IBM Security QRadar Risk Manager
Versão 7.2.5

Guia do Usuário

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 141.

Informações do produto

Este documento aplica-se ao IBM QRadar Security Intelligence Platform V7.2.5 e às liberações subsequentes, a não ser que seja substituído por uma versão atualizada.

Índice

Introdução ao IBM Security QRadar Risk Manager vii

Capítulo 1. O que há de novo para os usuários no QRadar Risk Manager V7.2.5 1

Capítulo 2. IBM Security QRadar Risk Manager 3
Conexões 3
Monitor de Configuração 3
Topologia 4
Monitor de política 4
Simulações 5
Relatórios do IBM Security QRadar Risk Manager 5
Navegadores da web suportados 6
Ativando o modo de documento e o modo de navegador no Internet Explorer 6
Acessar a interface com o usuário do IBM Security QRadar Risk Manager 6
Recursos não suportados no IBM Security QRadar Risk Manager 7

Capítulo 3. Configurar definições do IBM Security QRadar Risk Manager 9
Configurando acesso ao firewall 9
Atualizar a configuração do IBM Security QRadar Risk Manager 10
Configurar funções da interface com o usuário 10
Alterar senha raiz 11
Atualizar hora do sistema 11

Capítulo 4. Gerenciamento de Origem de Configuração 13
Credenciais 13
Conjunto de credenciais 14
Grupo de rede 14
Conjunto de endereços 14
Configurando credenciais para o IBM Security QRadar Risk Manager 14
Descoberta de dispositivo 16
Descobrindo dispositivos 16
Dispositivos de importação 17
Importando um arquivo CSV 18
Gerenciar dispositivos 18
Visualizando dispositivos 18
Incluindo um dispositivo 19
Editando dispositivos 19
Excluindo um dispositivo 20
Filtrando a lista de dispositivos 20
Obtendo a configuração do dispositivo 22
Coletando dados do vizinho 23
Coletando dados de um repositório de arquivo 23
Gerenciar tarefas de backup 24
Visualizar tarefas de backup 25
Visualizando status e logs da tarefa de backup 25
Incluindo uma tarefa de backup 25
Editando uma tarefa de backup 27
Renomear uma tarefa de backup 29
Excluindo uma tarefa de backup 29
Configurar protocolos 29
Configurando protocolos 30
Configurando o planejamento de descoberta 32

Capítulo 5. Topologia de rede 35
Recursos gráficos do modelo de topologia 35
Opções de menu ativado pelo botão direito da topologia 36
Pesquisas de caminho e ativos a partir da topologia 38
Indicadores NAT nos resultados da procura 38
Procurando aplicativos 39
Incluir um Sistema de Prevenção de Intrusão (IPS) 39
Remover um Sistema de Prevenção de Intrusão (IPS) 40

Capítulo 6. Monitor de política 41
Perguntas do Monitor de Política 41
Fator de importância 43
Visualizar informações de pergunta 43
Criando uma pergunta de ativo 43
Criando uma pergunta testada para regras em dispositivos 44
Enviando uma pergunta 45
Criando uma pergunta de conformidade do ativo 46
Editando uma referência de conformidade 47
Monitorando perguntas de conformidade do ativo 47
Exportar e importar perguntas do monitor de política 48
Exportando perguntas do monitor de política 48
Importando perguntas do monitor de política 49
Resultados do ativo 50
Resultados do dispositivo 53
Avaliar resultados das perguntas do Monitor de Política 55
Aprovar resultados 56
Perguntas do monitor 57
Criando um evento para monitorar resultados 57
Agrupar perguntas 58
Visualizando grupos 59
Criando um grupo 59
Editando um grupo 59
Copiando um item em outro grupo 59
Excluindo um item de um grupo 60
Designando um item a um grupo 60
Integração do IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager 60
Casos de uso do Monitor de Política 61
Comunicação real para protocolos permitidos por DMZ 61
Teste de ativos para possível comunicação em ativos protegidos 62
Comunicação de teste de dispositivo/regra sobre o acesso à Internet 63
Priorizando Vulnerabilidades de Alto Risco Aplicando Políticas de Risco 64
Perguntas do Monitor de Política 65
Contribuindo com perguntas para testes de comunicação reais 66
Contribuindo com perguntas para possíveis testes de comunicação 72
Parâmetros de pergunta restritivos para possíveis testes de comunicação 76
Perguntas do teste de dispositivo/regras 77

Capítulo 7. Investigar conexões 79
Visualizando conexões 79
Usar gráficos para visualizar dados de conexão 82
Usando o gráfico de série temporal 82
Usar gráfico de conexão para visualizar as conexões de rede 84
Usando gráficos de setor, barra e tabela 86
Procurar conexões 87
Salvando critérios de procura 88
Executando uma subprocura 91
Gerenciar resultados da procura 92
Cancelando uma procura 93
Excluindo uma procura 93
Exportando conexões 93

Capítulo 8. Mapeamento de origem de Log 95
Criando ou editando um mapeamento de origem de log 95

Capítulo 9. Investigando suas configurações do dispositivo de rede 97
Procurando regras de dispositivos 98
Comparando a configuração de seus dispositivos de rede 99

Capítulo 10. Gerenciando relatórios do IBM Security QRadar Risk Manager 101
Gerando manualmente um relatório 101
Usar o assistente de relatório 102
Criando um relatório 102
Editando um relatório 105
Duplicando um relatório 106
Compartilhando um relatório 106
Configurando gráficos 107
Gráficos de conexão 107
Gráficos Regras de Dispositivo 110
Gráficos Objetos de Dispositivo Não Usados 115

Capítulo 11. Gerenciamento de política 117

Capítulo 12. Usar simulações no IBM Security QRadar Risk Manager 119
Simulações 119
Criando uma simulação 120
Editando uma simulação 123
Duplicando uma simulação. 123
Excluindo uma simulação 124
Executando uma simulação manualmente 124
Gerenciando resultados da simulação 124
Visualizando resultados da simulação 124
Aprovando resultados da simulação 126
Revogando aprovação de simulação 127
Monitorando simulações 127
Agrupando simulações 128
Editando um grupo 129
Copiando um item em outro grupo 129
Excluindo um item de um grupo 129
Designando um item a um grupo 130

Capítulo 13. Modelos de topologia 131
Criando um modelo de topologia 131
Editando um modelo de topologia 134
Duplicando um modelo de topologia 134
Excluindo um modelo de topologia 134
Agrupar modelos de topologia 135
Visualizando grupos 135
Criando um grupo 135
Editando um grupo 135
Copiando um item em outro grupo 136
Excluindo um item de um grupo 136
Designar uma topologia a um grupo 136

Capítulo 14. Dados do log de auditoria 137
Ações registradas 137
Visualizando atividade do usuário 138
Visualizando o arquivo de log 139
Detalhes do arquivo de log 140

Avisos **141**
Marcas comerciais 143
Considerações de política de privacidade 143

Glossário **145**
A 145
C 145
D 145
G 145
I. 145
M 146
N 146
P 146
R 146
S 146
T 146
V 146

Índice Remissivo **147**

Introdução ao IBM Security QRadar Risk Manager

Estas informações são destinadas ao uso com IBM® Security QRadar Risk Manager. QRadar Risk Manager é um dispositivo usado para monitorar configurações de dispositivo, simular mudanças de rede e priorizar os riscos e vulnerabilidades em sua rede.

Este guia contém instruções para configurar e usar o IBM Security QRadar Risk Manager em um console IBM Security QRadar SIEM.

Público-alvo

Os administradores do sistema responsáveis pela configuração e uso do QRadar Risk Manager devem ter acesso administrativo ao IBM Security QRadar SIEM e aos dispositivos e firewalls de rede. O administrador do sistema deve ter conhecimento da rede corporativa e de tecnologias de rede.

Documentação técnica

Para obter informações sobre como acessar uma documentação mais técnica, notas técnicas e notas sobre a liberação, consulte Acessando a Nota Técnica da Documentação do IBM Security (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte Nota Técnica de Suporte e Download (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e de informações por meio de prevenção, detecção e resposta ao acesso incorreto de dentro e fora da empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. Sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que envolverá necessariamente procedimentos operacionais adicionais e podem requerer que outros sistemas, produtos ou serviços sejam mais eficazes. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

Capítulo 1. O que há de novo para os usuários no QRadar Risk Manager V7.2.5

O IBM Security QRadar Risk Manager V7.2.5 introduz o gerenciamento de política melhorado, suporte a diversos domínios e a habilidade de monitorar backups. Ele também inclui suporte para dispositivos Fortinet FortiGate que executam o FortiOS, e download e instalação mais fáceis de adaptadores suportados.

Gerenciar políticas mais facilmente

Use as novas páginas Gerenciamento de Política para realizar drill down a partir dos painéis **Risco** e **Mudança de Risco** a fim de visualizar resultados das últimas políticas de execução por ativo, por política e por verificação de política Saiba mais...

Suporte ao IP e domínio de sobreposição

Use recursos de suporte ao domínio QRadar Risk Manager para executar questões CIS em ativos em um domínio especificado. Saiba mais...

Backups de monitor e de solução de problemas

Use novas colunas na página Monitor de Configuração para visualizar o progresso e o status do backup de dispositivo e acessar logs de backup. Saiba mais...

Adaptador Fortinet FortiOS

O adaptador QRadar Risk Manager para Fortinet FortiOS suporta dispositivos Fortinet FortiGate que executam o sistema operacional Fortinet (FortiOS). Para obter informações adicionais, consulte o *IBM Security QRadar Risk Manager Adapter*

Download e instalação mais fáceis do adaptador

Agora você pode fazer download de todos os adaptadores suportados como um único arquivo compactado e instalá-los juntos. Para obter informações adicionais, consulte o *IBM Security QRadar Risk Manager Adapter*

Capítulo 2. IBM Security QRadar Risk Manager

O IBM Security QRadar Risk Manager é um dispositivo instalado separadamente para monitorar as configurações do dispositivo, simulando alterações no seu ambiente de rede e priorizando os riscos e vulnerabilidades em sua rede.

QRadar Risk Manager é acessado usando a guia **Riscos** em seu IBM Security QRadar SIEM Console.

QRadar Risk Manager usa os dados coletados pelo QRadar. Por exemplo, os dados de configuração de firewalls, roteadores, comutadores ou sistemas de prevenção de intrusão (IPSS), feeds de vulnerabilidades e origens de segurança de terceiros. As origens de dados permitem que o QRadar Risk Manager identifique os riscos de segurança, política e conformidade em sua rede e estime a probabilidade de exploração de risco.

O QRadar Risk Manager alerta para descobrir os riscos exibindo ofensas na guia **Ofensas**. Os dados de risco são analisados e relatados no contexto de todos os outros dados que o QRadar processa. No QRadar Risk Manager, é possível avaliar e gerenciar riscos em um nível aceitável que é baseado na tolerância de risco em sua empresa.

Também é possível usar o QRadar Risk Manager para consultar todas as conexões de rede, comparar as configurações do dispositivo, filtrar sua topologia de rede e simular os possíveis efeitos de atualizar as configurações do dispositivo.

É possível usar o QRadar Risk Manager para definir um conjunto de políticas (ou questões) sobre sua rede e monitorar as políticas para mudanças. Por exemplo, se desejar negar protocolos sem criptografia em seu DMZ a partir da Internet, será possível definir uma questão de monitor de política para detectar protocolos sem criptografia. Submeter a questão retorna uma lista de protocolos não criptografados que estão se comunicando a partir da internet para seu DMZ, e é possível determinar quais protocolos não criptografados são os riscos de segurança.

Conexões

Use a página Conexões para monitorar as conexões de rede de hosts locais.

É possível executar consultas e relatórios nas conexões de rede de hosts locais que são baseadas em qualquer aplicativo, porta, protocolo e websites com os quais os hosts locais podem se comunicar.

Para obter mais informações sobre Conexões, consulte Investigando conexões.

Monitor de Configuração

Use o Monitor de Configuração para revisar e comparar a configuração do dispositivo, permitindo reforçar as políticas de segurança e monitorar modificações do dispositivo dentro de sua rede.

As configurações do dispositivo podem incluir comutadores, roteadores, firewalls e dispositivos IPS em sua rede. Para cada dispositivo, é possível visualizar o

histórico de configuração do dispositivo, interfaces e regras. Também é possível comparar configurações dentro de um dispositivo e por meio de dispositivos.

As informações de configuração do dispositivo também são usadas para criar uma representação corporativa de sua topologia de rede, o que permite determinar atividades permitidas e proibidas em sua rede. A configuração do dispositivo permite identificar inconsistências e mudanças na configuração que apresentam risco em sua rede.

Topologia

A topologia é uma representação gráfica que representa a camada de rede de sua rede com base nos dispositivos incluídos do Gerenciamento de Origem de Configuração.

A camada de rede é a camada 3 do modelo Open Systems Interconnection (OSI).

A camada de aplicativo é a camada 7 do modelo OSI.

Use o gráfico interativo na topologia para visualizar as conexões entre os dispositivos, dispositivos de segurança de rede virtualizada com vários contextos, ativos, dispositivos Network Address Translation (NAT), indicadores NAT e informações sobre os mapeamentos NAT.

É possível procurar por eventos, dispositivos, caminhos e salvar layouts de rede.

Na topologia, você pode consultar o Camada de Transporte (camada 4) e filtrar caminhos de rede com base na porta e no protocolo. As informações de gráfico e conexão são criadas a partir de informações de configuração detalhadas obtidas a partir de dispositivos de rede, como firewalls, roteadores e sistemas IPS.

Para obter mais informações, consulte Topologia.

Monitor de política

Use o monitor de política para definir questões específicas sobre os riscos em sua rede, e envie a questão para IBM Security QRadar Risk Manager.

O QRadar Risk Manager avalia os parâmetros que você definiu na sua pergunta e retorna os ativos em sua rede para ajudar a avaliar o risco. As perguntas são baseados em uma série de testes que podem ser combinados e configurados conforme necessário. O QRadar Risk Manager fornece um grande número ou perguntas predefinidas do Monitor de Política e permite a criação de perguntas customizadas. As perguntas do Monitor de Política podem ser criadas para as seguintes situações:

- Comunicações que ocorreram
- Possíveis comunicações baseadas na configuração de firewalls e roteadores
- Regras de firewall reais (testes de dispositivo)

O Monitor de Política usa os dados obtidos dos dados de configuração, dados de atividade de rede, eventos de rede e de segurança e os dados de varredura de vulnerabilidade para determinar a resposta apropriada. O QRadar Risk Manager fornece modelos de política para ajudá-lo a determinar os riscos em vários mandatos regulamentares e melhores práticas de segurança de informações, como PCI, HIPAA e ISO 27001. É possível atualizar os modelos para alinhar com as suas

políticas de segurança da informação definidas corporativas. Quando a resposta for concluída, será possível aceitar a resposta para a pergunta e definir como você deseja que o sistema responda aos resultados não aceitos.

O Monitor de Política permite que um número ilimitado de perguntas seja monitorado ativamente. Quando uma pergunta é monitorada, o QRadar Risk Manager avalia continuamente a pergunta para resultados não aprovados. Como resultados não aprovados são descobertos, o QRadar Risk Manager tem a capacidade de enviar email, exibir notificações, gerar um evento do syslog ou criar uma ofensa no IBM Security QRadar SIEM.

Para obter mais informações sobre o Monitor de Política, consulte Monitor de Política.

Simulações

Use simulações para definir, planejar e executar simulações de exploração em sua rede.

É possível criar um ataque simulado em sua topologia com base em uma série de parâmetros que são configurados de maneira semelhante para o Monitor de Política. É possível criar um ataque simulado em sua topologia de rede atual ou criar um modelo de topologia. Um modelo de topologia é uma topologia virtual que permite fazer modificações na topologia virtual e simular um ataque. Isso permite simular como alterações nas regras de rede, portas, protocolos, ou conexões permitidas ou negadas podem afetar sua rede. Simulação é uma ferramenta poderosa para determinar o impacto do risco das mudanças propostas em sua configuração de rede antes de as mudanças serem implementadas.

Depois de uma simulação ser concluída, é possível revisar os resultados. Se você quiser aceitar os resultados, é possível configurar o modo de simulação, que permite definir como você deseja responder aos resultados inaceitáveis.

O IBM Security QRadar Risk Manager permite que até 10 simulações sejam monitoradas ativamente. Quando uma simulação é monitorada, o QRadar Risk Manager analisa continuamente na topologia resultados não aprovados. Como resultados não aprovados são descobertos, o QRadar Risk Manager tem a capacidade de enviar email, exibir notificações, gerar um evento do syslog ou criar uma ofensa no QRadar SIEM.

Para obter mais informações sobre Simulações, consulte Usando simulações.

Relatórios do IBM Security QRadar Risk Manager

Use a guia **Relatórios** para visualizar relatórios específicos, com base nos dados disponíveis no QRadar Risk Manager, como conexões, regras de dispositivo e objetos de dispositivo não usados.

Os relatórios detalhados adicionais a seguir estão disponíveis:

- conexões entre dispositivos
- regras de firewall em um dispositivo
- objetos não usados em um dispositivo

Para obter mais informações sobre relatórios, consulte Gerenciando relatórios do IBM Security QRadar Risk Manager.

Navegadores da web suportados

Para os recursos nos produtos IBM Security QRadar funcionarem de forma adequada, você deve usar um navegador da web suportado.

Ao acessar o sistema QRadar, será solicitado que você forneça um nome de usuário e uma senha. O nome de usuário e senha devem ser configurados com antecedência pelo administrador.

A tabela a seguir lista as versões suportadas de navegadores da web.

Tabela 1. Navegadores da web suportados para produtos QRadar

Navegador da web	Versões suportadas
Mozilla Firefox	17.0 24.0
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegador ativados	9.0 10.0
Google Chrome	A versão atual a partir da data de liberação dos produtos IBM Security QRadar V7.2.4

Ativando o modo de documento e o modo de navegador no Internet Explorer

Se você usa o Microsoft Internet Explorer para acessar produtos IBM Security QRadar, deve-se ativar o modo de navegador e o modo de documento.

Procedimento

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janela Ferramentas de desenvolvedor.
2. Clique em **Modo de navegador** e selecione a versão do seu navegador da web.
3. Clique em **Modo de documento**.
   - Para o Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**.
   - Para o Internet Explorer V10.0, selecione **Padrões do Internet Explorer 10**.

Acessar a interface com o usuário do IBM Security QRadar Risk Manager

O IBM Security QRadar Risk Manager usa as informações de login padrão da URL, nome de usuário e senha.

Acesse o QRadar Risk Manager através do IBM Security QRadar SIEM Console. Use as informações na tabela a seguir ao efetuar login no Console do QRadar.

Tabela 2. Informações de login padrão do QRadar Risk Manager

Informações de login	Padrão
URL	`https://<IP address>`, em que *<IP address>* é o endereço IP do Console do QRadar.
Nome de usuário	admin
Senha	A senha que é designada ao QRadar Risk Manager durante o processo de instalação.

Tabela 2. Informações de login padrão do QRadar Risk Manager (continuação)

Informações de login	Padrão
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

Recursos não suportados no IBM Security QRadar Risk Manager

É importante estar ciente dos recursos que não são suportados pelo QRadar Risk Manager.

Os recursos a seguir não são suportados no QRadar Risk Manager:

- Alta disponibilidade (HA)
- Roteamento Dinâmico para Protocolo de Roteamento de Borda (BGP), Open Shortest Path First (OSPF) ou Protocolo de Informações de Roteamento (RIP)
- IPv6
- Máscaras de rede não contíguas
- Rotas de carga balanceada
- Mapas de referência
- Armazenamento e Encaminhamento

Capítulo 3. Configurar definições do IBM Security QRadar Risk Manager

É possível configurar as definições de acesso para o QRadar Risk Manager a partir da guia **Admin** do IBM Security QRadar SIEM.

Se você tiver permissões apropriadas, é possível configurar várias definições de dispositivo para QRadar Risk Manager.

Os administradores podem executar as seguintes tarefas:

- Configurar dispositivos que o QRadar Risk Manager pode acessar por meio do firewall local. Para obter mais informações, consulte Configurando acesso ao firewall.
- Atualizar o servidor de email para o QRadar Risk Manager. Para obter mais informações, consulte Atualizar sua configuração do QRadar Risk Manager.
- Configurar as funções da interface para um host. Para obter mais informações, consulte Configurar funções da interface com o usuário.
- Alterar a senha para um host. Para obter mais informações, consulte Alterar a senha raiz.
- Atualizar a hora do sistema. Para obter mais informações, consulte Atualizar a hora do sistema.

As mudanças na configuração feitas por meio da administração do sistema baseado na web ocorrem imediatamente quando você as salva ou aplica.

Configurando acesso ao firewall

É possível configurar o acesso do firewall local para ativar ou desativar a comunicação entre o IBM Security QRadar Risk Manager e endereços IP, protocolos e portas específicos.

Sobre Esta Tarefa

Você pode definir uma lista de endereços IP com permissão para acessar a administração do sistema baseado na web. Por padrão, esses campos são deixados em branco, o que não restringe a comunicação com o QRadar Risk Manager. No entanto, quando você inclui um endereço IP, é concedido acesso ao sistema apenas para esse endereço IP. Todos os outros endereços IP são bloqueados.

Deve-se incluir o endereço IP da área de trabalho do cliente que você usa para acessar o QRadar Risk Manager. A falha dessa ação pode afetar a conectividade.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Clique no ícone **Gerenciamento de Sistemas**.
4. Efetue login como o usuário raiz para acessar a Administração do Sistema baseada na web. Os campos de nome do usuário e a senha fazem distinção entre maiúsculas e minúsculas.
5. No menu, selecione **Configuração do Host Gerenciado** > **Firewall Local**.

6. Na área de janela Acesso ao Dispositivo, configure os endereços IP, portas e protocolos que você deseja incluir como uma regra de firewall local no QRadar Risk Manager.
7. No campo **Endereço IP**, digite os endereços IP dos dispositivos que você deseja acessar.
8. Na lista **Protocolo**, selecione o protocolo para o qual deseja ativar o acesso para o endereço IP e porta especificados
9. No campo **Porta**, digite a porta na qual deseja ativar as comunicações e clique em **Permitir**.
10. Digite o endereço IP do host gerenciado ao qual deseja permitir o acesso ao sistema de administração baseado na Web e clique em **Permitir**. Apenas os endereços IP que são listados têm acesso à administração do sistema baseado na web. Se você deixar o campo em branco, todos os endereços IP terão acesso.
11. Clique em **Aplicar Controles de Acesso**.

Atualizar a configuração do IBM Security QRadar Risk Manager

É possível definir o servidor de correio usado para notificações do QRadar Risk Manager.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Clique no ícone **Gerenciamento de Sistemas**.
4. Efetue login como o usuário raiz para acessar a Administração do Sistema baseada na web. O nome do usuário e a senha fazem distinção entre maiúsculas e minúsculas.
5. No menu, selecione **Configuração do Host Gerenciado** > **Configuração do QRM**
6. No campo **Servidor de Correio**, digite o endereço IP ou nome do host para o servidor de correio que você quer que seja usado pelo QRadar Risk Manager.

   O QRadar Risk Manager usa esse servidor de correio para distribuir alertas e mensagens de eventos. Para utilizar o servidor de correio fornecido com o QRadar Risk Manager, digite **localhost**.
7. Clique em **Aplicar Configuração**.

O que Fazer Depois

Aguarde a tela para atualização antes de tentar fazer mudanças adicionais.

Configurar funções da interface com o usuário

Se o seu dispositivo contiver várias interfaces de rede, é possível designar funções específicas às interfaces de rede em cada sistema.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Clique no ícone **Gerenciamento de Sistemas**.

4. Efetue login como o usuário raiz para acessar a Administração do Sistema baseada na web. O nome do usuário e a senha fazem distinção entre maiúsculas e minúsculas.
5. No menu, selecione **Configuração do Host Gerenciado** > **Interfaces de Rede**.
6. Para cada interface listada, selecione a função que você deseja designar à interface utilizando a lista de Função.

   Na maioria dos casos, a configuração atual exibida não pode ser editada.
7. Clique em **Salvar Configuração**.
8. Aguarde a tela para atualização antes de tentar fazer mudanças adicionais.

Alterar senha raiz

É possível alterar a senha raiz.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Clique no ícone **Gerenciamento de Sistemas**.
4. Efetue login como o usuário raiz para acessar as configurações de Administração do Sistema. O nome do usuário e a senha fazem distinção entre maiúsculas e minúsculas.
5. No menu, selecione **Configuração do Host Gerenciado** > **Senha Raiz**.
6. No campo **Nova Senha Raiz**, digite a senha raiz usada para acessar o sistema de administração baseado na web e digite novamente a senha no campo **Confirmar Nova Senha Raiz**.
7. Clique em **Atualizar senha**.

Atualizar hora do sistema

É necessário contatar o suporte ao cliente antes de atualizar o tempo do sistema para o dispositivo IBM Security QRadar Risk Manager.

Antes de Iniciar

Todas as mudanças na hora do sistema devem ser salvas no console. O console então distribui as configurações de tempo atualizadas para todos os hosts gerenciados em sua implementação.

Para obter mais informações sobre como configurar a hora do sistema em seu Console, consulte o *IBM Security QRadar SIEM Administration Guide*.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Clique no ícone **Gerenciamento de Sistemas**.
4. Efetue login como o usuário raiz para acessar as configurações de Administração do Sistema. O nome do usuário e a senha fazem distinção entre maiúsculas e minúsculas.
5. No menu, selecione **Configuração do Host Gerenciado** > **Hora do Sistema**. A janela de configurações de tempo é dividida em duas seções. Você deve salvar

cada configuração antes de continuar. Por exemplo, quando você configura Hora do Sistema, deve-se clicar em **Aplicar** na área de janela Hora do Sistema antes de continuar.

6. Clique em **Configurar Hora**.
7. Em **Hora do Sistema**, selecione a data e hora atuais que deseja designar ao host gerenciado e, em seguida, clique em Aplicar.
8. Na área de janela **Hora do Hardware**, selecione a data e hora atuais que deseja designar ao host gerenciado e, em seguida, clique em Salvar.

Capítulo 4. Gerenciamento de Origem de Configuração

Use o Gerenciamento de Origem de Configuração para configurar credenciais, incluir ou descobrir dispositivos, visualizar configurações de dispositivo e fazer backup de configurações do dispositivo no IBM Security QRadar Risk Manager.

Os dados que são obtidos de dispositivos na sua rede são usados para preencher a topologia. Deve-se ter privilégios administrativos para acessar as funções de Gerenciamento de Origem de Configuração a partir da guia **Admin** no IBM Security QRadar SIEM.

Para configurar as origens de configuração, deve-se:

1. Configurar credenciais de dispositivo.
2. Descobrir ou importar dispositivos. Existem duas maneiras para incluir dispositivos de rede no QRadar Risk Manager: descobrir dispositivos usando Gerenciamento de Origem de Configuração ou importar uma lista de dispositivos de um arquivo CSV usando Importação de Dispositivo.
3. Obter a configuração do dispositivo de cada um de seus dispositivos.
4. Gerenciar tarefas de backup para assegurar que todas as atualizações na configuração do dispositivo sejam capturadas.
5. Configurar o planejamento de descoberta para assegurar que novos dispositivos sejam descobertos automaticamente.

Use o Gerenciamento de Origem de Configuração para:

- Incluir, editar, procurar e excluir origens de configuração. Para obter mais informações, consulte Gerenciar dispositivos.
- Configurar ou gerenciar protocolos de comunicação para seus dispositivos. Para obter mais informações, consulte Configurar protocolos.

Se você estiver usando o dispositivo Juniper NSM, deve-se também obter informações de configuração.

Para obter informações detalhadas sobre adaptadores usados para comunicação com dispositivos de fabricantes específicos, consulte o *IBM Security QRadar Risk Manager Adapter* .

Credenciais

No IBM Security QRadar Risk Manager, as credenciais são usadas para acessar e fazer download da configuração de dispositivos, tais como firewalls, roteadores, comutadores ou IPSs.

Administradores usam Gerenciamento de Origem de Configuração para inserir credenciais de dispositivo. Isso fornece ao QRadar Risk Manager acesso a um dispositivo específico. As credenciais de dispositivo individuais podem ser salvas para um dispositivo de rede específico. Se vários dispositivos de rede usarem as mesmas credenciais, é possível designar credenciais a um grupo.

Por exemplo, se todos os firewalls na organização tiverem o mesmo nome de usuário e senha, as credenciais serão associadas aos conjuntos de endereços para

todos os firewalls e usadas para fazer backup das configurações de dispositivo para todos os firewalls em sua organização.

Se uma credencial de rede não for necessária para um dispositivo específico, o parâmetro poderá ser deixado em branco no Gerenciamento de Origem de Configuração. Para obter uma lista de credenciais do adaptador necessárias, consulte o *IBM Security QRadar Risk Manager Adapter*.

É possível designar dispositivos diferentes em sua rede para grupos de rede, permitindo agrupar conjuntos de credenciais e endereços para seus dispositivos.

Conjunto de credenciais

Um conjunto de credenciais contém informações como valores de nome de usuário e senha para um conjunto de dispositivos.

Grupo de rede

Cada grupo de rede pode incluir vários conjuntos de endereço e credenciais. É possível configurar o IBM Security QRadar Risk Manager para priorizar como cada grupo de rede é avaliado.

O grupo de rede no início da lista possui a mais alta prioridade. O primeiro grupo de rede que corresponde ao endereço IP configurado é incluído como candidato ao fazer backup de um dispositivo. Um máximo de três conjuntos de credencial de um grupo de rede é considerado.

Por exemplo, se sua configuração incluir estes dois grupos de rede:

- Grupo de Rede 1 inclui dois conjuntos de credenciais
- Grupo de Rede 2 inclui dois conjuntos de credenciais

O QRadar Risk Manager tenta compilar uma lista de no máximo três conjuntos de credenciais. Como o Grupo de Rede 1 é o mais alto na lista, ambos os conjuntos de credenciais no Grupo Rede 1 são incluídos na lista de candidatos. Como três conjuntos de credenciais são necessárias, o primeiro conjunto de credenciais na Rede do Grupo 2 é incluído na lista.

Quando um conjunto de credenciais acessa um dispositivo com sucesso, o QRadar Risk Manager usa esse conjunto de credenciais para tentativas subsequentes de acessar o dispositivo. Se as credenciais nesse dispositivo mudarem, a autenticação falhará durante uma tentativa de acessar o dispositivo. Em seguida, na próxima tentativa de autenticação, o QRadar Risk Manager reconciliará as credenciais novamente para assegurar o êxito.

Conjunto de endereços

Um conjunto de endereços é uma lista de endereços IP que define um grupo de dispositivos que compartilham o mesmo conjunto de credenciais.

Configurando credenciais para o IBM Security QRadar Risk Manager

Os administradores devem configurar as credenciais para permitir que o IBM Security QRadar Risk Manager se conecte aos dispositivos na rede.

Sobre Esta Tarefa

É possível digitar um intervalo de endereços IP usando um traço ou curinga (*) para indicar um intervalo, como 10.100.20.0-10.100.20.240 ou 1.1.1*. Se você digitar 1.1.1.*, todos os endereços IP atendendo esse requisito serão incluídos.

Ao configurar o conjunto de endereços com Juniper Networks NSM ou um adaptador XML genérico, deve-se digitar o intervalo de endereços IP ou intervalo de endereços CIDR para todos os dispositivos gerenciados pelo Juniper Networks NSM ou arquivos para dispositivos no repositório.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela **Grupos de Rede**, clique no ícone **Incluir (+)**.
6. Digite um nome para um grupo de rede e, em seguida, clique em OK.
7. Mova o grupo de rede que você deseja que tenha a maior prioridade para a parte superior da lista. É possível usar os ícones **Mover para Cima** e **Mover para Baixo** para priorizar um grupo de rede.
8. No campo **Incluir Endereço**, digite o endereço IP ou intervalo CIDR que você deseja aplicar ao grupo de rede e, em seguida, clique no ícone **Incluir ()**.

   Repita para todos os endereços IP que você deseja incluir no endereço definido para este grupo de rede.
9. Na área de janela **Credenciais**, clique no ícone **Incluir (+)**.
10. Digite um nome para o novo conjunto de credenciais e, em seguida, clique em OK.
11. Digite valores para os parâmetros:

Opção	Descrição
Nome do usuário	Digite o nome de usuário para o conjunto de credenciais. Se você estiver usando um Juniper Networks NSM ou um adaptador XML genérico, digite um nome de usuário que possa acessar o servidor Juniper NSM ou um nome de usuário que possa acessar o repositório de arquivo que contém os arquivos SED.
Senha	Digite a senha para o conjunto de credenciais. Se você estiver usando Juniper Networks NSM ou um adaptador XML genérico, digite a senha para o servidor Juniper NSM ou a senha para efetuar login no repositório de arquivo que contém os arquivos SED.

Opção	Descrição
Ativar Nome de Usuário	Digite o nome de usuário para autenticação de segundo nível para o conjunto de credenciais.
Ativar Senha	Digite a senha para a autenticação de segundo nível para o conjunto de credenciais.
Comunidade SNMP Get	Digite a comunidade SNMP Get.
Usuário de Autenticação SNMPv3	Digite o nome de usuário que você deseja utilizar para autenticar SNMPv3.
Senha de Autenticação SNMPv3	Digite a senha que você deseja utilizar para autenticar SNMPv3.
Senha de Privacidade SNMPv3	Digite o protocolo que deseja usar para decriptografar os traps SNMP.

12. Mova o conjunto de credenciais que deseja tornar a primeira prioridade para a parte superior da lista. Use os ícones **Mover para Cima** e **Mover para Baixo** para priorizar um conjunto de credenciais.
13. Repita para cada conjunto de credenciais que deseja incluir.
14. Clique em **OK**.

Descoberta de dispositivo

O processo de descoberta usa o Protocolo Simples de Gerenciamento de Rede (SNMP) e a linha de comandos (CLI) para descobrir dispositivos de rede.

Depois que um endereço IP ou intervalo CIDR forem configurados, o mecanismo de descoberta executará uma varredura TCP relacionada ao endereço IP para determinar se as portas 22, 23 ou 443 estão sendo monitoradas pela conexão. Se a varredura TCP for bem-sucedida, e a consulta SNMP for configurada para determinar o tipo de dispositivo, o SNMP Get Community String será usado com base no endereço IP.

Essas informações são usadas para determinar para qual adaptador o dispositivo deverá ser mapeado quando for incluído. O IBM Security QRadar Risk Manager conecta-se ao dispositivo e coleta uma lista de interfaces e informações de vizinhos como tabelas CDP, NDP ou ARP. O dispositivo é então incluído no inventário.

O endereço IP configurado usado para iniciar o processo de descoberta não pode ser o endereço IP designado para o novo dispositivo. O QRadar Risk Manager inclui um dispositivo usando o endereço IP para a interface com a numeração mais baixa no dispositivo (ou endereço de loopback mais baixo, se houver algum).

Se você usar a caixa de seleção **Efetuar crawl na rede a partir dos endereços definidos acima**, o endereço IP dos vizinhos coletados do dispositivo serão reintroduzidos no processo de descoberta e o processo será repetido para cada endereço IP.

Descobrindo dispositivos

Os administradores utilizam Descobrir Dispositivos para determinar o tipo de dispositivo.

Sobre Esta Tarefa

Ao executar uma descoberta de dispositivo, qualquer dispositivo que não é suportado, mas responde ao SNMP, é incluído com o adaptador genérico SNMP. Se você deseja executar um filtro de caminho por meio do dispositivo com rotas simuladas, deve-se remover manualmente o dispositivo.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. No menu de navegação, clique em **Descobrir Dispositivos**.
5. Digite um endereço IP ou intervalo CIDR.

   Este endereço IP ou intervalo CIDR indica o local de dispositivos que você deseja descobrir.
6. Clique no ícone **Incluir (+)**.
7. Se também desejar procurar dispositivos na rede a partir do endereço IP ou intervalo CIDR definido, selecione a caixa de seleção **Efetuar crawl na rede a partir dos endereços definidos acima**.
8. Clique em **Executar**.

Dispositivos de importação

Utilize o Dispositivo de Importação para incluir uma lista de adaptadores e seus endereços IP de rede para o Configuration Source Manager utilizando um arquivo de valor separado por vírgula (.CSV).

A lista de importação do dispositivo pode conter até 5000 dispositivos, mas a lista deve conter uma linha para cada adaptador e seu endereço IP associado no arquivo de importação.

Por exemplo,

```
<Adapter::Name 1>,<IP Address>
<Adapter::Name 2>,<IP Address>
<Adapter::Name 3>,<IP Address>
```

Em que:

`<Adapter::Name>` contém o nome do fabricante e dispositivo, como Cisco::IOS.

`<IP Address>` contém o endereço IP do dispositivo, como 191.168.1.1.

Tabela 3. Exemplos de importação de dispositivo

Fabricante	Nome	Exemplo <Adapter::Name>,<IP Address>
Ponto de Verificação	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Dispositivo de Segurança Cisco	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus

Tabela 3. Exemplos de importação de dispositivo (continuação)

Fabricante	Nome	Exemplo <Adapter::Name>,<IP Address>
Genérico	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importando um arquivo CSV

É possível importar uma lista de dispositivos principais para o Configuration Source Management utilizando um arquivo com valor separado por vírgula (CSV).

Antes de Iniciar

Se você importar uma lista de dispositivos e, em seguida, fazer uma mudança em um endereço IP no arquivo CSV, talvez você acidentalmente duplique um dispositivo na lista Gerenciamento de origem de configuração. Por esse motivo, exclua um dispositivo do Configuration Source Management antes de importar a lista de dispositivos principais.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Plug-Ins**, clique em **Importação de Dispositivo**.
4. Clique em **Navegar**.
5. Localize o arquivo CSV, clique em **Abrir**.
6. Clique em **Importar Dispositivos**.

Resultados

Se um erro for exibido, então será necessário rever seu arquivo CSV para corrigir erros e importar o arquivo novamente. Uma importação do arquivo CSV poderá falhar se a lista de dispositivos for estruturada incorretamente ou se a lista de dispositivos contiver informações incorretas. Por exemplo, no seu arquivo CSV pode estar faltando dois pontos ou um comando, pode haver vários dispositivos em uma única linha ou um nome de adaptador pode ter um erro de digitação.

Se a importação do dispositivo for interrompida, então nenhum dispositivo do arquivo CSV será incluído Configuration Source Management.

Gerenciar dispositivos

Usando a guia Dispositivos na janela Gerenciamento de Origem de Configuração, é possível gerenciar os dispositivos em sua rede.

Na guia Dispositivos, é possível visualizar, incluir, editar e excluir dispositivos. Também é possível filtrar a lista de dispositivos, obter informações de configuração do dispositivo, coletar dados do vizinho e descobrir os dispositivos que estão em sua implementação.

Visualizando dispositivos

É possível visualizar todos os dispositivos em sua implementação na guia **Dispositivos**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Dispositivos**.
5. Para visualizar informações detalhadas para uma configuração de dispositivo, selecione o dispositivo que deseja visualizar e clique em **Abrir**.

Incluindo um dispositivo

É possível incluir adaptadores e dispositivos de rede usando Gerenciamento de Origem de Configuração.

Sobre Esta Tarefa

É possível incluir um dispositivo individual na lista de dispositivos Gerenciamento de Origem de Configuração ou incluir diversos dispositivos usando um arquivo CSV.

Para obter informações sobre como incluir vários dispositivos, consulte Importar dispositivos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Na área de janela de navegação, clique em **Incluir Dispositivo**.
5. Configure valores para os seguintes parâmetros:

Opção	Descrição
Endereço IP	Digite o endereço IP de gerenciamento do dispositivo.
Adaptador	No a lista suspensa **Adaptador**, selecione o adaptador que você deseja designar a este dispositivo.

6. Clique em **Incluir**.

   Se necessário, clique em **Ir** para atualizar a lista de adaptadores.

Editando dispositivos

É possível editar um dispositivo para corrigir o endereço IP ou o tipo de adaptador se houver um erro ou se a rede mudou e você precisar redesignar um endereço IP.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.

4. Selecione o dispositivo que você deseja editar.
5. Clique em **Editar**.
6. Configure valores para os seguintes parâmetros:

Opção	Descrição
Endereço IP	Digite o endereço IP de gerenciamento do dispositivo.
Adaptador	No a lista suspensa **Adaptador**, selecione o adaptador que você deseja designar a este dispositivo.

7. Clique em **Salvar**.

Excluindo um dispositivo

É possível excluir um dispositivo do IBM Security QRadar Risk Manager. Um dispositivo excluído é removido do Gerenciamento de Origem de Configuração, Monitor de Configurção e topologia.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Dispositivos**.
5. Selecione o dispositivo que você deseja excluir.
6. Clique em **Remover**.
7. Clique em **Sim** para excluir o dispositivo.

Resultados

Depois de excluir um dispositivo, o processo para remover o dispositivo da topologia pode requerer vários minutos.

Filtrando a lista de dispositivos

É possível usar filtros para localizar rapidamente os dispositivos na lista de dispositivos.

Sobre Esta Tarefa

O IBM Security QRadar Risk Manager pode manipular até 5000 dispositivos de rede no Gerenciamento de Origem de Configuração. Grandes números de dispositivos de rede podem fazer rolagem por meio de listas de dispositivo cansativas.

A tabela a seguir descreve os tipos de filtros que podem ser aplicados à lista de dispositivos para ajudar a encontrar dispositívos rapidamente.

Tabela 4. Tipos de filtro para a lista de dispositivos

Opção de Procura	Descrição
Endereço IP da Interface	Filtra dispositivos que possuem uma interface correspondente a um endereço IP ou intervalo CIDR. Digite o endereço IP ou intervalo CIDR no qual deseja procurar no campo IP/CIDR. Por exemplo, se você digitar um critério de procura de 10.100.22.6, os resultados da procura retornarão um dispositivo com um endereço IP de 10.100.22.6. Se você digitar um intervalo CIDR de 10.100.22.0/24, todos os dispositivos no 10.100.22.* serão retornados.
Endereço IP Admin	Filtra a lista de dispositivo com base no endereço IP da interface administrativa. Um endereço IP administrativo é o endereço IP que identifica exclusivamente um dispositivo. Digite o endereço IP ou intervalo CIDR no qual deseja procurar no campo **IP/CIDR**.
OS Version	Filtra a lista de dispositivos com base na versão do sistema operacional em que os dispositivos estão em execução. Selecione os valores para os seguintes parâmetros: • **Adaptador** – Utilizando a lista suspensa, selecione o tipo de adaptador desejado. • **Versão** – Usando a lista suspensa, selecione os critérios de procura para a versão. Por exemplo, maior que, menor que ou igual ao valor especificado. Digite o número da versão no campo no qual deseja procurar. Se você não selecionar uma opção de procura para a Versão, os resultados incluirão todos os dispositivos que estão configurados com o adaptador selecionado, independentemente da versão.
Modelo	Filtra a lista de dispositivos com base no número do fornecedor e modelo. Configure valores para os seguintes parâmetros: • **Fornecedor** – Usando a lista suspensa, selecione o fornecedor que você deseja procurar. • **Modelo** – Digite o modelo que você deseja procurar.

Tabela 4. Tipos de filtro para a lista de dispositivos (continuação)

Opção de Procura	Descrição
Nome do Host	Filtra a lista de dispositivo com base no nome do host. Digite o nome de host no qual você deseja procurar no campo **Nome do host**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela do Risk Manager, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Dispositivos**.
5. Usando a lista suspensa à esquerda da lista de dispositivos, selecione um filtro:
6. Clique em **Ir**.

Resultados

Todos os resultados da procura que corresponderem aos seus critérios serão exibidos na tabela.

O que Fazer Depois

Para reconfigurar um filtro, selecione **Endereço IP da Interface**, limpe o endereço **IP/CIDR** e, em seguida, clique em **Ir**.

Obtendo a configuração do dispositivo

O processo de fazer backup de um dispositivo para obter uma configuração de dispositivo pode ser concluído para um único dispositivo na lista de dispositivos ou é possível fazer backup de todos os dispositivos na guia **Dispositivos**.

Sobre Esta Tarefa

Depois de configurar conjuntos de credenciais e conjuntos de endereços para acessar os dispositivos de rede, deve-se fazer backup dos dispositivos para fazer download da configuração do dispositivo para as informações sobre o dispositivo incluídas na topologia.

Para obter mais informações sobre o planejamento de backups automatizados das configurações de dispositivo da guia **Tarefas**, consulte Gerenciar tarefas de backup.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Dispositivos**.

5. Para obter a configuração para todos os dispositivos, clique em **Fazer Backup de Todos** na área de janela de navegação e, em seguida, clique em **Sim** para continuar.
6. Para obter a configuração para um dispositivo, selecione o dispositivo. Para selecionar múltiplos dispositivos, mantenha pressionada a tecla CTRL e selecione todos os dispositivos necessários. Clique em **Fazer backup**.
7. Se necessário, clique em **Visualizar Erro** para visualizar os detalhes de um erro. Depois de corrigir o erro, clique em **Fazer Backup de Todos** na área de janela de navegação.

Coletando dados do vizinho

Use o processo de descoberta para obter dados do vizinho de um dispositivo usando SNMP e uma interface de linha de comandos (CLI).

Sobre Esta Tarefa

Os dados do vizinho são usados na topologia para desenhar as linhas de conexão para exibir o mapa de topologia gráfica de seus dispositivos de rede. O botão de descoberta permite selecionar dispositivos únicos ou múltiplos e atualizar os dados do vizinho para um dispositivo. Essas informações são usadas para atualizar as linhas de conexão para um ou vários dispositivos na topologia.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Dispositivos**.
5. Selecione o dispositivo para o qual você deseja obter dados. Para selecionar múltiplos dispositivos, mantenha pressionada a tecla CTRL e selecione todos os dispositivos necessários.
6. Clique em **Descobrir**.
7. Clique em **Sim** para continuar.

Resultados

Se você selecionar múltiplos dispositivos, o processo de descoberta pode levar vários minutos para ser concluído.

O que Fazer Depois

Selecione **Executar em Segundo Plano** para trabalhar em outras tarefas.

Coletando dados de um repositório de arquivo

É possível obter arquivos SED XML de dispositivo ou arquivos de entrada que contêm a configuração de dispositivo básica de um repositório de arquivo de rede.

Sobre Esta Tarefa

O repositório de arquivo que hospeda os arquivos deve suportar o protocolo FTP ou SFTP. O IBM Security QRadar Risk Manager obtém informações sobre o

dispositivo de todos os arquivos XML SED localizados no diretório de arquivo remoto do repositório de arquivos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Dispositivos**.
5. Selecione **Descobrir a partir do Repositório**.
6. Configure valores para os seguintes parâmetros:

Opção	Descrição
Protocolo	Na lista suspensa **Protocolo**, selecione **FTP** ou **SFTP** como o protocolo de comunicações para acessar seu repositório de arquivo de configuração.
Endereço IP	Digite o endereço IP do repositório do arquivo de configuração.
Caminho Remoto	Digite o caminho de arquivo remoto para o diretório que contém os arquivos XML SED. O caminho de arquivo padrão para arquivos SED é `<install directory>/output`. O <install directory> é o local do arquivo `ziptie-adapter.<date>–<build>.zip` extraído.
Nome de usuário	Digite o nome de usuário necessário para efetuar login no sistema que hospeda o repositório de arquivo de configuração.
Senha	Digite a senha necessária para efetuar login no sistema que hospeda o repositório de arquivo de configuração.

7. Clique em **OK** para descobrir um dispositivo de um repositório.
8. Clique em **Ir** para atualizar a lista de dispositivos.

Gerenciar tarefas de backup

Uma tarefa refere-se a uma tarefa de backup, que permite que você faça backup automaticamente de informações de configuração para todos os dispositivos na guia **Dispositivos** em um planejamento.

Usando a guia **Tarefas** do Gerenciamento de Origem de Configuração, é possível criar tarefas de backup para todos os dispositivos ou grupos individuais de dispositivos no Gerenciamento de Origem de Configuração.

Nenhuma tarefa de backup que você define na página Gerenciamento de Origem de Configuração afeta a configuração de backup do IBM Security QRadar SIEM usando o ícone **Backup e Recuperação** na guia **Admin**. A funcionalidade de backup e recuperação obtém as informações de configuração e dados para o QRadar SIEM. A tarefa de backup apenas obtém informações para dispositivos externos.

Visualizar tarefas de backup

As tarefas e os detalhes da tarefa são exibidos na guia **Tarefas**.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Tarefas**.
5. Dê um clique duplo em qualquer tarefa que você deseja visualizar com mais detalhes.

Visualizando status e logs da tarefa de backup

Você pode resolver problemas da tarefa de backup usando as informações de status de backup e de arquivos de log que são fornecidas na página **Monitor de Configuração**.

Sobre Esta Tarefa

Para visualizar o status e o progresso da tarefa de backup, use a página Monitor de Configuração. Para visualizar o arquivo de log da tarefa de backup, use o Visualizador de Log de Backup.

Procedimento

Acesse **Riscos** > **Monitor de Configuração**. As colunas a seguir na tabela **Lista de Dispositivos** fornecem informações sobre status da tarefa de backup:

Coluna	Descrição
Status de Backup	Indica o status de conclusão da tarefa de backup: • `COLLECTED`. A tarefa de backup está aguardando para ser processada. • `RUNNING`. A tarefa de backup está em andamento. • `SUCCESS`. A tarefa de backup foi concluída com êxito. • `FAILURE`. A tarefa de backup não foi concluída.
Progresso	Exibe uma barra de progresso que controla a taxa de conclusão da tarefa de backup. Para atualizar a barra de progresso, clique no ícone **Atualizar** na página Monitor de Configuração.
Log de Backup	Para abrir a janela Visualizador do Log de Backup da tarefa de backup, clique no link **Consultar Log** nesta coluna. Para atualizar a barra de progresso, clique em **Atualizar** na janela Visualizador do Log de Backup.

Incluindo uma tarefa de backup

É possível criar tarefas de backup para todos os dispositivos, ou grupos individuais de dispositivos, em Gerenciamento de Origem de Configuração.

Sobre Esta Tarefa

Depois de definir os critérios de procura, você define o planejamento de tarefa. A configuração do planejamento é exibida na coluna Acionadores. Os acionadores para uma tarefa representam o planejamento de tarefa. É possível ter vários planejamentos que estão configurados. Por exemplo, é possível configurar duas opções de planejamento para que uma tarefa seja executada toda segunda e no primeiro dia de cada mês.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Tarefas**.
5. Selecione **Nova Tarefa** > **Backup**.
6. Configure valores para os seguintes parâmetros:

Opção	Descrição
Nome da Tarefa	Digite o nome que você deseja aplicar a esta tarefa.
Grupo	Na lista Grupos, selecione o grupo ao qual você deseja designar esta tarefa. Se nenhum grupo for listado, é possível digitar um nome de grupo. É possível classificar tarefas após elas designadas a um grupo.
Comentário	Digite qualquer comentário que deseja associar a essa tarefa de backup. É possível digitar até 255 caracteres em sua descrição da tarefa de backup.

7. Clique em **OK**.
8. Selecione um dos seguintes métodos de procura:

Opção	Descrição
Lista estática	É possível usar uma lista estática para procurar dispositivos usando várias opções. Usando a opção de lista estática, é possível definir os dispositivos específicos nos quais você deseja executar a tarefa.
Procurar	Digite um endereço IP ou intervalo CIDR que você deseja incluir na tarefa. Quando você define os critérios de procura, a procura para dispositivos é executada depois que a tarefa é executada. Isso assegura que quaisquer dispositivos novos sejam incluídos na tarefa.

9. Se você escolher lista estática, defina os critérios de procura:
   a. Clique na guia **Dispositivos**.

b. Na lista na guia **Dispositivos**, selecione os critérios de procura. Para obter mais informações, consulte Critérios de procura para uma lista estática ou procura.
c. Clique em **Ir**.
d. Na guia **Dispositivos**, selecione os dispositivos que você deseja incluir na tarefa.
e. Na área da janela Detalhes da Tarefa, clique em **Incluir selecionado a partir da procura de visualização de dispositivo**.

10. Se você escolheu Procurar, defina os critérios de procura:
    a. Clique na guia **Dispositivos**.
    b. Usando a lista na guia **Dispositivos**, selecione os critérios de procura. Para obter mais informações, consulte Critérios de procura para uma lista estática ou procura.
    c. Clique em **Ir**.
    d. Na área de janela Detalhes da Tarefa, clique em **Usar procura da visualização de dispositivos**. Esse critério de procura é usado para determinar os dispositivos que estão associadas a esta tarefa.
11. Clique em **Planejamento** e configure valores para os seguintes parâmetros:

Opção	Descrição
Nome	Digite um nome para a configuração de planejamento.
Horário de início	Selecione uma data e hora em que deseja iniciar o processo de backup. A hora tem de ser especificada no horário militar.
Frequência	Selecione a frequência que você deseja associar a esse planejamento.
Cron	Digite uma expressão cron, que é interpretada na Hora de Greenwich (GMT). Para obter assistência, entre em contato com o administrador.
Especificar Data de Encerramento	Opcional. Selecione uma data para terminar o planejamento de tarefa.

12. Clique em **Salvar** na área de janela Acionador.
13. Repita as etapas 11 e 12 para criar vários planejamentos.
14. Se você deseja executar a tarefa imediatamente, clique em **Executar Agora**.
15. Clique em **Sim** para continuar.

Editando uma tarefa de backup

É possível editar tarefas de backup.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Tarefas**.
5. Clique duas vezes na tarefa que deseja editar.

6. Escolha uma das seguintes opções de procura a partir do parâmetro **Tipo de Seleção**:

Opção	Descrição
Lista estática	Uma lista estática permite procurar dispositivos usando várias opções. Usando a opção de lista estática, é possível definir os dispositivos específicos nos quais você deseja executar a tarefa.
Procurar	Digite um endereço IP ou intervalo CIDR que você deseja incluir na tarefa. Quando você define os critérios de procura, a procura por dispositivos ocorre após a execução da tarefa. Isso assegura que quaisquer dispositivos novos sejam incluídos na tarefa.

7. Se você escolher Lista Estática, defina os critérios de procura:
   a. Clique na guia **Dispositivos**.
   b. Na lista na guia **Dispositivos**, selecione os critérios de procura.
   c. Clique em **Ir**.
   d. Na guia **Dispositivos**, selecione os dispositivos que você deseja incluir na tarefa.
   e. Na área de janela **Detalhes da Tarefa**, clique em **Incluir selecionado a partir da procura de visualização de dispositivo**.
8. Se você escolheu Procurar, defina os critérios:
   a. Clique na guia **Dispositivos**.
   b. Usando a lista na guia **Dispositivos**, selecione os critérios de procura.
   c. Clique em **Ir**.
   d. Na área de janela Detalhes da Tarefa, clique em **Usar procura a partir da visualização de dispositivos**. Esse critério de procura é usado para determinar os dispositivos que estão associadas a esta tarefa.
9. Clique em **Planejamento** e configure valores para os seguintes parâmetros:

Opção	Descrição
Nome	Digite um nome para a configuração de planejamento.
Horário de início	Selecione uma data e hora em que deseja iniciar o processo de backup. A hora tem de ser especificada no horário militar.
Frequência	Selecione a frequência que você deseja associar a esse planejamento.
Cron	Digite uma expressão cron, que é interpretada na Hora de Greenwich (GMT). Para obter assistência, entre em contato com o administrador.
Especificar Data de Encerramento	Opcional. Selecione uma data para terminar o planejamento de tarefa.

10. Clique em **Salvar**.
11. Clique em **Executar Agora**.
12. Repita as etapas 9 e 10, conforme necessário.

13. Clique em **Sim** para continuar.

Renomear uma tarefa de backup

É possível renomear uma tarefa de backup.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Tarefas**.
5. Selecione a tarefa de backup que você deseja renomear.
6. Clique em **Renomear**.
7. Configure valores para os seguintes parâmetros:

Opção	Descrição
Nome da Tarefa	Digite o nome que você deseja aplicar a esta tarefa.
Grupo	Na lista **Grupo**, selecione o grupo ao qual você deseja designar esta tarefa. Também é possível especificar um novo nome de grupo.
Comentário	Opcional. Digite qualquer comentário que deseja associar a essa tarefa de backup. É possível digitar até 255 caracteres em sua descrição da tarefa de backup.

8. Clique em **OK**.

Excluindo uma tarefa de backup

É possível excluir uma tarefa de backup.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. Clique na guia **Tarefas**.
5. Selecione a tarefa de backup que você deseja excluir.
6. Clique em **Excluir**.

Configurar protocolos

Para o IBM Security QRadar Risk Manager se comunicar com dispositivos, deve-se definir o método de comunicação (protocolo) necessário para a comunicação com os dispositivos de rede.

O QRadar Risk Manager fornece a configuração do protocolo padrão para seu sistema. Se você precisar definir protocolos, é possível definir os protocolos para permitir que o QRadar Risk Manager obtenha e atualize a configuração do

dispositivo. Muitos ambientes de rede têm diferentes protocolos de comunicação de diferentes tipos ou funções do dispositivo. Por exemplo, um roteador pode usar um protocolo diferente dos firewalls na rede. Para obter uma lista de protocolos suportados pelo fabricante do dispositivo, consulte o *IBM Security QRadar Risk Manager Adapter*.

O QRadar Risk Manager usa conjuntos de protocolo para definir grupos de protocolos para um conjunto de dispositivos que requerem um protocolo de comunicação específico. É possível designar dispositivos a grupos de rede, que permitem agrupar conjuntos de protocolos e conjuntos de endereços para seus dispositivos.

Conjuntos de protocolo são um conjunto nomeado de protocolos para um conjunto de dispositivos que requerem credenciais de protocolo específicas.

Conjuntos de endereços são endereços IP que definem o grupo de rede.

Configurando protocolos

É possível definir protocolos para obter e atualizar a configuração do dispositivo.

Sobre Esta Tarefa

Você pode configurar os seguintes valores para os parâmetros do protocolo.

Tabela 5. Parâmetros do protocolo

Protocolo	Parâmetro
SSH	Configure os seguintes parâmetros: • **Porta** – Digite a porta que você quer que o protocolo SSH use ao se comunicar com e fazer backup de dispositivos de rede. A porta de protocolo SSH padrão é 22. • **Versão** - Selecione versão do SSH desejada para uso nesse grupo de rede quando for comunicar-se com dispositivos de rede. As opções disponíveis são as seguintes: **Automático** – Esta opção detecta automaticamente a versão SSH a ser usada para comunicação com dispositivos de rede. **1** – Use SSH-1 ao se comunicar com dispositivos de rede. **2** - Use SSH-2 para comunicar-se com dispositivos de rede.
Telnet	Digite o número da porta que deseja que o protocolo Telnet use ao se comunicar com e fazer backup de dispositivos de rede. A porta de protocolo Telnet padrão é 23.
HTTPS	Digite o número da porta que deseja que o protocolo HTTPS use ao se comunicar com e fazer backup de dispositivos de rede. A porta do protocolo HTTPS padrão é 443.

Tabela 5. Parâmetros do protocolo (continuação)

Protocolo	Parâmetro
HTTP	Digite o número da porta que deseja que o protocolo HTTP use ao se comunicar com e fazer backup de dispositivos de rede. A porta de protocolo HTTP padrão é 80.
SCP	Digite o número da porta que deseja que o protocolo SCP use ao se comunicar com e fazer backup de dispositivos de rede. A porta de protocolo SCP padrão é 22.
SFTP	Digite o número da porta que deseja que o protocolo SFTP use ao se comunicar com e fazer backup de dispositivos de rede. A porta de protocolo SFTP padrão é 22.
FTP	Digite o número da porta que deseja que o protocolo FTP use ao se comunicar com e fazer backup de dispositivos de rede. A porta de protocolo SFTP padrão é 22.
TFTP	O protocolo TFTP não tem nenhuma opção configurável.
SNMP	Configure os seguintes parâmetros: • **Porta** – Digite o número da porta que deseja que o protocolo SNMP use ao se comunicar com e fazer backup de dispositivos de rede. • **Tempo Limite(ms)** – Selecione a quantidade de tempo, em milissegundos, que deseja usar para determinar um tempo limite de comunicação. • **Novas Tentativas** – Selecione o número de vezes que deseja tentar novamente as comunicações com um dispositivo. • **Versão** – Selecione a versão do SNMP que deseja usar para as comunicações. As opções são v1, v2 ou v3. • **Autenticação V3** – Selecione o algoritmo que deseja usar para autenticar os traps SNMP. • **Criptografia V3** – Selecione o protocolo que deseja usar para decriptografar os traps SNMP.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. No menu de navegação, clique em **Protocolos**.
5. Configure um novo grupo de rede:

a. Na área de janela **Grupos de Rede**, clique no ícone **Incluir (+)**.
b. Digite um nome para um grupo de rede.
c. Clique em **OK**.
d. Use os ícones **Mover para Cima** e **Mover para Baixo** para priorizar os grupos de rede. Mova o grupo de rede que você deseja que tenha a maior prioridade para a parte superior da lista.

6. Configure o conjunto de endereços:
   a. No campo **Incluir Endereço**, digite o endereço IP ou intervalo CIDR que você deseja aplicar ao grupo de rede e, em seguida, clique no ícone **Incluir ()**. Por exemplo, digite um intervalo de endereços IP usando um traço ou curinga (*) *) para indicar um intervalo, como 10.100.20.0-10.100.20.240 ou 1.1.1*. Se você digitar 1.1.1.*, todos os endereços IP atendendo esse requisito serão incluídos.
   b. Repita para todos os endereços IP que você deseja incluir no endereço definido para este grupo de rede.
7. Configure o conjunto de protocolos:
   a. Na área de janela **Grupos de Rede**, verifique se o grupo de redes para o qual deseja configurar protocolos está selecionado.
   b. Selecione as caixas de seleção para aplicar um protocolo ao intervalo de endereços IP designado ao grupo de rede que você criou. A limpeza da caixa de seleção desativa a opção de comunicação para o protocolo durante a tentativa de fazer backup de um dispositivo de rede.
   c. Para cada protocolo que você selecionou, configure valores para os parâmetros.
   d. Use os ícones **Mover para Cima** e **Mover para Baixo** para priorizar os protocolos. Mova o protocolo que você deseja que tenha a primeira prioridade para a parte superior da lista.
8. Clique em **OK**.

Configurando o planejamento de descoberta

É possível configurar um planejamento de descoberta para preencher ARP, tabelas MAC e informações do vizinho para seus dispositivos. O planejamento de descoberta também permite que novos dispositivos sejam automaticamente incluídos no inventário.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Na área de janela **Risk Manager**, clique em **Gerenciamento de Origem de Configuração**.
4. No menu de navegação, clique em **Planejar Descoberta**.
5. Selecione a caixa de seleção **Ativar descoberta periódica** para ativar o planejamento de descoberta.
6. Configure valores para os seguintes parâmetros:

Opção	Descrição
Nome	Digite um nome para a configuração de planejamento.

Opção	Descrição
Horário de início	Selecione uma data e hora em que deseja iniciar o processo de backup. A hora tem de ser especificada no horário militar.
Frequência	Selecione a frequência que deseja associar a este planejamento.
Cron	Digite uma expressão cron, que é interpretada na Hora de Greenwich (GMT). Para obter assistência, entre em contato com o administrador.
Especificar Data de Encerramento	Opcional. Selecione uma data para terminar o planejamento de tarefa.
Efetuar crawl e descobrir novos dispositivos	Selecione a caixa de seleção se desejar que o processo de descoberta descubra novos dispositivos. Desmarque a caixa de seleção se não desejar incluir novos dispositivos no inventário.

7. Clique em **OK**.

Capítulo 5. Topologia de rede

No IBM Security QRadar Risk Manager, é possível usar o gráfico do modelo de topologia para visualizar, filtrar e investigar a conectividade física de rede.

O gráfico de topologia de rede é gerado a partir das informações de configuração obtidas a partir de dispositivos como firewalls, roteadores, comutadores e sistemas Intrusion Prevention System (IPS). É possível passar o mouse sobre linhas de conexão para exibir informações de conexão de rede. É possível filtrar a topologia por meio da procura de caminhos de potenciais ataques em protocolos permitidos, portas ou vulnerabilidades, visualizar o fluxo de tráfego entre dispositivos ou sub-redes e regras de dispositivos.

É possível usar topologia para:

- Visualizar caminhos de rede específicos e direção de tráfego para análise de ameaça avançada.
- Incorporar mapas de IPS de segurança passiva no gráfico de topologia.
- Customizar o layout da topologia, incluindo grupos de rede definidos pelo usuário.
- Criar filtros de procura para sua topologia de rede com base em protocolos, portas ou vulnerabilidades.
- Visualizar informações de conexão detalhadas entre dispositivos e sub-redes.
- Visualizar as regras do dispositivo em conexões de topologia com as portas e os protocolos permitidos.
- Visualizar dispositivos de conversão de endereço de rede (NAT), indicadores NAT e informações sobre os mapeamentos NAT.
- Visualizar dispositivos de segurança de rede virtualizados que tenham contextos múltiplos.

Quando você visualiza as portas e os protocolos permitidos entre dispositivos, TCP, UDP e ICMP são os únicos protocolos representados no modelo de topologia.

Recursos gráficos do modelo de topologia

É possível acessar os recursos gráficos no modelo de topologia.

Tabela 6. Recursos gráficos do modelo

Se desejar	Então
Visualizar detalhes adicionais sobre uma sub-rede	Mova o ponteiro do mouse sobre a sub-rede. As informações de configuração são exibidas.
Visualizar detalhes adicionais sobre um dispositivo	Mova o ponteiro do mouse sobre o dispositivo. As informações de configuração são exibidas.

Tabela 6. Recursos gráficos do modelo (continuação)

Se desejar	Então
Visualizar detalhes adicionais sobre uma conexão	Mova o ponteiro do mouse sobre uma linha de conexão entre um dispositivo ou sub-rede para visualizar detalhes da conexão. Várias bordas curvadas entre um dispositivo e uma sub-rede indicam que um dispositivo ou conjunto de contextos têm várias interfaces na mesma sub-rede.
Visualizar detalhes adicionais sobre um dispositivo de contexto múltiplo	Mova o ponteiro do mouse sobre o dispositivo de contexto múltiplo. As informações de configuração são exibidas.
Distribuir nós	Para distribuir os dispositivos, firewalls ou sub-redes no gráfico, use o ponteiro do seu mouse para arrastar o nó para o local preferencial.
Aumentar zoom ou diminuir zoom	Use a régua de controle na parte superior esquerda do gráfico para escalar o gráfico. Também é possível usar o botão de rolagem do mouse para escalar o gráfico.
Panoramizar para a esquerda, para a direita, para cima ou para baixo	Clique com o botão esquerdo do mouse no espaço em branco do modelo de topologia e arraste seu cursor para panoramizar uma direção. Também é possível usar a caixa delimitadora no canto inferior direito para panoramizar em qualquer direção do modelo de topologia.

Opções de menu ativado pelo botão direito da topologia

Na topologia, você pode clicar com o botão direito em um evento para acessar informações de filtro de eventos adicionais.

Tabela 7. Opções da topologia de clique com o botão direito

Se desejar	Então
Procurar Conexões	Para qualquer sub-rede na topologia, clique com o botão direito do mouse e selecione **Procurar Conexões**. Isso cria uma procura em que a origem ou o destino é o endereço IP da sub-rede que você selecionou. É possível incluir parâmetros de busca adicionais e clicar em **Procura** para visualizar os resultados.
Visualizar informações de configuração para um dispositivo.	Mova o mouse sobre o dispositivo, clique com o botão direito do mouse e selecione **Visualizar Configuração do Dispositivo**. Essas informações são obtidas do dispositivo.

Tabela 7. Opções da topologia de clique com o botão direito (continuação)

Se desejar	Então
Visualizar informações de configuração para um dispositivo de contexto de múltiplos.	Mova o mouse sobre o dispositivo, clique com o botão direito do mouse e selecione **Visualizar Configuração do Dispositivo**. Isso exibe uma lista de contextos que pertencem ao dispositivo de contextos múltiplos e inclui informações de configuração básicas do dispositivo. É possível visualizar informações detalhadas de configuração do dispositivo para um contexto se você der um clique duplo em um contexto na lista.
Procurar Eventos	Mova o ponteiro do mouse sobre um dispositivo ou sub-rede na topologia. Clique com o botão direito e selecione **Procurar Eventos**. • Se você procurar eventos em uma sub-rede, os parâmetros de procura serão preenchidos com o endereço de origem e de destino no filtro de procura. • Se você procurar eventos em um dispositivo que é mapeado para uma origem de log, uma procura de evento será preenchida com o nome de origem de log e endereço IP no filtro de procura. Isso permite procurar eventos ligados ao dispositivo da topologia. Se um dispositivo não for mapeado para uma origem de log, a opção **Procurar Eventos** não estará disponível.
Procurar fluxos associados a uma sub-rede	Mova o botão do mouse sobre a sub-rede. Clique com o botão direito e selecione **Procurar Fluxos**. A janela Procurar Fluxo é exibida. Para obter informações adicionais sobre fluxos de procura, consulte o *IBM Security QRadar SIEM Users Guide*.
Visualizar informação do perfil do ativo para uma sub-rede	Mova o ponteiro do mouse sobre a sub-rede. A janela Lista de Ativos exibe a lista de ativos para a sub-rede. Para obter mais informações sobre ativos, consulte o *IBM Security QRadar SIEM Users Guide*.
Incluir uma conexão IPS entre dois dispositivos.	Se a sua topologia incluir um dispositivo IPS, mova o ponteiro do mouse sobre uma linha de conexão que liga um nó de dispositivo a um nó de sub-rede. Clique com o botão direito e selecione **Incluir IPS**.

Tabela 7. Opções da topologia de clique com o botão direito (continuação)

Se desejar	Então
Remover IPS	Mova o ponteiro do mouse sobre a linha de conexão que liga um nó de dispositivo e um nó de sub-rede que inclui o IPS. Clique com o botão direito e selecione **Remover IPS**. Esse menu é exibido somente se existir um IPS na conexão.

Pesquisas de caminho e ativos a partir da topologia

No IBM Security QRadar Risk Manager, é possível pesquisar sua topologia para visualizar os ativos de rede, sub-redes e os caminhos entre as redes.

É possível procurar diretamente da visualização de topologia ou a partir do menu **Procura**.

Uma procura de caminho exibe a direção do tráfego, protocolos totais ou parcialmente permitidos e regras de dispositivos. Um indicador NAT é exibido no gráfico de topologia quando sua procura localiza um caminho que contém conversões de origem ou de destino.

Se estiver procurando um host, todos os dispositivos que se comunicam com o host serão exibidos. Se o host não corresponder a uma interface em um dispositivo, mas estiver incluído na sub-rede, então a sub-rede e todos dispositivos conectados serão exibidos.

Se houver conexões de porta entre redes, as portas permitidas serão exibidas em um resumo de caminho.

Uma conexão bloqueada é indicada na topologia por um quadrado vermelho. Passe o mouse sobre o quadrado vermelho para investigar regras de firewall que forçam a conexão bloqueada.

Indicadores NAT nos resultados da procura

Um indicador NAT, que é um ponto verde sólido, será exibido no gráfico de topologia se sua procura localizar um caminho que contém conversões de origem ou de destino.

Sobre Esta Tarefa

Um indicador NAT indica que o endereço IP de destino que foi especificado no filtro do caminho pode não ser o destino final. Você pode passar o mouse sobre o indicador para visualizar as seguintes informações sobre as conversões.

Tabela 8. Informações disponíveis a partir do indicador NAT

Parâmetro	Descrição
Origem	O CIDR ou IP de origem convertido.
Porta(s) de Origem	As portas de origem convertidas, se aplicável.
Origem Convertida	O resultado da conversão que foi aplicada à origem.

Tabela 8. Informações disponíveis a partir do indicador NAT (continuação)

Parâmetro	Descrição
Porta(s) de Origem Convertida	O resultado da conversão que foi aplicada à(s) porta(s) de origem, se aplicável.
Destino	O CIDR ou IP de destino convertido.
Porta(s) de Destino	As portas de destino convertidas, se aplicável.
Destino Convertido	O resultado da conversão que foi aplicada ao destino.
Porta(s) de Destino Convertida(s)	O resultado da conversão que foi aplicada à(s) porta(s) de destino, se aplicável.
Fase	A fase de roteamento quando a conversão foi aplicada. A conversão é aplicada pré ou pós-roteamento.

Procurando aplicativos

Procure aplicativos a partir da topologia do IBM Security QRadar Risk Manager na guia **Riscos**, ou quando selecionar um caminho na topologia, para visualizar detalhes do aplicativo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Topologia**.
3. Clique em **Procurar** > **Nova procura**.
4. Selecione a opção **Caminho**.
5. Clique em **Selecionar aplicativos**.
6. No menu suspenso **Adaptador de dispositivo**, selecione o tipo de adaptador de dispositivo necessário.
7. No campo **Nome do aplicativo**, insira o descritor para o aplicativo.
8. Clique em **Procurar**.
9. Clique em cada aplicativo em que você deseja procurar no campo **Resultados da procura** e clique em **Incluir**.
10. Clique em **OK**.

Incluir um Sistema de Prevenção de Intrusão (IPS)

Se a lista Gerenciamento de Origem de Configuração incluir um dispositivo sistema de prevenção de intrusão (IPS), é possível incluir um IPS em uma conexão entre nós dispositivo-para-sub-rede e nós dispositivo-para-dispositivo.

Sobre Esta Tarefa

Incluir uma conexão IPS é útil para determinar o local do IPS se o dispositivo for passivo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Topologia**.

3. Mova o ponteiro do mouse sobre a linha de conexão que liga um nó de dispositivo e um nó de sub-rede.
4. Clique com o botão direito na linha de conexão e selecione **Incluir IPS**.
5. Selecione o dispositivo e as interfaces para incluir a partir das seguintes listas:

Opção	Descrição
Colocar IPS	Selecione uma colocação da lista.
Conectar interface IPS	Selecione uma interface para se conectar ao dispositivo. Se houver dispositivos de múltipla escolha, você precisará selecionar um dispositivo (consulte a opção seguinte).
ao dispositivo	Selecione o dispositivo que você deseja conectar ao IPS. Essa opção estará disponível se houver vários dispositivos.
Conectar interface IPS	Selecione uma interface para conectar à sub-rede.

6. Usando as listas, selecione o dispositivo e as interfaces para incluir a conexão IPS em sua topologia.
7. Clique em **OK**.

Remover um Sistema de Prevenção de Intrusão (IPS)

É possível remover uma conexão IPS.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Topologia**.
3. Mova o ponteiro do mouse sobre a linha de conexão que liga um nó de dispositivo e um nó de sub-rede.
4. Clique com o botão direito na linha de conexão e selecione a opção Remover IPS idp.
5. Clique em **OK**.

Capítulo 6. Monitor de política

As organizações usam Monitor de Política para definir perguntas de riscos específicos sobre a rede para avaliar ou monitorar riscos com base na análise de indicadores de risco.

No Monitor de Política, é possível definir políticas, avaliar a aderência a uma política, avaliar resultados de perguntas e monitorar os riscos novos.

Os modelos de pergunta padrão são fornecidos para você avaliar e monitorar os riscos em sua rede. É possível usar um dos modelos de pergunta padrão como base para suas próprias perguntas ou criar uma nova pergunta. É possível localizar modelos de pergunta padrão no menu **Grupo** na página Monitor de Política.

É possível escolher a partir da lista de indicadores de risco a seguir:

- A atividade de rede mede o risco com base nas comunicações de rede que ocorreram no passado.
- A configuração e a topologia medem risco baseado na possível comunicação e conexões de rede.
- As vulnerabilidades medem um risco com base em sua configuração de rede e em dados de varredura de vulnerabilidade que são coletados de ativos de rede.
- Regras de firewall medem riscos com base na execução ou ausência de regras de firewall que são aplicadas em toda a rede.

É possível definir testes que são baseados nos indicadores de risco e depois restringir os resultados do teste para filtrar a consulta para violações ou resultados específicos.

Os profissionais de segurança criam perguntas para ativos ou dispositivos/regras para sinalizar riscos em suas redes. O nível de risco para um ativo ou um dispositivo/regra é relatado após uma pergunta ser enviada para o Monitor de Política. É possível aprovar resultados que são retornados de ativos ou definir como você deseja que o sistema responda aos resultados não aprovados.

Você pode usar os resultados para avaliar os casos de risco para cenários de segurança variados, por exemplo:

- Avalie se os usuários usaram protocolos proibidos para se comunicar.
- Avalie se os usuários, em redes específicas, podem se comunicar com redes ou ativos proibidos.
- Avalie se as regras de firewall atendem à política corporativa.
- Priorize vulnerabilidades avaliando quais sistemas podem ser comprometidos como resultado de uma configuração de rede.

Perguntas do Monitor de Política

É possível definir as perguntas no Monitor de política para avaliar e monitorar o risco com base na atividade de rede, nas vulnerabilidades e nas regras de firewall.

Ao enviar uma pergunta, a procura de topologia é baseada no tipo de dados selecionado:

- Para perguntas baseadas em ativos, a procura é baseada nos ativos da rede que violaram uma política definida ou nos ativos que introduziram risco na rede.
- Para perguntas baseadas em dispositivos/regras, a procura identifica as regras em um dispositivo que violaram uma política definida ou que introduziram risco na rede.
- Se uma pergunta é baseada na conformidade do ativo, a procura identifica se um ativo está em conformidade com uma referência do CIS.

Nota: Se tiver configurado o IBM Security QRadar para diversos domínios, as perguntas de ativos monitorarão apenas os ativos em seu domínio padrão. As perguntas de conformidade de ativos monitoram ativos em seu domínio padrão a menos que você tenha configurado outro domínio na janela **Admin** > **Gerenciamento de Domínio**. Para obter informações adicionais sobre gerenciamento de domínio, consulte o *IBM Security QRadar SIEM Administration Guide*.

Perguntas de dispositivos/regras procuram violações em regras e políticas e não têm componentes de teste restritivo. Também é possível fazer perguntas de dispositivos/regras para aplicativos.

Os testes de recurso são divididos nestas categorias:

- Um *teste de contribuição* usa os parâmetros da pergunta para examinar os indicadores de risco especificados na pergunta. Os resultados dos dados de risco são gerados, os quais podem ser filtrados ainda mais usando um *teste restritivo*. Os testes de contribuição são mostrados na área **Quais testes você deseja incluir em sua pergunta**. Testes de contribuição retornam dados com base em ativos detectados que correspondem à pergunta de teste.
- Um *teste restritivo* limita os resultados retornados por uma pergunta do *teste de contribuição*. Os testes restritivos são exibidos somente na área **Quais testes você deseja incluir em sua pergunta** depois da inclusão de um teste de contribuição. É possível incluir os testes restritivos somente após a inclusão de um teste de contribuição na pergunta. Se você remover ou excluir uma pergunta de teste de contribuição, a pergunta do teste restritivo não poderá ser salva.

As perguntas de conformidade do ativo procuram ativos que não estão em conformidade com as referências do CIS. Os testes que são incluídos na referência do CIS são configurados com o Editor de referência de conformidade.

Tarefas relacionadas:

"Enviando uma pergunta" na página 45
Você envia uma pergunta para determinar o risco associado. Também é possível determinar o tempo que é necessário para executar uma pergunta e a quantidade de dados que é consultada.

"Editando uma referência de conformidade" na página 47
Use o Editor de referência de conformidade no IBM Security QRadar Risk Manager para incluir ou remover testes das referências do CIS padrão.

Fator de importância

O Fator de Importância é usado para calcular a Pontuação de Risco e definir o número de resultados retornados para uma pergunta.

O intervalo é de 1 (baixa importância) a 10 (alta importância). O padrão é 5.

Tabela 9. Matriz de resultados do fator de importância

Fator de Importância	Resultados Retornados para Testes de Ativo	Resultados Retornados para Testes de Dispositivo/Regra
1 (baixa importância)	10,000	1,000
10 (alta importância)	1	1

Por exemplo, uma pergunta de política que diz **comunicação aceita a partir da Internet e incluir apenas as seguintes redes (DMZ)** exigiria um fator de importância alta de 10, pois qualquer resultado para a pergunta é inaceitável devido à natureza de alto risco da pergunta. No entanto, uma pergunta de política que diz comunicação aceita a partir da Internet e incluir apenas os seguintes aplicativos de entrada (P2P) pode requerer um fator de importância inferior, já que os resultados da pergunta não indicam alto risco, mas deve-se monitorar essa comunicação para propósitos informativos.

Visualizar informações de pergunta

É possível visualizar informações sobre perguntas do Monitor de Política e parâmetros na página Monitor de Política.

Se desejar visualizar mais informações sobre qualquer pergunta, é possível selecionar a pergunta para visualizar sua descrição.

Se uma pergunta estiver no monitor mode quando você selecioná-la, é possível visualizar os eventos e ofensas que são gerados como resultado da pergunta selecionada.

Criando uma pergunta de ativo

Procure ativos na rede que violam uma política definida ou ativos que introduziram risco.

Sobre Esta Tarefa

As perguntas do Monitor de política são avaliadas de cima para baixo. A ordem das perguntas do Monitor de política impacta os resultados.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. No menu **Ações**, selecione **Nova pergunta do ativo**.
4. No campo **Como deseja nomear esta pergunta**, digite um nome para a pergunta.
5. Na lista **Avaliar em**, selecione uma das opções a seguir:

Opção	Descrição
Comunicação Real	Inclui quaisquer ativos nos quais as comunicações que usam conexões foram detectadas.
Os de Comunicação	Inclui todos os ativos nos quais as comunicações são permitidas por meio de sua topologia de rede, como firewalls. Use essas perguntas para investigar se comunicações específicas são possíveis, independentemente de se uma comunicação foi detectada.

6. Na lista **Fator de importância**, selecione o nível de importância que você deseja associar a essa pergunta. O Fator de Importância é usado para calcular a Pontuação de Risco e definir o número de resultados retornados para uma pergunta.
7. Especifique o intervalo de tempo para a pergunta.
8. No campo **Quais testes você deseja incluir em sua pergunta**, selecione o ícone de inclusão (+) ao lado dos testes que você deseja incluir.
9. Configure os parâmetros para seus testes no campo **Localizar ativos que**.

   Parâmetros configuráveis são negrito e sublinhado. Clique em cada parâmetro para visualizar as opções disponíveis para sua pergunta.
10. Na área de grupos, clique nas caixas de seleção relevantes para designar uma associação ao grupo para essa pergunta.
11. Clique em **Salvar Pergunta**.

O que Fazer Depois

Envie uma pergunta para determinar o fator de risco. Consulte “Enviando uma pergunta” na página 45.

Conceitos relacionados:

“Fator de importância” na página 43
O Fator de Importância é usado para calcular a Pontuação de Risco e definir o número de resultados retornados para uma pergunta.

“Agrupar perguntas” na página 58
É possível agrupar e visualizar suas perguntas com base em seus critérios escolhidos

Criando uma pergunta testada para regras em dispositivos

Crie uma pergunta de dispositivos/regras no Monitor de política para identificar as regras em um dispositivo que violaram uma política definida ou que introduziram risco na rede.

Sobre Esta Tarefa

As perguntas do Monitor de política são avaliadas de cima para baixo. A ordem das perguntas do Monitor de política impacta os resultados.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.

3. No menu **Ações**, clique em **Nova pergunta de dispositivo/regras**.
4. No campo **Como deseja nomear esta pergunta**, digite um nome para a pergunta.
5. Na lista **Fator de importância**, selecione o nível de importância que você deseja associar a essa pergunta.
6. No campo **Quais testes você deseja incluir em sua pergunta**, selecione no ícone + ao lado dos testes que você deseja incluir.
7. No campo **Localizar dispositivos/regras que**, configure os parâmetros para seus testes.

   Parâmetros configuráveis são negrito e sublinhado. Clique em cada parâmetro para visualizar as opções disponíveis para sua pergunta.
8. Na área de grupos, clique nas caixas de seleção relevantes para designar uma associação ao grupo para essa pergunta.
9. Clique em **Salvar Pergunta**.

O que Fazer Depois

Envie uma pergunta para determinar o fator de risco.

Conceitos relacionados:

"Fator de importância" na página 43
O Fator de Importância é usado para calcular a Pontuação de Risco e definir o número de resultados retornados para uma pergunta.

"Agrupar perguntas" na página 58
É possível agrupar e visualizar suas perguntas com base em seus critérios escolhidos

Tarefas relacionadas:

"Enviando uma pergunta"
Você envia uma pergunta para determinar o risco associado. Também é possível determinar o tempo que é necessário para executar uma pergunta e a quantidade de dados que é consultada.

Enviando uma pergunta

Você envia uma pergunta para determinar o risco associado. Também é possível determinar o tempo que é necessário para executar uma pergunta e a quantidade de dados que é consultada.

Sobre Esta Tarefa

Quando você envia uma pergunta, as informações resultantes dependem dos dados que são consultados; ativos ou dispositivos e regras.

Depois de uma pergunta do Monitor de Política ser enviada, é possível visualizar quanto tempo a pergunta leva para ser executada. O tempo que é necessário para executar a política também indica a quantidade de dados que é consultada. Por exemplo, se o tempo de execução for 3 horas, haverá 3 horas de dados. É possível visualizar o tempo na coluna **Tempo de Execução da Política** para determinar uma frequência de intervalo eficiente para configurar para as perguntas que você deseja monitorar. Por exemplo, se o tempo de execução de política for de 3 horas, o intervalo da avaliação da política deverá ser maior que 3 horas.

Nota: Quando você edita uma pergunta depois de ela ser enviada, a edição afeta testes associados, então talvez leve-se até uma hora para se visualizar essas mudanças.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. Selecione a pergunta que deseja enviar.
4. Clique em **Enviar Pergunta**.

Criando uma pergunta de conformidade do ativo

Crie uma pergunta de conformidade do ativo no Monitor de política para procurar ativos na rede que falharam nos testes de referência do CIS.

Antes de Iniciar

As perguntas do Monitor de política são avaliadas de cima para baixo. A ordem das perguntas do Monitor de política impacta os resultados.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. No menu **Ações**, selecione **Nova pergunta de conformidade do ativo**.
4. No campo **Como deseja nomear esta pergunta**, digite um nome para a pergunta.
5. Selecione o nível de importância que deseja associar a essa pergunta na lista **Fator de importância**.
6. No campo **Quais testes você deseja incluir em sua pergunta**, selecione o ícone de inclusão (+) ao lado do teste **conformidade do teste dos ativos nas procuras salvas do ativo com as referências do CIS**.

   Selecione esse teste várias vezes, se necessário.
7. Configure os parâmetros para seus testes no campo **Localizar ativos que**.

   Clique em cada parâmetro para visualizar as opções disponíveis para sua pergunta. Especifique várias procuras salvas de ativos e várias listas de verificação nesse teste, se necessário.
8. Na área do grupo, clique nas caixas de seleção relevantes para designar uma associação ao grupo para essa pergunta.

   As perguntas de conformidade do ativo devem ser designadas a um grupo para inclusão nos relatórios ou nos painéis de conformidade.
9. Clique em **Salvar Pergunta**.

O que Fazer Depois

Associe um perfil de referência à pergunta criada e monitore os resultados dela.

Conceitos relacionados:

"Fator de importância" na página 43
O Fator de Importância é usado para calcular a Pontuação de Risco e definir o número de resultados retornados para uma pergunta.

"Agrupar perguntas" na página 58
É possível agrupar e visualizar suas perguntas com base em seus critérios

escolhidos

Tarefas relacionadas:

"Monitorando perguntas de conformidade do ativo"
Monitore as perguntas de conformidade do ativo selecionando os perfis de varredura do CIS. As varreduras de referência do CIS são executadas com relação aos ativos.

Editando uma referência de conformidade

Use o Editor de referência de conformidade no IBM Security QRadar Risk Manager para incluir ou remover testes das referências do CIS padrão.

Procedimento

1. Clique na guia **Riscos**.
2. Clique em **Monitor de política**.
3. Clique em **Conformidade** para abrir a janela Editor de referência de conformidade.
4. No menu de navegação, clique na referência do CIS padrão que você deseja editar.
5. No painel **Conformidade**, clique na caixa de seleção **Ativado** na linha designada ao teste que você deseja incluir.

   Clique em qualquer lugar em uma linha para ver uma descrição do teste de referência, uma lógica de implementação e informações sobre o que verificar antes de ativar o teste.

   Ao construir uma lista de verificação do CIS customizada, esteja ciente de que alguns testes de referência que não estão incluídos por padrão podem demorar bastante tempo para serem executados. Para obter mais informações, consulte a documentação do CIS.

O que Fazer Depois

Crie uma pergunta de conformidade do ativo para testar os ativos com relação à referência que você editou.

Tarefas relacionadas:

"Criando uma pergunta de conformidade do ativo" na página 46
Crie uma pergunta de conformidade do ativo no Monitor de política para procurar ativos na rede que falharam nos testes de referência do CIS.

Monitorando perguntas de conformidade do ativo

Monitore as perguntas de conformidade do ativo selecionando os perfis de varredura do CIS. As varreduras de referência do CIS são executadas com relação aos ativos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. No painel **Perguntas**, selecione a pergunta de conformidade do ativo que você deseja monitorar.
4. Clique em **Monitor** para abrir a janela Resultados do monitor.
5. Selecione um perfil de referência na lista **Qual perfil de referência associar a essa pergunta?**.

O perfil de varredura de referência selecionado usa um scanner QRadar Vulnerability Manager que está associado a um domínio. O nome do domínio é exibido na área **Detalhes do Perfil de Referência**. Para obter informações adicionais sobre gerenciamento de domínio, consulte o *IBM Security QRadar SIEM Administration Guide*.

6. Selecione a caixa de seleção **Ativar a função de resultados do monitor para essa pergunta/simulação**.
7. Clique em **Salvar Monitor**.

Tarefas relacionadas:

"Editando uma referência de conformidade" na página 47
Use o Editor de referência de conformidade no IBM Security QRadar Risk Manager para incluir ou remover testes das referências do CIS padrão.

"Criando uma pergunta de conformidade do ativo" na página 46
Crie uma pergunta de conformidade do ativo no Monitor de política para procurar ativos na rede que falharam nos testes de referência do CIS.

Exportar e importar perguntas do monitor de política

Os usuários com privilégios administrativos podem exportar e importar perguntas do Monitor de Política.

A exportação e a importação de perguntas fornecem um método para fazer backup de perguntas e compartilhar perguntas com outros usuários do IBM Security QRadar Risk Manager.

Restrições para informações confidenciais

As informações confidenciais de política ou da empresa podem ser incluídas em dependências. Quando você exporta ou importa perguntas do Monitor de Política, os dados sensíveis contidos nas dependências não são incluídos.

As perguntas do Monitor de Política devem conter os seguintes tipos de dependências:

- Blocos de construção de ativos
- Procuras salvas de ativos
- Redes
- Locais de rede remota
- Locais de rede geográficos
- Conjuntos de referência

Antes de exportar as perguntas que têm dependências, deve-se optar por fornecer mais contexto sobre o tipo de informações que estão contidas na dependência. O fornecimento dessa informação permite que outros usuários entendam qual tipo de informação referenciar ao importar a pergunta em seu Monitor de Política.

Exportando perguntas do monitor de política

É possível exportar uma ou mais perguntas do monitor de política para um arquivo XML. A exportação de perguntas do monitor de política é útil para fazer backup de suas perguntas ou compartilhar perguntas com outros usuários.

Sobre Esta Tarefa

Se qualquer pergunta do monitor de política contiver dependências, é possível fornecer mais contexto sobre o tipo de informações que estão contidas na dependência.

O nome do arquivo XML padrão para as perguntas exportadas é `policy_monitor_questions_export.xml`.

Procedimento

1. Na guia **Riscos**, clique em **Monitor de Política**.
2. Escolha uma das opções a seguir:
   - Para exportar todas as perguntas, no menu **Ações**, selecione **Exportar Todos**.
   - Para exportar perguntas de seleção, pressione a tecla Ctrl para selecionar cada pergunta que deseja exportar e, em seguida, no menu **Ações**, selecione **Exportar Selecionado**.
3. Opcional. Se alguma pergunta contiver dependências, clique no link do parâmetro para digitar informações mais específicas. O comprimento máximo de caracteres para esse campo é 255.
4. Clique em **Exportar Perguntas**.

Resultados

Um arquivo padrão, chamado `policy_monitor_questions_export.xml`, é exportado para o diretório de download.

Importando perguntas do monitor de política

É possível importar uma ou mais perguntas do monitor de política para o IBM Security QRadar Risk Manager.

Sobre Esta Tarefa

O processo de importação não atualiza perguntas existentes; cada pergunta é exibida como uma nova pergunta no monitor de política. Um registro de data e hora é incluído, como um sufixo, para todas as perguntas importadas.

Após você importar perguntas do monitor de política, um aviso será exibido na coluna **Status** se uma pergunta importada contiver uma dependência. Perguntas importadas com dependências contêm parâmetros sem valores. Para assegurar que as perguntas do monitor de política importadas funcionem como esperado, você deverá designar valores aos parâmetros vazios.

Procedimento

1. Na guia **Riscos**, clique em **Monitor de Política**.
2. No menu **Ações**, selecione **Importar**.
3. Clique em **Escolher Arquivo** e, em seguida, navegue para selecionar o arquivo XML que você deseja importar.
4. Clique em **Abrir**.
5. Selecione um ou mais grupos para designar a pergunta a um grupo.
6. Clique em **Importar Pergunta**.

7. Verifique a coluna **Status** para avisos. Se uma pergunta contiver um aviso, abra a pergunta e edite os parâmetros dependentes. É possível salvar a pergunta após os parâmetros serem concluídos.

O que Fazer Depois

O monitoramento é desativado para perguntas importadas. É possível criar um evento para monitorar os resultados das perguntas que foram importadas.

Resultados do ativo

Resultados do ativo são exibidos após o envio de uma pergunta do monitor de política.

Os parâmetros para os resultados do ativo são descritos na tabela a seguir.

Tabela 10. Resultados do ativo

Parâmetro	Descrição
Pontuação de Risco	A pontuação de risco é calculada com base no número de resultados e no Fator de Importância designado a esta pergunta. A pontuação de risco indica o nível de risco associado a esta pergunta.
IP	O endereço IP do ativo.
Nome	O nome do ativo, conforme obtido do perfil do ativo. Para obter informações adicionais sobre perfis de ativos, consulte o *IBM Security QRadar SIEM Users Guide*
Peso	O peso do ativo, conforme obtido do perfil do ativo.
Porta(s) de Destino	A lista de portas de destino associada a este ativo, no contexto dos testes de pergunta. Se houver várias portas associadas a esse ativo e essa pergunta, este campo indicará Vários e o número de várias portas. A lista de portas é obtida pela filtragem das conexões associadas a essa pergunta para obter todas as portas exclusivas em que o ativo foi a origem, o destino ou a conexão. Clique em Vários (N) para visualizar as conexões. Essa tela fornece as conexões agregadas por porta, filtradas pelo endereço IP do ativo e baseadas no intervalo de tempo especificado na pergunta.

Tabela 10. Resultados do ativo (continuação)

Parâmetro	Descrição
Protocolo(s)	A lista de protocolos associados a esse ativo, no contexto dos testes de pergunta. Se houver vários protocolos associados a esse ativo e essa pergunta, este campo indicará Vários e o número de protocolos. A lista de protocolos é obtida pela filtragem das conexões associadas a essa pergunta para obter todos os protocolos exclusivos em que o ativo foi a origem, o destino ou a conexão. Clique em Vários (N) para visualizar as Conexões. Essa tela fornece as conexões agregadas por protocolo, filtradas pelo endereço IP do ativo e baseadas no intervalo de tempo especificado na pergunta.
App(s) de Fluxo	A lista de aplicativos associados a esse ativo, no contexto dos testes de pergunta. Se houver vários aplicativos associados a esse ativo e essa pergunta, este campo indicará Vários e o número de aplicativos. A lista de aplicativos é obtido pela filtragem das conexões associadas a essa pergunta para obter todos os aplicativos exclusivos em que o ativo foi a origem, o destino ou a conexão. Clique em Vários (N) para visualizar as Conexões. Essa tela fornece as conexões agregadas pelo aplicativo, filtradas pelo endereço IP do ativo e baseadas no intervalo de tempo especificado na pergunta.
Vuln(s)	A lista de vulnerabilidades associadas a esse ativo, no contexto dos testes de pergunta. Se houver várias vulnerabilidades associadas a esse ativo e essa pergunta, este campo indicará Vários e o número de vulnerabilidades. A lista de vulnerabilidades é obtida usando uma lista de todas as vulnerabilidades compilada a partir de testes relevantes e usando essa lista para filtrar as vulnerabilidades detectadas nesse ativo. Se nenhuma vulnerabilidade for especificada para essa pergunta, todas as vulnerabilidades no ativo serão usadas para compilar essa lista. Clique em Vários (N) para visualizar os Ativos. Essa tela fornece as conexões agregadas por vulnerabilidade, filtradas pelo endereço IP do ativo e baseadas no intervalo de tempo especificado na pergunta.

Tabela 10. Resultados do ativo (continuação)

Parâmetro	Descrição
Contagem de Fluxo	A contagem de fluxo total associada a esse ativo, no contexto dos testes de pergunta. A contagem de fluxo é determinada pela filtragem das conexões associadas a essa pergunta para obter a contagem total de fluxo em que o ativo foi a origem, o destino ou a conexão.
Origem(ns)	A lista de endereços IP de origem associados a esse ativo, no contexto dos testes de pergunta. Se houver vários endereços IP de origem associados a esse ativo e essa pergunta, esse campo indicará Vários e o número de endereços IP de origem. A lista de endereços IP de origem é obtida pela filtragem das conexões associadas a essa pergunta para obter todos os endereços IP de origem exclusivos em que o ativo é o destino da conexão. Clique em Vários (N) para visualizar as Conexões. Essa tela fornece as conexões agregadas por endereço IP de origem filtradas pelo endereço IP do ativo com base no intervalo de tempo especificado na pergunta.
Destino(s)	A lista de endereços IP de destino associados a esse ativo, no contexto dos testes de pergunta. Se houver vários endereços IP de destino associados a esse ativo e essa pergunta, esse campo indicará Vários e o número de testes de pergunta. A lista de endereços IP de destino é obtida pela filtragem das conexões associadas a essa pergunta para obter todos os endereços IP de destino exclusivos em que o ativo é a origem da conexão. Clique em Vários (N) para visualizar as Conexões. Essa tela fornece as conexões agregadas por endereço IP de destino filtradas pelo endereço IP do ativo com base no intervalo de tempo especificado na pergunta.
Bytes de Fonte de Fluxo	O total de bytes de origem associado a esse ativo, no contexto dos testes de pergunta. Os bytes de origem são determinados pela filtragem das conexões associadas a essa pergunta para obter o total de bytes de origem em que o ativo é a origem da conexão.

Tabela 10. Resultados do ativo (continuação)

Parâmetro	Descrição
Bytes de Destino do Fluxo	O total de bytes de destino associado a esse ativo, no contexto do teste de pergunta. Os bytes de destino são determinados pela filtragem das conexões associadas a essa pergunta para obter o total de bytes de destino em que o ativo é o destino da conexão.

Resultados do dispositivo

Os resultados do dispositivo são exibidos após você enviar uma pergunta do monitor de política.

Os parâmetros para resultados de dispositivos e regras são descritos na tabela a seguir.

Tabela 11. Resultados de dispositivos e regras

Parâmetro	Descrição
Pontuação de Risco	O nível de risco associado a esta pergunta. A pontuação de risco é calculada com base no número de resultados e Fator de Importância designados a esta pergunta. O cálculo é baseado nos seguintes valores: • O peso de ativo dos ativos/dispositivos retornados nos resultados de uma pergunta. • O fator de importância da pergunta. • O número de resultados retornados como resultado da pergunta.
IP do Dispositivo	O endereço IP do dispositivo.
Nome do Dispositivo	O nome do dispositivo, conforme obtido do monitor de configuração.
Tipo do Dispositivo	O tipo de dispositivo, conforme obtido do perfil do ativo. Para obter informações adicionais sobre perfis de ativos, consulte o *IBM Security QRadar SIEM Users Guide*.
Lista	O nome da regra do dispositivo.
Entrada	O número de entrada da regra.
Ação	A ação associada à regra relevante do dispositivo. As opções são: permitir, negar ou ND.

Tabela 11. Resultados de dispositivos e regras (continuação)

Parâmetro	Descrição

Serviço(s) de Origem	As portas de origem e a comparação associadas à regra relevante do dispositivo no seguinte formato:
	`<comparison>:<port>`
	Em que
	`<comparison>`
	poderia incluir uma das seguintes opções:
	• eq - Equal
	• ne - Not equal
	• lt - Less than
	• gt - Greater than
	Por exemplo, se o parâmetro indicar ne:80, qualquer porta diferente de 80 se aplicará a esse serviço de origem. Se o parâmetro indicar lt:80, o intervalo de portas aplicáveis será de 0 a 79.
	Esse parâmetro exibe a porta de origem para a regra do dispositivo. Se nenhuma porta existir para essa regra de dispositivo, o termo ND será exibido.
	Os serviços de origem com um hyperlink indicam uma referência do grupo de objetos. Clique no link para visualizar informações detalhadas sobre referência(s) do grupo de objetos.

Tabela 11. Resultados de dispositivos e regras (continuação)

Parâmetro	Descrição

Serviço(s) de Destino	As portas de destino e a comparação associadas à regra relevante do dispositivo são exibidas no seguinte formato:
	`<comparison>:<port>`
	Em que
	`<comparison>`
	pode incluir uma das seguintes opções:
	• eq - Equal
	• ne - Not equal
	• lt - Less than
	• gt - Greater than
	Por exemplo, se o parâmetro indicar ne:80, qualquer porta diferente de 80 se aplicará a esse serviço de destino. Se o parâmetro indicar lt:80, o intervalo de portas aplicáveis será de 0 a 79.
	Esse parâmetro exibe a porta de origem para a regra do dispositivo. Se nenhuma porta existir para essa regra de dispositivo, o termo ND será exibido.
	Os serviços de destino com um hyperlink indicam uma referência do grupo de objetos. Clique no link para visualizar informações detalhadas sobre referência(s) do grupo de objetos.

Origem(ns)	A rede de origem associada a este ativo. Origens com um hyperlink indicam uma referência do grupo de objetos. Clique no link para visualizar informações detalhadas sobre referência(s) do grupo de objetos.
Destino(s)	A rede de destino associada à regra relevante do dispositivo. Destinos com um hyperlink indicam uma referência do grupo de objetos. Clique no link para visualizar informações detalhadas sobre referência(s) do grupo de objetos.
Protocolo(s)	O protocolo ou grupo de protocolos associados à regra relevante do dispositivo.
Assinatura(s)	A assinatura para esse dispositivo, que é exibida apenas para uma regra de dispositivo em um dispositivo IP.

Avaliar resultados das perguntas do Monitor de Política

É possível avaliar os resultados que são retornados a partir de uma pergunta do Monitor de Política.

A aprovação do resultado de uma pergunta é semelhante ao ajuste do sistema para informar o IBMIBM Security QRadar Risk Manager que o ativo associado ao resultado da pergunta é seguro ou pode ser ignorado no futuro.

Quando um usuário aprova um resultado de ativo, o Monitor de Política vê esse resultado de ativo como aprovado, e quando a a pergunta do Monitor de Política é enviada ou monitorada no futuro, o ativo não é listado nos resultados da pergunta. O ativo aprovado não é exibido na lista de resultados para a pergunta, a menos que a aprovação seja revogada. O Monitor de Política registra o usuário, endereço IP do dispositivo, motivo para aprovação, Dispositivo/Regra aplicável e data e hora para os administradores de segurança da rede.

Aprovar resultados

É possível avaliar a lista de ativos ou regras do dispositivo retornada para determinar o nível de risco envolvido. Após a avaliação, deve-se aprovar todos os resultados ou resultados específicos.

Procedimento

1. Na tabela de resultados, selecione a caixa de seleção ao lado dos resultados que você deseja aceitar.
2. Escolha uma das opções a seguir:

Opção	Descrição
Aprovar Todos	Selecione esta opção para aprovar todos os resultados.
Aprovar Selecionado	Selecione a caixa de seleção ao lado dos resultados que você deseja aprovar e clique em Aprovar selecionado.

3. Digite o motivo para aprovação.
4. Clique em **OK**.
5. Clique em **OK**.
6. Para visualizar os resultados aprovados para a pergunta, clique em **Visualizar Aprovado**.

Resultados

A janela Resultados da Pergunta Aprovados fornece as seguintes informações:

Tabela 12. Parâmetros de resultados da pergunta aprovados

Parâmetro	Descrição
Dispositivo/Regra	Para obter o resultado de uma pergunta de Dispositivo/Regra, isso indica o dispositivo associado a esse resultado.
IP	Para obter o resultado de uma pergunta de ativo, isso indica o endereço IP associado ao ativo.
Aprovado por	O usuário que aprovou os resultados.
Aprovado em	A data e hora em que os resultados foram aprovados.

Tabela 12. Parâmetros de resultados da pergunta aprovados (continuação)

Parâmetro	Descrição
Notas	Exibe o texto de notas associadas a esse resultado e o motivo pelo qual a pergunta foi aprovada.

Se desejar remover aprovações para quaisquer resultados, selecione a caixa de seleção para cada resultado para o qual deseja remover a aprovação e clique em **Revogar Selecionado**. Para remover todas as aprovações, clique em **Revogar Todos**.

Perguntas do monitor

Se você deseja gerar um evento quando os resultados de uma pergunta mudam, é possível configurar uma pergunta para ser monitorada.

Quando você seleciona uma pergunta para ser monitorada, o IBM Security QRadar Risk Manager analisa continuamente a pergunta para determinar se os resultados dela mudam. Se o QRadar Risk Manager detectar uma mudança de resultado, uma ofensa poderá ser gerada para alertá-lo sobre um desvio em sua política definida.

Uma pergunta no monitor mode é padronizada para um intervalo de tempo de 1 hora. Esse valor substitui o valor de tempo que é configurado quando a pergunta foi criada.

Criando um evento para monitorar resultados

É possível criar um evento para monitorar resultados de perguntas que foram criadas no Monitor de Política.

Sobre Esta Tarefa

Os parâmetros que você configura para um evento são descritos na tabela a seguir.

Tabela 13. Parâmetros para monitorar resultados da pergunta

Parâmetro	Descrição
Intervalo de avaliação da política	A frequência para o evento ser executado.
Nome do Evento	O nome do evento que você deseja exibir nas guias **Atividade do Log** e **Ofensas**.
Descrição do Evento	A descrição para o evento. A descrição é exibida em Anotações nos detalhes do evento.
Categoria de Alto Nível	A categoria de evento de alto nível que você deseja que esta regra use ao processar eventos.
Categoria de Baixo Nível	A categoria de evento de baixo nível que você deseja que esta regra use ao processar eventos.

Tabela 13. Parâmetros para monitorar resultados da pergunta (continuação)

Parâmetro	Descrição
Assegure-se de que o evento de dispatch faça parte de uma ofensa	Encaminha eventos para o componente Funcionários Públicos. Se nenhuma ofensa foi gerada, uma nova será criada. Se uma ofensa existir, o evento será incluído. Se você correlacionar por pergunta ou simulação, todos os eventos de uma pergunta serão associados a uma única ofensa. Se você correlacionar por ativo, uma ofensa exclusiva será criado ou atualizada para cada ativo exclusivo.
Dispatch de eventos aprovados da pergunta	Encaminha eventos que aprovam a pergunta do monitor de política para o componente Funcionários Públicos.
Ajustes de Pontuação de Vulnerabilidades	Ajusta a pontuação de risco de vulnerabilidade de um ativo, dependendo se a pergunta for aprovada ou falhar. As pontuações de risco de vulnerabilidade são ajustadas no IBM Security QRadar Vulnerability Manager.
Ações Adicionais	As ações adicionais a serem tomadas quando um evento é recebido. Separe vários endereços de email usando uma vírgula. Selecione **Notificação** se você desejar que os eventos gerados como resultado dessa pergunta monitorada exibam eventos no item Notificações do Sistema no painel. A saída syslog pode se parecer com: `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`
Ativar Monitor	Monitore a pergunta.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. Selecione a pergunta que deseja monitorar.
4. Clique em **Monitor**.
5. Configure valores para os parâmetros.
6. Clique em **Salvar Monitor**.

Agrupar perguntas

É possível agrupar e visualizar suas perguntas com base em seus critérios escolhidos

A categorização de suas perguntas permite visualizar e controlar de modo eficiente suas perguntas. Por exemplo, é possível visualizar todas as perguntas relacionadas à conformidade.

Conforme você cria novas perguntas, é possível designar a pergunta a um grupo existente.

Visualizando grupos

É possível visualizar um grupo de perguntas.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. Na lista **Grupo**, selecione o grupo que você deseja visualizar.

Criando um grupo

É possível criar um novo grupo para perguntas.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. Clique em **Grupos**.
4. Na árvore de menus, selecione o grupo sob o qual deseja criar um novo grupo.
5. Clique em **Novo**.
6. No campo **Nome**, especifique o nome que deseja designar ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
7. No campo **Descrição**, especifique uma descrição que deseja designar a esse grupo. A descrição pode ter até 255 caracteres de comprimento.
8. Clique em **OK**.
9. Se desejar alterar o local do novo grupo, clique no novo grupo e arraste a pasta para o local escolhido em sua árvore de menu.

Editando um grupo

É possível editar um grupo de perguntas.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione o grupo que deseja editar.
5. Clique em **Editar**.
6. Edite o **Nome** e **Descrição**, conforme necessário.

   Os campos de nome e descrição podem ter no máximo 255 caracteres.
7. Clique em **OK**.
8. Se desejar alterar o local do grupo, selecione o grupo e arraste a pasta para o local preferido na árvore de menu.
9. Feche a janela Grupos.

Copiando um item em outro grupo

Usando a funcionalidade de grupos, é possível copiar uma simulação em um ou vários grupos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.

3. Clique em **Grupos**.
4. Na árvore de menu, selecione a pergunta que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo no qual deseja copiar a simulação.
7. Clique em **Copiar**.

Excluindo um item de um grupo

É possível excluir um item de um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione o grupo de nível superior.
5. Na lista de grupos, selecione o item ou grupo que deseja excluir.
6. Clique em **Remover**.
7. Clique em **OK**.

Designando um item a um grupo

É possível designar uma pergunta a um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. Selecione a pergunta você deseja designar a um grupo.
4. Usando o menu **Ações**, selecione **Designar Grupos**.
5. Selecione o grupo ao qual você deseja que a pergunta seja designada.
6. Clique em **Designar Grupos**.

Integração do IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager

O IBM Security QRadar Vulnerability Manager se integra ao QRadar Risk Manager para ajudá-lo a priorizar os riscos e vulnerabilidades na rede.

Políticas de Risco e Priorização de Vulnerabilidade

É possível integrar-se ao QRadar Vulnerability Manager QRadar Risk Manager, definindo e monitorando as políticas de risco de ativo ou de vulnerabilidade.

Se transmitir ou falhar as políticas de risco definidas no QRadar Risk Manager, as pontuações de risco de vulnerabilidade no QRadar Vulnerability Manager serão ajustadas. Os níveis de ajuste dependem das políticas de risco na organização.

Ao ajustar as pontuações de risco de vulnerabilidade no QRadar Vulnerability Manager, os administradores poderão executar as tarefas a seguir:

- Ganhar visibilidade imediata das vulnerabilidades que falharam uma política de risco.

  Por exemplo, novas informações podem ser exibidas no painel do QRadar ou enviadas usando o email.

- Priorize novamente as vulnerabilidades que requerem atenção imediata.

  Por exemplo, um administrador pode usar a **Pontuação de Risco** para identificar rapidamente as vulnerabilidades de alto risco.

Se você aplicar as políticas de risco em um nível de ativo no QRadar Risk Manager, todas as vulnerabilidades neste ativo terão as pontuações de riscos ajustadas.

Casos de uso do Monitor de Política

Muitas opções estão disponíveis quando você cria perguntas para analisar sua rede em termos de riscos.

Os exemplos de Monitor de Política a seguir descrevem os casos de uso comuns que podem ser usados em seu ambiente de rede.

Comunicação real para protocolos permitidos por DMZ

Este caso de uso demonstra como criar uma pergunta do Monitor de política com base na lista conhecida de protocolos confiáveis para DMZ. Na maioria das organizações, o tráfego de rede cruzando a DMZ é restrito aos protocolos bem conhecidos e confiáveis, como HTTP ou HTTPS em portas especificadas.

Sobre Esta Tarefa

A partir de uma perspectiva de risco, é importante monitorar continuamente o tráfego na DMZ para assegurar que apenas os protocolos confiáveis estejam presentes. O IBM Security QRadar Risk Manager realiza isso criando uma pergunta do Monitor de Política baseada em um teste de ativo para comunicações reais.

Existem várias maneiras das quais uma pergunta do Monitor de Política pode ser gerada para esse objetivo de caso de uso. Como sabemos que a política de rede permite apenas alguns protocolos confiáveis, selecionamos uma opção para criar nossa pergunta do Monitor de Política com base na lista conhecida de protocolos confiáveis para DMZ.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. No menu **Ações**, selecione **Novo**.
4. No campo **Como você deseja nomear esta pergunta**, digite um nome para a pergunta.
5. Na lista suspensa **Qual o tipo de dados que você deseja retornar**, selecione Ativos.
6. Na lista suspensa **Avaliar em, selecione Comunicação Real.**
7. Na lista suspensa **Fator de Importância**, especifique um nível de importância para associar a sua pergunta.
8. Na seção **Intervalo de Tempo**, especifique um intervalo de tempo para a pergunta.
9. Na seção **Quais testes deseja incluir em sua pergunta**, selecione **comunicação aceita para redes de destino**.
10. Na seção **Localizar ativos que**, clique em **redes de destino** para configurar mais esse teste e especificar seu DMZ como a rede de destino.

11. Selecione **e incluir as seguintes portas de entrada**.
12. Na seção **Localizar Ativos que**, clique no parâmetro incluir apenas para que ele muda para excluir. O parâmetro agora é exibido e exclui as seguintes portas de entrada.
13. Clique em **portas**.
14. Inclua as portas 80 e 443 e, em seguida, clique em **OK**.
15. Clique em **Salvar Pergunta**.
16. Selecione a pergunta da DMZ do Monitor de Política que você criou.
17. Clique em **Enviar Pergunta**.
18. Revise os resultados para ver se algum outro protocolo além das portas 80 e 443 está se comunicando na rede.
19. Opcional. Após os resultados serem ajustados adequadamente, é possível monitorar sua pergunta da DMZ colocando a pergunta no modo de monitoramento.

O que Fazer Depois

É possível monitorar suas perguntas.

Teste de ativos para possível comunicação em ativos protegidos

Este caso de uso demonstra como criar uma pergunta do Monitor de Política com base no endereço IP. Todas as organizações têm redes que contêm servidores críticos em que o tráfego é monitorado e acessível apenas por funcionários confiáveis.

Sobre Esta Tarefa

A partir de uma perspectiva de risco, é importante saber quais usuários em sua organização podem se comunicar com ativos da rede crítica. IBM Security QRadar Risk Manager realiza essa tarefa criando uma pergunta do Monitor de Política baseada em um teste de ativo para possíveis comunicações.

Existem várias maneiras das quais uma pergunta do Monitor de Política pode ser gerada para esse objetivo de caso de uso. Você poderia examinar todas as conexões com o servidor crítico ao longo do tempo, mas talvez você esteja mais preocupado com o fato de os funcionários regionais não terem acesso a esses servidores críticos. Para realizar isso, é possível criar uma pergunta do Monitor de Política que consulte a topologia da rede por endereço IP.

Procedimento

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. No menu **Ações**, selecione **Novo**.
4. No campo **Como você deseja nomear esta pergunta**, digite um nome para a pergunta.
5. Na lista suspensa **Qual o tipo de dados que você deseja retornar**, selecione Ativos.
6. Na lista suspensa **Avaliar em, selecione Possível Comunicação**.

7. Na lista suspensa **Fator de Importância**, especifique um nível de importância para associar a sua pergunta.
8. Na seção **Intervalo de Tempo**, especifique um intervalo de tempo para a pergunta.
9. Na seção **Quais testes deseja incluir em sua pergunta**, dê um clique duplo para selecionar **comunicação aceita com blocos de construção do ativo de destino**.
10. Na seção Localizar Ativos que, clique em **blocos de construção do ativo** para configurar ainda mais esse teste e especifique **Ativos Protegidos**.

    Nota:

    Para definir seus ativos da rede remota, deve-se ter definido anteriormente os blocos de construção do ativo remoto.
11. Na seção **Quais testes deseja incluir em sua pergunta**, dê um clique duplo para selecionar o teste restritivo **e incluir apenas os seguintes endereços IP**.
12. Na seção Localizar Ativos que, clique em **Endereços IP**.
13. Especifique o intervalo de endereço IP ou CIDR de sua rede remota.
14. Clique em **Salvar Pergunta**.
15. Selecione a pergunta do Monitor de Política que você criou para ativos protegidos.
16. Clique em **Enviar Pergunta**.
17. Revise os resultados para ver se algum ativo protegido aceitou a comunicação a partir de um endereço IP ou intervalo CIDR desconhecido.
18. Opcional. Após os resultados serem adequadamente ajustados, é possível monitorar seus ativos protegidos colocando a pergunta no modo de monitoramento. Se um ativo protegido for conectado por um endereço IP desconhecido, o QRadar Risk Manager poderá gerar um alerta.

O que Fazer Depois

É possível monitorar suas perguntas.

Comunicação de teste de dispositivo/regra sobre o acesso à Internet

Este caso de uso demonstra como criar uma pergunta do Monitor de Política com base em regras / dispositivos. Testes de dispositivo identificam as regras em um dispositivo que violam uma política definida ou mudanças que introduziram risco no ambiente.

Sobre Esta Tarefa

Testes de dispositivo identificam as regras em um dispositivo que violam uma política definida ou mudanças que introduziram risco no ambiente. A partir de uma perspectiva de rede, é importante saber quais regras de dispositivo podem ter mudado e alertá-lo para a regra para que ela seja corrigida. Uma ocorrência muito comum é quando os servidores que não tinham acesso à Internet anteriormente recebem a concessão de acesso devido a uma mudança de firewall na rede. O IBM Security QRadar Risk Manager pode monitorar mudanças de regra em dispositivos de rede criando uma pergunta do Monitor de Política com base nas regras do dispositivo.

Existem várias maneiras das quais uma pergunta do Monitor de Política pode ser gerada para esse objetivo de caso de uso. Neste exemplo, você criará uma pergunta do Monitor de Política que procura saber quais dispositivos têm acesso à Internet.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Política**.
3. No menu **Ações**, selecione **Novo**.
4. Na lista suspensa **Qual o tipo de dados deseja retornar, selecione Dispositivos/Regras**.
5. Na lista suspensa **Fator de Importância**, especifique um nível de importância para associar a sua pergunta.
6. Na seção **Quais testes deseja incluir em sua pergunta**, dê um clique duplo para selecionar **permitir conexão com a internet**.
7. Clique em **Salvar Pergunta**.
8. Selecione a pergunta do Monitor de Política criada para monitorar as regras de dispositivo.
9. Clique em **Enviar Pergunta**.
10. Revise os resultados para ver se alguma das regras permite acesso à Internet.
11. Opcional. Após os resultados serem adequadamente ajustados, é possível monitorar seus ativos protegidos colocando a pergunta no modo de monitoramento.

O que Fazer Depois

É possível monitorar suas perguntas.

Priorizando Vulnerabilidades de Alto Risco Aplicando Políticas de Risco

No IBM Security QRadar Vulnerability Manager, é possível alertar os administradores para vulnerabilidades de risco mais alto, aplicando políticas de riscos à vulnerabilidades.

Ao aplicar uma política de risco, a pontuação de risco de uma vulnerabilidade será ajustada, permitindo aos administradores priorizar com mais precisão as vulnerabilidades que requerem atenção imediata.

Neste exemplo, a pontuação de risco de vulnerabilidade é automaticamente aumentada por um fator de porcentagem para qualquer vulnerabilidade que permanecer ativa na rede após 40 dias.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na barra de ferramentas, clique em **Procura** > **Nova Procura**.
4. Na área de janela Parâmetros de Procura, configure os filtros a seguir:
   a. **Iguais de Alto Risco**
   b. **Dias desde a descoberta das vulnerabilidades, maior ou igual a 40**
5. Clique em **Procura** e, em seguida, na barra de ferramentas, clique em **Salvar Critérios de Procura**.

Digite um nome de procura salva identificável no QRadar Risk Manager.

6. Clique na guia **Riscos**.
7. Na área de janela de navegação, clique em **Monitor de Política**.
8. Na barra de ferramentas, clique em **Ações** > **Novo**.
9. No campo **O Que Deseja para Nomear Esta Pergunta**, digite um nome.
10. No campo **Quais Testes Deseja Incluir na Pergunta**, clique em **são suscetíveis às vulnerabilidades contidas em procuras salvas de vulnerabilidade**.
11. No campo **Localizar Recursos Que**, clique no parâmetro sublinhado em **são suscetíveis às vulnerabilidades contidas em procuras salvas de vulnerabilidade**.
12. Identifique a procura salva da vulnerabilidade de alto risco do QRadar Vulnerability Manager, clique em **Incluir**, em seguida, clique em **OK**.
13. Clique em **Salvar Pergunta**.
14. Na área de janela Perguntas, selecione a pergunta na lista e, na barra de ferramentas, clique em **Monitor**.

    Restrição: O campo **Descrição do Evento** é obrigatório.
15. Clique em **Enviar Eventos Aprovados na Pergunta**.
16. No campo **Ajustes de Pontuação de Vulnerabilidade**, digite um valor de porcentagem de ajuste de risco no campo **Ajuste de Pontuação de Vulnerabilidade de Porcentagem na Falha da Pergunta**.
17. Clique em **Aplicar Ajuste a Todas as Vulnerabilidades em Um Ativo**, em seguida, clique em **Salvar Monitor**.

O que Fazer Depois

Na guia **Vulnerabilidades**, é possível procurar as vulnerabilidades de alto risco e priorizá-las

Perguntas do Monitor de Política

É possível definir perguntas de teste para identificar riscos em regras ou dispositivos de rede em dispositivos de rede.

Parâmetros específicos de teste e genéricos para testes do Monitor de Política

É possível configurar parâmetros para cada teste do Monitor de Política. Os parâmetros configuráveis são as partes em negrito e sublinhado. Você clica em um parâmetro para visualizar as opções disponíveis para sua pergunta.

Os testes do Monitor de Política usam dois tipos de parâmetros; genéricos e específicos do teste. Parâmetros genéricos oferecem 2 ou mais opções para customizar um teste. Um clique em um parâmetro genérico alterna as opções que estão disponíveis. Os parâmetros específicos de teste precisam de entrada do usuário. Você clica em parâmetros específicos de teste para especificar informações.

Por exemplo, o teste de ativo chamado **comunicação aceita com locais de rede de destino remoto** contém dois parâmetros genéricos e um parâmetro específico de teste. Clique no parâmetro genérico, **aceito**, para selecionar **aceito** ou **rejeitado**. Clique no parâmetro genérico, **para destino**, para selecionar **para destino** ou **a partir da origem**. Clique no parâmetro específico de teste, **locais de rede remota**,

para incluir um local remoto para o teste de ativo.

Perguntas de teste de ativo

Perguntas de ativo são usadas para identificar ativos na rede que violam uma política definida ou introduzem risco no ambiente.

Perguntas de teste de ativo são categorizadas por tipo de comunicação; real ou possível. Ambos os tipos de comunicações usam testes de contribuição e restritivos.

A comunicação real inclui quaisquer ativos nos quais as comunicações foram detectadas usando conexões. As perguntas de possível comunicação permitem que você revise se as comunicações específicas são possíveis em ativos, independentemente de uma comunicação ter ou não sido detectada.

Uma pergunta de teste de contribuição é a pergunta de teste base que define qual tipo de comunicação de real que você está tentando testar.

Uma pergunta de teste restritivo restringe os resultados do teste de contribuição para filtrar ainda mais a comunicação real para violações específicas.

Quando você usa um teste restritivo, a direção do teste restritivo deve seguir a mesma direção que o teste de contribuição. Testes restritivos que usam uma combinação de direções de entrada e de saída podem ser usados em situações em que você está tentando localizar ativos entre dois pontos, como duas redes ou endereços IP.

Entrada refere-se a um teste que está filtrando as conexões para as quais o ativo em questão é um destino. Saída refere-se a um teste que está filtrando conexões para as quais o ativo em questão é uma origem.

Perguntas de teste de dispositivos/regras

Dispositivos e regras são usados para identificar regras em um dispositivo que violam uma política definida que pode apresentar risco no ambiente.

Para obter uma lista detalhada de perguntas de regra de dispositivo, consulte Perguntas de teste de dispositivo/regras.

Contribuindo com perguntas para testes de comunicação reais

Os testes de comunicação reais para ativos incluem perguntas de contribuição e parâmetros que você escolhe quando cria um teste de monitor de política.

Quando você aplica a condição "não" a um teste, a condição "não" é associada ao parâmetro que você está testando.

Por exemplo, se você configurar um teste como **comunicação não aceita com redes de destino**, o teste detecta ativos que aceitaram comunicações com redes além da rede configurada. Outro exemplo é se você configurar um teste como comunicação não aceita com a Internet, então o teste detecta que os ativos aceitaram comunicações com ou a partir de áreas além da Internet.

A tabela a seguir lista e descreve os parâmetros de pergunta de contribuição para testes de comunicação reais.

Tabela 14. Parâmetros de pergunta de contribuição para testes de comunicação reais

Nome do Teste	Descrição
comunicação aceita para qualquer destino	Detecta os ativos que têm comunicações com qualquer rede configurada. Este teste permite que você defina um ponto inicial ou final para sua pergunta. Por exemplo, para identificar os ativos que aceitaram comunicação a partir da DMZ, configurar o teste da seguinte forma: comunicação aceita de qualquer origem É possível usar esse teste para detectar as comunicações fora da política.
comunicação aceita com redes de destino	Detecta os ativos que têm comunicações com ou a partir das redes especificadas. Este teste permite que você defina um ponto inicial ou final para sua pergunta. Por exemplo, para identificar os ativos que se comunicaram com a DMZ, configure o teste da seguinte forma: comunicação aceita a partir das <redes> de origem É possível usar esse teste para detectar as comunicações fora da política.
comunicação aceita com endereços IP de destino	Detecta ativos que têm comunicações com ou a partir do endereço IP especificado. Esse teste permite que você especifique o endereço IP ou CIDR. Por exemplo, se desejar identificar todos os ativos que se comunicaram com um servidor de conformidade específico, configure o teste da seguinte forma: comunicações aceitas com <endereço IP do servidor de conformidade> de destino
comunicação aceita com blocos de construção de ativo de destino	Detecta os ativos que têm comunicações com ou a partir dos blocos de construção do ativo especificados. Esse teste permite reutilizar blocos de construção definidos no Assistente de Regras do QRadar em sua consulta. Para obter mais informações sobre as regras, ativos e os blocos de construção, consulte o *IBM Security QRadar SIEM Administration Guide*.

Tabela 14. Parâmetros de pergunta de contribuição para testes de comunicação reais (continuação)

Nome do Teste	Descrição
comunicação aceita com procuras salvas do ativo de destino	Detecta ativos que têm comunicações com ou a partir dos ativos retornados pela procura salva especificada. Para obter informações sobre como criar e salvar uma procura de ativos, consulte o *IBM Security QRadar SIEM Users Guide*
comunicação aceita com conjuntos de referência de destino	Detecta ativos que se comunicaram com ou a partir dos conjuntos de referência definidos.
comunicação aceita com locais de rede remota de destino	Detecta ativos que se comunicaram com redes definidas como uma rede remota. Por exemplo, esse teste pode identificar hosts que se comunicaram com botnets ou outro espaço de endereço Internet suspeito.
comunicação aceita com locais de rede geográficos de destino	Detecta ativos que se comunicaram com redes definidas como redes geográficas. Por exemplo, esse teste pode detectar ativos que tentaram comunicações com países nos quais você não tem operações de negócios.
comunicação aceita com a Internet	Detecta comunicações de origem ou destino com ou a partir da Internet.
são suscetíveis a uma das vulnerabilidades a seguir	Detecta as vulnerabilidades específicas. Se você deseja detectar as vulnerabilidades de um tipo específico, utilize o teste, **são suscetíveis a vulnerabilidade com uma das seguintes classificações**. É possível procurar vulnerabilidades usando ID OSVDB, ID CVE, ID Bugtraq ou título.
são suscetíveis a vulnerabilidades com uma das seguintes classificações	A vulnerabilidade pode ser associada a uma ou mais classificações de vulnerabilidade. Esse teste filtra todos os ativos que incluem vulnerabilidades com as classificações especificadas. Configure o parâmetro **classificações** para identificar as classificações de vulnerabilidade que você deseja que este teste aplique. Por exemplo, uma classificação de vulnerabilidade pode ser Manipulação de Entrada ou Negação de Serviço.

Tabela 14. Parâmetros de pergunta de contribuição para testes de comunicação reais (continuação)

Nome do Teste	Descrição
são suscetíveis a vulnerabilidades com pontuação CVSS maior que 5	Um valor Common Vulnerability Scoring System (CVSS) é um padrão de mercado para avaliar a gravidade das vulnerabilidades. CVSS é composta de 3 grupos de métrica: Base, Temporal e Ambiental. Essas métricas permitem que a CVSS defina e comunique as características fundamentais de uma vulnerabilidade. Esse teste filtra ativos em sua rede que incluem vulnerabilidades com a pontuação CVSS que você especificar.
são suscetíveis a vulnerabilidades divulgadas após a data especificada	Detecta ativos em sua rede com uma vulnerabilidade que é divulgada depois, antes ou na data configurada.
são suscetíveis a vulnerabilidades em uma das portas a seguir	Detecta ativos em sua rede com uma vulnerabilidade que está associada com as portas configuradas. Configure o parâmetro **portas** para identificar portas que você deseja que este teste considere.
são suscetíveis a vulnerabilidades em que nome, fornecedor, versão ou serviço contém uma das seguintes entradas de texto	Detecta ativos em sua rede com uma vulnerabilidade que corresponde ao nome do ativo, fornecedor, versão ou serviço com base em um ou mais entradas de texto. Configure o parâmetro **entradas de texto** para identificar o nome do ativo, fornecedor, versão ou serviço que deseja que este teste considere.
são suscetíveis a vulnerabilidades em que nome, fornecedor, versão ou serviço contém uma das seguintes expressões regulares	Detecta ativos em sua rede com uma vulnerabilidade que corresponde ao nome do ativo, fornecedor, versão ou serviço com base em uma ou mais expressões regulares. Configure o parâmetro **expressões regulares** para identificar o nome do ativo, fornecedor, versão ou serviço que deseja que este teste considere.
são suscetíveis a vulnerabilidades contidas em procuras salvas de vulnerabilidade	Detecta os riscos que estão associados a procuras salvas que são criadas em IBM Security QRadar Vulnerability Manager.

Perguntas do teste de contribuição descontinuadas

Perguntas de contribuição que são substituídas por outro teste ficam ocultas no monitor de política.

Os seguintes testes ficam ocultos no Monitor de Política:

- ativos que estão suscetíveis a vulnerabilidades
- ativos que estão suscetíveis a vulnerabilidade dos serviços a seguir

Esses testes de contribuição foram substituídos por outros testes.

Perguntas restritivas para testes de comunicação reais

Os testes de comunicação reais para ativos incluem perguntas restritivas e parâmetros que podem ser escolhidos quando você cria um teste de monitor da política.

Quando você aplica a condição de exclusão a um teste, a condição de exclusão aplica-se ao parâmetro de protocolos.

Por exemplo, se você configurar esse teste como **excluir os seguintes protocolos**, o teste excluirá todos os resultados de ativo retornados que excluem os protocolos especificados diferentes dos protocolos configurados.

A tabela a seguir lista e descreve os parâmetros de perguntas restritivas para testes de comunicação reais.

Tabela 15. Parâmetros de perguntas restritivas para testes de comunicação reais

Nome do Teste	Descrição
incluir apenas os seguintes protocolos	Filtra ativos do teste de contribuição que incluem ou excluem os protocolos especificados. Esse teste é selecionável apenas quando um teste de ativo de contribuição é incluído nessa pergunta.
incluir apenas as seguintes portas de entrada	Filtra ativos do teste de contribuição que apenas incluem ou excluem as portas especificadas. Esse teste é selecionável apenas quando um teste de ativo de contribuição é incluído nessa pergunta.
incluir apenas os seguintes aplicativos de entrada	Filtra ativos da pergunta do teste de contribuição que incluem apenas ou excluem quaisquer aplicativos de entrada ou de saída. Esse teste filtra conexões que apenas incluem dados de fluxo.
incluir apenas se os bytes de de entrada de origem e saída de destino tiverem uma diferença de porcentagem menor que 10	Filtra ativos da pergunta de teste de contribuição que é baseada nas comunicações com uma proporção específica de bytes de entrada para saída (ou de saída para entrada). Esse teste é útil para detectar hosts que podem estar exibindo um comportamento de tipo de proxy (entrada igual a saída).

Tabela 15. Parâmetros de perguntas restritivas para testes de comunicação reais (continuação)

Nome do Teste	Descrição
incluir apenas se a contagem de fluxo de entrada e de saída tiver uma diferença de porcentagem menor que 10	Filtra ativos da pergunta de teste de contribuição que é baseada em comunicações com uma proporção específica de fluxos de entrada para saída (ou de saída para entrada). Esse teste filtra conexões que incluem dados de fluxo quando a contagem de fluxo está selecionada. Esse teste restritivo requer dois testes de contribuição que especificam uma origem e um destino. O teste a seguir destaca um conjunto de perguntas ao tentar determinar quais ativos entre dois pontos têm uma diferença de porcentagem de entrada e de saída maior que 40%. Por exemplo, • **Teste de contribuição** – comunicação aceita com a Internet. • **Teste de contribuição** – comunicação aceita a partir da Internet. • **Teste restritivo** – e incluir apenas se a contagem de fluxo de entrada e de saída tiver uma diferença de porcentagem maior que 40.
incluir apenas se o horário estiver entre o horário de início e o horário de encerramento inclusivo	Filtra comunicações dentro de sua rede que ocorreram dentro de um intervalo de tempo específico. Permite detectar comunicações fora da política. Por exemplo, se sua política corporativa permitir comunicações de FTP entre 13h e 15h, esses testes poderão detectar quaisquer tentativas de uso do FTP para comunicação fora desse intervalo de tempo.
incluir apenas se o dia da semana for entre o dia de início e dia de encerramento inclusivos	Filtra ativos da pergunta do teste de contribuição com base nas comunicações de rede que ocorreram dentro de um intervalo de tempo específico. Permite detectar comunicações fora da política.
incluir apenas se suscetível a vulnerabilidades que são exploráveis.	Filtra ativos de uma pergunta de teste de contribuição procurando vulnerabilidades específicas e restringe os resultados aos ativos exploráveis. Esse teste restritivo não contém parâmetros configuráveis, mas é usado em conjunto com o teste de contribuição, **são suscetíveis a uma das seguintes vulnerabilidades**. Essa regra de contribuição que contém um parâmetro de vulnerabilidades é necessária.
incluir apenas as seguintes redes	Filtra ativos de uma pergunta de teste de contribuição que inclui ou exclui as redes configuradas.

Tabela 15. Parâmetros de perguntas restritivas para testes de comunicação reais (continuação)

Nome do Teste	Descrição
incluir apenas os seguintes blocos de construção do ativo	Filtra ativos de uma pergunta de teste de contribuição que estão ou não associados com os blocos de construções do ativo configurados.
incluir apenas as seguintes procuras salvas do ativo	Filtra ativos de uma pergunta de teste de contribuição que estão ou não associados à procura salva do ativo.
incluir apenas os seguintes conjuntos de referência	Filtra ativos que são de uma pergunta de teste de contribuição que inclui ou exclui os conjuntos de referência configurados.
incluir apenas os seguintes endereços IP	Filtra ativos que estão ou não associadas aos endereços IP configurados.
incluir apenas se o service pack do Microsoft Windows para sistemas operacionais for abaixo de 0	Filtra ativos para determinar se um nível de service pack do Microsoft Windows para um sistema operacional está abaixo do nível especificado pela política de sua empresa.
incluir apenas se a configuração de segurança do Microsoft Windows for menor que 0	Filtra ativos para determinar se a configuração de segurança do Microsoft Windows está abaixo do nível especificado pela política de sua empresa.
incluir apenas se o serviço do Microsoft Windows for igual a status	Filtra ativos para determinar se um serviço do Microsoft Windows é desconhecido, inicialização, kernel, automático, demanda ou desativado.
incluir apenas se a configuração do Microsoft Windows for igual a expressões regulares	Filtra ativos para determinar se uma configuração do Microsoft Windows é a expressão regular especificada.

Contribuindo com perguntas para possíveis testes de comunicação

Os possíveis testes de comunicação para ativos incluem perguntas de contribuição e parâmetros que você pode escolher ao criar um teste do monitor de política.

A tabela a seguir lista e descreve os parâmetros de pergunta de contribuição para testes de comunicação possíveis.

Tabela 16. Parâmetros de possíveis perguntas de comunicação para testes de contribuição

Nome do Teste	Descrição
comunicação aceita para qualquer destino	Detecta ativos que têm possíveis comunicações com ou a partir de qualquer origem ou destino especificado. Por exemplo, para determinar se um servidor crítico pode possivelmente receber comunicações de qualquer origem, configure o teste da seguinte forma: comunicação aceita de qualquer origem É possível aplicar um teste restritivo para retornar se esse servidor crítico recebeu alguma comunicação na porta 21. Isso permite que você detecte comunicações fora da política para esse servidor crítico.
comunicação aceita com redes de destino	Detecta ativos que têm possíveis comunicações com ou a partir da rede configurada. Este teste permite que você defina um ponto inicial ou final para sua pergunta. Por exemplo, para identificar os ativos que têm a possibilidade de se comunicar com a DMZ, configure o teste da seguinte forma: comunicação aceita a partir das <redes> de origem É possível usar esse teste para detectar as comunicações fora da política.
comunicação aceita com endereços IP de destino	Detecta ativos que têm possíveis comunicações co ou a partir do endereço IP configurado. Esse teste permite que você especifique um endereço IP único como um foco de comunicações possíveis. Por exemplo, se desejar identificar todos os ativos que podem se comunicar com um servidor de conformidade específico, configure o teste da seguinte forma: comunicações aceitas com <endereço IP do servidor de conformidade> de destino

Tabela 16. Parâmetros de possíveis perguntas de comunicação para testes de contribuição (continuação)

Nome do Teste	Descrição
comunicação aceita com blocos de construção de ativo de destino	Detecta ativos que têm possíveis comunicações com ou a partir do ativo configurado usando blocos de construção. Esse teste permite reutilizar blocos de construção definidos no Assistente de Regras do QRadar em sua consulta. Por exemplo, se desejar identificar todos os ativos que podem se comunicar com um Ativo Protegido, configure o teste da seguinte forma: comunicações aceitas com `<BB:HostDefinition:Protected Assets>` de destino Para obter mais informações sobre as regras, ativos e os blocos de construção, consulte o *IBM Security QRadar SIEM Administration Guide*.
comunicação aceita com procuras salvas do ativo de destino	Detecta ativos que aceitaram comunicações com ou a partir dos ativos que são retornados pela procura salva especificada. Uma procura de ativo salva deve existir para que você possa usar esse teste. Para obter informações sobre como criar e salvar uma procura de ativos, consulte o *IBM Security QRadar SIEM Users Guide*
comunicação aceita com conjuntos de referência de destino	Detecta se a comunicação de origem ou destino é possível com ou partir de conjuntos de referência.
comunicação aceita com a Internet	Detecta se as comunicações de origem ou destino são possíveis com ou a partir da Internet. Especifique os parâmetros **para** ou **de** para considerar o tráfego de comunicação com a Internet ou a partir da Internet.
são suscetíveis a uma das vulnerabilidades a seguir	Detecta possíveis vulnerabilidades específicas. Se você deseja detectar as vulnerabilidades de um tipo específico, utilize o teste, **são suscetíveis a vulnerabilidade com uma das seguintes classificações**. Especifique as vulnerabilidades às quais deseja aplicar este teste. É possível procurar vulnerabilidades usando o ID OSVDB, ID CVE, ID Bugtraq ou título

Tabela 16. Parâmetros de possíveis perguntas de comunicação para testes de contribuição (continuação)

Nome do Teste	Descrição
são suscetíveis a vulnerabilidades com uma das seguintes classificações	A vulnerabilidade pode ser associada a uma ou mais classificações de vulnerabilidade. Esse teste filtra todos os ativos que tiverem possíveis vulnerabilidades com uma pontuação Common Vulnerability Scoring System (CVSS), conforme especificado. Configure o parâmetro de classificações para identificar as classificações de vulnerabilidade às quais deseja aplicar este teste.
são suscetíveis a vulnerabilidades com pontuação CVSS maior que 5	Um valor Common Vulnerability Scoring System (CVSS) é um padrão de mercado para avaliar a gravidade de vulnerabilidades possíveis. CVSS é composta de três grupos de métrica: Base, Temporal e Ambiental. Essas métricas permitem que a CVSS defina e comunique as características fundamentais de uma vulnerabilidade. Esse teste filtra ativos em sua rede que incluem o valor CVSS configurado.
são suscetíveis a vulnerabilidades divulgadas após a data especificada	Filtra ativos em sua rede com uma possível vulnerabilidade divulgada após, antes ou na data configurada.
são suscetíveis a vulnerabilidades em uma das portas a seguir	Filtra ativos em sua rede com uma possível vulnerabilidade que está associada com as portas configuradas. Configure o parâmetro de portas para identificar os ativos com possíveis vulnerabilidades com base no número de porta especificado.
são suscetíveis a vulnerabilidades em que nome, fornecedor, versão ou serviço contém uma das seguintes entradas de texto	Detecta ativos em sua rede com uma vulnerabilidade que corresponde ao nome do ativo, fornecedor, versão ou serviço com base em um ou mais entradas de texto. Configure o parâmetro **entradas de texto** para identificar o nome do ativo, fornecedor, versão ou serviço que deseja que este teste considere.
são suscetíveis a vulnerabilidades em que nome, fornecedor, versão ou serviço contém uma das seguintes expressões regulares	Detecta ativos em sua rede com uma vulnerabilidade que corresponde ao nome do ativo, fornecedor, versão ou serviço com base em uma ou mais expressões regulares. Configure o parâmetro **expressões regulares** para identificar o nome do ativo, fornecedor, versão ou serviço que deseja que este teste considere.
são suscetíveis a vulnerabilidades contidas em procuras salvas de vulnerabilidade	Detecta os riscos que estão associados a procuras salvas que são criadas em IBM Security QRadar Vulnerability Manager.

Perguntas do teste de contribuição descontinuadas

Se um teste for substituído por outro, ele ficará oculto no monitor de política.

Os seguintes testes ficam ocultos no Monitor de Política:

- ativos que estão suscetíveis a vulnerabilidade dos fornecedores a seguir
- ativos que estão suscetíveis a vulnerabilidade dos serviços a seguir

Esses testes de contribuição foram substituídos por outros testes.

Parâmetros de pergunta restritivos para possíveis testes de comunicação

Os possíveis testes de comunicação para ativos incluem parâmetros de pergunta restritivos.

A tabela a seguir lista e descreve os parâmetros pergunta restritivos para testes de comunicação possíveis.

Tabela 17. Testes restritivos para possíveis testes de comunicação

Nome do Teste	Descrição
incluir apenas os seguintes protocolos	Filtra ativos que possivelmente se comunicaram ou não com os protocolos configurados, juntamente com os outros testes incluídos nesta pergunta.
incluir apenas as seguintes portas de entrada	Filtra ativos que possivelmente se comunicaram ou não com as portas configuradas, juntamente com os outros testes incluídos nesta pergunta.
incluir apenas portas diferentes das seguintes portas de entrada	Filtra ativos partir de uma pergunta de teste de contribuição que possivelmente se comunicaram ou não com portas diferentes das configuradas, juntamente com os outros testes incluídos nesta pergunta.
incluir apenas se suscetível a vulnerabilidades que são exploráveis.	Filtra ativos a partir de uma pergunta de teste de contribuição procurando possíveis vulnerabilidades específicas e restringe os resultados aos ativos exploráveis. Esse teste restritivo não contém parâmetros configuráveis, mas é usado em conjunto com o teste de contribuição, **são suscetíveis a uma das seguintes vulnerabilidades**. Essa regra de contribuição que contém um parâmetro de vulnerabilidades é necessária.
incluir apenas as seguintes redes	Filtra ativos a partir de uma pergunta de teste de contribuição que apenas incluem ou excluem as redes configuradas.
incluir apenas os seguintes blocos de construção do ativo	Filtra ativos a partir de uma pergunta de teste de contribuição que apenas incluem ou excluem os blocos de construção do ativo configurado.
incluir apenas as seguintes procuras salvas do ativo	Filtra ativos a partir de uma pergunta de teste de contribuição que apenas incluem ou excluem a procura salva do ativo associado.

Tabela 17. Testes restritivos para possíveis testes de comunicação (continuação)

Nome do Teste	Descrição
incluir apenas os seguintes conjuntos de referência	Filtra ativos a partir de uma pergunta de teste de contribuição que apenas incluem ou excluem os configurados
incluir apenas os seguintes endereços IP	Filtra ativos a partir de uma pergunta de teste de contribuição que apenas incluem ou excluem os endereços IP configurados.
incluir apenas se o service pack do Microsoft Windows para sistemas operacionais for abaixo de 0	Filtra ativos para determinar se um nível de service pack do Microsoft Windows para um sistema operacional está abaixo do nível especificado pela política de sua empresa.
incluir apenas se a configuração de segurança do Microsoft Windows for menor que 0	Filtra ativos para determinar se a configuração de segurança do Microsoft Windows está abaixo do nível especificado pela política de sua empresa.
incluir apenas se o serviço do Microsoft Windows for igual a status	Filtra ativos para determinar se um serviço do Microsoft Windows é desconhecido, inicialização, kernel, automático, demanda ou desativado.
incluir apenas se a configuração do Microsoft Windows for igual a expressões regulares	Filtra ativos para determinar se uma configuração do Microsoft Windows é a expressão regular especificada.

Perguntas do teste de dispositivo/regras

Perguntas do teste de dispositivos/regras são usadas para identificar as regras em um dispositivo que violam uma política definida que pode introduzir risco no ambiente.

As perguntas do teste de dispositivo/regras estão descritas na tabela a seguir.

Tabela 18. Testes de dispositivos/regras

Nome do Teste	Descrição
permitir conexões com as redes a seguir	Filtra regras de dispositivo e as conexões com ou a partir das redes configuradas. Por exemplo, se você configurar o teste para permitir comunicações com uma rede, o teste filtrará todas as regras e conexões que permitem conexões com a rede configurada.
permitir conexões com os endereços IP a seguir	Filtra regras de dispositivo e conexões com ou a partir dos endereços IP configurados. Por exemplo, se você configurar o teste para permitir comunicações com um endereço IP, o teste filtrará todas as regras e conexões que permitem conexões com o endereço IP configurado.
permitir conexões com os seguintes blocos de construção ativo	Filtra regras de dispositivo e conexões com ou a partir dos blocos de construção de ativos configurados.
permitir conexões com os seguintes conjuntos de referência	Filtra regras de dispositivo e conexões com ou a partir dos conjuntos de referência configurados.

Tabela 18. Testes de dispositivos/regras (continuação)

Nome do Teste	Descrição
permitir conexões usando os protocolos e as portas de destino a seguir	Filtra regras de dispositivo e conexões com ou a partir dos protocolos e portas configurados
permitir conexões usando os protocolos a seguir	Filtra regras de dispositivo e conexões com ou a partir dos protocolos configurados.
permitir conexões à Internet	Filtra regras de dispositivo e conexões com e a partir da Internet.
são um dos dispositivos a seguir	Filtra todos os dispositivos de rede para os dispositivos configurados. Esse teste pode filtrar com base em dispositivos que estão ou não estão na lista configurada.
são um dos conjuntos de referência a seguir	Filtra regras de dispositivo com base nos conjuntos de referência que você especificar.
são uma das redes a seguir	Filtra regras de dispositivo com base nas redes que você especificar.
estão usando um dos adaptadores a seguir	Filtra regras de dispositivo com base nos adaptadores que você especificar.

Capítulo 7. Investigar conexões

Uma conexão é uma gravação de uma comunicação, incluindo comunicações negadas, entre dois endereços IP exclusivos por meio de uma porta de destino específica, conforme detectado em um determinado intervalo de tempo.

Se dois endereços IP se comunicarem várias vezes durante o mesmo intervalo em uma porta, somente uma comunicação será registrada, mas os bytes comunicados e o número de fluxos serão totalizados com a conexão. Ao final do intervalo, as informações de conexão serão acumuladas durante o intervalo e armazenadas no banco de dados.

Conexões permitem monitorar e investigar as conexões de dispositivo de rede ou executar procuras avançadas. É possível:

- Procurar conexões
- Procurar um subconjunto de conexões
- Marcar resultados de procura como positivo falso para ajustar eventos positivos falsos de ofensas criadas.
- Visualizar informações de conexão agrupadas por várias opções
- Exportar conexões no formato XML ou CSV
- Usar o gráfico interativo para visualizar conexões em sua rede

Visualizando conexões

É possível visualizar informações de conexão que são agrupadas por várias opções.

Sobre Esta Tarefa

Se uma procura salva for o padrão, os resultados dessa procura salvas serão exibidos. Por padrão, a janela Conexões exibe os seguintes gráficos:

- Gráfico de registros correspondidos ao longo do tempo fornece informações de série temporal que mostram o número de conexões com base em tempo.
- Gráfico de conexões que fornece uma representação visual das conexões recuperadas.

A janela Conexões exibe as seguintes informações:

Tabela 19. Janela Conexões – padrão

Parâmetro	Descrição
Filtros Atuais	A parte superior da tabela exibe os detalhes do filtro aplicado ao resultado da procura. Para limpar esses valores de filtro, clique em Limpar Filtro. Esse parâmetro só é exibido após a aplicação de um filtro.
Visualização	Permite especificar o intervalo de tempo que você deseja filtrar. Usando a lista suspensa, selecione o intervalo de tempo que você deseja filtrar.

Tabela 19. Janela Conexões – padrão (continuação)

Parâmetro	Descrição
Estatísticas Atuais	As estatísticas atuais incluem: • Total de Resultados – O número total de resultados que corresponderam aos seus critérios de procura. • Arquivos de Dados Procurados – O número total de arquivos de dados procurados durante o período de tempo especificado. • Arquivos de Dados Compactados Procurados – O número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • Contagem de Arquivos de Índice - O número total de arquivos de índice procurados durante o período de tempo especificado. • Duração - A duração da procura. • As Estatísticas Atuais são uma ferramenta de resolução de problemas útil. Quando você entrar em contato com o Suporte ao Cliente para resolver um problema, talvez seja solicitado que você forneça informações estatísticas atuais. Clique na seta ao lado das Estatísticas Atuais para exibir ou ocultar as estatísticas.
Gráficos	Exibe gráficos que representam os registros correspondidos pelo intervalo de tempo e/ou opção de agrupamento. Clique em Ocultar Gráficos se desejar remover o gráfico a partir de sua tela. Se você usar o Mozilla Firefox como seu navegador e a extensão do navegador Adblock Plus estiver instalada, os gráficos não serão exibidos. Para os gráficos a serem exibidos, é necessário remover a extensão do navegador Adblock Plus. Para obter mais informações, consulte a documentação do navegador.
Horário do Último Pacote	O período do Último Pacote é a data e a hora do último pacote processado para esta conexão.
Tipo de Fonte	O Tipo de Origem é o tipo de origem para esta conexão. As opções são: Host ou Remoto.

Tabela 19. Janela Conexões – padrão (continuação)

Parâmetro	Descrição
Origem	A origem desta conexão. As opções são: • Endereço IP - O endereço IP para a origem dessa conexão. O endereço IP é exibido se o Tipo de Origem for Host. • País – O país de origem (com o sinalizador país) para esta conexão. O sinalizador país só será exibido se o Tipo de Origem for remoto.
Tipo de destino	O tipo de destino para esta conexão. As opções são: Host ou Remoto.
Destino	O endereço IP para o tipo de host, incluindo o sinalizador do país. As opções são: • Endereço IP - Endereço IP para o destino dessa conexão. O endereço IP será exibido se o Tipo de Destino for Host. • País – O país de destino (com o sinalizador país) para esta conexão. O sinalizador país só será exibido se o Tipo de Destino for remoto.
Protocolo	O protocolo usado para esta conexão.
Porta de Destino	A porta de destino para esta conexão.
Aplicativo de Fluxo	O fluxo de aplicativo que gerou a conexão.
Fonte de Fluxo	A origem dos fluxos associada a essa conexão. Esse parâmetro aplica-se apenas a conexões aceitas.
Contagem de Fluxo	O número total de fluxos associados a esta conexão.
Bytes de Fonte de Fluxo	O número total de bytes de fonte de fluxo associados a esta conexão.
Bytes de Destino do Fluxo	O número total de bytes de destino associados a esta conexão.
Fonte de Log	A origem de eventos que contribuíram para esta conexão.
Contagem de Eventos	O número total de eventos detectados para a conexão.
Tipo de Conexão	O tipo de conexão. As opções são: • Permitir – Permitir a conexão. • Negar – Negar a conexão.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.
3. Usando a lista **Visualização**, selecione o período de tempo que você deseja exibir.

Usar gráficos para visualizar dados de conexão

É possível visualizar dados de conexão usando várias opções de gráfico. Por padrão, é possível visualizar dados usando registros correspondidos ao longo do tempo e o gráfico de conexão.

Registros correspondidos ao longo do tempo são uma opção que indica o número de conexões com base em tempo.

Um gráfico de conexão fornece uma representação visual da conexão recuperada. Se você deseja investigar conexões usando o gráfico de conexão, consulte Usando o gráfico de conexão.

Opções de gráfico disponíveis para conexões agrupadas são tabela, barras e setor. Para obter mais informações sobre a procura de conexões, consulte Procurar conexões.

Se você usar uma extensão de navegador Adblock Plus com navegador da Web Mozilla Firefox, os gráficos não poderão ser exibidos corretamente. Para os gráficos a serem exibidos, é necessário remover a extensão do navegador Adblock Plus. Para obter mais informações sobre a remoção de complementos, consulte a documentação do navegador da web.

Usando o gráfico de série temporal

Os gráficos de série temporal são representações gráficas de suas conexões no decorrer do tempo; picos e vales que são exibidos representam a atividade de conexão alta e baixa.

Antes de Iniciar

Se você salvou anteriormente uma procura para ser o padrão, os resultados para essa procura salva são exibidos na página Conexões. Se essa procura incluiu opções Agrupar por selecionadas na caixa Definições de Visualização Avançada, o gráfico Série Temporal não está disponível. Deve-se limpar os critérios de procura antes de continuar.

Sobre Esta Tarefa

Os gráficos de série temporal são úteis para tendência de dados a curto e longo prazos. Usando gráficos de série temporal, é possível acessar, navegar e investigar as conexões de várias visualizações e perspectivas.

A tabela a seguir fornece funções que podem ser usadas para visualizar gráficos de série temporal.

Tabela 20. Funções do gráfico de série temporal

Se desejar	Então
Visualizar conexões com mais detalhes	A ampliação dos dados em um gráfico de série temporal permite que você investigue segmentos de tempo menores das conexões. É possível ampliar o gráfico de série temporal usando uma das seguintes opções: • Pressione a tecla Shift e clique no gráfico no momento em que você deseja investigar. • Pressione as teclas Ctrl e Shift enquanto clica e arraste o ponteiro do mouse sobre o intervalo de tempo que você deseja visualizar. • Mova o ponteiro do mouse sobre o gráfico e pressione a tecla Seta para Cima no teclado. • Mova o ponteiro do mouse sobre o gráfico e, em seguida, use a roda de rolagem do mouse para aumentar o zoom (rolar a roda de rolagem do mouse para cima). Depois de você ampliar um gráfico de série temporal, o gráfico é atualizado para exibir um segmento de tempo menor.
Visualizar um período de tempo maior de conexões	Incluir intervalos de tempo adicionais no gráfico de série temporal permite que você investigue segmentos de tempo maiores ou retorne para o intervalo de tempo máximo. É possível visualizar um intervalo de tempo usando uma das seguintes opções: • Clique em Máx no canto superior esquerdo do gráfico ou pressione a tecla Home para retornar ao intervalo de tempo máximo. • Mova o ponteiro do mouse sobre o gráfico e pressione a seta para baixo no teclado. • Mova o ponteiro do mouse sobre o gráfico de plot e, em seguida, use a roda de rolagem do mouse para diminuir o zoom (rolar a roda de rolagem do mouse para baixo).

Tabela 20. Funções do gráfico de série temporal (continuação)

Se desejar	Então
Varra o gráfico	Para visualizar o gráfico para determinar informações em cada ponto de dados: • Clique e arraste o gráfico para varrer a linha de tempo. • Pressione a tecla Page Up para mover a linha de tempo uma página completa para a esquerda. • Pressione a tecla de seta esquerda para mover a linha de tempo meia página para a esquerda. • Pressione a tecla Page Down para mover a linha de tempo uma página completa para a direita. • Pressione a tecla de seta direita para mover a linha de tempo meia página para a direita

Procedimento

Procedimento

1. Clique na guia Riscos.
2. No menu de navegação, clique em **Conexões**.
3. Na área de janela de gráficos, clique no ícone **Configurar**.
4. Usando a lista suspensa **Tipo de Gráfico**, selecione Série Temporal.
5. Usando gráficos de série temporal interativos, é possível navegar por meio de uma linha de tempo para investigar as conexões.
6. Para atualizar as informações no gráfico, clique em Atualizar Detalhes.

Usar gráfico de conexão para visualizar as conexões de rede

O gráfico de conexão fornece uma representação visual das conexões em sua rede.

O gráfico que é exibido na janela Conexões não é interativo. Se você clicar no gráfico, a janela Visualizador de Dados Radial é exibida. A janela Visualizador de Dados Radial permite que você manipule o gráfico, conforme necessário.

Por padrão, o gráfico exibe suas conexões de rede, como a seguir:

- Somente conexões permitidas são exibidas.
- Todos os endereços IP locais são reduzidos para mostrar apenas redes folha.
- Todos nós de país são reduzidos a um nó denominado Países Remotos.
- Todos os nós da rede remota são reduzidos a um nó denominado Redes Remotas.
- Visualização em miniatura da visualização do gráfico exibe uma parte do gráfico principal. Isso é útil para gráficos grandes.

O Visualizador de Dados Radial inclui várias opções no menu, incluindo:

Tabela 21. Opções de menu do Visualizador de Dados Radial

Opção do menu	Descrição
Tipo de Conexão	Por padrão, o gráfico radial exibe conexões aceitas. Se você quiser visualizar as conexões negadas, selecione Negar na lista suspensa **Tipo de Conexão**.
Desfazer	Reduz a expansão do último nó. Se você deseja desfazer várias expansões, clique no botão Desfazer para cada expansão.
Download	Clique em **Download** para salvar a topologia atual como um arquivo de imagem JPEG ou um arquivo de desenho do Visio (VDX). Para fazer download e salvar a topologia atual como um arquivo de desenho do Visio (VDX), a versão mínima de software requerida é Microsoft Visio Standard 2010.

A tabela a seguir fornece funções adicionais para visualizar as conexões, incluindo:

Tabela 22. Funções do Visualizador de Dados Radial

Se desejar	Então
Aumentar zoom ou diminuir zoom	Use a régua de controle no lado superior direito do gráfico para alterar a escala.
Distribuir nós no gráfico para visualizar detalhes adicionais	Arraste o nó para o local preferencial para distribuir nós no gráfico.
Expandir um nó de rede	Dê um clique duplo no nó para expandir e visualizar ativos para esse nó. O nó é expandido para incluir os ativos específicos com os quais esse nó está se comunicando. Por padrão, essa expansão é limitada aos primeiros 100 ativos da rede.
Visualizar detalhes adicionais sobre uma conexão	Aponte o mouse sobre a linha de conexão para visualizar detalhes adicionais. Se a conexão for entre um nó de rede para uma rede remota ou país remoto, clique com o botão direito do mouse para exibir os seguintes menus **Origem** e **Visualizar Fluxos**: Se a conexão for entre dois endereços IP, as informações de origem, destino e porta serão exibidas quando você clicar na linha de conexão.
Determinar a quantidade de dados envolvidos na conexão	A espessura da linha no gráfico indica a quantidade de dados envolvidos na conexão. Uma linha espessa indica uma quantidade maior de dados. Essas informações são baseadas na quantidade de bytes envolvidos na comunicação

Tabela 22. Funções do Visualizador de Dados Radial (continuação)

Se desejar	Então
Destacar um caminho de conexão	Aponte o mouse sobre a linha de conexão. Se a conexão for permitida, o caminho será destacado em verde. Se a conexão for negada, o caminho será destacado em vermelho.
Determinar o caminho de conexão para um nó específico	Aponte o mouse sobre o nó. Se o nó for permitido, o caminho para o nó e o nó serão destacados em verde. Se o nó for negado, o caminho para o nó e o nó serão destacados em vermelho.
Alterar visualização do gráfico	Usando a miniatura de visualização, mova a miniatura para a parte do gráfico você deseja exibir.

Usando gráficos de setor, barra e tabela

É possível visualizar as conexões de dados usando um gráfico de setor, barras ou tabela.

Sobre Esta Tarefa

As opções de gráfico de setor, barra e tabela são exibidas apenas se a procura incluir as opções Agrupar por selecionadas nas opções Definição de Visualização Avançada.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.

   Nota: Os resultados da procura salva padrão são exibidos.
3. Execute uma procura.
4. Na área de janela de gráficos, clique no ícone **Configuração**.
5. Configure os parâmetros:

Opção	Descrição
Valor para Gráfico	Usando a lista **Valor para Gráfico**, selecione o tipo de objeto para o qual deseja criar um gráfico no gráfico. As opções incluem todos os parâmetros de fluxo normalizados e customizados incluídos em seus parâmetros de procura.
Tipo de Gráfico	Usando a lista **Tipo de Gráfico**, selecione o tipo de gráfico que você deseja visualizar. As opções incluem: • **Tabela** - Exibe dados em uma tabela. • **Barra** – Exibe dados em um gráfico de barras. • **Setor** – Exibe dados em um gráfico de pizza.

6. Clique em **Salvar**.

Os dados não são atualizados automaticamente, a menos que seus critérios de procura sejam exibidos para exibir automaticamente os detalhes.

7. Para atualizar os dados, clique em **Atualizar Detalhes**.

Procurar conexões

É possível procurar conexões usando critérios específicos e exibir conexões que correspondem ao critério de procura em uma lista de resultados. É possível criar uma nova procura ou carregar um conjunto de critérios de procura salvo anteriormente.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.

   Se aplicável, os resultados da procura salva padrão são exibidos.
3. Usando a lista **Procurar**, selecione **Nova Procura**.
4. Se desejar carregar uma procura alva previamente, use uma das opções a seguir:
   a. Na lista **Grupo**, selecione o grupo ao qual a procura salva está associada.
   b. Na lista **Procuras Salvas Disponíveis**, selecione a procura salva que você deseja carregar.
   c. No campo **Digitar Procura Salva ou Selecionar da Lista**, digite o nome da procura que você deseja carregar. Na lista Procuras Salvas Disponíveis, selecione a procura salva que deseja carregar.
   d. Clique em **Carregar**.
   e. Na área de janela **Editar Procura**, selecione as opções desejadas para essa procura.

Opção	Descrição
Incluir em Minhas Procuras Rápidas	Incluir essa procura nos itens de Procura Rápida.
Incluir em Meu Painel	Inclua os dados de sua procura salva em seu painel. Esse parâmetro estará disponível apenas se a procura for agrupada.
Definir como Padrão	Configurar essa procura como seu padrão de procura.
Compartilhar com Todos	Compartilhar esses requisitos de procura com todos os outros usuários do IBM Security QRadar Risk Manager.

5. Na área de janela Intervalo de Tempo, selecione uma opção para o intervalo de tempo que você deseja capturar para essa procura.

Opção	Descrição
Recente	Usando a lista, especifique o intervalo de tempo que você deseja filtrar.
Intervalo Específico	Usando o calendário, especifique a data e hora do intervalo você deseja filtrar.

6. Se você tiver terminado de configurar a procura e desejar visualizar os resultados, clique em Procurar.

7. Na área da janela Parâmetros de Procura, defina os critérios de sua procura específica:
   a. Usando a primeira lista, selecione um atributo no qual deseja procurar. Por exemplo, Tipo de Conexão, Rede de Origem ou Direção.
   b. Usando a segunda lista, selecione o modificador que deseja usar para a procura. A lista de modificadores que é exibida depende do atributo selecionado na primeira lista.
   c. No campo de texto, digite as informações específicas relacionadas a sua procura.
   d. Clique em **Incluir Filtro**.
   e. Repita da etapa a à e para cada filtro que você deseja incluir nos critérios de procura.
   f. Se você tiver terminado de configurar a procura e quiser visualizar os resultados, clique em **Procurar**. Caso contrário, continue na etapa seguinte.
8. Se você deseja salvar automaticamente os resultados da procura quando ela é concluída, selecione a caixa de seleção Salvar resultados quando a procura for concluída e especifique um nome.
9. Se você tiver terminado de configurar a procura e desejar visualizar os resultados, clique em **Procurar**. Caso contrário, continue com a próxima etapa.
10. Usando a área de janela Definição de Coluna, defina as colunas e o layout das colunas que deseja usar para visualizar os resultados:
    a. Usando a lista **Exibir**, selecione a visualização que você deseja associar a essa procura.
    b. Clique na seta ao lado de **Definição de Visualização Avançada** para exibir os parâmetros de procura avançada. Clique na seta novamente para ocultar os parâmetros.
11. Clique em **Procurar**.

Salvando critérios de procura

É possível criar uma procura especificando os critérios de procura e salvá-la para usar no futuro.

Sobre Esta Tarefa

É possível customizar as colunas que são exibidas nos resultados da procura. Estas opções estão disponíveis na seção Definição da Coluna e são chamadas de opções de Definição de Visualização Avançada.

Tabela 23. Opções de Definição de Visualização Avançada

Parâmetro	Descrição
Digitar Coluna ou Selecionar a partir da Lista	Filtra as colunas na lista Colunas Disponíveis. Digite o nome da coluna que você deseja localizar ou digite uma palavra-chave para exibir uma lista de nomes de coluna que incluem essa palavra-chave. Por exemplo, digite **Origem** para exibir uma lista de colunas que incluem Origem no nome da coluna.

Tabela 23. Opções de Definição de Visualização Avançada (continuação)

Parâmetro	Descrição
Colunas Disponíveis	Listas as colunas disponíveis associados à visualização selecionada. Colunas que estão atualmente em uso para esta procura salva são destacadas e exibidas na lista **Colunas**.
Botões incluir e remover coluna (configuração superior)	A configuração superior dos botões permite que você customize a lista **Agrupar por**. • **Incluir Coluna** – Selecione uma ou mais colunas da lista **Colunas Disponíveis** e clique no botão **Incluir Coluna**. • **Remover Coluna** – Selecione uma ou mais colunas da lista **Agrupar por** e clique no botão **Remover Coluna**.
Botões incluir e remover coluna (configuração inferior)	A configuração inferior de botões permite que você customize a lista **Colunas**. • **Incluir Coluna** – Selecione uma ou mais colunas da lista **Colunas Disponíveis** e clique no botão **Incluir Coluna**. • **Remover Coluna** – Selecione uma ou mais colunas da lista **Colunas** e clique no botão **Remover Coluna**.
Agrupar por	Especifica as colunas a partir das quais a procura salva agrupa os resultados. É possível customizar ainda mais a lista **Agrupar por** usando as seguintes opções: • **Mover para Cima** – Selecione uma coluna e mova-a para cima por meio da lista de prioridade usando o ícone **Mover para Cima**. • **Mover para Baixo** – Selecione uma coluna e mova-a para baixo por meio da lista de prioridade usando o ícone **Mover para Baixo**. A lista de prioridade especifica em qual ordem os resultados são agrupados. Os resultados da procura serão agrupados pela primeira coluna na lista **Agrupar por** e, em seguida, agrupados pela próxima coluna na lista.

Tabela 23. Opções de Definição de Visualização Avançada (continuação)

Parâmetro	Descrição
Colunas	Especifica as colunas escolhidas para a procura. As colunas são carregados a partir de uma procura salva. É possível customizar a lista **Colunas** selecionando colunas da lista **Colunas Disponíveis**. Você pode customizar ainda mais a lista **Colunas** usando as seguintes opções: • **Mover para Cima** – Selecione uma coluna e mova-a para cima por meio da lista de prioridade usando o botão mover para cima. • **Mover para Baixo** – Selecione uma coluna e mova-a para baixo por meio da lista de prioridade usando o botão mover para baixo. Se o tipo de coluna for numérico ou horário e houver uma entrada na lista **Agrupar por**, a coluna incluirá uma lista suspensa para permitir que você escolha como deseja agrupar a coluna.
Classificar Por	Usando a primeira lista, especifique a coluna pela qual deseja classificar os resultados da procura. Em seguida, usando a segunda lista, especifique a ordem que deseja exibir para os resultados da procura: **Decrescente** ou **Crescente**.

Procedimento

1. Clique na guia **Risco**s.
2. No menu de navegação, clique em **Conexões**.
3. Execute uma procura.
4. Clique em **Salvar Critérios**.
5. Configure valores para os seguintes parâmetros:

Opção	Descrição
Nome da Procura	Digite um nome que você deseja designar a este critério de procura.
Designar Procura ao(s) Grupo(s)	O grupo que você deseja designar a esta procura salva. Se você não selecionar um grupo, essa procura salva será designada ao grupo Outros por padrão.
Opções de amplitude de tempo	Escolha uma das opções a seguir: • Recente - Usando a lista suspensa, especifique o intervalo de tempo que deseja filtrar. • Intervalo Específico - Usando o calendário, especifique o intervalo de data e hora que deseja filtrar.

Opção	Descrição
Incluir em Minhas Procuras Rápidas	Selecione a caixa de seleção se desejar incluir essa procura em seus itens de Procura Rápida, que estão disponíveis na lista suspensa **Procura**.
Incluir em Meu Painel	Selecione a caixa de seleção se desejar incluir os dados da procura salva em seu Painel. Esse parâmetro só será exibido se a procura for agrupada.
Definir como Padrão	Selecione a caixa de seleção se desejar configurar esta procura como seu padrão de procura.
Compartilhar com Todos	Selecione a caixa de seleção se desejar compartilhar esses requisitos de procura com todos os outros usuários do IBM Security QRadar Risk Manager.

6. Clique em **OK**.

Executando uma subprocura

Todas as vezes que uma procura é executada, o banco de dados inteiro é consultado em busca de conexões que correspondem ao seu critério. Esse processo pode levar um longo período de tempo, dependendo do tamanho de seu banco de dados.

Sobre Esta Tarefa

Uma subprocura permite que você procure dentro de um conjunto de resultados de procura concluída. É possível refinar os resultados da procura sem procurar no banco de dados novamente. Uma subprocura não está disponível para procuras agrupadas ou em andamento.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.
3. Execute uma procura. Os resultados da procura são exibidos. Procuras adicionais usam o conjunto de dados da procura anterior quando subprocuras são executadas.
4. Para incluir um filtro, execute as seguintes etapas:
   a. Clique em **Incluir Filtro**.
   b. Usando a primeira lista, selecione um atributo no qual deseja procurar.
   c. Usando a segunda lista, selecione o modificador que deseja usar para a procura. A lista de modificadores que é exibida depende do atributo selecionado na primeira lista.
   d. No campo de texto, digite as informações específicas relacionadas a sua procura.
   e. Clique em **Incluir Filtro**.

      Nota: Se a procura permanecer em andamento, resultados parciais serão exibidos. A área de janela Filtro Original indica o filtro a partir do qual a procura original foi baseada. A área de janela Filtro Atual indica o filtro aplicado à subprocura.

Dica: Você pode limpar os filtros de procura sem reiniciar a procura original. Clique no link Limpar Filtro próximo do filtro que deseja limpar. Se você limpar um filtro na área Filtro Original, a procura original será reativada.

5. Clique em **Salvar Critérios** para salvar a subprocura.

Resultados

Se você excluir a procura original, é possível acessar a subprocura salva. Se um filtro for incluído, a subprocura procurará o banco de dados inteiro, já que a função de procura não se baseia mais em um conjunto de dados procurado anteriormente.

Gerenciar resultados da procura

É possível executar diversas procuras de conexões ao navegar para outras interfaces.

Sobre Esta Tarefa

É possível configurar o recurso de procura para enviar uma notificação por email quando uma procura é concluída. A qualquer momento, enquanto a procura está em andamento, é possível visualizar os resultados parciais dessa procura em andamento.

Os resultados da procura na barra de ferramentas fornecem as seguintes opções:

Parâmetro	Descrição
Nova Procura	Clique em **Nova Procura** para criar uma nova procura. Quando você clica nesse botão, a janela de procura é exibida.
Salvar Resultados	Clique em **Salvar Resultados** para salvar resultados da procura. Essa opção será ativada apenas quando você tiver selecionado uma linha na lista Gerenciar Resultados da Procura.
Cancelar	Clique em **Cancelar** para cancelar as procuras que estão em andamento ou estão enfileiradas para iniciar.
Excluir	Clique em **Excluir** para excluir um resultado da procura.
Notificar	Selecione a procura para a qual deseja receber notificação e, em seguida, clique em **Notificar** para ativar a notificação por email quando a procura for concluída.
Visualização	Na lista suspensa, especifique quais resultados da procura deseja listar na janela de resultados da procura. As opções são: • Resultados da Procura Salva • Todos os Resultados da Procura • Procuras Canceladas/Com Erro • Procuras em Andamento

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.
3. No menu, selecione **Procurar** > **Gerenciar Resultados da Procura**.

Salvando resultados da procura

É possível salvar os resultados de sua procura.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.
3. Execute uma procura de conexão ou subprocura.
4. Na janela Resultados da Procura, selecione **Procurar** > **Gerenciar Resultados da Procura** e selecione um resultado da procura.
5. Clique em **Salvar Resultados**.
6. Digite um nome para os resultados da procura.
7. Clique em **OK**.

Cancelando uma procura

É possível cancelar uma ou mais procuras.

Sobre Esta Tarefa

Se uma procura estiver em andamento quando for cancelada, os resultados acumulados, até o cancelamento da procura, serão mantidos.

Procedimento

1. Na janela Gerenciar Resultados da Procura, selecione o resultado da procura enfileirada ou em andamento que deseja cancelar. É possível selecionar várias procuras para cancelar.
2. Clique em **Cancelar Procura**.
3. Clique em **Sim**.

Excluindo uma procura

É possível excluir uma procura.

Procedimento

1. Na janela Gerenciar Resultados da Procura, selecione o resultado da procura que deseja excluir.
2. Clique em **Excluir**.
3. Clique em **Sim**.

Exportando conexões

É possível exportar conexões em formato de Linguagem de Marcação Extensível (XML) ou Comma Separated Values (CSV).

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Conexões**.

3. Se você deseja exportar a conexão no formato XML, selecione **Ações** > **Exportar para XML**.
4. Se você deseja exportar a conexão no formato CSV, selecione **Ações > Exportar para CSV**.
5. Se você deseja retomar suas atividades, clique em **Notificar Quando Pronto**.

Capítulo 8. Mapeamento de origem de Log

Para monitorar a frequência do acionador das regras de firewall e ativar as procuras de evento de topologia, o IBM Security QRadar Risk Manager identifica as origens de log do QRadar.

Ao compreender as regras de firewall, é possível manter a eficiência de firewall e evitar riscos de segurança.

Um máximo de 255 dispositivos podem ser mapeados para uma origem de log no QRadar Risk Manager, mas os dispositivos podem ter várias origens de log.

Opções de exibição de mapeamento de origem de log

Se o seu dispositivo de rede for configurado como uma origem de log do QRadar, a página do Monitor de Configuração exibe uma das entradas a seguir na coluna **Origem de Log**:

- **Auto-Mapeada** - Se QRadar Risk Manager identifica e mapeia a origem de log para o dispositivo automaticamente.
- **Nome de usuário** - Se um administrador incluiu ou editou manualmente uma origem de log.
- **Vazio** - Se o QRadar Risk Manager for incapaz de identificar uma origem de log para o dispositivo, a coluna **Origem de Log** não mostra nenhum valor. É possível criar manualmente um mapeamento de origem de log.

Para obter mais informações sobre como configurar as origens de log, consulte o *IBM Security QRadar Log Sources*.

Conceitos relacionados:

"Opções de menu ativado pelo botão direito da topologia" na página 36
Na topologia, você pode clicar com o botão direito em um evento para acessar informações de filtro de eventos adicionais.

Criando ou editando um mapeamento de origem de log

Se o IBM Security QRadar Risk Manager não puder identificar uma origem de log no QRadar, é possível configurar um mapeamento de origem de log.

Procedimento

1. Clique na guia **Riscos**.
2. Na área de janela de navegação, clique em **Monitor de Configuração**.
3. Clique no dispositivo sem um mapeamento de origem de log.
4. Na barra de ferramentas, clique em **Ação** > **Mapeamento de Origem de Log** > **Criar/Editar Mapeamento de Origem de Log**.
5. Na lista **Grupos de Origens de Log**, selecione um grupo.
6. Na lista **Origens de Log**, selecione uma origem de log e clique em (**>**).
7. Clique em **OK**.

Capítulo 9. Investigando suas configurações do dispositivo de rede

No IBM Security QRadar Risk Manager, é possível gerenciar a eficiência de seus dispositivos de rede, investigar as regras de firewall e identificar os riscos de segurança criados pelas regras de firewall inválidas.

Procedimento

1. Clique na guia **Riscos**.
2. Na área de janela de navegação, clique em **Monitor de Configuração**.
3. Para procurar seus dispositivos de rede, insira o endereço IP ou Nome do Host no campo **Endereço IP de Entrada ou Nome do Host**.
4. Clique duas vezes no dispositivo que deseja investigar.

   A coluna de regra **Contagem de Evento** exibe a frequência do acionador da regra de firewall. Uma regra de contagem de evento zero é exibida por uma das razões a seguir:

   - Uma regra não é acionada e pode causar um risco de segurança. É possível investigar seu dispositivo firewall e remover quaisquer regras que não estejam acionadas.
   - Um mapeamento de origem de log do QRadar não está configurado.
5. Para procurar as regras, na barra de ferramentas **Regras**, clique em **Procurar** > **Nova Procura**.

   Se um ícone for exibido na coluna **Status**, será possível passar o mouse sobre o ícone de status para exibir mais informações.
6. Para investigar as interfaces do dispositivo, na barra de ferramentas, clique em **Interfaces**.
7. Para investigar as regras do dispositivo da lista de controle de acesso (ACL), na barra de ferramentas, clique em **ACLs**.

   Cada lista de controle de acesso define as interfaces sobre as quais os dispositivos em sua rede estão se comunicando. Quando as condições de uma ACL são cumpridas, as regras que estão associadas a uma ACL são acionadas. Cada regra é testada para permitir ou negar a comunicação entre os dispositivos.
8. Para investigar as regras de dispositivo da conversão de endereço de rede (NAT), na barra de ferramentas, clique em **NAT**.

   A coluna **Fase** especifica quando o acionador excuta a regra NAT, por exemplo, antes ou depois do roteamento.
9. Para investigar a história ou comparar as configurações do dispositivo, na barra de ferramentas, clique em **Histórico**.

   É possível visualizar as regras do dispositivo em uma visualização de comparação normalizada ou configuração do dispositivo bruto. A configuração do dispositivo normalizado é uma comparação gráfica que mostra as regras incluídas, excluídas ou modificadas entre os dispositivos. A configuração do dispositivo bruto é uma visualização em XML ou de texto simples do arquivo de dispositivo.

Conceitos relacionados:

Capítulo 8, “Mapeamento de origem de Log”, na página 95
Para monitorar a frequência do acionador das regras de firewall e ativar as procuras de evento de topologia, o IBM Security QRadar Risk Manager identifica as origens de log do QRadar.

Procurando regras de dispositivos

No IBM Security QRadar Risk Manager, é possível procurar por regras que mudaram nos dispositivos em sua topologia. Também é possível descobrir mudanças de regra que ocorrem entre os backups de configuração do dispositivo.

Os resultados retornados para uma procura de regra são baseados no backup do gerenciamento de origem da configuração de seu dispositivo. Para garantir que as procuras de regras forneçam informações atualizadas, é possível planejar backups de dispositivos na sua página de atualizações de política de firewall.

Procedimento

1. Clique na guia **Riscos**.
2. Na área de janela de navegação, clique em **Monitor de Configuração**.
3. Dê um clique duplo em um dispositivo na página Monitor de Configuração.
4. Na barra de ferramentas da área de janela Regras, clique em **Procura** > **Nova Procura**.
5. Na área de janela **Critérios da Procura**, clique em um intervalo de tempo.
6. Para procurar suas regras de dispositivo, escolha a partir das opções a seguir:
   - Para procurar pelas regras **Sombreado**, **Excluída** ou **Outras**, clique em uma opção de status.

     Por padrão, todas as opções de status estão ativadas. Para procurar apenas por regras com sombras, desmarque as opções **Excluídas** e **Outras**.
   - Para procurar por uma lista de controle de acesso (ACL), digite no campo **Lista**.
   - Para procurar o número de pedido da entrada de regra, digite um valor numérico no campo **Entrada**.
   - Para procurar por uma origem ou destino, digite um endereço IP, endereço CIDR, nome do host ou referência de grupo de objeto.
   - Para procurar por portas ou referências de grupo de objeto, digite no campo **Serviço**.

     O serviço pode incluir intervalos de portas, como 100-200, ou expressões de porta, como 80(TCP). Se a porta for negada, as informações da porta também incluirão um ponto de exclamação e poderão ser cercadas por parênteses, por exemplo, !(100-200) ou !80(TCP).
   - Para procurar por informações sobre regras de vulnerabilidades como definido pelo dispositivo IPS, digite no campo **Assinatura**.
   - Para procurar por aplicativos pelo adaptador, clique em **Selecionar Aplicativos** e, em seguida, digite um nome de adaptador ou aplicativo.
7. Clique em **Procurar**.

Comparando a configuração de seus dispositivos de rede

No IBM Security QRadar Risk Manager, as configurações do dispositivo podem ser comparadas entre si por meio da comparação de vários backups em um único dispositivo ou comparando um backup de dispositivo de rede com outro.

Os tipos de configurações comuns podem incluir os itens a seguir:

- **Documentos de Elemento Padrão** - Os arquivos de Documento de Elemento Padrão (SED) são arquivos de dados XML que contêm informações sobre seus dispositivos de rede. Os arquivos SED são visualizados no formato XML bruto. Se um arquivo SED é comparado a outro arquivo SED, então a visualização é normalizada para exibir as diferenças de regras.
- **Config** - Os arquivos de configuração são fornecidos por determinados dispositivos de rede, dependendo do fabricante do dispositivo. É possível visualizar um arquivo de configuração clicando duas vezes nele.

Dependendo da informação que o adaptador coleta para seu dispositivo, vários outros tipos de configuração podem ser exibidos. Esses arquivos são exibidos na visualização de texto simples quando clicados duas vezes.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Monitor de Configuração**.
3. Clique duas vezes em qualquer dispositivo para visualizar as informações de configurações detalhadas.
4. Clique em **Histórico** para visualizar o histórico para este dispositivo.
5. Para comparar duas configurações em um único dispositivo:
   a. Selecione uma configuração primária.
   b. Pressione a tecla Ctrl e selecione uma segunda configuração para comparação.
   c. Na área de janela Histórico, clique em **Comparar Selecionado**.

      Se os arquivos de comparação forem documentos de elemento padrão (SEDs), então a janela Comparação de Configuração de Dispositivo Normalizado mostra as diferenças de regra entre os backups.

      Ao comparar configurações normalizadas, a cor do texto mostra as atualizações de dispositivo a seguir:

      - Uma estrutura de tópicos com pontilhado verde mostra uma regra ou configuração que foi incluída ao dispositivo.
      - Uma estrutura de tópicos com tracejado vermelho mostra uma regra ou configuração que foi excluída do dispositivo.
      - Uma estrutura de tópicos com sólidos amarelos mostra uma regra ou configuração que foi modificada no dispositivo.

   d. Para visualizar as diferenças de configuração brutas, clique em **Visualizar Comparação Bruta**.

      Se a comparação é um arquivo de configuração ou outro tipo de backup, então a comparação original é exibida.
6. Para comparar duas configurações em dispositivos diferentes:
   a. Selecione uma configuração primária a partir de um dispositivo.
   b. Clique em **Marcar para Comparação**.
   c. No menu de navegação, selecione **Todos os Dispositivos** para retornar à lista de dispositivos.

d. Dê um clique duplo no dispositivo para comparar e clique em **Histórico**.
e. Selecione uma configuração que você deseja comparar com a configuração marcada.
f. Clique em **Comparar com Marcado**.
g. Para visualizar as diferenças de configuração brutas, clique em **Visualizar Comparação Bruta**.

Capítulo 10. Gerenciando relatórios do IBM Security QRadar Risk Manager

É possível criar, editar, distribuir e gerenciar relatórios para seus dispositivos de rede. Relatórios detalhados sobre as regras de firewall e conexões entre os dispositivos muitas vezes são necessários para satisfazer vários padrões regulatórios, como a conformidade de PCI.

As opções de relatório a seguir são específicas para o QRadar Risk Manager:

Tabela 24. Opções de relatório para o QRadar Risk Manager

Opção de relatório	Descrição
Conexões	Os diagramas de conexão para os dispositivos de rede que ocorreram durante o período de tempo especificado.
Regras de dispositivo	As regras configuradas em sua rede de dispositivo durante o período de tempo especificado. É possível visualizar os seguintes tipos de regras para um ou vários dispositivos de rede usando esta opção de relatório: • Regras de aceitação mais usadas • Regras de negação mais usadas • Regras de aceitação menos usadas • Regras de negação menos usadas • Regras sombreadas • Regras de objetos não usados
Objetos de dispositivo não usados	Produz uma tabela com o nome, a configuração de data/hora e uma definição para quaisquer grupos de referência do objeto que não estão em uso no dispositivo. Um grupo de referência do objeto é um termo genérico usado para descrever uma coleção de endereços IP, endereços CIDR, nomes de host, portas ou outros parâmetros de dispositivo que são agrupados e designados às regras no dispositivo.

Gerando manualmente um relatório

Os relatórios podem ser iniciados manualmente. Se você iniciar vários relatórios manualmente, eles serão incluídos em uma fila e rotulados com seu gerenciador de posição.

Sobre Esta Tarefa

Gerar manualmente um relatório não reconfigura o planejamento de relatório existente. Por exemplo, se você gerar um relatório semanal para as negações de firewall mais ativas e depois gerar manualmente o relatório, o relatório semanal ainda será gerado no planejamento inicialmente configurado.

Quando um relatório é gerado, a coluna **Próximo Tempo de Execução** exibe uma das três mensagens a seguir:

- **Gerando** - O relatório está sendo gerado.
- **Enfileirado (posição na fila)**- O relatório é enfileirado para geração. A mensagem indica a posição que o relatório está na fila. Por exemplo, 1 de 3.
- **(x hora(s) x min(s) y seg(s))** – O relatório é planejado para ser executado. A mensagem é um cronômetro de contagem regressiva que especifica quando o relatório será executado pela próxima vez.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja gerar.
3. Clique em **Executar Relatório**.
4. Opcional. Clique em **Atualizar** para atualizar a visualização, incluindo as informações na coluna **Próximo Tempo de Execução**.

O que Fazer Depois

Depois que o relatório é gerado, é possível visualizar o relatório gerado a partir da coluna **Relatórios Gerados**.

Usar o assistente de relatório

É possível usar o Assistente de Relatório para criar um novo relatório. O Assistente de Relatório fornece um guia passo-a-passo de como projetar, planejar e gerar relatórios.

O assistente utiliza os seguintes elementos chave para ajudar a criar um relatório:

- **Layout** – Posição e tamanho de cada contêiner
- **Contêiner** – Lugar e local para conteúdo em seu relatório
- **Conteúdo** – Define os dados do relatório que o IBM Security QRadar Risk Manager inclui no gráfico para o contêiner

Ao selecionar o layout de um relatório, considere o tipo de relatório que você deseja criar. Por exemplo, não escolha um contêiner de gráfico pequeno para o conteúdo do gráfico que exibe um grande número de objetos. Cada gráfico inclui uma legenda e uma lista de redes das quais o conteúdo é derivado; escolha um contêiner suficientemente grande para conter os dados.

O tempo de planejamento deve decorrer para os relatórios que são gerados semanalmente ou mensalmente antes de o relatório gerado retornar resultados. Para obter um relatório planejado, você deve aguardar o período de tempo de planejamento para os resultados serem construídos. Por exemplo, uma pesquisa semanal requer 7 dias para construir os dados. Essa procura retorna resultados após 7 dias decorridos.

Criando um relatório

É possível criar relatórios para um intervalo específico e escolher um tipo de gráfico.

Sobre Esta Tarefa

Um relatório pode consistir em vários elementos de dados e pode representar dados de rede e de segurança em uma variedade de estilos, como tabelas, gráficos de linha, gráficos de pizza e gráficos de barras.

É possível especificar o Console de Relatório ou o email para as opções de distribuição do relatório. A tabela a seguir descreve os parâmetros para essas opções de distribuição.

Tabela 25. Opções de distribuição de relatório gerado

Opção	Descrição
Console de Relatórios	Selecione esta caixa de seleção para enviar o relatório gerado para a guia **Relatórios**. Esse é o canal de distribuição padrão.
Selecione os usuários que devem ser capazes de visualizar o relatório gerado.	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Console de Relatório**. Na lista de usuários, selecione os usuários do IBM Security QRadar Risk Manager aos quais você deseja conceder permissão para visualizar os relatórios gerados. Você deve ter permissões de rede apropriadas para compartilhar o relatório gerado com outros usuários. Para obter mais informações sobre permissões, consulte o *IBM Security QRadar SIEM Administration Guide*.
Selecionar todos os usuários	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Console de Relatório**. Selecione essa caixa de seleção se desejar conceder permissão a todos os usuários do QRadar Risk Manager para visualizar os relatórios gerados. Você deve ter permissões de rede apropriadas para compartilhar o relatório gerado com outros usuários. Para obter mais informações sobre permissões, consulte o *IBM Security QRadar SIEM Administration Guide*.
Email	Selecione esta caixa de seleção se você deseja distribuir o relatório gerado usando email.

Tabela 25. Opções de distribuição de relatório gerado (continuação)

Opção	Descrição
Inserir endereço(s) de email de distribuição de relatório	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Email**. Digite o endereço de email para cada destinatário do relatório gerado; separe uma lista de endereços de email com vírgulas. O máximo de caracteres para esse parâmetro é 255. Os destinatários de email recebem esse email de no_reply_reports@qradar.
Incluir Relatório como anexo (apenas não HTML)	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Email**. Selecione esta caixa de seleção para enviar o relatório gerado como um anexo.
Incluir link no Console de Relatórios	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Email**. Selecione essa caixa de seleção para incluir um link para o Console de Relatório no email.

Procedimento

1. Clique na guia **Relatórios**.
2. Na lista **Ações**, selecione **Criar**.
3. Clique em **Avançar** para ir para a próxima página do Assistente de Relatório.
4. Selecione a frequência para o planejamento do relatório.
5. Na área de janela Permitir que este relatório seja gerado manualmente, selecione **Sim** para ativar ou **Não** para desativar a geração manual deste relatório. Essa opção não está disponível para relatórios gerados manualmente.
6. Clique em **Avançar**.
7. Escolha um layout de seu relatório e clique em **Avançar**.
8. Insira o título do relatório. O título pode ter até 100 caracteres de comprimento. Não use caracteres especiais.
9. Escolha um logotipo. O logotipo QRadar é o padrão. Para obter mais informações sobre marcas em seu relatório, consulte o *IBM Security QRadar SIEM Administration Guide*.
10. Na lista **Tipo de Gráfico**, selecione um dos relatórios específicos do QRadar Risk Manager.
11. Configure os dados do relatório para o gráfico.
12. Clique em **Salvar Detalhes do Contêiner**.
13. Clique em **Avançar**.
14. Selecionar formatos de relatório. É possível selecionar várias opções.

    Nota: Os relatórios Regras de Dispositivo e Regras de Objeto Não Usado suportam apenas os formatos de relatório PDF, HTML e RTF.
15. Clique em **Avançar**.

16. Selecione os canais de distribuição que você deseja para seu relatório.
17. Clique em **Avançar**.
18. Digite uma descrição para este relatório. A descrição é exibida na página Resumo de Relatório e no email de distribuição do relatório gerado.
19. Selecione os grupos aos quais você deseja designar este relatório. Para obter mais informações sobre grupos, consulte Gerenciando Relatórios no *IBM Security QRadar SIEM Administration Guide*.
20. Opcional. Selecione sim para executar este relatório quando a configuração do assistente for concluída. Clique em **Avançar** para visualizar o resumo do relatório. É possível selecionar as guias disponíveis no relatório de resumo para visualizar as seleções de relatório.
21. Clique em **Concluir**.

Resultados

O relatório é gerado imediatamente. Se você limpou a caixa de seleção **Gostaria de executar o relatório agora** na página final do assistente, o relatório será salvo e gerado conforme planejado.

O título do relatório é o título padrão para o relatório gerado. Se você reconfigurar um relatório para inserir um novo título de relatório, o relatório será salvo como um novo relatório com o novo nome; no entanto, o relatório original permanecerá o mesmo.

Editando um relatório

É possível editar um relatório para ajustar um planejamento de relatório, layout, configuração, título, formato e método de entrega. Você pode editar relatórios existentes ou editar um relatório padrão.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que você deseja editar.
3. Na lista **Ações**, selecione **Editar**.
4. Selecione a frequência para o novo planejamento de relatório.
5. Na área de janela Permitir que este relatório seja gerado manualmente, selecione uma das seguintes opções:
   - **Sim** – Ativa a geração manual deste relatório.
   - **Não** - Destiva a geração manual deste relatório.
6. Clique em **Avançar** para ir para a próxima página do Assistente de Relatório.
7. Configure o layout do relatório:
   a. Na lista **Orientação**, selecione a orientação de página.
   b. Selecione uma opção de layout para o seu relatório do IBM Security QRadar Risk Manager.
   c. Clique em **Avançar**.
8. Especifique valores para os seguintes parâmetros:
   - **Título de Relatório** – Digite um título do relatório. O título pode ter até 100 caracteres de comprimento. Não use caracteres especiais.
   - **Logotipo** – Na lista, selecione um logotipo. O logotipo QRadar é o padrão. Para obter mais informações sobre marcas em seu relatório, consulte o *IBM Security QRadar SIEM Administration Guide*.

9. Configure o contêiner para o relatório de dados:
   a. Clique em **Definir**.
   b. Configure os dados do relatório para o gráfico.
   c. Clique em **Salvar Detalhes do Contêiner**.
   d. Se necessário, repita essas etapas para editar contêineres adicionais.
   e. Clique em **Avançar** para ir para a próxima página do Assistente de Relatório.
10. Clique em **Avançar** para ir para a próxima etapa do Assistente de Relatório.
11. Selecione as caixas de seleção para os formatos de relatório. Você pode selecionar mais de uma opção.

    Nota: Os relatórios específicos do QRadar Risk Manager, como relatórios Regra de Dispositivo e Objeto de Dispositivo Não Usado, suportam apenas formatos PDF, HTML e RTF.
12. Clique em **Avançar** para ir para a próxima página do Assistente de Relatório.
13. Selecione os canais de distribuição para seu relatório.
14. Clique em **Avançar** para ir à etapa final no Assistente de Relatório.
15. Digite uma descrição para este relatório. A descrição é exibida na página Relatório de Resumo e no email de distribuição do relatório gerado.
16. Selecione os grupos aos quais você deseja designar este relatório. Para obter mais informações sobre grupos, consulte Gerenciando Relatórios no *IBM Security QRadar SIEM Administration Guide*.
17. Opcional. Selecione sim para executar este relatório quando a configuração do assistente for concluída.
18. Clique em **Avançar** para visualizar o resumo do relatório. A página Relatório de Resumo é exibida, fornecendo os detalhes para o relatório. É possível selecionar as guias disponíveis no relatório de resumo para visualizar as seleções de relatório.
19. Clique em **Concluir**.

Duplicando um relatório

É possível duplicar qualquer relatório.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que você deseja duplicar.
3. Na lista **Ações**, clique em **Duplicar**.
4. Digite um novo nome, sem espaços, para o relatório.

Compartilhando um relatório

É possível compartilhar relatórios com outros usuários. Ao compartilhar um relatório, você fornece uma cópia do relatório selecionado para outro usuário para editar ou planejar.

Antes de Iniciar

Deve-se ter privilégios administrativos para compartilhar relatórios. Além disso, para um novo usuário para visualizar e acessar relatórios, um usuário

administrativo deve compartilhar todos os relatórios necessários com o novo usuário

Sobre Esta Tarefa

Nenhuma atualização que o usuário fizer em um relatório compartilhado afetará a versão original do relatório.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione os relatórios que você deseja compartilhar.
3. Na lista **Ações** , clique em **Compartilhar**.
4. Na lista de usuários, selecione os usuários com os quais você deseja compartilhar este relatório.

   Se nenhum usuário com acesso apropriado estiver disponível, uma mensagem é exibida.
5. Na etapa 5, clique em **Compartilhar**.

   Para obter mais informações sobre os relatórios, consulte o *IBM Security QRadar SIEM Users Guide*.

Configurando gráficos

O tipo de gráfico determina o dado configurado e exibido no gráfico. É possível criar vários gráficos específicos para os dados coletados pelos dispositivos no IBM Security QRadar Risk Manager.

Os tipos de gráficos a seguir são específicos ao QRadar Risk Manager:

- Conexão
- Regras de Dispositivo
- Objetos de Dispositivo Não Usados

Gráficos de conexão

É possível usar o gráfico Conexões para visualizar informações de conexão de rede. É possível basear seu gráficos nos dados de procuras de conexão salvas na guia Riscos.

É possível customizar os dados que você deseja exibir no relatório gerado. Você pode configurar o gráfico para criar um gráfico dos dados em um período de tempo configurável. Essa funcionalidade ajuda a detectar tendências de conexão.

A tabela a seguir fornece informações de configuração para o contêiner Gráfico de Conexões.

Tabela 26. Parâmetros do gráfico Conexões

Parâmetro	Descrição
Detalhes do Contêiner – Conexões	
Título do Gráfico	Digite um título de gráfico para um máximo de 100 caracteres.
Subtítulo do Gráfico	Desmarque a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título para um máximo de 100 caracteres.

Tabela 26. Parâmetros do gráfico Conexões (continuação)

Parâmetro	Descrição
Tipo de Gráfico	Na lista, selecione o tipo de gráfico para exibir no relatório gerado. As opções incluem: • **Barra** – Exibe os dados em um gráfico de barras. Esse é o tipo de gráfico padrão. Esse tipo de gráfico requer que uma procura salva seja uma procura agrupada. • **Linha** – Exibe os dados em um gráfico de linha. • **Setor** – Exibe os dados em um gráfico de pizza. Esse tipo de gráfico requer que uma procura salva seja uma procura agrupada. • **Barras Empilhadas** – Exibe os dados em um gráfico de barras empilhadas. • **Linhas Empilhadas** – Exibe os dados em um gráfico de linhas empilhadas. • **Tabela** – Exibe os dados em formato de tabela. A opção **Tabela** está disponível apenas para o contêiner de largura de página inteira.
Gráfico	Na lista, selecione o número de conexões a serem exibidas no relatório gerado.
Planejamento Manual	A área de janela Planejamento Manual é exibida apenas se você selecionou a opção de planejamento **Manualmente** no Assistente de Relatório. Para criar um planejamento manual: 1. Na caixa de listagem **De**, digite a data de início desejada para o relatório ou selecione a data usando o ícone **Calendário**. O padrão é a data atual. 2. Nas caixas de listagem, selecione o horário de início que deseja para o relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h. 3. Na lista **A**, digite a data de encerramento desejada para o relatório ou selecione a data usando o ícone **Calendário**. O padrão é a data atual. 4. Nas listas, selecione o horário de encerramento que deseja para o relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h.

Tabela 26. Parâmetros do gráfico Conexões (continuação)

Parâmetro	Descrição
Planejado de Hora em Hora	A área de janela Planejamento por Hora é exibida apenas se você selecionou a opção de planejamento **Por Hora** no Assistente de Relatório. O Planejamento por Hora insere automaticamente no gráfico todos os dados da hora anterior.
Planejamento Diário	A área de janela Planejamento Diário é exibida apenas se você selecionou a opção de planejamento **Diário** no Assistente de Relatório. Escolha uma das opções a seguir: • **Todos os dados do dia anterior (24 horas)** • **Dados do dia anterior a partir de** – Nas listas, selecione o período de tempo desejado para o relatório gerado. O horário está disponível em incrementos de meia hora. O padrão é 1h.
Planejamento Semanal	A área de janela Planejamento Semanal é exibida apenas se você selecionou a opção de planejamento **Semanal** no Assistente de Relatório. Escolha uma das opções a seguir: • **Todos os dados da semana anterior** • **Todos os dados da semana anterior** - Nas listas, selecione o período de tempo desejado para gerar relatório. O padrão é domingo.
Planejamento Mensal	A área de janela Planejamento Mensal é exibida apenas se você tiver selecionado a opção de planejamento **Mensal** no Assistente de Relatório. Escolha uma das opções a seguir: • **Todos os dados do mês anterior** • **Dados do mês anterior a partir de** – Nas listas, selecione o período de tempo que você deseja para o relatório gerado. O padrão é 1º a 31º.
Conteúdo do Gráfico	
Grupo	Na lista, selecione um grupo de procura salva para exibir as procuras salvas pertencentes ao grupo na lista **Procuras Salvas Disponíveis**.

Tabela 26. Parâmetros do gráfico Conexões (continuação)

Parâmetro	Descrição
Digitar Procura Salva ou Selecionar a partir da Lista	Para refinar a lista **Procuras Salvas Disponíveis**, digite o nome da procura que você deseja localizar no campo **Digitar procura salva ou selecionar na lista**. Também é possível digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite DMZ para exibir uma lista de todas as procuras que incluem DMZ no nome.
Procuras Salvas Disponíveis	Fornece uma lista de procuras salvas disponíveis. Por padrão, todas as procuras salvas disponíveis são exibidas. No entanto, você pode filtrar a lista selecionando um grupo na lista **Grupo** ou digitando o nome de uma procura salva conhecida no campo **Digitar Procura Salva ou Selecionar na Lista**.
Criar Nova Procura de Conexão	Clique em **Criar Nova Procura de Conexão** para criar uma nova procura.

Gráficos Regras de Dispositivo

É possível usar o gráfico Regras de Dispositivo para visualizar regras de firewall e a contagem de eventos de regras de firewall acionada em sua rede.

Os relatórios Regras de Dispositivo permitem criar um relatório para as seguintes regras de firewall:

- Regras de aceitação de dispositivo mais ativas
- Regras de negação de dispositivo mais ativas
- Regras de aceitação de dispositivo menos ativas
- Regras de negação de dispositivo menos ativas
- Regras de dispositivo não usadas
- Regras de dispositivo sombreadas

Os relatórios gerados permitem que você entenda quais regras são aceitas, negadas, não usadas ou não acionadas em um único dispositivo, um adaptador específico ou vários dispositivos. Relatórios permitem que o IBM Security QRadar Risk Manager automatize relatórios sobre o status de suas regras de dispositivo e exiba os relatórios no IBM Security QRadar SIEM Console.

Essa funcionalidade ajuda a identificar como regras são usadas em sua rede de dispositivos.

Para criar um contêiner Gráfico Regras de Dispositivo, configure valores para os seguintes parâmetros:

Tabela 27. Parâmetros do gráfico Regras de Dispositivo

Parâmetro	Descrição
Detalhes do Contêiner – Regras de Dispositivo	

Tabela 27. Parâmetros do gráfico Regras de Dispositivo (continuação)

Parâmetro	Descrição
Limitar Regras às Principais	Na lista, selecione o número de regras a serem exibidas no relatório gerado. Por exemplo, se você limitar o relatório às 10 regras principais e criar um relatório para as regras de aceitação mais usadas em todos os dispositivos, o relatório retornará 10 resultados. Os resultados contêm uma lista das 10 regras de aceitação mais usadas com base na contagem de eventos em todos os dispositivos que estão visíveis para o QRadar Risk Manager.

Tabela 27. Parâmetros do gráfico Regras de Dispositivo (continuação)

Parâmetro	Descrição
Tipo	Selecione o tipo de regras de dispositivo para exibir no relatório. As opções incluem: • **Regras de Aceitação Mais Usadas** – Exibe as regras de aceitação mais usadas por contagem de eventos para um único dispositivo ou um grupo de dispositivos. Este relatório lista as regras com contagem mais alta de eventos aceitos, em ordem decrescente, para o intervalo de tempo especificado no relatório. • **Regras de Negação Mais Usadas** – Exibe as regras de negação mais usadas por contagem de eventos para um único dispositivo ou um grupo de dispositivos. Este relatório lista as regras com contagem mais alta de eventos negados, em ordem decrescente, para o intervalo de tempo especificado no relatório. • **Regras Não Usadas** – Exibe quaisquer regras para um único dispositivo ou um grupo de dispositivos que não são usados. As regras não usadas têm zero contagens de eventos para o intervalo de tempo especificado para o relatório. • **Regras de Aceitação Menos Usadas** – Exibe as regras de aceitação menos usadas para um único dispositivo ou um grupo de dispositivos. Este relatório lista as regras com a contagem mais baixa de eventos aceitos, em ordem crescente, para o intervalo de tempo especificado no relatório. • **Regras de Negação Menos Usadas** – Exibe as regras de negação menos usadas para um único dispositivo ou um grupo de dispositivos. Este relatório lista as regras com a contagem mais baixa de eventos negados, em ordem crescente, para o intervalo de tempo especificado no relatório. • **Regras Sombreadas** – Exibe quaisquer regras para um único dispositivo que nunca podem ser acionadas porque a regra está bloqueada por uma regra de continuação. Os resultados exibem uma tabela da regra criando sombra e todas as regras que nunca podem ser acionadas em seu dispositivo porque são sombreadas por uma regra de continuação no dispositivo. **Nota:** Os relatórios de regras sombreadas só podem ser executados com relação a um único dispositivo. Essas regras têm zero contagens de eventos para o intervalo de tempo especificado para o relatório e são identificadas com um ícone na coluna Status.

Tabela 27. Parâmetros do gráfico Regras de Dispositivo (continuação)

Parâmetro	Descrição
Intervalo de Data/Hora	Selecione o intervalo de tempo para o relatório. As opções incluem: • **Configuração Atual** – Os resultados do relatório Regras de Dispositivo são baseados nas regras que existem na configuração atual do dispositivo. Esse relatório exibe regras e contagens de eventos para a configuração do dispositivo existente. A configuração atual para um dispositivo é baseada na última vez que o Gerenciamento da Origem da Configuração fez backup do seu dispositivo de rede. • **Intervalo** – Os resultados do relatório Regras de Dispositivo são baseados nas regras que existiam durante o período de tempo do intervalo. Esse relatório exibe regras e contagens de evento para o intervalo especificado na última hora para 30 dias. • **Intervalo Específico** – Os resultados do relatório Regras de Dispositivo são baseados nas regras que existiam entre o horário de início e o horário de encerramento do intervalo de tempo. Esse relatório exibe regras e contagens de evento para o intervalo de tempo especificado.
Fuso Horário	Selecione o fuso horário que deseja usar como base para seu relatório. O fuso horário padrão é baseado na configuração de seu QRadar SIEM Console. Ao configurar o parâmetro Fuso Horário para o relatório, considere a localização dos dispositivos associados com os dados relatados. Se o relatório usar dados abrangendo vários fusos horários, os dados usados para o relatório serão baseados no intervalo de tempo específico do fuso horário. Por exemplo, se o QRadar SIEM Console estiver configurado para Hora Padrão do Leste (EST) e você planejar um relatório diário entre 13h e 15h e configurar o fuso horário como Hora Padrão Central (CST), os resultados no relatório conterão informações das 14h às 16h EST.

Tabela 27. Parâmetros do gráfico Regras de Dispositivo (continuação)

Parâmetro	Descrição
Seleção de Dados de Destino	A Seleção de Dados de Destino é usada para filtrar o Intervalo de Data/Hora para um valor específico. Usando as opções Seleção de Dados de Destino, é possível criar um relatório para visualizar suas regras de dispositivo ao longo de um período de tempo definido customizado com a opção de incluir apenas dados das horas e dos dias selecionados. Por exemplo, é possível planejar um relatório para ser executado de 1 de outubro a 31 de outubro e visualizar suas regras mais ativas, menos ativas ou não usadas, além de suas contagens de regras que ocorrem durante o horário comercial, por exemplo, de segunda a sexta, das 8h às 21h. **Nota:** Os detalhes do filtro serão exibidos apenas quando você seleciona a caixa de seleção **Seleção de Dados de Destino** no Assistente de Relatório.
Formato	Selecione o formato para seu relatório de regras de dispositivo. As opções incluem: • **Um relatório agregado para dispositivos especificados** – Este formato de relatório agrega os dados do relatório em vários dispositivos. Por exemplo, se você criar um relatório para exibir as dez regras mais negadas, um relatório agregado exibirá as dez regras mais negadas em todos os dispositivos selecionados para o relatório. Esse relatório retorna 10 resultados no total para o relatório. • **Um relatório por dispositivo** – Este formato de relatório exibe os dados do relatório para um dispositivo. Por exemplo, se você criar um relatório para exibir as dez regras mais negadas, um relatório agregado exibirá as dez regras mais negadas para cada dispositivo selecionado para o relatório. Esse relatório retorna os 10 principais resultados para cada dispositivo selecionado para o relatório. Se você selecionou 5 dispositivos, o relatório retornará 50 resultados. **Nota:** Os relatórios de regras sombreadas têm capacidade de exibir apenas um relatório por dispositivo.

Tabela 27. Parâmetros do gráfico Regras de Dispositivo (continuação)

Parâmetro	Descrição
Dispositivos	Selecione os dispositivos incluídos no relatório. As opções incluem: • **Todos os Dispositivos** – Selecione esta opção para incluir todos os dispositivos no QRadar Risk Manager em seu relatório. • **Adaptador** – Na lista, selecione um tipo de adaptador para incluir no relatório. Apenas um tipo de adaptador pode ser selecionado na lista para um relatório. • **Dispositivos Específicos** – Selecione esta opção para incluir apenas dispositivos específicos em seu relatório. A janela Seleção de Dispositivo permite que você selecione e inclua dispositivos em seu relatório. Para incluir dispositivos individuais em seu relatório: 1. Clique em **Navegar** para exibir a janela Seleção de Dispositivo. 2. Selecione quaisquer dispositivos e clique em **Incluir Selecionado**. Para incluir todos os dispositivos em seu relatório: 1. Clique em **Navegar** para exibir a janela Seleção de Dispositivo. 2. Clique em **Incluir Todos**. Para procurar dispositivos para incluir no relatório: 1. Clique em **Navegar** para exibir a janela Seleção de Dispositivo. 2. Clique em **Procurar**. 3. Selecione as opções de procura para filtrar a lista completa de dispositivos por configuração obtida, endereço IP ou CIDR, nome do host, tipo, adaptador, fornecedor ou modelo. 4. Clique em **Procurar**. 5. Selecione quaisquer dispositivos e clique em **Incluir Selecionado**.

Gráficos Objetos de Dispositivo Não Usados

Um relatório Objetos de Dispositivo Não Usados exibe os grupos de referência do objeto que não estão sendo usados pelo seu dispositivo de rede.

Este relatório exibe referências do objeto, como uma coleta de endereço IP, variação de endereços CIDR ou ou nomes de hosts que não são usados por seu dispositivo de rede.

Ao configurar um contêiner de objetos não usados do dispositivo, você configura valores para os seguintes parâmetros:

Tabela 28. Parâmetros de relatório Objetos de Dispositivo Não Usados

Parâmetro	Descrição
Detalhes do Contêiner – Objetos de Dispositivo Não Usados	
Limitar Objetos aos Principais	Na lista, selecione o número de regras a serem exibidas no relatório gerado.
Dispositivos	Selecione os dispositivos incluídos no relatório. As opções incluem: • **Todos os Dispositivos** – Selecione esta opção para incluir todos os dispositivos no IBM Security QRadar Risk Manager em seu relatório. • **Adaptador** – Na lista, selecione um tipo de adaptador para incluir no relatório. Apenas um tipo de adaptador pode ser selecionado na lista para um relatório. • **Dispositivos Específicos** – Selecione esta opção para incluir apenas dispositivos específicos em seu relatório. A janela Seleção de Dispositivo permite que você selecione e inclua dispositivos em seu relatório. Para incluir dispositivos individuais em seu relatório: 1. Clique em **Navegar** para exibir a janela Seleção de Dispositivo. 2. Selecione quaisquer dispositivos e clique em **Incluir Selecionado**. Para incluir todos os dispositivos em seu relatório: 1. Clique em **Navegar** para exibir a janela Seleção de Dispositivo. 2. Clique em **Incluir Todos**. Para procurar dispositivos para incluir no relatório: 1. Clique em **Navegar** para exibir a janela Seleção de Dispositivo. 2. Clique em **Procurar**. 3. Selecione as opções de procura para filtrar a lista completa de dispositivos por configuração obtida, endereço IP ou CIDR, nome do host, tipo, adaptador, fornecedor ou modelo. 4. Clique em **Procurar**. 5. Selecione quaisquer dispositivos e clique em **Incluir Selecionado**.

Capítulo 11. Gerenciamento de política

Use as páginas Gerenciamento de Política do IBM Security QRadar Risk Manager para visualizar detalhes sobre conformidade de política e mudanças de risco de política para ativos, políticas e verificações de política.

As páginas Gerenciamento de Política do QRadar Risk Manager exibem dados da última política de execução. É possível filtrar os dados por ativo, por política ou por verificação de política.

Casos de uso de gerenciamento de política

Use as páginas Gerenciamento de Política com os itens de painel **Risco** para descobrir mais informações sobre ativos e políticas que não atenderam a conformidade.

- A página **Por Ativo** inclui informações e links para as políticas em que os ativos falharam.
- A página **Por Política** inclui informações sobre o número e a porcentagem de ativos que passaram ou falharam e, se relevante, um link para as verificações de política usadas pela política.
- A página **Por Verificação de Política** inclui informações sobre o número e as porcentagens de ativos que passam ou falham em verificações de política individuais.

Use as páginas Gerenciamento de Política com itens do painel **Mudança de Risco** para investigar políticas e verificações de políticas que exibem aumentos de risco. O item do painel **Mudança de Risco** contém links para as páginas **Por Política** e **Por Verificações de Política**.

Para obter informações adicionais sobre os itens do painel **Risco** e **Mudança de Risco**, consulte o *IBM Security QRadar SIEM Users Guide*.

Capítulo 12. Usar simulações no IBM Security QRadar Risk Manager

Use simulações para definir, planejar e executar simulações de exploração em sua rede. Você pode criar, visualizar, editar, duplicar e excluir simulações.

É possível criar simulações baseadas em uma série de regras que podem ser combinadas e configuradas. A simulação pode ser planejada para ser executada periodicamente ou manualmente. Depois de uma simulação ser concluída, é possível revisar os resultados da simulação e aprovar qualquer resultado aceitável ou de baixo risco que seja baseado em sua política de rede. Quando você revisa resultados, é possível aprovar ações aceitáveis ou o tráfego de seus resultados. Após o ajuste de sua simulação, é possível configurar a simulação para monitorar os resultados.

Ao monitorar uma simulação, você pode definir como deseja que o sistema responda quando os resultados não aprovados são retornados. Uma resposta do sistema pode ser um email, a criação de um evento ou o envio de uma resposta para syslog.

Simulações podem ser modeladas a partir de uma topologia ou modelo de topologia atual.

A página Simulação resume informações sobre simulações e resultados de simulação.

Os resultados da simulação são exibidos apenas após ela ser concluída. Depois de uma simulação ser concluída, a coluna **Resultados** lista as datas e os resultados correspondentes de sua simulação.

Simulações

Simulações criadas pelos usuários e os resultados da simulação podem ser visualizados na página Simulações.

A janela Simulações fornece as seguintes informações:

Tabela 29. Parâmetros de definições de simulação

Parâmetro	Descrição
Nome da Simulação	O nome da simulação, conforme definido pelo criador da simulação.
Modelo	O tipo de modelo. Simulações podem ser modeladas a partir de uma topologia ou modelo de topologia atual. As opções são: • Topologia Atual • O nome do modelo de topologia.
Grupos	Os grupos aos quais a simulação está associada.
Criado por	O usuário que criou a simulação.
Data de Criação	A data e a hora em que a simulação foi criada.

Tabela 29. Parâmetros de definições de simulação (continuação)

Parâmetro	Descrição
Última Modificação	A data e a hora em que a simulação foi modificada pela última vez.
Planejamento	A frequência com que a simulação está planejada para ser executada. As opções incluem: • **Manual** - A simulação é executada manualmente. • **Uma Vez** – Especifique a data e hora em que a simulação está planejada para ser executada. • **Diariamente** – Especifique a hora do dia em que a simulação está planejada para ser executada. • **Semanalmente** – Especifique o dia da semana e a hora em que a simulação está planejada para ser executada. • **Mensalmente** – Especifique o dia do mês e a hora em que a simulação está planejada para ser executada.
Última Execução	A última data e hora em que a simulação foi executada.
Próxima Execução	A data e a hora em que a simulação seguinte será executada.
Resultados	Se a simulação foi executada, esse parâmetro incluirá uma lista que contém uma lista de datas com os resultados de sua simulação. Se a simulação não foi executada, a coluna Resultados exibirá Sem Resultados.

Criando uma simulação

É possível criar simulações baseadas em uma série de regras que podem ser combinadas e configuradas.

Sobre Esta Tarefa

Os parâmetros que podem ser configurados para testes de simulação são sublinhados. A tabela a seguir descreve os testes de simulação que você pode configurar.

Tabela 30. Testes de simulação

Nome do Teste	Descrição	Parâmetros
Ataque contra um dos seguintes endereços IP	Simula ataques com relação a endereços IP ou intervalos CIDR específicos.	Configure o parâmetro de endereços IP para especificar o endereço IP ou intervalos CIDR aos quais deseja que a simulação se aplique.
Ataque contra uma das seguintes redes	Simula ataques contra redes que são membros de um ou mais locais de rede definidos.	Configure o parâmetro de redes para especificar as redes às quais deseja que a simulação se aplique.

Tabela 30. Testes de simulação (continuação)

Nome do Teste	Descrição	Parâmetros
Ataque contra um dos seguintes blocos de construção ativos	Simula ataques contra um ou mais blocos de construção de ativo definidos.	Configure os parâmetros de bloco de construção de ativo para especificar os blocos de construção de ativo aos quais deseja que a simulação se aplique.
Ataque contra um dos seguintes conjuntos de referência	Simula ataques contra uma ou conjuntos de referência definidos.	Configure os parâmetros de conjunto de referência para especificar a quais deseja que essa simulação se aplique.
Ataque contra uma vulnerabilidade em uma das seguintes portas usando protocolos	Simula ataques contra uma vulnerabilidade em uma ou mais portas definidas.	Configure os seguintes parâmetros: • Portas Abertas - Especifique as portas que você deseja que sejam consideradas por esta simulação. • Protocolos – Especifique o protocolo que você deseja que seja considerado por esta simulação.
Ataque contra ativos suscetíveis a uma das seguintes vulnerabilidades	Simula ataques contra ativos suscetíveis a uma ou mais vulnerabilidades definidas.	Configure o parâmetro **vulnerabilidades** para identificar as vulnerabilidades às quais deseja que este teste se aplique. É possível procurar vulnerabilidades no ID OSVDB, ID Bugtraq, ID CVE ou título.
Ataque contra ativos suscetíveis a vulnerabilidade com uma das seguintes classificações	Permite simular ataques contra um ativo que seja suscetível a vulnerabilidades para uma ou mais classificações definidas.	Configure o parâmetro **classificações** para identificar as classificações de vulnerabilidade. Por exemplo, uma classificação de vulnerabilidade pode ser Manipulação de Entrada ou Negação de Serviço.
Ataque contra ativos suscetíveis a vulnerabilidades com pontuação CVSS maior que 5	Um valor Common Vulnerability Scoring System (CVSS) é um padrão de mercado para avaliar a gravidade das vulnerabilidades. Essa simulação filtra ativos em sua rede que incluem o valor CVSS configurado. Permite simular ataques contra um ativo que seja suscetível a vulnerabilidade com uma pontuação CVSS maior que 5.	Configure os seguintes parâmetros: • **maior que** – Especifique se a pontuação Common Vulnerability Scoring System (CVSS) é maior que, maior que ou igual a, menor que, menor que ou igual a, igual a ou não igual ao valor configurado. O padrão é maior que. • **5** – Especifique a pontuação CVSS que você deseja que este teste considere. O padrão é 5.

Tabela 30. Testes de simulação (continuação)

Nome do Teste	Descrição	Parâmetros
Ataque contra ativos suscetíveis a vulnerabilidades divulgadas após essa data	Permite simular ataques contra um ativo que seja suscetível a vulnerabilidades descobertas antes, depois ou na data configurada.	Configure os seguintes parâmetros: • **antes de** | **depois de** | **em** - Especifique se deseja que a simulação considere as vulnerabilidades divulgadas como antes de, depois de ou em datas configuradas nos ativos. O padrão é antes. • **esta data** – Especifique a data que você deseja que esta simulação considere.
Ativos de meta de ataque suscetíveis a vulnerabilidades em que o nome, o fornecedor, a versão ou o serviço contém uma das entradas de texto a seguir	Permite simular ataques contra um ativo que seja suscetível a vulnerabilidades correspondentes ao nome do ativo, fornecedor, versão ou serviço com base em um ou mais entrada de texto.	Configure o parâmetro **entradas de texto** para identificar o nome do ativo, fornecedor, versão ou serviço que deseja que esta simulação considere.
Ativos de meta de ataque suscetíveis a vulnerabilidades em que o nome, o fornecedor, a versão ou o serviço contém uma das expressões regulares a seguir	Permite simular ataques contra um ativo que seja suscetível a vulnerabilidades correspondentes ao nome do ativo, fornecedor, versão ou serviço com base em uma ou mais expressões regulares.	Configure o parâmetro **expressões regulares** parâmetro para identificar o nome do ativo, fornecedor, versão ou serviço que deseja que esta simulação considere.

Os seguintes testes de contribuição foram descontinuados e ocultos no Monitor de Política:

- **ataque contra uma vulnerabilidade em um dos seguintes sistemas operacionais**
- **ataque contra ativos suscetíveis a vulnerabilidades de um dos seguintes fornecedores**
- **ataque contra ativos suscetíveis a vulnerabilidades de um dos seguintes produtos**

Os testes de contribuição descontinuados foram substituídos por outros testes.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. No menu **Ações**, selecione **Novo**.
4. Digite um nome para a simulação no parâmetro **Como você deseja nomear esta simulação**.
5. Na lista suspensa **Em qual modelo você deseja basear isto**, selecione o tipo de dados que você deseja retornar. Todos os modelos existentes de topologia são listados. Se você selecionar **Topologia Atual**, a simulação usará o modelo de topologia atual.
6. Escolha uma das opções a seguir:

Opção	Descrição
Selecione Usar Dados de Conexão	A simulação é baseada em dados de conexão e topologia.
Limpe Usar Dados de Conexão	A simulação é baseada apenas em dados de topologia. Se seu modelo de topologia não incluir nenhum dado e você desmarcar a caixa de seleção **Usar Dados de Conexão**, a simulação não retornará nenhum resultado.

7. Na lista **Fator de Importância**, selecione o nível de importância que deseja associar a essa simulação.

   O Fator de Importância é usado para calcular a Pontuação de Risco. O intervalo é de 1 (baixa importância) a 10 (alta importância). O padrão é 5.
8. Na lista **Onde você deseja que comece a simulação**, selecione uma origem para a simulação.

   O valor escolhido determina o ponto de início da simulação. Por exemplo, o ataque se origina em uma rede específica. O parâmetros de simulação selecionados são exibidos na janela **Gerar uma simulação onde**.
9. Inclua destinos de ataque de simulação para o teste de simulação.
10. Usando as simulações que você deseja incluir no campo de ataque, selecione o sinal **+** ao lado da simulação que deseja incluir.

    As opções de simulação são exibidas na janela **Gerar uma simulação onde**.
11. Na janela **Gerar uma simulação onde**, clique em qualquer parâmetro sublinhado para configurar ainda mais quaisquer parâmetros de simulação.
12. Na lista suspensa **Executar esta simulação para**, selecione o número de etapas para as quais deseja executar esta simulação (1 a 5).
13. Na lista drop-down de etapas, escolha o planejamento para executar a simulação.
14. Na área de grupos, selecione uma caixa de seleção para qualquer grupo para o qual você deseja designar essa simulação.
15. Clique em **Salvar Simulação**.

Editando uma simulação

É possível editar simulações.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Selecione a definição de simulação que você deseja editar.
4. No menu **Ações**, selecione **Editar**.
5. Atualize os parâmetros, conforme necessário.

   Para obter mais informações sobre os parâmetros de simulação, consulte Testes de simulação.
6. Clique em **Salvar Simulação**.

Duplicando uma simulação

É possível duplicar simulações.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Selecione a simulação que você deseja duplicar.
4. No menu **Ações**, selecione **Duplicar**.
5. Digite o nome para a simulação.
6. Clique em **OK**.

Excluindo uma simulação

É possível excluir simulações.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Selecione a simulação que você deseja excluir.
4. No menu **Ações**, selecione **Excluir**.
5. Clique em **OK**.

Executando uma simulação manualmente

Utilize o Editor de Simulação para executar manualmente uma simulação.

Procedimento

1. Clique na guia **Riscos**.
2. No menu **Ações**, selecione **Executar Simulação**.
3. Clique em **OK**.

Resultados

O processo de simulação poderá durar um período de tempo estendido. Enquanto a simulação é executada, a coluna Próxima Execução indica a porcentagem concluída. Na conclusão, a coluna Resultados exibe a data e hora da simulação.

Se você executar uma simulação e, em seguida, executar mudanças que afetam os testes associados com a simulação, essas mudanças podem demorar até uma hora para serem exibidas.

Gerenciando resultados da simulação

Depois de uma simulação ser executada, a coluna Resultados exibe uma lista suspensa contendo uma lista das datas em que ela foi gerada.

Os resultados da simulação são mantidos por 30 dias. Os resultados só são exibidos na coluna Resultados após a simulação ser executada.

Visualizando resultados da simulação

É possível visualizar os resultados da simulação na coluna Resultados da página Simulações.

Sobre Esta Tarefa

Os resultados só são exibidos na coluna Resultados após a simulação ser executada. Os resultados da simulação fornecem informações sobre cada etapa da simulação.

Por exemplo, a primeira etapa de uma simulação fornece uma lista dos ativos conectados diretamente afetados pela simulação. A segunda etapa lista ativos em sua rede que podem se comunicar com ativos de primeiro nível em sua simulação.

Quando você clica em Visualizar Resultado, as seguintes informações são fornecidas:

Tabela 31. Informações do resultado da simulação

Parâmetro	Descrição
Definição de Simulação	A descrição da simulação.
Usando Modelo	O nome do modelo com relação ao qual a simulação foi executada.
Resultado da Simulação	A data na qual a simulação foi executada.
Resultados da Etapa	O número de etapas para o resultado incluindo a etapa que está atualmente sendo exibida.
Ativos Comprometidos	O número do total de ativos comprometidos nesta etapa e em todas as etapas de simulação. Se o modelo de topologia incluir dados de um intervalo IP de /32 definido como acessível, o IBM Security QRadar Risk Manager não validará esses ativos com relação ao banco de dados. Portanto, esses ativos não são consideradas no total de Ativos Comprometidos. O QRadar Risk Manager apenas valida os ativos em intervalos IP mais amplos, como /24, para determinar quais ativos existem.
Pontuação de Risco	A pontuação de riscos é um valor calculado com base no número de resultados, etapas, número de ativos comprometidos e fator de importância designado à simulação. Esse valor indica o nível de severidade associado à simulação para a etapa exibida.

É possível mover o ponteiro do mouse sobre uma conexão para determinar a lista de ativos afetados por esta simulação.

Os 10 principais ativos serão exibidas quando você mover o mouse sobre a conexão.

Mova o ponteiro do mouse sobre a conexão para destacar o caminho por meio da rede, conforme definido pela sub-rede.

A página de resultado da simulação fornece uma tabela chamada Resultados para esta etapa. Essa tabela fornece as informações a seguir:

Tabela 32. Resultados para estas informações da etapa

Parâmetro	Descrição
Aprovar	Permite aprovar os resultados da simulação. Consulte Aprovando resultados da simulação.
Pai	O endereço IP de origem para a etapa exibida da simulação.
IP	O endereço IP do ativo afetado.
Rede	A rede dos endereços IP de destino, conforme definido na hierarquia da rede.
Nome do Recurso	O nome do ativo afetado, conforme definido pelo perfil do ativo.
Peso do Ativo	O peso do ativo afetado, conforme definido no perfil do ativo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Na coluna Resultados, selecione a data e a hora da simulação que você deseja visualizar utilizando a lista.
4. Clique em **Visualizar Resultados**. Você pode visualizar as informações de resultado de simulação, começando na etapa 1 da simulação.
5. Visualize os Resultados para esta tabela Etapa para determinar os ativos afetados.
6. Para visualizar a próxima etapa dos resultados da simulação, clique em **Próxima Etapa**.

Aprovando resultados da simulação

É possível aprovar resultados de simulação.

Sobre Esta Tarefa

Deve-se aprovar o tráfego de rede que é considerado de baixo risco ou comunicação normal no ativo. Ao aprovar resultados, você filtra a lista de resultados para que as simulações futuras ignorem as comunicações normais ou aprovadas.

Os resultados só são exibidos na coluna Resultados após a simulação ser executada.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Na coluna Resultados, selecione a data e a hora da simulação que você deseja visualizar utilizando a lista.
4. Clique em **Visualizar Resultados**.
5. Na tabela Resultados para esta etapa, utilize um dos seguintes métodos para aprovar ativos:

Opção	Descrição
Aprovar Selecionado	Selecione a caixa de seleção para cada ativo que você deseja aprovar e, em seguida, clique em **Aprovar selecionados.**
Aprovar Todos	Clique para aprovar todos os ativos listados.

6. Opcional. Clique em **Visualizar Aprovado** para visualizar todos os ativos aprovados.

Revogando aprovação de simulação

É possível deixar uma comunicação ou conexão aprovada desativada na lista aprovada. Depois de um resultado de simulação aprovado ser removido, simulações futuras exibem comunicações não aprovadas nos resultados da simulação.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Na coluna Resultados, selecione a data e a hora da simulação que você deseja visualizar utilizando a lista.
4. **Visualizar Resultado**.
5. Clique em **Visualizar Aprovado** para visualizar todos os ativos aprovados.
6. Escolha uma das opções a seguir:

Opção	Descrição
Revogar Selecionado	Selecione a caixa de seleção para cada ativo que você deseja revogare, em seguida, clique em **Revogar Selecionados.**
Revogar Todos	Clique para revogar todos os ativos listados.

Monitorando simulações

Você pode monitorar uma simulação para determinar se os resultados da simulação mudaram. Se ocorrer uma mudança, um evento será gerado. No máximo 10 simulações podem estar no monitor mode.

Sobre Esta Tarefa

Quando uma simulação está no monitor mode, o intervalo de tempo padrão é 1 hora. Esse valor substitui o valor de tempo configurado quando a simulação foi criada.

Para obter informações sobre as categorias de eventos, consulte o *IBM Security QRadar SIEM Users Guide*.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Selecione a simulação que você deseja monitorar.
4. Clique em **Monitor**.

5. No campo **Nome de Eventos**, digite o nome do evento que você deseja exibir nas guias **Atividade do Log** e **Ofensas**.
6. No campo **Descrição do Evento**, digite uma descrição para o evento. A descrição é exibida em Anotações nos detalhes do evento.
7. Na lista **Categoria de Alto Nível**, selecione a categoria de evento de alto nível que você quer que esta simulação use ao processar eventos.
8. Na lista **Categoria de Baixo Nível**, selecione a categoria de evento de baixo nível que você quer que esta simulação use ao processar eventos.
9. Selecione a caixa de seleção **Assegure-se de que o evento de dispatch faça parte de uma ofensa** se quiser, como resultado dessa simulação monitorada, os eventos que são encaminhados para o componente Funcionários Públicos. Se nenhuma ofensa foi gerada, uma nova será criada. Se uma ofensa existir, esse evento será incluído na ofensa existente. Se você selecionar a caixa de seleção, escolha uma das seguintes opções:

Opção	Descrição
Pergunta/Simulação	Todos os eventos de uma pergunta são associados a uma única ofensa.
Ativo	Uma ofensa exclusiva é criada (ou atualizada) para cada ativo exclusivo.

10. Na seção **Ações Adicionais**, selecione uma ou mais das seguintes opções:

Opção	Descrição
Email	Selecione esta caixa de seleção e especifique o endereço de email para o qual enviará notificações se o evento for gerado. Use uma vírgula para separar diversos endereços de email.
Enviar para Syslog	Selecione esta caixa de seleção se desejar registrar o evento. Por exemplo, a saída syslog pode se parecer com: `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`
Notificação	Marque esta caixa de seleção se você quiser que os eventos que são gerados como resultado dessa pergunta monitorada sejam exibidos no item Notificações do Sistema no Painel.

11. Na seção **Ativar Monitor**, selecione a caixa de seleção para monitorar a simulação.
12. Clique em **Salvar Monitor**.

Agrupando simulações

Designar simulações a grupos é uma maneira eficiente de visualizar e controlar todas as simulações. Por exemplo, é possível visualizar todas as simulações que estão relacionadas à conformidade.

Sobre Esta Tarefa

Conforme você cria novas simulações, é possível designá-las a um grupo existente.

Depois de criar um grupo, é possível arrastar grupos na árvore de menu para alterar a organização.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Clique em **Grupos**.
4. Na árvore de menus, selecione o grupo sob o qual deseja criar um novo grupo.
5. Clique em **Novo**.
6. No campo **Nome**, digite um nome para o novo grupo. O nome do grupo pode ter até 255 caracteres de comprimento.
7. No campo **Descrição**, digite uma descrição para o grupo. A descrição pode ter até 255 caracteres de comprimento.
8. Clique em **OK**.

Editando um grupo

É possível editar um grupo.

Sobre Esta Tarefa

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione o grupo que deseja editar.
5. Clique em **Editar**.
6. Atualize as informações nos campos Nome e Descrição conforme requerido.
7. Clique em **OK**.

Copiando um item em outro grupo

Usando a funcionalidade de grupos, é possível copiar uma simulação em um ou vários grupos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione a pergunta que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo no qual deseja copiar a simulação.
7. Clique em **Copiar**.

Excluindo um item de um grupo

É possível excluir um item de um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.

3. Clique em **Grupos**.
4. Na árvore de menu, selecione o grupo de nível superior.
5. Na lista de grupos, selecione o item ou grupo que deseja excluir.
6. Clique em **Remover**.
7. Clique em **OK**.

Designando um item a um grupo

É possível designar uma simulação a um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Selecione a simulação que você deseja designar a um grupo.
4. Usando o menu **Ações**, selecione **Designar Grupos**.
5. Selecione o grupo ao qual você deseja que a pergunta seja designada.
6. Clique em **Designar Grupos**.

Capítulo 13. Modelos de topologia

É possível usar um modelo de topologia para definir modelos de rede virtual com base em sua rede existente.

É possível criar um modelo de rede com base em uma série de modificações que podem ser combinadas e configuradas. Isso permite que você determine o efeito das mudanças de configuração em sua rede usando uma simulação. Para obter mais informações sobre simulações, consulte Usando simulações.

É possível visualizar modelos de topologia na página Simulações. Modelos de topologia fornecem as seguintes informações:

Tabela 33. Parâmetros de definição de modelo

Parâmetro	Descrição
Nome do modelo	O nome do modelo de topologia, conforme definido pelo usuário quando criado.
Grupo(s)	Os grupos aos quais essa topologia é associada.
Criado por	O usuário que criou a definição de modelo.
Criado em	A data e a hora em que a definição de modelo foi criada.
Última Modificação	O número de dias desde que a definição de modelo foi criada.

Criando um modelo de topologia

É possível criar um ou mais modelos de topologia.

Sobre Esta Tarefa

A tabela a seguir descreve os nomes de teste e parâmetros que você pode configurar.

Tabela 34. Testes de topologia

Nome do Teste	Parâmetros
Uma regra será incluída nos dispositivos selecionados que permitem conexões a partir de CIDRs de origem para CIDRs de destino em protocolos, portas	Configure os seguintes parâmetros: • **Dispositivos** – Especifique os dispositivos nos quais deseja incluir esta regra. Na janela Customizar Parâmetro, selecione a caixa de seleção Todos para incluir todos os dispositivos ou procure dispositivos usando um dos seguintes critérios de procura: – **IP/CIDR** – Selecione a opção IP/CIDR e especifique o endereço IP ou CIDR no qual deseja incluir esta regra. – **Nome do host** - Selecione a opção Nome do host e especifique o nome do host que deseja filtrar. Para procurar vários nomes de host, use um caractere curinga (*) no início ou no final da sequência. – **Adaptador** – Selecione a opção Adaptador e use a lista suspensa para filtrar a lista de dispositivos por adaptador. – **Fornecedor** – Selecione a opção Fornecedor e use a lista suspensa para filtrar a lista de dispositivos por fornecedor. Também é possível especificar um modelo para o fornecedor. Para procurar vários modelos, use um caractere curinga (*) no início ou no final da sequência. • **permite** | **nega** – Selecione a condição (aceito ou negado) para conexões às quais deseja que este teste se aplique. • **CIDRs** – Selecione quaisquer endereços IP de origem ou intervalos CIDR que deseja incluir nesta regra. • **CIDRs** – Selecione quaisquer endereços IP de destino ou intervalos CIDR que deseja incluir nesta regra. • **Protocolos** – Especifique os protocolos que deseja incluir nesta regra. Para incluir todos os protocolos, selecione a caixa de seleção Todos. • **Portas** – Especifique as portas que deseja incluir nesta regra. Para incluir todas as portas, selecione a caixa de opções Todos.

Tabela 34. Testes de topologia (continuação)

Nome do Teste	Parâmetros
Uma regra será incluída nos dispositivos IPS selecionados que permitem conexões a partir de CIDRs de origem para CIDRs de destino com as vulnerabilidades	Configure os seguintes parâmetros: • **Dispositivos IPS** – Especifique os dispositivos IPS que você quer que este modelo de topologia inclua. Para incluir todos os dispositivos IPS, selecione a caixa de seleção Todos. • permite | nega - Especifique a condição (aceito ou negado) para conexões às quais deseja que este teste se aplique. • **CIDRs** – Especifique quaisquer endereços IP de origem ou intervalos CIDR que você quer que este modelo de topologia inclua. • **CIDRs** – Especifique quaisquer endereços IP de destino ou intervalos CIDR que você quer que este modelo de topologia inclua. • **Vulnerabilidades** – Especifique as vulnerabilidades que deseja aplicar ao modelo de topologia. É possível procurar vulnerabilidades usando o ID Bugtraq, ID OSVDB, ID CVE ou título.
Os ativos a seguir permitem conexões com as portas selecionadas	Configure os seguintes parâmetros: • ativos - Especifique os ativos que você quer que este modelo de topologia inclua. • **permitir** | negar - Especifique a condição (permitir ou negar) para conexões às quais deseja que este modelo de topologia se aplique. O padrão é permitir. • portas – Especifique as portas que você deseja que este modelo de topologia inclua. Para incluir todas as portas, selecione a caixa de opções Todos.
Ativos nos blocos de construção de ativo a seguir permitem conexão com portas	Configure os seguintes parâmetros: • blocos de construção de ativos - Especifique os blocos de construção que você deseja que este modelo de topologia inclua. • **permitir** | negar - Especifique a condição (permitir ou negar) que você deseja que este modelo de topologia aplique. O padrão é permitir. • **portas** – Especifique as portas que você deseja que este modelo de topologia inclua. Para incluir todas as portas, selecione a caixa de opções Todos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**
3. No menu **Ações**, selecione Novo.

4. No campo **Como deseja nomear este modelo**, digite um nome para a definição de modelo.
5. Na área de janela **Quais modificações deseja aplicar ao modelo**, selecione as modificações que você deseja aplicar à topologia para criar seu modelo.
6. Configure os testes incluídos na área de janela **Configurar modelo como a seguir**.
7. Quando o teste é exibido na área da janela, os parâmetros configuráveis são sublinhados. Clique em cada parâmetro para configurar ainda mais essa modificação para seu modelo. Na área de grupos, selecione a caixa de seleção para designar grupos a esta questão.
8. Clique em **Salvar Modelo.**

Editando um modelo de topologia

É possível editar um modelo de topologia.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**.
3. Selecione a definição de modelo que você deseja editar.
4. No menu **Ações**, selecione Editar.
5. Atualize os parâmetros, conforme necessário.

   Para obter mais informações sobre os parâmetro do Editor de Modelo, consulte Criando um modelo de topologia.
6. Clique em **Salvar Modelo**.

Duplicando um modelo de topologia

É possível duplicar um modelo de topologia.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**.
3. Selecione a definição de modelo que deseja duplicar.
4. No menu **Ações**, selecione **Duplicar**.
5. Digite um nome que você deseja designar ao modelo de topologia copiado.
6. Clique em **OK**.
7. Edite o modelo.

Excluindo um modelo de topologia

É possível excluir um modelo de topologia.

Procedimento

1. Clique na guia **Risco**s.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**.
3. Selecione a definição de modelo que deseja excluir.
4. No menu **Ações**, selecione **Excluir**.
5. Clique em **OK**.

Agrupar modelos de topologia

É possível agrupar e visualizar seus modelos de topologia com base em seus critérios escolhidos.

A categorização de seu modelo de topologia é uma maneira eficiente de visualizar e controlar seus modelos. Por exemplo, é possível visualizar todos os modelos de topologia relacionados à conformidade.

Conforme você cria novos modelos de topologia, é possível designar os modelos de topologia a um grupo existente. Para obter informações sobre como designar um grupo, consulte Criando um modelo de topologia.

Visualizando grupos

É possível visualizar modelos de topologia usando grupos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**.
3. Usando a lista **Grupo**, selecione o grupo que deseja visualizar.

Criando um grupo

É possível criar um grupo para visualizar e controlar de modo eficiente os modelos de topologia.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**.
3. Clique em **Grupos**.
4. Na árvore de menus, selecione o grupo sob o qual deseja criar um novo grupo.

   Após criar o grupo, é possível arrastar e soltar os grupos nos itens da árvore de menu para alterar a organização.
5. Clique em **Novo**.
6. Digite o nome que deseja designar ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
7. Digite uma descrição para o grupo. A descrição pode ter até 255 caracteres de comprimento.
8. Clique em **OK**.
9. Se desejar alterar a localização do novo grupo, clique no novo grupo e arraste a pasta para o local em seu menu de árvore.

Editando um grupo

É possível editar um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Modelos de Topologia**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione o grupo que deseja editar.
5. Clique em **Editar**.

6. Atualize os valores para os parâmetros
7. Clique em **OK**.
8. Se desejar alterar o local do grupo, clique no novo grupo e arraste a pasta para o local na árvore de menu.

Copiando um item em outro grupo

Usando a funcionalidade de grupos, é possível copiar um modelo de topologia para um ou vários grupos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulações** > **Modelos de Topologia**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione a pergunta que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo no qual deseja copiar a simulação.
7. Clique em **Copiar**.

Excluindo um item de um grupo

É possível excluir um item de um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Clique em **Grupos**.
4. Na árvore de menu, selecione o grupo de nível superior.
5. Na lista de grupos, selecione o item ou grupo que deseja excluir.
6. Clique em **Remover**.
7. Clique em **OK**.

Designar uma topologia a um grupo

É possível designar um modelo de topologia a um grupo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Selecione o modelo de topologia você deseja designar a um grupo.
4. No menu **Ações**, selecione **Designar Grupo**.
5. Selecione o grupo ao qual você deseja que a pergunta seja designada.
6. Clique em **Designar Grupos**.

Capítulo 14. Dados do log de auditoria

As mudanças feitas por usuários do IBM Security QRadar Risk Manager são registradas na guia **Atividade do Log** do IBM Security QRadar SIEM.

Todos os logs exibidos na categoria Auditoria do Risk Manager. Para obter mais informações sobre o uso da guia **Atividade do Log** no QRadar SIEM, consulte o *IBM Security QRadar SIEM Users Guide*.

Ações registradas

Ações são registradas para os componentes.

A tabela a seguir lista as categorias e ações correspondentes que são registradas.

Tabela 35. Ações registradas

Categoria	Ação
Monitor de política	Criar uma pergunta.
	Editar uma pergunta.
	Excluir uma pergunta.
	Enviar uma pergunta manualmente.
	Enviar uma pergunta automaticamente.
	Aprovar resultados.
	Revogar aprovação de resultados.
Modelo de Topologia	Criar um modelo de topologia.
	Editar um modelo de topologia.
	Excluir um modelo de topologia.
Topologia	Salvar layout.
	Criar uma procura salva da topologia.
	Editar uma procura salva da topologia
	Excluir uma procura salva da topologia
	Colocando um IPS.
Monitor de Configuração	Criar um mapeamento de origem de log
	Editar um mapeamento de origem de log
	Excluir um mapeamento de origem de log
Simulações	Criar uma simulação.
	Editar uma simulação.
	Excluir uma simulação.
	Executar manualmente uma simulação.
	Executar automaticamente uma simulação.
	Aprovar resultados de simulação.
	Revogar resultados de simulação.

Tabela 35. Ações registradas (continuação)

Categoria	Ação
Gerenciamento de Origem de Configuração	Autenticar uma sessão pela primeira vez com sucesso.
	Incluir um dispositivo.
	Remover um dispositivo.
	Editar o endereço IP ou adaptador para um dispositivo.
	Salvar uma configuração de credencial.
	Excluir uma configuração de credencial.
	Salvar uma configuração de protocolo.
	Remover uma configuração de protocolo.
	Criar um planejamento para uma tarefa de backup.
	Excluir um planejamento para uma tarefa de backup.
	Editar uma tarefa de backup.
	Incluir uma tarefa de backup.
	Excluir uma tarefa de backup.
	Executar uma tarefa de backup planejado.
	Concluir uma tarefa planejada se a tarefa for bem-sucedida ou falhar.
	Depois que uma tarefa de backup tiver concluído o processamento e a configuração foi persistida, nenhuma mudança será descoberta.
	Depois que uma tarefa de backup tiver concluído o processamento e a configuração foi persistida, mudanças foram descobertas.
	Depois que uma tarefa de backup tiver concluído o processamento e a configuração foi persistida, mudanças não persistidas foram descobertas.
	Depois que uma tarefa de backup tiver concluído o processamento e a configuração que foi persistida anteriormente não residir mais no dispositivo.
	A tentativa de operação do adaptador foi iniciada, o que inclui protocolos e credenciais.
	A tentativa de operação do adaptador foi bem-sucedida, incluindo protocolos e credenciais.

Visualizando atividade do usuário

É possível visualizar a atividade de usuários do IBM Security QRadar Risk Manager.

Procedimento

1. Clique na guia **Atividade do Log**. Se você salvou anteriormente uma procura como o padrão, os resultados para essa procura salva serão exibidos.
2. Clique em **Procurar** > **Nova Procura** para criar uma procura.
3. Na área de janela **Intervalo de Tempo**, selecione uma opção para o intervalo de tempo que você deseja capturar para essa procura.
4. Na área de janela **Parâmetros de Procura**, defina seus critérios de procura:
   a. Na primeira lista, selecione **Categoria**.
   b. Na lista suspensa **Categoria de Alto Nível** , selecione **Auditoria do Risk Manager**.
   c. Opcional. Na lista suspensa **Categoria de Baixo Nível**, selecione uma categoria para refinar sua procura.
5. Clique em **Incluir Filtro**.
6. Clique em **Filtro** para procurar por eventos do QRadar Risk Manager.

Visualizando o arquivo de log

Logs de auditoria, que são armazenados em texto simples, são arquivados e compactados quando o arquivo de log de auditoria atinge um tamanho de 200 MB.

Sobre Esta Tarefa

O arquivo de log atual for denominado audit.log. Se o arquivo de log de auditoria atingir um tamanho de 200 MB uma segunda vez, ele será compactado e o log de auditoria antigo será renomeado como audit.1.gz. O número do arquivo é incrementado cada vez que um arquivo de log é arquivado. O IBM Security QRadar Risk Manager pode armazenar até 50 arquivos de log arquivados.

O tamanho máximo de qualquer mensagem de auditoria (não incluindo data, hora e nome do host) é de 1024 caracteres.

Cada entrada no arquivo de log é exibida utilizando o seguinte formato:

```
<date_time> <host name> <user>@<IP address>
(thread ID) [<category>] [<sub-category>]
[<action>] <payload>
```

A tabela a seguir descreve os parâmetros utilizados no arquivo de log.

Tabela 36. Informações do arquivo de log de auditoria

Parâmetro	Descrição
<date_time>	A data e hora da atividade no formato: Mês Data HH:MM:SS.
<host name>	O nome do host do Console no qual esta atividade foi registrada.
<user>	O nome do usuário que executou a ação.
<IP address>	O endereço IP do usuário que executou a ação.
(thread ID)	O identificador do encadeamento Java™ que registrou essa atividade.
<category>	A categoria de alto nível desta atividade.
<sub-category>	A categoria de nível inferior desta atividade.

Tabela 36. Informações do arquivo de log de auditoria (continuação)

Parâmetro	Descrição
<action>	A atividade que ocorreu.
<payload>	O registro completo que foi alterado, se houver.

Procedimento

1. Ao usar o SSH, efetue login no seu IBM Security QRadar SIEM Console como o usuário raiz.
2. Usando o SSH a partir do IBM Security QRadar SIEM Console, efetue login no dispositivo do QRadar Risk Manager como um usuário raiz.
3. Acesse o seguinte diretório: `/var/log/audit`
4. Abra o arquivo de log de auditoria.

Detalhes do arquivo de log

Os administradores usam os arquivos de log do IBM Security QRadar Risk Manager para visualizar a atividade do usuário e solucionar problemas do sistema.

A tabela a seguir descreve o local e o conteúdo dos arquivos de log do QRadar Risk Manager.

Tabela 37. Arquivos de log do QRadar Risk Manager

Nome do arquivo de log	Local	Descrição
`audit.log`	`/var/log/audit/`	Contém as informações de auditoria atuais.
`audit.<1-50>.gz`	`/var/log/audit/`	Contém informações de auditoria arquivadas. Quando o arquivo `audit.log` atinge 200 MB em tamanho, ele é compactado e renomeado para `audit.1.gz`. O número do arquivo é incrementado cada vez que um arquivo de log é arquivado. O QRadar Risk Manager pode armazenar até 50 arquivos de log arquivados.
`qradar.log`	`/var/log/`	Contém todas as informações de processo registradas pelo servidor do QRadar Risk Manager.
`qradar.error`	`/var/log/`	Todas as exceções e mensagens `System.out` e `System.err` geradas pelo servidor do QRadar Risk Manager são registradas nesse arquivo.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual
Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão

incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos

incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Considerações de política de privacidade

Os produtos de Software IBM, incluindo soluções de software como serviço, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto a fim de ajudar a melhorar a experiência do usuário final, customizar as interações com o usuário final ou para outros propósitos. Em muitas casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se essa Oferta de Software usar cookies para coletar informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies dessa oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de autenticação e gerenciamento de sessões. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para essa Oferta de Software fornecerem a você, como Cliente, a capacidade de coletar informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, será necessário buscar o seu próprio conselho jurídico a respeito de quaisquer leis aplicáveis a tal coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e a Declaração de Privacidade Online da IBM em http://www.ibm.com/privacy/details, na seção intitulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de software como serviço e de produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.

Glossário

Este glossário fornece termos e definições para o software IBM Security QRadar Risk Manager e produtos.

As seguintes referências cruzadas são usadas neste glossário:

- *Consulte* o encaminha de um termo não preferencial para um termo preferencial ou de uma abreviação para o formato soletrado.
- *Consulte também* leva você para um termo relacionado ou contrastante.

Para obter outros termos e definições, consulte o website de Terminologia da IBM (abre em uma nova janela).

"A" "C" "D" "G" "I" "M" na página 146 "N" na página 146 "R" na página 146 "S" na página 146 "T" na página 146 "V" na página 146

A

adaptador
Um componente de software intermediário que permite que dois outros componentes de software se comuniquem um com o outro.

ataque
Qualquer tentativa por uma pessoa desautorizada de comprometer a operação de um programa de software ou sistema de rede.

ativo Um objeto gerenciável que é implementado ou que pretende-se que seja implementado em um ambiente operacional.

atributo
Dados associados a um componente. Por exemplo, um nome do host, endereço IP ou o número de discos rígidos podem ser atributos associados a um componente do servidor.

C

caminho de ataque
A origem, destino e dispositivos associados a um ataque.

conversão de endereço de rede (NAT)
Em um firewall, a conversão de endereços seguros do Protocolo da Internet (IP) para endereços registrados externos. Isso permite a comunicação com redes externas, porém mascara os endereços IP que são utilizados dentro do firewall.

D

dados do vizinho
Os dados coletados a partir de adaptadores que são usados para descobrir informações sobre dispositivos que estão conectados aos hosts gerenciados do QRadar Quality Manager.

dispositivo de contextos múltiplos
Um dispositivo único que é particionado em múltiplos dispositivos virtuais. Cada dispositivo virtual é um dispositivo independente, com sua própria política de segurança.

G

gráfico de conexão
Um gráfico que mostra as conexões de nós da rede remota e endereços IP locais para nós de rede local.

gráfico de série temporal
Uma representação gráfica de conexões de rede com o passar do tempo.

gráfico de topologia
Um gráfico que descreve as sub-redes, dispositivos e firewalls.

I

indicador de risco
Uma medida da exposição potencial de um sistema a uma violação de segurança.

indicador NAT
Um indicador no gráfico de topologia que mostra que o caminho entre duas conexões de rede contém conversões do endereço de origem ou de destino.

linha de conexão
Uma linha no gráfico de conexão entre

um nó de rede remota e um nó de rede local ou entre dois nós da rede local.

M

modelo de topologia
Uma representação virtual dos disposição de ativos de rede que é utilizada para simular um ataque.

N

NAT Consulte Conversão de Endereço de Rede.

P

protocolo de risco
Um protocolo que é associado a serviços que são executados em uma porta aberta em comunicações de entrada da internet para o DMZ.

R

regra Um conjunto de instruções condicionais que permitem que os sistemas de computador identifiquem relacionamentos e executem respostas automatizadas adequadamente.

S

sub-procura
Uma função que permite que uma consulta de procura seja executada dentro de um conjunto de resultados de procura concluída.

T

teste de contribuição
Um teste que examina os indicadores de risco que são especificados em uma pergunta.

teste de recurso
Um de teste que é usado para identificar os indicadores de risco potencial que sinalizam quando os ativos em uma rede violam uma política definida ou introduzem risco no ambiente.

teste restritivo
Um teste que filtra os resultados retornados por uma pergunta de teste de contribuição.

V

violação
Um ato que ignora ou desrespeita política corporativa.

vulnerabilidade
Uma exposição de segurança em um sistema operacional, software do sistema ou componente de software de aplicativo.

Índice Remissivo

A

acesso ao firewall 9
administrador da rede vii
alta disponibilidade (HA) 7
aprovação de simulação
  revogando 127
arquivo de log 139, 140
assistente de relatório 102
atividade do usuário
  log de auditoria 139
atualização do servidor de correio 10

B

backup de informações 25

C

caso de uso do monitor de política
  comunicação de teste de dispositivo para acesso à Internet 63
  comunicação real para DMZ 61
  possível comunicação em ativos protegidos 62
coleção de dados 23
comunicação real 70
  perguntas de contribuição 66
conexões 3, 79, 93
  procurando 87
conexões de rede
  monitorar 3
configuração 9
configuração de dispositivo 22
  comparando 99
configurações de dispositivo de rede
  investigando 97
conformidade 47
conjunto de credenciais 14
Conjunto de endereços 14
credenciais 13
  configurando 15
critérios de procura 88

D

dados do log 137
dados do log de auditoria 137
dados do vizinho
  coletando 23
descoberta de dispositivo 16, 17
dispositivo
  excluindo 20
  importando 17
  incluindo 19
dispositivos 18
  incluindo 19

E

exportando 93
exportar 48

F

fator de importância 43
fazer o backup de informações de configuração 24
funções 10

G

Gerenciador de Risco QRadar
  integração 60
gerenciamento de origem de configuração 13
glossário 145
gráfico 82, 84, 86
gráfico de conexão 84
gráfico de série temporal 82, 86
gráficos 82
  conexões 107
  configurando 107
  Objetos de Dispositivo Não Usados 115
  Regras de Dispositivo 110
Grupo de rede 14
grupo de simulação
  copiar item 59, 129
  designar item 130
  editando 129

H

horário do sistema 11

I

importação de dispositivo, arquivo CSV 18
importar 48
indicadores NAT 38
informações de login 6
informações de login padrão 6
integrações de segurança
  Gerenciador de Risco QRadar 60
introdução vii
IPS 39
IPv6 7

L

lista de dispositivos
  filtragem 20
locais de logs 140
log de auditoria
  ações 137
log de backup 25

M

mapeamento de origem de log 95
  criando 95
máscaras de rede não contíguas 7
modelo de topologia 131
  copiar modelos em grupos 136
  criando 131
  criando um grupo 135
  designar a um grupo 136
  duplicando 134
  editando 134
  editando um grupo 135
  excluindo 134
  visualizando grupos 135
modelos de topologia
  agrupar 135
modo de documento
  navegador da web Internet Explorer 6
modo de navegador
  navegador da web Internet Explorer 6
monitor de configuração 3
monitor de política 4, 41
  casos de uso 61
  designar itens a grupos 60
  excluir item do grupo de pergunta 60, 129, 136
  gerenciando perguntas 41
  resultados para perguntas 57
monitor mode 47, 57
monitorar perguntas 47, 57

N

Navegador da web
  versões suportadas 6
nome de usuário 6
novos recursos
  visão geral do guia do usuário da versão 7.2.5 1

O

o que há de novo
  visão geral do guia do usuário da versão 7.2.5 1
opções do menu ativado pelo botão direito 36

P

pergunta 43, 44, 46
  enviando 45
pergunta de ativo 43

pergunta de conformidade do ativo 46, 47
pergunta de dispositivos/regras 44
perguntas de contribuição
descontinuadas 69
perguntas do monitor de política 48, 65
agrupando 58
avaliando resultados 56
criando um grupo 59
editando 59
exportando 49
importando 49
visualizando grupos 59
Perguntas do teste de contribuição
descontinuadas 76
Perguntas do teste de
dispositivo/regras 77
perguntas restritivas 70
planejamento de descoberta 32
possíveis testes de comunicação
perguntas de contribuição 72
testes restritivos 76
procura
cancelando 93
procurando 91
protocolos 29, 30

R

recursos não suportados 7
referências de conformidade 47
relatório 103
compartilhamento 106
duplicando 106
editando 105
relatórios
gerando manualmente 101
Gerenciador de Risco QRadar 5
gerenciando 101
renomeação da tarefa de backup 29
resultados
aprovando 56
resultados da procura 92, 93
resultados da simulação 125
aprovando 126
gerenciando 124
Resultados do ativo 50
resultados do dispositivo 53
roteamento dinâmico 7

S

salvando 93
senha 6, 11
simulação 5
duplicando 124
simulação *(continuação)*
excluindo 124
simulação manual 124
simulações 119
agrupando 128
editando 123
monitorando 127
Simulações 119
Sistema de Prevenção de Intrusão 39
removendo 40
status do backup 25
sub-procura 91

T

tarefa de backup 26, 27, 29
testes de simulação 120
topologia 4, 35
procurando 38
procurando aplicativos 39
recursos gráficos 35

V

visão geral do QRadar Risk Manager 3
Visualizador do Log de Backup 25
vulnerabilidades de alto risco
priorizando 64