seleccione los grupos a los que desea asignar este informe. Para obtener más información sobre grupos, consulte la gestión de informes en la publicación *IBM Security QRadar SIEM Administration Guide*.
17. Opcional. Seleccione yes para ejecutar este informe cuando se haya completado la configuración de asistente.
18. Pulse **Next** para ver el resumen de informe. Se visualiza la página Report Summary, proporcionando los detalles del informe. Puede seleccionar las pestañas disponibles en el informe de resumen para obtener una vista previa de las selecciones de informe.
19. Pulse **Finish**.

Duplicación de un informe

Puede duplicar cualquier informe.

Procedimiento

1. Pulse la pestaña **Informes**.
2. Seleccione el informe que desea duplicar.
3. En la lista **Acciones**, pulse **Duplicar**.
4. Escriba un nombre nuevo, sin espacios, para el informe.

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.

Antes de empezar

Debe tener privilegios administrativos para compartir informes. Además, para que un usuario nueva vea informes y acceda a ellos, un usuario administrativo debe compartir todos los informes necesarios con el nuevo usuario

Acerca de esta tarea

Las actualizaciones que el usuario realiza en un informe compartido no afecta a la versión original del informe.

Procedimiento

1. Pulse la pestaña **Reports**.
2. Seleccione los informes que desea compartir.
3. En la lista **Actions**, pulse **Share**.
4. En la lista de usuarios, seleccione los usuarios con los que desea compartir este informe.

Si no hay usuarios con el acceso adecuado disponibles, se visualiza un mensaje.

5. Paso 5 Pulse **Share**.

Para obtener más información sobre los informes, consulte la publicación *IBM Security QRadar SIEM Users Guide*.

Configuración de gráficos

El tipo de gráfico determina los datos configurados y visualizados en el gráfico. Puede crear varios gráficos para datos específicos recopilados por los dispositivos en IBM Security QRadar Risk Manager.

Los siguientes tipos de gráfico son específicos de QRadar Risk Manager:

- Conexión
- Reglas de dispositivo
- Objetos no utilizados de dispositivo

Gráficos de conexiones

Puede utilizar el gráfico de Conexiones para ver información de conexión de red. Puede basar los gráficos en los datos obtenidos en las búsquedas de conexión guardadas de la pestaña Risks.

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 conexión.

La tabla siguiente proporciona información de configuración para el contenedor de gráfico de Conexiones.

Tabla 27. Parámetros de gráfico de conexiones

Parámetro	Descripción
Detalles de contenedor - Conexiones	
Título de gráfico	Escriba un título de gráfico con un máximo de 100 caracteres.

Tabla 27. Parámetros de gráfico de conexiones (continuación)

Parámetro	Descripción
Subtítulo de gráfico	Quite la marca de la casilla de verificación para cambiar el subtítulo creado automáticamente. Escriba un título con un máximo de 100 caracteres.
Tipo de gráfico	<p>En la lista, seleccione el tipo de gráfico a visualizar en el informe generado. Las opciones incluyen:</p> <ul style="list-style-type: none"> • Barra: Muestra los datos en un gráfico de barras. Este es el tipo de gráfico predeterminado. Este tipo de gráfico requiere que la búsqueda guardada sea una búsqueda agrupada. • Línea: Muestra los datos en un gráfico de líneas. • Circular: Muestra los datos en un gráfico circular. Este tipo de gráfico requiere que la búsqueda guardada sea una búsqueda agrupada. • Barra apilada: Muestra los datos en un gráfico de barras apiladas. • Línea apilada: Muestra los datos en un gráfico de líneas apiladas. • Tabla: Muestra los datos en formato de tabla. La opción Tabla sólo está disponible para el contenedor de ancho de página completa.
Gráfico	En la lista, seleccione el número de conexiones que se deben visualizar en el informe generado.

Tabla 27. Parámetros de gráfico de conexiones (continuación)

Parámetro	Descripción
Planificación manual	<p>El panel Planificación manual solo se visualiza si ha seleccionado la opción de planificación Manualmente en el Asistente de informes.</p> <p>Para crear una planificación manual:</p> <ol style="list-style-type: none"> 1. En el cuadro de lista Desde, escriba la fecha de inicio que desea para el informe o seleccione la fecha utilizando el icono Calendario. El valor predeterminado es la fecha actual. 2. En los cuadros de lista, seleccione la hora de inicio que desea para el informe. La hora está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m. 3. En la lista Hasta, escriba la fecha de finalización que desea para el informe o seleccione la fecha utilizando el icono Calendario. El valor predeterminado es la fecha actual. 4. En las listas, seleccione la hora de finalización que desea para el informe. La hora está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.
Planificación para cada hora	<p>El panel Planificación para cada hora sólo se visualiza si ha seleccionado la opción de planificación Cada hora en el Asistente de informes.</p> <p>La Planificación para cada hora crea automáticamente un gráfico de todos los datos de la hora anterior.</p>
Planificación diaria	<p>El panel Planificación diaria sólo se visualiza si ha seleccionado la opción de planificación Diariamente en el Asistente de informes.</p> <p>Elija una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Todos los datos del día anterior (24 horas) • Datos de día anterior de: En las listas, seleccione el periodo de tiempo que desea para el informe generado. La hora está disponible en incrementos de media hora. El valor predeterminado es 1:00 a.m.

Tabla 27. Parámetros de gráfico de conexiones (continuación)

Parámetro	Descripción
Planificación semanal	<p>El panel Planificación semanal solo se visualiza si ha seleccionado la opción de planificación Semanalmente en el Asistente de informes.</p> <p>Elija una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Todos los datos de semana anterior • Todos los datos de semana anterior de: En las listas, seleccione el periodo de tiempo que desea para el informe generado. El valor predeterminado es Domingo.
Planificación mensual	<p>El panel Planificación mensual solo se visualiza si ha seleccionado la opción de planificación Mensualmente en el Asistente de informes.</p> <p>Elija una de las opciones siguientes:</p> <ul style="list-style-type: none"> • Todos los datos de mes anterior • Datos de mes anterior del: En las listas, seleccione el periodo de tiempo que desea para el informe generado. El valor predeterminado es del 1 al 31.
Contenido del gráfico	
Grupo	En la lista, seleccione un grupo de búsqueda guardada para visualizar las búsquedas guardadas que pertenecen a ese grupo en la lista Búsquedas guardadas disponibles .
Escriba la búsqueda guardada o seleccione en la lista	Para refinar la lista Búsquedas guardadas disponibles , escriba el nombre de la búsqueda que desea localizar en el campo Escriba la búsqueda guardada o seleccione en la lista . También puede escribir una palabra clave para visualizar una lista de búsquedas que incluyan dicha palabra clave. Por ejemplo, escriba DMZ para visualizar una lista de todas las búsquedas que incluyan DMZ en el nombre de búsqueda.
Búsquedas guardadas disponibles	Proporciona una lista de búsquedas guardadas disponibles. De forma predeterminada, se visualizan todas las búsquedas guardadas disponibles. Sin embargo puede filtrar la lista seleccionando un grupo en la lista Grupo o escribiendo el nombre de una búsqueda guardada conocida en el campo Escriba la búsqueda guardada o seleccione en la lista .
Crear nueva búsqueda de conexiones	Pulse Crear nueva búsqueda de conexiones para crear una nueva búsqueda.

Gráficos de reglas de dispositivo

Puede utilizar el gráfico Reglas de dispositivo para ver reglas de cortafuegos y el recuento de sucesos de reglas de cortafuegos desencadenadas en la red.

Los informes de regla de dispositivo le permiten crear un informe para las siguientes reglas de cortafuegos:

- Reglas de dispositivo de aceptación más activas
- Reglas de dispositivo de denegación más activas
- Reglas de dispositivo de aceptación menos activas
- Reglas de dispositivo de denegación menos activas
- Reglas de dispositivo no utilizadas
- Reglas de dispositivo enmascaradas

Los informes que genera le permiten conocer qué reglas se aceptan, deniegan, no se utilizan o se desencadenan en un único dispositivo, un adaptador específico o varios dispositivos. Los informes permiten que IBM Security QRadar Risk Manager automatice la creación de informes sobre el estado de las reglas de dispositivo y visualice los informes en IBM Security QRadar SIEM Console.

Esta funcionalidad le ayuda a identificar cómo se utilizan las reglas en los dispositivos de red.

Para crear un contenedor de gráfico de reglas de dispositivo, configure valores para los parámetros siguientes:

Tabla 28. Parámetros de gráfico de reglas de dispositivo

Parámetro	Descripción
Detalles de contenedor - Reglas de dispositivo	
Limitar reglas a principales	<p>En la lista, seleccione el número de reglas que se deben visualizar en el informe generado.</p> <p>Por ejemplo, si limita el informe a las 10 reglas principales y, a continuación, crea un informe para las reglas de aceptación más utilizadas en todos los dispositivos, el informe devuelve 10 resultados. Los resultados contienen una lista de las 10 reglas de aceptación más utilizadas basándose en el recuento de sucesos en todos los dispositivos que están visibles en QRadar Risk Manager.</p>

Tabla 28. Parámetros de gráfico de reglas de dispositivo (continuación)

Parámetro	Descripción
Tipo	<p>Seleccione el tipo de reglas de dispositivo a visualizar en el informe. Las opciones incluyen:</p> <ul style="list-style-type: none"> • Reglas de aceptación más utilizadas: Visualiza las reglas de aceptación más utilizadas por recuento de sucesos para un dispositivo único o un grupo de dispositivos. Este informe lista las reglas con recuentos de sucesos aceptados más altos, en orden descendente, para el periodo de tiempo especificado en el informe. • Reglas de denegación más utilizadas - Visualiza las reglas de denegación más utilizadas por recuento de sucesos para un dispositivo único o un grupo de dispositivos. Este informe lista las reglas con los recuentos de sucesos de denegación más altos, en orden descendente, para el periodo de tiempo especificado en el informe. • Reglas no utilizadas: Visualiza las reglas para un dispositivo único o un grupo de dispositivos que no se utilizan. Las reglas no utilizadas tienen cero recuentos de sucesos para el periodo de tiempo especificado para el informe. • Reglas de aceptación menos utilizadas: Visualiza las reglas de aceptación menos utilizadas para un dispositivo único o un grupo de dispositivos. Este informe lista las reglas con los recuentos de sucesos de aceptación más bajos, en orden ascendente, para el periodo de tiempo especificado en el informe. • Reglas de denegación menos utilizadas: Visualiza las reglas de denegación menos utilizadas para un dispositivo único o un grupo de dispositivos. Este informe lista las reglas con los recuentos de sucesos denegados más bajos, en orden ascendente, para el periodo de tiempo especificado en el informe. • Reglas enmascaradas: Visualiza las reglas para un dispositivo único que no se puede desencadenar nunca porque la regla está bloqueada por una regla siguiente. Los resultados muestran una tabla de la regla creando la máscara y las reglas que nunca se pueden desencadenar en el dispositivo porque están enmascaradas por una regla siguiente en el dispositivo. <p>Nota: Los informes de reglas enmascaradas sólo se pueden ejecutar en un dispositivo único. Estas reglas tienen cero recuentos de sucesos para el periodo de tiempo especificado para el informe y se identifican con un icono en la columna de Estado.</p>

Tabla 28. Parámetros de gráfico de reglas de dispositivo (continuación)

Parámetro	Descripción
Rango de fechas/horas	<p>Seleccione el periodo de tiempo para el informe. Las opciones incluyen:</p> <ul style="list-style-type: none"> • Configuración actual: Los resultados del informe Reglas de dispositivo se basan en las reglas que existen en la configuración de dispositivo actual. Este informe muestra las reglas y los recuentos de sucesos para la configuración de dispositivo existente. <p>La configuración actual para un dispositivo se basa en la última vez que la configuración de origen de gestión ha realizado la copia de seguridad del dispositivo de red.</p> <ul style="list-style-type: none"> • Intervalo: Los resultados del informe Reglas de dispositivo se basan en las reglas que existían durante el periodo de tiempo del intervalo. Este informe muestra las reglas y los recuentos de sucesos para el intervalo especificado desde la última hora hasta 30 días. • Rango específico: Los resultados del informe Reglas de dispositivo se basan en las reglas que existían entre la hora de inicio y la hora de finalización del rango de tiempo. Este informe muestra las reglas y los recuentos de sucesos para el periodo de tiempo especificado.
Huso horario	<p>Seleccione el huso horario que desea utilizar como base para el informe. El huso horario predeterminado se basa en la configuración de QRadar SIEM Console.</p> <p>Cuando se configura el parámetro de huso horario para el informe, tenga en cuenta la ubicación de los dispositivos asociados con los datos notificados. Si el informe utiliza datos que abarcan varios husos horarios, los datos utilizados para el informe se basan en el rango de tiempo específico del huso horario.</p> <p>Por ejemplo, si QRadar SIEM Console se ha configurado para la hora del este de EE. UU. (EST) y planifica un informe diario entre la 1pm y las 3pm y establece el huso horario como la hora de la zona central de EE. UU. (CST), los resultados del informe contienen información de las 2pm y las 4pm EST.</p>

Tabla 28. Parámetros de gráfico de reglas de dispositivo (continuación)

Parámetro	Descripción
Selección de datos elegidos como destino	<p>La Selección de datos elegidos como destino se utiliza para filtrar el rango de fecha/hora a un valor específico. Mediante el uso de las opciones de Selección de datos elegidos como destino, puede crear un informe para ver las reglas de dispositivo durante un periodo de tiempo definido personalizado, con la opción de incluir solo datos de las horas y los días que seleccione.</p> <p>Por ejemplo, puede planificar que un informe se ejecute desde 1 de octubre hasta el 31 de octubre y ver las reglas más activas, menos activas o no utilizadas y los recuentos de reglas que se producen durante el horario comercial, por ejemplo de lunes a viernes, de las 8 AM a las 9 PM.</p> <p>Nota: Los detalles de filtro solo se visualizan cuando se selecciona la casilla de verificación Selección de datos elegidos como destino en el Asistente de informes.</p>
Formato	<p>Seleccione el formato para el informe de reglas de dispositivo. Las opciones incluyen:</p> <ul style="list-style-type: none"> • Un informe agregado para dispositivos especificados: Este formato de informe agrega los datos de informe en varios dispositivos. <p>Por ejemplo, si crea un informe para mostrar las diez principales reglas más denegadas, un informe agregado visualiza las diez principales reglas más denegadas en todos los dispositivos que ha seleccionado para el informe. Este informe devuelve 10 resultados en total para el informe.</p> <ul style="list-style-type: none"> • Un informe por dispositivo: Este formato de informe visualiza los datos de informe para un dispositivo. <p>Por ejemplo, si crea un informe para mostrar las diez principales reglas más denegadas, un informe agregado muestra las diez principales reglas más denegadas para cada dispositivo que ha seleccionado para el informe. Este informe devuelve los 10 principales resultados para cada dispositivo seleccionado para el informe. Si ha seleccionado 5 dispositivos, el informe devuelve 50 resultados.</p> <p>Nota: Los informes de reglas enmascaradas solo son capaces de visualizar un informe por dispositivo.</p>

Tabla 28. Parámetros de gráfico de reglas de dispositivo (continuación)

Parámetro	Descripción
Devices	<p>Seleccione los dispositivos incluidos en el informe. Las opciones incluyen:</p> <ul style="list-style-type: none"> • All Devices: Seleccione esta opción para incluir todos los dispositivos de QRadar Risk Manager en el informe. • Adapter: En la lista, seleccione un tipo de adaptador a incluir en el informe. Solo se puede seleccionar un tipo de adaptador en la lista para un informe. • Specific Devices: Seleccione esta opción para incluir sólo dispositivos específicos en el informe. La ventana de selección de dispositivo le permite seleccionar y añadir dispositivos al informe. <p>Para añadir dispositivos individuales al informe:</p> <ol style="list-style-type: none"> 1. Pulse Browse para visualizar la ventana de selección de dispositivo. 2. Seleccione los dispositivos y pulse Add Selected. <p>Para añadir todos los dispositivos al informe:</p> <ol style="list-style-type: none"> 1. Pulse Browse para visualizar la ventana de selección de dispositivo. 2. Pulse Add All. <p>Para buscar dispositivos a incluir en el informe:</p> <ol style="list-style-type: none"> 1. Pulse Browse para visualizar la ventana de selección de dispositivo. 2. Pulse Search. 3. Seleccione las opciones de búsqueda para filtrar la lista de dispositivos completa por configuración obtenida, dirección IP o CIDR, nombre de host, tipo, adaptador, proveedor o modelo. 4. Pulse Search. 5. Seleccione los dispositivos y pulse Add Selected.

Gráficos de objetos no utilizados de dispositivo

Un informe de Objetos no utilizados de dispositivo visualiza grupos de referencia de objeto que el dispositivo de red no está utilizando.

Este informe visualiza referencias a objetos, por ejemplo una colección de direcciones IP, rangos de direcciones CIDR o nombres de host no utilizados por el dispositivo de red.

Cuando se configura un contenedor de objetos no utilizados de dispositivo, se configuran valores para los parámetros siguientes:

Tabla 29. Parámetros de informe de objetos no utilizados de dispositivo

Parámetro	Descripción
Detalles de contenedor - Objetos no utilizados de dispositivo	
Limitar objetos a principales	En la lista, seleccione el número de reglas que se deben visualizar en el informe generado.
Devices	<p>Seleccione los dispositivos incluidos en el informe. Las opciones incluyen:</p> <ul style="list-style-type: none"> • All Devices: Seleccione esta opción para incluir todos los dispositivos de IBM Security QRadar Risk Manager en el informe. • Adapter: En la lista, seleccione un tipo de adaptador a incluir en el informe. Solo se puede seleccionar un tipo de adaptador en la lista para un informe. • Specific Devices: Seleccione esta opción para incluir sólo dispositivos específicos en el informe. La ventana de selección de dispositivo le permite seleccionar y añadir dispositivos al informe. <p>Para añadir dispositivos individuales al informe:</p> <ol style="list-style-type: none"> 1. Pulse Browse para visualizar la ventana de selección de dispositivo. 2. Seleccione los dispositivos y pulse Add Selected. <p>Para añadir todos los dispositivos al informe:</p> <ol style="list-style-type: none"> 1. Pulse Browse para visualizar la ventana de selección de dispositivo. 2. Pulse Add all. <p>Para buscar dispositivos a incluir en el informe:</p> <ol style="list-style-type: none"> 1. Pulse Browse para visualizar la ventana de selección de dispositivo. 2. Pulse Search. 3. Seleccione las opciones de búsqueda para filtrar la lista de dispositivos completa por configuración obtenida, dirección IP o CIDR, nombre de host, tipo, adaptador, proveedor o modelo. 4. Pulse Search. 5. Seleccione los dispositivos y pulse Add Selected.

Capítulo 12. Gestión de políticas

Utilice las páginas de gestión de políticas de IBM Security QRadar Risk Manager para ver los detalles sobre el cumplimiento de las políticas y los cambios de riesgo de política para los activos, las políticas y las comprobaciones de política.

Las páginas de gestión de políticas de QRadar Risk Manager muestran datos de la última política ejecutada. Puede filtrar los datos por activo, por política o por comprobación de política.

Casos de uso de la gestión de políticas

Utilice las páginas de gestión de políticas con elementos del panel de control **Riesgo** para obtener más información acerca de los activos y las políticas que no han superado la conformidad.

- La página **Por activo** contiene información y enlaces a las políticas que los activos no han superado.
- La página **Por política** contiene información sobre el número y el porcentaje de activos que han pasado y los que no y, si procede, un enlace a las comprobaciones de política que la política utiliza.
- La página **Por comprobaciones de política** contiene información sobre el número y el porcentaje de activos que han superado o que no han superado cada comprobación de política.

Utilice las páginas de gestión de políticas con elementos del panel de control **Cambio de riesgo** para investigar las políticas y las comprobaciones de política que muestran un incremento del riesgo. El elemento del panel de control **Cambio de riesgo** contiene enlaces a las páginas **Por política** y **Por comprobaciones de política**.

Para obtener más información sobre los elementos del panel de control **Riesgo** y **Cambio de riesgo**, consulte la publicación *IBM Security QRadar SIEM Users Guide*.

Capítulo 13. Utilizar simulaciones en IBM Security QRadar Risk Manager

Utilizar simulaciones para definir, planificar y ejecutar simulaciones de explotación en la red. Puede crear, ver, editar, duplicar y suprimir simulaciones.

Puede crear simulaciones que se basen en una serie de reglas que se pueden combinar y configurar. La simulación se puede planificar para ejecutarse de forma periódica o ejecutarse manualmente. Después de que se haya completado una simulación, puede revisar los resultados de la simulación y aprobar cualquier resultado de riesgo aceptable o bajo que se base en la política de red. Al revisar los resultados puede aprobar acciones o tráfico aceptable de los resultados. Después de ajustar la simulación, puede configurar la simulación para supervisar los resultados.

Al supervisar una simulación, puede definir cómo desea que el sistema no responda cuando se devuelven resultados no aprobados. Una respuesta de sistema puede ser un correo electrónico, la creación de un suceso o enviar la respuesta a syslog.

Las simulaciones se pueden modelar a partir de una topología actual o un modelo de topología.

La página Simulation resume información acerca de las simulaciones y los resultados de la simulación.

Los resultados de simulación sólo se visualizan después de que se haya completado una simulación. Después de que se haya completado una simulación, la columna **Resultados** lista las fechas y los resultados correspondientes de la simulación.

Simulaciones

Las simulaciones creadas por los usuarios y los resultados de simulación se pueden ver desde la página Simulations.

La ventana Simulations proporciona la siguiente información:

Tabla 30. Parámetros de definiciones de simulación

Parámetro	Descripción
Simulation Name	Nombre de la simulación, tal como lo ha definido el creador de la simulación.
Model	Tipo de modelo. Las simulaciones se pueden modelar a partir de una topología actual o un modelo de topología. Las opciones son: <ul style="list-style-type: none">• Topología actual• Nombre del modelo de topología.
Groups	Grupos con los que está asociada la simulación.
Created By	Usuario que ha creado la simulación.

Tabla 30. Parámetros de definiciones de simulación (continuación)

Parámetro	Descripción
Creation Date	Fecha y la hora en que se ha creado la simulación.
Last Modified	Fecha y hora en que se ha modificado por última vez la simulación.
Schedule	Frecuencia con la que se ha planificado que se ejecute la simulación. Las opciones incluyen: <ul style="list-style-type: none"> • Manual: La simulación se ejecuta cuando se ejecuta manualmente. • Once: Especifique la fecha y la hora para la que se ha planificado que se ejecute la simulación. • Daily: Especifique la hora del día para la que se ha planificado que se ejecute la simulación. • Weekly: Especifique el día de la semana y la hora para los que se ha planificado que se ejecute la simulación. • Monthly: Especifique el día del mes y la hora para los que se ha planificado que se ejecute simulación.
Last Run	Última fecha y hora en la que se ha ejecutado la simulación.
Next Run	Fecha y hora en la que se ejecutará la próxima simulación.
Results	Si la simulación se ha ejecutado, este parámetro incluye una lista que contiene una lista de las fechas que contienen los resultados de la simulación. Si la simulación no se ha ejecutado, la columna Resultados no muestra ningún resultado.

Creación de una simulación

Puede crear simulaciones que se basen en una serie de reglas que se pueden combinar y configurar.

Acerca de esta tarea

Los parámetros que se pueden configurar para pruebas de simulación están subrayados. La tabla siguiente describe las pruebas de simulación que puede configurar.

Tabla 31. Pruebas de simulación

Nombre de prueba	Descripción	Parámetros
<u>El ataque va dirigido a una de las siguientes direcciones IP</u>	Simula ataques en direcciones IP o rangos CIDR específicos.	Configure el parámetro de direcciones de IP para especificar la dirección IP o los rangos CIDR a los que desea que se aplique esta simulación.

Tabla 31. Pruebas de simulación (continuación)

Nombre de prueba	Descripción	Parámetros
El ataque va dirigido a una de las redes siguientes	Simula ataques dirigidos a redes que son miembros de una o más ubicaciones de red definidas.	Configure el parámetro de redes para especificar las redes a las que desea que se aplique esta simulación.
El ataque va dirigido a uno de los siguientes componentes básicos de activo	Simula ataques que van dirigidos a uno o más componentes básicos de activo definidos.	Configure los parámetros de componentes básicos de activo para especificar los componentes básicos de activo a los que desea que se aplique esta simulación.
El ataque va dirigido a uno de los siguientes conjuntos de referencia	Simula ataques que van dirigidos a uno o varios conjuntos de referencia definidos.	Configura los parámetros de conjuntos de referencia para especificar los conjuntos de referencia a los que desea que se aplique esta simulación.
El ataque va dirigido a una vulnerabilidad en uno de los puertos siguientes utilizando protocolos	Simula ataques van dirigidos a una vulnerabilidad en uno o varios puertos definidos.	Configure los siguientes parámetros: <ul style="list-style-type: none"> • Puertos abiertos: Especifique los puertos que desea que esta simulación tenga en cuenta. • Protocolos: Especifique el protocolo que desea que esta simulación tenga en cuenta.
El ataque va dirigido a activos susceptibles a una de las siguientes vulnerabilidades	Simula ataques que van dirigidos a activos que son susceptibles a una o varias vulnerabilidades definidas.	Configure el parámetro vulnerabilities para identificar las vulnerabilidades que desea que aplique esta prueba. Puede buscar vulnerabilidades en el ID de OSVDB, ID de Bugtraq, ID de CVE o título.
El ataque va dirigido a activos susceptibles de vulnerabilidades con una de las siguientes clasificaciones	Le permite simular ataques que van dirigidos a un activo que es susceptible a vulnerabilidades para una o varias clasificaciones definidas.	Configure el parámetro classifications para identificar las clasificaciones de vulnerabilidad. Por ejemplo, una clasificación de vulnerabilidad puede ser manipulación de entrada o denegación de servicio.

Tabla 31. Pruebas de simulación (continuación)

Nombre de prueba	Descripción	Parámetros
El ataque va dirigido a activos susceptibles a vulnerabilidades con una puntuación CVSS mayor que 5	<p>Un valor de CVSS (Common Vulnerability Scoring System) es un estándar del sector para evaluar la gravedad de las vulnerabilidades. Esta simulación filtra activos en la red que incluyen el valor de CVSS configurado.</p> <p>Le permite simular ataques que van dirigidos a un activo que es susceptible a vulnerabilidades con una puntuación de CVSS mayor que 5.</p>	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • greater than - Especifique si la puntuación CVSS (Common Vulnerability Scoring System) es mayor que, mayor que o igual a, menor que, menor que o igual a, igual a o no igual al valor configurado. El valor predeterminado es mayor que. • 5: Especifique la puntuación CVSS que desea que esta prueba tenga en cuenta. El valor predeterminado es 5.
El ataque va dirigido a activos susceptibles a vulnerabilidades reveladas después de esta fecha	<p>Le permite simular ataques que van dirigidos a un activo que es susceptible a vulnerabilidades descubiertas antes de, después de o en la fecha configurada.</p>	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • before after on: Especifique si desea que la simulación considere que las vulnerabilidades reveladas son después de, antes de o en la fecha configurada en los activos. El valor predeterminado es before (antes). • this date: Especifique la fecha que desea que esta simulación tenga en cuenta.
El ataque va dirigido a activos susceptibles a vulnerabilidades donde el nombre, el proveedor, la versión o el servicio contiene una de las siguientes entradas de texto	<p>Le permite simular ataques dirigidos a un activo que es susceptible a vulnerabilidades que coinciden con el nombre de activo, el proveedor, la versión o el servicio basándose en uno o más entradas de texto.</p>	<p>Configure el parámetro text entries para identificar el nombre de activo, el proveedor, la versión o el servicio que desea que esta simulación tenga en cuenta.</p>
El ataque va dirigido a activos susceptibles a vulnerabilidades donde el nombre, el proveedor, la versión o el servicio contiene una de las siguientes expresiones regulares	<p>Le permite simular ataques dirigidos a un activo que es susceptible a vulnerabilidades que coinciden con el nombre de activo, el proveedor, la versión o el servicio basándose en una o más expresiones regulares.</p>	<p>Configure el parámetro regular expressions para identificar el nombre de activo, el proveedor, la versión o el servicio que desea que esta simulación tenga en cuenta.</p>

Las siguientes pruebas contribuyentes están en desuso y se ocultan en Policy Monitor:

- el ataque va dirigido a una vulnerabilidad en uno de los siguientes sistemas operativos
- el ataque va dirigido a activos susceptibles a vulnerabilidades de uno de los siguientes proveedores
- el ataque va dirigido a activos susceptibles a vulnerabilidades de uno de los siguientes productos

Las pruebas contribuyentes en desuso se han sustituido por otras pruebas.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. En el **menú Actions**, seleccione **New**.
4. Escriba un nombre para la simulación en el parámetro **What do you want to name this simulation**.
5. En la lista desplegable **Which model do you want to base this on**, seleccione el tipo de datos que desea que se devuelvan. Se listan todos los modelos de topología existentes. Si selecciona **Topología actual**, la simulación utiliza el modelo de topología actual.
6. Elija una de las opciones siguientes:

Opción	Descripción
Seleccione Use Connection Data	La simulación se basa en los datos de conexión y topología.
Borre Use Connection Data	La simulación sólo se basa en datos de topología. Si el modelo de topología no incluye datos y se borra la casilla de verificación Use Connection Data , la simulación no devuelve resultados.

7. En la lista **Importance Factor**, seleccione el nivel de importancia que desea asociar con esta simulación.
El Factor de importancia se utiliza para calcular la puntuación de riesgo. El rango es de 1 (importancia baja) a 10 (alta importancia). El valor predeterminado es 5.
8. En la lista **Where do you want the simulation to begin**, seleccione un origen para la simulación.
El valor elegido determina el punto de inicio de la simulación. Por ejemplo, el ataque se origina en una red específica. Los parámetros de simulación seleccionados se muestran en la ventana **Generate a simulation where**.
9. Añada destinos de ataque de simulación a la prueba de simulación.
10. Utilizando el campo que indica qué simulaciones desea incluir en el ataque, seleccione el signo + junto a la simulación que desea incluir.
Las opciones de simulación se muestran en la ventana **Generate a simulation where**.
11. En la ventana **Generate a simulation where**, pulse los parámetros subrayados para configurar adicionalmente los parámetros de simulación.
12. En la lista desplegable **Run this simulation for**, seleccione el número de pasos con los que desea ejecutar esta simulación (1 a 5).

13. En la lista desplegable de pasos, seleccione la planificación para ejecutar la simulación.
14. En el área de grupos, seleccione un casilla de verificación para cualquier grupo al que desee asignar esta simulación.
15. Pulse **Save Simulation**.

Edición de una simulación

Puede editar las simulaciones.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Seleccione la definición de simulación que desea editar.
4. En el menú **Actions**, seleccione **Edit**.
5. Actualice los parámetros como sea necesario.
Para obtener más información sobre los parámetros de simulación, consulte Pruebas de simulación.
6. Pulse **Save Simulation**.

Duplicación de una simulación

Puede duplicar las simulaciones.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Seleccione la simulación que desea duplicar.
4. En el menú **Actions**, seleccione **Duplicate**.
5. Escriba el nombre de la simulación.
6. Pulse **OK**.

Supresión de una simulación

Puede suprimir una simulación.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Seleccione la simulación que desea suprimir.
4. En el menú **Actions**, seleccione **Delete**.
5. Pulse **OK**.

Ejecución manual de una simulación

Utilice Simulation Editor para ejecutar una simulación manualmente.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú **Actions**, seleccione **Run Simulation**.
3. Pulse **OK**.

Resultados

El proceso de simulación puede tardar un periodo prolongado de tiempo. Mientras se ejecuta la simulación, la columna Next Run indica el porcentaje completado. Cuando se ha completado, la columna Results visualiza la fecha y hora de simulación.

Si ejecuta una simulación y, a continuación, realiza cambios que afectan a las pruebas asociadas con la simulación, es posible que estos cambios tarden hasta una hora en visualizarse.

Gestión de resultados de simulación

Después de que se ejecute una simulación, la columna Resultados muestra una lista desplegable que contiene una lista de las fechas en las que se ha generado la simulación.

Los resultados de simulación se conservan durante 30 días. Los resultados sólo se visualizan en la columna Resultados después de que se ejecute una simulación.

Visualización de resultados de simulación

Puede ver los resultados de simulación en la columna Resultados de la página Simulations.

Acerca de esta tarea

Los resultados sólo se visualizan en la columna Results después de que se ejecute una simulación. Los resultados de simulación proporcionan información sobre cada paso de la simulación.

Por ejemplo, el primer paso de una simulación proporciona una lista de los activos conectados directamente afectados por la simulación. El segundo paso lista los activos de la red que pueden comunicarse con los activos de primer nivel en la simulación.

Al pulsar View Result, se proporciona la siguiente información:

Tabla 32. Información de resultados de simulación

Parámetro	Descripción
Simulation Definition	Descripción de la simulación.
Using Model	Nombre del modelo para el que se ha ejecutado la simulación.
Simulation Result	Fecha en la que se ha ejecutado la simulación.
Step Results	Número de pasos para el resultado incluido el paso que está visualizando actualmente.

Tabla 32. Información de resultados de simulación (continuación)

Parámetro	Descripción
Assets Compromised	Número de activos totales comprometidos en este paso y en todos los pasos de la simulación. Si el modelo de topología incluye datos de un rango de IP de /32 definido como accesible, IBM Security QRadar Risk Manager no valida esos activos en la base de datos. Por lo tanto, dichos activos no se tienen en cuenta en el total de activos comprometidos. QRadar Risk Manager solo valida activos en rangos de IP más anchos, por ejemplo /24 para determinar qué activos existen.
Puntuación de riesgo	La puntuación de riesgo es un valor calculado basándose en el número de resultados, los pasos, el número de activos comprometidos y el factor de importancia asignado a la simulación. Este valor indica el nivel de gravedad asociado con la simulación para el paso visualizado.

Puede mover el puntero del ratón sobre una conexión para determinar la lista de activos afectados por esta simulación.

Se visualizan los 10 activos superiores al mover el ratón sobre la conexión.

Mueva el puntero del ratón sobre la conexión para resaltar la vía de acceso a través de la red, como lo define la subred.

La página de resultados de simulación proporciona una tabla denominada Resultados para este paso. Esta tabla proporciona la siguiente información:

Tabla 33. Resultados para esta información de paso

Parámetro	Descripción
Approve	Le permite aprobar los resultados de simulación. Consulte Aprobación de resultados de simulación.
Parent	Dirección IP de origen para el paso visualizado de la simulación.
IP	Dirección IP del activo afectado.
Network	Red de las direcciones IP de destino, tal como se define en la jerarquía de red.
Asset Name	Nombre del activo afectado, tal como lo define el perfil de activo.
Asset Weight	Peso del activo afectado, tal como se ha definido en el perfil de activo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. En la columna Results, seleccione la fecha y la hora de la simulación que desea ver utilizando la lista.
4. Pulse **View Result**. Puede ver la información de resultado de simulación, empezando en el paso 1 de la simulación.
5. Ve los resultados para esta tabla de pasos para determinar los activos afectados.
6. Para ver el siguiente paso de los resultados de simulación, pulse **Next Step**.

Aprobación de resultados de simulación

Puede aprobar los resultados de la simulación.

Acerca de esta tarea

Puede aprobar el tráfico de red que se considera comunicación de bajo riesgo o normal en el activo. Al aprobar los resultados, puede filtrar la lista de resultados para que las simulaciones futuras ignoren las comunicaciones normales o aprobadas.

Los resultados sólo se visualizan en la columna Resultados después de que se ejecute una simulación.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. En la columna Results, seleccione la fecha y la hora de la simulación que desea ver utilizando la lista.
4. Pulse **View Result**.
5. En los resultados de esta tabla de pasos, utilice uno de los métodos siguientes para aprobar activos:

Opción	Descripción
Approve Selected	Marque el recuadro de selección para cada activo que desea aprobar y, a continuación, pulse Approve Selected .
Approve All	Pulse aquí para aprobar todos los activos listados.

6. Opcional. Pulse **View Approved** para ver todos los activos aprobados.

Revocación de aprobación de simulación

Puede quitar una conexión o comunicación aprobada de la lista aprobada. Después de eliminar un resultado de simulación aprobado, las simulaciones futuras visualizan comunicaciones no aprobadas en los resultados de simulación.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.

3. En la columna Results, seleccione la fecha y la hora de la simulación que desea ver utilizando la lista.
4. **Vea el resultado.**
5. Pulse **View Approved** para ver todos los activos aprobados.
6. Elija una de las opciones siguientes:

Opción	Descripción
Revoke Selected	Marque el recuadro de selección para cada activo que desea revocar y, a continuación, pulse Revoke Selected .
Revoke All	Pulse aquí para revocar todos los activos listados.

Supervisión de simulaciones

Puede supervisar una simulación para determinar si los resultados de la simulación han cambiado. Si se produce un cambio, se genera un suceso. Puede haber un máximo de 10 simulaciones en modalidad de supervisión.

Acerca de esta tarea

Cuando una simulación está en modalidad de supervisión, el rango de tiempo predeterminado es de 1 hora. Este valor altera temporalmente el valor de tiempo configurado al crear la simulación.

Para obtener información sobre las categorías de sucesos, consulte la publicación *IBM Security QRadar SIEM Users Guide*.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Seleccione la simulación que desea supervisar.
4. Pulse **Monitor**.
5. En el campo **Event Name**, escriba el nombre del suceso que desea visualizar en la pestaña **Log Activity** y **Offenses**.
6. En el campo **Event Description**, escriba una descripción para el suceso. La descripción se visualiza en las anotaciones de los detalles de suceso.
7. En la lista **High-Level Category**, seleccione la categoría de suceso de alto nivel que desea que esta simulación utilice al procesar sucesos.
8. En la lista **Low-Level Category**, seleccione la categoría de suceso de alto nivel que desea que esta simulación utilice al procesar sucesos.
9. Seleccione el recuadro de selección **Ensure the dispatched event is part of an offense** si desea, como resultado de esta simulación supervisada, los sucesos que se reenvían al componente magistrado. Si no se ha generado ningún delito, se crea un nuevo delito. Si existe un delito, este suceso se añade al delito existente. Si selecciona el recuadro de selección, elija una de las opciones siguientes:

Opción	Descripción
Question/Simulation	Todos los sucesos de una pregunta están asociados con un solo delito.

Opción	Descripción
Asset	Se crea (o actualiza) un delito exclusivo para cada activo exclusivo.

10. En la sección **Additional Actions**, seleccione una o varias de las opciones siguientes:

Opción	Descripción
Email	Marque este recuadro de selección y especifique la dirección de correo electrónico para enviar notificaciones si se genera el suceso. Utilice una coma para separar varias direcciones de correo electrónico.
Send to Syslog	Marque este recuadro de selección si desea registrar el suceso. Por ejemplo, la salida de syslog parecerse a la siguiente: 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: Eventdescription
Notify	Marque este recuadro de selección si desea que los sucesos que se generan como resultado de esta pregunta supervisada se visualice en el elemento System Notifications del sistema en el panel de control.

11. En la sección **Enable Monitor**, seleccione el recuadro de selección para supervisar la simulación.

12. Pulse **Save Monitor**.

Agrupación de simulaciones

La asignación de simulaciones a grupos es una forma eficaz de ver y realizar el seguimiento de todas las simulaciones. Por ejemplo, puede ver todas las simulaciones que están relacionadas con la conformidad.

Acerca de esta tarea

Al crear simulaciones nuevas, puede asignar las simulaciones a un grupo existente.

Después de crear un grupo, puede arrastrar grupos al árbol de menús para cambiar la organización.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo en el que desea crear un nuevo grupo.
5. Pulse **New**.
6. En el campo **Name**, escriba un nombre para el nuevo grupo. El nombre de grupo puede tener hasta 255 caracteres de longitud.
7. En el campo **Description**, escriba una descripción para el grupo. La descripción puede tener un máximo de 255 caracteres de longitud.

8. Pulse **OK**.

Edición de un grupo

Puede editar un grupo.

Acerca de esta tarea

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo que desea editar.
5. Pulse **Edit**.
6. Actualice la información en los campos Name y Description según sea necesario.
7. Pulse **OK**.

Copia de un elemento en otro grupo

Mediante el uso de la funcionalidad de grupos, puede copiar una simulación en uno o muchos grupos.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione la pregunta que desea copiar en otro grupo.
5. Pulse **Copy**.
6. Marque este recuadro de selección para el grupo en el que desea copiar la simulación.
7. Pulse **Copy**.

Supresión de un elemento de un grupo

Puede suprimir un elemento de un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo de nivel superior.
5. En la lista de grupos, seleccione el elemento o grupo que desea suprimir.
6. Pulse **Remove**.
7. Pulse **OK**.

Asignación de un elemento a un grupo

Puede asignar una simulación a un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Seleccione la simulación que desea asignar a un grupo.
4. Mediante el uso del menú **Actions**, seleccione **Assign Groups**.
5. Seleccione el grupo al que desea que se asigne la pregunta.
6. Pulse **Assign Groups**.

Capítulo 14. Modelos de topología

Puede utilizar un modelo de topología para definir modelos de red virtual basándose en la red existente.

Puede crear un modelo de red basado en una serie de modificaciones que se puedan combinar y configurar. Esto le permite determinar el efecto de los cambios de configuración en la red utilizando una simulación. Para obtener más información sobre las simulaciones, consulte Utilización de simulaciones.

Puede ver modelos de topología en la página Simulations. Los modelos de topología proporcionan la siguiente información:

Tabla 34. Parámetros de definiciones de modelo

Parámetro	Descripción
Model Name	Nombre del modelo de topología, tal como lo ha definido el usuario al crearlo.
Group(s)	Grupos con los que está asociada esta topología.
Created By	Usuario que ha creado la definición de modelo.
Created On	Fecha y la hora en que se ha creado la definición de modelo.
Last Modified	Número de días desde que se ha creado la definición de modelo.

Creación de un modelo de topología

Puede crear uno o varios modelos de topología.

Acerca de esta tarea

La tabla siguiente describe los nombres de prueba y los parámetros que se pueden configurar.

Tabla 35. Pruebas de topología

Nombre de prueba	Parámetros
<p>Se añade una regla a los dispositivos seleccionados que permite conexiones de los CIDR de origen a los CIDR de destino en protocolos, puertos</p>	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • devices: Especifique los dispositivos a los que desea añadir esta regla. En la ventana Customize Parameter, marque el recuadro de selección All para incluir todos los dispositivos o puede buscar dispositivos utilizando uno de los siguientes criterios de búsqueda: <ul style="list-style-type: none"> - IP/CIDR: Seleccione la opción IP/CIDR y especifique la dirección IP o CIDR que desea añadir a esta regla. - Hostname: Seleccione la opción Hostname y especifique el nombre de host que desea filtrar. Para buscar varios nombres de host, utilice un carácter comodín (*) al principio o al final de la serie. - Adapter: Seleccione la opción Adapter y utilice la lista desplegable para filtrar la lista de dispositivos por adaptador. - Vendor: Seleccione la opción Vendor y utilice la lista desplegable para filtrar la lista de dispositivos por proveedor. También puede especificar un modelo para el proveedor. Para buscar varios modelos, utilice un carácter comodín (*) al principio o al final de la serie. • allows denies: Seleccione la condición (accept o denied) para las condiciones que desea que aplique esta prueba. • CIDRs: Seleccione las direcciones IP de origen o los rangos de CIDR a los que desea añadir esta regla. • CIDRs: Seleccione las direcciones IP de destino o los rangos CIDR a los que desea añadir esta regla. • protocols - Especifique los protocolos a los que desea añadir esta regla. Para incluir todos los protocolos, seleccione el recuadro de selección All. • ports: Especifique los puertos a los que desea añadir esta regla. Para incluir todos los puertos, seleccione el recuadro de selección All.

Tabla 35. Pruebas de topología (continuación)

Nombre de prueba	Parámetros
<p>Se añade una regla a los dispositivos IPS seleccionados que permite conexiones de los CIDR de origen a los CIDR de destino con vulnerabilidades</p>	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • IPS devices: Especifique los dispositivos IPS que desea que este modelo de topología incluya. Para incluir todos los dispositivos IPS, seleccione el recuadro de selección All. • allows denies: Especifique la condición (aceptar o denegar) para las conexiones a las que desea que se aplique esta prueba. • CIDRs: Especifique las direcciones IP de origen o los rangos CIDR que desea que este modelo de topología incluya. • CIDRs: Especifique las direcciones IP de destino o rangos CIDR que desea que este modelo de topología incluya. • vulnerabilities: Especifique las vulnerabilidades que desea aplicar al modelo de topología. Puede buscar vulnerabilidades utilizando el ID de Bugtraq, ID de OSVDB, ID de CVE o título.
<p>Los activos siguientes permiten conexiones a los puertos seleccionados</p>	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • assets: Especifique los activos que desea que este modelo de topología incluya. • allow deny: Especifique la condición (permitir o denegar) para las conexiones que desea que aplique este modelo de topología. El valor predeterminado es allow. • ports: Especifique los puertos que desea que este modelo de topología incluya. Para incluir todos los puertos, seleccione el recuadro de selección All.
<p>Los activos en los componentes básicos de activo siguientes permiten conexiones con puertos</p>	<p>Configure los siguientes parámetros:</p> <ul style="list-style-type: none"> • assets building blocks: Especifique los componentes básicos que desea que incluya este modelo de topología. • allow deny: Especifique la condición (permitir o denegar) que desea que este modelo de topología aplique. El valor predeterminado es allow. • ports: Especifique los puertos que desea que incluya este modelo de topología. Para incluir todos los puertos, seleccione el recuadro de selección All.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**

3. En el menú **Actions**, seleccione **New**.
4. En el campo **What do you want to name this model**, escriba un nombre para la definición de modelo.
5. En el panel **Which modifications do you want to apply to your model**, seleccione las modificaciones que desea aplicar a la topología para crear un modelo.
6. Configure las pruebas añadidas al panel **Configure model as follows** .
7. Cuando la prueba se visualiza en el panel, los parámetros configurables están subrayados. Pulse cada parámetro para configurar adicionalmente esta modificación para el modelo. En el área de grupos, seleccione el recuadro de selección para asignar grupos a esta pregunta.
8. Pulse **Save Model**.

Edición de un modelo de topología

Puede editar un modelo de topología.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**.
3. Seleccione la definición de modelo que desea editar.
4. En el menú **Actions**, seleccione **Edit**.
5. Actualice los parámetros como sea necesario.
Para obtener más información sobre los parámetros de Model Editor, Creación de un modelo de topología.
6. Pulse **Save Model**.

Duplicación de un modelo de topología

Puede duplicar un modelo de topología.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**.
3. Seleccione la definición de modelo que desea duplicar.
4. En el menú **Actions**, seleccione **Duplicate**.
5. Escriba un nombre que desee asignar al modelo de topología copiado.
6. Pulse **OK**.
7. Edite el modelo.

Supresión de un modelo de topología

Puede suprimir un modelo de topología.

Procedimiento

1. Pulse la pestaña **Riesgos**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**.
3. Seleccionar la definición de modelo que desea suprimir.
4. En el menú **Actions**, seleccione **Delete**.
5. Pulse **OK**.

Agrupar modelos de topología

Puede agrupar y ver los modelos de topología basándose en los criterios elegidos.

La categorización del modelo de topología es una forma eficaz de ver los modelos y realizar el seguimiento de los mismos. Por ejemplo, puede ver todos los modelos de topología relacionados con la conformidad.

Al crear modelos de topología nuevos, puede asignar los modelos de topología a un grupo existente. Para obtener información sobre la asignación de un grupo, consulte Creación de un modelo de topología.

Visualización de grupos

Puede ver modelos de topología utilizando grupos.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**.
3. Mediante el uso de la lista **Group**, seleccione el grupo que desea ver.

Creación de un grupo

Puede crear un grupo para ver y hacer un seguimiento de los modelos de topología de forma eficiente.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo en el que desea crear un nuevo grupo.
Después de crear el grupo, puede arrastrar y soltar grupos en los elementos de árbol de menús para cambiar la organización.
5. Pulse **New**.
6. Escriba el nombre que desee asignar al nuevo grupo. El nombre puede tener hasta 255 caracteres de longitud.
7. Escriba una descripción para el grupo. La descripción puede tener un máximo de 255 caracteres de longitud.
8. Pulse **OK**.
9. Si desea cambiar la ubicación del grupo nuevo, pulse el nuevo grupo y arrastre la carpeta a la ubicación en el árbol de menús.

Edición de un grupo

Puede editar un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Topology Models**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo que desea editar.
5. Pulse **Edit**.

6. Actualice los valores para los parámetros
7. Pulse **OK**.
8. Si desea cambiar la ubicación del grupo, pulse el nuevo grupo y arrastre la carpeta a la ubicación en el árbol de menús.

Copia de un elemento en otro grupo

Mediante el uso de la funcionalidad de grupos, puede copiar un modelo de topología en uno o muchos grupos.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulations > Topology Models**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione la pregunta que desea copiar en otro grupo.
5. Pulse **Copy**.
6. Marque este recuadro de selección para el grupo en el que desea copiar la simulación.
7. Pulse **Copy**.

Supresión de un elemento de un grupo

Puede suprimir un elemento de un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Pulse **Groups**.
4. En el árbol de menús, seleccione el grupo de nivel superior.
5. En la lista de grupos, seleccione el elemento o grupo que desea suprimir.
6. Pulse **Remove**.
7. Pulse **OK**.

Asignar una topología a un grupo

Puede asignar un modelo de topología a un grupo.

Procedimiento

1. Pulse la pestaña **Risks**.
2. En el menú de navegación, seleccione **Simulation > Simulations**.
3. Seleccione el modelo de topología que desea asignar a un grupo.
4. En el menú **Actions**, seleccione **Assign Group**.
5. Seleccione el grupo al que desea que se asigne la pregunta.
6. Pulse **Assign Groups**.

Capítulo 15. Datos de registro de auditoría

Los cambios realizados por los usuarios de IBM Security QRadar Risk Manager se registran en la pestaña **Actividad de registro** de IBM Security QRadar SIEM.

Todos los registros se visualizan en la categoría Auditoría de Risk Manager. Para obtener más información sobre la utilización de la pestaña **Actividad de registro** en QRadar SIEM, consulte la publicación *IBM Security QRadar SIEM Users Guide*.

Acciones registradas

Se registran acciones para los componentes.

La tabla siguiente lista las categorías y las acciones correspondientes que se registran.

Tabla 36. Acciones registradas

Categoría	Acción
Policy Monitor	Crear una pregunta.
	Editar una pregunta.
	Suprimir una pregunta.
	Enviar una pregunta manualmente.
	Enviar una pregunta automáticamente.
	Aprobar resultados.
	Revocar aprobación de resultados.
Topology Model	Crear un modelo de topología.
	Editar un modelo de topología.
	Suprimir un modelo de topología.
Topology	Guardar diseño.
	Crear una búsqueda guardada de topología.
	Editar una búsqueda guardada de topología
	Suprimir una búsqueda guardada de topología
	Colocación de un IPS.
Configuration Monitor	Crear una correlación de origen de registro
	Editar una correlación de origen de registro
	Suprimir una correlación de origen de registro
Simulations	Crear una simulación.
	Editar una simulación.
	Suprimir una simulación.
	Ejecutar manualmente una simulación.
	Ejecutar automáticamente una simulación.
	Aprobar resultados de simulación.
	Revocar resultados de simulación.

Tabla 36. Acciones registradas (continuación)

Categoría	Acción
Configuration Source Management	Autenticarse satisfactoriamente por primera vez en una sesión.
	Añadir un dispositivo.
	Eliminar un dispositivo.
	Editar la dirección IP o el adaptador para un dispositivo.
	Guardar una configuración de credenciales.
	Suprimir una configuración de credenciales.
	Guardar una configuración de protocolo.
	Eliminar una configuración de protocolo.
	Crear una planificación para un trabajo de copia de seguridad.
	Suprimir una planificación para un trabajo de copia de seguridad.
	Editar un trabajo de copia de seguridad.
	Añadir un trabajo de copia de seguridad.
	Suprimir un trabajo de copia de seguridad.
	Ejecutar un trabajo de copia de seguridad planificado
	Completar un trabajo planificado tanto si el trabajo ha sido satisfactorio como si ha fallado.
	Después de que un trabajo de copia de seguridad haya terminado de procesarse y haya persistido la configuración, no se han descubierto cambios.
	Después de que un trabajo de copia de seguridad haya terminado de procesarse y haya persistido la configuración, se han descubierto cambios.
	Después de que un trabajo de copia de seguridad haya terminado de procesarse y haya persistido la configuración, se han descubierto cambios no persistentes.
Después de que un trabajo de copia de seguridad haya terminado de procesarse y la configuración que persistía anteriormente ya no resida en el dispositivo.	
Ha empezado el intento de funcionamiento de adaptador, que incluye protocolos y credenciales.	
El intento de funcionamiento de adaptador ha sido satisfactoria, incluidos los protocolos y las credenciales.	

Visualización de actividad de usuario

Puede ver la actividad de los usuarios de IBM Security QRadar Risk Manager.

Procedimiento

1. Pulse la pestaña **Log Activity**. Si previamente ha guardado una búsqueda como valor predeterminado, se visualizan los resultados de esa búsqueda guardada.
2. Pulse **Search > New Search** para crear una búsqueda.
3. En el panel **Time Range**, seleccione una opción para el rango de tiempo que desea capturar para esta búsqueda.
4. En el panel **Search Parameters**, defina los criterios de búsqueda:
 - a. En la primera lista, seleccione **Category**.
 - b. En la lista desplegable **High Level Category**, seleccione **Risk Manager Audit**.
 - c. Opcional. En la lista desplegable **Low Level Category**, seleccione una categoría para refinar la búsqueda.
5. Pulse **Add Filter**.
6. Pulse **Filter** para buscar sucesos de QRadar Risk Manager.

Visualización del archivo de registro

Los registros de auditoría, que se almacenan en texto sin formato, se archivan y comprimen cuando el archivo de registro de auditoría alcanza un tamaño de 200 MB.

Acerca de esta tarea

El archivo de registro actual se denomina audit.log. Si el archivo de registro de auditoría alcanza un tamaño de 200 MB por segunda vez, el archivo se comprime y el registro de auditoría anterior se ha renombra como audit.1.gz. El número de archivo se incrementa cada vez que se archiva un archivo de registro. IBM Security QRadar Risk Manager puede almacenar hasta 50 archivos de registro archivados.

El tamaño máximo de cualquier mensaje de auditoría (sin incluir la fecha, la hora y el nombre de host) es de 1024 caracteres.

Cada entrada del archivo de registro se visualiza con el formato siguiente:

```
<fecha_hora> <nombre de host> <usuario>@<dirección IP>  
(ID de hebra) [<categoría>] [<subcategoría>]  
[<acción>] <carga útil>
```

La tabla siguiente describe los parámetros utilizados en el archivo de registro.

Tabla 37. Información de archivo de registro de auditoría

Parámetro	Descripción
<fecha_hora>	Fecha y hora de la actividad en el formato: Fecha del mes HH:MM:SS.
<nombre de host>	Nombre de host de la consola donde se ha registrado esta actividad.
<usuario>	Nombre del usuario que ha realizado la acción.

Tabla 37. Información de archivo de registro de auditoría (continuación)

Parámetro	Descripción
<dirección IP>	Dirección IP del usuario que ha realizado la acción.
(ID de hebra)	Identificador de la hebra Java™ que ha registrado esta actividad.
<categoría>	Categoría de alto nivel de esta actividad.
<subcategoría>	Categoría de bajo nivel de esta actividad.
<acción>	Actividad que se ha producido.
<carga útil>	Registro completo que ha cambiado, si hay alguno.

Procedimiento

1. Mediante el uso de SSH, inicie una sesión en IBM Security QRadar SIEM Console como usuario root.
2. Mediante el uso de SSH desde IBM Security QRadar SIEM Console, inicie la sesión en el dispositivo de QRadar Risk Manager como usuario root.
3. Vaya al directorio siguiente: /var/log/audit
4. Abra el archivo de registro de auditoría.

Detalles de archivo de registro

Los administradores utilizan archivos de registro de IBM Security QRadar Risk Manager para ver la actividad de usuario y para solucionar problemas de sistema.

La tabla siguiente describe la ubicación y el contenido de los archivos de registro de QRadar Risk Manager.

Tabla 38. Archivos de registro de QRadar Risk Manager

Nombre de archivo de registro	Ubicación	Descripción
audit.log	/var/log/audit/	Contiene la información de auditoría actual.
audit.<1-50>.gz	/var/log/audit/	Contiene información de auditoría archivada. Cuando el archivo audit.log alcanza un tamaño de 200 MB, se comprime y se renombra como audit.1.gz. El número de archivo se incrementa cada vez que se archiva un archivo de registro. QRadar Risk Manager puede almacenar hasta 50 archivos de registro archivados.
qradar.log	/var/log/	Contiene toda la información de proceso registrada por el servidor de QRadar Risk Manager.
qradar.error	/var/log/	Todas las excepciones y los mensajes System.out y System.err generados por el servidor de QRadar Risk Manager se registran en este archivo.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU.

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. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

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

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

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

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

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde dichas 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, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la exclusión de garantías, ni implícitas ni explícitas, en determinadas transacciones, por lo que es posible que esta declaración no se aplique en su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; 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.

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. Los materiales de dichos sitios web no forman parte de los materiales de este producto de IBM y el uso de dichos sitios web es a cuenta y riesgo del Cliente.

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 licenciarios de este programa que deseen tener información acerca del mismo con el fin de habilitar: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deben ponerse en contacto con:

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

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

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

Los datos de rendimiento aquí contenidos se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Es posible que algunas mediciones se hayan realizado en sistemas a nivel de desarrollo y no existe ninguna garantía de que estas mediciones sean las mismas en sistemas disponibles de forma general. Además es posible que algunas medidas se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para el entorno específico.

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

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

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

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y las direcciones utilizados por empresas comerciales reales es pura coincidencia.

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

Marca registradas

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

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

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en EE.UU. y/o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software como soluciones de servicio, ("Ofertas de software") pueden utilizar cookies u otras tecnologías para recopilar información de uso de producto, para ayudar a mejorar la experiencia del usuario final, para personalizar 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 el uso de cookies de esta oferta.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilen el ID de sesión de cada usuario para la gestión y autenticación de sesiones. Estas cookies se pueden inhabilitar, pero al hacerlo también se eliminará la funcionalidad que éstas habilitan.

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

Para obtener más información sobre el uso de diversas tecnologías, incluidas las 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>, en la sección titulada "Cookies, Web Beacons and Other Technologies e "IBM Software Products and Software--a-Service Privacy Statement" en <http://www.ibm.com/software/info/product-privacy>.

Glosario

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

En este glosario se utilizan las siguientes referencias cruzadas:

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

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

“A” “C” “D” “G” “I” “L” “M” en la página 168
“N” en la página 168 “P” en la página 168 “R” en la página 168 “S” en la página 168 “V” en la página 168

A

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

adaptador

Componente de software intermediario que permite que otros dos componentes de software se comuniquen entre sí.

ataque

Cualquier intento por parte de una persona no autorizada de comprometer el funcionamiento de un programa de software o sistema en red.

atributo

Datos asociados con un componente. Por ejemplo, un nombre de host, una dirección IP o el número de discos duros pueden ser atributos asociados a un componente de servidor.

C

Conversión de direcciones de red (NAT)

En un cortafuegos, conversión de las direcciones seguras de protocolo de Internet (IP) a direcciones registradas externas. Esto permite las comunicaciones

con redes externas, pero enmascara las direcciones IP utilizadas dentro del cortafuegos.

D

datos de vecino

Datos recopilados de adaptadores que se utilizan para descubrir información sobre los dispositivos que están conectados a hosts gestionados de QRadar.

dispositivo de contexto múltiple

Dispositivo único que se particiona en varios dispositivos virtuales. Cada dispositivo virtual es un dispositivo independiente, con su propia política de seguridad.

G

gráfico de conexión

Gráfico que muestra las conexiones de los nodos de red remotos y las direcciones IP locales a los nodos de red locales.

gráfico de serie temporal

Representación gráfica de conexiones de red a lo largo del tiempo.

gráfico de topología

Gráfico que describe subredes, dispositivos y cortafuegos.

I

indicador de riesgo

Medida de la exposición potencial de un sistema a una violación de seguridad.

indicador NAT

Indicador en el gráfico de topología que muestra que la vía de acceso entre dos conexiones de red contiene conversiones de dirección de origen o destino.

L

línea de conexión

Línea en el gráfico de conexión entre un nodo de red remoto y un nodo de red local o entre dos nodos de red locales.

M

modelo de topología

Representación virtual de la ordenación de activos de red que se utiliza para simular un ataque.

N

NAT Véase Conversión de direcciones de red.

P

protocolo arriesgado

Protocolo que se asocia con servicios que se ejecutan en un puerto abierto en las comunicaciones de entrada de Internet a la DMZ.

prueba contribuyente

Prueba que examina los indicadores de riesgo que se han especificado en una pregunta.

prueba de activo

Prueba que se utiliza para identificar indicadores de riesgo potencial que señalan cuándo los activos de una red violan una política definida o introducen riesgos en el entorno.

prueba restrictiva

Prueba que filtra los resultados devueltos por una pregunta de prueba contribuyente.

R

regla Conjunto de sentencias condicionales que permiten a los sistemas identificar relaciones y ejecutar respuestas automáticas como corresponde.

S

sub-búsqueda

Función que permite realizar una consulta de búsqueda en un conjunto de resultados de búsqueda completada.

V

vía de acceso de ataque

Origen, destino y dispositivos asociados con un ataque.

violación

Acto que ignora o contraviene la política corporativa.

vulnerabilidad

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

Índice

A

- acceso de cortafuegos 9
- actividad de usuario
 - registro de auditoría 161
- administrador de red vii
- alta disponibilidad (HA) 7
- añadir activo 66
- aprobación de simulación
 - revocar 147
- archivo de registro 161, 162
- asistente de informe 122

B

- Backup Log Viewer 25
- buscar 108
 - cancelar 110
 - configuración de recuento de reglas 81
 - CSM 80
 - SmartDashboard 77

C

- características no soportadas 7
- caso de uso de policy monitor
 - comunicación de prueba de dispositivos para acceso a Internet 62
 - comunicación posible en activos protegidos 61
 - comunicación real para DMZ 64
- CheckPoint SmartConsole
 - recuento de reglas 75
- comunicación real 86
 - preguntas contribuyentes 83
- conexiones 3, 97, 111
 - búsqueda 104
- conexiones de red
 - supervisar 3
- configuración 9
- configuración de dispositivo 22
 - comparar 117
- configuración de dispositivo de red
 - investigar 115
- configuration monitor 4
- configuration Source Management 13
- conformidad 47, 71
- conjunto de credenciales 14
- Conjunto de direcciones 14
- contraseña 6, 11
- correlación de origen de registro 113
 - crear 113
- CPSMS 78
- crear
 - perfiles de exploración de prueba de referencia 72
- credenciales 13
 - configurar 15
- Criterios de búsqueda 106

D

- datos de registro 159
- datos de registro de auditoría 159
- datos de vecino
 - recopilar 23
- descubrimiento de dispositivo 16, 17
- direccionamiento dinámico 7
- diseño 39
- dispositivo
 - añadir 19
 - importar 17
 - suprimir 20
- dispositivos 18
 - añadir 19

E

- editar activo 66
- estado de copia de seguridad 25
- exportar 48, 111

F

- factor de importancia 42
- filtrado de reglas de dispositivo 119

G

- glosario 167
- gráfico 100, 102, 103
- gráfico de conexión 102
- gráfico de serie temporal 100, 103
- gráfico de topología 35
- gráficos 99
 - conexiones 127
 - configurar 127
 - Objetos no utilizados de dispositivo 135
 - Reglas de dispositivo 131
- Grupo de red 14
- grupo de simulación
 - asignar elemento 151
 - copiar elemento 59, 150
 - editar 150
- grupos de dispositivos
 - agrupación de dispositivos 39
- guardar 110
- guardar criterios 70
- guardar criterios de búsqueda de activos 70

H

- hora del sistema 11

I

- importación de dispositivo, archivo CSV 18
- importar 48
- indicadores NAT 37
- información de configuración de copia de seguridad 24
- información de copia de seguridad 25
- información de inicio de sesión 6
- información de inicio de sesión predeterminada 6
- informe 123
 - compartir 127
 - duplicar 126
 - editar 125
- informes
 - generar manualmente 121
 - gestionar 121
 - QRadar Risk Manager 5
- integraciones de seguridad
 - QRadar Risk Manager 60
- introducción vii
- IPS 38
- IPv6 7

L

- lista de dispositivos
 - filtrado 20

M

- máscaras de red no contiguas 7
- modalidad de documento
 - navegador web Internet Explorer 6
- modalidad de navegador
 - navegador web Internet Explorer 6
- modalidad de supervisión 47, 57, 73
- modelo de topología 153
 - asignar a un grupo 158
 - copiar modelos en grupos 158
 - crear 153
 - crear un grupo 157
 - duplicar 156
 - editar 156
 - editar un grupo 157
 - suprimir 156
 - ver grupos 157
- modelos de topología
 - agrupar 157

N

- nombre de usuario 6
- novedades
 - versión 7.2.6, visión general de la guía del usuario 1

nuevas características
versión 7.2.6, visión general de la guía
del usuario 1

P

perfil de activo 66
perfiles de activo 70
pestaña Activos 66
planificación de descubrimiento 33
policy monitor 4
 suprimir elemento de grupo de
 preguntas 60, 150, 158
Policy Monitor 41
 asignar elementos a grupos 60
 casos de uso 61
 gestionar preguntas 41
 resultados de preguntas 56
pregunta 43, 44, 46, 72
 enviar 45
pregunta de activo 43
pregunta de conformidad de activo 46,
47, 72, 73
preguntas contribuyentes en desuso 86
preguntas de dispositivos/reglas 44
preguntas de policy monitor
 crear un grupo 59
 editar 59
 exportar 49
 importar 49
preguntas de Policy Monitor 48, 82
 agrupar 58
 evaluar resultados 55
 ver grupos 58
Preguntas de prueba contribuyentes en
desuso 93
Preguntas de prueba de
dispositivo/reglas 94

preguntas restrictivas 86
protocolos 30, 31
pruebas de comunicación posibles
 preguntas contribuyentes 89
 pruebas restrictivas 93
pruebas de referencia de
conformidad 47, 71
pruebas de simulación 140

Q

QRadar Risk Manager
 integración 60

R

recopilación de datos 23
registro de auditoría
 acciones 159
registro de copia de seguridad 25
resultados
 aprobar 56
Resultados de activos 50
resultados de búsqueda 109, 110
resultados de dispositivo 53
resultados de exploración
 ver 74
resultados de simulación 145
 aprobar 147
 gestionar 145
roles 10

S

servidor de correo electrónico 9
simulación 5
 duplicar 144

simulación (*continuación*)
 simulación manual 144
 suprimir 144
simulaciones 139
 agrupar 149
 editar 144
 supervisar 148
Simulations 139
Sistema de prevención de intrusiones 38
 eliminar 39
sub-búsqueda 108
supervisar preguntas 47, 57, 73

T

topología 4
 buscar aplicaciones 36
 búsqueda de vulnerabilidades 37
trabajo de copia de seguridad 26, 28, 29
trabajo de copia de seguridad,
 renombrar 29

U

ubicaciones de registro 162

V

ver
 resultados de exploración 74
versiones soportadas
 navegador web 6
visión general de QRadar Risk
Manager 3
vulnerabilidades de riesgo alto
 priorizar 63