IBM Security QRadar
Versão 7.2.5

Guia do Usuário

Observação

Antes de utilizar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 205.

Informações do produto

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

Índice

Sobre este guia

O Guia dos usuários do IBM® Security QRadar SIEM fornece informações sobre o gerenciamento do IBM Security QRadar SIEM, incluindo as guias Painel, Ofensas, Atividade de log, Atividade de rede, Ativos e Relatórios.

Público alvo

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

Documentação técnica

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

Entrando em contato com o suporte ao cliente

Para obter informações sobre como contatar o suporte ao cliente, consulte Suporte e download da nota técnica (http://www.ibm.com/support/ docview.wss?uid=swg21616144).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou 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 fazer parte de uma abordagem de segurança abrangente legal que, necessariamente, envolverá procedimentos operacionais adicionais, podendo precisar de outros sistemas, produtos ou serviços para se tornar mais efetiva. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

Observe:

O uso deste Programa pode implicar várias leis ou regulamentos, incluindo aqueles relacionados à privacidade, à proteção de dados, ao emprego, às comunicações eletrônicas e ao armazenamento. O IBM Security QRadar pode ser usado apenas para propósitos legais e de uma forma legal. O cliente concorda em usar este Programa conforme as leis, os regulamentos e as políticas aplicáveis e assume toda a responsabilidade de obedecê-los. O licenciado declara que irá obter ou obteve quaisquer consentimentos, permissões ou licenças necessários para ativar o uso legal do IBM Security QRadar.

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

O IBM Security QRadar V7.2.5 apresenta a correlação de histórico, aprimoramentos de relatório, clique com o botão direito no endereço IP e consultas URL para IBM Security X-Force Exchange e novas funções de consulta de Linguagem de consulta Ariel (AQL) para X-Force e mais.

Use correlação histórica para analisar os eventos decorridos

Use a correlação histórica ao analisar os eventos que foram carregados em massa, testar novas regras e recriar ofensas que foram perdidas ou limpas. Saiba mais...

Integração do X-Force Exchange com QRadar

Use X-Force Exchange para coletar e consultar endereços IP e obter informações adicionais sobre URLs que foram identificadas por QRadar em eventos, regras, fluxos e ofensas. É possível encaminhar qualquer endereço IP que seja exibido em QRadar para X-Force Exchange. Também é possível usar URLs de eventos na guia **Atividade de log**. Saiba mais...

Aprimoramentos de relatório

É possível compartilhar os relatórios com grupos de usuários. É possível incluir um relatório em um grupo de relatórios que é compartilhado com qualquer pessoa ou um grupo que esteja compartilhado somente com usuários que possuem funções de usuário específico e perfis de segurança. Saiba mais...

É possível configurar uma classificação para um relatório, como confidencial ou somente interno, que aparece no cabeçalho do relatório e rodapé. Também é possível incluir números de página e criar relatórios que sejam baseados em procuras de ativos salvas. Saiba mais...

Opções de pesquisa mais avançadas

Use o operador TEXT SEARCH para executar procura de texto completas e localizar o texto específico nas propriedades customizadas para eventos e fluxos. Saiba mais...

Funções de consulta de Linguagem de consulta Ariel (AQL)

Use as novas funções de consulta AQL X-Force para consultar o endereço IP X-Force e categorizações de URL. As categorizações podem ser usadas nos dados do resultado da consulta ou podem ser usados para filtrar eventos e fluxos.

Saiba mais...

Modificar uma regra customizada mantém as informações de estado para todas as regras

Ao editar uma regra customizada e salvar as mudanças, somente a regra que você está modificando e quaisquer regras que dependam dessa regra são afetadas. Todas as informações de estado, contadores e resultados de regra para outras regras são mantidas. Nas liberações anteriores, quando você editou uma regra customizada, todas as regras e contadores no mecanismo de regra customizada foram reconfiguradas. Por exemplo, se você estiver rastreando uma sequência de eventos, como 5 logons com falha seguidos por um logon bem-sucedido, a contagem foi reconfigurada quando modificou e salvou alguma regra.

Para obter mais informações, consulte Contador de texto de regra APAR (http://www-01.ibm.com/support/docview.wss?crawler=1&uid=swg1IV46111).

Capítulo 2. Sobre a QRadar SIEM

QRadar SIEM é uma plataforma de gerenciamento de segurança de rede que fornece reconhecimento situacional e suporte a conformidade através da combinação de conhecimento de rede baseado em fluxo, correlação de eventos de segurança e de avaliação de vulnerabilidades baseado em ativo.

Chave de licença padrão

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

Exceções e certificados de segurança

Se você estiver usando o navegador da web Mozilla Firefox, você deverá incluir uma exceção para o Mozilla Firefox 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. Você deve selecionar a **Continuar com esta opção de website** para efetuar login no QRadar SIEM.

Navegue para o aplicativo baseado na web

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

Navegadores da Web Suportados

Para os recursos em produtos IBM Security QRadar funcionarem corretamente, você deve usar um navegador da Web suportado.

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

A tabela a seguir lista as versões suportadas dos navegadores da Web.

Tabela 1. Navegadores da Web Suportados para Produtos QRadar

Navegador da Web	Versões suportadas
Mozilla Firefox	17.0 24.0
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegação ativados	9.0 10.0

Tabela 1. Navegadores da Web Suportados para Produtos QRadar (continuação)

Navegador da Web	Versões suportadas
Google Chrome	A versão atual a partir da data de liberação de produtos IBM Security QRadar V7.2.4

Ativando o Modo de Documento e o Modo de Navegador no Internet Explorer

Se usar o Microsoft Internet Explorer para acessar os produtos IBM Security QRadar, você deve ativar o modo de navegação e o modo de documento.

Procedimento

1. No seu navegador da Web Internet Explorer, pressione F12 para abrir a janela Ferramentas do Desenvolvedor.
2. Clique em **Modo de navegador** e selecione a versão do seu navegador da Web.
3. Clique em **Modo de Documento**.
   - Para o Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**.
   - Para o Internet Explorer V10.0, selecione **Padrões do Internet Explorer 10**.

Login do 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 em seu console do IBM Security QRadar.

Tabela 2. Informações de login padrão do QRadar

Informações de login	Padrão
URL	https://<Endereço IP>, em que <Endereço IP> é o endereço IP do console do QRadar. Para efetuar login para o QRadar em um IPv6 ou em um ambiente misto, agrupe os endereços IP em colchetes: `https://[<IP Address>]`
Nome de usuário	admin
Senha	A senha que é designada ao QRadar durante o processo de instalação.
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

API RESTful

Use a interface de programação de aplicativos (API) representational state transfer (REST) para fazer consultas HTTPS e integrar o IBM Security QRadar a outras soluções.

Acesso e permissões de função de usuário

Deve-se ter permissões de função de usuário administrativo no QRadar para acessar e usar APIs RESTful. Para obter mais informações sobre como gerenciar permissões de função de usuário, consulte o *IBM Security QRadar SIEM Administration Guide*.

Acessar a interface com o usuário da documentação técnica da API REST

A interface com o usuário da API fornece descrições e recursos para as interfaces da API REST a seguir:

Tabela 3. Interfaces API REST

API REST	Descrição
`/api/ariel`	Consultar bancos de dados, procuras, IDs de procura e resultados da procura.
`/api/asset_model`	Retorna uma lista de todos os ativos no modelo. Também é possível listar todos os tipos de propriedade de ativo e procuras salvas disponíveis e atualizar um ativo.
`/api/auth`	Efetuar logout e invalidar a sessão atual.
`/api/help`	Retorna uma lista de recursos de API.
`/api/siem`	Retorna uma lista de todas as ofensas.
`/api/qvm`	Revise e gerencie os dados do QRadar Vulnerability Manager.
`/api/reference_data`	Visualize e gerencie coletas de dados de referência.
`/api/qvm`	Recupera ativos, vulnerabilidades, redes, serviços abertos, redes e filtros. Também é possível criar ou atualizar chamados de remediação.
`/api/scanner`	Visualize, crie ou inicie uma varredura remota relacionada a um perfil de varredura.

A interface de documentação técnica da API REST fornece uma estrutura que pode ser usada para reunir o código requerido do qual você precisa para implementar funções do QRadar em outros produtos.

1. Insira a URL a seguir no seu navegador da web para acessar a interface de documentação técnica: `https://`*`ConsoleIPaddress`*`/api_doc/`.
2. Clique no cabeçalho para a API que você deseja acessar, por exemplo, **/ariel**.
3. Clique no subcabeçalho para o endpoint que você deseja acessar, por exemplo, **/databases**.
4. Clique no subcabeçalho Experimental ou Provisório.

Nota:

Os endpoints da API são anotados como *experimental* ou *estável*.

Experimental
Indica que o endpoint da API talvez não esteja totalmente testado e pode ser alterado ou removido no futuro sem qualquer aviso.

Estável
Indica que o endpoint da API está totalmente testado e é suportado.

5. Clique em **Testar** para receber respostas HTTPS apropriadamente formatadas.
6. Revise e reúna as informações que você precisa implementar em sua solução de terceiro.

Fórum da API e amostras de código do QRadar

O fórum da API fornece mais informações sobre a API REST, incluindo as respostas para as perguntas mais frequentes e as amostras de código anotadas que você pode usar em um ambiente de teste. Para obter mais informações, consulte Fórum da API (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

Guias da interface com o usuário

A funcionalidade é dividida em guias. A guia **Painel** é exibida quando você efetua login.

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

Guia Painel

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

A guia **Painel** fornece um ambiente de área de trabalho que suporta vários painéis 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 itens que fornecem informações de resumo e detalhadas sobre os crimes que ocorrem em sua rede. É possível também criar um painel customizado para permitir que sejam concentradas suas responsabilidades de operação de rede ou de segurança. Para obter mais informações sobre como usar a guia Painel, consulte Gerenciamento de painel.

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

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

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

Guia Atividade de rede

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

Um fluxo é uma sessão de comunicação entre dois hosts. Visualizar informações de fluxo permitirá que 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 operacionais em sua rede.

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

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

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

Para obter mais informações, consulte Gerenciamento de ativos.

Guia Relatórios

A guia **Relatórios** permitirá criar, distribuir e gerenciar relatórios para quaisquer dados noQRadar.

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

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

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

IBM Security QRadar Risk Manager

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

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

Tabela 4. Ferramentas de gerenciamento de administração disponíveis em QRadar

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

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

Procedimentos comuns do QRadar

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

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

Visualizando mensagens

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

Antes de Iniciar

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

Sobre Esta Tarefa

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

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

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

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

Tabela 5. Funções disponíveis na janela de mensagens

Função	Descrição
Todos	Clique em **Todos** para visualizar todas as notificações do sistema. Essa 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 severidade de funcionamento.
Erros	Clique em **Erros** para visualizar apenas as notificações do sistema que tenham um nível de severidade de erro.
Avisos	Clique em **Avisos** para visualizar apenas as notificações do sistema que tenham um nível de severidade de aviso.
Informações	Clique em **Informações** para visualizar apenas as notificações do sistema que tenham um nível de severidade de informações.
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 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 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 no QRadar.
2. No canto superior direito da interface com o usuário, clique em **Mensagens**.
3. Na janela **Mensagens**, visualize os detalhes de notificação do sistema.

4. Opcional. Para refinar a lista de notificações do sistema, clique em uma das opções a seguir:
   - **Erros**
   - **Avisos**
   - **Informações**
5. Opcional. Para fechar notificações do sistema, escolha uma das opções a seguir:

Opção	Descrição
Descartar todos	Clique para fechar todas as notificações do sistema.
Descartar	Clique no ícone **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

É possível atualizar, pausar e executar manualmente os dados exibidos nas guias.

Sobre Esta Tarefa

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

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

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

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

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

Procedimento

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

Opção	Descrição
Atualizar	Clique em **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 o cronômetro estiver pausado.

Investigando endereços IP

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

Procedimento

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

Tabela 6. Informações de endereços IP

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

Tabela 6. Informações de endereços IP (continuação)

Opção	Descrição
Informações > **Perfil de ativo**	Exibe informações do perfil de ativos. Essa opção será exibida se o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*. Essa opção de menu estará disponível se o QRadar adquiriu os dados de perfil ativamente através de uma varredura ou passivamente através de fontes de fluxo. Para obter informações, consulte *IBM Security QRadar SIEM Administration Guide*.
Informações > **Procurar eventos**	Procura por eventos associadas a esse endereço IP.
Informações > **Procurar fluxos**	Procura por fluxos associados a esse endereço IP.
Informações > **Procurar conexões**	Procura por conexões associados a esse endereço IP. Essa opção será exibida somente se você comprou oIBM Security QRadar Risk Manager e conectou o QRadar e o dispositivo do IBM Security QRadar Risk Manager. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*.
Informações > **Consulta de porta de comutador**	Determina a porta do comutador em um dispositivo Cisco IOS para esse endereço IP. Essa opção aplica-se somente a comutadores descobertos usando a opção **Descobrir dispositivos** na guia **Riscos**. **Nota:** Essa opção de menu não está disponível em QRadar Log Manager
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.
Executar Varredura de Vulnerabilidade	Selecione a opção **Executar Varredura de Vulnerabilidade** para uma varredura do IBM Security QRadar Vulnerability Manager nesse endereço IP. Essa opção será exibida somente quando o IBM Security QRadar Vulnerability Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Investigar nomes de usuário

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

Será possível investigar nomes de usuários quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter mais informações, consulte *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 7. Opções do menu para investigação do nome de usuário

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

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

Tempo do sistema

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

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

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

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

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

Atualizando preferências do usuário

É possível configurar as preferências do usuário, como código de idioma, na principal interface com o usuário do IBM Security QRadar SIEM.

Procedimento

1. Para acessar as informações sobre o usuário, clique em **Preferências**.
2. Atualizar as preferências.

Opção	Descrição
Nome de usuário	Exibe seu nome de usuário. Não é possível editar este campo.

Opção	Descrição
Senha	A senha deve atender aos seguintes critérios: • Mínimo de 6 caracteres • Máximo de 255 caracteres • Conter pelo menos 1 caractere especial • Conter 1 caractere maiúsculo
Password (Confirm)	Confirmação de senha
Email Address	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 você escolher um idioma diferente, a interface com o usuário será exibida em inglês. Outras convenções culturais associadas, como tipo de caractere, ordenação, formato de data e hora, unidade de moeda são usadas.
Enable Popup Notifications	Selecione esta caixa de seleção se você deseja ativar as notificações do sistema pop-up a serem exibidas em sua interface com o usuário.

Conceitos relacionados:

"Opções de procura de filtro rápido" na página 114
Procure cargas úteis de fluxos e de evento digitando uma sequência de caracteres de procura de texto que use palavras ou frases simples.

Acessar 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

É possível redimensionar as colunas em várias guias no QRadar.

Coloque o ponteiro do mouse sobre a linha que separa as colunas e arraste a borda da coluna para o novo local. 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.

Tamanho da página

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

Capítulo 3. Gerenciamento de painel

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

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

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

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

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

Painéis padrão

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

A guia **Painel** fornece cinco painéis padrão que estão 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.

Painéis customizados

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

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

- Criar painéis customizados que são relevantes para as suas responsabilidades. 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
Ofensas 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.

Tabela 8. Itens de ofensa (continuação)

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

Relatórios mais recentes

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

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

Resumo do sistema

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

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

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

Painel Monitoramento de risco

Use o painel **Monitoramento de risco** para monitorar o risco da política e a mudança de risco da política para ativos, políticas e grupos de política.

Por padrão, o painel **Monitoramento de risco** exibe os itens **Risco** e **Mudança de risco** que monitoram a pontuação de risco de política para ativos nos grupos de política Vulnerabilidades altas, Vulnerabilidades médias e Vulnerabilidades baixas, bem como as taxas de aprovação de conformidade e as mudanças históricas na pontuação de risco de política no grupo de política do CIS.

Os itens do painel Monitoramento de risco não exibem nenhum resultado, a menos que o IBM Security QRadar Risk Manager esteja licenciado. Para obter mais informações, consulte Guia dos usuários do QRadar Risk Manager.

Para visualizar o painel **Monitoramento de risco** padrão, selecione **Mostrar painel** > **Monitoramento de risco** na guia **Painel**.

Tarefas relacionadas:

"Conformidade da política de monitoramento" na página 21
Crie um item de painel que mostra as taxas de aprovação de conformidade da política e a pontuação de risco de política para ativos, políticas e grupos de políticas selecionados.

"Monitorando a mudança de risco" na página 22
Crie um item de painel que mostra a mudança de risco de política para ativos, políticas e grupos de políticas selecionados em uma base diária, semanal e mensal.

Conformidade da política de monitoramento

Crie um item de painel que mostra as taxas de aprovação de conformidade da política e a pontuação de risco de política para ativos, políticas e grupos de políticas selecionados.

Procedimento

1. Clique na guia **Painel**.
2. Na barra de ferramentas, clique em **Novo painel**.
3. Digite um nome e a descrição para o painel de conformidade de política.
4. Clique em **OK**.
5. Na barra de ferramentas, selecione **Incluir item** > **Gerenciador de risco** > **Risco**.

   Os itens do painel **Gerenciador de Risco** são exibidos somente quando o IBM Security QRadar Risk Manager estiver licenciado.
6. No cabeçalho do novo item do painel, clique no ícone **Configurações** amarelo.
7. Use as listas **Tipo de gráfico**, **Parte superior da exibição** e **Classificação** para configurar o gráfico.
8. Na lista **Grupo**, selecione o grupo que você deseja monitorar. Para obter mais informações, consulte a tabela na etapa 9.

   Quando você selecionar a opção **Ativo**, um link para a página **Riscos** > **Gerenciamento de Política** > **Por Ativo** aparece na parte inferior do item de painel **Risco**. A página **Por Ativo** exibe mais informações detalhadas sobre todos os resultados que são retornados para o **Grupo de Políticas** selecionado. Para obter informações adicionais sobre um ativo específico, selecione **Tabela** a partir da lista de **Tipos de Gráficos** e clique no link na coluna **Ativo**, para visualizar detalhes sobre o ativo na página **Por Ativo**.

   Quando você selecionar a opção **Política**, um link para a página **Riscos** > **Gerenciamento de Política** > **Por Política** aparece na parte inferior do item de painel **Risco**. A página **Por Política** exibe mais informações detalhadas sobre todos os resultados que são retornados para o **Grupo de Políticas** selecionado. Para obter informações adicionais sobre uma política específica, selecione **Tabela** a partir da lista de **Tipos de Gráficos** e clique no link na coluna **Política**, para visualizar detalhes sobre a política na página **Por Política**.
9. Na lista **Gráfico**, selecione o tipo de gráfico que você deseja usar. Para obter mais informações, consulte a tabela a seguir:

Grupo	Porcentagem de ativos aprovados	Porcentagem de verificações de política aprovadas	Porcentagem de grupo de política aprovado	Pontuação de risco de política
Todos	Retorna a taxa média percentual de aprovação de ativo em ativos, políticas e grupo de política.	Retorna a taxa média percentual de aprovação de verificação de política em ativos, políticas e grupo de política.	Retorna a taxa média percentual de aprovação do grupo de política em todos os ativos, políticas e grupo de política.	Retorna a pontuação média de risco de política em todos os ativos, políticas e grupo de política.

Grupo	Porcentagem de ativos aprovados	Porcentagem de verificações de política aprovadas	Porcentagem de grupo de política aprovado	Pontuação de risco de política
Ativo	Retorna se um ativo é aprovado na conformidade de ativo (100%=aprovado, 0%=reprovado). Use essa configuração para mostrar quais ativos estão associados a uma conformidade de aprovação do Grupo de política.	Retorna a porcentagem de verificações de política na qual um ativo é aprovado. Use essa configuração para mostrar a porcentagem das verificações de política aprovadas para cada ativo associado ao Grupo de política.	Retorna a porcentagem de subgrupos de política associados ao ativo aprovados na conformidade.	Retorna a soma de todos os valores de fator de importância para perguntas de política associadas a cada ativo. Use essa configuração para visualizar o risco de política para cada ativo associado a um grupo de política selecionado.
Política	Retorna se todos os ativos associados a cada política em um Grupo de política são aprovados na conformidade. Use essa configuração para monitorar se todos os ativos associados a cada política em um Grupo de política são aprovados ou não.	Retorna a porcentagem de verificações de política aprovadas por política no grupo de política. Use essa configuração para monitorar quantas verificações de política falham por política.	Retorna a porcentagem de subgrupos de política dos quais a política é uma parte aprovada na conformidade.	Retorna os valores de fator de importância para cada pergunta de política no Grupo de política. Use essa configuração para visualizar o fator de importância para cada política em um grupo de política.
Grupo de política	Retorna a porcentagem de ativos aprovados na conformidade para o Grupo de política selecionado como um todo.	Retorna a porcentagem de verificações de política aprovadas por política para o grupo de política como um todo.	Retorna a porcentagem de subgrupos de política dentro do Grupo de política aprovados na conformidade.	Retorna a soma de todos os valores de fator de importância para todas as perguntas de política no Grupo de política.

10. Na lista **Grupo de política**, selecione os grupos de política que você deseja monitorar.
11. Clique em **Salvar**.

Monitorando a mudança de risco

Crie um item de painel que mostra a mudança de risco de política para ativos, políticas e grupos de políticas selecionados em uma base diária, semanal e mensal.

Sobre Esta Tarefa

Use esse item de painel para comparar as mudanças nos valores de Pontuação de risco de política, Verificações de políticas e Políticas para um grupo de política com o passar do tempo.

O item de painel **Mudança de risco** usa setas para indicar onde o risco de política para os valores selecionados aumentou, diminuiu ou permaneceu o mesmo por um período de tempo escolhido:

- O número abaixo da seta vermelha indica os valores que mostram um risco aumentado.
- O número abaixo das setas cinza indica os valores em que não há nenhuma mudança no risco.
- O número abaixo da seta verde indica os valores que mostram um risco diminuído.

Procedimento

1. Clique na guia **Painel**.
2. Na barra de ferramentas, clique em **Novo painel**.
3. Digite um nome e uma descrição para o painel de conformidade de política histórica.
4. Clique em **OK**.
5. Na barra de ferramentas, selecione **Incluir item** > **Gerenciador de risco** > **Mudança de risco**.

   Os itens do painel **Gerenciador de risco** são exibidos apenas quando o IBM Security QRadar Risk Manager está licenciado.
6. No cabeçalho do novo item do painel, clique no ícone **Configurações** amarelo.
7. Na lista **Grupo de política**, selecione os grupos de política que você deseja monitorar.
8. Selecione uma opção a partir da lista de **Valores A Serem Comparados**:
   - Se desejar vir as mudanças acumulativas em fator de importância para todas as perguntas de política dentro dos grupos de política selecionados, selecione **Pontuação de risco de política**.
   - Se desejar vir quantas verificações de política foram alteradas dentro dos grupos de política selecionados, selecione **Verificações de políticas**.
   - Se desejar vir quantas políticas foram alteradas dentro dos grupos de política selecionados, selecione **Políticas**.
9. Selecione o período de mudança de risco que você deseja monitorar na lista **Tempo delta**:
   - Se desejar comparar as mudanças de risco da 00h de hoje com as mudanças de risco de ontem, selecione **Dia**.
   - Se desejar comparar as mudanças de risco de segunda-feira, à 00:00, desta semana com as mudanças de risco da semana passada, selecione **Semana**.
   - Se desejar comparar as mudanças de risco da 00:00 no primeiro dia do mês atual com as mudanças de risco do mês passado, selecione **Mês**.
10. Clique em **Salvar**.

Itens de gerenciamento de vulnerabilidade

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

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

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

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

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

Notificação do sistema

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

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

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

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

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

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

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

Ao incluir o item de painel **Notificações do sistema**, as notificações do sistema também poderão ser exibidas como notificações pop-up na interface com o usuário do QRadar. Estas notificações pop-up são exibidas no canto inferior direito da interface com o usuário, independentemente da guia selecionada.

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

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

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

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

Centro de informações de 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

É possível 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 eventos normalizados e customizados ou parâmetros de fluxo incluídos em seus parâmetros de procura.
Tipo de Gráfico	Na caixa de listagem, selecione o tipo de gráfico que você deseja visualizar. As opções incluem: 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

É possível remover itens de um painel e incluir o item novamente a qualquer momento.

Sobre Esta Tarefa

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

Procedimento

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

Removendo um item do painel

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

Sobre Esta Tarefa

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

Procedimento

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

Renomeando um painel

É possível renomear um painel e atualizar a descrição.

Procedimento

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

Excluindo um painel

É possível excluir um painel.

Sobre Esta Tarefa

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

Procedimento

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

Gerenciando notificações do sistema

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

Antes de Iniciar

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

Procedimento

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

Incluindo itens baseados em painel para a lista Incluir Itens

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

Antes de Iniciar

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

Procedimento

1. Escolha:
   - Para incluir um item de painel de procura de fluxo, clique na guia **Atividade de rede**.
   - Para incluir um item de painel de procura de evento, clique na guia **Atividade de log**.
2. Na caixa de listagem **Procurar**, escolha uma das seguintes opções:
   - Para criar uma procura, selecione **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 de Coluna, selecione uma coluna e clique no ícone **Incluir coluna** para mover a coluna para a lista **Grupo**.
4. Clique em **Filtrar**. Os resultados da procura são exibidos.
5. Clique em **Salvar critérios**. Consulte Salvando critérios de procura na guia Ofensa
6. Clique em **OK**.
7. Verifique se seus critérios de procura salva com êxito incluídos ao item de painel de procura de evento ou fluxo para a lista **Incluir itens**
   a. Clique na guia **Painel**.
   b. Escolha uma das opções a seguir:
   a. Para verificar um item de procura de eventos, selecione **Incluir item** > **Atividade de log** > **Procuras de eventos** > **Incluir item**.
   b. Para verificar um item de procura de fluxo, selecione **Incluir item** > **Atividade de rede** > **Procuras de fluxo**. O item de painel é exibido na lista com o mesmo nome que seus critérios de procura salva.

Capítulo 4. Gerenciamento de Ofensas

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 116.

Considerações de permissão de ofensa

Todos os usuários podem visualizar todas as ofensas, independentemente de qual origem de log ou fonte 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 *IBM Security QRadar SIEM Administration Guide*.

Termos chave

Usando a guia **Ofensas**, é possível acessar e analisar Ofensas, Endereços IP de origem, e Endereços IP de destino.

Item	Descrição
Ofensas	Uma ofensa inclui 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 Ofensas	Exibe todas as ofensas designadas a você.
Todas as ofensas	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

É possível 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. É possível 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.

Monitorando ofensas agrupadas por categoria

É possível 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 ofensas.

Monitorando ofensas agrupadas por IP de origem

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

Sobre Esta Tarefa

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

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por IP de origem**.
3. É possível 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 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 local.

Sobre Esta Tarefa

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

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Por IP de destino**.
3. É possível 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 com esse endereço IP de destino, clique em **Ofensas** na barra de ferramentas da página Destino.
6. Para visualizar uma lista de endereços IP de origem associada a esse endereço IP de destino, clique em **Origens** na barra de ferramentas da página Destino.
7. Dê um clique duplo na ofensa que você deseja visualizar.
8. Na página Resumo da ofensa, revise os detalhes da ofensa. Consulte Parâmetros da ofensa.
9. Execute quaisquer ações necessárias na ofensa. Consulte as Tarefas de gerenciamento de ofensas.

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 associada a essa rede, clique em **Origens** na barra de ferramentas da página Rede.
5. Para visualizar uma lista de endereços IP de destino associada a essa rede, clique em **Destinos** na barra de ferramentas da página Rede.
6. Para visualizar uma lista de ofensas associada 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 ofensas.

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

É possível 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 *IBM Security QRadar SIEM Administration Guide*.

Procedimento

1. Clique na guia **Ofensas**.
2. Clique em **Todas as ofensas**.
3. Escolha uma das opções a seguir:
   - Selecione o 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

É possível 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. É possível ter as ofensas que você deseja reter independentemente do período de retenção. É possível 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 *IBM Security QRadar SIEM Administration Guide*.

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

É possível 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

É possível 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, ela será exibida na página Minhas ofensas pertencente a esse usuário. Você deve ter privilégios apropriados para designar ofensas para os usuários.

É possível 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

É possível 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.
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.
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 mais informações, consulte *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. É possível customizar os parâmetros de procura, se necessário. Clique em **Procurar** para visualizar as informações de conexão.

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

Função	Descrição
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**.
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.

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

Função	Descrição
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 mais informações, consulte *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 mais informações, consulte *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	Localização	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 de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o nome do ativo, que pode ser designado usando a função Perfil de ativo. Para obter mais informações, consulte Gerenciamento de ativos.
Peso do ativo	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o peso do ativo, que é possível designar usando a função Perfil de ativo. Para obter mais informações, consulte Gerenciamento de ativos.
Assigned to	Tabela de ofensa	Especifica o usuário 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 10 últimos eventos	Especifica a categoria do evento.
Category Name	Página Por detalhes da categoria	Especifica o nome da categoria de alto nível.
Chained	• Tabela de origem de ofensa, se o Tipo de ofensa for o 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 ser o endereço IP de origem de outra ofensa. Se o endereço IP de destino for encadeado, clique em **Sim** para visualizar as ofensas encadeadas.

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

Parâmetro	Localização	Descrição
Data de Criação	Tabela 5 últimas notas	Especifica a data e a hora em que a nota foi criada.
Credibilidade	Tabela de ofensa	Especifica a credibilidade da ofensa, conforme determinado pela classificação de credibilidade a partir de dispositivos de origem. Por exemplo, a credibilidade é aumentada quando várias ofensas relatam o mesmo evento ou fluxo.
Parâmetros de Procura Atuais	• 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 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 de ofensa • Página Por IP de origem - Lista de ofensas • Página Por rede – Lista de ofensas • Página Por IP de destino – Lista de ofensas • Tabela de origem de ofensas, 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 10 últimos 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 Administrador, será possível visualizar o nome DNS apontando seu mouse no endereço IP.
Destination IP(s)	Tabela de ofensa	Especifica os endereços IP e o nome do ativo (se disponível) dos destinos locais ou remotos. Clique no link para visualizar mais detalhes.
Destination IPs	• 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 de endereços IP de destino.
Destination IPs	• 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 de ativos (se disponível) do destino que está associado à ofensa. Se consultas de DNS estiverem ativadas na guia Administração, será possível visualizar o nome DNS apontando seu mouse no endereço IP ou nome do ativo.
Destination IPs	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 QID, que está associado ao evento ou fluxo que criou a ofensa. Passe o seu mouse sobre o nome do evento para visualizar o QID.
Contagem de Eventos/Fluxos	Página Por detalhes da categoria	Especifica o número de eventos ativos ou fluxo (eventos ou fluxos que não estão encerrados ou ocultados) associados à ofensa na categoria. Ofensas só ficam ativas por um período de tempo se nenhum novo evento ou fluxo for recebido. As ofensas ainda são exibidas na guia Ofensas, mas não são contadas nesse campo.

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

Parâmetro	Localização	Descrição
Contagem de Eventos/Fluxos	Página de destino Página de rede	Especifica o número de eventos e fluxos que ocorreram na ofensa e o número de categorias. Clique no link eventos para investigar os eventos que são associados à ofensa. Ao clicar no link de eventos, os resultados da procura de eventos serão exibidos. Clique no link de fluxos para investigar detalhadamente os fluxos que são associados às ofensas. Ao clicar no link de fluxos, os resultados da procura de fluxo serão exibidos. **Nota:** Se a contagem de fluxo exibir N/A., a ofensa poderá ter uma data de início que precede a data que foi feito upgrade para a versão 7.1.0 (MR1) do seu produto QRadar. Portanto, os fluxos não podem ser contados. É possível, no entanto, clicar no link N/A para investigar os fluxos associados nos resultados da procura de fluxo.
Contagem de Eventos/Fluxos	Página Por detalhes da categoria	Especifica o número de eventos ativos ou fluxo (eventos ou fluxos que não estão encerrados ou ocultados) associados à ofensa na categoria. Ofensas só ficam ativas por um período de tempo se nenhum novo evento ou fluxo for recebido. As ofensas ainda são exibidas na guia Ofensas, mas não são contadas nesse campo.
Contagem de Eventos/Fluxos	Página de destino Página de rede	Especifica o número de eventos e fluxos que ocorreram na ofensa e o número de categorias. Clique no link eventos para investigar os eventos que são associados à ofensa. Ao clicar no link de eventos, os resultados da procura de eventos serão exibidos. Clique no link de fluxos para investigar detalhadamente os fluxos que são associados às ofensas. Ao clicar no link de fluxos, os resultados da procura de fluxo serão exibidos. **Nota:** Se a contagem de fluxo exibir N/A., a ofensa poderá ter uma data de início que precede a data que foi feito upgrade para a versão 7.1.0 (MR1) do seu produto QRadar. Portanto, os fluxos não podem ser contados. É possível, no entanto, clicar no link N/A para investigar os fluxos associados nos resultados da procura de fluxo.
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.

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

Parâmetro	Localização	Descrição
Events/Flows	• A tabela de origem de 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, Source IPv6 ou Destination IPv6, 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 são associados ao endereço IP de origem, endereço IP de destino, nome do evento, nome de usuário, endereço MAC, origem do log, nome do host, porta, origem do log, endereço ASN, endereço IPv6, regra, ASN, Aplicativo, rede ou categoria. Clique no link para visualizar mais detalhes.
First event/flow seen on	Página Detalhes da origem	Especifica a data e hora em que o endereço IP de origem gerou o primeiro evento ou fluxo.
Sinalizador	• 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, ela será exibida na página Minhas ofensas pertencente a esse usuário. Para obter mais informações sobre como designar ofensas para usuários, consulte Designando ofensas para usuários. • Notas – Indica que um usuário incluiu notas à ofensa. Notas pode incluir qualquer informação que desejar capturar para a ofensa. Por exemplo, é possível incluir uma nota que especifica 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 as ofensas especificadas sejam removidas do banco de dados após o período de retenção ter decorrido. Para obter mais informações sobre ofensas protegidas, consulte Protegendo ofensas. Passe seu mouse sobre o ícone para exibir mais informações.

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

Parâmetro	Localização	Descrição
Flag (continued)		• Ofensas inativas – Indica que esta é uma ofensa inativa. Uma ofensa se torna inativa após cinco dias decorridos desde que a ofensa recebeu o último evento. Além disso, todas as ofensas se tornam inativas após o realizar upgrade do seu software do 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 desempenhar as seguintes ações nas ofensas inativas: proteger, sinalizar para acompanhamento, incluir notas e designar aos usuários.
Sinalizador	• 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 detalhes de rede • Página Por rede – Lista de origens • Página Por rede – Lista de destinos do local	Especifica a ação tomada no endereço IP de origem, endereço IP de destino ou rede. Por exemplo, se um sinalizador for exibido, o crime é sinalizada para acompanhamento. Passe seu mouse sobre o ícone para exibir mais informações.
Fluxos	• 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/A, a ofensa poderá ter uma data de início anterior à data em que foi feito upgrade para o QRadar 7.1.0 (MR1).
Grupo	• Tabela de origem de ofensas, 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 de origem de ofensas, se o Tipo de ofensa for Regra	Especifica a qual grupo de regra a regra pertence.
Categoria de Alto Nível	Tabela de origem de ofensa, se o Tipo de ofensa for o Nome do evento	Especifica a categoria de alto nível do evento. Para obter mais informações sobre categorias de alto nível, consulte o *IBM Security QRadar SIEM Administration Guide*.
Nome do host	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o nome do host que está associado ao endereço IP de origem ou de destino. Se nenhum nome do host for identificado, este campo especificará Desconhecido.
Nome do host	Tabela de origem de 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 à ofensa.
IP	• Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem • Página Detalhes da origem	Especifica o endereço IP de origem que está associado ao evento ou fluxo que criou a ofensa.

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

Parâmetro	Localização	Descrição
IP/DNS Name	Página Destino	Especifica o endereço IP do destino. Se o DNS estiver ativado na guia **Administração**, será possível visualizar o nome DNS passando seu mouse sobre o endereço IP ou nome do ativo. Para obter mais informações, consulte *IBM Security QRadar SIEM Administration Guide*.
IPv6	Tabela de origem de ofensa, se o Tipo de ofensa for Source IPv6 ou Destination IPv6	Especifica o endereço IPv6 que está associado ao evento ou fluxo que criou a ofensa.
Last Event/Flow	• 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.
Last event/flow seen on	Página Detalhes da origem	Especifica a data e a hora do último evento ou fluxo gerado que está associado ao endereço IP de origem.
Last Event/Flow Time	Tabela de origem de ofensas, se o Tipo de ofensa for Fonte de log	Especifica a última data e hora em que a fonte de log foi observada no sistema.
Last Known Group	Tabela de 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 qual grupo atual o usuário, endereço MAC ou nome do host pertencem. Se nenhum grupo estiver associado, o valor desse campo será Desconhecido. **Nota:** Este campo não exibirá informações históricas.
Last Known Host	Tabela de origem de ofensa, se o Tipo for ofensa for Nome de usuário, Endereço MAC de origem ou Endereço MAC de destino	Especifica a qual host atual o usuário ou o endereço MAC está associado. Se nenhum host for identificado, este campo especificará Desconhecido. **Nota:** Este campo não exibirá informações históricas.
Last Known IP	Tabela de 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.
Last Known MAC	Tabela de 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 host. Se nenhum MAC for identificado, este campo especificará Desconhecido. **Nota:** Este campo não exibirá informações históricas.
Last Known Machine	Tabela de 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.
Last Known Username	Tabela de 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.
Last Observed	Tabela de 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, o endereço MAC ou o nome do host foi observado no sistema.
Horário do Último Pacote	Tabela Últimos 10 fluxos	Especifica a data e hora em que o último pacote do fluxo foi enviado.

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

Parâmetro	Localização	Descrição
Local Destination Count	Tabela 5 principais categorias Página Por detalhes da 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 com o endereço IP de origem. Para visualizar mais informações sobre os endereços IP de destino, clique no endereço IP ou no termo que é exibido. Se houver vários endereços IP de destino, o termo Vários será exibido.
Localização	• Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem • 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 destino. Se a localização for local, será possível clicar no link para visualizar as redes.
Fonte de log	Tabela 10 últimos eventos	Especifica a fonte de log que detectou o evento.
Log Source Identifier	Tabela de origem de ofensas, se o Tipo de ofensa for Fonte de log	Especifica o nome do host da fonte de log.
Log Source Name	Tabela de origem de ofensas, se o Tipo de ofensa for Fonte de log	Especifica o nome da fonte de log, conforme identificado na tabela Fontes de log, que é 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 Administrador e gerenciar as fontes de log. Para obter mais informações sobre o gerenciamento de fonte de log, consulte o *Guia de Gerenciamento do Log Sources* .
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, este campo especificará Vários e o número de fontes de log.
Categoria de Baixo Nível	Tabela de origem de ofensa, se o Tipo de ofensa for o Nome do evento	Especifica a categoria de nível inferior do evento.
MAC	• Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem • 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 quando a ofensa começou. Se o endereço MAC for desconhecido, este campo especificará Desconhecido.
MAC Address	Tabela de origem de ofensa, se o Tipo de ofensa for Endereço MAC de origem ou destino	Especifica o endereço MAC associado ao evento que criou a ofensa. Se nenhum endereço MAC for identificado, este campo especificará Desconhecido.

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

Parâmetro	Localização	Descrição
Magnitude	• Página Todas as ofensas • Página Minhas ofensas • Tabela de 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 10 últimos eventos • Página Por detalhes de rede • Página de 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 de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem • 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 de 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 destino ou origem. A barra de magnitude fornece uma representação visual do valor de risco de CVSS do ativo que está associado ao endereço IP. Passe seu mouse sobre a barra de magnitude para exibir a magnitude calculada.
Name	• 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 da rede ou nome.
Rede	Página Por detalhes de rede	Especifica o nome da rede.
Network(s)	Tabela de ofensa	Especifica a rede de destino para a ofensa. Se a ofensa possuir 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.
Comunicados	• Tabela de origem de ofensas, se o Tipo de ofensa for Regra • Tabela 5 últimas notas	Especifica as notas da regra.
Offense Count	Página Por detalhes da categoria	Especifica o número de crimes ativos em cada categoria. Os crimes ativos são ofensas que não foram ocultos ou encerrados. Se a página Por detalhes de categoria incluir o filtro Excluir ofensas ocultas, a contagem de ofensa 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.
Offense Source	• 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 fonte da ofensa. As informações que são exibidas no campo **Origem da ofensa** dependem do tipo de ofensa. Por exemplo, se o tipo de ofensa for Porta de origem, o campo **Origem de ofensa** exibirá a porta de origem do evento que criou a ofensa.

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

Parâmetro	Localização	Descrição
Offense Type	• Página Minhas ofensas • Tabela de 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 um evento de fonte de log, a regra que gerou a ofensa correlacionará os eventos que são 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 • Nome do host • 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 de origem de ofensa.
Offense(s)	• Página Detalhes da origem • Página Destino	Especifica os nomes das ofensas que são associadas ao endereço IP de origem ou destino. Para visualizar mais informações sobre a ofensa, clique no nome ou no termo que é exibido. Se houver várias ofensas, o termo Vários será exibido.
Offense(s) Launched	Página Rede	Especifica as ofensas que são ativadas a partir da rede. Se várias ofensas forem responsáveis, esse campo especificará Vários e o número de ofensas.
Offense(s) Targeted	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	• A tabela de origem de ofensas, se o Tipo de ofensa for IP de origem, IP de destino, Nome do evento, Nome, Endereço MAC de origem ou destino, Fonte de log, Nome de host, Porta de origem ou destino, Source IPv6 ou Destination IPv6, ASN de origem ou destino, Regra, ID do aplicativo • 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 são associadas ao endereço IP de origem, endereço IP de destino, nome do evento, nome de usuário, endereço MAC, origem do log, nome do host, porta, endereço IPv6, ASN, regra ou aplicativo. Clique no link para visualizar mais detalhes.

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

Parâmetro	Localização	Descrição
Offenses Launched	Página Por detalhes de rede	Especifica o número de ofensas que são originadas da rede.
Offenses Targeted	Página Por detalhes de rede	Especifica o número de ofensas que são direcionadas para a rede.
Port	Tabela de origem de ofensa, se o Tipo de ofensa for Porta de origem ou destino	Especifica a porta que está associada ao evento ou fluxo que criou a ofensa.
Relevância	Tabela de ofensa	Especifica a importância relativa da ofensa.
Response	Tabela de origem de ofensas, se o Tipo de ofensa for Regra	Especifica o tipo de resposta da regra.
Rule Description	Tabela de origem de ofensas, se o Tipo de ofensa for Regra	Especifica o resumo dos parâmetros de regra.
Nome da Regra	Tabela de origem de ofensas, 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 Regras	Tabela de origem de ofensas, se o Tipo de ofensa for Regra	Especifica o tipo de regra da ofensa.
Gravidade	• Tabela de origem de ofensa, se o Tipo de ofensa for o Nome do evento • Tabela de ofensa	Especifica a severidade do evento ou ofensa. A severidade especifica a quantidade de ameaças que uma ofensa representa em relação a quanto o endereço IP de destino está preparado para o ataque. Este valor é diretamente mapeado para a categoria de evento que se correlaciona à ofensa. Por exemplo, um ataque de Negação de Serviço (DoS) tem uma severidade de 10, que especifica uma ocorrência grave.
Source Count	Página Por detalhes da categoria	Especifica o número de endereços IP de origem associados a ofensas na categoria. Se um endereço IP de origem estiver associado a ofensas em cinco categorias diferentes de nível inferior, o endereço IP de origem será contado apenas uma vez.
IP de Origem	• 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 Administrador, será possível visualizar o nome DNS apontando seu mouse no endereço IP. Para obter mais informações, consulte *IBM Security QRadar SIEM Administration Guide*.
Source IP(s)	Tabela de 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.
Source IPs	• 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 tentou violar a segurança de um componente em sua rede. Se mais de um endereço IP de origem estiver associado à ofensa, este campo especificará Vários e o número de endereços IP de origem. Se consultas de DNS estiverem ativadas na guia Administração, será possível visualizar o nome DNS apontando seu mouse no endereço IP ou nome do ativo. Para obter mais informações, consulte *IBM Security QRadar SIEM Administration Guide*.
Source IPs	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 para o endereço IP de destino.

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

Parâmetro	Localização	Descrição
Source(s)	• Página Destino • Página Rede	Especifica os endereços IP de origem da ofensa que está associada ao endereço IP de destino ou rede. Para visualizar mais informações sobre os endereços IP de origem, clique no endereço IP, nome do ativo ou termo que é exibido. Se um endereço IP de fonte isolada for especificado, um endereço IP e o nome de ativo serão exibidos (se disponível). É possível clicar no endereço IP ou no nome de ativo para visualizar os detalhes do endereço IP de origem. Se houver vários endereços IP de origem, este campo especificará Vários e o número de endereços IP de origem.
Source(s)	Página Por rede – Lista de destinos do local	Especifica o número de endereços IP de origem associados a endereços IP de destino.
Start	Tabela de ofensa	Especifica a data e hora em que o primeiro evento ou fluxo ocorreu para a 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 de origem de ofensas, se o Tipo de ofensa for Fonte de log	Especifica o status da fonte de log.
Status	Tabela de ofensa	Exibe ícones para indicar o status de uma ofensa. Ícones de status incluem: **Ofensa inativa**. Uma ofensa se torna inativa após cinco dias decorridos desde que a ofensa recebeu o último evento. Todas as ofensas se tornarão inativas após o upgrade do seu software do 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 os usuários a uma ofensa inativa. Um sinalizador **Ofensa Oculta** na página Todas as Ofensas indica que o crime está oculta na visualização. Se você procurar ofensas ocultas, elas serão visíveis somente na página Todas as Ofensas em que estão sinalizadas como ofensa oculta. Para obter mais informações, consulte Ocultar ofensas. **Usuário** indica que a ofensa é designada a um usuário. Quando uma ofensa for designada a um usuário, a ofensa será exibida na página Minhas ofensas que pertence a esse usuário. Para obter mais informações, consulte Designando ofensas para usuários. **Proteger** evita que as ofensas especificadas sejam removidas do banco de dados após o período de retenção ter decorrido. Para obter mais informações, consulte Protegendo ofensas. **Ofensa encerrada** indica que a ofensa está encerrada. Para obter mais informações, consulte Encerrando ofensas.
Time	• Tabela 10 últimos 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 são especificadas pelo dispositivo que detectou o evento.
Time	Tabela 5 principais anotações	Especifica a data e a hora em que a anotação foi criada.

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

Parâmetro	Localização	Descrição
Total Bytes	Tabela Últimos 10 fluxos	Especifica o número total de bytes do fluxo.
Total Events/Flows	• Tabela 5 principais fontes de log • Tabela 5 principais usuários	Especifica o número total de eventos da fonte de log ou usuário.
User	• Tabela de origem de ofensa, se o Tipo de ofensa for IP de origem ou destino ou Nome de usuário • 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 usuário que está associado a um endereço IP de origem ou destino. Se nenhum usuário for identificado, este campo especificará Desconhecido.
Nome de usuário	Tabela de origem de ofensa, se o Tipo de Ofensa for Nome de usuário	Especifica o nome de usuário associado ao evento ou fluxo que criou a ofensa. **Nota:** Se mover seu ponteiro do mouse sobre o parâmetro Username, a dica de ferramenta exibida fornece o nome de usuário associado às informações de nome de usuário mais recentes na guia Ativos em vez do nome de usuário associado ao evento ou fluxo que criou a ofensa.
Nome de usuário	Tabela 5 últimas 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 que deseja visualizar nesta página. É possível visualizar todas as ofensas ou filtrar por ofensas que são baseadas em um intervalo de tempo. Na caixa de listagem, selecione o intervalo de tempo com o qual deseja filtrar.
Vulnerabilidades	Tabela de origem da ofensa, se o Tipo de origem for o IP de destino ou de origem	Especifica o número de vulnerabilidades identificadas que são associadas ao endereço IP de origem ou destino. Este valor também inclui o número de vulnerabilidades ativas e passivas.
Vulnerabilidades	Página Por IP de destino - Lista de Origens	Especifica se um endereço IP de origem possui vulnerabilidades.
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.

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

Parâmetro	Localização	Descrição
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 a ponderação do endereço IP de origem, endereço IP de destino, ou anotação. A ponderação de um endereço IP é designada na guia **Ativos**. Para obter mais informações, consulte Gerenciamento de ativos.

Capítulo 5. Investigação de atividade de log

É possível monitorar e investigar eventos em tempo real ou executar procuras avançadas.

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

Visão geral da guia Atividade de log

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

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

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

Barra de ferramentas da guia Atividade de log

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

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

Tabela 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 são exibidas na caixa de listagem **Procuras rápidas** apenas quando forem salvos os critérios de procura que especificam a opção **Incluir em minhas procuras salvas**.
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 a conclusão de uma procura. 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 ajustar eventos que são conhecidos como positivos falsos da criação de crimes. Esta opção está desativada no modo de fluxo. Para obter mais informações sobre o ajuste de positivos falsos, consulte Ajuste de positivos falsos.

Tabela 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 de evento customizado. As opções incluem: • **Regras** – Selecione esta opção para visualizar ou criar uma regra. Se tiver somente a permissão para visualizar as regras, a página de resumo do assistente de regras será exibida. Se tiver a permissão para manter as regras customizadas, o assistente de regras será exibido e será possível editar a regra. Para ativar as opções de regra de detecção de anomalias (Incluir limite de regra, Incluir regra comportamental e Incluir regra de anomalia), é necessário salvar critérios de procura agregados porque os critérios da procura salvos especificam os parâmetros requeridos. **Nota:** As opções de regra de detecção de anomalias serão visíveis apenas se tiver a permissão **Atividade de log** > **Manter regras customizadas**. • **Incluir limite de regra** – Selecione esta opção para criar uma regra de limite. Uma regra de limite testa o tráfego do evento para a atividade que excede um limite configurado. Os limites podem ser baseados em quaisquer dados que são coletados QRadar. Por exemplo, se for criada uma regra de limite indicando que não mais de 220 clientes podem efetuar login no servidor entre 8h e 17h, as regras gerarão um alerta quando o cliente 221º tentar efetuar login. Ao selecionar a opção **Incluir regra de limite**, o assistente de regras é exibido, pré-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 eventos da atividade anormal, como a existência de tráfego novo ou desconhecido, que é o tráfego que para subitamente ou uma alteração de porcentagem na quantidade de tempo que um objeto está ativo. Por exemplo, é possível criar uma regra comportamental para comparar o volume médio de tráfego dos últimos 5 minutos com o volume médio de tráfego durante a última hora. Se houver uma alteração de mais de 40%, a regra irá gerar uma resposta. Ao selecionar a opção **Incluir regra comportamental**, o assistente de regras será exibido e pré-preenchido 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 iniciar uma comunicação com os hosts nesse país, uma regra de anomalia gerará um alerta. Ao selecionar a opção **Incluir regra de anomalia**, o assistente de regras será exibido e pré-preenchido com as opções apropriadas para criar 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 evento. 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 Gerenciando resultados da procura de evento e de 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.
Barra de ferramentas de procura	**Procura avançada** Selecione **Procura avançada** na caixa de listagem para inserir uma sequência de caracteres de procura Ariel Query Language (AQL) para especificar os campos que você deseja que sejam retornados. **Filtro rápido** Selecione Filtro rápido na caixa de listagem para procurar cargas úteis usando palavras ou frases simples.

Opções de menu ativado pelo botão direito

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

As opções do menu ativado pelo botão direito são:

Tabela 15. Opções de menu ativado pelo botão direito

Opção	Descrição
Filtrar em	Selecione esta opção para filtrar o evento selecionado, dependendo do parâmetro selecionado no evento.
Positivo Falso	Selecione esta opção para abrir a janela Positivo falso, que permitirá ajustar eventos que são conhecidos como positivos falsos da criação de crimes. Esta opção está desativada no modo de fluxo. Consulte Ajustando positivos falsos.
Mais opções:	Selecione esta opção para investigar um endereço IP ou um nome de usuário. Para obter mais informações sobre como investigar um endereço IP, consulte Investigando endereços IP. Para obter mais informações sobre como investigar um nome de usuário, consulte Investigando nomes de usuário. **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 sucesso a partir 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 no modo de fluxo, permitindo que você visualize eventos em tempo real.

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

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

Visualizando eventos de fluxo

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

Sobre Esta Tarefa

Se você aplicar quaisquer filtros na guia **Atividade de Log** ou em seu critério de procura antes de ativar o modo de fluxo, os filtros serão mantidos em modo de fluxo. No entanto, o modo de fluxo não suporta procuras que incluem eventos agrupados. Se você ativar o modo de fluxo 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 o fluxo de eventos. Escolha uma das opções a seguir:

- Para selecionar um registro de eventos, clique no ícone **Pausar** para pausar o fluxo.
- Para reiniciar o modo de fluxo, clique no ícone **Executar**.

Visualizando eventos normalizados

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

Sobre Esta Tarefa

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

Nota: Se você selecionou um prazo para exibição, um gráfico de série temporal será exibido. Para obter mais informações sobre como usar gráficos de 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 – Parâmetro 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 procurados durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas atuais são úteis para a resolução de problemas. Quando contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em **Ocultar gráficos** se deseja remover os gráficos de sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Capacidade de gerenciamento do gráfico. **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 mais informações, consulte a documentação do navegador.
Ícone ofensas	Clique neste ícone para visualizar detalhes da ofensa associada a este evento. Para obter mais informações, consulte Capacidade de gerenciamento do gráfico. **Nota:** Dependendo do seu produto, esse ícone pode não estar disponível. Você deve ter o IBM Security QRadar SIEM.

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

Parâmetro	Descrição
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.
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 em que o QRadar recebeu o evento.
Categoria de Baixo Nível	Especifica a categoria de baixo nível associada a este evento. Para obter mais informações sobre as categorias de eventos, consulte o *IBM Security QRadar SIEM Administration Guide*.
IP de Origem	Especifica o endereço IP de origem do evento.
Porta de origem	Especifica a porta de origem do evento.
IP de destino	Especifica o endereço IP de destino do evento.
Porta de destino	Especifica a porta de destino do evento.
Nome de usuário	Especifica o nome de usuário associado a este evento. Os nomes de usuário estão frequentemente disponíveis em eventos de autenticação relacionada. Para todos os outros tipos de eventos onde o nome de usuário não estiver disponível, este campo especificará N/D.
Magnitude	Especifica a magnitude deste evento. Variáveis incluem credibilidade, relevância e gravidade. Passe o mouse sobre a barra de magnitude para exibir os valores e a magnitude calculada.

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

É possível visualizar dados do evento bruto, que são os dados do evento não analisados do registro de origem.

Sobre Esta Tarefa

Quando você visualiza dados dos eventos brutos, 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
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 procurados durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas Atuais são úteis para a resolução de problemas. Quando contatar o Suporte ao Cliente para solucionar problemas de eventos, você poderá ser solicitado a fornecer informações da estatística atual.
Gráficos	Exibe gráficos configuráveis que representam os registros correspondidos pelo intervalo de tempo e opção de agrupamento. Clique em **Ocultar gráficos** se deseja remover os gráficos de sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. **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 mais informações, 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 os 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 agrupada, 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 Baixo Nível	Exibe uma lista resumida dos eventos agrupados pela categoria de baixo nível do evento. Para obter mais informações sobre categorias, consulte o *IBM Security QRadar SIEM Administration Guide*.
Nome do evento	Exibe uma lista resumida dos eventos agrupados pelo nome normalizado do evento.
IP de destino	Exibe uma lista resumida dos eventos agrupados pelo endereço IP de destino do evento.
Porta de destino	Exibe uma lista resumida dos eventos agrupados pelo endereço de porta de destino do evento.
IP de Origem	Exibe uma lista resumida dos eventos agrupados pelo endereço IP de origem do evento.
Regra customizada	Exibe uma lista resumida dos eventos agrupados pela regra customizada associada.
Nome de usuário	Exibe uma lista resumida dos eventos agrupados pelo nome de usuário associado ao evento.
Fonte de log	Exibe uma lista resumida dos eventos agrupados pelas origens de log que enviaram o evento para QRadar.
Categoria de Alto Nível	Exibe uma lista resumida dos eventos agrupados pela categoria de alto nível do evento.
Rede	Exibe uma lista resumida dos eventos agrupados pela rede associada ao evento.
Porta de origem	Exibe uma lista resumida dos eventos agrupados pelo endereço de porta de origem do evento.

Depois de selecionar uma opção na caixa de listagem **Exibir**, o layout da coluna dos dados depende da opção do grupo escolhido. Cada linha na 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 no qual a procura está 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.
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 procurados 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 de estatística atuais.

Tabela 19. Parâmetros de eventos agrupados (continuação)

Parâmetro	Descrição
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. Cada gráfico fornece uma legenda, que é uma referência visual para ajudá-lo a associar os objetos de gráfico aos parâmetros que eles representam. Usando o recurso de legenda, é possível executar as seguintes ações: • Mova o ponteiro do mouse sobre um item de legenda para visualizar mais informações sobre os parâmetros que ele representa. • Clique com o botão direito no item de legenda para investigar melhor o item. • Clique em um item de legenda para ocultar os itens no gráfico. Clique no item de legenda novamente para mostrar o item oculto. É possível também clicar no item do gráfico correspondente para ocultar e mostrar o item. • Clique em **Legenda** se deseja remover a legenda da exibição do gráfico. **Nota:** Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. **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 gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.
IP de Origem (contagem exclusiva)	Especifica o endereço IP de origem 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.
IP de Destino (contagem exclusiva)	Especifica o endereço IP de destino associado a este evento. Se houver vários endereços IP associados a este evento, este campo especificará o termo Vários e o número de endereços IP.
Porta de destino (contagem exclusiva)	Especifica as portas de destino associadas a este evento. Se houver várias portas associadas a este evento, este campo especificará o termo Várias e o número de portas.
Nome do evento	Especifica o nome normalizado do evento.
Log Source (Unique Count)	Especifica as origens 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 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 vários protocolos associados a este evento, este campo especificará o termo Vários 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. As 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 são empacotados quando vários eventos do mesmo tipo, para o mesmo endereço IP de origem e destino, são vistos dentro de um curto período.
Contagem	Especifica o número total de eventos normalizados com este grupo de eventos.

Procedimento

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

3. Na caixa de lista de Exibição, escolha em qual parâmetro você deseja agrupar 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 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 no 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 de 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 Baixo Nível	Especifica a categoria de nível inferior deste evento. Para obter mais informações sobre categorias, consulte o *IBM Security QRadar SIEM Administration Guide*.
Descrição do Evento	Especifica uma descrição do evento, se disponível.
Magnitude	Especifica a magnitude deste evento. Para obter mais informações sobre magnitude, consulte o Glossário
Relevância	Especifica a relevância deste evento. Para obter mais informações sobre a relevância, consulte o Glossário.
Gravidade	Especifica a severidade deste evento. Para obter mais informações sobre 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 doQRadar.
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 fizeram com que a regra de detecção de anomalias gerasse 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 do evento. Para obter mais informações sobre ativos, consulte Gerenciamento de ativos
Porta de origem	Especifica a porta de origem deste evento.
Porta de destino	Especifica a porta de destino deste evento.
IP de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de Conversão de Endereço de Rede (NAT), este parâmetro especifica o endereço IP de origem antes dos valores NAT serem aplicados. O NAT converte um endereço IP em uma rede para um endereço IP diferente em outra rede.

Tabela 20. Detalhes do evento (continuação)

Parâmetro	Descrição
IP de Destino NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de destino antes dos valores de NAT serem aplicados.
Porta de Origem NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem antes dos valores de NAT serem aplicados.
Porta de Destino NAT Anterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino antes dos valores de NAT serem aplicados.
IP de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de origem após os valores de NAT serem aplicados.
IP de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará o endereço IP de destino após os valores de NAT serem aplicados.
Porta de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem após os valores de NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino após os valores de NAT serem aplicados.
Porta de Origem NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de origem após os valores de NAT serem aplicados.
Porta de Destino NAT Posterior	Para um firewall ou outro dispositivo capaz de NAT, este parâmetro especificará a porta de destino após os valores de NAT serem aplicados.
Origem de IPv6	Especifica o endereço IPv6 de origem do evento.
Destino de IPv6	Especifica o endereço IPv6 de destino do evento.
MAC de Origem	Especifica o endereço MAC de origem do evento.
MAC de Destino	Especifica o endereço MAC de destino do evento.
Informações de carga útil	
Payload	Especifica o conteúdo da carga útil do evento. Este campo oferece 3 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 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 o 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 são empacotados quando vários eventos do mesmo tipo, para o mesmo endereço IP de origem e destino, são vistos dentro de um curto período.
Custom Rules	Especifica as regras customizadas que correspondem a esse evento. .
Regras Customizadas Parcialmente Correspondidas	Especifica as regras customizadas que correspondem parcialmente esse evento.
Annotations	Especifica a anotação desse evento. As 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 disponível, a partir de mensagens da fonte de log. Informações de identidade fornecem detalhes adicionais sobre ativos em sua rede. Fontes de log geram 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 de 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 Base de Entrada/Saída (NetBios) do ativo que está associado a esse evento.
Campo **Identity Extended**	Especifica mais informações sobre o ativo que está associado a esse evento. O conteúdo deste campo é o texto definido pelo usuário e depende dos dispositivos em sua rede que estão disponíveis para fornecer informações de identificação. Exemplos incluem: localização física de dispositivos, políticas relevantes, comutador de rede e nomes de portas.

Tabela 20. Detalhes do evento (continuação)

Parâmetro	Descrição
Has Identity (Flag)	Especifica True se o QRadar tiver identificado as informações coletadas para o ativo que está associado a este evento. Para obter mais informações sobre quais dispositivos enviam 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 fornece várias funções para visualizar detalhes de eventos.

A barra de ferramentas **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 que estão associadas ao evento.
Anomalia	Clique em **Anomalia** para exibir os resultados da procura salva que fizeram com que a regra de detecção de anomalias gerasse este evento. **Nota:** Esse ícone só será exibido 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 de mapeamento de eventos.
Positivo Falso	Clique em **Positivo falso** para ajustar o QRadar para evitar que eventos positivos falsos sejam gerados em 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 de 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 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 Fazendo download do arquivo PCAP em 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 as regras, consulte o *IBM Security QRadar SIEM Administration Guide*.

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

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

Antes de Iniciar

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

Sobre Esta Tarefa

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

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

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

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

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

Procedimento

1. Clique na guia **Atividade de Log**.
2. Opcional. Se você estiver visualizando os eventos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento que você deseja mapear.
4. Clique em **Mapear evento**.
5. Se você souber o QID que você deseja mapear para esse evento, insira o QID no campo **Inserir QID**.

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

Ajustando positivos falsos

É possível usar a função Ajuste de Positivo Falso para evitar eventos positivos falsos de criar ofensas.

Antes de Iniciar

É possível ajustar os eventos de positivos falsos na página Lista de eventos ou Detalhes do evento.

Sobre Esta Tarefa

É possível ajustar os eventos de 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 *IBM Security QRadar SIEM Administration Guide*.

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 Propriedades do 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**.

dados do PCAP

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

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

Exibindo a coluna de dados do PCAP

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

Antes de Iniciar

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

Procedimento

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

6. Opcional. Se você estiver visualizando 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 a visualização e download de dados do PCAP, consulte as seções a seguir:

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

Visualizando informações do PCAP

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

Antes de Iniciar

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

Sobre Esta Tarefa

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

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

Procedimento

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

Fazendo download do arquivo PCAP para seu sistema de desktop

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

Antes de Iniciar

Para que seja possível visualizar as informações do PCAP, deve-se executar ou selecionar uma procura que exiba a coluna Dados do PCAP. Consulte **Exibindo a coluna de dados do PCAP**.

Procedimento

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

Exportando eventos

É possível exportar eventos no formato 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 você não selecionar o ícone **Notificar quando estiver pronto**, a janela de status será exibida.

Capítulo 6. Investigação de atividade de rede

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

Visão geral da guia Rede

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

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

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

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

É possível acessar várias opções na barra de ferramentas da guia **Atividade de rede**.

É possível acessar as opções a seguir na barra de ferramentas da guia **Atividade de rede**:

Tabela 22. Opções da barra de ferramentas da guia Atividade de rede

Opções	Descrição
Procurar	Clique em **Procurar** para concluir as procuras avançadas em fluxos. As opções de procura 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 a conclusão de uma procura. 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.

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

Opções	Descrição
Positivo Falso	Clique em **Positivo falso** a fim de abrir a janela Ajuste de positivo falso, para impedir que fluxos conhecidos por serem positivos falsos criem ofensas. Para obter mais informações sobre positivos falsos, consulte o Glossário. Esta opção está desativada no modo de fluxo. Consulte Exportando fluxos.
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 você possuir 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 for criada uma regra de limite indicando que não mais de 220 clientes podem efetuar login no servidor entre 8h e 17h, as regras gerarão um alerta quando o cliente 221º tentar efetuar login. **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 mais informações, consulte *IBM Security QRadar SIEM Administration Guide*.
Ações	Clique em **Ações** para concluir as ações a seguir: • **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** são desativadas no modo de fluxo e quando você visualiza resultados da procura parciais.
Barra de ferramentas de procura	**Procura avançada** Selecione **Procura avançada** na caixa de listagem e insira uma sequência de caracteres de procura Ariel Query Language (AQL) para especificar os campos que você deseja que sejam retornados. **Filtro rápido** Selecione **Filtro rápido** na caixa de listagem para procurar cargas úteis usando palavras ou frases simples.

Opções de 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 de menu ativado pelo botão direito

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

Monitorando a atividade de rede

Por padrão, a guia **Atividade de rede** exibe os fluxos em modo de fluxo, permitindo que sejam visualizados os fluxos em tempo real.

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

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 de 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.

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

Parâmetro	Descrição
Visualização	Na 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 procurados 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 estatísticas 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 os gráficos de sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Configurando gráficos. **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 gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, 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*.

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

Parâmetro	Descrição
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.
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
IP de origem ou destino	Exibe uma lista resumida dos fluxos agrupados pelo endereço IP associado ao fluxo.
IP de Origem	Exibe uma lista resumida dos fluxos agrupados pelo endereço IP de origem do fluxo.
IP de destino	Exibe uma lista resumida dos fluxos pelo endereço IP de destino do fluxo.

Tabela 25. Opções de fluxo agrupado (continuação)

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

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

Tabela 26. Parâmetros de fluxos agrupados

Cabeçalho	Descrição
Agrupar por	Especifica o parâmetro no qual a procura está 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.
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 procurados durante o período de tempo especificado. • **Duração** – Especifica a duração da procura. **Nota:** As estatísticas Atuais são úteis para resolução de problemas. Quando você contata o Suporte ao Cliente para solucionar problemas de fluxos, você pode ser solicitado a fornecer informações de estatísticas atuais.
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 da sua exibição. Os gráficos serão exibidos apenas depois que você selecionar o prazo de Último Intervalo (atualização automática), ou acima dele, e uma opção de agrupamento a ser exibida. Para obter mais informações sobre a configuração de gráficos, consulte Configurando gráficos. **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 gráficos, você deve remover a extensão do navegador bloqueador de anúncio. Para obter mais informações, consulte a documentação do navegador.
IP de Origem (contagem exclusiva)	Especifica o endereço IP de origem do fluxo.
IP de Destino (contagem exclusiva)	Especifica o endereço IP de destino do fluxo. Se houver vários endereços IP de destino associados a esse fluxo, este campo especificará o termo Vários e o número de endereços IP.
Porta de origem (contagem exclusiva)	Exibe a porta de origem do fluxo.

Tabela 26. Parâmetros de fluxos agrupados (continuação)

Cabeçalho	Descrição
Porta de destino (contagem exclusiva)	Especifica a porta de destino do fluxo. Se houver várias portas de destino associadas a este fluxo, este campo especificará o termo Várias e o número de portas.
Rede de origem (contagem exclusiva)	Especifica a rede de origem do fluxo. Se houver várias redes de origem associadas a este fluxo, este campo especificará o termo Várias e o número de redes.
Rede de destino (contagem exclusiva)	Especifica a rede de destino do fluxo. Se houver várias redes de destino associadas a este fluxo, este campo especificará o termo Várias e o número de redes.
Aplicativo (contagem exclusiva)	Especifica o aplicativo detectado dos fluxos. Se houver vários aplicativos associados a este fluxo, este campo especificará o termo Vários e o número de aplicativos.
Bytes de origem (soma)	Especifica o número de bytes de origem.
Bytes de destino (soma)	Especifica o número de bytes do destino.
Bytes Totais (soma)	Especifica o número total de bytes associados ao fluxo.
Pacotes de origem (soma)	Especifica o número de pacotes da origem.
Pacotes de origem (soma)	Especifica o número de pacotes da origem.
Pacotes de origem (soma)	Especifica o número de pacotes da origem.
Pacotes de destino (soma)	Especifica o número de pacotes do destino.
Total de pacotes (soma)	Especifica o número total de pacotes 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 você deseja agrupar os fluxos. Consulte a Tabela 2. Os grupos de fluxo são listados. Para obter mais informações sobre os detalhes do grupo de fluxo. Consulte a Tabela 1.
4. Para visualizar a página Lista de fluxos para um grupo, clique duas vezes no grupo de fluxo que você deseja investigar. A página Lista de fluxos não retém as configurações de gráfico que você pode ter definido na guia **Atividade de rede**. Para obter mais informações sobre o parâmetro da Lista de Fluxos, consulte a Tabela 2.
5. Para visualizar os detalhes de um fluxo, clique duas vezes no fluxo que você deseja investigar. Para obter mais informações sobre a página de detalhes do fluxo, consulte a Tabela 1.

Detalhes do fluxo

É possível visualizar uma lista de fluxos em vários modos, incluindo modo de fluxo ou 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. Para obter mais informações sobre os protocolos, consulte o *IBM Security QRadar Application*.
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.

Tabela 27. Detalhes do fluxo (continuação)

Parâmetro	Descrição
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.
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 *IBM Security QRadar SIEM Administration Guide*.
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 Baixo Nível	Especifica a categoria de nível inferior deste fluxo. Para obter mais informações sobre categorias, consulte o *IBM Security QRadar SIEM Administration Guide*.
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 *IBM Security QRadar SIEM Administration Guide*.
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

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

Sobre Esta Tarefa

Nota: É possível 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

É possível 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. Visão geral de gerenciamento de ativos

Coletar e visualizar os dados de ativo ajuda a identificar as ameaças e as vulnerabilidades. Um banco de dados de ativo exato facilita a conexão de ofensas que são acionadas em seu sistema para ativos físicos ou virtuais em sua rede.

Dados de ativo

Um *ativo* é qualquer terminal de rede que envie ou receba os dados em sua infraestrutura de rede. Por exemplo, blocos de notas, servidores, máquinas virtuais e dispositivos portáteis são todos ativos. Cada ativo no banco de dados de ativo é designado a um identificador exclusivo de modo que possa ser distinguido de outros registros de ativo.

Detectar os dispositivos também é útil na construção de um conjunto de dados de informações históricas sobre o ativo. Rastrear as informações de ativo conforme são alteradas ajuda a monitorar o uso de ativo em sua rede.

Perfis de ativos

Um *perfil de ativo* é uma coleção de todas as informações que o IBM Security QRadar SIEM coletou com o tempo sobre um ativo específico. O perfil inclui informações sobre os serviços que estão sendo executados no ativo e quaisquer informações de identidade que sejam conhecidas.

O QRadar SIEM cria automaticamente os perfis de ativo dos eventos de identidade e dados de fluxo bidirecionais ou, se estiverem configurados, varreduras de avaliação de vulnerabilidade. Os dados são correlacionados através de um processo que é denominado *reconciliação de ativo* e o perfil é atualizado conforme novas informações aparecem no QRadar. O nome do ativo é derivado das informações na atualização de ativo na ordem de precedência a seguir:

- Nome fornecido
- Nome de host NETBios
- Nome do host DNS
- endereço IP

Perfis de ativo de correlação para reduzir positivos falsos

Os administradores usam os perfis de ativo para relatar, procurar, auditar e criar regras para identificar ameaças, vulnerabilidades e uso de ativos. Os dados de ativo também são usados para propósitos de correlação para ajudar a reduzir positivos falsos. Por exemplo, se um invasor tentar usar um serviço específico que esteja em execução em um ativo, o QRadar pode determinar se o ativo é vulnerável a esse ataque, correlacionando o ataque ao perfil de ativo.

Origens de dados de ativo

Os dados de ativo são recebidos de diversas origens diferentes em sua implementação IBM Security QRadar.

Os dados de ativo são gravados para o banco de dados de ativo incrementalmente, geralmente duas ou três partes de dados por vez. Com exceção das atualizações de scanners de vulnerabilidade da rede, cada atualização de ativo contém informações sobre somente um ativo por vez.

Os dados do ativo geralmente são provenientes das origens de dados de ativo a seguir:

Eventos
Cargas úteis de evento, como aquelas criadas por DHCP ou servidores de autenticação, geralmente contêm logins de usuário, endereços IP, nomes de host, endereços MAC e outras informações de ativo. Esses dados são imediatamente fornecidos para o banco de dados de ativo para ajudar a determinar a qual ativo a atualização de ativo se aplica.

Os eventos são a causa primária para os desvios de crescimento de ativo.

Fluxos As cargas úteis de fluxo contêm informações de comunicação como endereços IP, porta e protocolo que são coletadas em intervalos regulares configuráveis. No fim de cada intervalo, os dados são fornecidos para o banco de dados de ativos, um endereço IP por vez.

Como os dados de ativo dos fluxos são combinados com um ativo baseado em um único identificador, o endereço IP, os fluxos de dados nunca são a causa de desvios de crescimento de ativo.

Scanners de vulnerabilidade
O QRadar é integrado a scanners de vulnerabilidade da IBM e de terceiros que podem fornecer dados de ativo como sistema operacional, software instalado e informações de correção. O tipo de dados varia de scanner para scanner, e pode variar de varredura para varredura. Conforme novos ativos, informações de porta e vulnerabilidade são descobertos, os dados são trazidos para o perfil de ativo com base nos intervalos de CIDR que são definidos na varredura.

É possível para os scanners introduzir desvios de crescimento de ativo, mas isso é raro.

Interface com o usuário
Os usuários que possuem a regra de Ativos podem importar ou fornecer informações de ativo diretamente para o banco de dados de ativo. As atualizações de ativo que são fornecidas diretamente por um usuário são para um ativo específico e, portanto, é efetuado bypass do estágio de reconciliação de ativo.

As atualizações de ativo que são fornecidas pelos usuários não apresentam desvios de crescimento de ativo.

Dados de ativo de domínio reconhecido

Quando a origem de dados de ativo é configurada com informações de domínio, todos os dados de ativo provenientes dessa origem de dados são automaticamente identificados com o mesmo domínio. Como os dados no modelo de ativo tem domínio reconhecido, as informações de domínio são aplicadas a todos os componentes do QRadar, incluindo identidades, ofensas, perfis de ativo e descoberta de servidor.

Ao visualizar o perfil de ativo, alguns campos podem estar em branco. Os campos em branco existem quando o sistema não tiver recebido essas informações em uma atualização de ativo ou as informações tiverem excedido o período de retenção de

ativo. O período de retenção padrão é de 120 dias. Um endereço IP que aparece como 0.0.0.0 indica que o ativo não contém informações de endereço IP.

Atualizações nos dados de ativo

O IBM Security QRadar usa as informações de identificação em uma carga útil do evento para determinar se deve criar um novo ativo ou atualizar um ativo existente.

Cada atualização de ativo deve conter informações confiáveis sobre um único ativo. Quando o QRadar recebe uma atualização de ativo, o sistema determina a qual ativo a atualização se aplica.

A *Reconciliação de ativo* é o processo de determinar o relacionamento entre as atualizações de ativo e o ativo relacionado no banco de dados de ativo. A reconciliação de ativo ocorre depois que o QRadar recebe a atualização mas antes que as informações sejam gravadas para o banco de dados de ativos.

Informações de identificação

Cada ativo deve conter pelo menos uma parte dos dados de identificação. As atualizações subsequentes que contêm uma ou mais partes dos mesmos dados de identificação são reconciliados com o ativo que possui esses dados. As atualizações que são baseadas em endereços IP são manipuladas cuidadosamente para evitar correspondências de ativo positivo falso. As correspondências de ativo positivo falso ocorrem quando um ativo físico tem a propriedade designada de um endereço IP que era anteriormente de propriedade de outro ativo no sistema.

Quando múltiplas partes dos dados de identificação forem fornecidas, o gerenciador de perfis de ativo priorizará as informações na ordem a seguir:

- Endereço MAC (mais determinista)
- Nome do host NetBIOS
- Nome do host DNS
- Endereço IP (menos determinista)

Endereços MAC, nomes de host NetBIOS e nomes de host DNS devem ser exclusivos e, portanto, são considerados como dados de identificação definitivos. As atualizações recebidas que correspondem a um ativo existente somente pelo endereço IP são manipuladas de forma diferente das atualizações que correspondem a dados de identificação mais definitivos.

Fluxo de trabalho de atualizações de ativo

Esse fluxo de trabalho descreve como o QRadar usa as informações de identificação em uma carga útil do evento para determinar se deve criar um novo ativo ou atualizar um ativo existente.

1. O QRadar recebe o evento. O gerenciador de perfis de ativo examina a carga útil do evento para informações de identificação.
2. Se as informações de identificação incluírem um endereço MAC, nomes de host NetBIOS ou nome de host DNS que já estejam associados a um ativo no banco de dados de ativo, esse ativo será atualizado com quaisquer novas informações.
3. Se as únicas informações de identificação disponíveis forem um endereço IP, o sistema reconciliará a atualização para o ativo existente que possui o mesmo endereço IP.

4. Se uma atualização de ativo incluir um endereço IP que corresponde a um ativo existente, mas também inclui mais informações de identificação que não corresponda ao ativo existente, o sistema usará outras informações para descartar uma correspondência de positivo falso antes que o ativo existente seja atualizado.
5. Se as informações de identificação não corresponderem a um ativo existente no banco de dados, um novo ativo será criado com base nas informações na carga útil do evento.

Conceitos relacionados:

"Regras de exclusão de reconciliação de ativo" na página 95
Com cada atualização de ativo que entra no IBM Security QRadar, as regras de exclusão de reconciliação de ativo aplicam testes no endereço MAC, nome do host NetBIOS, nome do host DNS e endereço IP na atualização de ativos.

Mesclagem de ativo

A *mesclagem de ativo* é o processo no qual as informações para um ativo são combinadas com as informações para outro ativo sob a premissa de que eles são realmente o mesmo ativo físico.

A mesclagem de ativos ocorre quando uma atualização de ativo contém dados de identificação que correspondem a dois perfis de ativo diferentes. Por exemplo, uma única atualização que contém um nome de host NetBIOS que corresponde a um perfil de ativo e um endereço MAC que corresponde a um perfil de ativo diferente pode acionar uma mesclagem de ativo.

Alguns sistemas podem causar altos volumes de mesclagem de ativos porque possuem origens de dados de ativos que combinam de forma inadvertida informações de identificação de dois ativos físicos diferentes em uma única atualização de ativos. Alguns exemplos desses sistemas incluem os ambientes a seguir:

- Servidores de syslog centrais que agem como um proxy de eventos
- Máquinas virtuais
- Ambientes de instalação automatizada
- Nomes de host não exclusivos, comuns com ativos como iPads e iPhones.
- As redes privadas virtuais que possuem endereços MAC compartilhados
- Extensões de origem de log em que o campo de identidade é `OverrideAndAlwaysSend=true`

Ativos que possuem vários endereços IP, endereços MAC ou nomes de host mostram desvios no crescimento de ativo e podem acionar notificações do sistema.

Conceitos relacionados:

"Desvios de crescimento de ativo"
Às vezes, as origens de dados de ativo produzem atualizações que causam desvios de crescimento de ativo em IBM Security QRadar.

Desvios de crescimento de ativo

Às vezes, as origens de dados de ativo produzem atualizações que causam desvios de crescimento de ativo em IBM Security QRadar.

Desvios de crescimento de ativo ocorrem quando o número de atualizações de ativo para um ativo alcançam o limite de retenção para um tipo específico de

informações de identidade. Para manter o funcionamento do banco de dados do ativo QRadar, a intervenção manual é necessária para resolver a acumulação de dados do ativo.

Espera-se que os perfis de ativo cresçam e enriqueçam nos dados com o tempo. Por exemplo, perfil de ativo inclui mais endereços IP conforme coleta leases IP e coleta mais nomes de usuário conforme novos usuários efetuam login. Os desvios de crescimento de ativo indicam que algo está fazendo com que o perfil de ativo colete uma grande quantia de dados em um ritmo inesperado.

O exemplo de servidor DHCP de crescimento de ativo não natural em um perfil de ativo

Considere um servidor de rede privada virtual (VPN) em uma rede do Protocolo de Configuração de Host Dinâmico (DHCP). O servidor VPN está configurado para designar endereços IP para clientes VPN recebidos, executando proxy de solicitações DHCP em nome do cliente para o servidor DHCP da rede.

Na perspectiva do servidor DHCP, o mesmo endereço MAC solicita repetidamente várias designações de endereço IP. No contexto de operações de rede, o servidor VPN está delegando os endereços IP para os clientes, mas o servidor DHCP não pode distinguir quando uma solicitação é feita por um ativo em nome de outro.

O log do servidor DHCP, que é configurado como origem de log QRadar, gera um evento de reconhecimento de DHCP (DHCP ACK) que associa o endereço MAC do servidor VPN ao endereço IP que é designado ao cliente VPN. Quando ocorre a reconciliação de ativos, o sistema reconcilia esse evento pelo endereço MAC, que resulta em um único ativo existente que aumenta em um endereço IP para cada evento DHCP ACK que é analisado.

Eventualmente, um perfil de ativo contém cada endereço IP que foi alocado para o servidor VPN. Esse desvio de crescimento de ativo é causado pelas atualizações de ativo que contêm informações sobre mais de um ativo.

Configurações de limite

Quando um ativo no banco de dados atinge um número específico de propriedades, tais como múltiplos endereços IP ou endereços MAC, o QRadar bloqueia esse ativo de receber mais atualizações.

As configurações do limite do Gerenciador de perfis do ativo especificam as condições sob as quais um ativo é bloqueado das atualizações. O ativo é atualizado normalmente até o valor limite. Quando o sistema coleta dados suficientes para exceder o limite, o ativo mostra um desvio no crescimento do ativo. As futuras atualizações para o ativo são bloqueadas até que o desvio de crescimento seja retificado.

Notificações do sistema para desvios de crescimento de ativo

IBM Security QRadar gera notificações do sistema para ajudar a identificar e gerenciar os desvios de crescimento de ativo em seu ambiente.

Os desvios de crescimento de ativo, que são crescimento não natural de dados de ativo, são específicos a um ambiente.

Quando um ativo é identificado por mostrar um desvio de crescimento, uma notificação de sistema aparece na lista **Mensagens** na parte superior direta do Console do QRadar. As notificações também aparecem nas **Notificações do sistema** no painel **Monitoramento de sistemas**.

As mensagens de sistema a seguir indicam que o QRadar identificou desvios de crescimento de ativo em potencial:

- `Os perfis de ativo detectados pelo sistema que excedem o limite de tamanho normal`
- `As regras de lista de bloqueio de ativo incluíram dados de novo ativo nas listas de bloqueio de ativos`

As mensagens de notificação do sistema incluem links para que os relatórios ajudem a identificar os ativos que possuem desvios de crescimento.

Conceitos relacionados:

"A resolução de problemas nos perfis de ativos que excedem o limite de tamanho normal"
O IBM Security QRadar gera a notificação de sistema a seguir quando a acumulação de dados em um único ativo excede os limites configurados para os dados de identificação.

"Os dados de ativo novo são incluídos nas listas de bloqueio de ativo" na página 93
IBM Security QRadar gera o notificação de sistema a seguir quando uma parte dos dados de ativo exibe o comportamento que é consistente com o crescimento de ativo de desvio.

A resolução de problemas nos perfis de ativos que excedem o limite de tamanho normal

O IBM Security QRadar gera a notificação de sistema a seguir quando a acumulação de dados em um único ativo excede os limites configurados para os dados de identificação.

`Os perfis de ativo detectados pelo sistema que excedem o limite de tamanho normal`

Explicação

A carga útil da notificação mostra uma lista dos cinco principais ativos frequentemente em desvios e porque o sistema marcou cada ativo como um desvio de crescimento. Conforme mostrado no exemplo a seguir, a carga útil também mostra o número de vezes em que o ativo tentou aumentar além do limite de tamanho do ativo.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Quando os dados de ativo excedem o limite configurado, o QRadar bloqueia o ativo de atualizações futuras. Essa intervenção evita que o sistema receba mais dados corrompidos e minimiza os impactos de desempenho que possam ocorrer, se o sistema tentar reconciliar as atualizações recebidas em um perfil de ativo estranhamente grande.

Ação do usuário necessária

Use as informações na carga útil de notificação para identificar os ativos que estão contribuindo para o desvio de crescimento de ativo e determinar o que está causando o crescimento anormal. A notificação fornece um link para um relatório de todos os ativos que estão vivenciando o crescimento de ativo de desvio nas últimas 24 horas.

Depois de resolver o desvio de crescimento de ativo em seu ambiente, é possível executar o relatório novamente.

1. Clique na guia **Atividade de log** e clique em **Procurar** > **Nova procura**.
2. Selecione a procura salva **Crescimento de ativo de desvio: Relatório de ativo**.
3. Use o relatório para identificar e reparar os dados de ativo inexatos que foram criados durante o desvio.

Se os dados de ativo forem válidos, QRadar os administradores podem aumentar os limites para os endereços IP, endereços MAC, nomes de host NetBIOS e nomes de host DNS na **Configuração do gerenciador de perfis de ativo** na guia QRadar **Admin**.

Conceitos relacionados:

"Notificações do sistema para desvios de crescimento de ativo" na página 91
IBM Security QRadar gera notificações do sistema para ajudar a identificar e gerenciar os desvios de crescimento de ativo em seu ambiente.

Os dados de ativo novo são incluídos nas listas de bloqueio de ativo

IBM Security QRadar gera o notificação de sistema a seguir quando uma parte dos dados de ativo exibe o comportamento que é consistente com o crescimento de ativo de desvio.

```
As regras de lista de bloqueio de ativo incluíram dados de novo ativo nas listas de
 bloqueio de ativos
```

Explicação

As regras de exclusão de ativo monitoram dados de ativo para consistência e integridade. As regras rastreiam partes específicas de dados de ativos com o tempo para assegurar que estão sendo observadas consistentemente com o mesmo subconjunto de dados em um tempo razoável.

Por exemplo, se uma atualização de ativo incluir um endereço MAC e um nome de host DNS, o endereço MAC será associado a esse nome de host DNS por um período sustentado. As atualizações de ativo subsequentes que contêm o endereço MAC também contêm esse mesmo nome de host DNS quando um é incluído na atualização de ativo. Se o endereço MAC for repentinamente associado a um nome de host DNS diferente por um curto período, a mudança será monitorada. Se o endereço MAC mudar novamente em um curto período, o endereço MAC será sinalizado por contribuir com uma instância de desvio ou crescimento de ativo anormal.

Ação do usuário necessária

Use as informações na carga útil de notificação para identificar as regras que são usadas para monitorar os dados de ativo. Clique no link **Desvios de ativo por origem de log** na notificação para ver os desvios de ativo que ocorreram nas últimas 24 horas.

Se os dados de ativo forem válidos, os administradores do QRadar podem configurar QRadar para resolver o problema.

- Se suas listas de bloqueio estiverem sendo preenchidas muito agressivamente, será possível ajustar as regras de exclusão de reconciliação de ativo que as preenche.
- Se você deseja incluir os dados no banco de dados de ativo, é possível remover os dados de ativo da lista de bloqueio e incluí-lo na lista de desbloqueio de ativo correspondente. Incluir os dados de ativo na lista de desbloqueio evita que eles reapareçam inadvertidamente na lista de bloqueio.

Conceitos relacionados:

"Regras de exclusão de reconciliação de ativo" na página 95
Com cada atualização de ativo que entra no IBM Security QRadar, as regras de exclusão de reconciliação de ativo aplicam testes no endereço MAC, nome do host NetBIOS, nome do host DNS e endereço IP na atualização de ativos.

"Listas de bloqueio de ativos"
Uma *lista de bloqueio de ativos* é uma coleção de dados que o IBM Security QRadar considera não confiável com base nas regras de exclusão de reconciliação de ativos. Os dados na lista de bloqueio de ativos provavelmente contribuem com os desvios de crescimento de ativo e o QRadar evita que os dados sejam incluídos no banco de dados de ativos.

Listas de bloqueio de ativos

Uma *lista de bloqueio de ativos* é uma coleção de dados que o IBM Security QRadar considera não confiável com base nas regras de exclusão de reconciliação de ativos. Os dados na lista de bloqueio de ativos provavelmente contribuem com os desvios de crescimento de ativo e o QRadar evita que os dados sejam incluídos no banco de dados de ativos.

Cada atualização de ativo no QRadar é comparado às listas de bloqueio do ativo. Os dados de ativo incluídos na lista de bloqueio são aplicados globalmente para todos os domínios. Se a atualização de ativo contiver informações de identificação (endereço MAC, nome do host NetBIOS, nome do host DNS ou endereço IP) que sejam encontradas em uma lista de bloqueio, a atualização recebida será descartada e o banco de dados de ativo não será atualizado.

A tabela a seguir mostra o nome de coleção de referência e o tipo para cada tipo de dados de ativo de identidade.

Tabela 29. Nomes de coleção de referência para dados da lista de bloqueio de ativos

Tipo de dados de identificação	Nome de coleção de referência	Tipo de coleção de referência
Endereços IP (v4)	Lista de bloqueio IPv4 de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: IP]
Nomes do host DNS	Lista negra de DNS de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: ALNIC*]
Nomes do host NetBIOS	Lista de bloqueio NetBIOS de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: ALNIC*]
Endereços MAC	Lista de bloqueio MAC de reconciliação de ativo	Conjunto de referência [Tipo de conjunto: ALNIC*]

* ALNIC é um tipo alfanumérico que pode acomodar os valores de nome do host e de endereço MAC.

Regras de exclusão de reconciliação de ativo

Com cada atualização de ativo que entra no IBM Security QRadar, as regras de exclusão de reconciliação de ativo aplicam testes no endereço MAC, nome do host NetBIOS, nome do host DNS e endereço IP na atualização de ativos.

Por padrão, cada parte dos dados de ativo são controlados sobre um período de duas horas. Se alguma parte dos dados de identificação na atualização do ativo exibir comportamento suspeito duas ou mais vezes em 2 horas, essa parte dos dados será incluída nas listas de
bloqueio de ativo. Existe uma lista de bloqueio separada para cada tipo de dados de ativo de identidade que é testada.

Em ambientes de domínio reconhecido, as regras de exclusão de reconciliação de ativo rastreiam o comportamento de dados de ativo separadamente para cada domínio.

As regras de exclusão de reconciliação de ativo testam os cenários a seguir:

Tabela 30. Regra de testes e respostas

Cenário	Resposta da regra
Quando um endereço MAC é associado a três ou mais endereços IP diferentes em 2 horas ou menos	Inclua o endereço MAC na lista de bloqueio MAC de domínio de reconciliação de ativo
Quando um nome de host DNS é associado a três ou mais endereços IP diferentes em 2 horas ou menos	Inclua o nome do host DNS na lista negra de DNS de Domínio de reconciliação de ativo
Quando um nome de host NetBIOS é associado a três ou mais endereços IP diferentes em 2 horas ou menos	Inclua o nome do host NetBIOS na lista de bloqueio NetBIOS de Domínio de reconciliação de ativo
Quando um endereço IPv4 é associado a três ou mais endereços MAC diferentes em 2 horas ou menos	Inclua o endereço IP na lista de bloqueio IPv4 de domínio de reconciliação de ativo
Quando um nome de host NetBIOS é associado a três ou mais endereços MAC diferentes em 2 horas ou menos	Inclua o nome do host NetBIOS na lista de bloqueio NetBIOS de Domínio de reconciliação de ativo
Quando um nome de host DNS é associado a três ou mais endereços MAC diferentes em 2 horas ou menos	Inclua o nome do host DNS na lista negra de DNS de Domínio de reconciliação de ativo
Quando um endereço IPv4 é associado a três ou mais nomes de host DNS diferente em 2 horas ou menos	Inclua o endereço IP na lista de bloqueio IPv4 de domínio de reconciliação de ativo
Quando um nome de host NetBIOS é associado a três ou mais nomes de host DNS diferentes em 2 horas ou menos	Inclua o nome do host NetBIOS na lista de bloqueio NetBIOS de Domínio de reconciliação de ativo
Quando um endereço MAC é associado a três ou mais nomes de host DNS diferente em 2 horas ou menos	Inclua o endereço MAC na lista de bloqueio MAC de domínio de reconciliação de ativo
Quando um endereço IPv4 é associado a três ou mais nomes de host NetBIOS diferentes em 2 horas ou menos	Inclua o endereço IP na lista de bloqueio IPv4 de domínio de reconciliação de ativo
Quando um nome de host DNS é associado a três ou mais nomes de host NetBIOS diferentes em 2 horas ou menos	Inclua o nome do host DNS na lista negra de DNS de Domínio de reconciliação de ativo
Quando um endereço MAC é associado a três ou mais nomes de host NetBIOS diferentes em 2 horas ou menos	Inclua o endereço MAC na lista de bloqueio MAC de domínio de reconciliação de ativo

É possível visualizar essas regras na guia **Ofensas**, clicando em **Regras** e, em seguida, selecionando o grupo **exclusão de reconciliação de ativo** na lista suspensa.

Conceitos relacionados:

"Exemplo: Regras de exclusão de ativo que são ajustadas para excluir endereços IP da lista de bloqueio"
É possível excluir endereços IP de estarem incluídos na lista de bloqueio ajustando as regras de exclusão de ativo.

Exemplo: Regras de exclusão de ativo que são ajustadas para excluir endereços IP da lista de bloqueio

É possível excluir endereços IP de estarem incluídos na lista de bloqueio ajustando as regras de exclusão de ativo.

Como administrador de segurança de Rede, gerencie uma rede corporativa que inclua um segmento de rede pública wifi em que os leases de endereço IP geralmente são curtos e frequentes. Os ativos neste segmento da rede tendem a ser transitórios, principalmente blocos de notas e dispositivos portáteis que efetuam login e logout do wifi público frequentemente. Normalmente, um único endereço IP é usado várias vezes por diferentes dispositivos em um curto período.

No restante de sua implementação, você tem uma rede cuidadosamente gerenciada que consiste somente em dispositivos de empresa inventariadas e bem nomeadas. Os leases de endereço IP são muito maiores nessa parte da rede e os endereços IP são acessados somente por autenticação. Nesse segmento de rede, você deve saber imediatamente quando existem quaisquer desvios de crescimento de ativo e você deseja manter as configurações padrão para as regras de exclusão de reconciliação de ativo.

Endereços IP de listagem negra

Nesse ambiente, as regras de exclusão de reconciliação de ativo padrão colocam na lista de bloqueio inadvertidamente a rede inteira em um curto tempo.

Sua equipe de segurança consideram um incômodo as notificações relacionadas ao ativo geradas pelo segmento wifi. Você deseja evitar que o wifi acione quaisquer notificações adicionais de crescimento de ativo de desvio.

Ajustando as regras de reconciliação de ativo para ignorar algumas atualizações de ativo

Revise o relatório **Desvio de ativo por origem de log** na última notificação do sistema. Determine se os dados incluídos na lista de bloqueio são provenientes do servidor DHCP em seu wifi.

Os valores na coluna **Contagem de evento/fluxo** e a coluna **Ofensas** para a linha correspondente pra a regra **AssetExclusion: Excluir IP por endereço MAC** indicam que seu servidor DHCP de wifi está acionando essa regra.

Inclua um teste nas regras de exclusão de reconciliação de ativo existente para impedir que as regras incluam os dados de wifi na lista de bloqueio.

```
Aplicar AssetExclusion: Excluir IP por endereço MAC em eventos que são detectados pelo
sistema Local e NÃO quando o(s) evento(s) foram detectados por um ou mais
MicrosoftDHCP @ microsoft.dhcp.test.com
e NÃO quando algum Domínio for a chave e algum IP de identidade for o valor em
em qualquer lista de bloqueio da Reconciliação de Ativos de Domínio IPv4
- Lista de bloqueio IPv4 de domínio de reconciliação de ativo de IP - IP
e quando, pelo menos, 3 eventos forem vistos com o mesmo IP de identidade e
diferente MAC de identidade em 2 horas.
```

A regra atualizada testa somente os eventos das origens de log que não estão em seu servidor DHCP de wifi. Para evitar que eventos DHCP de wifi passem por testes de análise de comportamento e conjunto de referência mais onerosos, você também moveu esse teste para a parte superior da pilha de teste

Exemplo: Como os erros de configuração para extensões de origem de log podem causar desvios de crescimento de ativo

Extensões de origem de log customizadas que são incorretamente configuradas podem causar desvios de crescimento de ativo.

Configure uma extensão de origem de log customizada para fornecer atualizações de ativo para QRadar analisando nomes de usuário da carga útil de eventos que estão em um servidor de log central. Configure a extensão da origem de log para substituir a propriedade de nome de host de evento de modo que as atualizações de ativos geradas pela origem de log customizada sempre especifiquem o nome de host DNS do servidor de log central.

Em vez de o QRadar receber uma atualização que tenha o nome do host do ativo no qual o usuário efetuou login, a origem de log gera várias atualizações de ativo que possuem o mesmo nome de host.

Nessa situação, o desvio de crescimento de ativo é causado por um perfil de ativo que contém vários endereços IP e nomes de usuário.

Capítulo 8. 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 várias opções de configuração do gráfico para visualizar seus dados.

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

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

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

Os tipos de gráfico incluem:

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

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

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

Suas configurações de gráfico não serão retidas quando você:

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

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

Visão geral do gráfico de série temporal

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

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

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

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

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

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

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

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

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

Tabela 31. Funções dos gráficos de séries temporais

Função	Descrição
Exibir dados com mais detalhes	Usando o recurso de zoom, é possível investigar segmentos de tempo menores do tráfego de evento. • Mova o ponteiro do mouse sobre o gráfico e use o botão de rolagem do mouse para aumentar o gráfico (role o botão de rolagem do mouse para cima). • Destaque a área do gráfico que deseja ampliar. Ao liberar o botão do mouse, o gráfico exibirá um segmento de tempo menor. Agora é possível clicar e arrastar o gráfico para verificar o gráfico. Ao aumentar o gráfico de série temporal, o gráfico será 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 para o intervalo de tempo máximo. É possível expandir um intervalo de tempo usando uma das seguintes opções: • Clique em Reconfiguração de zoom no canto superior esquerdo do gráfico. • Mova o ponteiro do mouse sobre o gráfico e, em seguida, use o botão de roda do mouse para expandir a visualização (role o botão de roda do mouse para baixo).

Tabela 31. Funções dos gráficos de séries temporais (continuação)

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

Legendas do gráfico

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

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

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

Configurando gráficos

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

Antes de Iniciar

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

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

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

Sobre Esta Tarefa

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

Procedimento

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

Opção	Descrição
Parâmetro	Descrição
Value to Graph	Na caixa de listagem, selecione o tipo de objeto que você deseja que apareça no eixo Y do gráfico. As opções incluem todos os eventos normalizados e customizados ou parâmetros de fluxo incluídos em seus parâmetros de procura.
Display Top	Na caixa de listagem, selecione o número de objetos que você deseja visualizar no gráfico. O padrão é 10. A representação de gráfico com mais de 10 itens pode fazer com que os dados de gráfico fiquem ilegíveis.
Tipo de gráfico	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
Capturar Dados de Série Temporal	Selecione essa caixa de seleção se você desejar ativar a captura de dados das séries temporais. Ao selecionar essa caixa de seleção, o recurso de gráfico começará a acumular dados para os gráficos de séries temporais. Por padrão, esta opção está desativada. Essa opção está apenas disponível em gráficos Séries Temporais.
Intervalo de tempo	Na caixa de listagem, selecione o intervalo de tempo que você deseja visualizar. Essa opção está apenas disponível em gráficos Séries Temporais.

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

Capítulo 9. 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 por itens que correspondem aos seus critérios

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

Sobre Esta Tarefa

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

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

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

Tabela 32. Opções da pesquisa

Opções	Descrição
Grupo	Selecione um Grupo de Procura de fluxo ou grupo de procura de evento para visualizar na lista **Procuras salvas disponíveis**.
Digitar Procura Salva ou Selecionar a partir da Lista	Digite o nome de uma procura salva ou uma palavra-chave para filtrar a lista de **Procuras salvas disponíveis**.
Procuras Salvas Disponíveis	Essa lista exibe todas as procuras disponíveis, a menos que você use as opções **Procura salva de tipo ou grupo** ou **Selecionar a partir da lista** para aplicar um filtro na lista. É possível selecionar uma procura salva nessa lista para exibir ou editar.
Procura	O ícone **Procurar** está disponível em várias áreas de janela na página de procura. É possível clicar em Procurar quando você terminar de configurar a procura e desejar visualizar os resultados.
Inclua em Minhas Procuras Rápidas	Selecione essa caixa de seleção para incluir esta procura em seu menu **Procura rápida**.
Incluir em Meu Painel	Selecione esta caixa de seleção para incluir os dados da 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 for agrupada.
Defina como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esta pesquisa com todos os outros usuários.
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 o Tempo Real (fluxo) estiver ativado, você não conseguirá agrupar seus resultados da procura. Se você selecionar qualquer opção de agrupamento na área de janela Definição de Coluna, uma mensagem de erro será aberta.

Tabela 32. Opções da pesquisa (continuação)

Opções	Descrição
Último Intervalo (atualização automática)	Exibe os resultados da procura no modo de atualização automática. No modo de atualização automática, as guias **Atividade do log** e **Atividade de rede** atualizam em intervalos de um minuto para exibir as informações mais recentes.
Recente	Selecione um intervalo de tempo predefinido para sua procura. Depois de selecionar essa opção, você deve selecionar uma opção de intervalo de tempo na caixa de listagem.
Intervalo Específico	Selecione um intervalo de tempo customizado para sua procura. Após selecionar essa opção, deve-se selecionar o intervalo de data e hora nos calendários de **Horário de início** e **Horário de encerramento**.
Acumulação de Dados	Esta área de janela será exibida apenas quando você carregar uma procura salva. A ativação de contagens exclusivas em dados acumulados que são compartilhados com muitas outras procuras e relatórios salvos pode diminuir o desempenho do sistema. Quando você carrega uma procura salva, esta área de janela exibe as seguintes opções: • Se nenhum dado estiver acumulando para esta procura salva, a mensagem de informação a seguir será exibida: `Dados não estão sendo acumulados para esta procura`. • Se os dados forem acumulando para esta procura salva, as seguintes opções serão exibidas: – **colunas** – Quando você clica ou passa o mouse sobre esse link, uma lista das colunas que estão acumulando dados é aberta. – **Ativar contagens exclusivas/desativar contagens exclusivas** – Este link permite que você ative ou desative os resultados da procura para exibir evento exclusivo e contagens de fluxo em vez de média de contagens ao longo do tempo. Depois de clicar no link **Ativar contagens exclusivas**, uma caixa de diálogo é aberta e indica quais procuras e relatórios salvos compartilham os dados acumulados.
Filtros Atuais	Esta lista exibe os filtros que são aplicados a esta procura. As opções para incluir um filtro estão localizadas acima da lista **Filtros atuais**.
Salve os resultados quando a procura for concluída	Selecione esta caixa de seleção para salvar e nomear os resultados da procura.
Exibir	Selecione esta lista para especificar uma coluna predefinida que está configurada para exibir nos resultados da procura.
Digitar Coluna ou Selecionar a partir da Lista	É possível usar o campo para filtrar as colunas que são listadas na lista Colunas Disponíveis. Digite o nome da coluna que você deseja localizar ou digite uma palavra-chave para exibir uma lista de nomes de colunas. Por exemplo, digite `Dispositivo` para exibir uma lista de colunas que incluem Dispositivo no nome da coluna.
Colunas Disponíveis	Essa lista exibe as colunas disponíveis. Colunas que estão atualmente em uso para esta procura salva são realçadas e exibidas na lista **Colunas**.
Inclua e remova ícones de coluna (conjunto superior)	Use o conjunto de ícones na parte superior para customizar a lista **Agrupado 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 da 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 32. Opções da pesquisa (continuação)

Opções	Descrição
Agrupar Por	Esta lista especifica as colunas nas quais a procura salva agrupa os resultados. Use as opções a seguir para customizar adicionalmente a lista Agrupar Por: • Mover para Cima – Selecione uma coluna e mova-a para cima através da lista de prioridade usando o ícone **Mover para cima**. • Mover para Baixo – Selecione uma coluna e mova-o 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 pela primeira coluna na lista **Agrupado por** e, em seguida, agrupados pela próxima coluna na lista.
Colunas	Especifica colunas que são escolhidas para a procura. É possível selecionar mais colunas na lista **Colunas disponíveis**. É possível customizar ainda mais a lista **Colunas** usando as seguintes opções: • **Mover para cima** – Move a coluna selecionada para cima na lista de prioridades. • **Mover para baixo** – Move o próprio selecionado na lista de prioridades. Se o tipo de coluna for numérico ou baseado 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.
Classificar por	Na primeira caixa de listagem, selecione a coluna pela qual você deseja classificar os resultados da procura. Em seguida, a partir da segunda caixa de listagem, selecione a ordem que você deseja exibir para os resultados de procura. As opções incluem **Decrescente** e **Crescente**.
Limite de Resultados	É possível especificar o número de linhas que uma pesquisa retorna na janela Editar Procura. O campo **Limitar resultados** também aparece na janela Resultados. • Para uma procura salva, o limite será armazenado na procura salva e reaplicado no carregamento da procura. • Ao classificar em uma coluna no resultado de procura que tem limite de linha, a classificação será feita dentro das linhas limitadas mostradas na grade de dados. • Para obter um agrupado por procura com gráfico de série temporal ligado, o limite da linha somente se aplica à grade de dados. O suspenso **Parte superior** no gráfico de série temporal ainda controla quantas séries de tempo são desenhadas no gráfico.

Procedimento

1. Escolha uma das opções a seguir:
   - Para procurar eventos, clique na guia **Atividade do log**.
   - Para fluxos de procura, clique na guia **Atividade de rede**.
2. Na caixa de listagem **Procurar**, selecione **Nova procura**.
3. Para selecionar uma procura salva anteriormente:
   a. Escolha uma das seguintes opções: `A partir da lista de Procuras Salvas Disponíveis, selecione a procura salva que você deseja carregar. No campo Digitar a procura salva ou Selecionar na lista, digite 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 do Intervalo de Tempo, selecione as opções para o intervalo de tempo que você deseja capturar para essa procura.
5. Opcional. Na área de janela de Acumulação de Dados, ative contagens exclusivas:

a. Clique em **Ativar contagens exclusivas**.
b. Na janela Aviso, leia a mensagem de aviso e clique em **Continuar**. Para obter mais informações sobre a ativação de conta exclusiva, consulte a Tabela 1.

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

Resultados

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

.

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

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

Salvando critérios de procura

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

Sobre Esta Tarefa

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

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

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

Procedimento

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

Opção	Descrição
Parâmetro	Descrição
Nome da Procura	Digite o nome exclusivo que deseja designar a esses critérios de procura.
Designar procura ao(s) grupo(s)	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, essa procura salva será designada ao grupo Outros por padrão. Para obter mais informações, consulte Gerenciando grupos de procura.
Gerenciar Grupos	Clique em **Gerenciar grupos** para gerenciar grupos de procura. Para obter mais informações, consulte Gerenciando grupos de procura.
Timespan options:	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 (atualização automática)** – selecione essa opção para filtrar os resultados da procura durante o 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 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 a data e hora do intervalo 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
Include in my Dashboard	Selecione esta caixa de seleção para incluir os dados da 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 for agrupada.
Configurar como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.
Compartilhar com Todos	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

5. Clique em **OK**.

Procura planejada

Use a opção Procura planejada para planejar uma procura e visualizar os resultados.

É possível planejar uma procura que seja executada em um horário específico do dia ou da noite.

Exemplo:
Se você planejar uma procura para ser executada na noite, poderá investigar de manhã. Ao contrário dos relatórios, você tem a opção de agrupar os resultados da procura e investigar ainda mais. É possível procurar pelo número de logins com falha no grupo de rede. Se o resultado for geralmente 10 e o resultado da procura for 100, é possível agrupar os resultados da procura para facilitar a investigação. Para ver qual usuário possui mais logins com falha, é possível agrupar pelo nome de usuário. É possível aprofundar a investigação.

É possível planejar uma procura nos eventos ou nos fluxos na guia **Relatórios**. Deve-se selecionar um conjunto de critérios de procura salvo anteriormente para planejamento.

1. Criar um relatório

   Especifique as informações a seguir na janela **Assistente de relatório**:

   - O tipo de gráfico é Eventos/Logs ou Fluxos.
   - O relatório baseia-se em uma procura salva.
   - Gerar uma ofensa.

     É possível escolher a opção **criar uma ofensa individual** ou a opção **incluir resultado em uma ofensa existente**.

     Também é possível gerar uma procura manual.
2. Visualizar resultados da procura

É possível visualizar os resultados da procura planejada na guia **Ofensas**.

- As ofensas da procura planejada são identificadas pela coluna **Tipo de ofensa**.

  Se você criar uma ofensa individual, será gerada uma ofensa sempre que o relatório for executado. Se incluir o resultado da procura salva em uma ofensa existente, será criada uma ofensa na primeira vez que o relatório for executado. O relatório subsequente é executado anexado a essa ofensa. Se nenhum resultado for retornado, o sistema não anexará ou criará uma ofensa.

- Para visualizar o resultado da procura mais recente na janela Sumarização de ofensas, dê um clique duplo em uma ofensa da procura planejada na lista de ofensas. Para visualizar a lista de todas as execuções de procura planejada, clique em **Resultados da procura** na área de janela **Últimos cinco resultados da procura**.

É possível designar uma ofensa da Procura planejada a um usuário.

Tarefas relacionadas:

"Procurando por itens que correspondem aos seus critérios" na página 103
É possível procurar por dados que correspondem ao seu critério de procura.

"Designando ofensas para usuários" na página 39
Usando a guia **Ofensas**, você pode designar ofensas aos usuários para investigação.

Opções de procura avançada

Use o campo **Procura avançada** para inserir uma Ariel Query Language (AQL) que especifique os campos que você deseja e como você deseja agrupá-los para executar uma consulta.

O campo **Procura avançada** tem conclusão automática e destaque da sintaxe.

Use a conclusão automática e o destaque da sintaxe para ajudar a criar consultas. Para obter informações sobre os navegadores da web suportados, consulte "Navegadores da Web Suportados" na página 3

Acessando a procura avançada

Acesse a opção **Procura avançada** na barra de ferramentas **Procurar** que está nas guias **Atividade de rede** e **Atividade de log** para digitar uma consulta AQL.

Selecione **Procura avançada** na caixa de listagem na barra de ferramentas **Procurar**.

Expanda o campo **Procura avançada** seguindo estas etapas:

1. Arraste o ícone de expansão que está à direita do campo.
2. Pressione Shift + Enter para acessar a próxima linha.
3. Pressione Enter.

É possível clicar com o botão direito em qualquer valor no resultado da procura e filtrar por esse valor.

Dê um clique duplo em qualquer linha no resultado da procura para ver mais detalhes.

Todas as procuras, incluindo procuras AQL, são incluídas no log de auditoria.

Exemplos de sequência de caracteres de procura AQL

A tabela a seguir fornece exemplos de sequências de caracteres de procura AQL.

Tabela 33. Exemplos de sequências de caracteres de procura AQL

Descrição	Exemplo
Selecione colunas padrão de eventos.	`SELECT * FROM events`
Selecione colunas padrão de fluxos.	`SELECT * FROM flows`

Tabela 33. Exemplos de sequências de caracteres de procura AQL (continuação)

Descrição	Exemplo
Selecione colunas específicas.	`SELECT sourceip, destinationip FROM events`
Selecione colunas específicas e ordene os resultados.	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
Execute uma consulta de procura agregada.	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
Execute uma chamada de função em uma cláusula SELECT.	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
Filtre os resultados da procura usando uma cláusula WHERE.	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
Procure eventos que acionaram uma regra específica, a qual é baseada no nome da regra ou no texto parcial no nome da regra.	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
Referencie nomes do campo que contenham caracteres especiais, como caracteres aritméticos ou espaços, colocando o nome do campo entre aspas duplas.	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

A tabela a seguir fornece exemplos de sequências de caracteres de procura AQL para X-Force.

Tabela 34. Exemplos de sequência de caracteres de procura AQL para X-Force

Descrição	Exemplo
Verifique um endereço IP em uma categoria X-Force com um valor de confiança.	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3`
Procure pelas categorias de URL de X-Force associadas a uma URL.	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
Recupere as categorias de IP X-Force que estão associadas a um IP.	`select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

Para obter informações adicionais sobre funções, campos de procura e operadores, consulte o *Guia de Idioma de Consulta Ariel*.

Exemplos de sequência de caracteres de procura AQL

Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

Relatando o uso da conta

Comunidades de usuário diferentes podem ter indicadores de uso e de ameaça diferentes.

Use os dados de referência para relatar várias propriedades de usuário, por exemplo, departamento, local ou gerente.

É possível usar dados de referência externa.

A consulta a seguir retorna informações de metadados sobre o usuário de seus eventos de login.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Insight em vários identificadores de conta

Nesse exemplo, usuários individuais possuem várias contas na rede. A organização requer uma única visualização de uma atividade de usuários.

Use os dados de referência para mapear IDs do usuário local para um ID global.

A consulta a seguir retorna as contas do usuário usadas por um ID global em eventos sinalizados como suspeitos.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

A consulta a seguir mostra as atividades concluídas por um ID global.

```
SELECT
QIDNAME(qid) as 'Event name,
starttime as Time,
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event  Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Identificar indicadores suspeitos de longo prazo

Muitas ameaças usam comando e controle para se comunicarem periodicamente por dias, semanas e meses.

Procuras avançadas podem identificar padrões de conexão com o passar do tempo. Por exemplo, é possível consultar um volume consistente, curto e baixo, o número de conexões por dia/semana/mês entre endereços IP ou um endereço IP e uma localização geográfica.

Use a API REST do IBM Security QRadar para gerar uma ofensa ou para preencher um conjunto de referência ou uma tabela de referência.

A consulta a seguir detecta possíveis instâncias de indicadores por hora.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'hh')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING 'different hours' > 20
AND 'total flows' < 25
LAST 24 hours
```

Dica: É possível modificar essa consulta para funcionar em logs de proxy e outros tipos de eventos.

A consulta a seguir detecta possíveis instâncias de indicadores diários.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING 'different days' > 4
AND 'total flows' < 14
LAST 7 days
```

A consulta a seguir detecta indicadores diários entre um IP de origem e um IP de destino. Os tempos dos indicadores não ficam no mesmo horário todos os dias. O lapso de tempo entre os indicadores é curto.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and 'total flows' < 10
LAST 7 days
```

A consulta a seguir detecta indicadores diários para um domínio usando eventos de log de proxy. Os tempos dos indicadores não ficam no mesmo horário todos os dias. O lapso de tempo entre os indicadores é curto.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

A propriedade **url_domain** é uma propriedade customizada dos logs de proxy.

Inteligência de ameaça externa

Os dados de uso e de segurança correlacionados aos dados de inteligência de ameaça externa podem fornecer indicadores de ameaça importantes.

Procuras avançadas podem fazer uma referência cruzada de indicadores de inteligência de ameaça externa com outros eventos de segurança e dados de uso.

Essa consulta mostra como é possível criar um perfil dos dados de ameaça externa por muitos dias, semanas ou meses para identificar e priorizar o nível de risco de ativos e contas.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Inteligência e configuração de ativo

Os indicadores de uso e ameaça variam por tipo de ativo, sistema operacional, variação de vulnerabilidade, classificação e outros parâmetros.

Nessa consulta, as procuras avançadas e o modelo de ativo fornecem insight operacional para um local.

A função **Assetproperty** recupera valores de propriedade dos ativos, os quais permitem que você inclua dados de ativo nos resultados.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

A consulta a seguir mostra como é possível usar as procuras avançadas e o rastreamento de identidade do usuário no modelo de ativo.

A função **AssetUser** recupera o nome de usuário do banco de dados de ativo.

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY 'Total Flows' DESC
LAST 3 HOURS
```

Função Network LOOKUP

É possível usar a função **Network LOOKUP** para recuperar o nome da rede que está associado a um endereço IP.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Função Rule LOOKUP

É possível usar a função **Rule LOOKUP** para recuperar o nome de uma regra por seu ID.

```
SELECT RULENAME(123) FROM events
```

A consulta a seguir retorna eventos que acionaram um nome da regra específico.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

TEXT SEARCH Completa

É possível usar o operador TEXT SEARCH para executar procuras de texto completas usando a opção **Procura avançada**.

Nesse exemplo, há uma série de eventos que contêm a palavra "firewall" na carga útil. É possível procurar esses eventos usando a opção **Filtro rápido** e a opção **Procura avançada** na guia **Atividade de log**.

- Para usar a opção **Filtro rápido**, digite o texto a seguir na caixa **Filtro rápido**: `'firewall'`
- Para usar a opção **Procura avançada**, digite a consulta a seguir na caixa **Procura avançada**:

  ```
  SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
  ```

Propriedade customizada

É possível acessar propriedades customizadas para eventos e fluxos quando você usar a opção **Procura avançada**.

A consulta a seguir usa a propriedade customizada "MyWebsiteUrl" para classificar eventos por uma determinada URL da web:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Conceitos relacionados:

"Opções de procura de filtro rápido"
Procure cargas úteis de fluxos e de evento digitando uma sequência de caracteres de procura de texto que use palavras ou frases simples.

Tarefas relacionadas:

"Criando uma propriedade customizada baseada em regex" na página 132
É possível criar uma propriedade customizada baseada em regex para corresponder às cargas úteis de fluxo ou evento para uma expressão regular.

Opções de procura de filtro rápido

Procure cargas úteis de fluxos e de evento digitando uma sequência de caracteres de procura de texto que use palavras ou frases simples.

É possível filtrar suas procuras a partir destes locais:

Barras de ferramentas Atividade de log e Atividade de rede
Selecione **Filtro rápido** na caixa de listagem na barra de ferramentas **Procurar** para digitar uma sequência de caracteres de procura de texto. Clique no ícone **Filtro rápido** para aplicar seu **Filtro rápido** à lista de eventos ou fluxos.

Caixa de diálogo Incluir filtro
Clique no ícone **Incluir filtro** na guia **Atividade de log** ou **Atividade de rede**.

Selecione **Filtro rápido** como seu parâmetro de filtro e digite uma sequência de caracteres de procura de texto.

Páginas de procura de fluxo
Inclua um filtro rápido na lista de filtros.

Ao visualizar **fluxos** no último modo de intervalo ou no modo de intervalo em tempo real (fluxo), é possível digitar somente palavras ou frases simples no campo **Filtro rápido**. Ao visualizar **eventos** ou **fluxos** em um intervalo de tempo, siga essas diretrizes de sintaxe:

Tabela 35. Diretrizes de sintaxe de filtro rápido.

Descrição	Exemplo
Inclua qualquer texto simples que você espera localizar na carga útil.	`Firewall`
Procure frases exatas incluindo vários termos entre aspas duplas.	`"Negação de firewall"`
Inclua curingas de caracteres únicos e múltiplos. O termo de procura não pode começar com um curinga.	`F?rewall` ou `F??ew*`
Agrupe termos com expressões lógicas, como AND, OR e NOT. Para serem reconhecidas como expressões lógicas e não como termos de procura, a sintaxe e os operadores devem estar em maiúscula.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
Ao criar critérios de procura que incluem a expressão lógica NOT, deve-se incluir pelo menos um outro tipo de expressão lógica, caso contrário, nenhum resultado será retornado.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
Preceda os seguintes caracteres por uma barra invertida para indicar que o caractere faz parte do termo de pesquisa: `+ - && || ! () {} [] ^ " ~ * ? : \.`	`"%PIX\-5\-304001"`

Os termos de procura são combinados em sequência a partir do primeiro caractere na palavra ou frase da carga útil. O `usuário` do termo de procura corresponde ao `user_1` e `user_2`, mas não corresponde às frases a seguir: `ruser`, `myuser` ou `anyuser`.

Procuras de filtro rápido usam o código de idioma em inglês. *Código de idioma* é uma configuração que identifica o idioma ou a geografia e determina convenções de formatação como ordenação, conversão de caso, classificação de caractere, o idioma de mensagens, a representação de data e hora e a representação numérica.

O código de idioma é configurado pelo seu sistema operacional. É possível configurar o QRadar para substituir a configuração do código de idioma do sistema operacional. Por exemplo, é possível configurar o código de idioma para **inglês** e o Console do QRadar pode ser configurado para **Italiano (Italian)**.

Se você usar caracteres Unicode em sua Consulta de procura de filtro rápido, resultados da procura inesperados podem ser retornados.

Se você escolher um código de idioma que não está em inglês, é possível usar a opção Procura avançada no QRadar para procurar evento e dados de carga útil.

Conceitos relacionados:

Capítulo 9, “Procuras de dados”, na página 103
Nas guias **Atividade de log**, **Atividade de rede** e **Ofensas**, é possível procurar eventos, fluxos e ofensas usando critérios específicos.

“Opções de procura avançada” na página 109
Use o campo **Procura avançada** para inserir uma Ariel Query Language (AQL) que especifique os campos que você deseja e como você deseja agrupá-los para executar uma consulta.

“Exemplos de sequência de caracteres de procura AQL” na página 110
Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

Tarefas relacionadas:

“Atualizando preferências do usuário” na página 13
É possível configurar as preferências do usuário, como código de idioma, na principal interface com o usuário do IBM Security QRadar SIEM.

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 categorias, consulte o *IBM Security SIEM QRadar Guia de Administração*.

Tabela 36. Opções de procura da página Minhas ofensas e Todas as 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**. É possível selecionar uma procura salva nessa lista para exibir ou editar.
Todas as ofensas	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. Depois de selecionar essa opção, você deve selecionar uma opção de intervalo de tempo na caixa de listagem.
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 da Ofensa	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.

Tabela 36. Opções de procura da página Minhas ofensas e Todas as ofensas (continuação)

Opções	Descrição
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.
Exclude	As opções nessa área de janela permitem que você exclua as ofensas dos resultados da procura. As opções incluem: • Ofensas Ativas • Ofensas Ocultas • Ofensas Encerradas • 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.

Tabela 36. Opções de procura da página Minhas ofensas e Todas as ofensas (continuação)

Opções	Descrição
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 Ofensa	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 37. 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.
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. É possível 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 de 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.

Tabela 37. Opções de tipo de ofensa (continuação)

Tipos de ofensas	Descrição
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 38. Opções de procura da página Por IP de origem

Opções	Descrição
Todas as ofensas	É possível selecionar essa opção para procurar todos os endereços IP de origem, independentemente do intervalo de tempo.
Recente	É possível selecionar essa opção e, nessa caixa de listagem, selecione o intervalo de tempo que você deseja procurar.
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	É possível selecionar as caixas de seleção para as ofensas às quais você deseja excluir dos resultados da procura. As opções incluem: • **Ofensas Ativas** • **Ofensas Ocultas** • **Ofensas Encerradas** • **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 39. Opções de procura da página Por IP de destino

Opções	Descrição
Todas as ofensas	É possível selecionar essa opção para procurar todos os endereços IP de destino, independentemente do intervalo de tempo.
Recente	É possível 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	É possível 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.

Tabela 39. Opções de procura da página Por IP de destino (continuação)

Opções	Descrição
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 40. 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 os grupos de procura. Consulte Gerenciando grupos de pesquisa.

Opção	Descrição
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 para as 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.`
Configurar como Padrão	Selecione esta caixa de seleção para configurar essa procura como sua procura padrão.

5. Clique em **OK**.

Excluindo critérios de procura

É possível excluir os critérios de procura.

Sobre Esta Tarefa

Ao excluir uma procura salva, objetos associados a ela poderão não funcionar. Os relatórios e as regras de detecção de anomalias são objetos do QRadar que usam os critérios de procura salvos. Após excluir uma procura salva, edite os objetos associados para assegurar-se de que eles continuarão a funcionar.

Procedimento

1. Escolha uma das opções a seguir:
   - Clique na guia **Atividade de Log**.
   - Clique na guia **Atividade de Rede**.
2. Na caixa de listagem **Procurar**, selecione **Nova procura** ou **Editar procura**.
3. Na área de janela Procuras Salvas, selecione uma procura salva na caixa de listagem **Procuras salvas disponíveis**.
4. Clique em **Excluir**.
   - Se os critérios de procura salvos não estiverem associados a outros objetos do QRadar, uma janela de confirmação será exibida.

- Se os critérios de procura salvos estiverem associados a outros objetos, a janela Excluir procura salva será exibida. A janela lista os objetos associados à 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 forem associados a outros objetos do QRadar, acesse os objetos associados que você observou e edite-os para remover ou substituir a associação com a procura salva excluída.

Usando uma subprocura para refinar resultados da procura

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

Antes de Iniciar

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

Sobre Esta Tarefa

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

Procedimento

1. Escolha uma das opções a seguir:
   - Clique na guia **Atividade de Log**.
   - Clique na guia **Atividade de Rede**.
2. Execute uma procura.
3. Quando a procura estiver concluída, inclua outro filtro:
   a. Clique em **Incluir filtro**.
   b. Na primeira caixa de listagem, selecione um parâmetro que você deseja procurar.
   c. Na segunda caixa de listagem, selecione o modificador que você deseja usar para a procura. A lista de modificadores disponíveis depende do atributo selecionado na primeira lista.
   d. No campo de entrada, insira as informações específicas relacionadas à sua procura.
   e. Clique em **Incluir filtro**.

Resultados

A área de janela Filtro Original especifica os filtros originais aplicados à procura de base. A área de janela Filtro do Current especifica os filtros aplicados na subprocura. É possível limpar os filtros de subprocura sem reiniciar a procura de

base. Clique no link **Limpar filtro** ao lado do filtro que você deseja limpar. Se você limpar um filtro na área de janela Filtro Original, a procura de base será reativada.

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

O que Fazer Depois

Salvar critérios de procura

Gerenciando resultados da procura

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

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

A qualquer momento quando uma procura estiver em andamento, será possível retornar às guias **Atividade de log** ou **Atividade de rede** para visualizar os resultados de procura parciais ou completos.

Cancelando uma procura

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

Sobre Esta Tarefa

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

Procedimento

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

Excluindo uma procura

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

Procedimento

1. Escolha uma das opções a seguir:
   - Clique na guia **Atividade de Log**.
   - Clique na guia **Atividade de Rede**.
2. No menu **Procurar**, selecione **Gerenciar resultados da procura**.

3. Selecione o resultado da procura que deseja excluir.
4. Clique em **Excluir**.
5. Clique em **Sim**.

Gerenciando grupos de procura

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

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

Visualizando grupos de procura

Um conjunto padrão de grupos e subgrupos estão disponíveis.

Sobre Esta Tarefa

É possível visualizar grupos de procura nas janelas Grupos de procura de eventos, Grupo de procura de fluxo ou Grupo de procura.

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

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

Tabela 41. Parâmetros da janela de grupo de procura

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

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

Tabela 42. Funções da janela barra de ferramentas do grupo de procura

Função	Descrição
Novo grupo	Para criar um novo grupo de procura, você pode clicar em **Novo grupo**. Consulte Criando um grupo de procura novo.
Editar	Para editar um grupo de procura existente, você pode clicar em **Editar**. Consulte Editando um grupo de procura.
Copiar	Para copiar uma procura salva em 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 você deseja remover e 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. Visualize os grupos de procura.

Criando um novo grupo de procura

É possível criar um novo grupo de procura.

Procedimento

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

Editando um grupo de procura

É possível editar os campos **Nome** e **Descrição** de um grupo de procura.

Procedimento

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

Copiando uma procura salva em outro grupo

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

Procedimento

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

Removendo um grupo ou uma procura salva de um grupo

É possível usar o ícone **Remover** para remover uma procura de um grupo ou remover um grupo de procura.

Sobre Esta Tarefa

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

Não é possível remover os seguintes grupos do sistema:

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

Procedimento

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

Capítulo 10. 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 requeridas

Para criar propriedades customizadas se 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, também poderá criar e modificar propriedades customizadas na guia Administração.

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

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

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

Tipos de propriedades customizadas

É possível criar um tipo de propriedade customizada.

Ao criar uma propriedade customizada, 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 do usuário real ou a conta que foi alterada não pode ser exibida. É possível criar uma propriedade customizada para

extrair essas informações dos logs e, em seguida, usar a propriedade em procuras e relatórios. O uso desse recurso requer conhecimento avançado de expressões regulares (regex).

Regex define o campo que você deseja que se torne a propriedade customizada. Após inserir uma instrução regex, será possível validá-la em relação à carga útil. Ao definir padrões regex customizados, 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 no 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 com base no cálculo, é possível executar cálculos sobre as propriedades de fluxo ou evento numérico existentes para produzir uma propriedade calculada.

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

Criando uma propriedade customizada baseada em regex

É possível criar uma propriedade customizada baseada em regex para corresponder às cargas úteis de fluxo ou evento para uma expressão regular.

Sobre Esta Tarefa

Ao configurar uma propriedade customizada baseada em regex, a janela Propriedade de Evento Customizado ou Propriedade de Fluxo Customizado fornece parâmetros. A tabela a seguir fornece informações de referência para alguns parâmetros.

Tabela 43. Janela de parâmetros (regex) de Propriedades de Evento Customizado

Parâmetro	Descrição
Campo de teste	
Nova Propriedade	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`.
Otimizar análise para regras, relatórios e procuras	Analisa e armazena a propriedade na primeira vez em que o evento ou fluxo for recebido. Ao selecionar a caixa de seleção, a propriedade não necessitará de mais análise para relatar, procurar ou testar a regra. Se limpar essa caixa de seleção, a propriedade será analisada todas as vezes em que um teste de relatório, de pesquisa ou de regra for aplicado.
Origem de Log	Se várias fontes de log estiverem associadas a esse evento, esse campo especifica o termo Vários e o número de fontes de log.

Tabela 43. Janela de parâmetros (regex) de Propriedades de Evento Customizado (continuação)

Parâmetro	Descrição
RegEx	A expressão regular que 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 Flutuantes: `([-+]?\d*\.?\d*$)` • Número Inteiro: `([-+]?\d*$)` • Endereço IP: `(\b\d{1,3}\. \ \d{1,3}. \ \d{1,3}. \b \d{1,3})` Os grupos de captura devem estar entre parênteses.
Grupo de Captura	Os grupos de captura tratam vários caracteres como uma unidade única. Em um grupo de captura, os caracteres são agrupados dentro de um conjunto de parênteses.
Ativado	Se você limpar a caixa de seleção, essa propriedade customizada não será exibida em filtros de procura ou listas de coluna e a propriedade não será analisada a partir das cargas úteis.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Se você estiver visualizando eventos ou fluxos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Dê um clique duplo no evento ou fluxo na qual você deseja basear a propriedade customizada.
4. Dê um clique duplo no evento ao qual você deseja basear a propriedade customizada
5. Clique em **Extrair propriedade**.
6. Na área de janela **Seleção do Tipo de Propriedade**, selecione a opção **Baseado em Regex**.
7. Configure os parâmetros de 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 fluxos ou eventos, você deve selecionar a propriedade customizada na lista de colunas disponíveis ao criar uma pesquisa.

Conceitos relacionados:

"Exemplos de sequência de caracteres de procura AQL" na página 110
Use a Ariel Query Language (AQL) para recuperar campos específicos dos eventos, dos fluxos e das tabelas simarc no banco de dados do Ariel.

Criando uma propriedade customizada baseada em cálculo

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

Sobre Esta Tarefa

Ao configurar uma propriedade customizada baseada em cálculo, a janela Propriedade de Evento Customizado ou Propriedade de Fluxo Customizado fornece os parâmetros a seguir:

Tabela 44. Parâmetros de janela de definição de propriedade customizada (cálculo)

Parâmetro	Descrição
Definição de Propriedade	
Nome da Propriedade	Digite um nome exclusivo para essa propriedade customizada. O novo nome da propriedade não pode ser o nome de uma propriedade normalizada, como Nome do Usuário, IP de Origem ou de Destino.
Descrição	Digite uma descrição dessa propriedade customizada.
Definição de Cálculo da Propriedade	
Propriedade 1	Na caixa de listagem, selecione a primeira propriedade que você deseja usar em seu cálculo. As opções incluem todas as propriedades customizadas numéricas e normalizadas numéricas. Também é possível especificar um valor numérico específico. Na caixa de listagem **Propriedade 1**, selecione a opção **Definido pelo usuário**. O parâmetro **Numeric Property** é exibido. Digite um valor numérico específico.
Operador	Na caixa de listagem, selecione o operador que você deseja aplicar para as propriedades selecionadas no cálculo. As opções incluem: • Incluir • Subtrair • Multiplicar • Dividir
Propriedade 2	Na caixa de listagem, selecione a segunda propriedade que você deseja usar em seu cálculo. As opções incluem todas as propriedades customizadas numéricas e normalizadas numéricas. Também é possível especificar um valor numérico específico. Na caixa de listagem **Propriedade 1**, selecione a opção **Definido pelo usuário**. O parâmetro **Numeric Property** é exibido. Digite um valor numérico específico.
Ativado	Selecione esta caixa de seleção para ativar essa propriedade customizada. Se você desmarcar a caixa de seleção, essa propriedade customizada não será exibida em 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 eventos ou fluxos no modo de fluxo, clique no ícone **Pausar** para pausar o fluxo.
3. Clique duas vezes no evento ou fluxo no qual que você deseja basear a propriedade customizada.
4. Clique em **Extrair propriedade**.
5. Na área de janela Seleção de Tipo de Propriedade, selecione a opção **Baseado em cálculo**.
6. Configure os parâmetros de 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 deve selecionar a propriedade customizada da lista de colunas disponíveis ao criar uma procura.

Modificando uma propriedade customizada

É possível modificar uma propriedade customizada.

Sobre Esta Tarefa

É possível 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 45. Colunas da janela de propriedades customizadas

Coluna	Descrição
Nome da Propriedade	Especifica um nome exclusivo para essa propriedade customizada.
Tipo	Especifica o tipo para essa propriedade customizada.
Descrição da Propriedade	Especifica uma descrição para essa propriedade customizada.
Tipo de Fonte de Log	Especifica o nome do tipo de origem 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 a 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 de propriedade customizada: Para uma propriedade customizada baseada em regex, esse parâmetro especifica a expressão regular que você deseja usar para extrair os dados da carga útil. Para 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.

As barras de ferramentas Propriedade de Evento Customizado e Propriedade de Fluxo Customizado fornecem as funções a seguir:

Tabela 46. 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.

Tabela 46. Opções da barra de ferramentas da propriedade customizada (continuação)

Opção	Descrição
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 dos 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 você deseja editar e clique em **Editar**.
5. Editar os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testar a expressão regular com relação à carga útil.
7. Clique em **Salvar**.

Copiando uma propriedade customizada

Para criar uma nova propriedade customizada baseada em uma propriedade customizada existente, você 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. Editar os parâmetros necessários.
6. Opcional. Se você editou a expressão regular, clique em **Testar** para testar a expressão regular com relação à carga útil.
7. Clique em **Salvar**.

Excluindo uma propriedade customizada

É possível 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 deseja excluir e clique em **Excluir**.
6. Clique em **Sim**.

Capítulo 11. 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 de log, deve-se ter **Atividade de log** > **Manter regra customizada**.

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

Visão geral de regras

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

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

Categorias de regra

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

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 regras

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

Regra de evento

Uma regra de evento executa testes em eventos conforme eles são processados em tempo real pelo Processador de eventos. É possível criar uma regra de evento para detectar um único evento (dentro de determinadas propriedades) ou sequências de eventos. Por exemplo, se desejar monitorar tentativas de login malsucedidas, acessovários hosts ou um evento de reconhecimento seguido por uma exploração em sua rede, você poderá criar uma regra de evento. É comum para regras de evento criar ofensas como uma resposta.

Regra de fluxo

Um fluxo de regra executa testes em fluxos à medida que são processados em tempo real pelo Coletor QFlow. É possível 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 testa campos que são comuns a ambos os registros de eventos e 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 criarem 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 planejou a reavaliação por ofensa. É comum para regras de ofensa enviarem uma notificação por email como resposta.

Condições da regra

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

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

Um bloco de construção é uma regra sem uma resposta e é usado como uma variável comum em várias regras ou para construir regras complexas ou lógicas que deseja usar em outras regras. É possível salvar um grupo de testes como blocos de construção para uso com outras funções. Blocos de construção permitirão que reutilize testes de uma regra específica em outras regras. Por exemplo, é possível salvar um bloco de construção que inclui os endereços IP de todos os servidores de correio em sua rede e, em seguida, usar esse bloco de construção para excluir os servidores de correio 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.

Nota: Os blocos de construção não são carregados por padrão. Defina uma regra para construir blocos de construção.

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

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

Respostas da regra

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

As regras podem gerar uma ou mais das seguintes respostas:

- Crie uma ofensa.
- Envie um email.
- Gere notificações do sistema no recurso do Painel.
- Incluir 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 coleção 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). O QRadar suporta os seguintes tipos de coleta de dados:

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

Mapa de referência
Os dados são armazenados em registros de que mapeiam uma tecla para um valor. Por exemplo, para correlacionar a atividade do usuário em sua rede, 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 de que mapeiam uma tecla para vários valores. Por exemplo, para testar o acesso autorizado a uma patente, use uma propriedade de evento customizada para **Patent ID** como a chave e o parâmetro **Username** como o valor. Use um mapa de 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, que é, então, mapeada para valor único. A segunda chave tem um tipo designado. Esse mapeamento é semelhante a uma tabela de banco de dados em que cada coluna da tabela é associada a um tipo. Por exemplo, é possível criar uma tabela de referência que armazena o parâmetro **Username** como a primeira chave, e possui várias chaves secundárias que possuem um tipo designado pelo usuário como **Tipo IP** com o parâmetro **Source IP** ou **Source Port** como um valor. É possível configurar uma resposta da regra para incluir uma ou mais chaves definidas na tabela. É possível também incluir valores customizados à resposta da regra. O valor customizado deve ser válido para o tipo de chave secundária.

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

Visualizando regras

É possível visualizar os detalhes de uma regra, incluindo os testes, blocos de construção e respostas.

Antes de Iniciar

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

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

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 Grupo ou o campo **Regras da procura** 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 você 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. É possível revisar e editar detalhes da regra.

Criando uma regra customizada

É possível 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**.

É possível testar regras localmente ou globalmente. Um teste local significa que a regra é testada no processador de eventos local e não compartilhada com o sistema. Um teste global significa que a regra é compartilhada e testada por 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 Teste de Regra.
6. No campo **Inserir o nome da regra aqui** na área de janela Regra, insira um nome exclusivo que você deseja designar a essa regra.
7. Na caixa de listagem, selecione **Local** ou **Global**.
8. Incluir um ou mais testes em uma regra:

a. Opcional. Para filtrar as opções na caixa de listagem **Grupo de teste**, insira o texto que você deseja filtrar no campo Tipo a ser filtrado.
b. Na caixa de listagem **Grupo de teste**, selecione o tipo de teste que você deseja incluir nessa regra.
c. Para cada teste que você deseja incluir na regra, selecione o sinal de mais (+) ao lado do teste.
d. Opcional. Para identificar um teste como teste excluído, clique em **e** no início do teste na área de janela Regra. O **e** é exibido como **e não**.
e. Clique nos parâmetros configuráveis sublinhados para customizar as variáveis do teste.
f. Na caixa de diálogo, selecione os valores para a variável e, em seguida, clique em **Enviar**.

9. Para exportar a regra configurada como um bloco de construção para o uso com outras regras:
   a. Clique em **Exportar como blocos de construção**.
   b. Insira um nome exclusivo para esse bloco de construção.
   c. Clique em **Salvar**.
10. Na área de janela Grupos, 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 Comuns, consulte Tabela 49 na página 152
    - Para configurar as respostas para uma Regra de Ofensa, consulte Tabela 50 na página 155
13. Clique em **Avançar**.
14. Revise a página Resumo de regra para assegurar-se de que as configurações estejam corretas. Faça as alterações, se necessário, e, em seguida, clique em **Concluir**.

Criando uma regra de detecção de anomalia

Use o assistente Regra de Detecção de 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 anomalia serão exibidas após executar uma procura agrupada e salvar os critérios de procura.

Sobre Esta Tarefa

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

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

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

Ao criar uma regra de detecção de anomalias, a regra será preenchida com uma pilha de teste padrão. É possível editar os testes padrão ou incluir 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 Teste de Regra.

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

Essa opção **Testar o valor [Selected Accumulated Property] de cada [group] separadamente** é dinâmica. O valor **[Selected Accumulated Property]** depende de qual opção foi selecionada no campo **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 Teste 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, insira o texto que você deseja filtrar no campo Tipo a ser filtrado.
   b. Na caixa de listagem Grupo de Teste, selecione o tipo de teste que deseja incluir nessa regra.
   c. Para cada teste que você deseja incluir na regra, selecione o sinal + ao lado do teste.

d. Opcional. Para identificar um teste como teste excluído, clique 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 Gerenciamento de grupo de regra.
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 Resposta de regra" na página 152
12. Clique em **Avançar**.
13. Revise a regra configurada. Clique em **Concluir**.

Tarefas de gerenciamento de regra

É possível gerenciar regras customizadas e de anomalia.

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

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

Para gerenciar 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 o sistema irá gerar ofensas significativas para seu ambiente.

Sobre Esta Tarefa

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

Procedimento

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

Editando uma regra

É possível editar uma regra para alterar o nome da regra, tipo de regra, testes ou respostas.

Sobre Esta Tarefa

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

Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na caixa de listagem **Exibir** na página **Regras**, selecione **Regras**.
4. Dê um clique duplo na regra que você deseja editar.
5. Na caixa de listagem **Ações**, selecione **Abrir**.
6. Opcional. Se você desejar alterar o tipo de regra, clique em **Voltar** e selecione um novo tipo de regra.
7. Na página Editor de pilha de 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 deve ter a permissão de função **Ofensas** > **Manter regras customizadas** para poder ativar ou desativar uma regra.

Procedimento

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

Excluindo uma regra

É possível excluir uma regra de seu sistema.

Sobre Esta Tarefa

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

Procedimento

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

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

Gerenciamento de grupo de regras

Se você for um administrador, estará apto a criar, editar e excluir grupos de regras. Categorizar suas regras ou blocos de construção em grupos permite 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 novas regras são criadas, é possível designar a regra para um grupo existente. Para obter informações sobre como designar um grupo usando o assistente de regra, consulte Criando 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 se você deseja visualizar 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 os 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 no qual você deseja criar um novo grupo.
5. Clique em **Novo grupo**.
6. Insira os valores para os parâmetros a seguir:
   - **Nome** – digite um nome exclusivo para ser designado ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
   - **Descrição** – insira uma descrição que você deseje designar a esse grupo. A descrição pode ter até 255 caracteres de comprimento.
7. Clique em **OK**.
8. Opcional. Para alterar o local do novo grupo, clique no novo grupo e arraste a pasta para o novo local em sua árvore de navegação.

Designando um item a um grupo

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

Procedimento

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

Editando um grupo

É possível 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** – digite um nome exclusivo para ser designado ao novo grupo. O nome pode ter até 255 caracteres de comprimento.
   - **Descrição** – insira uma descrição que você deseje 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

É possível copiar um bloco de regra ou construção de um grupo para outros grupos.

Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Clique em **Grupos**.
4. Na árvore de navegação, selecione o bloco de regra ou construção que deseja copiar para outro grupo.
5. Clique em **Copiar**.
6. Selecione a caixa de seleção para o grupo 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. Quando você excluir um item de um grupo, a regra ou bloco de construção é apenas excluído do grupo; ele permanece 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 e selecione o item que deseja excluir.
5. Clique em **Remover**.
6. Clique em **OK**.

Excluindo um grupo

É possível 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, selecione e navegue até o grupo que você deseja excluir.
5. Clique em **Remover**.
6. Clique em **OK**.

Editando blocos de construção

É possível editar qualquer um dos blocos de construção padrão para corresponder com as 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 o bloco de construção que você deseja editar.
5. Atualize o bloco de construção, conforme necessário.
6. Clique em **Avançar**.
7. Continue pelo assistente. Para obter mais informações, consulte Criando uma regra customizada.
8. Clique em **Concluir**.

Parâmetros de página Regra

Uma descrição dos parâmetros na página Regras.

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

Tabela 47. Parâmetros da página Regras

Parâmetro	Descrição
Nome da Regra	Exibe o nome da regra.
Grupo	Exibe o grupo ao qual esta regra é designada. Para obter mais informações sobre grupos, consulte Gerenciamento de regras de grupo.
Rule Category	Exibe a categoria de regra para a regra. As opções incluem Regra customizada e Regra de detecção de anomalias.
Tipo de Regras	Exibe o tipo de regra. Os tipos de regra incluem: • Evento • Fluxo • Comum • Ofensa • Anomalia • Limite • Comportamental Para obter mais informações sobre os tipos de regra, 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. Respostas de regra incluem: • Enviar Novo Evento • Email • Notificação de log • SNMP • Conjunto de referência • Dados de referência • Resposta 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 que serão associados a esta regra quando a regra contribuir para uma ofensa.
Offense Count	Exibe o número de ofensas que são gerados 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 que essa regra foi criada.
Data da Modificação	Especifica a data e hora que essa regra foi modificada.

Barra de ferramentas da página Regras

A barra de ferramentas da página Regras é usada exibir as regras, blocos de construção ou grupos. É possível gerenciar grupos de regras e trabalhar com regras.

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

Tabela 48. Função da barra de ferramentas da página Regras

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

Tabela 48. Função da barra de ferramentas da página 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 modificada 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, duplique a regra e use a opção **Reverter regra** na regra modificada.
Procurar regras	Digite seus critérios de procura no campo **Procurar regras** e clique no ícone **Procurar regras** ou pressione Enter no teclado. Todas as regras que correspondem aos seus critérios de procura serão exibidas na lista de regras. Procura-se, nos parâmetros a seguir, uma correspondência com seus critérios de procura: • Nome da Regra • Rule (description) • Comunicados • Response O recurso Procurar regra tenta localizar uma correspondência da sequência de texto direta. Se nenhuma correspondência for encontrada, o recurso Procurar regra tentará uma correspondência de expressão regular (regex).

Parâmetros da página Resposta de regra

Há parâmetros para a página Resposta de regra.

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

Tabela 49. Parâmetros de página Resposta de regra comum, de fluxo e de evento

Parâmetro	Descrição
Gravidade	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a severidade. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de severidade apropriado.
Credibilidade	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste credibilidade. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de credibilidade apropriado.
Relevância	Selecione esta caixa de seleção se quiser que essa regra configure ou ajuste a relevância. Quando selecionada, será possível usar as caixas de listagem para configurar o nível de relevância apropriado.

Tabela 49. Parâmetros de página Resposta de regra comum, de fluxo e de evento (continuação)

Parâmetro	Descrição
Ensure that the detected event is part of an offense	Selecione essa caixa de seleção se 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 na ofensa. Ao selecionar essa caixa de seleção, as seguintes opções serão exibidas: **Ofensa do índice com base em** Na caixa de listagem, selecione o parâmetro no qual desejar indexar a ofensa. O padrão é IPv6 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, fonte 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 o 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 de IP de destino, porta de destino, regra, IP de origem, identidade de IP de origem e porta de origem. **Annotate this offense** Selecione esta caixa de seleção para incluir uma anotação a esta ofensa e digite a anotação. **Incluir eventos detectados por <índice> desse ponto em diante, por segundo(s), na ofensa** Selecione esta caixa de seleção e digite o número de segundos que deseja incluir eventos detectados por <índice> na guia **Ofensas**. Este campo especifica o parâmetro no qual a ofensa foi indexada. O padrão é IP de origem.
Annotate event	Selecione essa caixa de seleção se desejar incluir uma anotação a este evento e digite a anotação que deseja incluir no evento.
Drop the detected event	Selecione esta caixa de seleção para forçar um evento, que normalmente é enviado para o componente Magistrate, a ser enviado para o banco de dados Ariel, para geração de relatórios ou pesquisa. Este evento não é exibido na guia **Ofensas**.
Enviar Novo Evento	Selecione essa caixa de seleção para enviar um novo evento além do fluxo ou evento original, que é processado como todos os outros eventos no sistema. Selecione essa caixa de seleção para enviar um novo evento além do evento original, que é processado como todos os outros eventos no sistema. Os parâmetros **Dispatch New Event** serão exibidos ao selecionar esta caixa de seleção. Por padrão, a caixa de seleção não é selecionada.
Nome do evento	Digite um nome exclusivo para o evento que deseja que seja exibido na guia **Ofensas**.
Descrição do Evento	Digite uma descrição do evento. A descrição é exibida na área de janela Anotações dos detalhes do evento.
Gravidade	Na caixa de listagem, selecione a severidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 0. A severidade é exibida na área de janela Anotação dos detalhes do evento.
Credibilidade	Na caixa de listagem, selecione a credibilidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 10. A credibilidade é exibida na área de janela Anotação dos detalhes do evento.
Relevância	Na caixa de listagem, selecione a relevância do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 10. A relevância é exibida na área de janela Anotação dos detalhes do evento.
High-Level Category	Na caixa de listagem, selecione a categoria de evento de alto nível que deseja que esta regra use ao processar eventos.
Low-Level Category	Na caixa de listagem, selecione a categoria de evento de baixo nível que deseja que esta regra use ao processar eventos.
Annotate this offense	Selecione esta caixa de seleção para incluir uma anotação a esta ofensa e digite a anotação.

Tabela 49. Parâmetros de página Resposta de regra comum, de fluxo e de evento (continuação)

Parâmetro	Descrição
Ensure that the dispatched event is part of an offense	Selecione essa caixa de seleção se desejar, como resultado dessa regra, o evento que será encaminhado para o componente Magistrate. Se nenhuma ofensa for criada na guia **Ofensas**, uma nova ofensa será criada. Se uma ofensa existir, esse evento será incluído. Ao selecionar essa caixa de seleção, as seguintes opções serão exibidas: **Ofensa do índice com base em** Na caixa de listagem, selecione o parâmetro no qual 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, fonte 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 o 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 de IP de destino, porta de destino, regra, IP de origem, identidade de IP de origem e porta de origem. **Incluir eventos detectados por <índice> desse ponto em diante, por segundo(s), na ofensa** Selecione esta caixa de seleção e digite o número de segundos que deseja incluir eventos detectados por <índice> na guia **Ofensas**. Este campo especifica o parâmetro no qual a ofensa foi indexada. O padrão é IP de origem. **Nomenclatura de Ofensas** Selecione uma das opções a seguir: **Estas informações devem contribuir para o nome da(s) ofensa(s) associada(s)** Selecione esta opção se desejar que as informações de Nome de evento contribuam para o nome da ofensa. **Estas informações devem configurar ou substituir o nome da(s) ofensa(s) associada(s)** Selecione esta opção se desejar que o Nome do evento configurado seja o nome da ofensa. **Estas informações não devem contribuir para a nomenclatura da(s) ofensa(s) associada(s)** 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. **Nota:** Para alterar a configuração **Código de idioma do email**, selecione **Configurações do sistema** na guia **Administrador**.
Insira o endereço de email a ser notificado	Digite o endereço de email para enviar uma notificação se esta regra for gerada. Use uma vírgula para separar vários endereços de email.
SNMP Trap	Esse parâmetro só será exibido quando os parâmetros SNMP Settings forem definidos nas configurações do sistema. Selecione esta caixa de seleção para ativar que esta regra envie uma notificação SNMP (trap). A saída de trap SNMP inclui o tempo do sistema, o OID de trap e os dados de notificação, conforme definidos pelo MIB.
Enviar para syslog local	Selecione essa caixa de seleção se desejar registrar o evento ou fluxo localmente. Por padrão, essa caixa de seleção está limpa. **Nota:** Apenas os eventos normalizados podem ser registrados localmente em um dispositivo. Se desejar enviar dados do evento brutos, 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 será exibida apenas para regras de eventos. Selecione essa caixa de seleção se desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema fornecedor, como SIEM, chamado ou sistemas de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento será exibida. Selecione a caixa de seleção para o destino de encaminhamento para o qual deseja enviar este evento ou fluxo. Para incluir, editar ou excluir um destino de encaminhamento, clique no link **Gerenciar destinos**.

Tabela 49. Parâmetros de página Resposta de regra comum, de fluxo e de evento (continuação)

Parâmetro	Descrição
Notify	Selecione essa caixa de seleção se desejar que os eventos que são gerados como resultado desta regra sejam exibidos no item Notificações do sistema na guia Painel. Se ativar notificações, configure o parâmetro **Response Limiter**.
Add to Reference Set	Selecione essa caixa de seleção se desejar que eventos que são gerados como resultado desta regra incluam dados em um conjunto de referência. Para incluir dados em um conjunto de referência: 1. Usando a caixa de listagem pela primeira vez, selecione os dados que deseja incluir. As opções incluem todos os dados normalizados ou customizados. 2. Usando a segunda caixa de listagem, selecione a referência que está configurada para a 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-se de 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 tiver permissões administrativas.
Incluir de Dados de Referência	Antes de poder usar essa resposta de regra, você deverá 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* do seu produto. Selecione essa caixa de seleção se desejar que eventos que são gerados como resultado dessa regra sejam incluídos em uma coleta de dados de referência. Após selecionar a caixa de seleção, selecione uma das seguintes opções: **Incluir em um Mapa de Referência** Selecione esta opção para enviar dados para uma coleção de pares de chave única/valor múltiplo. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência no qual deseja incluir o registro de dados. **Incluir em um Mapa de Referência de Conjuntos** Selecione esta opção para enviar dados para uma coleção de pares de chave/valor único. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência de conjuntos no qual deseja incluir o registro de dados. **Incluir em um Mapa de Referência de Mapas** Selecione esta opção para enviar dados para uma coleção de pares de chave múltipla/valor único. É necessário selecionar uma chave para o primeiro mapa, uma chave para o segundo mapa e, em seguida, o valor para o registro de dados. Deve-se também selecionar o mapa de referência de mapas nos quais deseja incluir o registro de dados. **Incluir em uma Tabela de Referência** Selecione esta opção para enviar dados para uma coleção de pares de chave única/valor múltiplo, onde um tipo foi designado para as chaves secundárias. Selecione a tabela de referência para a qual deseja incluir dados e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.
Publish on the IF-MAP Server	Se os parâmetros IF-MAP estiverem configurados e implementados nas configurações do sistema, selecione esta opção para publicar as informações de evento do servidor IF-MAP.
Limitador de Resposta	Selecione esta caixa de seleção e use as caixas de listagem para configurar a frequência com a qual deseja que esta regra responda.
Enable Rule	Selecione esta caixa de seleção para ativar esta regra.

A tabela a seguir fornece os parâmetros da página Resposta de regra, caso o tipo de regra seja Ofensa.

Tabela 50. Parâmetros de página Resposta da regra de ofensa

Parâmetro	Descrição
Name/Annotate the detected offense	Selecione essa caixa de seleção para exibir as opções de nome.
New Offense Name	Digite o nome que deseja designar à ofensa.
Offense Annotation	Digite a anotação de ofensa que deseja que seja exibida na guia Ofensas.

Tabela 50. Parâmetros de página Resposta da regra de ofensa (continuação)

Parâmetro	Descrição
Offense Name	Selecione uma das opções a seguir: **Estas informações devem contribuir para o nome da ofensa** Selecione esta opção se 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 desejar que o Nome do evento configurado seja o nome da ofensa.
Email	Selecione essa caixa de seleção para exibir as opções de email. **Nota:** Para alterar a configuração **Código de idioma do email**, selecione **Configurações do sistema** na guia **Administrador**.
Enter email address to notify	Digite o endereço de email para enviar a notificação se o evento for gerado. Use uma vírgula para separar vários endereços de email.
SNMP Trap	Esse parâmetro só será exibido quando os parâmetros SNMP Settings forem definidos nas configurações do sistema. Selecione esta caixa de seleção para ativar que esta regra envie uma notificação SNMP (trap). Para uma regra de ofensa, a saída do trap SNMP inclui o tempo do sistema, o OID do trap, e os dados de notificação, conforme definido pelo MIB.
Enviar para syslog local	Selecione essa caixa de seleção se desejar registrar o evento ou fluxo localmente.
Enviar para Destinos de Encaminhamento	Selecione essa caixa de seleção se desejar registrar o evento ou fluxo em um destino de encaminhamento. Um destino de encaminhamento é um sistema fornecedor, como SIEM, chamado ou sistemas de alerta. Ao selecionar essa caixa de seleção, uma lista de destinos de encaminhamento será exibida. Selecione a caixa de seleção para o destino de encaminhamento para o qual deseja enviar este evento ou fluxo. Para incluir, editar ou excluir um destino de encaminhamento, clique no link **Gerenciar destinos**.
Publish on the 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 deseja que esta regra responda.
Enable Rule	Selecione esta caixa de seleção para ativar esta regra. Por padrão, a caixa de seleção é selecionada.

A tabela a seguir fornece os parâmetros da página Resposta de regra, se o tipo de regra for Anomalia.

Tabela 51. Parâmetros de página Resposta de regra de detecção de anomalias

Parâmetro	Descrição
Enviar Novo Evento	Especifica que esta regra envia um novo evento além do evento ou fluxo 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 deseja que seja exibido na guia Ofensas.
Descrição do Evento	Digite uma descrição do 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(s) ofensa(s) associada(s)** Selecione esta opção se desejar que as informações de Nome de evento contribuam para o nome da ofensa. **Estas informações devem configurar ou substituir o nome da(s) ofensa(s) associada(s)** Selecione esta opção se desejar que o Nome do evento configurado seja o nome da ofensa. **Estas informações não devem contribuir para a nomenclatura da(s) ofensa(s) associada(s)** Selecione esta opção se não desejar que as informações de Nome de evento contribuam para o nome da ofensa.
Severity Usando as caixas de listagem, selecione a severidade do evento.	O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A severidade é exibida na área de janela Anotações dos detalhes do evento.
Credibilidade	Usando as caixas de listagem, selecione a credibilidade do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A credibilidade é exibida na área de janela Anotações dos detalhes do evento.
Relevância	Usando as caixas de listagem, selecione a relevância do evento. O intervalo é de 0 (mais baixo) a 10 (mais alto) e o padrão é 5. A relevância é exibida na área de janela Anotações dos detalhes do evento.
Categoria de Alto Nível	Na caixa de listagem, selecione a categoria de evento de alto nível que deseja que esta regra use ao processar eventos.
Categoria de Baixo Nível	Na caixa de listagem, selecione a categoria de evento de baixo nível que deseja que esta regra use ao processar eventos.

Tabela 51. Parâmetros de página Resposta de regra de detecção de anomalias (continuação)

Parâmetro	Descrição
Annotate this offense	Selecione esta caixa de seleção para incluir uma anotação a esta ofensa e digite a anotação.
Ensure that the dispatched event is part of an offense	Como resultado dessa regra, o evento é encaminhado para o componente Magistrate. Se uma ofensa existir, esse evento será incluído. Se nenhuma ofensa for criada na guia Ofensas, uma nova ofensa será 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. **Inclui eventos detectados por Nome do evento a partir desse ponto, por segundo(s), na ofensa** Selecione esta caixa de seleção digite o número de segundos que deseja para incluir eventos ou fluxos detectados a partir da origem na guia **Ofensas**.
Email	Selecione essa caixa de seleção para exibir as opções de email. **Nota:** Para alterar a configuração **Código de idioma do email**, selecione **Configurações do sistema** na guia **Administrador**.
Enter email address to notify	Digite o endereço de email para enviar uma notificação se esta regra for gerada. Use uma vírgula para separar vários endereços de email.
Enter email address to notify	Digite o endereço de email para enviar uma notificação se esta regra for gerada. Use uma vírgula para separar vários endereços de email.
Notify	Selecione essa caixa de seleção se desejar que os eventos que são gerados como resultado desta regra sejam exibidos no item Notificações do sistema na guia **Painel**. Se ativar notificações, configure o parâmetro **Response Limiter**.
Enviar para syslog local	Selecione essa caixa de seleção se 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 desejar enviar dados do evento brutos, deverá usar a opção Enviar para destinos de encaminhamento para enviar os dados para um host syslog remoto.
Add to Reference Set	Selecione essa caixa de seleção se desejar que eventos que são gerados como resultado desta regra incluam dados em um conjunto de referência. Para incluir dados em um conjunto de referência: 1. Usando a caixa de listagem pela primeira vez, selecione os dados que 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 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-se de 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 tiver permissões administrativas.

Tabela 51. Parâmetros de página Resposta de regra de detecção de anomalias (continuação)

Parâmetro	Descrição
Incluir de Dados de Referência	Antes de poder usar essa resposta de regra, você deverá 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* do seu produto. Selecione essa caixa de seleção se desejar que eventos que são gerados como resultado dessa regra sejam incluídos em uma coleta de dados de referência. Após selecionar a caixa de seleção, selecione uma das seguintes opções: **Incluir em um Mapa de Referência** Selecione esta opção para enviar dados para uma coleção de pares de chave única/valor múltiplo. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência no qual deseja incluir o registro de dados. **Incluir em um Mapa de Referência de Conjuntos** Selecione esta opção para enviar dados para uma coleção de pares de chave/valor único. Deve-se selecionar a chave e o valor do registro de dados e, em seguida, selecionar o mapa de referência de conjuntos no qual deseja incluir o registro de dados. **Incluir em um Mapa de Referência de Mapas** Selecione esta opção para enviar dados para uma coleção de pares de chave múltipla/valor único. É necessário selecionar uma chave para o primeiro mapa, uma chave para o segundo mapa e, em seguida, o valor para o registro de dados. Deve-se também selecionar o mapa de referência de mapas nos quais deseja incluir o registro de dados. **Incluir em uma Tabela de Referência** Selecione esta opção para enviar dados para uma coleção de pares de chave única/valor múltiplo, onde um tipo foi designado para as chaves secundárias. Selecione a tabela de referência para a qual deseja incluir dados e, em seguida, selecione uma chave primária. Selecione suas chaves internas (chaves secundárias) e seus valores para os registros de dados.
Publish on the 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 a qual deseja que esta regra responda
Enable Rule	Selecione esta caixa de seleção para ativar esta regra. Por padrão, a caixa de seleção é selecionada.

Uma notificação SNMP pode se parecer com:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

Uma saída de syslog pode se parecer com:

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

Capítulo 12. Correlação histórica

Use correlação histórica para executar eventos e fluxos decorridos através do mecanismo de regras customizadas (CRE) e analise dados com base no perfil histórico que você configurou.

Por padrão, uma implementação do IBM Security QRadar SIEM analisa informações que são coletadas a partir de fontes de log e fontes de fluxo quase em tempo real. Com correlação histórica, é possível correlacionar pelo horário de início ou pelo horário do dispositivo. *Horário de início* é o horário em que o evento foi recebido pelo QRadar. *Horário do dispositivo* é o horário em que o evento ocorreu no dispositivo.

A correlação histórica pode ser útil nas seguintes situações:

Analisando eventos históricos que foram carregados em massa
A sua implementação do QRadar pode ser configurada para carregar eventos em massa. Por exemplo, para evitar degradação de desempenho durante o horário comercial, os eventos podem ser carregados a partir de várias fontes de log todas as noites à meia-noite.

É possível usar correlação histórica para analisar esses dados de carregamento em massa e correlacionar os eventos por horário do dispositivo ou horário de início.

Teste de regra de uma vez
É possível executar correlação histórica para testar novas regras. Por exemplo, um de seus servidores foi atacado recentemente por um novo malware para o qual você não tem regras adequadas. É possível criar uma regra para testar para esse malware. Então, você pode utilizar correlação histórica para ver se a regra acionaria uma resposta se ela estivesse em vigor no momento do ataque. De forma semelhante, você pode utilizar correlação histórica para determinar quando o ataque ocorreu pela primeira vez ou a frequência do ataque.

Recriando ofensas que foram perdidas ou limpas
Se o seu sistema perdeu ofensas devido a uma indisponibilidade ou outro motivo, é possível recriar as ofensas executando correlação histórica em eventos que surgiram durante esse tempo.

Manipulação de regra

A correlação histórica coleta todos os eventos que são retornados pela procura salva e, em seguida, o console do QRadar os processa. Como o processamento de correlação histórica ocorre em um único local, as regras que são incluídas no perfil de correlação histórica são tratadas como regras globais. O processamento não altera a regra de local para global, mas manipula a regra como se fosse global durante a execução de correlação histórica.

Algumas regras, como regras stateful, podem não acionar a mesma resposta que fariam em uma correlação normal que é executada em um processador de evento local. Por exemplo, uma regra stateful local que rastreia cinco logins com falha em 5 minutos do mesmo nome de usuário se comporta de forma diferente em execuções de correlação normais e históricas. Em correlação normal, essa regra local mantém um contador para o número de logins com falha que são recebidos

por cada processador de evento local. Na correlação histórica, essa regra mantém um único contador para o sistema QRadar inteiro. Nessa situação, as ofensas podem ser criadas de maneira diferente em comparação a uma execução de correlação normal.

Considerações ao usar correlação histórica

Considere as seguintes informações ao usar correlação histórica:

- É possível configurar perfis históricos somente no IBM Security QRadar SIEM. Não é possível criar perfis históricos no IBM Security QRadar Log Manager.
- Eventos podem ser correlacionados por horário de início ou horário do dispositivo. Fluxos podem ser correlacionados somente por horário de início.
- Uma regra deve ser ativada antes que seja possível incluí-la em um perfil de correlação histórica.
- Respostas de regra, como geração de relatórios, notificações de mensagens ou outras opções de regra são ignoradas durante a correlação histórica.
- É possível usar somente procuras salvas não agregadas para correlação histórica. A procura salva não pode especificar um grupo por coluna.
- Um perfil de correlação histórica não será executado se qualquer das seguintes condições for verdadeira:
  - A procura salva especificada está excluída.
  - Todas as regras de perfis foram desativadas.
  - A procura salva do perfil não retornou nenhum evento ou fluxo que ocorreu dentro do prazo especificado.
- Não é possível construir relatórios sobre dados de correlação histórica diretamente do QRadar SIEM. Se você deseja usar programas de terceiro para construir relatórios, é possível exportar a partir do QRadar ou usar a API RESTful do QRadar.
- Recomenda-se que os usuários que criam perfis de correlação histórica tenham permissões para eventos e fluxos. Os usuários que não possuem permissões para eventos e fluxos não podem incluir regras comuns no perfil. As regras comuns são removidas automaticamente do perfil de correlação histórica, se o perfil for editado por um usuário que não possui permissões para eventos e fluxos.

Visualizando resultados da correlação histórica

Quando a correlação histórica é executada, eventos que atendem aos critérios de teste da regra criam uma ou mais ofensas. A correlação histórica não contribui com uma ofensa em tempo real e nem contribui com uma ofensa que foi criada a partir de uma execução de correlação histórica anterior, mesmo quando o mesmo perfil é usado.

É possível fazer drill down na ofensa para ver mais detalhes sobre a ofensa e os eventos e fluxos que a acionaram. Quando você faz drill down para visualizar informações sobre eventos, a coluna **Horário** na lista de eventos representa o horário de início do evento, que é o horário em que o QRadar recebeu o evento.

Ofensas de correlação histórica incluem conjuntos de dados de evento e de fluxo que correspondem aos critérios de correlação. Elas são preservadas e apresentadas como um resultado da procura dentro do visualizador de ofensa. Esses resultados de procura de dados historicamente correlacionados não podem ser procurados usando a funcionalidade **Procura avançada** ou **Filtro rápido**.

Um ícone de relógio identifica as ofensas de correlação no visualizador de ofensa.

Retenção de dados de correlação histórica

Cada correlação histórica que você executa cria um arquivo de banco de dados compactado no console QRadar. Os arquivos de banco de dados são removidos automaticamente depois de 15 dias. Se o arquivo de banco de dados for removido antes de você ter concluído isso, é possível executar novamente a correlação histórica com o mesmo perfil.

Criando um perfil de correlação histórica

Perfis de correlação histórica contêm os parâmetros de configuração que são usados para correlações históricas.

É possível configurar o perfil para limitar o período de tempo para dados que estiverem sendo analisados. Também é possível identificar regras específicas para testar e definir um planejamento para a execução da correlação histórica.

Procedimento

1. Abra a caixa de diálogo Correlação Histórica.
   - Na guia **Atividade de Log**, clique em **Ações** > **Correlação Histórica**.
   - Na guia **Atividade de Rede**, clique em **Ações** > **Correlação Histórica**.
   - Na guia **Ofensas**, clique em **Regras** > **Ações** > **Correlação Histórica**.
2. Clique em **Incluir** para configurar um perfil de correlação histórica.
3. Configure as definições de perfil.

   O perfil é colocado em uma fila para ser processado. Perfis enfileirados com base em um planejamento configurado têm prioridade sobre execuções manuais.
4. Clique em **Salvar**.
5. Após a correlação histórica ser executada, clique na guia **Ofensas** para verificar se há ofensas de correlação histórica, as quais são identificadas no visualizador de ofensa pelo ícone de relógio na coluna de sinalização.

Capítulo 13. Integração do feed do X-Force Threat Intelligence

O feed do IBM Security X-Force Threat Intelligence fornece uma lista em tempo real de endereços IP potencialmente maliciosos e URLs. Use esses endereços IP e URLs com IBM QRadar Security Intelligence Platform para identificar atividade suspeita em seu ambiente.

Você deve ter uma extensão de licença QRadar para usar o feed X-Force Threat Intelligence com QRadar.

O conteúdo no feed do X-Force recebe uma pontuação de ameaça relativa. Os usuários do QRadar podem usar essa pontuação de ameaça para priorizar incidentes e ofensas gerados por esse conteúdo. Os dados dessas fontes de inteligência são automaticamente incorporados nas funções de correlação e análise do QRadar e enriquecem suas capacidades de detecção de ameaça com os dados de ameaça da Internet mais recentes. Quaisquer dados de evento de segurança ou de atividade de rede que envolvam esses endereços são sinalizados automaticamente e, portanto, incluem um contexto importante para análises e investigações de incidente de segurança.

Para priorizar a ameaça e identificar os incidentes de segurança que requerem mais exame, é possível escolher os feeds do X-Force a serem incorporados nas regras, ofensas e eventos do QRadar. Por exemplo, é possível usar os feeds para identificar estes tipos de incidentes:

- Uma série de tentativas de logins para um intervalo dinâmico de endereços IP
- Uma conexão proxy anônima com um portal de parceiro de negócios
- Uma conexão entre um endpoint interno e um comando e um controle botnet conhecidos
- Comunicação entre um endpoint e um site de distribuição de malware conhecido

O feed do X-Force Threat Intelligence categoriza endereços IP e cria uma classificação de confiança que é usada para avaliar a ameaça. Os endereços IP são agrupados nas categorias a seguir:

- Hosts de malware
- Fontes SPAM
- Endereços IP dinâmicos
- Proxies anônimos
- Comando e controle botnet
- Varrendo endereços IP

O feed do X-Force Threat Intelligence também categoriza endereços de URL. Por exemplo, os endereços de URL podem ser categorizados como sites de encontro, aposta ou pornografia. Para ver a lista completa de categorias para a classificação de URL, consulte o website do X-Force (www.xforce-security.com).

Antes que você possa usar regras baseadas em URL, deve-se criar uma propriedade de evento customizado para extrair a URL da carga útil. A propriedade customizada da URL já está definida para eventos de várias fontes, como as fontes de log Blue Coat SG e Juniper Networks Secure Access.

Para obter mais informações sobre a criação de propriedades de evento customizado, consulte Propriedades de fluxo e de evento customizado.

Regras X-Force Threat Intelligence aprimoradas

Depois de incluir o feed no IBM Security X-Force Threat Intelligence, é possível receber os dados de ameaça avançados imediatamente.

As regras a seguir fazem parte do grupo **Regras do X-Force aprimoradas**. Elas podem ser usadas no estado em que se encontram ou é possível customizá-las.

Estas regras são baseadas em IP:

X-Force Premium: conexão interna com um possível host de malware
Essa comunicação indica uma forte possibilidade de que foi feita uma tentativa de infectar o sistema do cliente ou de que o malware foi transferido por download.

X-Force Premium: hosts internos que se comunicam com proxies anônimos
Proxies anônimos são endereços conhecidos por mascarar a identidade. Geralmente, eles são usados por malware ou durante ameaças persistentes avançadas para ocultar a origem das comunicações com fontes externas. Esses endereços podem estar relacionados a atividades, como comunicação de malware ou exfiltração de dados.

X-Force Premium: servidor de correio interno que envia email ao possível host SPAM
Geralmente, os servidores de correio que se comunicam com hosts SPAM são usados incorretamente.

X-Force Premium: servidores que não são de correio que se comunicam com hosts de envio de SPAM conhecidos
Esse comportamento é um forte indicador de que o servidor foi comprometido e que está sendo usado como uma retransmissão de spam.

X-Force Premium: não servidores que se comunicam com IP dinâmico externo
Os endereços IP designados dinamicamente geralmente não são associados a servidores legítimos na Internet. Estações de trabalho internas que se comunicam com endereços dinâmicos podem indicar atividade interna suspeita ou atividade de malware ou de botnet.

X-Force Premium: o servidor iniciou uma conexão com hosts dinâmicos
Geralmente, os servidores se comunicam com hosts que possuem uma identidade fixa e não endereços IP dinâmicos.

Como a URL é um indicador mais específico dos dados transferidos, as regras baseadas em URL podem ser mais precisas do que as regras baseadas em IP.

Estas regras são baseadas em URL:

X-Force Premium: host interno que se comunica com a URL de comando e controle botnet
Às vezes, servidores legítimos podem ser usados para fornecer conectividade botnet em endereços de URL específicos.

X-Force Premium: comunicação do host interno com a URL de malware
Às vezes, servidores legítimos podem ser usados para entregar malware em endereços de URL específicos.

Exemplo: criando uma regra usando a categorização de URL para monitorar o acesso a certos tipos de websites

É possível criar uma regra que enviará uma notificação por email se os usuários da rede interna acessarem endereços de URL categorizados como websites de aposta.

Antes de Iniciar

Para usar as regras de categorização de URL, deve-se possuir uma assinatura para o feed do X-Force Threat Intelligence.

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

Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Regras**.
3. Na lista **Ações**, selecione **Nova regra de evento**.
4. Leia o texto introdutório no assistente Regra e clique em **Avançar**.
5. Clique em **Eventos** e em **Avançar**.
6. Na caixa de listagem **Grupo de teste**, selecione **Testes do X-Force**.
7. Clique no sinal de mais (+) ao lado do teste **quando esta propriedade de URL for categorizada pelo X-Force como uma das categorias a seguir**.
8. No campo **Inserir o nome da regra aqui** na área de janela Regra, insira um nome exclusivo que você deseja designar a essa regra.
9. Na caixa de listagem, selecione **Local** ou **Global**.
10. Clique nos parâmetros configuráveis sublinhados para customizar as variáveis do teste.
    a. Clique em **URL (customizada)**.
    b. Selecione a propriedade de URL que contém a URL extraída da carga útil e clique em **Enviar**.
    c. Clique em **uma das categorias a seguir**.
    d. Selecione **Aposta/Loteria** nas categorias de URL do X-Force, clique em **Incluir +** e clique em **Enviar**.
11. Para exportar a regra configurada como um bloco de construção para o uso com outras regras:
    a. Clique em **Exportar como blocos de construção**.
    b. Insira um nome exclusivo para esse bloco de construção.
    c. Clique em **Salvar**.
12. Na área de janela Grupos, marque as caixas de seleção dos grupos aos quais você deseja designar essa regra.
13. No campo **Notas**, insira uma nota que você deseja incluir para essa regra e clique em **Avançar**.
14. Na página Respostas de regra, clique em **Email** e digite os endereços de email que recebem a notificação. Para obter informações sobre outros parâmetros de resposta para uma regra de evento, consulte Parâmetros da página de evento, fluxo e resposta de regra comum.
15. Clique em **Avançar**.
16. Se a regra for precisa, clique em **Concluir**.

Consultando endereço IP e informações de URL no X-Force Exchange

Use as opções de menu ativado pelo botão direito em IBM Security QRadar para consultar informações encontradas no IBM Security X-Force Exchange sobre endereços IP e URLs. É possível usar as informações de suas procuras, ofensas e regras do QRadar para pesquisar melhor e para incluir informações sobre endereços IP ou URLs em uma coleção X-Force Exchange.

Sobre Esta Tarefa

É possível contribuir com as informações públicas ou privadas para rastrear os dados nas coleções ao pesquisar por problemas de segurança.

Uma *coleção* é um repositório no qual você armazena as informações localizadas durante uma investigação. É possível usar uma coleção para salvar relatórios X-Force Exchange, comentários ou qualquer outro conteúdo. Um relatório X-Force Exchange contém uma versão do relatório para o momento em que foi salvo e um link para a versão atual do relatório. A coleção também contém uma seção (linha de tempo) que possui um notepad em estilo wiki no qual você poderá incluir comentários relevantes para a coleção.

Para obter informações adicionais sobre o X-Force Exchange, consulte X-Force Exchange (https://exchange.xforce.ibmcloud.com/).

Procedimento

1. Para consultar um endereço IP no X-Force Exchange a partir de QRadar, siga estas etapas:
   a. Selecione a guia **Atividade de log** ou **Atividade de rede**.
   b. Clique com o botão direito no endereço IP que deseja visualizar em X-Force Exchange e selecione **Mais opções** > **Opções de plug-in** > **Consulta X-Force Exchange** para abrir a interface X-Force Exchange.
2. Para consultar uma URL no X-Force Exchange a partir de QRadar, siga estas etapas:
   a. Selecione a guia **Ofensas** ou as janelas de detalhes de evento disponíveis em **Ofensas**.
   b. Clique com o botão direito na URL que você deseja consultar em X-Force Exchange e selecione **Opções de plug-in > Consulta X-Force Exchange** para abrir a interface X-Force Exchange.

Capítulo 14. Parâmetros da página Perfil de ativo

É possível localizar as descrições de parâmetro da página Perfil de ativo para a área de janela Resumo de ativo, Interface de rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de risco e Produtos.

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

Perfis de ativos

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

A informação do perfil de ativos é usada para propósitos de correlação para ajudar a reduzir positivos falsos. Por exemplo, se uma origem tentar explorar um serviço específico em execução em um ativo, o QRadar determinará se o ativo está vulnerável a este ataque correlacionando o ataque ao perfil de ativo.

Perfis de ativos são descobertos automaticamente se você tiver varreduras de dados de fluxo ou de avaliação de vulnerabilidades (VA) configuradas. Para transmitir dados para preencher perfis de ativos, fluxos bidirecionais são necessários. Perfis de ativos também podem ser criados automaticamente a partir de eventos da identidade. Para obter mais informações sobre VA, consulte o *Guia de Avaliação do IBM Security QRadar Vulnerability*.

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

Vulnerabilidades

É possível usar o QRadar Vulnerability Manager e os scanners de terceiros para identificar vulnerabilidades.

Scanners de terceiros identificam e relatam as vulnerabilidades descobertas usando referências externas, como o Banco de Dados de Vulnerabilidade de Software Livre (OSVDB), Banco de Dados de Vulnerabilidade Nacional (NVDB) e Critical Watch. Exemplos de scanners de terceiros incluem QualysGuard e nCircle ip360. O OSVDB designa um identificador de referência exclusivo (ID do OSVDB) para cada vulnerabilidade. Referências externas designam um identificador de referência exclusivo para cada vulnerabilidade. Exemplos de IDs de referência de dados externos incluem Vulnerabilidade Comum e Exposições (CVE) ou ID de Bugtraq. Para obter mais informações sobre os scanners e avaliação de vulnerabilidades, consulte o *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

O QRadar Vulnerability Manager é um componente que pode ser comprado separadamente e ativado usando uma chave de licença. O QRadar Vulnerability Manager é uma plataforma de varredura de rede que fornece reconhecimento de vulnerabilidades que existem em aplicativos, sistemas ou dispositivos em sua rede. Após varreduras identificarem vulnerabilidades, será possível procurar e revisar dados de vulnerabilidade, corrigir vulnerabilidades e executar varreduras novamente para avaliar o novo nível de risco.

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

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

Visão geral da guia Ativos

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

Usando a guia **Ativos**, é possível:

- Visualizar todos os ativos descobertos.
- Incluir manualmente os perfis de ativos.
- Procurar ativos específicos.
- Visualizar informações sobre ativos descobertos.
- Editar os perfis de ativos para ativos manualmente incluídos ou descobertos.
- Ajustar vulnerabilidades de positivo falso.
- Importar ativos.
- Imprimir ou exportar perfis de ativo.
- Descobrir os ativos.
- Configurar e gerenciar varreduras de vulnerabilidade de terceiros.
- Iniciar as varreduras do Gerenciador de Vulnerabilidade do QRadar.

Para obter informações sobre a opção Descoberta de servidor na área de janela de navegação, consulte o *IBM Security QRadar SIEM Administration Guide*

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

Lista da guia Ativo

A página Perfis de ativo fornece informações sobre ID, endereço IP, nome do ativo, pontuação do CVSS agregado, vulnerabilidades e serviços.

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

Tabela 52. Parâmetros da página Perfil de ativo

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

Tabela 52. Parâmetros da página Perfil de ativo (continuação)

Parâmetro	Descrição
Risk Score	Exibe uma das seguintes pontuações do Sistema de Pontuação de Vulnerabilidade Comum (CVSS): • Pontuação do CVSS ambiental agregada unida • Agregar pontuação do CVSS temporal • Agregar pontuação base do CVSS • Essas pontuações são exibidas na ordem de prioridade. Por exemplo, se a pontuação do CVSS ambiental agregada unida não estiver disponível, a pontuação do CVSS temporal agregada será exibida. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras. A contagem do CVSS é calculada a partir dos 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 de ativo" na página 171. Para obter mais informações sobre o 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 pela última vez.

Opções de menu ativado pelo botão direito

Clicar com o botão direito em um ativo na guia Ativo exibe menus para obter mais informações sobre filtro de eventos.

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

Tabela 53. Opções de menu ativado pelo botão direito

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

Tabela 53. Opções de menu ativado pelo botão direito (continuação)

Opção	Descrição
Informações	O menu **Informações** fornece as seguintes opções: • **Consulta DNS** – Procura por entradas DNS que são baseadas no endereço IP. • **Consulta WHOIS** - Procura o proprietário registrado de um endereço IP remoto. O servidor de WHOIS padrão é whois.arin.net. • **Varredura de porta** – Executa uma varredura do Mapeador de Rede (NMAP) do endereço IP selecionado. Essa opção estará disponível somente se o NMAP estiver instalado em seu sistema. Para obter mais informações sobre a instalação do NMAP, consulte a documentação do seu fornecedor. • **Perfil de ativo** – Exibe informações de perfil de ativo. Essa opção de menu só ficará disponível quando os dados do perfil forem adquiridos ativamente por uma varredura ou passivamente por fontes de fluxo. • **Procurar eventos** – Selecione a opção **Procurar eventos** para procurar eventos que são associados a este endereço IP. • **Procurar fluxos** – Selecione a opção Procurar fluxos para procurar fluxos que estão associados a este endereço IP.
Executar Varredura de Vulnerabilidade	Selecione esta opção para executar uma varredura do Gerenciador de Vulnerabilidades no ativo selecionado. Essa opção será exibida somente após o QRadar Vulnerability Manager estar instalado.

Visualizando um perfil de ativos

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

Sobre Esta Tarefa

Informações do perfil de ativo são descobertas automaticamente por meio do Server Discovery ou configuradas manualmente. É possível editar informações de perfil de ativo geradas automaticamente.

A página Perfil de Ativo fornece as informações sobre o ativo que está organizado em várias áreas de janela. Para visualizar uma área de janela, você pode clicar na seta **(>)** na área de janela para visualizar mais detalhes ou selecionar a área de janela da caixa de listagem **Exibir** na barra de ferramentas.

A barra de ferramentas da página Perfil de Ativo fornece as seguintes funções:

Tabela 54. Funções da barra de ferramentas da página Perfil de Ativo

Opções	Descrição
Retornar à lista de ativos	Clique nesta opção para retornar à lista de ativos.
Exibir	Na caixa de listagem, você pode selecionar a área de janela que você deseja visualizar na área de janela de Perfil de Ativo. As áreas de janela Resumo de Ativo e Resumo de Interface de Rede são sempre exibidas. Para obter mais informações sobre os parâmetros que são exibidos em cada área de janela, consulte Ativos página parâmetros de perfil.
Editar ativo	Clique nesta opção para editar o Perfil de Ativo. Consulte “Incluindo ou editando um perfil de ativo” na página 171.
Visualização por rede	Se esse ativo estiver associado a um crime, essa opção permitirá que você visualize a lista de redes associadas a esse ativo. Quando você clica **Visualização por rede**, a janela Lista de Redes é exibida. Consulte “Monitorando ofensas agrupadas por rede” na página 35.
Visualizar resumo de origem	Se esse ativo for a origem de um crime, essa opção permitirá que você visualize as informações de resumo da origem. Quando você clicar em **Visualizar resumo de origem**, a janela Lista de crimes é exibida. Consulte “Monitorando ofensas agrupadas por IP de origem” na página 34.

Tabela 54. Funções da barra de ferramentas da página Perfil de Ativo (continuação)

Opções	Descrição
Visualizar resumo de destino	Se este ativo for o destino de um crime, essa opção permitirá que você visualize informações de resumo de destino. Quando você clica em **Visualizar resumo de destino**, a janela Lista de Destinos é exibida. Consulte "Monitorando ofensas agrupadas por IP de destino" na página 34.
Histórico	Clique em **Histórico** para visualizar informações do histórico de eventos para este ativo. Quando você clica no ícone **Histórico**, a janela Procura de eventos é exibida, pré-preenchida com critérios de procura de eventos: É possível customizar os parâmetros de procura, se necessário. Clique em **Procurar** para visualizar as informações do histórico de eventos.
Aplicativos	Clique em **Aplicativos** para visualizar informações do aplicativo para este ativo. Quando você clica no ícone **Aplicativos**, a janela Procura de Fluxo é exibida, pré-preenchida com critérios de procura do evento. É possível customizar os parâmetros de procura, se necessário. Clique em **Procurar** para visualizar as informações do aplicativo.
Conexões de procura	Clique em **Conexões de procura** para procurar por conexões. A janela Procura de conexão é exibida. Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*.
Visualizar Topologia	Clique em **Visualizar topologia** para investigar melhor o ativo. A janela Topologia atual é exibida. Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*.
Ações	Na lista **Ações**, selecione **Histórico de vulnerabilidade.** Essa opção será exibida apenas quando o IBM Security QRadar Risk Manager estiver sendo comprado e licenciado. Para obter mais informações, consulte *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 várias áreas de janela de informação do perfil de ativos. Consulte Editando um perfil de ativo.
5. Para pesquisar as vulnerabilidades associadas, clique em cada vulnerabilidade na área de janela Vulnerabilidades. Consulte a Tabela 10-10
6. Se necessário, edite o perfil de ativo. Consulte Editando um perfil de ativo.
7. Clique em **Retornar para Lista de Ativos** para selecionar e visualizar outro ativo, se necessário.

Incluindo ou editando um perfil de ativo

Perfis de ativos são descobertos e incluídos automaticamente; no entanto, talvez seja necessário que você inclua um perfil manualmente

Sobre Esta Tarefa

Quando ativos são descobertos usando a opção de Descoberta do Servidor, alguns detalhes do perfil de ativos são preenchidos automaticamente. É possível incluir manualmente as informações para o perfil do ativo e você pode editar determinados parâmetros.

Você só pode editar os parâmetros que foram inseridos manualmente. Os parâmetros que foram gerados pelo sistema são exibidos em itálico e não são editáveis. É possível excluir os parâmetros gerados pelo sistema, se necessário.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Escolha uma das opções a seguir:
   - Para incluir um ativo, clique em **Incluir ativo** e digite o endereço IP ou intervalo do CIDR do ativo no campo **Novo endereço IP**.
   - Para editar um ativo, clique duas vezes no ativo que você deseja visualizar e clique em **Editar ativo**.
4. Configure os parâmetros na área de janela do Endereço IP & do MAC. Configure uma ou mais das seguintes opções:
   - Clique no ícone **Novo endereço MAC** e digite um Endereço MAC na caixa de diálogo.
   - Clique no ícone **Novo endereço IP** e digite um endereço IP na caixa de diálogo.
   - Se **NIC desconhecido** estiver listado, você poderá selecionar esse item, clicar no ícone **Editar** e digitar um novo endereço MAC na caixa de diálogo.
   - Selecione um endereço MAC ou IP da lista, clique no ícone **Editar** e digite um novo endereço MAC na caixa de diálogo.
   - Selecione um endereço MAC ou IP na lista e clique no ícone **Remover**.
5. Configure os parâmetros na área de janela Descrição de & Nomes. Configure uma ou mais das seguintes opções:

Parâmetro	Descrição
DNS	Escolha uma das opções a seguir: • Digite um nome de DNS e clique em **Incluir**. • Selecione um nome de DNS na lista e clique em **Editar**. • Selecione um nome de DNS na lista e clique em **Remover**.
NetBIOS	Escolha uma das opções a seguir: • Digite 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	Digite um nome para este perfil de ativo.
Localização	Digite um local para este perfil de ativo.
Descrição	Digite uma descrição para o perfil de ativo.
Wireless AP	Digite o Ponto de Acesso Wireless (PA) para este perfil de ativo.
Wireless SSID	Digite o Service Set Identifier (SSID) do wireless para este perfil de ativo.
ID do Comutador	Digite o ID do comutador para este perfil de ativo.
ID da Porta do Comutador	Digite o ID de porta do comutador para este perfil de ativo.

6. Configure os parâmetros na área de janela Sistema Operacional:
   a. Na caixa de listagem **Fornecedor**, selecione um fornecedor do sistema operacional.
   b. Na caixa de listagem **Produto**, selecione o sistema operacional para o perfil de ativo.
   c. Na caixa de listagem **Versão**, selecione a versão para o sistema operacional selecionado.
   d. Clique no ícone **Incluir**.

e. Na caixa de listagem **Substituir**, selecione uma das seguintes opções:
   - **Até a próxima varredura** – Selecione esta opção para especificar que o scanner fornece informações do sistema operacional e as informações podem ser temporariamente editadas. Se você editar os parâmetros do sistema operacional, o scanner irá restaurar as informações em sua próxima varredura.
   - **Para sempre** – Selecione esta opção para especificar que você deseja inserir manualmente as informações do sistema operacional e desativar o scanner de atualizar as informações.

f. Selecione um sistema operacional na lista.

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

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

Parâmetro	Descrição
Potencial de Danos Colaterais	Configure esse parâmetro para indicar o potencial de perda de vida ou ativos físicos por dano ou furto desse ativo. Você também pode usar esse parâmetro para indicar um potencial de perda ecônomica de produtividade ou receita. O potencial de dano colateral aumentado aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Potencial de danos colaterais**, selecione uma das seguintes opções: • Nenhum • Baixo • Média baixa • Média alta • 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 neste ativo. O impacto de confidencialidade aumentada aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Requisito de confidencialidade**, selecione uma das seguintes opções: • Baixo • Médio • Alto • Não definido
Requisito de Disponibilidade	Configure esse parâmetro para indicar o impacto para disponibilidade do ativo quando uma vulnerabilidade é explorada com êxito. Ataques que consumem a largura da banda da rede, ciclos do processador ou espaço em disco impactará na disponibilidade de um ativo. O impacto de disponibilidade aumentada aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Requisito de disponibilidade**, selecione uma das seguintes opções: • 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 é explorada com êxito. Integridade refere-se à fidelidade e a veracidade garantida de informações. O impacto de integridade aumentada aumenta o valor calculado no parâmetro CVSS Score. Na caixa de listagem **Requisito de integridade**, selecione uma das seguintes opções: • Baixo • Médio • Alto • Não definido
Peso	Na caixa de listagem **Peso**, selecione um peso para este perfil de ativo. O intervalo é de 0 – 10. Ao configurar o parâmetro de **Weight**, o parâmetro de **Collateral Damage Potential** é atualizado automaticamente.

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

Parâmetro	Descrição
Business Owner	digitar o nome doproprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento. O comprimento máximo é de 255 caracteres.
Business Owner Contact	Digite as informações de contato para o proprietário de negócios. O comprimento máximo é de 255 caracteres.
Technical Owner	Digite o proprietário técnico do ativo. Um exemplo de um proprietário de negócios é o gerenciador ou diretor de TI. O comprimento máximo é de 255 caracteres.
Technical Owner Contact	Digite as informações de contato para o proprietário técnico. O comprimento máximo é de 255 caracteres.
Technical User	Na caixa de listagem, selecione o nome do usuário que você deseja associar a esse perfil do ativo. Você também pode usar esse parâmetro para ativar a correção automática de vulnerabilidade para IBM SecutiryQRadar Vulnerability Manager. Para obter mais informações sobre a correção automática, consulte o Guia do Usuário do *IBM Security QRadar Vulnerability Manager*.

9. Clique em **Salvar**.

Procurando perfis de ativos

É possível configurar os parâmetros de procura para exibir apenas os perfis de ativos que você deseja investigar a partir da 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 ativos, você pode gerenciar os Grupos de Procura de Ativos. Para obter mais informações sobre Grupos de procura de ativo. 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 identificação 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 receberá uma notificação de que ID CVE: CVE-2010-000 é ativamente usada no campo. Para verificar se quaisquer hosts em sua implementação são vulneráveis a esta exploração, você pode selecionar **Referência externa de vulnerabilidade** na lista de parâmetros de procura, selecionar **CVE**, e, em seguida, inserir o
`2010-000`

Para visualizar uma lista de todos os hosts vulneráveis a este ID CVE específico.

Nota: Para obter mais informações sobre o OSVDB, consulte *http://osvdb.org/* . Para obter mais informações sobre o 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** > **Nova procura**.
4. Escolha uma das opções a seguir:
   - Para carregar uma procura salva anteriormente, vá para a Etapa 5.
   - Para criar uma nova procura, 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 ativo 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 na lista**, digite o nome da procura que você deseja carregar.
   b. Clique em **Carregar**.
6. Na área de janela Parâmetros de Procura, defina seus critérios de procura:
   a. Na primeira caixa de listagem, selecione o parâmetro de ativos que você deseja procurar. Por exemplo, **Nome do host**, **Classificação de risco de vulnerabilidade** ou **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

É possível salvar seu critério de procura de ativo. Consulte Salvando critério de procura de ativo.

Salvando critérios de procura de ativos

Na guia **Ativos**, você pode salvar o critério de procura configurado para que você possa reutilizar os critérios. Os critérios de procura salvos não expiram.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Execute uma procura. Consulte Procurando perfis de ativo.
4. Clique em **Salvar critérios**.
5. Insira os valores para os parâmetros:

Parâmetro	Descrição
Insira o nome desta procura	Digite o nome exclusivo que deseja designar a esses critérios de procura.
Gerenciar Grupos	Clique em **Gerenciar grupos** para gerenciar os grupos de procura. Para obter mais informações, consulte Grupos de procura de ativo. Essa opção será exibida somente se você tiver permissões administrativas.
Designar procura aos grupos	Selecione a caixa de seleção para o grupo que você deseja designar a essa procura salva. Se você não selecionar um grupo, esta procura salva será designada ao grupo **Outro** por padrão. Para obter mais informações, consulte Grupos de procura de ativo.
Incluir em minhas procuras rápidas	Selecione essa caixa de seleção para incluir essa procura em sua caixa de listagem **Procura rápida**, que está na barra de ferramentas da guia **Ativos**.
Configurar como Padrão	Selecione esta caixa de seleção para configurar esta procura como sua procura padrão quando você acessar a guia **Recursos**.
Compartilhar com todos	Selecione essa caixa de seleção para compartilhar esses requisitos de procura com todos os usuários.

Grupos de procura de ativos

Usando a janela Grupos de procura de ativos, é possível criar e gerenciar grupos de procura de ativos.

Esses grupos permitem localizar facilmente critérios de procura salvos na guia **Ativos**.

Visualizando grupos de procura

Use a janela Grupos de Procura de Ativo para visualizar um grupo e subgrupos de lista.

Sobre Esta Tarefa

Na janela Grupos de procura de ativos, é possível 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 55. Funções da barra de ferramentas da janela Grupos de Procura de Ativos

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

Tabela 55. Funções da barra de ferramentas da janela Grupos de Procura de Ativos (continuação)

Função	Descrição
Copiar	Para copiar uma procura salva em 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 você deseja remover e clique em **Remover**. 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 **Procurar** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Visualize os grupos de procura.

Criando um novo grupo de procura

Na janela Grupos de Procura de Ativo, você pode criar um novo grupo de procura.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a pasta para o grupo no qual você deseja criar o novo grupo.
6. Clique em **Novo grupo**.
7. No campo **Nome**, digite um nome exclusivo para o novo grupo.
8. Opcional. No campo **Descrição**, digite uma descrição.
9. Clique em **OK**.

Editando um grupo de procura

É possível editar os campos **Nome** e **Descrição** de um grupo de procura.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione o grupo que você deseja editar.
6. Clique em **Editar**.
7. Digite um novo nome no campo **Nome**.
8. Digite uma nova descrição no campo **Descrição**.
9. Clique em **OK**.

Copiando uma procura salva em outro grupo

É possível copiar uma procura salva para outro grupo. Você também pode copiar a procura salva em mais de um grupo.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que deseja copiar.
6. Clique em **Copiar**.
7. Na janela Grupos de item, selecione a caixa de seleção para o grupo que você deseja copiar a procura salva.
8. Clique em **Designar grupos**.

Removendo um grupo ou uma procura salva de um grupo

É possível usar o ícone **Remover** para remover uma procura de um grupo ou remover um grupo de procura.

Sobre Esta Tarefa

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

Não é possível remover os seguintes grupos do sistema:

- Grupos de Procura de Ativo
- Outro

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione **Procurar** > **Nova procura**.
4. Clique em **Gerenciar grupos**.
5. Selecione a procura salva que você deseja remover do grupo:
   - Selecione a procura salva que você deseja remover do grupo.
   - Selecione o grupo que você deseja remover.

Tarefas de gerenciamento de perfil do ativo

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

Sobre Esta Tarefa

Usando a guia **Ativos**, é possível excluir, importar e exportar perfis de ativos.

Excluindo ativos

É possível excluir ativos específicos ou todos os perfis de ativo listados.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Selecione o ativo que deseja excluir e, em seguida, selecione **Excluir ativo** na caixa de listagem **Ações**.

4. Clique em **OK**.

Importando perfis de ativos

É possível importar informações do perfil de ativos.

Antes de Iniciar

O arquivo importado deve ser um arquivo CSV no seguinte formato:

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

Em que:

- **IP** – Especifica qualquer endereço IP válido no formato de número com decimal. Por exemplo: 192.168.5.34.
- **Nome** – Especifica o nome deste ativo até 255 caracteres de comprimento. Vírgulas não são válidas neste campo e invalidam o processo de importação. Por exemplo: WebServer01 está correto.
- **Peso** – Especifica um número de 0 a 10, que indica a importância deste ativo em sua rede. Um valor de 0 denota importância baixa e 10 é muito alta.
- **Descrição** – Especifica uma descrição textual para este ativo até 255 caracteres de comprimento. Esse valor é opcional.

Por exemplo, as entradas a seguir podem ser incluídas em um arquivo CSV:

-
```
192.168.5.34,WebServer01,5,Main Production Web Server
```
-
```
192.168.5.35,MailServ01,0,
```

O processo de importação mescla os Perfis de ativos importados com informações do perfil de ativos que você tem atualmente armazenado no sistema.

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na caixa de listagem **Ações**, selecione **Importar ativos**.
4. Clique em **Navegar** para localizar e selecionar o arquivo CSV que você deseja importar.
5. Clique em **Importar ativos** para iniciar o processo de importação.

Exportando ativos

É possível exportar Perfis de ativos listados em um arquivo Extended Markup Language (XML) ou Comma-Separated Value (CSV).

Procedimento

1. Clique na guia **Ativos**.
2. No menu de navegação, clique em **Perfis de ativos**.
3. Na caixa de listagem **Ações**, selecione uma das opções a seguir:
   - Exportar para XML
   - Exportar para CSV
4. Visualize a janela de status para o status do processo de exportação.

5. Opcional: Se você desejar usar outras guias e páginas enquanto a exportação estiver em andamento, clique no link **Notificar quando estiver pronto**.

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

Pesquisar vulnerabilidades de ativos

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

Sobre Esta Tarefa

É possível clicar duas vezes na vulnerabilidade para exibir mais detalhes de vulnerabilidade.

A janela Pesquisar Detalhes de Vulnerabilidade fornece os seguintes detalhes:

Parâmetro	Descrição
Vulnerability ID	Especifica o ID da vulnerabilidade. O ID de Vuln é um identificador exclusivo que é gerado pelo Sistema de Informação de Vulnerabilidade (VIS).
Published Date	Especifica a data na qual os detalhes de vulnerabilidade foram publicados no OSVDB.
Name	Especifica o nome da vulnerabilidade.
Assets	Especifica o número de ativos em sua rede que possuem esta vulnerabilidade. Clique no link para visualizar a lista de ativos.
Assets, including exceptions	Especifica o número de ativos em sua rede que possuem exceções de vulnerabilidade. Clique no link para visualizar a lista de ativos.
CVE	Especifica o identificador CVE para a vulnerabilidade. Os identificadores CVE são fornecidos pelo NVDB. Clique no link para obter mais informações. Quando você clica no link, o site NVDB é exibido em uma nova janela do navegador.
xforce	Especifica o identificador X-Force para a vulnerabilidade. Clique no link para obter mais informações. Quando você clica no link, o website da IBM Internet Security Systems é exibido em uma nova janela do navegador.
OSVDB	Especifica o identificador do OSVDB para a vulnerabilidade. Clique no link para obter mais informações. Quando você clica no link, o website do OSVDB é exibido em uma nova janela do navegador.
Detalhes do plug-in	Especifica o ID do QRadar Vulnerability Manager. Clique no link para visualizar as Definições ovais, as entradas de Base de conhecimento do Windows ou os consultores do UNIX para a vulnerabilidade. Esse recurso fornece informações sobre como o QRadar Vulnerability Manager verifica os detalhes de vulnerabilidade durante uma varredura de correção. É possível usá-lo para identificar por que uma vulnerabilidade foi aumentada em um ativo ou por que não foi.

Parâmetro	Descrição
Base de pontuação do CVSS	Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras. A pontuação do 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 de ativo” na página 171. Para obter mais informações sobre o CVSS, consulte *http://www.first.org/cvss/* .
Impact	Exibe o tipo de prejuízo ou dano que pode ser esperado se essa vulnerabilidade for explorada.
Métricas Base de CVSS	Exibe as métricas usadas para calcular a pontuação CVSS de base, 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 está disponível somente 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 associadas 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 deseja instalar a correção virtual, consulte as informações do fornecedor de IPS.
Referência	Exibe uma lista de referências externas, incluindo: • **Tipo de referência** – Especifica o tipo de referência que está listada, como uma URL consultiva ou lista de postagem do correio. • **URL** – especifica a URL na qual 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 ativos.
4. Na área de janela Vulnerabilidades, clique no valor do parâmetro **ID** ou **Vulnerability** para a vulnerabilidade que você deseja investigar.

Parâmetros da página Perfil de ativo

É possível localizar as descrições de parâmetro da página Perfil de ativo para a área de janela Resumo de ativo, Interface de rede, Vulnerabilidade, Serviços, Pacotes, Correções do Windows, Propriedades, Políticas de risco e Produtos.

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

Área de janela de resumo de ativo

É possível localizar Descrições de parâmetros da área de janela Resumo de ativo que é acessada a partir da página Perfil de ativo.

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

Tabela 10-8 Parâmetros da área de janela Resumo de ativo

Parâmetro	Descrição
Asset ID	Exibe o número do ID que é designado para o perfil de ativo.
IP Address	Exibe o último endereço IP reportado do ativo.
MAC Address	Exibe o último endereço MAC conhecido do ativo.
Network	Exibe a última rede relatada associada ao ativo.
NetBIOS Name	Exibe o nome NetBIOS do ativo, se conhecido. Se o ativo tiver mais de um nome NetBIOS, este campo indicará o número de nomes NetBIOS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes NetBIOS associados.
DNS Name	Exibe o endereço IP ou nome DNS do ativo, se conhecido. Se o ativo tiver mais de um nome DNS, este campo indicará o número de nomes DNS. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de nomes DNS associados.
Nome Dado	Exibe o nome do ativo. Por padrão, este campo está vazio. Para fornecer um determinado nome para o ativo, edite o perfil de ativo.
Group Name	Exibe o grupo último grupo de usuário conhecido do ativo, se conhecido.
Último Usuário	Exibe o último usuário conhecido do ativo. As informações de usuário são derivadas de eventos de identidade. Se mais de um usuário estiver associado a este ativo, será possível clicar no link para exibir todos os usuários.
Operating System	Exibe o sistema operacional que está em execução no ativo. Se o ativo tiver mais de um sistema operacional, este campo indicará o número de sistemas operacionais. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de sistemas operacionais associados. É possível editar esse parâmetro diretamente se o parâmetro **Override** for especificado como **Até a próxima varredura** ou **Indefinidamente**.
Weight	Exibe o nível de importância que está associado a este ativo. O intervalo é de 0 (Não Importante) a 10 (Muito Importante). Por padrão, este campo está vazio. Para fornecer uma ponderação para o ativo, edite o perfil de ativo.

Parâmetro	Descrição
Aggregate CVSS Score	Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras. A pontuação do 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 de ativo” na página 171. Para obter mais informações sobre o CVSS, consulte *http://www.first.org/cvss/* .
Business Owner	Exibe o nome do proprietário de negócios do ativo. Um exemplo de um proprietário de negócios é um gerente de departamento.
Business Owner Contact Info	Exibe as informações de contato do proprietário de negócios.
CVSS Collateral Damage Potential	Exibe o potencial que esse ativo tem para danos colaterais. Este valor é incluído na fórmula para calcular o parâmetro **CVSS Score**. Por padrão, esse campo não está definido. Para fornecer um local para o ativo, edite o perfil de ativo.
Technical Owner	Exibe o responsável técnico do ativo. Um exemplo de um responsável técnico é um gerenciador de TI ou diretor.
Technical Owner Contact Info	Exibe as informações de contato do responsável técnico.
CVSS Availability	Exibe o impacto de disponibilidade do ativo quando uma vulnerabilidade for explorada com sucesso.
Wireless AP	Exibe o ponto de acesso (AP) wireless deste perfil de ativo.
SSID Wireless	Exibe o Identificador de Conjunto de Serviço Wireless (SSID) deste perfil de ativo.
CVSS Confidentiality Requirements	Exibe o impacto na confidencialidade de uma vulnerabilidade explorada com sucesso neste ativo.
Switch ID	Exibe o ID do comutador deste perfil ativo.
Switch Port ID	Exibe o ID da porta do comutador deste perfil de ativo.
CVSS Integrity Requirements	Exibe o impacto à integridade do ativo quando uma vulnerabilidade for explorada de maneira bem-sucedida.
Technical User	Especifica o nome do usuário que está associado a este perfil de ativo.
Open Services	Exibe o número de aplicativos exclusivos da Camada 7 que são executados neste perfil de ativo.
Vulnerabilidades	Exibe o número de vulnerabilidades que são descobertas nesse perfil de ativo.
Location	Especifica o local físico do ativo. Por padrão, este campo está vazio. Para fornecer um local para o ativo, edite o perfil de ativo.
Asset Description	Especifica uma descrição deste ativo. Por padrão, este campo está vazio. Para fornecer uma descrição para o ativo, edite o perfil de ativo.
Extra Data	Especifica quaisquer informações estendidas que são baseadas em um evento.

Área de janela de resumo da interface de rede

É possível localizar as descrições de parâmetros para a área de janela Resumo da interface de rede acessada a partir da página Perfil de ativo.

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

Tabela 1 Parâmetros de área de janela Resumo de interface de rede

Parâmetro	Descrição
MAC Address	Exibe o endereço MAC deste ativo, se conhecido.
IP Address	Exibe o endereço IP que é detectado para este endereço MAC.
Network	Exibe a rede com a qual o endereço IP está associado, se conhecido.
Last Seen	Exibe a data e hora em que o endereço IP foi detectado por último nesse endereço MAC.

Área de janela Vulnerabilidade

É possível localizar descrições de parâmetros da área de janela Vulnerabilidade acessada a partir da página Perfil de ativo.

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

Tabela 56. Parâmetros da área de janela Vulnerabilidade

Parâmetro	Descrição
ID	Exibe o ID da vulnerabilidade. O ID é um identificador exclusivo que é gerado pelo Sistema de Informação de Vulnerabilidade (VIS).
Gravidade	Exibe a severidade da Indústria de Segurança de Pagamento (PCI) que está associada à vulnerabilidade.
Risk	O nível de risco que está associado à vulnerabilidade. A classificação nessa coluna deve ser pelo código de nível de risco subjacente
Service	O serviço que está associado à vulnerabilidade (como descoberto pela varredura). Se somente um serviço estiver associado, exibe o serviço. Caso contrário, exibe Vários (N) onde N indica ao número total de serviços associados a esta vulnerabilidade.
Port	Exibe o número da porta na qual esta vulnerabilidade foi descoberta. Se a vulnerabilidade for descoberta em mais de uma porta, este campo indicará o número de números de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números da porta.
Vulnerability	Nome ou título desta vulnerabilidade.
Details	Texto detalhado específico que está associado a essa vulnerabilidade, conforme determinado pela varredura. Se somente um detalhe estiver associado, exibe o texto desse Detalhe. Caso contrário, exibe Vários (N) onde N indica ao número total de Detalhes que estão associados a esta vulnerabilidade.
CVSS Score	Exibe a pontuação do Common Vulnerability Scoring System (CVSS) agregado das vulnerabilidades neste ativo. Uma pontuação do CVSS é uma métrica de avaliação da severidade de uma vulnerabilidade. É possível usar pontuações do CVSS para medir quanto interesse uma vulnerabilidade garante, em comparação a outras. A pontuação do 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 de ativo” na página 171. Para obter mais informações sobre o CVSS, consulte *http://www.first.org/cvss/* .
Found	Exibe a data na qual essa vulnerabilidade foi originalmente encontrada em uma varredura.
Last seen	Exibe a data na qual essa vulnerabilidade foi vista pela última vez em uma varredura.

Área de janela Serviços

É possível localizar descrições de parâmetros da área de janela Serviços acessada a partir da página Perfil de ativo.

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

Tabela 57. parâmetros da área de janela serviços

Parâmetro	Descrição
Service	Exibe o nome do serviço aberto.
Produto	Exibe o produto que executa este serviço, se conhecido.
Port	Exibe a porta na qual o aplicativo Camada 7 foi descoberto. Se esse serviço tiver mais que uma porta, esse campo indicará o número de portas. Mova o ponteiro do mouse sobre o valor para visualizar uma lista de números da porta.
Protocol	Exibe uma lista separada por vírgula de protocolos que são descobertos na porta que executa o serviço aberto.
Last Seen Passive	Exibe a data e hora em que o serviço aberto foi visto pela última vez passivamente.
Last Seen Active	Exibe a data e hora em que o serviço aberto foi visto pela última vez ativamente.
Service Default Ports	Exibe uma lista separada por vírgula de portas conhecidas que o aplicativo Camada 7 é conhecido por executar.
Vulnerabilities	Exibe o número de vulnerabilidades que estão associadas a este serviço aberto.

Área de janela de Serviços do Windows

É possível localizar as descrições de parâmetros da área de janela Serviços do Windows acessada a partir da página Perfil de ativo. A área de janela Serviços do Windows será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

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

Tabela 58. Parâmetros da área de janela Serviços do Windows

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

Área de janela de pacotes

É possível localizar as descrições de parâmetros para a área de janela Pacotes acessada a partir da página Perfil de ativo.

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

Tabela 59. Parâmetros da área de janela Pacotes

Parâmetro	Descrição
Packages	Exibe o nome do pacote que é aplicado ao ativo.
Version	Exibe a versão do pacote que é aplicada ao ativo.
Revision	Exibe a revisão do pacote que é aplicada ao ativo.

Área de janela de correções do Windows

É possível localizar descrições de parâmetros para a área de janela Correções do Windows que é acessada a partir da página Perfil de ativo.

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

Tabela 60. Parâmetros da área de janela Correções do Windows

Parâmetro	Descrição
Microsoft KB Number	Exibe número da Base de Conhecimento (KB) da Microsoft da correção do Windows que é executada no ativo.
Description	Exibe a descrição da correção do Windows.
Bulletin ID	Exibe o número do ID do boletim da correção do Windows.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade da correção do Windows.
CVE-ID	Exibe o ID de CVE associado à correção do Windows. Se mais de um ID de CVE for associado à correção do Windows, mova o seu mouse sobre o link Vários para exibir a lista de IDs de CVE. É possível clicar em um link do ID de CVE para acessar mais informações.
System	Exibe o sistema Windows para a correção.
Service Pack	Exibe o Service Pack da correção.

Área de janela de propriedades

É possível localizar descrições de parâmetros para a área de janela Propriedades acessada na página Perfil de ativo. A área de janela Propriedades será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

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

Tabela 61. Parâmetros da área de janela Propriedades

Parâmetro	Descrição
Name	Exibe o nome da propriedade de configuração que foi vista ativamente no ativo.
Value	Exibe o valor da propriedade de configuração.

Área de janela Políticas de risco

É possível localizar descrições de parâmetros da área de janela Políticas de risco, acessada a partir da página Perfil de ativo. A área de janela Políticas de riscos será exibida apenas quando o QRadar Vulnerability Manager for instalado em seu sistema.

A área de janela Políticas de risco em Perfil de ativo fornece as seguintes informações:

Tabela 62. Parâmetros da área de janela Políticas de risco

Parâmetro	Descrição
Policy	Especifica o nome da política associada a esse ativo.
Pass/Fail	Indica se a política tem um status **Aprovado** ou **Reprovado**.
Last Evaluated	Exibe a data da última vez que esta política foi avaliada.

Área de janela Produtos

É possível localizar descrições de parâmetros para a área de janela de Produtos que você acessa na página Perfil de ativos.

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

Tabela 63. parâmetros da área de janela de produtos

Parâmetro	Descrição
Produto	Exibe o nome do produto que é executado no ativo.

Tabela 63. parâmetros da área de janela de produtos (continuação)

Parâmetro	Descrição
Porta	Exibe a porta que o produto usa.
Vulnerabilidade	Exibe o número de vulnerabilidades que estão associadas a este produto.
ID de vulnerabilidade	Exibe o ID de vulnerabilidade.

Capítulo 15. Gerenciamento de relatório

É possível usar a guia **Relatórios** para criar, editar, distribuir e gerenciar relatórios.

As opções de relatório flexíveis e detalhadas satisfazem seus vários padrões regulatórios, como conformidade de PCI.

É possível criar seus próprios relatórios customizados ou usar relatórios padrão. É possível customizar e remarcar relatórios padrão e distribui-los para outros usuários.

A guia **Relatórios** poderá requerer um período de tempo estendido para ser atualizada se seu sistema incluir muitos relatórios.

Nota: Se estiver executando o Microsoft Exchange Server 5.5, caracteres de fontes indisponíveis poderão ser exibidos na linha de assunto de relatórios enviados por email. Para resolver isso, faça download e instale o Service Pack 4 do Microsoft Exchange Server 5.5. Para obter mais informações, entre em contato com o suporte da Microsoft.

Considerações sobre fuso horário

Para assegurar-se de 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 do QRadar esteja sincronizada com o fuso horário.

Permissões da guia Relatório

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

Os usuários não administrativos podem visualizar somente relatórios que eles criaram ou relatórios que são compartilhados por outros usuários.

Parâmetros da guia Relatório

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

Na guia **Relatórios**, é possível visualizar informações estatísticas sobre o modelo de relatórios, executar ações nos modelos de relatório, visualizar os relatórios gerados e excluir conteúdo gerado.

Se um relatório não especificar um planejamento de intervalo, será necessário gerar manualmente o relatório.

É possível passar o mouse sobre qualquer relatório para visualizar um resumo do relatório em uma dica de ferramenta. O resumo especifica a configuração do relatório e o tipo de conteúdo que o relatório gera.

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 pequeno contêiner de gráfico para o conteúdo de gráfico que exibe muitos objetos. Cada gráfico inclui uma legenda e uma lista de redes a partir das quais o conteúdo é derivado; escolha um contêiner suficientemente grande para conter os dados. Para visualizar como cada gráfico exibe dados, consulte Tipos de diagrama.

Tipos de gráfico

Ao criar um relatório, 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.

É possível usar qualquer um dos seguintes tipos de gráficos:

- **Nenhum** – Use esta opção para exibir um contêiner vazio no relatório. Essa opção pode ser útil para criar espaço em branco em seu relatório. Se 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. Será possível 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 mais informações, consulte *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 mais informações, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*.
- **Objetos do dispositivo não usados** – Esta opção de gráfico será exibida apenas se tiver comprado e licenciado o IBM Security QRadar Risk Manager. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*.
- **Eventos/logs** – Use este gráfico para visualizar informações de evento. É possível basear seus gráficos nos dados de procuras salvas a partir da guia **Atividade de log**. É possível customizar os dados que deseja exibir no relatório gerado. É possível configurar o gráfico para criar gráficos de dados em um período de tempo configurável. Esta funcionalidade ajuda a detectar tendências de eventos. Para obter mais informações sobre procuras salvas, consulte Procuras salvas.
- **Origens de log** - Use este gráfico para exportar ou relatar origens de log. Selecione as origens de log e os grupos de origem de log que você deseja que apareçam no relatório. Classifique as origens de log por colunas do relatório. Inclua as origens de log não relatadas por um período de tempo definido. Inclua as origens de log que foram criadas em um horário especificado.

- **Fluxos** – Use este gráfico para visualizar informações do fluxo. É possível basear seus gráficos nos dados de procuras salvas a partir da guia Atividade de rede. Isso permite que sejam customizados os dados que desejar exibir no relatório gerado. É possível usar procuras salvas para configurar o gráfico para criar gráficos de dados por um período de tempo configurável. Esta funcionalidade ajuda a detectar tendências de fluxo. Para obter mais informações sobre procuras salvas, consulte Procuras salvas.
- **Principais IPs de destino** – Use este gráfico para exibir os principais IPs de destino nos locais de rede selecionados.
- **Principais Ofensas** - Use esse gráfico para exibir as Principais ofensas que ocorrem no tempo presente 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 sua rede ou ativos de negócios.
- **Vulnerabilidades** – A opção Vulnerabilidades será exibida somente quando o IBM Security QRadar Vulnerability Manager for comprado e licenciado. Para obter mais informações, consulte *Guia do Usuário do IBM Security QRadar Vulnerability Manager*.

Barra de ferramentas da guia Relatório

É possível usar a barra de ferramentas para executar várias ações em relatórios.

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

Tabela 64. Opções da barra de ferramentas Relatórios

Opção	Descrição
Grupo	
Gerenciar grupos	Clique em **Gerenciar grupos** para gerenciar os grupos de relatórios. Usando o recurso Gerenciar grupos, é possível organizar seus relatórios em grupos funcionais. É possível compartilhar grupos de relatórios com outros usuários.
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. É possível também 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 relatórios. • **Compartilhar** – Selecione essa opção para compartilhar o relatório selecionado com outros usuários. Deve-se ter privilégios administrativos para compartilhar relatórios. • **Alternar planejamento** – Selecione esta opção para alternar o relatório selecionado para o estado Ativo ou 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 deseja gerar. • **Executar relatório em dados brutos** – Selecione esta opção para gerar o relatório selecionado usando dados brutos. Essa opção será útil quando desejar gerar um relatório antes que os dados acumulados requeridos estejam disponíveis. Por exemplo, se desejar executar um relatório semanal antes que uma semana completa tenha decorrido desde a criação do relatório, será possível gerar o relatório usando esta opção. • **Excluir relatório** – Selecione esta opção para excluir o relatório selecionado. Para excluir vários relatórios, mantenha a tecla Control pressionada e clique nos relatórios que deseja excluir. • **Excluir conteúdo gerado** – Selecione esta opção para excluir todo o conteúdo gerado nas linhas selecionadas. Para excluir vários relatórios gerados, mantenha pressionada a tecla Control e clique em gerar relatórios que deseja excluir.

Tabela 64. Opções da barra de ferramentas Relatórios (continuação)

Opção	Descrição
Ocultar relatórios interativos	Selecione esta caixa de seleção para ocultar os modelos de relatório inativo. A guia **Relatórios** será atualizada automaticamente e exibirá apenas os relatórios ativos. Limpe a caixa de seleções 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 seus critérios especificados: • Título do Relatório • Descrição do relatório • Grupo de relatórios • Grupos de relatórios • Nome de usuário do autor do relatório

Tipos de diagrama

Cada tipo de gráfico suporta vários tipos de diagrama 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 gráficos que estão disponíveis para cada tipo de diagrama.

Tabela 65. Tipos de diagrama

Tipo de gráfico	Tipos de gráfico disponíveis
Linha	• Eventos/logs • Fluxos • Conexões • Vulnerabilidades
Linha Empilhada	• Eventos/logs • Fluxos • Conexões • Vulnerabilidades
Barra	• Eventos/logs • Fluxos • Conexões de vulnerabilidades do ativo • Conexões • Vulnerabilidades
Barra Horizontal	• Principais IPs de Origem • Principais Ofensas • Principais IPs de Destino
Barra Empilhada	• Eventos/logs • Fluxos • Conexões

Tabela 65. Tipos de diagrama (continuação)

Tipo de gráfico	Tipos de gráfico disponíveis
Setor	• Eventos/logs • Fluxos • Vulnerabilidades de Ativo • Conexões • Vulnerabilidades
Tabela	• Eventos/logs • Fluxos • Principais IPs de Origem • Principais Ofensas • Principais IPs de Destino • Conexões • Vulnerabilidades Para exibir o conteúdo de uma tabela, é necessário projetar o relatório com um contêiner com largura de página inteira.
Tabela agregada	Disponível com o gráfico Vulnerabilidades de ativo. Para exibir o conteúdo de uma tabela, é necessário projetar o relatório com um contêiner com largura de página inteira.

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

Use o assistente de Relatório para criar e customizar um novo relatório.

Antes de Iniciar

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

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

Sobre Esta Tarefa

O assistente de Relatório fornece um guia passo a passo sobre como projetar, planejar e gerar relatórios.

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

- **Layout** – Posição e tamanho de cada contêiner

- **Contêiner** - Marcador para o conteúdo de recurso
- **Conteúdo** – Definição do gráfico que é colocado no contêiner

Após você criar um relatório que é gerado semanalmente ou mensalmente, o tempo planejado deve ter decorrido antes que o relatório gerado retorne resultados. Para obter um relatório planejado, você deve aguardar o período de tempo planejado para os resultados construam. Por exemplo, uma procura semanal requer sete dias para construir os dados. Essa procura retornará resultados após 7 dias.

Quando você especifica o formato de saída para o relatório, considere que o tamanho do arquivo de relatórios gerados podem ser de um a 2 megabytes, dependendo do formato de saída selecionado. O formato PDF é menor em tamanho e não usa uma grande quantidade de espaço de armazenamento em disco.

Procedimento

1. Clique na guia **Relatórios**.
2. Na caixa de listagem de **Ações**, selecione **Criar**.
3. Na janela Bem-vindo ao assistente do Relatório! , clique em **Avançar**.
4. Selecione uma das opções a seguir:

Opção	Descrição
Manualmente	Por padrão, o relatório é gerado 1 vez. É possível gerar o relatório tantas vezes quanto você desejar.
Por hora	Planeja o relatório para ser gerado no final de cada hora. Os dados da hora anterior são usados. Nas caixas de listagem, selecione um prazo para começar e terminar o ciclo do relatório. Um relatório é gerado para cada hora dentro desse prazo. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã para os campos **De** e **Para**.
Semanal	Planeja o relatório para gerar semanalmente usando os dados da semana anterior. Selecione o dia que você deseja gerar o relatório. O padrão é Segunda-feira. Na caixa de listagem, selecione uma hora para iniciar o ciclo do relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã.
Mensal	Planeja o relatório para gerar mensalmente usando os dados do mês anterior. Na caixa de listagem, selecione a data que você deseja gerar o relatório. O padrão é o primeiro dia do mês. Selecione um horário para iniciar o ciclo do relatório. O horário está disponível em incrementos de meia hora. O padrão é 1h da manhã.

5. Na área de janela **Permitir que este relatório gere manualmente**, **Sim** ou **Não**.

6. Configure o layout do relatório:
   a. A partir da caixa de listagem **Orientação**, selecione **Retrato** ou **Paisagem** para a orientação da página.
   b. Selecione uma das seis opções de layout exibidas no assistente de Relatório.
   c. Clique em **Avançar**.
7. Especifique valores para os seguintes parâmetros:

Parâmetro	Valores
Título do Relatório	O título pode ter até 100 caracteres de comprimento. Não use caracteres especiais.
Logotipo	A partir da caixa de listagem, selecione um logotipo.
Opções de Paginação	A partir da caixa de listagem, selecione um local para números de página a serem exibidos no relatório. É possível escolher não ter exibição de números de página.
Classificação do Relatório	Digite uma classificação para esse relatório. É possível digitar até 75 caracteres de comprimento. É possível usar espaços iniciais, caracteres especiais e caracteres de byte duplo. A classificação do relatório é exibida no cabeçalho e no rodapé do relatório. Talvez você queira classificar o seu relatório como `confidencial`, `altamente confidencial`, `sensível` ou `interno`.

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, configure os parâmetros do gráfico.

      Nota: Também é possível criar procuras salvas de ativo. A partir da caixa de listagem **Procurar para usar**, selecione a sua procura salva.
   c. Clique em **Salvar detalhes do contêiner**.
   d. Se você selecionou mais de um contêiner, repita as etapas a até c.
   e. Clique em **Avançar**.
9. Visualize a página de Visualização de Layout e, em seguida, clique em **Avançar**.
10. Selecione as caixas de seleção para os formatos de relatório que você deseja gerar e, em seguida, clique em **Avançar**.

    Importante: A Linguagem de Marcação Extensível está disponível apenas para tabelas.
11. Selecione os canais de distribuição para o relatório e, em seguida, clique em **Avançar**. As opções incluem os seguintes canais de distribuição:

Opção	Descrição
Console do Relatório	Selecione esta caixa de seleção para enviar o relatório gerado para a guia **Relatórios**. **Console do Relatório** é o canal de distribuição padrão.

Opção	Descrição
Selecione os usuários que devem ser capazes de visualizar o relatório gerado.	Essa opção é exibida depois que você seleciona a caixa de seleção **Console de relatório**. Na lista de usuários, selecione os usuários que você deseja conceder permissão para visualizar os relatórios gerados.
Selecionar todos os usuários	Essa opção é exibida somente depois que você selecionar a caixa de seleção **Console de relatório**. Selecione essa caixa de seleção se você desejar conceder permissão a todos os usuários para visualizar os relatórios gerados. Você deve ter permissões da rede apropriadas para compartilhar o relatório gerado com outros usuários.
Email	Selecione essa caixa de seleção se desejar distribuir o relatório gerado por email.
Insira o(s) endereço(s) de email de distribuição de relatório	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Email**. Digite o endereço de email para cada destinatário de relatório gerado; separe uma lista de endereços de email com vírgulas. Os caracteres máximos para este parâmetro são 255. Destinatários de email recebem este email do no_reply_reports@qradar.
Incluir Relatório como anexo (apenas não HTML)	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Email**. Selecione esta caixa de seleção para enviar o relatório gerado como um anexo.
Incluir link no Console do Relatório	Essa opção é exibida somente depois que você seleciona a caixa de seleção **Email**. Selecione essa caixa de seleção para incluir um link para o Console do Relatório no email.

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

Opção	Descrição
Descrição do Relatório	Digite uma descrição para este relatório. A descrição é exibida na página Resumo de relatório e no email de distribuição de relatório gerado.
Selecione quaisquer grupos dos quais gostaria que esse relatório fosse membro	Selecione os grupos aos quais você deseja designar esse relatório. Para obter mais informações sobre grupos, consulte Grupos de Relatório.
Deseja executar o relatório agora?	Selecione essa caixa de seleção se você desejar gerar o relatório quando o assistente for concluído. Por padrão, a caixa de seleção é selecionada.

13. Clique em **Avançar** para visualizar o resumo do relatório.
14. Na página Resumo de relatório, selecione as guias disponíveis no relatório de resumo para visualizar suas configurações 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 na hora programada. O título do relatório é o título padrão para o relatório gerado. Se você reconfigurar um relatório para inserir um novo título de relatório, o relatório será salvo como um novo relatório com o novo nome; no entanto, o relatório original permanecerá o mesmo.

Editando um relatório

Usando o assistente Relatório, você pode editar qualquer relatório padrão ou customizado a ser alterado.

Sobre Esta Tarefa

É possível 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.

Nota: Quando você customizar um relatório planejado para ser gerado manualmente, selecione o período de tempo **Data de Encerramento** antes de selecionar a **Data de Início**.

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 necessitar.

Resultados

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

Visualizando relatórios gerados

Na guia **Relatórios**, um ícone será exibido na coluna **Formatos** se um relatório possuir conteúdo gerado. É possível clicar no ícone para visualizar o relatório.

Sobre Esta Tarefa

Quando um relatório gerado possui conteúdo, a coluna **Relatórios gerados** exibe uma caixa de listagem. A caixa de listagem exibe todo o conteúdo gerado, que é organizado pelo registro de data e hora do relatório. Os relatórios mais recentes são exibidos no topo da lista. Se um relatório não possui conteúdo gerado, o valor **Nenhum** é exibido na coluna **Relatórios gerados**.

Ícones que representam o formato do relatório gerado 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 relatórios que usam um formato de tabela de gráfico único (retrato ou paisagem).

É possível visualizar apenas os relatórios para o qual você 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. Essa ativação da nova janela é o resultado da configuração do navegador da web Mozilla Firefox e não afeta o QRadar. É possível 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 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 gerar automaticamente; entretanto, você pode gerar um relatório manualmente a qualquer momento.

Sobre Esta Tarefa

Enquanto um relatório é gerado, a coluna Próximo tempo de execução exibirá uma das três mensagens a seguir:

- **Gerando** – o relatório está sendo gerado.
- **Enfileirado (posição na fila)** – o relatório 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 decrescente que especifica quando o relatório irá executar o próximo.

É possível 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

É possível customizar o relatório duplicado.

Compartilhando um relatório

É possível 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 afetarão 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 quem você deseja compartilhar esse relatório.

Relatórios de marca

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

Antes de Iniciar

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

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

Sobre Esta Tarefa

Atribuir marca ao relatório será benéfico para sua empresa se você suportar mais de um logotipo. Ao fazer upload de uma imagem, a imagem é automaticamente salva como Gráfico de Rede Móvel (PNG).

Quando você faz upload de uma nova imagem e configura a imagem como seu padrão, a nova imagem padrão não é aplicada aos relatórios que foram gerados anteriormente. Atualizar o logotipo nos relatórios gerados anteriormente requer que você gere manualmente o 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 ajustar o cabeçalho; isso é de aproximadamente 50 pixels de altura.

Procedimento

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

Grupos de relatórios

É possível classificar relatórios em grupos funcionais. Se categorizar relatórios em grupos, será possível organizar de forma eficiente e localizar os relatórios.

Por exemplo, é possível visualizar todos os relatórios que são relacionados à conformidade com o Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento (PCIDSS).

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

- Conformidade
- Executivo
- Fontes de log
- Gerenciamento de redes
- Segurança
- VoIP
- Outro

Ao criar um novo relatório, será possível designar o relatório em um grupo existente ou criar um novo grupo. Deve-se ter acesso administrativo para criar, editar ou excluir grupos.

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

Criando um grupo de relatórios

É possível criar novos grupos.

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Usando a árvore de navegação, selecione o grupo no qual você deseja criar um novo grupo.
4. Clique em **Novo grupo**.
5. Insira os valores para os parâmetros a seguir:
   - **Nome** - Digite o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
   - **Descrição** - Opcional. Digite uma descrição para este 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

É possível editar um grupo de relatórios para alterar o nome ou a descrição.

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, selecione o grupo que você deseja editar.
4. Clique em **Editar**.
5. Atualize os valores para os parâmetros, conforme necessário:
   - **Nome** - Digite o nome para o novo grupo. O nome pode ter até 255 caracteres de comprimento.
   - **Descrição** - Opcional. Digite uma descrição para este 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.

Compartilhando grupos de relatórios

É possível compartilhar grupos de relatórios com outros usuários.

Antes de Iniciar

Você deve ter permissões administrativas para compartilhar um grupo de relatórios com outros usuários.

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

Não é possível usar a Ferramenta de Gerenciamento de Conteúdo (CMT) para compartilhar grupos de relatórios.

Para obter informações adicionais sobre a CMT, consulte o *IBM Security QRadar SIEM Administration Guide*

Sobre Esta Tarefa

Na janela Grupos de Relatórios, usuários compartilhados podem ver o grupo de relatórios na lista de relatórios.

Quaisquer atualizações que o usuário fizer em um grupo de relatórios compartilhados não afetam a versão original do relatório. Somente o proprietário pode excluir ou modificar.

Uma cópia do relatório é criada quando um usuário duplica ou executa o relatório compartilhado. O usuário pode editar ou planejar relatórios dentro do grupo de relatórios copiado.

A opção de compartilhamento de grupo substitui opções de compartilhamento de relatório anterior que foram configuradas para relatórios no grupo.

Procedimento

1. Clique na guia **Relatórios**.
2. Na janela **Relatórios**, clique em **Gerenciar Grupos**.
3. Na janela **Grupos de Relatórios**, selecione o grupo de relatórios que você deseja compartilhar e clique em **Compartilhar**.
4. Na janela **Opções de Compartilhamento**, selecione uma das opções a seguir.

Opção	Descrição
Padrão (herdar do pai)	O grupo de relatórios não é compartilhado. Qualquer grupo de relatórios copiado ou relatório gerado permanece na lista de relatórios dos usuários. Cada relatório no grupo é designado com qualquer opção de compartilhamento de relatório-pai que foi configurada.
Compartilhar com Todos	O grupo de relatórios é compartilhado com todos os usuários.
Compartilhe com usuários que correspondem aos seguintes critérios...	O grupo de relatórios é compartilhado com usuários específicos. **Funções de Usuário** Selecione a partir da lista de funções de usuário e pressione o ícone incluir (+). **Perfis de Segurança** Selecione a partir da lista de perfis de segurança e pressione o ícone incluir (+).

5. Clique em **Salvar**.

Resultados

Na janela Grupos de Relatórios, usuários compartilhados veem o grupo de relatórios na lista de relatórios. Relatórios gerados exibem conteúdo com base na configuração do perfil de segurança.

Designar um relatório a um grupo

É possível usar a opção **Designar grupos** para designar um relatório para outro grupo.

Procedimento

1. Clique na guia **Relatórios**.
2. Selecione o relatório que deseja designar para um grupo.
3. Na caixa de listagem **Ações**, selecione **Designar grupos**.
4. Na lista **Grupos de itens**, selecione a caixa de seleção do grupo que deseja designar para este relatório.
5. Clique em **Designar grupos**.

Copiando um relatório para outro grupo

Use o ícone **Copiar** para copiar um relatório para um ou mais grupos de relatórios

Procedimento

1. Clique na guia **Relatórios**.
2. Clique em **Gerenciar grupos**.
3. Na árvore de navegação, selecione o relatório que você deseja copiar.
4. Clique em **Copiar**.
5. Selecione o grupo ou grupos aos quais você deseja copiar o relatório.
6. Clique em **Designar grupos**.
7. Feche a janela Grupos de relatórios.

Removendo um relatório

Use o ícone **Remover** para remover um relatório de um grupo.

Sobre Esta Tarefa

Ao remover um relatório de um grupo, 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 ao qual 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.

Avisos

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

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

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

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

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

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

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

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

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-14
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

Os preços da IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Considerações sobre política de privacidade

Os produtos de Software IBM, including software as a service solutions, (“Ofertas de software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação de identificação pessoal é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar na coleta de informações de identificação pessoal. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão estabelecidas a seguir.

Dependendo das configurações implementadas, esta Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de gerenciamento e autenticação de sessão. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade ativada.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico sobre as leis aplicáveis a essa coleta de dados, incluindo requisitos para aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy e a Declaração de privacidade online da IBM em http://www.ibm.com/privacy/details, a seção intitulada “Cookies, web beacons e

outras tecnologias" e a "Declaração de privacidade de produtos de software IBM e de software como serviço" em http://www.ibm.com/software/info/product-privacy.

Glossário

Este glossário fornece termos e definições para o software e produtos IBM Security QRadar SIEM.

As referências cruzadas a seguir 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 a um termo relacionado ou contrastante.

Para outros termos e definições adicionais, veja o website IBM Terminology (abre em uma nova janela).

A

accumulator
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 é reconfigurado quando as falhas do nó ou do daemon ocorrem 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 Address Resolution Protocol.

ARP (Address Resolution Protocol)
Um protocolo que mapeia dinamicamente um endereço IP em um endereço de endereço de adaptador de rede em uma rede local.

ASN Consulte número do sistema autônomo.

assinatura de aplicativo
Um conjunto exclusivo de características que são derivadas pelo exame de carga útil do pacote e, em seguida, usadas para identificar um aplicativo específico.

C

camada de rede
Na arquitetura de 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 de carga útil configurável 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 a classe C de endereços Internet Protocol (IP). Os endereços são oferecidos aos Provedores de Serviço da Internet (ISPs) para serem usados por seus clientes. Os endereços CIDR reduzem o tamanho das tabelas de roteamento e disponibilizam mais endereços IP nas organizações.

cliente
Um programa de software ou um computador que solicita serviços de um servidor.

Cluster HA
Uma configuração de alta disponibilidade que consiste em um servidor principal e um servidor secundário.

Common Vulnerability Scoring System (CVSS)
Um sistema de pontuação pelo qual a gravidade de uma vulnerabilidade é medida.

comportamento
Os efeitos observáveis de uma operação ou 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 usuário.

console
Uma estação de exibição a partir da qual um operado pode controlar e observar a operação do sistema.

contexto do host
Um serviço que monitora os componentes para assegurar que cada componente esteja funcionando conforme o esperado.

credencial
Um conjunto de informações que concede a um usuário ou processo certos direitos de acesso.

credibility
Uma classificação numérica entre 0 e 10 usada para determinar a integridade de um evento ou de um crime. A credibilidade aumentará, conforme diversas origens relatarem o mesmo evento ou crime.

crime Uma mensagem enviada ou um evento gerado em resposta a uma condição monitorada. Por exemplo, um crime fornecerá informações sobre uma política ter sido violada ou sobre a rede estar sob ataque.

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 possam ser obtidos apenas usando um processo de decriptografia.

cronômetro de atualização
Um dispositivo interno que é disparado manualmente ou automaticamente em intervalos de tempo, que atualiza os dados da atividade de rede atual.

CVSS Consulte Common Vulnerability Scoring System.

D

dados de carga útil
Dados do aplicativo contidos em um fluxo de IP, excluindo cabeçalho e informações administrativas.

datapoint
Um valor calculado de uma métrica em um momento.

destino de encaminhamento
Um ou mais sistemas do fornecedor que recebem dados brutos e normalizados de fontes de log e fontes de fluxo.

destino externo
Um dispositivo que está longe do site primário que recebe fluxo de dados ou de evento de um coletor de eventos.

Device Support Module (DSM)
Um arquivo de configuração que analisa os eventos recebidos de diversas origens de log e os converte a um formato de taxonomia padrão que pode ser exibido como saída.

DHCP Consulte Dynamic Host Configuration Protocol.

DNS Veja Domain Name System.

DSM Consulte Device Support Module.

Dynamic Host Configuration Protocol (DHCP)
Um protocolo de comunicação usado para gerenciar as informações de configuração de maneira centralizada. Por exemplo, o DHCP automaticamente designa endereços IP para computadores em uma rede.

E

endereço IP virtual de cluster
Um endereço IP que é compartilhado entre o host primário ou secundário e o cluster de Alta Disponibilidade.

F

falso positivo
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 uma vulnerabilidade).

fluxo Uma única transmissão de dados transmitidos através de um link durante uma conversa.

fluxo duplicado
Diversas instâncias da mesma transmissão de dados recebidas de diferentes fontes de fluxo.

folha Em uma árvore, uma entrada ou nó que não tem filhos.

fonte externa
Um dispositivo que está longe do site

primário que envia dados normalizados a um coletor de eventos.

fontes de fluxo
A origem a partir do qual o fluxo é capturado. Uma fonte de fluxo será classificada como interna, quando o fluxo for fornecido a partir do hardware instalado em um host gerenciado ou será classificada como externa quando o fluxo for enviado para um coletor de fluxo.

FQDN
Consulte nome completo do domínio.

FQNN
Consulte nome completo da rede.

funcionário público
Um componente interno que analisa o tráfego de rede e os eventos de segurança com relação às regras customizadas definidas.

G

gateway
Um dispositivo ou programa usado para conectar redes ou sistemas com diferentes arquiteturas de rede.

gravidade
Uma medida da ameaça relativa que uma fonte apresenta em um destino.

H

HA Consulte alta disponibilidade.

Hash-Based Message Authentication Code (HMAC)
Um código criptográfico que usa uma função hash críptica e uma chave secreta.

hierarquia de rede
Um tipo de contêiner que é uma coleção hierárquica de objetos de rede.

HMAC
Consulte Hash-Based Message Authentication Code.

host de Alta Disponibilidade primária
O computador principal que está conectado ao cluster de Alta Disponibilidade.

host de Alta Disponibilidade secundário
O computador em espera que está conectado ao cluster de Alta Disponibilidade. O host de Alta Disponibilidade secundário assumirá a responsabilidade do host de Alta Disponibilidade primário, se o host de Alta Disponibilidade primário falhar.

I

ICMP Consulte Internet Control Message Protocol.

identidade
Uma coleta de atributos de uma origem de dados que representa uma pessoa, organização, lugar ou item.

IDS Consulte sistema de detecção de intrusão.

interconexão de sistemas abertos (OSI)
A interconexão de sistemas abertos de acordo com os padrões da ISO (International Organization for Standardization) para a troca de informações.

Internet Control Message Protocol (ICMP)
Um protocolo da Internet usado por um gateway para se comunicar com um host de origem, por exemplo, para relatar um erro em um datagrama.

intervalo de relatório
Um intervalo de tempo configurável no final do qual o processador de evento deve enviar todos os eventos capturados e dados de fluxo para o console.

intervalo de união
O intervalo no qual os eventos são agrupados. O pacote configurável do evento ocorre em intervalos de 10 segundos e é iniciado com o primeiro evento que não corresponde a nenhum evento de união atual. No intervalo de união, os três primeiros eventos correspondentes são agrupados e enviados ao processador de evento.

IP Consulte Protocolo Internet.

IP multicast
Transmissão de um datagrama Internet Protocol (IP) a um conjunto de sistemas que formam um único grupo de multicast.

IPS Consulte sistema de prevenção de intrusão.

ISP Consulte provedor de serviços da Internet.

L

LDAP Consulte Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (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 Directory Access Protocol (DAP) X.500 mais complexo. Por exemplo, o LDAP pode ser utilizado para localizar pessoas, organizações e outros recursos em um diretório da Internet ou da intranet.

L2L Consulte Local para Local.

Local para Local (L2L)
Pertencente ao tráfego interno de uma rede local a outra rede local.

Local Para Remoto (L2R)
Pertencente ao tráfego interno de uma rede local a outra rede remota.

log de fluxo
Uma coleta de registros de fluxo.

L2R Consulte Local para Remoto.

M

magnitude
Uma medida da importância relativa de um determinado crime. Magnitude é um valor ponderado calculado a partir de relevância, gravidade 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 vários valores. Por exemplo, o mapeamento de uma lista de usuários privilegiados para um host.

Mapa QID
Uma taxonomia que identifica cada evento exclusivo e mapeia os eventos para categorias de baixo nível e alto nível para determinar como um evento deve ser correlacionado e organizado.

mapa referência de mapas
Um registro de dados de duas chaves mapeadas para vários valores. Por exemplo, o mapeamento do total de bytes de um aplicativo para um IP de origem.

máscara de sub-rede
Para sub-rede da Internet, uma máscara de 32 bits usada para identificar os bits do endereço da sub-rede na parte do host de um endereço IP.

N

NAT Consulte Conversão de Endereço de Rede.

NAT (Network Address Translation)
Em um firewall, a conversão de endereços seguros do Protocolo da Internet (IP) para endereços registrados externos. Isto permite comunicações com redes externas, mas mascara os endereços IP usados dentro do firewall.

NetFlow
Um protocolo de rede Cisco que monitora dados de fluxo do tráfego de rede. Os dados NetFlow incluem as informações do cliente e do servidor, quais portas são usadas e o número de bytes e pacotes que fluem através dos comutadores e roteadores conectados a uma rede. Os dados são enviados para coletores NetFlow, nos quais a análise de dados ocorre.

nome completo da rede (FQNN)
Em uma hierarquia da rede, o nome de um objeto que inclui todos os departamentos. Um exemplo de um Fully Qualified Network Name 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 de domínio completo é rchland.vnet.ibm.com.

número do sistema autônomo (ASN)
Em TCP/IP, um número designado a um sistema autônomo pela mesma autoridade central que designa os endereços IP. O número de sistema autônomo possibilita aos algoritmos de roteamento automatizados distinguir sistemas autônomos.

O

objeto de rede
Um componente de uma hierarquia de rede.

objeto folha de banco de dados
Um objeto terminal ou um nó em uma hierarquia de banco de dados.

Open Source Vulnerability Database (OSVDB)
Criado pela comunidade de segurança de rede para a comunidade de segurança de rede, um banco de dados de software livre que fornece informações técnicas sobre as vulnerabilidades de segurança de rede.

origem do log
O equipamento de segurança ou o equipamento de rede a partir da qual um log de eventos se origina.

OSI Consulte interconexão de sistemas abertos.

OSVDB
Consulte Open Source Vulnerability Database.

P

peso de rede
O valor numérico aplicado a cada rede que significa a importância da rede. O peso de rede é definido pelo usuário.

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 da Internet (IP)
Um protocolo que encaminha dados através de uma rede ou redes interconectadas. Esse protocolo atua como um intermediário entre as camadas de protocolo mais altas e as redes físicas. Consulte também Protocolo de Controle de Transmissões.

Provedor de serviços da Internet (ISP)
Uma organização que fornece acesso à Internet.

R

Rede Local
Consulte rede local.

rede local (LAN)
Uma rede que conecta vários dispositivos em uma área limitada (tal 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 existe um problema em uma rede.

regra de roteamento
Uma condição que, quando seus critérios forem atendidos por dados do evento, uma coleção de condições e o roteamento subsequente serão executados.

relevância
Uma medida de impacto relativo de um evento, categoria ou crime 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.

report No gerenciamento de consultas, os dados formatados resultantes da execução de um consulta e da aplicação de um formulário.

R2L Consulte Remoto para Local.

R2R Consulte Remoto para Remoto.

rule Um conjunto de instruções condicionais que permitem que os sistemas de computador identifiquem relacionamentos e executem respostas automatizadas adequadamente.

S

servidor whois
Um servidor usado para recuperar as informações sobre recursos registrados de uma Internet, como nomes de domínio e alocações de endereço IP.

Simple Network Management Protocol (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 Base de Informações de Gerenciamento (MIB).

sistema ativo
Em um cluster de alta disponibilidade (HA), o sistema que tem todos os seus serviços em execução.

sistema de detecção de intrusão (intrusion detection system) (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

sistema de espera
Um sistema que automaticamente se torna ativo quando o sistema ativo falhar. Se a replicação de disco estiver ativada, replicará os dados do sistema ativo.

Sistema de Nomes de Domínio (DNS)
O sistema de banco de dados distribuído que mapeia nomes de domínio para endereços IP.

sistema de prevenção de intrusão (IPS)
Um sistema que tenta negar a atividade potencialmente maliciosa. Os mecanismos de negação poderão envolver a filtragem, rastreamento ou limites de taxa de configuração.

SNMP
Consulte Simple Network Management Protocol.

SOAP Um protocolo leve, baseado em XML para troca de informações em um ambiente distribuído, descentralizado. SOAP pode ser usado para consultar e retornar informações e chamar os serviços através da Internet.

subprocura
Uma função que permite que uma consulta de procura seja executada dentro de um conjunto de resultados da procura concluída.

sub-rede
Consulte sub-rede.

sub-rede (subnet)
Uma rede dividida em subgrupos independentes menores, que ainda estão interconectados.

superflow
Um fluxo único que é composto por diversos fluxos com propriedades semelhantes para aumentar a capacidade de processamento ao reduzir as restrições de armazenamento.

T

tabela de referência
Uma tabela em que as chaves de mapa de registro de dados que possuem um tipo designado para outras chaves, que são então mapeadas para um valor único.

TCP Consulte Transmission Control Protocol.

Transmission Control Protocol (TCP)
Um protocolo de comunicação usado na Internet e em qualquer rede que segue os padrões do Internet Engineering Task Force (IETF) para o protocolo de interligação de redes. O TCP fornece um protocolo de host para host confiável nas redes de comunicação comutadas por pacote e em sistemas interconectados dessas redes. Consulte também Protocolo da Internet.

V

violação
Um ato que ignora ou desrespeita a política corporativa.

visualização dos sistemas
Uma representação visual de ambos os hosts, primário e gerenciado, que compõem um sistema.

Índice Remissivo

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

X