IBM Security QRadar Risk Manager
Versão 7.2.4

Guia de Iniciação

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 33.

Informações do produto

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

Índice

Introdução ao IBM Security QRadar Risk Manager

Essas informações são destinadas ao uso com o IBM® Security QRadar Risk Manager. O QRadar Risk Manager é uma ferramenta utilizada para monitorar configurações de dispositivo, simular mudanças em seu ambiente de rede e priorizar riscos e vulnerabilidades em sua rede.

Público alvo

Este guia é destinado aos administradores de rede que são responsáveis pela instalação e configuração dos sistemas QRadar Risk Manager em sua rede.

Documentação técnica

Para encontrar a documentação do produto do IBM Security QRadar na Web, incluindo toda a documentação traduzida, acesse o IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obter informações sobre como acessar a documentação mais técnica na biblioteca dos produtos QRadar, consulte Acessando o IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Entrando em contato com o suporte ao cliente

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

Observe que:

O uso desse programa pode implicar em várias leis ou regulamentos. Incluindo aquelas relacionadas à 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 este programa conforme as leis aplicáveis, regulamentos e políticas e assume

todas as responsabilidades para obedecê-las. 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. Introdução ao IBM Security QRadar Risk Manager

O IBM Security QRadar Risk Manager é um dispositivo instalado separadamente. Use o QRadar Risk Monitor para monitorar as configurações do dispositivo, simular mudanças no seu ambiente de rede e priorizar riscos e vulnerabilidades em sua rede.

O QRadar Risk Manager é acessado a partir da guia **Riscos** no console do IBM Security QRadar SIEM.

O QRadar Risk Manager aprimora o QRadar SIEM dando ao administrador ferramentas para concluir as tarefas a seguir:

- Centralizar o gerenciamento de risco.
- Usar uma topologia para visualizar sua rede.
- Configurar e monitorar dispositivos de rede.
- Visualizar conexões entre dispositivos de rede.
- Procurar regras de firewall.
- Visualizar as regras existentes e a contagem de eventos para as regras acionadas.
- Procurar dispositivos e caminhos para os dispositivos de rede.
- Monitorar e auditar sua rede para garantir a conformidade.
- Definir, planejar e executar simulações de exploração em sua rede.
- Procurar vulnerabilidades.

Gerenciamento de risco e conformidade centralizados para inteligência melhorada de informações podem envolver a cooperação de muitas equipes internas. Como um SIEM da próxima geração com um dispositivo adicional do Risk Management, reduzimos o número de etapas que são necessárias a partir dos produtos SIEM da primeira geração. Fornecemos topologia de rede e avaliação de risco para ativos que são gerenciados no QRadar SIEM.

Durante o processo de avaliação, seu sistema é consolidado, bem como a segurança, a análise de risco e as informações de rede por meio da agregação e correlação, fornecendo visibilidade completa no seu ambiente de rede. Um portal para seu ambiente também é definido, o que fornece visibilidade e eficácia que não podem ser alcançados usando processos manuais e outras tecnologias de ponta do produto.

Capítulo 2. Implementar o IBM Security QRadar Risk Manager

Seu dispositivo QRadar Risk Manager é instalado com a versão mais recente do software QRadar Risk Manager.

Deve-se instalar o dispositivo de avaliação do IBM Security QRadar Risk Manager. O software requer ativação e deve-se designar um endereço IP para o dispositivo QRadar Risk Manager.

Se for necessário algum tipo de assistência para ativar o software e designar um endereço IP, entre em contato com o suporte ao cliente.

O aplicativo está pronto para aceitar informações de seus dispositivos de rede.

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

Para implementar o QRadar Risk Manager em seu ambiente, você deve:

1. Assegurar-se de que a versão mais recente do IBM Security QRadar SIEM esteja instalada.
2. Verificar se todos os requisitos de pré-instalação foram atendidos.
3. Configurar e ligar seu QRadar Risk Manager.
4. Instalar o plug-in do QRadar Risk Manager em seu console do QRadar SIEM.
5. Estabelecer comunicação entre QRadar SIEM e o dispositivo QRadar Risk Manager.
6. Definir funções de usuário para seus usuários do QRadar Risk Manager.

Antes de instalar

Deve-se concluir o processo de instalação para um console do IBM Security QRadar SIEM antes de instalar o IBM Security QRadar Risk Manager. Como uma boa prática, instale o QRadar SIEM e o QRadar Risk Manager no mesmo comutador de rede.

Deve-se revisar as seguintes informações:

- Configurar porta de acesso do firewall
- Identificar as configurações de rede
- Recursos não suportados no QRadar Risk Manager
- Navegadores da web suportados

Antes de instalar o aplicativo de avaliação do IBM Security QRadar Risk Manager, assegure-se de ter:

- espaço para um dispositivo de duas unidades
- trilhos e estantes do rack que são montados

Opcionalmente, você pode desejar um teclado USB e monitor VGA padrão para acessar o console do QRadar SIEM.

Configurar o acesso a portas em firewalls

Os firewalls entre o console do IBM Security QRadar e o IBM Security QRadar Risk Manager devem permitir tráfego em determinadas portas.

Assegure-se de que qualquer firewall localizado entre o console QRadar SIEM e o QRadar Risk Manager permita tráfego nas seguintes portas:

- Porta 443 (HTTPS)
- Porta 22 (SSH)
- Porta 37 UDP (Horário)

Identificar configurações de rede

Deve-se reunir informações sobre suas configurações de rede antes de iniciar o processo de instalação.

Reúna as seguintes informações para suas configurações de rede:

- Nome do host
- endereço IP
- Endereço da máscara de rede
- Máscara de sub-rede
- Endereço de gateway padrão
- Endereço do servidor Sistema de Nomes de Domínio (DNS) principal
- Endereço do servidor DNS secundário (opcional)
- Endereço IP público para redes que usem nome de servidor de email de Conversão de Endereço de Rede (NAT)
- Nome do servidor de e-mail
- Servidor Network Time Protocol (NTP) (Console somente) ou nome do servidor de horário

Recursos não suportados no QRadar Risk Manager

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

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

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

Navegadores da web suportados

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

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

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

Tabela 1. Navegadores da web suportados para produtos QRadar

Navegador da web	Versão suportada
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegação ativados	9.0 10
Google Chrome	A versão atual a partir da data da liberação dos produtos IBM Security QRadar V7.2.4

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

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

Procedimento

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janelaFerramentas de Desenvolvedor.
2. Clique em **Modo de Navegador** e selecione a versão do seu navegador da web.
3. Clique em **Modo de Documento**.
   - Para o Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**
   - Para o Internet Explorer V8.0, selecione **Padrões do Internet Explorer 8**

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

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

Você acessa o IBM Security QRadar Risk Manager por meio do console do QRadar. Use as informações na tabela a seguir ao efetuar login no console do IBM Security QRadar.

Tabela 2. Informações de login padrão para o QRadar Risk Manager

Informações de login	Padrão
URL	https://<IP address>, em que <IP address> é o endereço IP do console do QRadar.
Nome de usuário	admin
Senha	A senha que é designada para o QRadar Risk Manager durante o processo de instalação.
Chave de licença	Uma chave de licença padrão fornece acesso ao sistema por 5 semanas.

Configurando um dispositivo QRadar Risk Manager

Deve-se conectar a interface de gerenciamento e assegurar que as conexões de alimentação estejam conectadas ao dispositivo QRadar Risk Manager.

Antes de Iniciar

Ler, entender e obter os pré-requisitos.

Sobre Esta Tarefa

O dispositivo de avaliação do IBM Security QRadar Risk Manager é um servidor de montagem em rack de duas unidades. Trilhos e estantes do rack não são fornecidos com equipamentos de avaliação.

O dispositivo QRadar Risk Manager inclui quatro interfaces de rede. Para essa avaliação, utilize a interface de rede identificada como ETH0 como a interface de gerenciamento. As outras interfaces são interfaces de monitoramento. Todas as interfaces encontram-se no painel posterior do dispositivo QRadar Risk Manager.

O botão de energia está no painel frontal.

Procedimento

1. Conecte a interface de rede de gerenciamento à porta identificada como ETH0.
2. Assegure-se de que as conexões de energia dedicada estejam conectadas na parte traseira do dispositivo.
3. Opcional. Para acessar o console do QRadar SIEM, conecte o teclado USB e um monitor VGA padrão.
4. Se houver uma área de janela frontal no dispositivo, remova-a empurrando nas guias em qualquer lado e puxe-o para fora da ferramenta.
5. Pressione o botão de energia na parte frontal para ligar o dispositivo.

Resultados

O dispositivo começa o processo de inicialização.

Incluindo o QRadar Risk Manager no console do QRadar

Você deve incluir o IBM Security QRadar Risk Manager como um host gerenciado no console do IBM Security QRadar.

Antes de Iniciar

Se desejar ativar a compactação, então, a versão mínima para cada host gerenciado deverá ser QRadar console 7.1 or QRadar Risk Manager 7.1.

Para incluir um host gerenciado não NATed em sua implementação quando o Console for NATed, você deverá alterar o console QRadar para um host em NAT. Deve-se alterar o console antes de incluir o host gerenciado em sua implementação. Para obter mais informações, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

Procedimento

1. Abra seu navegador da web.

2. Digite a URL, `https://<IP Address>`, em que <IP Address> é o endereço IP do console do QRadar.
3. Digite seu nome de usuário e senha.
4. Na guia **Admin**, clique em **Editor de Implementação**.
5. No menu, selecione **Ações** e, em seguida, selecione **Incluir um Host Gerenciado**.
6. Clique em **Avançar**.
7. Inserir valores para o parâmetros a seguir:

Opção	Descrição
Insira o IP do servidor ou dispositivo para incluir	O endereço IP do QRadar Risk Manager.
Insira a senha raiz do host	A senha raiz para o host.
Confirme a senha raiz do host	Confirmação para sua senha.
O host é NATed	Para ativar NAT para um host gerenciado, a rede NATed deve estar usando tradução estática NAT. Para obter informações adicionais, consulte o Guia de Administração do *IBM Security QRadar SIEM*.
Ativar Criptografia	Cria um túnel de criptografia SSH para o host. Para ativar a criptografia entre dois hosts gerenciados, cada host gerenciado deverá estar executando o console do QRadar 7.1 ou o QRadar Risk Manager 7.1.
Ativar Compactação	Ativa a compactação de dados entre dois hosts gerenciados.

8. Escolha uma das opções a seguir:
   - Se você tiver marcado a caixa de seleção **Host é NATed**, deverá inserir valores para os parâmetros NAT.

Opção	Descrição
Insira o IP público do servidor ou dispositivo a incluir	O endereço IP público do host gerenciado. O host gerenciado usa esse endereço IP para se comunicar com outros hosts gerenciados em diferentes redes que usam NAT.
Selecione rede NATed	A rede que você deseja que este host gerenciado use. Se o host gerenciado estiver na mesma sub-rede do console do QRadar, selecione o console da rede em NAT. Se o host gerenciado não estiver na mesma sub-rede do console do QRadar, selecione o host gerenciado da rede em NAT.

   - Se você não tiver marcado a caixa de seleção **O Host é NATed**, clique em **Avançar**.
9. Clique em **Concluir**. Este processo pode levar vários minutos para ser concluído. Se a sua implementação incluir mudanças, você deverá implementar todas as mudanças.
10. Clique em **Implementar**.

O que Fazer Depois

Limpe o cache do navegador da web e, em seguida, efetue login no console do QRadar. A guia **Riscos** agora está disponível.

Estabelecendo comunicação

Deve-se estabelecer comunicação entre seu dispositivo do QRadar Risk Manager e seu console do QRadar SIEM antes de instalar e configurar o QRadar Risk Manager.

Sobre Esta Tarefa

O processo para estabelecer comunicações pode levar vários minutos para ser concluído. Se o endereço IP de seu QRadar Risk Manager for alterado ou precisar conectar o QRadar Risk Manager a outro console do QRadar SIEM, será possível usar o **Risk Manager Settings** na guia QRadar SIEM **Admin**.

Procedimento

1. Abra seu navegador da web e, em seguida, limpe o cache do navegador da web.
2. Efetue login no QRadar SIEM. Para obter informações sobre o endereço IP, nome de usuário ou senha raiz, consulte Acessando a interface com o usuário do IBM Security QRadar Risk Manager.
3. Clique na guia **Riscos**.
4. Digite os valores para os parâmetros a seguir:

Opção	Descrição
IP/Host	O endereço IP ou o nome do host do dispositivo QRadar Risk Manager
Senha raiz	A senha raiz do dispositivo QRadar Risk Manager.

5. Clique em **Salvar**.

O que Fazer Depois

Definir funções de usuário.

Incluindo a função de usuário do Risk Manager

Deve-se designar a função de usuário do Risk Manager para fornecer acesso ao QRadar Risk Manager.

Sobre Esta Tarefa

Por padrão, o QRadar SIEM fornece uma função administrativa padrão, que fornece acesso a tudo no QRadar Risk Manager. Ao usuário que é designado a privilégios administrativos, incluindo a função administrativa padrão, não é possível editar sua própria conta. Outro usuário administrativo deve fazer as alterações necessárias.

Para obter informações sobre como criar e gerenciar funções do usuário, consulte o *Guia de Administração do IBM Security QRadar SIEM*.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Configuração do Sistema**.
3. Na área de janela **Gerenciamento de Usuário**, clique em **Funções do Usuário**.
4. Na área de janela à esquerda, selecione a função do usuário que você deseja editar.
5. Selecione a caixa de opções **Risk Manager**.
6. Clique em **Salvar**
7. Clique em **Fechar**.
8. Na guia **Admin**, clique em **Implementar Mudanças**.

Capítulo 3. Coleta de dados da rede

Deve-se configurar QRadar Risk Manager para ler as informações de configuração a partir dos dispositivos em sua rede.

As informações de configuração que são coletadas de seus dispositivos de rede geram a topologia para sua rede e permite que o QRadar Risk Manager entenda a sua configuração de rede.

Os dados que são coletados no QRadar Risk Manager são utilizados para preencher a topologia com informações chave sobre seu ambiente de rede.

A coleta de dados é um processo de três etapas:

- Fornecer o QRadar Risk Manager com as credenciais para fazer download de configurações do dispositivo de rede.
- Descobrir dispositivos para criar uma lista de dispositivos no Configuration Source Management.
- Faça backup da lista de dispositivos para obter as configurações do dispositivo e preencher a topologia com dados sobre sua rede.

Credenciais

O QRadar Risk Manager deve ser configurado com as credenciais para acessar e fazer download das configurações do dispositivo. As credenciais permitem que o QRadar Risk Manager se conecte a firewalls, roteadores, comutadores ou dispositivos Intrusion Prevention System (IPS).

Os administradores utilizam o **Configuration Source Management** para as credenciais do dispositivo de entrada, que fornecem ao QRadar Risk Manager acesso a um dispositivo específico. O QRadar Risk Manager pode salvar credenciais do dispositivo individual para um dispositivo de rede específico. Se diversos dispositivos de rede usarem as mesmas credenciais, será possível designar credenciais a um grupo. Por exemplo, você pode designar credenciais para um grupo se todos os firewalls na organização tiverem o mesmo nome de usuário e senha. As credenciais são associadas aos conjuntos de endereços para todos os firewalls e são utilizadas para fazer backup das configurações do dispositivo para todos os firewalls em sua organização.

Nota: Se uma credencial de rede não é necessária para um dispositivo específico, então o parâmetro poderá ser deixado em branco no **Configuration Source Management**.

Configurando credenciais

Os dispositivos de rede são configurados para que o QRadar Risk Manager possa ter acesso aos dispositivos.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Noa área de janela **Risk Manager**, clique em **Configuration Source Management**.

4. No menu de navegação, clique em **Credenciais**.
5. Na área de janela **Grupos de Rede**, clique em **Incluir um novo grupo de rede**.
6. Digite um nome para o grupo de rede e clique em **OK**.
7. No campo **Incluir endereço**, digite o endereço IP de seu dispositivo e clique em **Incluir**. Repita essa etapa para cada endereço que deve ser incluído.

   Nota: Assegure-se de que os endereços incluídos sejam exibidos na seção de endereço da Rede ao lado da caixa **Incluir endereço**. Não replique os endereços dos dispositivos que já existem em outros grupos de rede em **Configuration Source Management**.
   Você pode digitar um endereço IP, um intervalo de endereços IP, uma sub-rede CIDR ou um curinga. Por exemplo, para utilizar um curinga, digite 10,1.*.* ou para utilizar um CIDR 10.2.1.0/24.
8. Na área de janela **Credenciais**, clique em **Incluir um novo conjunto de credencial**.
9. Digite um nome para o novo conjunto de credenciais e clique em **OK**.
10. Selecione o nome do conjunto de credenciais criado e, em seguida, defina valores para os seguintes parâmetros:

Opção	Descrição
Nome de usuário	Um nome de usuário válido para efetuar login no adaptador. Para adaptadores, o nome de usuário e senha requerem acesso a diversos arquivos, como rule.C, objects.C, implied_rules.C, e Standard.PF.
Senha	A senha para o dispositivo.
Ativar Senha	Digite a senha para a autenticação de segundo nível. Essa senha é necessária quando as credenciais solicitarem as credenciais do usuário para o Modo Expert.
SNMP Get Community	Opcional
Nome de Usuário de Autenticação SNMPv3	Parâmetro opcional.
Senha de Autenticação SNMPv3	Parâmetro opcional.
Senha de Privacidade SNMPv3	Parâmetro opcional. O protocolo que você deseja usar para decriptografar os traps SNMPv3.

11. Clique em **OK**.

Descobrindo dispositivos

O processo de descoberta inclui dispositivos de rede para a interface de topologia utilizando as credenciais incluídas.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.

3. Na seção **Risk Manager**, clique em **Configuration Source Management**.
4. No menu de navegação, clique em **Descobrir Dispositivos**.
5. Digite um endereço IP ou intervalo do CIDR para especificar o local de dispositivos que se deseja descobrir.
6. Clique no ícone **Incluir (+)**.
7. Se você quiser procurar dispositivos na rede a partir do endereço IP definido ou do intervalo do CIDR, selecione a caixa **Efetuar crawl na rede dos endereços definidos acima**.
8. Clique em **Executar**.

Obtendo a configuração do dispositivo

É feito backup dos seus dispositivos para fazer download da configuração do dispositivo para que o QRadar Risk Manager possa incluir as informações dos dispositivos na topologia.

Antes de Iniciar

Deve-se configurar credenciais antes que você possa fazer download de configurações do dispositivo.

Sobre Esta Tarefa

É possível fazer backup de um único dispositivo ou todos os dispositivos.

Para obter informações sobre como planejar backups automatizados das configurações do dispositivo do guia **Tarefas**, consulte o *Guia do Usuário do IBM Security QRadar Risk Manager*.

Procedimento

1. Clique na guia **Admin**.
2. No menu de navegação, clique em **Plug-ins**.
3. Noa área de janela **Risk Manager**, clique em **Configuration Source Management**.
4. Clique na guia **Dispositivos**.
5. Para obter a configuração para todos os dispositivos, clique em **Fazer Backup de Tudo** na área de janela de navegação. Clique em **Sim** para continuar.
6. Para obter a configuração para dispositivos específicos, selecione o dispositivo individual. Para selecionar vários dispositivos para fazer backup, mantenha pressionada a tecla Ctrl. Clique em **Fazer backup**.

Dispositivos de importação

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

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

Por exemplo,

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

Em que:

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

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

Tabela 3. Exemplos de importação de dispositivo

Fabricante	Nome	Exemplo <Adapter::Name>,<IP Address>
Ponto de Verificação	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Dispositivo de Segurança Cisco	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Genérico	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

Importando um arquivo CSV

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

Antes de Iniciar

Se você importar uma lista de dispositivos e, em seguida, fazer uma alteração em um endereço IP no arquivo CSV, acidentalmente, será possível duplicar um dispositivo na lista Configuration Source Management. Por esse motivo, exclua um dispositivo do Configuration Source Management antes de importar a lista de dispositivos principais.

Procedimento

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

Resultados

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

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

Importação de dispositivo de resolução de problemas

Se uma mensagem de erro for recebida depois da tentativa de importação de um dispositivo, pode ser que a importação do arquivo CSV tenha falhado.

Importar um dispositivo pode falhar se a lista de dispositivos estiver estruturada incorretamente. Por exemplo, no arquivo CSV pode estar faltando dois pontos ou um comando, ou vários dispositivos podem estar em uma única linha.

Como alternativa, a importação poderá falhar se a lista de dispositivos contiver informações incorretas. Por exemplo, um erro tipográfico para um nome de adaptador.

Se a importação do dispositivo for interrompida, então nenhum dispositivo do arquivo CSV será incluído Configuration Source Management. Uma lista de nomes de adaptador válido para os adaptadores instalados é exibido na mensagem. Se um erro for exibido, então deve-se revisar seu arquivo CSV para corrigir quaisquer erros. É possível reimportar o arquivo após os erros serem corrigidos.

Capítulo 4. Gerenciar auditorias

O IBM Security QRadar Risk Manager ajuda a simplificar a avaliação das políticas de segurança de rede e os requisitos de conformidade, auxiliando o usuário na resolução de suas perguntas.

A auditoria de conformidade é uma tarefa necessária e complexa para os administradores de segurança. O QRadar Risk Manager ajuda a responder as questões a seguir:

- Como meus dispositivos de rede estão configurados?
- Como meus recursos de rede estão comunicando?
- Onde a minha rede é vulnerável?

Caso de uso: Auditoria de configuração

É possível utilizar as informações de configuração para dispositivos de rede, que são capturadas pelo QRadar Risk Manager, para conformidade de auditoria e para backups de configuração de planejamento.

Os backups de configuração fornecem um método centralizado e automático de mudanças do dispositivo de registro para a conformidade de auditoria. Os backups de configuração arquivam as mudanças na configuração e fornecem uma referência histórica; é possível capturar um registro histórico ou comparar uma configuração em relação a outro dispositivo de rede.

Auditoria de configuração no QRadar Risk Manager fornece as opções a seguir:

- Um registro histórico das configurações do seu dispositivo de rede.
- Uma visão normalizada, que exibe as mudanças do dispositivo quando as configurações são comparadas.
- Uma ferramenta para procurar regras no dispositivo.

As informações de configuração para seus dispositivos são coletadas a partir de backups de dispositivo no Configuration Source Management. Cada vez que o QRadar Risk Manager faz backup de sua lista de dispositivos, ele arquiva uma cópia da configuração do dispositivo para fornecer uma referência histórica. Quanto mais frequentemente o Configuration Source Management é planejado, mais registros de configuração o usuário tem para comparação e para referência histórica.

Visualizando o histórico de configuração do dispositivo

É possível visualizar o histórico de configuração de um dispositivo de rede.

Sobre Esta Tarefa

É possível visualizar as informações de histórico para os dispositivos de rede que foram submetidos a backup. Essas informações são acessíveis a partir da janela **Histórico** na página **Configuration Monitor**. A área de janela do histórico fornece informações sobre a configuração de um dispositivo de rede e a data em que a configuração do dispositivo foi submetida ao último backup utilizando o Configuration Source Management.

A configuração exibe o tipo dos arquivos que são armazenados para o seu dispositivo de rede no QRadar Risk Manager. Os tipos de configuração comuns são:

- **Standard-Element-Document** (SED), que são arquivos de dados XML que contêm informações sobre o dispositivo de rede. Os arquivos SED individuais são visualizados em seu formato XML bruto. Se um SED é comparado a outro arquivo SED, então a visualização é normalizada para exibir as diferenças de regras.
- **Config**, que são arquivos de configuração fornecidos por determinados dispositivos de rede. Esses arquivos dependem do fabricante do dispositivo. Um arquivo de configuração pode ser visualizado dando um clique duplo no arquivo de configuração.

Nota: Dependendo de seu dispositivo, vários outros arquivos de configuração podem ser exibidos. Dar um clique duplo nesses arquivos exibe o conteúdo em texto simples. A visualização de texto simples suporta localizar (Ctrl +f), colar (Ctrl+v) e as funções de cópia (Ctrl+C) a partir da janela do navegador da web.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Configuration Monitor**.
3. Clique duas vezes em uma configuração para visualizar as informações detalhadas do dispositivo.
4. Clique em **Histórico**.
5. Na área de janela **Histórico**, selecione uma configuração.
6. Clique em **Visualizar Selecionado**.

Comparando configurações de dispositivo para um dispositivo único

É possível comparar configurações do dispositivo para dispositivo único.

Sobre Esta Tarefa

Se os arquivos comparados são Standard-Elemento-Documentos (SEDs), então será possível visualizar as diferenças de regras entre os arquivos de configuração.

Ao comparar configurações normalizadas, a cor do texto indica as regras a seguir:

- Estrutura de tópicos com pontilhado verde indica uma regra ou configuração que foram incluídas ao dispositivo.
- Estrutura de tópicos com tracejado vermelho indica uma regra ou configuração que foram excluídas do dispositivo.
- Estrutura de tópicos com sólidos amarelos indica uma regra ou configuração que foram modificadas no dispositivo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Configuration Monitor**.
3. Clique duas vezes em qualquer dispositivo para visualizar as informações de configuração detalhadas.
4. Clique em **Histórico** para visualizar o histórico para este dispositivo.
5. Selecione uma configuração primária.

6. Pressione a tecla Ctrl e selecione uma segunda configuração para comparação.
7. Na área de janela **Histórico**, clique em **Comparar Selecionado**.
8. Opcional. Para visualizar as diferenças de configuração brutas, clique em **Visualizar Comparação Bruta**. Se a comparação é para um arquivo de configuração ou outro tipo de backup, então a comparação original é exibida.

Comparando configurações de dispositivo para dispositivos diferentes

É possível comparar duas configurações para dispositivos diferentes.

Sobre Esta Tarefa

Se os arquivos comparados são Standard-Elemento-Documentos (SEDs), então será possível visualizar as diferenças de regras entre os arquivos de configuração.

Ao comparar configurações normalizadas, a cor do texto indica as regras a seguir:

- Estrutura de tópicos com pontilhado verde indica uma regra ou configuração que foram incluídas ao dispositivo.
- Estrutura de tópicos com tracejado vermelho indica uma regra ou configuração que foram excluídas do dispositivo.
- Estrutura de tópicos com sólidos amarelos indica uma regra ou configuração que foram modificadas no dispositivo.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Configuration Monitor**.
3. Clique duas vezes em qualquer dispositivo para visualizar as informações de configuração detalhadas.
4. Clique em **Histórico** para visualizar o histórico para este dispositivo.
5. Selecione uma configuração primária.
6. Clique em **Marcar para Comparação**.
7. No menu de navegação, selecione **All Devices** para retornar para a lista de dispositivos.
8. Clique duas vezes no dispositivo para comparar, e clique em **Histórico**.
9. Selecione outro backup de configuração a ser comparado com a configuração marcada.
10. Clique em **Comparar com Marcado**.
11. Opcional. Para visualizar as diferenças de configuração brutas, clique em **Visualizar Comparação Bruta**. Se a comparação é para um arquivo de configuração ou outro tipo de backup, então a comparação original é exibida.

Caso de uso: Visualizar caminhos de rede na topologia

A topologia no QRadar Risk Manager exibe uma representação gráfica dos seus dispositivos de rede.

Uma procura de caminho de topologia pode determinar como seus dispositivos de rede estão se comunicando e o caminho de rede que eles utilizam para se comunicar. A procura pelo caminho permite que o QRadar Risk Manager exiba visivelmente o caminho entre uma origem e o destino, juntamente com as portas, protocolos e regras.

É possível visualizar como os dispositivos se comunicam, o que é importante em ativos de acesso seguro ou restrito.

Os recursos-chave incluem:

- Capacidade para visualizar comunicações entre os dispositivos em sua rede.
- Utilize os filtros para procurar a topologia para os dispositivos de rede.
- Rápido acesso para visualizar as regras e a configuração do dispositivo.
- Capacidade para visualizar eventos que são gerados a partir de um caminho de procura.

Procurando na topologia

É possível visualizar a comunicação do dispositivo procurando a topologia.

Sobre Esta Tarefa

Um caminho de procura é utilizado para filtrar o modelo de topologia. Um caminho de procura inclui todas as sub-redes que contêm os endereços IP de origem ou intervalos de CIDR e sub-redes que contêm endereços IP ou CIDR que também são permitidos para se comunicar utilizando o protocolo e porta configurados. A busca examina o modelo de topologia existente e inclui os dispositivos que estão envolvidos no caminho de comunicação entre a origem e o destino e as informações de conexão detalhadas.

É possível utilizar as vulnerabilidades para filtrar a procura se sua topologia incluir um Intrusion Prevention System (IPS). Para obter mais informações, consulte o *IBM Security QRadar Risk Manager Guia do Usuário*.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Topologia**.
3. Na caixa de listagem **Procurar**, selecione **Nova procura**.
4. Na área de janela **Critérios de Procura**, selecione **Caminho**.
5. No campo **IP/CIDR de Origem**, digite o endereço IP ou intervalo do CIDR nos quais você deseja filtrar o modelo de topologia. Separe as várias entradas utilizando uma vírgula.
6. No campo **IP/CIDR de Destino**, digite o endereço IP de destino ou intervalo do CIDR nos quais você deseja filtrar o modelo de topologia. Separe as várias entradas utilizando uma vírgula.
7. Opcional. Na lista **Protocolo**, selecione o protocolo que você deseja utilizar para filtrar o modelo de topologia.
8. Opcional. No campo **Porta de Destino**, digite a porta de destino na qual deseja filtrar o modelo de topologia. Separe várias portas utilizando uma vírgula.
9. Clique em **OK**.
10. Mova o mouse sobre uma linha de conexão para visualizar detalhes sobre a conexão. Se a procura se conectar a um dispositivo que contém regras, um link de regras de dispositivo é exibido no diálogo.

Caso de uso: Visualizar o caminho de ataque de uma ofensa

Ofensas no QRadar Risk Manager são eventos que são gerados pelo sistema para alertar sobre uma condição ou evento de rede.

A visualização do caminho de ataque vincula as ofensas com procuras de topologia. Esta visualização permite que os operadores de segurança visualizem os detalhes da ofensa e o caminho que a ofensa tomou através de sua rede. O caminho do ataque fornece uma representação visual. A representação visual mostra os ativos em sua rede que estão se comunicando para permitir que uma ofensa viaje através da rede. Estes dados são críticos durante a auditoria para provar a monitoração de ofensas, mas também demonstra que a ofensa não possui um caminho alternativo em sua rede para um ativo crítico.

Os recursos-chave para visualização são:

- Impulsionar a regra existente e o sistema de ofensas a partir do QRadar SIEM.
- Exibe um caminho visual para todos os dispositivos entre a origem e o destino da ofensa.
- Rápido acesso às configurações de dispositivo e regras que permitem que a ofensa.

Visualizando o caminho do ataque de uma ofensa

É possível visualizar o caminho de ataque de uma ofensa. O caminho de ataque mostra a origem, destino e os dispositivos associados.

Procedimento

1. Clique na guia **Ofensas**.
2. No menu de navegação, clique em **Todas ofensas**. A página **Todas as Ofensas** exibe uma lista de ofensas que estão em sua rede. As ofensas são listadas com a magnitude mais alta primeiro.
3. Clique duas vezes em uma ofensa para abrir o seu resumo.
4. Na barra de ferramentas **Ofensas**, clique em **Visualizar Caminho de Ataque**.

Capítulo 5. Caso de uso: Políticas do monitor

A auditoria de política e o controle de mudança são processos fundamentais que permitem que os administradores e profissionais de segurança controlem o acesso e as comunicações entre os ativos de negócios críticos.

Os critérios para monitoramento de política podem incluir monitoramento de ativos e de comunicações para os seguintes cenários:

- Minha rede contém ativos com configurações de risco para auditorias da Seção 1 do PCI?
- Meus ativos não permitem comunicações utilizando protocolos de risco para auditorias da Seção 10 do PCI?
- Como posso saber quando uma mudança de política coloca a minha rede em violação?
- Como eu visualizo vulnerabilidades para ativos de alto risco ou mais resistentes?
- Como eu visualizo os ativos na rede com as vulnerabilidades e acesso à Internet?

Utilize o Policy Monitor para definir testes que são baseados no indicadores de risco, depois, restrinja os resultados do teste para filtrar a consulta para resultados, violações, protocolos ou vulnerabilidades específicos.

O IBM Security QRadar Risk Manager inclui várias questões do Policy Monitor que estão agrupados por categoria do PCI. Por exemplo, as questões do PCI 1, PCI 6 e PCI 10. As questões podem ser criadas para ativos ou dispositivos e regras para expor o risco de segurança da rede. Após uma questão sobre um ativo ou um dispositivo/regra ser submetida ao Policy Monitor, os resultados retornados especificam o nível de risco. É possível aprovar os resultados que são retornados de ativos ou definir como você quer que o sistema responda aos resultados não aprovados.

O Policy Monitor fornece os seguintes recursos-chave:

- Questões predefinidas do Policy Monitor para ajudar com o fluxo de trabalho.
- Determina se os usuários usaram protocolos proibidos para se comunicar.
- Avaliar se os usuários em redes específicas podem se comunicar com redes ou ativos proibidos.
- Avaliar se as regras de firewall atendem à política corporativa.
- Monitoramento contínuo de políticas que geram ofensas ou alertas aos administradores.
- Prioriza as vulnerabilidades avaliando quais sistemas podem estar comprometidos como resultado da configuração do dispositivo.
- Ajuda a identificar problemas de conformidade.

Caso de uso: Avaliar ativos que possuem configurações suspeitas

As organizações utilizam políticas de segurança corporativa para definir os riscos e as comunicações que são permitidas entre os ativos e redes. Para ajudar com conformidade e violações de políticas corporativas, as organizações utilizam o Policy Monitor para avaliar e monitorar os riscos que podem ser desconhecidos.

A conformidade do PCI ordena que os dispositivos que contêm dados do titular do cartão sejam identificados, em seguida, faça diagramas, verifique comunicações e monitore as configurações de firewall para proteger os ativos que contêm dados sensíveis. O Policy Monitor fornece métodos para atender estes requisitos rapidamente e permite aos administradores aderir às políticas corporativas. Os métodos comuns de redução de riscos incluem a identificação e monitoramento de ativos que se comunicam com os protocolos descobertos. Estes protocolos são roteadores, firewalls, ou comutadores que permitem conexões telnet ou FTP. Utilize o Policy Monitor para identificar ativos em sua topologia com configurações de risco.

Questões da seção 1 do PCI podem incluir os critérios a seguir:

- Ativos que permitem protocolos proibidos.
- Ativos que permitem protocolos de risco.
- Ativos que permitem aplicativos fora da política através da rede.
- Ativos que permitem aplicativos fora da política para redes que contêm ativos protegidos.

Avaliando os dispositivos que permitem os protocolos de risco

Utilize o Policy Monitor para avaliar os dispositivos que permitem os protocolos de risco.

Sobre Esta Tarefa

O QRadar Risk Manager avalia uma questão e exibe os resultados de quaisquer ativos, em sua topologia, que correspondem à questão de teste. Os profissionais de segurança, administradores ou auditores em sua rede podem aprovar comunicações que não são um risco para ativos específicos. Eles também podem criar ofensas para o comportamento.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Policy Monitor**.
3. Na caixa de listagem Grupo, selecione **PCI 1**.
4. Selecione a questão **Avalia quaisquer dispositivos (por exemplo, firewalls) que permitem os protocolos de risco (respectivamente, telnet e FTP – de tráfego de porta 21 e 23) a partir da Internet ao DMZ**.
5. Clique em **Enviar Questão**.

Caso de uso: Avaliar ativos com comunicação suspeita

Use o Policy Monitor para identificar a conformidade com a seção 10 do PCI ao rastrear, criar logs e exibir o acesso aos ativos de rede.

O QRadar Risk Manager pode ajudar a identificar a conformidade com a seção 10 do PCI identificando ativos na topologia que permitem comunicações que envolvam dúvidas ou riscos. O QRadar Risk Manager podem examinar esses ativos para comunicações possíveis ou reais. As comunicações reais exibem ativos que usaram os critérios de sua questão para se comunicar. As comunicações possíveis exibem ativos que podem usar os critérios de sua questão para se comunicar.

As questões da seção 10 do PCI podem incluir os critérios a seguir:

- Ativos que permitem questões de entrada para redes internas.
- Ativos que se comunicam a partir de locais não confiáveis para locais confiáveis.
- Ativos que se comunicam a partir de uma VPN para locais confiáveis.
- Ativos que permitem protocolos fora da política não criptografados dentro de um local confiável.

Localizar recursos que permitem a comunicação

É possível localizar recursos que permitem a comunicação a partir da Internet.

Sobre Esta Tarefa

O QRadar Risk Manager avalia a questão e exibe os resultados de quaisquer ativos internos que permitam conexões de entrada a partir da Internet. Os profissionais de segurança, administradores ou auditores em sua rede podem aprovar comunicações para ativos que não são considerados seguros ou que contêm dados do cliente. Conforme mais eventos são gerados, será possível criar ofensas no QRadar SIEM para monitorar esse tipo de comunicação de risco.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Policy Monitor**.
3. Na caixa de listagem Grupo, selecione **PCI 10**.
4. Selecione a questão de teste **Avalie quaisquer conexões de entrada a partir da Internet para qualquer lugar na rede interna**.
5. Clique em **Enviar Questão**.

Caso de uso: Monitorar políticas para violações

O QRadar Risk Manager pode monitorar continuamente questões predefinidas ou geradas por usuários no Policy Monitor. É possível utilizar o monitor mode para gerar eventos no QRadar Risk Manager.

Quando uma questão a ser monitorada é selecionada, o QRadar Risk Manager analisa a questão em relação a sua topologia a cada hora para determinar se um ativo ou uma mudança de regra geram um resultado não aprovado. Se o QRadar Risk Manager detecta um resultado não aprovado, uma ofensa pode ser gerada para alertar sobre um desvio na sua política definida. No monitor mode, o QRadar Risk Manager pode monitorar simultaneamente os resultados de 10 questões.

O monitoramento de questões fornece os recursos principais a seguir:

- Monitorar para alterações de regra ou ativo por hora para resultados não aprovados.
- Usar sua categoria de evento de alto e baixo níveis para categorizar resultados não aprovados.
- Gerar ofensas, emails, mensagens syslog ou notificações de painel sobre resultados não aprovados.
- Usar visualização de evento, correlação, geração de relatórios do evento, regras customizadas e painéis no QRadar SIEM.

Configurando uma questão

É possível utilizar o Policy Monitor para configurar uma questão a ser monitorada.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Policy Monitor**.
3. Selecione a questão que você deseja monitorar.
4. Clique em **Monitor**.
5. Configure qualquer uma das opções necessárias para monitorar sua questão.
6. Clique em **Salvar Monitor**.

Resultados

O monitoramento é ativado para a questão e os eventos ou para ofensas que são gerados com base em seus critérios de monitoramento.

Caso de uso: Use as vulnerabilidades para priorizar riscos

As vulnerabilidades expostas são um fator de risco significativo para os ativos de rede.

O QRadar Risk Manager utiliza informações de ativo e informações de vulnerabilidade no Policy Monitor. Essas informações são utilizadas para determinar se os ativos estão suscetíveis a ataques do tipo de entrada, como; injeção SQL, campos ocultos e clickjacking.

Vulnerabilidades que são detectadas em seus ativos podem ser priorizadas por seu local de rede ou uma conexão com outro dispositivo que esteja vulnerável.

Questões sobre o ativo vulnerabilidade podem incluir os critérios a seguir:

- Ativos com novas vulnerabilidades relatadas após uma data específica.
- Ativos com as vulnerabilidades específicas ou pontuação do CVSS.
- Ativos com uma classificação específica de vulnerabilidade, como manipulação de entrada, negação de serviço, OSVDB verificado.

Localizando ativos que possuem vulnerabilidades

É possível localizar recursos que possuem vulnerabilidades.

Sobre Esta Tarefa

O QRadar Risk Manager avalia uma questão e exibe os resultados de ativos que contêm a vulnerabilidade. Os profissionais de segurança, administradores ou os auditores podem identificar recursos em sua rede que contêm as vulnerabilidades de injeção SQL conhecidas. Eles podem corrigir imediatamente qualquer ativo conectado a uma rede protegida. À medida que mais eventos são gerados, é possível criar eventos ou ofensas no QRadar SIEM para monitorar ativos que contêm vulnerabilidades de injeção de SQL.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Policy Monitor**.
3. Na lista **Grupo**, selecione **Vulnerabilidade**.
4. Selecione a questão de teste **Avaliar ativos com vulnerabilidades de injeção SQL em localnet(s) específico(s) (por exemplo, rede do servidor protegido)**.
5. Clique em **Enviar Questão**.

Caso de uso: Priorizar vulnerabilidades de ativos por zona ou comunicação de rede

Sistemas com vulnerabilidades na mesma rede que os ativos protegidos estão em um maior risco de perda de dados.

Detectar vulnerabilidades em ativos por zona ou rede são medidas fundamentais para evitar explorações antes que elas ocorram em sua rede. As seções 6.1 e 6.2 do PCI determinam que você revise e corrija os sistemas no prazo de um mês de uma liberação de correção de vulnerabilidade. O QRadar Risk Manager ajuda a automatizar e priorizar o processo de correção. Como as vulnerabilidades são detectadas em seus ativos, é possível priorizar pelo local de rede ou por uma conexão com outro dispositivo que seja vulnerável. Priorizar é importante para as redes seguras que podem ser conectadas a regiões suspeitas, ou ativos que contêm uma pontuação CVSS maior do que a sua política interna permite.

As questões de ativos vulneráveis podem incluir os critérios a seguir:

- Ativos com uma vulnerabilidade do lado do cliente, que comunicou regiões geográficas suspeitas e contêm ativos protegidos.
- Ativos com vulnerabilidades de negação de serviço em uma rede específica.
- Ativos com vulnerabilidades de correio em uma rede específica.
- Ativos com vulnerabilidades e a pontuação específica do Common Scoring Vulnerabilidade do Sistema (CVSS).

Localizando ativos que possuem vulnerabilidades em uma rede

É possível localizar ativos que possuem vulnerabilidades em uma rede específica.

Sobre Esta Tarefa

O QRadar Risk Manager avalia a questão e exibe os resultados no local específico que contém as vulnerabilidades específicas do S.O. Os profissionais de segurança, administradores ou auditores de sua rede podem aprovar comunicações para ativos que não são considerados seguros ou que contém dados do cliente. Conforme mais eventos são gerados, é possível criar ofensas para monitorar esse tipo de comunicação de risco.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, clique em **Policy Monitor**.
3. A partir da caixa de listagem **Grupo**, selecione **Vulnerabilidade**.
4. Selecione a questão de teste **Avaliar ativos com vulnerabilidades específicas do S.O. em localnet(s) específico(s)**.
5. Clique em **Enviar Questão**.

Capítulo 6. Casos de uso para simulações

Caso de uso: Simular ataques nos ativos de rede

É possível utilizar uma simulação para testar sua rede para vulnerabilidades a partir de várias origens.

É possível utilizar simulações de ataque para auditar as configurações do dispositivo em sua rede.

As simulações fornecem os recursos-chave a seguir:

- Exibem as permutações do caminho teórico em um ataque que pode ser executado contra sua rede.
- Exibem como os ataques podem propagar através dos seus dispositivos de rede para se espalhar para outros ativos.
- Permitem o monitoramento para detectar novos sites exposição.

Criando uma Simulação

É possível criar uma simulação para um ataque de rede em um protocolo SSH.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Na lista **Ações** , selecione **Nova**.
4. Digite um nome para a simulação.
5. Selecione **Topologia Atual**.
6. Selecione a caixa de seleção **Utilizar Conexão de Dados**.
7. Na lista **Onde você quer que a simulação inicie**, selecione uma origem para a simulação.
8. Inclua o ataque de simulação, **Ataque os destinos de uma das seguintes portas abertas utilizando protocolos**.
9. Para esta simulação, clique em **abrir portas** e, em seguida, inclua a porta 22.
10. Clique em **protocolos** e, em seguida, selecione **TCP**. O SSH utiliza o TCP.
11. Clique em **OK**.
12. Clique em **Salvar Simulação**.
13. Na lista **Ações**, selecione **Executar Simulação**. A coluna de resultados contém uma lista com a data em que a simulação foi executada e um link para visualizar os resultados.
14. Clique em **Visualizar Resultados**.

Resultados

Uma lista de ativos que contêm as vulnerabilidades SSH será exibida nos resultados, permitindo que os administradores de rede aprovem as conexões SSH que são permitidas ou esperadas em sua rede. As comunicações que não são aprovadas podem ser monitoradas para eventos ou ofensas.

Os resultados que são exibidos fornecem a seus administradores de rede ou profissionais de segurança uma representação visual do caminho de ataque e as conexões que o ataque poderia tomar em sua rede. Por exemplo, a primeira etapa fornece uma lista dos ativos diretamente conectados pela simulação. A segunda etapa lista ativos em sua rede que podem se comunicar com ativos de primeiro nível em sua simulação.

As informações fornecidas no ataque permite reforçar e testar a sua rede contra milhares de cenários de ataque possíveis.

Caso de uso: Simule o risco de mudanças da configuração de rede

É possível utilizar um modelo de topologia para definir modelos de rede virtual com base em sua rede existente. É possível criar um modelo de rede baseado em uma série de modificações que podem ser combinadas e configuradas.

É possível utilizar um modelo de topologia para determinar o efeito das mudanças na configuração em sua rede utilizando uma simulação.

Modelos de topologia fornecem as seguintes principais funcionalidades:

- Criar topologias virtuais para testar as mudanças da rede.
- Simular ataques contra redes virtuais.
- Menor risco e exposição aos ativos protegido através de teste.
- Os segmentos de rede virtual permitem confinar e testar partes sensíveis da rede ou dos recursos.

Para simular uma mudança na configuração de rede:

1. Criar um modelo de topologia.
2. Simular um ataque contra o modelo de topologia.

Criando um modelo de topologia

É possível criar um modelo de topologia para testar as alterações de rede e simular ataques.

Procedimento

1. Clique na guia **Riscos** .
2. No menu de navegação, selecione **Simulações** > **Modelos de Topologia**.
3. Na lista **Ações** , selecione **Nova**.
4. Digite um nome para o modelo.
5. Selecione quaisquer modificações que deseja aplicar na topologia.
6. Configure os testes incluídos na área de janela **Configurar modelo como segue** .
7. Clique em **Salvar Modelo**.

O que Fazer Depois

Crie uma simulação para seu novo modelo de topologia.

Simulando um ataque

É possível simular um ataque nas portas e protocolos.

Procedimento

1. Clique na guia **Riscos**.
2. No menu de navegação, selecione **Simulação** > **Simulações**.
3. Na caixa de lista **Ações**, selecione **Nova**.
4. Digite um nome para a simulação.
5. Selecione um modelo de topologia criado.
6. Na lista **Onde você quer que a simulação inicie**, selecione uma origem para a simulação.
7. Inclua o ataque de simulação, **Ataque os destinos de uma das seguintes portas abertas utilizando protocolos**.
8. Para esta simulação, clique em **abrir portas** e, em seguida, inclua a porta 22.
9. Clique em **protocolos**, e então selecione TCP. O SSH utiliza o TCP.
10. Clique em **OK**.
11. Clique em **Salvar Simulação**.
12. Na lista **Ações**, selecione **Executar Simulação**. A coluna de resultados contém uma caixa de listagem com a data em que a simulação foi executada e um link para visualizar os resultados.
13. Clique em **Visualizar Resultados**.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA.

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 se 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 dessa publicação não concede ao Cliente nenhuma licença para essas patentes. É possível enviar consultas sobre licença, 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:

Licenciamento de Propriedade Intelectual
Lei de Propriedade Intelectual e Jurídica
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 NÃO SE LIMITANDO A, 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.

Estas informações podem conter 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 websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e o uso 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.

Os licenciados deste programa que desejarem obter informações sobre ele com a finalidade de: (i) trocar informações entre programas criados independentemente e outros programas (inclusive este) e (ii) uso mútuo de informações que tenham sido trocadas, devem entrar em contato com:

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

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

O programa licenciado descrito nesta publicação e todo 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.

Todos os dados sobre desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem divergir de maneira significativa. Algumas medidas podem ter sido tomadas em sistemas de 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 relativas a produtos não IBM foram obtidas dos fornecedores desses produto, de seus anúncios publicados ou de outras fontes publicamente disponíveis. 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 relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento 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 alteração sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios usados em operações comerciais diárias. Para ilustrá-los da forma mais completa possível, os exemplos contam com nomes de pessoas, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com nomes e endereços usados por uma empresa real é totalmente coincidência.

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

Marcas Comerciais

A 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 indicarão marcas registradas ou de direito consuetudinário dos Estados Unidos, de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou marcas comerciais de direito consuetudinário em outros países. Uma lista atual de marcas registradas da IBM está disponível na web em Informações de copyright e de marca registrada (www.ibm.com/legal/copytrade.shtml).

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

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

Considerações sobre 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 sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, ajustar as interações com o usuário final ou para outras finalidades. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de software. Algumas de nossas Ofertas de software podem ajudar você a coletar as informações de identificação pessoal. Se esta Oferta de software usar cookies para coletar as informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies desta oferta serão apresentadas a seguir.

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

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.

Índice Remissivo