IBM Security QRadar SIEM
Versão 7.2.4

Guia de Introdução

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 25.

Informações do produto

Esse documento se aplica ao IBM QRadar Security Intelligence Platform V7.2.4 e às liberações subsequentes a menos que seja substituído por uma versão atualizada desse documento.

Índice

Introdução ao QRadar SIEM v

Capítulo 1. Visão Geral do QRadar SIEM 1
Atividade de log 1
Atividade da rede 1
Ativos 1
Ofensas 2
Relatórios 2
Coleta de Dados 2
Coleção de Dados do Evento 2
Coleção de Dados de Fluxo 3
Informações de Avaliação de Vulnerabilidade 4
regras do QRadar SIEM 4
Navegadores da web suportados 4

Capítulo 2. Introdução à Implementação do QRadar SIEM 7
Instalando o Dispositivo QRadar SIEM 7
O dispositivo QRadar SIEM 7
Configuração do QRadar SIEM 8
Hierarquia de Rede 8
Revisando a Hierarquia de Rede 9
Atualizações Automáticas 9
Definindo Configurações de Atualização Automática 10
Coletando Eventos 10
Coletando Fluxos 11
Importando as Informações de Avaliação de Vulnerabilidade 11
Ajuste do QRadar SIEM 12
Indexação de Carga Útil 12
Ativando Indexação de Carga Útil 12
Servidores e Blocos de Construção 13
Incluindo Servidores Automaticamente nos Blocos de Construção 13
Incluindo Servidores em Blocos de Construção Manualmente 14
Configurando Regras 14
Limpando o Modelo de SIM 15

Capítulo 3. Introdução ao QRadar SIEM 17
Procurando Eventos 17
Salvando Critérios de Procura de Eventos 17
Configurando Um Gráfico de Série Temporal 18
Procurando Fluxos 18
Salvando Critérios de Procura de Fluxo 19
Criando Um Item de Painel 19
Procurando Recursos 20
Investigações de Ofensas 21
Visualizando Ofensas 21
Exemplo: Ativando os Modelos de Relatório de PCI 21
Exemplo: Criando Um Relatório Customizado com Base em Uma Procura Salva 22

Avisos 25
Marcas Registradas 27
Considerações sobre a política de privacidade 27

Glossário 29
A 29

C 29
D 30
E 30
F 30
G 31
H 31
I 31
L 32
M 32
N 32
O 33
P 33
R 33
S 33
T 34
V 34

Índice Remissivo 35

Introdução ao QRadar SIEM

O Guia de Introdução ao IBM Security QRadar SIEM apresenta os principais conceitos, uma visão geral do processo de instalação e tarefas básicas que você pode executar na interface com o usuário.

Público Pretendido

Essas informações são destinadas ao uso pelos administradores de segurança que são responsáveis pela investigação e gerenciamento de segurança de rede. Para usar este guia, você deve ter um conhecimento de sua infraestrutura de rede corporativa e tecnologias de rede.

Documentação técnica

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

Entrando em Contato com o Suporte ao Cliente

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

Declaração de Boas Práticas de Segurança

A segurança do sistema de TI envolve proteger sistemas e informações por meio de prevenção, detecção e resposta ao acesso incorreto dentro e fora da empresa. O acesso incorreto pode resultar em informações sendo alteradas, destruídas, desapropriadas ou usurpadas ou pode resultar em danos ou usurpação do seu sistema, incluindo o uso em ataques a terceiros. Nenhum sistema de TI ou produto deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança únicos pode ser completamente efetivo na prevenção de uso ou acesso incorreto. Os sistemas, produtos e serviços IBM foram projetados para serem parte de uma abordagem de segurança legal abrangente, que envolverá necessariamente, procedimentos operacionais adicionais e podem precisar de outros sistemas, produtos ou serviços para serem mais efetivos. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS SEJAM IMUNES OU TORNEM SUA EMPRESA IMUNE CONTRA A CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PARTE.

Observação:

O uso desse programa pode implicar em várias leis ou regulamentos. Incluindo aqueles relacionados a privacidade, proteção de dados, empregabilidade, e comunicações eletrônicas e armazenamento. O IBM Security QRadar pode ser usado apenas para propósitos legais e de maneira legal. O cliente concorda em usar esse programa conforme, e assume todas as responsabilidades de obedecer a, leis aplicáveis, regulamentos e políticas. O licenciado declara que irá obter ou obteve quaisquer consentimentos, permissões ou licenças requeridas para ativar o uso legal do IBM Security QRadar.

Capítulo 1. Visão Geral do QRadar SIEM

O IBM Security QRadar SIEM é uma plataforma de gerenciamento de segurança de rede que fornece reconhecimento situacional e suporte de conformidade. O QRadar SIEM usa uma combinação de conhecimento de rede baseados em fluxo, correlação de eventos de segurança e avaliação de vulnerabilidades baseada em ativo.

Para a introdução, configure uma instalação básica do QRadar SIEM, colete dados do evento e do fluxo e gere relatórios.

Atividade de log

No IBM Security QRadar SIEM, é possível monitorar e exibir eventos de rede em tempo real ou executar procuras avançadas.

A guia **Atividade de Log** guia exibe informações de evento como registros de uma origem de log, como um dispositivo de firewall ou roteador. Usando a guia **Atividade de Log**, é possível executar as tarefas a seguir:

- Investigar dados do evento.
- Investigar logs de eventos que são enviados para o QRadar SIEM em tempo real.
- Procurar eventos.
- Monitorar atividade de log usando gráficos de série temporal configuráveis.
- Identificar positivos falsos para ajustar o QRadar SIEM.

Atividade da rede

No IBM Security QRadar SIEM, é possível investigar as sessões de comunicação entre dois hosts.

A guia **Atividade de Rede** exibirá informações sobre como o tráfego de rede é comunicado e o que foi comunicado, se a opção de captura de conteúdo estiver ativada. Usando a guia **Atividade de Rede**, é possível executar as tarefas a seguir:

- Investigar os fluxos enviados ao QRadar SIEM em tempo real.
- Procurar fluxos de rede.
- Monitorar atividade de rede usando gráficos de série temporal configuráveis.

Ativos

O QRadar SIEM cria automaticamente perfis de ativos usando dados de fluxo e dados de vulnerabilidade passivos para descobrir os hosts e servidores de rede.

Os perfis de ativos fornecem informações sobre cada ativo conhecido na rede, incluindo os serviços em execução. As informações do perfil de ativos são usadas para fins de correlação, que ajuda a reduzir positivos falsos.

Usando a guia Ativos, é possível executar as tarefas a seguir:

- Procurar ativos.
- Visualizar todos os ativos aprendidos.
- Visualizar informações de identidade para ativos aprendidos.
- Ajustar vulnerabilidades positivas falsas.

Ofensas

No IBM Security QRadar SIEM, é possível investigar ofensas para determinar a causa-raiz de um problema de rede.

Usando a guia **Ofensas**, é possível visualizar todas as ofensas que ocorrem em sua rede e concluir as tarefas a seguir:

- Investigar ofensas, origem e endereços IP de destino, comportamentos de rede e anomalias na rede.
- Correlacionar eventos e fluxos que são originados de várias redes para o mesmo endereço IP de destino.
- Navegar as várias páginas da guia **Ofensas** para investigar detalhes do evento e do fluxo.
- Determinar os eventos exclusivos que causaram uma ofensa.

Relatórios

No IBM Security QRadar SIEM, é possível criar relatórios customizados ou usar relatórios padrão.

O QRadar SIEM fornece modelos de relatórios padrão que você pode customizar, remarcar e distribuir aos usuários do QRadar SIEM.

Os modelos de relatórios são agrupados em tipos de relatórios, como conformidade, dispositivo, executivo e relatórios da rede. Use a guia **Relatórios** para concluir as tarefas a seguir:

- Criar, distribuir e gerenciar relatórios para dados do QRadar SIEM.
- Criar relatórios customizados para uso operacional e executivo.
- Combinar informações de segurança e de rede em um único relatório.
- Usar ou editar modelos de relatórios pré-instalados.
- Marcar seus relatórios com logotipos customizados. A marca é benéfica para distribuir relatórios a públicos diferentes.
- Configurar um planejamento para gerar ambos os relatórios, customizado e padrão.
- Publicar relatórios em vários formatos.

Coleta de Dados

O QRadar SIEM aceita informações em vários formatos e de uma ampla gama de dispositivos, incluindo eventos de segurança, tráfego de rede e resultados de varredura.

Os dados coletados são categorizados em três seções principais: eventos, fluxos e informações de avaliação de vulnerabilidades.

Coleção de Dados do Evento

Os eventos são gerados por origens de log, como firewalls, roteadores, servidores e sistemas de detecção de intrusão (IDS) ou sistemas de prevenção de intrusão (IPS).

A maioria das origens de log envia informações para o QRadar SIEM usando o protocolo syslog. O QRadar SIEM também suporta os protocolos a seguir:

- Simple Network Management Protocol (SNMP)

- Java™ Database Connectivity (JDBC)
- Security Device Event Exchange (SDEE)

Por padrão, o QRadar SIEM detecta automaticamente as origens de log após um número específico de logs identificáveis serem recebidos dentro de um período de tempo determinado. Após as origens de log serem detectadas com êxito, o QRadar SIEM incluirá o módulo de suporte de dispositivo (DSM) adequado na janela Origens de Log na guia **Admin**.

Embora a maioria dos DSMs inclua o recurso de envio de log nativo, vários DSMs requerem configuração extra ou um agente, ou ambos, para enviar logs. A configuração varia entre os tipos de DSM. Você deve assegurar que os DSMs estejam configurados para enviar logs em um formato que o QRadar SIEM suporta. Para obter mais informações sobre como configurar DSMs, consulte o *Guia de Configuração de DSM*.

Determinados tipos de origem de log, como roteadores e comutadores, não enviam logs suficientes ao QRadar SIEM para detectar e incluí-los rapidamente na lista Origem de Log. É possível incluir manualmente essas origens de log. Para obter mais informações sobre como incluir origens de log manualmente, consulte o *Guia do Usuário de Origens de Log*.

Os dados coletados são categorizados em três seções principais: eventos, fluxos e informações de avaliação de vulnerabilidade (VA).

Coleção de Dados de Fluxo

Os fluxos fornecem informações sobre o tráfego de rede e podem ser enviados ao QRadar SIEM em vários formatos, incluindo os arquivos flowlog, NetFlow, J-Flow, sFlow e Packeteer.

Ao aceitar diversos formatos de fluxo simultaneamente, o QRadar SIEM poderá detectar as ameaças e atividades que, de outra forma, serão perdidas, contando estritamente em eventos para obter informações.

O QRadar QFlow Collectors fornece a detecção completa de aplicativo do tráfego de rede, independentemente da porta na qual o aplicativo está funcionando. Por exemplo, se o protocolo Internet Relay Chat (IRC) estiver se comunicando na porta 7500/TCP, um QRadar QFlow Collector identificará o tráfego como o IRC e fornecerá uma captura de pacote do início da conversa. NetFlow e J-Flow notificam apenas que há tráfego na porta 7500/TCP sem fornecer qualquer contexto para qual protocolo está sendo usado.

Os locais de porta de espelho comuns incluem núcleo, DMZ, servidor e comutadores de aplicativo, com NetFlow que fornece informações complementares a partir de roteadores e comutadores de borda.

Por padrão, os QRadar QFlow Collectors são ativados e requerem um espelho, span ou grampo para ser conectado a uma interface disponível no dispositivo QRadar SIEM. A análise de fluxo será iniciada automaticamente quando a porta do espelho for conectada a uma das interfaces de rede no dispositivo QRadar SIEM. Por padrão, o QRadar SIEM é monitorado na interface de gerenciamento para o tráfego NetFlow na porta 2055/UDP. Será possível designar portas NetFlow extras, se necessário.

Informações de Avaliação de Vulnerabilidade

O QRadar SIEM pode importar informações de avaliação de vulnerabilidade de vários scanners de terceiros.

As informações de avaliação de vulnerabilidade ajudam o QRadar Risk Manager a identificar hosts ativos, portas abertas e vulnerabilidades potenciais.

O QRadar Risk Manager usa informações de avaliação de vulnerabilidade para classificar a magnitude das ofensas na rede.

Dependendo do tipo de scanner de avaliação de vulnerabilidade, o QRadar Risk Manager pode importar os resultados da varredura a partir do servidor do scanner ou iniciar remotamente uma varredura.

regras do QRadar SIEM

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

O QRadar SIEM inclui regras que detectam uma grande variedade de atividades, incluindo negações excessivas de firewall, diversas tentativas de login com falha e atividade botnet potencial. Para obter mais informações sobre regras, consulte o *Guia de administração do IBM Security QRadar SIEM*.

A lista a seguir descreve as duas categorias de regra:

- As regras customizadas executam testes em eventos, fluxos e ofensas para detectar atividade incomum na rede.
- As regras de detecção de anomalia executam testes nos resultados das pesquisas salvas de fluxo ou evento para detectar quando os padrões de tráfego incomum ocorrem na rede.

Importante: Um usuário com acesso não administrativo pode criar regras para as áreas da rede que podem ser acessadas. Você deve ter as permissões de função apropriada para gerenciar as regras. Para obter mais informações sobre permissões de função de usuário, consulte o *Guia de administração do IBM Security QRadar SIEM*.

Navegadores da web suportados

Para os recursos nos produtos IBM Security QRadar funcionarem adequadamente, é preciso usar um navegador da web suportado.

Ao acessar o sistema QRadar, será solicitado um nome de usuário e uma senha. O nome de usuário e a senha devem ser configurados previamente pelo administrador.

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

Tabela 1. Navegadores da Web para Produtos QRadar

Navegador da Web	Versão suportada
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release

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

Navegador da Web	**Versão suportada**
Microsoft Internet Explorer de 32 bits, com modo de documento e modo de navegador ativados	9.0 10
Google Chrome	A versão atual a partir da data de liberação dos produtos IBM Security QRadar V7.2.4

Capítulo 2. Introdução à Implementação do QRadar SIEM

Antes de poder avaliar recursos principais do IBM Security QRadar SIEM, um administrador deve implementar o QRadar SIEM.

Para implementar o QRadar SIEM, os administradores devem executar as tarefas a seguir:

- Instalar o dispositivo QRadar SIEM.
- Configure sua instalação do QRadar SIEM.
- Coletar dados do evento, fluxo e avaliação de vulnerabilidade (VA).
- Ajustar a instalação do QRadar SIEM.

Instalando o Dispositivo QRadar SIEM

Os administradores devem instalar o dispositivo QRadar SIEM para ativar o acesso à interface com o usuário.

Antes de Iniciar

Antes de instalar o dispositivo de avaliação QRadar SIEM, assegure-se de ter:

- Espaço para um dispositivo de duas unidades.
- Trilhos do rack e prateleiras (montados).
- Opcional. Um teclado USB e monitor VGA padrão para acesso ao Console.

Procedimento

1. Conecte a interface de rede de gerenciamento à porta rotulada Ethernet 1.
2. Ligue as conexões de energia dedicada na parte traseira do dispositivo.
3. Se você precisar de acesso ao Console, conecte o teclado USB e o monitor VGA padrão.
4. Se houver um painel frontal no dispositivo. Remova o painel pressionando nas guias na lateral e puxando o painel para fora do dispositivo.
5. Ligue o dispositivo.

O dispositivo QRadar SIEM

O dispositivo de avaliação do QRadar SIEM é um servidor de montagem de rack de duas unidades. Os trilhos do rack ou prateleiras não são fornecidos com equipamentos de avaliação.

O dispositivo QRadar SIEM inclui quatro interfaces de rede. Por essa avaliação, use a interface rotulada Ethernet 1 como a interface de gerenciamento.

Você pode usar as três interfaces de monitoramento restantes para a coleção de fluxos. O QRadar QFlow Collector fornece análise completa do aplicativo de rede e pode executar capturas de pacote no início de cada conversa. Dependendo do dispositivo QRadar SIEM, a análise de fluxo será iniciada automaticamente, quando um grampo ou porta de span estiver conectada a qualquer interface diferente da Ethernet 1. As etapas extras poderão ser necessárias para ativar o componente QRadar QFlow Collector no QRadar SIEM.

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

Restrição: O dispositivo de avaliação QRadar SIEM possui um limite de 50 Mbps para a análise de fluxo. Assegure-se de que o tráfego agregado nas interfaces de monitoramento para a coleção de fluxos não exceda 50 Mbps.

Configuração do QRadar SIEM

Configurando o QRadar SIEM é possível revisar a hierarquia de rede e customizar atualizações automáticas.

Procedimento

1. Assegure-se de que os aplicativos a seguir estejam instalados em todos os sistemas de desktop usados para acessar a interface com o usuário do produto QRadar:
   - Java Runtime Environment (JRE) version 1.7 ou IBM 64-bit Runtime Environment for Java V7.0
   - Adobe Flash versão 10.x
2. Assegure-se de estar usando um navegador da web suportado. Consulte "Navegadores da web suportados" na página 4.
3. Se você usar o Internet Explorer, ative modo de documento e modo de navegador.
   a. No navegador da web do Internet Explorer, pressione F12 para abrir a janela Ferramentas de Desenvolvedor.
   b. Clique em **Modo de Navegador** e selecione a versão do seu navegador da web.
   c. Clique em **Modo de Documento** e selecione **Padrões do Internet Explorer 7.0**.
4. Efetue login na interface com o usuário do QRadar SIEM digitando a URL a seguir:

   https://<IP Address>

   Em que <IP Address> é o endereço IP do QRadar SIEM Console.

Hierarquia de Rede

É possível visualizar diferentes áreas de sua rede organizadas pela função de negócios e priorizar informações de ameaça e política de acordo com o risco de valor de negócios.

O QRadar SIEM usa a hierarquia de rede para executar as tarefas a seguir:

- Entender o tráfego de rede e visualizar a atividade de rede.
- Monitorar serviços ou grupos lógicos específicos na rede, como marketing, DMZ ou VoIP.
- Monitorar o tráfego e perfilar o comportamento de cada grupo e host no grupo.
- Determinar e identificar os hosts locais e remotos.

Para fins de avaliação, uma hierarquia de rede padrão é incluída contendo grupos lógicos predefinidos. Reveja a hierarquia de rede para precisão e integralidade. Se seu ambiente incluir intervalos de rede que não são exibidos na hierarquia da rede pré-configurada, você deverá incluí-los manualmente.

Os objetos definidos em sua hierarquia de rede não devem estar fisicamente em seu ambiente. Todos os intervalos de rede lógica pertencentes a sua infraestrutura devem ser definidos como um objeto de rede.

Nota: Se o sistema não incluir uma hierarquia de rede concluída, use a guia **Admin** para criar uma hierarquia específica para seu ambiente.

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

Revisando a Hierarquia de Rede

É possível revisar a hierarquia de rede.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Configuração do Sistema**.
3. Clique no ícone **Hierarquia de Rede**.
4. Na lista **Gerenciar Group:Top**, clique em **Regulatory_Compliance_Servers**.

   Se sua hierarquia de rede não incluir um componente do servidor de conformidade regulamentar, você poderá usar o componente Correio para o restante deste procedimento.
5. Clique no ícone **Editar este objeto**.
6. Para incluir servidores de conformidade:
   a. No campo **IP/CIDR(s)**, digite o endereço IP ou intervalo do CIDR dos servidores de conformidade.
   b. Clique em **Incluir**.
   c. Repita para todos os servidores de conformidade.
   d. Clique em **Salvar**.
   e. Repita esse processo para as outras redes que deseja editar.
7. No menu da guia **Admin**, clique em **Implementar Mudanças**.

   É possível atualizar automaticamente ou manualmente os arquivos de configuração com as informações de segurança de rede mais recentes. O QRadar SIEM usa os arquivos de configuração do sistema para fornecer caracterizações úteis de fluxos de dados de rede.

Atualizações Automáticas

O console do QRadar SIEM deve estar conectado à Internet para receber atualizações. Se o console não estiver conectado à Internet, você deverá configurar um servidor de atualização interna.

Para obter informações sobre como configurar um servidor atualização automática, consulte o *Guia de Usuários do IBM Security QRadar SIEM*.

Usando o QRadar SIEM, é possível substituir os arquivos de configuração existentes ou integrar os arquivos atualizados aos arquivos existentes.

As atualizações de software estão disponíveis para download a partir do website a seguir:

http://www.ibm.com/support/fixcentral/

Os arquivos de atualização podem incluir as atualizações a seguir:

- As atualizações de configuração, que incluem mudanças no arquivo de configuração, vulnerabilidade, mapa QID e atualização de informações de ameaça de segurança.
- Atualizações de DSM, que incluem correções para problemas de análise, mudanças do scanner e atualizações de protocolos.
- Atualizações maiores, que incluem itens, como arquivos JAR atualizados.
- Atualizações menores, que incluem itens, como conteúdo de ajuda online extra ou scripts atualizados.

Definindo Configurações de Atualização Automática

É possível customizar a frequência de atualizações, tipos de atualização, configuração do servidor e configurações de backup do QRadar SIEM.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Configuração do Sistema**.
3. Clique no ícone **Atualização Automática**.
4. Na área de janela de navegação, clique em **Alterar Configurações**.
5. Na área de janela **Planejamento de Atualização Automática**, aceite os parâmetros padrão.
6. Na área de janela **Tipos de Atualização**, configure os parâmetros a seguir:
   a. Na caixa de listagem **Atualizações de Configuração**, selecione **Atualização Automática**.
   b. Aceite os valores padrão para os parâmetros a seguir:
      - Atualizações de DSM, Scanner, Protocolo.
      - Atualizações Maiores.
      - Atualizações Menores.
7. Limpe a caixa de seleção **Implementação Automática**.

   Por padrão, a caixa de opções fica selecionada. Se a caixa de opção não estiver selecionada, uma notificação do sistema será exibida na guia **Painel** para indicar que você deve implementar mudanças depois que as atualizações forem instaladas.
8. Clique na guia **Avançado**.
9. Na área de janela **Configuração do Servidor**, aceite os parâmetros padrão.
10. Na área de janela **Outras Configuração**, aceite os parâmetros padrão.
11. Clique em **Salvar** e feche a janela Atualizações.
12. Na barra de ferramentas, clique em **Implementar Mudanças**.

Coletando Eventos

Coletando eventos, é possível investigar os logs enviados ao QRadar SIEM em tempo real.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Origens de Dados**.
3. Clique no ícone **Origens de Log**.
4. Revise a lista de fontes de log e faça as mudanças necessárias na fonte de log.

Para obter informações sobre como configurar fontes de log, consulte o *Guia do Usuário de Fontes de Log*.

5. Feche a janela Fontes de Log.
6. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Coletando Fluxos

Ao coletar fluxos, será possível investigar as sessões de comunicação de rede entre os hosts.

Para obter mais informações sobre como ativar os fluxos em dispositivos de rede de terceiros, como comutadores e roteadores, consulte a documentação do fornecedor.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados** > **Fluxos**.
3. Clique no ícone **Fontes de Fluxo**.
4. Revise a lista de fontes de fluxo e faça as mudanças necessárias nas fontes de fluxo.

   Para obter mais informações sobre como configurar fontes de fluxo, consulte o *Guia de administração do IBM Security QRadar SIEM*.
5. Feche a janela Fontes de Fluxo.
6. No menu da guia **Admin**, clique em **Implementar Mudanças**.

Importando as Informações de Avaliação de Vulnerabilidade

Importando as informações de avaliação de vulnerabilidade (VA), é possível identificar os hosts ativos, portas abertas e vulnerabilidades potenciais.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Origens de Dados** > **Vulnerabilidade**.
3. Clique no ícone **Scanners VA**.
4. Na barra de ferramentas, clique em **Incluir**.
5. Insira valores para os parâmetros.

   Os parâmetros dependem do tipo do scanner que deseja incluir. Para obter mais informações, consulte o *Guia de Configuração de Avaliação de Vulnerabilidade*.

   Importante: O Intervalo do CIDR especifica quais redes o QRadar SIEM integra nos resultados da varredura. Por exemplo, se desejar realizar uma varredura com relação à rede 192.168.0.0/16 e especificar 192.168.1.0/24 como o intervalo CIDR, apenas os resultados do intervalo 192.168.1.0/24 serão integrados.
6. Clique em **Salvar**.
7. No menu da guia **Admin**, clique em **Implementar Mudanças**.
8. Clique no ícone **Planejar Scanners VA**.
9. Clique em **Incluir**.
10. Especifique os critérios para a frequência que você deseja que a varredura ocorra.

Dependendo do tipo de varredura, isso inclui o quão frequentemente o QRadar SIEM importará os resultados da varredura ou iniciará uma nova varredura. Você também deve especificar as portas a serem incluídas nos resultados da varredura.

11. Clique em **Salvar**.

Ajuste do QRadar SIEM

É possível ajustar o QRadar SIEM para atender às necessidades de seu ambiente.

Antes de ajustar o QRadar SIEM, aguarde um dia para ativar o QRadar SIEM para detectar os servidores na rede, armazenar eventos e fluxos e criar ofensas baseados em regras existentes.

Os administradores podem executar as tarefas de ajuste a seguir:

- Otimizar procuras de carga útil do evento e do fluxo ativando um índice de carga útil na **Atividade de Log** e **Atividade de Rede** da propriedade **Filtro Rápido**.
- Fornecer uma implementação inicial mais rápida e um ajuste mais fácil incluindo servidores automaticamente ou manualmente nos blocos de construção.
- Configurar respostas para condições de eventos, fluxo e ofensa criando ou modificando regras customizadas e regras de detecção de anomalias.
- Assegurar-se de que cada host na rede crie infração com base na maioria das regras atuais, servidores descobertos e hierarquia de rede.

Indexação de Carga Útil

Use a função **Filtro Rápido**, disponível nas guias **Atividade do Log** e **Atividade de Rede**, para procurar cargas úteis de evento e de fluxo.

Para otimizar o **Filtro Rápido**, é possível ativar uma propriedade de **Filtro Rápido** de índice de carga útil.

Ativar a indexação de carga útil pode diminuir o desempenho do sistema. Monitorar as estatísticas de índice após a ativação da indexação de carga útil na propriedade **Filtro Rápido**.

Para obter mais informações sobre o gerenciamento de índice e estatísticas, consulte o *Guia de administração do IBM Security QRadar SIEM*.

Ativando Indexação de Carga Útil

É possível otimizar as procuras de carga útil de fluxo e de evento ativando um índice de carga útil na propriedade **Filtro Rápido** de **Atividade de Log** e **Atividade de Rede**.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela de navegação, clique em **Configuração do Sistema**.
3. Clique no ícone **Gerenciamento de Index**.
4. No campo **Procura Rápida**, digite **Filtro Rápido**.
5. Clique na propriedade **Filtro Rápido** que deseja indexar.
6. Clique em **Ativar Índice**.

7. Clique em **Salvar**.
8. Clique em **OK**.
9. Opcional: Para desativar um índice de carga útil, escolha uma das opções a seguir:
   - Clique em **Desativar Índice**.
   - Clique com o botão direito em uma propriedade e selecione **Desativar Índice** no menu.

O que Fazer Depois

Para obter informações detalhadas sobre os parâmetros exibidos na janela Gerenciamento de Índice, consulte o *Guia de administração do IBM Security QRadar SIEM*.

Servidores e Blocos de Construção

O QRadar SIEM descobre e classifica automaticamente os servidores na rede, fornecendo uma implementação inicial mais rápida e ajuste mais fácil quando ocorrerem mudanças na rede.

Para assegurar que as regras apropriadas sejam aplicadas ao tipo de servidor, você pode incluir dispositivos individuais ou intervalos de endereço completo de dispositivos. É possível inserir manualmente os tipos de servidor, que não estão em conformidade com os protocolos exclusivos, em seu respectivo Bloco de Construção de Definição do Host. Por exemplo, incluir os tipos de servidores a seguir em blocos de construção reduz a necessidade de mais ajuste de positivo falso:

- Incluir servidores de gerenciamento de rede no bloco de construção **BB:HostDefinition: Servidores de Gerenciamento de Rede**.
- Incluir servidores proxies no bloco de construção **BB:HostDefinition: Servidores Proxies**.
- Incluir vírus e servidores de atualização Windows no bloco de construção **BB:HostDefinition: Definição de Vírus e Outros Servidores de Atualização**.
- Incluir Scanners de avaliação de vulnerabilidade no bloco de construção **BB-HostDefinition: IP de Origem do Scanner de Avaliação de Vulnerabilidade**.

A função Descoberta de Servidor usa o banco de dados do perfil de ativos para descobrir vários tipos de servidores na rede. A função Descoberta de Servidor lista os servidores descobertos automaticamente e você pode selecionar quais servidores deseja incluir nos blocos de construção.

Para obter mais informações sobre como descobrir servidores, consulte o *Guia de administração do IBM Security QRadar SIEM*.

Usando Blocos de Construção, é possível reutilizar testes de regra específica em outras regras. É possível reduzir o número de positivos falsos, usando blocos de construção para ajustar o QRadar SIEM e ativar regras de correlação extra.

Incluindo Servidores Automaticamente nos Blocos de Construção

É possível incluir servidores automaticamente nos blocos de construção.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Descoberta de Servidor**.
3. Na lista **Tipo de Servidor**, selecione o tipo de servidor que deseja descobrir.

   Deixe os parâmetros restantes como padrão.
4. Clique em **Descobrir Servidores**.
5. Na área de janela Servidores Correspondentes, marque a caixa de seleção de todos os servidores que deseja designar à função de servidor.
6. Clique em **Aprovar Servidores Selecionados**.

   Lembre-se: É possível clicar com o botão direito em qualquer endereço IP ou nome do host para exibir informações de resolução de DNS.

Incluindo Servidores em Blocos de Construção Manualmente

Se um servidor não for detectado automaticamente, você poderá incluir manualmente o servidor em seu Bloco de Construção de Definição do Host correspondente.

Procedimento

1. Clique na guia **Ofensas**.
2. Na área de janela de navegação, clique em **Regras**.
3. Na lista **Exibir**, selecione **Blocos de Construção**.
4. Na lista **Grupo**, selecione **Definições do Host**.

   O nome do bloco de construção corresponde ao tipo de servidor. Por exemplo, **BB:HostDefinition: Servidores Proxies** se aplica a todos os servidores proxies em seu ambiente.
5. Para incluir manualmente um host ou rede, clique duas vezes no Bloco de Construção de Definição do Host correspondente ao seu ambiente.
6. No campo **Bloco de Construção**, clique no valor sublinhado depois da frase **quando o IP de origem ou de destino for um dos seguintes**.
7. No campo **Inserir um Endereço IP ou CIDR**, digite os nomes dos hosts ou os intervalos do endereço IP que deseja designar ao bloco de construção.
8. Clique em **Incluir**.
9. Clique em **Enviar**.
10. Clique em **Concluir**.
11. Repita estas etapas para cada tipo de servidor que deseja incluir.

Configurando Regras

Na guia **Atividade de Log**, **Atividade de Rede** e **Ofensas**, é possível configurar regras ou blocos de construção.

Procedimento

1. Clique na guia **Ofensas**.
2. Clique duas vezes na ofensa que deseja investigar.
3. Clique em **Exibir** > **Regras**.
4. Clique duas vezes em uma regra.

   É possível ajustar ainda mais as regras. Para obter mais informações sobre como ajustar as regras, consulte o *Guia de administração do IBM Security QRadar SIEM*

5. Feche o assistente Regras.
6. Na página Regras, clique em **Ações**.
7. Opcional: Se desejar impedir que a ofensa seja removida do banco de dados depois que o período de retenção da ofensa tiver decorrida, selecione **Proteger Ofensa**.
8. Opcional: Se desejar designar a ofensa a um usuário do QRadar SIEM, selecione **Designar**.

Conceitos relacionados:

"regras do QRadar SIEM" na página 4
As regras executam testes em eventos, fluxos ou ofensas, e se todas as condições de um teste forem atendidas, a regra gerará uma resposta.

Limpando o Modelo de SIM

Limpe o modelo de SIEM para assegurar-se de que cada host crie ofensas com base nas regras, servidores descobertos e hierarquia de rede mais atuais.

Procedimento

1. Clique na guia **Admin**.
2. Na barra de ferramentas, selecione **Avançado** > **Limpar Modelo de SIM**.
3. Clique na opção requerida:

   `Soft Clean` para configurar as ofensas para inativo.

   `Soft Clean` com o opcional `Desativar todos as ofensas` para fechar todos as ofensas.

   `Hard Clean` para apagar todas as entradas.
4. Clique em **Tem certeza de que deseja reconfigurar o modelo de dados?**.
5. Clique em **Prosseguir**.
6. Após a conclusão do processo de reconfiguração do SIM, atualize seu navegador.

Resultados

Ao limpar o modelo de SIM, todas as ofensas existentes serão fechadas. Limpar o modelo de SIM não afeta os eventos e fluxos existentes.

Capítulo 3. Introdução ao QRadar SIEM

Para iniciar no IBM Security QRadar SIEM, aprenda sobre como procurar eventos, fluxos e ativos. Aprenda também como investigar ofensas e criar relatórios.

Por exemplo, é possível procurar informações usando o padrão salvo de procuras nas guias **Atividade de Log** e **Atividade de Rede**. Também é possível criar e salvar suas próprias procuras customizadas.

Os administradores podem executar as tarefas a seguir:

- Procurar dados do evento usando critérios específicos e exibir eventos que correspondam aos critérios de procura em uma lista de resultados. Selecionar, organizar e agrupar as colunas de dados do evento.
- Monitorar visualmente e investigar os dados de fluxo em tempo real ou executar procuras avançadas para filtrar os fluxos exibidos. Visualizar as informações de fluxo para determinar como e qual tráfego de rede é comunicado.
- Visualizar todos os ativos aprendidos ou procurar ativos específicos em seu ambiente.
- Investigar ofensas, origem e endereços IP de destino, comportamentos de rede e anomalias na rede.
- Editar, criar, planejar e distribuir relatórios padrão ou customizado.

Procurando Eventos

É possível procurar por todos os eventos de autenticação que o QRadar SIEM recebeu nas últimas 6 horas.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.
3. Na área de janela Intervalo de Tempo, defina o intervalo de tempo para a procura de eventos:
   a. Clique em **Recente**.
   b. Na lista **Recente**, selecione **Últimas 6 Horas**.
4. Na área de janela Parâmetros de Procura, defina os parâmetros de procura:
   a. Na primeira lista, selecione **Categoria**.
   b. Na segunda lista, selecione **Iguais**.
   c. Na lista **Categoria de Alto Nível**, selecione **Autenticação**.
   d. Na lista **Categoria de Baixo Nível**, aceite o valor padrão de **Qualquer**.
   e. Clique em **Incluir Filtro**.
5. Na área de janela Definição de Coluna, selecione **Nome do Evento** na lista **Exibir**.
6. Clique em **Procura**.

Salvando Critérios de Procura de Eventos

É possível salvar os critérios de procura de eventos especificados para uso futuro.

Procedimento

1. Clique na guia **Atividade de Log**.
2. Na barra de ferramentas, clique em **Salvar Critérios**.
3. No campo **Nome da Procura**, digite **Procura 1 de Exemplo**.
4. Na área de janela Opções de Período de Tempo, clique em **Recente**.
5. Na lista **Recente**, selecione **Últimas 6 Horas**.
6. Clique em **Incluir em Minhas Procuras Rápidas**.
7. Clique em **Incluir em Meu Painel**.

   Se **Incluir em Meu Painel** não for exibido, clique em **Procura** > **Editar Procura** para verificar se você selecionou **Nome do Evento** na área de janela Definição de Coluna.
8. Clique em **OK**.

O que Fazer Depois

Configure um gráfico de série temporal. Para obter informações adicionais, consulte o "Configurando Um Gráfico de Série Temporal".

Configurando Um Gráfico de Série Temporal

É possível exibir gráficos de série temporal interativos que representam os registros que são correspondidos por uma procura de intervalo de tempo específico.

Procedimento

1. Na barra de título do gráfico, clique no ícone **Configurar**.
2. Na lista **Valor para Gráfico**, selecione **IP de Destino (Contagem Exclusiva)**.
3. Na lista **Tipo de Gráfico**, selecione **Série Temporal**.
4. Clique em **Capturar Dados de Série Temporal**.
5. Clique em **Salvar**.
6. Clique em **Detalhes da Atualização**.
7. Filtre os resultados da procura:
   a. Clique com o botão direito no evento que deseja filtrar.
   b. Clique em **O Filtro no Nome do Evento é <Nome do Evento>**.
8. Para exibir a lista de eventos que são agrupados pelo nome de usuário, selecione **Username** na lista **Exibir**.
9. Verifique se a procura está visível na guia **Painel**:
   a. Clique na guia **Painel**.
   b. Clique no ícone **Novo Painel**.
   c. No campo **Nome**, digite **Painel Customizado de Exemplo**.
   d. Clique em **OK**.
   e. Na lista **Incluir Item**, selecione **Atividade de Log** > **Procuras de Eventos** > **Procura 1 de Exemplo**.

Resultados

Os resultados da procura de eventos salvos são exibidos no Painel.

Procurando Fluxos

É possível procurar, monitorar e investigar dados de fluxo em tempo real.

Também é possível executar procuras avançadas para filtrar os fluxos exibidos. Visualizar as informações de fluxo para determinar como e qual tráfego de rede é comunicado.

Procedimento

1. Clique na guia **Atividade de Rede**.
2. Na barra de ferramentas, clique em **Procura** > **Nova Procura**.
3. Na área de janela Intervalo de Tempo, defina o intervalo de tempo de procura de fluxo:
   a. Clique em **Recente**.
   b. Na lista **Recente**, selecione **Últimas 6 Horas**.
4. Na área de janela Parâmetros de Procura, defina os critérios de procura:
   a. Na primeira lista, selecione **Direção de Fluxo**.
   b. Na segunda lista, selecione **Iguais**.
   c. Na terceira lista, selecione **R2L**.
   d. Clique em **Incluir Filtro**.
5. Na lista **Exibir** na área de janela Definição de Coluna, selecione **Aplicativo**.
6. Clique em **Procura**.

Resultados

Todos os fluxos com uma direção de fluxo de remoto para local (R2L) nas últimas 6 horas são exibidos e classificados pelo campo **Nome do Aplicativo**.

Salvando Critérios de Procura de Fluxo

É possível salvar os critérios de procura de fluxo especificados para uso futuro.

Procedimento

1. Na barra de ferramentas da guia **Atividade de Rede**, clique em **Salvar Critérios**.
2. No campo **Nome da Procura**, digite o nome **Procura 2 de Exemplo**.
3. Na lista **Recente**, selecione **Últimas 6 Horas**.
4. Clique em **Incluir em Meu Painel** e em **Incluir em Minhas Procuras Rápidas**.
5. Clique em **OK**.

O que Fazer Depois

Crie um item do painel. Para obter informações adicionais, consulte o “Criando Um Item de Painel”.

Criando Um Item de Painel

É possível criar um item de painel usando critérios de procura de fluxo salvo.

Procedimento

1. Na barra de ferramentas **Rede de Atividade**, selecione **Procuras Rápidas** > **Procura 2 de Exemplo**.
2. Verifique se a procura está incluída no Painel:
   a. Clique na guia **Painel**.
   b. Na lista **Mostrar Painel**, selecione **Painel Customizado de Exemplo**.

c. Na lista **Incluir Item**, selecione **Procuras de Fluxo** > **Procura 2 de Exemplo**.

3. Configure o gráfico de painel:
   a. Clique no ícone **Configurações**.
   b. Usando as opções de configuração, altere o valor representado em gráfico, quantos objetos são exibidos, o tipo de gráfico ou o intervalo de tempo exibido no gráfico.
4. Para investigar os fluxos exibidos atualmente no gráfico, clique em **Visualizar na Atividade de Rede**.

Resultados

A página Atividade de Rede exibe resultados que correspondem aos parâmetros do gráfico de série temporal. Para obter mais informações sobre os gráficos de série temporal, consulte o *Guia de Usuários do IBM Security QRadar SIEM*.

Procurando Recursos

Ao acessar a guia **Ativos**, a página Ativo será exibida preenchida com todos os ativos descobertos na rede. Para refinar essa lista, é possível configurar parâmetros de procura para exibir apenas os perfis de ativos que deseja investigar.

Sobre Esta Tarefa

Use o recurso de procura para procurar perfis do host, ativos e informações de identidade. As informações de identidade fornecem mais detalhes, como informações de DNS, logins do usuário e endereços MAC na rede.

Por exemplo:

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Perfis de Ativos**.
3. Na barra de ferramentas, clique em **Procura** > **Nova Procura**.
4. Se desejar carregar uma procura salva, execute as etapas a seguir:
   a. Opcional: Na lista **Grupo**, selecione o grupo de procura de ativos que deseja exibir na lista **Procuras Salvas Disponíveis**.
   b. Escolha uma das opções a seguir:
      - No campo **Digitar Procura Salva ou Selecionar na Lista**, digite o nome da procura que deseja carregar.
      - Na lista **Procuras Salvas Disponíveis**, selecione a procura salva que deseja carregar.
   c. Clique em **Carregar**.
5. Na área de janela Parâmetros de Procura, defina os critérios de procura:
   a. Na primeira lista, selecione o parâmetro do ativo que deseja procurar. Por exemplo, **Nome do Host**, **Classificação de Risco de Vulnerabilidade** ou **Proprietário Técnico**.
   b. Na segunda lista, selecione o modificador que deseja usar para a procura.
   c. No campo **Entrada**, digite as informações específicas relacionadas ao parâmetro de procura.
   d. Clique em **Incluir Filtro**.

e. Repita estas etapas para cada filtro que deseja incluir nos critérios de procura.

6. Clique em **Procura**.

Exemplo

Você recebe uma notificação de que CVE ID: CVE-2010-000 está sendo ativamente explorado. Para determinar se alguns hosts na implementação são vulneráveis a essa exploração, execute as etapas a seguir:

1. Na lista de parâmetros de procura, selecione **Referência Externa de Vulnerabilidade**.
2. Selecione **CVE**.
3. Digite 2010-000 para visualizar uma lista de todos os hosts que são vulneráveis a esse ID de CVE específico.

Para obter mais informações, consulte o website Banco de Dados de Vulnerabilidade de Software Livre (*http://osvdb.org/*) e o Banco de Dados de Vulnerabilidade Nacional (*http://nvd.nist.gov/*).

Investigações de Ofensas

Usando a guia **Ofensas**, é possível investigar ofensas, endereços IP de origem e de destino, comportamentos de rede e anomalias na rede.

O QRadar SIEM pode correlacionar eventos e fluxos de mensagens com endereços IP de destino localizados em várias redes na mesma ofensa, e, finalmente, o mesmo incidente de rede. Isso permite investigar efetivamente cada ofensa em sua rede.

Visualizando Ofensas

É possível investigar cada ofensa na rede.

Por exemplo, é possível investigar ofensas, endereços IP de origem e destino, comportamentos de rede e anomalias na rede.

Procedimento

1. Clique na guia **Ofensas**.
2. Clique duas vezes na ofensa que deseja investigar.
3. Na barra de ferramentas, selecione **Exibir** > **Destinos**.

   É possível investigar cada destino para determinar se o destino está comprometido ou apresentando comportamento suspeito.
4. Na barra de ferramentas, clique em **Eventos**.

Resultados

A janela Lista de Eventos exibe todos os eventos associados à ofensa. É possível procurar, classificar e filtrar eventos.

Exemplo: Ativando os Modelos de Relatório de PCI

Usando a guia **Relatórios**, é possível ativar, desativar e editar os modelos de relatório.

Nesta tarefa de introdução, ative os modelos de relatório de Payment Card Industry (PCI).

Procedimento

1. Clique na guia **Relatórios** .
2. Limpe a caixa de seleção **Ocultar Relatórios Inativos**.
3. Na lista **Grupo**, selecione **Conformidade** > **PCI**.
4. Selecione todos os modelos de relatório na lista:
   a. Clique no primeiro relatório na lista.
   b. Selecione todos os modelos de relatório, mantendo pressionada a tecla Shift, enquanto clica no último relatório na lista.
5. Na lista **Ações**, selecione **Alternar Planejamento**.
6. Acesse os relatórios gerados:
   a. Na lista na coluna **Relatórios Gerados**, selecione o registro de data e hora do relatório que deseja visualizar.
   b. Na coluna **Formato**, clique no ícone para o formato do relatório que deseja visualizar.

Exemplo: Criando Um Relatório Customizado com Base em Uma Procura Salva

É possível criar relatórios importando uma procura ou criando critérios customizados.

Sobre Esta Tarefa

Nesta tarefa de introdução, crie um relatório baseado nas procuras de evento e de fluxo criadas em "Procurando Eventos" na página 17.

Procedimento

1. Clique na guia **Relatórios** .
2. Na lista **Ações**, selecione **Criar**.
3. Clique em **Avançar**.
4. Configure o planejamento de relatório.
   a. Selecione a opção **Diário**.
   b. Selecione as opções **Segunda-feira, Terça-feira, Quarta-feira, Quinta-feira e Sexta-feira**.
   c. Usando as listas, selecione **8:00** e **AM**.
   d. Certifique-se de que a opção **Sim – gerar relatório manualmente** esteja selecionada.
   e. Clique em **Avançar**.
5. Configure o layout do relatório:
   a. Na lista **Orientação**, selecione **Paisagem**.
   b. Selecione o layout com dois contêineres de gráfico.
   c. Clique em **Avançar**.
6. No campo **Título de Relatório**, digite **Relatório de Amostra**.
7. Configure o contêiner de gráfico da parte superior:
   a. Na lista **Tipo de Gráfico**, selecione **Eventos/Logs**.
   b. No campo **Título do Gráfico**, digite **Procura do Evento de Amostra**.

c. Na lista **Limitar Eventos/Logs até o Máximo**, selecione **10**.
d. Na lista **Tipo de Gráfico**, selecione **Barra Empilhada**.
e. Clique em **Todos os dados anteriores (24 horas)**.
f. Na lista **Basear este relatório de eventos em**, selecione **Procura 1 de Exemplo**.

   Os parâmetros restantes são preenchidos automaticamente usando as configurações da procura salva Procura 1 de Exemplo.
g. Clique em **Salvar Detalhes do Contêiner**.

8. Configure o contêiner de gráfico da parte inferior:
   a. Na lista **Tipo de Gráfico**, selecione **Fluxos**.
   b. No campo **Título do Gráfico**, digite **Procura do Fluxo de Amostra**.
   c. Na lista **Limitar Fluxos até o Máximo**, selecione **10**.
   d. Na lista **Tipo de Gráfico**, selecione **Barra Empilhada**.
   e. Clique em **Todos os dados das 24 horas anteriores**.
   f. Na lista **Procuras Salvas Disponíveis**, selecione **Procura 2 de Exemplo**.

      Os parâmetros restantes são preenchidos automaticamente usando as configurações da procura salva Procura 2 de Exemplo.
   g. Clique em **Salvar Detalhes do Contêiner**.
9. Clique em **Avançar**.
10. Clique em **Avançar**.
11. Escolha o formato do relatório:
    a. Clique nas caixas de opções **PDF e HTML**.
    b. Clique em **Avançar**.
12. Escolha os canais de distribuição do relatório:
    a. Clique em **Console de Relatório**.
    b. Clique em **E-mail**.
    c. No campo **Inserir o(s) endereço(s) de email de destino do relatório**, digite seu endereço de email.
    d. Clique em **Incluir Relatório como Anexo**.
    e. Clique em **Avançar**.
13. Complete os detalhes do assistente Relatório Final:
    a. No campo **Descrição de Relatório**, digite uma descrição do modelo.
    b. Clique em **Sim – Executar este relatório quando o assistente for concluído**.
    c. Clique em **Concluir**.
14. Usando a caixa de listagem na coluna **Relatórios Gerados**, selecione o registro de data e hora do seu relatório.

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 usados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser usado 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 consultas sobre licenças a respeito de informações do conjunto de caracteres de byte duplo (DBCS), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie consultas, por escrito, para:

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

O parágrafo a seguir não se aplica 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 estados não permitem a exclusão de garantias expressas ou implícitas em determinadas transações, portanto, essa declaração pode não se aplicar ao Cliente.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. Periodicamente são feitas alterações 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 documentos ou 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 usar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-14
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriados, incluindo, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do IBM Customer Agreement, do Contrato de Licença do Programa Internacional da IBM ou de qualquer outro contrato equivalente entre as partes.

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 meio de extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações sobre 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. As perguntas sobre os recursos de produtos não IBM devem ser endereçadas aos fornecedores desses produtos.

Todas as declarações, referentes a futuros planos ou intenções da IBM, estão sujeitas à alteração ou remoção sem aviso prévio e representam apenas metas e objetivos.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos a mudança sem aviso. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e de relatórios usados em operações de negócios diárias. 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 nomes e endereços usados por uma empresa real é mera coincidência.

Se estiver visualizando esta cópia digital das informações, as fotografias e as ilustrações coloridas podem não aparecer.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca registrada da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca registrada (® ou ™), esses símbolos indicam marcas registradas ou marcas de direitos consuetudinários nos Estados Unidos pertencentes à IBM no momento em que essas informações foram publicadas. Essas marcas registradas também são marcas registradas ou de direito comum em outros países. Uma lista atual de marcas registradas IBM está disponível na Web em Informações de copyright e de marca registrada (www.ibm.com/legal/copytrade.shtml).

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas ou marcas de serviços de terceiros.

Considerações sobre a política de privacidade

Os produtos de software IBM, incluindo software como soluções de serviços, (“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 ajudá-lo a coletar informações identificáveis pessoalmente. Se esta Oferta de software usar cookies para coletar as informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies desta oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, essa Oferta de software poderá usar cookies de sessão que coletam o ID da sessão de cada usuário para fins de gerenciamento de sessões e autenticação. Esses cookies podem ser desativados, mas desativá-los também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas para esta Oferta de software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu

próprio conselho jurídico a respeito das leis aplicáveis a essa coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy, a seção intitulada "Cookies, web beacons e outras tecnologias", na Declaração de privacidade online da IBM em http://www.ibm.com/privacy/details/br/pt/ e "IBM Software Products and Software-as-a-Service Privacy Statement" em http://www.ibm.com/software/info/product-privacy.

Glossário

Este glossário fornece termos e definições para 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" "C" "D" na página 30 "E" na página 30 "F" na página 30 "G" na página 31 "H" na página 31 "I" na página 31 "L" na página 32 "M" na página 32 "N" na página 32 "O" na página 33 "P" na página 33 "R" na página 33 "S" na página 33 "T" na página 34 "V" na página 34

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

A

administrador da rede v
ajustando
  indexação de carga útil 12
ajuste
  Bloco de construção 13
  indexação de carga útil 12
  servidores 13
  visão geral 12
atividades de log
  coleção de eventos 10
  coletando eventos 10
  procurando eventos 17
  salvando os critérios de procura 18
  visão geral 1
atividades de rede
  procurando fluxos 19
  salvando os critérios de procura 19
  visão geral 1
atualizações de software
  configurando 10
avaliações de vulnerabilidades
  coleta de dados 4
  importando 11

B

Bloco de construção
  ajustando servidores 13
  incluindo servidores
    automaticamente 14
  incluindo servidores
    manualmente 14
  visão geral 13

C

Carga útil
  indexação
    configuração 12
coleta de dados
  eventos 2
  fluxos 3
  visão geral 2
configuração
  configurações de atualização
    automática 10
  Dispositivo QRadar SIEM 8
correções
  configurando atualizações
    automáticas 10

D

Dispositivo QRadar SIEM
  visão geral 7
documentação online v
documentação técnica v

E

eventos
  coleta de dados 2
  coletando 10
  procurando 17

F

filtro rápido
  indexação de carga útil 12
filtros
  indexação de carga útil 12
fluxos
  coleta de dados 3
  coletando 11
  procurando 19

G

glossário 29
gráficos
  configuração
    série temporal 18
gráficos de série temporal
  configurando 18

H

hierarquia de rede
  revendo 9
  visão geral 8

I

indexação de carga útil
  ajuste 12
  ativando 12
  propriedade do filtro rápido 12
  visão geral 12
instalações
  Dispositivo QRadar SIEM 7
introdução v

M

modelos de SIM
  atualizando 15
  limpando 15

N

navegador da web
  versões suportadas 4

O

ofensas
  investigações 21
  visão geral 2
  visualizando 21

P

painéis
  items
    criando 19
procurando
  eventos 17
  fluxos 19
  recursos 20
  salvando os critérios de procura de eventos 18
  salvando os critérios de procura de fluxo 19

R

recursos
  perfis 1
  procurando 20
redes
  coleção de fluxo 11
regras
  configuração 14
  visão geral 4
relatórios
  exemplo
    ativando o modelo de relatório de PCI 22
    criando com base em procura salva 22
  visão geral 2

S

servidores
  Bloco de construção
    visão geral 13
  incluindo em blocos de construção
    manualmente 14
suporte ao cliente v