

Guia do Usuário do IBM Security QRadar  
Versão 7.2.2

## *Guia do Usuário*



**Nota**

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 185.

---

# Índice

<b>Sobre este guia</b> . . . . .	<b>ix</b>
<b>Capítulo 1. O que há de novo para os usuários no QRadar V7.2.2.</b> . . . . .	<b>1</b>
<b>Capítulo 2. Sobre o QRadar SIEM.</b> . . . . .	<b>3</b>
Navegadores da web suportados . . . . .	3
Ativar o modo de documento e modo de navegação no Internet Explorer . . . . .	4
Acesso ao IBM Security QRadar . . . . .	4
Guias da interface com o usuário . . . . .	4
Guia Paineis . . . . .	4
Guia Crimes . . . . .	5
Guia Atividade de log . . . . .	5
Guia Atividade de rede. . . . .	5
Guia Ativos. . . . .	5
Guia Relatórios . . . . .	6
IBM Security QRadar Risk Manager . . . . .	6
Guia Administração . . . . .	6
Procedimentos comuns do QRadar . . . . .	7
Visualizando mensagens . . . . .	7
Classificando resultados . . . . .	8
Atualizando e pausando a interface com o usuário . . . . .	8
Investigando endereços IP . . . . .	9
Investigar nomes de usuário. . . . .	10
Tempo do sistema . . . . .	11
Atualizando preferências do usuário . . . . .	11
Acessar ajuda online . . . . .	12
Redimensionar colunas . . . . .	12
Configurar tamanho da página . . . . .	12
<b>Capítulo 3. Gerenciamento de painel</b> . . . . .	<b>13</b>
Painéis padrão . . . . .	13
Painéis customizados . . . . .	13
Customizar painel . . . . .	14
Procura de fluxo. . . . .	14
Ofensas. . . . .	14
Atividade de log . . . . .	15
Relatórios mais recentes . . . . .	15
Resumo do sistema. . . . .	16
Risk Manager. . . . .	16
Itens de Gerenciamento de vulnerabilidade. . . . .	16
Notificação do sistema. . . . .	17
Centro de informações de ameaça da Internet . . . . .	18
Criando um painel customizado . . . . .	18
Usando o painel para investigar a atividade de log ou de rede . . . . .	19
Configurando gráficos. . . . .	20
Removendo itens do painel . . . . .	20
Removendo um item do painel. . . . .	21
Renomeando um painel . . . . .	21
Excluindo um painel . . . . .	21
Gerenciando notificações do sistema . . . . .	22
Incluindo itens de painel baseados em procura na lista Incluir itens . . . . .	22
<b>Capítulo 4. Gerenciamento de crimes</b> . . . . .	<b>25</b>
Visão geral da ofensa . . . . .	25

Considerações de permissão de crime . . . . .	25
Termos chave. . . . .	25
Retenção de crime . . . . .	26
Monitoramento de crime . . . . .	26
Monitorando as páginas Todas Ofensas ou Minhas Ofensas . . . . .	26
Monitorando ofensas agrupadas por categoria . . . . .	27
Monitorando ofensas agrupadas por IP de origem . . . . .	28
Monitorando ofensas agrupadas por IP de destino . . . . .	28
Monitorando ofensas agrupadas por rede . . . . .	29
Tarefas de gerenciamento de crime . . . . .	29
Incluindo notas . . . . .	30
Ocultando ofensas . . . . .	30
Mostrando ofensas ocultas . . . . .	30
Fechando ofensas . . . . .	31
Protegendo crimes . . . . .	32
Desprotegendo ofensas . . . . .	32
Exportando ofensas. . . . .	33
Designando ofensas para usuários. . . . .	33
Enviando notificação por email . . . . .	34
Marcando um item para acompanhamento . . . . .	35
Funções da barra de ferramentas da guia de crime . . . . .	35
Parâmetros da ofensa . . . . .	38

## **Capítulo 5. Investigação de atividade de log . . . . . 51**

Visão geral da guia Atividade de log . . . . .	51
Barra de ferramentas da guia Atividade de log . . . . .	51
Sintaxe de Filtro Rápido . . . . .	53
Opções do menu ativado pelo botão direito . . . . .	54
Barra de status . . . . .	54
Monitorando a atividade de log . . . . .	55
Visualizando eventos de fluxo . . . . .	55
Visualizando eventos normalizados . . . . .	56
Visualizando eventos brutos . . . . .	57
Visualizando eventos agrupados . . . . .	58
Detalhes do evento . . . . .	61
Barra de ferramentas de detalhes do evento . . . . .	63
Visualizando ofensas associadas . . . . .	63
Modificando mapeamento de eventos . . . . .	64
Ajustando falsos positivos . . . . .	65
Gerenciando dados de PCAP . . . . .	66
Exibindo a coluna de dados do PCAP . . . . .	66
Visualizando informações do PCAP . . . . .	67
Fazendo download do arquivo PCAP para seu sistema de desktop . . . . .	68
Exportando eventos . . . . .	68

## **Capítulo 6. Investigação de atividade de rede . . . . . 71**

Visão geral da guia Rede . . . . .	71
Barra de ferramentas da guia Atividade de rede . . . . .	71
Sintaxe de Filtro Rápido . . . . .	72
Opções do menu ativado pelo botão direito . . . . .	73
Barra de status . . . . .	74
Registros do Overflow . . . . .	74
Monitorando a atividade de rede . . . . .	74
Visualizando fluxos de fluxo. . . . .	74
Visualizando fluxos normalizados . . . . .	75
Visualizando fluxos agrupados . . . . .	77
Detalhes do fluxo . . . . .	79
Barra de ferramenta de detalhes do fluxo . . . . .	81
Ajustando falsos positivos . . . . .	81
Exportando fluxos . . . . .	82

<b>Capítulo 7. Gerenciamento de gráfico</b>	<b>85</b>
Gerenciamento de gráfico.	85
Visão geral do gráfico de série temporal.	86
Legendas do gráfico	87
Configurando gráficos.	87
<b>Capítulo 8. Procuras de dados</b>	<b>89</b>
Procuras de eventos e de fluxo	89
Procurando por itens que correspondem aos seus critérios.	89
Salvando critérios de procura	92
Procuras de crime	94
Procurando ofensas nas páginas Minhas Ofensas e Todas as Ofensas	94
Procurando ofensas na página Por IP de Origem	98
Procurando ofensas na página Por IP de Destino	100
Procurando ofensas na página Por Redes	101
Salvando critérios de procura na guia <b>Ofensas</b>	101
Excluindo critérios de procura.	102
Usando uma subprocura para refinar resultados da procura.	103
Gerenciando resultados da procura	104
Salvando resultados da procura	104
Visualizando gerenciar resultados da procura.	105
Cancelando uma procura	106
Excluindo uma procura	106
Gerenciando grupos de procura	107
Visualizando grupos de procura	107
Criando um novo grupo de procura.	107
Editando um grupo de procura	108
Copiando uma procura salva para outro grupo	108
Removendo um grupo ou uma procura salva de um grupo	108
<b>Capítulo 9. Propriedades de fluxo e de evento customizadas</b>	<b>111</b>
Permissões requeridas	111
Tipos de propriedades customizadas.	111
Criando uma propriedade customizada baseada em regex	112
Criando uma propriedade customizada baseada em cálculo	113
Modificando uma propriedade customizada	115
Copiando uma propriedade customizada	116
Excluindo uma propriedade customizada	116
<b>Capítulo 10. Gerenciamento de regra</b>	<b>117</b>
Considerações de permissão de regra	117
Visão geral de regras	117
Categorias de regra	117
Tipos de regra	118
Condições da regra	119
Respostas da regra	119
Visualizando regras	120
Criando uma regra customizada	121
Criando uma regra de detecção de anomalia	122
Tarefas de gerenciamento de regra	124
Ativando e desativando regras	124
Editando uma regra	124
Copiando uma regra	125
Excluindo uma regra	125
Gerenciamento do grupo de regras	126
Visualizando um grupo de regra	126
Criando um grupo	126
Designando um item a um grupo	126
Editando um grupo	127
Copiando um item para outro grupo	127

Excluindo um item de um grupo . . . . .	127
Excluindo um grupo . . . . .	128
Editando blocos de construção . . . . .	128
Parâmetros da página Regra . . . . .	129
Barra de ferramentas da página Regras . . . . .	129
Parâmetros da página Regra de Resposta . . . . .	130

## **Capítulo 11. Parâmetros da página Perfil de ativo . . . . . 137**

Perfis de ativos . . . . .	137
Sobre vulnerabilidades . . . . .	137
Visão geral da guia Ativos . . . . .	138
Lista da guia Ativo . . . . .	138
Opções do menu ativado pelo botão direito . . . . .	139
Visualizando um perfil de ativo . . . . .	140
Incluindo ou editando um perfil do ativo . . . . .	141
Procurando perfis de ativos . . . . .	144
Salvando critérios de procura de ativo . . . . .	146
Grupos de procura de ativos . . . . .	146
Visualizando grupos de procura . . . . .	146
Criando um novo grupo de procura . . . . .	147
Editando um grupo de procura . . . . .	147
Copiando uma procura salva para outro grupo . . . . .	148
Removendo um grupo ou uma procura salva de um grupo . . . . .	148
Tarefas de gerenciamento do Perfil de ativo . . . . .	148
Excluindo ativos . . . . .	148
Importando perfis de ativos . . . . .	149
Exportando ativos . . . . .	149
Pesquisar vulnerabilidades de ativo . . . . .	150
Parâmetros da página Perfil de ativo . . . . .	152
Área de janela Resumo de ativo . . . . .	152
Área de janela Resumo de interface de rede . . . . .	153
Área de janela Vulnerabilidade . . . . .	154
Área de janela Serviços . . . . .	154
Área de janela Serviços do Windows . . . . .	155
Área de janela Pacotes . . . . .	155
Área de janela Correções do Windows . . . . .	155
Área de janela Propriedades . . . . .	156
Área de janela Políticas de risco . . . . .	156
Área de janela Produtos . . . . .	156

## **Capítulo 12. Gerenciamento de relatório . . . . . 159**

Barra de status . . . . .	160
Layout de relatório . . . . .	160
Tipos de gráfico . . . . .	160
Barra de ferramentas da guia Relatório . . . . .	161
Tipos de diagrama . . . . .	162
Criando relatórios customizados . . . . .	163
Editando um relatório . . . . .	167
Visualizando relatórios gerados . . . . .	167
Excluindo conteúdo gerado . . . . .	168
Gerando um relatório manualmente . . . . .	168
Duplicando um relatório . . . . .	169
Compartilhando um relatório . . . . .	169
Relatórios de marca . . . . .	170
Grupos de relatórios . . . . .	170
Criando um grupo de relatórios . . . . .	171
Editando um grupo . . . . .	171
Designar um relatório a um grupo . . . . .	172
Copiando um relatório para outro grupo . . . . .	172
Removendo um relatório . . . . .	172

Contêiner do gráfico . . . . .	172
Parâmetros do contêiner do gráfico Vulnerabilidades de Ativo . . . . .	173
Parâmetros do contêiner do gráfico de eventos/logs . . . . .	174
Parâmetros do contêiner do gráfico de fluxo . . . . .	177
Parâmetros do contêiner do gráfico Principais IPs de origem . . . . .	181
Parâmetros do contêiner do gráfico Principais ofensas . . . . .	181
Parâmetros do contêiner do gráfico Principais IPs de destino . . . . .	182
<b>Avisos . . . . .</b>	<b>185</b>
Marcas registradas. . . . .	187
Considerações de política de privacidade . . . . .	187
<b>Glossário . . . . .</b>	<b>189</b>
A . . . . .	189
B . . . . .	189
C . . . . .	189
D . . . . .	190
E . . . . .	190
F . . . . .	190
G . . . . .	190
H . . . . .	191
I . . . . .	191
L . . . . .	191
M . . . . .	191
N . . . . .	192
O . . . . .	192
P . . . . .	193
R . . . . .	193
S . . . . .	194
T . . . . .	194
V . . . . .	194
<b>Índice Remissivo . . . . .</b>	<b>195</b>





---

## Sobre este guia

O Guia do Usuário do IBM Security QRadar SIEM fornece informações sobre como gerenciar o IBM Security QRadar SIEM incluindo as guias Painel, Ofensas, Log de atividades, Atividade de rede, Ativos e Relatórios.

### **Público alvo**

Este guia destina-se a todos os usuários QRadar SIEM responsáveis pela investigação e gerenciamento de segurança de rede. Este guia presume que você tenha acesso ao QRadar SIEM e um conhecimento de sua rede corporativa e das tecnologias de rede.

### **Documentação técnica**

Para obter informações sobre como acessar a documentação mais técnica, notas técnicas e notas sobre a liberação, consulte Acessando a nota de documentação técnica do IBM® Security (<http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861>).

### **Contatando o suporte ao cliente**

Para obter informações sobre como contatar o suporte ao cliente, consulte Suporte e download da nota técnica (<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 as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mal uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum sistema de TI ou produto deve ser considerado completamente seguro e nenhum único produto, serviço ou medida de segurança pode ser completamente efetivo(a) na prevenção de uso ou acesso impróprio. Os sistemas, produtos e serviços da IBM foram projetados para serem parte de uma abordagem de segurança abrangente, que envolverá, necessariamente, procedimentos operacionais adicionais e podem precisar de outros sistemas, produtos ou serviços para ser mais efetiva. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS SEJAM IMUNES OU TORNEM SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE NENHUMA PARTE.




---


## Capítulo 1. O que há de novo para os usuários no QRadar V7.2.2

O IBM Security QRadar V7.2.2 apresenta atualizações para as preferências do usuário para seleção de idioma, para selecionar códigos de idiomas diferentes para valores numéricos, visualizar mensagens do sistema e interface com dados fornecidos pelo usuário.

### **Os usuários podem configurar sua preferência de idioma**

QRadar está disponível nos seguintes idiomas: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol, russo e português (Brasil). Os usuários podem selecionar seu idioma preferencial escolhendo a configuração de **Código de Idioma** na lista de **Preferências**.  Saiba mais...

### **Suporte para valores numéricos em diferentes códigos de idiomas para eventos customizados**

O QRadar agora tem a capacidade de suportar valores numéricos usando diferentes códigos de idiomas para eventos customizados.  Saiba mais...

### **Novas funções do usuário podem visualizar notificações do sistema**

Os usuários podem ver notificações do sistema no Painel.

### **Novas funções do usuário podem promover interface com seus dados**

Os usuários podem promover interface com coletas de dados que fornecerem.



---

## Capítulo 2. Sobre o QRadar SIEM

O QRadar SIEM é uma plataforma de gerenciamento de segurança de rede que fornece reconhecimento situacional e suporte de conformidade por meio da combinação de conhecimentos de rede baseado em fluxo, correlação de eventos de segurança e de avaliação de vulnerabilidades com base em ativos.

### Chave de licença padrão

Uma chave de licença padrão fornece acesso à interface com o usuário por cinco semanas. Após efetuar login no QRadar SIEM, uma janela exibirá a data em que a chave de licença temporária expirará. Para obter mais informações sobre a instalação de uma chave de licença, consulte o *IBM Security QRadar SIEM Administration Guide*.

### Exceções e certificados de segurança

Se estiver usando o navegador da web Mozilla Firefox, deverá incluir uma exceção para o Mozilla Firefox para efetuar login no QRadar SIEM. Para obter mais informações, consulte a documentação do navegador da web Mozilla Firefox.

Se estiver usando o navegador da web Microsoft Internet Explorer, uma mensagem do certificado de segurança do website será exibida ao acessar o sistema QRadar SIEM. Deve-se selecionar a opção **Continuar para esse website** para efetuar login no QRadar SIEM.

### Navegue para o aplicativo baseado na web

Ao usar QRadar SIEM, use as opções de navegação disponíveis na interface com o usuário QRadar SIEM em vez do botão **Voltar** do seu navegador da web.

---

## 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 dos navegadores da web.

*Tabela 1. Navegadores da web suportados para produtos QRadar*

Navegador da web	Versão suportada
Mozilla Firefox	Liberação de Suporte Estendido do Firefox 17.0 Liberação de Suporte Estendido do Firefox 24.0
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegação ativados	8.0 9.0
Google Chrome	A versão atual a partir da data da liberação dos produtos IBM Security QRadar V7.2.2

---

## Ativar o modo de documento e modo de navegação no Internet Explorer

Se você usar o Microsoft Internet Explorer para acessar os produtos IBM Security QRadar, você deve ativar o modo de navegação 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 **Internet Explorer 9**
  - Para o Internet Explorer V8.0, selecione **Internet Explorer 7.0 Standards**

---

## Acesso ao IBM Security QRadar

O IBM Security QRadar é um aplicativo baseado na web. O QRadar usa as informações de login padrão da URL, nome de usuário e senha.

Use as informações na tabela a seguir ao efetuar login no seu console do IBM Security QRadar.

*Tabela 2. Informações de login padrão do QRadar*

Informações de login	Padrão
URL	https://<Endereço IP>, em que <Endereço IP> é o endereço IP do console do QRadar.  Para efetuar login no QRadar em um ambiente misto ou IPv6, coloque o endereço IP entre colchetes:  https://[<Endereço IP>]
Nome de usuário	admin
Senha	A senha que é designada para o QRadar durante o processo de instalação.
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

---

## Guias da interface com o usuário

A funcionalidade é dividida em guias. A guia **Painel** é exibida ao efetuar login.

É possível facilmente navegar nas guias para localizar os dados ou funcionalidade requeridos.

### Guia Painel

A guia **Painel** é a guia padrão que será exibida ao efetuar login.

A guia **Painel** fornece um ambiente de área de trabalho que suporta vários painéis, no qual é possível exibir visualizações de segurança de rede, atividade ou dados que o QRadar coleta. Cinco painéis padrão estão disponíveis. Cada painel contém itens que fornecem informações de resumo e detalhadas sobre os crimes que ocorrem em sua rede. É possível também criar um painel customizado para permitir que sejam concentradas suas responsabilidades de operação de rede ou de segurança. Para obter mais informações sobre como usar a guia Painel, consulte Gerenciamento de painel.

## Guia Crimes

A guia **Ofensas** permitirá que você visualize ofensas que ocorrem em sua rede, que podem ser localizadas usando várias opções de navegação ou por meio de pesquisas poderosas.

Na guia **Ofensas**, é possível investigar um crime para determinar a causa raiz de um problema. É possível também resolver o problema.

Para obter mais informações sobre a guia **Ofensas**, consulte Gerenciamento de crimes.

## Guia Atividade de log

A guia **Atividade de log** permitirá que você investigue os logs de evento enviados para o QRadar em tempo real, execute procuras poderosas e visualize a atividade de log usando gráficos de séries temporais configuráveis.

A guia **Atividade de log** permitirá que seja executada uma investigação detalhada sobre os dados do evento.

Para obter mais informações, consulte Investigação da atividade de log.

## Guia Atividade de rede

Use a guia **Atividade de rede** para investigar os fluxos que são enviados em tempo real, executar procuras poderosas e visualizar a atividade da rede usando gráficos de série temporal configuráveis.

Um fluxo é uma sessão de comunicação entre dois hosts. Visualizar informações de fluxo permitirá que seja determinado como o tráfego é comunicado, o que é comunicado (se a opção de captura de conteúdo estiver ativada), e quem está se comunicando. Os dados de fluxo também incluem detalhes como protocolos, valores ASN, valores IRI e prioridades.

Para obter mais informações, consulte Investigação da atividade de rede.

## Guia Ativos

O QRadar descobre automaticamente ativos, servidores e hosts operacionais em sua rede.

Descoberta automática é baseada em dados de fluxo passivo e de vulnerabilidade, permitindo que o QRadar crie um perfil de ativo.

Perfis de ativo fornecem informações sobre cada ativo conhecido em sua rede, incluindo informações de identidade, se disponíveis, e quais serviços estão em execução em cada ativo. Esses dados de perfil são usados para propósitos de correlação para ajudar a reduzir positivos falsos.

Por exemplo, um ataque tenta usar um serviço específico que está em execução em um ativo específico. Nesta situação, o QRadar pode determinar se o ativo está vulnerável a este ataque correlacionando o ataque com o perfil de ativo. Usando a guia **Ativos**, é possível visualizar os ativos aprendidos ou procurar ativos específicos para visualizar seus perfis.

Para obter mais informações, consulte Gerenciamento de ativos.

## Guia Relatórios

A guia **Relatórios** permitirá criar, distribuir e gerenciar relatórios para quaisquer dados no QRadar.

O recurso Relatórios permitirá a criação de relatórios customizados para uso operacional e executivo. Para criar um relatório, é possível combinar informações (como segurança ou rede) em um único relatório. É possível também usar modelos de relatório pré-instalados que são incluídos com QRadar.

A guia **Relatórios** também permitirá que você marque seus relatórios com logotipos customizados. Esta customização é útil para distribuir relatórios para diferentes públicos.

Para obter mais informações sobre relatórios, consulte Gerenciamento de relatórios.

## 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.

O IBM Security QRadar Risk Manager usa dados que são coletados pelos dados de configuração do dispositivo de rede e de segurança, tais como firewalls, roteadores, comutadores ou IPs, feeds de vulnerabilidade e fontes de segurança do fornecedor. Esses dados são usados para identificar os riscos de conformidade, segurança e política dentro de infraestrutura de segurança de rede e a probabilidade de os riscos que estão sendo explorados.

**Nota:** Para obter mais informações sobre o IBM Security QRadar Risk Manager, entre em contato com seu representante de vendas local.

## Guia Administração

Os administradores usam a guia Administração para configurar e gerenciar os usuários, sistemas, redes, plug-ins e componentes. Os usuários com privilégios de administração podem acessar a guia **Administração**.

As ferramentas de administração que os administradores podem acessar na guia **Administração** estão descritas na Tabela 1.

*Tabela 3. Ferramentas de gerenciamento de administração disponíveis em QRadar*

Ferramenta de administração	Descrição
Configuração do Sistema	Configure o sistema e as opções de gerenciamento do usuário.
Origens de Dados	Configure origens de log, origens de fluxo e opções de vulnerabilidade.
Configuração de Redes e Serviços Remotos	Configure redes remotas e grupos de serviços.
Editor de Implementação	Gerencie os componentes individuais da implementação do QRadar.

Todas as atualizações de configuração feitas na guia **Administração** são salvas em uma área de preparação. Quando todas as alterações estiverem concluídas, será possível implementar as atualizações de configuração no host gerenciado em sua implementação.



---

## Procedimentos comuns do QRadar

Vários controles na interface com o usuário do QRadar são comuns à maioria das guias da interface com o usuário.

As informações sobre esses procedimentos comuns estão descritas nas seções a seguir.

### Visualizando mensagens

O menu **Mensagens**, no canto superior direito da interface com o usuário, fornece acesso a uma janela na qual você pode ler e gerenciar suas notificações do sistema.

#### Antes de Iniciar

Para as notificações do sistema serem mostradas na janela **Mensagens**, o administrador deve criar uma regra baseada em cada tipo de mensagem de notificação e selecionar a caixa de opções **Notificar** no **Assistente de regras customizadas**.

#### Sobre Esta Tarefa

O menu **Mensagens** indica quantas notificações não lidas do sistema você tem em seu sistema. Este indicador incrementa o número até que você feche as notificações do sistema. Para cada notificação do sistema, a janela **Mensagens** fornece um resumo e o registro de data para quando a notificação do sistema foi criada. Você pode passar o ponteiro do mouse sobre uma notificação para visualizar mais detalhes. Usando as funções na janela **Mensagens**, você pode gerenciar as notificações do sistema.

As notificações do sistema também estão disponíveis na guia **Painel** e em uma janela pop-up opcional que pode ser exibida no canto inferior esquerdo da interface com o usuário. As ações que você executar na janela **Mensagens** são propagadas para a guia **Painel** e a janela pop-up. Por exemplo, se você fechar uma notificação do sistema da janela **Mensagens**, a notificação do sistema será removida de todas as exibições das notificações do sistema.

Para obter mais informações sobre notificações do sistema do Painel, consulte Item de notificações do sistema.

A janela **Mensagens** fornece as seguintes funções:

*Tabela 4. Funções disponíveis na janela de mensagens*

Função	Descrição
<b>Todos</b>	Clique em <b>Todos</b> para visualizar todas as notificações do sistema. Essa opção é o padrão, portanto, você clicará em <b>Todos</b> apenas se você selecionar outra opção e deseja exibir todas as notificações do sistema novamente.
<b>Funcionamento</b>	Clique em <b>Funcionamento</b> para visualizar apenas as notificações do sistema que tenham um nível de severidade de funcionamento.
<b>Erros</b>	Clique em <b>Erros</b> para visualizar apenas as notificações do sistema que tenham um nível de severidade de erro.
<b>Avisos</b>	Clique em <b>Avisos</b> para visualizar apenas as notificações do sistema que tenham um nível de severidade de aviso.
<b>Informações</b>	Clique em <b>Informações</b> para visualizar apenas as notificações do sistema que tenham um nível de severidade de informações.

Tabela 4. Funções disponíveis na janela de mensagens (continuação)

Função	Descrição
Descartar todos	<p>Clique em <b>Descartar todos</b> para fechar todas as notificações do sistema de seu sistema. Se você filtrou a lista de notificações do sistema usando o <b>Funcionamento</b>, <b>Erros</b>, <b>Avisos</b> ou <b>Ícones de informações</b>, o texto no ícone <b>Visualizar tudo</b> será alterado para uma das opções a seguir:</p> <ul style="list-style-type: none"> <li>• Descartar todos os erros</li> <li>• Descartar todo funcionamento</li> <li>• Descartar todos os avisos</li> <li>• Descartar todos os avisos</li> <li>• Descartar todas as informações</li> </ul>
Visualizar tudo	<p>Clique em <b>Visualizar tudo</b> para visualizar os eventos de notificação do sistema na guia <b>Atividade de Log</b>. Se você filtrou a lista de notificações do sistema usando o <b>Funcionamento</b>, <b>Erros</b>, <b>Avisos</b> ou <b>Ícones de informações</b>, o texto no ícone <b>Visualizar tudo</b> será alterado para uma das opções a seguir:</p> <ul style="list-style-type: none"> <li>• Visualizar todos os erros</li> <li>• Visualizar todo funcionamento</li> <li>• Visualizar todos os avisos</li> <li>• Visualizar todas as informações</li> </ul>
Descartar	<p>Clique no ícone <b>Descartar</b> ao lado de uma notificação do sistema para fechar a notificação do sistema de seu sistema.</p>

## Procedimento

1. Efetuar login no QRadar.
2. No canto superior direito da interface com o usuário, clique em **Mensagens**.
3. Na janela **Mensagens**, visualize os detalhes de notificação do sistema.
4. Opcional. Para refinar a lista de notificações do sistema, clique em uma das opções a seguir:
  - Erros
  - Avisos
  - Informações
5. Opcional. Para fechar notificações do sistema, escolha uma das opções a seguir:

Opção	Descrição
Descartar todos	Clique para fechar todas as notificações do sistema.
Descartar	Clique no ícone <b>Descartar</b> próximo à notificação do sistema que você deseja fechar.

6. Opcional. Para visualizar os detalhes da notificação do sistema, passe o ponteiro do mouse sobre a notificação do sistema.

## Classificando resultados

É possível classificar os resultados em tabelas clicando em um título da coluna. Uma seta na parte superior da coluna indica a direção da classificação.

### Procedimento

1. Efetue login no QRadar.
2. Clique no cabeçalho da coluna uma vez para classificar a tabela em ordem decrescente; duas vezes para classificar a tabela em ordem crescente.

## Atualizando e pausando a interface com o usuário

Você pode atualizar, pausar e executar manualmente os dados exibidos nas guias.

## Sobre Esta Tarefa

As guias **Painel** e **Ofensas** atualizam automaticamente a cada 60 segundos.

As guias **Atividade de log** e **Atividade de rede** atualizarão automaticamente a cada 60 segundos, se você estiver visualizando a guia no modo Último Intervalo (atualização automática).

O cronômetro, que está no canto superior direito da interface, indica a quantidade de tempo até que a guia seja atualizada automaticamente.

Ao visualizar a guia **Atividade de log** ou **Atividade de rede** no modo Tempo Real (fluxo) ou Último Minuto (atualização automática), você poderá usar o ícone **Pausar** para pausar a exibição atual.

Você também pode pausar a exibição atual na guia **Painel**. Clicando em qualquer lugar dentro de um item do painel pausa automaticamente a guia. O cronômetro pisca em vermelho para indicar que a exibição atual está pausada.

## Procedimento

1. Efetue login no QRadar.
2. Clique na guia que você deseja visualizar.
3. Escolha uma das opções a seguir:

Opção	Descrição
Atualizar	Clique em <b>Atualizar</b> , no canto direito da guia para atualizar a guia.
Pausar	Clique para pausar a exibição na guia.
Executar	Clique para reiniciar o cronômetro depois que o cronômetro estiver pausado.

## Investigando endereços IP

Você pode usar diversos métodos para investigar as informações sobre endereços IP nas guias Painel, Atividade de log e Atividade de rede.

## Sobre Esta Tarefa

Você pode localizar mais informações sobre um endereço IP por qualquer um dos métodos listados na tabela a seguir.

*Tabela 5. Informações de endereços IP*

Opção	Descrição
Navegar > Visualização por rede	Exibe as redes associados ao endereço IP selecionado.
Navegar > Visualizar resumo de origem	Exibe as ofensas associadas com o endereço IP de origem selecionado.
Navegar > Visualizar resumo de destino	Exibe as ofensas associadas com o endereço IP de destino selecionado.
Informações > Consulta de DNS	Procura por entradas de DNS baseadas no endereço IP.
Informações > Consulta de WHOIS	Procura pelo proprietário registrado de um endereço IP remoto. O servidor de WHOIS padrão é whois.arin.net.
Informações > Varredura de porta	Executa uma varredura de Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível somente se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do seu fornecedor.

Tabela 5. Informações de endereços IP (continuação)

Opção	Descrição
Informações > Perfil de ativo	Exibe informações do perfil de ativos.  Essa opção será exibida se o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter informações adicionais, consulte <i>IBM Security QRadar Vulnerability Manager User Guide</i> .  Essa opção de menu estará disponível se o QRadar adquiriu os dados de perfil ativamente através de uma varredura ou passivamente através de origens de fluxo.  Para obter informações, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Informações > Procurar eventos	Procura por eventos associadas a esse endereço IP.
Informações > Procurar fluxos	Procura por fluxos associados a esse endereço IP.
Informações > Procurar conexões	Procura por conexões associados a esse endereço IP. Essa opção será exibida somente se você comprou o IBM Security QRadar Risk Manager e conectou o QRadar e o dispositivo do IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i> .
Informações > Consulta de porta de comutador	Determina a porta do comutador em um dispositivo Cisco IOS para esse endereço IP. Essa opção aplica-se somente a comutadores descobertos usando a opção <b>Descobrir dispositivos</b> na guia <b>Riscos</b> .
Informações > Visualizar topologia	Exibe a guia <b>Riscos</b> que representa a topologia da camada 3 de sua rede. Essa opção estará disponível se você comprou o IBM Security QRadar Risk Manager e conectou o QRadar e o dispositivo do IBM Security QRadar Risk Manager. dispositivo.
Execução de informações > Varredura QVM	Selecione a opção Executar varredura QVM para uma varredura do IBM Security QRadar Vulnerability Manager nesse endereço IP. Essa opção será exibida somente quando o IBM Security QRadar Vulnerability Manager estiver sendo comprado e licenciado. Para obter informações adicionais, consulte <i>IBM Security QRadar Vulnerability Manager User Guide</i> .

Para obter informações sobre a guia Riscos ou o IBM Security QRadar Risk Manager, consulte o *IBM Security QRadar Risk Manager User Guide*.

## Procedimento

1. Efetue login no QRadar.
2. Clique na guia que você deseja visualizar.
3. Mova o ponteiro do mouse sobre um endereço IP para visualizar o local do endereço IP.
4. Clique com o botão direito no endereço IP ou no nome do recurso e selecione uma das opções a seguir:

## Investigar nomes de usuário

É possível clicar com o botão direito em um nome de usuário para acessar mais opções de menu. Use essas opções para visualizar mais informações sobre o nome de usuário ou endereço IP.

Será possível investigar nomes de usuários quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*.

Ao clicar com o botão direito em um nome de usuário, será possível escolher as seguintes opções de menu.

Tabela 6. Opções do menu para investigação do nome de usuário

Opção	Descrição
Visualizar ativos	Exibe os ativos atuais que estão associados ao nome de usuário selecionado. Para obter mais informações sobre a visualização de ativos, consulte Gerenciamento de ativos.
Visualizar Histórico de Usuário	Exibe todos os ativos que estão associados ao nome de usuário selecionado durante as 24 horas anteriores.

Tabela 6. Opções do menu para investigação do nome de usuário (continuação)

Opção	Descrição
Visualizar eventos	Exibe os eventos que estão associados ao nome de usuário selecionado. Para obter mais informações sobre a janela Lista de eventos, consulte Registrar monitoramento de atividade.

Para obter mais informações sobre como customizar o menu ativado pelo botão direito, consulte o *Guia de Administração* de seu produto.

## Tempo do sistema

O canto direito da interface com o usuário do QRadar exibe o tempo do sistema, que é o tempo no console.

O tempo do console sincroniza os sistemas QRadar na implementação do QRadar. O tempo do console é usado para determinar quais eventos de tempo foram recebidos de outros dispositivos para correlação de sincronização de tempo correta.

Em uma implementação distribuída, o console pode estar em um fuso horário diferente de seu computador desktop.

Ao aplicar filtros e procuras com base em tempo nas guias **Atividade de log** e **Atividade de rede**, será necessário usar o tempo do sistema do console para especificar um intervalo de tempo.

Ao aplicar filtros e procuras com base em tempo na guia **Atividade de log**, será necessário usar o tempo do sistema do console para especificar um intervalo de tempo.

## Atualizando preferências do usuário

É possível configurar sua preferência de usuário, como código de idioma, na interface principal com o usuário do QRadar.

### Procedimento

1. Para acessar suas informações de usuário, clique em **Preferências**.
2. Atualize suas preferências.

Opção	Descrição
Nome de Usuário	Exibe seu nome de usuário. Você não pode editar esse campo.
Senha	A senha deve atender aos seguintes critérios: <ul style="list-style-type: none"> <li>• Mínimo de 6 caracteres</li> <li>• Máximo de 255 caracteres</li> <li>• Conter pelo menos um caractere especial</li> <li>• Conter um caractere maiúsculo</li> </ul>
Senha (Confirmar)	Confirmação de senha,
Endereço de email	O endereço de email deve atender aos seguintes requisitos: <ul style="list-style-type: none"> <li>• Mínimo de 10 caracteres</li> <li>• Máximo de 255 caracteres</li> </ul>

Opção	Descrição
<b>Código do Idioma</b>	<p>O QRadar está disponível nos seguintes idiomas: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol, russo e português (Brasil).</p> <p>Se um código de idioma não for listado, a interface com o usuário não será traduzida no idioma associado. No entanto, outras convenções culturais associadas, como tipo de caractere, ordenação, formato de data e hora e unidade de moeda são suportadas.</p>
<b>Ativar Notificações Pop-up</b>	<p>Selecione essa caixa de seleção se você desejar ativar notificações do sistema pop-up a serem exibidas em sua interface com o usuário.</p>

## Acessar ajuda online

É possível acessar Ajuda online do QRadar por meio da interface com o usuário principal do QRadar.

Para acessar a Ajuda online, clique em **Ajuda > Conteúdo de ajuda**.

## Redimensionar colunas

É possível redimensionar as colunas em várias guias no QRadar.

Coloque o ponteiro do mouse sobre a linha que separa as colunas e arraste a borda da coluna para o novo local. É possível também redimensionar colunas clicando duas vezes na linha que separa as colunas para redimensionar automaticamente a coluna à largura do maior campo.

**Nota:** Redimensionamento de coluna não funcionará em navegadores da web Microsoft Internet Explorer, Versão 7.0 quando as guias estiverem exibindo os registros no modo de fluxo.

## Configurar tamanho da página

Os usuários com privilégios administrativos podem configurar o número máximo de resultados que são exibidos nas tabelas em várias guias no QRadar.

---

## Capítulo 3. Gerenciamento de painel

A guia **Painel** é a visualização padrão quando é efetuado login.

Ele fornece um ambiente de área de trabalho que suporta vários painéis nos quais é possível exibir visualizações de segurança de rede, atividade ou dados que são coletados.

Os painéis permitem que seus itens de painel sejam organizados em visualizações funcionais, que permitem que você se concentre em áreas específicas de sua rede.

Use a guia Painel para monitorar o comportamento do evento de segurança.

É possível customizar seu painel. O conteúdo que é exibido na guia **Painel** é específico do usuário. As alterações que são feitas dentro de uma sessão afetam apenas o seu sistema.

---

### Painéis padrão

Use o painel padrão para customizar seus itens em visualizações funcionais. Estas visualizações funcionais se concentram em áreas específicas de sua rede.

A guia **Painel** fornece cinco painéis padrão que estão concentrados em segurança, atividade de rede, atividade do aplicativo, monitoramento do sistema e conformidade.

Cada painel exibe um padrão que é um conjunto de itens do painel. Os itens do painel agem como ponto de início para navegar para dados mais detalhados. A tabela a seguir define os painéis padrão.

---

### Painéis customizados

É possível customizar seus painéis. O conteúdo que é exibido na guia **Painel** é específico do usuário. As alterações que são feitas dentro de uma sessão do QRadar afetam apenas o seu sistema.

Para customizar a guia **Painel**, é possível executar as seguintes tarefas:

- Criar painéis customizados que são relevantes para as suas responsabilidades. 255 painéis por usuário é o máximo; no entanto, problemas de desempenho podem ocorrer se forem criados mais de 10 painéis.
- Incluir e remover itens do painel a partir de painéis padrão ou customizado.
- Mover e posicionar itens para atender seus requisitos. Ao posicionar itens, cada item é redimensionado automaticamente na proporção para o painel.
- Incluir itens do painel customizado que são baseados em quaisquer dados.

Por exemplo, é possível incluir um item do painel que fornece um gráfico de série temporal ou um gráfico de barras que representa as 10 principais atividades de rede.

Para criar itens customizados, é possível criar as procuras salvas nas guias **Atividade de rede** ou **Atividade de log** e escolher como deseja os resultados

representados em seu painel. Cada gráfico de painel exibe os dados atualizados em tempo real. Gráficos de série temporal no painel são atualizados a cada 5 minutos.

---

## Customizar painel

É possível incluir vários itens do painel nos seus painéis padrão ou customizados.

É possível customizar seus painéis para exibir e organizar os itens de painéis que atendem aos requisitos de segurança da rede.

Há 5 painéis padrão, que podem ser acessados a partir da caixa de listagem **Mostrar painel** na guia **Painel**. Se você visualizou anteriormente um painel e retornou para a guia **Painel**, o último painel visualizado será exibido.

## Procura de fluxo

É possível exibir um item de painel customizado que é baseado em critérios de procura salvos a partir da guia **Atividade de rede**.

Itens de procura de fluxo são listados no menu **Incluir item > Atividade de rede > Procuras de fluxo**. O nome do item de procura de fluxo corresponde ao nome do critério de procura salvo no qual o item é baseado.

Os critérios de procura salvos padrão estão disponíveis e são pré-configurados para exibir itens de procura de fluxo no menu da guia **Painel**. É possível incluir mais itens de painel de procura de fluxo em seu menu da guia **Painel**. Para obter mais informações, consulte Incluindo itens de painel com base em procura na lista Incluir itens.

Em um item de painel de procura de fluxo, os resultados da procura exibem os dados mais recentes em tempo real em um gráfico. Os tipos de gráficos suportados são série temporal, tabela, pizza e barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis. Para obter mais informações sobre a configuração de gráficos, consulte Configurando gráficos.

Os gráficos de série temporal são interativos. Usando os gráficos de série temporal, é possível ampliar e verificar uma linha do tempo para investigar a atividade de rede.

## Ofensas

É possível incluir vários itens relacionados à ofensa ao seu painel.

**Nota:** Ofensas ocultas ou encerradas não são incluídas nos valores que são exibidos na guia **Painel**. Para obter mais informações sobre eventos ocultos ou encerrados, consulte Gerenciamento de crime.

A tabela a seguir descreve os itens de Ofensa:

*Tabela 7. Itens de crime*

Itens de painel	Descrição
Crimes mais recentes	Os cinco crimes mais recentes são identificados com uma barra de magnitude para informá-lo sobre a importância da ofensa. Aponte para o nome da ofensa para visualizar informações detalhadas do endereço IP.
Crimes Mais Severos	As cinco ofensas mais graves são identificadas com uma barra de magnitude para informá-lo sobre a importância da ofensa. Aponte para o nome da ofensa para visualizar informações detalhadas do endereço IP.



*Tabela 7. Itens de crime (continuação)*

Itens de painel	Descrição
Meus Crimes	O item <b>Minhas ofensas</b> exibe 5 dos crimes mais recentes que são designadas a você. As ofensas são identificadas com uma barra de magnitude para informá-lo sobre a importância da ofensa. Aponte para o endereço IP para visualizar informações detalhadas do endereço IP.
Origens Principais	O item <b>Principais origens</b> exibe as principais origens de crime. Cada origem está identificada com uma barra de magnitude para informá-lo sobre a importância da origem. Aponte para o endereço IP para visualizar informações detalhadas do endereço IP.
Principais Destinos do Local	O item <b>Principais destinos do local</b> exibe os principais destinos do local. Cada destino é identificado com uma barra de magnitude para informá-lo sobre a importância do destino. Aponte para o endereço IP para visualizar as informações detalhadas do endereço IP.
Categorias	O item <b>Principais tipos de categorias</b> exibe as 5 principais categorias que são associadas ao maior número de crimes.

## Atividade de log

Os itens do painel **Atividade de log** permitirão monitorar e investigar eventos em tempo real.

**Nota:** Eventos fechados ou ocultos não são incluídos nos valores que são exibidos na guia **Painel**.

*Tabela 8. Itens de atividade de log*

Item do painel	Descrição
Procuras de Eventos	<p>É possível exibir um item do painel customizado que é baseado em critérios de procura salvos a partir da guia <b>Atividade de log</b>. Itens de procura de eventos são listados no menu <b>Incluir item &gt; Atividade de rede &gt; Procuras de eventos</b>. O nome do item de procura de eventos corresponde ao nome dos critérios de procura salvos nos quais o item é baseado.</p> <p>O QRadar inclui critérios de procura salvos que são pré-configurados para exibir itens de procura de evento em seu menu de guia <b>Painel</b>. É possível incluir mais itens de painel de procura em seu menu da guia <b>Painel</b>. Para obter mais informações, consulte Incluindo itens de painel baseados em procura na lista <b>Incluir itens</b>.</p> <p>Em um item de painel <b>Atividade de log</b>, os resultados da procura exibem dados reais de última hora em um gráfico. Os tipos de gráficos suportados são série temporal, tabela, pizza e barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis.</p> <p>Os gráficos de série temporal são interativos. É possível ampliar e verificar por meio de uma linha do tempo para investigar a atividade de log.</p>
Eventos por Gravidade	O item de painel <b>Eventos por severidade</b> exibe o número de eventos ativos que são agrupados por severidade. Este item permitirá que você veja o número de eventos que são recebidos pelo nível de severidade designado. A severidade indica a quantidade de ameaça que uma origem de crime representa em relação a quão preparado o destino está para o ataque. O intervalo de severidade é 0 (baixo) a 10 (alto). Os tipos de gráficos suportados são tabela, de pizza e de barras.
Principais Origens de Log	<p>O item de painel <b>Principais origens de log</b> exibe as 5 principais origens de log que enviaram eventos para o QRadar nos últimos 5 minutos.</p> <p>O número de eventos que são enviados da origem de log especificada é indicado no gráfico de pizza. Este item permitirá visualizar alterações potenciais no comportamento, por exemplo, se uma origem de log de firewall que não esteja geralmente na lista dos 10 principais agora contribuir com uma grande porcentagem da contagem de mensagens geral, será necessário investigar esta ocorrência. Os tipos de gráficos suportados são tabela, de pizza e de barras.</p>

## Relatórios mais recentes

O item de painel **Relatórios mais recentes** exibe os principais relatórios gerados recentemente.

O monitor fornece o título do relatório, a hora e a data em que o relatório foi gerado e o formato do relatório.

## Resumo do sistema

O item de painel **Resumo do sistema** fornece um resumo de alto nível de atividade nas últimas 24 horas.

Dentro do item de resumo, é possível visualizar as seguintes informações:

- **Fluxos atuais por segundo** – Exibe a taxa de fluxo por segundo.
- **Fluxos (últimas 24 horas)** – Exibe o número total de fluxos ativos que são vistos nas últimas 24 horas.
- **Eventos atuais por segundo** – Exibe a taxa de eventos por segundo.
- **Novos eventos (últimas 24 horas)** – Exibe o número total de novos eventos que são recebidos nas últimas 24 horas.
- **Ofensas atualizadas (últimas 24 horas)** – Exibe o número total de crimes que foram criadas ou modificadas com novas evidências nas últimas 24 horas.
- **Proporção de redução de dados** – Exibe a proporção de dados reduzidos com base no total de eventos que são detectados nas últimas 24 horas e o número de crimes modificadas nas últimas 24 horas.

## Risk Manager

Os itens de painel do Risk Manager serão exibidos apenas quando IBM Security QRadar Risk Manager for adquirido e licenciado.

Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.

É possível exibir um item do painel customizado que é baseado em critérios de procura salvos a partir da guia **Riscos**. Os itens de procura de conexão são listados no menu **Incluir item > Risk Manager > Procuras de conexão**. O nome do item de procura de conexão corresponde ao nome do critério de procura salvo no qual o item é baseado.

Os critérios de procura padrão salvos estão disponíveis e são pré-configurados para exibir itens de procura de conexão em seu menu da guia **Painel**. É possível incluir mais itens de painel de procura de conexão ao seu menu da guia **Painel**.

Em um item de painel **Procura de conexões**, os resultados da procura exibem os dados mais recentes em tempo real em um gráfico. Os tipos de gráficos suportados são série temporal, tabela, pizza e barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis. Para obter mais informações sobre a configuração do gráfico, consulte *Configurando gráficos*.

Os gráficos de série temporal são interativos. É possível ampliar e verificar por meio de uma linha do tempo para investigar a atividade de log.

## Itens de Gerenciamento de vulnerabilidade

Os itens do painel Gerenciamento de vulnerabilidade serão exibidos somente quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado.

Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*.

É possível exibir um item do painel customizado baseado em critérios de procura salvos a partir da guia **Vulnerabilidades**. Os itens de procura são listados no menu **Incluir item > Gerenciamento de vulnerabilidade > Procuras de vulnerabilidade**. O nome do item de procura corresponde ao nome do critério de procura salvo no qual o item é baseado.

O QRadar inclui o critério de procura salvo padrão que é pré-configurado para exibir itens de procura no menu da **guia Painel**. É possível incluir mais itens de painel de procura em seu menu da **guia Painel**.

Os tipos de gráficos suportados são tabela, de pizza e de barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis.

## Notificação do sistema

O item de painel **Notificação do sistema** exibe notificações de eventos que são recebidos pelo sistema.

Para notificações para mostrar no item de painel **Notificação do sistema**, o Administrador deve criar uma regra que é baseada em cada tipo de mensagem de notificação e selecionar a caixa de seleção **Notificar** no Assistente de Regras Customizadas.

Para obter mais informações sobre como configurar notificações do evento e criar regras de evento, consulte o *IBM Security QRadar SIEM Administration Guide*.

No item de painel **Notificações do sistema**, é possível visualizar as seguintes informações:

- **Sinalizador** – Exibe um símbolo para indicar o nível de severidade da notificação. Aponte para o símbolo para visualizar mais detalhes sobre o nível de severidade.
  - Ícone **Funcionamento**
  - Ícone **Informações (?)**
  - Ícone **Erro (X)**
  - Ícone **Aviso (!)**
- **Criado** - Exibe a quantidade de tempo decorrida desde que a notificação foi criada.
- **Descrição** – Exibe informações sobre a notificação.
- **Descartar ícone (x)** – Permitirá que seja fechada uma notificação do sistema.

É possível apontar o mouse sobre uma notificação para visualizar mais detalhes:

- **IP de host** – Exibe o endereço IP do host do host que originou a notificação.
- **Severidade** – Exibe o nível de severidade do incidente que criou esta notificação.
- **Categoria de nível inferior** – Exibe a categoria de nível inferior que está associada ao incidente que gerou esta notificação. Por exemplo: interrupção de serviço.
- **Carga útil** – Exibe o conteúdo de carga útil que está associado ao incidente que gerou esta notificação.
- **Criado** - Exibe a quantidade de tempo decorrida desde que a notificação foi criada.

Ao incluir o item de painel **Notificações do sistema**, as notificações do sistema também poderão ser exibidas como notificações pop-up na interface com o usuário

do QRadar. Estas notificações pop-up são exibidas no canto inferior direito da interface com o usuário, independentemente da guia selecionada.

Notificações pop-ups estão disponíveis apenas para usuários com permissões administrativas e são ativados por padrão. Para desativar notificações pop-up, selecione **Preferências do usuário** e limpe a caixa de seleção **Ativar notificações pop-up**.

Na janela pop-up Notificações do sistema, o número de notificações na fila é destacado. Por exemplo, se (1 a 12) for exibido no cabeçalho, a notificação atual é 1 de 12 notificações a serem exibidas.

A janela pop-up Notificação do sistema fornece as seguintes opções:

- **Próximo ícone (>)** – Exibe a próxima mensagem de notificação. Por exemplo, se a mensagem de notificação atual for 3 de 6, clique no ícone para visualizar 4 de 6.
- **Ícone fechar (X)** – Fecha essa janela pop-up de notificação.
- **(Detalhes)** - Exibe mais informações sobre essa notificação do sistema.

## Centro de informações de ameaça da Internet

O item de painel Centro de informações de ameaça da internet é um feed RSS integrado que fornece recomendações atualizadas sobre problemas de segurança, avaliações de ameaças diárias, notícias de segurança e repositórios de ameaças.

O diagrama Nível de ameaça atual indica o nível de ameaça atual e fornece um link para a página Nível de ameaça da Internet atual do website do IBM Internet Security Systems.

As recomendações atuais são listadas no painel de item. Para visualizar um resumo da recomendação, clique no ícone **Seta** próximo à recomendação. A recomendação é expandida para exibir um resumo. Clique no ícone **Seta** novamente para ocultar o resumo.

Para investigar a recomendação completa, clique no link associado. O site do IBM Internet Security Systems é aberto em uma janela do navegador e exibe os detalhes de recomendações completas.

---

## Criando um painel customizado

Você pode criar um painel customizado para visualizar um grupo de itens do painel que atendam a um determinado requisito.

### Sobre Esta Tarefa

Após criar um painel customizado, o novo painel será exibido na guia **Painel** e listado na caixa de listagem **Mostrar painel**. Um novo painel customizado é vazio por padrão; portanto, você deve incluir itens no painel.

### Procedimento

1. Clique na guia **Painel**.
2. Clique no ícone **Novo painel**.
3. No campo **Nome**, insira um nome exclusivo para o painel. O comprimento máximo é de 65 caracteres.

4. No campo **Descrição**, insira uma descrição do painel. O comprimento máximo é de 255 caracteres. Essa descrição é exibida na dica de ferramenta para o nome do painel na caixa de listagem **Mostrar painel**.
5. Clique em **OK**.

---

## Usando o painel para investigar a atividade de log ou de rede

Os itens do painel baseado em procuras fornecem um link para as guias **Atividade de log** ou **Atividade de rede**, permitindo a investigação de atividade de log ou de rede adicional.

### Sobre Esta Tarefa

Para investigar os fluxos de um item de painel **Atividade de log**:

1. Clique no link **Visualizar na atividade de log**. A guia **Atividade de log** é exibida, mostrando resultados e dois gráficos que correspondem aos parâmetros de seu item de painel.

Para investigar os fluxos de um item de painel **Atividade de rede**:

1. Clique no link **Visualizar na atividade de rede**. A guia **Atividade de rede** é exibida, mostrando resultados e dois gráficos que correspondem aos parâmetros do seu item de painel.

A guia **Atividade de rede** é exibida, mostrando resultados e dois gráficos que correspondem aos parâmetros do seu item de painel. Os tipos de gráficos exibidos na guia **Atividade de log** ou **Atividade de rede** dependem de qual gráfico foi configurado no item de painel:

Tipo de gráfico	Descrição
Barra, Pizza e Tabela	A guia <b>Atividade de log</b> ou a guia <b>Atividade de rede</b> exibe o gráfico de barras, gráfico de pizza e uma tabela dos detalhes de fluxo.
Séries Temporais	A guia <b>Atividade de log</b> ou <b>Atividade de rede</b> exibe gráficos de acordo com os critérios a seguir: <ol style="list-style-type: none"> <li>1. Se o intervalo de tempo for menor ou igual a 1 hora, um gráfico de séries temporais, um gráfico de barras e uma tabela de detalhes do evento ou fluxo serão exibidos.</li> <li>2. Se o intervalo de tempo for maior do que 1 hora, um gráfico de séries temporais será exibido e você será solicitado a clicar em <b>Atualizar Detalhes</b>. Essa ação inicia a procura que preenche os detalhes do evento ou fluxo e gera o gráfico de barras. Quando a procura for concluída, o gráfico de barras e tabela de detalhes do evento ou fluxo serão exibidos.</li> </ol>

---

## Configurando gráficos

Você pode configurar os itens do painel **Atividade do log**, **Atividade de rede** e **Conexões**, se aplicável, para especificar o tipo de gráfico e quantos objetos de dados você deseja visualizar.

### Sobre Esta Tarefa

*Tabela 9. Configurando gráficos. Opções de parâmetros.*

Opção	Descrição
Value to Graph	Na caixa de listagem, selecione o tipo de objeto que você deseja que apareça no gráfico. As opções incluem todos os eventos normalizados e customizados ou parâmetros de fluxo incluídos em seus parâmetros de procura.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico que você deseja visualizar. As opções incluem: <ol style="list-style-type: none"><li>1. <b>Gráfico de barras</b> – exibe dados em um gráfico de barras. Essa opção está disponível somente para eventos ou fluxos agrupados.</li><li>2. <b>Gráfico de pizza</b> – exibe dados em um gráfico de pizza. Essa opção está disponível somente para eventos ou fluxos agrupados.</li><li>3. <b>Tabela</b> - exibe dados em uma tabela. Essa opção está disponível somente para eventos ou fluxos agrupados.</li><li>4. <b>Séries temporais</b> – exibe um gráfico de linha interativo que representa os registros correspondentes para um intervalo de tempo especificado.</li></ol>
Display Top	Na caixa de listagem, selecione o número de objetos que você deseja visualizar no gráfico. As opções incluem 5 e 10. O padrão é 10.
Capturar Dados de Série Temporal	Selecione essa caixa de opção para ativar a captura de séries temporais. Ao selecionar essa caixa de seleção, o recurso gráfico iniciará a acumular dados para gráficos de séries temporais. Por padrão, essa opção está desativada.
Intervalo de tempo	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar.

As configurações de gráfico customizadas são retidas, para que elas sejam exibidas conforme configuradas cada vez que você acessar a guia **Painel**.

Os dados são acumulados para que, ao executar uma procura salva de séries temporais, haverá um cache de dados do evento ou fluxo disponível para exibir os dados para o período de tempo anterior. Os parâmetros acumulados são indicados por um asterisco (\*) na caixa de listagem **Value to graph**. Se você selecionar um value to graph que não for acumulado (sem asterisco), os dados de séries temporais não estarão disponíveis.

### Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que contém o item que você deseja customizar.
3. No cabeçalho do item painel que você deseja configurar, clique no ícone **Configurações**.
4. Configure os parâmetros do gráfico.

---

## Removendo itens do painel

Você pode remover itens de um painel e incluir o item novamente a qualquer momento.

## Sobre Esta Tarefa

Ao remover um item do painel, o item não será removido completamente.

### Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel do qual você deseja remover um item.
3. No cabeçalho de item do painel, clique no ícone vermelho [x] para remover o item do painel.

---

## Removendo um item do painel

Você pode remover um item do painel e exibi-lo em uma nova janela no sistema do desktop.

### Sobre Esta Tarefa

Ao remover um item do painel, o item do painel original permanecerá na guia **Painel**, enquanto uma janela separada com um item do painel duplicado permanecerá aberta e se atualizará durante os intervalos planejados. Se você fechar o aplicativo do QRadar, a janela separada permanecerá aberta para monitoramento e continuará a atualizar até que você feche a janela manualmente ou encerre o sistema de computador.

### Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel a partir do qual você deseja remover um item.
3. No cabeçalho de item do painel, clique no ícone verde para remover o item do painel e abri-o em uma janela separada.

---

## Renomeando um painel

Você pode renomear um painel e atualizar a descrição.

### Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que você deseja editar.
3. Na barra de ferramentas, clique no ícone **Renomear painel**.
4. No campo **Nome**, insira um novo nome para o painel. O comprimento máximo é de 65 caracteres.
5. No campo **Descrição**, insira uma nova descrição do painel. O comprimento máximo é de 255 caracteres.
6. Clique em **OK**.

---

## Excluindo um painel

Você pode excluir um painel.

## Sobre Esta Tarefa

Após excluir um painel, a guia **Painel** será atualizada e o primeiro painel listado na caixa de listagem **Mostrar painel** será exibido. O painel que você excluiu não será mais exibido na caixa de listagem **Mostrar painel**.

### Procedimento

1. Clique na guia **Painel**.
2. Na caixa de listagem **Mostrar painel**, selecione o painel que você deseja excluir.
3. Na barra de ferramentas, clique em **Excluir painel**.
4. Clique em **Sim**.

---

## Gerenciando notificações do sistema

Você pode especificar o número de notificações que você deseja exibir em seu item do painel **Notificação do sistema** e fechar as notificações do sistema após lê-las.

### Antes de Iniciar

Assegure-se de que o item do painel **Notificação do sistema** foi incluído em seu painel.

### Procedimento

1. No cabeçalho de item do painel **Notificação do sistema**, clique no ícone **Configurações**.
2. Na caixa de listagem **Exibir**, selecione o número de notificações do sistema que você deseja visualizar.
  - As opções são **5**, **10** (padrão), **20**, **50** e **Todos**.
  - Para visualizar todas as notificações do sistema efetuadas login nas últimas 24 horas, clique em **Todos**.
3. Para fechar uma notificação do sistema, clique no ícone **Excluir**.

---

## Incluindo itens de painel baseados em procura na lista **Incluir itens**

É possível incluir itens de painel baseados em procura no seu menu **Incluir itens**.

### Antes de Iniciar

Para incluir um item de painel de procura de evento e fluxo no menu **Incluir item** na guia **Painel**, é necessário acessar a guia **Atividade de log** ou **Atividade de rede** para criar critérios de procura que especificam que os resultados da procura podem ser exibidos na guia **Painel**. O critério de procura também deve especificar que os resultados sejam agrupados em um parâmetro.

## Sobre Esta Tarefa

Este procedimento se aplica a todos os itens de painel baseados em procura, incluindo os itens de painel do IBM Security QRadar Risk Manager. Os itens de painel do QRadar Risk Manager serão exibidos somente quando o QRadar Risk Manager for comprado e licenciado, e a conexão tenha sido estabelecida entre o Console e o dispositivo QRadar Risk Manager. Para obter mais informações, consulte o *IBM Security QRadar Risk Manager User Guide*



## Procedimento

1. Escolha:
  - Para incluir um item de painel de procura de fluxo, clique na guia **Atividade de rede**.
  - Para incluir um item de painel de procura de evento, clique na guia **Atividade de log**.
2. Na caixa de listagem **Procurar**, escolha uma das seguintes opções:
  - Para criar uma procura, selecione **Nova procura**.
  - Para editar uma procura salva, selecione **Editar procura**.
3. Configure ou edite seus parâmetros de procura, conforme necessário.
  - Na área de janela Editar procura, selecione a opção **Incluir em meu painel**.
  - Na área de janela Definição de coluna, selecione uma coluna e clique no ícone **Incluir coluna** para mover a coluna para a lista **Grupo por**.
4. Clique em **Filtrar**. Os resultados da procura são exibidos.
5. Clique em **Salvar critérios**. Consulte Salvando critérios de procura na guia Ofensa
6. Clique em **OK**.
7. Verifique se o seu critério de procura salvo incluiu de maneira bem-sucedida o item de painel da pesquisa de evento ou fluxo na lista **Incluir itens**
  - a. Clique na guia **Painel**.
  - b. Escolha uma das opções a seguir:
    - a. Para verificar um item de procura de eventos, selecione **Incluir item > Atividade de log > Procuras de eventos > Incluir item**.
    - b. Para verificar um item de procura de fluxo, selecione **Incluir item > Atividade de rede > Procuras de fluxo**. O item de painel é exibido na lista com o mesmo nome que os seus critérios de procura salvos.



---

## Capítulo 4. Gerenciamento de crimes

Eventos e fluxos com endereços IP de destino localizados em várias redes na mesma ofensa podem ser correlacionados. É possível investigar cada ofensa efetivamente em sua rede.

É possível navegar nas várias páginas da guia **Ofensas** para investigar detalhes de eventos e fluxos para determinar os eventos e fluxos exclusivos que causaram o crime.

---

### Visão geral da ofensa

Usando a guia **Ofensas**, é possível investigar um crime, endereços IP de origem e de destino, comportamentos de rede e anomalias em sua rede.

É possível também procurar ofensas baseadas em vários critérios. Para obter mais informações sobre a procura de crimes, consulte “Procuras de crime” na página 94.

### Considerações de permissão de crime

Todos os usuários podem visualizar todas as ofensas, independentemente de qual origem de log ou é fonte de fluxo está associada à ofensa.

A guia **Ofensas** não usa as permissões de usuário de nível de dispositivo para determinar quais ofensas cada usuário é capaz de visualizar, conforme determinado pelas permissões da rede.

Para obter mais informações sobre permissões no nível de dispositivo, consulte o *IBM Security QRadar SIEM Administration Guide*.

### Termos chave

Usando a guia **Ofensas**, é possível acessar e analisar Ofensas, endereços IP de Origem e endereços IP de Destino.

Item	Descrição
Ofensas	Uma ofensa inclui vários eventos ou fluxos que se originam de uma origem, como um host ou origem de log. A guia <b>Ofensas</b> exibe ofensas que incluem o tráfego e vulnerabilidades que colaboram e validam a magnitude de um crime. A magnitude de um crime é determinada por vários testes executados na ofensa cada vez que ela é reavaliada. A reavaliação ocorrerá quando eventos forem incluídos na ofensa e em intervalos planejados.
Endereços IP de origem	Um endereço IP de origem especifica o dispositivo que tenta violar a segurança de um componente em sua rede. Um endereço IP de origem pode usar vários métodos de ataque, como reconhecimento ou ataques de Negação de Serviço (DoS) para uma tentativa de acesso não autorizada.

Item	Descrição
Endereços IP de destino	Um endereço IP de destino especifica o dispositivo de rede que um endereço IP de origem tenta acessar.

## Retenção de crime

Na guia **Administração**, é possível definir as configurações do sistema do período de retenção de crimes para remover ofensas do banco de dados após um período de tempo configurado.

O período de retenção de crime padrão é três dias. Deve-se ter permissão administrativa para acessar a guia **Admin** e definir as configurações do sistema. Ao configurar os limites, são incluídos cinco dias em qualquer limite definido.

Ao fechar ofensas, as ofensas fechadas serão removidas do banco de dados após o período de retenção de crime transcorrer. Se mais eventos ocorrerem para um crime, uma nova ofensa será criada. Se for executada uma procura que inclui ofensas fechadas, o item será exibido nos resultados da procura se ele não tiver sido removido do banco de dados.

## Monitoramento de crime

Usando as visualizações diferentes disponíveis na guia **Ofensas**, é possível monitorar para determinar quais ofensas estão ocorrendo atualmente em sua rede.

As ofensas são listadas com a magnitude mais alta primeiro. É possível localizar e visualizar os detalhes de uma determinada ofensa, e, em seguida, executar uma ação em relação à ofensa, se necessário.

Após iniciar a navegação por meio de diversas visualizações, o topo da guia exibirá a trilha de navegação da visualização atual. Se quiser retornar para uma página visualizada anteriormente, clique no nome da página na trilha de navegação.

No menu de navegação na guia **Ofensas**, é possível acessar as páginas a seguir que estão listadas na tabela abaixo.

*Tabela 10. Páginas que podem ser acessadas a partir da guia Ofensas*

Página	Descrição
Meus Crimes	Exibe todas as ofensas que são designadas a você.
Todos os Crimes	Exibe todas as ofensas globais na rede.
Por Categoria	Exibe todas as ofensas que são agrupadas por categoria de alto e de baixo nível.
Por IP de Origem	Exibe todas as ofensas que são agrupadas por endereços IP de origem envolvidas em um crime.
Por IP de destino	Exibe todas as ofensas que são agrupadas por endereços IP de destino envolvidas em um crime.
Por rede	Exibe todas as ofensas que são agrupadas pelas redes envolvidas em um crime.
Regras	Fornecer acesso à página Regras, a partir da qual é possível visualizar e criar regras customizadas. Essa opção será exibida somente se tiver a permissão de função Visualizar regras customizadas. Para obter mais informações, consulte Gerenciamento de regra.

## Monitorando as páginas Todas Ofensas ou Minhas Ofensas

Você pode monitorar as ofensas na página Todas ofensas ou Minhas ofensas.

## Antes de Iniciar

A página Todas ofensas exibe uma lista de todas as ofensas que estão ocorrendo em sua rede. A página Minhas ofensas exibe uma lista de crimes que estão designados a você.

## Sobre Esta Tarefa

A parte superior da tabela exibe os detalhes dos parâmetros de procura de crime, caso exista, aplicados aos resultados da procura. Para limpar esses parâmetros da procura, você pode clicar em **Limpar filtro**. Para obter mais informações sobre a procura de crimes, consulte de procura.

**Nota:** Para visualizar uma área de janela na página de resumo em maiores detalhes, clique na opção da barra de ferramentas associada. Por exemplo, se você desejar visualizar os detalhes dos endereços IP de origem, clique em **Origens**. Para obter mais informações sobre as opções da barra de ferramentas, consulte as funções da barra de ferramentas na guia Ofensa.

## Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, selecione **Todas ofensas** ou **Minhas ofensas**.
3. Você pode refinar a lista de crimes com as opções a seguir:
  - Na caixa de listagem **Visualizar ofensas**, selecione uma opção para filtrar a lista de crimes para um prazo específico.
  - Clique no link **Limpar filtro** ao lado de cada filtro exibido na área de janela **Parâmetros de procura atuais**.
4. Dê um clique duplo na ofensa que você deseja visualizar.
5. Na página Resumo da ofensa, revise os detalhes da ofensa. Consulte os Parâmetros da ofensa.
6. Execute quaisquer ações necessárias na ofensa. Consulte as tarefas Gerenciamento de crime.

## Monitorando ofensas agrupadas por categoria

Você pode monitorar ofensas na página de detalhes Por categoria, que fornece uma lista de crimes agrupadas na categoria de nível superior.

## Sobre Esta Tarefa

Os campos de contagem, como **Contagem de eventos/fluxos** e **Contagem de origem**, não consideram as permissões de rede do usuário.

## Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Por categoria**.
3. Para visualizar grupos de categoria de nível inferior para uma determinada categoria de nível superior particular, clique no ícone de seta ao lado do nome da categoria de nível superior.
4. Para visualizar uma lista de crimes para uma categoria de nível inferior, dê um clique duplo na categoria de nível inferior.
5. Dê um clique duplo na ofensa que você deseja visualizar.

6. Na página Resumo da ofensa, revise os detalhes da ofensa. Consulte os Parâmetros da ofensa.
7. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de crime.

## Monitorando ofensas agrupadas por IP de origem

Na página Origem, você pode monitorar as ofensas agrupadas por endereço IP de origem.

### Sobre Esta Tarefa

Um endereço IP de origem especifica o host que gerou ofensas como um resultado de um ataque ao seu sistema. Todos os endereços IP de origem são listados com a mais alta grandeza primeiro. A lista de crimes exibe somente os endereços IP de origem com ofensas ativas.

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por IP de origem**.
3. Você pode refinar a lista de crimes que usam as opções a seguir:
  - Na caixa de listagem **Visualizar ofensas**, selecione uma opção para filtrar a lista de crimes para um prazo específico.
  - Clique no link **Limpar filtro** ao lado de cada filtro exibido na área de janela **Parâmetros de procura atuais**.
4. Dê um clique duplo no grupo que você deseja visualizar.
5. Para visualizar uma lista de endereços IP de destino local para o endereço IP de origem, clique em **Destinos** na barra de ferramentas da página Origem.
6. Para visualizar uma lista de crimes associadas a esse endereço IP de origem, clique em **Ofensas** na barra de ferramentas da página Origem.
7. Dê um clique duplo na ofensa que você deseja visualizar.
8. Na página Resumo da ofensa, revise os detalhes da ofensa. Consulte os Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de crime.

## Monitorando ofensas agrupadas por IP de destino

Na página Destinos, você pode monitorar ofensas agrupadas por endereços IP de destino do local.

### Sobre Esta Tarefa

Todos os endereços IP de destino são listados com a mais alta grandeza primeiro.

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por IP de destino**.
3. Você pode refinar a lista de crimes que usam as opções a seguir:
  - Na caixa de listagem **Visualizar ofensas**, selecione uma opção para filtrar a lista de crimes para um prazo específico.
  - Clique no link **Limpar filtro** ao lado de cada filtro exibido na área de janela **Parâmetros de procura atuais**.

4. Dê um clique duplo no endereço IP de destino que você deseja visualizar.
5. Para visualizar uma lista de crimes associada a esse endereço IP de destino, clique em **Ofensas** na barra de ferramentas da página Destino.
6. Para visualizar uma lista de endereços IP de origem associada a esse endereço IP de destino, clique em **Origens** na barra de ferramentas da página Destino.
7. Dê um clique duplo na ofensa que você deseja visualizar.
8. Na página Resumo da ofensa, revise os detalhes da ofensa. Consulte os Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de crime.

## Monitorando ofensas agrupadas por rede

Na página redes, você pode monitorar as ofensas que estão agrupadas por rede.

### Sobre Esta Tarefa

Todas as redes são listadas com a mais alta grandeza primeiro.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Por Rede**.
3. Dê um clique duplo na rede que você deseja visualizar.
4. Para visualizar uma lista de endereços IP de origem associado a essa rede, clique em **Origens** na barra de ferramentas da página Rede.
5. Para visualizar uma lista de endereços IP de destino associado a essa rede, clique em **Destinos** na barra de ferramentas da página Rede.
6. Para visualizar uma lista de crimes associadas a essa rede, clique em **Ofensas** na barra de ferramentas da página Rede.
7. Dê um clique duplo na ofensa que você deseja visualizar.
8. Na página Resumo da ofensa, revise os detalhes da ofensa. Consulte os Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de crime.

---

## Tarefas de gerenciamento de crime

Ao monitorar ofensas, é possível executar ações na ofensa.

É possível executar as seguintes ações:

- Incluir notas
- Remover ofensas
- Proteger ofensas
- Exportar dados de crime para XML ou CSV
- Designar ofensas para outros usuários
- Enviar notificações por email
- Marcar um crime para acompanhamento
- Ocultar ou fechar um crime de qualquer lista de crimes

Para realizar uma ação em vários crimes, mantenha a tecla Control pressionada ao selecionar cada ofensa desejada. Para visualizar detalhes da ofensa em uma nova página, mantenha pressionada a tecla Control ao clicar duas vezes em um crime.

## Incluindo notas

É possível incluir notas em qualquer ofensa na guia **Ofensas**. As notas podem incluir informações que você deseja capturar para o crime, como o número de chamado do Suporte ao Cliente ou informações de gerenciamento de crime.

### Sobre Esta Tarefa

As notas podem incluir até 2000 caracteres.

### Procedimento

1. Clique na guia **Ofensas**.
2. Navegue para o crime na qual deseja incluir notas.
3. Dê um clique duplo no crime.
4. Na caixa de listagem **Ações**, selecione **Incluir nota**.
5. Digite a nota que deseja incluir nesta ofensa.
6. Clique em **Incluir nota**.

### Resultados

A nota é exibida na área de janela Últimas 5 notas no resumo Ofensa. O ícone **Notas** é exibido na coluna de sinalizador da lista **Ofensas**. Se passar o mouse sobre o indicador de notas na coluna **Sinalizador** da lista **Ofensas**, a nota dessa ofensa será exibida.

## Ocultando ofensas

Para evitar que um crime seja exibida no guia **Ofensas**, você pode ocultar o crime.

### Sobre Esta Tarefa

Após ocultar um crime, ela não será mais exibida em qualquer lista (por exemplo, Todas as ofensas) na guia **Ofensas**; entretanto, se você executar uma procura que inclua as ofensas ocultas, o item será exibido nos resultados da procura.

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Selecione o ofensa que você deseja ocultar.
4. Na caixa de listagem **Ações**, selecione **Ocultar**.
5. Clique em **OK**.

## Mostrando ofensas ocultas

Ofensas ocultas não estão visíveis na guia **Ofensas**, no entanto, você pode mostrar ofensas ocultas se desejar visualizá-las novamente.

### Sobre Esta Tarefa

Para mostrar ofensas ocultas, você deve executar uma procura que inclui ofensas ocultas. Os resultados da pesquisa incluem todas as ofensas, incluindo as ofensas



ocultas e não ocultas. Ofensas são especificadas como ocultas pelo ícone **Oculto** na coluna **Sinalizar**.

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Procure por ofensas ocultas:
  - a. Na caixa de listagem **Procurar**, selecione **Nova procura**.
  - b. Na lista **Opção Excluir** na área de janela Procurar Parâmetros, limpe a caixa de seleção **Ofensas ocultas**.
  - c. Clique em **Procurar**.
4. Localize e selecione o crime oculta que deseja mostrar.
5. Na caixa de listagem **Ações**, selecione **Mostrar**.

## Fechando ofensas

Para remover um crime completamente do sistema, é possível fechar o crime.

### Sobre Esta Tarefa

Após fechar (excluir) as ofensas, as ofensas não serão mais exibidas em nenhuma lista (por exemplo, Todas as ofensas) na guia **Ofensas**. As ofensas encerradas são removidas do banco de dados após o período de retenção de crime transcorrer. O período de retenção de crime padrão é três dias. Se mais eventos ocorrerem para um crime, uma nova ofensa será criada. Se for executada uma procura que inclui ofensas fechadas, o item será exibido nos resultados da procura se ele não tiver sido removido do banco de dados.

Ao fechar ofensas, será necessário selecionar um motivo para fechar o crime e é possível incluir uma nota. O campo **Notas** exibe a nota que é inserida para o fechamento da ofensa anterior. Notas não devem exceder 2.000 caracteres. Essa nota é exibida na área de janela Notas desta ofensa. Se tiver a permissão Gerenciar fechamento da ofensa, será possível incluir novos motivos customizados na caixa de listagem **Motivo para fechamento**.

Para obter informações adicionais, consulte o *IBM Security QRadar SIEM Administration Guide*.

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Escolha uma das opções a seguir:
  - Selecione o crime que deseja fechar e, em seguida, selecione **Fechar** da caixa de listagem **Ações**.
  - Na caixa de listagem **Ações**, selecione **Fechar listados**.
4. Na caixa de listagem **Razão para fechamento**, selecione um motivo. O motivo padrão é **non-issue**.
5. Opcional. No campo **Notas**, digite uma nota para fornecer mais informações sobre o fechamento da nota.
6. Clique em **OK**.

## Resultados

Após fechar as ofensas, as contagens que são exibidas na área de janela Por categoria da guia **Ofensas** podem levar vários minutos para refletir as ofensas fechadas.

## Protegendo crimes

Você pode evitar com que as ofensas sejam removidas do banco de dados depois que o período de retenção decorrer.

### Sobre Esta Tarefa

As ofensas são retidas por um período de retenção configurável. O período de retenção padrão é de três dias; no entanto, os Administradores podem customizar o período de retenção. Você pode ter as ofensas que você deseja reter independentemente do período de retenção. Você pode evitar com que essas ofensas sejam removidas do banco de dados após o período de retenção ter decorrido.

Para obter mais informações sobre o Período de Retenção de Ofensa, consulte o *IBM Security QRadar SIEM Administration Guide*.

#### CUIDADO:

**Quando o modelo de dados do SIM for reconfigurado na opção Limpeza Permanente, todas as ofensas, incluindo as ofensas protegidas, serão removidas do banco de dados e do disco. Você deve ter os privilégios administrativos para reconfigurar o modelo de dados SIM.**

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Escolha uma das opções a seguir:
  - Selecione o crime que você deseja proteger e, em seguida, selecione **Proteger** na caixa de listagem **Ações**.
  - Na caixa de listagem **Ações**, selecione **Proteger listados**.
4. Clique em **OK**.

### Resultados

A ofensa protegida é indicada por um ícone **Protegido** na coluna **Sinalizador**.

## Desprotegendo ofensas

Você pode desproteger as ofensas que foram protegidas anteriormente à remoção após o período de retenção da ofensa ter decorrido.

### Sobre Esta Tarefa

Para listar apenas ofensas protegidas, você pode executar uma procura que os filtra apenas para ofensas protegidas. Se você desmarcar a caixa de seleção **Protegido** e certificar-se de que todas as outras opções estejam selecionadas na lista **Exclui opção** na área de janela Parâmetros de Procura, apenas ofensas protegidas serão exibidas.

## Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Opcional. Execute uma procura que exibe apenas ofensas protegidas.
4. Escolha uma das opções a seguir:
  - Selecione o crime que você deseja proteger e, em seguida, selecione **Desproteger** na caixa de listagem **Ações**.
  - Na caixa de listagem **Ações**, selecione **Desproteger listados**.
5. Clique em **OK**.

## Exportando ofensas

Você pode exportar ofensas no formato de Linguagem de Marcação Extensível (XML) ou de valores separados por vírgulas (CSV).

### Sobre Esta Tarefa

Se você desejar reutilizar ou armazenar seus dados de crime, será possível exportar as ofensas. Por exemplo, você pode exportar as ofensas para criar relatórios não baseados no produto QRadar. Você também pode exportar ofensas como uma estratégia de retenção de longo prazo secundária. O Suporte ao Cliente pode requerer que você exporte as ofensas a fim de resolver os problemas.

O arquivo CSV ou XML resultante inclui os parâmetros especificados na área de janela Definição de coluna de seus parâmetros de procura. A duração de tempo necessária para exportar seus dados depende do número de parâmetros especificados.

## Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Todas ofensas**.
3. Selecione o crime que você deseja exportar.
4. Escolha uma das opções a seguir:
  - Para exportar as ofensas em formato XML, selecione **Ações > Exportar para XML** na caixa de listagem **Ações**.
  - Para exportar as ofensas em formato CSV, selecione **Ações > Exportar para CSV** na caixa de listagem **Ações**.
5. Escolha uma das opções a seguir:
  - Para abrir a lista para visualização imediata, selecione a opção **Abrir com** e selecione um aplicativo da caixa de listagem.
  - Para salvar a lista, selecione a opção **Salvar no disco**.
6. Clique em **OK**.

## Designando ofensas para usuários

Usando a guia **Ofensas**, é possível designar ofensas a usuários para investigação.

### Sobre Esta Tarefa

Quando um crime for designada a um usuário, ela será exibida na página Minhas ofensas pertencente a esse usuário. Deve-se ter os privilégios apropriados para designar ofensas a usuários.

É possível designar ofensas a usuários a partir da guia **Ofensas** ou da página Resumo de crimes. Este procedimento fornece instruções sobre como designar ofensas na guia **Ofensas**.

**Nota:** A caixa de listagem **Nome de usuário** só exibirá os usuários que possuem privilégios da guia **Ofensas**.

### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Selecione o crime que deseja designar.
4. Na caixa de listagem **Ações**, selecione **Designar**.
5. Na caixa de listagem **Nome de usuário**, selecione o usuário ao qual você deseja designar essa ofensa.
6. Clique em **Salvar**.

### Resultados

A ofensa é designada ao usuário selecionado. O ícone **Usuário** é exibido na coluna Sinalizador da guia **Ofensas** para indicar que o crime foi designada. O usuário designado pode ver esta ofensa na página Minhas ofensas.

## Enviando notificação por email

Você pode enviar um email contendo um resumo de crime para qualquer endereço de email válido.

### Sobre Esta Tarefa

O corpo da mensagem de email inclui as informações a seguir, se disponíveis:

- Endereço IP de origem
- Nome do usuário de origem, nome do host ou nome do recurso
- Número total de fontes
- As cinco principais fontes de magnitude
- Redes de origem
- Endereço IP de destino
- Nome do usuário de destino, nome do host ou nome do recurso
- Número total de destinos
- Os cinco principais destinos de magnitude
- Redes de destino
- Número total de eventos
- As regras que fizeram com que a regra de evento ou ofensa disparasse
- A descrição da regra de evento ou ofensa
- ID da ofensa
- As cinco categorias principais
- Horário de início da ofensa ou horário em que o evento foi gerado
- As cinco anotações principais
- Link para a interface com o usuário da ofensa
- Contribuindo com as regras do CRE

## Procedimento

1. Clique na guia **Ofensas**.
2. Navegue até o crime a qual você deseja enviar uma notificação por email.
3. Dê um clique duplo no crime.
4. Na caixa de listagem **Ações**, selecione **Email**.
5. Configure os parâmetros a seguir:

Opção	Descrição
Parâmetro	Descrição
Para	Insira o endereço de email do usuário que você deseja notificar, se uma alteração ocorrer na ofensa selecionada. Separe diversos endereços de emails com uma vírgula.
De	Insira o endereço de email de origem padrão. O padrão é root@localhost.com.
Assunto do E-mail	Insira o assunto padrão no email. O padrão é o ID da Ofensa.
Mensagem de Email	Insira a mensagem padrão que você deseja acompanhar no email de notificação.

6. Clique em **Enviar**.

## Marcando um item para acompanhamento

Usando a guia **Ofensas**, você pode marcar um crime, um endereço IP de origem, um endereço IP de destino e uma rede para acompanhamento. Isso permitirá que você controle um item específico para investigação adicional.

## Procedimento

1. Clique na guia **Ofensas**.
2. Navegue até o crime que você deseja marcar para acompanhamento.
3. Dê um clique duplo no crime.
4. Na caixa de listagem **Ações**, selecione **Acompanhar**.

## Resultados

A ofensa agora exibe um sinalizador na coluna **Sinalizadores**, indicando que o crime está sinalizada para o acompanhamento. Se você não vir sua ofensa sinalizada na lista de crimes, será possível classificar a lista para exibir todas as ofensas sinalizadas primeiro. Para classificar uma lista de crime por ofensa sinalizada, dê um clique duplo no cabeçalho da coluna **Sinalizadores**.

---

## Funções da barra de ferramentas da guia de crime

Cada página e tabela na guia **Ofensas** possui uma barra de ferramentas para fornecer as funções necessárias para executar determinadas ações ou para investigar os fatores que contribuem com um crime.

*Tabela 11. Funções da barra de ferramentas da guia de crime*

Função	Descrição
Incluir Nota	Clique em <b>Incluir nota</b> para incluir uma nova nota a um crime. Esta opção está disponível somente na área de janela Últimas 5 Notas da página Resumo de crimes

Tabela 11. Funções da barra de ferramentas da guia de crime (continuação)

Função	Descrição
Ações	<p>As opções disponíveis na caixa de listagem <b>Ações</b> variam com base na página, tabela ou item (como um crime ou endereço IP de origem). A caixa de listagem <b>Ações</b> talvez não exiba exatamente conforme listado a seguir.</p> <p>Na caixa de listagem <b>Ações</b>, é possível escolher uma das seguintes ações:</p> <ul style="list-style-type: none"> <li>• <b>Acompanhamento</b> – Selecione esta opção para marcar um item para acompanhamento posterior. Consulte Marcar um item para acompanhamento.</li> <li>• <b>Ocultar</b> – Selecione esta opção para ocultar um crime. Para obter mais informações sobre ocultar ofensas, consulte Ocultando ofensas.</li> <li>• <b>Mostrar</b> – Selecione esta opção para mostrar todos os crimes ocultos.</li> <li>• <b>Proteger ofensas</b> – Selecione esta opção para proteger um crime. Para obter mais informações sobre como proteger os crimes, consulte Protegendo ofensas.</li> <li>• <b>Fechar</b> – Selecione esta opção para fechar um crime. Para obter mais informações sobre o fechamento de crimes, consulte Fechamento de crimes.</li> <li>• <b>Fechar listada</b> – Selecione essa opção para fechar um crime listada. Para obter mais informações sobre o fechamento de crimes listadas, consulte Fechamento de crimes.</li> <li>• <b>Email</b> – Selecione esta opção para enviar por email um resumo de crime para um ou mais destinatários. Consulte Enviando notificação por email.</li> <li>• <b>Incluir nota</b> – Selecione esta opção para incluir notas em um item. Consulte Incluindo notas.</li> <li>• <b>Designar</b> – Selecione esta opção para designar um crime a um usuário. Consulte Designando ofensas a usuários.</li> <li>• <b>Imprimir</b> – Selecione esta opção para imprimir um crime</li> </ul>
Annotations	<p>Clique em <b>Anotações</b> para visualizar todas as anotações de um crime.</p> <ul style="list-style-type: none"> <li>• <b>Anotação</b> – Especifica os detalhes da anotação. Anotações são descrições de texto que podem incluir automaticamente regras para ofensas como parte da resposta da regra.</li> <li>• <b>Horário</b> – Especifica a data e hora em que a anotação foi criada.</li> <li>• <b>Ponderação</b> – Especifica a ponderação da anotação.</li> </ul>
Anomalia	<p>Clique em <b>Anomalia</b> para exibir os resultados da procura salva que fazem com que a regra de detecção de anomalia gere o crime. <b>Nota:</b> Este botão será exibido apenas se o crime for gerada por uma regra de detecção de anomalia.</p>
Categorias	<p>Clique em <b>Categorias</b> para visualizar as informações sobre categoria da ofensa.</p> <p>Para investigar os eventos que são relacionados a uma categoria específica, é possível também clicar com o botão direito em uma categoria e selecionar <b>Eventos</b> ou <b>Fluxos</b>. Como alternativa, é possível destacar a categoria e clicar no ícone <b>Eventos</b> ou <b>Fluxos</b> na barra de ferramentas Lista de Categorias de Eventos.</p>
Conexões	<p>Clique em <b>Conexões</b> para investigar ainda mais as conexões. <b>Nota:</b> Esta opção estará disponível apenas se você tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i>.</p> <p>Quando o ícone <b>Conexões</b> for clicado, a página de critérios de procura de conexão será exibida em uma nova página, preenchida previamente com critérios de procura de eventos.</p> <p>Você pode customizar os parâmetros de procura, se necessário. Clique em <b>Procurar</b> para visualizar as informações de conexão.</p>
Destino	<p>Clique em <b>Destinos</b> para visualizar todos os endereços IP de destino do local de um crime, endereço IP de origem, ou rede. <b>Nota:</b> Se os endereços IP de destino forem remotos, uma página separada será aberta fornecendo informações de endereços IP de destino remoto.</p>
Exibir	<p>A página Resumo de crime exibe muitas tabelas de informações relacionadas a um crime. Para localizar uma tabela, é possível rolar para a tabela que deseja visualizar, ou selecionar a opção da caixa de listagem <b>Exibir</b>.</p>
Eventos	<p>Clique em <b>Eventos</b> para visualizar todos os eventos de um crime. Ao clicar em <b>Eventos</b>, os resultados da procura de eventos serão exibidos.</p>

Tabela 11. Funções da barra de ferramentas da guia de crime (continuação)

Função	Descrição
Fluxos	Clique em <b>Fluxos</b> para investigar mais detalhadamente os fluxos que estão associados a um crime. Ao clicar em <b>Fluxos</b> , os resultados da procura de fluxo serão exibidos.
Origens de Log	Clique em <b>Origens de Log</b> para visualizar todas as origens de log de um crime.
Redes	Clique em <b>Redes</b> para visualizar todas as redes de destino de um crime.
Notas	Clique em <b>Notas</b> para visualizar todas as notas de um crime, endereço IP de origem, endereço IP de destino ou rede. Para obter mais informações sobre as notas, consulte Incluindo notas
Ofensas	Clique em <b>Ofensas</b> para visualizar uma lista de crimes que estão associadas a um endereço IP de origem, endereço IP de destino ou rede.
Imprimir	Clique em <b>Imprimir</b> para imprimir um crime.
Regras	Clique em <b>Regras</b> para visualizar todas as regras que contribuíram para um crime. A regra que criou o crime é listada primeiro.  Se tiver permissões apropriadas para editar uma regra, clique duas vezes na regra para iniciar a página Editar regras.  Se a regra for excluída, um ícone vermelho (x) será exibido ao lado da regra. Se clicar duas vezes em uma regra excluída, uma mensagem será exibida para indicar que a regra não existe mais.
Salvar Critérios	Após executar uma procura de crime, clique em <b>Salvar critérios</b> para salvar seus critérios de procura para uso futuro.
Salvar Layout	Por padrão, a página Detalhes por categoria é classificada pelo parâmetro Offense Count. Se alterar a ordem de classificação ou classificar por um parâmetro diferente, clique em <b>Salvar layout</b> para salvar a exibição atual como sua visualização padrão. Na próxima vez que for efetuado login na guia <b>Ofensas</b> , o layout salvo será exibido.
Procura	Esta opção está disponível somente na barra de ferramentas da tabela Lista de Destinos do Local.  Clique em <b>Procurar</b> para filtrar os IPs de destino para um endereço IP de origem. Para filtrar destinos:  1. Clique em <b>Procurar</b> .  2. Insira valores para os seguintes parâmetros: <ul style="list-style-type: none"> <li>• <b>Rede de destino</b> – Na caixa de listagem, selecione a rede que deseja filtrar.</li> <li>• <b>Magnitude</b> – Na caixa de listagem, selecione se deseja filtrar por magnitude Igual a, Menor que ou Maior que o valor configurado.</li> <li>• <b>Classificar por</b> – Na caixa de listagem, selecione como deseja classificar os resultados do filtro.</li> </ul> 3. Clique em <b>Procurar</b> .
Mostrar Categorias Inativas	Na página de detalhes Por categoria, as contagens de cada categoria são acumuladas a partir dos valores nas categorias de nível inferior. As categorias de nível inferior com ofensas associadas são exibidas com uma seta. É possível clicar na seta para visualizar as categorias de nível inferior associadas. Se desejar visualizar todas as categorias, clique em <b>Mostrar categorias inativas</b> .
Origens	Clique em <b>Origens</b> para visualizar todos os endereços IP de origem da ofensa, endereço IP de destino ou rede.
Resumo	Se uma opção for clicada na lista de exibição <b>Exibir</b> , será possível clicar em <b>Resumo</b> para retornar para a visualização de resumo detalhada.
Users	Clique em <b>Usuários</b> para visualizar todos os usuários que estão associados a um crime.
Visualizar caminho de ataque	Clique em <b>Visualizar caminho de ataque</b> para investigar mais detalhadamente o caminho de ataque de um crime. Ao clicar no ícone <b>Visualizar caminho de ataque</b> , a página Topologia atual será exibida em uma nova página. <b>Nota:</b> Esta opção estará disponível apenas se você tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i> .
Visualizar topologia	Clique em <b>Visualizar topologia</b> para fazer uma investigação adicional da origem de um crime. Ao clicar no ícone <b>Visualizar topologia</b> , a página Topologia atual será exibida em uma nova página. <b>Nota:</b> Esta opção estará disponível somente quando IBM Security QRadar Risk Manager for adquirido e licenciado. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i> .

## Parâmetros da ofensa

Esta tabela fornece descrições de parâmetros que são fornecidos na guia Ofensas.

A tabela a seguir fornece descrições de parâmetros que são fornecidos em todas as páginas da guia Ofensas.

*Tabela 12. Descrição dos parâmetros da guia Ofensas*

Parâmetro	Localização	Descrição
Annotation	Tabela 5 principais anotações	Especifica os detalhes da anotação. Anotações são descrições de texto que podem incluir automaticamente regras para ofensas como parte da resposta da regra. .
Anomalia	Tabela 10 últimos eventos (eventos de anomalia)	Selecione esta opção para exibir os resultados da procura salvos que fazem com que a regra de detecção de anomalias gere o evento.
Texto de Anomalia	Tabela 10 últimos eventos (eventos de anomalia)	Especifica uma descrição do comportamento anômalo detectado pela regra de detecção de anomalia.
Valor da Anomalia	Tabela 10 últimos eventos (eventos de anomalia)	Especifica o valor que faz com que a regra de detecção de anomalias gere o crime.
Aplicativo	Tabela 10 últimos fluxos	Especifica o aplicativo que está associado ao fluxo.
Nom do Aplicativo	Tabela de origem da ofensa, se o Tipo de crime for ID do aplicativo	Especifica o aplicativo que está associado ao fluxo que criou o crime.
ASN Index	Tabela de origem da ofensa, se o Tipo de crime for ASN de origem ou de destino	Especifica o valor ASN que está associado ao fluxo que criou o crime.
Nome do Ativo	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o nome do ativo, que pode ser designado usando a função Perfil de ativo.
Ponderação do ativo	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica a ponderação do ativo, que pode ser designada usando a função Perfil de ativo.
Designado a	Tabela de crime	Especifica o usuário designado à ofensa.  Se nenhum usuário for designado, este campo especificará Não designado. Clique em Não designado para designar o crime a um usuário.
Categoria	Tabela 10 últimos eventos	Especifica a categoria do evento.
Nome da Categoria	Página Por detalhes da categoria	Especifica o nome da categoria de alto nível.
Encadeado	<ul style="list-style-type: none"> <li>Tabela de origem de crime, se o Tipo de crime for o IP de destino</li> <li>Tabela 5 principais IPs de destino</li> </ul>	Especifica se o endereço IP de destino está encadeado.  Um endereço IP de destino encadeado é associado a outras ofensas. Por exemplo, um endereço IP de destino pode ser o endereço IP de origem de outra ofensa. Se o endereço IP de destino for encadeado, clique em <b>Sim</b> para visualizar as ofensas encadeadas.
Data de Criação	Tabela 5 últimas notas	Especifica a data e a hora em que a nota foi criada.
Credibilidade	Tabela de crime	Especifica a credibilidade da ofensa, conforme determinado pela classificação de credibilidade a partir de dispositivos de origem. Por exemplo, a credibilidade é aumentada quando várias ofensas relatam o mesmo evento ou fluxo.
Parâmetros de Procura Atuais	<ul style="list-style-type: none"> <li>Página Por detalhes de IP de origem</li> <li>Página Por detalhes de IP de destino</li> </ul>	A parte superior da tabela exibe os detalhes dos parâmetros de procura aplicados aos resultados da procura. Para limpar esses parâmetros de procura, clique em <b>Limpar filtro</b> . <b>Nota:</b> Esse parâmetro só será exibido após você aplicar um filtro.



Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Descrição	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Tabela de crime</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> <li>• Tabela de origem de crimes, se o Tipo de crime for Fonte de log</li> <li>• Tabela 5 principais origens de log</li> </ul>	Especifica a descrição da ofensa ou origem de log.
IP de Destino	<ul style="list-style-type: none"> <li>• Tabela 10 últimos eventos</li> <li>• Tabela 10 últimos fluxos</li> </ul>	Especifica o endereço IP de destino do evento ou fluxo.
IP de Destino	<ul style="list-style-type: none"> <li>• Tabela 5 principais IPs de destino</li> <li>• Página Por IP de origem – Lista de destinos do local</li> <li>• Página Por detalhes de IP de destino</li> <li>• Página Por rede – Lista de destinos do local</li> </ul>	Especifica o endereço IP do destino. Se as consultas de DNS estiverem ativadas na guia Administrador, será possível visualizar o nome DNS apontando seu mouse no endereço IP.
Destination IP(s)	Tabela de crime	Especifica os endereços IP e o nome do ativo (se disponível) dos destinos locais ou remotos. Clique no link para visualizar mais detalhes.
IPs de Destino	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> </ul>	Especifica os endereços IP e o nome do ativo (se disponível) dos destinos locais ou remotos. Se mais de um endereço IP de destino estiver associado à ofensa, este campo especificará Vários e o número de endereços IP de destino.
IPs de Destino	<ul style="list-style-type: none"> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> </ul>	Especifica os endereços IP e nomes de ativos (se disponível) do destino que está associado à ofensa. Se consultas de DNS estiverem ativadas na guia Administração, será possível visualizar o nome DNS apontando seu mouse no endereço IP ou nome do ativo.
IPs de Destino	Página Por detalhes de rede	Especifica o número de endereços IP de destino associados à rede.
Porta de destino	Tabela 10 últimos fluxos	Especifica a porta de destino do fluxo.
Destino(s)	<ul style="list-style-type: none"> <li>• Tabela 5 principais IPs de origem</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Por IP de destino – Lista de origens</li> <li>• Página Por rede – Lista de origens</li> </ul>	Especifica o nome do evento, conforme identificado no mapa QID, que está associado ao evento ou fluxo que criou o crime. Passe o seu mouse sobre o nome do evento para visualizar o QID.
Contagem de Eventos/Fluxos	Página Por detalhes da categoria	<p>Especifica o número de eventos ativos ou fluxo (eventos ou fluxos que não estão encerrados ou ocultados) associados à ofensa na categoria.</p> <p>Ofensas só ficam ativas por um período de tempo se nenhum novo evento ou fluxo for recebido. As ofensas ainda são exibidas na guia Ofensas, mas não são contadas nesse campo.</p>

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Contagem de Eventos/Fluxos	Página de destino Página de rede	Especifica o número de eventos e fluxos que ocorreram na ofensa e o número de categorias.  Clique no link eventos para investigar os eventos que são associados à ofensa. Ao clicar no link de eventos, os resultados da procura de eventos serão exibidos.  Clique no link de fluxos para investigar detalhadamente os fluxos que são associados às ofensas. Ao clicar no link de fluxos, os resultados da procura de fluxo serão exibidos.  <b>Nota:</b> Se a contagem de fluxo exibir N/A., o crime poderá ter uma data de início que precede a data que foi feito upgrade para a versão 7.1.0 (MR1) do seu produto QRadar. Portanto, os fluxos não podem ser contados. É possível, no entanto, clicar no link N/A para investigar os fluxos associados nos resultados da procura de fluxo.
Contagem de Eventos/Fluxos	Página Por detalhes da categoria	Especifica o número de eventos ativos ou fluxo (eventos ou fluxos que não estão encerrados ou ocultados) associados à ofensa na categoria.  Ofensas só ficam ativas por um período de tempo se nenhum novo evento ou fluxo for recebido. As ofensas ainda são exibidas na guia Ofensas, mas não são contadas nesse campo.
Contagem de Eventos/Fluxos	Página de destino Página de rede	Especifica o número de eventos e fluxos que ocorreram na ofensa e o número de categorias.  Clique no link eventos para investigar os eventos que são associados à ofensa. Ao clicar no link de eventos, os resultados da procura de eventos serão exibidos.  Clique no link de fluxos para investigar detalhadamente os fluxos que são associados às ofensas. Ao clicar no link de fluxos, os resultados da procura de fluxo serão exibidos.  <b>Nota:</b> Se a contagem de fluxo exibir N/A., o crime poderá ter uma data de início que precede a data que foi feito upgrade para a versão 7.1.0 (MR1) do seu produto QRadar. Portanto, os fluxos não podem ser contados. É possível, no entanto, clicar no link N/A para investigar os fluxos associados nos resultados da procura de fluxo.
Eventos	<ul style="list-style-type: none"> <li>• Página Todos os crimes</li> <li>• Página Minhas ofensas</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino - Lista de crimes</li> </ul>	Especifica o número de eventos da ofensa.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Events/Flows	<ul style="list-style-type: none"> <li>• A tabela de origem de crime, se o Tipo de crime for IP de origem, IP de destino, Nome do host, Porta de origem ou destino do nome de usuário, Nome do evento, Porta, Endereço MAC de origem ou destino, Fonte de log, Source IPv6 ou Destination IPv6, ASN de origem ou destino, Regra, ID do aplicativo</li> <li>• Tabela 5 principais IPs de origem</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Por IP de destino – Lista de origens</li> <li>• Página Por rede – Lista de origens</li> <li>• Página Detalhes da origem</li> <li>• Tabela 5 principais IPs de destino</li> <li>• Página Por IP de origem – Lista de destinos do local</li> <li>• Página Por detalhes de IP de destino</li> <li>• Página Por rede – Lista de destinos do local</li> <li>• Tabela 5 principais usuários</li> <li>• Tabela 5 principais origens de log</li> <li>• Tabela 5 principais categorias</li> <li>• Página Por detalhes de rede</li> <li>• Tabela 5 principais categorias</li> </ul>	Especifica o número de eventos ou fluxos que são associados ao endereço IP de origem, endereço IP de destino, nome do evento, nome de usuário, endereço MAC, origem do log, nome do host, porta, origem do log, endereço ASN, endereço IPv6, regra, ASN, Aplicativo, rede ou categoria. Clique no link para visualizar mais detalhes.
First event/flow seen on	Página Detalhes da origem	Especifica a data e hora em que o endereço IP de origem gerou o primeiro evento ou fluxo.
Sinalizador	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> </ul>	<p>Indica a ação que será tomada na ofensa. As ações são representadas pelos seguintes ícones:</p> <ul style="list-style-type: none"> <li>• Sinalizador – Indica que o crime está marcada para acompanhamento. Isso permite controlar um item específico para investigação adicional. Para obter mais informações sobre como marcar um crime para acompanhamento, consulte Marcando um item para acompanhamento.</li> <li>• Usuário - Indica que o crime foi designada a um usuário. Quando um crime for designada a um usuário, ela será exibida na página Minhas ofensas pertencente a esse usuário. Para obter mais informações sobre como designar ofensas para usuários, consulte Designando ofensas para usuários.</li> <li>• Notas – Indica que um usuário incluiu notas à ofensa. Notas pode incluir qualquer informação que deseja capturar para o crime. Por exemplo, é possível incluir uma nota que especifica informações que não são automaticamente incluídas em um crime, como um número de chamado do Suporte ao Cliente ou informações de gerenciamento de crime. Para obter mais informações sobre a inclusão de notas, consulte Incluindo notas.</li> <li>• Protegido - Indica que o crime está protegida. O recurso Proteger evita que as ofensas especificadas sejam removidas do banco de dados após o período de retenção ter decorrido. Para obter mais informações sobre ofensas protegidas, consulte Protegendo crimes.</li> </ul> <p>Passa seu mouse sobre o ícone para exibir mais informações.</p>

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Flag (continued)		<ul style="list-style-type: none"> <li>Ofensas inativas – Indica que esta é um crime inativa. Uma ofensa se torna inativa após cinco dias decorridos desde que o crime recebeu o último evento. Além disso, todas as ofensas se tornam inativas após o realizar upgrade do seu software do produto QRadar.</li> </ul> <p>Uma ofensa inativa não pode se tornar ativa novamente. Se novos eventos forem detectados para o crime, uma nova ofensa será criada e o crime inativa será retida até o período de retenção de crime ter decorrido. É possível desempenhar as seguintes ações nas ofensas inativas: proteger, sinalizar para acompanhamento, incluir notas e designar aos usuários.</p>
Sinalizador	<ul style="list-style-type: none"> <li>Página Por detalhes do IP de origem</li> <li>Página Por IP de origem – Lista de destinos do local</li> <li>Página Por detalhes de IP de destino</li> <li>Página Por IP de destino – Lista de origens</li> <li>Página Por detalhes de rede</li> <li>Página Por rede – Lista de origens</li> <li>Página Por rede – Lista de destinos do local</li> </ul>	Especifica a ação tomada no endereço IP de origem, endereço IP de destino ou rede. Por exemplo, se um sinalizador for exibido, o crime é sinalizada para acompanhamento. Passe seu mouse sobre o ícone para exibir mais informações.
Fluxos	<ul style="list-style-type: none"> <li>Página Todas as ofensas</li> <li>Página Minhas ofensas</li> <li>Página Por IP de origem - Lista de crimes</li> <li>Página Por rede – Lista de crimes</li> <li>Página Por IP de destino – Lista de crimes</li> </ul>	Especifica o número de fluxos da ofensa. <b>Nota:</b> Se a coluna Fluxos exibir N/A, o crime poderá ter uma data de início anterior à data em que foi feito upgrade para o QRadar 7.1.0 (MR1).
Grupo	<ul style="list-style-type: none"> <li>Tabela de origem de crimes, se o Tipo de crime for Fonte de log</li> <li>Tabela 5 principais origens de log</li> </ul>	Especifica a qual grupo a origem de log pertence.
Grupo(s)	Tabela de origem de crimes, se o Tipo de crime for Regra	Especifica a qual grupo de regra a regra pertence.
Categoria de Alto Nível	Tabela de origem de crime, se o Tipo de crime for o Nome do evento	Especifica a categoria de alto nível do evento.  Para obter mais informações sobre categorias de alto nível, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Nome do Host	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o nome do host que está associado ao endereço IP de origem ou de destino. Se nenhum nome do host for identificado, este campo especificará Desconhecido.
Nome do Host	Tabela de origem de crime, se o Tipo de crime for Nome do host	Especifica o nome do host que está associado ao fluxo que criou o crime.
ID	<ul style="list-style-type: none"> <li>Página Todas as ofensas</li> <li>Página Minhas ofensas</li> <li>Página Por IP de origem - Lista de crimes</li> <li>Página Por rede – Lista de crimes</li> <li>Página Por IP de destino - Lista de crimes</li> <li>Página Por IP de origem - Lista de crimes</li> <li>Página Por rede – Lista de crimes</li> </ul>	Especifica o número de identificação exclusivo que o QRadar designa à ofensa.
IP	<ul style="list-style-type: none"> <li>Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem</li> <li>Página Detalhes da origem</li> </ul>	Especifica o endereço IP de origem que está associado ao evento ou fluxo que criou o crime.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
IP/DNS Name	Página Destino	Especifica o endereço IP do destino. Se o DNS estiver ativado na guia <b>Administração</b> , será possível visualizar o nome DNS passando seu mouse sobre o endereço IP ou nome do ativo.  Para obter informações adicionais, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
IPv6	Tabela de origem de crime, se o Tipo de crime for Source IPv6 ou Destination IPv6	Especifica o endereço IPv6 que está associado ao evento ou fluxo que criou o crime.
Last Event/Flow	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Página Por IP de origem – Lista de destinos do local</li> <li>• Tabela 5 principais IPs de origem</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Por rede – Lista de origens</li> <li>• Tabela 5 principais IPs de destino</li> <li>• Página Por detalhes de IP de destino</li> <li>• Página Por IP de destino – Lista de origens</li> <li>• Página Por rede – Lista de destinos do local</li> <li>• Tabela 5 principais categorias</li> </ul>	Especifica o tempo decorrido desde que o último evento ou fluxo foi observado para o crime, categoria, endereço IP de origem ou endereço IP de destino.
Last event/flow seen on	Página Detalhes da origem	Especifica a data e a hora do último evento ou fluxo gerado que está associado ao endereço IP de origem.
Last Event/Flow Time	Tabela de origem de crimes, se o Tipo de crime for Fonte de log	Especifica a última data e hora em que a origem de log foi observada no sistema.
Last Known Group	Tabela de origem de crime, se o Tipo de crime for Nome de usuário, Endereço MAC de origem, Endereço MAC de destino ou Nome do host	Especifica a qual grupo atual o usuário, endereço MAC ou nome do host pertencem. Se nenhum grupo estiver associado, o valor desse campo será Desconhecido. <b>Nota:</b> Este campo não exibirá informações históricas.
Last Known Host	Tabela de origem de crime, se o Tipo de ofensa for Nome de usuário, Endereço MAC de origem ou Endereço MAC de destino	Especifica a qual host atual o usuário ou o endereço MAC está associado. Se nenhum host for identificado, este campo especificará Desconhecido. <b>Nota:</b> Este campo não exibirá informações históricas.
Last Known IP	Tabela de origem de crime, se o Tipo de crime for Nome de usuário, Endereço MAC de origem, Endereço MAC de destino ou Nome do host	Especifica o endereço IP atual do usuário, MAC ou nome do host. Se nenhum endereço IP for identificado, este campo especificará Desconhecido. <b>Nota:</b> Este campo não exibirá informações históricas.
Last Known MAC	Tabela de origem de crime, se o Tipo de crime for Nome de usuário ou Nome do host	Especifica o último endereço MAC conhecido do nome de usuário ou host. Se nenhum MAC for identificado, este campo especificará Desconhecido. <b>Nota:</b> Este campo não exibirá informações históricas.
Last Known Machine	Tabela de origem de crime, se o Tipo de crime for Nome de usuário, Endereço MAC de origem, Endereço MAC de destino ou Nome do host	Especifica o nome da máquina atual que está associado ao usuário, endereço MAC ou nome do host. Se nenhum nome de máquina for identificado, este campo especificará Desconhecido. <b>Nota:</b> Este campo não exibirá informações históricas.
Last Known Username	Tabela de origem de crime, se o Tipo de crime for Endereço MAC de origem, Endereço MAC de destino ou Nome do host	Especifica o usuário atual do endereço MAC ou nome do host. Se nenhum endereço MAC for identificado, este campo especificará Desconhecido. <b>Nota:</b> Este campo não exibirá informações históricas.
Last Observed	Tabela de origem de crime, se o Tipo de crime for Nome de usuário, Endereço MAC de origem, Endereço MAC de destino ou Nome do host	Especifica a data e hora em que o usuário, o endereço MAC ou o nome do host foi observado no sistema.
Horário do Último Pacote	Tabela 10 últimos fluxos	Especifica a data e hora em que o último pacote do fluxo foi enviado.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Contagem de Destino do Local	Tabela 5 principais categorias Página Por detalhes da categoria	Especifica o número de endereços IP de destino do local associados à categoria.
Destino(s) do Local	Página Detalhes da Origem	Especifica os endereços IP de destino do local associados com o endereço IP de origem. Para visualizar mais informações sobre os endereços IP de destino, clique no endereço IP ou no termo que é exibido.  Se houver vários endereços IP de destino, o termo Vários será exibido.
Localização	<ul style="list-style-type: none"> <li>• Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem</li> <li>• Tabela 5 principais IPs de origem</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Detalhes da Origem</li> <li>• Página Por IP de destino - Lista de Origens</li> <li>• Página Por rede – Lista de origens</li> </ul>	Especifica o local de rede do endereço IP de origem ou destino. Se a localização for local, será possível clicar no link para visualizar as redes.
Origem de Log	Tabela 10 últimos eventos	Especifica a origem de log que detectou o evento.
Identificador de Origem de Log	Tabela de origem de crimes, se o Tipo de crime for Fonte de log	Especifica o nome do host da origem de log.
Nome da Origem de Log	Tabela de origem de crimes, se o Tipo de crime for Fonte de log	Especifica o nome da origem de log, conforme identificado na tabela Origens de Log, que é associada ao evento que criou o crime. <b>Nota:</b> As informações que são exibidas para ofensas de origem de log são derivadas da página Origens de Log na guia Administrador. É necessário ter acesso administrativo para acessar a guia Administrador e gerenciar as origens de log. Para obter mais informações sobre o gerenciamento de origem de log, consulte o <i>Gerenciando guia de origem de log</i> .
Origens de log	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> </ul>	Especifica as origens de log que são associadas à ofensa. Se mais de uma origem de log estiver associada à ofensa, este campo especificará Vários e o número de origens de log.
Categoria de Nível Baixo	Tabela de origem de crime, se o Tipo de crime for o Nome do evento	Especifica a categoria de nível inferior do evento.
MAC	<ul style="list-style-type: none"> <li>• Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem</li> <li>• Tabela 5 principais IPs de origem</li> <li>• Tabela 5 principais IPs de destino</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Por IP de origem - Lista de destinos do local</li> <li>• Página Por detalhes de IP de destino</li> <li>• Página Por IP de destino - Lista de Origens</li> <li>• Página Por rede – Lista de origens</li> <li>• Página Por rede - Lista de destinos do local</li> </ul>	Especifica o endereço MAC do endereço IP de origem ou destino quando o crime começou. Se o endereço MAC for desconhecido, este campo especificará Desconhecido.
MAC Address	Tabela de origem de crime, se o Tipo de crime for Endereço MAC de origem ou destino	Especifica o endereço MAC associado ao evento que criou o crime. Se nenhum endereço MAC for identificado, este campo especificará Desconhecido.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Magnitude	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Tabela de crime</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino - Lista de crimes</li> <li>• Tabela 5 principais categorias</li> <li>• Tabela 10 últimos eventos</li> <li>• Página Por detalhes de rede</li> <li>• Página de rede</li> </ul>	Especifica a importância relativa da ofensa, categoria, evento ou rede. A barra de magnitude fornece uma representação visual de todas as variáveis correlacionadas. As variáveis incluem Relevância, Severidade e Credibilidade. Passe o mouse sobre a barra de magnitude para exibir os valores e a magnitude calculada.
Magnitude	<ul style="list-style-type: none"> <li>• Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem</li> <li>• Tabela 5 principais IPs de origem</li> <li>• Tabela 5 principais IPs de destino</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Detalhes da origem</li> <li>• Página Por IP de origem – Lista de destinos do local</li> <li>• Página Destino</li> <li>• Página Por detalhes de IP de destino</li> <li>• Página Por IP de destino – Lista de origens</li> <li>• Página Por rede – Lista de origens</li> <li>• Página Por rede – Lista de destinos do local</li> </ul>	Especifica a importância relativa do endereço IP de destino ou origem. A barra de magnitude fornece uma representação visual do valor de risco de CVSS do ativo que está associado ao endereço IP. Passe seu mouse sobre a barra de magnitude para exibir a magnitude calculada.
Name	<ul style="list-style-type: none"> <li>• Tabela 5 principais origens de log</li> <li>• Tabela 5 principais usuários</li> <li>• Tabela 5 principais categorias</li> <li>• Página Rede</li> </ul>	Especifica o nome da origem de log, usuário, categoria, endereço IP da rede ou nome.
Rede	Página Por detalhes de rede	Especifica o nome da rede.
Rede(s)	Tabela de crime	Especifica a rede de destino para o crime. Se o crime possuir uma rede de destino, este campo exibirá a folha de rede. Clique no link para visualizar as informações de rede. Se o crime possuir mais de uma rede de destino, o termo Vários será exibido. Clique no link para visualizar mais detalhes.
Notes	<ul style="list-style-type: none"> <li>• Tabela de origem de crimes, se o Tipo de crime for Regra</li> <li>• Tabela 5 últimas notas</li> </ul>	Especifica as notas da regra.
Contagem de Crime	Página Por detalhes da categoria	Especifica o número de crimes ativos em cada categoria. Os crimes ativos são ofensas que não foram ocultados ou encerrados.  Se a página Por detalhes de categoria incluir o filtro Excluir ofensas ocultas, a contagem de crime exibida no parâmetro Offense Count talvez não esteja correta. Se desejar visualizar a contagem total na área de janela Por categoria, clique em <b>Limpar filtro</b> ao lado do filtro Excluir ofensas ocultas na página Por detalhes de categoria.
Origem da Ofensa	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> </ul>	Especifica informações sobre a fonte da ofensa. As informações que são exibidas no campo <b>Origem da ofensa</b> dependem do tipo de crime. Por exemplo, se o tipo de crime for Porta de origem, o campo <b>Origem de crime</b> exibirá a porta de origem do evento que criou o crime.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Tipo da Ofensa	<ul style="list-style-type: none"> <li>• Página Minhas ofensas</li> <li>• Tabela de crime</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> </ul>	<p>Especifica o tipo de crime. O Tipo de crime é determinado pela regra que criou o crime. Por exemplo, se o tipo de crime for um evento de origem de log, a regra que gerou o crime correlacionará os eventos que são baseados no dispositivo que detectou o evento.</p> <p>Os tipos de crime incluem:</p> <ul style="list-style-type: none"> <li>• IP de Origem</li> <li>• IP de Destino</li> <li>• Nome do Evento</li> <li>• Nome do Usuário</li> <li>• Endereço MAC de origem</li> <li>• Endereço MAC de destino</li> <li>• Origem de Log</li> <li>• Nome do Host</li> <li>• Porta de origem</li> <li>• Porta de Destino</li> <li>• IPv6 de Origem</li> <li>• IPv6 de Destino</li> <li>• ASN de Origem</li> <li>• ASN de Destino</li> <li>• Regra</li> <li>• ID do aplicativo</li> </ul> <p>O tipo de crime determina que tipo de informação é exibido na área de janela Resumo de origem de crime.</p>
Offense(s)	<ul style="list-style-type: none"> <li>• Página Detalhes da origem</li> <li>• Página Destino</li> </ul>	<p>Especifica os nomes das ofensas que são associadas ao endereço IP de origem ou destino. Para visualizar mais informações sobre o crime, clique no nome ou no termo que é exibido.</p> <p>Se houver várias ofensas, o termo Vários será exibido.</p>
Offense(s) Launched	Página Rede	<p>Especifica as ofensas que são ativadas a partir da rede.</p> <p>Se várias ofensas forem responsáveis, esse campo especificará Vários e o número de crimes.</p>
Offense(s) Targeted	Página Rede	<p>Especifica as ofensas que são direcionadas para a rede.</p> <p>Se várias ofensas forem responsáveis, este campo especificará Vários e o número de crimes</p>
Ofensas	<ul style="list-style-type: none"> <li>• A tabela de origem de crimes, se o Tipo de crime for IP de origem, IP de destino, Nome do evento, Nome, Endereço MAC de origem ou destino, Fonte de log, Nome de host, Porta de origem ou destino, Source IPv6 ou Destination IPv6, ASN de origem ou destino, Regra, ID do aplicativo</li> <li>• Tabela 5 principais IPs de origem</li> <li>• Tabela 5 principais IPs de destino</li> <li>• Tabela 5 principais origens de log</li> <li>• Tabela 5 principais usuários</li> <li>• Página Por detalhes de IP de origem</li> <li>• Página Por IP de origem – Lista de destinos do local</li> <li>• Página Por detalhes de IP de destino</li> <li>• Página Por IP de destino – Lista de origens</li> <li>• Página Por rede – Lista de origens</li> <li>• Página Por rede – Lista de destinos do local</li> </ul>	<p>Especifica o número de crimes que são associadas ao endereço IP de origem, endereço IP de destino, nome do evento, nome de usuário, endereço MAC, origem do log, nome do host, porta, endereço IPv6, ASN, regra ou aplicativo. Clique no link para visualizar mais detalhes.</p>



Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Offenses Launched	Página Por detalhes de rede	Especifica o número de crimes que são originadas da rede.
Offenses Targeted	Página Por detalhes de rede	Especifica o número de crimes que são direcionadas para a rede.
Port	Tabela de origem de crime, se o Tipo de crime for Porta de origem ou destino	Especifica a porta que está associada ao evento ou fluxo que criou o crime.
Relevância	Tabela de crime	Especifica a importância relativa da ofensa.
Resposta	Tabela de origem de crimes, se o Tipo de crime for Regra	Especifica o tipo de resposta da regra.
Descrição da Regra	Tabela de origem de crimes, se o Tipo de crime for Regra	Especifica o resumo dos parâmetros de regra.
Nome da Regra	Tabela de origem de crimes, se o Tipo de crime for Regra	Especifica o nome da regra que está associada ao evento ou fluxo que criou o crime. <b>Nota:</b> As informações que são exibidas para ofensas de regra são derivadas da guia <b>Regras</b> .
Tipo de Regra	Tabela de origem de crimes, se o Tipo de crime for Regra	Especifica o tipo de regra da ofensa.
Gravidade	<ul style="list-style-type: none"> <li>Tabela de origem de crime, se o Tipo de crime for o Nome do evento</li> <li>Tabela de crime</li> </ul>	Especifica a severidade do evento ou ofensa. A severidade específica a quantidade de ameaças que um crime representa em relação a quanto o endereço IP de destino está preparado para o ataque. Este valor é diretamente mapeado para a categoria de evento que se correlaciona à ofensa. Por exemplo, um ataque de Negação de Serviço (DoS) tem uma severidade de 10, que especifica uma ocorrência grave.
Contagem de Origem	Página Por detalhes da categoria	Especifica o número de endereços IP de origem associados a ofensas na categoria. Se um endereço IP de origem estiver associado a ofensas em cinco categorias diferentes de nível inferior, o endereço IP de origem será contado apenas uma vez.
IP de Origem	<ul style="list-style-type: none"> <li>Página Por detalhes de IP de origem</li> <li>Página Por IP de destino – Lista de origens</li> <li>Página Por rede – Lista de origens</li> <li>Tabela 5 principais IPs de origem</li> <li>Tabela 10 últimos fluxos</li> </ul>	Especifica o endereço IP ou o nome do host do dispositivo que tentou violar a segurança de um componente em sua rede. Se as consultas de DNS estiverem ativadas na guia Administrador, será possível visualizar o nome DNS apontando seu mouse no endereço IP.  Para obter informações adicionais, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Source IP(s)	Tabela de crime	Especifica o endereço IP ou o nome do host do dispositivo que tentou violar a segurança de um componente em sua rede. Clique no link para visualizar mais detalhes.
Source IPs	<ul style="list-style-type: none"> <li>Página Todas as ofensas</li> <li>Página Minhas ofensas</li> <li>Página Por IP de origem - Lista de crimes</li> <li>Página Por rede – Lista de crimes</li> <li>Página Por IP de destino – Lista de crimes</li> </ul>	Especifica os endereços IP ou o nome do host do dispositivo que tentou violar a segurança de um componente em sua rede. Se mais de um endereço IP de origem estiver associado à ofensa, este campo especificará Vários e o número de endereços IP de origem. Se consultas de DNS estiverem ativadas na guia Administração, será possível visualizar o nome DNS apontando seu mouse no endereço IP ou nome do ativo.  Para obter informações adicionais, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Source IPs	Página Por detalhes de rede	Especifica o número de endereços IP de origem associados à rede.
Porta de origem	Tabela 10 últimos fluxos	Especifica a porta de origem do fluxo.
Source(s)	<ul style="list-style-type: none"> <li>Tabela 5 principais IPs de destino</li> <li>Página Por IP de origem – Lista de destinos do local</li> <li>Página Por detalhes de IP de destino</li> </ul>	Especifica o número de endereços IP de origem para o endereço IP de destino.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
Source(s)	<ul style="list-style-type: none"> <li>• Página Destino</li> <li>• Página Rede</li> </ul>	<p>Especifica os endereços IP de origem da ofensa que está associada ao endereço IP de destino ou rede. Para visualizar mais informações sobre os endereços IP de origem, clique no endereço IP, nome do ativo ou termo que é exibido.</p> <p>Se um endereço IP de fonte isolada for especificado, um endereço IP e o nome de ativo serão exibidos (se disponível). É possível clicar no endereço IP ou no nome de ativo para visualizar os detalhes do endereço IP de origem. Se houver vários endereços IP de origem, este campo especificará Vários e o número de endereços IP de origem.</p>
Source(s)	Página Por rede – Lista de destinos do local	Especifica o número de endereços IP de origem associados a endereços IP de destino.
Start	Tabela de crime	Especifica a data e hora em que o primeiro evento ou fluxo ocorreu para o crime.
Start Date	<ul style="list-style-type: none"> <li>• Página Todas as ofensas</li> <li>• Página Minhas ofensas</li> <li>• Página Por IP de origem - Lista de crimes</li> <li>• Página Por rede – Lista de crimes</li> <li>• Página Por IP de destino – Lista de crimes</li> </ul>	Especifica a data e hora do primeiro evento ou fluxo que está associado à ofensa.
Status	Tabela de origem de crimes, se o Tipo de crime for Fonte de log	Especifica o status da origem de log.
Status	Tabela de crime	<p>Exibe ícones para indicar o status de um crime. Ícones de status incluem:</p> <p><b>Ofensa inativa.</b> Uma ofensa se torna inativa após cinco dias decorridos desde que o crime recebeu o último evento. Todas as ofensas se tornarão inativas após o upgrade do seu software do produto QRadar.</p> <p>Uma ofensa inativa não pode se tornar ativa novamente. Se novos eventos forem detectados para o crime, uma nova ofensa será criada e o crime inativa será retida até o período de retenção de crime ter decorrido. É possível proteger, sinalizar para acompanhamento, incluir notas e designar os usuários a um crime inativa.</p> <p>Um sinalizador <b>Ofensa Oculta</b> na página Todas as Ofensas indica que o crime está oculta na visualização. Se você procurar ofensas ocultas, elas serão visíveis somente na página Todas as Ofensas em que estão sinalizadas como ofensa oculta. Para obter mais informações, consulte Ocultar ofensas.</p> <p><b>Usuário</b> indica que o crime é designada a um usuário. Quando um crime for designada a um usuário, o crime será exibida na página Minhas ofensas que pertence a esse usuário. .</p> <p><b>Protegido</b> evita que ofensas especificadas sejam removidas do banco de dados após o período de retenção acabar.</p> <p><b>Ofensa encerrada</b> indica que o crime está encerrada.</p>
Time	<ul style="list-style-type: none"> <li>• Tabela 10 últimos eventos</li> <li>• Tabela 10 últimos eventos (eventos de anomalia)</li> </ul>	Especifica a data e a hora em que o primeiro evento foi detectado no evento normalizado. Esta data e hora são especificadas pelo dispositivo que detectou o evento.
Horário	Tabela 5 principais anotações	Especifica a data e a hora em que a anotação foi criada.
Total de Bytes	Tabela 10 últimos fluxos	Especifica o número total de bytes do fluxo.
Total de Eventos/Fluxos	<ul style="list-style-type: none"> <li>• Tabela 5 principais origens de log</li> <li>• Tabela 5 principais usuários</li> </ul>	Especifica o número total de eventos da origem de log ou usuário.

Tabela 12. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Localização	Descrição
User	<ul style="list-style-type: none"> <li>Tabela de origem de crime, se o Tipo de crime for IP de origem ou destino ou Nome de usuário</li> <li>Tabela 5 principais IPs de origem</li> <li>Tabela 5 principais IPs de destino</li> <li>Página Por detalhes de IP de origem</li> <li>Página Por IP de origem – Lista de destinos do local</li> <li>Página Por detalhes de IP de destino</li> <li>Página Por IP de destino – Lista de origens</li> <li>Página Por rede – Lista de origens</li> <li>Página Por rede – Lista de destinos do local</li> </ul>	Especifica o usuário que está associado a um endereço IP de origem ou destino. Se nenhum usuário for identificado, este campo especificará Desconhecido.
Nome de Usuário	Tabela de origem de crime, se o Tipo de Ofensa for Nome de usuário	Especifica o nome de usuário associado ao evento ou fluxo que criou o crime. <b>Nota:</b> Se mover seu ponteiro do mouse sobre o parâmetro Username, a dica de ferramenta exibida fornece o nome de usuário associado às informações de nome de usuário mais recentes na guia Ativos em vez do nome de usuário associado ao evento ou fluxo que criou o crime.
Nome de Usuário	Tabela 5 últimas notas	Especifica o usuário que criou a nota.
Users	<ul style="list-style-type: none"> <li>Página Todos os crimes</li> <li>Página Minhas ofensas</li> <li>Página Por IP de origem - Lista de crimes</li> <li>Página Por rede – Lista de crimes</li> <li>Página Por IP de destino - Lista de crimes</li> </ul>	Especifica os nomes de usuário que são associados à ofensa. Se mais de um nome de usuário for associado à ofensa, este campo especificará Vários e o número de nomes de usuários. Se nenhum usuário for identificado, este campo especificará Desconhecido.
Visualizar Ofensas	<ul style="list-style-type: none"> <li>Página Por detalhes de IP de origem</li> <li>Página Por detalhes de IP de destino</li> </ul>	Selecione uma opção a partir desta caixa de listagem para filtrar as ofensas que deseja visualizar nesta página. É possível visualizar todas as ofensas ou filtrar por ofensas que são baseadas em um intervalo de tempo. Na caixa de listagem, selecione o intervalo de tempo com o qual deseja filtrar.
Vulnerabilidades	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o número de vulnerabilidades identificadas que são associadas ao endereço IP de origem ou destino. Este valor também inclui o número de vulnerabilidades ativas e passivas.
Vulnerabilidades	Página Por IP de destino - Lista de Origens	Especifica se um endereço IP de origem possui vulnerabilidades.
Vulnerabilidade	<ul style="list-style-type: none"> <li>Tabela 5 principais IPs de origem</li> <li>Página Por detalhes de IP de origem</li> <li>Página Por rede – Lista de origens</li> <li>Tabela 5 principais IPs de destino</li> <li>Página Por IP de origem - Lista de destinos do local</li> <li>Página Por detalhes de IP de destino</li> <li>Página Por rede - Lista de destinos do local</li> </ul>	Especifica se o endereço IP de origem ou de destino possui vulnerabilidades.
Peso	<ul style="list-style-type: none"> <li>Tabela 5 principais IPs de origem</li> <li>Tabela 5 principais IPs de destino</li> <li>Página Por IP de origem - Lista de destinos do local</li> <li>Página Por detalhes de IP de origem</li> <li>Página Por detalhes de IP de destino</li> <li>Página Por IP de destino - Lista de Origens</li> <li>Página Por rede – Lista de origens</li> <li>Página Por rede - Lista de destinos do local</li> <li>Tabela 5 principais anotações</li> </ul>	Especifica a ponderação do endereço IP de origem, endereço IP de destino, ou anotação. A ponderação de um endereço IP é designada na guia Ativos.



---

## Capítulo 5. Investigação de atividade de log

É possível monitorar e investigar a atividade de log (eventos) em tempo real ou executar procuras avançadas.

Usando a guia **Atividade de log**, é possível monitorar e investigar a atividade de log (eventos) em tempo real ou executar procuras avançadas.

---

### Visão geral da guia Atividade de log

Um evento é um registro a partir de uma origem de log, como um dispositivo de firewall ou roteador, que descreve uma ação em uma rede ou host.

A guia **Atividade de log** especifica quais eventos estão associados a ofensas.

É necessário ter permissão para visualizar a guia **Atividade de log**.

### Barra de ferramentas da guia Atividade de log

É possível acessar várias opções a partir da barra de ferramentas Atividade de log

Usando a barra de ferramentas, é possível acessar as seguintes opções:

*Tabela 13. Opções da barra de ferramentas Atividade de log*

Opção	Descrição
Procura	Clique em <b>Procurar</b> para executar procuras avançadas em eventos. As opções incluem: <ul style="list-style-type: none"><li>• <b>Nova procura</b> – Selecione esta opção para criar uma nova procura de evento.</li><li>• <b>Editar procura</b> – Selecione esta opção para selecionar e editar uma procura de evento.</li><li>• <b>Gerenciar resultados da procura</b> – Selecione esta opção para visualizar e gerenciar resultados da procura.</li></ul>
Procuras Rápidas	Nesta caixa de listagem, é possível executar procuras salvas anteriormente. As opções são exibidas na caixa de listagem <b>Procuras rápidas</b> apenas quando forem salvas os critérios de procura que especificam a opção <b>Incluir em minhas procuras salvas</b> .
Incluir filtro	Clique em <b>Incluir filtro</b> para incluir um filtro aos resultados da procura atual.
Salvar Critérios	Clique em <b>Salvar Critérios</b> para salvar os critérios de procura atuais.
Salvar resultados	Clique em <b>Salvar resultados</b> para salvar os resultados da procura atual. Essa opção será exibida somente após a conclusão de uma procura. Esta opção está desativada no modo de fluxo.
Cancelar	Clique em <b>Cancelar</b> para cancelar uma procura em andamento. Esta opção está desativada no modo de fluxo.
Positivo Falso	Clique em <b>Positivo falso</b> para abrir a janela Ajuste de positivo falso, que permitirá ajustar eventos que são conhecidos como positivos falsos da criação de crimes.  Esta opção está desativada no modo de fluxo. Para obter mais informações sobre o ajuste de positivos falsos, consulte Ajuste de positivos falsos.

Tabela 13. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Regras	<p>A opção Regras estará visível apenas se tiver permissão para visualizar as regras.</p> <p>Clique em <b>Regras</b> para configurar as regras de evento customizado. As opções incluem:</p> <ul style="list-style-type: none"> <li>• <b>Regras</b> – Selecione esta opção para visualizar ou criar uma regra. Se tiver somente a permissão para visualizar as regras, a página de resumo do assistente de regras será exibida. Se tiver a permissão para manter as regras customizadas, o assistente de regras será exibido e será possível editar a regra. Para ativar as opções de regra de detecção de anomalias (Incluir limite de regra, Incluir regra comportamental e Incluir regra de anomalia), é necessário salvar critérios de procura agregados porque os critérios da procura salvos especificam os parâmetros requeridos. <b>Nota:</b> As opções de regra de detecção de anomalias serão visíveis apenas se tiver a permissão <b>Atividade de log &gt; Manter regras customizadas</b>.</li> <li>• <b>Incluir limite de regra</b> – Selecione esta opção para criar uma regra de limite. Uma regra de limite testa o tráfego do evento para a atividade que excede um limite configurado. Os limites podem ser baseados em quaisquer dados que são coletados QRadar. Por exemplo, se for criada uma regra de limite indicando que não mais de 220 clientes podem efetuar login no servidor entre 8h e 17h, as regras gerarão um alerta quando o cliente 221º tentar efetuar login.</li> </ul> <p>Ao selecionar a opção <b>Incluir regra de limite</b>, o assistente de regras é exibido, pré-preenchido com as opções apropriadas para criar uma regra de limite.</p>
Regras (continuação)	<ul style="list-style-type: none"> <li>• <b>Incluir regra comportamental</b> – Selecione esta opção para criar uma regra comportamental. Uma regra comportamental testa o tráfego de eventos da atividade anormal, como a existência de tráfego novo ou desconhecido, que é o tráfego que para subitamente ou uma alteração de porcentagem na quantidade de tempo que um objeto está ativo. Por exemplo, é possível criar uma regra comportamental para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego durante a última hora. Se houver mais que uma alteração de 40%, a regra gerará uma resposta.</li> </ul> <p>Ao selecionar a opção <b>Incluir regra comportamental</b>, o assistente de regras será exibido e pré-preenchido com as opções apropriadas para criar uma regra comportamental.</p> <ul style="list-style-type: none"> <li>• <b>Incluir regra de anomalia</b> – Selecione esta opção para criar uma regra de anomalia. Uma regra de anomalia testa o tráfego de evento da atividade anormal, como a existência de tráfego novo ou desconhecido, que é o tráfego que para subitamente ou uma alteração de porcentagem na quantidade de tempo que um objeto está ativo. Por exemplo, se uma área de sua rede que nunca se comunica com a Ásia iniciar uma comunicação com os hosts nesse país, uma regra de anomalia gerará um alerta.</li> </ul> <p>Ao selecionar a opção <b>Incluir regra de anomalia</b>, o assistente de regras será exibido e pré-preenchido com as opções apropriadas para criar uma regra de anomalia.</p>

Tabela 13. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Ações	<p>Clique em <b>Ações</b> para executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>• <b>Mostrar todos</b> – Selecione esta opção para remover todos os filtros nos critérios de procura e exibir todos os eventos não filtrados.</li> <li>• <b>Imprimir</b> – Selecione esta opção para imprimir os eventos que são exibidos na página.</li> <li>• <b>Exportar para XML &gt; Colunas visíveis</b> – Selecione esta opção para exportar somente as colunas que estão visíveis na guia Atividade de log. Essa é a opção recomendada. Consulte Exportando eventos.</li> <li>• <b>Exportar para XML &gt; Exportação integral (todas as colunas)</b> – Selecione esta opção para exportar todos os parâmetros de evento. Uma exportação integral pode demorar um longo período de tempo para ser concluída. Consulte Exportando eventos.</li> <li>• <b>Exportar para CSV &gt; Colunas visíveis</b> – Selecione esta opção para exportar somente as colunas que estão visíveis na guia Atividade de log. Essa é a opção recomendada. Consulte Exportando eventos.</li> <li>• <b>Exportar para CSV &gt; Exportação integral (todas as colunas)</b> – Selecione esta opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída. Consulte Exportando eventos.</li> <li>• <b>Excluir</b> – Selecione esta opção para excluir um resultado da procura. Consulte Gerenciando resultados da procura de evento e de fluxo.</li> <li>• <b>Notificar</b> – Selecione esta opção para especificar que deseja que uma notificação seja enviada por email para você na conclusão das procuras selecionadas. Esta opção está ativada apenas para procuras em andamento.</li> </ul> <p><b>Nota:</b> As opções <b>Imprimir</b>, <b>Exportar para XML</b> e <b>Exportar para CSV</b> estão desativadas no modo de fluxo e ao visualizar resultados parciais de procura.</p>
Filtro rápido	<p>Digite seus critérios de procura no campo <b>Filtro rápido</b> e clique no ícone <b>Filtro rápido</b> ou pressione Enter no teclado. Todos os eventos que correspondem aos seus critérios de procura são exibidos na lista de eventos. Uma procura de texto é executada na carga útil do evento para determinar quais correspondem aos critérios especificados.</p> <p><b>Nota:</b> Ao clicar no campo <b>Filtro rápido</b>, uma dica de ferramenta será exibida, fornecendo informações sobre a sintaxe apropriada para usar no critério de procura. Para obter mais informações de sintaxe, consulte Sintaxe de filtro rápido.</p>

## Sintaxe de Filtro Rápido

O recurso Filtro Rápido permitirá que pesquise as cargas úteis de eventos usando uma sequência de procura de texto.

A funcionalidade Filtro Rápido está disponível nos seguintes locais na interface com o usuário:

- Barra de ferramentas **Atividade do log** – Na barra de ferramentas, um campo **Filtro rápido** permitirá que digite uma sequência de procura de texto e clique no ícone **Filtro rápido** para aplicar seu filtro rápido à lista atualmente exibida de eventos.
- Caixa de diálogo **Incluir filtro**. Na caixa de diálogo **Incluir filtro**, que é acessada clicando no ícone **Incluir filtro** na guia **Atividade de log**, é possível selecionar **Quick Filter** como seu parâmetro de filtragem e digitar uma sequência de procura de texto. Isso permitirá aplicar seu filtro rápido na lista atualmente exibida de eventos ou fluxos. Para obter mais informações sobre a caixa de diálogo **Incluir filtro**, consulte Sintaxe de Filtro rápido.
- Páginas de procura Evento e Fluxo – Nas páginas de procura de evento e de fluxo, é possível incluir um **Filtro rápido** para sua lista de filtros a serem incluídos em seus critérios de procura.

Ao visualizar eventos em tempo real (fluxo) ou modo de último intervalo, será possível apenas digitar palavras ou frases simples no campo **Filtro rápido**. Ao visualizar eventos usando um intervalo de tempo, use as seguintes diretrizes de sintaxe para digitar seus critérios de procura de texto:

- Termos de procura podem incluir qualquer texto simples que você espere localizar na carga útil. Por exemplo, "Firewall"
- Inclua vários termos entre aspas duplas para indicar que deseja procurar a frase exata. Por exemplo, "Negação de Firewall"
- Termos de procura podem incluir curingas de caracteres únicos e múltiplos. O termo de procura não pode começar com um curinga. Por exemplo, "F?rewall" ou "F??ew\*"
- Os termos de procura são correspondidos em sequência a partir do primeiro caractere na palavra ou frase da carga útil. Por exemplo, o termo de procura "user" não corresponde às seguintes frases: "ruser", "myuser" ou "anyuser". O termo de procura "user\*" corresponde com qualquer palavra que inicie com "user", por exemplo, "user\_1", "user\_2".
- Agrupa termos usando expressões lógicas, como AND, OR e NOT. A sintaxe faz distinção entre maiúsculas e minúsculas e os operadores devem estar em letras maiúsculas para serem reconhecidos como expressões lógicas e não como termos de procura. Por exemplo: (%PIX\* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.\*) Ao criar critérios de procura que incluem a expressão lógica NOT, é necessário incluir pelo menos um outro tipo de expressão lógica, caso contrário, o filtro não retornará nenhum resultado. Por exemplo: (%PIX\* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.\*)
- Os seguintes caracteres devem ser precedidos por uma barra invertida para indicar que o caractere é parte de seu termo de procura: + - && | ! () {} [] ^ " ~ \* ? : \. Por exemplo: "%PIX\ -5\ -304001"

## Opções do menu ativado pelo botão direito

Na guia **Atividade de log**, é possível clicar com o botão direito em um evento para acessar mais informações de filtro de eventos.

As opções do menu ativado pelo botão direito são:

*Tabela 14. Opções do menu ativado pelo botão direito*

Opção	Descrição
Filtrar em	Selecione esta opção para filtrar o evento selecionado, dependendo do parâmetro selecionado no evento.
Positivo Falso	Selecione esta opção para abrir a janela Positivo falso, que permitirá ajustar eventos que são conhecidos como positivos falsos da criação de crimes. Esta opção está desativada no modo de fluxo. Consulte Ajustando positivos falsos.
Mais opções:	Selecione esta opção para investigar um endereço IP ou um nome de usuário. Para obter mais informações sobre como investigar um endereço IP, consulte Investigando endereços IP. Para obter mais informações sobre como investigar um nome de usuário, consulte Investigando nomes de usuário. <b>Nota:</b> Esta opção não é exibida no modo de fluxo.

## Barra de status

Ao transmitir eventos, a barra de status exibirá o número médio de resultados que são recebidos por segundo.

Este é o número de resultados que o Console recebeu com sucesso a partir dos processadores de eventos. Se o número for maior que 40 resultados por segundo,



somente 40 resultados serão exibidos. O restante é acumulado no buffer de resultado. Para visualizar mais informações de status, mova o ponteiro do mouse sobre a barra de status.

Quando os eventos não estiverem sendo transmitidos, a barra de status exibirá o número de resultados da procura que são atualmente exibidos na guia e a quantidade de tempo que é necessária para processar os resultados da procura.

---

## Monitorando a atividade de log

Por padrão, a guia **Atividade de log** exibe eventos no modo de fluxo, que permite visualizar os eventos em tempo real.

Para obter mais informações sobre o modo de fluxo, consulte **Visualizando eventos de fluxo**. É possível especificar um intervalo de tempo diferente para filtrar eventos usando a caixa de listagem **Visualização**.

Se os critérios de procura salvos forem configurados anteriormente como o padrão, os resultados dessa procura serão exibidos automaticamente ao acessar a guia **Atividade de log**. Para obter mais informações sobre como salvar os critérios de procura, consulte **Salvando os critérios de procura de evento e de fluxo**.

### Visualizando eventos de fluxo

O modo de fluxo permitirá que você visualize os dados do evento inseridos no seu sistema. Este modo fornece a você uma visualização em tempo real do seu evento de atividade atual, exibindo os últimos 50 eventos.

#### Sobre Esta Tarefa

Se você aplicar quaisquer filtros na guia **Atividade de Log** ou em seu critério de procura antes de ativar o modo de fluxo, os filtros serão mantidos em modo de fluxo. No entanto, o modo de fluxo não suporta procuras que incluem eventos agrupados. Se você ativar o modo de fluxo em eventos agrupados ou critério de procura agrupado, a guia **Atividade de Log** exibirá os eventos normalizados. Consulte **Visualizando eventos normalizados**.

Quando você deseja selecionar um evento para visualizar detalhes ou executar uma ação, você deve pausar o fluxo antes de clicar duas vezes em um evento. Quando o fluxo é pausado, os últimos 1.000 eventos são exibidos.

#### Procedimento

1. Clique na guia **Atividade de log**.
2. Na caixa de listagem **Visualização**, selecione **Tempo real (fluxo)**. Para obter informações sobre as opções da barra de ferramentas, consulte a Tabela 4-1. Para obter mais informações sobre os parâmetros exibidos no modo de fluxo, consulte a Tabela 4-7.
3. Opcional. Pausar ou executar o fluxo de eventos. Escolha uma das opções a seguir:
  - Para selecionar um registro de eventos, clique no ícone **Pausar** para pausar o fluxo.
  - Para reiniciar o modo de fluxo, clique no ícone **Executar**.

## Visualizando eventos normalizados

Os eventos são coletados em formato bruto, e então normalizados para exibição na guia **Atividade de Log**.

### Sobre Esta Tarefa

A normalização envolve a análise de dados de evento brutos e a preparação dos dados para exibir informações legíveis sobre a guia. Quando os eventos são normalizados, o sistema normaliza os nomes também. Portanto, o nome exibido na guia **Atividade de Log** pode não corresponder ao nome exibido no evento.

**Nota:** Se você selecionou um prazo para exibição, um gráfico de série temporal será exibido. Para obter mais informações sobre como usar gráficos de séries temporais, consulte Visão geral de gráficos de séries temporais.

A guia **Atividade de Log** exibirá os seguintes parâmetros quando você visualizar os eventos normalizados:

*Tabela 15. Guia de atividade de log – Parâmetro padrão (normalizado)*

Parâmetro	Descrição
Current Filters	A parte superior da tabela exibe os detalhes dos filtros aplicados aos resultados da procura. Para limpar esses valores de filtro, clique em <b>Limpar filtro</b> . <b>Nota:</b> Esse parâmetro só será exibido após você aplicar um filtro.
Visualização	Nessa caixa de listagem, você pode selecionar o intervalo de tempo que deseja filtrar.
Estatística Atual	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: <b>Nota:</b> Clique na seta ao lado de <b>Estatísticas Atuais</b> para exibir ou ocultar as estatísticas <ul style="list-style-type: none"><li>• <b>Resultados totais</b> – Especifica o número total de resultados que correspondeu ao seu critério de procura.</li><li>• <b>Arquivos de dados procurados</b> – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado.</li><li>• <b>Arquivos de dados compactados procurados</b> – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado.</li><li>• <b>Contagem de arquivo de índice</b> – Especifica o número total de arquivos de índice procurados durante o período de tempo especificado.</li><li>• <b>Duração</b> – Especifica a duração da procura. <b>Nota:</b> Estatísticas atuais são úteis para resolução de problemas. Quando contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.</li></ul>
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em <b>Ocultar gráficos</b> se desejar remover os gráficos da sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Capacidade de gerenciamento do gráfico. <b>Nota:</b> Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para gráficos exibidos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.
Ícone Ofensas	Clique neste ícone para visualizar detalhes da ofensa associada a este evento. Para obter mais informações, consulte Capacidade de gerenciamento do gráfico. <b>Nota:</b> Dependendo do seu produto, esse ícone pode não estar disponível. Você deve ter o IBM Security QRadar SIEM.
Horário de Início	Especifica a hora do primeiro evento, conforme reportado para QRadar pela origem de log.
Nome do Evento	Especifica o nome normalizado do evento.
Origem de Log	Especifica a origem de log que originou o evento. Se houver várias origens de log associadas a esse evento, este campo especificará o termo Várias e o número de origens de log.

Tabela 15. Guia de atividade de log – Parâmetro padrão (normalizado) (continuação)

Parâmetro	Descrição
Contagem de Evento	Especifica o número total de eventos que são empacotados nesse evento normalizado. Os eventos serão empacotados quando muitos do mesmo tipo de evento para o mesmo endereço IP de origem e destino são detectados dentro de um curto período.
Horário	Especifica a data e hora em que o QRadar recebeu o evento.
Categoria de Nível Baixo	Especifica a categoria de baixo nível associada a este evento.  Para obter mais informações sobre categorias de eventos, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
IP de Origem	Especifica o endereço IP de origem do evento.
Porta de origem	Especifica a porta de origem do evento.
IP de Destino	Especifica o endereço IP de destino do evento.
Porta de Destino	Especifica a porta de destino do evento.
Nome de Usuário	Especifica o nome de usuário associado a este evento. Os nomes de usuário estão frequentemente disponíveis em eventos de autenticação relacionada. Para todos os outros tipos de eventos onde o nome de usuário não estiver disponível, este campo especificará N/D.
Magnitude	Especifica a magnitude deste evento. Variáveis incluem credibilidade, relevância e gravidade. Passe o mouse sobre a barra de magnitude para exibir os valores e a magnitude calculada. Para obter mais informações sobre credibilidade, relevância e gravidade, consulte o Glossário.

## Procedimento

1. Clique na guia **Atividade de log**.
2. Na caixa da lista de **Exibição**, selecione **Padrão (normalizado)**.
3. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
4. Clique no ícone **Pausar** para pausar o fluxo.
5. Clique duas vezes no evento que deseja exibir com mais detalhes. Para obter mais informações, consulte **Detalhe do evento**.

## Visualizando eventos brutos

Você pode visualizar dados dos eventos brutos, que são os dados do evento não analisado da origem de log.

### Sobre Esta Tarefa

Quando você visualiza dados dos eventos brutos, a guia **Atividade de Log** fornece os seguintes parâmetros para cada evento.

Tabela 16. Parâmetros de Evento Bruto

Parâmetro	Descrição
Current Filters	A parte superior da tabela exibe os detalhes dos filtros aplicados aos resultados da procura. Para limpar esses valores de filtro, clique em <b>Limpar filtro</b> . <b>Nota:</b> Esse parâmetro só será exibido após você aplicar um filtro.
Visualização	Nessa caixa de listagem, você pode selecionar o intervalo de tempo que deseja filtrar.

Tabela 16. Parâmetros de Evento Bruto (continuação)

Parâmetro	Descrição
Current Statistics	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: <b>Nota:</b> Clique na seta ao lado de <b>Estatísticas Atuais</b> para exibir ou ocultar as estatísticas <ul style="list-style-type: none"> <li>• <b>Resultados totais</b> – Especifica o número total de resultados que correspondeu ao seu critério de procura.</li> <li>• <b>Arquivos de dados procurados</b> – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado.</li> <li>• <b>Arquivos de dados compactados procurados</b> – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado.</li> <li>• <b>Contagem de arquivo de índice</b> – Especifica o número total de arquivos de índice procurados durante o período de tempo especificado.</li> <li>• <b>Duração</b> – Especifica a duração da procura. <b>Nota:</b> As estatísticas Atuais são úteis para resolução de problemas. Quando contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.</li> </ul>
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em <b>Ocultar gráficos</b> se desejar remover os gráficos da sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. <b>Nota:</b> Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para gráficos exibidos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.
Ícone Ofensas	Clique neste ícone para visualizar detalhes da ofensa associada a este evento.
Horário de Início	Especifica a hora do primeiro evento, conforme reportado para QRadar pela origem de log.
Origem de Log	Especifica a origem de log que originou o evento. Se houver várias origens de log associadas a esse evento, este campo especificará o termo Várias e o número de origens de log.
Carga Útil	Especifica as informações de carga útil do evento original no formato UTF-8.

## Procedimento

1. Clique na guia **Atividade de log**.
2. Na caixa de listagem **Exibir**, selecione **Eventos brutos**.
3. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
4. Clique duas vezes no evento que deseja exibir com mais detalhes. Consulte **Detalhes do evento**.

## Visualizando eventos agrupados

Usando a guia **Atividade de Log**, você pode visualizar eventos que são agrupados por várias opções. Na caixa de listagem **Exibir**, você pode selecionar o parâmetro que deseja para os eventos do grupo.

### Sobre Esta Tarefa

A caixa de lista de Exibição não é exibida no modo de fluxo porque o modo de fluxo não suporta eventos agrupados. Se você inseriu o modo de fluxo usando critério de procura não agrupado, esta opção será exibida.

A caixa de lista de Exibição fornece as seguintes opções:

Tabela 17. Opções de eventos agrupados

Opção de grupo	Descrição
Categoria de Nível Baixo	Exibe uma lista resumida de eventos agrupados pela categoria do evento de baixo nível.  Para obter mais informações sobre categorias, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Nome do Evento	Exibe uma lista resumida de eventos agrupados pelo nome normalizado do evento.
IP de Destino	Exibe uma lista resumida de eventos agrupados pelo endereço IP de destino do evento.
Porta de Destino	Exibe uma lista resumida de eventos agrupados pelo endereço de porta de destino do evento.
IP de Origem	Exibe uma lista resumida de eventos agrupados pelo endereço IP de origem do evento.
Regra customizada	Exibe uma lista resumida de eventos agrupados pela regra customizada associada.
Nome de Usuário	Exibe uma lista resumida de eventos agrupados pelo nome de usuário associado com os eventos.
Origem de Log	Exibe uma lista resumida de eventos agrupados pela origem de log que enviou o evento para QRadar.
Categoria de Alto Nível	Exibe uma lista resumida de eventos agrupados pela categoria de alto nível do evento.
Rede	Exibe uma lista resumida de eventos agrupados pela rede associada com o evento.
Porta de origem	Exibe uma lista resumida de eventos agrupados pelo endereço de porta de origem do evento.

Depois de selecionar uma opção na caixa de listagem **Exibir**, o layout da coluna dos dados depende da opção do grupo escolhido. Cada linha da tabela de eventos representa um grupo de eventos. A guia **Atividade de Log** fornece as seguintes informações para cada grupo de eventos

Tabela 18. Parâmetros de eventos agrupados

Parâmetro	Descrição
Agrupar por	Especifica o parâmetro no qual a procura está agrupada.
Current Filters	A parte superior da tabela exibe os detalhes do filtro aplicado aos resultados da procura. Para limpar esses valores de filtro, clique em <b>Limpar filtro</b> .
Visualização	Na caixa de listagem, selecione o intervalo de tempo para o qual você deseja filtrar.
Current Statistics	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: <b>Nota:</b> Clique na seta ao lado de <b>Estatísticas atuais</b> para exibir ou ocultar as estatísticas. <ul style="list-style-type: none"> <li>• <b>Resultados totais</b> – Especifica o número total de resultados que correspondeu ao seu critério de procura.</li> <li>• <b>Arquivos de dados procurados</b> – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado.</li> <li>• <b>Arquivos de dados compactados procurados</b> – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado.</li> <li>• <b>Contagem de arquivo de índice</b> – Especifica o número total de arquivos de índice procurados durante o período de tempo especificado.</li> <li>• <b>Duração</b> – Especifica a duração da procura.</li> </ul> <b>Nota:</b> As estatísticas Atuais são úteis para resolução de problemas. Quando você contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.

Tabela 18. Parâmetros de eventos agrupados (continuação)

Parâmetro	Descrição
Gráficos	<p>Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em <b>Ocultar gráficos</b> se você deseja remover o gráfico da sua tela.</p> <p>Cada gráfico fornece uma legenda, que é uma referência visual para ajudá-lo a associar os objetos de gráfico aos parâmetros que eles representam. Usando o recurso de legenda, é possível executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>• Mova o ponteiro do mouse sobre um item de legenda para visualizar mais informações sobre os parâmetros que ele representa.</li> <li>• Clique com o botão direito no item de legenda para investigar melhor o item.</li> <li>• Clique em um item da legenda para ocultar os itens no gráfico. Clique no item de legenda novamente para mostrar o item oculto. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item.</li> <li>• Clique em <b>Legenda</b> se deseja remover a legenda da exibição de gráfico.</li> </ul> <p><b>Nota:</b> Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida.</p> <p><b>Nota:</b> Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para exibir gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.</p>
IP de Origem (contagem exclusiva)	Especifica o endereço IP de origem associado a este evento. Se houver vários endereços IP associados a este evento, este campo especificará o termo Vários e o número de endereços IP.
IP de Destino (contagem exclusiva)	Especifica o endereço IP de destino associado a este evento. Se houver vários endereços IP associados a este evento, este campo especificará o termo Vários e o número de endereços IP.
Porta de destino (contagem exclusiva)	Especifica as portas de destino associadas a este evento. Se houver várias portas associadas a este evento, este campo especificará o termo Várias e o número de portas.
Nome do Evento	Especifica o nome normalizado do evento.
Origem de Log (contagem exclusiva)	Especifica as origens de log que enviaram o evento para QRadar. Se houver várias origens de log associadas a esse evento, este campo especificará o termo Várias e o número de origens de log.
Categoria de Alto Nível (contagem exclusiva)	Especifica a categoria de alto nível desse evento. Se houver várias categorias associadas a este evento, este campo especificará o termo Várias e o número de categorias.
Categoria de Nível Baixo (contagem exclusiva)	Especifica a categoria de baixo nível desse evento. Se houver várias categorias associadas a este evento, este campo especificará o termo Várias e o número de categorias.
Protocolo (contagem exclusiva)	Especifica o ID do protocolo associado a este evento. Se houver vários protocolos associados a este evento, este campo especificará o termo Vários e o número de IDs do protocolo.
Nome de usuário (contagem exclusiva)	Especifica o nome de usuário associado a este evento, se disponível. Se houver vários nomes de usuários associados a este evento, este campo especificará o termo Vários e o número de nomes de usuários.
Magnitude (Máximo)	Especifica a magnitude máxima calculada para eventos agrupados. As variáveis usadas para calcular a magnitude incluem credibilidade, relevância, e gravidade. Para obter mais informações sobre credibilidade, relevância e gravidade, consulte o Glossário.
Contagem de Evento (soma)	Especifica o número total de eventos que são empacotados nesse evento normalizado. Os eventos são empacotados quando muitos eventos do mesmo tipo para o mesmo endereço IP de origem e de destino são vistos dentro de um curto período.
Contagem	Especifica o número total de eventos normalizados com este grupo de eventos.

## Procedimento

1. Clique na guia **Atividade de log**.
2. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.

3. Na caixa lista de exibição, escolha o parâmetro que você deseja no grupo de eventos. Consulte a Tabela 2. Os grupos de eventos são listados. Para obter mais informações sobre os detalhes do grupo de eventos. Consulte a Tabela 1.
4. Para visualizar a página Lista de eventos para um grupo, clique duas vezes no grupo de eventos que você deseja investigar. A página Lista de eventos não retém as configurações de gráfico que você pode ter definido na guia **Atividade de Log**. Para obter mais informações sobre os parâmetros da página Lista de eventos, consulte a Tabela 1.
5. Para visualizar os detalhes de um evento, clique duas vezes no evento que você deseja investigar. Para obter mais informações sobre detalhes do evento, consulte a Tabela 2.

## Detalhes do evento

É possível visualizar uma lista de eventos em vários modos, incluindo modo de fluxo ou em grupos de eventos. No modo escolhido para visualizar eventos, é possível localizar e visualizar os detalhes de um evento único.

A página de detalhes do evento fornece as seguintes informações:

*Tabela 19. Detalhes do evento*

Parâmetro	Descrição
Nome do Evento	Especifica o nome normalizado do evento.
Categoria de Nível Baixo	Especifica a categoria de baixo nível desse evento.  Para obter mais informações sobre categorias, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Descrição do Evento	Especifica uma descrição do evento, se disponível.
Magnitude	Especifica a magnitude deste evento. Para obter mais informações sobre magnitude, consulte o Glossário.
Relevância	Especifica a relevância deste evento. Para obter mais informações sobre a relevância, consulte o Glossário.
Gravidade	Especifica a severidade deste evento. Para obter mais informações sobre a severidade, consulte o Glossário.
Credibilidade	Especifica a credibilidade deste evento. Para obter mais informações sobre credibilidade, consulte o Glossário.
Nome de Usuário	Especifica o nome de usuário associado a este evento, se disponível.
Horário de Início	Especifica o horário que o evento foi recebido da origem de log.
Horário do Armazenamento	Especifica o horário em que o evento foi armazenado no banco de dados do QRadar.
Horário da Origem de Log	Especifica o horário do sistema, conforme relatado pela origem de log na carga útil do evento.
Informações de detecção de anomalia – Esta área de janela é exibida somente se esse evento foi gerado por uma regra de detecção de anomalias. Clique no ícone <b>Anomalia</b> para visualizar os resultados da procura salva que fazem com que a regra de detecção de anomalias gere este evento.	
Descrição da Regra	Especifica a regra de detecção de anomalia que gerou este evento.
Descrição da Anomalia	Especifica uma descrição do comportamento anômalo detectado pela regra de detecção de anomalia.
Valor de Alerta de Anomalia	Especifica o valor de alerta de anomalia.
<b>Informações de origem e destino</b>	
IP de Origem	Especifica o endereço IP de origem do evento.
IP de Destino	Especifica o endereço IP de destino do evento.
Nome do Ativo-fonte	Especifica nome de ativo definido pelo usuário da origem de eventos. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos.
Nome do Ativo de Destino	Especifica o nome de ativo definido pelo usuário do destino do evento. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos.
Porta de origem	Especifica a porta de origem deste evento.
Porta de Destino	Especifica a porta de destino deste evento.
IP de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de Conversão de Endereço de Rede (NAT), este parâmetro especifica o endereço IP de origem antes dos valores NAT serem aplicados. O NAT converte um endereço IP em uma rede para um endereço IP diferente em outra rede.

**Tabela 19. Detalhes do evento (continuação)**

Parâmetro	Descrição
IP de Destino NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de destino antes dos valores de NAT serem aplicados.
Porta de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem antes dos valores NAT serem aplicados.
Porta de Destino NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino antes dos valores de NAT serem aplicados.
IP de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, esse parâmetro especificará o endereço IP de origem após os valores de NAT serem aplicados.
IP de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de destino após os valores de NAT serem aplicados.
Porta de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem após os valores de NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, esse parâmetro especificará a porta de destino após os valores de NAT serem aplicados.
Porta de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem após os valores de NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, esse parâmetro especificará a porta de destino após os valores de NAT serem aplicados.
Origem de IPv6	Especifica o endereço IPv6 de origem do evento.
Destino de IPv6	Especifica o endereço IPv6 de destino do evento.
MAC de Origem	Especifica o endereço MAC de origem do evento.
MAC de Destino	Especifica o endereço MAC de destino do evento.
<b>Informações de carga útil</b>	
Carga Útil	Especifica o conteúdo da carga útil do evento. Este campo oferece 3 guias para visualizar a carga útil: <ul style="list-style-type: none"> <li>• Formato de Transformação Universal (UTF) - Clique em UTF.</li> <li>• Hexadecimal - Clique em HEX.</li> <li>• Base64 - Clique em Base64.</li> </ul>
<b>Informações adicionais</b>	
Protocolo	Especifica o protocolo que está associado a esse evento.
QID	Especifica o QID desse evento. Cada evento tem um QID exclusivo. Para obter mais informações sobre o mapeamento de um QID, consulte Modificando mapeamento de eventos.
Origem de Log	Especifica a origem de log que enviou o evento para QRadar. Se houver várias origens de log associadas a esse evento, este campo especificará o termo Várias e o número de origens de log.
Contagem de Evento	Especifica o número total de eventos que são empacotados nesse evento normalizado. Os eventos são empacotados quando muitos eventos do mesmo tipo para o mesmo endereço IP de origem e de destino são vistos dentro de um curto período.
Regras Customizadas	Especifica regras customizadas que correspondam a esse evento. .
Regras Customizadas Parcialmente Correspondidas	Especifica regras customizadas que correspondam parcialmente a esse evento.
Anotações	Especifica a anotação desse evento. Anotações são descrições de texto que as regras podem incluir automaticamente para eventos como parte da resposta de regra.
<b>Informações de identidade</b> – O QRadar coleta informações de identidade, se disponíveis, a partir das mensagens de origem do log. As informações de identidade fornecem detalhes adicionais sobre ativos em sua rede. Origens de Log gerarão informações de identificação somente se a mensagem de log enviada para QRadar contiver um endereço IP e pelo menos um dos seguintes itens: nome de usuário ou endereço MAC. Nem todas as origens de log geram informações de identificação. Para obter mais informações sobre identidade e ativos, consulte Gerenciamento de ativos.	
Nome de Usuário de Identidade	Especifica o nome do usuário do ativo que está associado a esse evento.
IP de Identidade	Especifica o endereço IP do ativo que está associado a esse evento.
Nome BIOS de Rede de Identidade	Especifica o nome do Sistema Básico de Entrada/Saída de Rede (NetBios) do ativo que está associado a esse evento.
Campo Identidade estendida	Especifica mais informações sobre o ativo que está associado a este evento. O conteúdo deste campo é o texto definido pelo usuário e depende dos dispositivos em sua rede que estão disponíveis para fornecer informações de identificação. Exemplos incluem: localização física de dispositivos, políticas relevantes, comutação de rede e nomes de portas.



Tabela 19. Detalhes do evento (continuação)

Parâmetro	Descrição
Has Identity (Flag)	Especifica Verdadeiro se QRadar tiver coletado informações de identidade do ativo que está associado a este evento.  Para obter mais informações sobre para quais dispositivos enviar informações de identidade, consulte <i>Guia de configuração do IBM Security QRadar DSM</i> .
Nome do Host de Identidade	Especifica o nome do host do ativo que está associado a esse evento.
MAC de Identidade	Especifica o endereço MAC do ativo que está associado a esse evento.
Nome do Grupo de Identidades	Especifica o nome do grupo do ativo que está associado a esse evento.

## Barra de ferramentas de detalhes do evento

A barra de ferramentas de detalhes dos eventos fornece várias funções para visualizar detalhes de eventos.

A barra de ferramentas **Detalhes do evento** fornece as seguintes funções:

Tabela 20. Barra de ferramentas de detalhes do evento

Retornar para lista de eventos	Clique em <b>Retornar</b> para <b>Lista de eventos</b> para retornar para a lista de eventos.
Ofensa	Clique em <b>Ofensa</b> para exibir as ofensas que são associadas ao evento.
Anomalia	Clique em <b>Anomalia</b> para exibir os resultados da procura salva que fizeram com que a regra de detecção de anomalias gere este evento. <b>Nota:</b> Esse ícone será exibido apenas se esse evento tiver sido gerado por uma regra de detecção de anomalias.
Mapear Evento	Clique em <b>Mapear evento</b> para editar o mapeamento do evento. Para obter mais informações, consulte Modificando mapeamento de eventos.
Positivo Falso	Clique em <b>Positivo falso</b> para ajustar o QRadar para evitar que eventos positivos falsos sejam gerados em ofensas.
Extrair Propriedade	Clique em <b>Extrair propriedade</b> para criar uma propriedade de evento customizada do evento selecionado.
Anterior	Clique em <b>Anterior</b> para visualizar o evento anterior na lista de eventos.
Avançar	Clique em <b>Avançar</b> para visualizar o próximo evento na lista de eventos.
Dados do PCAP	<b>Nota:</b> Essa opção será exibida somente se o seu Console do QRadar estiver configurado para se integrar com o Juniper JunOS Platform DSM. Para obter mais informações sobre como gerenciar os dados do PCAP, consulte Gerenciando dados do PCAP.  <ul style="list-style-type: none"> <li>• <b>Visualizar informações do PCAP</b> – Selecione esta opção para visualizar as informações do PCAP. Para obter mais informações, consulte Visualizando informações do PCAP.</li> <li>• <b>Fazer download do arquivo PCAP</b> – Selecione esta opção para fazer download do arquivo PCAP para seu sistema de área de trabalho. Para obter mais informações, consulte Fazendo download do arquivo PCAP para sua área de trabalho do sistema.</li> </ul>
Imprimir	Clique em <b>Imprimir</b> para imprimir os detalhes do evento.

## Visualizando ofensas associadas

Na guia Log de Atividades, você pode visualizar o crime que está associada ao evento.

### Sobre Esta Tarefa

Se um evento corresponder a uma regra, um crime pode ser gerada no guia **Ofensas**.

Para obter mais informações sobre as regras, consulte o *IBM Security QRadar SIEM Administration Guide*.

Para obter mais informações sobre como gerenciar ofensas, consulte Gerenciamento de Ofensa.

Quando você visualizar um crime na guia **Atividade do log**, o crime pode não exibir se o Magistrado ainda não foi salvo o crime que está associada ao evento selecionado para o disco ou o crime foi tirada do banco de dados. Se isso ocorrer, o sistema irá notificá-lo.

### Procedimento

1. Clique na guia **Atividade de log**.
2. Opcional. Se você estiver visualizando eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Clique no ícone **Ofensa** ao lado do evento que você deseja investigar.
4. Visualize o crime associada.

---

## Modificando mapeamento de eventos

Você pode mapear manualmente um evento normalizado ou bruto para uma categoria de nível superior e inferior (ou QID).

### Antes de Iniciar

Esta ação manual é usada para mapear eventos de origem de log desconhecidos para eventos do QRadar conhecidos, para que eles possam ser categorizados e processados apropriadamente.

### Sobre Esta Tarefa

Para fins de normalização, o QRadar mapeia automaticamente eventos de origens de log para categorias de nível superior e inferior.

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

Se os eventos forem recebidos de origens de log que o sistema não puder categorizar, eles serão categorizados como desconhecidos. Esses eventos ocorrem por vários motivos, incluindo:

- **Eventos definidos pelo usuário** - algumas origens de log, como Snort, permitem que você crie eventos definidos pelo usuário.
- **Eventos novos ou antigos** – as origens de log do fornecedor podem atualizar seu software com as liberações de manutenção para suportar novos eventos que o QRadar pode não suportar.

**Nota:** O ícone **Mapear evento** será desativado para eventos quando a categoria de alto nível for Auditoria SIM ou o tipo de origem de log for Simple Object Access Protocol (SOAP).

### Procedimento

1. Clique na guia **Atividade de log**.
2. Opcional. Se você estiver visualizando eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.

3. Dê um clique duplo no evento que você deseja mapear.
4. Clique em **Mapear evento**.
5. Se você souber o QID que você deseja mapear para esse evento, insira o QID no campo **Inserir QID**.
6. Se você não souber o QID que deseja mapear para esse evento, será possível procurar um QID específico:
  - a. Escolha uma das opções a seguir: Para procurar um QID pela categoria, selecione a categoria de nível superior na caixa de listagem Categoria de nível superior. Para procurar um QID pela categoria, selecione a categoria de nível inferior na caixa de listagem Categoria de nível inferior. Para procurar um QID pelo tipo de origem de log, selecione um tipo de origem de log na caixa de listagem Tipo de Origem de Log. Para procurar um QID pelo nome, insira um nome no campo QID/Nome.
  - b. Clique em **Procurar**.
  - c. Selecione o **QID** ao qual você deseja associar esse evento.
7. Clique em **OK**.

---

## Ajustando falsos positivos

Você pode usar a função Ajuste de Positivo Falso para evitar que eventos falsos positivos criem ofensas.

### Antes de Iniciar

Você pode ajustar eventos falsos positivos da lista Lista de Eventos ou da página Detalhes do Evento.

### Sobre Esta Tarefa

Você pode ajustar eventos falsos positivos da lista Lista de Eventos ou da página Detalhes do Evento.

Você deve ter as permissões apropriadas para criar regras customizadas para ajustar falsos positivos.

Para obter mais informações sobre funções, consulte o *IBM Security QRadar SIEM Administration Guide*.

Para obter mais informações sobre falsos positivos, consulte o Glossário.

### Procedimento

1. Clique na guia **Atividade de log**.
2. Opcional. Se você estiver visualizando eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Selecione o evento que você deseja ajustar.
4. Clique em **Positivo falso**.
5. Na área de janela de Propriedade de Evento/Fluxo na janela Positivo Falso, selecione uma das opções a seguir:
  - Evento/Fluxo(s) com um QID específico de <Event>
  - Qualquer Evento/Fluxo com uma categoria de nível inferior de <Event>
  - Qualquer Evento/Fluxo com uma categoria de alto nível de <Event>

6. Na área de janela Direção do Tráfego, selecione uma das seguintes opções:
  - <Endereço IP de Origem> para <Endereço IP de Destino>
  - <Endereço IP de Origem> para Qualquer Destino
  - Qualquer Origem para <Endereço IP de Destino>
  - Qualquer Origem para qualquer Destino
7. Clique em **Ajustar**.

---

## Gerenciando dados de PCAP

Se o Console do QRadar estiver configurado para se integrar ao Juniper JunOS Platform DSM, em seguida, a Captura de Pacotes (PCAP) poderá ser recebida, processada e os dados poderão ser armazenados a partir de uma origem de log do Juniper SRX-Series Services Gateway.

Para obter mais informações sobre o Juniper JunOS Platform DSM, consulte o *Guia de configuração do IBM Security QRadar DSM*.

## Exibindo a coluna de dados do PCAP

A coluna **Dados do PCAP** não é exibida na guia **Atividade de log** por padrão. Ao criar critérios de procura, você deverá selecionar a coluna **Dados do PCAP** na área de janela Definição de Coluna.

### Antes de Iniciar

Antes que você possa exibir os dados do PCAP na guia **Atividade de log**, a origem de log do Gateway de Serviços da série SRX da Juniper deverá ser configurada com o protocolo Combinação de Syslog do PCAP. Para obter mais informações sobre como configurar os protocolos de origem de log, consulte o *Gerenciando guia de origem de log*.

### Sobre Esta Tarefa

Ao executar uma procura que inclua a coluna **Dados do PCAP**, um ícone será exibido na coluna **Dados do PCAP** dos resultados da procura, se os dados do PCAP estiverem disponíveis para um evento. Usando o ícone **PCAP**, você pode visualizar os dados do PCAP ou fazer o download do arquivo **PCAP** para seu sistema de desktop.

### Procedimento

1. Clique na guia **Atividade de log**.
2. Na caixa de listagem **Procurar**, selecione **Nova Procura**.
3. Opcional. Para procurar eventos que possuam dados do PCAP, configure os critérios de procura a seguir:
  - a. Na primeira caixa de listagem, selecione **Dados do PCAP**.
  - b. Na segunda caixa de listagem, selecione **Iguais**.
  - c. Na terceira caixa de listagem, selecione **Verdadeiro**.
  - d. Clique em **Incluir filtro**.
4. Configure suas definições de coluna para incluir a coluna **Dados do PCAP**:
  - a. Na lista **Colunas disponíveis** na área de janela Definição de Coluna, clique em **Dados do PCAP**.
  - b. Clique no ícone **Incluir coluna** no conjunto de ícones inferior para mover a coluna **Dados do PCAP** para a lista **Colunas**.

- c. Opcional. Clique no ícone **Incluir coluna** no conjunto de ícones superior para mover a coluna **Dados do PCAP** para a lista **Por grupo**.
5. Clique em **Filtrar**.
6. Opcional. Se você estiver visualizando eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
7. Dê um clique duplo no evento que você deseja investigar.

## O que Fazer Depois

Para obter mais informações sobre a visualização e download de dados do PCAP, consulte as seções a seguir:

- Visualizando informações do PCAP
- Fazendo download do arquivo PCAP para seu sistema de desktop

## Visualizando informações do PCAP

No menu da barra de ferramentas **Dados do PCAP**, você pode visualizar uma versão legível dos dados no arquivo PCAP ou fazer o download do arquivo PCAP para seu sistema da área de trabalho.

### Antes de Iniciar

Antes de poder visualizar informações do PCAP, você deve executar ou selecionar uma procura que exiba a coluna **Dados do PCAP**.

### Sobre Esta Tarefa

Antes que os dados do PCAP possam ser exibidos, o arquivo PCAP deve ser recuperado para exibição na interface com o usuário. Se o processo de download tomar um longo período, a janela de Informações para download do pacote PCAP será exibida. Na maioria dos casos, o processo de download é rápido e essa janela não é exibida.

Depois que o arquivo for recuperado, uma janela pop-up fornecerá uma versão legível do arquivo PCAP. Você pode ler as informações exibidas na janela, ou fazer o download das informações para seu sistema da área de trabalho.

### Procedimento

1. Para o evento que você deseja investigar, escolha uma das opções a seguir:
  - Selecione o evento e clique no ícone **PCAP**.
  - Clique com o botão direito do mouse no ícone **PCAP** para o evento e selecione **Mais opções > Visualizar informações do PCAP**.
  - Clique duas vezes no evento que você deseja investigar e, em seguida, selecione **Dados do PCAP > Visualizar informações do PCAP** na barra de ferramentas detalhes do evento.
2. Se você deseja fazer o download das informações para o seu sistema da área de trabalho, escolha uma das opções a seguir:
  - Clique em **Fazer o download do arquivo do PCAP** para fazer o download do arquivo PCAP original a ser usado em um aplicativo externo.
  - Clique em **Fazer o download do texto PCAP** para fazer o download das informações do PCAP em formato TXT.
3. Escolha uma das opções a seguir:

- Se você deseja abrir o arquivo para visualização imediata, selecione a opção **Abrir com** e selecione um aplicativo na caixa de listagem.
  - Se você deseja salvar a lista, selecione a opção **Salvar arquivo**.
4. Clique em **OK**.

## Fazendo download do arquivo PCAP para seu sistema de desktop

Você pode fazer download do arquivo PCAP para seu sistema de desktop para armazenamento ou uso em outros aplicativos.

### Antes de Iniciar

Antes que você possa visualizar as informações do PCAP, você deverá executar ou selecionar uma procura que exiba a coluna Dados do PCAP. Consulte **Exibindo a coluna de dados do PCAP**.

### Procedimento

1. Para o evento que você deseja investigar, escolha uma das opções a seguir:
  - Selecione o evento e clique no ícone **PCAP**.
  - Clique com o botão direito do mouse no ícone do PCAP para o evento e selecione **Mais opções > Fazer download do arquivo PCAP**.
  - Dê um clique duplo no evento que você deseja investigar e, em seguida, selecione **Dados do PCAP > Fazer download do arquivo PCAP** na barra de ferramentas de detalhes do evento.
2. Escolha uma das opções a seguir:
  - Se você deseja abrir o arquivo para visualização imediata, selecione a opção **Abrir com** e selecione um aplicativo na caixa de listagem.
  - Se você deseja salvar a lista, selecione a opção **Salvar arquivo**.
3. Clique em **OK**.

---

## Exportando eventos

Você pode exportar eventos no formato Linguagem de Marcação Extensível (XML) ou Valores Separados por Vírgulas (CSV).

### Antes de Iniciar

A duração de tempo necessária para exportar seus dados depende do número de parâmetros especificados.

### Procedimento

1. Clique na guia **Atividade de log**.
2. Opcional. Se você estiver visualizando eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Na caixa de listagem **Ações**, selecione uma das opções a seguir:
  - **Exportar para XML > Colunas visíveis** – selecione essa opção para exportar somente as colunas visíveis na guia Atividade de log. Essa é a opção recomendada.
  - **Exportar para XML > Exportação integral (todas as colunas)** – selecione essa opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída.

- **Exportar para CSV > Colunas visíveis** – selecione essa opção para exportar somente as colunas visíveis na guia **Atividade de log**. Essa é a opção recomendada.
  - **Exportar para CSV > Exportação integral (todas as colunas)** – Selecione esta opção para exportar todos os parâmetros de eventos. Uma exportação integral pode demorar um longo período de tempo para ser concluída.
4. Se você deseja continuar suas atividades enquanto a exportação estiver em andamento, clique em **Notificar quando estiver pronto**.

## **Resultados**

Quando a exportação for concluída, você receberá uma notificação que a exportação foi concluída. Se você não selecionar o ícone **Notificar quando estiver pronto**, a janela de status será exibida.





---

## Capítulo 6. Investigação de atividade de rede

É possível usar a guia **Atividade de Rede** para monitorar e investigar atividade de rede (fluxos) em tempo real ou conduzir procuras avançadas

---

### Visão geral da guia Rede

Usando a guia **Atividade de Rede**, é possível monitorar e investigar atividade de rede (fluxos) em tempo real ou conduzir procuras avançadas.

Deve-se ter permissão para visualizar a guia **Atividade de rede**.

Para obter mais informações sobre permissões e designar funções, consulte o *IBM Security QRadar SIEM Administration Guide*.

Selecione a guia **Atividade de Rede** para monitorar visualmente e investigar dados de fluxo em tempo real ou conduzir procuras avançadas para filtrar os fluxos exibidos. Um fluxo é uma sessão de comunicação entre dois hosts. É possível visualizar informações de fluxo para determinar como o tráfego é comunicado e o que foi comunicado (se a opção capturar conteúdo estiver ativada). As informações de fluxo também podem incluir detalhes como protocolos, valores de Número de Sistema Autônomo (ASN) ou valores de Índice de Interface (IFIndex).

### Barra de ferramentas da guia Atividade de rede

Opções da barra de ferramentas Atividade de rede

Usando a barra de ferramentas, é possível acessar as seguintes opções:

*Tabela 21. Opções da barra de ferramentas da guia Atividade de rede*

Opções	Descrição
Procura	Clique em <b>Procurar</b> para executar procuras avançadas em fluxos. As opções incluem: <ul style="list-style-type: none"><li>• <b>Nova procura</b> – Selecione esta opção para criar uma nova procura de fluxo.</li><li>• <b>Editar procura</b> – Selecione esta opção para selecionar e editar uma procura de fluxo.</li><li>• <b>Gerenciar resultados da procura</b> – Selecione esta opção para visualizar e gerenciar resultados da procura.</li></ul> Para obter mais informações sobre o recurso de procura, consulte Procuras de dados.
Procuras Rápidas	Nesta caixa de listagem, é possível executar procuras salvas anteriormente. As opções são exibidas na caixa de listagem <b>Procuras rápidas</b> apenas quando forem salvos os critérios de procura que especificam a opção <b>Incluir em minhas procuras rápidas</b> .
Incluir Filtro	Clique em <b>Incluir filtro</b> para incluir um filtro aos resultados de procura atual.
Salvar Critérios	Clique em <b>Salvar Critérios</b> para salvar os critérios de procura atuais.
Salvar Resultados	Clique em <b>Salvar resultados</b> para salvar os resultados da procura atual. Essa opção será exibida somente após a conclusão de uma procura. Esta opção está desativada no modo de fluxo.
Cancelar	Clique em <b>Cancelar</b> para cancelar uma procura em andamento. Esta opção está desativada no modo de fluxo.
Positivo Falso	Clique em <b>Positivo falso</b> para abrir a janela Ajuste de positivo falso, o qual permite que você ajuste os fluxos que são conhecidos por serem positivos falsos de criação de crimes. Para obter mais informações sobre falsos positivos, consulte o Glossário.  Esta opção está desativada no modo de fluxo. Consulte Exportando fluxos.

Tabela 21. Opções da barra de ferramentas da guia Atividade de rede (continuação)

Opções	Descrição
Regras	<p>A opção <b>Regras</b> estará visível somente se você tiver permissão para visualizar regras customizadas.</p> <p>Selecione uma das opções a seguir:</p> <p><b>Regras</b> para visualizar ou criar uma regra. Se tiver somente a permissão para visualizar as regras, a página de resumo do assistente de regras será exibida. Se tiver a permissão para manter as regras customizadas, será possível editar a regra.</p> <p><b>Nota:</b> As opções de regra de detecção de anomalia estarão visíveis apenas se tiver a permissão <b>Atividade de rede &gt; Manter regras customizadas</b>.</p> <p>Para ativar as opções de regra de detecção de anomalia, é necessário salvar o critério de procura agregada. Os critérios de procura salvos especificam os parâmetros requeridos. Selecione uma das opções a seguir</p> <p><b>Incluir regra de limite</b> para criar uma regra de limite. Uma regra de limite testa o tráfego de fluxo da atividade que excede um limite configurado. Os limites podem ser baseados em quaisquer dados que são coletados. Por exemplo, se for criada uma regra de limite indicando que não mais de 220 clientes podem efetuar login no servidor entre 8h e 17h, as regras gerarão um alerta quando o cliente 221° tentar efetuar login.</p> <p><b>Incluir regra comportamental</b> para criar uma regra comportamental. Uma regra comportamental testa o tráfego de fluxo para mudanças no comportamento que ocorrem em padrões sazonais regulares. Por exemplo, se um servidor de correio geralmente se comunica com 100 hosts por segundo no meio da noite e de repente começa a se comunicar com 1.000 hosts por segundo, uma regra comportamental gerará um alerta.</p> <p><b>Incluir regra de anomalia</b> para criar uma regra de anomalia. Uma regra de anomalia testa o tráfego de fluxo para atividade anormal, como tráfego novo ou desconhecido. Por exemplo, é possível criar uma regra de anomalia para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego da última hora. Se houver mais que uma alteração de 40%, a regra gerará uma resposta.</p> <p>Para obter informações adicionais, consulte o <i>IBM Security QRadar SIEM Administration Guide</i>.</p>
Ações	<p>Clique em <b>Ações</b> para executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>• <b>Mostrar todos</b> – Selecione esta opção para remover todos os filtros nos critérios de procura e exibir todos os fluxos não filtrados.</li> <li>• <b>Imprimir</b> – Selecione esta opção para imprimir os fluxos que são exibidos na página.</li> <li>• <b>Exportar para XML</b> – Selecione esta opção para exportar os fluxos no formato XML. Consulte Exportando fluxos.</li> <li>• <b>Exportar para CSV</b> – Selecione esta opção para exportar os fluxos no formato CSV. Consulte Exportando fluxos.</li> <li>• <b>Excluir</b> – Selecione esta opção para excluir um resultado da procura. Consulte Procuras de dados.</li> <li>• <b>Notificar</b> – Selecione esta opção para especificar que deseja que uma notificação seja enviada por email para você na conclusão das procuras selecionadas. Esta opção está ativada apenas para procuras em andamento.</li> </ul> <p><b>Nota:</b> As opções <b>Imprimir</b>, <b>Exportar para XML</b> e <b>Exportar para CSV</b> estão desativadas no modo de fluxo e ao visualizar resultados parciais de procura.</p>
Filtro Rápido	<p>Digite seus critérios de procura no campo <b>Filtro rápido</b> e clique no ícone <b>Filtro rápido</b> ou pressione Enter no teclado. Todos os fluxos que correspondem aos seus critérios de procura são exibidos na lista de fluxos. Uma procura de texto é executada na carga útil do evento para determinar quais correspondem aos critérios especificados.</p> <p><b>Nota:</b> Ao clicar no campo <b>Filtro rápido</b>, uma dica de ferramenta será exibida, fornecendo informações sobre a sintaxe apropriada para usar no critério de procura. Para obter mais informações de sintaxe, consulte Sintaxe de filtro rápido.</p>

## Sintaxe de Filtro Rápido

O recurso Filtro Rápido permitirá procurar as cargas úteis de fluxo usando uma sequência de procura de texto.

A funcionalidade Filtro Rápido está disponível nos seguintes locais na interface com o usuário:

- Barra de ferramentas **Atividade de rede** – Na barra de ferramentas, um campo **Filtro rápido** permite que você digite uma sequência de procura de texto e clique no ícone **Filtro rápido** para aplicar seu filtro rápido na lista de fluxos atualmente exibida.
- Caixa de diálogo **Incluir filtro** – A partir da caixa de diálogo **Incluir filtro**, que é acessada clicando no ícone **Incluir filtro** na guia **Atividade de Rede**, é possível selecionar **Quick Filter** como seu parâmetro de filtragem e digitar uma sequência de procura de texto. Isso permite que seu filtro rápido seja aplicado para a lista atualmente exibida dos fluxos. Para obter mais informações sobre a caixa de diálogo **Incluir filtro**, consulte Procuras de dados.
- Páginas **Procura de fluxo** – Nas páginas de procura de fluxo, é possível incluir um Filtro Rápido para sua lista de filtros a serem incluídos em seus critérios de procura. Para obter mais informações sobre como configurar critérios de procura, consulte Procuras de dados.

Ao visualizar os fluxos em tempo real (fluxo) ou modo de último intervalo, será possível somente digitar palavras ou frases simples no campo **Filtro rápido**. Ao visualizar o fluxo usando um intervalo de tempo, use as seguintes diretrizes de sintaxe para inserir seus critérios de procura de texto:

- Termos de procura podem incluir qualquer texto simples que você espere localizar na carga útil. Por exemplo, Firewall
- Inclua vários termos entre aspas duplas para indicar que deseja procurar a frase exata. Por exemplo, "Negação de firewall"
- Termos de procura podem incluir curingas de caracteres únicos e múltiplos. O termo de procura não pode começar com um curinga. Por exemplo, F?rewall or F??ew\*
- Os termos de procura são correspondidos em sequência a partir do primeiro caractere na palavra ou frase da carga útil. Por exemplo, o termo de procura user corresponde a user\_1 e user\_2, mas não correspondem às seguintes frases: ruser, myuser ou anyuser.
- Termos de grupo usando expressões lógicas, como AND, OR e NOT. A sintaxe faz distinção entre maiúsculas e minúsculas e os operadores devem estar em letras maiúsculas para serem reconhecidos como expressões lógicas e não como termos de procura. Por exemplo: (%PIX\* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.\*)

Ao criar critérios de procura que inclui a expressão lógica NOT, será necessário incluir pelo menos um outro tipo de expressão lógica, caso contrário, o filtro não retornará nenhum resultado. Por exemplo: (%PIX\* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.\*)

- Os seguintes caracteres devem ser precedidos por uma barra invertida para indicar que o caractere é parte de seu termo de procura: + - && || ! () {} [] ^ " ~ \* ? : \. Por exemplo: "%PIX\5\304001"

## Opções do menu ativado pelo botão direito

Na guia **Atividade de rede**, é possível clicar com o botão direito em um fluxo para acessar mais critérios de filtro de fluxo.

As opções do menu ativado pelo botão direito são:

*Tabela 22. Opções do menu ativado pelo botão direito*

Opção	Descrição
Filtro em	Selecione esta opção para filtrar no fluxo selecionado, dependendo do parâmetro selecionado no fluxo.

Tabela 22. Opções do menu ativado pelo botão direito (continuação)

Opção	Descrição
Positivo Falso	Selecione esta opção para abrir a janela Ajuste positivo falso, que permite o ajuste de fluxos que são conhecidos por serem positivos falsos de criação de crimes. Esta opção está desativada no modo de fluxo. Consulte Exportando fluxos.
Mais opções:	Selecione esta opção para investigar um endereço IP. Consulte Investigando endereços IP. <b>Nota:</b> Esta opção não é exibida no modo de fluxo.

## Barra de status

Ao transmitir fluxos, a barra de status exibirá o número médio de resultados que são recebidos por segundo.

Este é o número de resultados que o Console recebeu com sucesso a partir dos processadores de eventos. Se o número for maior que 40 resultados por segundo, somente 40 resultados serão exibidos. O restante é acumulado no buffer de resultado. Para visualizar mais informações de status, mova o ponteiro do mouse sobre a barra de status.

Quando os fluxos não estiverem sendo transmitidos, a barra de status exibirá o número de resultados da procura que são atualmente exibidos e a quantidade de tempo que é necessária para processar os resultados da procura.

## Registros do Overflow

Com permissões administrativas, é possível especificar o número máximo de fluxos que deseja enviar do QRadar QFlow Collector para os Processadores de eventos.

Se tiver permissões administrativas, será possível especificar o número máximo de fluxos que deseja enviar a partir do QRadar QFlow Collector para os Processadores de eventos. Todos os dados que são coletados após o limite de fluxo configurado ser atingido serão agrupados em um registro de fluxo. Este registro de fluxo é, então, exibido na guia **Atividade de rede** com o endereço IP de origem 127.0.0.4 e um endereço IP de destino 127.0.0.5. Esse registro de fluxo especifica Overflow na guia **Atividade de rede**.

---

## Monitorando a atividade de rede

Por padrão, a guia **Atividade de rede** exibe os fluxos no modo de fluxo, permitindo que visualize os fluxos em tempo real.

Para obter mais informações sobre o modo de fluxo, consulte Visualizando os fluxos. É possível especificar um intervalo de tempo diferente para filtrar fluxos usando a caixa de listagem **Visualização**.

Se uma procura salva for configurada anteriormente como o padrão, os resultados dessa procura serão exibidos automaticamente ao acessar a guia **Atividade de rede**. Para obter mais informações sobre como salvar os critérios de procura, consulte Salvando critérios de procura de fluxo e de evento.

## Visualizando fluxos de fluxo

O modo de fluxo permite que você visualize os dados de fluxo inseridos no seu sistema. Este modo fornece a você uma visualização em tempo real de sua atividade do fluxo atual exibindo os últimos 50 fluxos.

## Sobre Esta Tarefa

Se você aplicar quaisquer filtros na guia Atividade de Rede ou em seu critério de procura antes de ativar o modo de fluxo, os filtros serão mantidos em modo de fluxo. No entanto, o modo de fluxo não suporta procuras que incluem fluxos agrupados. Se você ativar o modo de fluxo agrupado ou critério de procura agrupado, a guia Atividade de Rede exibirá os fluxos normalizados. Consulte visualizando fluxos normalizados.

Quando você deseja selecionar um fluxo para visualizar detalhes ou executar uma ação, você deve pausar o fluxo antes de clicar duas vezes em um evento. Quando o fluxo é pausado, os últimos 1.000 fluxos são exibidos.

## Procedimento

1. Clique na guia **Atividade de rede**.
2. Na caixa de listagem Visualização, selecione **Tempo real (fluxo)**. Para obter informações sobre as opções da barra de ferramentas, consulte a Tabela 5-1. Para obter mais informações sobre os parâmetros exibidos no modo de fluxo, consulte a Tabela 5-3.
3. Opcional. Pausar ou executar fluxos de fluxo. Escolha uma das opções a seguir:
  - Para selecionar um registro de eventos, clique no ícone **Pausar** para pausar o fluxo.
  - Para reiniciar o modo de fluxo, clique no ícone **Executar**.

## Visualizando fluxos normalizados

O fluxo de dados é coletado, normalizado e exibido na guia **Atividade de rede**.

## Sobre Esta Tarefa

A normalização envolve preparar os dados de fluxo para exibir informações legíveis sobre a guia.

**Nota:** Se você selecionar um prazo para exibição, um gráfico de série temporal será exibido. Para obter mais informações sobre como usar os gráficos de série temporal, consulte Visão geral dos gráfico de série temporal.

A guia **Atividade de rede** exibirá os seguintes parâmetros quando você visualizar os fluxos normalizados:

*Tabela 23. Parâmetros para a guia atividade de rede*

Parâmetro	Descrição
Filtros Atuais	A parte superior da tabela exibe os detalhes dos filtros aplicados aos resultados da procura. Para limpar esses valores de filtro, clique em <b>Limpar filtro</b> . <b>Nota:</b> Esse parâmetro só será exibido após você aplicar um filtro.
Visualização	Na caixa de listagem, você pode selecionar o intervalo de tempo para o qual você deseja filtrar.

Tabela 23. Parâmetros para a guia atividade de rede (continuação)

Parâmetro	Descrição
Estatística Atual	<p>Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo:</p> <p><b>Nota:</b> Clique na seta ao lado das Estatísticas Atuais para exibir ou ocultar as estatísticas.</p> <ul style="list-style-type: none"> <li>• <b>Resultados totais</b> – Especifica o número total de resultados que correspondeu ao seu critério de procura.</li> <li>• <b>Arquivos de dados procurados</b> – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado.</li> <li>• <b>Arquivos de dados compactados procurados</b> – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado.</li> <li>• <b>Contagem de arquivo de índice</b> – Especifica o número total de arquivos de índice procurados durante o período de tempo especificado.</li> <li>• <b>Duração</b> – Especifica a duração da procura.</li> </ul> <p><b>Nota:</b> Estatísticas atuais são úteis para resolução de problemas. Quando você contata o Suporte ao Cliente para solucionar problemas de fluxos, você pode ser solicitado a fornecer informações de estatísticas atuais.</p>
Gráficos	<p>Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em <b>Ocultar gráficos</b> se desejar remover os gráficos da sua exibição.</p> <p>Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Configurando gráficos.</p> <p><b>Nota:</b> Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para exibir gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.</p>
Offense icon	Clique no ícone <b>Ofensas</b> para visualizar detalhes da ofensa associada a este fluxo.
Tipo de Fluxo	<p>Especifica o tipo de fluxo. Tipos de fluxo são medidos pela proporção de atividade recebida para atividade de saída. Tipos de fluxo incluem:</p> <ul style="list-style-type: none"> <li>• <b>Fluxo padrão</b> – Tráfego bidirecional</li> <li>• <b>Tipo A</b> – Um para Muitos (unidirecional), por exemplo, um único host que executa uma varredura de rede.</li> <li>• <b>Tipo B</b> – Muitos para Um (unidirecional), por exemplo, um ataque do DoS Distribuído (DDoS).</li> <li>• <b>Tipo C</b> – Um para Um (unidirecional), por exemplo, um host para uma varredura de porta do host.</li> </ul>
Horário do Primeiro Pacote	Especifica a data e a hora em que o fluxo é recebido.
Horário do Armazenamento	Especifica o horário em que o fluxo é armazenado no banco de dados QRadar.
IP de Origem	Especifica o endereço IP de origem do fluxo.
Porta de origem	Especifica a porta de origem do fluxo.
IP de Destino	Especifica o endereço IP de destino do fluxo.
Porta de Destino	Especifica a porta de destino do fluxo.
Bytes de Origem	Especifica o número de bytes enviado do host de origem.
Bytes de Destino	Especifica o número de bytes enviado do host de destino.
Total de Bytes	Especifica o número total de bytes associados ao fluxo.
Pacotes de Origem	Especifica o número total de pacotes enviado do host de origem.
Pacotes de Destino	Especifica o número total de pacotes enviado do host de destino.
Total de Pacotes	Especifica o número total de pacotes associado ao fluxo.
Protocolo	Especifica o protocolo associado ao fluxo.
Aplicativo	Especifica o aplicativo detectado do fluxo. Para obter mais informações sobre detecção do aplicativo, consulte o <i>IBM Security QRadar Application Configuration Guide</i> .
Tipo/Código de ICMP	<p>Especifica o tipo de Internet Control Message Protocol (ICMP) e o código, se aplicável.</p> <p>Se o fluxo tem o tipo ICMP e informações de código em um formato conhecido, este campo será exibido como Tipo &lt;A&gt;. Código &lt;B&gt;, em que &lt;A&gt; e &lt;B&gt; são os valores numéricos do tipo e do código.</p>

Tabela 23. Parâmetros para a guia atividade de rede (continuação)

Parâmetro	Descrição
Sinalizadores de Origem	Especifica os sinalizadores do Protocolo de Controle de Transmissão (TCP) detectados no pacote de origem, se aplicável.
Sinalizadores de Destino	Especifica os sinalizadores TCP detectados no pacote de destino, se aplicável.
QoS de Origem	Especifica o nível de serviço da Qualidade de Serviço (QoS) para o fluxo. O QoS habilita uma rede para fornecer vários níveis de serviço para os fluxos. QoS fornece os seguintes níveis de serviço básicos: <ul style="list-style-type: none"> <li>• <b>Melhor esforço</b> – Este nível de serviço não garante a entrega. A entrega do fluxo é considerada o melhor esforço.</li> <li>• <b>Serviço diferenciado</b> – Parte dos fluxos é prioridade concedida sobre outros fluxos. Esta prioridade é concedida pela classificação do tráfego.</li> <li>• <b>Serviço garantido</b> – Este nível de serviço garante a reserva de recursos de rede para parte dos fluxos.</li> </ul>
QoS de Destino	Especifica o nível de QoS de serviço para o fluxo de destino.
Origem do Fluxo	Especifica o sistema que detectou o fluxo.
Interface do Fluxo	Especifica a interface que recebeu o fluxo.
If Index de Origem	Especifica o número da interface de origem do índice (IFIndex).
If Index de Destino	Especifica o número IFIndex de destino.
ASN de Origem	Especifica o valor do número de sistema autônomo de origem (ASN).
ASN de Destino	Especifica o valor de destino ASN.

## Procedimento

1. Clique na guia **Atividade de rede**.
2. Na caixa da lista de **Exibição**, selecione **Padrão (normalizado)**.
3. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
4. Clique no ícone **Pausar** para pausar o fluxo.
5. Clique duas vezes no fluxo que deseja visualizar com mais detalhes. Consulte **Detalhes do fluxo**.

## Visualizando fluxos agrupados

Usando a guia **Atividade de rede**, você pode visualizar os fluxos agrupados por várias opções. Na caixa **Lista de exibição**, você pode selecionar o parâmetro pelo qual deseja para fluxos de grupo.

### Sobre Esta Tarefa

A caixa de listagem **Exibir** não é exibida no modo de fluxo porque o modo de fluxo não suporta fluxos agrupados. Se você inseriu o modo de fluxo usando critério de procura não agrupado, esta opção será exibida.

A caixa de listagem **Exibir** fornece as seguintes opções:

Tabela 24. Opções de fluxo agrupado

Opção de grupo	Descrição
Fluxos unidos	Exibe vários fluxos em um padrão ininterrupto em vários intervalos, em um único registro. Por exemplo, se um fluxo tiver um comprimento de cinco minutos, o fluxo unido será exibido como um único fluxo de cinco minutos. Sem o fluxo unido, o fluxo será exibido como 5 fluxos: um fluxo para cada minuto.  Os fluxos unidos exibem uma lista resumida de fluxos agrupados por informações de fluxo unido.
IP de origem ou destino	Exibe uma lista resumida dos fluxos agrupados pelo endereço IP associado ao fluxo.
IP de Origem	Exibe uma lista resumida dos fluxos agrupados pelo endereço IP de origem do fluxo.
IP de Destino	Exibe uma lista resumida dos fluxos pelo endereço IP de destino do fluxo.



Tabela 24. Opções de fluxo agrupado (continuação)

Opção de grupo	Descrição
Porta de origem	Exibe uma lista resumida dos fluxos agrupados pela porta de origem do fluxo.
Porta de Destino	Exibe uma lista resumida dos fluxos agrupados pela porta de destino do fluxo.
Rede de origem	Exibe uma lista resumida dos fluxos agrupados pela rede de origem do fluxo.
Rede de destino	Exibe uma lista resumida dos fluxos agrupados pela rede de destino do fluxo.
Aplicativo	Exibe uma lista resumida dos fluxos agrupados pelo aplicativo que originou o fluxo.
Geográfico	Exibe uma lista resumida dos fluxos agrupados por localização geográfica.
Protocolo	Exibe uma lista resumida dos fluxos agrupados pelo protocolo associado ao fluxo.
Propensão de Fluxo	Exibe uma lista resumida dos fluxos agrupados pela direção do fluxo.
Tipo de ICMP	Exibe uma lista resumida dos fluxos agrupados pelo tipo de ICMP do fluxo.

Depois de selecionar uma opção na caixa de listagem **Exibir**, o layout da coluna dos dados depende da opção do grupo escolhido. Cada linha da tabela de fluxos representa um grupo de fluxo. A guia **Atividade de rede** fornece as seguintes informações para cada grupo de fluxo.

Tabela 25. Parâmetros de fluxos agrupados

Cabeçalho	Cabeçalho
Agrupar por	Especifica o parâmetro no qual a procura está agrupada.
Current Filters	A parte superior da tabela exibe os detalhes do filtro aplicado aos resultados da procura. Para limpar esses valores de filtro, clique em <b>Limpar filtro</b> .
Visualização	Na caixa de listagem, selecione o intervalo de tempo para o qual você deseja filtrar.
Current Statistics	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: <b>Nota:</b> Clique na seta ao lado de <b>Estatísticas atuais</b> para exibir ou ocultar as estatísticas. <ul style="list-style-type: none"> <li>• <b>Resultados totais</b> – Especifica o número total de resultados que correspondeu ao seu critério de procura.</li> <li>• <b>Arquivos de dados procurados</b> – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado.</li> <li>• <b>Arquivos de dados compactados procurados</b> – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado.</li> <li>• <b>Contagem de arquivo de índice</b> – Especifica o número total de arquivos de índice procurados durante o período de tempo especificado.</li> <li>• <b>Duração</b> – Especifica a duração da procura.  <b>Nota:</b> As estatísticas Atuais são úteis para resolução de problemas. Quando você contata o Suporte ao Cliente para solucionar problemas de fluxos, você pode ser solicitado a fornecer informações de estatísticas atuais.</li> </ul>
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em <b>Ocultar gráficos</b> se deseja remover o gráfico da sua exibição.  Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Configurando gráficos. <b>Nota:</b> Se você usar o Mozilla Firefox como seu navegador e uma extensão do navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para exibir gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.
IP de Origem (contagem exclusiva)	Especifica o endereço IP de origem do fluxo.
IP de Destino (contagem exclusiva)	Especifica o endereço IP de destino do fluxo. Se houver vários endereços IP de destino associados a esse fluxo, este campo especificará o termo Vários e o número de endereços IP.
Porta de origem (contagem exclusiva)	Exibe a porta de origem do fluxo.



**Tabela 25. Parâmetros de fluxos agrupados (continuação)**

Cabeçalho	Cabeçalho
Porta de destino (contagem exclusiva)	Especifica a porta de destino do fluxo. Se houver várias portas de destino associadas a este fluxo, este campo especificará o termo Várias e o número de portas.
Rede de origem (contagem exclusiva)	Especifica a rede de origem do fluxo. Se houver várias redes de origem associadas a este fluxo, este campo especificará o termo Várias e o número de redes.
Rede de destino (contagem exclusiva)	Especifica a rede de destino do fluxo. Se houver várias redes de destino associadas a este fluxo, este campo especificará o termo Várias e o número de redes.
Aplicativo (contagem exclusiva)	Especifica o aplicativo detectado dos fluxos. Se houver vários aplicativos associados a este fluxo, este campo especificará o termo Vários e o número de aplicativos.
Bytes de origem (soma)	Especifica o número de bytes de origem.
Bytes de destino (soma)	Especifica o número de bytes do destino.
Bytes Totais (soma)	Especifica o número total de bytes associados ao fluxo.
Pacotes de origem (soma)	Especifica o número de pacotes da origem.
Pacotes de origem (soma)	Especifica o número de pacotes da origem.
Pacotes de origem (soma)	Especifica o número de pacotes da origem.
Pacotes de destino (soma)	Especifica o número de pacotes do destino.
Total de pacotes (soma)	Especifica o número total de pacotes associado ao fluxo.
Contagem	Especifica o número de fluxos enviados ou recebidos.

## Procedimento

1. Clique na guia **Atividade de rede**.
2. Na caixa de listagem **Visualização**, selecione o prazo que você deseja exibir.
3. Na caixa de listagem **Exibir**, selecione o parâmetro no qual você deseja agrupar os fluxos. Consulte a Tabela 2. Os grupos de fluxo são listados. Para obter mais informações sobre os detalhes do grupo de fluxo. Consulte a Tabela 1.
4. Para visualizar a página Lista de fluxos para um grupo, clique duas vezes no grupo de fluxo que você deseja investigar. A página Lista de fluxos não retém as configurações de gráfico que você pode ter definido na guia **Atividade de rede**. Para obter mais informações sobre o parâmetro da Lista de Fluxos, consulte a Tabela 2.
5. Para visualizar os detalhes de um fluxo, clique duas vezes no fluxo que você deseja investigar. Para obter mais informações sobre a página de detalhes do fluxo, consulte a Tabela 1.

## Detalhes do fluxo

É possível visualizar uma lista de fluxos em vários modos, incluindo modo de fluxo ou grupos de fluxo. Em qualquer modo escolhido para visualizar fluxos, é possível localizar e visualizar os detalhes de um único fluxo.

A página de detalhes do fluxo fornece as seguintes informações:

**Tabela 26. Detalhes do fluxo**

Parâmetro	Descrição
<b>Informações de fluxo</b>	
Protocolo	Especifica o protocolo que está associado a este fluxo.  Para obter mais informações sobre protocolos, consulte o <i>IBM Security QRadar Application Configuration Guide</i> .
Aplicativo	Especifica o aplicativo detectado do fluxo. Para obter mais informações sobre detecção do aplicativo, consulte o <i>IBM Security QRadar Application Configuration Guide</i> .
Magnitude	Especifica a magnitude deste fluxo. Para obter mais informações sobre magnitude, consulte o Glossário.
Relevância	Especifica a relevância deste fluxo. Para obter mais informações sobre relevância, consulte o Glossário.

Tabela 26. Detalhes do fluxo (continuação)

Parâmetro	Descrição
Gravidade	Especifica a severidade deste fluxo. Para obter mais informações sobre a severidade, consulte o Glossário.
Credibilidade	Especifica a credibilidade deste fluxo. Para obter mais informações sobre credibilidade, consulte o Glossário.
Horário do Primeiro Pacote	Especifica o horário de início do fluxo, conforme relatado pela fonte de fluxo.  Para obter mais informações sobre origens de fluxo, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Horário do Último Pacote	Especifica o horário de encerramento do fluxo, conforme relatado pela fonte de fluxo.
Horário do Armazenamento	Especifica o horário em que o fluxo foi armazenado no banco de dados do QRadar.
Nome do Evento	Especifica o nome normalizado do fluxo.
Categoria de Nível Baixo	Especifica a categoria de nível inferior deste fluxo.  Para obter mais informações sobre categorias, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Descrição do Evento	Especifica uma descrição do fluxo, se disponível.
<b>Informações de origem e destino</b>	
IP de Origem	Especifica o endereço IP de origem do fluxo.
IP de Destino	Especifica o endereço IP de destino do fluxo.
Nome do Ativo-fonte	Especifica o nome do ativo-fonte do fluxo. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos.
Nome do Ativo de Destino	Especifica o nome do ativo de destino do fluxo. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos.
Origem de IPv6	Especifica o endereço IPv6 da origem do fluxo.
Destino de IPv6	Especifica o endereço IPv6 do destino do fluxo.
Porta de origem	Especifica a porta de origem do fluxo.
Porta de Destino	Especifica a porta de destino do fluxo.
QoS de Origem	Especifica o nível de serviço do QoS do fluxo de origem.
QoS de Destino	Especifica o nível de QoS de serviço para o fluxo de destino.
ASN de Origem	Especifica o número ASN de origem. <b>Nota:</b> Se este fluxo possuir registros duplicados a partir de várias origens de fluxo, os números ASN de origem correspondentes serão listados.
ASN de Destino	Especifica o número ASN de destino. <b>Nota:</b> Se este fluxo possuir registros duplicados a partir de várias origens de fluxo, os números ASN de destino correspondentes serão listados.
If Index de Origem	Especifica o número IFIndex de origem. <b>Nota:</b> Se este fluxo tiver registros duplicados a partir de várias origens de fluxo, os números IFIndex de origem correspondentes serão listados.
If Index de Destino	Especifica o número IFIndex de destino. <b>Nota:</b> Se este fluxo tiver registros duplicados a partir de várias origens de fluxo, os números IFIndex de origem correspondentes serão listados.
Carga Útil de Origem	Especifica a contagem de pacotes e bytes da carga útil de origem.
Carga Útil de Destino	Especifica a contagem de pacotes e bytes da carga útil de destino.
<b>Informações de carga útil</b>	
Carga Útil de Origem	Especifica o conteúdo de carga útil de origem do fluxo. Este campo oferece três formatos para visualizar a carga útil: <ul style="list-style-type: none"> <li>• Formato de Transformação Universal (UTF) - Clique em UTF.</li> <li>• Hexadecimal - Clique em HEX.</li> <li>• Base64 - Clique em Base64.</li> </ul> <b>Nota:</b> Se o seu fluxo de origem for Netflow v9 ou IPFIX, os campos não analisados a partir dessas origens poderão ser exibidos no campo <b>Carga útil de origem</b> . O formato do campo não analisado é <name>=<value>. Por exemplo, <code>MN_TTL=x</code>
Carga Útil de Destino	Especifica o conteúdo de carga útil de destino do fluxo. Este campo oferece três formatos para visualizar a carga útil: <ul style="list-style-type: none"> <li>• Formato de Transformação Universal (UTF) - Clique em UTF.</li> <li>• Hexadecimal - Clique em HEX.</li> <li>• Base64 - Clique em Base64.</li> </ul>
<b>Informações adicionais</b>	

Tabela 26. Detalhes do fluxo (continuação)

Parâmetro	Descrição
Tipo de Fluxo	Especifica o tipo de fluxo. Tipos de fluxo são medidos pela proporção de atividade recebida para atividade de saída. Tipos de fluxo incluem: <ul style="list-style-type: none"> <li>• Padrão - Tráfego bidirecional</li> <li>• Tipo A – Único para muitos (unidirecional)</li> <li>• Tipo B – Muitos para único (unidirecional)</li> <li>• Tipo C – Único para único (unidirecional)</li> </ul>
Direção de Fluxo	Especifica a direção do fluxo. As direções de fluxo incluem: <ul style="list-style-type: none"> <li>• L2L - Tráfego interno de uma rede local para outra rede local.</li> <li>• L2R - Tráfego interno de uma rede local para uma rede remota.</li> <li>• R2L - Tráfego interno de uma rede remota para uma rede local.</li> <li>• R2R - Tráfego interno de uma rede remota para outra rede remota.</li> </ul>
Regras Customizadas	Especifica as regras customizadas que correspondem a este fluxo.  Para obter mais informações sobre as regras, consulte o <i>IBM Security QRadar SIEM Administration Guide</i> .
Regras Customizadas Parcialmente Correspondidas	Especifica regras customizadas que correspondem parcialmente a este fluxo.
Origem/Interface de Fluxo	Especifica o nome da fonte de fluxo do sistema que detectou o fluxo. <b>Nota:</b> Se este fluxo possuir registros duplicados a partir de várias origens de fluxo, as origens de fluxo correspondentes serão listadas.
Anotações	Especifica a anotação ou as notas deste fluxo. Anotações são descrições de texto que as regras podem incluir automaticamente em fluxos como parte da resposta da regra.

## Barra de ferramenta de detalhes do fluxo

A barra de ferramentas de detalhes do fluxo fornece várias funções.

A barra de ferramentas de detalhes do fluxo fornece as seguintes funções

Tabela 27. Descrição da barra de ferramentas de detalhes do fluxo

Função	Descrição
Retornar para resultados	Clique em <b>Retornar para resultados</b> para retornar para a lista de fluxos.
Extrair Propriedade	Clique em <b>Extrair propriedade</b> para criar uma propriedade de fluxo customizada do fluxo selecionado. Para obter mais informações, consulte Propriedades de fluxo e de evento customizado.
Positivo Falso	Clique em <b>Positivo falso</b> para abrir a janela Ajuste de positivo falso, o qual permite que você ajuste os fluxos que são conhecidos por serem positivos falsos de criação de crimes. Esta opção está desativada no modo de fluxo. Consulte Exportando fluxos.
Anterior	Clique em <b>Anterior</b> para visualizar o fluxo anterior na lista de fluxo.
Avançar	Clique em <b>Avançar</b> para visualizar o próximo fluxo na lista de fluxo.
Imprimir	Clique em <b>Imprimir</b> para imprimir os detalhes do fluxo.
Ofensa	Se a <b>Ofensa</b> estiver disponível, clique para visualizar a página Resumo de Ofensa.

## Ajustando falsos positivos

Você pode usar a função Ajuste Positivo Falso para evitar que fluxos de falsos positivos criem ofensas. Você pode ajustar fluxos de falsos positivos da lista de fluxo ou da página de detalhes de fluxo.

### Sobre Esta Tarefa

**Nota:** Você pode ajustar fluxos falsos positivos da página de resumo ou detalhes.

Você deve ter as permissões apropriadas para criar regras customizadas para ajustar falsos positivos. Para obter mais informações sobre falsos positivos, consulte o Glossário.

### Procedimento

1. Clique na guia **Atividade de rede**.
2. Opcional. Se você estiver visualizando os fluxos em modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Selecione o fluxo que você deseja ajustar.
4. Clique em **Positivo falso**.
5. Na área de janela de Propriedade de Evento/Fluxo na janela Positivo falso, selecione uma das opções a seguir:
  - Evento/Fluxo(s) com um QID específico de <Event>
  - Qualquer Evento/Fluxo com uma categoria de nível inferior de <Event>
  - Qualquer Evento/Fluxo com uma categoria de alto nível de <Event>
6. Na área de janela Direção do Tráfego, selecione uma das seguintes opções:
  - <Endereço IP de Origem> para <Endereço IP de Destino>
  - <Endereço IP de Origem> para qualquer Destino
  - Qualquer Origem para <Endereço IP de Destino>
  - Qualquer Origem para qualquer Destino
7. Clique em **Ajustar**.

---

## Exportando fluxos

Você pode exportar os fluxos no formato Linguagem de Marcação Extensível (XML) ou Valores Separados por Vírgulas (CSV). A duração de tempo necessária para exportar seus dados depende do número de parâmetros especificados.

### Procedimento

1. Clique na guia **Atividade de rede**.
2. Opcional. Se você estiver visualizando os fluxos em modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Na caixa de listagem **Ações**, selecione uma das opções a seguir:
  - **Exportar para XML > Colunas visíveis** – selecione essa opção para exportar somente as colunas visíveis na guia Atividade de log. Essa é a opção recomendada.
  - **Exportar para XML > Exportação integral (todas as colunas)** – selecione essa opção para exportar todos os parâmetros de fluxo. Uma exportação integral pode demorar um longo período de tempo para ser concluída.
  - **Exportar para CSV > Colunas visíveis** – selecione essa opção para exportar somente as colunas visíveis na guia Atividades de log. Essa é a opção recomendada.
  - **Exportar para CSV > Exportação integral (todas as colunas)** – selecione essa opção para exportar todos os parâmetros de fluxo. Uma exportação integral pode demorar um longo período de tempo para ser concluída.
4. Se você deseja continuar suas atividades, clique em **Notificar quando estiver pronto**.

## Resultados

Quando a exportação for concluída, você receberá uma notificação que a exportação foi concluída. Se você não selecionou o ícone **Notificar quando estiver pronto**, a janela Status será exibida.



---

## Capítulo 7. Gerenciamento de gráfico

É possível visualizar seus dados usando várias opções de configuração de gráfico diferentes.

Usando os gráficos nas guias **Atividade de log** e **Atividade de rede**, é possível visualizar seus dados usando várias opções de configuração do gráfico.

---

### Gerenciamento de gráfico

É possível usar várias opções de configuração do gráfico para visualizar seus dados.

Se for selecionado um prazo ou uma opção de agrupamento para visualizar seus dados, os gráficos serão exibidos acima da lista de evento ou de fluxo.

Os gráficos não serão exibidos quando estiverem no modo de fluxo.

É possível configurar um gráfico para selecionar quais dados deseja criar um gráfico. É possível configurar gráficos independentes um do outro para exibir seus resultados de procura de diferentes perspectivas.

Os tipos de gráfico incluem:

- Gráfico de barras – Exibe dados em um gráfico de barras. Essa opção está disponível somente para eventos agrupados.
- Gráfico de pizza – Exibe os dados em um gráfico de pizza. Essa opção está disponível somente para eventos agrupados.
- Tabela – Exibe os dados em uma tabela. Essa opção está disponível somente para eventos agrupados.
- Séries temporais – Exibe um gráfico de linha interativo que representa os registros que são correspondidos por um intervalo de tempo especificado. Para obter informações sobre como configurar os critérios de procura de série temporal, consulte Visão geral do gráfico de série temporal.

Após configurar um gráfico, as configurações do gráfico serão retidas quando você:

- Alterar sua visualização usando a caixa de listagem **Exibir**.
- Aplicar um filtro.
- Salvar seus critérios de procura.

Suas configurações de gráfico não serão retidas quando você:

- Iniciar uma nova procura.
- Acessar uma procura rápida.
- Visualizar resultados agrupados em uma janela de ramificação.
- Salvar resultados da procura.

**Nota:** Se o navegador da web Mozilla Firefox for usado e uma extensão de navegador bloqueador de anúncio for instalada, os gráficos não serão exibidos. Para exibir gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.

## Visão geral do gráfico de série temporal

Gráficos de série temporal são representações gráficas de sua atividade no decorrer do tempo.

Picos e vales que são exibidos nos gráficos representam atividade de volume alta e baixa. Gráficos de série temporais são úteis para tendência de dados a curto e longo prazo.

Usando gráficos de série temporal, é possível acessar, navegar e investigar atividade de rede ou de log a partir de várias visualizações e perspectivas.

**Nota:** Deve-se ter permissões de função apropriadas para gerenciar e visualizar gráficos de série temporal.

Para exibir gráficos de série temporal, é necessário criar e salvar uma procura que inclui séries temporais e opções de agrupamento. É possível salvar até 100 procuras de série temporal.

Procuras salvas de série temporal padrão são acessíveis a partir da lista de procuras disponíveis na página de procura de fluxo ou evento.

É possível identificar facilmente as procuras de série temporal salvas no menu **Procuras rápidas**, pois o nome de procura está anexado ao intervalo de tempo especificado nos critérios de procura.

Se seus parâmetros de procura corresponderem a uma procura salva anteriormente para definição de coluna e as opções de agrupamento, um gráfico de série temporal poderá exibir automaticamente seus resultados da procura. Se um gráfico de série temporal não exibir automaticamente seus critérios de procura não salvos, nenhum critério de procura salvo anteriormente existirá para corresponder aos seus parâmetros de procura. Se isso ocorrer, você deverá ativar a captura de dados da série temporal e salvar seus critérios de procura.

É possível ampliar e verificar uma linha de tempo em um gráfico de série temporal para investigar a atividade. A tabela a seguir fornece funções que podem ser usadas para visualizar gráficos de série temporal.

*Tabela 28. Funções dos gráficos de séries temporais*

Função	Descrição
Exibir dados com mais detalhes	<p>Usando o recurso de zoom, é possível investigar segmentos de tempo menores do tráfego de evento.</p> <ul style="list-style-type: none"><li>• Mova o ponteiro do mouse sobre o gráfico e use o botão de rolagem do mouse para aumentar o gráfico (role o botão de rolagem do mouse para cima).</li><li>• Destaque a área do gráfico que deseja ampliar. Ao liberar o botão do mouse, o gráfico exibirá um segmento de tempo menor. Agora é possível clicar e arrastar o gráfico para verificar o gráfico.</li></ul> <p> Ao aumentar o gráfico de série temporal, o gráfico será atualizado para exibir um segmento de tempo menor.</p>
Visualizar um período de tempo maior de dados	<p>Usando o recurso de zoom, é possível investigar segmentos de tempo maior ou retornar para o intervalo de tempo máximo. É possível expandir um intervalo de tempo usando uma das seguintes opções:</p> <ul style="list-style-type: none"><li>• Clique em Reconfiguração de zoom no canto superior esquerdo do gráfico.</li><li>• Mova o ponteiro do mouse sobre o gráfico e, em seguida, use o botão de roda do mouse para expandir a visualização (role o botão de roda do mouse para baixo).</li></ul>



Tabela 28. Funções dos gráficos de séries temporais (continuação)

Função	Descrição
Verifique o gráfico	Quando tiver ampliado um gráfico de série temporal, será possível clicar e arrastar o gráfico para a esquerda ou para a direita para verificar a linha.

---

## Legendas do gráfico

Cada gráfico fornece uma legenda, que é uma referência visual para ajudá-lo a associar os objetos de gráfico aos parâmetros que eles representam.

Usando o recurso de legenda, é possível executar as seguintes ações:

- Mova o ponteiro do mouse sobre um item de legenda ou sobre bloco de cor da legenda para visualizar mais informações sobre os parâmetros que ele representa.
- Clique com o botão direito no item de legenda para investigar melhor o item.
- Clique em um item de legenda de um gráfico de barras ou de pizza para ocultar o item no gráfico. Clique no item de legenda novamente para mostrar o item oculto. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item.
- Clique em **Legenda** ou na seta ao lado dela, se desejar remover a legenda da sua exibição de gráfico.

---

## Configurando gráficos

Você pode usar as opções de configurações para alterar o tipo de gráfico, o tipo de objeto que você deseja registrar em gráfico e o número de objetos representados no gráfico. Para os gráficos de séries temporais, você também pode selecionar um intervalo de tempo e ativar a captura de dados de séries temporais.

### Antes de Iniciar

Os gráficos não são exibidos quando você visualiza os eventos ou fluxos no modo Tempo Real (fluxo). Para exibir os gráficos, você deve acessar a guia **Atividade do log** ou **Atividade de rede** e escolher uma das opções a seguir:

- Selecione as opções nas caixas de listagem **Visualizar** e **Exibir** e, em seguida, clique em **Salvar Critérios** na barra de ferramentas. Consulte Salvando evento e critérios de procura de fluxo.
- Na barra de ferramentas, selecione uma procura salva na lista **Procura rápida**.
- Execute uma procura agrupada, e, em seguida, clique em **Salvar Critérios** na barra de ferramentas.

Se você planeja configurar um gráfico de séries temporais, assegure-se de que os critérios de procura salvos estejam agrupados e especifiquem um intervalo de tempo.

### Sobre Esta Tarefa

Os dados podem ser acumulados para que, ao executar uma procura de séries temporais, um cache de dados esteja disponível para exibir dados para o período de tempo anterior. Após ativar a captura de dados das séries temporais para um parâmetro selecionado, um asterisco (\*) será exibido ao lado do parâmetro na caixa de listagem Value to Graph.

## Procedimento

1. Clique na guia **Atividade de log** ou **Atividade de rede**.
2. Na área de janela Gráficos, clique no ícone **Configurar**.
3. Configure valores para os parâmetros a seguir:

Opção	Descrição
<b>Parâmetro</b>	Descrição
<b>Value to Graph</b>	Na caixa de listagem, selecione o tipo de objeto que você deseja que apareça no eixo Y do gráfico.  As opções incluem todos os eventos normalizados e customizados ou parâmetros de fluxo incluídos em seus parâmetros de procura.
<b>Display Top</b>	Na caixa de listagem, selecione o número de objetos que você deseja visualizar no gráfico. O padrão é 10. A representação de gráfico com mais de 10 itens pode fazer com que os dados de gráfico fiquem ilegíveis.
<b>Tipo de gráfico</b>	Na caixa de listagem, selecione o tipo de gráfico que você deseja visualizar.  Se o gráfico de barras, pizza ou tabela for baseado em critérios de procura salvos com um intervalo de tempo de mais de 1 hora, você deverá clicar em <b>Atualizar detalhes</b> para atualizar o gráfico e preencher os detalhes do evento
<b>Capturar Dados de Série Temporal</b>	Selecione essa caixa de seleção se você deseja ativar a captura de dados das séries temporais. Ao selecionar essa caixa de seleção, o recurso de gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, essa opção está desativada.  Essa opção está apenas disponível em gráficos Séries Temporais.
<b>Intervalo de tempo</b>	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar.  Essa opção está apenas disponível em gráficos Séries Temporais.

4. Se você selecionou a opção do gráfico **Séries temporais** e ativou a opção **Capturar dados de séries temporais**, clique em **Salvar critérios** na barra de ferramentas.
5. Para visualizar a lista de eventos ou fluxos, se seu intervalo de tempo for maior que 1 hora, clique em **Atualizar detalhes**.

---

## Capítulo 8. Procuras de dados

Nas guias **Log de atividade**, **Atividade de rede** e **Ofensas**, é possível procurar eventos, fluxos e ofensas usando critérios específicos.

É possível criar uma nova procura ou carregar um conjunto de critérios de pesquisa salvo anteriormente. É possível selecionar, organizar e agrupar as colunas de dados a serem exibidas nos resultados da procura

---

### Procuras de eventos e de fluxo

É possível executar procuras nas guias **Atividade de log** e **Atividade de rede**.

Após executar uma procura, é possível salvar os critérios de procura e os resultados da procura.

### Procurando por itens que correspondem aos seus critérios

É possível procurar por dados que correspondem ao seu critério de procura.

#### Sobre Esta Tarefa

Como o banco de dados inteiro é procurado, as procuras podem demorar muito tempo, dependendo do tamanho do seu banco de dados.

É possível usar o parâmetro de procura **Quick Filter** para procurar por itens que correspondem à sua sequência de caracteres de texto na carga útil do evento.

Para obter mais informações sobre como usar o parâmetro Quick Filter, consulte **Sintaxe de Filtro Rápido (eventos)** ou **Sintaxe de Filtro Rápido (fluxos)**.

A tabela a seguir descreve as opções de procura que você pode usar para procurar dados de evento e fluxo:

*Tabela 29. Opções da pesquisa*

Opções	Descrição
Grupo	Selecione um Grupo de Procura de fluxo ou grupo de procura de evento para visualizar na lista <b>Procuras salvas disponíveis</b> .
Digitar Procura Salva ou Selecionar a partir da Lista	Digite o nome de uma procura salva ou uma palavra-chave para filtrar a lista de <b>Procuras salvas disponíveis</b> .
Procuras Salvas Disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você use as opções <b>Procura salva de tipo ou grupo</b> ou <b>Selecionar a partir da lista</b> para aplicar um filtro na lista. É possível selecionar uma procura salva nessa lista para exibir ou editar.
Procura	O ícone <b>Procurar</b> está disponível em várias áreas de janela na página de procura. Você pode clicar em Procurar quando você terminar de configurar a procura e desejar visualizar os resultados.
Inclua em Minhas Procuras Rápidas	Selecione essa caixa de seleção para incluir esta procura em seu menu <b>Procura rápida</b> .
Incluir em Meu Painel	Selecione esta caixa de seleção para incluir os dados da procura salva na guia <b>Painel</b> . Para obter mais informações sobre a guia <b>Painel</b> , consulte Gerenciamento de painel. <b>Nota:</b> Esse parâmetro só será exibido se a procura for agrupada.
Defina como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esta pesquisa com todos os outros usuários.

Tabela 29. Opções da pesquisa (continuação)

Opções	Descrição
Tempo Real (fluxo)	Exibe os resultados no modo de fluxo. Para obter mais informações sobre o modo de fluxo, consulte Visualizando eventos de fluxo. <b>Nota:</b> Quando o Tempo Real (fluxo) estiver ativado, você não conseguirá agrupar seus resultados da procura. Se você selecionar qualquer opção de agrupamento na área de janela Definição de Coluna, uma mensagem de erro será aberta.
Último Intervalo (atualização automática)	Exibe os resultados da procura no modo de atualização automática.  No modo de atualização automática, as guias <b>Atividade do log</b> e <b>Atividade de rede</b> atualizam em intervalos de um minuto para exibir as informações mais recentes.
Recente	Selecione um intervalo de tempo predefinido para sua procura. Depois de selecionar essa opção, você deve selecionar uma opção de intervalo de tempo na caixa de listagem.
Intervalo Específico	Selecione um intervalo de tempo customizado para sua procura. Após selecionar essa opção, deve-se selecionar o intervalo de data e hora nos calendários de <b>Horário de início</b> e <b>Horário de encerramento</b> .
Acumulação de Dados	Esta área de janela será exibida apenas quando você carregar uma procura salva.  Ativar contagens exclusivas em dados acumulados que são compartilhados com muitas outras procuras e relatórios salvos poderá diminuir o desempenho do sistema.  Quando você carrega uma procura salva, esta área de janela exibe as seguintes opções: <ul style="list-style-type: none"> <li>• Se nenhum dado estiver acumulando para esta procura salva, a mensagem de informação a seguir será exibida: Dados não estão sendo acumulados para esta procura.</li> <li>• Se os dados forem acumulando para esta procura salva, as seguintes opções serão exibidas: <ul style="list-style-type: none"> <li>– <b>colunas</b> – Quando você clica ou passa o mouse sobre esse link, uma lista das colunas que estão acumulando dados é aberta.</li> <li>– <b>Ativar contagens exclusivas/desativar contagens exclusivas</b> – Este link permite que você ative ou desative os resultados da procura para exibir evento exclusivo e contagens de fluxo em vez de média de contagens ao longo do tempo. Depois de clicar no link <b>Ativar contagens exclusivas</b>, uma caixa de diálogo é aberta e indica quais procuras e relatórios salvos compartilham os dados acumulados.</li> </ul> </li> </ul>
Filtros Atuais	Esta lista exibe os filtros que são aplicados a esta procura. As opções para incluir um filtro estão localizadas acima da lista <b>Filtros atuais</b> .
Salve os resultados quando a procura for concluída	Selecione esta caixa de seleção para salvar e nomear os resultados da procura.
Exibir	Selecione esta lista para especificar uma coluna predefinida que está configurada para exibir nos resultados da procura.
Digitar Coluna ou Selecionar a partir da Lista	Você pode usar o campo para filtrar as colunas que são listadas 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 colunas. Por exemplo, digite <b>D</b> ispositivo para exibir uma lista de colunas que incluem <b>D</b> ispositivo no nome da coluna.
Colunas Disponíveis	Essa lista exibe as colunas disponíveis. Colunas que estão atualmente em uso para esta procura salva são realçadas e exibidas na lista <b>Colunas</b> .
Inclua e remova ícones de coluna (conjunto superior)	Use o conjunto de ícones na parte superior para customizar a lista <b>Agrupado por</b> . <ul style="list-style-type: none"> <li>• <b>Incluir coluna</b> - Selecione uma ou mais colunas na lista <b>Colunas disponíveis</b> e clique no ícone <b>Incluir coluna</b>.</li> <li>• <b>Remover coluna</b> – Selecione uma ou mais colunas na lista <b>Agrupar por</b> e clique no ícone <b>Remover coluna</b>.</li> </ul>
Incluir e remover os ícones da coluna (conjunto inferior)	Use o conjunto inferior do ícone para customizar a lista <b>Colunas</b> . <ul style="list-style-type: none"> <li>• <b>Incluir coluna</b> – Selecione uma ou mais colunas da lista Colunas Disponíveis e clique no ícone <b>Incluir coluna</b>.</li> <li>• <b>Remover coluna</b> – Selecione uma ou mais colunas da lista Colunas e clique no ícone <b>Remover coluna</b>.</li> </ul>

Tabela 29. Opções da pesquisa (continuação)

Opções	Descrição
Agrupar Por	<p>Esta lista especifica as colunas nas quais a procura salva agrupa os resultados. Use as opções a seguir para customizar adicionalmente a lista Agrupar Por:</p> <ul style="list-style-type: none"> <li>• Mover para Cima – Selecione uma coluna e mova-a para cima através da lista de prioridade usando o ícone <b>Mover para cima</b>.</li> <li>• Mover para Baixo – Selecione uma coluna e mova-o para baixo através da lista de prioridade usando o ícone <b>Mover para baixo</b>.</li> </ul> <p>A lista de prioridade especifica em qual ordem os resultados são agrupados. Os resultados da procura são agrupados pela primeira coluna na lista <b>Agrupado por</b> e, em seguida, agrupados pela próxima coluna na lista.</p>
Colunas	<p>Especifica colunas que são escolhidas para a procura. Você pode selecionar mais colunas na lista <b>Colunas disponíveis</b>. Você pode customizar ainda mais a lista <b>Colunas</b> usando as seguintes opções:</p> <ul style="list-style-type: none"> <li>• <b>Mover para cima</b> – Move a coluna selecionada para cima na lista de prioridades.</li> <li>• <b>Mover para baixo</b> – Move o próprio selecionado na lista de prioridades.</li> </ul> <p>Se o tipo de coluna for numérico ou baseado em tempo e houver uma entrada na lista <b>Agrupar por</b>, então a coluna incluirá uma caixa de listagem. Use a caixa de listagem para escolher como deseja agrupar a coluna.</p> <p>Se o tipo de coluna for um grupo, a coluna incluirá uma caixa de listagem para selecionar quantos níveis você deseja incluir para o grupo.</p>
Classificar por	<p>Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura. Em seguida, a partir da segunda caixa de listagem, selecione a ordem que você deseja exibir para os resultados de procura. As opções incluem <b>Decrescente</b> e <b>Crescente</b>.</p>
Limite de Resultados	<p>Você pode especificar o número de linhas que uma pesquisa retorna na janela Editar Procura. O campo <b>Limitar resultados</b> também aparece na janela Resultados.</p> <ul style="list-style-type: none"> <li>• Para uma procura salva, o limite será armazenado na procura salva e replicado no carregamento da procura.</li> <li>• Ao classificar em uma coluna no resultado de procura que tem limite de linha, a classificação será feita dentro das linhas limitadas mostradas na grade de dados.</li> <li>• Para obter um agrupado por procura com gráfico de série temporal ligado, o limite da linha somente se aplica à grade de dados. O suspenso <b>Parte superior</b> no gráfico de série temporal ainda controla quantas séries de tempo são desenhadas no gráfico.</li> </ul>

## Procedimento

- Escolha uma das opções a seguir:
  - Para procurar eventos, clique na guia **Atividade do log**.
  - Para fluxos de procura, clique na guia **Atividade de rede**.
- Na caixa de listagem **Procurar**, selecione **Nova procura**.
- Para selecionar uma procura salva anteriormente:
  - Escolha uma das seguintes opções: Na lista de Procuras Salvas Disponíveis, selecione a procura salva que você deseja carregar. No campo Digital Procura Salva ou Selecionar da Lista, digite o nome da procura que você deseja carregar.
  - Clique em **Carregar**.
  - Na área de janela Editar Procura, selecione as opções que você deseja para essa procura. Consulte a Tabela 1.
- Para criar uma procura, na área de janela do Intervalo de Tempo, selecione as opções para o intervalo de tempo que você deseja capturar para essa procura.
- Opcional. Na área de janela de Acumulação de Dados, ative contagens exclusivas:

- a. Clique em **Ativar contagens exclusivas**.
  - b. Na janela Aviso, leia a mensagem de aviso e clique em **Continuar**. Para obter mais informações sobre a ativação de conta exclusiva, consulte a Tabela 1.
6. Na área de janela Parâmetros de Procura, defina seus critérios de procura:
- a. Na primeira caixa de listagem, selecione um parâmetro que você deseja procurar. Por exemplo, Dispositivo, Porta de Origem ou Nome do Evento.
  - b. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura.
  - c. No campo de entrada, digite informações específicas que estão relacionadas ao seu parâmetro de procura.
  - d. Clique em **Incluir filtro**.
  - e. Repita as etapas de a a d para cada filtro que você deseja incluir nos critérios de procura.
7. Opcional. Para salvar automaticamente os resultados da procura quando a procura for concluída, selecione a caixa de seleção **Salvar resultados quando a procura for concluída** e, em seguida, digite um nome para a procura salva.
8. Na área de janela Definição de Coluna, defina o layout de colunas e colunas que você deseja usar para visualizar os resultados:
- a. Na caixa de listagem **Exibir**, selecione a coluna pré-configurada que está configurada para associar com essa pesquisa.
  - b. Clique na seta ao lado de **Definição de visualização avançada** para exibir os parâmetros de procura avançada.
  - c. Customize as colunas a serem exibidas nos resultados da procura. Consulte a Tabela 1.
  - d. Opcional. No campo **Limite de resultados**, digite o número de linhas que você deseja que a procura retorne.
9. Clique em **Filtrar**.

## Resultados

O status **Em progresso** (<percent>%Complete) será exibido no canto superior direito.

.

Ao visualizar resultados da procura parcial, o mecanismo de procura funciona em segundo plano para concluir a procura e atualiza os resultados parciais para atualizar sua visualização.

Quando a procura estiver completa, o status **Concluído** será exibido no canto superior direito.

## Salvando critérios de procura

Você pode salvar os critérios de procura configurados para que você possa reutilizar os critérios e usar os critérios de procura salvos em outros componentes, como relatórios. Os critérios de procura salvos não expiram.

## Sobre Esta Tarefa

Se você especificar um intervalo de tempo para a sua procura, então o nome da procura será anexado ao intervalo de tempo especificado. Por exemplo, uma

procura salva nomeada Explora por Origem com um intervalo de tempo de Últimos 5 minutos torna-se Explora por Origem – Últimos 5 minutos.

Se você alterar um conjunto de colunas em uma procura salva anteriormente e, em seguida, salvar os critérios de procura usando o mesmo nome, as acumulações anteriores para os gráficos de séries temporais serão perdidas.

## Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Execute uma procura.
3. Clique em **Salvar critérios**.
4. Insira valores para os parâmetros:

Opção	Descrição
Parâmetro	Descrição
Nome da Procura	Digite o nome exclusivo que você deseja designar a esses critérios de procura.
Designar procura a grupo(s)	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, essa procura salva será designada ao grupo Outros por padrão. Para obter mais informações, consulte Gerenciando grupos de procuras.
Gerenciar Grupos	Clique em <b>Gerenciar grupos</b> para gerenciar grupos de procuras. Para obter mais informações, consulte Gerenciando grupos de procuras.
Opções de amplitude de tempo:	<p>Escolha uma das opções a seguir:</p> <ul style="list-style-type: none"> <li>• <b>Tempo real (fluxo)</b> – selecione essa opção para filtrar os resultados da procura durante o modo de fluxo.</li> <li>• <b>Último intervalo (atualização automática)</b> – selecione essa opção para filtrar os resultados da procura durante o modo de atualização automática. As guias <b>Atividade de log</b> e <b>Atividade de rede</b> são atualizadas em intervalos de um minuto para exibir as informações mais recentes.</li> <li>• <b>Recente</b> – selecione essa opção e, dessa caixa de listagem, selecione o intervalo de tempo ao qual você deseja filtrar.</li> <li>• <b>Intervalo específico</b> – selecione essa opção e, no calendário, selecione a data e o intervalo de tempo para o qual você deseja filtrar.</li> </ul>
Incluir em minhas procuras rápidas	Selecione essa caixa de seleção para incluir essa procura na caixa de listagem <b>Procura rápida</b> na barra de ferramentas.

Opção	Descrição
Incluir em Meu Painel	Selecione esta caixa de seleção para incluir os dados da procura salva na guia <b>Painel</b> . Para obter mais informações sobre a guia <b>Painel</b> , consulte Gerenciamento de painel. <b>Nota:</b> Esse parâmetro só será exibido se a procura for agrupada.
Definir como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

5. Clique em OK.

## Procuras de crime

É possível procurar ofensas usando critérios específicos para exibir ofensas que correspondem ao critério de procura em uma lista de resultados.

É possível criar uma nova procura ou carregar um conjunto de critérios de pesquisa salvo anteriormente.

## Procurando ofensas nas páginas Minhas Ofensas e Todas as Ofensas

Nas páginas Minhas Ofensas e Todas as Ofensas da guia **Ofensa**, é possível procurar por ofensas que correspondam aos seus critérios.

### Sobre Esta Tarefa

A tabela a seguir descreve as opções de procura que você pode usar para procurar dados de crime nas páginas **Minhas ofensas** e **Todas as ofensas**.

Para obter informações sobre categorias, consulte o Guia de Administração do *IBM SecurityQRadar SIEM*.

*Tabela 30. Opções de procura de página Minhas Ofensas e Todas as Ofensas*

Opções	Descrição
Grupo	Esta caixa de listagem permite que você selecione um crime de Grupo de Procura para visualizar na lista <b>Procuras salvas disponíveis</b> .
Digitar procura salva ou selecionar a partir da lista	Este campo permite que você digite o nome de uma procura salva ou uma palavra-chave para filtrar a lista de <b>Procuras salvas disponíveis</b> .
Procuras salvas disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você aplique um filtro à lista usando a Seleção ou Procura salva de tipo ou grupo a partir de opções de <b>Lista</b> . É possível selecionar uma procura salva nessa lista para exibir ou editar.
Todos os Crimes	Essa opção permite que você procure todas as ofensas independentemente do intervalo de tempo.
Recente	Esta opção permite que você selecione um intervalo de tempo predefinido que você deseja filtrar. Depois de selecionar essa opção, você deve selecionar uma opção de intervalo de tempo na caixa de listagem.



Tabela 30. Opções de procura de página Minhas Ofensas e Todas as Ofensas (continuação)

Opções	Descrição
Intervalo específico	Essa opção permite que você configure um intervalo de tempo customizado para sua procura. Depois de selecionar essa opção, você deve selecionar uma das opções a seguir. <ul style="list-style-type: none"> <li>• <b>Data de Início entre</b> – Selecione esta caixa de seleção para pesquisar ofensas que começaram durante um determinado período de tempo. Depois de selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.</li> <li>• <b>Último evento/fluxo entre</b> – Selecione esta caixa de seleção para procurar ofensas para as quais o último evento detectado ocorreu dentro de um determinado período de tempo. Depois de selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.</li> </ul>
Procura	O ícone <b>Procurar</b> está disponível em várias áreas de janela na página de procura. Você pode clicar em <b>Procurar</b> quando você terminar de configurar a procura e desejar visualizar os resultados.
ID do Crime	Nesse campo, você pode digitar o ID da Ofensa que você deseja procurar.
Descrição	Neste campo, você pode digitar a descrição que você deseja procurar.
Designado ao usuário	Nesta caixa de listagem, você pode selecionar o nome do usuário que você deseja procurar.
Orientação	Nesta caixa de listagem, você pode selecionar a direção da ofensa que você deseja procurar. As opções incluem: <ul style="list-style-type: none"> <li>• Local para Local</li> <li>• Local para Remoto</li> <li>• Remoto para Local</li> <li>• Remoto para Remoto</li> <li>• Local para Remoto ou Local</li> <li>• Remoto para Remoto ou Local</li> </ul>
IP de origem	Neste campo, você pode digitar o endereço IP de origem ou o intervalo do CIDR que você deseja procurar.
IP de destino	Neste campo, você pode digitar o endereço IP de destino ou intervalo do CIDR que você deseja procurar.
Magnitude	Nesta caixa de listagem, você pode especificar uma magnitude e, em seguida, selecionar para exibir apenas as ofensas com uma magnitude que seja igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Gravidade	Nesta caixa de listagem, você pode especificar uma gravidade e, em seguida, selecionar para exibir apenas as ofensas com uma gravidade que seja igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Credibilidade	Nesta caixa de listagem, você pode especificar uma credibilidade e, em seguida, selecionar para exibir apenas as ofensas com uma credibilidade que seja igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Relevância	Nesta caixa de listagem, você pode especificar uma relevância e, em seguida, selecionar para exibir apenas as ofensas com uma relevância que seja igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Contém nome de usuário	Nesse campo, você pode digitar uma instrução de expressão regular (regex) para procurar ofensas contendo um nome de usuário específico. Ao definir padrões regex customizados, siga para regras regex conforme definidas pela linguagem de programação do Java™. Para obter mais informações, é possível consultar tutoriais regex disponíveis na web.
Rede de origem	Nesta caixa de listagem, você pode selecionar a rede de origem que você deseja procurar.
Rede de destino	Nesta caixa de listagem, você pode selecionar a rede de destino que você deseja procurar.
Categoria de alto nível	Nesta caixa de listagem, você pode selecionar a categoria de alto nível que você deseja procurar. .
Categoria de baixo nível	Nesta caixa de listagem, você pode selecionar a categoria de baixo nível que você deseja procurar.

Tabela 30. Opções de procura de página Minhas Ofensas e Todas as Ofensas (continuação)

Opções	Descrição
Exclusão	As opções nessa área de janela permitem que você exclua ofensas dos resultados da procura. As opções incluem: <ul style="list-style-type: none"> <li>• Crimes Ativos</li> <li>• Crimes Ocultos</li> <li>• Crimes Encerrados</li> <li>• Ofensas inativas</li> <li>• Ofensas Protegidas</li> </ul>
Fechar por usuário	Este parâmetro é exibido somente quando a caixa de seleção <b>Ofensas fechadas</b> estiverem limpas na área de janela Excluir.  Nesta caixa de listagem, você pode selecionar o nome do usuário que você deseja procurar ofensas fechadas ou selecionar Any para exibir todas as ofensas fechadas.
Motivo do fechamento	Este parâmetro é exibido somente quando a caixa de seleção <b>Ofensas fechadas</b> estiverem limpas na área de janela Excluir.  Nesta caixa de listagem, você pode selecionar um motivo pelo que você deseja procurar ofensas fechadas ou selecionar Any para exibir todas as ofensas fechadas.
Eventos	Nesta caixa de listagem, você pode especificar uma contagem de eventos e, em seguida, selecionar para exibir apenas ofensas com uma contagem de eventos que seja igual a, menor que ou maior que o valor configurado.
Fluxos	Nesta caixa de listagem, você pode especificar uma contagem de fluxo e, em seguida, selecionar para exibir apenas ofensas com uma contagem de fluxo que seja igual a, menor que ou maior que o valor configurado.
Total de eventos/fluxos	Nesta caixa de listagem, você pode especificar um evento total e uma contagem de fluxo e, em seguida, selecionar para exibir apenas ofensas com um evento total e uma contagem de fluxo que seja igual a, menor que ou maior que o valor configurado.
Destinos	Nesta caixa de listagem, você pode especificar uma contagem de endereço IP de destino e, em seguida, selecionar para exibir apenas ofensas com uma contagem do endereço IP de destino que seja igual a, menor que ou maior que o valor configurado.
Grupo de origens de log	Nesta caixa de listagem, você pode selecionar um grupo de origem de log que contém a origem de log que você deseja procurar. A caixa de listagem <b>Origem de log</b> exibe todas as origens de log que são designadas ao grupo de origem de log selecionado.
Origem de Log	Nesta caixa de listagem, você pode selecionar a origem do log que você deseja procurar.
Grupo de regras	Nesta caixa de listagem, você pode selecionar um grupo de regras que contém a regra de contribuição que você deseja procurar. A caixa de listagem <b>Regra</b> exibe todas as regras que são designadas ao grupo de regras selecionado.
Regra	Nesta caixa de listagem, você pode selecionar a regra de contribuição que você deseja procurar.
Tipo de Crime	Nesta caixa de listagem, você pode selecionar um tipo de crime que você deseja procurar. Para obter mais informações sobre as opções na caixa de listagem <b>Tipo de crime</b> , consulte a Tabela 2.

A tabela a seguir descreve as opções disponíveis na caixa de listagem **Tipo de crime**:

Tabela 31. Opções de tipo de crime

Tipos de crime	Descrição
Qualquer	Essa opção procura todas as origens de crime.
IP de origem	Para procurar por ofensas com um endereço IP de origem específica, você pode selecionar essa opção e, em seguida, digitar o endereço IP de origem que você deseja procurar.
IP de destino	Para procurar por ofensas com um endereço IP de destino específico, você pode selecionar essa opção, e, em seguida, digitar o endereço IP de destino que você deseja procurar.

Tabela 31. Opções de tipo de crime (continuação)

Tipos de crime	Descrição
Nome do evento	<p>Para procurar por ofensas com um nome de evento específico, você pode clicar no ícone <b>Navegar</b> para abrir o Navegador de Eventos e selecionar o nome do evento (QID) que você deseja procurar.</p> <p>Você pode procurar por um QID determinado usando uma das seguintes opções:</p> <ul style="list-style-type: none"> <li>Para procurar um QID por categoria, selecione a caixa de seleção <b>Procurar por categoria</b> e selecione a categoria de alto ou nível inferior nas caixas de listagem.</li> <li>Para procurar um tipo de origem de log QID, selecione a caixa de listagem de Tipo <b>Procurar origem de log</b> e selecione um tipo de origem de log da caixa de listagem <b>Tipo de origem de log</b>.</li> <li>Para procurar um QID por tipo de origem de log, selecione a caixa de seleção <b>Procurar por tipo de origem de log</b> e selecione um tipo de origem de log da caixa de listagem <b>Tipo de origem de log</b>.</li> <li>Para procurar um QID por nome, selecione a caixa de seleção <b>Procura de QID</b> e digite um nome no campo <b>QID/nome</b>.</li> </ul>
Nome de usuário	Para procurar por ofensas com um nome de usuário específico, você pode selecionar essa opção e, em seguida, digitar o nome do usuário que você deseja procurar.
Endereço MAC de origem	Para procurar por ofensas com um endereço MAC de origem específica, você pode selecionar essa opção e, em seguida, digitar o endereço MAC de origem que você deseja procurar.
Endereço MAC de destino	Para procurar por ofensas com um endereço MAC de destino específico, você pode selecionar essa opção e, em seguida, digitar o endereço MAC de destino que você deseja procurar.
Origem de Log	<p>Na caixa de listagem <b>Grupo de origem de log</b>, é possível selecionar o grupo de origem de log que contém a origem de log que você deseja procurar. A caixa de listagem <b>Origem de log</b> exibe todas as origens de log que são designadas ao grupo de origem de log selecionado.</p> <p>Na caixa de listagem <b>Origem de log</b>, selecione a origem do log que você deseja procurar.</p>
Nome do host	Para procurar por ofensas com um nome de host específico, você pode selecionar esta opção e, em seguida, digitar o nome do host que você deseja procurar.
Porta de origem	Para procurar por ofensas com uma porta de origem específica, você pode selecionar esta opção e, em seguida, digitar a porta de origem que você deseja procurar.
Porta de destino	Para procurar por ofensas com uma porta de destino específica, você pode selecionar esta opção e, em seguida, digitar a porta de destino que você deseja procurar.
IPv6 de origem	Para procurar por ofensas com um endereço IPv6 de origem específico, você pode selecionar essa opção e, em seguida, digitar o endereço IPv6 de origem que você deseja procurar.
IPv6 de destino	Para procurar por ofensas com um endereço IPv6 do destino específico, você pode selecionar essa opção e, em seguida, digitar o endereço IPv6 do destino que você deseja procurar.
ASN de origem	Para procurar por ofensas com um ASN de Origem específico, você pode selecionar a ASN de origem a partir da caixa de listagem <b>ASN de origem</b> .
ASN de destino	Para procurar por ofensas com um ASN de destino específico, você pode selecionar o ASN de destino da caixa de listagem <b>ASN de destino</b> .
Regra	Para procurar por ofensas que estão associadas a uma regra específica, você pode selecionar o grupo de regras que contém a regra que você deseja procurar da caixa de listagem <b>Grupo da regra</b> . A caixa de listagem <b>Grupo de regra</b> exibe todas as regras designadas ao grupo de regra selecionado. Na caixa de listagem <b>Regra</b> , selecione a regra que você deseja procurar.
ID do aplicativo	Para procurar por ofensas com um ID de aplicativo, você pode selecionar o ID do aplicativo da caixa de listagem <b>ID do aplicativo</b> .

## Procedimento

1. Clique na guia **Ofensas**.
2. Na caixa de listagem **Procurar**, selecione **Nova procura**.
3. Escolha uma das opções a seguir:
  - Para carregar uma procura salva anteriormente, acesse a Etapa 4.

- Para criar uma nova procura, acesse a Etapa 7.
4. Selecione uma pesquisa anteriormente salva usando uma das opções a seguir:
    - Na lista **Procuras salvas disponíveis**, selecione a procura salva que você deseja carregar.
    - No campo **Digitar procura salva** ou **Selecionar a partir da lista**, digite o nome da procura que você deseja carregar.
  5. Clique em **Carregar**.
  6. Opcional. Selecione a caixa de seleção **Configurar como padrão** na área de janela Editar Procura para configurar esta procura como sua procura padrão. Se você configurar esta procura como sua procura padrão, a procura automaticamente irá executar e exibir os resultados cada vez que você acessar a guia **Ofensas**.
  7. Na área de janela de Intervalo de Tempo, selecione uma opção para o intervalo de tempo que você deseja capturar para essa procura. Consulte a Tabela 1.
  8. Na área de janela Parâmetros de Procura, defina seus critérios de procura específicos. Consulte a Tabela 1.
  9. Na área de janela Origem de Ofensa, especifique o tipo de crime e de origem de crime que você deseja procurar:
    - a. Na caixa de listagem, selecione o tipo de crime que você deseja procurar.
    - b. Digite seus parâmetros de procura. Consulte a Tabela 2.
  10. Na área de janela Definição de Coluna, defina a ordem na qual você deseja classificar os resultados:
    - a. Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura.
    - b. Na segunda caixa de listagem, selecione a ordem que você deseja exibir para os resultados da procura. As opções incluem Descendente e Ascendente.
  11. Clique em **Procurar**.

## O que Fazer Depois

Salvando critérios de procura na guia Ofensa

## Procurando ofensas na página Por IP de Origem

Este tópico fornece o procedimento para como procurar ofensas na página **Por IP de origem** da guia **Ofensa**.

### Sobre Esta Tarefa

A tabela a seguir descreve as opções de procura que você pode usar para procurar dados de crime na página Por IP de origem:

*Tabela 32. Por opções de procura da página de IP de Origem*

Opções	Descrição
Todos os Crimes	Você pode selecionar essa opção para procurar todos os endereços IP de origem, independentemente do intervalo de tempo.
Recente	Você pode selecionar esta opção e, nesta caixa de listagem, selecionar o intervalo de tempo que você deseja procurar.

Tabela 32. Por opções de procura da página de IP de Origem (continuação)

Opções	Descrição
Intervalo Específico	Para especificar um intervalo para procurar, você pode selecionar a opção Intervalo Específico e, em seguida, selecione uma das seguintes opções: <ul style="list-style-type: none"> <li>• <b>Data de início entre</b> – Selecione esta caixa de seleção para pesquisar endereços IP de origem associado a ofensas que começou durante um determinado período de tempo. Depois de selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.</li> <li>• <b>Último evento/fluxo entre</b> – Selecione esta caixa de seleção para pesquisar endereços IP de origem associados a ofensas para os quais o último evento detectado ocorreram dentro de um determinado período de tempo. Depois de selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.</li> </ul>
Procura	O ícone <b>Procurar</b> está disponível em várias áreas de janela na página de procura. Você pode clicar em <b>Procurar</b> quando você terminar de configurar a procura e desejar visualizar os resultados.
IP de origem	Neste campo, você pode digitar o endereço IP de origem ou o intervalo do CIDR que você deseja procurar.
Magnitude	Nesta caixa de listagem, você pode especificar uma magnitude e, em seguida, selecione para exibir apenas ofensas com uma magnitude que é igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Risco de VA	Nesta caixa de listagem, você pode especificar um risco VA e, em seguida, selecione para exibir apenas ofensas com um risco VA que é igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Eventos/fluxos	Nesta caixa de listagem, você pode especificar uma contagem de eventos ou fluxo e, em seguida, selecionar para exibir apenas ofensas com uma magnitude que seja igual a, menor que ou maior que o valor configurado.
Exclusão	Você pode selecionar as caixas de seleção para as ofensas que você deseja excluir dos resultados da procura. As opções incluem: <ul style="list-style-type: none"> <li>• Crimes Ativos</li> <li>• Crimes Ocultos</li> <li>• Crimes Encerrados</li> <li>• Ofensas inativas</li> <li>• Ofensa protegida</li> </ul>

## Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por IP de origem**.
3. Na caixa de listagem **Procurar**, selecione **Nova procura**.
4. Na área de janela de Intervalo de Tempo, selecione uma opção para o intervalo de tempo que você deseja capturar para essa procura. Consulte a Tabela 1.
5. Na área de janela Parâmetros de Procura, defina seus critérios de procura específicos. Consulte a Tabela 1.
6. Na área de janela Definição de Coluna, defina a ordem na qual você deseja classificar os resultados:
  - a. Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura.
  - b. Na segunda caixa de listagem, selecione a ordem que você deseja exibir para os resultados da procura. As opções incluem **Decrescente** e **Crescente**.
7. Clique em **Procurar**.

## O que Fazer Depois

Salvando critérios de procura na guia Ofensa

## Procurando ofensas na página Por IP de Destino

Na página **Por IP de destino** da guia **Ofensa**, você pode procurar as ofensas que estão agrupadas pelo endereço IP de destino.

### Sobre Esta Tarefa

A tabela a seguir descreve as opções de procura que você pode usar para ofensas de procura na página Por IP de Destino:

*Tabela 33. Por opções de procura da página de IP de Destino*

Opções	Descrição
Todos os Crimes	Você pode selecionar essa opção para procurar todos os endereços IP de destino, independentemente do intervalo de tempo.
Recente	Você pode selecionar esta opção e, nesta caixa de listagem, selecionar o intervalo de tempo que você deseja procurar.
Intervalo específico	Para especificar um intervalo específico para procurar, você pode selecionar a opção <b>Intervalo específico</b> e, em seguida, selecione uma das seguintes opções: <ul style="list-style-type: none"><li>• Para especificar um intervalo específico para procurar, você pode selecionar a opção <b>Intervalo específico</b> e, em seguida, selecione uma das seguintes opções:</li><li>• <b>Último evento/fluxo entre</b> – Selecione esta caixa de seleção para pesquisar endereços IP de destino associado a ofensas para os quais o último evento detectado ocorreu dentro de um determinado período de tempo. Depois de selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar</li></ul>
Procura	O ícone <b>Procurar</b> está disponível em várias áreas de janela na página de procura. Você pode clicar em <b>Procurar</b> quando você terminar de configurar a procura e desejar visualizar os resultados.
IP de destino	Você pode digitar o endereço IP de destino ou intervalo do CIDR que você deseja procurar.
Magnitude	Nessa caixa de listagem, você pode especificar uma magnitude e selecionar para exibir apenas ofensas com uma magnitude igual a, menor que ou maior que o valor configurado.
Risco de VA	Nesta caixa de listagem, você pode especificar um risco de VA e, em seguida, selecionar para exibir apenas ofensas com um risco de VA que é igual a, menor que ou maior que o valor configurado. O intervalo é 0 – 10.
Eventos/fluxos	Nesta caixa de listagem, você pode especificar uma magnitude de contagem de eventos ou fluxo e, em seguida, selecionar exibir apenas ofensas com uma contagem de eventos ou fluxo que é igual a, menor que ou maior que o valor configurado.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Por IP de destino**.
3. Na caixa de listagem **Procurar**, selecione **Nova procura**.
4. Na área de janela de Intervalo de Tempo, selecione uma opção para o intervalo de tempo que você deseja capturar para essa procura. Consulte a Tabela 1.
5. Na área de janela Parâmetros de Procura, defina seus critérios de procura específicos. Consulte a Tabela 1.
6. Na área de janela Definição de Coluna, defina a ordem na qual você deseja classificar os resultados:
  - a. Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura.
  - b. Na segunda caixa de listagem, selecione a ordem na qual você deseja exibir os resultados da procura. As opções incluem **Decrescente** e **Crescente**.
7. Clique em **Procurar**.

## O que Fazer Depois

Salvando critérios de procura na guia Ofensa

### Procurando ofensas na página Por Redes

Na página **Por Rede** da guia **Ofensa**, você pode procurar ofensas que são agrupadas pelas redes associadas.

#### Sobre Esta Tarefa

A tabela a seguir descreve as opções de procura que você pode usar para procurar dados de crime na página **Por Redes**:

*Tabela 34. Opções de procura para dados de crime de procura na página Por Redes*

Opção	Descrição
Rede	Nesta caixa de listagem, você pode selecionar a rede que você deseja procurar.
Magnitude	Nessa caixa de listagem, você pode especificar uma magnitude e selecionar para exibir apenas ofensas com uma magnitude igual a, menor que ou maior que o valor configurado.
Risco de VA	Nesta caixa de listagem, você pode especificar um risco de VA e, em seguida, selecionar para exibir apenas ofensas com um risco de VA que é igual a, menor que ou maior que o valor configurado.
Eventos/fluxos	Nesta caixa de listagem, você pode especificar uma contagem de eventos ou fluxo e, em seguida, selecionar para exibir apenas ofensas com uma contagem de eventos ou fluxo que é igual a, menor que ou maior que o valor configurado.

#### Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por Redes**.
3. Na caixa de listagem **Procurar**, selecione **Nova procura**.
4. Na área de janela **Parâmetros de Procura**, defina seus critérios de procura específicos. Consulte a Tabela 1.
5. Na área de janela **Definição de Coluna**, defina a ordem na qual você deseja classificar os resultados:
  - a. Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura.
  - b. Na segunda caixa de listagem, selecione a ordem na qual você deseja exibir os resultados da procura. As opções incluem **Decrescente** e **Crescente**.
6. Clique em **Procurar**.

## O que Fazer Depois

Salvando critérios de procura na guia Ofensa

### Salvando critérios de procura na guia Ofensas

Na guia **Ofensas**, você pode salvar os critérios de procura configurados para que você possa reutilizar os critérios para procuras futuras. Os critérios de procura salvos não expiram.

#### Procedimento

1. Procedimento
2. Execute uma procura. Consulte **Procuras de crimes**.
3. Clique em **Salvar critérios**.

4. Insira valores para os seguintes parâmetros:

Opção	Descrição
Parâmetro	Descrição
Nome da Procura	Insira um nome que você deseja designar a esse critério de procura.
Gerenciar Grupos	Clique em <b>Gerenciar grupos</b> para gerenciar os grupos de procura. Consulte Gerenciando grupos de procura.
Opções de amplitude de tempo:	Escolha uma das opções a seguir: <ul style="list-style-type: none"><li>• <b>Todas ofensas</b> – selecione essa opção para procurar todas as ofensas, independentemente do intervalo de tempo.</li><li>• <b>Recente</b> – selecione a opção e, dessa caixa de listagem, selecione o intervalo de tempo ao qual você deseja procurar.</li><li>• <b>Intervalo específico</b> – para especificar um intervalo específico para procurar, selecione a opção <b>Intervalo específico</b> e, em seguida, selecione uma das opções a seguir: Data de início entre – selecione essa caixa de seleção para procurar as ofensas que começaram durante um determinado período de tempo. Após selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que deseja procurar. Último evento/Fluxo entre – selecione essa caixa de seleção para procurar as ofensas as quais o último evento detectado ocorreu dentro de um determinado período de tempo. Após selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.</li></ul>
Definir como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.

5. Clique em OK.

---

## Excluindo critérios de procura

Você pode excluir critérios de procura.

### Sobre Esta Tarefa

Ao excluir uma procura salva, em seguida, os objetos associados à procura salva poderão não funcionar. Os relatórios e regras de detecção de anomalia são objetos do QRadar que usam critérios de procura salvos. Após excluir uma procura salva, edite os objetos associados para assegurar-se de que eles continuam a funcionar.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.



- Clique na guia **Atividade de rede**.
- 2. Na caixa de listagem **Procurar**, selecione **Nova procura** ou **Editar procura**.
- 3. Na área de janela Procuras Salvas, selecione uma procura salva na caixa de listagem **Procuras salvas disponíveis**.
- 4. Clique em **Excluir**.
  - Se os critérios de procura salvos não estiverem associados a outros objetos do QRadar, uma janela de confirmação será exibida.
  - Se os critérios de procura salvos estiverem associados a outros objetos, a janela Excluir procura salva será exibida. A janela lista os objetos associados com a procura salva que você deseja excluir. Observe os objetos associados.
- 5. Clique em **OK**.
- 6. Escolha uma das opções a seguir:
  - Clique em **OK** para continuar.
  - Clique em **Cancelar** para fechar a janela Excluir procura salva.

### O que Fazer Depois

Se os critérios de procura salvos foram associados a outros objetos do QRadar, acesse os objetos associados que você observou e edite-os para remover ou substituir a associação com a procura salva excluída.

---

## Usando uma subprocura para refinar resultados da procura

É possível usar uma subprocura para procurar em um conjunto de resultados da procura concluído. A subprocura é usada para refinar resultados da procura sem procurar o banco de dados novamente.

### Antes de Iniciar

Ao definir uma procura que você deseja usar como base para a subprocura, certifique-se de que a opção Tempo Real (fluxo) esteja desativada e a procura não esteja agrupada.

### Sobre Esta Tarefa

Esse recurso não está disponível para pesquisas agrupadas, pesquisas em andamento ou em modo de fluxo.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Execute uma procura.
3. Quando a procura estiver concluída, inclua outro filtro:
  - a. Clique em **Incluir filtro**.
  - b. Na primeira caixa de listagem, selecione um parâmetro que você deseja procurar.
  - c. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura. A lista de modificadores disponíveis depende do atributo selecionado na primeira lista.

- d. No campo de entrada, insira as informações específicas relacionadas à sua procura.
- e. Clique em **Incluir filtro**.

## Resultados

A área de janela Filtro Original especifica os filtros originais aplicados à procura de base. A área de janela Filtro do Current especifica os filtros aplicados na subprocura. Você pode limpar os filtros de subprocura sem reiniciar a procura de base. Clique no link **Limpar filtro** ao lado do filtro que você deseja limpar. Se você limpar um filtro na área de janela Filtro Original, a procura de base será reativada.

Se você excluir os critérios de procura de base nos critérios de subprocura salva, você ainda terá o acesso aos critérios de subprocura salva. Se você adicionar um filtro, a subprocura irá pesquisar o banco de dados inteiro, visto que a função de procura não mais baseia a procura em um conjunto de dados procurado anteriormente.

## O que Fazer Depois

Salvar critérios de procura

---

## Gerenciando resultados da procura

É possível iniciar várias procuras, e, em seguida, navegar para outras guias para executar outras tarefas enquanto suas procuras são concluídas em segundo plano.

É possível configurar uma procura para enviar uma notificação por email quando a procura for concluída.

A qualquer momento enquanto uma procura estiver em andamento, será possível retornar às guias **Atividade de log** ou **Atividade de rede** para visualizar resultados da procura parcial ou completa.

## Salvando resultados da procura

Você pode salvar os resultados da procura.

### Sobre Esta Tarefa

Se você executar uma procura e não salvar explicitamente os resultados da procura, eles estarão disponíveis em Gerenciar janelas de procura por 24 horas e, em seguida, automaticamente excluídos.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Execute uma procura.
3. Clique em **Salvar resultados**.
4. Na janela Salvar resultado da procura, insira um nome exclusivo para os resultados da procura.
5. Clique em **OK**.

## Visualizando gerenciar resultados da procura

Usando a página Gerenciar resultados da procura, você pode visualizar os resultados da procura de forma parcial ou completa.

### Sobre Esta Tarefa

Os resultados da procura salvos retêm as configurações do gráfico dos critérios de procura associados, no entanto, se o resultado da procura for baseado em critérios de procura que foram excluídos, os gráficos padrão (de barras e de setores) serão exibidos.

A página Gerenciar resultados da procura fornece os parâmetros a seguir

*Tabela 35. Parâmetros da página gerenciar resultados da procura*

Parâmetro	Descrição
Flags	Indica que uma notificação por email ficará pendente para quando a procura for concluída.
User	Especifica o nome do usuário que iniciou a procura.
Name	Especifica o nome da procura, se a procura foi salva. Para obter mais informações sobre como salvar uma procura, consulte Salvando resultados da procura.
Started On	Especifica a data e hora em que a procura foi iniciada.
Ended On	Especifica a data e a hora em que a procura terminou.
Duration	Especifica a quantidade de tempo que a procura levou para ser concluída. Se a procura estiver em andamento, o parâmetro de <b>Duração</b> especificará quanto tempo a procura levou no processamento para a data de conclusão. Se a procura for cancelada, o parâmetro de <b>Duration</b> especificará o período de tempo em que a procura estava em processamento antes de ter sido cancelada.
Expires On	Especifica a data e hora em que um resultado da procura não salvo irá expirar. O número de retenção da procura salva é configurado nas configurações do sistema.  Para obter mais informações sobre a configuração das definições do sistema, consulte o <i>Guia de Administração IBM Security QRadar SIEM</i> .
Status	Especifica o status da procura. Os status são: <ul style="list-style-type: none"><li>• <b>Enfileirado</b> – Especifica que a procura será enfileirada para iniciar.</li><li>• <b>&lt;percentual&gt;%Concluído</b> – Especifica o progresso da procura em termos de porcentagem concluída. Você pode clicar no link para visualizar resultados parciais.</li><li>• <b>Classificação</b> – Especifica que a procura concluiu a coleta dos resultados e está atualmente preparando os resultados para visualização.</li><li>• <b>Cancelado</b> – Especifica que a procura foi cancelada. Você pode clicar no link para visualizar os resultados que foram coletados antes do cancelamento.</li><li>• <b>Concluído</b> – Especifica que a procura foi concluída. Você pode clicar no link para visualizar os resultados. Consulte o Monitoramento da atividade de log ou o Monitoramento da atividade de rede.</li></ul>
Size	Especifica o tamanho do arquivo do conjunto de resultados da procura.

A janela barra de ferramentas Gerenciar resultados da procura fornece as seguintes funções

*Tabela 36. Barra de ferramentas gerenciar resultados da procura*

Função	Descrição
Nova Procura	Clique em <b>Nova procura</b> para criar uma nova procura. Quando você clicar nesse ícone, a página de procura será exibida.
Salvar Resultados	Clique em <b>Salvar Resultados</b> para salvar os resultados da procura selecionados. Consulte Salvando resultados da procura.
Cancelar	Clique em <b>Cancelar</b> para cancelar o resultado da procura selecionado em andamento ou enfileirado para iniciar. Consulte Cancelando uma procura.

Tabela 36. Barra de ferramentas gerenciar resultados da procura (continuação)

Função	Descrição
Delete	Clique em <b>Excluir</b> para excluir o resultado da procura selecionado. Consulte Excluindo um resultado da procura.
Notify	Clique em <b>Notificar</b> para ativar a notificação por email quando a procura selecionada estiver concluída.
View	Nessa caixa de listagem, você poderá selecionar quais resultados da procura você deseja listar na página Resultados da procura. As opções são: <ul style="list-style-type: none"> <li>• Resultados da procura salvos</li> <li>• Todos os resultados da procura</li> <li>• Procuras canceladas/com erros</li> <li>• Procuras em andamento</li> </ul>

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. No menu **Procurar**, selecione **Gerenciar resultados da procura**.
3. Visualize a lista de resultados da procura.

## Cancelando uma procura

Enquanto uma procura está na fila ou em andamento, é possível cancelar a procura na página Gerenciar resultados da procura.

### Sobre Esta Tarefa

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

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. A partir do menu **Procurar**, selecione **Gerenciar resultados da procura**.
3. Selecione o resultado da procura na fila ou em andamento que deseja cancelar.
4. Clique em **Cancelar**.
5. Clique em **Sim**.

## Excluindo uma procura

Se um resultado da procura não for mais necessário, será possível excluí-lo da página Gerenciar resultados da procura.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. No menu **Procurar**, selecione **Gerenciar resultados da procura**.
3. Selecione o resultado da procura que deseja excluir.
4. Clique em **Excluir**.
5. Clique em **Sim**.

---

## Gerenciando grupos de procura

Usando a janela Procurar grupos, é possível criar e gerenciar grupos de procura de eventos, fluxo e ofensas.

Esses grupos permitem que sejam localizados facilmente critérios de procura salvos nas guias **Atividade de log**, **Atividade de rede** e **Ofensas** e no assistente de relatório.

## Visualizando grupos de procura

Um conjunto padrão de grupos e subgrupos estão disponíveis.

### Sobre Esta Tarefa

Você pode visualizar grupos de procura nas janelas Grupos de procura de eventos, Grupo de procura de fluxo ou Grupo de procura.

Todas as procuras salvas não designadas a um grupo estão no grupo **Outro**.

As janelas Grupos de procura de eventos, Grupo de procura de fluxo e Grupo de procura de crime exibem os seguintes parâmetros para cada grupo.

*Tabela 37. Parâmetros da janela de grupo de procura*

Parâmetro	Descrição
Name	Especifica o nome do grupo de procura.
User	Especifica o nome de usuário que criou o grupo de procura.
Descrição	Especifica a descrição do grupo de procura.
Date Modified	Especifica a data que o grupo de procura foi modificado.

As janelas de ferramentas Grupos de procura de eventos, Grupo de procura de fluxo e Grupo de procura de crime fornecem as seguintes funções.

*Tabela 38. Funções da janela barra de ferramentas do grupo de procura*

Função	Descrição
Novo grupo	Para criar um novo grupo de procura, você pode clicar em <b>Novo grupo</b> . Consulte Criando um grupo de procura novo.
Editar	Para editar um grupo de procura existente, você pode clicar em <b>Editar</b> . Consulte Editando um grupo de procura.
Copiar	Para copiar uma procura salva em outro grupo de procura, você pode clicar em <b>Copiar</b> . Consulte Copiando uma procura salva para outro grupo.
Remover	Para remover um grupo de procura ou uma procura salva de um grupo de procura, selecione o item que você deseja remover e clique em <b>Remover</b> . Consulte Removendo um grupo ou uma procura salva de um grupo.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. **Selecionar procura >Editar procura.**
3. Clique em **Gerenciar grupos**.
4. Visualize os grupos de procura.

## Criando um novo grupo de procura

Você pode criar um novo grupo de procura.

## Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. **Selecionar Procura Editar Procura**.
3. Clique em **Gerenciar grupos**.
4. Selecione a pasta para o grupo no qual você deseja criar o novo grupo.
5. Clique em **Novo grupo**.
6. No campo **Nome**, digite um nome exclusivo para o novo grupo.
7. Opcional. No campo **Descrição**, digite uma descrição.
8. Clique em **OK**.

## Editando um grupo de procura

Você pode editar os campos **Nome** e **Descrição** de um grupo de procura.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Selecione **Procurar > Editar procura**.
3. Clique em **Gerenciar grupos**.
4. Selecione o grupo que você deseja editar.
5. Clique em **Editar**.
6. Edite os parâmetros:
  - Digite um novo nome no campo **Nome**.
  - Digite uma nova descrição no campo **Descrição**.
7. Clique em **OK**.

## Copiando uma procura salva para outro grupo

É possível copiar uma procura salva para um ou mais grupos.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Selecione **Procurar > Editar procura**.
3. Clique em **Gerenciar grupos**.
4. Selecione a procura salva que deseja copiar.
5. Clique em **Copiar**.
6. Na janela Grupos de item, selecione a caixa de seleção para o grupo que você deseja copiar a procura salva.
7. Clique em **Designar grupos**.

## Removendo um grupo ou uma procura salva de um grupo

Você pode usar o ícone **Remover** para remover uma procura de um grupo ou remover um grupo de procura.

## Sobre Esta Tarefa

Ao remover uma procura salva de um grupo, a procura salva não será excluída do sistema. A procura salva é removida do grupo e automaticamente movida para o grupo **Outros**.

Não é possível remover os seguintes grupos do sistema:

- Grupos de Procura de Evento
- Grupos de Procura de Fluxo
- Grupos de Procura de Crime
- Outro

## Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Selecione **Procurar > Editar procura**.
3. Clique em **Gerenciar grupos**.
4. Escolha uma das opções a seguir:
  - Selecione a procura salva que você deseja remover do grupo.
  - Selecione o grupo que você deseja remover.
5. Clique em **Remover**.
6. Clique em **OK**.





---

## Capítulo 9. Propriedades de fluxo e de evento customizadas

Use as propriedades de fluxo e evento customizado para procurar, visualizar e relatar sobre informações em logs que o QRadar geralmente não normaliza e exibe.

É possível criar propriedades de evento e de fluxo customizadas a partir de vários locais nas guias **Atividade de log** ou **Atividade de rede**:

- Na guia **Atividade de Log**, clique duas vezes em um evento e clique em **Extrair Propriedade**.
- Na guia **Atividade de Rede**, clique duas vezes em um fluxo e clique em **Extrair Propriedade**.
- É possível criar ou editar um evento customizado ou propriedade de fluxo na página Procura. Quando você cria uma propriedade customizada na página Procura, a propriedade não é derivada de nenhum evento ou fluxo específico; assim, a janela Propriedades do Evento Customizado não é preenchida previamente. É possível copiar e colar as informações de carga útil a partir de outra origem.

---

### Permissões requeridas

Para criar propriedades customizadas se tiver a permissão correta.

É necessário ter a permissão Propriedades do evento definidas pelo usuário ou Propriedades de fluxo definidas pelo usuário.

Se tiver permissões administrativas, também poderá criar e modificar propriedades customizadas na guia Administração.

Clique em **Administração > Origens de dados > Propriedade de evento customizado >** ou **Administração > Origens de dados > Propriedades de fluxo customizado**.

Verifique com seu administrador, para assegurar-se de que tem as permissões corretas.

Para obter mais informações, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

---

### Tipos de propriedades customizadas

É possível criar um tipo de propriedade customizada.

Ao criar uma propriedade customizada, é possível optar por criar um Regex ou um tipo de propriedade calculada.

Usando instruções de expressão regular (Regex), é possível extrair dados não normalizados a partir de cargas úteis de eventos ou de fluxo.

Por exemplo, um relatório é criado para relatar todos os usuários que fazem alterações de permissões de usuário em um servidor Oracle. Uma lista de usuários e o número de vezes que eles fizeram uma alteração na permissão da outra conta serão relatados. No entanto, normalmente a conta do usuário real ou a conta que

foi alterada não pode ser exibida. É possível criar uma propriedade customizada para extrair essas informações dos logs e, em seguida, usar a propriedade em procuras e relatórios. O uso desse recurso requer conhecimento avançado de expressões regulares (regex).

Regex define o campo que você deseja que se torne a propriedade customizada. Após inserir uma instrução regex, será possível validá-la em relação à carga útil. Ao definir padrões regex customizados, realize adesão às regras regex conforme definido pela linguagem de programação Java.

Para obter mais informações, é possível consultar tutoriais regex disponíveis na web. Uma propriedade customizada pode ser associada a várias expressões regulares.

Quando um evento ou fluxo for analisado, cada padrão regex será testado no evento ou no fluxo até que um padrão regex corresponda à carga útil. O primeiro padrão regex a corresponder à carga útil do evento ou do fluxo determina os dados a serem extraídos.

Usando propriedades customizadas com base no cálculo, é possível executar cálculos sobre as propriedades de fluxo ou evento numérico existentes para produzir uma propriedade calculada.

Por exemplo, é possível criar uma propriedade que exibe uma porcentagem dividindo uma propriedade numérica por outra propriedade numérica.

---

## Criando uma propriedade customizada baseada em regex

É possível criar uma propriedade customizada com base em regex para corresponder cargas úteis de fluxo ou de evento a uma expressão regular.

### Sobre Esta Tarefa

Ao configurar uma propriedade customizada com base em regex, as janelas Propriedade de Evento Customizado ou Propriedade de Fluxo Customizado fornecem parâmetros. A tabela a seguir fornece informações de referência para alguns parâmetros.

*Tabela 39. Parâmetros da janela Propriedades de Evento Customizado (regex)*

Parâmetro	Descrição
Campo de Teste	
Nova propriedade	O nome da nova propriedade não pode ser o nome de uma propriedade normalizada, como nome do usuário, IP de Origem ou IP de Destino.
Otimizar análise para regras, relatórios e procuras	Analisa e armazena a propriedade da primeira vez que o evento ou fluxo é recebido. Quando você selecionar a caixa de seleção, a propriedade não irá requerer mais análises para relatar, procurar ou testar regra.  Se você limpar essa caixa de seleção, a propriedade será analisada cada vez que um relatório, procura ou teste de regra for aplicado.
Origem de Log	Se várias origens de log estiverem associadas com esse evento, esse campo especificará o termo Várias e o número de origens de log.

Tabela 39. Parâmetros da janela Propriedades de Evento Customizado (regex) (continuação)

Parâmetro	Descrição
RegEx	<p>A expressão regular que você deseja usar para extrair os dados da carga útil. As expressões regulares fazem distinção entre maiúsculas e minúsculas.</p> <p>Os exemplos a seguir mostram expressões regulares de amostra:</p> <ul style="list-style-type: none"> <li>• Email: <code>(.+@[^\.]*.?[a-z]{2,})\$</code></li> <li>• URL: <code>(http\:\/\/[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}\/\S*)?\$</code></li> <li>• Nome do Domínio: <code>(http[s]?:\/\/(. ?)\/?::)</code></li> <li>• Número de Pontos Flutuantes: <code>([-+]?\d*\.\d*\$)</code></li> <li>• Número Inteiro: <code>([-+]?\d*\$)</code></li> <li>• Endereço IP: <code>(\b\d{1,3}\. \d{1,3}\. \d{1,3}\. \b \d{1,3})</code></li> </ul> <p>Os grupos de captura devem estar entre parênteses.</p>
Grupo de Captura	Os grupos de captura tratam vários caracteres como uma única unidade. Em um grupo de captura, os caracteres são agrupados dentro de um conjunto de parênteses.
Enabled	Se você desmarcar a caixa de seleção, essa propriedade customizada não será exibida em filtros de procura ou listas de coluna e a propriedade não será analisada a partir das cargas úteis.

## Procedimento

1. Clique na guia **Atividade de log**.
2. Se estiver visualizando eventos ou fluxos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento ou fluxo em que deseja basear a propriedade customizada.
4. Dê um clique duplo no evento em que você deseja basear a propriedade customizada
5. Clique em **Extrair propriedade**.
6. Na área de janela **Seleção de Tipo de Propriedade**, selecione a opção **Com base em Regex**.
7. Configure os parâmetros da propriedade customizada.
8. Clique em **Testar** para testar a expressão regular com relação à carga útil.
9. Clique em **Salvar**.

## Resultados

A propriedade customizada é exibida como uma opção na lista de colunas disponíveis na página de procura. Para incluir uma propriedade customizada em uma lista de eventos ou fluxos, você deve selecionar a propriedade customizada na lista de colunas disponíveis ao criar uma procura.

---

## Criando uma propriedade customizada baseada em cálculo

É possível criar uma propriedade customizada baseada em cálculo para corresponder às cargas úteis do cliente em uma expressão comum.

### Sobre Esta Tarefa

Ao configurar uma propriedade customizada baseada em cálculo, as janelas Propriedade de Evento Customizado ou Propriedade de Fluxo Customizado fornecem os seguintes parâmetros:

Tabela 40. Parâmetros da janela Definição de propriedade customizada (cálculo)

Parâmetro	Descrição
Definição de Propriedade	
Nome da Propriedade	Digite um nome exclusivo para essa propriedade customizada. O novo nome da propriedade não pode ser o nome de uma propriedade normalizada, como Nome de usuário, IP de origem ou IP de destino.
Descrição	Digite uma descrição dessa propriedade customizada.
Definição de Cálculo de Propriedade	
Property 1	Na caixa de listagem, selecione a primeira propriedade que deseja usar em seu cálculo. As opções incluem todas as propriedades customizadas numéricas e customizadas.  É possível também especificar um valor numérico específico. Na caixa de listagem <b>Propriedade 1</b> , selecione a opção <b>Definido pelo usuário</b> . O parâmetro <b>Numeric Property</b> é exibido. Digite um valor numérico específico.
Operator	Na caixa de listagem, selecione o operador que deseja aplicar para as propriedades selecionadas no cálculo. As opções incluem: <ul style="list-style-type: none"> <li>• Incluir</li> <li>• Subtrair</li> <li>• Multiplicar</li> <li>• Dividir</li> </ul>
Property 2	Na caixa de listagem, selecione a segunda propriedade que deseja usar em seu cálculo. As opções incluem todas as propriedades customizadas numéricas e customizadas.  É possível também especificar um valor numérico específico. Na caixa de listagem <b>Propriedade 1</b> , selecione a opção <b>Definido pelo usuário</b> . O parâmetro <b>Numeric Property</b> é exibido. Digite um valor numérico específico.
Ativado	Selecione esta caixa de seleção para ativar essa propriedade customizada.  Se a caixa de seleção for desmarcada, essa propriedade customizada não será exibida em filtros de procura de evento ou fluxo ou listas de coluna e a propriedade de evento ou fluxo não será analisada a partir de cargas úteis.

## Procedimento

1. Escolha um dos seguintes: Clique na guia **Atividade de log**.
2. Opcional. Se estiver visualizando eventos ou fluxos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Clique duas vezes no evento ou fluxo no qual deseja basear a propriedade customizada.
4. Clique em **Extrair propriedade**.
5. Na área de janela Seleção do tipo de propriedade, selecione a opção **Com base em cálculo**.
6. Configure os parâmetros da propriedade customizada.
7. Clique em **Testar** para testar a expressão regular com relação à carga útil.
8. Clique em **Salvar**.

## Resultados

A propriedade customizada é agora exibida como uma opção na lista de colunas disponíveis na página de procura. Para incluir uma propriedade customizada em uma lista de eventos ou fluxos, é necessário selecionar a propriedade customizada a partir da lista de colunas disponíveis ao criar uma procura.

## Modificando uma propriedade customizada

Você pode modificar uma propriedade customizada.

### Sobre Esta Tarefa

Você pode usar a janela Propriedades de eventos customizados ou Propriedades de fluxos customizados para modificar uma propriedade customizada.

As propriedades customizadas são descritas na tabela a seguir.

*Tabela 41. Colunas de janela de propriedades customizadas*

Coluna	Descrição
Nome da Propriedade	Especifica um nome exclusivo para essa propriedade customizada.
Tipo	Especifica o tipo para essa propriedade customizada.
Descrição da Propriedade	Especifica uma descrição para essa propriedade customizada.
Tipo de Fonte de Log	Especifica o nome do tipo de origem do log para o qual essa propriedade customizada se aplica.  Essa coluna é exibida somente na janela Propriedades do eventos customizados.
Origem de Log	Especifica a origem do log para o qual essa propriedade customizada se aplica.  Se houver várias origens de log associadas a esse evento ou fluxo, esse campo especificará o termo Várias e o número de origens de log.  Essa coluna é exibida somente na janela Propriedades de eventos customizados.
Expressão	Especifica a expressão para essa propriedade customizada. A expressão depende do tipo de propriedade customizada:  Para uma propriedade customizada baseada em regex, esse parâmetro especifica a expressão regular que você deseja usar para extrair os dados da carga útil.  Para obter uma propriedade customizada baseada em cálculo, esse parâmetro especifica o cálculo que deseja usar para criar o valor da propriedade customizada.
Nome de Usuário	Especifica o nome do usuário que criou essa propriedade customizada.
Ativado	Especifica se essa propriedade customizada está ativada. Esse campo especifica se é Verdadeiro ou Falso.
Data de Criação	Especifica a data que essa propriedade customizada foi criada.
Data da Modificação	Especifica a última vez que essa propriedade customizada foi modificada.

A barra de ferramentas Propriedade de Evento Customizado e Propriedade de Fluxo Customizado fornece as funções a seguir:

*Tabela 42. Opções da barra de ferramentas da propriedade customizada*

Opção	Descrição
Incluir	Clique em <b>Incluir</b> para incluir uma nova propriedade customizada.
Editar	Clique em <b>Editar</b> para editar a propriedade customizada selecionada.
Copiar	Clique em <b>Copiar</b> para copiar as propriedades customizadas selecionadas.
Excluir	Clique em <b>Excluir</b> para excluir as propriedades customizadas selecionadas.
Ativar/Desativar	Clique em <b>Ativar/Desativar</b> para ativar ou desativar as propriedades customizadas selecionadas para análise e visualização nos filtros de procura ou nas listas de colunas.

## Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Na caixa de listagem **Procurar**, selecione **Editar procura**.
3. Clique em **Gerenciar propriedades customizadas**.
4. Selecione a propriedade customizada que deseja editar e clique em **Editar**.
5. Editar os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testar a expressão regular com relação à carga útil.
7. Clique em **Salvar**.

---

## Copiando uma propriedade customizada

Para criar uma nova propriedade customizada baseada em uma propriedade customizada existente, você pode copiar a propriedade customizada existente e, em seguida, modificar os parâmetros.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Na caixa de listagem **Procurar**, selecione **Editar procura**.
3. Clique em **Gerenciar propriedades customizadas**.
4. Selecione a propriedade customizada que deseja copiar e clique em **Copiar**.
5. Editar os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testar a expressão regular com relação à carga útil.
7. Clique em **Salvar**.

---

## Excluindo uma propriedade customizada

Você pode excluir qualquer propriedade customizada, desde que ela não esteja associada a outra.

### Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Atividade de log**.
  - Clique na guia **Atividade de rede**.
2. Clique na guia **Atividade de log**.
3. Na caixa de listagem **Procurar**, selecione **Editar procura**.
4. Clique em **Gerenciar propriedades customizadas**.
5. Selecione a propriedade customizada que deseja excluir e clique em **Excluir**.
6. Clique em **Sim**.

---

## Capítulo 10. Gerenciamento de regra

A partir das guias **Atividade de log**, **Atividade de rede** e **Ofensas**, é possível visualizar e manter as regras.

Este tópico se aplica a usuários que têm as permissões de função de usuário **Visualizar regras customizadas** ou **Manter regras customizadas**.

---

### Considerações de permissão de regra

É possível visualizar e gerenciar regras para as áreas da rede que podem ser acessadas se tiver as permissões de função do usuário **Visualizar regras customizadas** e **Manter regras customizadas**.

Para criar regras de detecção de anomalias, é necessário ter a permissão **Manter regra customizada** apropriada para a guia na qual deseja criar a regra. Por exemplo, para poder criar uma regra de detecção de anomalias na guia **Atividade de log**, deve-se ter **Atividade de log > Manter regra customizada**.

Para obter mais informações sobre as permissões de função de usuário, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

---

### Visão geral de regras

As regras executam testes em eventos, fluxos ou ofensas, e se todas as condições de um teste forem atendidas, a regra gerará uma resposta.

Os testes em cada regra também podem referenciar outros blocos de construção e regras. Não é necessário criar regras em qualquer ordem específica porque o sistema verifica as dependências cada vez que uma nova regra for incluída, editada ou excluída. Se uma regra que foi referenciada por outra regra for excluída ou desativada, um aviso será exibido e nenhuma ação será tomada.

Para obter uma lista completa de regras padrão, consulte o *IBM Security QRadar SIEM Administration Guide*.

### Categorias de regra

Há duas categorias de regras; regras customizadas e regras de anomalias.

Regras customizadas executam testes em eventos, fluxos e ofensas para detectar atividade incomum em sua rede.

Regras de detecção de anomalia executam testes nos resultados das procuras salvas de evento ou de fluxo como um meio de detectar quando padrões de tráfego incomuns ocorrerem em sua rede.

Regras de detecção de anomalia executam testes nos resultados das procuras salvas de evento ou de fluxo como um meio de detectar quando padrões de tráfego incomuns ocorrerem em sua rede. Essa categoria de regra inclui os seguintes tipos de regra: de anomalia, de limite e de comportamento.

Uma regra de anomalia testa tráfego de fluxo e de evento em busca de atividade anormal, como a existência de tráfego novo ou desconhecido, que é o tráfego que para subitamente ou uma alteração de porcentagem na quantidade de tempo que um objeto está ativo. Por exemplo, é possível criar uma regra de anomalia para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego da última hora. Se houver mais que uma alteração de 40%, a regra gerará uma resposta.

Uma regra de limite testa o tráfego de evento e fluxo em busca de atividades que são menores que, iguais a ou maiores que um limite configurado, ou dentro de um intervalo especificado. Os limites podem ser baseados em quaisquer dados que são coletados. Por exemplo, é possível criar uma regra de limite que especifica que não mais de 220 clientes podem efetuar login no servidor entre às 8h e 17h. A regra de limite gera um alerta quando o cliente 221º tentar efetuar login.

Uma regra comportamental testa o tráfego de evento e fluxo em busca de mudanças de volume no comportamento que ocorrem em padrões sazonais regulares. Por exemplo, se um servidor de correio geralmente se comunica com 100 hosts por segundo no meio da noite e de repente começa a se comunicar com 1.000 hosts por segundo, uma regra comportamental gerará um alerta.

## Tipos de regra

Há quatro tipos diferentes de regras: evento, fluxo, comum e ofensa.

### Regra de evento

Uma regra de evento executa testes em eventos à medida que eles são processados em tempo real pelo processador de eventos. É possível criar uma regra de evento para detectar um único evento (em determinadas propriedades) ou sequências de eventos. Por exemplo, se desejar monitorar sua rede em busca de tentativas de login malsucedidas, acesso vários hosts ou um evento de reconhecimento seguido por uma exploração, será possível criar uma regra de evento. É comum que as regras de evento criem ofensas como resposta.

### Regra de fluxo

Uma regra de fluxo executa testes em fluxos à medida que eles são processados em tempo real pelo QFlow Collector. É possível criar uma regra de fluxo para detectar um único fluxo (dentro de determinadas propriedades) ou sequências de fluxo. É comum que regras de fluxo criem ofensas como resposta.

### Regra comum

Uma regra comum executa testes em campos que são comuns a ambos os registros de evento e de fluxo. Por exemplo, é possível criar uma regra comum para detectar eventos e fluxos que possuem um endereço IP de origem específico. É comum que regras comuns criem ofensas como uma resposta.

### Regra de crime

Uma regra de crime processará ofensas apenas quando alterações forem feitas na ofensa, como quando novos eventos forem adicionados ou o sistema planejar o crime para reavaliação. É comum que regras de crime enviem por email uma notificação como resposta.



## Condições da regra

Cada regra pode conter funções, blocos de construção ou testes.

Com as funções, é possível usar blocos de construção e outras regras para criar uma função de vários eventos, vários fluxos, ou várias ofensas. É possível conectar regras usando funções que suportam operadores booleanos, como OR e AND. Por exemplo, se desejar conectar-se a regras de evento, será possível usar quando um evento corresponder alguma ou todas as funções das regras a seguir.

Um bloco de construção é uma regra sem uma resposta e é usado como uma variável comum em várias regras ou para construir regras complexas ou lógicas que deseja usar em outras regras. É possível salvar um grupo de testes como blocos de construção para uso com outras funções. Blocos de construção permitirão que você reutilize testes de regra específicos em outras regras. Por exemplo, é possível salvar um bloco de construção que inclui os endereços IP de todos os servidores de correio em sua rede e, em seguida, usar esse bloco de construção para excluir os servidores de correio a partir de outra regra. Os blocos de construção padrão são fornecidos como diretrizes, que devem ser revistas e editadas com base nas necessidades de sua rede.

Para obter uma lista completa de blocos de construção, consulte o *IBM Security QRadar SIEM Administration Guide*.

É possível executar testes na propriedade de um evento, fluxo ou ofensa, como endereço IP de origem, severidade de evento ou análise de taxa.

## Respostas da regra

Quando as condições da regra forem atendidas, uma regra poderá gerar uma ou mais respostas.

As regras podem gerar uma ou mais das seguintes respostas:

- Criar um crime.
- Enviar um email.
- Gerar notificações do sistema no recurso Painel.
- Incluir dados em conjuntos de referência.
- Incluir dados em coleções de dados de referência.
- Gerar uma resposta para um sistema externo.
- Incluir dados em coleções de dados de referência que podem ser usados em testes de regras.

### Tipos de coleção de dados de referência

Antes de poder configurar uma resposta da regra para enviar dados para uma coleção de dados de referência, deve-se criar a coleção de dados de referência usando a interface da linha de comandos (CLI). O QRadar suporta os seguintes tipos de coleta de dados:

#### Conjunto de referência

Um conjunto de elementos, como uma lista de endereços IP ou nomes de usuário, que são derivados de eventos e fluxos que ocorrem em sua rede.

#### Mapa de referência

Os dados são armazenados em registros de que mapeiam uma tecla para um valor. Por exemplo, para correlacionar a atividade do usuário em sua

rede, é possível criar um mapa de referência que usa o parâmetro **Username** como uma chave e o **Global ID** do usuário como um valor.

#### **Mapa de referência de conjuntos**

Os dados são armazenados em registros de que mapeiam uma tecla para vários valores. Por exemplo, para testar o acesso autorizado a uma patente, use uma propriedade de evento customizada para **Patent ID** como a chave e o parâmetro **Username** como o valor. Use um mapa de conjuntos para preencher uma lista de usuários autorizados.

#### **Mapa de referência de mapas**

Os dados são armazenados em registros de que mapeiam uma chave para outra, que é, então, mapeada para um valor único. Por exemplo, para testar por violações da largura da banda da rede, é possível criar um mapa de mapas. Use o parâmetro **Source IP** como a primeira chave, o parâmetro **Application** como a segunda chave e o parâmetro **Total Bytes** como o valor.

#### **Tabela de referência**

Em uma tabela de referência, os dados são armazenados em uma tabela que mapeia uma chave para outra, que é, então, mapeada para valor único. A segunda chave tem um tipo designado. Esse mapeamento é semelhante a uma tabela de banco de dados em que cada coluna da tabela é associada a um tipo. Por exemplo, é possível criar uma tabela de referência que armazena o parâmetro **Username** como a primeira chave, e possui várias chaves secundárias que possuem um tipo designado pelo usuário como **Tipo IP** com o parâmetro **Source IP** ou **Source Port** como um valor. É possível configurar uma resposta da regra para incluir uma ou mais chaves definidas na tabela. É possível também incluir valores customizados à resposta da regra. O valor customizado deve ser válido para o tipo de chave secundário.

**Nota:** Para obter informações sobre conjuntos de referência e as coleções de dados de referência, consulte o *Guia de Administração* do seu produto.

---

## **Visualizando regras**

Você pode visualizar os detalhes de uma regra, incluindo os testes, blocos de construção e respostas.

### **Antes de Iniciar**

Dependendo das permissões da função de usuário, você poderá acessar a página regras da guia **Ofensas**, **Atividade de Log** ou **Atividade de rede**.

Para obter mais informações sobre as permissões da função de usuário, consulte o *IBM Security QRadar SIEM Administration Guide*.

Para obter mais informações sobre as permissões da função de usuário, consulte o *IBM Security QRadar Network Anomaly Detection Administration Guide*.

### **Sobre Esta Tarefa**

A Página regras exibe uma lista de regras com seus parâmetros associados. Para localizar a regra que você deseja abrir e visualizar seus detalhes, você pode usar a caixa da lista de grupo ou o campo **Regras de busca** na barra de ferramentas.

## Procedimento

1. Escolha uma das opções a seguir:
  - Clique na guia **Ofensas** e, em seguida, clique em **Regras** no menu de navegação.
  - Clique na guia **Atividade de Log** e, em seguida, selecione **Regras** da caixa de listagem **Regras** na barra de ferramentas.
  - Clique na guia **Atividade de rede** e, em seguida, selecione **Regras** da caixa de listagem **Regras** na barra de ferramentas.
2. Na caixa de listagem **Exibir**, selecione **Regras**.
3. Clique duas vezes na regra que você deseja visualizar.
4. Revisão dos detalhes da regra.

## Resultados

Se você tiver a permissão **Visualização de regras customizadas**, mas não tem a permissão **Manter regras customizadas**, a página **Regra de resumo** será exibida e a regra não poderá ser editada. Se você tiver a permissão **Manter regra customizada**, a página **Editor de pilha de testes da regra** será exibida. Você pode revisar e editar os detalhes da regra “Editando uma regra” na página 124.

---

## Criando uma regra customizada

Você pode criar novas regras para atender às necessidades de sua implementação.

### Sobre Esta Tarefa

Para criar uma nova regra, você deve ter a permissão **Ofensas > Manter regras customizadas**.

Você pode testar as regras localmente ou globalmente. Um teste local significa que a regra é testada no processador de eventos local e não compartilhada com o sistema. Um teste global significa que a regra é compartilhada e testada por algum processador de eventos no sistema. As regras globais enviam eventos e fluxos para o processador de eventos central, o que pode diminuir o desempenho no processador de eventos central.

## Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na lista **Ações**, selecione uma das opções a seguir:
  - Nova regra de evento
  - Nova Regra de Fluxo
  - Nova Regra Comum
  - Nova Regra de Crime
4. Leia o texto de introdução no assistente Regra. Clique em **Avançar**.
5. Clique em **Avançar** para visualizar a página Editor de Pilha de Teste de Regra.
6. No campo **Inserir o nome da regra aqui** na área de janela Regra, insira um nome exclusivo que você deseja designar a essa regra.
7. Na caixa de listagem, selecione **Local** ou **Global**.
8. Incluir um ou mais testes em uma regra:

- a. Opcional. Para filtrar as opções na caixa de listagem **Grupo de teste**, insira o texto que você deseja filtrar no campo Tipo a ser filtrado.
  - b. Na caixa de listagem **Grupo de teste**, selecione o tipo de teste que você deseja incluir nessa regra.
  - c. Para cada teste que você deseja incluir na regra, selecione o sinal de mais (+) ao lado do teste.
  - d. Opcional. Para identificar um teste como teste excluído, clique em **e** no início do teste na área de janela Regra. O **e** é exibido como **e não**.
  - e. Clique nos parâmetros configuráveis sublinhados para customizar as variáveis do teste.
  - f. Na caixa de diálogo, selecione os valores para a variável **e**, em seguida, clique em **Enviar**.
9. Para exportar a regra configurada como um bloco de construção para o uso com outras regras:
    - a. Clique em **Exportar como blocos de construção**.
    - b. Insira um nome exclusivo para esse bloco de construção.
    - c. Clique em **Salvar**.
  10. Na área de janela Grupos, selecione as caixas de seleção dos grupos aos quais você deseja designar essa regra.
  11. No campo **Notas**, insira uma nota que você deseja incluir a essa regra. Clique em **Avançar**.
  12. Na página Respostas da regra, configure as respostas que você deseja que essa regra gere.
    - Para configurar as respostas para uma Regra de Evento, Regra de Fluxo ou Regras Comuns, consulte Tabela 45 na página 130
    - Para configurar as respostas para uma Regra de Ofensa, consulte Tabela 46 na página 133
  13. Clique em **Avançar**.
  14. Revise a página Resumo de regra para assegurar-se de que as configurações estejam corretas. Faça as alterações, se necessário, e, em seguida, clique em **Concluir**.

---

## Criando uma regra de detecção de anomalia

Use o assistente Regra de Detecção de Anomalia para criar regras que se apliquem a critérios de intervalo de tempo, usando testes de Data e Hora.

### Antes de Iniciar

Para criar uma nova regra de detecção de anomalia, você deverá atender aos requisitos a seguir:

- Ter a permissão Manter Regras Customizadas.
- Executar uma procura agrupada.

As opções de detecção de anomalia serão exibidas após executar uma procura agrupada e salvar os critérios de procura.

### Sobre Esta Tarefa

Você deve ter a permissão de função apropriada para poder criar uma regra de detecção de anomalia.

Para criar as regras de detecção de anomalia na guia **Atividade de log**, você deve ter a permissão de função **Atividade de log Manter regras customizadas**.

Para criar as regras de detecção de anomalia na guia **Atividade de rede**, você deve ter a permissão de função **Rede Manter regras customizadas**.

As regras de detecção de anomalia usam todo o agrupamento e os critérios de filtros dos critérios de procura salvos nos quais a regra é baseada, mas não usam quaisquer intervalos de tempo dos critérios de procura.

Ao criar uma regra de detecção de anomalia, a regra será preenchida com uma pilha de teste padrão. Você pode editar os testes padrão ou incluir testes na pilha de teste. Pelo menos um teste Propriedade Acumulada devem ser incluído na pilha de teste.

Por padrão, a opção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente** é selecionada na página Editor de Pilha de Teste de Regra.

Isso faz com que uma regra de detecção de anomalia teste a propriedade acumulada selecionada para cada grupo de eventos ou fluxos separadamente. Por exemplo, se o valor acumulado selecionado for **UniqueCount(sourceIP)**, a regra testará cada endereço IP de origem exclusivo para cada grupo de eventos ou fluxo.

Essa opção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente** é dinâmica. O valor **[Selected Accumulated Property]** depende de qual opção foi selecionada no campo **Esse teste de propriedade acumulada** da pilha de teste padrão. O valor **[group]** depende das opções de agrupamento especificadas nos critérios de procura salvos. Se diversas opções de agrupamento estiverem incluídas, o texto poderá estar truncado. Mova o ponteiro do mouse sobre o texto para visualizar todos os grupos.

## Procedimento

1. Clique na guia **Atividade de log** ou **Atividade de rede**.
2. Execute uma procura.
3. No menu **Regras**, selecione o tipo de regra que você deseja criar. As opções incluem:
  - Incluir regra de anomalia
  - Incluir regra de limite
  - Incluir regra comportamental
4. Leia o texto de introdução no assistente Regra. Clique em **Avançar**. A regra que você escolheu anteriormente será selecionada.
5. Clique em **Avançar** para visualizar a página Editor de Pilha de Teste de Regra.
6. No campo **Inserir o nome da regra aqui**, insira um nome exclusivo que você deseja designar a essa regra.
7. Para incluir um teste em uma regra:
  - a. Opcional. Para filtrar as opções na caixa de listagem Grupo de Teste, insira o texto que você deseja filtrar no campo Tipo a ser filtrado.
  - b. Na caixa de listagem Grupo de Teste, selecione o tipo de teste que deseja incluir nessa regra.
  - c. Para cada teste que você deseja incluir na regra, selecione o sinal + ao lado do teste.

- d. Opcional. Para identificar um teste como teste excluído, clique e no início do teste na área de janela Regra. O e é exibido como e não.
- e. Clique nos parâmetros configuráveis sublinhados para customizar as variáveis do teste.
- f. Na caixa de diálogo, selecione os valores para a variável e clique em **Enviar**.
8. Opcional. Para testar o total de propriedades acumuladas selecionadas para cada grupo de eventos ou fluxo, limpe a caixa de seleção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente**.
9. Na área de janela grupos, selecione as caixas de seleção dos grupos aos quais você deseja designar essa regra. Para obter mais informações, consulte Gerenciamento de grupo de regra.
10. No campo **Notas**, insira todas as notas que você deseja incluir a essa regra. Clique em **Avançar**.
11. Na página Respostas da regra, configure as respostas que você deseja que essa regra gere. “Parâmetros da página Regra de Resposta” na página 130
12. Clique em **Avançar**.
13. Revise a regra configurada. Clique em **Concluir**.

---

## Tarefas de gerenciamento de regra

É possível gerenciar regras customizadas e de anomalia.

É possível ativar e desativar as regras, conforme necessário. É possível também editar, copiar ou excluir uma regra.

É possível criar regras de detecção de anomalias somente nas guias **Atividade de log** e **Atividade de rede**.

Para gerenciar as regras de detecção de anomalias, é necessário usar a página Regras na guia **Ofensas**.

### Ativando e desativando regras

Ao ajustar seu sistema, você poderá ativar ou desativar as regras apropriadas para assegurar-se de que o sistema irá gerar ofensas significativas em seu ambiente.

#### Sobre Esta Tarefa

Você deve ter a permissão de função **Ofensas > Manter regras customizadas** para poder ativar ou desativar uma regra.

#### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir** na página **Regras**, selecione **Regras**.
4. Selecione a regra que você deseja ativar ou desativar.
5. Na caixa de listagem **Ações**, selecione **Ativar/Desativar**.

### Editando uma regra

Você pode editar uma regra para alterar o nome da regra, tipo de regra, testes ou respostas.

## Sobre Esta Tarefa

Você deve ter a permissão de função **Ofensas > Manter regras customizadas** para poder ativar ou desativar uma regra.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir** na página **Regras**, selecione **Regras**.
4. Dê um clique duplo na regra que você deseja editar.
5. Na caixa de listagem **Ações**, selecione **Abrir**.
6. Opcional. Se você desejar alterar o tipo de regra, clique em **Voltar** e selecione um novo tipo de regra.
7. Na página Editor de pilha de teste de regra, edite os parâmetros.
8. Clique em **Avançar**.
9. Na página Resposta de regra, edite os parâmetros.
10. Clique em **Avançar**.
11. Revise a regra editada. Clique em **Concluir**.

## Copiando uma regra

Você pode copiar uma regra existente, inserir um novo nome a regra e customizar os parâmetros na nova regra, conforme necessário.

## Sobre Esta Tarefa

Você deve ter a permissão de função **Ofensas > Manter regras customizadas** para poder ativar ou desativar uma regra.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione **Regras**.
4. Selecione a regra que você deseja duplicar.
5. Na caixa de listagem **Ações**, selecione **Duplicar**.
6. No nome Inserir no campo de regra copiada, insira um nome para a nova regra. Clique em **OK**.

## Excluindo uma regra

Você pode excluir uma regra de seu sistema.

## Sobre Esta Tarefa

Você deve ter a permissão de função **Ofensas > Manter regras customizadas** para poder ativar ou desativar uma regra.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione **Regras**.
4. Selecione a regra que você deseja excluir.



5. Na caixa de listagem **Ações**, selecione **Excluir**.

---

## Gerenciamento do grupo de regras

Se você for um administrador, estará apto a criar, editar e excluir grupos de regras. Categorizar suas regras ou blocos de construção em grupos permite visualizar e rastrear suas regras de maneira eficiente.

Por exemplo, é possível visualizar todas as regras que são relacionadas à conformidade.

À medida que novas regras são criadas, é possível designar a regra para um grupo existente. Para obter informações sobre como designar um grupo usando o assistente de regra, consulte Criando uma regra customizada ou Criando uma regra de detecção de anomalias.

### Visualizando um grupo de regra

Na página Regras, você pode filtrar as regras ou blocos de construção para visualizar apenas as regras ou blocos de construção que pertencem a um grupo específico.

#### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione se você deseja visualizar as regras ou blocos de construção.
4. Na caixa de listagem **Filtros**, selecione a categoria do grupo que você deseja visualizar.

### Criando um grupo

A página Regras fornece grupos de regras padrão, no entanto, você pode criar um novo grupo.

#### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o grupo no qual você deseja criar um novo grupo.
5. Clique em **Novo grupo**.
6. Insira valores para os seguintes parâmetros:
  - **Nome** – insira um nome exclusivo para designar ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
  - **Descrição** – insira uma descrição que deseja designar a esse grupo. A descrição pode ter até 255 caracteres de comprimento.
7. Clique em **OK**.
8. Opcional. Para alterar o local do novo grupo, clique no novo grupo e arraste a pasta para o novo local em sua árvore de navegação.

### Designando um item a um grupo

É possível designar uma regra selecionada ou um bloco de construção a um grupo.



### **Procedimento**

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Selecione a regra ou bloco de construção que deseja designar para um grupo.
4. Na caixa de listagem **Ações**, selecione **Designar grupos**.
5. Selecione o grupo para o qual deseja designar a regra ou o bloco de construção.
6. Clique em **Designar grupos**.
7. Feche a janela **Escolher grupos**.

## **Editando um grupo**

Você pode editar um grupo para alterar o nome ou a descrição.

### **Procedimento**

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o grupo que você deseja editar.
5. Clique em **Editar**.
6. Atualizar os valores para os parâmetros a seguir:
  - **Nome** – insira um nome exclusivo para designar ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
  - **Descrição** – insira uma descrição que deseja designar a esse grupo. A descrição pode ter até 255 caracteres de comprimento.
7. Clique em **OK**.
8. Opcional. Para alterar o local do grupo, clique no novo grupo e arraste a pasta para o novo local em sua árvore de navegação.

## **Copiando um item para outro grupo**

Você pode copiar um bloco de regra ou construção de um grupo para outros grupos.

### **Procedimento**

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o bloco de regra ou construção que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo onde você deseja copiar o bloco de regra ou construção.
7. Clique em **Copiar**.

## **Excluindo um item de um grupo**

É possível excluir um item de um grupo. Ao excluir um item de um grupo, a regra ou o bloco de construção só será excluído do grupo; permanecerá disponível na página Regras.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Clique em **Grupos**.
4. Usando a árvore de navegação, navegue até e selecione o item que deseja excluir.
5. Clique em **Remover**.
6. Clique em **OK**.

## Excluindo um grupo

Você pode excluir um grupo. Ao excluir um grupo, as regras ou blocos de construção desse grupo permanecerão disponíveis na página Regras.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Clique em **Grupos**.
4. Usando a árvore de navegação, navegue até e selecione o grupo que você deseja excluir.
5. Clique em **Remover**.
6. Clique em **OK**.

---

## Editando blocos de construção

É possível editar qualquer um dos blocos de construção padrão para corresponder às necessidades de sua implementação.

### Sobre Esta Tarefa

Um bloco de construção é uma pilha de teste da regra reutilizável que você pode incluir como um componente em outras regras.

Por exemplo, você pode editar o BB:HostDefinition: bloco de construção do Servidor de Correio para identificar todos os servidores de correio na sua implementação. Em seguida, você poderá configurar qualquer regra para excluir seus servidores de correio dos testes de regras.

### Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir**, selecione **Blocos de construção**.
4. Dê um clique duplo no bloco de construção que você deseja editar.
5. Atualize o bloco de construção, conforme necessário.
6. Clique em **Avançar**.
7. Continue através do assistente. Para obter mais informações, consulte Criando um regra customizada.
8. Clique em **Concluir**.

---

## Parâmetros da página Regra

Uma descrição dos parâmetros na página Regras.

A lista de regras implementadas fornece as seguintes informações para cada regra:

*Tabela 43. Parâmetros da página Regras*

Parâmetro	Descrição
Nome da Regra	Exibe o nome da regra.
Grupo	Exibe o grupo ao qual esta regra foi designada. Para obter mais informações sobre grupos, consulte Gerenciamento de grupo de regra.
Categoria da Regra	Exibe a categoria de regra para a regra. As opções incluem Regra customizada e Regra de detecção de anomalias.
Tipo de Regra	Exibe o tipo de regra.  Os tipos de regra incluem: <ul style="list-style-type: none"><li>• Evento</li><li>• Fluxo</li><li>• Comum</li><li>• Ofensa</li><li>• Anomalia</li><li>• Limite</li><li>• Comportamental</li></ul> Para obter mais informações sobre os tipos de regras, consulte Tipos de regra.
Ativado	Indica se a regra está ativada ou desativada. Para obter mais informações sobre como ativar e desativar regras, consulte Ativando e desativando regras.
Resposta	Exibe a resposta da regra, se houver. Respostas de regras incluem: <ul style="list-style-type: none"><li>• Enviar novo evento</li><li>• Email</li><li>• Notificação de log</li><li>• SNMP</li><li>• Conjunto de referência</li><li>• Dados de referência</li><li>• Resposta de IF-MAP</li></ul> Para obter mais informações sobre as respostas de regra, consulte Respostas de regra.
Contagem de Eventos/Fluxos	Exibe o número de eventos ou fluxos que são associados a esta regra quando a regra contribuir para um crime.
Contagem de Crime	Exibe o número de crimes que são geradas por essa regra.
Origem	Exibe se essa regra é uma regra padrão (Sistema) ou uma regra customizada (Usuário).
Data de Criação	Especifica a data e hora que essa regra foi criada.
Data da Modificação	Especifica a data e hora que essa regra foi modificada.

---

## Barra de ferramentas da página Regras

A barra de ferramentas da página Regras é usada para exibir as regras, blocos de construção ou grupos. É possível gerenciar grupos de regras e trabalhar com regras.

A barra de ferramentas da página Regras fornece as seguintes funções:

*Tabela 44. Função da barra de ferramentas da página Regras*

Função	Descrição
Exibir	Na caixa de listagem, selecione se deseja exibir as regras ou blocos de construção na lista de regras.
Grupo	Na caixa de listagem, selecione qual grupo de regra deseja que seja exibido na lista de regras.
Grupos	Clique em <b>Grupos</b> para gerenciar grupos de regra.

Tabela 44. Função da barra de ferramentas da página Regras (continuação)

Função	Descrição
Ações	<p>Clique em <b>Ações</b> e selecione uma das opções a seguir:</p> <ul style="list-style-type: none"> <li>• <b>Nova regra de evento</b> – Selecione esta opção para criar uma nova regra de evento.</li> <li>• <b>Novo fluxo de regra</b> – Selecione esta opção para criar um novo fluxo de regra.</li> <li>• <b>Nova regra comum</b> – Selecione esta opção para criar uma nova regra comum.</li> <li>• <b>Nova regra de crime</b> – Selecione esta opção para criar uma nova regra de crime.</li> <li>• <b>Ativar/desativar</b> – Selecione esta opção para ativar ou desativar as regras selecionadas.</li> <li>• <b>Duplicar</b> – Selecione esta opção para copiar uma regra selecionada.</li> <li>• <b>Editar</b> – Selecione esta opção para editar uma regra selecionada.</li> <li>• <b>Excluir</b> – Selecione esta opção para excluir uma regra selecionada.</li> <li>• <b>Designar grupos</b> – Selecione esta opção para designar regras selecionadas para grupos de regra.</li> </ul>
Reverter regra	<p>Clique em <b>Reverter regra</b> para reverter uma regra do sistema modificado para o valor padrão. Ao clicar em <b>Reverter regra</b>, uma janela de confirmação será exibida. Ao reverter uma regra, quaisquer modificações anteriores são removidas permanentemente.</p> <p>Para reverter a regra e manter uma versão modificada, duplique a regra e use a opção <b>Reverter regra</b> na regra modificada.</p>
Procurar regras	<p>Digite seus critérios de procura no campo <b>Procurar regras</b> e clique no ícone <b>Procurar regras</b> ou pressione Enter no teclado. Todas as regras que correspondem aos seus critérios de procura são exibidas na lista de regras.</p> <p>Os seguintes parâmetros são pesquisados para uma correspondência com seus critérios de procura:</p> <ul style="list-style-type: none"> <li>• Nome da Regra</li> <li>• Regra (descrição)</li> <li>• Notes</li> <li>• Resposta</li> </ul> <p>O recurso Procurar regra tenta localizar uma correspondência direta da sequência de texto. Se nenhuma correspondência for encontrada, o recurso Procurar regra tentará uma correspondência de expressão regular (regex).</p>

## Parâmetros da página Regra de Resposta

Há parâmetros para a página Resposta de regra.

A tabela a seguir fornece os parâmetros de página Resposta de regra.

Tabela 45. Parâmetros de página Evento, Fluxo, e Resposta de regra

Parâmetro	Descrição
Gravidade	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a severidade. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de severidade apropriado.
Credibilidade	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a credibilidade. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de credibilidade apropriado.
Relevância	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a relevância. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de relevância apropriado.

Tabela 45. Parâmetros de página Evento, Fluxo, e Resposta de regra (continuação)

Parâmetro	Descrição
Assegure-se de que o evento detectado é parte de um crime	<p>Selecione essa caixa de seleção se desejar que o evento seja encaminhado para o componente Magistrate. Se nenhum crime existir na guia Ofensas, uma nova ofensa será criada. Se um crime existir, esse evento será incluído na ofensa.</p> <p>Ao selecionar essa caixa de seleção, as seguintes opções serão exibidas:</p> <p><b>Indexar ofensa com base em</b></p> <p>Na caixa de listagem, selecione o parâmetro no qual você deseja indexar o crime. O padrão é IPv6 de origem.</p> <p>Para regras de eventos, as opções incluem IP de destino, IPv6 de destino, endereço MAC de destino, porta de destino, nome do evento, nome do host, origem do log, regra, IP de origem, IPv6 de origem, endereço MAC de origem, porta de origem ou nome de usuário.</p> <p>Para as regras de fluxo, as opções incluem ID do aplicativo, ASN de destino, IP de destino, identidade do IP de destino, porta de destino, nome do evento, regra, ASN de origem, identidade de IP de origem ou porta de origem.</p> <p>Para regras comuns, as opções incluem IP de destino, identidade de IP de destino, porta de destino, regra, IP de origem, identidade de IP de origem e porta de origem.</p> <p><b>Anotar essa ofensa</b> Selecione essa caixa de seleção para incluir uma anotação a essa ofensa e digite a anotação.</p> <p><b>Incluir eventos detectados por &lt;índice&gt; desse ponto em diante, por segundo(s), na ofensa</b> Selecione essa caixa de seleção e digite o número de segundos que deseja para incluir os eventos detectados por &lt;índice&gt; na guia <b>Ofensas</b>. Este campo especifica o parâmetro no qual o crime é indexada. O padrão é IP de origem.</p>
Annotate event	Selecione essa caixa de seleção se desejar incluir uma anotação neste evento e digite a anotação que deseja incluir no evento.
Drop the detected event	<p>Selecione esta caixa de seleção para forçar um evento, que normalmente é enviado para o componente Magistrate, a ser enviado para o banco de dados Ariel, para geração de relatórios ou procura.</p> <p>Este evento não é exibido na guia <b>Ofensas</b>.</p>
Enviar novo evento	<p>Selecione essa caixa de seleção para enviar um novo evento além do fluxo ou evento original, que é processado como todos os outros eventos no sistema.</p> <p>Selecione essa caixa de seleção para enviar um novo evento além do original, que é processado como todos os outros eventos no sistema.</p> <p>Os parâmetros <b>Dispatch New Event</b> serão exibidos ao selecionar essa caixa de seleção. Por padrão, a caixa de seleção está limpa.</p>
Nome do Evento	Digite um nome exclusivo para o evento que deseja que seja exibido na guia <b>Ofensas</b> .
Descrição do Evento	Digite uma descrição para o evento. A descrição é exibida na área de janela Anotações dos detalhes do evento.
Gravidade	Na caixa de listagem, selecione a severidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 0. A severidade é exibida na área de janela Anotação dos detalhes do evento.
Credibilidade	Na caixa de listagem, selecione a credibilidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 10. Credibilidade é exibida na área de janela Anotação dos detalhes do evento.
Relevância	Na caixa de listagem, selecione a relevância do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 10. A relevância é exibida na área de janela Anotação dos detalhes do evento.
Categoria de Alto Nível	Na caixa de listagem, selecione a categoria de evento de alto nível que deseja que esta regra use ao processar eventos.
Categoria de Nível Baixo	Na caixa de listagem, selecione a categoria de evento de nível inferior que deseja que esta regra use ao processar eventos.
Anotar essa ofensa	Selecione essa caixa de seleção para incluir uma anotação a essa ofensa e digite a anotação.

Tabela 45. Parâmetros de página Evento, Fluxo, e Resposta de regra (continuação)

Parâmetro	Descrição
Assegure-se de que o evento de envio é parte de um crime	<p>Marque esta caixa de seleção se desejar, como resultado desta regra, o evento que é enviado para o componente Magistrate. Se nenhum crime for criada na guia <b>Ofensas</b>, uma nova ofensa será criada. Se um crime existir, esse evento será incluído.</p> <p>Ao selecionar essa caixa de seleção, as seguintes opções serão exibidas:</p> <p><b>Indexar ofensa com base em</b></p> <p>Na caixa de listagem, selecione o parâmetro no qual você deseja indexar o crime. O padrão é IP de origem.</p> <p>Para regras de eventos, as opções incluem IP de destino, IPv6 de destino, endereço MAC de destino, porta de destino, nome do evento, nome do host, origem do log, regra, IP de origem, IPv6 de origem, endereço MAC de origem, porta de origem ou nome de usuário.</p> <p>Para as regras de fluxo, as opções incluem ID do aplicativo, ASN de destino, IP de destino, identidade do IP de destino, porta de destino, nome do evento, regra, ASN de origem, identidade de IP de origem ou porta de origem.</p> <p>Para regras comuns, as opções incluem IP de destino, identidade de IP de destino, porta de destino, regra, IP de origem, identidade de IP de origem e porta de origem.</p> <p><b>Incluir eventos detectados por &lt;índice&gt; desse ponto em diante, por segundo(s), na ofensa</b>                      Selecione essa caixa de seleção e digite o número de segundos que deseja para incluir os eventos detectados por &lt;índice&gt; na guia <b>Ofensas</b>. Este campo especifica o parâmetro no qual o crime é indexada. O padrão é IP de origem.</p> <p><b>Nomenclatura de crime</b>                      Selecione uma das opções a seguir:</p> <p><b>Essas informações devem contribuir para o nome da(s) ofensa(s) associada(s)</b>                      Selecione esta opção se desejar que as informações de Nome de Evento contribuam para o nome da ofensa.</p> <p><b>Esta informação deverá configurar ou substituir o nome da(s) ofensa(s) associada(s)</b>                      Selecione esta opção se desejar que o Nome do Evento configurado seja o nome da ofensa.</p> <p><b>Essas informações não deveriam contribuir para a nomenclatura da(s) ofensa(s) associada(s)</b>                      Selecione esta opção se não desejar que as informações de Nome de Evento contribuam para o nome da ofensa.</p>
Email	Selecione essa caixa de seleção para exibir as opções de email. Por padrão, a caixa de seleção está limpa.
Insira endereços de email a serem notificados	Digite o endereço de email para o qual enviar uma notificação se esta regra gerar. Use uma vírgula para separar diversos endereços de email.
SNMP Trap	<p>Esse parâmetro só será exibido quando os parâmetros de Configurações SNMP forem definidos nas configurações do sistema.</p> <p>Selecione esta caixa de seleção para ativar esta regra para enviar uma notificação SNMP (trap).</p> <p>A saída do trap SNMP inclui o tempo do sistema, OID de trap e dados de notificação, conforme definido pelo MIB.</p>
Send to Local SysLog	<p>Selecione essa caixa de seleção se desejar registrar o evento ou fluxo localmente.</p> <p>Por padrão, essa caixa de seleção é limpa.</p> <p><b>Nota:</b> Apenas os eventos normalizados podem ser registrados localmente em um dispositivo. Se desejar enviar dados de eventos brutos, você deverá usar a opção Enviar para destinos de encaminhamento para enviar os dados para um host syslog remoto.</p>
Send to Forwarding Destinations	<p>Esta caixa de seleção é exibida apenas para regras de eventos.</p> <p>Selecione essa caixa de seleção se desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema do fornecedor, como sistema SIEM, de chamadas ou de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento será exibida. Selecione a caixa de seleção do destino de encaminhamento que deseja para enviar este evento ou fluxo.</p> <p>Para incluir, editar ou excluir um destino de encaminhamento, clique no link <b>Gerenciar destinos</b>.</p>

Tabela 45. Parâmetros de página Evento, Fluxo, e Resposta de regra (continuação)

Parâmetro	Descrição
Notify	<p>Selecione essa caixa de seleção se desejar eventos que são gerados como resultado desta regra a ser exibida no item Notificações do sistema na guia Painel.</p> <p>Se ativar notificações, configure o parâmetro <b>Response Limiter</b>.</p>
Add to Reference Set	<p>Selecione essa caixa de seleção se desejar que eventos que foram gerados como resultado desta regra incluam dados a um conjunto de referência.</p> <p>Para incluir dados em um conjunto de referência:</p> <ol style="list-style-type: none"> <li>Usando a primeira caixa de listagem, selecione os dados que deseja incluir. As opções incluem todos os dados normalizados ou customizados.</li> <li>Usando a segunda caixa de listagem, selecione a referência configurada na qual deseja incluir os dados especificados.</li> </ol> <p>A resposta de regra <b>Incluir no conjunto de referência</b> fornece as seguintes funções:</p> <p><b>Atualizar</b> Clique em <b>Atualizar</b> para atualizar a primeira caixa de listagem para assegurar-se de que a lista é atual.</p> <p><b>Configurar Conjuntos de Referência</b> Clique em <b>Configurar conjuntos de referência</b> para configurar o conjunto de referência. Esta opção estará disponível apenas se tiver permissões administrativas.</p>
Add to Reference Data	<p>Antes de poder usar essa resposta de regra, é necessário criar a coleção de dados de referência usando a interface da linha de comandos (CLI). Para obter mais informações sobre como criar e usar as coleções de dados de referência, consulte o <i>Guia de Administração</i> do seu produto.</p> <p>Selecione essa caixa de seleção se desejar eventos que são gerados como resultado desta regra para incluir uma coleção de dados de referência. Após selecionar a caixa de seleção, selecione uma das seguintes opções:</p> <p><b>Incluir em um mapa de referência</b> Selecione esta opção para enviar dados para uma coleção de coleção pares de valor chave múltiplo/único. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência ao qual deseja incluir o registro de dados.</p> <p><b>Incluir a um mapa de referência de conjuntos</b> Selecione esta opção para enviar dados para uma coleção de pares de chave/valor único. É necessário selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência de conjuntos ao qual deseja incluir o registro de dados.</p> <p><b>Incluir a um mapa de referência de mapas</b> Selecione esta opção para enviar dados para uma coleção de vários pares de chave múltipla/valor único. É necessário selecionar uma chave para o primeiro mapa, uma chave para o segundo mapa, e, em seguida, o valor para o registro de dados. É necessário também selecionar o mapa de referência de mapas ao qual deseja incluir o registro de dados.</p> <p><b>Incluir a uma tabela de referência</b> Selecione esta opção para enviar dados para uma coleção pares de valor chave múltiplo/único, onde um tipo foi designado às chaves secundárias. Selecione a tabela de referência para a qual deseja incluir dados e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.</p>
Publish on the IF-MAP Server	Se os parâmetros IF-MAP estiverem definidos e implementados nas configurações do sistema, selecione esta opção para publicar as informações de evento sobre o servidor IF-MAP.
Response Limiter	Selecione esta caixa de opções e use as caixas de listagem para configurar a frequência com a qual deseja que esta regra responda.
Enable Rule	Selecione esta caixa de seleção para ativar esta regra.

A tabela a seguir fornece os parâmetros de página Resposta de regra se o tipo de regra for Ofensa.

Tabela 46. Parâmetros da página Resposta da regra de crime

Parâmetro	Descrição
Name/Annotate the detected offense	Selecione essa caixa de seleção para exibir as opções de Nome.
New Offense Name	Digite o nome que deseja designar à ofensa.
Offense Annotation	Digite a anotação de crime que deseja que sejam exibidos na guia Ofensas.

**Tabela 46. Parâmetros da página Resposta da regra de crime (continuação)**

Parâmetro	Descrição
Offense Name	<p>Selecione uma das opções a seguir:</p> <p><b>Essas informações devem contribuir para o nome da ofensa</b>                      Selecione esta opção se desejar que as informações de Nome de Evento contribuam para o nome da ofensa.</p> <p><b>Esta informação deverá configurar ou substituir o nome da ofensa</b>                      Selecione esta opção se desejar que o Nome do Evento configurado seja o nome da ofensa.</p>
Email	Selecione essa caixa de seleção para exibir as opções de email.
Enter email address to notify	Digite o endereço de email para enviar a notificação se o evento for gerado. Use uma vírgula para separar diversos endereços de email.
SNMP Trap	<p>Esse parâmetro só será exibido quando os parâmetros de Configurações SNMP forem definidos nas configurações do sistema.</p> <p>Selecione esta caixa de seleção para ativar esta regra para enviar uma notificação SNMP (trap). Para uma regra de crime, a saída do trap SNMP inclui o tempo do sistema, o OID de trap e os dados de notificação, conforme definido pelo MIB.</p>
Send to Local SysLog	Selecione essa caixa de seleção se desejar registrar o evento ou fluxo localmente.
Send to Forwarding Destinations	<p>Selecione essa caixa de seleção se desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema do fornecedor, como sistema SIEM, de chamadas ou de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento será exibida. Selecione a caixa de seleção do destino de encaminhamento que deseja para enviar este evento ou fluxo.</p> <p>Para incluir, editar ou excluir um destino de encaminhamento, clique no link <b>Gerenciar destinos</b>.</p>
Publish on the IF-MAP Server	Se os parâmetros IF-MAP estiverem configurados e implementados nas configurações do sistema, selecione esta opção para publicar as informações de crime sobre o servidor IF-MAP.
Response Limiter	Selecione esta caixa de seleção e use as caixas de listagem para configurar a frequência com a qual deseja que esta regra responda.
Enable Rule	Selecione esta caixa de seleção para ativar esta regra. Por padrão, a caixa de seleção fica selecionada.

A tabela a seguir fornece os parâmetros de página Resposta de regra se o tipo de regra for Anomalia.

**Tabela 47. Parâmetros de página Resposta da regra de detecção de anomalias**

Parâmetro	Descrição
Enviar novo evento	Especifica que esta regra envia um novo evento além do evento ou fluxo adicional, que é processado como todos os outros eventos no sistema. Por padrão, essa caixa de seleção será selecionada e não poderá ser limpa.
Nome do Evento	Digite o nome exclusivo do evento que deseja que seja exibido na guia Ofensas.
Descrição do Evento	Digite uma descrição para o evento. A descrição é exibida na área de janela Anotações dos detalhes do evento.
Nomenclatura do Crime	<p>Selecione uma das opções a seguir:</p> <p><b>Essas informações devem contribuir para o nome da(s) ofensa(s) associada(s)</b>                      Selecione esta opção se desejar que as informações de Nome de Evento contribuam para o nome da ofensa.</p> <p><b>Esta informação deverá configurar ou substituir o nome da(s) ofensa(s) associada(s)</b>                      Selecione esta opção se desejar que o Nome do Evento configurado seja o nome da ofensa.</p> <p><b>Essas informações não deveriam contribuir para a nomenclatura da(s) ofensa(s) associada(s)</b>                      Selecione esta opção se não desejar que as informações de Nome de Evento contribuam para o nome da ofensa.</p>
Gravidade Usando as caixas de listagem, selecione a severidade do evento.	O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A Severidade é exibida na área de janela Anotações dos detalhes do evento.
Credibilidade	Usando as caixas de listagem, selecione a credibilidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A credibilidade é exibida na área de janela Anotações dos detalhes do evento.
Relevância	Usando as caixas de listagem, selecione a relevância do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A relevância é exibida na área de janela Anotações dos detalhes do evento.
Categoria de Alto Nível	Na caixa de listagem, selecione a categoria de evento de alto nível que deseja que esta regra use ao processar eventos.
Categoria de Nível Baixo	Na caixa de listagem, selecione a categoria de evento de nível inferior que deseja que esta regra use ao processar eventos.
Anotar essa ofensa	Selecione essa caixa de seleção para incluir uma anotação a essa ofensa e digite a anotação.



Tabela 47. Parâmetros de página Resposta da regra de detecção de anomalias (continuação)

Parâmetro	Descrição
Assegure-se de que o evento de envio é parte de um crime	<p>Como resultado dessa regra, o evento é encaminhado para o componente Magistrate. Se um crime existir, esse evento será incluído. Se nenhum crime for criada na guia Ofensas, uma nova ofensa será criada.</p> <p>As opções a seguir são exibidas:</p> <p><b>Indexar ofensa com base em</b> Especifica que a nova ofensa é baseada no nome do evento. Este parâmetro é ativado por padrão.</p> <p><b>Incluir eventos detectados por Nome do evento desse ponto em diante, por segundo(s), na ofensa</b> Selecione esta caixa de seleção e digite o número de segundos que deseja para incluir eventos detectados ou fluxos a partir da origem na guia Ofensas.</p>
Email	Selecione essa caixa de seleção para exibir as opções de email.
Enter email address to notify	Digite o endereço de email para o qual enviar uma notificação se esta regra gerar. Use uma vírgula para separar diversos endereços de email.
Enter email address to notify	Digite o endereço de email para o qual enviar uma notificação se esta regra gerar. Use uma vírgula para separar diversos endereços de email.
Notify	Selecione essa caixa de seleção se desejar que os eventos que forem gerados como resultado dessa regra sejam exibidos no item Notificações do sistema na guia Painel. Se ativar notificações, configure o parâmetro <b>Response Limiter</b> .
Send to Local SysLog	<p>Selecione essa caixa de seleção se desejar registrar o evento ou fluxo localmente. Por padrão, a caixa de seleção está limpa.</p> <p><b>Nota:</b> Apenas os eventos normalizados podem ser registrados localmente em um dispositivo QRadar. Se desejar enviar dados de eventos brutos, você deverá usar a opção Enviar para destinos de encaminhamento para enviar os dados para um host syslog remoto.</p>
Add to Reference Set	<p>Selecione essa caixa de seleção se desejar que eventos que foram gerados como resultado desta regra incluam dados a um conjunto de referência.</p> <p>Para incluir dados em um conjunto de referência:</p> <ol style="list-style-type: none"> <li>Usando a primeira caixa de listagem, selecione os dados que deseja incluir. As opções incluem todos os dados normalizados ou customizados.</li> <li>Usando a segunda caixa de listagem, selecione o conjunto de referência no qual deseja incluir os dados especificados.</li> </ol> <p>A resposta de regra <b>Incluir no conjunto de referência</b> fornece as seguintes funções:</p> <p><b>Atualizar</b> Clique em <b>Atualizar</b> para atualizar a primeira caixa de listagem para assegurar-se de que a lista é atual.</p> <p><b>Configurar Conjuntos de Referência</b> Clique em <b>Configurar conjuntos de referência</b> para configurar o conjunto de referência. Esta opção estará disponível apenas se tiver permissões administrativas.</p>

Tabela 47. Parâmetros de página Resposta da regra de detecção de anomalias (continuação)

Parâmetro	Descrição
Add to Reference Data	<p>Antes de poder usar essa resposta de regra, é necessário criar a coleção de dados de referência usando a interface da linha de comandos (CLI). Para obter mais informações sobre como criar e usar as coleções de dados de referência, consulte o <i>Guia de Administração</i> do seu produto.</p> <p>Selecione essa caixa de seleção se desejar eventos que são gerados como resultado desta regra para incluir uma coleção de dados de referência. Após selecionar a caixa de seleção, selecione uma das seguintes opções:</p> <p><b>Incluir em um mapa de referência</b> Selecione esta opção para enviar dados para uma coleção de coleção pares de valor chave múltiplo/único. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência ao qual deseja incluir o registro de dados.</p> <p><b>Incluir a um mapa de referência de conjuntos</b> Selecione esta opção para enviar dados para uma coleção de pares de chave/valor único. É necessário selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência de conjuntos ao qual deseja incluir o registro de dados.</p> <p><b>Incluir a um mapa de referência de mapas</b> Selecione esta opção para enviar dados para uma coleção de vários pares de chave múltipla/valor único. É necessário selecionar uma chave para o primeiro mapa, uma chave para o segundo mapa, e, em seguida, o valor para o registro de dados. É necessário também selecionar o mapa de referência de mapas ao qual deseja incluir o registro de dados.</p> <p><b>Incluir a uma tabela de referência</b> Selecione esta opção para enviar dados para uma coleção pares de valor chave múltiplo/único, onde um tipo foi designado às chaves secundárias. Selecione a tabela de referência para a qual deseja incluir dados e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.</p>
Publish on the IF-MAP Server	Se os parâmetros IF-MAP estiverem configurados e implementados nas configurações do sistema, selecione esta opção para publicar as informações de crime sobre o servidor IF-MAP.
Response Limiter	Selecione essa caixa de seleção e use as caixas de listagem para configurar a frequência com que você deseja que essa regra responda
Enable Rule	Selecione esta caixa de seleção para ativar esta regra. Por padrão, a caixa de seleção fica selecionada.

Uma notificação SNMP pode se parecer com:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
ICMP Destination Unreachable Communication with Destination Host is
Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
Offense description"
```

Uma 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
```

---

## Capítulo 11. Parâmetros da página Perfil de ativo

É possível localizar as descrições de parâmetro da página Perfil de ativo para a área de janela Resumo de ativo, Interface de rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de risco e Produtos.

Esta referência inclui tabelas que descrevem os parâmetros que são exibidos em cada área de janela da guia **Perfil de ativo**.

---

### Perfis de ativos

Perfis de ativos fornecem informações sobre cada ativo conhecido em sua rede, incluindo quais serviços estão em execução em cada ativo.

A informação do perfil de ativos é usada para propósitos de correlação para ajudar a reduzir positivos falsos. Por exemplo, se uma origem tentar explorar um serviço específico em execução em um ativo, o QRadar determinará se o ativo está vulnerável a este ataque correlacionando o ataque ao perfil de ativo.

Perfis de ativos são descobertos automaticamente se você tiver varreduras de dados de fluxo ou de avaliação de vulnerabilidades (VA) configuradas. Para transmitir dados para preencher perfis de ativos, fluxos bidirecionais são necessários. Perfis de ativos também podem ser criados automaticamente a partir de eventos da identidade. Para obter mais informações sobre VA, consulte o *Guia de Avaliação do IBM Security QRadar Vulnerability*.

Para obter mais informações sobre origens de fluxo, consulte o *IBM Security QRadar SIEM Administration Guide*.

---

### Sobre vulnerabilidades

É possível usar o QRadar Vulnerability Manager e os scanners de terceiros para identificar vulnerabilidades.

Scanners de terceiros identificam e relatam as vulnerabilidades descobertas usando referências externas, como o Banco de Dados de Vulnerabilidade de Software Livre (OSVDB), Banco de Dados de Vulnerabilidade Nacional (NVDB) e Critical Watch. Exemplos de scanners de terceiros incluem QualysGuard e nCircle ip360. O OSVDB designa um identificador de referência exclusivo (ID do OSVDB) para cada vulnerabilidade. Referências externas designam um identificador de referência exclusivo para cada vulnerabilidade. Exemplos de IDs de referência de dados externos incluem Vulnerabilidade Comum e Exposições (CVE) ou ID de Bugtraq. Para obter mais informações sobre os scanners e avaliação de vulnerabilidades, consulte o *IBM Security QRadar Vulnerability Manager User Guide*.

O QRadar Vulnerability Manager é um componente que pode ser comprado separadamente e ativado usando uma chave de licença. O QRadar Vulnerability Manager é uma plataforma de varredura de rede que fornece reconhecimento de vulnerabilidades que existem em aplicativos, sistemas ou dispositivos em sua rede. Após varreduras identificarem vulnerabilidades, será possível procurar e revisar dados de vulnerabilidade, corrigir vulnerabilidades e executar varreduras novamente para avaliar o novo nível de risco.

Quando QRadar Vulnerability Manager for ativado, será possível executar tarefas de avaliação de vulnerabilidades na guia **Vulnerabilidades**. Na guia **Ativos**, é possível executar varreduras nos ativos selecionados.

Para obter mais informações, consulte *IBM Security QRadar Vulnerability Manager User Guide*

---

## Visão geral da guia Ativos

A guia **Ativos** fornece uma área de trabalho a partir da qual é possível gerenciar seus ativos de rede e investigar as vulnerabilidades, portas, aplicativos, histórico e outras associações de um ativo.

Usando a guia **Ativos**, é possível:

- Visualizar todos os ativos descobertos.
- Incluir manualmente os perfis de ativos.
- Procurar ativos específicos.
- Visualizar informações sobre ativos descobertos.
- Editar os perfis de ativos para ativos manualmente incluídos ou descobertos.
- Ajustar vulnerabilidades de positivo falso.
- Importar ativos.
- Imprimir ou exportar perfis de ativo.
- Descobrir os ativos.
- Configurar e gerenciar varreduras de vulnerabilidade de terceiros.
- Iniciar as varreduras do Gerenciador de Vulnerabilidade do QRadar.

Para obter informações sobre a opção Descoberta de servidor na área de janela de navegação, consulte o *IBM Security QRadar SIEM Administration Guide*

Para obter mais informações sobre a opção Varredura VA na área de janela de navegação, consulte o *IBM Security QRadar Risk Manager User Guide*.

## Lista da guia Ativo

A página Perfis de ativo fornece informações sobre ID, endereço IP, nome do ativo, pontuação do CVSS agregado, vulnerabilidades e serviços.

A página Perfis de ativo fornece as seguintes informações sobre cada ativo:

*Tabela 48. Parâmetros da página Perfil de ativo*

Parâmetro	Descrição
ID	Exibe o número do ID de ativo do ativo. O número do ID de ativo será automaticamente gerado ao incluir um perfil de ativo manualmente ou quando os ativos forem descobertos por meio de fluxos, eventos ou varreduras de vulnerabilidade.
IP Address	Exibe o último endereço IP conhecido do ativo.
Asset Name	Exibe o nome fornecido, nome NetBios, nome DSN ou endereço MAC do ativo. Se desconhecido, esse campo exibirá o último endereço IP conhecido. <b>Nota:</b> Estes valores são exibidos em ordem de prioridade. Por exemplo, se o ativo não tiver um nome fornecido, o nome NetBios agregado será exibido.  Se o ativo for descoberto automaticamente, esse campo será preenchido automaticamente, no entanto, é possível editar o nome do ativo, se necessário.

Tabela 48. Parâmetros da página Perfil de ativo (continuação)

Parâmetro	Descrição
Risk Score	<p>Exibe uma das seguintes pontuações do Sistema de Pontuação de Vulnerabilidade Comum (CVSS):</p> <ul style="list-style-type: none"> <li>• Pontuação do CVSS ambiental agregada unida</li> <li>• Agregar pontuação do CVSS temporal</li> <li>• Agregar pontuação base do CVSS</li> <li>•</li> </ul> <p>Essas pontuações são exibidas na ordem de prioridade. Por exemplo, se a pontuação do CVSS ambiental agregada unida não estiver disponível, a pontuação do CVSS temporal agregada será exibida.</p> <p>Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A contagem do CVSS é calculada a partir dos seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> <li>• Potencial de Danos Colaterais</li> <li>• Requisito de Confidencialidade</li> <li>• Requisito de Disponibilidade</li> <li>• Requisito de Integridade</li> </ul> <p>Para obter mais informações sobre como configurar estes parâmetros, consulte "Incluindo ou editando um perfil do ativo" na página 141.</p> <p>Para obter mais informações sobre o CVSS, consulte <a href="http://www.first.org/cvss/">http://www.first.org/cvss/</a>.</p>
Vulnerabilidades	Exibe o número de vulnerabilidades exclusivas que são descobertas neste ativo. Este valor também inclui o número de vulnerabilidades ativas e passivas.
Serviços	Exibe o número de aplicativos de Camada 7 exclusivos executados neste ativo.
Último Usuário	Exibe o último usuário associado ao ativo.
Último Usuário Visto	Exibe a hora em que o último usuário associado ao ativo foi visto pela última vez.

## Opções do menu ativado pelo botão direito

Clicar com o botão direito em um ativo na guia Ativo exibe os menus Navegar, Informações e Executar varredura de QVM para obter mais informações sobre filtro de eventos.

Na guia **Ativos**, é possível clicar com o botão direito em um ativo para acessar mais informações de filtro de eventos.

Tabela 49. Opções do menu ativado pelo botão direito

Opção	Descrição
Navegar	<p>O menu <b>Navegar</b> fornece as seguintes opções:</p> <ul style="list-style-type: none"> <li>• <b>Visualização por rede</b> – Exibe a janela Lista de redes, que exibe todas as redes que são associadas ao endereço IP selecionado.</li> <li>• <b>Visualizar resumo de origem</b> – Exibe a janela Lista de crimes, que exibe todas as ofensas que são associadas ao endereço IP de origem selecionado.</li> <li>• <b>Visualizar resumo de destino</b> – Exibe a janela Lista de crimes, que exibe todas as ofensas associadas ao endereço IP de destino selecionado.</li> </ul>

Tabela 49. Opções do menu ativado pelo botão direito (continuação)

Opção	Descrição
Informações	<p>O menu <b>Informações</b> fornece as seguintes opções:</p> <ul style="list-style-type: none"> <li>• <b>Consulta DNS</b> – Procura por entradas DNS que são baseadas no endereço IP.</li> <li>• <b>Consulta WHOIS</b> - Procura o proprietário registrado de um endereço IP remoto. O servidor de WHOIS padrão é whois.arin.net.</li> <li>• <b>Varredura de porta</b> – Executa uma varredura do Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível somente se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do seu fornecedor.</li> <li>• <b>Perfil de ativo</b> – Exibe informações de perfil de ativo. Essa opção de menu só ficará disponível quando os dados do perfil forem adquiridos ativamente por uma varredura ou passivamente por origens de fluxo.</li> <li>• <b>Procurar eventos</b> – Selecione a opção <b>Procurar eventos</b> para procurar eventos que são associados a este endereço IP.</li> <li>• <b>Procurar fluxos</b> – Selecione a opção <b>Procurar fluxos</b> para procurar fluxos que estão associados a este endereço IP.</li> </ul>
Executar varredura do QVM	<p>Selecione esta opção para executar uma varredura do Gerenciador de Vulnerabilidades no ativo selecionado.</p> <p>Essa opção será exibida somente após o QRadar Vulnerability Manager estar instalado.</p>

## Visualizando um perfil de ativo

Na lista de ativos na guia **Ativos**, você pode selecionar e visualizar um perfil de ativo. Um perfil de ativos fornece informações sobre cada perfil.

### Sobre Esta Tarefa

Informações do perfil de ativo são descobertas automaticamente por meio do Server Discovery ou configuradas manualmente. Você pode editar informações de perfil de ativo geradas automaticamente.

A página Perfil de Ativo fornece as informações sobre o ativo que está organizado em várias áreas de janela. Para visualizar uma área de janela, você pode clicar na seta (>) na área de janela para visualizar mais detalhes ou selecionar a área de janela da caixa de listagem **Exibir** na barra de ferramentas.

A barra de ferramentas da página Perfil de Ativo fornece as seguintes funções:

Tabela 50. Funções da barra de ferramentas da página Perfil de Ativo

Opções	Descrição
Retornar à lista de ativos	Clique nesta opção para retornar à lista de ativos.
Exibir	<p>Na caixa de listagem, você pode selecionar a área de janela que você deseja visualizar na área de janela de Perfil de Ativo. As áreas de janela Resumo de Ativo e Resumo de Interface de Rede são sempre exibidas.</p> <p>Para obter mais informações sobre os parâmetros que são exibidos em cada área de janela, consulte <b>Ativos</b> página parâmetros de perfil.</p>
Editar ativo	Clique nesta opção para editar o Perfil de Ativo. Consulte “Incluindo ou editando um perfil do ativo” na página 141.
Visualização por rede	Se esse ativo estiver associado a um crime, essa opção permitirá que você visualize a lista de redes associadas a esse ativo. Quando você clica <b>Visualização por rede</b> , a janela Lista de Redes é exibida. Consulte “Monitorando ofensas agrupadas por rede” na página 29.
Visualizar resumo de origem	Se esse ativo for a origem de um crime, essa opção permitirá que você visualize as informações de resumo da origem. Quando você clicar em <b>Visualizar resumo de origem</b> , a janela Lista de crimes é exibida. Consulte “Monitorando ofensas agrupadas por IP de origem” na página 28.

Tabela 50. Funções da barra de ferramentas da página Perfil de Ativo (continuação)

Opções	Descrição
Visualizar resumo de destino	<p>Se este ativo for o destino de um crime, essa opção permitirá que você visualize informações de resumo de destino.</p> <p>Quando você clica em <b>Visualizar resumo de destino</b>, a janela Lista de Destinos é exibida. Consulte “Monitorando ofensas agrupadas por IP de destino” na página 28.</p>
Histórico	<p>Clique em <b>Histórico</b> para visualizar informações do histórico de eventos para este ativo. Quando você clica no ícone <b>Histórico</b>, a janela Procura de eventos é exibida, pré-preenchida com critérios de procura de eventos:</p> <p>Você pode customizar os parâmetros de procura, se necessário. Clique em <b>Procurar</b> para visualizar as informações do histórico de eventos.</p>
Aplicativos	<p>Clique em <b>Aplicativos</b> para visualizar informações do aplicativo para este ativo. Quando você clica no ícone <b>Aplicativos</b>, a janela Procura de Fluxo é exibida, pré-preenchida com critérios de procura do evento.</p> <p>Você pode customizar os parâmetros de procura, se necessário. Clique em <b>Procurar</b> para visualizar as informações do aplicativo.</p>
Conexões de procura	<p>Clique em <b>Conexões de procura</b> para procurar por conexões. A janela Procura de conexão é exibida.</p> <p>Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i>.</p>
Visualizar topologia	<p>Clique em <b>Visualizar topologia</b> para investigar melhor o ativo. A janela Topologia atual é exibida.</p> <p>Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i>.</p>
Ações	<p>Na lista <b>Ações</b>, selecione <b>Histórico de vulnerabilidade</b>.</p> <p>Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter informações adicionais, consulte <i>IBM Security QRadar Risk Manager User Guide</i>.</p>

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**
3. Clique duas vezes no ativo que você deseja visualizar.
4. Use as opções na barra de ferramentas para exibir várias áreas de janela de informação do perfil de ativos. Consulte Editando um perfil de ativo.
5. Para pesquisar as vulnerabilidades associadas, clique em cada vulnerabilidade na área de janela Vulnerabilidades. Consulte a Tabela 10-10
6. Se necessário, edite o perfil de ativo. Consulte Editando um perfil de ativo.
7. Clique em **Retornar para Lista de Ativos** para selecionar e visualizar outro ativo, se necessário.

## Incluindo ou editando um perfil do ativo

Perfis de ativos são descobertos e incluídos automaticamente; no entanto, talvez seja necessário que você inclua um perfil manualmente

### Sobre Esta Tarefa

Quando ativos são descobertos usando a opção de Descoberta do Servidor, alguns detalhes do perfil de ativos são preenchidos automaticamente. Você pode incluir manualmente as informações para o perfil do ativo e você pode editar determinados parâmetros.

Você só pode editar os parâmetros que foram inseridos manualmente. Os parâmetros que foram gerados pelo sistema são exibidos em itálico e não são editáveis. Você pode excluir os parâmetros gerados pelo sistema, se necessário.

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Escolha uma das opções a seguir:
  - Para incluir um ativo, clique em **Incluir ativo** e digite o endereço IP ou intervalo do CIDR do ativo no campo **Novo endereço IP**.
  - Para editar um ativo, clique duas vezes no ativo que você deseja visualizar e clique em **Editar ativo**.
4. Configure os parâmetros na área de janela do Endereço IP & do MAC. Configure uma ou mais das seguintes opções:
  - Clique no ícone **Novo endereço MAC** e digite um Endereço MAC na caixa de diálogo.
  - Clique no ícone **Novo endereço IP** e digite um endereço IP na caixa de diálogo.
  - Se **NIC desconhecido** estiver listado, você poderá selecionar esse item, clicar no ícone **Editar** e digitar um novo endereço MAC na caixa de diálogo.
  - Selecione um endereço MAC ou IP da lista, clique no ícone **Editar** e digite um novo endereço MAC na caixa de diálogo.
  - Selecione um endereço MAC ou IP na lista e clique no ícone **Remover**.
5. Configure os parâmetros na área de janela Descrição de & Nomes. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
DNS	Escolha uma das opções a seguir: <ul style="list-style-type: none"> <li>• Digite um nome de DNS e clique em <b>Incluir</b>.</li> <li>• Selecione um nome de DNS na lista e clique em <b>Editar</b>.</li> <li>• Selecione um nome de DNS na lista e clique em <b>Remover</b>.</li> </ul>
NetBIOS	Escolha uma das opções a seguir: <ul style="list-style-type: none"> <li>• Digite um nome NetBIOS e clique em <b>Incluir</b>.</li> <li>• Selecione um nome NetBIOS na lista e clique em <b>Editar</b>.</li> <li>• Selecione um nome NetBIOS na lista e clique em <b>Remover</b>.</li> </ul>
Nome Dado	Digite um nome para este perfil de ativo.
Localização	Digite um local para este perfil de ativo.
Descrição	Digite uma descrição para o perfil de ativo.
Wireless AP	Digite o Ponto de Acesso Wireless (PA) para este perfil de ativo.
Wireless SSID	Digite o Service Set Identifier (SSID) do wireless para este perfil de ativo.
ID do Computador	Digite o ID do computador para este perfil de ativo.
ID da Porta do Computador	Digite o ID de porta do computador para este perfil de ativo.

6. Configure os parâmetros na área de janela Sistema Operacional:
  - a. Na caixa de listagem **Fornecedor**, selecione um fornecedor do sistema operacional.
  - b. Na caixa de listagem **Produto**, selecione o sistema operacional para o perfil de ativo.
  - c. Na caixa de listagem **Versão**, selecione a versão para o sistema operacional selecionado.
  - d. Clique no ícone **Incluir**.



- e. Na caixa de listagem **Substituir**, selecione uma das seguintes opções:
- **Até a próxima varredura** – Selecione esta opção para especificar que o scanner fornece informações do sistema operacional e as informações podem ser temporariamente editadas. Se você editar os parâmetros do sistema operacional, o scanner irá restaurar as informações em sua próxima varredura.
  - **Para sempre** – Selecione esta opção para especificar que você deseja inserir manualmente as informações do sistema operacional e desativar o scanner de atualizar as informações.
- f. Selecione um sistema operacional na lista.
- g. Selecione um sistema operacional e clique no ícone **Alternar substituição**.
7. Configure os parâmetros na área de janela CVSS & de Peso. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
Potencial de Danos Colaterais	<p>Configure esse parâmetro para indicar o potencial de perda de vida ou ativos físicos por dano ou furto desse ativo. Você também pode usar esse parâmetro para indicar um potencial de perda econômica de produtividade ou receita. O potencial de dano colateral aumentado aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem <b>Potencial de danos colaterais</b>, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> <li>• Nenhum</li> <li>• Baixo</li> <li>• Média baixa</li> <li>• Média alta</li> <li>• Alto</li> <li>• Não definido</li> </ul> <p>Ao configurar o parâmetro <b>Collateral Damage Potential</b>, o parâmetro <b>Weight</b> será atualizado automaticamente.</p>
Requisito de Confidencialidade	<p>Configure esse parâmetro para indicar o impacto sobre a confidencialidade de uma vulnerabilidade explorada com êxito neste ativo. O impacto de confidencialidade aumentada aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem <b>Requisito de confidencialidade</b>, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> <li>• Baixo</li> <li>• Médio</li> <li>• Alto</li> <li>• Não definido</li> </ul>
Requisito de Disponibilidade	<p>Configure esse parâmetro para indicar o impacto para disponibilidade do ativo quando uma vulnerabilidade é explorada com êxito. Ataques que consomem a largura da banda da rede, ciclos do processador ou espaço em disco impactará na disponibilidade de um ativo. O impacto de disponibilidade aumentada aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem <b>Requisito de disponibilidade</b>, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> <li>• Baixo</li> <li>• Médio</li> <li>• Alto</li> <li>• Não definido</li> </ul>

Parâmetro	Descrição
Requisito de Integridade	<p>Configure esse parâmetro para indicar o impacto para a integridade do ativo quando uma vulnerabilidade é explorada com êxito. Integridade refere-se à fidelidade e a veracidade garantida de informações. O impacto de integridade aumentada aumenta o valor calculado no parâmetro CVSS Score.</p> <p>Na caixa de listagem <b>Requisito de integridade</b>, selecione uma das seguintes opções:</p> <ul style="list-style-type: none"> <li>• Baixo</li> <li>• Médio</li> <li>• Alto</li> <li>• Não definido</li> </ul>
Peso	<p>Na caixa de listagem <b>Peso</b>, selecione um peso para este perfil de ativo. O intervalo é 0 – 10.</p> <p>Ao configurar o parâmetro de <b>Weight</b>, o parâmetro de <b>Collateral Damage Potential</b> é atualizado automaticamente.</p>

8. Configure os parâmetros na área de janela Proprietário. Escolha uma ou mais das seguintes opções:

Parâmetro	Descrição
Business Owner	digitar o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento. O comprimento máximo é de 255 caracteres.
Business Owner Contact	Digite as informações de contato para o proprietário de negócios. O comprimento máximo é de 255 caracteres.
Technical Owner	Digite o proprietário técnico do ativo. Um exemplo de um proprietário de negócios é o gerenciador ou diretor de TI. O comprimento máximo é de 255 caracteres.
Technical Owner Contact	Digite as informações de contato para o proprietário técnico. O comprimento máximo é de 255 caracteres.
Technical User	<p>Na caixa de listagem, selecione o nome do usuário que você deseja associar a esse perfil do ativo.</p> <p>Você também pode usar esse parâmetro para ativar a correção automática de vulnerabilidade para IBM Security QRadar Vulnerability Manager. Para obter mais informações sobre a correção automática, consulte o Guia do Usuário do <i>IBM Security QRadar Vulnerability Manager</i>.</p>

9. Clique em **Salvar**.

## Procurando perfis de ativos

Você pode configurar parâmetros de procura para exibir apenas os Perfis de ativos que você deseja investigar na página Ativo na guia **Ativos**.

### Sobre Esta Tarefa

Ao acessar a guia **Ativos**, a página Ativo será exibida preenchida com todos os ativos descobertos em sua rede. Para refinar essa lista, você pode configurar parâmetros de procura para exibir apenas os Perfis de ativos que você deseja investigar.

Na página Procura do Ativo, você pode gerenciar Grupos de Procura de Ativo. Para obter mais informações sobre Grupos de Procura de Ativo, consulte Consultar grupos de procura de Ativo.

O recurso de procura permitirá que você procure perfis do host, ativos e informações de identificação. As informações de identidade fornecem mais detalhes sobre as origens de log em sua rede, incluindo informações de DNS, logins do usuário e endereços MAC.

Usando o recurso de procura de ativo, você pode procurar ativos por referências de dados externos para determinar se as vulnerabilidades conhecidas existem em sua implementação.

Por Exemplo:

Você receberá uma notificação de que o ID do CVE: CVE-2010-000 está sendo ativamente usado no campo. Para verificar se quaisquer hosts em sua implementação estão vulneráveis a esta exploração, você pode selecionar **Referência externa de vulnerabilidade** na lista de parâmetros de procura, selecionar **CVE** e, em seguida, digitar o  
2010-000

Para visualizar uma lista de todos os hosts que são vulneráveis a esse ID de CVE específico.

**Nota:** Para obter mais informações sobre OSVDB, consulte <http://osvdb.org/> . Para obter mais informações sobre NVDB, consulte <http://nvd.nist.gov/> .

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na barra de ferramentas, clique em **Procurar > Nova procura**.
4. Escolha uma das opções a seguir:
  - Para carregar uma procura salva anteriormente, acesse a Etapa 5.
  - Para criar uma nova procura, acesse a Etapa 6.
5. Selecione uma procura salva anteriormente:
  - a. Escolha uma das opções a seguir:
    - Opcional. Na caixa de listagem **Grupo**, selecione o grupo de procura de ativos que você deseja exibir na lista **Procuras salvas disponíveis**.
    - Na lista **Procuras salvas disponíveis**, selecione a procura salva que você deseja carregar.
    - No campo **Digitar procura salva ou selecionar da lista**, digite o nome da procura que você deseja carregar.
  - b. Clique em **Carregar**.
6. Na área de janela Parâmetros de Procura, defina seus critérios de procura:
  - a. Na primeira caixa de listagem, selecione o parâmetro de ativos que você deseja procurar. Por exemplo, **Nome do host**, **Classificação de risco de vulnerabilidade** ou **Proprietário técnico**.
  - b. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura.
  - c. No campo de entrada, digite informações específicas que estão relacionadas ao seu parâmetro de procura.
  - d. Clique em **Incluir filtro**.
  - e. Repita estas etapas para cada filtro que você deseja incluir nos critérios de procura.
7. Clique em **Procurar**.

## Resultados

Você pode salvar o seu critério de procura de ativo. Consulte Salvando critérios de procura de ativo.

---

## Salvando critérios de procura de ativo

Na guia **Ativos**, você pode salvar o critério de procura configurado para que você possa reutilizar os critérios. Os critérios de procura salvos não expiram.

### Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Execute uma procura. Consulte Procurando perfis de ativo.
4. Clique em **Salvar critérios**.
5. Insira valores para os parâmetros:

Parâmetro	Descrição
Insira o nome desta procura	Digite o nome exclusivo que você deseja designar a esses critérios de procura.
Gerenciar Grupos	Clique em <b>Gerenciar grupos</b> para gerenciar os grupos de procura. Para obter mais informações, consulte Grupos de procura de ativo. Essa opção será exibida somente se você tiver permissões administrativas.
Designar procura aos grupos	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, esta procura salva será designada ao grupo <b>Outro</b> por padrão. Para obter mais informações, consulte Grupos de procura de ativo.
Incluir em minhas procuras rápidas	Selecione essa caixa de seleção para incluir essa procura em sua caixa de listagem <b>Procura rápida</b> , que está na barra de ferramentas da guia <b>Ativos</b> .
Definir como Padrão	Selecione esta caixa de seleção para configurar esta procura como sua procura padrão quando você acessar a guia <b>Recursos</b> .
Compartilhar com todos	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

---

## Grupos de procura de ativos

Usando a janela Grupos de procura de ativos, é possível criar e gerenciar grupos de procura de ativos.

Esses grupos permitem localizar facilmente critérios de procura salvos na guia **Ativos**.

## Visualizando grupos de procura

Use a janela Grupos de Procura de Ativo para visualizar um grupo e subgrupos de lista.

### Sobre Esta Tarefa

Da janela Grupos de Procura de Ativos, você pode visualizar detalhes sobre cada grupo, incluindo uma descrição e a data em que o grupo foi modificado pela última vez.

Todas as procuras salvas não designadas a um grupo estão no grupo **Outro**.

A janela Grupos de Procura de Ativos exibe os seguintes parâmetros para cada grupo:

Tabela 51. Funções da barra de ferramentas da janela Grupos de Procura de Ativos

Função	Descrição
Novo grupo	Para criar um novo grupo de procura, você pode clicar em <b>Novo grupo</b> . Consulte Consultar Criando uma nova procura de grupo.
Editar	Para editar um grupo de procura existente, você pode clicar em <b>Editar</b> . Consulte Consultar Editando um grupo de procura.
Copiar	Para copiar uma procura salva em outro grupo de procura, você pode clicar em <b>Copiar</b> . Consulte Consultar Copiando uma procura salva para outro grupo.
Remover	Para remover um grupo de procura ou uma procura salva de um grupo de procura, selecione o item que você deseja remover e clique em <b>Remover</b> . Consulte Consultar Removendo um grupo ou uma procura salva de um grupo.

### Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Visualize os grupos de procura.

## Criando um novo grupo de procura

Na janela Grupos de Procura de Ativo, você pode criar um novo grupo de procura.

### Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a pasta para o grupo no qual você deseja criar o novo grupo.
6. Clique em **Novo grupo**.
7. No campo **Nome**, digite um nome exclusivo para o novo grupo.
8. Opcional. No campo **Descrição**, digite uma descrição.
9. Clique em **OK**.

## Editando um grupo de procura

Você pode editar os campos **Nome** e **Descrição** de um grupo de procura.

### Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione o grupo que você deseja editar.
6. Clique em **Editar**.
7. Digite um novo nome no campo **Nome**.
8. Digite uma nova descrição no campo **Descrição**.
9. Clique em **OK**.

## Copiando uma procura salva para outro grupo

Você pode copiar uma procura salva para outro grupo. Você também pode copiar a procura salva em mais de um grupo.

### Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que deseja copiar.
6. Clique em **Copiar**.
7. Na janela Grupos de item, selecione a caixa de seleção para o grupo que você deseja copiar a procura salva.
8. Clique em **Designar grupos**.

## Removendo um grupo ou uma procura salva de um grupo

Você pode usar o ícone **Remove** para remover uma procura de um grupo ou remover um grupo de procura.

### Sobre Esta Tarefa

Ao remover uma procura salva de um grupo, a procura salva não será excluída do sistema. A procura salva é removida do grupo e automaticamente movida para o grupo **Outros**.

Não é possível remover os seguintes grupos do sistema:

- Grupos de Procura de Ativo
- Outro

### Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar > Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que você deseja remover do grupo:
  - Selecione a procura salva que você deseja remover do grupo.
  - Selecione o grupo que você deseja remover.

---

## Tarefas de gerenciamento do Perfil de ativo

É possível excluir, importar e exportar perfis de ativo usando a guia **Ativos**.

### Sobre Esta Tarefa

Usando a guia **Ativos**, é possível excluir, importar e exportar perfis de ativos.

## Excluindo ativos

Você pode excluir ativos específicos ou todos os perfis de ativo listados.

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione o ativo que deseja excluir e, em seguida, selecione **Excluir ativo** na caixa de listagem **Ações**.
4. Clique em **OK**.

## Importando perfis de ativos

É possível importar informações do perfil de ativos.

### Antes de Iniciar

O arquivo importado deve ser um arquivo CSV no seguinte formato:

```
ip,name,weight,description
```

Em que:

- **IP** – Especifica qualquer endereço IP válido no formato de número com decimal. Por exemplo: 192.168.5.34.
- **Nome** – Especifica o nome deste ativo até 255 caracteres de comprimento. Vírgulas não são válidas neste campo e invalidam o processo de importação. Por exemplo: WebServer01 está correto.
- **Peso** – Especifica um número de 0 a 10, que indica a importância deste ativo em sua rede. Um valor de 0 denota importância baixa e 10 é muito alta.
- **Descrição** – Especifica uma descrição textual para este ativo até 255 caracteres de comprimento. Esse valor é opcional.

Por exemplo, as entradas a seguir podem ser incluídas em um arquivo CSV:

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

O processo de importação mescla os Perfis de ativos importados com informações do perfil de ativos que você tem atualmente armazenado no sistema.

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na caixa de listagem **Ações**, selecione **Importar ativos**.
4. Clique em **Navegar** para localizar e selecionar o arquivo CSV que você deseja importar.
5. Clique em **Importar ativos** para iniciar o processo de importação.

## Exportando ativos

Você pode exportar Perfis de ativos listados em um arquivo Extended Markup Language (XML) ou Comma-Separated Value (CSV).

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.

3. Na caixa de listagem **Ações**, selecione uma das opções a seguir:
  - Exportar para XML
  - Exportar para CSV
4. Visualize a janela de status para o status do processo de exportação.
5. Opcional: Se você desejar usar outras guias e páginas enquanto a exportação estiver em andamento, clique no link **Notificar quando estiver pronto**.  
Quando a exportação for concluída, a janela Download de Arquivo será exibida.
6. Na janela Download de Arquivo, escolha uma das seguintes opções:
  - **Abrir** – Selecione esta opção para abrir os resultados de exportação em sua opção de navegador.
  - **Salvar** – Selecione esta opção para salvar os resultados em seu desktop.
7. Clique em **OK**.

---

## Pesquisar vulnerabilidades de ativo

A área de janela de Vulnerabilidades na página Perfil de Ativo exibe uma lista de vulnerabilidades descobertas para o ativo.

### Sobre Esta Tarefa

Você pode clicar duas vezes na vulnerabilidade para exibir mais detalhes de vulnerabilidade.

A janela Pesquisar Detalhes de Vulnerabilidade fornece os seguintes detalhes:

Parâmetro	Descrição
Vulnerability ID	Especifica o ID da vulnerabilidade. O ID de Vuln é um identificador exclusivo que é gerado pelo Sistema de Informação de Vulnerabilidade (VIS).
Published Date	Especifica a data na qual os detalhes de vulnerabilidade foram publicados no OSVDB.
Name	Especifica o nome da vulnerabilidade.
Assets	Especifica o número de ativos em sua rede que possuem esta vulnerabilidade. Clique no link para visualizar a lista de ativos.
Assets, including exceptions	Especifica o número de ativos em sua rede que possuem exceções de vulnerabilidade. Clique no link para visualizar a lista de ativos.
CVE	Especifica o identificador CVE para a vulnerabilidade. Os identificadores CVE são fornecidos pelo NVD.  Clique no link para obter mais informações. Quando você clica no link, o site NVD é exibido em uma nova janela do navegador.
xforce	Especifica o identificador X-Force para a vulnerabilidade.  Clique no link para obter mais informações. Quando você clica no link, o website da IBM Internet Security Systems é exibido em uma nova janela do navegador.
OSVDB	Especifica o identificador do OSVDB para a vulnerabilidade.  Clique no link para obter mais informações. Quando você clica no link, o website do OSVDB é exibido em uma nova janela do navegador.



Parâmetro	Descrição
CVSS Score	<p>Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A pontuação do CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> <li>• Potencial de Danos Colaterais</li> <li>• Requisito de Confidencialidade</li> <li>• Requisito de Disponibilidade</li> <li>• Requisito de Integridade</li> </ul> <p>Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil do ativo” na página 141.</p> <p>Para obter mais informações sobre o CVSS, consulte <a href="http://www.first.org/cvss/">http://www.first.org/cvss/</a>.</p>
Impact	Exibe o tipo de prejuízo ou dano que poderá ser esperado se esta vulnerabilidade for explorada.
CVSS Base Metrics	<p>Exibe as métricas que são usadas para calcular a pontuação base de CVSS, incluindo:</p> <ul style="list-style-type: none"> <li>• Vetor de Acesso</li> <li>• Complexidade de Acesso</li> <li>• Autenticação</li> <li>• Impacto de Confidencialidade</li> <li>• Impacto de Integridade</li> <li>• Impacto de disponibilidade</li> </ul>
Descrição	Especifica uma descrição da vulnerabilidade detectada. Este valor está disponível apenas quando o sistema integra ferramentas VA.
Preocupação	Especifica os efeitos que a vulnerabilidade pode ter em sua rede.
Solução	Siga as instruções que são fornecidas para resolver a vulnerabilidade.
Correção Virtual	Exibe informações de correção virtual que estão associadas com esta vulnerabilidade, se disponível. Uma correção virtual é uma solução de mitigação de curto prazo para uma vulnerabilidade recentemente descoberta. Estas informações são derivadas de eventos Intrusion Protection System (IPS). Se você deseja instalar a correção virtual, consulte as informações do fornecedor de seu IPS.
Referência	<p>Exibe uma lista de referências externas, incluindo:</p> <ul style="list-style-type: none"> <li>• <b>Tipo de referência</b> – Especifica o tipo de referência que está listada, como uma URL consultiva ou lista de postagem do correio.</li> <li>• <b>URL</b> – Especifica a URL que você pode clicar para visualizar a referência.</li> </ul> <p>Clique no link para obter mais informações. Quando você clica no link, o recurso externo é exibido em uma nova janela do navegador.</p>
Produtos	<p>Exibe uma lista de produtos que estão associados a esta vulnerabilidade.</p> <ul style="list-style-type: none"> <li>• <b>Fornecedor</b> – Especifica o fornecedor do produto.</li> <li>• <b>Produto</b> – Especifica o nome do produto.</li> <li>• <b>Versão</b> – Especifica o número da versão do produto.</li> </ul>

## Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione um perfil de ativo.
4. Na área de janela Vulnerabilidades, clique no valor do parâmetro **ID** ou **Vulnerability** para a vulnerabilidade que você deseja investigar.

## Parâmetros da página Perfil de ativo

É possível localizar as descrições de parâmetro da página Perfil de ativo para a área de janela Resumo de ativo, Interface de rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de risco e Produtos.

Esta referência inclui tabelas que descrevem os parâmetros que são exibidos em cada área de janela da guia **Perfil de ativo**.

### Área de janela Resumo de ativo

É possível localizar Descrições de parâmetros da área de janela Resumo de ativo que é acessada a partir da página Perfil de ativo.

A área de janela Resumo de ativo na página Perfil de ativo fornece as seguintes informações:

Tabela 10-8 Parâmetros da área de janela Resumo de ativo

Parâmetro	Descrição
Asset ID	Exibe o número do ID que é designado para o perfil de ativo.
IP Address	Exibe o último endereço IP reportado do ativo.
MAC Address	Exibe o último endereço MAC conhecido do ativo.
Network	Exibe a última rede relatada associada ao ativo.
NetBIOS Name	Exibe o nome NetBIOS do ativo, se conhecido. Se o ativo tiver mais de um nome NetBIOS, este campo indicará o número de nomes NetBIOS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes NetBIOS associados.
DNS Name	Exibe o endereço IP ou nome DNS do ativo, se conhecido. Se o ativo tiver mais de um nome DNS, este campo indicará o número de nomes DNS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes DNS associados.
Nome Dado	Exibe o nome do ativo. Por padrão, este campo está vazio. Para fornecer um determinado nome para o ativo, edite o perfil de ativo.
Group Name	Exibe o grupo último grupo de usuário conhecido do ativo, se conhecido.
Último Usuário	Exibe o último usuário conhecido do ativo. As informações de usuário são derivadas de eventos de identidade. Se mais de um usuário estiver associado a este ativo, será possível clicar no link para exibir todos os usuários.
Operating System	Exibe o sistema operacional que está em execução no ativo. Se o ativo tiver mais de um sistema operacional, este campo indicará o número de sistemas operacionais. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de sistemas operacionais associados.  É possível editar esse parâmetro diretamente se o parâmetro <b>Override</b> for especificado como <b>Até a próxima varredura</b> ou <b>Indefinidamente</b> .
Weight	Exibe o nível de importância que está associado a este ativo. O intervalo é de 0 (Não Importante) a 10 (Muito Importante). Por padrão, este campo está vazio. Para fornecer uma ponderação para o ativo, edite o perfil de ativo.

Parâmetro	Descrição
Aggregate CVSS Score	<p>Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A pontuação do CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> <li>• Potencial de Danos Colaterais</li> <li>• Requisito de Confidencialidade</li> <li>• Requisito de Disponibilidade</li> <li>• Requisito de Integridade</li> </ul> <p>Para obter mais informações sobre como configurar estes parâmetros, consulte "Incluindo ou editando um perfil do ativo" na página 141.</p> <p>Para obter mais informações sobre o CVSS, consulte <a href="http://www.first.org/cvss/">http://www.first.org/cvss/</a>.</p>
Business Owner	Exibe o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento.
Business Owner Contact Info	Exibe as informações de contato do proprietário de negócios.
CVSS Collateral Damage Potential	<p>Exibe o potencial que esse ativo tem para danos colaterais. Este valor é incluído na fórmula para calcular o parâmetro <b>CVSS Score</b>.</p> <p>Por padrão, esse campo não está definido. Para fornecer um local para o ativo, edite o perfil de ativo.</p>
Technical Owner	Exibe o responsável técnico do ativo. Um exemplo de um responsável técnico é um gerenciador de TI ou diretor.
Technical Owner Contact Info	Exibe as informações de contato do responsável técnico.
CVSS Availability	Exibe o impacto de disponibilidade do ativo quando uma vulnerabilidade for explorada com sucesso.
Wireless AP	Exibe o ponto de acesso (AP) wireless deste perfil de ativo.
SSID Wireless	Exibe o Identificador de Conjunto de Serviço Wireless (SSID) deste perfil de ativo.
CVSS Confidentiality Requirements	Exibe o impacto na confidencialidade de uma vulnerabilidade explorada com sucesso neste ativo.
Switch ID	Exibe o ID do comutador deste perfil ativo.
Switch Port ID	Exibe o ID da porta do comutador deste perfil de ativo.
CVSS Integrity Requirements	Exibe o impacto à integridade do ativo quando uma vulnerabilidade for explorada de maneira bem-sucedida.
Technical User	Especifica o nome do usuário que está associado a este perfil de ativo.
Open Services	Exibe o número de aplicativos exclusivos da Camada 7 que são executados neste perfil de ativo.
Vulnerabilidades	Exibe o número de vulnerabilidades que são descobertas nesse perfil de ativo.
Location	Especifica o local físico do ativo. Por padrão, este campo está vazio. Para fornecer um local para o ativo, edite o perfil de ativo.
Asset Description	Especifica uma descrição deste ativo. Por padrão, este campo está vazio. Para fornecer uma descrição para o ativo, edite o perfil de ativo.
Extra Data	Especifica quaisquer informações estendidas que são baseadas em um evento.

## Área de janela Resumo de interface de rede

É possível localizar as descrições de parâmetros para a área de janela Resumo da interface de rede acessada a partir da página Perfil de ativo.

A área de janela Resumo da interface de rede na página Perfil de ativo fornece as seguintes informações:

Tabela 1 Parâmetros de área de janela Resumo de interface de rede

Parâmetro	Descrição
MAC Address	Exibe o endereço MAC deste ativo, se conhecido.
IP Address	Exibe o endereço IP que é detectado para este endereço MAC.
Network	Exibe a rede com a qual o endereço IP está associado, se conhecido.
Last Seen	Exibe a data e hora em que o endereço IP foi detectado por último nesse endereço MAC.

## Área de janela Vulnerabilidade

É possível localizar descrições de parâmetros da área de janela Vulnerabilidade acessada a partir da página Perfil de ativo.

A área de janela Vulnerabilidade na página Perfil de ativo fornece as seguintes informações:

*Tabela 52. Parâmetros da área de janela Vulnerabilidade*

Parâmetro	Descrição
ID	Exibe o ID da vulnerabilidade. O ID é um identificador exclusivo que é gerado pelo Sistema de Informação de Vulnerabilidade (VIS).
Gravidade	Exibe a severidade da Indústria de Segurança de Pagamento (PCI) que está associada à vulnerabilidade.
Risk	O nível de risco que está associado à vulnerabilidade. A classificação nessa coluna deve ser pelo código de nível de risco subjacente
Service	O serviço que está associado à vulnerabilidade (como descoberto pela varredura). Se somente um serviço estiver associado, exibe o serviço. Caso contrário, exibe Vários (N) onde N indica ao número total de serviços associados a esta vulnerabilidade.
Port	Exibe o número da porta na qual esta vulnerabilidade foi descoberta. Se a vulnerabilidade for descoberta em mais de uma porta, este campo indicará o número de números de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números da porta.
Vulnerability	Nome ou título desta vulnerabilidade.
Details	Texto detalhado específico que está associado a essa vulnerabilidade, conforme determinado pela varredura. Se somente um detalhe estiver associado, exibe o texto desse Detalhe. Caso contrário, exibe Vários (N) onde N indica ao número total de Detalhes que estão associados a esta vulnerabilidade.
CVSS Score	<p>Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras.</p> <p>A pontuação do CVSS é calculada usando os seguintes parâmetros definidos pelo usuário:</p> <ul style="list-style-type: none"> <li>• Potencial de Danos Colaterais</li> <li>• Requisito de Confidencialidade</li> <li>• Requisito de Disponibilidade</li> <li>• Requisito de Integridade</li> </ul> <p>Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil do ativo” na página 141.</p> <p>Para obter mais informações sobre o CVSS, consulte <a href="http://www.first.org/cvss/">http://www.first.org/cvss/</a>.</p>
Found	Exibe a data na qual essa vulnerabilidade foi originalmente encontrada em uma varredura.
Last seen	Exibe a data na qual essa vulnerabilidade foi vista pela última vez em uma varredura.

## Área de janela Serviços

É possível localizar descrições de parâmetros da área de janela Serviços acessada a partir da página Perfil de ativo.

A área de janela Serviços na página Perfil de ativo fornece as seguintes informações:

*Tabela 53. parâmetros da área de janela serviços*

Parâmetro	Descrição
Service	Exibe o nome do serviço aberto.
Product	Exibe o produto que executa este serviço, se conhecido.
Port	Exibe a porta na qual o aplicativo Camada 7 foi descoberto. Se esse serviço tiver mais que uma porta, esse campo indicará o número de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números da porta.
Protocol	Exibe uma lista separada por vírgula de protocolos que são descobertos na porta que executa o serviço aberto.
Last Seen Passive	Exibe a data e hora em que o serviço aberto foi visto pela última vez passivamente.
Last Seen Active	Exibe a data e hora em que o serviço aberto foi visto pela última vez ativamente.
Service Default Ports	Exibe uma lista separada por vírgula de portas conhecidas que o aplicativo Camada 7 é conhecido por executar.
Vulnerabilities	Exibe o número de vulnerabilidades que estão associadas a este serviço aberto.

## Área de janela Serviços do Windows

É possível localizar as descrições de parâmetros da área de janela Serviços do Windows acessada a partir da página Perfil de ativo. A área de janela Serviços do Windows será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

A área de janela Serviços do Windows na página Perfil de ativo fornece as seguintes informações:

*Tabela 54. Parâmetros da área de janela Serviços do Windows*

Parâmetro	Descrição
Name	Exibe o nome do serviço do Windows que foi visto ativamente no ativo.
Status	Exibe o status do serviço do Windows. As opções incluem: <ul style="list-style-type: none"> <li>• Ativado</li> <li>• Manual</li> <li>• Desativado</li> </ul>

## Área de janela Pacotes

É possível localizar as descrições de parâmetros para a área de janela Pacotes acessada a partir da página Perfil de ativo.

A área de janela Pacotes será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema. A área de janela Pacotes na página Perfil de ativo fornece as seguintes informações:

*Tabela 55. Parâmetros da área de janela Pacotes*

Parâmetro	Descrição
Packages	Exibe o nome do pacote que é aplicado ao ativo.
Version	Exibe a versão do pacote que é aplicada ao ativo.
Revision	Exibe a revisão do pacote que é aplicada ao ativo.

## Área de janela Correções do Windows

É possível localizar descrições de parâmetros para a área de janela Correções do Windows que é acessada a partir da página Perfil de ativo.

A área de janela Correções do Windows será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema. A área de janela Correções do Windows na página Perfil de ativo fornece as seguintes informações:

*Tabela 56. Parâmetros da área de janela Correções do Windows*

Parâmetro	Descrição
Microsoft KB Number	Exibe número da Base de Conhecimento (KB) da Microsoft da correção do Windows que é executada no ativo.
Description	Exibe a descrição da correção do Windows.
Bulletin ID	Exibe o número do ID do boletim da correção do Windows.
Vulnerability ID	Exibe o ID de vulnerabilidade da correção do Windows.
CVE-ID	Exibe o ID de CVE associado à correção do Windows. Se mais de um ID de CVE for associado à correção do Windows, mova o seu mouse sobre o link Vários para exibir a lista de IDs de CVE. É possível clicar em um link do ID de CVE para acessar mais informações.
System	Exibe o sistema Windows para a correção.
Service Pack	Exibe o Service Pack da correção.

## Área de janela Propriedades

É possível localizar descrições de parâmetros para a área de janela Propriedades acessada na página Perfil de ativo. A área de janela Propriedades será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

A área de janela Propriedades na página Perfil de ativo fornece as seguintes informações:

*Tabela 57. Parâmetros da área de janela Propriedades*

Parâmetro	Descrição
Name	Exibe o nome da propriedade de configuração que foi vista ativamente no ativo.
Value	Exibe o valor da propriedade de configuração.

## Área de janela Políticas de risco

É possível localizar descrições de parâmetros da área de janela Políticas de risco, acessada a partir da página Perfil de ativo. A área de janela Políticas de riscos será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

A área de janela Políticas de risco em Perfil de ativo fornece as seguintes informações:

*Tabela 58. Parâmetros da área de janela Políticas de risco*

Parâmetro	Descrição
Policy	Especifica o nome da política associada a esse ativo.
Pass/Fail	Indica se a política tem um status <b>Aprovado</b> ou <b>Reprovado</b> .
Last Evaluated	Exibe a data da última vez que esta política foi avaliada.

## Área de janela Produtos

É possível localizar descrições de parâmetros da área de janela Produtos que é acessada a partir da página Perfil de ativo.

A área de janela Produtos na página Perfil de ativo fornece as seguintes informações:

*Tabela 59. Parâmetros da área de janela Produtos*

Parâmetro	Descrição
Product	Exibe o nome do produto que é executado no ativo.

*Tabela 59. Parâmetros da área de janela Produtos (continuação)*

Parâmetro	Descrição
Port	Exibe a porta que o produto usa.
Vulnerabilidade	Exibe o número de vulnerabilidades associadas a esse produto.
Vulnerability ID	Exibe o ID de vulnerabilidade.





---

## Capítulo 12. Gerenciamento de relatório

É possível usar a guia **Relatórios** para criar, editar, distribuir e gerenciar relatórios.

Opções de relatório flexíveis e detalhadas satisfazem seus diversos padrões regulamentários, como a conformidade de PCI.

É possível criar seus próprios relatórios customizados ou usar um relatório padrão. É possível customizar e remarcar relatórios padrão e distribuir estes para outros usuários.

A guia **Relatórios** pode requerer um período de tempo estendido para ser atualizada se o seu sistema incluir muitos relatórios.

**Nota:** Se estiver executando o Microsoft Exchange Server 5.5, os caracteres de fonte indisponíveis podem ser exibidos na linha de assunto de relatórios enviados por email. Para resolver isso, faça download e instale o Service Pack 4 do Microsoft Exchange Server 5.5. Para obter mais informações, entre em contato com o suporte da Microsoft.

### Contraprestações de fuso horário

Para assegurar-se de que o recurso Relatórios usa a data e hora corretas para relatar dados, sua sessão deve ser sincronizada com o fuso horário.

Durante a instalação e a configuração dos produtos do QRadar, o fuso horário é configurado. Verifique com seu administrador, para assegurar-se de que sua sessão QRadar está sincronizada com o seu fuso horário.

### Permissões da guia Relatório

Usuários administrativos podem visualizar todos os relatórios que são criados por outros usuários.

Os usuários não administrativos podem visualizar somente relatórios que eles criaram ou relatórios que são compartilhadas por outros usuários.

### Parâmetros da guia Relatório

A guia **Relatórios** exibe uma lista de relatórios padrão e customizados.

Na guia **Relatórios**, é possível visualizar informações estatísticas sobre o modelo de relatórios, executar ações nos modelos de relatório, visualizar os relatórios gerados e excluir o conteúdo gerado.

Se um relatório não especificar um planejamento de intervalo, será necessário gerar manualmente o relatório.

É possível passar o mouse sobre qualquer relatório para visualizar um resumo do relatório em uma dica de ferramenta. O resumo especifica a configuração do relatório e o tipo de conteúdo que o relatório gera.

---

## Barra de status

A barra de status exibe o número de resultados da procura (Exibindo 1 de 10 itens) atualmente exibido e a quantidade de tempo (Tempo decorrido:) necessária para processar os resultados da procura.

---

## Layout de relatório

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

Ao seleccionar o layout de um relatório, considere o tipo de relatório que deseja criar. Por exemplo, não escolha um pequeno contêiner de gráfico para o conteúdo de gráfico que exibe muitos objetos. Cada gráfico inclui uma legenda e uma lista de redes a partir das quais o conteúdo é derivado; escolha um contêiner suficientemente grande para conter os dados. Para visualizar como cada gráfico exibe dados, consulte Tipos de diagrama.

---

## Tipos de gráfico

Ao criar um relatório, será necessário escolher um tipo de gráfico para cada gráfico que desejar incluir no relatório.

O tipo de gráfico determina como o relatório gerado apresenta dados e objetos de rede. É possível classificar os dados com diversas características e criar os gráficos em um único relatório gerado.

É possível usar qualquer um dos seguintes tipos de gráficos:

- **Nenhum** – Use esta opção para exibir um contêiner vazio no relatório. Essa opção pode ser útil para criar espaço em branco em seu relatório. Se seleccionar a opção **Nenhum** para qualquer contêiner, nenhuma configuração adicional será necessária para esse contêiner.
- **Vulnerabilidades de ativos** – Use este gráfico para visualizar dados de vulnerabilidade de cada ativo definido em sua implementação. É possível gerar gráficos de Vulnerabilidade de ativo quando vulnerabilidades forem detectadas por uma varredura VA. Este gráfico estará disponível após instalar o IBM Security QRadar Vulnerability Manager.
- **Conexões** – Esta opção de gráfico será exibida apenas se tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.
- **Regras do dispositivo** – Esta opção de gráfico será exibida apenas se tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.
- **Objetos do dispositivo não usados** – Esta opção de gráfico será exibida apenas se tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte *IBM Security QRadar Risk Manager User Guide*.
- **Eventos/logs** – Use este gráfico para visualizar informações de evento. É possível basear seus gráficos nos dados de procuras salvas a partir da guia **Atividade de log**. É possível customizar os dados que deseja exibir no relatório gerado. É possível configurar o gráfico para criar gráficos de dados em um período de tempo configurável. Esta funcionalidade ajuda a detectar tendências de eventos. Para obter mais informações sobre procuras salvas, consulte Procuras de dados.

- **Fluxos** – Use este gráfico para visualizar informações do fluxo. É possível basear seus gráficos nos dados de procuras salvas a partir da guia Atividade de rede. Isso permite que sejam customizados os dados que desejar exibir no relatório gerado. É possível usar procuras salvas para configurar o gráfico para criar gráficos de dados por um período de tempo configurável. Esta funcionalidade ajuda a detectar tendências de fluxo. Para obter mais informações sobre procuras salvas, consulte Procuras salvas.
- **Principais IPs de destino** – Use este gráfico para exibir os principais IPs de destino nos locais de rede selecionados.
- **Principais ofensas** – Use este gráfico para exibir as principais N ofensas que ocorrem no momento atual para os locais de rede selecionados.
- **Principais IPs de origem** – Use este gráfico para exibir e classificar as principais origens de crime (endereços IP) que atacam sua rede ou ativos de negócios.
- **Vulnerabilidades** – A opção Vulnerabilidades será exibida somente quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter informações adicionais, consulte *IBM Security QRadar Vulnerability Manager User Guide*.

Para obter mais informações sobre esses tipos de gráfico, consulte Parâmetros do contêiner de gráfico.

---

## Barra de ferramentas da guia Relatório

É possível usar a barra de ferramentas para executar várias ações em relatórios.

A tabela a seguir identifica e descreve as opções da barra de ferramentas Relatórios.

*Tabela 60. Opções da barra de ferramentas Relatório*

Opção	Descrição
Grupo	
Gerenciar grupos	Clique em <b>Gerenciar grupos</b> para gerenciar Grupos de relatórios. Usando o recurso Gerenciar grupos, é possível organizar seus relatórios em grupos funcionais.

Tabela 60. Opções da barra de ferramentas Relatório (continuação)

Opção	Descrição
Ações	<p>Clique em <b>Ações</b> para executar as seguintes ações:</p> <ul style="list-style-type: none"> <li>• <b>Criar</b> – Selecione esta opção para criar um novo relatório.</li> <li>• <b>Editar</b> – Selecione esta opção para editar o relatório selecionado. É possível também clicar duas vezes em um relatório para editar o conteúdo.</li> <li>• <b>Duplicar</b> – Selecione esta opção para duplicar ou renomear o relatório selecionado.</li> <li>• <b>Designar grupos</b> - Selecione essa opção para designar o relatório selecionado a um grupo de relatórios.</li> <li>• <b>Compartilhar</b> – Selecione essa opção para compartilhar o relatório selecionado com outros usuários. Deve-se ter privilégios administrativos para compartilhar relatórios.</li> <li>• <b>Alternar planejamento</b> – Selecione esta opção para alternar o relatório selecionado para o estado Ativo ou Inativo.</li> <li>• <b>Executar relatório</b> - Selecione essa opção para gerar o relatório selecionado. Para gerar vários relatórios, mantenha pressionada a tecla Control e clique nos relatórios que deseja gerar.</li> <li>• <b>Executar relatório em dados brutos</b> – Selecione esta opção para gerar o relatório selecionado usando dados brutos. Essa opção será útil quando desejar gerar um relatório antes dos dados acumulados requeridos estarem disponíveis. Por exemplo, se quiser executar um relatório semanal antes que uma semana completa tenha decorrido desde que o relatório foi criado, será possível gerar o relatório usando esta opção.</li> <li>• <b>Excluir relatório</b> – Selecione esta opção para excluir o relatório selecionado. Para excluir vários relatórios, mantenha pressionada a tecla Control e clique nos relatórios que deseja excluir.</li> <li>• <b>Excluir conteúdo gerado</b> – Selecione esta opção para excluir todo o conteúdo gerado para as linhas selecionadas. Para excluir vários relatórios gerados, mantenha pressionada a tecla Control e clique em gerar relatórios que você deseja excluir.</li> </ul>
Ocultar relatórios interativos	<p>Selecione esta caixa de opções para ocultar os modelos de relatórios inativos. A guia <b>Relatórios</b> é atualizada automaticamente e exibe apenas os relatórios ativos. Limpe a caixa de opções para mostrar os relatórios inativos ocultos.</p>
Relatórios de procura	<p>Digite seus critérios de procura no campo <b>Relatórios de procura</b> e clique no ícone <b>Procurar relatórios</b>. Uma procura é executada nos parâmetros a seguir para determinar quais correspondem seus critérios especificados:</p> <ul style="list-style-type: none"> <li>• Título do Relatório</li> <li>• Descrição do Relatório</li> <li>• Grupo de Relatórios</li> <li>• Grupos de Relatórios</li> <li>• Nome de Usuário do Autor do Relatório</li> </ul>

## Tipos de diagrama

Cada tipo de diagrama suporta vários tipos de diagramas que podem ser usados para exibir dados.

Os arquivos de configuração de rede determinam as cores que os gráficos usam para representar o tráfego na rede. Cada endereço IP é representado usando uma cor exclusiva. A tabela a seguir fornece exemplos de como os dados de rede e de segurança são usados nos gráficos. A tabela descreve os tipos de gráficos que estão disponíveis para cada tipo de gráfico.

Tabela 61. Tipos de diagrama

Tipo de gráfico	Tipos de gráficos disponíveis
Linha	<ul style="list-style-type: none"> <li>• Eventos/logs</li> <li>• Fluxos</li> <li>• Conexões</li> <li>• Vulnerabilidades</li> </ul>

Tabela 61. Tipos de diagrama (continuação)

Tipo de gráfico	Tipos de gráficos disponíveis
Linha empilhada	<ul style="list-style-type: none"> <li>• Eventos/logs</li> <li>• Fluxos</li> <li>• Conexões</li> <li>• Vulnerabilidades</li> </ul>
Barra	<ul style="list-style-type: none"> <li>• Eventos/logs</li> <li>• Fluxos</li> <li>• Conexões de vulnerabilidades do ativo</li> <li>• Conexões</li> <li>• Vulnerabilidades</li> </ul>
Barra horizontal	<ul style="list-style-type: none"> <li>• Principais IPs de Origem</li> <li>• Principais Crimes</li> <li>• Principais IPs de Destino</li> </ul>
Barras empilhadas	<ul style="list-style-type: none"> <li>• Eventos/logs</li> <li>• Fluxos</li> <li>• Conexões</li> </ul>
Pizza	<ul style="list-style-type: none"> <li>• Eventos/logs</li> <li>• Fluxos</li> <li>• Vulnerabilidades do Ativo.</li> <li>• Conexões</li> <li>• Vulnerabilidades</li> </ul>
Tabela	<ul style="list-style-type: none"> <li>• Eventos/logs</li> <li>• Fluxos</li> <li>• Principais IPs de Origem</li> <li>• Principais Crimes</li> <li>• Principais IPs de Destino</li> <li>• Conexões</li> <li>• Vulnerabilidades</li> </ul> <p>Para exibir o conteúdo de uma tabela, é necessário projetar o relatório com um contêiner de largura de página inteira.</p>
Tabela agregada	<p>Disponível com o gráfico Vulnerabilidades do ativo.</p> <p>Para exibir o conteúdo de uma tabela, é necessário projetar o relatório com um contêiner de largura de página inteira.</p>

Os seguintes tipos de diagramas estão disponíveis para relatórios do Gerenciador de Log do QRadar:

- Gráfico de linhas
- Gráfico de linhas empilhadas
- Gráfico de barras
- Gráfico de barras empilhadas
- Gráfico em pizza
- Gráfico de tabela

## Criando relatórios customizados

Você pode usar o assistente Relatório para criar um novo relatório.

### Antes de Iniciar

Você deve ter as permissões da rede apropriadas para compartilhar um relatório gerado com outros usuários.

Para obter mais informações sobre as permissões, consulte o *IBM Security QRadar SIEM Administration Guide* *IBM Security QRadar SIEM: Guia de Administração*.

## Sobre Esta Tarefa

O assistente Relatório fornece um guia passo a passo sobre como projetar, planejar e gerar relatórios.

O assistente usa os elementos chave a seguir para ajudá-lo a criar um relatório:

- **Layout** – posição e tamanho de cada contêiner
- **Contêiner** – marcador para o conteúdo de destaque
- **Conteúdo** – definição do gráfico colocado no contêiner

Após criar um relatório que seja gerado semanalmente ou mensalmente, o tempo de planejamento deverá ter decorrido antes que o relatório gerado retorne os resultados. Para um relatório planejado, você deve esperar o período de tempo de planejamento para os resultados sejam construídos. Por exemplo, uma procura semanal requer sete dias para construir os dados. Essa procura não retorna resultados antes que sete dias tenham decorrido.

Ao especificar o formato de saída para o relatório, considere que o tamanho do arquivo dos relatórios gerados pode ser de 1 a 2 megabytes, dependendo do formato de saída selecionado. O formato PDF é menor em tamanho e não consome uma grande quantidade de espaço de armazenamento em disco.

## Procedimento

1. Clique na guia **Relatórios**.
2. Na caixa de listagem **Ações**, selecione **Criar**.
3. Na alteração do assistente Boas-vindas ao Relatório, clique em **Avançar** para mover para a próxima página do assistente Relatório.
4. Selecione uma das opções a seguir:

Opção	Descrição
<b>Manualmente</b>	Gera um relatório uma vez. Essa é a configuração padrão; entretanto, você pode gerar esse relatório quando se fizer necessário.
<b>Por hora</b>	Planeja o relatório a ser gerado no fim de cada hora usando os dados da hora anterior.  Se você escolher a opção Por Hora, a configuração adicional será necessária. Nas caixas de listagem, selecione um prazo para começar e terminar o ciclo do relatório. Um relatório é gerado para cada hora dentro desse prazo. O horário está disponível em incrementos de meia hora. O padrão é de 1h para os campos <b>De</b> e <b>Para</b> .

Opção	Descrição
<b>Semanalmente</b>	Planeja o relatório a ser gerado semanalmente usando os dados da semana anterior.  Se você escolher a opção <b>Semanalmente</b> , a configuração adicional será necessária. Selecione o dia em que você deseja gerar o relatório. O padrão é segunda-feira. Na caixa de listagem, selecione uma hora para iniciar o ciclo do relatório. O horário está disponível em incrementos de meia hora. O padrão é de 1h.
<b>Mensalmente</b>	Planeja o relatório a ser gerado mensalmente usando os dados do mês anterior.  Se você escolher a opção <b>Mensalmente</b> , a configuração adicional será necessária. Na caixa de listagem, selecione a data em que você deseja gerar o relatório. O padrão é o primeiro dia do mês. Também use a caixa de listagem para selecionar um horário para o início do ciclo de relatório. O horário está disponível em incrementos de meia hora. O padrão é de 1h.

5. Na área de janela **Permitir com que esse relatório seja gerado manualmente, Sim ou Não**.
6. Configure o layout do relatório:
  - a. Na caixa de listagem **Orientação**, selecione a orientação da página: retrato ou paisagem.
  - b. Selecione uma das seis opções de layout que são exibidas no assistente Relatório.
  - c. Clique em **Avançar** para mover para a próxima página do assistente Relatório.
7. Especifique os valores para os parâmetros a seguir:
  - **Título do relatório** – insira um título do relatório. O título pode ter até 100 caracteres de comprimento. Não use caracteres especiais.
  - **Logotipo** – na caixa de listagem, selecione um logotipo.
  -
8. Configure cada contêiner no relatório:
  - a. Na caixa de listagem **Tipo de gráfico**, selecione um tipo de gráfico.
  - b. Na janela Detalhes do contêiner – <chart\_type>, configure os parâmetros do gráfico.
  - c. Clique em **Salvar detalhes do contêiner**.
  - d. Se necessário, repita as etapas a até c para todos os contêineres.
  - e. Clique em **Avançar** para mover para a próxima página do assistente Relatório.
9. Visualize a página Visualização de layout e, em seguida, clique em **Avançar** para mover para a próxima etapa do assistente Relatório.
10. Selecione as caixas de seleção para os formatos de relatório que você deseja gerar, e, em seguida, clique em **Avançar**.

**Nota:** A Linguagem de Marcação Extensível está disponível apenas para tabelas.

11. Selecione os canais de distribuição para o relatório, e, em seguida, clique em **Avançar**. As opções incluem os canais de distribuição a seguir:

Opção	Descrição
<b>Console de relatório</b>	Selecione essa caixa de seleção para enviar o relatório gerado para a guia <b>Relatórios</b> . Esse é o canal de distribuição padrão.
<b>Selecione os usuários que devem ser capazes de visualizar o relatório gerado.</b>	Essa opção será exibida após selecionar a caixa de seleção <b>Console de relatório</b> .  Na lista de usuários, selecione os usuários aos quais você deseja conceder a permissão para visualizar os relatórios gerados.
<b>Selecionar todos os usuários</b>	Essa opção será exibida somente após selecionar a caixa de seleção <b>Console de relatório</b> . Selecione essa caixa de seleção se você deseja conceder a permissão a todos os usuários para visualizar os relatórios gerados.  Você deve ter as permissões de rede apropriadas para compartilhar o relatório gerado com outros usuários.
<b>Email</b>	Selecione essa caixa de seleção se você deseja distribuir o relatório gerado usando o email.
<b>Insira o(s) endereço(s) de email de distribuição de relatório</b>	Essa opção será exibida somente após selecionar a caixa de seleção <b>Email</b> .  Insira 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 de 255.  Os destinatários de email recebem esse email de no_reply_reports@qradar.
<b>Incluir Relatório como anexo (apenas não HTML)</b>	Essa opção será exibida somente após selecionar a caixa de seleção <b>Email</b> . Selecione essa caixa de seleção para enviar o relatório gerado como um anexo.
<b>Incluir link no Console de Relatórios</b>	Essa opção será exibida somente após selecionar a caixa de seleção <b>Email</b> . Selecione essa caixa de opção para incluir um link no Console de Relatórios no email.

12. Na página Concluindo, insira os valores para os parâmetros a seguir:

Opção	Descrição
<b>Descrição do Relatório</b>	Insira uma descrição para esse relatório. A descrição é exibida na página Resumo do relatório e no email distribuição de relatório gerado.



Opção	Descrição
<b>Grupos</b>	Selecione os grupos aos quais você deseja designar esse relatório. Para obter mais informações sobre os grupos, consulte Grupos de relatório.
<b>Deseja executar o relatório agora?</b>	Selecione essa caixa de seleção, se você deseja gerar o relatório quando o assistente for concluído. Por padrão, a caixa de seleção fica selecionada.

13. Clique em **Avançar** para visualizar o resumo do relatório.
14. Na página Resumo do relatório, selecione as guias disponíveis no relatório de resumo para visualizar a configuração do relatório.

## Resultados

O relatório é gerado imediatamente. Se você limpou a caixa de seleção **Você gostaria de executar o relatório agora** na página final do assistente, o relatório será salvo e irá gerar o tempo de planejamento. 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

Usando o assistente Relatório, você pode editar qualquer relatório padrão ou customizado a ser alterado.

### Sobre Esta Tarefa

Você pode usar ou customizar um número significativo de relatórios padrão. A guia padrão **Relatórios** exibe a lista de relatórios. Cada relatório captura e exibe os dados existentes.

### Procedimento

1. Clique na guia **Relatórios**.
2. Dê um clique duplo no relatório que você deseja customizar.
3. No assistente Relatório, altere os parâmetros para customizar o relatório para gerar o conteúdo que você necessita.

### Resultados

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.

---

## Visualizando relatórios gerados

Na guia **Relatórios**, um ícone será exibido na coluna **Formatos** se um relatório possuir conteúdo gerado. Você pode clicar no ícone para visualizar o relatório.

## Sobre Esta Tarefa

Quando um relatório gerado possui conteúdo, a coluna **Relatórios gerados** exibe uma caixa de listagem. A caixa de listagem exibe todo o conteúdo gerado, que é organizado pelo registro de data e hora do relatório. Os relatórios mais recentes são exibidos no topo da lista. Se um relatório não possui conteúdo gerado, o valor **Nenhum** será exibido na coluna **Relatórios gerados**.

Ícones que representam o formato do relatório do relatório gerado são exibidos na coluna de **Formatos**.

Os relatórios podem ser gerados nos formatos de PDF, HTML, RTF, XML e XLS.

**Nota:** Os formatos XML e XLS estão disponíveis apenas para relatórios que usam um formato de tabela de gráfico único (retrato ou paisagem).

Você pode visualizar apenas os relatórios para o qual você tenha recebido acesso do administrador. Usuários administrativos podem acessar todos os relatórios.

Se você usar o navegador da web Mozilla Firefox e selecionar o formato do relatório RTF, o navegador da web Mozilla Firefox iniciará uma nova janela do navegador. Essa ativação da nova janela é o resultado da configuração do navegador da web Mozilla Firefox e não afeta o QRadar. Você pode fechar a janela e continuar com a sessão QRadar.

### Procedimento

1. Clique na guia **Relatórios**.
2. Na caixa de listagem da coluna **Relatórios gerados**, selecione o registro de data e hora do relatório que você deseja visualizar.
3. Clique no ícone para o formato que você deseja visualizar.

---

## Excluindo conteúdo gerado

Ao excluir o conteúdo gerado, todos os relatórios que foram gerados a partir do modelo de relatório serão excluídos, mas o modelo de relatório será retido.

### Procedimento

1. Clique na guia **Relatórios**.
2. Selecione os relatórios para o qual você deseja excluir o conteúdo gerado.
3. Na caixa de listagem **Ações**, clique em **Excluir conteúdo gerado**.

---

## Gerando um relatório manualmente

Um relatório pode ser configurado para gerar automaticamente; entretanto, você pode gerar um relatório manualmente a qualquer momento.

### Sobre Esta Tarefa

Enquanto um relatório é gerado, a coluna Próximo tempo de execução exibirá uma das três mensagens a seguir:

- **Gerando** – o relatório está sendo gerado.
- **Enfileirado (posição na fila)** – o relatório está enfileirado para ser gerado. 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 decrescente que especifica quando o relatório irá executar o próximo.

Você pode selecionar o ícone **Atualizar** para atualizar a visualização, incluindo as informações na coluna **Próximo tempo de execução**.

### Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja gerar.
3. Clique em **Executar relatório**.

### O que Fazer Depois

Após o relatório ser gerado, você poderá visualizar o relatório gerado na coluna **Relatórios gerados**.

---

## Duplicando um relatório

Para criar um relatório que se parece muito com um relatório existente, será possível duplicar o relatório que você deseja modelar e, em seguida, customizá-lo.

### Procedimento

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

### O que Fazer Depois

Você pode customizar o relatório duplicado.

---

## Compartilhando um relatório

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

### Sobre Esta Tarefa

Quaisquer atualizações que o usuário fizer em um relatório compartilhado não afetarão a versão original do relatório.

Você deve ter privilégios administrativos para compartilhar relatórios. Além disso, para um novo usuário visualizar e acessar relatórios, um usuário administrativo deve compartilhar todos os relatórios necessários com o novo usuário.

Você só pode compartilhar o relatório com usuários que têm o acesso apropriado.

### Procedimento

1. Clique na guia **Relatórios**.
2. Selecione os relatórios que você deseja compartilhar.
3. Na caixa de listagem **Ações**, clique em **Compartilhar**.

4. Na lista de usuários, selecione os usuários com quem você deseja compartilhar esse relatório.

---

## Relatórios de marca

Para relatórios de marca, é possível importar logotipos e imagens específicas. Para relatórios de marca com logotipos customizados, é necessário fazer upload e configurar os logotipos antes de começar a usar o assistente de relatório.

### Antes de Iniciar

Assegure-se de que o gráfico que deseja usar é de 144 x 50 pixels com um plano de fundo branco.

Para se assegurar-se de que seu navegador exibirá o novo logotipo, limpe o cache do navegador.

### Sobre Esta Tarefa

Marcação de relatório será benéfica para sua empresa se mais de um logotipo for suportado. Ao fazer upload de uma imagem, a imagem será automaticamente salva como Gráfico de Rede Móvel (PNG).

Ao fazer upload de uma nova imagem e configurar a imagem como seu padrão, a nova imagem padrão não será aplicada aos relatórios que foram gerados anteriormente. Atualizar o logotipo nos relatórios gerados anteriormente requer que seja gerado manualmente novo conteúdo a partir do relatório.

Se fizer upload de uma imagem que é maior em comprimento do que o cabeçalho do relatório pode suportar, a imagem será automaticamente redimensionada para se ajustar ao cabeçalho; isso significa aproximadamente 50 pixels de altura.

### Procedimento

1. Clique na guia **Relatórios**.
2. No menu de navegação, clique em **Marca**.
3. Clique em **Procurar** para procurar os arquivos que estão localizados em seu sistema.
4. Selecione o arquivo que contém o logotipo que deseja fazer upload. Clique em **Abrir**.
5. Clique em **Fazer upload da imagem**.
6. Selecione o logotipo que deseja usar como padrão e clique em **Configurar imagem padrão**.

---

## Grupos de relatórios

É possível classificar relatórios em grupos funcionais. Se categorizar relatórios em grupos, será possível organizar de forma eficiente e localizar os relatórios.

Por exemplo, é possível visualizar todos os relatórios que são relacionados à conformidade com o Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento (PCIDSS).

Por padrão, a guia **Relatórios** exibe a lista de todos os relatórios; no entanto, é possível categorizar os relatórios em grupos como, por exemplo:

- Conformidade
- Executivo
- Origens de log
- Gerenciamento de rede
- Segurança
- VoIP
- Outro

Ao criar um novo relatório, será possível designar o relatório em um grupo existente ou criar um novo grupo. Deve-se ter acesso administrativo para criar, editar ou excluir grupos.

Para obter mais informações sobre funções de usuário, consulte o *IBM Security QRadar SIEM Administration Guide*.

## Criando um grupo de relatórios

Você pode criar novos grupos.

### Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Usando a árvore de navegação, selecione o grupo no qual você deseja criar um novo grupo.
4. Clique em **Novo grupo**.
5. Insira valores para os seguintes parâmetros:
  - **Nome** – insira o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
  - **Descrição** - opcional. Insira uma descrição para esse grupo. A descrição pode ter até 255 caracteres de comprimento.
6. Clique em **OK**.
7. Para alterar o local do novo grupo, clique no novo grupo e arraste a pasta para o novo local na árvore de navegação.
8. Feche a janela Grupos de relatórios.

## Editando um grupo

Você pode editar um grupo de relatórios para alterar o nome ou a descrição.

### Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, selecione o grupo que você deseja editar.
4. Clique em **Editar**.
5. Atualize os valores para os parâmetros, conforme necessário:
  - **Nome** – insira o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
  - **Descrição** - opcional. Insira uma descrição para esse grupo. A descrição pode ter até 255 caracteres de comprimento. Esse campo é opcional.
6. Clique em **OK**.
7. Feche a janela Grupos de relatórios.

## Designar um relatório a um grupo

É possível usar a opção **Designar grupos** para designar um relatório para outro grupo.

### Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja designar para um grupo.
3. Na caixa de listagem **Ações**, selecione **Designar grupos**.
4. Na lista **Grupos de itens**, selecione a caixa de seleção do grupo que deseja designar para este relatório.
5. Clique em **Designar grupos**.

## Copiando um relatório para outro grupo

Use o ícone **Copiar** para copiar um relatório para um ou mais grupos de relatórios.

### Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, selecione o relatório que você deseja copiar.
4. Clique em **Copiar**.
5. Selecione o grupo ou grupos aos quais você deseja copiar o relatório.
6. Clique em **Designar grupos**.
7. Feche a janela Grupos de relatórios.

## Removendo um relatório

Use o ícone **Remover** para remover um relatório de um grupo.

### Sobre Esta Tarefa

Ao remover um relatório de um grupo, o relatório ainda existirá na guia **Relatórios**. O relatório não é removido do sistema.

### Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, navegue até a pasta que contém o relatório que você deseja remover.
4. Na lista de grupos, selecione o relatório que você deseja remover.
5. Clique em **Remover**.
6. Clique em **OK**.
7. Feche a janela Grupos de relatórios.

---

## Contêiner do gráfico

O tipo de gráfico determina como o relatório gerado apresenta dados e objetos de rede.

É possível classificar os dados com diversas características e criar os gráficos em um único relatório gerado.

## Parâmetros do contêiner do gráfico Vulnerabilidades de Ativo

A tabela a seguir descreve os parâmetros do contêiner do gráfico Vulnerabilidades de Ativo

Parâmetro	Descrição
<b>Detalhes do contêiner – Ativos</b>	
Chart Title	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Assets to Top	Na caixa de listagem, selecione quantos ativos você deseja incluir neste relatório.
Tipo de Gráfico	<p>Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem:</p> <ul style="list-style-type: none"> <li>• <b>Tabela agregada</b> – Exibe os dados em uma tabela agregada, que é uma tabela que contém subtabelas (sub-relatórios). Ao selecionar essa opção, será necessário configurar os detalhes de sub-relatório. A opção <b>Tabela</b> está disponível somente no contêiner com a página inteira de largura.</li> <li>• <b>Barra</b> – Exibe os dados em um gráfico de barras. Ao selecionar essa opção, o relatório não incluirá dados do sub-relatório. Este é o padrão. Este tipo de gráfico requer que a procura salva seja uma procura agrupada.</li> <li>• <b>Pizza</b> – Exibe os dados em um gráfico de pizza. Ao selecionar essa opção, o relatório não incluirá dados do sub-relatório. Este tipo de gráfico requer que a procura salva seja uma procura agrupada.</li> </ul> <p>Para visualizar exemplos de cada tipo de dados de diagramas, consulte <a href="#">Consulte tipos de diagrama</a>.</p>
Ordenar Ativos por	<p>Selecione o tipo de dados com o qual você deseja que o gráfico seja ordenado. As opções incluem:</p> <ul style="list-style-type: none"> <li>• <b>Ponderação do ativo</b> – Ordena os dados pela ponderação do ativo que está definido no perfil ativo.</li> <li>• <b>Risco CVSS</b> – Ordena os dados pelo nível de risco do Sistema de Pontuação de Vulnerabilidade Comum (CVSS). Para obter mais informações sobre o CVSS, consulte <a href="http://www.first.org/cvss/">http://www.first.org/cvss/</a>.</li> <li>• <b>Contagem de vulnerabilidade</b> – Ordena os dados pela contagem de vulnerabilidade dos ativos.</li> </ul>
<b>Detalhes do sub-relatório</b>	
Sub-relatório	Especifica o tipo de informações que é exibido no sub-relatório.
Classificar Sub-relatórios por	<p>Selecione o parâmetro pelo qual você deseja organizar os dados do sub-relatório. As opções incluem:</p> <ul style="list-style-type: none"> <li>• Risco (pontuação de base)</li> <li>• ID do OSVDB</li> <li>• Título OSVDB</li> <li>• Última data de modificação</li> <li>• Data da divulgação</li> <li>• Data da descoberta</li> </ul> <p>Para obter mais informações sobre o Banco de Dados de Vulnerabilidade de Software Livre (OSVDB), consulte <a href="http://osvdb.org/">http://osvdb.org/</a>.</p>
Limit Sub-report to Top	Na caixa de listagem, selecione quantas vulnerabilidades você deseja incluir nesse sub-relatório.
Graph Content	
Vulnerabilidades	<p>Para especificar as vulnerabilidades que deseja relatar:</p> <ol style="list-style-type: none"> <li>1. Clique em <b>Pesquisar</b>.</li> <li>2. Na caixa de listagem <b>Procurar por</b>, selecione o atributo de vulnerabilidade que deseja procurar. As opções incluem o ID do CVE, ID do Bugtraq, ID do OSVDB e Título do OSVDB. Para obter mais informações sobre atributos de vulnerabilidade, consulte <a href="#">Gerenciamento de ativos</a>.</li> <li>3. Na lista <b>Resultados da procura</b>, selecione as vulnerabilidades que deseja relatar. Clique em <b>Incluir</b>.</li> <li>4. Clique em <b>Enviar</b>.</li> </ol>

Parâmetro	Descrição
IP Address	Digite o endereço IP, o CIDR ou uma lista delimitada por vírgulas de endereços IP que deseja relatar. CIDRs parciais são permitidas.
Redes	Na árvore de navegação, selecione uma ou mais redes a partir das quais reunir dados do gráfico.

## Parâmetros do contêiner do gráfico de eventos/logs

A tabela a seguir descreve os parâmetros do contêiner do gráfico de eventos/logs:

*Tabela 62. Parâmetros do contêiner do gráfico de eventos/logs*

Parâmetro	Descrição
<i>Detalhes do contêiner – Eventos/logs</i>	
Chart Title	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Events/Logs to Top	Na caixa de listagem, selecione o número de eventos/logs a serem exibidos no relatório gerado.
Tipo de Gráfico	<p>Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem:</p> <ul style="list-style-type: none"> <li>• <b>Barra</b> – Exibe os dados em um gráfico de barras. Este é o tipo de gráfico padrão. Este tipo de gráfico requer que a procura salva seja uma procura agrupada.</li> <li>• <b>Linha</b> – Exibe os dados em um gráfico de linha.</li> <li>• <b>Pizza</b> – Exibe os dados em um gráfico de pizza. Este tipo de gráfico requer que a procura salva seja uma procura agrupada.</li> <li>• <b>Barras empilhadas</b> – Exibe os dados em um gráfico de barras empilhadas.</li> <li>• <b>Linhas empilhadas</b> – Exibe os dados em um gráfico de linhas empilhadas.</li> <li>• <b>Tabela</b> – Exibe os dados em formato de tabela. A opção <b>Tabela</b> está disponível somente para o contêiner com largura de página completa.</li> </ul> <p>Para visualizar exemplos de cada tipo de dados do gráfico, consulte Consulte Tipos de diagrama.</p>



Tabela 62. Parâmetros do contêiner do gráfico de eventos/logs (continuação)

Parâmetro	Descrição
Manual Scheduling	<p>A área de janela Planejamento manual é exibida apenas se a opção de planejamento <b>Manualmente</b> tiver sido selecionada no assistente Relatório.</p> <p>Usando as opções Planejamento manual, é possível criar um planejamento manual que pode executar um relatório em período de tempo definido customizado, com a opção de incluir apenas dados a partir das horas e dias que você selecionar. Por exemplo, é possível planejar um relatório para ser executado de 1 de outubro a 31 de outubro, incluindo apenas os dados que são gerados durante horários comerciais, como de segunda a sexta, das 8h às 21h.</p> <p>Para criar um planejamento manual:</p> <ol style="list-style-type: none"> <li>1. Na caixa de listagem <b>De</b>, digite a data de início que deseja para o relatório ou selecione a data usando o ícone <b>Calendário</b>. O padrão é a data atual.</li> <li>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 de 1h.</li> <li>3. Na caixa de listagem <b>Para</b>, digite a data de encerramento que deseja para o relatório, ou selecione a data usando o ícone <b>Calendário</b>. O padrão é a data atual.</li> <li>4. Nas caixas de listagem, selecione o horário de encerramento que deseja para o relatório. O horário está disponível em incrementos de meia hora. O padrão é de 1h.</li> <li>5. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>6. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos Processadores de eventos que estão associados à procura de eventos usada para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol>
Planejamento manual (continuação)	<p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> <li>1. Selecione a caixa de seleção <b>Seleção de dados de destino</b>. Opções adicionais são exibidas.</li> <li>2. Selecione a caixa de opções <b>Somente horas a partir de e</b>, em seguida, usando as caixas de listagem, selecione o intervalo de tempo que deseja para seu relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h.</li> <li>3. Selecione a caixa de seleção para cada dia da semana que deseja programar o relatório.</li> </ol>
Hourly Scheduling	<p>A área de janela Planejamento horário será exibida apenas se for selecionada a opção de planejamento <b>Horário</b> no assistente de relatório.</p> <ul style="list-style-type: none"> <li>• Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>• Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ul> <p>O Planejamento horário coloca em gráficos automaticamente todos os dados da hora anterior.</p>

Tabela 62. Parâmetros do contêiner do gráfico de eventos/logs (continuação)

Parâmetro	Descrição
Planejamento diário	<p>A área de janela Planejamento diário é exibida apenas se for selecionada a opção de planejamento <b>Diário</b> no assistente Relatório.</p> <ol style="list-style-type: none"> <li>1. Escolha uma das opções a seguir:</li> <li>2. <b>Todos os dados do dia anterior (24 horas)</b></li> <li>3. <b>Dados do dia anterior a partir de</b> – Nas caixas de listagem, selecione o período de tempo que você deseja para o relatório gerado. O horário está disponível em incrementos de meia hora. O padrão é de 1h.</li> <li>4. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>5. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol>
Planejamento semanal	<p>A área de janela Planejamento semanal é exibida apenas se for selecionada a opção de planejamento <b>Semanal</b> no assistente de relatório.</p> <ol style="list-style-type: none"> <li>1. Escolha uma das opções a seguir:</li> <li>2. <b>Todos os dados da semana anterior</b></li> <li>3. <b>Todos os dados da semana anterior a partir de</b> – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é domingo.</li> <li>4. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>5. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol> <p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> <li>1. Selecione a caixa de seleção <b>Seleção de dados de destino</b>. Opções adicionais são exibidas.</li> <li>2. Selecione a caixa de opções <b>Somente horas a partir de e</b>, em seguida, usando as caixas de listagem, selecione o intervalo de tempo que deseja para seu relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h.</li> <li>3. Selecione a caixa de seleção para cada dia da semana que deseja programar o relatório.</li> </ol>

Tabela 62. Parâmetros do contêiner do gráfico de eventos/logs (continuação)

Parâmetro	Descrição
Planejamento mensal	<p>A área de janela Planejamento mensal será exibida somente se a opção de planejamento <b>Mensal</b> for selecionada no assistente Relatório.</p> <ol style="list-style-type: none"> <li>Escolha uma das opções a seguir:</li> <li><b>Todos os dados do mês anterior</b></li> <li><b>Dados do mês anterior a partir de</b> – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é do dia 1 ao 31.</li> <li>Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de eventos usados para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol> <p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> <li>Selecione a caixa de seleção <b>Seleção de dados de destino</b>. Opções adicionais são exibidas.</li> <li>Selecione a caixa de opções <b>Somente horas a partir de e</b>, em seguida, usando as caixas de listagem, selecione o intervalo de tempo que deseja para seu relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h.</li> <li>Selecione a caixa de seleção para cada dia da semana que deseja programar o relatório.</li> </ol>
Graph Content	
Grupo	Na caixa de listagem, selecione um grupo de procura salvo para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem <b>Procuras salvas disponíveis</b> .
Digitar Procura Salva ou Selecionar a partir da Lista	Para refinar a lista <b>Procuras salvas disponíveis</b> , digite o nome da procura que você deseja localizar no campo <b>Digitar procura salva ou selecionar a partir da lista</b> . É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite <i>Firewall</i> para exibir uma lista de todas as procuras que incluem Firewall no nome da procura.
Procuras Salvas Disponíveis	Fornecer uma lista de procuras salvas disponíveis. Por padrão, todas as procuras salvas disponíveis são exibidas, no entanto, é possível filtrar a lista selecionando um grupo da caixa de listagem <b>Grupo</b> ou digitando o nome de uma procura conhecida salva no campo <b>Digitar procura salva ou selecionar a partir da lista</b> .
Create New Event Search	Clique em <b>Criar nova procura de eventos</b> para criar uma nova procura. Para obter mais informações sobre como criar uma procura de evento, consulte Consultar Investigação de atividade de log.

## Parâmetros do contêiner do gráfico de fluxo

A tabela a seguir descreve os parâmetros do contêiner do gráfico de fluxo:

Tabela 63. Detalhes do contêiner do gráfico do fluxo

Parâmetro	Descrição
Detalhes do contêiner - Fluxos	
Chart Title	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Flows to Top	Na caixa de listagem, selecione o número de fluxos a serem exibidos no relatório gerado.

Tabela 63. Detalhes do contêiner do gráfico do fluxo (continuação)

Parâmetro	Descrição
Tipo de Gráfico	<p>Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem:</p> <ul style="list-style-type: none"> <li>• <b>Barra</b> – Exibe os dados em um gráfico de barras. Este é o tipo de gráfico padrão. Este tipo de gráfico requer que a procura salva seja uma procura agrupada.</li> <li>• <b>Linha</b> – Exibe os dados em um gráfico de linha.</li> <li>• <b>Pizza</b> – Exibe os dados em um gráfico de pizza. Este tipo de gráfico requer que a procura salva seja uma procura agrupada.</li> <li>• <b>Barras empilhadas</b> – Exibe os dados em um gráfico de barras empilhadas.</li> <li>• <b>Linhas empilhadas</b> – Exibe os dados em um gráfico de linhas empilhadas.</li> <li>• <b>Tabela</b> – Exibe os dados em formato de tabela.</li> </ul>
Manual Scheduling	<p>A área de janela Planejamento manual é exibida apenas se a opção de planejamento <b>Manualmente</b> tiver sido selecionada no assistente Relatório.</p> <p>Usando as opções Planejamento manual, é possível criar um planejamento manual que pode executar um relatório em período de tempo definido customizado, com a opção de incluir apenas dados a partir das horas e dias que você selecionar. Por exemplo, é possível planejar um relatório para ser executado de 1 de outubro a 31 de outubro, incluindo apenas os dados que são gerados durante horários comerciais, como de segunda a sexta, das 8h às 21h.</p> <p>Para criar um planejamento manual:</p> <ol style="list-style-type: none"> <li>1. Na caixa de listagem <b>De</b>, digite a data de início que deseja para o relatório ou selecione a data usando o ícone <b>Calendário</b>. O padrão é a data atual.</li> <li>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 de 1h.</li> <li>3. Na caixa de listagem <b>Para</b>, digite a data de encerramento que deseja para o relatório, ou selecione a data usando o ícone <b>Calendário</b>. O padrão é a data atual.</li> <li>4. Nas caixas de listagem, selecione o horário de encerramento que deseja para o relatório. O horário está disponível em incrementos de meia hora. O padrão é de 1h.</li> <li>5. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>6. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos Processadores de Eventos que serão associados ao fluxo de procura usado para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol>
	<p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> <li>1. Selecione a caixa de seleção <b>Seleção de dados de destino</b>. Opções adicionais são exibidas.</li> <li>2. Selecione a caixa de opções <b>Somente horas a partir de e</b>, em seguida, usando as caixas de listagem, selecione o intervalo de tempo que deseja para seu relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h.</li> <li>3. Selecione a caixa de seleção para cada dia da semana que deseja programar o relatório.</li> </ol>


Tabela 63. Detalhes do contêiner do gráfico do fluxo (continuação)

Parâmetro	Descrição
Hourly Scheduling	<p>A área de janela Planejamento horário será exibida apenas se for selecionada a opção de planejamento <b>Horário</b> no assistente de relatório.</p> <ul style="list-style-type: none"> <li>• Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>• Ao configurar o parâmetro <b>Timezone</b>, considere o local dos Processadores de Eventos que serão associados ao fluxo de procura usado para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ul> <p>O Planejamento horário coloca em gráficos automaticamente todos os dados da hora anterior.</p>
Planejamento diário	<p>A área de janela Planejamento diário é exibida apenas se for selecionada a opção de planejamento <b>Diário</b> no assistente Relatório.</p> <ol style="list-style-type: none"> <li>1. Escolha uma das opções a seguir:</li> <li>2. <b>Todos os dados do dia anterior (24 horas)</b></li> <li>3. <b>Dados do dia anterior a partir de</b> – Nas caixas de listagem, selecione o período de tempo que você deseja para o relatório gerado. O horário está disponível em incrementos de meia hora. O padrão é de 1h.</li> <li>4. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>5. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de fluxo usada para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol>

Tabela 63. Detalhes do contêiner do gráfico do fluxo (continuação)

Parâmetro	Descrição
Planejamento semanal	<p>A área de janela Planejamento semanal é exibida apenas se for selecionada a opção de planejamento <b>Semanal</b> no assistente de relatório.</p> <ol style="list-style-type: none"> <li>1. Escolha uma das opções a seguir:</li> <li>2. Todos os dados da semana anterior</li> <li>3. <b>Todos os dados da semana anterior a partir de</b> – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é domingo.</li> <li>4. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>5. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de fluxo usada para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol> <p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> <li>1. Selecione a caixa de seleção <b>Seleção de dados de destino</b>. Opções adicionais são exibidas.</li> <li>2. Selecione a caixa de opções <b>Somente horas a partir de e</b>, em seguida, usando as caixas de listagem, selecione o intervalo de tempo que deseja para seu relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h.</li> <li>3. Selecione a caixa de seleção para cada dia da semana que deseja programar o relatório.</li> </ol>
Planejamento mensal	<p>A área de janela Planejamento mensal será exibida somente se a opção de planejamento <b>Mensal</b> for selecionada no assistente Relatório.</p> <ol style="list-style-type: none"> <li>1. Escolha uma das opções a seguir:</li> <li>2. <b>Todos os dados do mês anterior</b></li> <li>3. <b>Dados do mês anterior a partir de</b> – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é do dia 1 ao 31.</li> <li>4. Na caixa de listagem <b>Fuso horário</b>, selecione o fuso horário que deseja usar para o relatório.</li> <li>5. Ao configurar o parâmetro <b>Timezone</b>, considere o local dos processadores de evento associados à procura de fluxo usada para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários processadores de Eventos ampliando vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir de processadores de Eventos na América do Norte e Europa e o fuso horário for configurado para <b>GMT -5.00 America/New_York</b>, os dados da Europa relatarão o fuso horário incorretamente.</li> </ol> <p>Para refinar ainda mais seu planejamento:</p> <ol style="list-style-type: none"> <li>1. Selecione a caixa de seleção <b>Seleção de dados de destino</b>. Opções adicionais são exibidas.</li> <li>2. Selecione a caixa de opções <b>Somente horas a partir de e</b>, em seguida, usando as caixas de listagem, selecione o intervalo de tempo que deseja para seu relatório. Por exemplo, é possível selecionar apenas horas das 8h às 17h.</li> <li>3. Selecione a caixa de seleção para cada dia da semana que deseja programar o relatório.</li> </ol>
Conteúdo do gráfico	
Grupo	<p>Na caixa de listagem, selecione um grupo de procura salvo para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem <b>Procuras salvas disponíveis</b>.</p>

Tabela 63. Detalhes do contêiner do gráfico do fluxo (continuação)

Parâmetro	Descrição
Digitar Procura Salva ou Seleccionar a partir da Lista	Para refinar a lista <b>Procuras salvas disponíveis</b> , digite o nome da procura que você deseja localizar no campo <b>Digitar procura salva ou seleccionar a partir da lista</b> . É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite    para exibir uma lista de todas as procuras que incluem Firewall no nome de procura.
Procuras Salvas Disponíveis	Fornece uma lista de procuras salvas disponíveis. Por padrão, todas as procuras salvas disponíveis são exibidas, no entanto, é possível filtrar a lista selecionando um grupo da caixa de listagem <b>Grupo</b> ou digitando o nome de uma procura conhecida salva no campo <b>Digitar procura salva ou seleccionar a partir da lista</b> .
Criar Nova Procura de Fluxo	Clique em <b>Criar nova procura de fluxo</b> para criar uma nova procura.

## Parâmetros do contêiner do gráfico Principais IPs de origem

A tabela a seguir descreve os parâmetros do contêiner do gráfico Principais IPs de origem

Parâmetro	Descrição
<b>Container Details - Top Source IPs</b>	
Chart Title	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Top Source IPs to	Na caixa de listagem, selecione o número de IPs de origem a serem exibidos no relatório gerado.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: <ul style="list-style-type: none"> <li>• <b>Tabela</b> Exibe os dados no formato de tabela (somente com contêiner com largura total).</li> <li>• <b>Barra horizontal</b> Exibe os dados em um gráfico de barras.</li> </ul>
Classificar Resultados por	Na caixa de listagem, selecione como os dados são classificados no gráfico. As opções incluem: <ul style="list-style-type: none"> <li>• Ponderação do ativo</li> <li>• Risco</li> <li>• Magnitude</li> </ul>
<b>Conteúdo do gráfico</b>	
Redes	Na árvore de navegação, selecione uma ou mais redes a partir das quais reunir dados do gráfico.

## Parâmetros do contêiner do gráfico Principais ofensas

A tabela a seguir descreve os parâmetros do contêiner do gráfico Principais ofensas

Tabela 64. Parâmetros do contêiner do gráfico Principais ofensas

Parâmetro	Descrição
<b>Detalhes do contêiner – Principais ofensas</b>	
Chart Title	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Top Offenses To	Na caixa de listagem, selecione o número de crimes a incluir nos gráficos. O padrão é 10.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: <ul style="list-style-type: none"> <li>• <b>Tabela</b> – Exibe os dados em formato de tabela (somente contêiner com largura total).</li> <li>• <b>Barra horizontal</b> – Exibe os dados em um gráfico de barras.</li> </ul>

Tabela 64. Parâmetros do contêiner do gráfico Principais ofensas (continuação)

Parâmetro	Descrição
Ordenar Resultados por:	Na caixa de listagem, selecione como os dados são classificados no gráfico. As opções incluem: <ul style="list-style-type: none"> <li>• Gravidade</li> <li>• Magnitude</li> <li>• Relevância</li> <li>• Credibilidade</li> </ul>
<b>Conteúdo do gráfico - Parameter Based</b>	
Parameter Based	Selecione essa opção se desejar incluir um gráfico Principais ofensas baseado em parâmetro em seu relatório. Quando essa opção for selecionada, os parâmetros <b>Include</b> , <b>Offenses Category</b> e <b>Networks</b> serão exibidos.
Include	Essa opção será exibida somente se a opção <b>Baseado em parâmetro</b> for selecionada.  Selecione a caixa de seleção ao lado da opção que deseja incluir no relatório gerado. As opções são: <ul style="list-style-type: none"> <li>• Crimes Ativos</li> <li>• Crimes Inativos</li> <li>• Crimes Ocultos</li> <li>• Crimes Encerrados</li> </ul> As opções <b>Ofensas ativas</b> e <b>Ofensas inativas</b> são selecionadas por padrão.  Se limpar todas as caixas de seleção, nenhuma restrição será aplicada ao relatório gerado; portanto, o relatório gerado incluirá todas as ofensas.
Offenses Category	Essa opção será exibida somente se a opção <b>Baseado em parâmetro</b> for selecionada.  Na caixa de listagem <b>Categoria de alto nível</b> , selecione a categoria de alto nível que deseja incluir no relatório gerado.  Na caixa de listagem <b>Categoria de nível inferior</b> , selecione uma categoria de baixo nível que deseja incluir no relatório gerado.  Para obter mais informações sobre categorias de alto e de nível inferior, consulte <i>IBM Security QRadar SIEM Administration Guide</i> .
Redes	Essa opção será exibida somente se a opção <b>Baseado em parâmetro</b> for selecionada.  Na árvore de navegação, selecione uma ou mais redes a partir das quais reunir dados do gráfico.
<b>Conteúdo do gráfico - Baseado em procura salva</b>	
Saved Search Based	Selecione essa opção se quiser incluir um gráfico Principais ofensas baseado em procura salva em seu relatório. Quando essa opção estiver selecionada, os parâmetros <b>Group</b> , <b>Type Saved Search ou Select from List e Available Saved Searches</b> serão exibidos.
Grupo	Na caixa de listagem, selecione um grupo de procura salva para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem <b>Procuras salvas disponíveis</b> .
Digitar Procura Salva ou Selecionar a partir da Lista	Para refinar a lista <b>Procuras salvas disponíveis</b> , digite o nome da procura que você deseja localizar no campo <b>Digitar procura salva ou selecionar a partir da lista</b> . É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite <code>Firewall</code> para exibir uma lista de todas as procuras que incluem <code>Firewall</code> no nome da procura.
Procuras Salvas Disponíveis	Fornece uma lista de procuras salvas disponíveis. Por padrão, todas as procuras salvas disponíveis são exibidas, no entanto, é possível filtrar a lista selecionando um grupo da caixa de listagem <b>Grupo</b> ou digitando o nome de uma procura conhecida salva no campo <b>Digitar procura salva ou selecionar a partir da lista</b> .

## Parâmetros do contêiner do gráfico Principais IPs de destino

A tabela a seguir descreve os parâmetros do contêiner do gráfico Principais IPs de Destino:



*Tabela 65. Parâmetros do contêiner do gráfico Principais IPs de destino*

Parâmetro	Descrição
<b>Detalhes do contêiner – Principais IPs de destino</b>	
Chart Title	Digite um título de gráfico de, no máximo, 100 caracteres.
Chart Sub-Title	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limit Top Destination IPs to	Na caixa de listagem, selecione o número de IPs de destino a ser exibido no relatório gerado.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: <ul style="list-style-type: none"> <li>• <b>Tabela</b> – Exibe os dados em formato de tabela (somente contêiner com largura total).</li> <li>• <b>Barra horizontal</b> – Exibe os dados em um gráfico de barras.</li> </ul>
Classificar Resultados por	Na caixa de listagem, selecione como os dados são exibidos no gráfico. As opções incluem: <ul style="list-style-type: none"> <li>• Ponderação do ativo</li> <li>• Nível de risco</li> <li>• Magnitude</li> </ul>
<b>Conteúdo do gráfico</b>	
Redes	Na árvore de navegação, selecione uma ou mais redes a partir das quais reunir dados do gráfico.



---

## 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 documentação em outros países. Consulte seu representante IBM local para obter informações sobre os 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 garante ao Cliente nenhum direito 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 consultas sobre licenças a respeito de informações do conjunto de caracteres de byte duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, 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 ao Reino Unido ou a qualquer 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 estados não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Estas informações podem incluir 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.

Quaisquer referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes 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 ele para o propósito de ativação: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações que foram trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil  
Av. Pasteur, 138-14  
Botafogo  
Rio de Janeiro, RJ  
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriados, 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 IBM Customer Agreement, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados sobre desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais poderão variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido estimadas por meio de 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 instruções relativas às direções ou intenções futuras da IBM estão sujeitas a mudanças ou retirada sem aviso prévio, e apenas representam metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso. Os preços dos revendedores podem variar.

Essas informações contêm exemplos de dados e relatórios usados em operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em formato eletrônico, as fotografias e ilustrações coloridas podem não aparecer.

---

## Marcas registradas

A IBM, o logotipo IBM e [ibm.com](http://ibm.com) são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca registrada da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca registrada (® ou ™), esses símbolos indicarão marcas registradas ou de direito consuetudinário dos Estados Unidos, de propriedade da IBM no momento em que estas informações foram publicadas. Essas marcas registradas também podem ser marcas registradas ou marcas registradas de direito consuetudinário em outros países. Uma lista atual de marcas registradas da IBM está disponível na web em Informações de copyright e de marca registrada ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)).

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros



países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows NT e o logotipo Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e nomes de serviços podem ser marcas ou marcas de serviço de terceiros.

---

## Considerações de política de privacidade

Os produtos de Software IBM, incluindo soluções de software as a service, (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, ajustar as interações com o usuário final ou para outras finalidades. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar as informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies desta oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, essa Oferta de Software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de gerenciamento de sessões e autenticação. Estes cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de Software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos

usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis a essa 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>, a seção intitulada “Cookies, Web Beacons e Outras Tecnologias”, na Declaração de Privacidade Online da IBM em <http://www.ibm.com/privacy/details/br/pt/> e “IBM Software Products and Software-as-a-Service Privacy Statement” em <http://www.ibm.com/software/info/product-privacy>.

---

## Glossário

Este glossário fornece termos e definições para software e produtos do IBM Security QRadar SIEM.

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 completo.
- *Consulte também* o encaminha para um termo relacionado ou contrastante.

Para obter outros termos e definições, consulte o Website de terminologia IBM (abre em uma nova janela).

"A" "B" "C" "D" na página 190 "E" na página 190 "F" na página 190 "G" na página 190 "H" na página 191 "I" na página 191 "L" na página 191 "M" na página 191 "N" na página 192 "O" na página 192 "P" na página 193 "R" na página 193 "S" na página 194 "T" na página 194 "V" na página 194

---

### A

#### acumulador

Um registro no qual um operando de uma operação pode ser armazenado e, subsequentemente, substituído pelo resultado dessa operação.

#### alta disponibilidade (HA)

Relativo a um sistema em cluster que será reconfigurado quando as falhas do nó ou do daemon ocorrerem de forma que as cargas de trabalho possam ser redistribuídas para os nós restantes no cluster.

#### anomalia

Um desvio do comportamento esperado da rede.

**ARP** Consulte Protocolo de Resolução de Endereço.

**ASN** Consulte número de sistema autônomo.

#### assinatura de aplicativo

Um conjunto exclusivo de características que são derivadas pelo exame da carga

útil do pacote e, em seguida, são usadas para identificar um aplicativo específico.

---

### B

#### Banco de Dados de Vulnerabilidade de Software Livre (OSVDB)

Criado pela comunidade de segurança de rede para a comunidade de segurança de rede, é um banco de dados de software livre que fornece informações técnicas sobre vulnerabilidades de segurança de rede.

---

### C

#### camada de rede

Na arquitetura OSI, a camada que fornece serviços para estabelecer um caminho entre sistemas abertos com uma qualidade de serviço previsível.

#### captura de conteúdo

Um processo que captura uma quantidade configurável de carga útil e em seguida, armazena os dados em um log de fluxo.

**CIDR** Consulte Classless Inter-Domain Routing.

#### Classless Inter-Domain Routing (CIDR)

Um método para incluir endereços Internet Protocol (IP) de classe C. Os endereços são oferecidos aos Provedores de Serviços da Internet (ISPs) para uso de seus clientes. Os endereços CIDR reduzem o tamanho das tabelas de roteamento e tornam mais endereços IP disponíveis nas organizações.

#### cliente

Um programa de software ou um computador que solicita serviços de um servidor.

#### cluster de HA

Uma configuração de alta disponibilidade que consiste em um servidor primário e um servidor secundário.

#### Código de Autenticação de Mensagem com Base em Hash (HMAC)

Um código criptográfico que usa uma função hash criptográfica e uma chave secreta.

**comportamento**

Os efeitos observáveis de uma operação ou de um evento, incluindo seus resultados.

**conjunto de referência**

Uma lista de elementos únicos derivados de eventos ou fluxos em uma rede. Por exemplo, uma lista de endereços IP ou uma lista de nomes de usuários.

**console**

Uma estação de exibição a partir da qual um operador pode controlar e observar a operação do sistema.

**contexto do host**

Um serviço que monitora os componentes para assegurar-se de que cada componente está operando conforme o esperado.

**Conversão de Endereço de Rede (NAT)**

Em um firewall, a conversão dos endereços Internet Protocol (IP) seguros para endereços registrados externos. Isto ativa comunicações com redes externas, mas mascara os endereços IP usados dentro do firewall.

**credencial**

Um conjunto de informações que concede a um usuário ou processo determinados direitos de acesso.

**credibilidade**

Uma classificação numérica de 0 a 10 que é usada para determinar a integridade de um evento ou de um crime. A credibilidade aumenta à medida que várias origens relatam o mesmo evento ou ofensa.

**criptografia**

Em segurança de computadores, o processo de transformar dados em um formato ininteligível, de forma que os dados originais não possam ser obtidos ou só possam ser obtidos com o uso de um processo de decifração.

**cronômetro de atualização**

Um dispositivo interno que é acionado manual ou automaticamente em intervalos planejados que atualiza os dados de atividade de rede atuais.

**CVSS** Consulte Sistema de Pontuação de Vulnerabilidade Comum.

---

**D****dados de carga útil**

Os dados do aplicativo contidos em um fluxo de IP, excluindo informações de cabeçalho e administrativas.

**destino de encaminhamento**

Um ou mais sistemas do fornecedor que recebem dados brutos e normalizados de origens de log e de fluxo.

**destino externo**

Um dispositivo que está ausente do site primário que recebe fluxo de dados ou eventos de um coletor de eventos.

**DHCP** Consulte Protocolo de Configuração de Host Dinâmico.

**DNS** Consulte Sistema de Nomes de Domínio.

**DSM** Consulte Módulo de Suporte de Dispositivo.

**duplicar fluxo**

Várias instâncias da mesma transmissão de dados receberam de diferentes origens de fluxos.

---

**E****endereço IP virtual de cluster**

Um endereço IP que é compartilhado entre o host primário ou secundário e o cluster de HA.

---

**F**

**fluxo** Uma única transmissão de dados transmitida per meio de um link durante uma conversação.

**folha** Em uma árvore, uma entrada ou nó que não tem filhos.

**FQDN** Consulte o nome completo do domínio.

**FQNN** Consulte nome completo de rede.

---

**G****gateway**

Um dispositivo ou programa usado para conectar redes ou sistemas com diferentes arquiteturas de rede.



---

## H

**HA** Consulte alta disponibilidade.

### **hierarquia de rede**

Um tipo de contêiner que é uma coleção hierárquica de objetos da rede.

### **HMAC**

Consulte Código de Autenticação de Mensagem com Base em Hash.

### **host de HA primário**

O computador principal que está conectado ao cluster de HA.

### **host de HA secundário**

O computador em espera que está conectado ao cluster de HA. O host de HA secundário assumirá a responsabilidade do host de HA primário se o host de HA primário falhar.

---

## I

**ICMP** Consulte Internet Control Message Protocol.

### **identidade**

Uma coleção de atributos de uma origem de dados que representa uma pessoa, organização, local ou item.

**IDS** Consulte sistema de detecção de intrusão.

### **Interconexão de sistemas abertos (OSI)**

A interconexão de sistemas abertos em concordância com padrões da Organização Internacional para Normatização (ISO) para a troca de informações.

### **Internet Control Message Protocol (ICMP)**

Um Internet Protocol que é usado por um gateway para se comunicar com outro host de origem como, por exemplo, para relatar um erro em um datagrama.

### **Internet Protocol (IP)**

Um protocolo que roteia dados por meio de uma rede ou redes interconectadas. Esse protocolo atua como um intermediário entre camadas de protocolo superiores e a rede física. Consulte também Protocolo de Controle de Transmissões.

### **intervalo de relatório**

Um intervalo de tempo configurável no final do qual o processador de evento

deverá enviar todos os dados de fluxo e de eventos capturados para o console.

### **intervalo de união**

O intervalo no qual os eventos são empacotados. O pacote configurável de eventos ocorre em intervalos de 10 segundos e começa com o primeiro evento que não corresponde a nenhum evento de união atual. No intervalo de união, os três primeiros eventos correspondentes são empacotados e enviados para o processador de eventos.

**IP** Consulte Internet Protocol.

### **IP multicast**

Transmissão de um datagrama de Internet Protocol (IP) para um conjunto de sistemas que formam um único grupo multicast.

**IPS** Consulte sistema de prevenção de intrusão.

**ISP** Consulte provedor de serviços da internet.

---

## L

**LAN** Consulte rede local.

**LDAP** Consulte protocolo LDAP.

**L2L** Consulte Local para Local.

### **Local para Local (L2L)**

Relativo ao tráfego interno de uma rede local para outra rede local.

### **Local para Remoto (L2R)**

Relativo ao tráfego interno de uma rede local para outra rede remota.

### **log de fluxo**

Uma coleção de registros de fluxo.

**L2R** Consulte Local para Remoto.

---

## M

### **magistrate**

Um componente interno que analisa o tráfego de rede e os eventos de segurança com relação a regras customizadas definidas.

### **magnitude**

Uma medida da importância relativa de uma determinada ofensa. Magnitude é um valor ponderado calculado a partir da relevância, severidade e credibilidade.

### **mapa de referência**

Um registro de dados de mapeamento direto de uma chave para um valor, por exemplo, um nome de usuário para um ID global.

### **Mapa de referência de conjuntos**

Um registro de dados de uma chave mapeada para muitos valores. Por exemplo, o mapeamento de uma lista de usuários privilegiados para um host.

### **Mapa de referência de mapas**

Um registro de dados de duas chaves mapeado para muitos valores. Por exemplo, o mapeamento do total de bytes de um aplicativo para um IP de origem.

### **Mapa QID**

Uma taxonomia que identifica cada evento exclusivo e mapeia os eventos das categorias de alto e nível inferior para determinar como um evento deve ser correlacionado e organizado.

### **máscara de sub-rede**

Para sub-rede da Internet, uma máscara de 32 bits é usada para identificar os bits do endereço da sub-rede na parte do host de um endereço IP.

### **Módulo de Suporte de Dispositivo (DSM)**

Um arquivo de configuração que analisa os eventos recebidos a partir de várias origens de log e converte-os em um formato de taxonomia padrão que pode ser exibida como saída.

---

## **N**

**NAT** Consulte Conversão de Endereço de Rede.

### **NetFlow**

Um protocolo de rede Cisco que monitora dados de fluxo de tráfego de rede. Os dados NetFlow incluem as informações do cliente e do servidor, quais portas estão sendo usadas e o número de bytes e pacotes que são transmitidos por meio dos comutadores e roteadores conectados a uma rede. Os dados são enviados para coletores NetFlow em que a análise de dados ocorre.

### **nome completo da rede (FQNN)**

Em uma hierarquia de rede, o nome de um objeto que inclui todos os departamentos. Um exemplo de um nome

completo de rede é  
CompanyA.Department.Marketing.

### **nome completo do domínio (FQDN)**

Em comunicações da Internet, o nome de um sistema host que inclui todos os subnomes do nome de domínio. Um exemplo de um nome completo do domínio é rchland.vnet.ibm.com.

### **número do sistema autônomo (ASN)**

Em TCP/IP, um número que é designado para um sistema autônomo pela mesma autoridade central que designa endereços IP. O número de sistema autônomo possibilita que algoritmos de roteamento automatizado façam distinção entre sistemas autônomos.

---

## **O**

### **objeto de rede**

Um componente de uma hierarquia de rede.

### **objeto folha de banco de dados**

Um objeto terminal ou nó em uma hierarquia de banco de dados.

**ofensa** Uma mensagem enviada ou um evento gerado em resposta a uma condição monitorada. Por exemplo, um crime fornecerá informações sobre se uma política foi violada ou se a rede está sob ataque.

### **origem de log**

O equipamento de segurança ou o equipamento de rede a partir do qual é originado um log de eventos.

### **origem externa**

Um dispositivo que está fora do site primário que encaminha dados normalizados a um coletor de eventos.

### **origens de fluxo**

A fonte a partir da qual o fluxo é capturado. Uma fonte de fluxo será classificada como interna quando o fluxo for proveniente do hardware instalado em um host gerenciado ou será classificada como externa quando o fluxo for enviado para um coletor de fluxo.

**OSI** Consulte interconexão de sistemas abertos.

## OSVDB

Consulte Banco de Dados de Vulnerabilidade de Software Livre.

---

## P

### peso da rede

O valor numérico aplicado a cada rede que significa a importância da rede. O peso da rede é definido pelo usuário.

### ponto de dados

Um valor calculado de uma métrica em um momento.

### positivo falso

Um resultado de teste classificado como positivo (indicando que o site está vulnerável ao ataque), que o usuário decide que é na realidade negativo (não é uma vulnerabilidade).

### protocolo

Um conjunto de regras que controlam a comunicação e transferência de dados entre dois ou mais dispositivos ou sistemas em uma rede de comunicação.

### Protocolo de Configuração de Host Dinâmico (DHCP)

Um protocolo de comunicação que é usado para gerenciar centralmente as informações de configuração. Por exemplo, o DHCP designa automaticamente endereços IP para computadores em uma rede.

### Protocolo de Controle de Transmissões (TCP)

Um protocolo de comunicação usado na Internet e em todas as redes que seguem os padrões da Internet Engineering Task Force (IETF) para protocolo de interligação de redes. O TCP oferece um protocolo confiável de host para host em redes de comunicação comutadas por pacotes e em sistemas interconectados dessas redes. Consulte também Internet Protocol.

### Protocolo de Resolução de Endereço (ARP)

Um protocolo que mapeia dinamicamente um endereço IP para um endereço de adaptador de rede em uma rede local.

### protocolo LDAP (LDAP)

Um protocolo aberto que usa o TCP/IP para fornecer acesso a diretórios que suportam um modelo X.500 e que não está sujeito aos requisitos de recursos do

Protocolo de Acesso a Diretório (DAP) X.500 mais complexo. Por exemplo, o LDAP pode ser usado para localizar pessoas, organizações e outros recursos em um diretório da Internet ou da intranet.

### Protocolo Simples de Gerenciamento de Rede (SNMP)

Um conjunto de protocolos para sistemas de monitoramento e dispositivos em redes complexas. As informações sobre os dispositivos gerenciados são definidas e armazenadas em uma Management Information Base (MIB).

### Provedor de serviços de internet (ISP)

Uma organização que fornece acesso à Internet.

---

## R

### Rede local (LAN)

Uma rede que conecta diversos dispositivos em uma área limitada (como um único edifício ou campus) e que pode ser conectada a uma rede maior.

### Redirecionamento do ARP

Um método ARP para notificar o host se existir um problema em uma rede.

**regra** Um conjunto de instruções condicionais que permitem que os sistemas de computador identifiquem relacionamentos e executem respostas automatizadas adequadamente.

### regra de roteamento

Uma condição que, quando seus critérios forem atendidos por dados do evento, uma coleção de condições e roteamento subsequente será executada.

### relatório

Em um gerenciamento de consulta, os dados formatados que resultam da execução de uma consulta e da aplicação de um formulário a ela.

### relevância

Uma medida de impacto relativo de um evento, categoria ou ofensa na rede.

### Remoto para Local (R2L)

O tráfego externo de uma rede remota para uma rede local.

**Remoto para Remoto (R2R)**

O tráfego externo de uma rede remota para outra rede remota.

**R2L** Consulte Remoto para Local.

**R2R** Consulte Remoto para Remoto.

---

**S****servidor whois**

Um servidor que é usado para recuperar informações sobre recursos registrados na Internet, como nomes de domínio e alocações de endereço IP.

**severidade**

Uma medida da ameaça relativa que uma origem coloca em um destino.

**sistema ativo**

Em um cluster de alta disponibilidade (HA), o sistema que possui todos os seus serviços em execução.

**sistema de detecção de intrusão (IDS)**

Software que detecta tentativas ou ataques bem sucedidos a recursos monitorados que fazem parte de uma rede ou sistema host.

**sistema de espera**

Um sistema que automaticamente se torna ativo quando o sistema ativo falhar. Se a replicação de disco estiver ativada, ela replicará dados do sistema ativo.

**Sistema de Nomes de Domínio (DNS)**

O sistema de banco de dados distribuído que mapeia os nomes de domínio para endereços IP.

**Sistema de Pontuação de Vulnerabilidade Comum (CVSS)**

Um sistema de pontuação pelo qual a severidade de uma vulnerabilidade é medida.

**sistema de prevenção de intrusão (IPS)**

Um sistema que tenta negar atividade potencialmente maliciosa. Os mecanismos de negação podem envolver filtragem, rastreamento ou configuração de limites de taxa.

**SNMP**

Consulte Protocolo Simples de Gerenciamento de Rede.

**SOAP** Um protocolo leve baseado em XML para troca de informações em um ambiente

distribuído e descentralizado. O SOAP pode ser usado para consultar e retornar informações e chamar serviços na Internet.

**sub-procura**

Uma função que permite que uma consulta de procura seja executada em um conjunto de resultados da procura concluída.

**sub-rede**

Uma rede que é dividida em subgrupos independentes menores, que ainda são interconectados.

**sub-rede**

Consulte sub-rede.

**super fluxo**

Um único fluxo que é composto de vários fluxos com propriedades semelhantes para aumentar a capacidade de processamento reduzindo as restrições de armazenamento.

---

**T****tabela de referência**

Uma tabela em que o registro de dados mapeia chaves que têm um tipo designado para outras chaves que são, em seguida, mapeadas para um único valor.

**TCP** Consulte Protocolo de Controle de Transmissões.

---

**V****violação**

Um ato que ignora ou desrespeita a política corporativa.

**visualização do sistema**

Uma representação visual dos hosts primários e gerenciados que compõem um sistema.

# Índice Remissivo

## A

- ações 30
- ações em um crime 29
- administrador da rede ix
- ajuda 12
- ajuda online 12
- ajustando falsos positivos 65
- Ajustando falsos positivos 81
- ameaça 13
- aplicativo 13
- área de janela correções do Windows 137, 152
- área de janela interface de rede 137, 152
- Área de janela Pacotes 137, 152
- Área de janela Políticas de risco 137, 152
- Área de janela Produtos 137, 152
- área de janela propriedades 137, 152
- Área de janela Serviços 137, 152
- Área de janela Vulnerabilidade 137, 152
- assistente de regra de detecção de anomalia 122
- assistente de regras customizadas 7, 17
- ativar regras 124
- atividade de log 9, 12, 13, 19, 22, 51, 64, 65, 85, 86, 87, 89, 103, 104, 106, 107, 108, 111, 117
  - critérios de procura 92
  - visão geral 51
- atividade de rede 9, 12, 13, 14, 19, 22, 71, 74, 75, 85, 86, 87, 89, 92, 102, 103, 104, 106, 107, 108, 111, 117
- ativos 5, 12, 13
- atualizar dados 9
- atualizar detalhes do usuário 11

## B

- barra de ferramenta de atividade de log 53
- barra de ferramenta de detalhes do evento 63
- Barra de ferramenta de detalhes do fluxo 81
- barra de ferramentas 51
- Barra de ferramentas da guia Atividade de rede 71
- barra de ferramentas da página regras 129
- barra de ferramentas de atividade de rede 72
- barra de status 54, 160
- Barra de status 74
- blocos de construção 119
  - editando 128

## C

- caixa de lista de exibição 77
- Caixa de lista de exibição 58
- cancelar uma procura 106

- centro de informações de ameaça da internet 18
- certificado de segurança 3
- chave de licença 3
- classificar resultados em tabelas 8
- coletor de QFlow 74
- coluna de dados do PCAP 66, 68
- compartilhar relatórios 169
- configurando atividade de log 20
- configurando atividade de rede 20
- configurando conexões 20
- configurando gráficos 87
- configurando itens do painel 20
- configurar e gerenciar redes, plug-ins e componentes 6
- configurar e gerenciar sistemas 6
- configurar e gerenciar usuários 6
- configurar tamanho da página 13
- conformidade 13
- Contêiner do gráfico 172
- conteúdo de ajuda 12
- controles 7
- copiar procura salva 108, 148
- copiar um item para um grupo 127
- copiar uma regra 125
- criando grupos de procura 107
- criando regras customizadas 121
- criando um novo grupo de procura 108
- criar novo grupo de procura 147
- criar relatórios 6
- criar um grupo de regras 126
- critérios de filtro de fluxo 73
- critérios de procura
  - excluindo 102
  - guia atividade de log 102
  - salva disponível 102
  - salvando 92
- critérios de procura salvos 14
- customizar painéis 14

## D

- dados de Captura de Pacotes (PCAP) 66
- dados de configuração 6
- dados do evento não analisado 57
- dados do PCAP 66, 67
- dados dos eventos brutos 57
- desativar regras 124
- descrição do evento 61
- designar itens para um grupo 127
- desproteger ofensas 32
- detalhes da vulnerabilidade 150
- detalhes de evento único 61
- detalhes do evento 63
- detalhes do fluxo 75, 79
- dispositivo 6
- distribuir relatórios 6
- Duplicar um relatório 169

## E

- editar ativo 141
- editar blocos de construção 128
- editar grupo de procura 147
- editar um grupo 127
- Editar um grupo 171
- editar um grupo de procura 108
- endereço IP 9, 138
- endereços IP de destino 25
- endereços IP de origem 25
- especificar número de objetos de dados a serem visualizados 20
- especificar tipo de gráfico 20
- eventos 16, 63, 87, 89
- eventos normalizados 56
- exceção de segurança 3
- exclui a opção 32
- excluindo ativos 149
- excluindo uma procura 106
- excluir painel 22
- excluir perfil de ativo 148
- excluir uma regra 125
- executando uma subprocura 103
- executar dados 9
- exibir em uma nova janela 21
- exibir itens 17
- exportando ativos 149
- exportando eventos 68
- Exportando fluxos 82
- exportar ofensas 33
- exportar para CSV 82
- exportar para XML 82
- exportar perfil de ativo 148

## F

- fazer download do arquivo PCAP 68
- fazer o download do arquivo de dados do PCAP 67
- fechando ofensas 31
- filtro rápido 53, 89
- fluxo de eventos 55
- fluxos 16, 71, 74, 87, 89
- fluxos normalizados 75
- funções 119
- funções da barra de ferramentas 35
- funções da barra de ferramentas de detalhes do evento 63

## G

- gerar um relatório manualmente 168
- Gerenciador de Vulnerabilidade QRadar 137
- gerenciamento de crimes 25
- gerenciamento de gráfico 85
- gerenciamento de painel 13
- gerenciamento de regras 117, 124
- gerenciamento do grupo de regras 126
- gerenciando grupos de procura 107



- Gerenciar grupos 148
- gerenciar grupos de procura 101
- gerenciar rede 138
- gerenciar relatórios 6, 161
- gerenciar resultados da procura 106
- glossário 189
- gráfico de série temporal 86
- grupo
  - copiando um item 127
  - designando itens 127
  - editando 127
  - excluindo 128
  - excluindo um item 128
  - removendo 109
- grupo de procura
  - criando 108
  - editando 108
- grupo de procura de crimes 108
- grupo de procura de eventos 107, 108
- grupo de procura de fluxo 107, 108
- grupo de regras
  - criando 126
  - visualização 126
- grupos de fluxo 79
- grupos de procura
  - gerenciando 107
  - visualização 107
- grupos de procura de ativos 146
- Guia Administração 6, 26
- guia atividade de log 5, 8, 51, 54, 55, 56, 57, 58, 63, 66, 68, 89, 104
- guia atividade de rede 5, 8, 71, 77, 89, 104
- Guia Atividade de rede 73, 74, 75, 81, 82
- guia ativo 137, 138, 139, 146
- guia ativos 141, 146, 149
- Guia Ativos 5, 138, 140, 147, 148, 149
- guia crime 30, 35
- Guia crime 98, 100, 101
- guia crimes 8, 25, 30, 31, 32, 33, 35, 38
- Guia Crimes 5, 101
- guia minhas ofensas 94
- guia padrão 4
- guia painel 4, 7, 13, 14, 18, 19, 21, 22
- Guia Painel 4, 15, 16
- guia relatório 161
- guia relatórios 8
- Guia Relatórios 6
- guia riscos 16
- guia todas as ofensas 94
- guias 4
- guias da interface com o usuário 4, 7

## H

- hosts 5

## I

- IBM Security QRadar Risk Manager 6
- ícone Remover 148
- ID 138
- identificação de painel 14
- imagem
  - relatórios
    - marcas 170

- imagem (*continuação*)
  - upload 170
- importar ativos 149
- importar perfil de ativo 148
- imprimir perfil de ativo 138
- incluindo itens de eventos 22
- incluindo itens de procura de fluxo 22
- incluir ativo 138, 141
- incluir filtro 72, 103
- incluir item 14
- incluir itens 22
- incluir nota 30
- incluir um item do painel 13
- informações de login 4
- informações de login padrão 4
- informações do filtro de eventos 139
- informações do usuário 11
- interface com o usuário 4
- introdução ix
- investigando eventos 15
- investigar 71
- investigar a atividade de log 51
- investigar atividade de rede 71
- investigar ativo 138
- investigar fluxos 5
- investigar o evento 25
- investigar o fluxo 25
- investigar ofensas 5
- investigar os logs de eventos 5
- item de painel customizado 14
- item de painel notificação do sistema 17
- item de painel resumo do sistema 16
- item do painel 22
- Itens de crime 14
- itens de painel de crime 14
- itens do painel atividade de log 15
- itens procura de conexão 16

## J

- janela grupos de procura 107

## L

- Layout de relatório 160
- legendas do gráfico 87
- lista de eventos 61
- lista de fluxos em vários modos 79

## M

- manter a regra customizada 117
- manter regras customizadas 117
- mapear evento 64
- marcar ofensa para acompanhamento 35
- mensagem de notificação 17
- menu ativado pelo botão direito 54, 73
- menu de mensagens 7
- menu de navegação 26
- modificar mapeamento de evento 64
- modo de documento
  - Navegador da web do Internet Explorer 4
- modo de fluxo 75

- modo do navegador
  - Navegador da web do Internet Explorer 4
- monitoramento de crimes 29
- monitorando a atividade de rede 74
- monitorando eventos 15
- monitorar 71
- monitorar ofensas 27, 28
- monitorar rede 71
- mostrar painel 14, 18, 21, 22

## N

- Navegador da web
  - versões suportadas 3
- navegar pelo QRadar SIEM 3
- nível de ameaça atual 18
- nível de ameaça da internet 18
- nome de usuário 4
- nome do ativo 138
- nomes de usuários 10
- notificação do sistema 22
- notificação por email 34
- notificações do sistema 7
- nova procura 147
- novo painel 18
- novos recursos
  - visão geral do guia do usuário versão 7.2.2 1
- número de resultados da procura 74

## O

- o que há de novo
  - visão geral do guia do usuário versão 7.2.2 1
- objetos do gráfico 87
- ocultar ofensa 30
- ofensa 25, 63
- ofensas 13, 25, 26, 29, 32, 89, 107, 108, 117
  - designando a usuários 33
- ofensas atualizadas 16
- ofensas de grupo por IP de origem 28
- ofensas ocultas 30
- ofensas por categoria 27
- ofensas por IP de destino 28
- ofensas por rede 29
- opções de eventos agrupados 58
- opções de menu ativado pelo botão direito 139
- organizar os itens do painel 13
- origem de log 57

## P

- página de detalhes do evento 61
- página de IP de origem 98
- página de procura de ativo 144
- Página Minhas ofensas 27
- página perfil de ativo 150, 152, 153, 154, 155, 156
- página perfis de ativo 138
- Página por IP de destino 100
- Página Todos os crimes 27
- painel 22

- painel customizado 13, 16, 18
- painel do Risk Manager 16
- painel gerenciador de vulnerabilidade 17
- parâmetros da área de janela correções do Windows 156
- Parâmetros da área de janela Pacotes 155
- parâmetros da área de janela políticas de risco 156
- Parâmetros da área de janela Produtos 156
- Parâmetros da área de janela Propriedades 156
- Parâmetros da área de janela Resumo da interface de rede 153
- parâmetros da área de janela resumo de ativo 152
- parâmetros da área de janela serviços 155
- parâmetros da área de janela serviços do Windows 155
- Parâmetros da área de janela Vulnerabilidade 154
- parâmetros da página perfil de ativo 137, 152
- parâmetros de crime 38
- parâmetros de eventos agrupados 58
- parâmetros de regra 129
- pausar dados 9
- perfil do ativo 140, 141
- perfis de ativos 137, 146, 149
- Perfis de ativos 147, 148
- permissão de crime 25
- permissão de regra 117
- permissão do nível de dispositivo 25
- permissões
  - propriedades customizadas 111
- pontuação do CVSS agregado 138
- Por página Rede 101
- positivo falso 65, 81
- positivos falsos 137
- principais ofensas 181
- Processador de evento 74
- processadores de evento 74
- procura 147
  - copiando para um grupo 108
- procurando 89
- procurando crimes 25, 94, 98, 100, 101
- procurando Perfis de ativos 144
- procurar por ativo 138
- procuras de crime 94
- procuras de dados 89
- procuras de evento e de fluxo 89
- procuras de fluxo 14
- propriedade
  - copiando customizado 116
  - modificando customizada 115
- propriedade customizada 116
- propriedade de cálculo 113
- propriedade regex 112

- propriedades de fluxo e de evento customizadas 111
- protegendo ofensas 32

## Q

- QID 64

## R

- rede 13, 29
- redimensionar colunas 12
- Registros do Overflow 74
- regra
  - copiando 125
  - editar 125
  - respostas 119
- regra comum 118
- regra de crime 118
- regra de detecção de anomalias 122
- regra de evento 118
- regra de fluxo 118
- regras 117, 119
  - ativando 124
  - desativando 124
  - visualização 120
- regras customizadas 117
- regras de detecção de anomalias 117
- relatório
  - editando 167
- relatórios 12, 13
  - visualização 168
- relatórios customizados 163
- Relatórios gerados mais recentemente 16
- remover grupo 109, 148
- remover item do painel 21
- remover procura salva 148
- remover procura salva de um grupo 109
- remover um item do painel 21
- renomear painel 21
- resposta de regra 130
- resultados da procura
  - cancelar 106
  - excluindo 106
  - gerenciando 104
  - salvando 104
  - visualizando gerenciados 105
- resultados do processador de evento 54
- resumo de atividade nas últimas 24 horas 16
- resumo de crime 34
- retenção de crime 32

## S

- salvando critérios de procura 101
- salvando os critérios de procura de evento e de fluxo 55
- salvando resultados da procura 104
- salvar critérios 146

- Salvar Critérios 101
- salvar critérios de procura de ativo 146
- scanners de terceiros 137
- segurança 13
- senha 4
- serviços 138
- servidores 5
- Sinalizador 17
- sintaxe de filtro rápido 72
- sistema 13

## T

- tabelas 13
- tempo do console 11
- tempo do sistema 11
- tempo real 55
- tempo real (fluxo) 9
- termos chave 25
- testes 119
- tipo de propriedade calculada 111
- tipo de propriedade regex 111
- tipos de diagrama 162
- tipos de gráficos 160
- tipos de propriedade 111

## U

- último minuto (atualização automática) 9

## V

- vários painéis 13
- visão geral de gráficos 85
- visualização de dados do PCAP 67
- visualização de eventos agrupados 58
- visualização do grupo de regra 126
- visualizando eventos de fluxo 55
- visualizando fluxos agrupados 77
- visualizando fluxos de fluxo 75
- visualizando gerenciar resultados da procura 105
- visualizando grupos de procura 107, 146
- visualizando mensagens 7
- visualizando ofensas associadas a eventos 63
- visualizar ativos 138
- visualizar notificações do sistema 22
- visualizar perfil de ativo 140
- visualizar regras customizadas 117
- vulnerabilidades 137
- Vulnerabilidades 138
- vulnerabilidades de ativo 150