IBM Security QRadar Network Anomaly Detection
Versão 7.2.1

Guia de Usuário

S517-1606-00

Nota

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 181.

Índice

Sobre este guia ix

Capítulo 1. O que há de novo para os usuários no QRadar Network Anomaly DetectionV7.2.2 1

Capítulo 2. Sobre o QRadar Network Anomaly Detection 3
Navegadores da web suportados 3
Ativando o modo de documento e o modo de navegador no Internet Explorer 4
Acesso ao IBM Security QRadar 4
Guias da interface com o usuário 4
Guia Painel 4
Guia ofensas 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
Visualizando mensagens 7
Classificando resultados 8
Atualizando e pausando a interface com o usuário 9
Investigando endereços IP 9
Investigar nomes de usuário 10
Tempo do sistema 11
Atualizando preferências do usuário 11
Acessar a ajuda online 12
Redimensionar colunas 12
Configurar o tamanho da página 12

Capítulo 3. Gerenciamento de painel 13
Painéis padrão 13
Painéis customizados 14
Customização do painel 14
Procura de fluxo 15
Ofensas 15
Atividade de log 16
Relatórios mais recentes 16
Resumo do sistema 17
Gerenciador de risco 17
Itens de gerenciamento de vulnerabilidade 17
Notificação do sistema 18
Centro de informações de ameaças da Internet 19
Criando um painel customizado 19
Usando o painel para investigar a atividade de log ou de rede 20
Configurando gráficos 20
Removendo itens do painel 21
Removendo um item do painel 22
Renomeando um painel 22
Excluindo um painel 22
Gerenciando notificações do sistema 23
Incluindo itens de painel baseados na procura à lista Incluir Itens 23

Capítulo 4. Gerenciamento de ofensa 25
Visão geral da ofensa 25

Considerações de permissão de ofensa . . . 25
Termos chave . . . 25
Retenção de ofensa . . . 26
Monitoramento de ofensa . . . 26
Monitorando as páginas Todas as ofensas ou Minhas ofensas . . . 27
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 ofensa . . . 29
Incluindo notas . . . 30
Ocultando ofensas . . . 30
Mostrando ofensas ocultas . . . 30
Fechando ofensas . . . 31
Protegendo ofensas . . . 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 Ofensa . . . 36
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 do 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 positivos falsos . . . 65
Gerenciando dados de PCAP . . . 66
Exibindo a coluna de dados do PCAP . . . 66
Visualizando informações do PCAP . . . 67
Fazendo download do arquivo do PCAP para seu sistema de área de trabalho . . . 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 do filtro rápido . . . 72
Opções do menu ativado pelo botão direito . . . 73
Barra de status . . . 74
Registros de estouro . . . 74
Monitoramento da atividade de rede . . . 74
Visualizando fluxos de fluxo . . . 74
Visualizando fluxos normalizados . . . 75
Visualizando fluxos agrupados . . . 77
Detalhes do fluxo . . . 79
Barra de ferramentas Detalhes do fluxo . . . 81
Ajustando positivos falsos . . . 81
Exportando fluxos . . . 82

Capítulo 7. Gerenciamento de gráfico 85
Gerenciamento de gráfico 85
Visão geral do gráfico de série 86
Legendas do gráfico 87
Configurando gráficos 87

Capítulo 8. Procuras de dados 89
Procuras de evento e de fluxo 89
Procurando itens que correspondam com seus critérios 89
Salvando critérios de procura 92
Procuras da ofensa 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 **Ofensas** 101
Excluindo critérios de procura 102
Usando uma subprocura para refinar resultados da procura 103
Gerenciando resultados da procura 104
Cancelando uma procura 104
Excluindo uma procura 105
Gerenciando grupos de procura 105
Visualizando grupos de procura 105
Criando um novo grupo de procura 106
Editando um grupo de procura 106
Copiando uma procura salva em outro grupo 107
Removendo um grupo ou uma procura salva de um grupo 107

Capítulo 9. Propriedades de fluxo e evento customizado. 109
Permissões necessárias 109
Tipos de propriedades customizadas 109
Criando uma propriedade customizada baseada em regex 110
Criando uma propriedade customizada baseada em cálculo 111
Modificando uma propriedade customizada 113
Copiando uma propriedade customizada 114
Excluindo uma propriedade customizada 114

Capítulo 10. Gerenciamento de regra 115
Considerações sobre permissão de regra 115
Visão geral de regras 115
Categorias de regra 115
Tipos de regra 116
Condições da regra 116
Respostas da regra 117
Visualizando regras 118
Criando uma regra customizada 119
Criando uma regra de detecção de anomalias 120
Tarefas de gerenciamento de regra 122
Ativando e desativando regras 122
Editando uma regra 122
Copiando uma regra 123
Excluindo uma regra 123
Gerenciamento de grupo de regra 124
Visualizando um grupo de regra 124
Criando um grupo 124
Designando um item a um grupo 124
Editando um grupo 125
Copiando um item para outro grupo 125
Excluindo um item de um grupo 125
Excluindo um grupo 126

Editando blocos de construção 126
Parâmetros de página de regra 127
Barra de ferramentas da página de regras 127
Parâmetros da página de Resposta de Regra 128

Capítulo 11. Parâmetros da página de perfil de ativos 135
Perfis de ativos 135
Sobre as vulnerabilidades 135
Visão geral da guia Ativos 136
Lista da guia Ativo 136
Opções do menu ativado pelo botão direito 137
Visualizando um perfil de ativos 138
Incluindo ou editando um perfil ativo 139
Procurando perfis de ativos 142
Salvando critério de procura de ativo 144
Grupos de procura de ativos 144
Visualizando grupos de procura 144
Criando um novo grupo de procura 145
Editando um grupo de procura 145
Copiando uma procura salva em outro grupo 146
Removendo um grupo ou uma procura salva de um grupo 146
Tarefas de gerenciamento de perfil do ativo 146
Excluindo ativos 146
Importando perfis de ativos 147
Exportando ativos 147
Pesquisar vulnerabilidades de ativos 148
Parâmetros da página de perfil de ativos 150
Área de janela de Resumo de Ativo 150
Área de janela de resumo de interface de rede 151
Área de janela de vulnerabilidade 152
Área de janela de serviços 152
Área de janela do serviço do Windows 153
Área de janela de pacotes 153
Área de janela de Correções do Windows 153
Área de janela de propriedades 154
Área de janela de políticas de risco 154
Área de janela de produtos 154

Capítulo 12. Gerenciamento de relatório 157
Barra de status 158
Layout de relatório 158
Tipos de gráfico 158
Barra de ferramentas da guia Relatório 159
Tipos de diagramas 160
Criando relatórios customizados 161
Editando um relatório 165
Visualizando relatórios gerados 165
Excluindo conteúdo gerado 166
Gerando um relatório manualmente 166
Duplicando um relatório 167
Compartilhando um relatório 167
Registrando relatórios 168
Grupos de relatórios 168
Criando um grupo de relatórios 169
Editando um grupo 169
Designar um relatório a um grupo 170
Copiando um relatório para outro grupo 170
Removendo um relatório 170
Contêiner do gráfico 170
Parâmetros do contêiner do gráfico Vulnerabilidades do Ativo 171

Parâmetros do contêiner do gráfico Eventos/logs 172
Parâmetros do contêiner do gráfico Fluxos 175
Parâmetros de contêiner do gráfico de IPs de Principais Origens 178
Parâmetros de contêiner do gráfico de Principais Ofensas 179
Parâmetros do contêiner do gráfico de IP de Principais Destinos 180

Avisos 181
Marcas Registradas 183
Considerações de política de privacidade 183

Glossário 185
A 185
B 185
C 185
D 186
E 186
F 186
G 186
H 187
I. 187
L 187
M 187
N 188
O 188
P 189
R 189
S 190
T 190
V 190

Índice Remissivo 191

Sobre este guia

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

Público desejado

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

Documentação técnica

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

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte o Suporte e download de 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 por meio da prevenção, detecção e resposta ao acesso incorreto 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 mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. Os sistemas, produtos e serviços IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que, necessariamente, envolverá procedimentos operacionais adicionais e poderá precisar de outros sistemas, produtos ou serviços para se tornar mais efetiva. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU QUE DEIXARÃO SUA EMPRESA ESTEJA IMUNE DE CONDUTAS MALICIOSAS OU ILEGAIS DE TERCEIROS.

Capítulo 1. O que há de novo para os usuários no QRadar Network Anomaly DetectionV7.2.2

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

Os usuários podem configurar sua preferência de idioma

O QRadar está disponível nos seguintes idiomas: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol e português (Brasil). Os usuários podem selecionar seu idioma preferencial usando a escolha de configuração de **código de idioma** na lista **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 visualizar 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 Network Anomaly Detection

O IBM Security QRadar Network Anomaly Detection é uma plataforma de gerenciamento de segurança de rede que fornece reconhecimento situacional e suporte de conformidade por meio da combinação de conhecimento de rede baseado em fluxo, correlação de eventos de segurança e avaliação de vulnerabilidade baseada em ativos.

Chave de licença padrão

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

Exceções e certificados de segurança

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

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

Navegue para o aplicativo baseado na web

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

Navegadores da web suportados

Acesse o console do IBM Security QRadar a partir de um navegador da web padrão.

Quando você acessa o sistema, é exibido um prompt pedindo um nome de usuário e uma senha. O nome do usuário e a senha devem ser configurados antecipadamente pelo administrador.

Tabela 1. Navegadores da web suportados

Navegador da web	Versão suportada
Mozilla Firefox	• 10.0 ESR • 17.0 ESR O Mozilla Firefox tem um ciclo de liberação curto. Nós não podemos nos comprometer em testar as versões mais recentes do navegador Mozilla Firefox. No entanto, nós assumimos integralmente o compromisso de investigar quaisquer problemas que sejam relatados.
Microsoft Internet Explorer, com Visualização de Compatibilidade Ativada	• 8.0 • 9.0

Tabela 1. Navegadores da web suportados (continuação)

Navegador da web	Versão suportada
Google Chrome	• Versão mais recente Nós assumimos integralmente o compromisso de investigar quaisquer problemas que sejam relatados.

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

É necessário ativar a visualização de compatibilidade se você usar o Microsoft Internet Explorer para acessar o IBM Security QRadar.

Procedimento

1. Em seu navegador Microsoft Internet Explorer, pressione F12 para abrir a janela Ferramentas do Desenvolvedor.
2. Para configurar o modo de navegador, na caixa de listagem **Modo do Navegador**, selecione a versão de seu navegador da web.
3. Para configurar o modo de documento, na caixa de listagem **Modo de Documento**, **selecione Padrões do Internet Explorer 7.0**.

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 IBM Security QRadar.

Tabela 2. Informações de login padrão do QRadar

Informações de login	Padrão
URL	https://<Endereço de IP>, em que <Endereço de IP> é o endereço IP do console 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 designada para o QRadar durante o processo de instalação.
Chave da 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 quando você efetua login.

Você pode facilmente navegar nas guias para localizar os dados ou a funcionalidade que você necessita.

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 nos quais é possível exibir visualizações de segurança de rede, atividade ou dados que o QRadar coleta. Cinco painéis padrão estão disponíveis. Cada painel contém os itens que fornecem informações detalhadas e de resumo sobre ofensas que ocorrem em sua rede. É possível também criar um painel customizado para

permitir que se concentre nas suas responsabilidades de operação de rede ou segurança. Para obter mais informações sobre como usar a guia Painel, consulte Gerenciamento de painel.

Guia ofensas

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

Na guia **Ofensas**, você pode investigar uma ofensa para determinar a causa raiz de um problema. Você também pode resolver o problema.

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

Guia Atividade de log

A guia **Atividade de log** permitirá investigar os logs de evento sendo enviados para o QRadar em tempo real, executar procuras poderosas e visualizar a atividade de log usando gráficos de série temporal configuráveis.

A guia **Atividade de log** permitirá que seja executada uma investigação detalhada dos 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 você determine como o tráfego é comunicado, o que é comunicado (se a opção capturar conteúdo estiver ativada), e quem está comunicando. Os dados de fluxo também incluem detalhes como protocolos, valores ASN, valores IFIndex e prioridades.

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

Guia ativos

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

Descoberta automática é baseada em dados de fluxo passivos e dados 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 finalidades 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. Nessa situação, o QRadar poderá determinar se o ativo estiver

vulnerável a esse ataque correlacionando o ataque ao perfil do 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 ativo.

Guia Relatórios

A guia **Relatórios** permitirá que você crie, distribua e gerencie relatórios para quaisquer dados dentro de QRadar.

O recurso Relatórios permitirá que você crie relatórios customizados para uso operacional e executivo. Para criar um relatório, você pode combinar as informações (como, segurança ou rede) em um único relatório. Você também pode usar modelos de relatório pré-instalados incluídos com QRadar.

A guia **Relatórios** também permitirá que você crie logotipos customizados para o seu relatório. 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

IBM Security QRadar Risk Manager é um dispositivo instalado separadamente para as configurações do dispositivo de monitoramento, simulando alterações para seu ambiente de rede e priorizando os riscos e a vulnerabilidades em sua rede.

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 IPSs, feeds de vulnerabilidade e fontes de segurança do fornecedor. Esses dados são usados para identificar os riscos de segurança, política e conformidade dentro da infraestrutura de segurança da rede e a probabilidade desses riscos que estão sendo explorados.

Nota: Para obter mais informações sobre 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 usuários, sistemas, redes, plug-ins e componentes. Os usuários com privilégios administrativos 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 no QRadar

Ferramenta de administração	Descrição
Configuração do Sistema	Configura o sistema e as opções de gerenciamento do usuário.
Origens de Dados	Configura fontes de log, fontes de fluxo e opções de vulnerabilidade.
Configuração de Redes e Serviços Remotos	Configurar redes remotas e grupos de serviços.
Editor de Implementação	Gerencie os componentes individuais da sua 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 para o host gerenciado em sua implementação.

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 seleção **Notificação** em **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. Ações que você executa na janela **Mensagens** são propagadas para a guia **Painel** e a janela pop-up. Por exemplo, se você fechar uma notificação do sistema na janela **Mensagens**, a notificação do sistema será removida de todas as exibições de notificação 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 mensagens

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

Tabela 4. Funções disponíveis na janela mensagens (continuação)

Função	Descrição
Descartar todos	Clique em **Descartar todos** para fechar todas as notificações do sistema de seu sistema. Se você filtrou a lista de notificações do sistema usando o **Funcionamento**, **Erros**, **Avisos** ou **Ícones de informações**, o texto no ícone **Visualizar tudo** será alterado para uma das opções a seguir: • **Descartar todos os erros** • **Descartar todo o funcionamento** • **Descartar todos os avisos** • **Descartar todos os avisos** • **Descartar todas as informações**
Visualizar tudo	Clique em **Visualizar tudo** para visualizar os eventos de notificação do sistema na guia **Atividade de Log**. Se você filtrou a lista de notificações do sistema usando o **Funcionamento**, **Erros**, **Avisos** ou **Ícones de informações**, o texto no ícone **Visualizar tudo** será alterado para uma das opções a seguir: • **Visualizar todos os erros** • **Visualizar todo o funcionamento** • **Visualizar todos os avisos** • **Visualizar todas as informações**
Descartar	Clique no ícone **Descartar** ao lado de uma notificação do sistema para fechar a notificação do sistema de seu sistema.

Procedimento

1. Efetuar login para QRadar.
2. No canto superior direito da interface com o usuário, clique em **Mensagens**.
3. Na janela **Mensagens**, visualizar 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 as notificações do sistema, escolha uma das opções seguir:

Opção	Descrição
Descartar todos	Clique para fechar todas as notificações do sistema.
Descartar	Clique no ícone **Descartar** 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 manualmente, pausar e executar os dados exibidos nas guias.

Sobre Esta Tarefa

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

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

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

Ao visualizar a guia **Atividade de log** ou **Atividade de rede** no modo de 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**. Ao clicar em qualquer lugar dentro de um item do painel, a guia pausará automaticamente . 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 **Atualizar**, 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 ele estiver pausado.

Investigando endereços IP

Você pode usar diversos métodos para investigar as informações sobre os 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 > **Visualizar por rede**	Exibe as redes associadas ao endereço IP selecionado.
Navegar > **Visualizar resumo de origem**	Exibe as ofensas associadas ao endereço IP de origem selecionado.
Navegar > **Visualizar resumo de destino**	Exibe as ofensas associadas ao endereço IP de destino selecionado.
Informações > **Consulta DNS**	Procura por entradas DNS baseadas no endereço IP.
Informações > **Consulta do WHOIS**	Procura pelo proprietário registrado de um endereço IP remoto. O servidor de WHOIS padrão é whois.arin.net.

Tabela 5. Informações de endereços IP (continuação)

Opção	Descrição
Informações > **Varredura de porta**	Executa uma varredura do Mapeador de Rede (NMAP) do endereço IP selecionado. Esta opção estará disponível apenas se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do fornecedor.
Informações > **Perfil de ativo**	Exibir informação do perfil de ativos. Essa opção é exibida se o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*. Essa opção de menu estará disponível se o QRadar adquirir os dados de perfil ativamente através de uma varredura ou passivamente através das fontes de fluxo. Para obter informações, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.
Informações > **Procurar eventos**	Procura por eventos associados a esse endereço IP.
Informações > **Procurar fluxos**	Procura por fluxos associados a esse endereço IP.
Informações > **Procurar conexões**	Procura por conexões associadas a esse endereço IP. Essa opção será exibida somente se você comprou oIBM Security QRadar Risk Manager e conectou o QRadar e o dispositivo do IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
Informações > **Consulta da porta do comutador**	Determina a porta do comutador em um dispositivo Cisco IOS para esse endereço IP. Esta opção aplica-se somente a comutadores descobertos usando a opção **Descobrir dispositivos** na guia **Risco**.
Informações > **Visualizar topologia**	Exibe a guia **Riscos** 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 varrer uma varredura do IBM Security QRadar Vulnerability Manager nesse endereço IP. Essa opção será exibida apenas quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Para obter informações sobre a guia Riscos ou o IBM Security QRadar Risk Manager, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

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 do mouse 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 para acessar mais opções de menu. Use essas opções para visualizar mais informações sobre o nome de usuário ou endereço IP.

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

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

Tabela 6. Opções de 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 nas 24 horas anteriores.
Visualizar eventos	Exibe os eventos que são associados ao nome de usuário selecionado. Para obter mais informações sobre a janela Lista de eventos, consulte Monitoramento da atividade de log.

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

Tempo do sistema

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

O tempo do console sincroniza os sistemas QRadar dentro da 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 de área de trabalho.

Quando você aplica filtros e procuras baseadas em tempo nas guias **Atividade do log** e **Atividade de rede**, você deve usar o tempo do sistema do console para especificar um intervalo de tempo.

Quando você aplica filtros e procuras baseadas em tempo na guia **Atividade do log**, você deve usar o tempo do sistema do console para especificar um intervalo de tempo.

Atualizando preferências do usuário

é possível configurar suas preferências de usuário, como código de idioma, na interface principal com o usuário doQRadar.

Procedimento

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

Opção	Descrição
Nome de usuário	Exibe seu nome de usuário. Este campo não pode ser editado.
Senha	A senha deve atender aos seguintes critérios: • Mínimo de 6 caracteres • Máximo de 255 caracteres • Conter pelo menos um caractere especial • Contém um caractere maiúsculo
Senha (Confirmar)	Confirmação de senha,

Opção	Descrição
Endereço de email	O endereço de email deve atender aos seguintes requisitos: • Mínimo de 10 caracteres • Máximo de 255 caracteres
Código de Idioma	O QRadar está disponível nos seguintes idiomas: inglês, chinês simplificado, chinês tradicional, japonês, coreano, francês, alemão, italiano, espanhol, russo e português (Brasil). Se um código de idioma não estiver listado, a interface com o usuário não será traduzida para o idioma associado. No entanto, outras convenções culturais associadas, como tipo de caractere, ordenação, formato de data e hora e unidade de moeda são suportadas.
Ativar notificações pop-up	Selecione essa caixa de seleção se você deseja ativar as notificações do sistema pop-up a serem exibidas em sua interface com o usuário.

Acessar a ajuda online

É possível acessar a 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

Você pode 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. Você também pode redimensionar colunas dando um clique duplo na linha que separa as colunas para redimensionar automaticamente a coluna à largura do maior campo.

Nota: O redimensionamento de coluna não funciona nos navegadores da web Microsoft Internet Explorer, Versão 7.0 quando as guias estão exibindo os registros no modo de fluxo.

Configurar o 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 ao efetuar 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 os itens de painel sejam organizados em visualizações funcionais, que permitem o foco em áreas específicas de sua rede.

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

É possível customizar seu painel. O conteúdo que é exibido na guia **Painel** é específico ao usuário. As alterações que são feitas dentro de uma sessão afetam somente 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 preocupados com a segurança, atividade de rede, atividade do aplicativo, o monitoramento do sistema e a conformidade.

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

O conteúdo exibido na guia Painel é específico do usuário. É possível customizar seus painéis. As alterações feitas dentro de uma sessão QRadar Network Anomaly Detection afetam somente o seu sistema.

Tabela 7. Painéis padrão

Painel padrão	Itens
Visão geral dos aplicativos	O painel **Visão geral do aplicativo** inclui os itens padrão a seguir: • Tráfego de entrada por país/região (série temporal) • Tráfego de transmissão por país/região (série temporal) • Aplicativos Principais (série temporal) • Entrada de Aplicativos Principais da Internet (série temporal) • Saída de Aplicativos Principais da Internet (série temporal) • DSCP – Precedência (série temporal)
Inteligência de Rede	O painel **Inteligência de rede** inclui os itens padrão a seguir: • Talkers Principais (tempo real) • Tipo/Código de ICMP (série temporal) • Redes Principais por Volume de Tráfego (série temporal) • Negação de Firewall pela Porta DST (série temporal) • Negação de Firewall por IP de DST (série temporal) • Negação de Firewall por IP de SRC (série temporal) • Aplicativos Principais (série temporal) • Utilização de Link (tempo real) • DSCP – Precedência (série temporal)

Tabela 7. Painéis padrão (continuação)

Painel padrão	Itens
Monitoramento do Sistema	O painel **Monitoramento do Sistema** inclui os seguintes itens padrão: • Principais Fontes de Log (Contagem de Eventos) • Utilização de Link (tempo real) • Notificações do Sistema • Distribuição do Processador de Eventos (série temporal) • Taxa de Evento (Eventos por Segundo Unido - Média de 1 Mín.) • Taxa de Fluxo (Fluxos por Segundo - Média de 1 Mín.)
Monitoramento de Ameaça e Segurança	O painel **Monitoramento de ameaça e segurança** inclui os itens padrão a seguir: • IDS Padrão/Todo IPS: Principais Assinaturas de Alarme (série temporal) • Principais Sistemas Atacados (série temporal) • Principais Ataques de Fornecimento de Sistemas (série temporal) • Meus Crimes • Crimes Mais Severos • Crimes Mais Recentes • Eventos de Saída por País/região (em tempo real) • Centro de Informações de Ameaças da Internet • Propensão de Fluxo • Principais Tipos de Categoria • Origens Principais • Principais Destinos do Local

Painéis customizados

É possível customizar seus painéis. O conteúdo que é exibido na guia **Painel** é específico ao usuário. Alterações que são feitas em uma sessão QRadar afetam apenas o seu sistema.

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

- Criar painéis customizados que são relevantes para as suas responsabilidades. O máximo é 255 painéis por usuário; no entanto, problemas de desempenho poderão ocorrer se você criar mais de 10 painéis.
- Adicionar e remover itens do painel a partir de painéis padrão ou customizados.
- Mover e posicionar itens para atender seus requisitos. Ao posicionar os itens, cada item redimensiona automaticamente em proporção para o painel.
- Incluir itens de painel customizados 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 que são representados em seu painel. Cada gráfico do painel exibe os dados atualizados em tempo real. Os gráficos de série temporal no painel são atualizados a cada 5 minutos.

Customização do painel

É possível incluir vários itens do painel aos 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 tiver visualizado anteriormente um painel e retornado para a guia **Painel**, o último painel visualizado será exibido.

Procura de fluxo

É possível exibir um item de painel customizado com base nos critérios de procura salvos a partir da guia **Atividade de rede**.

Os 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 Procura de fluxo, os resultados da procura exibem em tempo real os últimos dados em um gráfico. Os tipos de gráfico suportados são série temporal, tabela, de pizza e de 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 magnificar e verificar por meio de uma linha de tempo para investigar a atividade de rede.

Ofensas

É possível incluir diversos itens relacionados à ofensa em seu painel.

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

A tabela a seguir descreve os itens da Ofensa:

Tabela 8. Itens de ofensa

Itens do painel	Descrição
Crimes Mais Recentes	As cinco ofensas mais recentes 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 para o 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 para o endereço IP.
Meus Crimes	O item **Minhas ofensas** exibe cinco das ofensas mais recentes 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 para o endereço IP.
Origens Principais	O item **Principais origens** exibe as principais origens de ofensa. Cada origem é identificada com uma barra de magnitude para informá-lo sobre a importância da origem. Aponte para o endereço IP para visualizar informações detalhadas para o endereço IP.

Tabela 8. Itens de ofensa (continuação)

Itens do painel	Descrição
Principais Destinos do Local	O item **Principais destinos do local** 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 informações detalhadas do IP.
Categorias	O item **Principais tipos de categorias** exibe as cinco principais categorias que estão associadas ao maior número de ofensas.

Atividade de log

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

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

Tabela 9. Itens de atividade de log

Item do painel	Descrição
Procuras de Eventos	É possível exibir um item de painel customizado baseado em critérios de procura salvos na guia Log de atividades. Itens de procura de eventos são listados no menu **Incluir item** > **Atividade de rede** > **Procuras de evento**. O nome do item de procura de evento corresponde ao nome do critério de procura salvo no qual o item é baseado. O QRadar inclui os critérios de procura salvos padrão que são pré-configurados para exibir itens de procura de evento em seu menu da guia **Painel**. É possível incluir mais itens de painel de procura de evento em sua guia do menu **Painel**. Para obter mais informações, consulte Incluindo itens de painel com base em procuras na lista Incluir itens. Em um item de painel **Atividade de log**, os resultados da procura exibem os últimos dados em tempo real em um gráfico. Os tipos de gráfico suportados são série temporal, tabela, de pizza e de barras. O tipo de gráfico padrão é de barras. Esses gráficos são configuráveis. 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.
Eventos por Gravidade	O item de painel **Eventos por severidade** exibe o número de eventos ativos agrupados por severidade. Este item permitirá ver o número de eventos que são recebidos pelo nível de severidade designado. A severidade indica a quantidade de ameaça que uma origem de ofensa representa em relação a quão preparado está o destino para o ataque. O intervalo de severidade é 0 (baixo) a 10 (alto). Os tipos de gráficos suportados são Tabela, Pizza e Barras.
Principais Fontes de Log	O item de painel **Principais fontes de log** exibe as 5 principais fontes de log que enviaram eventos para o QRadar nos últimos 5 minutos. O número de eventos que são enviados da fonte de log especificada é indicado no gráfico de pizza. Este item permitirá a visualização de potenciais alterações no comportamento, por exemplo, se a fonte de log de um firewall que normalmente não está na lista dos 10 principais agora contribuir para uma grande porcentagem da contagem de mensagens geral, será necessário investigar essa ocorrência. Os tipos de gráficos suportados são Tabela, Pizza e Barras.

Relatórios mais recentes

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

A exibição 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 dentro das últimas 24 horas.

Dentro do item de resumo, você pode 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 ofensas que foram criadas ou modificadas com nova evidência 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 ofensas modificadas nas últimas 24 horas.

Gerenciador de risco

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

Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

Você pode exibir um item do painel customizado baseado em critérios de procura salvos a partir da guia **Riscos**. Os itens de procura de conexão são listados no menu **Incluir Item** > **Genrenciador de Risco** > **Procuras de Conexão**. O nome do item de procura de conexão corresponde ao nome dos critérios de procura salvos no qual o item está baseado.

Os critérios padrão de procura salvos estão disponíveis e pré-configurados para exibir itens de procura de conexão em seu menu da guia **Painel**. Você pode incluir mais itens do painel de procura de conexão em seu menu da guia**Painel**.

Em um item do painel de **procura de conexões**, os resultados da procura exibem em tempo real dados de última hora em um gráfico. Os tipos de gráfico suportados são série temporal, tabela, de pizza e de 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 de Gerenciamento de Vulnerabilidade são exibidos apenas quando IBM Security QRadar Vulnerability Manager é adquirido e licenciado.

Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Você pode exibir um item do painel customizado baseado em critérios de procura salvos da guia **Vulnerabilidades**. Itens de procura são listados no menu **Incluir**

item > **Gerenciamento de vulnerabilidade** > **Procuras de vulnerabilidade**. O nome do item de procura corresponde ao nome dos critérios de procura salva que o item é baseado.

O QRadar inclui os critérios de procura salva padrão que são pré-configurados para exibir itens de procura no seu menu da **guia Painel**. Você pode incluir mais itens do painel de procura em seu menu da guia **Painel**.

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

Notificação do sistema

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

Para notificações mostrarem 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 **Notificação** no Assistente de Regras Customizadas.

Para obter mais informações sobre como configurar notificações de eventos e criar regras de eventos, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

No item de painel **Notificações do sistema**, você pode visualizar as seguintes informações:

- **Sinalizador** - Exibe um símbolo para indicar o nível de gravidade da notificação. Aponte para o símbolo para visualizar mais detalhes sobre o nível de gravidade.
  - Ícone de **Funcionamento**
  - Ícone de **Informações** (?)
  - Ícone de **Erros** (X)
  - Ícone de **Aviso** (!)
- **Criado** – Exibe a quantidade de tempo decorrido desde que a notificação foi criada.
- **Descrição** – Exibe informações sobre a notificação.
- **Descartar ícone (x)** – Irá permitir que você feche uma notificação do sistema.

Você pode apontar o mouse sobre uma notificação para visualizar mais detalhes:

- **IP do host** – Exibe o endereço IP do host do host que originou a notificação.
- **Gravidade** – Exibe o nível de gravidade do incidente que criou esta notificação.
- **Categoria de Nível Baixo** – 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 associada ao incidente que gerou esta notificação.
- **Criado** – Exibe a quantidade de tempo decorrido desde que a notificação foi criada.

Ao incluir o item de painel **Notificações do sistema**, as notificações do sistema também podem exibir 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.

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

Na janela pop-up Notificações do sistema, o número de notificações na fila é realçado. Por exemplo, se (1 – 12) for exibido no cabeçalho, a notificação atual será 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.
- **Fechar ícone (X)** – Fecha essa janela pop-up de notificação.
- **(Detalhes)** - Exibe mais informações sobre essa notificação do sistema.

Centro de informações de ameaças da Internet

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

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 item de painel. 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 website do IBM Internet Security Systems abre em outra janela do navegador e exibe os detalhes completos da recomendação.

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 está 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**, digite 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 baseados em procura fornecem um link para as guias **Atividade de log** ou **Atividade de rede**, permitindo a investigação de atividade de log ou de rede.

Sobre Esta Tarefa

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

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

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

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

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

Tipo de gráfico	Descrição
Barras, Pizza e Tabela	A guia **Atividade de log** ou **Atividade de rede** exibe um gráfico de barras, gráfico de pizza e uma tabela de detalhes do fluxo.
Séries temporais	A guia **Atividade de log** ou **Atividade de rede** exibe os gráficos de acordo com os critérios a seguir: 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. 2. Se o intervalo de tempo for maior do que 1 hora, um gráfico da séries temporais será exibido e você será solicitado a clicar em Atualizar detalhes. 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 a tabela de detalhes do evento ou fluxo serão exibidos.

Configurando gráficos

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

Sobre Esta Tarefa

Tabela 10. Configurando gráficos. Opções de parâmetros.

Opção	Descrição
Value to Graph	Na caixa de listagem, selecione o tipo de objeto que você deseja no gráfico. As opções incluem todos os parâmetros de eventos ou fluxo normalizados e customizados 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: 1. **Gráfico de barras** – exibe dados em um gráfico de barras. Esta opção está disponível somente para eventos ou fluxos agrupados. 2. **Gráfico de pizza** – exibe dados em um gráfico de pizza. Esta opção está disponível somente para eventos ou fluxos agrupados. 3. **Tabela** - Exibe dados em uma tabela. Esta opção está disponível somente para eventos ou fluxos agrupados. 4. **Séries temporais** – exibe um gráfico de linha interativa que representa os registros correspondidos por um intervalo de tempo especificado.
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 seleção para ativar a captura de séries temporais. Ao selecionar essa caixa de seleção, o recurso gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, esta opção está desativada.
Time Range	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar.

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

Os dados são acumulados para que, ao executar uma procura salva de séries temporais, haja um cache de dados do evento ou fluxo disponível para exibir os dados do período de tempo anterior. Os parâmetros acumulados são indicados por um asterisco (*) na caixa de listagem **Valor para Gráfico**. Se você selecionar um valor para gráfico que não esteja 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 contenha o item que você deseja customizar.
3. No cabeçalho do item do painel que você deseja configurar, clique no ícone **Configurações**.
4. Configurar os parâmetros de gráfico.

Removendo itens do painel

Você pode remover itens de um painel e incluí-lo novamente a qualquer momento.

Sobre Esta Tarefa

Ao remover um item do painel, ele 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

É possível remover um item de seu painel e exibi-lo em uma nova janela em seu sistema da área de trabalho.

Sobre Esta Tarefa

Ao desconectar um item do painel, o item do painel original permanecerá na guia **Painel**, enquanto uma janela removida com um item do painel duplicado permanecerá aberto e atualizará durante intervalos planejados. Se você fechar o aplicativo do QRadar, a janela removida permanecerá aberta para monitoramento e continuará a atualizar até você fechar manualmente a janela ou encerrar o sistema de computador.

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 do item de painel, clique no ícone verde para remover o item do painel e abra-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**, digite 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 lista **Mostrar painel** será exibido. O painel que foi excluído 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** esteja 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 na procura à lista Incluir Itens

Você pode incluir itens de painel baseados na procura para seu menu **Incluir itens**.

Antes de Iniciar

Para incluir um item de painel de procura de evento e fluxo para o menu **Incluir item** na guia **Painel**, você deve acessar a guia **Atividade do log** ou **Atividade sa rede** para criar critérios de procura que especifica que os resultados da procura podem ser exibidos na guia **Painel**. O critério de procura também deve especificar que os resultados são agrupados em um parâmetro.

Sobre Esta Tarefa

Este procedimento se aplica a todos os itens de painel baseados em procura, incluindo itens de painel do IBM Security QRadar Risk Manager. Os itens de painel do QRadar Risk Manager serão exibidos apenas quando QRadar Risk Manager for adquirido e licenciado e você estabelecer a conexão entre o Console e o dispositivo do QRadar Risk Manager. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*

Procedimento

1. Escolha:
   - Para incluir um item de painel de procura de fluxo, clique na guia **Atividade da rede**.
   - Para incluir um item do painel de procura de evento, clique na guia **Atividade do Log**.
2. Na caixa de listagem **Procurar**, escolha uma das seguintes opções:
   - Para criar uma procura, selecione **Novo 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 da Coluna, selecione uma coluna e clique no ícone **Incluir Coluna** para mover a coluna para a lista **Agrupar**.

4. Clique em **Filtrar**. Os resultados da procura são exibidos.
5. Clique em **Salvar critérios**. Consulte critérios de procura na guia Ofensa
6. Clique em **OK**.
7. Verifique se o critério de procura salva incluiu com êxito o item de painel de procura de evento ou fluxo à lista **Incluir itens**
   a. Clique na guia **Painel**.
   b. Escolha uma das opções a seguir:
   a. Para verificar um item de procura de evento, selecione **Incluir item** > **Atividade de log** > **Procuras de evento** > **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 como critérios de procura salva.

Capítulo 4. Gerenciamento de ofensa

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 fluxo para determinar os eventos e fluxos exclusivos que causaram a ofensa.

Visão geral da ofensa

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

É possível também procurar por ofensas que são baseadas em vários critérios. Para obter mais informações sobre a procura de ofensas, consulte "Procuras da ofensa" na página 94.

Considerações de permissão de ofensa

Todos os usuários podem visualizar todas as ofensas, independentemente de qual origem de log ou origem de fluxo esteja 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 *Guia de Administração* para seu produto.

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 múltiplos eventos ou fluxos que se originam de uma origem, como um host ou fonte de log. A guia **Ofensas** exibe ofensas, que incluem o tráfego e vulnerabilidades que colaboram e validam a magnitude de uma ofensa. A magnitude de uma ofensa é determinada por vários testes executados na ofensa cada vez que ela for reavaliada. A reavaliação ocorrerá quando os eventos forem incluídos na ofensa e em intervalos planejados.
Endereço IP de origem	Um endereço IP de origem especifica o dispositivo que tentativas 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
Endereço IP de destino	Um endereço IP de destino especifica o dispositivo de rede que um endereço IP de origem tenta acessar.

Retenção de ofensa

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

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

Quando você fecha ofensas, as ofensas fechadas são removidas do banco de dados depois que o período de retenção da ofensa já tiver decorrido. Se mais eventos ocorrerem para uma ofensa, uma nova ofensa será criada. Se você executar uma procura que inclui ofensas encerradas, o item será exibido nos resultados da procura, se ele não tiver sido removido do banco de dados.

Monitoramento de ofensa

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

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

Após começar a navegar nas diversas visualizações, a parte superior da guia exibirá a trilha de navegação da visualização atual. Se desejar retornar a 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 são listadas na tabela a seguir.

Tabela 11. Páginas que podem ser acessadas a partir da guia **Ofensas**

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

Monitorando as páginas Todas as ofensas ou Minhas ofensas

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

Antes de Iniciar

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

Sobre Esta Tarefa

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

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

Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, selecione **Todas as ofensas** ou **Minhas ofensas**.
3. Você pode refinar a lista de ofensas com as opções a seguir:
   - Na caixa de listagem **Visualizar ofensas**, selecione uma opção para filtrar a lista de ofensas 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 Parâmetros da ofensa.
6. Execute quaisquer ações necessárias na ofensa. Consulte as tarefas Gerenciamento de ofensas.

Monitorando ofensas agrupadas por categoria

Você pode monitorar as ofensas na página de detalhes Por categoria, que fornece uma lista de ofensas 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 os grupos de categoria de nível inferior para uma 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 ofensas 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 Parâmetros da ofensa.
7. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de ofensa.

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 gerou ofensas como resultado de um ataque em seu sistema. Todos os endereços IP de origem são listados com a mais alta grandeza primeiro. A lista de ofensas exibe apenas 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 ofensas que use as opções a seguir:
   - Na caixa de listagem **Visualizar ofensas**, selecione uma opção para filtrar a lista de ofensas 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 do local para o endereço IP de origem, clique em **Destinos** na barra de ferramentas da página Origem.
6. Para visualizar uma lista de ofensas 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 Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de ofensa.

Monitorando ofensas agrupadas por IP de destino

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

Sobre Esta Tarefa

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

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por IP de destino**.
3. Você pode refinar a lista de ofensas que use as opções a seguir:

- Na caixa de listagem **Visualizar ofensas**, selecione uma opção para filtrar a lista de ofensas 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 ofensas associadas 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 associado 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 Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de ofensa.

Monitorando ofensas agrupadas por rede

Na página de redes, você pode monitorar as ofensas 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 ofensas 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 Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de ofensa.

Tarefas de gerenciamento de ofensa

Ao monitorar ofensas, será possível executar ações na ofensa.

É possível executar as seguintes ações:

- Incluir notas
- Remover ofensas
- Proteger ofensas
- Exportar dados de ofensa para XML ou CSV
- Designar ofensas para outros usuários
- Enviar notificações por email
- Marcar uma ofensa para acompanhamento

- Ocultar ou fechar uma ofensa de qualquer lista de ofensa

Para executar uma ação em várias ofensas, mantenha a tecla Control pressionada ao selecionar cada ofensa que deseja selecionar. Para visualizar os detalhes da ofensa em uma nova página, mantenha pressionada a tecla Control ao clicar duas vezes em uma ofensa.

Incluindo notas

Você pode incluir notas em qualquer ofensa na guia **Ofensas**. Notas pode incluir informações que você deseja capturar para a ofensa, como um número de bilhete com o Suporte ao Cliente ou informações de gerenciamento de ofensa.

Sobre Esta Tarefa

As notas podem incluir até 2000 caracteres.

Procedimento

1. Clique na guia **Ofensas**.
2. Navegue para a ofensa na qual deseja incluir notas.
3. Dê um clique duplo na ofensa.
4. Na caixa de listagem **Ações**, selecione **Incluir nota**.
5. Digite a nota que você deseja incluir para esta ofensa.
6. Clique em **Incluir nota**.

Resultados

A nota é exibida na área de janela Últimas 5 notas no resumo da ofensa. Um ícone de **Notas** é exibido na coluna do sinalizador da lista de **ofensas**. Se você passar o ponteiro do mouse sobre o indicador de notas na coluna **Sinalizador** da lista de **Ofensas**, a nota para essa ofensa será exibida.

Ocultando ofensas

Para evitar uma ofensa de ser exibida na guia **Ofensas**, você pode ocultar a ofensa.

Sobre Esta Tarefa

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

Procedimento

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

Mostrando ofensas ocultas

As ofensas ocultas não são visíveis na guia **Ofensas**, no entanto, você poderá mostrar as ofensas ocultas se desejar visualizá-las novamente.

Sobre Esta Tarefa

Para mostrar as ofensas ocultas, você deve executar uma procura que inclua as ofensas ocultas. Os resultados da pesquisa incluem todas as ofensas, incluindo as ofensas ocultas e não ocultas. As ofensas são especificadas como ocultas pelo ícone **Oculto** na coluna **Sinalizador**.

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Procurar ofensas ocultas:
   a. Na caixa de listagem **Procurar**, selecione **Nova procura**.
   b. Na lista **Excluir opção** na área de janela Procurar parâmetros, limpe a caixa de seleção **Ofensas Ocultas**.
   c. Clique em **Procurar**.
4. Localize e selecione as ofensas ocultas que você deseja mostrar.
5. Na caixa de listagem **Ações**, selecione **Mostrar**.

Fechando ofensas

Para remover complatamente uma ofensa do sistema, você poderá fechar a ofensa.

Sobre Esta Tarefa

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

Ao fechar as ofensas, será necessário selecionar um motivo para o fechamento da ofensa e você poderá incluir uma observação. O campo **Observações** exibe a observação inserida para o fechamento da ofensa anterior. As Observações não devem exceder 2.000 caracteres. Essa observação é exibida na área de janela Observações dessa ofensa. Se você tiver a permissão Gerenciar Fechamento de Ofensa, será possível incluir novos motivos customizados na caixa de listagem **Razão para fechamento**.

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

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Escolha uma das opções a seguir:
   - Selecione o ofensa que deseja fechar e, em seguida, selecione **Fechar** na caixa de listagem **Ações**.
   - Na caixa de listagem **Ações**, selecione **Fechar listadas**.
4. Na caixa de listagem **Razão para fechamento**, selecione um motivo. O motivo padrão é **non-issue**.

5. Opcional. No campo **Observações**, insira uma observação para fornecer mais informações sobre o fechamento da nota.
6. Clique em **OK**.

Resultados

Após fechar as ofensas, as contagens exibidas na área de janela Por Categoria da guia **Ofensas** poderão levar vários minutos para refletir as ofensas fechadas.

Protegendo ofensas

Você pode evitar ofensas de serem removidas do banco de dados depois que o período de retenção transcorra.

Sobre Esta Tarefa

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 essas ofensas de serem removidas do banco de dados depois que o período de retenção transcorra.

Para obter mais informações sobre o Período de Retenção de Ofensa, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.

CUIDADO:
Quando o modelo de dados SIM for reconfigurada da opção Limpeza rigorosa, 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 ofensa 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 ofensas protegida é indicada por um ícone **Protegido** na coluna **Sinalizador**.

Desprotegendo ofensas

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

Sobre Esta Tarefa

Para listar apenas as ofensas protegidas, você pode executar uma procura que filtra apenas para ofensas protegidas. Se você limpar a caixa de seleção **Protegido** e assegurar que todas as outras opções estejam selecionadas na lista **Excluir opção**

na área de janela dos parâmetros de procura, apenas as ofensas protegidas serão exibidas.

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Opcional. Execute uma procura que exibe apenas as ofensas protegidas.
4. Escolha uma das opções a seguir:
   - Selecione a ofensa 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 Linguagem de Marcação Extensível (XML) ou valores separados por vírgula (CSV).

Sobre Esta Tarefa

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

O arquivo XML ou CSV resultante inclui os parâmetros especificados no área de janela Definição de Coluna de seus parâmetros de procura. O período de tempo necessário para exportar seus dados depende do número de parâmetros especificados.

Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Todos as ofensas**.
3. Selecione a ofensa 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**, você pode designar ofensas aos usuários para investigação.

Sobre Esta Tarefa

Quando uma ofensa for designada a um usuário, a ofensa será exibida na página Minhas ofensas pertencente a este usuário. Você deve ter privilégios apropriados para designar ofensas para os usuários.

Você pode designar ofensas a usuários da guia **Ofensas** ou das páginas Resumo da ofensa. Este procedimento fornece instruções sobre como designar ofensas na guia **Ofensas**.

Nota: A caixa de listagem **Nome do usuário** irá apenas exibir os usuários que possuem privilégios da guia **Ofensas**.

Procedimento

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

Resultados

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

Enviando notificação por email

Você pode enviar um email que contenha um resumo de ofensa 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 de usuário de origem, nome de host ou nome do recurso
- Número total de origens
- Os cinco principais origens por magnitude
- Redes de origem
- Endereço IP de destino
- Nome de usuário de destino, nome de host ou nome do recurso
- Número total de destinos
- Os cinco principais destinos por magnitude
- Redes de destino
- Número total de eventos
- Regras que fez com que a ofensa ou regra de evento disparasse
- A descrição integral da ofensa ou da regra de evento
- ID da ofensa
- As cinco principais categorias

- Horário de início de ofensa ou horário do evento gerado
- As cinco principais anotações
- Link para a interface com o usuário da ofensa
- Contribuindo com as regras do CRE

Procedimento

1. Clique na guia **Ofensas**.
2. Navegue até a ofensa a qual você deseja enviar uma notificação por email.
3. Dê um clique duplo na ofensa.
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 email 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 para o email. O padrão é o ID da Ofensa.
Mensagem de Email	Insira a mensagem padrão que você deseja acompanhar o email de notificação.

6. Clique em **Enviar**.

Marcando um item para acompanhamento

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

Procedimento

1. Clique na guia **Ofensas**.
2. Navegue até a ofensa que você deseja marcar para acompanhamento.
3. Dê um clique duplo na ofensa.
4. Na caixa de listagem **Ações**, selecione **Acompanhar**.

Resultados

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

Funções da barra de ferramentas da guia Ofensa

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 para uma ofensa.

Tabela 12. Funções da barra de ferramentas da guia Ofensa

Função	Descrição
Incluir Nota	Clique em **Incluir nota** para incluir uma nova nota a uma ofensa. Esta opção está disponível somente na área Últimas 5 notas da página Resumo de ofensa
Ações	As opções disponíveis na caixa de listagem **Ações** varia com base na página, tabela ou item (como uma ofensa ou endereço IP de origem). A caixa de listagem **Ações** talvez não exiba exatamente conforme listado a seguir. Na caixa de listagem **Ações**, é possível escolher uma das seguintes ações: • **Acompanhamento** – Selecione esta opção para marcar um item para acompanhamento adicional. Consulte Marcando um item para acompanhamento. • **Ocultar** – Selecione esta opção para ocultar uma ofensa. Para obter mais informações sobre ocultar ofensas, consulte Ocultar ofensas. • **Mostrar** – Selecione esta opção para mostrar todas as ofensas ocultas. • **Proteger ofensas** – Selecione esta opção para proteger uma ofensa. Para obter mais informações sobre como proteger as ofensas, consulte Protegendo ofensas. • **Fechar** - Selecione essa opção para fechar uma ofensa. Para obter mais informações sobre o fechamento de ofensas, consulte Fechamento de ofensas. • **Fechar listados** – Selecione esta opção para fechar a ofensa listada. Para obter mais informações sobre o fechamento de ofensas listadas, consulte Fechamento de ofensas. • **Email** – Selecione esta opção para enviar por email um resumo da ofensa para um ou mais destinatários. Consulte Enviando notificação por email. • **Incluir nota** – Selecione esta opção para incluir notas a um item. Consulte Incluindo notas. • **Designar** – Selecione esta opção para designar uma ofensa a um usuário. Consulte Designando ofensas para usuários. • **Imprimir** – Selecione esta opção para imprimir uma ofensa
Annotations	Clique em **Anotações** para visualizar todas as anotações de uma ofensa. • **Anotação** – Especifica os detalhes da anotação. As anotações são descrições de texto que as regras podem incluir automaticamente nas ofensas como parte da resposta da regra. • **Horário** – Especifica a data e hora que a anotação foi criada. • **Peso** – Especifica o peso da anotação.
Anomalia	Clique em **Anomalia** para exibir os resultados da procura salva que fazem com que a regra de detecção de anomalias gere a ofensa. **Nota:** Este botão será exibido apenas se a ofensa for gerada por uma regra de detecção de anomalias.
Categorias	Clique em **Categorias** para visualizar as informações de categoria da ofensa. Para investigar mais detalhadamente os eventos que são relacionados a uma categoria específica, é possível também clicar com o botão direito em uma categoria e selecionar **Eventos** ou **Fluxos**. Como alternativa, é possível destacar a categoria e clicar no ícone **Eventos** ou **Fluxos** na barra de ferramentas Lista de categorias de eventos.

Tabela 12. Funções da barra de ferramentas da guia Ofensa (continuação)

Função	Descrição
Conexões	Clique em **Conexões** para investigar ainda mais as conexões. **Nota:** Esta opção estará disponível apenas se tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*. Ao clicar no ícone **Conexões**, a página de critérios de procura de conexão será exibida em uma nova página, preenchida previamente com critérios de procura do evento. Você pode customizar os parâmetros de procura, se necessário. Clique em **Procurar** para visualizar as informações de conexão.
Destino	Clique em **Destinos** para visualizar todos os endereços IP de destino local de uma ofensa, endereço IP de origem ou rede. **Nota:** Se os endereços IP de destino forem remotos, uma página separada será aberta fornecendo informações dos endereços IP de destino remotos.
Exibir	A página Resumo de ofensa exibe muitas tabelas de informações que são relacionadas a uma ofensa. Para localizar uma tabela, é possível rolar para a tabela que deseja visualizar ou selecionar a opção da caixa de listagem **Exibir**.
Events	Clique em **Eventos** para visualizar todos os eventos de uma ofensa. Ao clicar em **Eventos**, os resultados da procura de eventos serão exibidos.
Fluxos	Clique em **Fluxos** para investigar os fluxos que estão associados a uma ofensa. Ao clicar em **Fluxos**, os resultados da procura de fluxo serão exibidos.
Fontes de Log	Clique em **Fontes de log** para visualizar todas as fontes de log de uma ofensa.
Redes	Clique em **Redes** para visualizar todas as redes de destino de uma ofensa.
Notes	Clique em **Notas** para visualizar todas as notas de uma ofensa, endereço IP de origem, endereço IP de destino, ou rede. Para obter mais informações sobre as notas, consulte Incluindo notas
Ofensas	Clique em **Ofensas** para visualizar uma lista de ofensas que são associadas a um endereço IP de origem, endereço IP de destino ou rede.
Imprimir	Clique em **Imprimir** para imprimir uma ofensa.
Regras	Clique em **Regras** para visualizar todas as regras que contribuíram para uma ofensa. A regra que criou a ofensa é listada primeiro. Se tiver as 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 ofensa, clique em **Salvar critérios** para salvar seus critérios de procura para uso futuro.
Salvar Layout	Por padrão, a página Por detalhes de categoria é classificada pelo parâmetro Offense Count. Se alterar a ordem de classificação ou classificar por um parâmetro diferente, clique em **Salvar layout** para salvar a exibição atual como sua visualização padrão. A próxima vez que efetuar login na guia **Ofensas**, o layout salvo será exibido.
Procurar	Esta opção está disponível somente na barra de ferramentas da tabela Lista de destinos do local. Clique em **Procurar** para filtrar IPs de destino para um endereço IP de origem. Para filtrar destinos: 1. Clique em **Procurar**. 2. Insira os valores para os parâmetros a seguir: • **Rede de destino** – Na caixa de listagem, selecione a rede que deseja filtrar. • **Magnitude** – Na caixa de listagem, selecione se você deseja filtrar por magnitude Igual a, Menor que ou Maior que o valor configurado. • **Classificar por** – Na caixa de listagem, selecione como deseja classificar os resultados do filtro. 3. Clique em **Procurar**.

Tabela 12. Funções da barra de ferramentas da guia Ofensa (continuação)

Função	Descrição
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 **Mostrar categorias inativas**.
Origens	Clique em **Origens** para visualizar todos os endereços IP de origem, endereço IP de destino, ou rede da ofensa.
Resumo	Se clicar em uma opção na lista de opções **Exibir**, é possível clicar em **Resumo** para retornar para a visualização de resumo detalhada.
Users	Clique em **Usuários** para visualizar todos os usuários que estão associados a uma ofensa.
Visualizar caminho de ataque	Clique em **Visualizar caminho de ataque** para investigar o caminho de ataque de uma ofensa. Ao clicar no ícone **Visualizar caminho de ataque**, a página Topologia atual será exibida em uma nova página. **Nota:** Esta opção estará disponível apenas se tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
Visualizar Topologia	Clique em **Visualizar topologia** para investigar a origem de uma ofensa. Ao clicar no ícone **Visualizar topologia**, a página Topologia atual será exibida em uma nova página. **Nota:** Esta opção está disponível apenas quando o IBM Security QRadar Risk Manager estiver sido comprado e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

Parâmetros da ofensa

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

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

Tabela 13. Descrição dos parâmetros da guia Ofensas

Parâmetro	Local	Descrição
Annotation	Tabela 5 principais anotações	Especifica os detalhes da anotação. As anotações são descrições de texto que as regras podem incluir automaticamente nas ofensas como parte da resposta da regra. .
Anomalia	Tabela Últimos 10 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.
Anomaly Text	Tabela Últimos 10 eventos (eventos de anomalia)	Especifica uma descrição do comportamento anômalo que foi detectado pela regra de detecção de anomalias.
Anomaly Value	Tabela Últimos 10 eventos (eventos de anomalia)	Especifica o valor que fez com que a regra de detecção de anomalias gerasse a ofensa.
Aplicativo	Tabela Últimos 10 fluxos	Especifica o aplicativo que está associado ao fluxo.
Application Name	Tabela Origem da ofensa, se o Tipo de ofensa for ID do aplicativo	Especifica o aplicativo que está associado ao fluxo que criou a ofensa.
ASN Index	Tabela Origem de ofensa, se o Tipo de ofensa for ASN de origem ou de destino	Especifica o valor ASN que está associado ao fluxo que criou a ofensa.
Asset Name	Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino	Especifica o nome do ativo, que pode ser designado usando a função Perfil de ativo. Para obter mais informações, consulte Gerenciamento de ativo.
Peso do ativo	Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino	Especifica o peso do ativo, que é possível designar usando a função Perfil de ativo. Para obter mais informações, consulte Gerenciamento de ativo.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Assigned to	Tabela Ofensa	Especifica o usuário que está designado à ofensa. Se nenhum usuário for designado, este campo especificará Não designado. Clique em Não designado para designar a ofensa a um usuário. Para obter mais informações, consulte Designando ofensas para usuários.
Category	Tabela Últimos 10 eventos	Especifica a categoria do evento.
Category Name	Página Por detalhes de categoria	Especifica o nome da categoria de alto nível.
Chained	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de destino • Tabela 5 principais IPs de destino	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 se tornar o endereço IP de origem de outra ofensa. Se o endereço IP de destino for encadeado, clique em **Sim** para visualizar as ofensas encadeadas.
Data de Criação	Tabela Últimas 5 Notas	Especifica a data e a hora em que a nota foi criada.
Credibilidade	Tabela Ofensa	Especifica a credibilidade da ofensa, conforme determinado pela classificação de credibilidade dos dispositivos de origem. Por exemplo, a credibilidade será aumentada quando várias ofensas relatarem o mesmo evento ou fluxo.
Parâmetros de Procura Atuais	• Página Por detalhes de IP de origem • Página Por detalhes de IP de destino	A parte superior da tabela exibe os detalhes dos parâmetros de procura que são aplicados aos resultados da procura. Para limpar esses parâmetros de procura, clique em **Limpar filtro**. **Nota:** Este parâmetro só será exibido após você aplicar um filtro.
Descrição	• Página Todas as ofensas • Página Minhas ofensas • Tabela Ofensa • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas • Tabela Origem de ofensa, se o Tipo de ofensa for Fonte de log • Tabela 5 principais fontes de log	Especifica a descrição da ofensa ou fonte de log.
IP de Destino	• Tabela Últimos 10 eventos • Tabela Últimos 10 fluxos	Especifica o endereço IP de destino do evento ou fluxo.
IP de Destino	• Tabela 5 principais IPs de destino • Página Por IP de origem – Lista de destinos do local • Página Por detalhes de IP de destino • Página Por rede – Lista de destinos do local	Especifica o endereço IP do destino. Se as consultas de DNS estiverem ativadas na guia Administração, será possível visualizar o nome do DNS passando seu mouse sobre o endereço IP.
Destination IP(s)	Tabela Ofensa	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	• Página Todas as ofensas • Página Minhas ofensas	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 dos endereços IP de destino.
IPs de Destino	• Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica os endereços IP e nomes dos ativos (se disponível) do destino que estão associados à ofensa. Se o DNS estiver ativado na guia Administração, será possível visualizar o nome de DNS passando seu mouse sobre o endereço IP ou nome do ativo.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
IPs de Destino	Página Por detalhes de rede	Especifica o número de endereços IP de destino associados à rede.
Porta de destino	Tabela Últimos 10 fluxos	Especifica a porta de destino do fluxo.
Destination(s)	• Tabela 5 principais IPs de origem • Página Por detalhes de IP de origem • Página Por IP de destino – Lista de origens • Página Por rede – Lista de origens	Especifica o nome do evento, conforme identificado no mapa de QID, que está associado ao evento ou fluxo que criou a ofensa. Passe o mouse sobre o nome do evento para visualizar o QID.
Contagem de Eventos/Fluxos	Página Por detalhes de categoria	Especifica o número de eventos ou fluxos ativos (eventos ou fluxos que não estão encerrados ou ocultos) associados à ofensa na categoria. As ofensas permanecerão ativas por um período de tempo apenas 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 Destino Página Rede	Especifica o número de eventos e fluxos que ocorreram na ofensa e no número de categorias. Clique no link de eventos para investigar detalhadamente 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 à ofensa. Ao clicar no link de fluxos, os resultados da procura de fluxo serão exibidos. **Nota:** Se a contagem de fluxo exibir N/D, a ofensa poderá ter uma data de início que precede a data em 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/D para investigar os fluxos associados nos resultados da procura de fluxo.
Contagem de Eventos/Fluxos	Página Por detalhes de categoria	Especifica o número de eventos ou fluxos ativos (eventos ou fluxos que não estão encerrados ou ocultos) associados à ofensa na categoria. As ofensas permanecerão ativas por um período de tempo apenas 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 Destino Página Rede	Especifica o número de eventos e fluxos que ocorreram na ofensa e no número de categorias. Clique no link de eventos para investigar detalhadamente 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 à ofensa. Ao clicar no link de fluxos, os resultados da procura de fluxo serão exibidos. **Nota:** Se a contagem de fluxo exibir N/D, a ofensa poderá ter uma data de início que precede a data em 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/D para investigar os fluxos associados nos resultados da procura de fluxo.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Events	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem - Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino - Lista de ofensas	Especifica o número de eventos da ofensa.
Events/Flows	• Tabela Origem da ofensa, se o Tipo de ofensa 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, IPv6 de origem ou destino, ASN de origem ou destino, Regra, ID do aplicativo • Tabela 5 principais IPs de origem • Página Por detalhes de IP de origem • Página Por IP de destino – Lista de origens • Página Por rede – Lista de origens • Página Detalhes da origem • Tabela 5 principais IPs de destino • Página Por IP de origem – Lista de destinos do local • Página Por detalhes de IP de destino • Página Por rede – Lista de destinos do local • Tabela 5 principais usuários • Tabela 5 principais fontes de log • Tabela 5 principais categorias • Página Por detalhes de rede • Tabela 5 principais categorias	Especifica o número de eventos ou fluxos que estão associados ao endereço IP de origem, endereço IP de destino, nome do evento, nome de usuário, endereço MAC, fonte de log, nome do host, porta, fonte de log, endereço ASN, endereço IPv6, regra, ASN, Aplicativo, rede ou categoria. Clique no link para visualizar mais detalhes.
Primeiro evento/fluxo visto em	Página Detalhes da origem	Especifica a data e hora em que o endereço IP de origem gerou o primeiro evento ou fluxo.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Sinalizador	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem - Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Indica a ação que será tomada na ofensa. As ações são representadas pelos seguintes ícones: • Sinalizador - Indica que a ofensa está marcada para acompanhamento. Isso permite controlar um item específico para investigação adicional. Para obter mais informações sobre como marcar uma ofensa para acompanhamento, consulte Marcando um item para acompanhamento. • Usuário - Indica que a ofensa foi designada a um usuário. Quando uma ofensa for designada a um usuário, a ofensa será exibida na página Minhas ofensas pertencente a este usuário. Para obter mais informações sobre como designar ofensas a usuários, consulte Designando ofensas a usuários. • Notas - Indica que um usuário incluiu notas na ofensa. As notas podem incluir quaisquer informações que você deseje capturar para a ofensa. Por exemplo, é possível incluir uma nota que especifica as informações que não são automaticamente incluídas em uma ofensa, como um número de chamado do Suporte ao Cliente ou informações de gerenciamento de ofensa. Para obter mais informações sobre a inclusão de notas, consulte Incluindo notas. • Protegido - Indica que a ofensa está protegida. O recurso Proteger evita que ofensas especificadas sejam removidas do banco de dados após o período de retenção ter decorrido. Para obter mais informações sobre ofensas protegidas, consulte Protegendo ofensas. Passe o seu mouse sobre o ícone para exibir mais informações.
Flag (continued)		• Ofensa inativa – Indica que esta é uma ofensa inativa. Uma ofensa se torna inativa após terem decorrido cinco dias desde que a ofensa recebeu o último evento. Além disso, todas as ofensas se tornarão inativas após o upgrade do seu software de produto QRadar. Uma ofensa inativa não pode se tornar ativa novamente. Se novos eventos forem detectados para a ofensa, uma nova ofensa será criada e a ofensa inativa será retida até o período de retenção de ofensa ter decorrido. É possível executar as seguintes ações em ofensas inativas: proteger, sinalizar para acompanhamento, incluir notas e designar aos usuários.
Sinalizador	• Página Por detalhe do IP de origem • Página Por IP de origem – Lista dos destinos do local • Página Por detalhes de IP de destino • Página Por IP de destino – Lista de origem • Página Por detalhes de rede • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local	Especifica a ação que será tomada no endereço IP de origem, endereço IP de destino ou rede. Por exemplo, se um sinalizador for exibido, a ofensa será sinalizada para acompanhamento. Passe o seu mouse sobre o ícone para exibir mais informações.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Fluxos	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica o número de fluxos da ofensa. **Nota:** Se a coluna Fluxos exibir N/D, a ofensa poderá ter uma data de início que precede a data que foi feito upgrade para QRadar 7.1.0 (MR1).
Grupo	• Tabela Origem de ofensa, se o Tipo de ofensa for Fonte de log • Tabela 5 principais fontes de log	Especifica a qual grupo a fonte de log pertence.
Group(s)	Tabela Origem de ofensa, se o Tipo de ofensa for Regra	Especifica a qual grupo de regra a regra pertence.
Categoria de Alto Nível	Tabela Origem de ofensa, se o Tipo de ofensa for Nome do evento	Especifica a categoria de alto nível do evento.
Host Name	Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino	Especifica o nome do host que está associado ao endereço IP de origem ou de destino. Se nenhum nome de host for identificado, este campo especificará Desconhecido.
Host Name	Tabela Origem de ofensa, se o Tipo de ofensa for Nome do host	Especifica o nome do host que está associado ao fluxo que criou a ofensa.
ID	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino - Lista de ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas	Especifica o número de identificação exclusivo que o QRadar designa para a ofensa.
IP	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino • Página Detalhes da origem	Especifica o endereço IP de origem que está associado ao evento ou fluxo que criou a ofensa.
Nome de IP/DNS	Página Destino	Especifica o endereço IP do destino. Se o DNS estiver ativado na guia **Administração**, será possível visualizar o nome DNS passando seu mouse sobre o endereço IP ou nome do ativo.
IPv6	Tabela Origem de ofensa, se o Tipo de ofensa for IPv6 de origem ou de destino	Especifica o endereço IPv6 que está associado ao evento ou fluxo que criou a ofensa.
Último Evento/Fluxo	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de destinos do local • Tabela 5 principais IPs de origem • Página Por detalhes de IP de origem • Página Por rede – Lista de origens • Tabela 5 principais IPs de destino • Página Por detalhes de IP de destino • Página Por IP de destino – Lista de origens • Página Por rede – Lista de destinos do local • Tabela 5 principais categorias	Especifica o tempo decorrido desde que o último evento ou fluxo foi observado para a ofensa, categoria, endereço IP de origem ou endereço IP de destino.
Último evento/fluxo visto em	Página Detalhes da origem	Especifica a data e a hora do último evento ou fluxo gerado que está associado ao endereço IP de origem.
Horário do Último Evento/Fluxo	Tabela Origem de ofensa, se o Tipo de ofensa for Fonte de log	Especifica data e hora que a fonte de log foi observada pela última vez no sistema.
Último Grupo Conhecido	Tabela Origem de ofensa, se o Tipo de ofensa for Nome de usuário, Endereço MAC de origem, Endereço MAC de destino ou Nome do host	Especifica o grupo atual ao qual o usuário, endereço MAC ou nome do host pertence. Se nenhum grupo estiver associado, o valor desse campo será Desconhecido. **Nota:** Este campo não exibirá informações históricas.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Último Host Conhecido	Tabela Origem de ofensa, se o Tipo de ofensa for o Nome de usuário, Endereço MAC de origem ou Endereço MAC de destino	Especifica o host atual ao qual o usuário ou endereço MAC está associado. Se nenhum host for identificado, este campo especificará Desconhecido. **Nota:** Este campo não exibirá informações históricas.
Último IP Conhecido	Tabela Origem de ofensa, se o Tipo de ofensa 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. **Nota:** Este campo não exibirá informações históricas.
Último MAC Conhecido	Tabela Origem de ofensa, se o Tipo de ofensa for Nome de usuário ou Nome do host	Especifica o último endereço MAC conhecido do nome de usuário ou do host. Se nenhum MAC for identificado, este campo especificará Desconhecido. **Nota:** Este campo não exibirá informações históricas.
Última Máquina Conhecida	Tabela Origem de ofensa, se o Tipo de ofensa 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. **Nota:** Este campo não exibirá informações históricas.
Último Nome de Usuário Conhecido	Tabela Origem de ofensa, se o Tipo de ofensa 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. **Nota:** Este campo não exibirá informações históricas.
Último Observado	Tabela Origem de ofensa, se o Tipo de ofensa 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, endereço MAC ou nome do host foi observado pela última vez no sistema.
Horário do Último Pacote	Tabela Últimos 10 fluxos	Especifica a data e hora em que o último pacote do fluxo foi enviado.
Contagem de Destinos do Local	Tabela 5 principais categorias Página Por detalhes de categoria	Especifica o número de endereços IP de destino do local associados à categoria.
Local Destination(s)	Página Detalhes da origem	Especifica os endereços IP de destino do local associados ao 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 exibida.
Local	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino • Tabela 5 principais IPs de origem • Página Por detalhes de IP de origem • Página Detalhes da origem • Página Por IP de destino - Lista de origens • Página Por rede – Lista de origens	Especifica o local de rede do endereço IP de origem ou endereço IP de destino. Se a localização for local, será possível clicar no link para visualizar as redes.
Fonte de Log	Tabela Últimos 10 eventos	Especifica a fonte de log que detectou o evento.
Identificador de Fonte de Log	Tabela Origem de ofensa, se o Tipo de ofensa for Fonte de log	Especifica o nome do host da fonte de log.
Nome da Fonte de Log	Tabela Origem de ofensa, se o Tipo de ofensa for Fonte de log	Especifica o nome da fonte de log, conforme identificado na tabela Fontes de log, que está associada ao evento que criou a ofensa. **Nota:** As informações que são exibidas para ofensas de fonte de log são derivadas da página Fontes de log na guia Administrador. É necessário ter acesso administrativo para acessar a guia Administração e gerenciar as fontes de log. Para obter mais informações sobre o gerenciamento da fonte de log, consulte o *Guia de Gerenciamento do Log Sources* .

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Fontes de log	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica as fontes de log que são associadas à ofensa. Se mais de uma fonte de log estiver associada à ofensa, esse campo especificará Vários e o número das fontes de log.
Categoria de Nível Baixo	Tabela Origem de ofensa, se o Tipo de ofensa for Nome do evento	Especifica a categoria de nível inferior do evento.
MAC	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino • Tabela 5 principais IPs de origem • Tabela 5 principais IPs de destino • Página Por detalhes de IP de origem • Página Por IP de origem - Lista de destinos do local • Página Por detalhes de IP de destino • Página Por IP de destino - Lista de origens • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local	Especifica o endereço MAC do endereço IP de origem ou destino de quando a ofensa foi iniciada. Se o endereço MAC for desconhecido, este campo especificará Desconhecido.
MAC Address	Tabela Origem de ofensa, se o Tipo ofensa for Endereço MAC de origem ou de destino	Especifica o endereço MAC que está associado ao evento que criou a ofensa. Se nenhum endereço MAC for identificado, este campo especificará Desconhecido.
Magnitude	• Página Todas as ofensas • Página Minhas ofensas • Tabela Ofensa • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino - Lista de ofensas • Tabela 5 principais categorias • Tabela Últimos 10 eventos • Página Por detalhes de rede • Página Rede	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	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino • Tabela 5 principais IPs de origem • Tabela 5 principais IPs de destino • Página Por detalhes de IP de origem • Página Detalhes da origem • Página Por IP de origem – Lista dos destinos do local • Página Destino • Página Por detalhes de IP de destino • Página Por IP de destino – Lista de origens • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local	Especifica a importância relativa do endereço IP de origem ou de destino. A barra de magnitude fornece uma representação visual do valor de risco de CVSS do ativo que está associado ao endereço IP. Passe o mouse sobre a barra de magnitude para exibir a magnitude calculada.
Name	• Tabela 5 principais fontes de log • Tabela 5 principais usuários • Tabela 5 principais categorias • Página Rede	Especifica o nome da fonte de log, usuário, categoria, endereço IP de rede ou nome.
Rede	Página Por detalhes de rede	Especifica o nome da rede.

Tabela 13. Descrição dos parâmetros da guia Ofensas (continuação)

Parâmetro	Local	Descrição
Network(s)	Tabela Ofensa	Especifica a rede de destino da ofensa. Se a ofensa tiver uma rede de destino, este campo exibirá a folha de rede. Clique no link para visualizar as informações de rede. Se a ofensa possuir mais de uma rede de destino, o termo Vários será exibido. Clique no link para visualizar mais detalhes.
Notas	• Tabela Origem de ofensa, se o Tipo de ofensa for Regra • Tabela Últimas 5 Notas	Especifica as notas da regra.
Contagem de Crimes	Página Por detalhes de categoria	Especifica o número de ofensas ativas em cada categoria. As ofensas ativas são ofensas que não foram ocultas ou encerradas. Se a página Por detalhes de categoria incluir o filtro Excluir ofensas ocultas, a contagem de ofensa que será exibida no parâmetro Offense Count talvez não esteja correta. Se desejar visualizar a contagem total na área de janela Por categoria, clique em **Limpar filtro** ao lado do filtro Excluir ofensas ocultas na página Por detalhes de categoria.
Origem do Crime	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica informações sobre a origem da ofensa. As informações que são exibidas no campo **Origem de ofensa** dependem do tipo de ofensa. Por exemplo, se o tipo de ofensa for Porta de origem, o campo **Fonte de origem** exibirá a porta de origem do evento que criou a ofensa.
Offense Type	• Página Minhas ofensas • Tabela Ofensa • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica o tipo de ofensa. O Tipo de ofensa é determinado pela regra que criou a ofensa. Por exemplo, se o tipo de ofensa for o evento de fonte do log, a regra que gerou a ofensa correlaciona eventos que estão baseados no dispositivo que detectou o evento. Os tipos de ofensa incluem: • IP de Origem • IP de Destino • Nome do Evento • Nome de Usuário • Endereço MAC de Origem • Endereço MAC de Destino • **Fonte de Log** • Host Name • Porta de origem • Porta de destino • IPv6 de Origem • IPv6 de Destino • ASN de Origem • ASN de Destino • Regra • ID do aplicativo O tipo de ofensa determina que tipo de informação é exibido na área de janela Resumo da origem da ofensa.
Offense(s)	• Página Detalhes da origem • Página Destino	Especifica os nomes das ofensas que são associadas ao endereço IP de origem ou de destino. Para visualizar mais informações sobre a ofensa, clique no nome ou termo exibido. Se houver várias ofensas, o termo Vários será exibida.

Crime(s) Ativado(s)	Página Rede	Especifica as ofensas que são ativadas a partir da rede. Se várias ofensas forem responsáveis, este campo especificará Vário e o número de ofensas.
Crime(s) de Destino	Página Rede	Especifica as ofensas que são direcionadas para a rede. Se várias ofensas forem responsáveis, este campo especificará Vários e o número de ofensas
Ofensas	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem, IP de destino, Nome do evento, Nome de usuário, Endereço MAC de origem ou de destino, Fonte de log, nome do host, Porta de origem ou de destino, IPv6 de origem ou de destino, ASN de origem ou destino, Regra, ID do aplicativo • Tabela 5 principais IPs de origem • Tabela 5 principais IPs de destino • Tabela 5 principais fontes de log • Tabela 5 principais usuários • Página Por detalhes de IP de origem • Página Por IP de origem – Lista de destinos do local • Página Por detalhes de IP de destino • Página Por IP de destino – Lista de origens • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local	Especifica o número de ofensas que estão associadas ao endereço IP de origem e de destino, nome do evento, nome de usuário, endereço MAC, fonte de log, nome do host, porta, endereço IPv6, ASN, regra ou aplicativo. Clique no link para visualizar mais detalhes.
Crimes Ativados	Página Por detalhes de rede	Especifica o número de ofensas que são originadas da rede.
Crimes Visados	Página Por detalhes de rede	Especifica o número de ofensas que são direcionados para a rede.
Port	Tabela Origem de ofensa, se o Tipo de ofensa for Porta de origem ou de destino	Especifica a porta associada ao evento ou fluxo que criou a ofensa.
Relevância	Tabela Ofensa	Especifica a importância relativa da ofensa.
Response	Tabela Origem de ofensa, se o Tipo de ofensa for Regra	Especifica o tipo de resposta da regra.
Rule Description	Tabela Origem de ofensa, se o Tipo de ofensa for Regra	Especifica o resumo dos parâmetros de regra.
Rule Name	Tabela Origem de ofensa, se o Tipo de ofensa for Regra	Especifica o nome da regra que está associada ao evento ou fluxo que criou a ofensa. **Nota:** As informações que são exibidas para ofensas de regra são derivadas da guia **Regras**.
Tipo de Regra	Tabela Origem de ofensa, se o Tipo de ofensa for Regra	Especifica o tipo de regra da ofensa.
Gravidade	• Tabela Origem de ofensa, se o Tipo de ofensa for Nome do evento • Tabela Ofensa	Especifica a severidade do evento ou ofensa. Severidade especifica a quantidade de ameaça que uma ofensa representa em relação a quão preparado está o endereço IP de destino para o ataque. Este valor é diretamente mapeado para a categoria de evento que é correlacionada à ofensa. Por exemplo, um ataque de Negação de Serviço (DoS) tem uma severidade 10, que especifica uma ocorrência grave.
Contagem de Origens	Página Por detalhes de 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	• Página Por detalhes de IP de origem • Página Por IP de destino – Lista de origens • Página Por rede – Lista de origens • Tabela 5 principais IPs de origem • Tabela Últimos 10 fluxos	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 Administração, será possível visualizar o nome do DNS passando seu mouse sobre o endereço IP.

Source IP(s)	Tabela Ofensa	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. Para obter mais informações sobre endereços IP de origem, consulte Monitorando ofensas agrupadas por IP de origem.
IPs de Origem	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica os endereços IP ou o nome do host do dispositivo que tentaram 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 o DNS estiver ativado na guia Administração, será possível visualizar o nome de DNS passando seu mouse sobre o endereço IP ou nome do ativo.
IPs de Origem	Página Por detalhes de rede	Especifica o número de endereços IP de origem associados à rede.
Porta de origem	Tabela Últimos 10 fluxos	Especifica a porta de origem do fluxo.
Source(s)	• Tabela 5 principais IPs de destino • Página Por IP de origem – Lista de destinos do local • Página Por detalhes de IP de destino	Especifica o número de endereços IP de origem do endereço IP de destino.
Source(s)	• Página Destino • Página Rede	Especifica os endereços IP de origem da ofensa que estão associados ao endereço IP de destino ou de rede. Para visualizar mais informações sobre os endereços IP de origem, clique no endereço IP, nome do ativo ou termo que é exibido. Se um endereço IP de fonte isolada for especificado, um endereço IP e o nome do ativo serão exibidos (se disponível). É possível clicar no endereço IP ou nome do ativo para visualizar os detalhes do endereço IP de origem. Se houver vários endereços IP de origem, este campo especifica Vários e o número de endereços IP de origem.
Source(s)	Página Por rede – Lista de destinos do local	Especifica o número de endereços IP de origem associados ao endereço IP de destino.
Start	Tabela Ofensa	Especifica a data e hora em que o primeiro evento ou fluxo ocorreu na ofensa.
Start Date	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem – Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas	Especifica a data e hora do primeiro evento ou fluxo que está associado à ofensa.
Status	Tabela Origem de ofensa, se o Tipo de ofensa for Fonte de log	Especifica o status da fonte de log.

Status	Tabela Ofensa	Exibe ícones para indicar o status de uma ofensa. Os ícones de status incluem: **Ofensa inativa**. Uma ofensa se torna inativa após terem decorrido cinco dias desde que a ofensa recebeu o último evento. Todas as ofensas se tornam inativas após o upgrade do seu software de produto QRadar. Uma ofensa inativa não pode se tornar ativa novamente. Se novos eventos forem detectados para a ofensa, uma nova ofensa será criada e a ofensa inativa será retida até o período de retenção de ofensa ter decorrido. É possível proteger, sinalizar para acompanhamento, incluir notas e designar a usuários para uma ofensa inativa. Um sinalizador **Ofensa Oculta** na página Todas as Ofensas indica que a ofensa está oculta na visualização. Se você procurar ofensas ocultas, elas ficam visíveis somente na página Todas as Ofensas, em que estão sinalizadas como ofensa oculta. Para obter mais informações, consulte Ocultar ofensas. **Usuário** indica que a ofensa foi designada a um usuário. Quando uma ofensa for designada a um usuário, ela será exibida na página Minhas ofensas pertencente a este usuário. Para obter mais informações, consulte Designando ofensas para usuários. **Protegido** evita que ofensas especificadas sejam removidas do banco de dados depois do período de retenção transcorrer. Para obter mais informações, consulte Protegendo ofensas. **Ofensa encerrada** indica que a ofensa foi encerrada. Para obter mais informações, consulte Encerrando ofensas.
Time	• Tabela Últimos 10 eventos • Tabela Últimos 10 eventos (eventos de anomalia)	Especifica a data e a hora em que o primeiro evento foi detectado no evento normalizado. Esta data e hora foi especificada pelo dispositivo que detectou o evento.
Time	Tabela 5 principais anotações	Especifica a data e a hora em que a anotação foi criada.
Total Bytes	Tabela Últimos 10 fluxos	Especifica o número total de bytes do fluxo.
Total de Eventos/Fluxos	• Tabela 5 principais fontes de log • Tabela 5 principais usuários	Especifica o número total de eventos da fonte de log ou usuário.
User	• Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino, ou Nome de usuário • Tabela 5 principais IPs de origem • Tabela 5 principais IPs de destino • Página Por detalhes do IP de origem • Página Por IP de origem – Lista de destinos do local • Página Por detalhes de IP de destino • Página Por IP de destino – Lista de origens • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local	Especifica o usuário que está associado a um endereço IP de origem ou de destino. Se nenhum usuário for identificado, este campo especificará Desconhecido.
Nome de usuário	Tabela Origem de ofensa, se o Tipo de ofensa for Nome de usuário	Especifica o nome de usuário que está associado ao evento ou fluxo que criou a ofensa. **Nota:** Se mover o ponteiro do mouse sobre o parâmetro Username, a dica de ferramenta que é exibida fornece o nome do usuário que está associado às informações de nome de usuário mais recentes a partir da guia Ativos em vez do nome do usuário que está associado ao evento ou fluxo que criou a ofensa.
Nome de usuário	Tabela Últimas 5 Notas	Especifica o usuário que criou a nota.

Users	• Página Todas as ofensas • Página Minhas ofensas • Página Por IP de origem - Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino - Lista de ofensas	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.
View Offenses	• Página Por detalhes de IP de origem • Página Por detalhes de IP de destino	Selecione uma opção a partir desta caixa de listagem para filtrar as ofensas 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 pelo qual deseja filtrar.
Vulnerabilidades	Tabela Origem de ofensa, se o Tipo de ofensa for IP de origem ou de destino	Especifica o número de vulnerabilidades identificadas que são associadas ao endereço IP de origem ou de 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.
Vulnerability	• Tabela 5 principais IPs de origem • Página Por detalhes de IP de origem • Página Por rede – Lista de origens • Tabela 5 principais IPs de destino • Página Por IP de origem - Lista de destinos do local • Página Por detalhes de IP de destino • Página Por rede – Lista de destinos do local	Especifica se o endereço IP de origem ou de destino possui vulnerabilidades.
Peso	• Tabela 5 principais IPs de origem • Tabela 5 principais IPs de destino • Página Por IP de origem - Lista de destinos do local • Página Por detalhes de IP de origem • Página Por detalhes de IP de destino • Página Por IP de destino - Lista de origens • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local • Tabela 5 principais anotações	Especifica o peso do endereço IP de origem, endereço IP de destino ou anotação. O peso de um endereço IP é designado na guia **Ativos**. Para obter mais informações, consulte Gerenciamento de ativo.

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 de uma fonte 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.

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

Barra de ferramentas da guia Atividade de log

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

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

Tabela 14. Opções da barra de ferramentas Atividade de log

Opção	Descrição
Procura	Clique em **Procurar** para executar procuras avançadas em eventos. As opções incluem: • **Nova procura** – Selecione esta opção para criar uma nova procura de evento. • **Editar procura** – Selecione esta opção para selecionar e editar uma procura de evento. • **Gerenciar resultados da procura** – Selecione esta opção para visualizar e gerenciar resultados da procura.
Procuras Rápidas	Nesta caixa de listagem, é possível executar procuras salvas anteriormente. As opções serão exibidas na caixa de listagem **Procuras rápidas** somente quando você tiver salvado critérios de procura que especificam a opção **Incluir em minhas procuras rápidas**.
Incluir filtro	Clique em **Incluir filtro** para incluir um filtro aos resultados da procura atuais.
Salvar critérios	Clique em **Salvar critérios** para salvar os critérios de procura atuais.
Salvar resultados	Clique em **Salvar resultados** para salvar os resultados da procura atual. Essa opção será exibida somente após uma procura ser concluída. Esta opção está desativada no modo de fluxo.
Cancelar	Clique em **Cancelar** para cancelar uma procura em andamento. Esta opção está desativada no modo de fluxo.
Positivo Falso	Clique em **Positivo falso** para abrir a janela Ajuste de positivo falso, que permitirá descartar eventos que são conhecidos como falsos positivos da criação de ofensas. Esta opção está desativada no modo de fluxo. Para obter mais informações sobre o ajuste de positivos falsos, consulte Ajuste de positivos falsos.

Tabela 14. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Regras	A opção Regras estará visível apenas se tiver permissão para visualizar as regras. Clique em **Regras** para configurar as regras do evento customizado. As opções incluem: • **Regras** – Selecione esta opção para visualizar ou criar uma regra. Se tiver apenas a permissão para visualizar as regras, a página de resumo do assistente Regras será exibida. Se tiver a permissão para manter as regras customizadas, o assistente Regras será exibido e você poderá 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), deve-se salvar critérios de procura agregados porque os critérios da procura salva especificam os parâmetros requeridos. **Nota:** As opções de regra de detecção de anomalias serão visíveis apenas se tiver a permissão **Atividade de log** > **Manter regras customizadas**. • **Incluir regra de limite** – Selecione esta opção para criar uma regra de limite. Uma regra de limite testa o tráfego de evento da atividade que excede um limite configurado. Os limites podem ser baseados em quaisquer dados que são coletados peloQRadar. Por exemplo, se criar 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 221º cliente tentar efetuar login. Ao selecionar a opção **Incluir regra de limite**, o assistente Regras será exibido, preenchido com as opções apropriadas para criar uma regra de limite.
Regras (continuação)	• **Incluir regra comportamental** – Selecione esta opção para criar uma regra comportamental. Uma regra comportamental 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, é possível criar uma regra comportamental para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego da última hora. Se houver uma alteração de mais de 40%, a regra irá gerar uma resposta. Ao selecionar a opção **Incluir regra comportamental**, o assistente Regras será exibido, preenchido previamente com as opções apropriadas para criar uma regra comportamental. • **Incluir regra de anomalia** – 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 começar a se comunicar com os hosts nesse país, uma regra de anomalia gerará um alerta. Ao selecionar a opção **Incluir regra de anomalia**, o assistente Regras será exibido e preenchido previamente com as opções apropriadas para a criação de uma regra de anomalia.

Tabela 14. Opções da barra de ferramentas Atividade de log (continuação)

Opção	Descrição
Ações	Clique em **Ações** para executar as seguintes ações: • **Mostrar todos** – Selecione esta opção para remover todos os filtros nos critérios de procura e exibir todos os eventos não filtrados. • **Imprimir** – Selecione esta opção para imprimir os eventos que são exibidos na página. • **Exportar para XML** > **Colunas visíveis** – Selecione esta opção para exportar somente as colunas que estão visíveis na guia Atividade de log. Esta é a opção recomendada. Consulte Exportando eventos. • **Exportar para XML** > **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. Consulte Exportando eventos. • **Exportar para CSV** >**Colunas visíveis** – Selecione esta opção para exportar somente as colunas que estão visíveis na guia Atividade de log. Esta é a opção recomendada. Consulte Exportando eventos. • **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. Consulte Exportando eventos. • **Excluir** – Selecione esta opção para excluir um resultado da procura. Consulte Gerenciamento de resultados da procura de evento e fluxo. • **Notificar** – Selecione esta opção para especificar que deseja uma notificação por email na conclusão das procuras selecionadas. Esta opção é ativada apenas para procuras em andamento. **Nota:** As opções **Imprimir**, **Exportar para XML** e **Exportar para CSV** estão desativadas no modo de fluxo e ao visualizar resultados parciais de procura.
Filtro rápido	Digite seus critérios de procura no campo **Filtro rápido** e clique no ícone **Filtro rápido** 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 seus critérios especificados. **Nota:** Ao clicar no campo **Filtro rápido**, uma dica de ferramenta será exibida, fornecendo informações sobre a sintaxe apropriada para usar para o critério de procura. Para obter mais informações sobre sintaxe, consulte Sintaxe de Filtro rápido.

Sintaxe do filtro rápido

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

A funcionalidade de 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 você digite uma sequência de procura de texto e clique no ícone **Filtro Rápido** para aplicar seu filtro rápido à lista de eventos atualmente exibida.
- Caixa de diálogo **Incluir Filtro**. Na caixa de diálogo **Incluir Filtro** acessada ao clicar no ícone **Incluir Filtro** na guia **Atividade de Log**, você pode selecionar **Filtro Rápido** como seu parâmetro de filtro e digitar uma sequência de procura de texto. Isso permitirá que você aplique seu filtro rápido à lista de eventos ou fluxos atualmente exibida. Para obter mais informações sobre a caixa de diálogo **Incluir filtro**, consulte Sintaxe de Filtro Rápido.
- Páginas de procura de Evento e Fluxo - Nas páginas de procura de evento e fluxo, você pode incluir um **Filtro rápido** em sua lista de filtros a serem incluídos em seus critérios de procura.

Ao visualizar os eventos em tempo real (fluxo) ou o último modo de intervalo, é possível digitar apenas 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 espera localizar na carga útil. Por exemplo, "Firewall"
- Inclua vários termos entre aspas duplas para indicar que você deseja procurar pela 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 frase ou palavra 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".
- Agrupe 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 ("URL acessada" OR "Negar udp src") AND 10.100.100.*)` Ao criar critérios de procura que inclui a expressão lógica NOT, você deve incluir pelo menos um outro tipo de expressão lógica, caso contrário, o filtro não retornará nenhum resultado. Por exemplo: `(%PIX* AND ("URL acessada" OR "Negar 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 do log**, você pode clicar com o botão direito do mouse em um evento para acessar mais informações de filtro de eventos.

As opções do menu ativado pelo botão direito são:

Tabela 15. Opções do menu ativado pelo botão direito

Opção	Descrição
Filtrar	Selecione esta opção para filtrar no 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 ofensas. 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 endereços IP. Para obter mais informações sobre como investigar um nome de usuário, consulte Investigando nomes de usuário. **Nota:** Esta opção não é exibida no modo de fluxo.

Barra de status

Durante o fluxo de eventos, a barra de status exibe o número médio dos resultados recebidos por segundo.

Este é o número de resultados que o Console recebeu com êxito dos processadores de Eventos. Se o número for maior que 40 resultados por segundo, apenas 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 estão em fluxo, a barra de status exibe o número dos resultados da procura atualmente exibidos na guia e a quantia de tempo necessária para processar os resultados da procura.

Monitorando a atividade de log

Por padrão, a guia **Atividade de log** exibe eventos em modo de fluxo, o que permite a visualização de 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 **Visualizar**.

Se os critérios de procura salvos foram 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 critérios de procura de fluxo e de evento.

Visualizando eventos de fluxo

O modo de fluxo permitirá que você visualize os dados do evento inserido em seu sistema. Este modo fornece a você uma visualização em tempo real de sua atividade de evento 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 de eventos agrupados ou o 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 os eventos 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 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 do evento bruto 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 série temporal, consulte visão geral do gráfico de série temporal.

A guia **Atividade de Log** exibe os seguintes parâmetros quando você visualiza os eventos normalizados:

Tabela 16. Guia de atividade de log – Parâmetros do padrão (normalizado)

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 **Limpar filtro**. **Nota:** Este parâmetro só será exibido após você aplicar um filtro.
Visualização	Nesta caixa de listagem, você pode selecionar o intervalo de tempo que 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: **Nota:** Clique na seta ao lado de **Estatísticas atuais** para exibir ou ocultar as estatísticas. • **Resultados totais** – Especifica o número total de resultados que correspondeu ao seu critério de procura. • **Arquivos de dados procurados** – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • **Arquivos de dados compactados procurados** – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • **Contagem de arquivo de índice** – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas atuais são úteis para a resolução de problemas. Quando você contata o Suporte ao Cliente para resolver eventos, você poderá ser solicitado a fornecer informações de estatística atual.
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e a opção de agrupamento. Clique em **Ocultar gráficos** se deseja remover os gráficos de sua exibição. Os gráficos apenas serão exibidos após você selecionar um 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. **Nota:** 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 informações adicionais, 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. **Nota:** Dependendo do produto, este ícone pode não estar disponível. Você deve ter IBM Security QRadar SIEM.
Start Time	Especifica a hora do primeiro evento, conforme reportado para QRadar pela origem de log.
Nome do Evento	Especifica o nome normalizado do evento.

Tabela 16. Guia de atividade de log – Parâmetros do padrão (normalizado) (continuação)

Parâmetro	Descrição
Fonte de Log	Especifica a origem de log que originou o evento. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
Contagem de eventos	Especifica o número total de eventos empacotados neste evento normalizado. Os eventos são empacotados quando vários eventos do mesmo tipo para o mesmo endereço IP de origem e destino são detectados dentro de um curto período.
Time	Especifica a data e hora quando o QRadar recebeu o evento.
Categoria de Nível Baixo	Especifica a categoria de baixo nível associada a este evento. Para obter mais informações sobre as categorias de eventos, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.
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. As 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 a credibilidade, relevância e gravidade, consulte o Glossário.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Exibir**, 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 Detalhes do evento.

Visualizando eventos brutos

Você pode visualizar dados do evento bruto, que são os dados do evento não analisados do registro de origem.

Sobre Esta Tarefa

Quando você visualiza dados do evento bruto, a guia **Atividade de Log** fornece os seguintes parâmetros para cada evento.

Tabela 17. Parâmetros de evento bruto

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 **Limpar filtro**. **Nota:** Este parâmetro só será exibido após você aplicar um filtro.
Visualização	Nesta caixa de listagem, você pode selecionar o intervalo de tempo que você deseja filtrar.

Tabela 17. Parâmetros de evento bruto (continuação)

Parâmetro	Descrição
Estatísticas Atuais	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: **Nota:** Clique na seta ao lado de **Estatísticas atuais** para exibir ou ocultar as estatísticas. • **Resultados totais** – Especifica o número total de resultados que correspondeu ao seu critério de procura. • **Arquivos de dados procurados** – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • **Arquivos de dados compactados procurados** – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • **Contagem de arquivo de índice** – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas Atuais são úteis para a resolução de problemas. Quando você contata o Suporte ao Cliente para resolver eventos, você poderá ser solicitado a fornecer informações de estatística atual.
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e a opção de agrupamento. Clique em **Ocultar gráficos** se deseja remover os gráficos de sua exibição. Os gráficos apenas serão exibidos após você selecionar um prazo de Último Intervalo (atualização automática) ou acima dele, e uma opção de agrupamento a ser exibida. **Nota:** 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 informações adicionais, consulte a documentação do navegador.
Ícone ofensas	Clique neste ícone para visualizar detalhes da ofensa associada a este evento.
Start Time	Especifica a hora do primeiro evento, conforme reportado para QRadar pela origem de log.
Fonte de Log	Especifica a origem de log que originou o evento. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
Payload	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 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 o critério de procura não agrupado, esta opção será exibida.

A caixa de lista de Exibição fornece as opções a seguir:

Tabela 18. Opções de eventos agrupados

Opção de grupo	Descrição
Categoria de Nível Baixo	Exibe uma lista resumida de eventos agrupados pela categoria de baixo nível do evento.
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 aos eventos.
Fonte de Log	Exibe uma lista resumida de eventos agrupados pelas origens de log que enviaram 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 ao 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 dependerá 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 19. Parâmetros de eventos agrupados

Parâmetro	Descrição
Agrupar por	Especifica o parâmetro pelo qual a procura é agrupada.
Filtros Atuais	A parte superior da tabela exibe os detalhes do filtro aplicado aos resultados da procura. Para limpar esses valores de filtro, clique em **Limpar filtro**.
Visualização	Na caixa de listagem, selecione o intervalo de tempo que você deseja filtrar.
Estatísticas Atuais	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: **Nota:** Clique na seta ao lado de **Estatísticas atuais** para exibir ou ocultar as estatísticas. • **Resultados totais** – Especifica o número total de resultados que correspondeu ao seu critério de procura. • **Arquivos de dados procurados** – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • **Arquivos de dados compactados procurados** – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • **Contagem de arquivo de índice** – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas Atuais são úteis para a resolução de problemas. Quando você contata o Suporte ao Cliente para resolver eventos, você pode ser solicitado a fornecer informações da estatística atual.

Tabela 19. Parâmetros de eventos agrupados (continuação)

Parâmetro	Descrição
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e a opção de agrupamento. Clique em **Ocultar gráficos** se você deseja remover o gráfico de sua exibição. 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 legenda, você pode executar as ações a seguir: • Mova o ponteiro do mouse sobre um item de legenda para visualizar mais informações sobre os parâmetros que ele representa. • Clique com o botão direito no item de legenda para investigar mais detalhadamente o item. • Clique em um item de legenda para ocultar os itens no gráfico. Clique no item de legenda novamente para mostrar os itens ocultos. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item. • Clique em **Legenda** se deseja remover a legenda da exibição de seu gráfico. **Nota:** Os gráficos apenas serão exibidos após você selecionar um prazo de Último Intervalo (atualização automática) ou acima dele, e uma opção de agrupamento a ser exibida. **Nota:** 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 os gráficos, você deve remover a extensão do navegador bloqueadora de anúncios. Para obter informações adicionais, consulte a documentação do navegador.
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 esse 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.
Log Source (Unique Count)	Especifica a origem de log que enviou o evento para QRadar. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
High Level Category (Unique Count)	Especifica a categoria de alto nível deste evento. Se houver várias categorias associadas a este evento, este campo especificará o termo Várias e o número de categorias. Para obter mais informações sobre categorias, consulte o *Guia de Administração do IBM Security QRadar Log Manager*.
Low Level Category (Unique Count)	Especifica a categoria de nível inferior deste evento. Se houver várias categorias associadas a este evento, este campo especificará o termo Várias e o número de categorias.
Protocol (Unique Count)	Especifica o ID do protocolo associado a este evento. Se houver múltiplos protocolos associados a este evento, este campo especificará o termo Múltiplos e o número de IDs de protocolo.
Username (Unique Count)	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 (Maximum)	Especifica a magnitude máxima calculada para eventos agrupados. Variáveis usadas para calcular a magnitude incluem credibilidade, relevância e gravidade. Para obter mais informações sobre a credibilidade, relevância e gravidade, consulte o Glossário.
Event Count (Sum)	Especifica o número total de eventos empacotados neste evento normalizado. Os eventos serão empacotados quando vários do mesmo tipo de evento para o mesmo endereço IP de origem e destino forem vistos em um curto período.
Contagem	Especifica o número total de eventos normalizados neste 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 de 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 único evento.

A página detalhes do evento fornece as seguintes informações:

Tabela 20. Detalhes do evento

Parâmetro	**Descrição**
Nome do Evento	Especifica o nome normalizado do evento.
Categoria de Nível Baixo	Especifica a categoria de nível inferior deste evento.
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 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.
Start Time	Especifica a hora que o evento foi recebido da fonte de log.
Horário de Armazenamento	Especifica a hora em que o evento foi armazenado no banco de dados do QRadar.
Horário da Fonte de Log	Especifica a hora do sistema, conforme relatada pela fonte de log na carga útil do evento.
Informações de detecção de anomalias – Esta área de janela será exibida somente se esse evento for gerado por uma regra de detecção de anomalias. Clique no ícone **Anomalia** para visualizar os resultados da procura salvos que fazem com que a regra de detecção de anomalias gere este evento.	
Rule Description	Especifica a regra de detecção de anomalias que gerou este evento.
Descrição da Anomalia	Especifica uma descrição do comportamento anômalo que foi detectado pela regra de detecção de anomalias.
Valor de Alerta de Anomalia	Especifica o valor de alerta de anomalia.
Informações de origem e destino	
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 o 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 de eventos. 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.
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 NAT serem aplicados.

Tabela 20. Detalhes do evento (continuação)

Parâmetro	Descrição
Porta de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especifica 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 NAT serem aplicados.
IP de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de origem após os valores 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 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 NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino após os valores 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 NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino após os valores NAT serem aplicados.
Origem de IPv6	Especifica o endereço IPv6 de origem do evento.
Destino de IPv6	Especifica o endereço IPv6 do 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.
Informações de carga útil	
Payload	Especifica o conteúdo da carga útil do evento. Este campo oferece três guias para visualizar a carga útil: • Formato de Transformação Universal (UTF) – Clique em UTF. • Hexadecimal – Clique em HEX. • Base64 – Clique em Base64.
Informações adicionais	
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.
Fonte de Log	Especifica a fonte de log que enviou o evento para QRadar. Se houver várias fontes de log associadas a esse evento, este campo especificará o termo Várias e o número de fontes de log.
Contagem de eventos	Especifica o número total de eventos empacotados neste evento normalizado. Os eventos serão empacotados quando vários do mesmo tipo de evento para o mesmo endereço IP de origem e destino forem vistos em um curto período.
Custom Rules	Especifica regras customizadas que correspondam a esse evento. .
Regras Customizadas Parcialmente Correspondidas	Especifica as regras customizadas que correspondem parcialmente a esse evento.
Annotations	Especifica a anotação desse evento. Anotações são descrições de texto que as regras podem incluir automaticamente para eventos como parte da resposta da regra.
Informações de identificação – O QRadar coleta informações de identificação, se disponíveis, a partir das mensagens de fonte de log. As informações de identificação fornecem detalhes adicionais sobre ativos em sua rede. As fontes 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 fontes 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 as informações de identificação. Exemplos incluem: localização física de dispositivos, políticas relevantes, comutação de rede e os nomes da portas.

Tabela 20. Detalhes do evento (continuação)

Parâmetro	Descrição
Has Identity (Flag)	Especifica True se o QRadar tiver coletado informações de identificação para o ativo que está associado a este evento. Para obter mais informações sobre para quais dispositivos enviar informações de identificação, consulte o *Guia de Configuração do IBM Security QRadar DSM*.
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 de eventos fornece várias funções para visualizar detalhes de eventos.

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

Tabela 21. Barra de ferramentas de detalhes do evento

Retornar para lista de eventos	Clique em **Retornar** para **Lista de eventos** para retornar para a lista de eventos.
Ofensa	Clique em **Ofensa** para exibir as ofensas associadas ao evento.
Anomalia	Clique em **Anomalia** para exibir os resultados da procura salvos que fazem com que a regra de detecção de anomalias gere este evento. **Nota:** Esse ícone será exibido apenas se esse evento for gerado por uma regra de detecção de anomalias.
Mapear Evento	Clique em **Mapear evento** para editar o mapeamento de eventos. Para obter mais informações, consulte Modificando o mapeamento de eventos.
Positivo Falso	Clique em **Positivo falso** para descartar o QRadar para evitar que eventos positivos falsos gerem ofensas.
Extrair Propriedade	Clique em **Extrair propriedade** para criar uma propriedade de evento customizada do evento selecionado.
Anterior	Clique em **Anterior** para visualizar o evento anterior na lista de eventos.
Avançar	Clique em **Avançar** para visualizar o próximo evento na lista de eventos.
Dados do PCAP	**Nota:** Essa opção será exibida somente se o QRadar Console estiver configurado para se integrar com o Juniper JunOS Platform DSM. Para obter mais informações sobre o gerenciamento dos dados PCAP, consulte Gerenciando dados PCAP. • **Visualizar informações de PCAP** – Selecione esta opção para visualizar as informações de PCAP. Para obter mais informações, consulte Exibindo informações de PCAP. • **Fazer o download do arquivo PCAP** – Selecione esta opção para fazer download do arquivo PCAP para seu sistema de área de trabalho. Para obter mais informações, consulte Download do arquivo PCAP para seu sistema de área de trabalho.
Imprimir	Clique em **Imprimir** para imprimir os detalhes do evento.

Visualizando ofensas associadas

Na guia Atividades de Log, você pode visualizar a ofensa associada ao evento.

Sobre Esta Tarefa

Se um evento corresponder a uma regra, uma ofensa poderá ser gerada na guia **Ofensas**.

Para obter mais informações sobre como gerenciar ofensas, consulte Capacidade de gerenciamento de ofensa.

Quando você visualiza uma ofensa na guia **Atividade de Log**, a ofensa poderá não ser exibida se o funcionário público ainda não tiver salvo a ofensa associada ao evento selecionado para o disco ou a ofensa for eliminada do banco de dados. Se isso ocorrer, o sistema o notificará.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Opcional. Se você estiver visualizando os 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. Visualizar a ofensa 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

Essa ação manual é usada para mapear eventos de origem de log desconhecidos para eventos do QRadar conhecido para que eles possam ser categorizados e processado apropriadamente.

Sobre Esta Tarefa

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

Para obter mais informações sobre as categorias de eventos, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

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

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

Nota: O ícone **Mapear evento** será desativado para os eventos quando a categoria de nível superior for Auditoria de 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 os eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento que 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 você deseja mapear para esse evento, você poderá procurar por um QID determinado:
   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 **QID** ao qual você deseja associar esse evento.
7. Clique em **OK**.

Ajustando positivos falsos

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

Antes de Iniciar

Você pode ajustar os eventos positivos falsos na página Lista de eventos ou Detalhes do evento.

Sobre Esta Tarefa

Você pode ajustar os eventos positivos falsos na página Lista de eventos ou Detalhes do evento.

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

Para obter mais informações sobre as funções, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

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

Procedimento

1. Clique na guia **Atividade de Log**.
2. Opcional. Se você estiver visualizando os 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 Propriedade de evento/fluxo na janela Positivo falso, selecione uma das opções a seguir:
   - Evento/Fluxo(s) com um QID específico do <Evento>
   - Qualquer Evento/Fluxo(s) com uma categoria de nível inferior do <Evento>
   - Qualquer Evento/Fluxo(s) com uma categoria de nível superior do <Evento>
6. Na área de janela Direção do tráfego, selecione uma das opções a seguir:
   - <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 QRadar Console estiver configurado para se integrar com o Juniper JunOS Platform DSM, a Captura de Pacotes (PCAP) poderá ser recebida, processada, os dados poderão ser armazenados a partir de uma fonte 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 das Séries SRX da Juniper deverá ser configurada com o protocolo de Combinação de Syslog do PCAP. Para obter mais informações sobre como configurar os protocolos de origem de log, consulte o *Guia de Gerenciamento do Log Sources* .

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 download do arquivo **PCAP** para seu sistema de área de trabalho.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na caixa de listagem **Procurar**, selecione **Nova Procura**.
3. Opcional. Para procurar eventos que possuam os 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 **Agrupar por**.
5. Clique em **Filtrar**.

6. Opcional. Se você estiver visualizando os 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 como visualizar e fazer download dos dados do PCAP, consulte as seções a seguir:

- Exibindo informações do PCAP
- Fazendo download do arquivo PCAP para seu sistema de área de trabalho

Visualizando informações do PCAP

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

Antes de Iniciar

Antes que você possa visualizar as informações do PCAP, é necessário 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 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 o sistema de sua 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** da barra de ferramentas detalhes do evento.
2. Se você deseja fazer o download das informações em seu sistema da área de trabalho, escolha uma das opções a seguir:
   - Clique em **Download do arquivo do PCAP** para fazer o download do arquivo PCAP original a ser usado em um aplicativo externo.
   - Clique em **Download do texto do 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 da caixa de listagem.
   - Se você deseja salvar a lista, selecione a opção **Salvar arquivo**.
4. Clique em **OK**.

Fazendo download do arquivo do PCAP para seu sistema de área de trabalho

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

Antes de Iniciar

Antes que você possa visualizar as informações do PCAP, será necessário 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 do PCAP**.
   - Dê um clique duplo no evento que você deseja investigar e, em seguida, selecione **Dados do PCAP** > **Fazer download do arquivo do 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 da 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 de Linguagem de Marcação Extensível (XML) ou Valores Separados por Vírgulas (CSV).

Antes de Iniciar

O período de tempo necessário para exportar seus dados depende do número de parâmetros especificados.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Opcional. Se você estiver visualizando os 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. Esta 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**. Esta 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 de que a exportação foi concluída. Se não foi selecionado 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 designação de funções, consulte o*Guia de Administração* do seu produto.

Selecione a guia **Atividade de Rede** para monitorar visualmente e investigar os 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 podem também 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 22. Opções da barra de ferramentas da guia Atividade de rede

Opções	Descrição
Procurar	Clique em **Procurar** para executar procuras avançadas em fluxos. As opções incluem: • **Nova procura** – Selecione esta opção para criar uma nova procura de fluxo. • **Editar procura** – Selecione esta opção para selecionar e editar uma procura de fluxo. • **Gerenciar resultados da procura** – Selecione esta opção para visualizar e gerenciar resultados da procura. 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 serão exibidas na caixa de listagem **Procuras rápidas** apenas quando tiverem sido salvos os critérios de procura que especificam a opção **Incluir em minhas procuras rápidas**.
Incluir Filtro	Clique em **Incluir filtro** para incluir um filtro aos resultados da procura atual.
Salvar Critérios	Clique em **Salvar critérios** para salvar os critérios de procura atuais.
Salvar resultados	Clique em **Salvar resultados** para salvar os resultados da procura atual. Essa opção será exibida somente após uma procura ser concluída. Esta opção está desativada no modo de fluxo.
Cancelar	Clique em **Cancelar** para cancelar uma procura em andamento. Esta opção está desativada no modo de fluxo.
Positivo Falso	Clique em **Positivo falso** para abrir a janela Ajuste de positivo falso, que permite descartar os fluxos que são conhecidos por serem falsos positivos de criarem ofensas. Para obter mais informações sobre positivos falsos, consulte o Glossário. Esta opção está desativada no modo de fluxo. Consulte Exportando fluxos.

Tabela 22. Opções da barra de ferramentas da guia Atividade de rede (continuação)

Opções	Descrição
Regras	A opção **Regras** estará visível somente se tiver permissão para visualizar as regras customizadas. Selecione uma das opções a seguir: **Regras** para visualizar ou criar uma regra. Se tiver apenas a permissão para visualizar as regras, a página de resumo do assistente Regras será exibida. Se tiver a permissão para manter as regras customizadas, será possível editar a regra. **Nota:** As opções de regra de detecção de anomalias estarão visíveis apenas se tiver a permissão **Atividade de rede** > **Manter regras customizadas**. Para ativar as opções de regra de detecção de anomalias, é necessário salvar o critério de procura agregado. Os critérios de procura salvos especificam os parâmetros requeridos. Selecione uma das seguintes opções: **Incluir regra de limite** 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 qualquer dado coletado. Por exemplo, se criar 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 221º cliente tentar efetuar login. **Incluir regra comportamental** para criar uma regra comportamental. Uma regra comportamental testa o tráfego de fluxo de mudanças de volume no comportamento que ocorre em padrões sazonais regulares. Por exemplo, se um servidor de correio geralmente se comunica com 100 hosts por segundo durante a noite e, de repente, começa a se comunicar com 1.000 hosts por segundo, uma regra comportamental irá gerar um alerta. **Incluir regra de anomalia** para criar uma regra de anomalia. Uma regra de anomalia testa o tráfego de fluxo da atividade anormal, como tráfego novo ou desconhecido. Por exemplo, você pode criar uma regra de anomalias para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego durante a última hora. Se houver uma alteração de mais de 40%, a regra irá gerar uma resposta. Para obter informações adicionais, consulte o *Guia de Administração do IBM Security QRadar SIEM*.
Ações	Clique em **Ações** para executar as seguintes ações: • **Mostrar todos** – Selecione esta opção para remover todos os filtros nos critérios de procura e exibir todos os fluxos não filtrados. • **Imprimir** – Selecione esta opção para imprimir os fluxos que são exibidos na página. • **Exportar para XML** – Selecione esta opção para exportar os fluxos no formato XML. Consulte Exportando fluxos. • **Exportar para CSV** – Selecione esta opção para exportar os fluxos no formato CSV. Consulte Exportando fluxos. • **Excluir** – Selecione esta opção para excluir um resultado da procura. Consulte Procuras de dados. • **Notificar** – Selecione esta opção para especificar que deseja uma notificação por email na conclusão das procuras selecionadas. Esta opção é ativada apenas para procuras em andamento. **Nota:** As opções **Imprimir**, **Exportar para XML** e **Exportar para CSV** estão desativadas no modo de fluxo e ao visualizar resultados parciais de procura.
Filtro Rápido	Digite seus critérios de procura no campo **Filtro rápido** e clique no ícone **Filtro rápido** 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 seus critérios especificados. **Nota:** Ao clicar no campo **Filtro rápido**, uma dica de ferramenta será exibida, fornecendo informações sobre a sintaxe apropriada para usar para o critério de procura. Para obter mais informações de sintaxe, consulte Sintaxe de filtro rápido.

Sintaxe do filtro rápido

O recurso Filtro Rápido permite que você procure cargas úteis de fluxo usando uma sequência de procura de texto.

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

- **Barra de ferramentas de atividade de rede** – Na barra de ferramentas, um campo de **Filtro rápido** permite que você digite uma sequência de procura de texto e clique no ícone **Filtro rápido** para aplicar seu filtro rápido à lista de fluxos atualmente exibida.
- **Caixa de diálogo Incluir filtro** – Na caixa de diálogo **Incluir filtro**, que é acessada clicando no ícone **Incluir filtro** na guia **Atividade de rede**, é possível selecionar **Filtro rápido** como seu parâmetro de filtro e digitar uma sequência de procura de texto. Isso permite que você aplique seu filtro rápido à lista de fluxos atualmente exibida. Para obter mais informações sobre a caixa de diálogo **Incluir filtro**, consulte Procuras de dados.
- **Páginas de procura de fluxo** – Na páginas de procura de fluxo, você pode incluir um Filtro Rápido à 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 o último modo de intervalo, é possível digitar apenas palavras ou frases simples no campo **Filtro rápido**. Ao visualizar o fluxo 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 espera localizar na carga útil. Por exemplo, `Firewall`
- Inclua vários termos entre aspas duplas para indicar que você deseja procurar pela 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 frase ou palavra da carga útil. Por exemplo, o termo de procura user corresponde a user_1 e user_2, mas não corresponde 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 ("URL acessada" OR "Negar udp src") AND 10.100.100.*)`

  Ao criar critérios de procura que incluem a expressão lógica NOT, você deverá incluir pelo menos um outro tipo de expressão lógica, caso contrário, o seu filtro não retornará nenhum resultado. Por exemplo: `(%PIX* AND ("URL acessada" OR "Negar 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: `+ – && || ! () {} [] ^ " ~ * ? : \. For example: "%PIX\-5\-304001"`

Opções do menu ativado pelo botão direito

Na guia **Atividade de rede**, você pode clicar com o botão direito do mouse em um fluxo para acessar mais critérios de filtro de fluxo.

As opções do menu ativado pelo botão direito são:

Tabela 23. Opções do menu ativado pelo botão direito

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

Tabela 23. Opções do menu ativado pelo botão direito (continuação)

Opção	Descrição
Positivo Falso	Selecione esta opção para abrir a janela Ajuste positivo falso, que permite que você ajuste fluxos que são conhecidos por serem positivos falsos da criação de ofensas. 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. **Nota:** Esta opção não é exibida no modo de fluxo.

Barra de status

Quando fluxos de fluxo, a barra de status exibe o número médio de resultados que são recebidos por segundo.

Este é o número de resultados que o Console recebeu com êxito dos processadores de Eventos. Se o número for maior que 40 resultados por segundo, apenas 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 fluxo, a barra de status exibirá o número de resultados da procura que são atualmente exibidos e a quantidade de tempo que é necessário para processar os resultados da procura.

Registros de estouro

Com permissões administrativas, você pode especificar o número máximo de fluxos que você deseja enviar a partir do QRadar QFlow Collector para os processadores de Eventos.

Se você tiver permissões administrativas, poderá especificar o número máximo de fluxos que desejar 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 são agrupados em um registro de fluxo. Esse registro de fluxo é, então, exibido na guia **Atividade de Rede** com um endereço IP de origem 127.0.0.4 e um endereço IP de destino 127.0.0.5. Este registro de fluxo especifica o Estouro na guia **Atividade de rede**.

Monitoramento da atividade de rede

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

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

Se tiver configurado anteriormente uma procura salva 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 evento e fluxo.

Visualizando fluxos de fluxo

O modo permite que você visualize os dados de fluxo inserido no seu sistema. Este modo fornece a você uma visualização em tempo real de sua atividade de 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 nos fluxos agrupados ou no 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 os 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, em seguida, exibido na guia **Atividade de rede**.

Sobre Esta Tarefa

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

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

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

Tabela 24. 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 **Limpar filtro**. **Nota:** Este parâmetro só será exibido após você aplicar um filtro.
Visualização	Na caixa de listagem, você pode selecionar o intervalo de tempo que você deseja filtrar.

Tabela 24. Parâmetros para a guia atividade de rede (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: **Nota:** Clique na seta ao lado de Estatísticas Atuais para exibir ou ocultar as estatísticas. • **Resultados totais** – Especifica o número total de resultados que correspondeu ao seu critério de procura. • **Arquivos de dados procurados** – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • **Arquivos de dados compactados procurados** – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • **Contagem de arquivo de índice** – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas atuais são úteis para a resolução de problemas. Quando você contata o Suporte ao Cliente para solucionar problemas de fluxos, você pode ser solicitado a fornecer informações de estatística atuais.
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e a opção de agrupamento. Clique em **Ocultar gráficos** se deseja remover os gráficos de sua exibição. Os gráficos apenas serão exibidos após você selecionar um 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. **Nota:** 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 os gráficos, você deve remover a extensão do navegador bloqueadora de anúncios. Para obter informações adicionais, consulte a documentação do navegador.
Offense icon	Clique no ícone **Ofensas** para visualizar detalhes da ofensa associada a este fluxo.
Flow Type	Especifica o tipo de fluxo. Os tipos de fluxo são medidos pela razão entre as atividades recebidas e as atividades de saída. Os tipos de fluxo incluem: • **Fluxo padrão** – Tráfego bidirecional • **Tipo A** – Um para Muitos (unidirecional), por exemplo, um único host que executa uma varredura de rede. • **Tipo B** – Muitos para um (unidirecional), por exemplo, um ataque do DoS Distribuído (DDoS). • **Tipo C** – Um para um (unidirecional), por exemplo, um host para host de varredura de porta.
Horário do Primeiro Pacote	Especifica a data e hora em que o fluxo é recebido.
Storage time	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.
Source Bytes	Especifica o número de bytes enviados do host de origem.
Destination Bytes	Especifica o número de bytes enviados do host de destino.
Total Bytes	Especifica o número total de bytes associados ao fluxo.
Source Packets	Especifica o número total de pacotes enviados do host de origem.
Destination Packets	Especifica o número total de pacotes enviados do host de destino.
Total Packets	Especifica o número total de pacotes associados ao fluxo.
Protocolo	Especifica o protocolo associado ao fluxo.
Aplicativo	Especifica o aplicativo detectado do fluxo. Para obter mais informações sobre detecção de aplicativo, consulte o *IBM Security QRadar Application*.
ICMP Type/Code	Especifica o tipo de Internet Control Message Protocol (ICMP) e o código, se aplicável. Se o fluxo tem o tipo ICMP e informações de código em um formato conhecido, este campo será exibido como Tipo <A>. Código <B>, em que <A> e <B> são os valores numéricos do tipo e código.

Tabela 24. Parâmetros para a guia atividade de rede (continuação)

Parâmetro	Descrição
Source Flags	Especifica os sinalizadores do Protocolo de Controle de Transmissão (TCP) detectados no pacote de origem, se aplicável.
Destination Flags	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 permite que uma rede forneça vários níveis de serviço para os fluxos. O QoS fornece os seguintes níveis de serviço básico: • **Melhor esforço** – Este nível de serviço não garante a entrega. A entrega do fluxo é considerada o melhor esforço. • **Serviço diferenciado** – Parte dos fluxos é prioridade concedida sobre outros fluxos. Esta prioridade é concedida pela classificação do tráfego. • **Serviço garantido** – O nível de serviço garante a reserva de recursos de rede para determinados fluxos.
QoS de Destino	Especifica o nível de QoS de serviço para o fluxo de destino.
Flow Source	Especifica o sistema que detectou o fluxo.
Flow Interface	Especifica a interface que recebeu o fluxo.
Índice If de Origem	Especifica o número da interface de origem de índice (IFIndex).
Índice If de Destino	Especifica o número IFIndex de destino.
ASN de Origem	Especifica o valor do número de sistema autônomo (ASN) de origem.
ASN de Destino	Especifica o valor ASN de destino.

Procedimento

1. Clique na guia **Atividade de Rede**.
2. Na caixa de listagem **Exibir**, 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 você deseja visualizar em maiores 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 que deseja para os 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 o critério de procura não agrupado, esta opção será exibida.

A caixa de listagem **Exibir** fornece as opções a seguir:

Tabela 25. Opções de fluxo agrupado

Opção de grupo	Descrição
Fluxos unidos	Exibe vários fluxos em um padrão ininterrupto em vários intervalos, em um registro único. 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 de fluxos agrupados pelo endereço IP associado ao fluxo.
IP de Origem	Exibe uma lista resumida de fluxos agrupados pelo endereço IP de origem do fluxo.
IP de Destino	Exibe uma lista resumida de fluxos agrupados pelo endereço IP de destino do fluxo.

Tabela 25. Opções de fluxo agrupado (continuação)

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

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

Tabela 26. Parâmetros de fluxo agrupado

Cabeçalho	Cabeçalho
Agrupar por	Especifica o parâmetro pelo qual a procura é agrupada.
Filtros Atuais	A parte superior da tabela exibe os detalhes do filtro aplicado aos resultados da procura. Para limpar esses valores de filtro, clique em **Limpar filtro**.
Visualização	Na caixa de listagem, selecione o intervalo de tempo que você deseja filtrar.
Estatísticas Atuais	Quando não em Tempo Real (fluxo) ou no modo de Último Minuto (atualização automática), as estatísticas atuais são exibidas, incluindo: **Nota:** Clique na seta ao lado de **Estatísticas atuais** para exibir ou ocultar as estatísticas. • **Resultados totais** – Especifica o número total de resultados que correspondeu ao seu critério de procura. • **Arquivos de dados procurados** – Especifica o número total de arquivos de dados procurados durante o período de tempo especificado. • **Arquivos de dados compactados procurados** – Especifica o número total de arquivos de dados compactados procurados dentro do período de tempo especificado. • **Contagem de arquivo de índice** – Especifica o número total de arquivos de índice procurado durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas Atuais são úteis para a resolução de problemas. Quando você contata o Suporte ao Cliente para solucionar problemas de fluxos, você pode ser solicitado a fornecer informações de estatística atuais.
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em **Ocultar gráficos** se deseja remover o gráfico de sua exibição. Os gráficos apenas serão exibidos após você selecionar um 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. **Nota:** 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 os gráficos, você deve remover a extensão do navegador bloqueadora de anúncios. Para obter informações adicionais, 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 este 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 26. Parâmetros de fluxo agrupado (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 múltiplas redes de destino associadas a este fluxo, esse campo especificará o termo Múltiplas e o número de redes.
Aplicativo (contagem exclusiva)	Especifica o aplicativo detectado dos fluxos. Se houver múltiplos aplicativos associados a este fluxo, este campo especificará o termo Múltiplos 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 de destino.
Total de Bytes (soma)	Especifica o número total de bytes associados ao fluxo.
Pacotes de origem (soma)	Especifica o número de pacotes de origem.
Pacotes de origem (soma)	Especifica o número de pacotes de origem.
Pacotes de origem (soma)	Especifica o número de pacotes de origem.
Pacotes de destino (soma)	Especifica o número de pacotes de destino.
Total de pacotes (soma)	Especifica o número total de pacotes associados 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 deseja agrupar o 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 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 os parâmetros 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 em grupos de fluxo. No modo escolhido para visualizar fluxos de mensagens, é possível localizar e visualizar os detalhes de um único fluxo.

A página de detalhes do fluxo fornece as seguintes informações:

Tabela 27. Detalhes do fluxo

Parâmetro	Descrição
Informações do fluxo	
Protocolo	Especifica o protocolo que está associado a este fluxo.
Aplicativo	Especifica o aplicativo detectado do fluxo. Para obter mais informações sobre detecção de aplicativo, consulte o *IBM Security QRadar Application*.
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 a relevância, consulte o Glossário.
Gravidade	Especifica a severidade deste fluxo. Para obter mais informações sobre severidade, consulte o Glossário.
Credibilidade	Especifica a credibilidade deste fluxo. Para obter mais informações sobre credibilidade, consulte o Glossário.

Tabela 27. Detalhes do fluxo (continuação)

Parâmetro	Descrição
Horário do Primeiro Pacote	Especifica o horário de início do fluxo, conforme relatado pela fonte de fluxo. Para obter mais informações sobre fontes de fluxo, consulte o *Guia de Administração* do seu produto.
Horário do Último Pacote	Especifica o horário de encerramento do fluxo, conforme relatado pela fonte de fluxo.
Horário de 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 *Guia de Administração* do seu produto.
Descrição do Evento	Especifica uma descrição do fluxo, se disponível.
Informações de origem e destino	
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 os ativos, consulte Gerenciamento de ativos.
Origem de IPv6	Especifica o endereço IPv6 de origem do fluxo.
Destino de IPv6	Especifica o endereço IPv6 de 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 de QoS para o 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. **Nota:** Se este fluxo possuir registros duplicados a partir de várias fontes de fluxo, os números ASN de origem correspondentes serão listados.
ASN de Destino	Especifica o número ASN de destino. **Nota:** Se este fluxo possuir registros duplicados a partir de várias fontes de fluxo, os números ASN de destino correspondentes serão listados.
Índice If de Origem	Especifica o número IFIndex de origem. **Nota:** Se este fluxo tiver registros duplicados a partir de várias fontes de fluxo, os números IFIndex de origem correspondentes serão listados.
Índice If de Destino	Especifica o número IFIndex de destino. **Nota:** Se este fluxo tiver registros duplicados a partir de várias fontes 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.
Informações de carga útil	
Carga Útil de Origem	Especifica o conteúdo de carga útil de origem do fluxo. Esse campo oferece três formatos para visualizar a carga útil: • Formato de Transformação Universal (UTF) – Clique em UTF. • Hexadecimal - Clique em HEX. • Base64 – Clique em Base64. **Nota:** Se seu fluxo de origem for Netflow v9 ou IPFIX, os campos não analisados dessas origens poderão ser exibidos no campo **Carga útil de origem**. O formato do campo não analisado é <name>=<value>. Por exemplo, `MN_TTL=x`
Carga Útil de Destino	Especifica o conteúdo de carga útil de destino do fluxo. Esse campo oferece três formatos para visualizar a carga útil: • Formato de Transformação Universal (UTF) – Clique em **UTF**. • Hexadecimal - Clique em **HEX**. • Base64 - Clique em **Base64**.
Informações adicionais	

Tabela 27. Detalhes do fluxo (continuação)

Parâmetro	Descrição
Flow Type	Especifica o tipo de fluxo. Os tipos de fluxo são medidos pela razão entre as atividades recebidas e as atividades de saída. Os tipos de fluxo incluem: • Padrão – Tráfego bidirecional • Tipo A – Muitos para único (unidirecional) • Tipo B – Muitos para único (unidirecional) • Tipo C – Único para único (unidirecional)
Flow Direction	Especifica a direção do fluxo. Direções de fluxo incluem: • L2L - Tráfego interno de uma rede local para outra rede local. • L2R - Tráfego interno de uma rede local para uma rede remota. • R2L - Tráfego interno de uma rede remota para uma rede local. • R2R - Tráfego interno de uma rede remota para outra rede remota.
Custom Rules	Especifica regras customizadas que correspondam a este fluxo. Para obter mais informações sobre as regras, consulte o *Guia de Administração* do seu produto.
Regras Customizadas Parcialmente Correspondidas	Especifica as regras customizadas que correspondem parcialmente a este fluxo.
Fonte/Interface de Fluxo	Especifica o nome da fonte de fluxo do sistema que detectou o fluxo. **Nota:** Se este fluxo possuir registros duplicados de várias fontes de fluxo, as fontes de fluxo correspondentes serão listadas.
Annotations	Especifica a anotação ou notas deste fluxo. Anotações são descrições de texto que as regras podem incluir automaticamente para fluxos como parte da resposta da regra.

Barra de ferramentas Detalhes do fluxo

A barra de ferramentas Detalhes do fluxo fornece várias funções.

A barra de ferramentas Detalhes do fluxo fornece as seguintes funções

Tabela 28. Descrição da barra de ferramentas detalhes do fluxo

Função	Descrição
Retornar para resultados	Clique em **Retornar para resultados** para retornar para a lista de fluxos.
Extrair Propriedade	Clique em **Extrair propriedade** para criar uma propriedade de fluxo customizada a partir do fluxo selecionado. Para obter mais informações, consulte Propriedades de evento r fluxo customizadas.
Positivo Falso	Clique em **Positivo falso** para abrir a janela Ajuste de positivo falso, que permite descartar os fluxos que são conhecidos por serem falsos positivos de criarem ofensas. Esta opção está desativada no modo de fluxo. Consulte Exportando fluxos.
Anterior	Clique em **Anterior** para visualizar o fluxo anterior na lista de fluxo.
Avançar	Clique em **Avançar** para visualizar o próximo fluxo na lista de fluxo.
Imprimir	Clique em **Imprimir** para imprimir os detalhes do fluxo.
Ofensa	Se a **Ofensa** estiver disponível, clique para visualizar a página Resumo da Ofensa.

Ajustando positivos falsos

Você pode usar a função Ajuste Positivo Falso para evitar fluxos de positivo falso de criar ofensas. Você pode ajustar os fluxos positivos falsos na lista de fluxos ou na página de detalhes de fluxos.

Sobre Esta Tarefa

Nota: Você pode ajustar os fluxos positivos falsos na página de resumo ou detalhes.

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

Procedimento

1. Clique na guia **Atividade de Rede**.
2. Opcional. Se você estiver visualizando os fluxos no 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 Propriedade de evento/fluxo na janela Positivo falso, selecione uma das opções a seguir:
   - Evento/Fluxo(s) com um QID específico do <Evento>
   - Qualquer Evento/Fluxo(s) com uma categoria de nível inferior do <Evento>
   - Qualquer Evento/Fluxo(s) com uma categoria de nível superior do <Evento>
6. Na área de janela Direção do tráfego, selecione uma das opções a seguir:
   - <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 de Linguagem de Marcação Extensível (XML) ou Valores Separados por Vírgulas (CSV). O período de tempo necessário 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 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. Esta 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 Atividade de log. Esta 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 com suas atividades, clique em **Notificar quando estiver pronto**.

Resultados

Quando a exportação for concluída, você receberá uma notificação de que a exportação foi concluída. Se não foi selecionado 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.

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

Gerenciamento de gráfico

É possível usar as opções várias 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 fluxo.

Os gráficos não são exibidos enquanto estiver modo de fluxo.

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

Tipos de gráfico incluem:

- Gráfico de barras - Exibe de 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.
- Série Temporal – 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 suas configurações do gráfico serão retidas quando:

- 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:

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

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

Visão geral do gráfico de série

Gráficos de série temporal são representações gráficas de sua atividade com o tempo.

Picos e vales que são exibidos nos gráficos representam a atividade de volume alto e baixo. Os gráficos de série tempotal são úteis para tendência de dados acurto e longo prazo.

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

Nota: Você deve ter permissões de função apropriada para gerenciar e visualizar gráficos de série temporal.

Para exibir gráficos de série temporal, você deverá criar e salvar uma procura que inclui séries temporais e opções de agrupamento. Você pode salvar até 100 procuras de série temporal.

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

É possível identificar facilmente as procuras salvas de série temporal no menu **Procuras rápidas**, porque o nome da procura é anexado com o 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 para os resultados da procura. Se um gráfico de série temporal não exibir automaticamente para seus critérios de procura não salva, nenhum critério de procura salva anteriormente existirá para corresponder a seus parâmetros de procura. Se isso ocorrer, você deverá ativar a captura de dados da série temporal e salvar seus critérios de procura.

Você pode ampliar e varrer 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 29. Funções de gráficos de série temporal

Função	Descrição
Visualizar dados em mais detalhes	Usando o recurso de zoom, é possível investigar segmentos de tempo menores de tráfego de evento. • Mova o ponteiro do mouse sobre o gráfico e, em seguida, use a roda do mouse para ampliar o gráfico (rolar a roda de rolagem do mouse para cima). • Realce a área do gráfico que você deseja ampliar. Quando você liberar o botão do mouse, o gráfico exibirá um segmento de tempo menor. Agora é possível clicar e arrastar o gráfico para varrê-lo. Quando você amplia um gráfico de série temporal, o gráfico é atualizado para exibir um segmento de tempo menor.
Visualizar um período de tempo maior de dados	Usando o recurso de zoom, é possível investigar segmentos de tempo maior ou retornar ao intervalo de tempo máximo. É possível expandir um intervalo de tempo usando uma das seguintes opções: • Clique em Reconfigurar Zoom no canto superior esquerdo do gráfico. • Mova o ponteiro do mouse sobre o gráfico e, em seguida, use a roda do mouse para expandir a visualização (rolar a roda de rolagem do mouse para baixo).

Tabela 29. Funções de gráficos de série temporal (continuação)

Função	Descrição
Varra o gráfico	Quando você tiver ampliado um gráfico de série temporal, você poderá clicar e arrastar o gráfico para a esquerda ou para a direita para varrer a linha de tempo.

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 legenda, você pode executar as ações a seguir:

- Mova o ponteiro do mouse sobre um item de legenda ou o 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 mais detalhadamente o item.
- Clique em um item de legenda de um gráfico de barras ou de pizza para ocultar os itens no gráfico. Clique no item de legenda novamente para mostrar os itens ocultos. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item.
- Clique em **Legenda** ou na seta ao lado, se desejar remover a legenda da exibição do gráfico.

Configurando gráficos

É possível usar as opções de configuração 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 de temporais.

Antes de Iniciar

Os gráficos não serão exibidos ao visualizar os eventos ou fluxos em modo de Tempo Real (fluxo). Para exibir gráficos, você deverá acessar a guia **Atividade de 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 critérios de procura de evento e 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 os dados para o período de tempo anterior. Após ativar a captura de dados de 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. Configurar valores para os parâmetros a seguir:

Opção	Descrição
Parâmetro	Descrição
Value to Graph	Na caixa de listagem, selecione o tipo de objeto que você deseja registrar em gráfico no eixo Y do gráfico. As opções incluem todos os parâmetros de eventos ou fluxo normalizados e customizados incluídos em seus parâmetros de procura.
Display Top	Na caixa de listagem, selecione o número de objetos que você deseja visualizar no gráfico. O padrão é 10. Representando o gráfico com mais de 10 itens pode fazer com que os dados do gráfico se tornem ilegíveis.
Chart Type	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 **Atualizar detalhes** para atualizar o gráfico e preencher os detalhes do evento
Capture Time Series Data	Selecione essa caixa de seleção, se você desejar ativar a captura de dados de séries temporais. Ao selecionar essa caixa de seleção, o recurso do gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, esta opção está desativada. Essa opção está disponível apenas nos gráficos Séries Temporais.
Time Range	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar. Essa opção está disponível apenas nos gráficos Séries Temporais.

4. Se você selecionou a opção de 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 **Atividade de log**, **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 procura salvo anteriormente. É possível selecionar, organizar e agrupar as colunas de dados a serem exibidas nos resultados da procura

Procuras de evento e de fluxo

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

Após executar uma procura, será possível salvar o critério de procura e os resultados da procura.

Procurando itens que correspondam com seus critérios

Você pode procurar dados que correspondam com seu critério de procura.

Sobre Esta Tarefa

Visto que o banco de dados inteiro será procurado, as procuras poderão demorar um longo tempo, dependendo do tamanho do seu banco de dados.

Você pode usar o parâmetro de procura **Quick Filter** para procurar itens que correspondam com a sequência 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 em Sintaxe de filtro rápido (fluxos).

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

Tabela 30. Opções de procura

Opções	Descrição
Grupo	Selecione um grupo de procura de evento ou Grupo de Procura de fluxo para visualizar na lista **Procuras salvas disponíveis**.
Digitar Procura Salva ou Selecionar a partir da Lista	Insira o nome de uma procura salva ou uma palavra-chave para filtrar a lista **Procuras salvas disponíveis**.
Procuras Salvas Disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você use as opções **Grupo ou inserir procura salva** ou **Selecionar da lista** para aplicar um filtro na lista. Você pode selecionar uma procura salva nessa lista para ser exibida ou editada.
Procura	O ícone **Procurar** está disponível em várias áreas de janela na página de procura. Você pode clicar em Procurar ao terminar de configurar a procura e desejar visualizar os resultados.
Incluir em Minhas Procuras Rápidas	Selecione essa caixa de seleção para incluir essa procura em seu menu **Procura rápida**.
Incluir em Meu Painel	Selecione essa caixa de seleção para incluir os dados de sua procura salva na guia **Painel**. Para obter mais informações sobre a guia **Painel**, consulte Gerenciamento de painel. **Nota:** Esse parâmetro será exibido somente se a procura estiver agrupada.
Configurar como padrão	Selecione essa caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar essa procura com todos os outros usuários.

Tabela 30. Opções de procura (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. **Nota:** Quando Tempo Real (fluxo) estiver ativado, não será possível agrupar seus resultados da procura. Se você selecionar qualquer opção de agrupamento no painel 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 **Atividade de log** e **Atividade de rede** são atualizadas em intervalos de um minuto para exibir as informações mais recentes.
Recente	Selecione um intervalo de tempo predefinido para sua procura. Após selecionar essa opção, você deverá 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, você deverá selecionar o intervalo de data e hora nos calendários **Horário de início** e **Horário de encerramento**.
Acumulação de Dados	Essa área de janela será exibida apenas ao carregar uma procura salva. Ativando as contagens exclusivas nos dados acumulados compartilhados com muitas outras procuras salvas e relatórios poderá diminuir o desempenho do sistema. Ao carregar uma procura salva, essa área de janela exibirá as opções a seguir: • Se nenhum dado estiver acumulando para essa procura salva, a mensagem informativa a seguir será exibido: `Dados não estão sendo acumulados para essa procura`. • Se os dados forem acumulados para essa procura salva, as opções a seguir serão exibidas: – **Colunas** – quando você clica ou passa o ponteiro do mouse sobre esse link, uma lista das colunas que está acumulando dados será aberta. – **Ativar contagens exclusivas/Desativar contagens exclusivas** – esse link permite que você ative ou desative os resultados da procura para exibir contagens de evento e fluxo exclusivas em vez de contagens médias ao longo do tempo. Após clicar no link **Ativar contagens exclusivas**, uma caixa de diálogo será aberta e indicará quais procuras salvas e relatórios compartilham os dados acumulados.
Filtros Atuais	Essa lista exibe os filtros aplicados a essa procura. As opções para incluir um filtro localizado acima da lista **Filtros atuais**.
Salvar resultados quando a procura for concluída	Selecione essa caixa de seleção para salvar e nomear os resultados da procura.
Exibir	Selecione essa lista para especificar uma coluna predefinida configurada para exibir nos resultados da procura.
Digitar Coluna ou Selecionar a partir da Lista	Você pode usar o campo para filtrar as colunas listadas na lista Colunas disponíveis. Insira o nome da coluna que você deseja localizar ou insira uma palavra-chave para exibir uma lista de nomes de colunas. Por exemplo, digite `Dispositivo` para exibir uma lista de colunas que inclua o Dispositivo no nome da coluna.
Colunas disponíveis	Essa lista exibe as colunas disponíveis. As colunas que estão atualmente em uso com essa procura salva estão destacadas e exibidas na lista **Colunas**.
Incluir e remover os ícones da coluna (conjunto superior)	Use o conjunto de ícones na parte superior para customizar a lista **Agrupar por**. • **Incluir coluna** - selecione uma ou mais colunas na lista **Colunas disponíveis** e clique no ícone **Incluir coluna**. • **Remover coluna** – selecione uma ou mais colunas na lista **Agrupar por** e clique no ícone **Remover coluna**.
Incluir e remover os ícones da coluna (conjunto inferior)	Use o conjunto inferior do ícone para customizar a lista **Colunas**. • **Incluir coluna** - selecione uma ou mais colunas na lista Colunas disponíveis e clique no ícone **Incluir coluna**. • **Remover coluna** – selecione uma ou mais colunas da lista Colunas e clique no ícone **Remover coluna**.

Tabela 30. Opções de procura (continuação)

Opções	Descrição
Agrupar por	Essa lista especifica as colunas nas quais a procura salva agrupa os resultados. Use as opções a seguir para customizar a lista adicional Agrupar por: • Mover para cima – selecione uma coluna e a mova para cima através da lista de prioridade usando o ícone **Mover para cima**. • Mover para baixo – selecione uma coluna e a mova para baixo através da lista de prioridade usando o ícone **Mover para baixo**. A lista de prioridade especifica em qual ordem os resultados são agrupados. Os resultados da procura são agrupados na primeira coluna na lista **Agrupar por** e, então, agrupados na próxima coluna na lista.
Colunas	Especifica as colunas que são escolhidos para a procura. Você pode selecionar mais colunas na lista **Colunas disponíveis**. Você pode customizar ainda mais a lista **Colunas**, usando as opções a seguir: • **Mover para cima** – move a coluna selecionada para cima na lista de prioridades. • **Mover para baixo** - move a coluna selecionada para baixo na lista de prioridades. Se o tipo de coluna for numérica ou baseada em tempo e houver uma entrada na lista **Agrupar por**, então a coluna incluirá uma caixa de listagem. Use a caixa de listagem para escolher como deseja agrupar a coluna. 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.
Ordenar por	Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura. Em seguida, na segunda caixa de listagem, selecione a ordem em que você deseja exibir para os resultados da procura. As opções incluem **Decrescente** e **Crescente**.
Limite de Resultados	Você pode especificar o número de linhas que um pesquisa retorna na janela Editar procura. O campo **Limite de resultados** também aparece na janela Resultados. • Para uma procura salva, o limite é armazenado na procura salva e reaplicado ao carregar a procura. • Ao classificar em uma coluna no resultado da procura que tem um limite de linha, a classificação será feita dentro das linhas limitadas mostradas na grade de dados. • Para um agrupamento por procura com o gráfico de séries temporais ativado, o limite da linha somente se aplica à grade de dados. O suspenso **Top N** no gráfico de séries temporais ainda controla quantas séries temporais são desenhadas no gráfico.

Procedimento

1. Escolha uma das opções a seguir:
   - Para procurar eventos, clique na guia **Atividade de log**.
   - Para fluxos de procura, clique na guia **Atividade de rede**.
2. Na caixa de listagem **Procurar**, selecione **Nova procura**.
3. Para selecionar uma procura salva anteriormente:
   a. Escolha uma das opções a seguir: `na lista Procuras salvas disponível, selecione a procura salva que você deseja carregar. No InserirProcura Salva ou Selecionar no campo Lista, insira o nome da procura que você deseja carregar.`
   b. Clique em **Carregar**.
   c. Na área de janela Editar procura, selecione as opções que você deseja para essa procura. Consulte a Tabela 1.
4. Para criar uma procura, na área de janela Intervalo de tempo, selecione as opções para o intervalo de tempo que você deseja capturar para essa procura.
5. Opcional. Na área de janela Acumulação de dados, ative as 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 contagens exclusivas, 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 as informações específicas relacionadas ao seu parâmetro de procura.
   d. Clique em **Incluir filtro**.
   e. Repita as etapas de a até 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, insira um nome para a procura salva.
8. Na área de janela Definição de coluna, defina o layout de colunas e as colunas que você deseja usar para visualizar os resultados:
   a. Na caixa de listagem **Exibir**, selecione a coluna pré-configurada definida para ser associada a essa procura.
   b. Clique na seta ao lado de **Definição de visualização avançada** para exibir os parâmetros de procura avançada.
   c. Customizar as colunas a serem exibidas nos resultados da procura. Consulte a Tabela 1.
   d. Opcional. No campo **Limites de Resultados**, insira o número de linhas que você deseja que a procura retorne.
9. Clique em **Filtrar**.

Resultados

O status **Em Progresso (<percentual>%Concluído)** será exibido no canto superior direito.

.

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

Quando a procura estiver concluída, 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 em 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 estará anexado com o intervalo de tempo especificado. Por exemplo, uma

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

Se você alterar uma coluna configurada 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 deseja designar a este critério de procura.
Designar procura ao(s) grupo(s)	Selecione a caixa de seleção para o grupo que você deseja designar 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 procura.
Gerenciar Grupos	Clique em **Gerenciar grupos** para gerenciar grupos de procura. Para obter mais informações, consulte Gerenciando grupos de procura.
Opções de Período de Tempo:	Escolha uma das opções a seguir: • **Tempo real (fluxo)** – selecione essa opção para filtrar os resultados da procura durante o modo de fluxo. • **Último intervalo (autoatualização)** - selecione essa opção para filtrar os resultados da procura durante o modo de autoatualização. As guias **Atividade de log** e **Atividade de rede** são atualizadas em intervalos de um minuto para exibir as informações mais recentes. • **Recente** – selecione essa opção e, nessa caixa de listagem, selecione o intervalo de tempo que você deseja filtrar. • **Intervalo específico** – selecione essa opção e, no calendário, selecione o intervalo de data e hora que você deseja filtrar.
Incluir em Minhas Procuras Rápidas	Selecione essa caixa de seleção para incluir essa procura na caixa de listagem **Procura rápida** na barra de ferramentas.

Opção	Descrição
Incluir em Meu Painel	Selecione essa caixa de seleção para incluir os dados de sua procura salva na guia **Painel**. Para obter mais informações sobre a guia **Painel**, consulte Gerenciamento de painel. **Nota:** Esse parâmetro será exibido somente se a procura estiver agrupada.
Configurar como padrão	Selecione essa caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione esta caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

5. Clique em **OK**.

Procuras da ofensa

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

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

Procurando ofensas nas páginas Minhas ofensas e Todas as ofensas

Nas páginas Minhas ofensas e Todas as ofensas do guia **Ofensa**, você pode procurar as ofensas que correspondam a seus critérios.

Sobre Esta Tarefa

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

Para obter informações sobre as categorias, consulte o *IBM Security QRadar Guia de Administração de Detecção de Anomalia de Rede*.

Tabela 31. Opções de procura da página Minhas ofensas e Todas os ofensas

Opções	Descrição
Grupo	Essa caixa de listagem permite que você selecione um Grupo de Procura de ofensa para visualizar na lista **Procuras salvas disponíveis**.
Digitar Procura Salva ou Selecionar a partir da Lista	Esse campo permite que você insira o nome de uma procura salva ou uma palavra-chave para filtrar a lista **Procuras salvas disponíveis**.
Procuras Salvas Disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você aplique um filtro à lista usando o Grupo ou Inserir Procura Salva ou Selecionar nas opções **Lista**. Você pode selecionar uma procura salva nessa lista para ser exibida ou editada.
Todos os Crimes	Essa opção permite que você procure todas as ofensas, independentemente do intervalo de tempo.
Recente	Essa opção permite que você selecione um intervalo de tempo predefinido que você deseje filtrar. Após selecionar essa opção, você deverá selecionar uma opção de intervalo de tempo na caixa de listagem.

Tabela 31. Opções de procura da página Minhas ofensas e Todas os ofensas (continuação)

Opções	Descrição
Intervalo Específico	Essa opção permite que você configure um intervalo de tempo customizado para sua procura. Após selecionar essa opção, você deverá selecionar uma das opções a seguir. • **Data de início entre** – selecione essa caixa de seleção para procurar 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 você deseja procurar. • **Último evento/fluxo entre** - selecione essa caixa de seleção para procurar as ofensas às quais o último evento detectado ocorreu dentro de um certo período de tempo. Após selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.
Procurar	O ícone **Procurar** está disponível em várias áreas de janela na página de procura. Você poderá clicar em **Procurar** ao concluir a configuração da procura e desejar visualizar os resultados.
ID do Crime	Nesse campo, você pode inserir o ID da ofensa a qual você deseja procurar.
Descrição	Nesse campo, você pode inserir a descrição a qual você deseja procurar.
Designado ao usuário	Nessa caixa de listagem, você pode selecionar o nome do usuário o qual você deseja procurar.
Orientação	Nessa caixa de listagem, você pode selecionar a direção da ofensa a qual você deseja procurar. As opções incluem: • Local para Local • Local para Remoto • Remoto para Local • Remoto para Remoto • Local para Remoto ou Local • Remoto para Remoto ou Local
IP de Origem	Nesse campo, você pode inserir o endereço IP de origem ou o intervalo do CIDR ao qual você deseja procurar.
IP de Destino	Nesse campo, você pode inserir o endereço IP de destino ou o intervalo do CIDR ao qual você deseja procurar.
Magnitude	Nessa caixa de listagem, você pode especificar uma magnitude e, em seguida, selecione para exibir apenas as ofensas com uma magnitude que seja igual a, menor que ou maior do que o valor configurado. O intervalo é de 0 – 10.
Gravidade	Nessa caixa de listagem, você pode especificar uma gravidade e, em seguida, selecione para exibir apenas as ofensas com uma gravidade que seja igual a, menor que ou maior do que o valor configurado. O intervalo é de 0 – 10.
Credibilidade	Nessa caixa de listagem, você pode especificar uma credibilidade e, em seguida, selecione para exibir apenas as ofensas com uma credibilidade que seja igual a, menor que ou maior do que o valor configurado. O intervalo é de 0 – 10.
Relevância	Nessa caixa de listagem, você pode especificar uma relevância e, em seguida, selecione para exibir apenas as ofensas com uma relevância que seja igual a, menor que ou maior do que o valor configurado. O intervalo é de 0 – 10.
Contém Nome de Usuário	Nesse campo, você pode inserir uma instrução de expressão regular (regex) para procurar as ofensas que contenham um nome de usuário específico. Ao definir os padrões regex customizado, siga para as regras de regex conforme definido pela linguagem de programação doJava™. Para obter mais informações, é possível consultar os tutoriais regex disponíveis na web.
Rede de Origem	Nessa caixa de listagem, você pode selecionar a rede de origem a qual você deseja procurar.
Rede de Destino	Nessa caixa de listagem, você pode selecionar a rede de destino a qual você deseja procurar.
Categoria de Alto Nível	Nessa caixa de listagem, você pode selecionar a categoria de nível superior a qual você deseja procurar. .
Categoria de Nível Baixo	Nessa caixa de listagem, você pode selecionar a categoria de nível inferior a qual você deseja procurar.

Tabela 31. Opções de procura da página Minhas ofensas e Todas os ofensas (continuação)

Opções	Descrição
Exclude	As opções nessa área de janela permitem que você exclua as ofensas dos resultados da procura. As opções incluem: • Crimes Ativos • Crimes Ocultos • Crimes Encerrados • Ofensas Inativas • Ofensa Protegida
Close by User	Esse parâmetro é exibido somente quando a caixa de seleção **Ofensas fechadas** estiver limpa na área de janela Excluir. Nessa caixa de listagem, você pode selecionar o nome do usuário que você deseja procurar as ofensas fechadas ou selecione `Quaisquer` para exibir todas as ofensas fechadas.
Reason For Closing	Esse parâmetro é exibido somente quando a caixa de seleção **Ofensas fechadas** estiver limpa na área de janela Excluir. Nessa caixa de listagem, você pode selecionar um motivo que você deseja procurar as ofensas fechadas ou selecione **Quaisquer** para exibir todas as ofensas fechadas.
Events	Nessa caixa de listagem, você pode especificar uma contagem de eventos e, em seguida, selecione para exibir apenas as ofensas com uma contagem de eventos que seja igual a, menor que ou maior do que o valor configurado.
Fluxos	Nessa caixa de listagem, você pode especificar uma contagem de fluxo e, em seguida, selecione para exibir apenas as ofensas com uma contagem de fluxo que seja igual a, menor que ou maior do que o valor configurado.
Total de Eventos/Fluxos	Nessa caixa de listagem, você pode especificar uma contagem total de fluxo e evento e, em seguida, selecione para exibir apenas as ofensas com um evento total e a contagem de fluxo que seja igual a, menor que ou maior do que o valor configurado.
Destinos	Nessa caixa de listagem, você pode especificar uma contagem de endereço IP de destino e, em seguida, selecione para exibir apenas as ofensas com uma contagem de endereço IP de destino que seja igual a, menor que ou maior do que o valor configurado.
Grupo de Fontes de Log	Nessa caixa de listagem, você pode selecionar um grupo de origem de log que contenha a origem de log que você deseja procurar. A caixa de listagem **Origens de log** exibe todas as origens de log designadas ao grupo de origem de log selecionado.
Origem de Log	Nessa caixa de listagem, você pode selecionar a origem de log que você deseja procurar.
Grupo de regras	Nessa caixa de listagem, é possível selecionar um grupo de regras que contenha a regra de contribuição pela qual você deseja procurar. A caixa de listagem **Regra** exibe todas as regras designadas ao grupo de regras selecionadas.
Regra	Nessa caixa de listagem, você pode selecionar a regra de contribuição que você deseja procurar.
Tipo de Crime	Nessa caixa de listagem, você pode selecionar um tipo de ofensa a qual você deseja procurar. Para obter mais informações sobre as opções na caixa de listagem **Tipo de ofensa**, consulte a Tabela 2.

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

Tabela 32. Opções de tipo de ofensa

Tipos de ofensas	Descrição
Quaisquer	Essa opção procura todas as origens de ofensa.
IP de Origem	Para procurar por ofensas com um endereço IP de origem específica, você pode selecionar essa opção e, em seguida, inserir o endereço IP de origem ao qual 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, inserir o endereço IP de destino ao qual você deseja procurar.

Tabela 32. Opções de tipo de ofensa (continuação)

Tipos de ofensas	Descrição
Nome do Evento	Para procurar por ofensas com um nome de evento específico, você pode clicar no ícone **Procurar** para abrir o Navegador de Eventos e selecionar o nome do evento (QID) que você deseja procurar. Você pode procurar um determinado QID usando uma das opções a seguir: • Para procurar um QID por categoria, selecione a caixa de seleção **Pesquisar por categoria** e selecione a categoria de nível superior ou inferior nas caixas de listagem. • Para procurar um QID por tipo de origem de log, selecione a caixa de seleção de Tipo **Pesquisar por origem de log** e selecione um tipo de origem de log na caixa de listagem **Tipo de origem de log**. • Para procurar um QID por tipo de origem de log, selecione a caixa de seleção **Pesquisar por tipo de origem de log** e selecione um tipo de origem de log na caixa de listagem **Tipo de origem de log**. • Para procurar um QID por nome, selecione a caixa de seleção **Procura de QID** e insira um nome no campo **QID/Nome**.
Nome do usuário	Para procurar por ofensas com um nome de usuário específico, você pode selecionar essa opção e, em seguida, inserir o nome do usuário ao qual 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, inserir o endereço MAC de origem ao qual 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, inserir o endereço MAC de destino ao qual você deseja procurar.
Origem de Log	Na caixa de listagem **Grupo de origem de log**, você pode selecionar o grupo de origem de log que contenha a origem de log a qual você deseja procurar. A caixa de listagem **Origens de log** exibe todas as origens de log designadas ao grupo de origem de log selecionado. Na caixa de listagem **Origens de log**, selecione a origem de log a qual você deseja procurar.
Nome do host	Para procurar por ofensas com um nome do host específico, você pode selecionar essa opção e, em seguida, inserir o nome do host ao qual vocêdeseja procurar.
Porta de Origem	Para procurar por ofensas com uma porta de origem específica, você pode selecionar essa opção e, em seguida, inserir a porta de origem a qual você deseja procurar.
Porta de Destino	Para procurar por ofensas com uma porta de destino específico, você pode selecionar essa opção e, em seguida, inserir a porta de destino a qual 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, inserir o endereço IPv6 de origem ao qual deseja procurar.
IPv6 de Destino	Para procurar por ofensas com um endereço IPv6 do destino específico, você pode selecionar essa opção e, em seguida, inserir o endereço IPv6 do destino ao qual você deseja procurar.
ASN de Origem	Para procurar por ofensas com um ASN de origem específico, você pode selecionar o ASN de origem na caixa de listagem **ASN de origem**.
ASN de Destino	Para procurar por ofensas com um ASN de destino específico, você pode selecionar o ASN de destino na caixa de listagem **ASN de destino**.
Regra	Para procurar por ofensas associadas a uma regra específica, você pode selecionar o grupo de regras que contenha a regra a qual você deseja procurar na caixa de listagem **Grupo da regras**. A caixa de listagem **Grupo da regras** exibe todas as regras designadas ao grupo de regras selecionado. Na caixa de listagem **Regra**, você seleciona a regra a qual você deseja procurar.
ID de app	Para procurar por ofensas com um ID de aplicativo, você pode selecionar o ID do aplicativo na caixa de listagem **ID do app**.

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, vá para a Etapa 4.

- Para criar uma nova procura, vá para a Etapa 7.

4. Selecione uma procura salva anteriormente usando uma das opções a seguir:
   - Na lista **Procuras salvas disponíveis**, selecione a procura salva que deseja carregar.
   - No campo **Inserir procura salva** ou **Selecionar da lista**, insira 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 essa procura como a procura padrão. Se você configurar essa procura como sua procura padrão, ela automaticamente executará e exibirá os resultados cada vez que você acessar a guia **Ofensas**.
7. Na área de janela Intervalo de tempo, selecione uma opção para o intervalo de tempo ao qual 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 da ofensa, especifique o tipo de ofensa e a origem da ofensa ao qual você deseja procurar:
   a. Na caixa de listagem, selecione o tipo de ofensa ao qual você deseja procurar.
   b. Insira 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 em que você deseja exibir os resultados da procura. As opções incluem Decrescente e Crescente.
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 de 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 da ofensa na página Por IP de origem:

Tabela 33. Opções de procura da página Por 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 essa opção e, nessa caixa de listagem, selecione o intervalo de tempo que você deseja procurar.

Tabela 33. Opções de procura da página Por IP de origem (continuação)

Opções	Descrição
Intervalo Específico	Para especificar um intervalo ao qual procurar, você pode selecionar a opção Intervalo específico e, em seguida, selecionar uma das opções a seguir: • **Data de início entre** – selecione essa caixa de seleção para procurar os endereços IP de origem associados às ofensas que iniciaram durante um determinado período de tempo. Após selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas as quais você deseja procurar. • **Último evento/fluxo entre** – selecione essa caixa de seleção para procurar os endereços IP de origem associados as ofensas para os 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 as quais você deseja procurar.
Procurar	O ícone **Procurar** está disponível em várias áreas de janela na página de procura. Você poderá clicar em **Procurar** ao concluir a configuração da procura e desejar visualizar os resultados.
IP de Origem	Nesse campo, você pode inserir o endereço IP de origem ou o intervalo do CIDR ao qual você deseja procurar.
Magnitude	Nessa 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 do que o valor configurado. O intervalo é de 0 – 10.
Risco de VA	Nessa caixa de listagem, você pode especificar um risco de VA e, em seguida, selecionar para exibir apenas as ofensas com um risco de VA que seja igual a, menor que ou maior do que o valor configurado. O intervalo é de 0 – 10.
Eventos/Fluxos	Nessa caixa de listagem, você pode especificar uma contagem de eventos ou fluxo e, em seguida, selecionar para exibir apenas as ofensas com uma magnitude que seja igual a, menor que ou maior do que o valor configurado.
Exclude	Você pode selecionar as caixas de seleção para as ofensas às quais você deseja excluir dos resultados da procura. As opções incluem: • **Crimes Ativos** • **Crimes Ocultos** • **Crimes Encerrados** • **Ofensas inativas** • **Ofensa protegida**

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 Intervalo de tempo, selecione uma opção para o intervalo de tempo ao qual 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 em que 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 em que 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 IP de destino

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

Sobre Esta Tarefa

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

Tabela 34. Opções de procura da página Por 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 essa opção e, nessa caixa de listagem, selecionar o intervalo de tempo ao qual você deseja procurar.
Intervalo Específico	Para especificar um intervalo específico ao qual procurar, você pode selecionar a opção **Intervalo específico** e, em seguida, selecionar uma das opções a seguir: • Para especificar um intervalo específico ao qual procurar, você pode selecionar a opção **Intervalo específico** e, em seguida, selecionar uma das opções a seguir: • **Último evento/fluxo entre** – selecione essa caixa de seleção para procurar os endereços IP de destino associados as ofensas para 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 as quais você deseja procurar
Procurar	O ícone **Procurar** está disponível em várias áreas de janela na página de procura. Você poderá clicar em **Procurar** ao concluir a configuração da procura e desejar visualizar os resultados.
IP de Destino	Você pode inserir o endereço IP de destino ou o intervalo do CIDR ao qual você deseja procurar.
Magnitude	Nessa 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 do que o valor configurado.
Risco de VA	Nessa caixa de listagem, você pode especificar um risco VA e, em seguida, selecionar para exibir apenas as ofensas com um risco de VA que seja igual a, menor que ou maior do que o valor configurado. O intervalo é de 0 – 10.
Eventos/Fluxos	Nessa caixa de listagem, você pode especificar uma magnitude de contagem de eventos ou fluxo e, em seguida, selecionar para exibir apenas as ofensas com uma contagem de eventos ou fluxo que seja igual a, menor que ou maior do 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 Intervalo de tempo, selecione uma opção para o intervalo de tempo ao qual 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 em que 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 em que 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 as ofensas agrupadas pelas redes associadas.

Sobre Esta Tarefa

A tabela a seguir descreve as opções de procura que você pode usar para procurar dados da ofensa na página Por redes:

Tabela 35. Opções de procura para dados de ofensa de procura na página Por redes

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

3. Clique em **Salvar critérios**.
4. Insira os valores para os parâmetros a seguir:

Opção	Descrição
Parâmetro	Descrição
Nome da Procura	Digite um nome que você deseja designar a esse critério de procura.
Gerenciar Grupos	Clique em **Gerenciar grupos** para gerenciar grupos de procura. Consulte Gerenciando grupos de pesquisa.
Opções de Período de Tempo:	Escolha uma das opções a seguir: • **Todas as ofensas** – selecione essa opção para procurar todas as ofensas, independentemente do intervalo de tempo. • **Recente** – selecione a opção e, nessa caixa de listagem, selecione o intervalo de tempo ao qual você deseja procurar. • **Intervalo específico** – Para especificar um intervalo específico para procurar, selecione a opção **Intervalo específico** e, em seguida, selecione uma das opções a seguir: `Data de início entre – selecione essa caixa de seleção para procurar ofensas que iniciou durante um determinado período de tempo. Após selecionar essa caixa de seleção, use as caixas de listagem para selecionar as datas que você deseja procurar.Último evento/fluxo entre – selecione essa caixa de seleção para procurar as ofensas às 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.`
Configurar como padrão	Selecione essa 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 com a procura salva poderão não funcionar. Os relatórios e as regras de detecção de anomalias 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 salvo estiverem associados a outros objetos, a janela Excluir procura salva será exibida. A janela lista os objetos que estejam 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 foram observados e edite os para remover ou substituir a associação com a procura salva excluída.

Usando uma subprocura para refinar resultados da procura

Você pode usar uma subprocura para procurar dentro de um conjunto de resultados de procuras concluídas. A subprocura é usada para refinar os resultados da procura, sem procurar no banco de dados novamente.

Antes de Iniciar

Ao definir uma procura que você deseja usar como base para uma 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 procuras agrupadas, procuras em andamento ou no 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 base. A área de janela Filtro doCurrent especifica os filtros aplicados a 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 base será reativada.

Se você excluir os critérios de procura de base para os critérios de subprocura salvos, você ainda terá acesso para os critérios de subprocura salvos. Se você incluir um filtro, a subprocura irá procurar o banco de dados inteiro visto que a função de procura não baseia mais a procura em um conjunto de dados procurados 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 em que 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.

Cancelando uma procura

Enquanto uma procura estiver na fila ou em andamento, você poderá cancelar a procura na página Gerenciar resultados da procura.

Sobre Esta Tarefa

Se a procura estiver em andamento ao ser 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. No 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 necessária, será possível excluir o resultado da procura 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 de procura que você 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 ofensa.

Esses grupos permitem que os critérios de procura salvos sejam localizados rapidamente nas guias **Atividade de log**, **Rede de atividade** e **Ofensas** e no assistente Relatório.

Visualizando grupos de procura

Um conjunto padrão de grupos e subgrupos está disponível.

Sobre Esta Tarefa

Você pode visualizar grupos de procura no Grupos de procura de eventos, Grupo de procura de fluxo ou as janelas do Grupo de procura de ofensas.

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 ofensa exibem os seguintes parâmetros para cada grupo.

Tabela 36. Parâmetros da janela grupo de procura

Parâmetro	Descrição
Nome	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.
Dados modificados	Especifica a data que o grupo de procura foi modificado.

A barra de ferramentas das janelas Grupos de procura de eventos, Grupo de procura de fluxo e Grupo de procura de ofensa fornece as seguintes funções.

Tabela 37. As funções da barra de ferramentas da janela Grupo de Procura

Função	Descrição
Novo grupo	Para criar um grupo de procura novo, você pode clicar em **Novo grupo**. Consulte Criando um grupo de procura novo.
Editar	Para editar um grupo de procura existente, é possível clicar em **Editar**. Consulte Editando um grupo de procura.

Tabela 37. As funções da barra de ferramentas da janela Grupo de Procura (continuação)

Função	Descrição
Copiar	Para copiar uma procura salva para outro grupo de procura, você pode clicar em **Copiar**. 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 deseja remover, e, em seguida, clique em **Remover**. 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. Visualização dos 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 ao qual você deseja criar o novo grupo.
5. Clique em **Novo grupo**.
6. No campo **Nome**, insira um nome exclusivo para o novo grupo.
7. Opcional. No campo **Descrição**, insira 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. Editar os parâmetros:
   - Insira um novo nome no campo **Nome**.
   - Insira uma nova descrição no campo **Descrição**.
7. Clique em **OK**.

Copiando uma procura salva em outro grupo

Você pode 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 você deseja copiar.
5. Clique em **Copiar**.
6. Na janela Grupos de itens, marque a caixa de seleção para o grupo para o qual 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 de 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 **Outro**.

Não é possível remover os seguintes grupos de seu 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 evento customizado

Use as propriedades de evento e fluxo customizadas 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. Ao criar uma propriedade customizada na página de Procura, a propriedade não é derivada de nenhum evento ou fluxo específico; portanto, 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 necessárias

Para criar propriedades customizadas se você tiver a permissão correta.

Você deve ter a permissão Propriedades do Evento Definidas pelo Usuário ou Propriedades de Fluxo Definidas pelo Usuário.

Se tiver permissões Administrativas, você também poderá criar e modificar as propriedades customizadas da guia Admin.

Clique em **Admin** > **Origens de Dados** > **Propriedades de Evento Customizado** > ou **Admin** > **Origens de Dados** > **Propriedades de Fuxo Customizado**.

Verifique com seu administrador para assegurar-se de que você possui as permissões corretas.

Para obter informações adicionais, consulte o Guia de Administração do*IBM Security QRadar Network Anomaly Detection*.

Tipos de propriedades customizadas

É possível criar um tipo de propriedade customizada.

Ao criar uma propriedade customizada, será possível optar por criar um Regex ou um tipo de propriedade calculado.

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

Por exemplo, um relatório é criado para relatar todos os usuários que fazem suas mudanças de permissão 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 de usuário real ou permissão 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).

O regex define o campo que deseja que se torne a propriedade customizada. Após digitar uma instrução regex, será possível validá-la com relação à carga útil. Ao definir padrões regex customizados, siga para as regras regex conforme definidas pela linguagem de programação Java.

Para obter mais informações, é possível consultar os 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 fluxo até que um padrão regex corresponda à carga útil. O primeiro padrão de regex a corresponder à carga útil do evento ou fluxo determina os dados a serem extraídos.

Usando propriedades customizadas baseadas no cálculo, é possível executar cálculos em propriedades de fluxo ou evento numérico existentes para produzir uma propriedade calculada.

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

Criando uma propriedade customizada baseada em regex

É possível criar uma propriedade customizada baseada em regex para corresponder cargas úteis de fluxo ou 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 38. 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 de 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. Ao 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 forem associadas a este evento, este campo especificará o termo Várias e o número de origens de log.

Tabela 38. Parâmetros da janela Propriedades de Evento Customizado (regex) (continuação)

Parâmetro	Descrição
RegEx	A expressão regular que você deseja usar para extrair os dados da carga útil. As expressões regulares fazem distinção entre maiúsculas e minúsculas. Os exemplos a seguir mostram expressões regulares de amostra: • Email: `(.+@[^\.].*\.[a-z]{2,}$)` • URL: `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • Nome de domínio: `(http[s]?://(.+?)["/?:])` • Número de pontos flutuante: `([-+]?\d*\.?\d*$)` • Número inteiro: `([-+]?\d*$)` • Endereço IP: `(\b\d{1,3}\. \ \d{1,3}. \ \d{1,3}. \b \d{1,3})` Grupos de captura devem estar entre parênteses.
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 limpar a caixa de seleção, essa propriedade customizada não será exibida nos 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 você estiver visualizando os eventos ou fluxos em modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento ou fluxo em que você 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 **Baseado 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, deve-se selecionar a propriedade customizada da lista de colunas disponíveis ao criar uma procura.

Criando uma propriedade customizada baseada em cálculo

Você pode criar uma propriedade customizada baseada em cálculo para corresponder às cargas úteis em uma expressão regular.

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 39. Parâmetros da janela de definição de propriedade customizada (cálculo)

Parâmetro	Descrição
Definição de Propriedade	
Nome da Propriedade	Insira 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	Insira uma descrição dessa propriedade customizada.
Definição de Cálculo da Propriedade	
Property 1	Na caixa de listagem, selecione a primeira propriedade que você deseja usar em seu cálculo. As opções incluem todas as propriedades normalizadas numéricas e customizadas numéricas. Você também pode especificar um valor numérico específico. Na caixa de listagem **Propriedade 1**, selecione a opção **Definido pelo usuário**. O parâmetro **Number Property** é exibido. Insira um valor numérico específico.
Operator	Na caixa de listagem, selecione o operador que você deseja aplicar as propriedades selecionadas no cálculo. As opções incluem: • Incluir • Subtrair • Multiplicar • Dividir
Property 2	Na caixa de listagem, selecione a segunda propriedade que você deseja usar em seu cálculo. As opções incluem todas as propriedades normalizadas numéricas e customizadas numéricas. Você também pode especificar um valor numérico específico. Na caixa de listagem **Propriedade 1**, selecione a opção **Definido pelo usuário**. O parâmetro **Number Property** é exibido. Insira um valor numérico específico.
Ativado	Selecione essa caixa de seleção para ativar essa propriedade customizada. Se você desmarcar a caixa de seleção, essa propriedade customizada não será exibida nos filtros de procura de evento ou fluxo ou em 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 você estiver visualizando os eventos ou fluxos em modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento ou fluxo no qual você deseja basear a propriedade customizada.
4. Clique em **Extrair propriedade**.
5. Na área de janela Seleção de Tipo de Propriedade, selecione a opção **Baseada 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 agora 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 deverá selecionar a propriedade customizada na 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 evento Customizado ou Propriedades de fluxo Customizado para modificar uma propriedade customizada.

As propriedades customizadas são descritas na tabela a seguir.

Tabela 40. Colunas da janela 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 de log para o qual essa propriedade customizada se aplica. Essa coluna é exibida somente na janela Propriedades de evento customizado.
Fonte de Log	Especifica a origem de 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 evento customizado.
Expressão	Especifica a expressão para essa propriedade customizada. A expressão depende do tipo da 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 41. Opções da barra de ferramentas da propriedade customizada

Opção	Descrição
Incluir	Clique em **Incluir** para incluir uma nova propriedade customizada.
Editar	Clique em **Editar** para editar a propriedade customizada selecionada.
Copiar	Clique em **Copiar** para copiar as propriedades customizadas selecionadas.
Excluir	Clique em **Excluir** para excluir as propriedades customizadas selecionadas.
Ativar/Desativar	Clique em **Ativar/Desativar** para ativar ou desativar as propriedades customizadas selecionadas para análise e visualização nos filtros de procura ou 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. Edite os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testá-la 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 poderá 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 você deseja copiar e clique em **Copiar**.
5. Edite os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testá-la com relação à carga útil.
7. Clique em **Salvar**.

Excluindo uma propriedade customizada

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

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 você deseja excluir e clique em **Excluir**.
6. Clique em **Sim**.

Capítulo 10. Gerenciamento de regra

Nas guias **Atividade do log**, **Atividade de rede** e **Ofensas**, você pode visualizar e manter as regras.

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

Considerações sobre permissão de regra

É possível visualizar e gerenciar regras para as áreas da rede a que você tem acesso, se você tiver as permissões de função do usuário Visualizar Regras Customizadas e Manter Regras Customizadas.

Para criar regras de detecção de anomalias, você deve 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 do Log, você deverá ter o **Atividade do log** > **Manter regra customizada**.

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

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 irá gerar uma resposta.

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

Categorias de regra

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

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

As regras de detecção de anomalia executam testes nos resultados de pesquisas salvas de evento ou fluxo como um meio de detectar quando os padrões de tráfego incomum ocorrerem em sua rede.

As regras de detecção de anomalia executam testes nos resultados de pesquisas salvas de evento ou fluxo como um meio de detectar quando os padrões de tráfego incomum ocorrerem em sua rede. Essa categoria de regra inclui os seguintes tipos de regra; anomalia, limite e comportamental.

Uma regra de anomalia testa o tráfego de evento e fluxo para a atividade anormal, como a existência de tráfego novo ou desconhecido, referente ao tráfego que cessa subitamente ou uma alteração de porcentagem na quantidade de tempo em que um objeto está ativo. Por exemplo, você pode criar uma regra de anomalias para

comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego durante a última hora. Se houver uma alteração de mais de 40%, a regra irá gerar uma resposta.

Uma regra de limite testa o tráfego de evento e fluxo para atividades que são menores, igual ou maior que um limite configurado ou dentro de um intervalo especificado. Os limites podem ser baseados em qualquer dado coletado. Por exemplo, você pode criar uma regra de limite, especificando que não mais de 220 clientes podem efetuar login no servidor entre 8h e 17h. A regra de limite gera um alerta quando o 221º cliente tenta efetuar login.

Uma regra comportamental testa o tráfego de evento e fluxo para mudanças no comportamento que ocorre em padrões sazonais regulares. Por exemplo, se um servidor de correio geralmente se comunica com 100 hosts por segundo durante a noite e, de repente, começa a se comunicar com 1.000 hosts por segundo, uma regra comportamental irá gerar 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 são processados em tempo real pelo processador de eventos. Você pode criar uma regra de evento para detectar um único evento (em certas propriedades) ou sequências de eventos. Por exemplo, se você desejar monitorar sua rede para tentativas de login malsucedidas, acessar vários hosts ou um evento de reconhecimento seguido por uma exploração, você poderá criar uma regra de evento. É comum para regras de evento criar ofensas como uma resposta.

Regra de fluxo

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

Regra comum

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

Regra de ofensa

Uma regra de ofensa processa ofensas apenas quando alterações são feitas na ofensa, como, quando novos eventos são incluídos ou o sistema planeja a reavaliação da ofensa. É comum para regras de ofensa enviar uma notificação por email como uma resposta.

Condições da regra

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

Com as funções, você pode usar blocos de construção e outras regras para criar um multievento, multifluxo ou função de multiofensas. Você pode conectar regras usando funções que suportam operadores booleanos, como OR e AND. Por exemplo, se desejar conectar regras de evento, você poderá usar quando um evento corresponder a qualquer | todas as seguintes funções de regras.

Um bloco de construção é uma regra sem uma resposta e é usado como uma variável comum em regras múltiplas ou para construir regras complexas ou lógicas que você deseja usar em outras regras. Você pode 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, você pode salvar um bloco de construção que inclui os endereços IP de todos os servidores de correio em sua rede e, então, usar esse bloco de construção para excluir esses servidores de correio 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 *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

Você pode executar testes na propriedade de um evento, fluxo ou de uma ofensa, como endereço IP de origem, gravidade de evento ou análise de taxa.

Respostas da regra

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

As regras podem gerar uma ou mais das seguintes respostas:

- Crie uma ofensa.
- Envie um email.
- Gere notificações do sistema no recurso do Painel.
- Inclua dados em conjuntos de referência.
- Inclua dados em coletas de dados de referência.
- Gere uma resposta para um sistema externo.
- Inclua dados em coletas de dados de referência que podem ser usados em testes de regras.

Tipos de coleta de dados de referência

Antes de poder configurar uma resposta da regra para enviar dados para uma coleta de dados de referência, você deve criar a coleta de dados de referência usando a interface da linha de comandos (CLI). 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 que mapeiam uma tecla para um valor. Por exemplo, para correlacionar a atividade do usuário em sua rede, você pode 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 que mapeiam uma tecla para vários valores. Por exemplo, para testar para acesso autorizado para uma patente, use uma propriedade de evento customizado para **Patent ID** como a chave e o parâmetro **Username** como o valor. Use um mapa de configurações para preencher uma lista de usuários autorizados.

Mapa de referência de mapas
Os dados são armazenados em registros que mapeiam uma chave para outra chave, que é, então, mapeada para um valor único. Por exemplo, para testar para violações de largura da banda da rede, você pode 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 chave, que é, então, mapeada para um valor único. A segunda chave possui um tipo designado. Esse mapeamento é semelhante a uma tabela de banco de dados em que cada coluna na tabela é associada a um tipo. Por exemplo, você pode 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 definido como **Tipo de IP** com o parâmetro **Source IP** ou **Source Port** como um valor. Você pode configurar a resposta de regra para incluir uma ou mais chaves definidas na tabela. Você também pode incluir valores customizados para a resposta da regra. O valor customizado deve ser válido para o tipo de chave secundária.

Nota: Para obter informações sobre os conjuntos de referência e a coleta de dados de referência, consulte o *Guia do Administrador* para 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 das **Ofensas**, **Atividade de Log** ou na guia **Atividade de rede**.

Sobre Esta Tarefa

A Página regras exibe uma lista de regras com seus parâmetros associados. Para localizar a regra a qual você deseja abrir e visualizar os detalhes, você pode usar a caixa de lista de grupos 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** na caixa de listagem **Regras** na barra de ferramentas.
   - Clique na guia **Atividade de rede** e, em seguida, selecione **Regras** na caixa de listagem **Regras** na barra de ferramentas.

2. Na caixa de listagem **Exibir**, selecione **Regras**.
3. Clique duas vezes na regra que deseja visualizar.
4. Revise os detalhes da regra.

Resultados

Se você tiver a permissão **Visualizar regras customizadas**, mas não tem a permissão **Manter regras customizadas**, a página **Resumo da regra** será exibida e a regra não poderá ser editada. Se você tiver a permissão **Manter regras customizadas**, a página **Editor de regra de teste de pilha** será exibida. Você pode revisar e editar os detalhes da regra.

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 deverá ter a permissão **Ofensas** > **Manter regras customizadas**.

Você pode testar regras localmente ou globalmente. Um teste local significa que a regra é testada no Processador de evento local e não é compartilhada com o sistema. Um teste global significa que a regra é compartilhada e testada por qualquer Processador de eventos no sistema. As regras globais enviam eventos e fluxos ao Processador de evento central que pode diminuir o desempenho no Processador de evento 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 Criem
4. Leia o texto de introdução no assistente Regra. Clique em **Avançar**.
5. Clique em **Avançar** para visualizar a página Editor de pilha de testes 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 desejar 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 bloco de construção**.
   b. Insira um nome exclusivo para esse bloco de construção.
   c. Clique em **Salvar**.
10. Na área de janela Grupos, marque as caixas de seleção dos grupos aos quais você deseja designar essa regra.
11. No campo **Notas**, insira uma nota que você deseja incluir para 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 Comum, consulte Tabela 44 na página 128
    - Para configurar as respostas para uma Regra de Ofensa, consulte Tabela 45 na página 131
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 anomalias

Use o assistente Regra de Detecção de Anomalias para criar regras que se aplicam aos critérios de intervalo de tempo, usando os testes de Data e Hora.

Antes de Iniciar

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

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

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

Sobre Esta Tarefa

Você deverá ter a permissão de função apropriada para poder criar uma regra de detecção de anomalias.

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

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

As regras de detecção de anomalias usam todos os critérios de filtro e agrupamento dos critérios de procura salvos em que a regra se baseia, mas não usam nenhum intervalo de tempo dos critérios de procura.

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

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

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 **Este teste de propriedade acumulada** da pilha de testes padrão. O valor **[group]** depende das opções de agrupamento especificadas nos critérios de procura salvos. Se diversas opções de agrupamento forem incluídas, o texto poderá ficar 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 Limite
   - Incluir Regra comportamental
4. Leia o texto de introdução no assistente Regra. Clique em **Avançar**. A regra que você escolheu anteriormente está selecionada.
5. Clique em **Avançar** para visualizar a página Editor de pilha de testes de regra.
6. No campo **digite o nome da regra aqui**, digite 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, digite 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 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**.

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 de grupos, marque as caixas de seleção dos grupos para os quais você deseja designar essa regra. Para obter mais informações, consulte Regra de gerenciamento de grupo.
10. No campo **Notas**, insira todas as notas que você deseja incluir nessa regra. Clique em **Avançar**.
11. Na página Respostas da regra, configure as respostas que você deseja que essa regra gere. "Parâmetros da página de Resposta de Regra" na página 128
12. Clique em **Avançar**.
13. Revise a regra configurada. Clique em **Concluir**.

Tarefas de gerenciamento de regra

Você pode gerenciar regras customizadas e de anomalia.

Você pode ativar e desativar regras, conforme necessário. Você também pode editar, copiar ou excluir uma regra.

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

Para gerenciar regras de detecção de anomalia criadas anteriormente e padrão, você deve 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 seu sistema irá gerar ofensas significativas para seu ambiente.

Sobre Esta Tarefa

Você deverá 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 deverá 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 desejar alterar o tipo de regra, clique em **Voltar** e selecione um novo tipo de regra.
7. Na página Editor de pilha de testes de regra, editar os parâmetros.
8. Clique em **Avançar**.
9. Na página Resposta da regra, editar os parâmetros.
10. Clique em **Avançar**.
11. Revise a regra editada. Clique em **Concluir**.

Copiando uma regra

É possível copiar uma regra existente, inserir um novo nome para a regra e, em seguida, customizar os parâmetros na nova regra, conforme necessário.

Sobre Esta Tarefa

Você deverá 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 campo Inserir nome para o 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 deverá 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 de grupo de regra

Se for um administrador, você estará apto a criar, editar e excluir grupos de regras. Categorizar suas regras ou blocos de construção em grupos permite que você visualize e rastreie suas regras de forma eficiente.

Por exemplo, você pode visualizar todas as regras que estão relacionadas à conformidade.

À medida que você cria novas regras, pode designar a regra para um grupo existente. Para obter informações sobre como designar um grupo usando o assistente de regra, consulte Criando um regra customizada ou Criando uma regra de detecção de anomalia.

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 o que deseja visualizar, se as regras ou blocos de construção.
4. Na caixa de listagem **Filtro**, 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 **Grupo**s.
4. Na árvore de navegação, selecione o grupo ao qual você deseja criar um novo grupo.
5. Clique em **Novo grupo**.
6. Insira 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 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

Você pode designar uma regra selecionada ou 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 a um grupo.
4. Na caixa de listagem **Ações**, selecione **Designar grupos**.
5. Selecione o grupo que você deseja designar ao bloco de regra ou 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. Atualize 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 uma regra ou um bloco de 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 a regra ou o bloco de construção que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo ao qual você deseja copiar a regra ou o bloco de 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 será excluído apenas do grupo; ele 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 o item que deseja excluir e selecione-o.
5. Clique em **Remover**.
6. Clique em **OK**.

Excluindo um grupo

Você pode excluir um grupo. Ao excluir um grupo, as regras ou os 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 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 que corresponda às necessidades de sua implementação.

Sobre Esta Tarefa

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

Por exemplo, você pode editar o BB:HostDefinition: bloco de construção dos Servidores de correio para identificar todos os servidores de correio na sua implementação. Em seguida, você pode 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 de página de regra

Uma descrição dos parâmetros na página Regras.

A lista de regras implementadas fornece as seguintes informações para cada regra:

Tabela 42. Parâmetros da página de regras

Parâmetro	Descrição
Rule Name	Exibe o nome da regra
Grupo	Exibe o grupo para o qual essa regra é 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 Anomalia.
Tipo de Regra	Exibe o tipo de regra. Tipos de regra incluem: • Evento • Fluxo • Comum • Ofensa • Anomalia • Limite • Comportamental 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 a ativação e desativação de regras, consulte Ativando e desativando regras.
Response	Exibe a resposta da regra, se houver. As respostas da regra incluem: • Enviar Novo Evento • Email • Notificação de Log • SNMP • Conjunto de referência • Dados de referência • Reposta IF-MAP Para obter mais informações sobre as respostas de regra, consulte Respostas de regra.
Contagem de Eventos/Fluxos	Exibe o número de eventos ou fluxos associados a esta regra quando a regra contribui para uma ofensa.
Contagem de Crimes	Exibe o número de ofensas que são geradas por essa regra.
Origin	Exibe se essa regra será uma regra padrão (Sistema) ou uma regra customizada (Usuário).
Data de Criação	Especifica a data e hora em que esta regra foi criada.
Data da Modificação	Especifica a data e hora em que esta regra foi modificada.

Barra de ferramentas da página de regras

Use a barra de ferramentas da página de Regras para exibir regras, blocos de construção ou grupos. Você pode gerenciar grupos de regras e trabalhar com regras.

A barra de ferramentas da página de Regras fornece as seguintes funções:

Tabela 43. Função da barra de ferramentas da página de regras

Função	Descrição
Exibir	Na caixa de listagem, selecione se deseja exibir regras ou blocos de construção na lista de regras.
Grupo	Na caixa de listagem, selecione qual grupo de regra você deseja que seja exibido na lista de regras.
Grupos	Clique em **Grupos** para gerenciar grupos de regra.

Tabela 43. Função da barra de ferramentas da página de regras (continuação)

Função	Descrição
Ações	Clique em **Ações** e selecione uma das opções a seguir: • **Nova Regra de Evento** – Selecione esta opção para criar uma nova regra de evento. • **Nova regra de fluxo** – Selecione esta opção para criar uma nova regra de fluxo. • **Nova regra comum** – Selecione esta opção para criar uma nova regra comum. • **Nova regra de ofensa** – Selecione esta opção para criar uma nova regra de ofensa. • **Ativar/desativar** – Selecione esta opção para ativar ou desativar as regras selecionadas. • **Duplicar** – Selecione esta opção para copiar uma regra selecionada. • **Editar** – Selecione esta opção para editar uma regra selecionada. • **Excluir** – Selecione esta opção para excluir uma regra selecionada. • **Designar grupos** – Selecione esta opção para designar regras selecionadas para grupos de regra.
Reverter regra	Clique em **Reverter regra** para reverter uma regra do sistema modificado para o valor padrão. Ao clicar em **Reverter regra**, uma janela de confirmação será exibida. Ao reverter uma regra, quaisquer modificações anteriores são removidas permanentemente. Para reverter a regra e manter uma versão modificada, duplicar a regra e usar a opção **Reverter regra** na regra modificada.
Regras de busca	Digite seus critérios de procura no campo **Regras de busca** e clique no ícone **Regras de busca** ou pressione Enter no teclado. Todas as regras que correspondem aos seus critérios de procura são exibidas na lista de regras. Os seguintes parâmetros são pesquisados para uma correspondência com seus critérios de procura: • Rule Name • Rule (description) • Notes • Response O recurso Regra de Busca tenta localizar uma correspondência de sequência de texto direto. Se nenhuma correspondência for localizada, o recurso Regra de Busca, em seguida, tentará uma correspondência de expressão comum (regex).

Parâmetros da página de Resposta de Regra

Há parâmetros para a página Resposta de regra.

A tabela a seguir fornece os parâmetros da página Resposta de regra.

Tabela 44. Parâmetros da página de Resposta de Regra Comum, de Evento e Fluxo

Parâmetro	Descrição
Gravidade	Selecione esta caixa de seleção caso deseje que essa regra configure ou ajuste a gravidade. Quando selecionada, você pode usar as caixas de listagem para configurar o nível de gravidade apropriado.
Credibilidade	Selecione esta caixa de seleção caso deseje que essa regra configure ou ajuste a credibilidade. Quando selecionada, você pode usar as caixas de listagem para configurar o nível de credibilidade apropriado.
Relevância	Selecione esta caixa de seleção caso deseje que essa regra para configure ou ajuste a relevância. Quando selecionada, você pode usar as caixas de listagem para configurar o nível de relevância apropriado.

Tabela 44. Parâmetros da página de Resposta de Regra Comum, de Evento e Fluxo (continuação)

Parâmetro	Descrição
Assegure-se de que o evento detectado seja parte de uma ofensa	Selecione essa caixa de seleção se você desejar que o evento seja redirecionado para o componente Magistrate. Se nenhuma ofensa existir na guia Ofensas, uma nova ofensa será criada. Se uma ofensa existir, esse evento será incluído à ofensa. Ao selecionar essa caixa de seleção, as seguintes opções são exibidas: **Ofensa do índice com base em** Na caixa de listagem, selecione o parâmetro na qual você desejar indexar a ofensa. O padrão é Origem IPv6. 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 de log, regra, IP de origem, IPv6 de origem, endereço MAC de origem, porta de origem ou nome de usuário. Para 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, IP de origem, identidade de IP de origem ou Porta de origem. Para regras comuns, as opções incluem IP de destino, identidade do IP de destino, porta de destino, regra, IP de origem, identidade do IP de origem e porta de origem. **Anote esta ofensa** Selecione esta caixa de seleção para incluir uma anotação para esta ofensa e digite a anotação. **Inclua eventos detectados por <index> a partir desse ponto em diante, por segundo(s), na ofensa** Selecione esta caixa de seleção e digite o número de segundos que você deseja para incluir eventos detectados por <index> na guia **Ofensas**. Este campo especifica o parâmetro no qual a ofensa é indexada. O padrão é IP de Origem.
Anotar evento	Selecione essa caixa de seleção se você desejar incluir uma anotação para este evento e digite a anotação que você deseja incluir no evento.
Descartar o evento detectado	Selecione esta caixa de seleção para forçar um evento, que normalmente é enviado para o componente Magistratura, a ser enviado para o banco de dados Ariel para relatar ou pesquisar. Este evento não é exibido na guia **Ofensas**.
Enviar Novo Evento	Selecione essa caixa de seleção para despachar um novo evento além do evento ou fluxo original, que é processado como todos os outros eventos no sistema. Selecione essa caixa de seleção para despachar um novo evento além do evento original, que é processado como todos os outros eventos no sistema. Os parâmetros **Despachar novo evento** são exibidos quando você seleciona essa caixa de seleção. Por padrão, a caixa de seleção não é selecionada.
Nome do Evento	Digite um nome exclusivo para o evento que você 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.
Gravidade	Na caixa de listagem, selecione a gravidade para o evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 0. A Gravidade 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. A Credibilidade é exibida na área de janela Anotação dos detalhes do evento.
Relevância	Na caixa de listagem, selecione a importância 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 você deseja que esta regra use ao processar eventos.
Categoria de nível inferior	Na caixa de listagem, selecione a categoria de evento de baixo nível que você deseja que esta regra use ao processar eventos.
Anote esta ofensa	Selecione esta caixa de seleção para incluir uma anotação para esta ofensa e digite a anotação.

Tabela 44. Parâmetros da página de Resposta de Regra Comum, de Evento e Fluxo (continuação)

Parâmetro	Descrição
Assegure-se de que o evento despachado seja parte de uma ofensa	Marque esta caixa de seleção se você desejar que, como resultado desta regra, o evento que é enviado para o componente Magistrate. Se nenhuma ofensa foi criada na guia de **Ofensas**, uma nova ofensa será criada. Se uma ofensa existir, esse evento será incluído. Ao selecionar essa caixa de seleção, as seguintes opções são exibidas: **Ofensa do índice com base em** Na caixa de listagem, selecione o parâmetro na qual você desejar indexar a ofensa. O padrão é IP de Origem. 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 de log, regra, IP de origem, IPv6 de origem, endereço MAC de origem, porta de origem ou nome de usuário. Para 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, IP de origem, identidade de IP de origem ou Porta de origem. Para regras comuns, as opções incluem IP de destino, identidade do IP de destino, porta de destino, regra, IP de origem, identidade do IP de origem e porta de origem. **Inclua eventos detectados por <index> a partir desse ponto em diante, por segundo(s), na ofensa** Selecione esta caixa de seleção e digite o número de segundos que você deseja para incluir eventos detectados por <index> na guia **Ofensas**. Este campo especifica o parâmetro no qual a ofensa é indexada. O padrão é IP de Origem. **Nomenclatura de Ofensas** Selecione uma das opções a seguir: **Estas informações devem contribuir para o nome da ofensa associada** Selecione esta opção se você desejar que as informações de Nome de Evento contribuam para o nome da ofensa. **Estas informações devem configurar ou substituir o nome da ofensa associada** Selecione esta opção se você desejar que o Nome do Evento configurado seja o nome da ofensa. **Estas informações não deveriam contribuir para a nomenclatura da ofensa associada** Selecione esta opção se não desejar que as informações de Nome de Evento contribuam para o nome da ofensa.
Email	Selecione essa caixa de seleção para exibir as opções de email. Por padrão, a caixa de seleção não é selecionada.
Insira endereços de email para notificar	Digite o endereço de email para enviar uma notificação se esta regra gerar. Use uma vírgula para separar vários endereços de email.
Trap SNMP	Esse parâmetro só é exibido quando os parâmetros de Configuração SNMP são configurados nas configurações do sistema. Selecione esta caixa de seleção para ativar esta regra para enviar uma notificação SNMP (trap). A saída do trap SNMP inclui o tempo do sistema, o trap OID e os dados de notificação, conforme definidos pelo MIB.
Enviar para syslog local	Selecione essa caixa de seleção se você desejar registrar o evento ou fluxo localmente. Por padrão, essa caixa de seleção fica limpa. **Nota:** Apenas os eventos normalizados podem ser registrados localmente em um dispositivo. Se quiser enviar dados de eventos brutos, você deverá usar a opção Enviar para Destinos de Encaminhamento para enviar os dados para um host syslog remoto.
Enviar para Destinos de Encaminhamento	Esta caixa de seleção é exibida apenas para regras de Evento. Selecione essa caixa de seleção se você desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema fornecedor, como SIEM, bilheteria ou sistemas de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento é exibida. Selecione a caixa de seleção para o destino de encaminhamento que você deseja enviar este evento ou fluxo. Para incluir, editar ou excluir um destino de encaminhamento, clique no link **Gerenciar destinos**.
Notificação	Selecione essa caixa de seleção se você desejar que os eventos que geram como resultado desta regra a ser exibida no item de Notificações do Sistema na guia Painel. Se você ativar notificações, configure o parâmetro do **Limitador de resposta**.

Tabela 44. Parâmetros da página de Resposta de Regra Comum, de Evento e Fluxo (continuação)

Parâmetro	Descrição
Incluir ao Conjunto de Referência	Selecione essa caixa de seleção se você desejar eventos que são gerados como resultado desta regra para incluir dados em um conjunto de referência. Para incluir dados em um conjunto de referência: 1. Usando a primeira caixa de listagem, selecione os dados que você deseja incluir. As opções incluem todos os dados normalizados ou customizados. 2. Usando a segunda caixa de listagem, selecione a referência que é configurada para o qual você deseja incluir os dados especificados. A resposta de regra **Incluir ao conjunto de referência** fornece as seguintes funções: **Atualizar** Clique em **Atualizar** para atualizar a primeira caixa de listagem para assegurar que a lista é atual. **Configurar Conjuntos de Referência** Clique em **Configurar Conjuntos de Referência** para configurar o conjunto de referência. Esta opção estará disponível apenas se você tiver permissões administrativas.
Incluir de Dados de Referência	Antes de poder usar essa resposta da regra, você deve criar a coleta de dados de referência usando a interface da linha de comandos (CLI). Para obter mais informações sobre como criar e usar as coletas de dados de referência, consulte o *Guia de Administração* para seu produto. Selecione essa caixa de seleção se você desejar que os eventos gerados como um resultado dessa regra sejam incluídos em uma coleta de dados de referência. Depois de selecionar a caixa de seleção, selecione uma das seguintes opções: **Incluir em um Mapa de Referência** Selecione esta opção para enviar dados para uma coleta de pares de valor múltiplo/chave única. Você deve selecionar a chave e o valor para o registro de dados e, em seguida, selecionar o mapa de referência que você deseja incluir ao registro de dados. **Incluir em um Mapa de Referência de Conjuntos** Selecione esta opção para enviar dados para uma coleta de pares de valor único/de chave. Você deve selecionar a chave e o valor para o registro de dados e, em seguida, selecionar o mapa de referência de conjuntos que você deseja incluir ao registro de dados. **Incluir em um Mapa de Referência de Mapas** Selecione esta opção para enviar dados para uma coleção de pares de valor único/chave múltipla. 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. Você também deve selecionar o mapa de referência de mapas que você deseja incluir ao registro de dados. **Incluir em uma Tabela de Referência** Selecione esta opção para enviar dados para uma coleta de pares de valor único/chave múltipla, onde um tipo foi designado para as chaves secundárias. Selecione a tabela de referência tal qual você deseja incluir dados, e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.
Publicar no IF-MAP Server	Se os parâmetros IF-MAP forem configurados e implementados nas definições do sistema, selecione esta opção para publicar as informações de evento sobre o servidor IF-MAP.
Limitador de Resposta	Selecione esta caixa de seleção e use as caixas de listagem para configurar a frequência na qual você deseja que esta regra responda.
Ativar Regra	Selecione essa caixa de seleção para ativar essa regra.

A tabela a seguir fornecerá os parâmetros de página Resposta de regra se o tipo de regra for Ofensa.

Tabela 45. Parâmetros da página de Resposta da Regra de Ofensa

Parâmetro	Descrição
Nomear/Anotar a ofensa detectada	Selecione essa caixa de seleção para exibir as opções de Nome.
Novo Nome de Ofensa	Digite o nome que deseja designar à ofensa.
Anotação da Ofensa	Digite a anotação da ofensa que você deseja que seja exibida na guia Ofensas.

Tabela 45. Parâmetros da página de Resposta da Regra de Ofensa (continuação)

Parâmetro	Descrição
Nome da Ofensa	Selecione uma das opções a seguir: **Estas informações devem contribuir para o nome da ofensa** Selecione esta opção se você desejar que as informações de Nome de Evento contribuam para o nome da ofensa. **Estas informações devem configurar ou substituir o nome da ofensa** Selecione esta opção se você desejar que o Nome do Evento configurado seja o nome da ofensa.
Email	Selecione essa caixa de seleção para exibir as opções de email.
Insira o endereço de email para notificar	Digite o endereço de email para enviar a notificação se o evento gerar. Use uma vírgula para separar vários endereços de email.
Trap SNMP	Esse parâmetro só é exibido quando os parâmetros de Configuração SNMP são configurados nas configurações do sistema. Selecione esta caixa de seleção para ativar esta regra para enviar uma notificação SNMP (trap). Para uma regra de ofensa, a saída de trap SNMP inclui o tempo do sistema, o trap OID e os dados de notificação, como definido pelo MIB.
Enviar para syslog local	Selecione essa caixa de seleção se você desejar registrar o evento ou fluxo localmente.
Enviar para Destinos de Encaminhamento	Selecione essa caixa de seleção se você desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema fornecedor, como SIEM, bilheteria ou sistemas de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento é exibida. Selecione a caixa de seleção para o destino de encaminhamento que você deseja enviar este evento ou fluxo. Para incluir, editar ou excluir um destino de encaminhamento, clique no link **Gerenciar destinos**.
Publicar no IF-MAP Server	Se os parâmetros IF-MAP forem configurados e implementados nas configurações do sistema, selecione esta opção para publicar as informações de ofensa sobre o servidor IF-MAP.
Limitador de Resposta	Selecione esta caixa de seleção e use as caixas de listagem para configurar a frequência com que você deseja que esta regra responda.
Ativar Regra	Selecione essa caixa de seleção para ativar essa regra. Por padrão, a caixa de seleção fica marcada.

A tabela a seguir fornecerá os parâmetros de página Regra de resposta se o tipo de regra for Anomalia.

Tabela 46. Parâmetros da página de Resposta de Regra de Detecção de Anomalias

Parâmetro	Descrição
Enviar Novo Evento	Especifica que esta regra despacha um novo evento além do fluxo ou evento original, 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 você 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 de Ofensas	Selecione uma das opções a seguir: **Estas informações devem contribuir para o nome da ofensa associada** Selecione esta opção se você desejar que as informações de Nome de Evento contribuam para o nome da ofensa. **Estas informações devem configurar ou substituir o nome da ofensa associada** Selecione esta opção se você desejar que o Nome do Evento configurado seja o nome da ofensa. **Estas informações não deveriam contribuir para a nomenclatura da ofensa associada** Selecione esta opção se não desejar que as informações de Nome de Evento contribuam para o nome da ofensa.
Gravidade usando as caixas de listagem, selecione a gravidade para o evento.	O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A Gravidade 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 importância 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 você deseja que esta regra use ao processar eventos.
Categoria de Nível Baixo	Na caixa de listagem, selecione a categoria de evento de baixo nível que você deseja que esta regra use ao processar eventos.
Anote esta ofensa	Selecione esta caixa de seleção para incluir uma anotação para esta ofensa e digite a anotação.

Tabela 46. Parâmetros da página de Resposta de Regra de Detecção de Anomalias (continuação)

Parâmetro	Descrição
Assegure-se de que o evento despachado seja parte de uma ofensa	Como resultado dessa regra, o evento é redirecionado para o componente Magistrate. Se uma ofensa existir, esse evento será incluído. Se nenhuma ofensa foi criada na guia Ofensas, uma nova ofensa é criada. As opções a seguir são exibidas: **Ofensa do índice com base em** Especifica que a nova ofensa é baseada no nome do evento. Este parâmetro é ativado por padrão. **Inclua eventos detectados por Nome do Evento a partir desse ponto em diante, por segundo, na ofensa** Selecione esta caixa de seleção e digite o número de segundos que você deseja incluir eventos detectados ou fluxos a partir da origem na guia **Ofensas**.
Email	Selecione essa caixa de seleção para exibir as opções de email.
Insira o endereço de email para notificar	Digite o endereço de email para enviar uma notificação se esta regra gerar. Use uma vírgula para separar vários endereços de email.
Insira o endereço de email para notificar	Digite o endereço de email para enviar uma notificação se esta regra gerar. Use uma vírgula para separar vários endereços de email.
Notificação	Selecione essa caixa de seleção se você desejar que os eventos que geram como um resultado desta regra sejam exibidos no item de Notificações do Sistema na guia **Painel**. Se você ativar notificações, configure o parâmetro do **Limitador de resposta**.
Enviar para syslog local	Selecione essa caixa de seleção se você desejar registrar o evento ou fluxo localmente. Por padrão, a caixa de seleção não é selecionada. **Nota:** Apenas os eventos normalizados podem ser registrados localmente em um dispositivo QRadar. Se quiser enviar dados de eventos brutos, você deverá usar a opção Enviar para Destinos de Encaminhamento para enviar os dados para um host syslog remoto.
Incluir ao Conjunto de Referência	Selecione essa caixa de seleção se você desejar eventos que são gerados como resultado desta regra para incluir dados em um conjunto de referência. Para incluir dados em um conjunto de referência: 1. Usando a primeira caixa de listagem, selecione os dados que você deseja incluir. As opções incluem todos os dados normalizados ou customizados. 2. Usando a segunda caixa de listagem, selecione o conjunto de referência no qual você deseja incluir os dados especificados. A resposta de regra **Incluir ao conjunto de referência** fornece as seguintes funções: **Atualizar** Clique em **Atualizar** para atualizar a primeira caixa de listagem para assegurar que a lista é atual. **Configurar Conjuntos de Referência** Clique em **Configurar Conjuntos de Referência** para configurar o conjunto de referência. Esta opção estará disponível apenas se você tiver permissões administrativas.

Tabela 46. Parâmetros da página de Resposta de Regra de Detecção de Anomalias (continuação)

Parâmetro	Descrição
Incluir de Dados de Referência	Antes de poder usar essa resposta da regra, você deve criar a coleta de dados de referência usando a interface da linha de comandos (CLI). Para obter mais informações sobre como criar e usar as coletas de dados de referência, consulte o *Guia de Administração* para seu produto. Selecione essa caixa de seleção se você desejar que os eventos gerados como um resultado dessa regra sejam incluídos em uma coleta de dados de referência. Depois de selecionar a caixa de seleção, selecione uma das seguintes opções: **Incluir em um Mapa de Referência** Selecione esta opção para enviar dados para uma coleta de pares de valor múltiplo/chave única. Você deve selecionar a chave e o valor para o registro de dados e, em seguida, selecionar o mapa de referência que você deseja incluir ao registro de dados. **Incluir em um Mapa de Referência de Conjuntos** Selecione esta opção para enviar dados para uma coleta de pares de valor único/de chave. Você deve selecionar a chave e o valor para o registro de dados e, em seguida, selecionar o mapa de referência de conjuntos que você deseja incluir ao registro de dados. **Incluir em um Mapa de Referência de Mapas** Selecione esta opção para enviar dados para uma coleção de pares de valor único/chave múltipla. 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. Você também deve selecionar o mapa de referência de mapas que você deseja incluir ao registro de dados. **Incluir em uma Tabela de Referência** Selecione esta opção para enviar dados para uma coleta de pares de valor único/chave múltipla, onde um tipo foi designado para as chaves secundárias. Selecione a tabela de referência tal qual você deseja incluir dados, e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.
Publicar no IF-MAP Server	Se os parâmetros IF-MAP forem configurados e implementados nas configurações do sistema, selecione esta opção para publicar as informações de ofensa sobre o servidor IF-MAP.
Limitador de Resposta	Selecione esta caixa de seleção e use as caixas de listagem para configurar a frequência com que você deseja que esta regra responda
Ativar Regra	Selecione essa caixa de seleção para ativar essa regra. Por padrão, a caixa de seleção fica marcada.

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"
```

A syslog output might resemble:

```
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 de perfil de ativos

Você pode localizar as descrições de parâmetro de página do perfil de ativos para a área de janela de Resumo de Ativo, Interface de Rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de Risco e de Produtos.

Essa referência inclui tabelas que descrevem os parâmetros exibidos em cada área de janela da guia **Perfil de ativo**.

Perfis de ativos

Os perfis de ativo fornecem informações sobre cada ativo conhecido em sua rede, incluindo quais serviços estão em execução em cada ativo.

As informações de perfil do ativo são usadas para finalidades de correlação para ajudar a reduzir positivos falsos. Por exemplo, se uma origem tentar explorar um serviço específico em execução em um ativo, em seguida, QRadar irá determinar se o ativo está vulnerável a este ataque pela correlação de ataque para o perfil de ativo.

Os perfis de ativos são descobertos automaticamente se você tiver varreduras dados de fluxo ou de avaliação de vulnerabilidades (VA) configuradas. Para o fluxo de dados preencher perfis de ativos, fluxos bidirecionais são necessários. Os 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 de Vulnerabilidade do *IBM Security QRadar*.

Para obter mais informações sobre fontes de fluxo, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

Sobre as vulnerabilidades

Você pode usar QRadar Vulnerability Manager e scanners de terceiros para identificar vulnerabilidades.

Scanners de terceiros identificam e relatam as vulnerabilidades descobertas usando referências externas, como o Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB) e Critical Watch. Exemplos de scanners de terceiros incluem QualysGuard e nCircle ip360. O OSVDB designa um identificador de referência exclusiva (ID do OSVDB) para cada vulnerabilidade. Referências externas designam um identificador de referência exclusiva para cada vulnerabilidade. Exemplos de IDs de referência de dados externos incluem ID de Commom Vulnerability and Exposures (CVE) ou ID de Bugtraq. Para obter mais informações sobre a avaliação de scanners e de vulnerabilidades, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

QRadar Vulnerability Manager é um componente que você pode adquirir separadamente e ativar usando uma chave de licença. QRadar Vulnerability Manager é uma plataforma de varredura de rede que fornece reconhecimento das vulnerabilidades existentes nos aplicativos, sistemas ou dispositivos em sua rede. Depois que as varreduras identificam vulnerabilidades, você pode procurar e revisar dados de vulnerabilidade, corrijir vulnerabilidades e executar novamente varreduras para avaliar o novo nível de risco.

Quando QRadar Vulnerability Manager for ativado, você pode executar tarefas de avaliação de vulnerabilidades na guia **Vulnerabilidades**. Na guia **Ativos**, você pode executar varreduras nos ativos selecionados.

Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*

Visão geral da guia Ativos

A guia **Ativos** fornece a você uma área de trabalho a partir da qual você pode gerenciar seus ativos de rede e investigar as vulnerabilidades de ativo, portas, aplicativos, histórico e outras associações.

Usando a guia **Ativos**, você pode:

- Visualizar todos os ativos descobertos.
- Inclua perfis de ativos manualmente.
- Procure ativos específicos.
- Visualize informações sobre os ativos descobertos.
- Edite perfis de ativos para ativos manualmente incluídos ou descobertos.
- Ajuste vulnerabilidades de positivo falso.
- Importe os ativos.
- Imprima ou exporte perfis de ativo.
- Descubra ativos.
- Configure e gerencie varredura de vulnerabilidade de terceiros.
- Inicie varreduras de Gerenciador de Vulnerabilidade QRadar.

Para obter informações sobre a opção Discovery Server na área de janela de navegação, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

Para obter mais informações sobre a opção Varrer VA na área de janela de navegação, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

Lista da guia Ativo

A página Perfis de ativos fornece informações sobre ID, endereço IP, nome do ativo, Agregar pontuação CVSS, Vulnerabilidades e Serviços.

A página Perfis de ativos fornece as seguintes informações sobre cada ativo:

Tabela 47. Parâmetros de página do Perfil de Ativos

Parâmetro	Descrição
ID	Exibe o número do ID do Ativo do ativo. O número do ID de Ativo é automaticamente gerado quando você inclui um perfil de ativo manualmente ou quando os ativos são descobertos através de fluxos, eventos ou varreduras de vulnerabilidade.
Endereço IP	Exibe o último endereço IP conhecido do ativo.
Nome do ativo	Exibe o nome fornecido, nome NetBios, nome DSN ou o endereço MAC do ativo. Se desconhecido, esse campo exibe o último endereço IP conhecido. **Nota:** Estes valores são exibidos em ordem de prioridade. Por exemplo, se o ativo não possuir um dado nome, o nome agregado do NetBios será exibido. Se o ativo for descoberto automaticamente, esse campo será preenchido automaticamente, no entanto, você poderá editar o nome do ativo, se necessário.

Tabela 47. Parâmetros de página do Perfil de Ativos (continuação)

Parâmetro	Descrição
Pontuação de risco	Exibe uma das seguintes pontuações Common Scoring Vulnerability System (CVSS): • Pontuação CVSS ambiental agregada • Agregar pontuação CVSS temporal • Agregar pontuação base CVSS • Essas pontuações são exibidas em ordem de prioridade. Por exemplo, se a pontuação CVSS ambiental agregado não estiver disponível, a pontuação CVSS temporal agregada será exibida. Uma pontuação CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades. A pontuação CVSS é calculada dos parâmetros definidos pelo usuário a seguir: • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade Para obter mais informações sobre como configurar esses parâmetros, consulte “Incluindo ou editando um perfil ativo” na página 139. Para obter mais informações sobre CVSS, consulte http://www.first.org/cvss/ .
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.

Opções do menu ativado pelo botão direito

Clicando com o botão direito do mouse em um ativo na guia Ativos exibirá os menus Navegar, Informações e Executar Varredura QVM para obter mais informações sobre filtro de eventos.

Na guia **Ativos**, você pode clicar com o botão direito do mouse em um ativo para acessar mais informações de filtro de evento.

Tabela 48. Opções do menu ativado pelo botão direito

Opção	Descrição
Navegar	O menu **Navegar** fornece as seguintes opções: • **Visualizar por rede** - Exibe a janela Lista de redes, que exibe todas as redes associadas ao endereço IP selecionado. • **Visualizar resumo de origem** – Exibe a janela Lista de ofensas, que exibe todas as ofensas que estão associadas ao endereço IP de origem selecionado. • **Visualizar resumo de destino** – Exibe a janela Lista de ofensas, que exibe todas as ofensas que estão associadas ao endereço IP de destino selecionado.

Tabela 48. Opções do menu ativado pelo botão direito (continuação)

Opção	Descrição
Informações	O menu **Informações** fornece as seguintes opções: • **Consulta DNS** – Procura por entradas de DNS que são baseadas no endereço IP. • **Consulta WHOIS** – Procura pelo proprietário registado de um endereço IP remoto. O servidor de WHOIS padrão é whois.arin.net. • **Varredura de porta** – Desempenha uma varredura de Mapeador de Rede (NMAP) do endereço IP selecionado. Esta opção estará disponível apenas se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do fornecedor. • **Perfil de ativo** – Exibe informações do perfil de ativo. Essa opção de menu só ficará disponível quando um dado de perfil for adquirido ativamente por uma varredura ou passivamente por fontes de fluxo. • **Procurar eventos** – Selecione a opção **Procurar eventos** para procurar eventos que estejam associados com este endereço IP. • **Procura fluxos** – Selecione a opção Procurar Fluxos para procurar fluxos que estejam associados a este endereço IP.
Executar varredura QVM	Selecione esta opção para executar uma varredura do Gerenciado de Vulnerabilidade no ativo selecionado. Essa opção será exibida somente depois que você instalar o QRadar Vulnerability Manager.

Visualizando um perfil de ativos

Na lista de ativos na guia **Ativos**, você pode selecionar e visualizar um perfil de ativos. Um perfil de ativos fornece informações sobre cada perfil.

Sobre Esta Tarefa

As informações do perfil de ativos são automaticamente descobertas por meio do Server Discovery ou configuradas manualmente. Você pode editar as informações do perfil de ativos geradas automaticamente.

A página Perfil de ativos fornece as informações sobre o ativo 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 na caixa de listagem **Exibir** na barra de ferramentas.

A página Perfil de ativos na barra de ferramentas fornece as seguintes funções:

Tabela 49. Funções da barra de ferramentas da página perfil de ativos

Opções	Descrição
Retornar à lista de ativos	Clique nesta opção para retornar à lista de ativos.
Exibir	Na caixa de listagem, você pode selecionar a área de janela que deseja visualizar na área da janela do perfil de ativos. As áreas de janela do Resumo de Ativo e do Resumo de Interface de Rede são sempre exibidas. Para obter mais informações sobre os parâmetros exibidos em cada área de janela, consulte Parâmetros da página do perfil de ativos.
Editar ativos	Clique nesta opção para editar o perfil de ativos. Consulte “Incluindo ou editando um perfil ativo” na página 139.
Visualização por rede	Se este ativo estiver associado a uma ofensa, esta opção permitirá que você exiba a lista de redes associada a este ativo. Ao clicar em **Visualização por rede**, a janela Lista de redes é exibida. Consulte “Monitorando ofensas agrupadas por rede” na página 29.
Visualização do resumo de origem	Se este ativo for a origem de uma ofensa, essa opção permitirá que você visualize as informações de resumo de origem. Ao clicar em **Visualização do resumo de origem**, a janela Lista de ofensas é exibida. Consulte “Monitorando ofensas agrupadas por IP de origem” na página 28.

Tabela 49. Funções da barra de ferramentas da página perfil de ativos (continuação)

Opções	Descrição
Visualização do resumo de destino	Se este ativo for o destino de uma ofensa, esta opção permitirá que você visualize as informações de resumo de destino. Ao clicar em **Visualização do resumo de destino**, a janela Lista de destinos é exibida. Consulte "Monitorando ofensas agrupadas por IP de destino" na página 28.
Histórico	Clique em **Histórico** para visualizar as informações do histórico de eventos para este ativo. Quando você clica no ícone **Histórico**, a janela Procura de eventos é exibida, pré-preenchida com o critério de procura de eventos: Você pode customizar os parâmetros de procura, se necessário. Clique em **Procura** para visualizar as informações do histórico de eventos.
Aplicativos	Clique em **Aplicativos** para visualizar as informações do aplicativo para este ativo. Quando você clica no ícone **Aplicativos**, a janela Procura de fluxo é exibida, pré-preenchida com o critério de procura de eventos. Você pode customizar os parâmetros de procura, se necessário. Clique em **Procura** para visualizar as informações do aplicativo.
Conexões de procura	Clique em **Conexões de procura** para procurar por conexões. A janela Conexão de procura é exibida. Esta opção será exibida apenas quando o IBM Security QRadar Risk Manager for adquirido e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
Visualizar Topologia	Clique em **Visualização da topologia** para investigar o ativo. A janela Topologia atual é exibida. Esta opção será exibida apenas quando o IBM Security QRadar Risk Manager for adquirido e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
Ações	Na lista **Ações**, selecione **Histórico de vulnerabilidade**. Esta opção será exibida apenas quando o IBM Security QRadar Risk Manager for adquirido e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

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 as várias áreas de janela de informação do perfil de ativos. Consulte Editando um perfil de ativos.
5. Para pesquisar as vulnerabilidades associadas, clique em cada vulnerabilidade na área de janela de Vulnerabilidades. Consulte a Tabela 10-10
6. Se necessário, edite o perfil de ativos. Consulte Editando um perfil de ativos.
7. Clique em **Retornar à lista de ativos** para selecionar e visualizar outro ativo, se necessário.

Incluindo ou editando um perfil ativo

Os perfis ativos são automaticamente descobertos e incluídos; no entanto, pode ser necessário incluir um perfil manualmente

Sobre Esta Tarefa

Quando os ativos forem descobertos usando a opção Descoberta do Servidor, alguns detalhes do perfil de ativos serão preenchidos automaticamente. É possível incluir as informações manualmente no perfil de ativo e 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 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 insira o endereço IP ou o intervalo do CIDR do ativo no campo **Novo endereço IP**.
   - Para editar um ativo, dê um clique duplo no ativo que você deseja visualizar e clique em **Editar ativo**.
4. Configure os parâmetros na área de janela MAC & Endereço IP. Configure uma ou mais das seguintes opções:
   - Clique no ícone **Novo endereço MAC** e insira um Endereço MAC na caixa de diálogo.
   - Clique no ícone **Novo endereço IP** e insira um endereço IP na caixa de diálogo.
   - Se **NIC desconhecido** for listado, você poderá selecionar esse item, clique no ícone **Editar** e insira um novo endereço MAC na caixa de diálogo.
   - Selecione um endereço MAC ou IP na lista, clique no ícone **Editar** e insira 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 Nomes & Descrição. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
DNS	Escolha uma das opções a seguir: • Insira um nome DNS e clique em **Incluir**. • Selecione um nome DNS na lista e clique em **Editar**. • Selecione um nome DNS na lista e clique em **Remover**.
NetBIOS	Escolha uma das opções a seguir: • Insira um nome NetBIOS e clique em **Incluir**. • Selecione um nome NetBIOS na lista e clique em **Editar**. • Selecione um nome NetBIOS na lista e clique em **Remover**.
Nome Dado	Insira um nome para esse perfil do ativo.
Local	Insira um local para esse perfil de ativo.
Descrição	Insira uma descrição para o perfil de ativo.
AP Wireless	Insira o Ponto de Acesso (AP) wireless desse perfil de ativo.
SSID Wireless	Insira o Service Set Identifier (SSID) do wireless para esse perfil de ativo.
ID do Comutador	Insira o ID do comutador para esse perfil de ativo.
ID da Porta do Comutador	Insira o ID de porta do comutador para esse 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 opções a seguir:
   - **Até a próxima varredura** – selecione essa opção para especificar que o scanner fornece as informações do sistema operacional e elas podem ser temporariamente editadas. Se você editar os parâmetros do sistema operacional, o scanner irá restaurar as informações em sua próxima varredura.
   - **Contínuo** – selecione essa opção para especificar que você deseja inserir as informações do sistema operacional manualmente e desativar o scanner de atualizar as informações.

f. Selecione um sistema operacional da lista.

g. Selecione um sistema operacional e clique no ícone **Alternar substituição**.

7. Configure os parâmetros na área de janela CVSS & Peso. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
Potencial de Danos Colaterais	Configure esse parâmetro para indicar o potencial de perda de vidas ou ativos físicos através de dano ou furto desse ativo. Você também pode usar esse parâmetro para indicar um potencial de perda econômica de produtividade ou renda. O potencial de danos colateral aumentado, aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Potencial de dano colateral**, selecione uma das opções a seguir: • Nenhum • Baixo • Médio baixo • Médio alto • Alto • Não definido Ao configurar o parâmetro **Collateral Damage Potential**, o parâmetro **Weight** será atualizado automaticamente.
Requisito de Confidencialidade	Configure esse parâmetro para indicar o impacto sobre a confidencialidade de uma vulnerabilidade explorada com êxito nesse ativo. O impacto de confidencialidade aumentada, aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Requisito de confidencialidade**, selecione uma das opções a seguir: • Baixo • Médio • Alto • Não definido
Requisito de Disponibilidade	Configure esse parâmetro para indicar o impacto de disponibilidade do ativo quando uma vulnerabilidade for explorada com êxito. Os ataques que consumem a largura da banda da rede, os ciclos do processador ou o espaço em disco impactará a disponibilidade de um ativo. O impacto de disponibilidade aumentada, aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Requisito de disponibilidade**, selecione uma das opções a seguir: • Baixo • Médio • Alto • Não definido

Parâmetro	Descrição
Requisito de Integridade	Configure esse parâmetro para indicar o impacto para a integridade do ativo quando uma vulnerabilidade for explorada com êxito. A integridade refere-se à fidelidade e a veracidade garantida de informações. O impacto de integridade aumentada, aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Requisito de integridade**, selecione uma das opções a seguir: • Baixo • Médio • Alto • Não definido
Peso	Na caixa de listagem **Weight**, selecione um peso para esse perfil de ativo. O intervalo é de 0 – 10. Ao configurar o parâmetro **Weight**, o parâmetro **Collateral Damage Potential** será atualizado automaticamente.

8. Configure os parâmetros na área de janela Proprietário. Escolha uma ou mais das seguintes opções:

Parâmetro	Descrição
Proprietário de Negócios	Insira 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.
Contato do Proprietário de Negócios	Insira as informações de contato para o proprietário de negócios. O comprimento máximo é de 255 caracteres.
Responsável Técnico	Insira o proprietário técnico do ativo. Um exemplo de um proprietário de negócios é o gerenciador de TI ou diretor. O comprimento máximo é de 255 caracteres.
Contato do Responsável Técnico	Insira as informações de contato para o proprietário técnico. O comprimento máximo é de 255 caracteres.
Usuário Técnico	Na caixa de listagem, selecione o nome do usuário que você deseja associar a esse perfil de ativo. Você também pode usar esse parâmetro para ativar a correção de vulnerabilidade automática para o IBM Security QRadar Vulnerabilidade Manager. Para obter mais informações sobre a correção automática, consulte o *Guia do usuário IBM Security QRadar Vulnerabilidade Manager*.

9. Clique em **Salvar**.

Procurando perfis de ativos

Você pode configurar os 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 é exibida preenchida com todos os ativos descobertos em sua rede. Para refinar esta lista, você pode configurar os parâmetros de procura para exibir apenas os perfis de ativos que você deseja investigar.

Na página Procura de ativo, você pode gerenciar os grupos de procura de ativo. Para obter mais informações sobre Grupos de Procura de Ativo, consulte Consulte grupos de procura de ativo.

O recurso de procura permite 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 por ativos pelas referências de dados externos para determinar se as vulnerabilidades conhecidas existem em sua implementação.

Por exemplo:

Você recebe uma notificação de que o CVE ID: CVE-2010-000 está sendo ativamente usado no campo. Para verificar se quaisquer hosts em sua implementação são vulneráveis a esta exploração, você poderá selecionar **Referência externa de vulnerabilidade** na lista de parâmetros de procura, selecionar **CVE**, e, em seguida, inserir

```
2010-000
```

Para visualizar uma lista de todos os hosts que são vulneráveis a este CVE ID 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 **Procura** > **Procura nova**.
4. Escolha uma das opções a seguir:
   - Para carregar uma procura salva anteriormente, vá para a Etapa 5.
   - Para criar uma procura nova, vá para 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 deseja carregar.
      - No campo **Digitar procura salva ou selecionar a partir 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 ativo que você deseja procurar. Por exemplo, **Nome do host**, **Classificação de risco de vulnerabilidade** ou **Responsável técnico**.
   b. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura.
   c. No campo de entrada, digite as informações específicas relacionadas ao seu parâmetro de procura.
   d. Clique em **Incluir filtro**.
   e. Repita estas etapas para cada filtro que você deseja incluir no critério de procura.
7. Clique em **Procurar**.

Resultados

Você pode salvar o seu critério de procura de ativo. Consulte Salvando critério de procura de ativo.

Salvando critério de procura de ativo

Na guia **Ativo**, você pode salvar o critério de procura configurado para que você possa reutilizar o critério. 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 ativos.
4. Clique em **Salvar critério**.
5. Insira valores para os parâmetros:

Parâmetro	Descrição
Enter the name of this search	Digite o nome exclusivo que deseja designar a este critério de procura.
Gerenciar Grupos	Clique em **Gerenciar grupos** para gerenciar grupos de procura. Para obter mais informações, consulte Grupos de procura de ativo. Esta opção estará disponível apenas se você tiver permissões administrativas.
Assign Search to Group(s)	Selecione a caixa de seleção para o grupo que você deseja designar essa procura salva. Se você não selecionar um grupo, esta procura salva será designada para o grupo **Outro** por padrão. Para obter mais informações, consulte Grupos de procura de ativo.
Incluir em Minhas Procuras Rápidas	Selecione esta caixa de seleção para incluir esta procura em sua caixa de listagem **Procura rápida**, na guia **Ativos** da barra de ferramentas.
Configurar como padrão	Selecione esta caixa de seleção para configurar esta procura como sua procura padrão quando você acessar a guia **Ativos**.
Share with Everyone	Selecione esta caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

Grupos de procura de ativos

Usando a janela de Grupos de Procura de Ativo, você pode criar e gerenciar grupos de procura de ativo.

Esses grupos permitem que você localize facilmente critérios de procura salva na guia **Ativos**.

Visualizando grupos de procura

Use a janela Grupos de procura de ativos para visualizar uma lista de grupos e subgrupos.

Sobre Esta Tarefa

Na 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 50. Funções da barra de ferramentas da janela grupos de procura de ativos

Função	Descrição
Novo grupo	Para criar um grupo de procura novo, você pode clicar em **Novo grupo**. Consulte o Consulte criando um grupo de procura novo.
Editar	Para editar um grupo de procura existente, é possível clicar em **Editar**. Consulte o Consulte editando um grupo de procura.
Copiar	Para copiar uma procura salva para outro grupo de procura, você pode clicar em **Copiar**. Consulte 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 deseja remover, e, em seguida, clique em **Remover**. Consulte o Consulte 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 **Procura** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Visualização dos 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 **Procura** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a pasta para o grupo ao qual você deseja criar o novo grupo.
6. Clique em **Novo grupo**.
7. No campo **Nome**, insira um nome exclusivo para o novo grupo.
8. Opcional. No campo **Descrição**, insira 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 **Procura** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione o grupo que você deseja editar.
6. Clique em **Editar**.
7. Insira um novo nome no campo **Nome**.
8. Insira uma nova descrição no campo **Descrição**.
9. Clique em **OK**.

Copiando uma procura salva em outro grupo

Você pode copiar uma procura salva em 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 **Procura** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que você deseja copiar.
6. Clique em **Copiar**.
7. Na janela Grupos de itens, marque a caixa de seleção para o grupo para o qual 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 **Remover** para remover uma procura de um grupo ou de 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 **Outro**.

Não é possível remover os seguintes grupos de seu 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 **Procura** > **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 de perfil do ativo

É possível excluir, importar e exportar perfis do ativo usando a guia Ativos.

Sobre Esta Tarefa

Usando a guia **Ativos**, você pode excluir, importar e exportar perfis de ativos.

Excluindo ativos

Você pode excluir ativos específicos ou todos os perfis ativos 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 as informação do perfil de ativos.

Antes de Iniciar

O arquivo importado deve ser um arquivo CSV no formato a seguir:

```
ip,name,weight,description
```

Em que:

- **IP** – especifica qualquer endereço IP válido no formato decimal pontilhado. Por exemplo: 192.168.5.34.
- **Nome** – especifica o nome desse ativo até 255 caracteres de comprimento. Vírgulas não são válidas nesse campo e invalida o processo de importação. Por exemplo: WebServer01 está correto.
- **Peso** – especifica um número de 0 a 10 ao qual indica a importância desse ativo em sua rede. Um valor de 0 indica baixa importância e 10 é muito alto.
- **Descrição** – especifica uma descrição textual para esse ativo de 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 as informações do perfil de ativos que você tem atualmente armazenados 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 **Pesquisar** 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 os perfis de ativos listados para um arquivo de Linguagem de Marcações Extendida (XML) ou Valor Separado por Vírgula (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. Visualizar a janela de status para o status do processo de exportação.
5. Opcional: Se você deseja usar outras guias e páginas enquanto a exportação estiver em andamento, clique no link **Notificar quando pronto**.

   Quando a exportação for concluída, a janela Download de arquivo será exibida.
6. Na janela Download de arquivo, escolha uma das opções a seguir:
   - **Abrir** – Selecione esta opção para abrir os resultados da exportação em sua opção de navegador.
   - **Salvar** – Selecione esta opção para salvar os resultados em seu desktop.
7. Clique em **OK**.

Pesquisar vulnerabilidades de ativos

A área de janela Vulnerabilidades na página Perfil de ativo exibe uma lista de vulnerabilidades descobertas para o ativo.

Sobre Esta Tarefa

Você pode dar um clique duplo na vulnerabilidade para exibir mais detalhes de vulnerabilidade.

A janela Pesquisar detalhes de vulnerabilidade fornece os detalhes a seguir:

Parâmetro	Descrição
Vulnerability ID	Especifica o ID da vulnerabilidade. O ID de Vuln é um identificador exclusivo gerado pelo Vulnerability Information System (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 possui essa vulnerabilidade. Clique no link para visualizar a lista de ativos.
Assets, including exceptions	Especifica o número de ativos em sua rede que possui as exceções de vulnerabilidade. Clique no link para visualizar a lista de ativos.
CVE	Especifica o identificador CVE para a vulnerabilidade. Os identificadores de CVE são fornecidos pelo NVDB. Clique no link para obter mais informações. Ao clicar no link, o website do NVDB será exibido em uma nova janela do navegador.
xforce	Especifica o identificador X-Force para a vulnerabilidade. Clique no link para obter mais informações. Ao clicar no link, o website do IBM Internet Security Systems será exibido em uma nova janela do navegador.
OSVDB	Especifica o identificador do OSVDB para a vulnerabilidade. Clique no link para obter mais informações. Ao clicar no link, o website do OSVDB será exibido em uma nova janela do navegador.

Parâmetro	Descrição
CVSS Score	Exibe a pontuação Common Vulnerability Scoring System (CVSS) agregada das vulnerabilidades neste ativo. Uma pontuação CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades. A pontuação CVSS é calculada usando os seguintes parâmetros definidos pelo usuário: • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil ativo” na página 139. Para obter mais informações sobre CVSS, consulte *http://www.first.org/cvss/*.
Impact	Exibe o tipo de prejuízo ou dano que poderá ser esperado se essa vulnerabilidade for explorada.
CVSS Base Metrics	Exibe as métricas usadas para calcular a pontuação base do CVSS, incluindo: • Vetor de Acesso • Complexidade de Acesso • Autenticação • Impacto de Confidencialidade • Impacto de Integridade • Impacto de disponibilidade
Descrição	Especifica uma descrição da vulnerabilidade detectada. Esse valor estará disponível apenas quando o sistema integra as ferramentas de VA.
Dúvida	Especifica os efeitos que a vulnerabilidade pode ter em sua rede.
Solução	Siga as instruções fornecidas para resolver a vulnerabilidade.
Correção Virtual	Exibe as informações de correção virtual associada a essa vulnerabilidade, se disponível. Uma correção virtual é uma solução de mitigação de curto prazo para uma vulnerabilidade recentemente descoberta. Essas informações são derivadas de eventos do Intrusion Protection System (IPS). Se você desejar instalar a correção virtual, consulte as informações do fornecedor de seu IPS.
Referência	Exibe uma lista de referências externas, incluindo: • **Tipo referência** – especifica o tipo de referência listada, como uma URL consultiva ou uma lista de post de correio. • **URL** – especifica a URL que você pode clicar para visualizar a referência. Clique no link para obter mais informações. Ao clicar no link, o recurso externo será exibido em uma nova janela do navegador.
Produtos	Exibe uma lista de produtos associados a essa vulnerabilidade. • **Fornecedor** – especifica o fornecedor do produto. • **Produto** – especifica o nome do produto. • **Versão** - especifica o número da versão do produto.

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 de parâmetro **ID** ou **Vulnerability** para a vulnerabilidade que você desejar investigar.

Parâmetros da página de perfil de ativos

Você pode localizar as descrições de parâmetro de página do perfil de ativos para a área de janela de Resumo de Ativo, Interface de Rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de Risco e de Produtos.

Essa referência inclui tabelas que descrevem os parâmetros exibidos em cada área de janela da guia **Perfil de ativo**.

Área de janela de Resumo de Ativo

Você pode localizar descrições de parâmetro para a área de janela de Resumo de Ativo que você acessa a partir da página Perfil de ativo.

A área de janela de Resumo de Ativo na página Perfil de ativo fornece as seguintes informações:

Parâmetros de área de janela de Resumo de Ativo de 10-8 da tabela

Parâmetro	Descrição
ID do ativo	Exibe o número do ID que é designado ao perfil do ativo.
Endereço IP	Exibe o último endereço IP reportado do ativo.
Endereço MAC	Exibe o último endereço MAC conhecido do ativo.
Rede	Exibe a última rede relatada que está associada ao ativo.
Nome de NetBIOS	Exibe o nome do 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.
Nome DNS	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 associado.
Nome Dado	Exibe o nome do ativo. Por padrão, este campo fica vazio. Para fornecer um nome dado ao ativo, edite o perfil do ativo.
Nome do grupo	Exibe o último grupo do usuário conhecido do ativo, se conhecido.
Último Usuário	Exibe o último usuário conhecido do ativo. As informações do usuário são derivadas de eventos da identidade. Se mais de um usuário estiver associado a este ativo, você poderá clicar no link para exibir todos os usuários.
Sistema Operacional	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 **Override** for especificado como **Até a próxima varredura** ou **Indefinidamente**.
Peso	Exibe o nível de importância que está associado a este ativo. O intervalo é 0 (Não Importante) a 10 (Muito Importante). Por padrão, este campo fica vazio. Para fornecer um peso para o ativo, edite o perfil de ativo.

Parâmetro	Descrição
Pontuação CVSS agregada	Exibe a pontuação Common Vulnerability Scoring System (CVSS) agregada das vulnerabilidades neste ativo. Uma pontuação CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades. A pontuação CVSS é calculada usando os seguintes parâmetros definidos pelo usuário: • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil ativo” na página 139. Para obter mais informações sobre CVSS, consulte *http://www.first.org/cvss/*.
Proprietário de negócios	Exibe o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento.
Informações de contato do proprietário de negócios	Exibe as informações de contato para o proprietário de negócios.
Potencial de danos colaterais de CVSS	Exibe o potencial que este ativo possui para danos colaterais. Este valor será incluído na fórmula para calcular o parâmetro **Pontuação do CVSS**. Por padrão, esse campo não está definido. Para fornecer um local para o ativo, edite o perfil de ativo.
Proprietário técnico	Exibe o proprietário técnico do ativo. Um exemplo de um proprietário técnico é um gerenciador ou diretor de TI.
Informações de contato do proprietário técnico	Exibe as informações de contato do proprietário técnico.
Disponibilidade de CVSS	Exibe o impacto de disponibilidade do ativo quando uma vulnerabilidade é explorada com êxito.
PA Wireless	Exibe o ponto de acesso wireless (PA) para este perfil de ativo.
SSID Wireless	Exibe o Service Set Identifier (SSID) sem fio para este perfil do ativo.
Requisito de confidencialidade de CVSS	Exibe o impacto sobre a confidencialidade de uma vulnerabilidade explorada com êxito neste ativo.
ID do comutador	Exibe o ID do comutador para este perfil do ativo.
ID da porta do comutador	Exibe o ID da porta do comutador para este perfil do ativo.
Requisitos de integridade de CVSS	Exibe o impacto para a integridade do ativo quando uma vulnerabilidade é explorada com êxito.
Usuário técnico	Especifica o nome de usuário associado a esse perfil de ativo.
Serviços abertos	Exibe o número de aplicativos de Camada 7 executados neste perfil de ativo.
Vulnerabilidades	Exibe o número de vulnerabilidades que são descobertas neste perfil de ativo.
Local	Especifica o local físico do ativo. Por padrão, este campo fica vazio. Para fornecer um local para o ativo, edite o perfil de ativo.
Descrição do ativo	Especifica uma descrição para este ativo. Por padrão, este campo fica vazio. Para fornecer uma descrição para o ativo, edite o perfil de ativo.
Dados extras	Especifica quaisquer informações estendidas que são baseadas em um evento.

Área de janela de resumo de interface de rede

Você pode localizar descrições de parâmetros para a área de janela de resumo de interface de rede que você acessa da página Perfil de ativo.

A área de janela de resumo de interface de rede na página Perfil de ativo fornece as seguintes informações:

Parâmetros da área de janela de resumo de interface de rede área de tablea 1

Parâmetro	Descrição
Endereço MAC	Exibe o endereço MAC deste ativo, se conhecido.
Endereço IP	Exibe o endereço IP que é detectado para este endereço MAC.
Rede	Exibe a rede que o endereço IP está associado, se conhecida.
Visto pela última vez	Exibe a data e hora em que o endereço IP foi detectado pela última vez nesse endereço MAC.

Área de janela de vulnerabilidade

Você pode localizar descrições de parâmetro para a área de janela de Vulnerabilidade que você acessa na página Perfil de ativo.

A área de janela de Vulnerabilidade na página Perfil de ativo fornece as seguintes informações:

Tabela 51. Área de janela de parâmetros de vulnerabilidade

Parâmetro	Descrição
ID	Exibe o ID de vulnerabilidade. O ID é um identificador exclusivo que é gerado pelo Vulnerability Information System (VIS).
Gravidade	Exibe a gravidade do Payment Security Industry (PCI) associada à vulnerabilidade.
Risco	Nível de risco que está associado à vulnerabilidade. Classificar nessa coluna deve ser pelo código de nível de risco subjacente
Serviço	Serviço que está associado à vulnerabilidade (como descoberto pela varredura). Se somente 1 serviço estiver associado, em seguida, exiba o serviço. Caso contrário, exiba Vários (N) onde N indica ao número total de serviços associados a esta vulnerabilidade.
Porta	Exibe o número da porta que esta vulnerabilidade foi descoberta. Se a vulnerabilidade foi descoberta em mais de uma porta, este campo indica o número de números de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números de porta.
Vulnerabilidade	Nome ou título desta vulnerabilidade.
Detalhes	Texto detalhado específico que está associado a essa vulnerabilidade, conforme determinado pela varredura. Se somente 1 Detalhe estiver associado, em seguida, exiba o texto desse Detalhe. Caso contrário, exiba Vários (N) onde N indica ao número total de Detalhes que estão associados a esta vulnerabilidade.
Pontuação de CVSS	Exibe a pontuação Common Vulnerability Scoring System (CVSS) agregada das vulnerabilidades neste ativo. Uma pontuação CVSS é uma métrica de avaliação para a gravidade de uma vulnerabilidade. Você pode usar pontuações CVSS para medir o quanto uma vulnerabilidade garante em comparação a outras vulnerabilidades. A pontuação CVSS é calculada usando os seguintes parâmetros definidos pelo usuário: • Potencial de Danos Colaterais • Requisito de Confidencialidade • Requisito de Disponibilidade • Requisito de Integridade Para obter mais informações sobre como configurar estes parâmetros, consulte “Incluindo ou editando um perfil ativo” na página 139. Para obter mais informações sobre CVSS, consulte *http://www.first.org/cvss/*.
Encontrado	Exibe a data quando esta vulnerabilidade foi originalmente encontrada em uma varredura.
Visto pela última vez	Exibe a data quando esta vulnerabilidade foi vista pela última vez em uma varredura.

Área de janela de serviços

Você pode localizar descrições de parâmetros para a área de janela de Serviços que você acessa na página do Perfil de ativo.

A área de janela de Serviços na página Perfil de ativo fornece as seguintes informações:

Tabela 52. Parâmetros da área de janela de serviços

Parâmetro	Descrição
Serviço	Exibe o nome dos serviços abertos.
Produto	Exibe o produto que executa este serviço, se conhecido.
Porta	Exibe a porta que o aplicativo de 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 de porta.
Protocolo	Exibe uma lista separada por vírgula de protocolos que são descobertos na porta que executa o serviço aberto.
Último passivo visto	Exibe a data e hora em que o último serviço abertos foi visto passivamente.
Último ativo visto	Exibe a data e hora em que o serviço aberto foi visto ativamente pela última vez.
Portas padrão de serviço	Exibe uma lista separada por vírgula de portas conhecidas que o aplicativo de Camada 7 é conhecido para executar.
Vulnerabilidades	Exibe o número de vulnerabilidades que estão associadas a este serviço aberto.

Área de janela do serviço do Windows

Você pode localizar descrições de parâmetro para área de janela de Serviços do Windows que você acessa na página do Perfil de ativo. A área de janela de Serviços do Windows é exibida apenas quando QRadar Vulnerability Manager é instalado em seu sistema.

A área de janela de Serviços do Windows na página do Perfil de ativo que fornece as seguintes informações:

Tabela 53. Parâmetros da área de janela de Serviços do Windows

Parâmetro	Descrição
Nome	Exibe o nome do serviço do Windows que foi visto ativamente no ativo.
Status	Exibe o status do serviço do Windows. As opções incluem: • Ativado • Manual • Desativado

Área de janela de pacotes

Você pode localizar descrições de parâmetro para a área de janela Pacotes que você acessa na página Perfil de ativo.

A área de janela Pacotes será exibida apenas quando QRadar Vulnerability Manager for instalado em seu sistema. A área de janela Pacotes na página Perfil do ativo fornece as seguintes informações:

Tabela 54. Parâmetros de área de janela de pacotes

Parâmetro	Descrição
Pacotes	Exibe o nome do pacote que é aplicado ao ativo.
Versão	Exibe a versão do pacote que é aplicado ao ativo.
Revisão	Exibe a revisão do pacote que é aplicado ao ativo.

Área de janela de Correções do Windows

Você pode localizar descrições de parâmetro para a área de janela Correções do Windows que você acessa na página do Perfil de ativo.

A área de janela de Correções do Windows é exibida apenas quando QRadar Vulnerability Manager é instalado em seu sistema. A área de janela de correções do Windows na página Perfil de ativo fornece as seguintes informações:

Tabela 55. Parâmetros de área de janela de correções do Windows

Parâmetro	Descrição
Número de KB da Microsoft	Exibe o número do Microsoft Knowledge Base (KB) da correção do Windows que é executado no ativo.
Descrição	Exibe a descrição da correção do Windows.
ID de Avisos	Exibe o número do ID do boletim da correção do Windows.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade da correção do Windows.
ID do CVE	Exibe o ID do CVE associado à correção do Windows. Se mais de um ID do CVE associado à correção do Windows, mais seu mouse sobre o link Múltiplo para exibir a lista de IDs do CVE. Você pode clicar em um link de ID do CVE para acessar mais informações.
Sistema	Exibe o sistema do Windows para a correção.
Service Pack	Exibe o service pack para a correção.

Área de janela de propriedades

Você pode localizar descrições de parâmetro para a área de janela de Propriedades que você acessa na página Perfil de ativo. A área de janela de Propriedades é exibida apenas quando QRadar Vulnerability Manager estiver instalado em seu sistema.

A área de janela de Propriedades na página do Perfil de ativo fornece as seguintes informações:

Tabela 56. Parâmetros da área de janela de propriedades

Parâmetro	Descrição
Nome	Exibe o nome da propriedade de configuração que foi vista ativamente no ativo.
Valor	Exibe o valor para a propriedade de configuração.

Área de janela de políticas de risco

Você pode localizar descrições de parâmetros para a área de janela de Políticas de Risco que você acessa na página Perfil de ativo. A área de janela de Políticas de Risco é exibida apenas quando QRadar Vulnerability Manager está instalado em seu sistema.

A área de janela de Políticas de Risco na página Perfil de ativo fornece as seguintes informações:

Tabela 57. Parâmetros da área de janela de Políticas de Risco

Parâmetro	Descrição
Política	Exibe o nome da política que está associado a este ativo.
Aprovado/Reprovado	Indica se a política tiver um status de **Aprovado** ou **Reprovado**.
Última avaliação	Exibe a data em que esta política foi avaliada pela última vez.

Área de janela de produtos

É possível encontrar descrições de Parâmetro para a área de janela de Produtos que você acessa a partir da página Perfil de ativo.

A área de janela de Produtos na página Perfil do Ativo fornece as seguintes informações:

Tabela 58. Parâmetros da área de janela de produtos

Parâmetro	Descrição
Produto	Exibe o nome do produto que é executado no ativo.
Porta	Exibe a porta que o produto usa.
Vulnerabilidade	Exibe o número de vulnerabilidades que estão associadas com este produto.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade.

Capítulo 12. Gerenciamento de relatório

Você pode usar a guia **Relatórios** para criar, editar, distribuir e gerenciar relatórios.

As opções de relatório detalhadas e flexíveis satisfazem suas várias normas reguladoras, como a conformidade de PCI.

É possível criar seus próprios relatórios customizados ou usar relatórios padrão. Você pode customizar e remarcar relatórios padrão e distribuir esses para outros usuários.

A guia **Relatórios** pode requerer um período de tempo estendido para atualizar, caso o seu sistema inclua muitos relatórios.

Nota: Se você estiver executando Microsoft Exchange Server 5.5, os caracteres de fonte indisponível podem ser exibidos na linha de assunto do relatórios por email. Para resolver isso, faça download e instale o Service Pack 4 do Microsoft Exchange Server 5.5. Para obter mais informações, contate o suporte Microsoft.

Considerações sobre fuso horário

Para assegurar que o recurso Relatórios use data e hora corretas para relatar dados, sua sessão deverá estar sincronizada com o fuso horário.

Durante a instalação e configuração de produtos QRadar, o fuso horário é configurado. Verifique com seu administrador para assegurar-se de que sua sessão QRadar esteja sincronizada com seu fuso horário.

Permissões da guia Relatórios

Usuários administrativos podem visualizar todos os relatórios que são criados por outros usuários.

Usuários não administrativos podem visualizar apenas relatórios que eles criaram ou relatórios compartilhados por outros usuários.

Parâmetros da guia Relatório

A guia **Relatórios** exibe uma lista de relatórios padrão e customizado.

Na guia **Relatórios**, você pode 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, você deverá gerar manualmente o relatório.

Você pode apontar o mouse sobre qualquer relatório para visualizar um resumo do relatório em dicas 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 exibidos e a quantidade de tempo (Tempo decorrido:) necessário 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.

Quando você seleciona o layout de um relatório, considere o tipo de relatório que você deseja criar. Por exemplo, não escolha um contêiner de gráfico pequeno para o conteúdo do gráfico que exibe muitos objetos. Cada gráfico inclui uma legenda e uma lista de redes a partir dos quais o conteúdo é derivado; escolha um contêiner suficientemente grande para conter os dados. Para visualizar como cada gráfico exibe um dado, consulte Tipos de diagramas.

Tipos de gráfico

Ao criar um relatório, você deve escolher um tipo de gráfico para cada gráfico que você deseja incluir no relatório.

O tipo de gráfico determina como o relatório gerado apresenta dados e objetos da rede. É possível colocar em gráfico dados com diversas características e criar os gráficos em um único relatório gerado.

Você pode 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 você selecionar a opção **Nenhum** para qualquer contêiner, nenhuma configuração adicional será necessária para esse contêiner.
- **Vulnerabilidades do ativo** - Use este gráfico para visualizar dados de vulnerabilidade para cada ativo definido em sua implementação. Você poderá gerar gráficos de Vulnerabilidade de Ativo quando vulnerabilidades forem detectadas por uma varredura de VA. Este gráfico estará disponível após você instalar IBM Security QRadar Vulnerability Manager.
- **Conexões** – Esta opção de gráfico é exibida apenas se você tiver adquirido e licenciado IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
- **Regras de dispositivo** – Esta opção de gráfico será exibida apenas se você tiver adquirido e licenciado IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
- **Objetos sem uso do dispositivo** – Esta opção de gráfico será exibida apenas se você tiver adquirido e licenciado IBM Security QRadar Risk Manager. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.
- **Eventos/logs** – Use este gráfico para visualizar informações de evento. Você pode basear seus gráficos nos dados de procuras salvas na guia **Atividade do log**. Você pode customizar os dados que você deseja exibir no relatório gerado. Você pode configurar o gráfico para dados de plotagem durante 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 as informações do fluxo. Você pode basear seu gráficos em dados das procuras salvas a partir da guia Atividade de Rede. Isso permite que você customize os dados que deseja exibir no relatório gerado. Você pode usar procuras salvas para configurar o gráfico para dados de fluxo de plotagem por um período de tempo configurável. Esta funcionalidade ajuda a detectar tendências de fluxos. Para obter mais informações sobre procuras salvas, consulte Procuras de dados.
- **Principais IPs de destino** - Use esse 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 para os locais de rede que você selecionar.
- **Principais IPs de origem** – Use este gráfico para exibir e classificar as principais origens de ofensa (endereços IP) que atacam a sua rede ou ativos de negócios.
- **Vulnerabilidades** – A opção Vulnerabilidades será exibida somente quando o IBM Security QRadar Vulnerability Manager tiver sido adquirido e licenciado. Para obter informações adicionais, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Para obter mais informações sobre esses tipos de gráfico, consulte parâmetros de contêiner do gráfico.

Barra de ferramentas da guia Relatório

Você pode usar a barra de ferramentas para executar várias ações em relatórios.

A tabela a seguir identifica e descreve as opções da barra de ferramentas dos Relatórios.

Tabela 59. Opções da barra de ferramentas do Relatório

Opção	Descrição
Grupo	
Gerenciar grupos	Clique em **Gerenciar grupos** para gerenciar grupos de relatório. Usando o recurso Gerenciar Grupos, você pode organizar seus relatórios em grupos funcionais.

Tabela 59. Opções da barra de ferramentas do Relatório (continuação)

Opção	Descrição
Ações	Clique em **Ações** para executar as seguintes ações: • **Criar** – Selecione esta opção para criar um novo relatório. • **Editar** – Selecione esta opção para editar o relatório selecionado. Você também pode clicar duas vezes em um relatório para editar o conteúdo. • **Duplicar** – Selecione esta opção para duplicar ou renomear o relatório selecionado. • **Designar grupos** – Selecione esta opção para designar o relatório selecionado para um grupo de relatório. • **Compartilhar** – Selecione esta opção para compartilhar o relatório selecionado com outros usuários. Você deve ter privilégios administrativos para compartilhar relatórios. • **Alternar planejamento** – Selecione esta opção para comutar o relatório selecionado entre o estado Ativo ou e o Inativo. • **Executar relatório** – Selecione esta opção para gerar o relatório selecionado. Para gerar vários relatórios, mantenha pressionada a tecla Control e clique nos relatórios que você deseja gerar. • **Executar relatório em dados brutos** – Selecione esta opção para gerar o relatório selecionado usando dados brutos. Essa opção é útil quando você deseja gerar um relatório antes que os dados acumulados necessários estejam disponíveis. Por exemplo, se desejar executar um relatório semanal antes de uma semana inteira decorrida desde que você criou o relatório, você poderá gerar o relatório usando esta opção. • **Excluir relatório** – Selecione esta opção para excluir o relatório selecionado. Para excluir vários relatórios, mantenha pressionada a tecla Control e clique nos relatórios que você deseja excluir. • **Excluir conteúdo gerado** – 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.
Ocultar relatórios interativos	Selecione esta caixa de seleção para ocultar os modelos de relatórios inativos. A guia **Relatórios** é atualizada automaticamente e exibe apenas os relatórios ativos. Limpe a caixa de seleção para mostrar os relatórios inativos ocultos.
Relatórios de procura	Digite seus critérios de procura no campo **Relatórios de procura** e clique no ícone **Relatórios de Procura**. Uma pesquisa é executada nos parâmetros a seguir para determinar quais correspondem aos seus critérios especificados: • Título do Relatório • Descrição do Relatório • Grupo de Relatórios • Grupos de Relatórios • Nome do Usuário Autor do Relatório

Tipos de diagramas

Cada tipo de gráfico 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 única cor. 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 gráfico disponíveis para cada tipo de diagrama.

Tabela 60. Tipos de diagramas

Tipo de diagrama	Tipos de diagrama disponíveis
Linha	• Eventos/logs • Fluxos • Conexões • Vulnerabilidades

Tabela 60. Tipos de diagramas (continuação)

Tipo de diagrama	Tipos de diagrama disponíveis
Linha Empilhada	• Eventos/logs • Fluxos • Conexões • Vulnerabilidades
Barra	• Eventos/logs • Fluxos • Conexões das vulnerabilidades do ativo • Conexões • Vulnerabilidades
Barra Horizontal	• Principais IPs de Origem • Principais Crimes • Principais IPs de Destino
Barra Empilhada	• Eventos/logs • Fluxos • Conexões
Setor	• Eventos/logs • Fluxos • Vulnerabilidades do Ativo. • Conexões • Vulnerabilidades
Tabela	• Eventos/logs • Fluxos • Principais IPs de Origem • Principais Crimes • Principais IPs de Destino • Conexões • Vulnerabilidades Para exibir o conteúdo de uma tabela, é necessário projetar o relatório com um contêiner de largura de página completa.
Tabela agregada	Disponível com o gráfico Vulnerabilidades do ativo. Para exibir o conteúdo de uma tabela, é necessário projetar o relatório com um contêiner de largura de página completa.

Os seguintes tipos de diagramas estão disponíveis para relatórios do QRadar Log Manager:

- Gráfico de linhas
- Gráfico de linhas empilhadas
- Gráfico de barras
- Gráfico de barras empilhadas
- Gráfico de pizza
- Gráfico de tabela

Criando relatórios customizados

Você pode usar o assistente Relatório para criar um novo relatório.

Antes de Iniciar

Você deve ter permissões da rede apropriada para compartilhar um relatório gerado com outros usuários.

Para obter mais informações sobre permissões, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

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 planejado deverá ter decorrido antes que o relatório gerado retorne os resultados. Para um relatório planejado, você deve esperar o período de tempo planejado para os resultados a serem 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 poderá 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 Bem-vindo ao Relatório, clique em **Avançar** para mover para a próxima página do assistente Relatório.
4. Selecione uma das opções a seguir:

Opção	Descrição
Manualmente	Gera um relatório uma vez. Essa é a configuração padrão; entretanto, você pode gerar esse relatório com a frequência necessária.
Por hora	Planeja o relatório a ser gerado no final de cada hora usando os dados da hora anterior. Se você escolher a opção Por hora, uma configuração adicional será necessária. Nas caixas de listagem, selecione um intervalo de tempo para iniciar e terminar o ciclo do relatório. Um relatório é gerado para cada hora dentro desse período de tempo. O tempo está disponível em incrementos de meia hora. O padrão é 1h para os campos **De** e **Para**.

Opção	Descrição
Semanalmente	Planeja o relatório para ser gerado semanalmente usando os dados da semana anterior. Se você escolher a opção **Semanalmente**, uma configuração adicional será necessária. Selecione o dia que você deseja gerar o relatório. O padrão é segunda-feira. Na caixa de listagem, selecione um horário para iniciar o ciclo do relatório. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã.
Mensalmente	Planeja o relatório para ser gerado mensalmente usando os dados do mês anterior. Se você escolher a opção **Mensalmente**, uma configuração adicional será necessária. Na caixa de listagem, selecione a data que você deseja gerar o relatório. O padrão é o primeiro dia do mês. Além disso, use a caixa de listagem para selecionar uma hora para iniciar o ciclo do relatório. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã.

5. Na área de janela **Permitir 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 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** – digite 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 de 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 Layout de visualização e, em seguida, clique em **Avançar** para mover para a próxima etapa do assistente Relatório.
10. Selecione as caixas de opção para os formatos dos relatórios que você deseja gerar e, em seguida, clique em **Avançar**.

Nota: A Linguagem de Marcação Extensível está disponível somente 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
Console de relatório	Selecione essa caixa de seleção enviar o relatório gerado para a guia **Relatórios**. Esse é o canal de distribuição padrão.
Selecione os usuários que devem ser capazes de visualizar o relatório gerado.	Essa opção será exibida após selecionar a caixa de seleção **Console de relatório**. Na lista de usuários, selecione os usuários que você deseja conceder a permissão para visualizar os relatórios gerados.
Selecionar todos os usuário	Essa opção é exibida somente após selecionar a caixa de seleção **Console de relatório**. Selecione essa caixa de seleção se você desejar conceder a permissão a todos os usuários para visualizar os relatórios gerados. Você deve ter as permissões da rede apropriada para compartilhar o relatório gerado com outros usuários.
Email	Selecione essa caixa de seleção se você desejar distribuir o relatório gerado usando o email.
Insira o(s) endereço(s) de email de distribuição de relatório	Essa opção é exibida somente após selecionar a caixa de seleção **Email**. Insira o endereço de email para cada destinatário de relatório gerado; separe, em uma lista, os endereços de emails com vírgulas. O máximo de caracteres para esse parâmetro é de 255. Os destinatários de email recebem esse email de no_reply_reports@qradar.
Incluir Relatório como anexo (apenas não HTML)	Essa opção é exibida somente após selecionar a caixa de seleção **Email**. Selecione essa caixa de seleção para enviar o relatório gerado como um anexo.
Incluir link no Console de Relatórios	Essa opção é exibida somente após selecionar a caixa de seleção **Email**. Selecione essa caixa de seleção para incluir um link no Console de relatórios no email.

12. Na página Concluindo, insira os valores para os parâmetros a seguir:

Opção	Descrição
Descrição do Relatório	Insira uma descrição para esse relatório. A descrição é exibida na página Resumo do relatório e no email de distribuição de relatório gerado.

Opção	Descrição
Grupos	Selecione os grupos aos quais você deseja designar esse relatório. Para obter mais informações sobre os grupos, consulte Grupos de relatórios.
Deseja executar o relatório agora?	Selecione essa caixa de seleção se você deseja gerar o relatório quando o assistente for concluído. Por padrão, a caixa de seleção fica marcada.

13. Clique em **Avançar** para visualizar o resumo do relatório.
14. Na página Resumo do relatório, selecione as guias disponíveis no relatório do 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 no 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 para alterar.

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, ele 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 tiver gerado conteúdo. 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 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** é exibido na coluna **Relatórios gerados**.

Os ícones que representam o formato do relatório dos relatórios gerados são exibidos na coluna **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 os relatórios que usam um formato de tabela do gráfico único (retrato ou paisagem).

Você pode visualizar apenas os relatórios para os quais tenha recebido acesso do administrador. Os 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. Esta janela de ativação nova 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 de 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 eliminados, mas o modelo de relatório será retido.

Procedimento

1. Clique na guia **Relatório**s.
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 ser gerado 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 é enfileirado para a geração. A mensagem indica a posição que o relatório está na fila. Por exemplo, 1 de 3.

- **(x hora(s) x min.(s) y seg.(s))** – o relatório é planejado para ser executado. A mensagem é um cronômetro de contagem regressiva que especifica quando será a próxima vez que o relatório será executado.

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

Depois que o relatório for gerado, será possível visualizar o relatório gerado na coluna Relatórios gerados.

Duplicando um relatório

Para criar um relatório muito parecido com um relatório existente, você pode duplicar o relatório que 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. Insira 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 fornecerá 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 afetará a versão original do relatório.

Você deve ter os privilégios administrativos para compartilhar os relatórios. Além disso, para um novo usuário visualizar e acessar relatórios, um usuário administrativo deverá compartilhar todos os relatórios necessários com o novo usuário.

Você só pode compartilhar o relatório com usuários que possuam 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 os quais você deseja compartilhar esse relatório.

Registrando relatórios

Para registrar relatórios, você pode importar logotipos e imagens específicas. Para registrar relatórios com logotipos customizados, você deve fazer upload e configurar os logotipos antes de começar a usar o assistente Relatório.

Antes de Iniciar

Assegure-se de que o gráfico que você deseja usar seja de 144 x 50 pixels com um plano de fundo branco.

Para se certificar de que seu navegador exibirá o novo logotipo, limpe o cache do navegador.

Sobre Esta Tarefa

Relatório registrado será benéfico para sua empresa se você suportar mais de um logotipo. Ao fazer upload de uma imagem, a imagem será automaticamente salva como um Portable Network Graphic (PNG).

Ao fazer upload de uma nova imagem e configurá-la como padrão, a nova imagem padrão não será aplicada aos relatórios gerados anteriormente. Atualizar o logotipo nos relatórios gerados anteriormente requer que você gere manualmente um novo conteúdo do relatório.

Se você fizer upload de uma imagem que seja maior em comprimento do que o cabeçalho do relatório pode suportar, a imagem será automaticamente redimensionada para se ajustar ao cabeçalho; aproximadamente 50 pixels de altura.

Procedimento

1. Clique na guia **Relatórios**.
2. No menu de navegação, clique em **Registrando**.
3. Clique em **Procurar** para procurar os arquivos localizados em seu sistema.
4. Selecione o arquivo que contenha o logotipo que você deseja fazer upload. Clique em **Abrir**.
5. Clique em **Fazer upload de imagem**.
6. Selecione o logotipo que você deseja usar como o padrão e clique em **Configurar imagem padrão**.

Grupos de relatórios

Você pode classificar relatórios em grupos funcionais. Se você categorizar relatórios em grupos, poderá organizar de forma eficiente e localizar os relatórios.

Por exemplo, você pode visualizar todos os relatórios que são relacionados à conformidade Payment Card Industry Data Security Standard (PCIDSS).

Por padrão, a guia **Relatórios** exibe a lista de todos os relatórios, no entanto, você pode categorizar relatórios em grupos como:

- Conformidade

- Executivo
- Fontes de log
- Gerenciamento de rede
- Segurança
- VoIP
- Outro

Ao criar um novo relatório, você poderá designar o relatório em um grupo existente ou criar um novo grupo. Você deve ter acesso administrativo para criar, editar ou excluir grupos.

Para obter mais informações sobre funções de usuário, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.

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 sob o qual você deseja criar um novo grupo.
4. Clique em **Novo grupo**.
5. Insira os valores para os parâmetros a seguir:
   - **Nome** – insira o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
   - **Descrição** - opcional. Digite 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 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. Digite 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

Você pode usar a opção **Designar grupos** para designar um relatório para outro grupo.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que você deseja designar para um grupo.
3. Na caixa de listagem **Ações**, selecione **Designar grupos**.
4. Na lista **Grupos de item**, selecione a caixa de seleção do grupo que você 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(s) grupo(s) para o(s) qual(is) 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, ele 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 da rede.

É possível colocar em gráfico dados com diversas características e criar os gráficos em um único relatório gerado.

Parâmetros do contêiner do gráfico Vulnerabilidades do Ativo

A tabela a seguir descreve os parâmetros do contêiner do gráfico Vulnerabilidades do Ativo

Parâmetro	Descrição
Detalhes do contêiner – Ativos	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Subtítulo do gráfico	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 deseja incluir neste relatório.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: • **Tabela agregada** – 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 sub-relatório. A opção **Tabela** está disponível somente para o contêiner com largura de página inteira. • **Barras** – Exibe os dados em um gráfico de barras. Ao selecionar essa opção, o relatório não incluirá dados do sub-relatório. Esse é o padrão. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. • **Pizza** – 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. Para visualizar exemplos de cada tipo de dados do gráfico do diagrama, consulte Consulte tipos de diagramas.
Order Assets By	Selecione o tipo de dados com qual deseja que o gráfico seja ordenado. As opções incluem: • **Peso do ativo** – Ordena os dados pelo peso do ativo que está definido no perfil de ativo. • **Risco CVSS** – Ordena os dados pelo nível de risco do Sistema de Pontuação de Vulnerabilidade Comum (CVSS). Para obter mais informações sobre CVSS, consulte *http://www.first.org/cvss/*. • **Contagem de vulnerabilidade** – Ordena os dados pela contagem de vulnerabilidade dos recursos.
Detalhes do sub-relatório	
Sub-report	Especifica o tipo de informações que são exibidas no sub-relatório.
Order Subreport By	Selecione o parâmetro pelo qual deseja organizar os dados do sub-relatório. As opções incluem: • Risco (pontuação de base) • ID do OSVDB • Título do OSVDB • Última data de modificação • Data de divulgação • Data de descoberta Para obter mais informações sobre o Banco de Dados de Vulnerabilidade de Software Livre (OSVDB), consulte *http://osvdb.org/*.
Limit Sub-report to Top	Na caixa de listagem, selecione quantas vulnerabilidades deseja incluir nesse sub-relatório.
Conteúdo do Gráfico	
Vulnerabilidades	Para especificar as vulnerabilidades que desejar relatar: 1. Clique em **Navegar**. 2. Na caixa de listagem **Procurar por**, selecione o atributo de vulnerabilidade que deseja procurar. As opções incluem ID de CVE ID, ID de Bugtraq, ID de OSVDB ID e Título do OSVDB. Para obter mais informações sobre atributos de vulnerabilidade, consulte Gerenciamento de ativos. 3. Na lista **Resultados da procura**, selecione as vulnerabilidades que deseja relatar. Clique em **Incluir**. 4. Clique em **Enviar**.

Parâmetro	Descrição
Endereço IP	Digite o endereço IP, CIDR ou uma lista delimitada por vírgulas de endereços IP que deseja relatar. Os CIDRs parciais são permitidos.
Redes	Na árvore de navegação, selecione uma ou mais redes a partir das quais são reunidos dados do gráfico.

Parâmetros do contêiner do gráfico Eventos/logs

A tabela a seguir descreve os parâmetros do contêiner do gráfico Eventos/logs

Tabela 61. Parâmetros do contêiner do gráfico Eventos/logs

Parâmetro	Descrição
Detalhes do contêiner – Eventos/logs	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Subtítulo do gráfico	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	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: • **Barras** – 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. • **Linha** – Exibe os dados em um gráfico de linha. • **Pizza** – Exibe os dados em um gráfico de pizza. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. • **Barra empilhada** – Exibe os dados em um gráfico de barras empilhadas. • **Linha empilhada** – Exibe os dados em um gráfico de linhas empilhadas. • **Tabela** – Exibe os dados em formato de tabela. A opção **Tabela** está disponível somente para o contêiner com largura completa de página. Para visualizar exemplos de cada tipo de dados do gráfico do diagrama, consulte Consulte tipos de diagramas.

Tabela 61. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Manual Scheduling	A área de janela Planejamento manual será exibida apenas se for selecionada a opção de planejamento **Manualmente** no assistente de relatório. Usando as opções de Planejamento manual, é possível criar um planejamento manual que pode executar um relatório ao longo de um período de tempo definido customizado, com a opção para incluir apenas dados a partir das horas e dias selecionados. Por exemplo, é possível planejar um relatório para ser executado de 1 de outubro a 31 de outubro, incluindo dados que são gerados apenas durante o horário comercial, como segunda a sexta, 8h às 21h. Para criar um planejamento manual: 1. Na caixa de listagem **De**, digite a data de início que deseja para o relatório, ou selecione a data usando o ícone **Calendário**. O valor padrão é a data atual. 2. Nas caixas de listagem, selecione o horário de início que deseja para o relatório. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã. 3. Na caixa de listagem **Para**, digite a data de encerramento que deseja para o relatório, ou selecione a data usando o ícone **Calendário**. O valor padrão é a data atual. 4. Nas caixas de listagem, selecione o horário de encerramento que deseja para o relatório. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã. 5. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 6. Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de Eventos que estão associados ao evento de procura usado para reunir dados para alguns dos dados relatados. Se o relatório usar dados a partir de vários Processadores de Eventos que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente.
Manual Scheduling (continued)	Para refinar ainda mais seu planejamento: 1. Selecione a caixa de seleção **Seleção de dados de destino**. Opções adicionais são exibidas. 2. Selecione a caixa de seleção **Apenas horas a partir de** e, 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. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.
Hourly Scheduling	A área de janela Planejamento horário será exibida apenas se for selecionada a opção de planejamento **Horário** no assistente de relatório. • Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. • Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de evento 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente. O Planejamento Horário automaticamente cria gráficos de todos os dados da hora anterior.

Tabela 61. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Daily Scheduling	O Planejamento diário será exibido apenas se for selecionada a opção de planejamento **Diário** no assistente de relatório. 1. Escolha uma das opções a seguir: 2. **Todos os dados do dia anterior (24 horas)** 3. **Dados do dia anterior de** – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã. 4. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de evento 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente.
Weekly Scheduling	A área de janela Planejamento semanal será exibida apenas se a opção de planejamento **Semanal** tiver sido selecionada no assistente de relatório. 1. Escolha uma das opções a seguir: 2. **Todos os dados da semana anterior** 3. **Todos os dados da semana passada a partir de** - Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é domingo. 4. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de evento 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente. Para refinar ainda mais seu planejamento: 1. Selecione a caixa de seleção **Seleção de dados de destino**. Opções adicionais são exibidas. 2. Selecione a caixa de seleção **Apenas horas a partir de** e, 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. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.

Tabela 61. Parâmetros do contêiner do gráfico Eventos/logs (continuação)

Parâmetro	Descrição
Monthly Scheduling	A área de janela Planejamento mensal será exibida somente se tiver selecionado a opção planejamento **Mensal** no assistente de relatório. 1. Escolha uma das opções a seguir: 2. **Todos os dados do mês anterior** 3. **Dados do mês anterior do** – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é 1 a 31. 4. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de evento 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente. Para refinar ainda mais seu planejamento: 1. Selecione a caixa de seleção **Seleção de dados de destino**. Opções adicionais são exibidas. 2. Selecione a caixa de seleção **Apenas horas a partir de** e, 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. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.
Conteúdo do Gráfico	
Grupo	Na caixa de listagem, selecione um grupo de procura salvo para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem **Procuras salvas disponíveis**.
Digitar Procura Salva ou Selecionar a partir da Lista	Para refinar a lista **Procuras salvas disponíveis**, digite o nome da procura que deseja localizar no campo **Digitar procura salva ou Selecionar da lista**. É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite *Firewall* 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 **Grupo** ou digitando o nome de uma procura salva conhecida no campo **Digitar procura salva ou Selecionar da lista**.
Criar Nova Procura de Evento	Clique em **Criar nova procura de evento** para criar uma nova procura. Para obter mais informações sobre como criar uma procura de evento, consulte Consultar investigação do log de atividade.

Parâmetros do contêiner do gráfico Fluxos

A tabela a seguir descreve os parâmetros do contêiner do gráfico Fluxos:

Tabela 62. Detalhes do contêiner do gráfico Fluxos

Parâmetro	Descrição
Detalhes do contêiner – Fluxos	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Subtítulo do gráfico	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 62. Detalhes do contêiner do gráfico Fluxos (continuação)

Parâmetro	Descrição
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: • **Barras** – 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. • **Linha** – Exibe os dados em um gráfico de linha. • **Pizza** – Exibe os dados em um gráfico de pizza. Este tipo de gráfico requer que a procura salva seja uma procura agrupada. • **Barra empilhada** – Exibe os dados em um gráfico de barras empilhadas. • **Linha empilhada** – Exibe os dados em um gráfico de linhas empilhadas. • **Tabela** – Exibe os dados em formato de tabela.
Manual Scheduling	A área de janela Planejamento manual será exibida apenas se for selecionada a opção de planejamento **Manualmente** no assistente de relatório. Usando as opções de Planejamento manual, é possível criar um planejamento manual que pode executar um relatório ao longo de um período de tempo definido customizado, com a opção para incluir apenas dados a partir das horas e dias selecionados. Por exemplo, é possível planejar um relatório para ser executado de 1 de outubro a 31 de outubro, incluindo dados que são gerados apenas durante o horário comercial, como segunda a sexta, 8h às 21h. Para criar um planejamento manual: 1. Na caixa de listagem **De**, digite a data de início que deseja para o relatório, ou selecione a data usando o ícone **Calendário**. O valor padrão é a data atual. 2. Nas caixas de listagem, selecione o horário de início que deseja para o relatório. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã. 3. Na caixa de listagem **Para**, digite a data de encerramento que deseja para o relatório, ou selecione a data usando o ícone **Calendário**. O valor padrão é a data atual. 4. Nas caixas de listagem, selecione o horário de encerramento que deseja para o relatório. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã. 5. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 6. Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de eventos que são 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente.
	Para refinar ainda mais seu planejamento: 1. Selecione a caixa de seleção **Seleção de dados de destino**. Opções adicionais são exibidas. 2. Selecione a caixa de seleção **Apenas horas a partir de** e, 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. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.

Tabela 62. Detalhes do contêiner do gráfico Fluxos (continuação)

Parâmetro	Descrição
Hourly Scheduling	A área de janela Planejamento horário será exibida apenas se for selecionada a opção de planejamento **Horário** no assistente de relatório. • Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. • Ao configurar o parâmetro **Timezone**, considere o local dos Processadores de eventos que são 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente. O Planejamento Horário automaticamente cria gráficos de todos os dados da hora anterior.
Daily Scheduling	O Planejamento diário será exibido apenas se for selecionada a opção de planejamento **Diário** no assistente de relatório. 1. Escolha uma das opções a seguir: 2. **Todos os dados do dia anterior (24 horas)** 3. **Dados do dia anterior de** – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O tempo está disponível em incrementos de meia hora. O padrão é 1h da manhã. 4. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro **Timezone**, 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente.
Weekly Scheduling	A área de janela Planejamento semanal será exibida apenas se a opção de planejamento **Semanal** tiver sido selecionada no assistente de relatório. 1. Escolha uma das opções a seguir: 2. Todos os dados da semana anterior 3. **Todos os dados da semana passada a partir de** - Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é domingo. 4. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro **Timezone**, 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente. Para refinar ainda mais seu planejamento: 1. Selecione a caixa de seleção **Seleção de dados de destino**. Opções adicionais são exibidas. 2. Selecione a caixa de seleção **Apenas horas a partir de** e, 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. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.

Tabela 62. Detalhes do contêiner do gráfico Fluxos (continuação)

Parâmetro	Descrição
Monthly Scheduling	A área de janela Planejamento mensal será exibida somente se tiver selecionado a opção planejamento **Mensal** no assistente de relatório. 1. Escolha uma das opções a seguir: 2. **Todos os dados do mês anterior** 3. **Dados do mês anterior do** – Nas caixas de listagem, selecione o período de tempo que deseja para o relatório gerado. O padrão é 1 a 31. 4. Na caixa de listagem **Fuso horário**, selecione o fuso horário que deseja usar para o relatório. 5. Ao configurar o parâmetro **Timezone**, 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 que ampliam vários fusos horários, o fuso horário configurado poderá estar incorreto. Por exemplo, se o seu relatório estiver associado aos dados coletados a partir dos Processadores de eventos na América do Norte e Europa, e o fuso horário for configurado como **GMT -5.00 America/New_York**, os dados da Europa relatarão o fuso horário incorretamente. Para refinar ainda mais seu planejamento: 1. Selecione a caixa de seleção **Seleção de dados de destino**. Opções adicionais são exibidas. 2. Selecione a caixa de seleção **Apenas horas a partir de** e, 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. 3. Selecione a caixa de seleção para cada dia da semana para o qual deseja programar o relatório.
Conteúdo do Gráfico	
Grupo	Na caixa de listagem, selecione um grupo de procura salvo para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem **Procuras salvas disponíveis**.
Digitar Procura Salva ou Selecionar a partir da Lista	Para refinar a lista **Procuras salvas disponíveis**, digite o nome da procura que deseja localizar no campo **Digitar procura salva ou selecionar na lista**. É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite: `Firewall` para exibir uma lista de todas as procuras que incluem Firewall 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 **Grupo** ou digitando o nome de uma procura salva conhecida no campo **Digitar procura salva ou Selecionar da lista**.
Criar Nova Procura de Fluxo	Clique em **Criar nova procura de fluxo** para criar uma nova procura.

Parâmetros de contêiner do gráfico de IPs de Principais Origens

A tabela a seguir descreve os parâmetros do contêiner do gráfico de IPs de Principais Origens

Parâmetro	Descrição
Detalhes do contêiner – IPs de principais origens	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Subtítulo do gráfico	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limite os IPs de Principais Origens para	Na caixa de listagem, selecione o número de IPs de origem a serem exibidos no relatório gerado.

Parâmetro	Descrição
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico a ser exibido no relatório gerado. As opções incluem: • **Tabela** exibe os dados no formato de tabela (com contêiner de largura total apenas). • **Barra horizontal** Exibe os dados em um gráfico de barras.
Ordenar resultados por	Na caixa de listagem, selecione como os dados são classificados no gráfico. As opções incluem: • Peso do ativo • Risco • Magnitude
Conteúdo do Gráfico	
Redes	Na árvore de navegação, selecione uma ou mais redes a partir das quais são reunidos dados do gráfico.

Parâmetros de contêiner do gráfico de Principais Ofensas

A tabela a seguir descreve os parâmetros do contêiner do gráfico de Principais Ofensas

Tabela 63. Parâmetros de contêiner do gráfico de Principais Ofensas

Parâmetro	Descrição
Detalhes do Contêiner – Principais Ofensas	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Subtítulo do gráfico	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limite as Principais Ofensas para	Na caixa de listagem, selecione o número de ofensas para 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: • **Tabela** – Exibe os dados em formato de tabela (contêiner de largura total apenas). • **Barra Horizontal** – Exibe os dados em um gráfico de barras.
Ordenar Resultados por:	Na caixa de listagem, selecione como os dados são classificados no gráfico. As opções incluem: • Gravidade • Magnitude • Relevância • Credibilidade
Conteúdo do gráfico – baseado em parâmetro	
Baseado em Parâmetro	Selecione essa opção se você desejar incluir um gráfico de Principais Ofensas baseado em parâmetro em seu relatório. Quando esta opção é selecionada, os parâmetros **Incluir**, **Categoria de ofensas** e **Redes** são exibidos.
Incluir	Essa opção só será exibida se a opção **Baseado em parâmetro** for selecionada. Selecione a caixa de seleção ao lado da opção que você deseja incluir no relatório gerado. As opções são: • Crimes Ativos • Crimes Inativos • Crimes Ocultos • Crimes Encerrados As opções **Ofensas ativas** e **Ofensas inativas** são selecionadas por padrão. Se você limpar todas as caixas de seleção, nenhuma restrição será aplicada ao relatório gerado; portanto, o relatório gerado inclui todas as ofensas.

Tabela 63. Parâmetros de contêiner do gráfico de Principais Ofensas (continuação)

Parâmetro	Descrição
Categoria de ofensas	Essa opção só será exibida se a opção **Baseado em parâmetro** for selecionada. Na caixa de listagem **Categoria de alto nível**, selecione a categoria de alto nível que você deseja incluir no relatório gerado. Na caixa de listagem **Categoria de baixo nível**, selecione uma categoria de baixo nível que você deseja incluir no relatório gerado. Para obter mais informações sobre categorias de alto e de baixo nível, consulte o *Guia de Administração do IBM Security QRadar Network Anomaly Detection*.
Redes	Essa opção só será exibida se a opção **Baseado em parâmetro** for selecionada. Na árvore de navegação, selecione uma ou mais redes a partir das quais são reunidos dados do gráfico.
Conteúdo do gráfico – baseado em Procura Salva	
Baseado em Procura Salva	Selecione essa opção se quiser incluir um gráfico de Principais Ofensas baseado em procura salva em seu relatório. Quando essa opção estiver selecionada, os parâmetros **Grupo, digitar procura salva ou selecionar na lista e procuras salvas disponíveis** serão exibidos.
Grupo	Na caixa de listagem, selecione um grupo de procura salvo para exibir as procuras salvas pertencentes a esse grupo na caixa de listagem **Procuras salvas disponíveis**.
Digitar Procura Salva ou Selecionar a partir da Lista	Para refinar a lista **Procuras salvas disponíveis**, digite o nome da procura que deseja localizar no campo **Digitar procura salva ou Selecionar da lista**. É possível também digitar uma palavra-chave para exibir uma lista de procuras que incluem essa palavra-chave. Por exemplo, digite `Firewall` 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 **Grupo** ou digitando o nome de uma procura salva conhecida no campo **Digitar procura salva ou Selecionar da lista**.

Parâmetros do contêiner do gráfico de IP de Principais Destinos

A tabela a seguir descreve os parâmetros do contêiner do gráfico de IPs de Principais Destinos:

Tabela 64. Parâmetros do contêiner do gráfico de IP de Principais Destinos

Parâmetro	Descrição
Detalhes do contêiner – IPs de Principais Destinos	
Título do Gráfico	Digite um título de gráfico de, no máximo, 100 caracteres.
Subtítulo do gráfico	Limpe a caixa de seleção para alterar o subtítulo criado automaticamente. Digite um título de, no máximo, 100 caracteres.
Limite os IPs de Principais Destinos para	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: • **Tabela** – Exibe os dados em formato de tabela (contêiner de largura total apenas). • **Barra Horizontal** – Exibe os dados em um gráfico de barras.
Ordenar resultados por	Na caixa de listagem, selecione como os dados são exibidos no gráfico. As opções incluem: • Peso do ativo • Nível de risco • Magnitude
Conteúdo do Gráfico	
Redes	Na árvore de navegação, selecione uma ou mais redes a partir das quais são reunidos 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

IBM, o logotipo IBM e 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 ™), estes símbolos indicarão marcas registradas dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações forem publicadas. Essas marcas também podem ser marcas registradas ou marcas 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).

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.

Os logotipos da Microsoft, Windows NT e do Windows são marcas registradas da Microsoft Corporation nos Estados Unidos, outros países ou ambos.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviços 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 186 "E" na página 186 "F" na página 186 "G" na página 186 "H" na página 187 "I" na página 187 "L" na página 187 "M" na página 187 "N" na página 188 "O" na página 188 "P" na página 189 "R" na página 189 "S" na página 190 "T" na página 190 "V" na página 190

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 quantia 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 críptica 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 decriptografia.

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 uma ofensa 29
administrador da rede ix
agregar pontuação CVSS 136
ajuda 12
ajuda online 12
ajustando positivos falsos 65
Ajustando positivos falsos 81
ameaça 13
aplicativo 13
área de janela de correções do Windows, 135, 150
área de janela de interface de rede 135, 150
Área de janela de pacotes 135, 150
Área de janela de parâmetros de vulnerabilidade 152
Área de janela de políticas de risco 135, 150
Área de janela de produtos 135, 150
área de janela de propriedades 135, 150
Área de janela de serviços 135, 150
Área de janela de vulnerabilidade 135, 150
assistente de regras customizadas 7, 18
assistente Regra de Detecção de Anomalias 120
ativar regras 122
atividade de log 9, 12, 13, 20, 23, 51, 64, 65, 85, 86, 87, 89, 103, 104, 105, 106, 107, 109, 115
  critérios de procura 92
  visão geral 51
atividade de rede 9, 12, 13, 15, 20, 23, 71, 74, 75, 85, 86, 87, 89, 92, 102, 103, 104, 105, 106, 107, 109, 115
ativos 5, 12, 13
atualizar dados 9
atualizar detalhes do usuário 11

B

barra de atividade de log 53
barra de ferramentas 51
Barra de ferramentas da guia Atividade de rede 71
barra de ferramentas da página de regras 127
barra de ferramentas de atividade de rede 72
barra de ferramentas detalhes do evento 63
Barra de ferramentas Detalhes do fluxo 81
barra de status 54, 158
Barra de status 74
blocos de construção 117
  editando 126

C

caixa de lista de exibição 58, 77
cancelar uma procura 104
centro de informações de ameaças da internet 19
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 167
configurando atividade de log 21
configurando atividade de rede 21
configurando conexões 21
configurando gráficos 87
configurando itens do painel 21
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 170
conteúdo da ajuda 12
copiar procura salva 107, 146
copiar um item para um grupo 125
copiar uma regra 123
criando grupos de procura 105
criando regras customizadas 119
criando um novo grupo de procura 106
criar novo grupo de procura 145
criar relatórios 6
criar um grupo de regras 124
critérios de filtro de fluxo 73
critérios de procura
  excluindo 102
  guia atividade de log 102
  salvando 92
  salvos disponíveis 102
critérios de procura salvos 15
customizar painéis 15

D

dados de captura de pacote (PCAP) 66
dados de configuração 6
dados do evento bruto 57
dados do evento não analisados 57
dados do PCAP 66, 67
desativar regras 122
descrição do evento 61
designar items a um grupo 125
desproteger as ofensas 32
detalhes da vulnerabilidade 148
detalhes do evento 63
detalhes do evento único 61
detalhes do fluxo 75, 79
dispositivo 6
distribuir relatórios 6
download do arquivo de dados do PCAP 67
Duplicar um relatório 167

E

editar ativo 139
editar blocos de construção 126
editar grupo de procura 145
editar um grupo 125
Editar um grupo 169
editar um grupo de procura 106
endereço IP 9, 136
endereços IP de destino 25
endereços IP de origem 25
especificar o número de objetos de dados para visualizar 21
especificar tipo de gráfico 21
eventos 17, 63, 87, 89
eventos de fluxo 55
eventos de monitoramento 16
eventos normalizados 56
exceção de segurança 3
excluindo ativos 147
excluindo uma procura 105
excluir opção 32
excluir painel 22
excluir perfil do ativo 146
excluir uma regra 123
executando uma procura 103
executar dados 9
exibir em uma nova janela 22
exibir itens 17
exportando ativos 147
exportando eventos 68
Exportando fluxos 82
exportar ofensas 33
exportar para CSV 82
exportar para XML 82
exportar perfil do ativo 146

F

falso positivo 65, 81
fazer download do arquivo 68
fechando ofensas 31
filtro rápido 53, 89
fluxos 17, 71, 87, 89
fluxos de fluxo 74
fluxos normalizados 75
funções 117
funções da barra de ferramentas 36
funções da barra de ferramentas de detalhes do evento 63

G

gerar um relatório manualmente 166
Gerenciador de Vulnerabilidade QRadar 135

gerenciamento de gráfico 85
gerenciamento de grupo de regra 124
gerenciamento de ofensa 25
gerenciamento de regra 115, 122
gerenciamento do painel 13
gerenciando grupos de procura 105
Gerenciar grupos 146
gerenciar grupos de procura 101
gerenciar rede 136
gerenciar relatórios 6, 159
gerenciar resultados da procura 104, 105
glossário 185
gráfico de série temporal 86
grupo
  copiando um item 125
  designando itens 125
  editando 125
  excluindo 126
  excluindo um item 126
  removendo 107
grupo de procura
  criando 106
  editando 106
grupo de procura de evento 105, 106
grupo de procura de fluxo 105, 106
grupo de procura de ofensa 106
grupo de regras
  criando 124
  visualização 124
grupos de fluxo 79
grupos de procura
  gerenciando 105
  visualização 105
grupos de procura de ativos 144
Guia administração 6, 26
guia atividade de log 5, 8, 51, 54, 55, 56, 57, 58, 63, 66, 68, 89
guia atividade de rede 5, 8, 71, 77, 89
Guia Atividade de rede 73, 74, 75, 81, 82
guia ativo 135, 136, 137, 144
guia ativos 5, 136, 138, 139, 144, 145, 146, 147
guia minhas ofensas 94
guia ofensa 31, 36, 98, 100, 101
guia ofensas 8, 25, 30, 31, 32, 33, 35, 38
Guia ofensas 5, 101
guia padrão 4
guia painel 4, 7, 13, 15, 19, 20, 21, 22
Guia Painel 4, 16, 17
guia relatório 159
guia relatórios 8
Guia Relatórios 6
guia Riscos 17
guia todas as ofensas 94
guias 4
guias da interface com o usuário 4

H

hosts 5

I

IBM Security QRadar Risk Manager 6
ícone remover 146
ID 136
identificação de painel 15
imagem
  fazer upload 168
  relatórios
    registrando 168
importar ativos 147
importar perfil do ativo 146
imprimir perfil de ativo 136
incluindo itens de eventos 23
incluindo itens de procura de fluxo 23
incluir ativo 136, 139
incluir filtro 72, 103
incluir item 15
incluir itens 23
incluir nota 30
incluir um item de painel 14
informações de login 4
informações de login padrão 4
informações do filtro de eventos 137
informações sobre o usuário 11
interface com o usuário 4
introdução ix
investigando eventos 16
investigar 71
investigar atividade de log 51
investigar atividade de rede 71
investigar ativo 136
investigar evento 25
investigar fluxo 25
investigar fluxos 5
investigar logs de eventos 5
investigar ofensa 5
Item de painel de Notificação do Sistema 18
item de painel Resumo do Sistema 17
item do painel 23
item do painel customizado 15
Itens de ofensa 15
itens de procura de conexão 17
itens do painel atividade de log 16
itens do painel de ofensa 15

J

janela grupos de procura 105

L

Layout de relatório 158
legendas do gráfico 87
lista de eventos 61
lista de fluxos em vários modos 79

M

manter regra customizada 115
manter regras customizadas 115
mapear evento 64
marcar ofensa para acompanhamento 35
mensagem de notificação 18
menu ativado pelo botão direito 54, 73
menu de mensagens 7
menu de navegação 26
modificar mapeamento de evento 64
modo de fluxo 75
monitoramento da atividade de rede 74
monitorando ofensas 29
monitorar 71
monitorar ofensas 27, 28
monitorar rede 71
mostrar painel 15, 19, 21, 22

N

Navegador da web Microsoft Internet Explorer 4
navegadores da web
  versões suportadas 3
navegue QRadar SIEM 3
nível de ameaça atual 19
nível de ameaça da internet 19
nome de usuário 4
nome do ativo 136
nomes de usuários 10
notificação do sistema 23
notificação por email 34
notificações do sistema 7
nova procura 145
novo painel 19
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, 105, 106, 107, 115
  designando a usuários 34
ofensas atualizadas 17
ofensas de grupo por IP de origem 28
ofensas ocultas 31
ofensas por categoria 27
ofensas por IP de destino 28
ofensas por rede 29
opções de eventos agrupados 58
opções do menu ativado pelo botão direito 137
organizar seus itens do painel 13
origem de log 57

P

página de perfis de ativos 136
página de procura de ativo 142
página detalhes do evento 61
página do perfil de ativo 148, 150, 151, 152, 153, 154
página IP de origem 98
Página Minhas ofensas 27
página por IP de destino 100
página por rede 101
Página Todas as ofensas 27
painel 23
painel customizado 14, 17, 19
painel de Gerenciador de Risco 17

painel de gerenciamento de vulnerabilidade 17
parâmetros da área de janela de políticas de risco 154
Parâmetros da área de janela de produtos 154
Parâmetros da área de janela de propriedades 154
parâmetros da área de janela de resumo de interface de rede 151
Parâmetros da área de janela de serviços 153
parâmetros da área de janela do resumo de ativo 150
parâmetros de área de janela de correções do Windows 154
Parâmetros de área de janela de pacotes 153
parâmetros de área de janela de serviço do Windows 153
parâmetros de eventos agrupados 58
parâmetros de ofensa 38
parâmetros de página do perfil de ativos 135, 150
parâmetros de regra 127
pausar dados 9
perfil de ativos 138, 139
perfis de ativos 135, 144, 147
Perfis de ativos 146
Perfis de Ativos 145, 146
permissão de ofensa 25
permissão de regra 115
permissão do nível de dispositivo 25
permissões
  propriedades customizadas 109
positivos falsos 135
principais ofensas 179
processador de evento 74
processadores de evento 74
procura 145
  copiando para um grupo 107
procurando 89
procurando ofensas 25, 94, 98, 100, 101
procurando perfis de ativos 142
procurar por ativo 136
procuras da ofensa 94
procuras de dados 89
procuras de evento e de fluxo 89
procuras de fluxo 15
propriedade
  copiando customizada 114
  modificando customizada 113
propriedade customizada 114
propriedade de cálculo 111
propriedade regex 110
propriedades de evento e fluxo customizadas 109
protegendo ofensas 32

Q

QID 64

R

rede 13, 29
redimensionar colunas 12
Registros de estouro 74
regra
  copiando 123
  editar 122
  respostas 117
regra comum 116
regra de detecção de anomalias 120
regra de evento 116
regra de fluxo 116
regra de ofensa 116
regras 115, 117
  ativando 122
  desativando 122
  visualização 118
regras customizadas 115
regras de detecção de anomalias 115
relatório
  editando 165
relatórios 12, 13
  visualização 166
relatórios customizados 161
relatórios mais recentes gerados 16
remover grupo 107, 146
remover item do painel 21
remover procura salva 146
remover procura salva de um grupo 107
remover um item do painel 22
renomear painel 22
Resposta de Regra 128
resultados da procura
  cancelar 104
  excluindo 105
  gerenciando 104
resultados do processador de evento 54
resumo de atividade nas últimas 24 horas 17
resumo de ofensa 34
retenção de ofensa 32

S

salvando critérios de procura 101
salvando critérios de procura de evento e de fluxo 55
salvar critério 144
salvar critério de procura de ativo 144
Salvar critérios 101
scanner de terceiros 135
segurança 13
senha 4
Serviços 136
servidores 5
Sinalizador 18
sintaxe do 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 117
tipo de propriedade calculado 109
tipo de propriedade regex 109
tipos de diagramas 160
tipos de gráfico 158
tipos de propriedade 109

U

último minuto (atualização automática) 9

V

vários painéis 13
visão geral de gráficos 85
visualização de compatibilidade 4
visualização de dados do PCAP 67
visualização de eventos agrupados 58
visualização de mensagens 7
visualização do grupo de regra 124
visualização do perfil de ativos 138
visualizando eventos de fluxo 55
visualizando fluxos agrupados 77
visualizando fluxos de fluxo 75
visualizando grupos de procura 105, 144
visualizando ofensas associadas a eventos 63
visualizar ativos 136
visualizar notificações do sistema 23
visualizar regras customizadas 115
vulnerabilidades 135
Vulnerabilidades 136
vulnerabilidades do ativo 148