IBM Security QRadar Vulnerability Manager
Versão 7.2.5

Guia do Usuário

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 95.

Informações do produto

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

Índice

Introdução ao IBM Security QRadar Vulnerability Manager

Estas informações são destinadas ao uso com o IBM® Security QRadar Vulnerability Manager. O QRadar Vulnerability Manager é uma plataforma de varredura usada para identificar, gerenciar e priorizar vulnerabilidades nos ativos de rede.

Este guia contém instruções para configurar e usar o QRadar Vulnerability Manager em um IBM Security QRadar SIEM ou em um console do IBM Security QRadar Log Manager.

Público desejado

Os administradores do sistema responsáveis pela configuração do IBM Security QRadar Vulnerability Manager devem ter acesso administrativo ao IBM Security QRadar SIEM e aos dispositivos e firewalls de rede. O administrador do sistema deve ter conhecimento da rede corporativa e de tecnologias de rede.

Documentação técnica

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

Entrando em contato com o suporte ao cliente

Para obter informações sobre como contatar o suporte ao cliente, consulte Suporte e download da nota técnica (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mal uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança pode ser completamente efetivo(a) na prevenção de uso ou acesso impróprios. Os sistemas, produtos e serviços da IBM foram projetados para serem parte de uma abordagem de segurança abrangente, que envolverá, necessariamente, procedimentos operacionais adicionais e podem precisar de outros sistemas, produtos ou serviços para ser mais efetiva. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS SEJAM IMUNES OU TORNEM SUA EMPRESA IMUNE CONTRA A CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

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

O IBM Security QRadar Vulnerability Manager V7.2.5 introduz suporte para a sobreposição de endereços IP em redes que têm vários domínios. Ele também inclui aprimoramentos na retenção e remoção de dados de vulnerabilidade, um novo item de painel do feed RSS e muito mais.

Sobreposição de IPs e suporte de domínio

Use os recursos do QRadar Vulnerability Manager que funcionam com domínios para assegurar que os ativos que têm o mesmo endereço IP em deres diferentes não sejam confundidos durante a varredura. Saiba mais...

Configurar períodos de retenção de vulnerabilidades e dos resultados de varreduras

Configure o período de retenção para os dados de tendências de vulnerabilidade e os resultados da varredura, para que os dados não necessários sejam removidos regularmente do sistema. Saiba mais...

Remover dados de vulnerabilidade indesejados

Use os recursos de limpeza de vulnerabilidades do QRadar Vulnerability Manager para remover dados de vulnerabilidade antigos do modelo de ativo. Saiba mais...

Feeds RSS

Use o item de painel **Feeds RSS** para ver as mais recentes notícias de segurança, recomendações e informações sobre o andamento e a conclusão de varreduras. Saiba mais...

Estender o período de licença temporária do QRadar Vulnerability Manager

Quando a licença temporária do QRadar Vulnerability Manager expirar, use o ícone **Gerenciador de Vulnerabilidade** na guia **Administrador** para estendê-la por mais quatro semanas Saiba mais...

Capítulo 2. Instalações e Implementações do QRadar Vulnerability Manager

É possível acessar o IBM Security QRadar Vulnerability Manager usando a guia **Vulnerabilidades**.

Acesso à Guia Vulnerabilidades

Dependendo do produto instalado e se você fizer upgrade do QRadar ou instalar um novo sistema, a guia **Vulnerabilidades** não poderá ser exibida.

- Se você instalar o QRadar SIEM, por padrão, a guia **Vulnerabilidades** será ativada com uma chave de licença temporária.
- Se você instalar o QRadar Log Manager, a guia **Vulnerabilidades** não será ativada.
- Dependendo de como você fizer upgrade do QRadar, a guia **Vulnerabilidades** poderá não ser ativada.

Para usar o QRadar Vulnerability Manager após uma instalação ou upgrade, você deve fazer upload e alocar uma chave de licença válida. Para obter mais informações, consulte o *Guia de Administração* para o produto.

Para obter mais informações sobre como fazer upgrade, consulte o *IBM Security QRadar Upgrade Guide*.

Processamento de Vulnerabilidade e Implementações de Varredura

Ao instalar e licenciar QRadar Vulnerability Manager, um processador de vulnerabilidade será automaticamente implementado no console do QRadar. Um processador não será implementado automaticamente, se você usar uma chave de ativação de software no console do QRadar.

Por padrão, o processador de vulnerabilidade fornece um componente de varredura. Se necessário, você poderá implementar mais scanners, nos dispositivos de scanner do host gerenciado do QRadar Vulnerability Manager dedicado ou nos hosts gerenciados do QRadar. Por exemplo, é possível implementar um scanner de vulnerabilidade em um Coletor de eventos ou em um QRadar QFlow Collector. Não é possível implementar um scanner de vulnerabilidade em um host gerenciado de alta disponibilidade.

Se necessário, você poderá mover o processador de vulnerabilidade para um host gerenciado diferente na implementação. É possível mover o processador para preservar espaço em disco no console do QRadar.

Restrição: É possível ter apenas um processador de vulnerabilidade na implementação. O processador de vulnerabilidade pode ser movido apenas para um dispositivo de processador dedicado do QRadar Vulnerability Manager.

Importante: Após alterar a implementação do processador de vulnerabilidade, você deverá aguardar a implementação ser totalmente configurada. Na página Perfis de Varredura, a mensagem a seguir é exibida: **QVM está no processo de ser implementada**.

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) versão 1.7 ou IBM Runtime Environment 64 bits for Java V7.0
- Adobe Flash versão 10.x

Conceitos relacionados:

"Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager" na página 8
Se você tiver uma grande rede e requerer opções flexíveis de varredura, poderá incluir mais scanners na implementação do IBM Security QRadar Vulnerability Manager.

"Opções para Mover o Processador de Vulnerabilidade na Implementação do QRadar Vulnerability Manager" na página 5
Se necessário, é possível mover o processador de vulnerabilidade do console do QRadar para um dispositivo do host gerenciado do QRadar Vulnerability Manager aplicado.

Processador de Vulnerabilidade e Chaves de Ativação de Dispositivo de Scanner

É possível varrer e processar as vulnerabilidades usando dispositivos de host gerenciado do QRadar Vulnerability Manager dedicado.

Ao instalar um processador ou scanner no dispositivo de host gerenciado, você deverá digitar uma chave de ativação válida.

Para obter mais informações sobre como instalar um dispositivo de host gerenciado, consulte o *Guia de Instalação* para o produto.

A chave de ativação é uma sequência alfanumérica de 24 dígitos e quatro partes, recebida da IBM. A chave de ativação especifica quais módulos de software aplicam-se a cada tipo de dispositivo:

- O dispositivo do processador QRadar Vulnerability Manager inclui o processamento de vulnerabilidade e componentes de varredura.
- O dispositivo de scanner QRadar Vulnerability Manager inclui apenas um componente de vulnerabilidade.

É possível obter a chave de ativação a partir dos locais a seguir:

- Se você tiver adquirido um software do QRadar Vulnerability Manager ou tiver feito download do dispositivo virtual, uma lista de chaves de ativação será incluída no documento *Introdução* anexado em um email de confirmação. É possível usar este documento para referência cruzada do número de peça para o dispositivo com o qual você é equipado.
- Se você tiver adquirido um dispositivo que é pré-instalado com o software do QRadar Vulnerability Manager, a chave de ativação será incluída na caixa de remessa ou no CD.

Backup e Recuperação de Vulnerabilidade

É possível fazer backup e recuperar seus dados de vulnerabilidade, incluindo as configurações de vulnerabilidade. Por exemplo, é possível fazer backup de perfis de varredura.

O backup e a recuperação de QRadar Vulnerability Manager são gerenciados usando a guia **Admin**.

Para obter mais informações sobre o backup e a recuperação de vulnerabilidade, consulte o *Guia de Administração* para o produto.

Opções para Mover o Processador de Vulnerabilidade na Implementação do QRadar Vulnerability Manager

Se necessário, é possível mover o processador de vulnerabilidade do console do QRadar para um dispositivo do host gerenciado do QRadar Vulnerability Manager aplicado.

Por exemplo, você pode mover a capacidade de processamento de vulnerabilidade de um host gerenciado para minimizar o impacto no espaço em disco no console do QRadar.

Restrição: É possível ter apenas um processador de vulnerabilidade na implementação. Além disso, você deve implementar o processador de vulnerabilidade apenas em um console do QRadar ou em um dispositivo do processador do host gerenciado do QRadar Vulnerability Manager.

Para mover o processador de vulnerabilidade, escolha uma das opções a seguir:

Opção 1: Implemente um dispositivo de processador dedicado doQRadar Vulnerability Manager

Para implementar um dispositivo do processador você deve concluir as tarefas a seguir:

1. Instale um dispositivo de processador dedicado do QRadar Vulnerability Manager.
2. Inclua o dispositivo de processador do host gerenciado no Console do QRadar, usando a ferramenta **Gerenciamento de Sistema e de Licença** na guia Administrador.

   Ao selecionar a opção de host gerenciado, o processador é automaticamente removido do console do QRadar.

Opção 2: Mova o processador de vulnerabilidade de seu console para seu host gerenciado

Se o processador de vulnerabilidade estiver no console do QRadar, posteriormente, é possível mover o processador de vulnerabilidade para um dispositivo do processador do host gerenciado do QRadar Vulnerability Manager instalado anteriormente.

A qualquer momento, é possível mover o processador de vulnerabilidade de volta ao console do QRadar.

Implementando um Dispositivo do Processador QRadar Vulnerability Manager Dedicado

É possível implementar um dispositivo de processador dedicado do QRadar Vulnerability Manager como um host gerenciado.

Ao implementar o processador de vulnerabilidade em um host gerenciado, todas as vulnerabilidades serão processadas no host gerenciado.

Restrição: Após implementar o processamento em um host gerenciado do QRadar Vulnerability Manager dedicado, os perfis de varredura ou resultados de varredura associados a um processador do console do QRadar não serão exibidos. É possível continuar a procurar e visualizar dados de vulnerabilidade nas páginas **Gerenciar Vulnerabilidades**.

Antes de Iniciar

Assegure-se de que um host gerenciado do QRadar Vulnerability Manager dedicado esteja instalado e que uma chave de ativação do dispositivo do processador válido seja aplicada. Para obter mais informações, consulte o *Guia de Instalação* para o produto.

Procedimento

1. Efetue login no Console do QRadar como um administrador:

   `https://IP_Address_QRadar`

   O nome de usuário padrão é `admin`. A senha é a senha da conta do usuário raiz que foi digitada durante a instalação.
2. Clique na guia **Admin**.
3. Na área de janela **Configuração do Sistema**, clique em **Gerenciamento de Sistema e de Licença**.
4. Na tabela de host, clique no host do Console do QRadar e clique em > **Ações de Implementação** > **Incluir Host**.
5. Insira o endereço IP do Host e a senha.
6. Clique em **Incluir**.
7. Feche a janela Gerenciamento de Sistema e de Licença.
8. Na barra de ferramentas da guia **Administrador**, clique em **Avançado** > **Implementar Configuração Integral**.
9. Clique em **OK**.

Conceitos relacionados:

"Processador de Vulnerabilidade e Chaves de Ativação de Dispositivo de Scanner" na página 4
É possível varrer e processar as vulnerabilidades usando dispositivos de host gerenciado do QRadar Vulnerability Manager dedicado.

Tarefas relacionadas:

"Verificando Se Um Processsador de Vulnerabilidade Está Implementado" na página 7
No IBM Security QRadar Vulnerability Manager, é possível verificar se o processador de vulnerabilidade está implementado em um console do QRadar ou em um host gerenciado do QRadar Vulnerability Manager.

Movendo o Processador de Vulnerabilidade para um Console ou Host Gerenciado

Se necessário, é possível mover o processador de vulnerabilidade entre um dispositivo do host gerenciado do QRadar Vulnerability Manager e o console do QRadar.

Antes de Iniciar

Assegure-se de que um host gerenciado do QRadar Vulnerability Manager dedicado esteja instalado e que uma chave de ativação do dispositivo do processador válido seja aplicada.

Procedimento

1. Na guia **Administrador**, clique em **Gerenciamento do Sistema e de Licença** > **Ações de Implementação** > **Gerenciar Implementação de Vulnerabilidade**.
2. Clique em **Ativar Processador**.
3. Selecione um host gerenciado ou console na lista **Processadores**.

   Se o processador estiver no host gerenciado, você poderá selecionar apenas o console do QRadar.
4. Clique em **Salvar**.
5. Na barra de ferramentas da guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
6. Clique em **OK**.

Conceitos relacionados:

"Processador de Vulnerabilidade e Chaves de Ativação de Dispositivo de Scanner" na página 4
É possível varrer e processar as vulnerabilidades usando dispositivos de host gerenciado do QRadar Vulnerability Manager dedicado.

Verificando Se Um Processsador de Vulnerabilidade Está Implementado

No IBM Security QRadar Vulnerability Manager, é possível verificar se o processador de vulnerabilidade está implementado em um console do QRadar ou em um host gerenciado do QRadar Vulnerability Manager.

Procedimento

1. Efetue login no console do QRadar.
2. Na guia **Administrador**, clique em **Gerenciamento do Sistema e de Licença** > **Ações de Implementação** > **Gerenciar Implementação de Vulnerabilidade**.
3. Verifique se o processador é exibido na lista **Processador**.

Removendo Um Processador de Vulnerabilidade do Console ou do Host Gerenciado

Se necessário, é possível remover o processador de vulnerabilidade de um console do QRadar ou de um host gerenciado do QRadar Vulnerability Manager.

Procedimento

1. Efetue login no console do QRadar.
2. Na guia **Administrador**, clique em **Gerenciamento de Sistema e de Licença** > **Ações de Implementação** > **Gerenciamento de Implementação de Vulnerabilidade**.
3. Clique na caixa de seleção **Ativar Processador** para desmarcá-la.
4. Clique em **Remover**.
5. Clique em **Salvar**.
6. Feche a janela Gerenciamento de Sistema e de Licença.

7. Na barra de ferramentas da guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
8. Clique em **OK**.

Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager

Se você tiver uma grande rede e requerer opções flexíveis de varredura, poderá incluir mais scanners na implementação do IBM Security QRadar Vulnerability Manager.

O processador do QRadar Vulnerability Manager é implementado automaticamente com um componente de varredura. Implementando mais scanners é possível aumentar a flexibilidade das operações de varredura. Por exemplo, é possível varrer áreas específicas da rede com scanners diferentes e em horários planejados diferentes.

Varreduras de Vulnerabilidade Dinâmica

Os scanners de vulnerabilidades implementados podem não ter acesso a todas as áreas de sua rede. No QRadar Vulnerability Manager, é possível designar diferentes scanners para intervalos CIDR de rede. Durante uma varredura, cada recurso do intervalo de CIDR que você desejar varrer será associado dinamicamente com o scanner correto.

Para incluir mais scanners de vulnerabilidade, escolha qualquer uma das opções a seguir:

Implemente um dispositivo de scanner do host gerenciado dedicado QRadar Vulnerability Manager

É possível varrer vulnerabilidades usando um dispositivo de scanner do host gerenciado do QRadar Vulnerability Manager dedicado.

Para implementar um dispositivo de scanner, você deve concluir as tarefas a seguir:

1. Instalar um dispositivo de scanner do host gerenciado do QRadar Vulnerability Manager dedicado.
2. Inclua o dispositivo de scanner do host gerenciado no Console do QRadar, usando a ferramenta **Gerenciamento de Sistema e de Licença** na guia **Administrador**.

Implemente um scanner do QRadar Vulnerability Manager em seu console QRadar ou host gerenciado

Se você mover o processador de vulnerabilidade do console do QRadar para um host gerenciado do QRadar Vulnerability Manager, poderá incluir um scanner no console.

Também é possível incluir um scanner de vulnerabilidade em quaisquer hosts gerenciados QRadar pré-existentes em sua implementação. Por exemplo, é possível incluir um scanner em um coletor de eventos, coletor de fluxo ou processador de eventos.

Restrição: Não é possível incluir um scanner de vulnerabilidade em um host gerenciado de alta disponibilidade.

Configure o acesso a um scanner hospedado pela IBM e verifique a DMZ
É possível configurar o acesso a um scanner hospedado pela IBM e verificar os ativos na DMZ.

Conceitos relacionados:

"Varreduras de Vulnerabilidade Dinâmica" na página 53
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura para usar determinados scanners de vulnerabilidade para intervalos de CIDR específicos de sua rede. Por exemplo, os scanners podem ter acesso apenas a determinadas áreas da rede.

Tarefas relacionadas:

"Associando Scanners de Vulnerabilidades com Intervalos de CIDR" na página 54
No IBM Security QRadar Vulnerability Manager, para executar varredura dinâmica, deve-se associar os scanners de vulnerabilidade com diferentes segmentos de sua rede.

"Varrendo Intervalos de CIDR com Diferentes Scanners de Vulnerabilidade" na página 54
No IBM Security QRadar Vulnerability Manager, é possível varrer áreas da rede com diferentes scanners de vulnerabilidade.

Implementando Um Dispositivo de Scanner do QRadar Vulnerability Manager Dedicado

É possível implementar um dispositivo de scanner do host gerenciado do QRadar Vulnerability Manager dedicado.

Antes de Iniciar

Assegure-se de que um dispositivo de scanner do host gerenciado do QRadar Vulnerability Manager dedicado esteja instalado e que uma chave de ativação do dispositivo válido seja aplicada.

Procedimento

1. Na guia **Administrador**, clique em **Gerenciamento de Sistema e de Licença** > **Ações de Implementação** > **Incluir Host Gerenciado**.
2. Digite o endereço IP e a senha do dispositivo de scanner do host gerenciado do QRadar Vulnerability Manager.
3. Clique em **Incluir**.
   Você deve aguardar alguns minutos enquanto o host gerenciado é incluído.
4. Feche a janela Gerenciamento de Sistema e de Licença.
5. Na barra de ferramentas da guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
6. Clique em **OK**.

Conceitos relacionados:

"Processador de Vulnerabilidade e Chaves de Ativação de Dispositivo de Scanner" na página 4
É possível varrer e processar as vulnerabilidades usando dispositivos de host gerenciado do QRadar Vulnerability Manager dedicado.

Implementando Um Scanner de Vulnerabilidade em Um Console ou Host Gerenciado do QRadar

É possível implementar um scanner do QRadar Vulnerability Manager em um console do QRadar ou no host gerenciado do QRadar. Por exemplo, é possível implementar um scanner em um coletor de fluxo, processador de fluxo, coletor de eventos ou processador de evento.

Antes de Iniciar

Para implementar um scanner no console do QRadar, certifique-se de que o processador de vulnerabilidade seja movido para um dispositivo do host gerenciado do QRadar Vulnerability Manager dedicado.

Para implementar scanners nos hosts gerenciados do QRadar, assegure-se de ter hosts gerenciados existentes na implementação. Para obter mais informações, consulte o *Guia de Instalação* para o produto.

Procedimento

1. Na guia **Administrador**, clique em **Gerenciamento do Sistema e de Licença** > **Ações de Implementação** > **Gerenciar Implementação de Vulnerabilidade**.
2. Clique em **Incluir Scanners de Vulnerabilidade Adicionais**.
3. Clique no ícone **+**.
4. Na lista **Host**, selecione o host gerenciado ou console do QRadar.

   Restrição: Não será possível incluir um scanner em um console do QRadar, quando o processador de vulnerabilidade estiver no console. Você deve mover o processador de vulnerabilidade para um host gerenciado do QRadar Vulnerability Manager.
5. Clique em **Salvar**.
6. Feche a janela Gerenciamento de Sistema e de Licença.
7. Na barra de ferramentas da guia **Admin**, selecione **Avançado** > **Implementar Configuração Completa**.
8. Clique em **OK**.
9. Verifique a lista **Servidor de Varredura** na página Configuração de Perfis de Varredura para assegurar-se de que o scanner tenha sido incluído.

   Para obter mais informações, consulte “Criando um Perfil de Varredura” na página 27.

O que Fazer Depois

Execute uma atualização automática depois de incluir o scanner ou outro host gerenciado com capacidades de varredura. Alternativamente, é possível fazer a varredura após a atualização automática padrão planejada diariamente ser executada.

Tarefas relacionadas:

“Movendo o Processador de Vulnerabilidade para um Console ou Host Gerenciado” na página 6
Se necessário, é possível mover o processador de vulnerabilidade entre um dispositivo do host gerenciado do QRadar Vulnerability Manager e o console do QRadar.

Varrendo os Recursos na sua DMZ

No IBM Security QRadar Vulnerability Manager, é possível se conectar a um scanner externo e varrer os recursos na sua DMZ para vulnerabilidades.

Se desejar varrer os recursos na DMZ para vulnerabilidades, você não precisará implementar um scanner em sua DMZ. O QRadar Vulnerability Manager deve ser configurado com um scanner IBM hospedado que está localizado fora da rede.

As vulnerabilidades detectadas são processadas pelo processador no console do QRadar ou no host gerenciado do QRadar Vulnerability Manager.

Procedimento

1. Configure a rede e os recursos para varreduras externas.
2. Configure o QRadar Vulnerability Manager para varrer os recursos externos.

Configurando a Rede e os Recursos para Varreduras Externas

Para verificar os recursos da DMZ, deve-se configurar a rede e informar a IBM sobre os ativos a serem verificados.

Procedimento

1. Configure acesso à Internet de saída na porta 443.
2. Envie as informações a seguir para `QRadar-QVM-Hosted-Scanner@hursley.ibm.com`:
   - Endereço IP externo da organização.

     Restrição: O endereço IP deve ser configurado antes que você possa executar varreduras externas.
   - O intervalo de endereço IP dos recursos em sua DMZ.

Configurando o QRadar Vulnerability Manager para Varrer os Recursos Externos

Para verificar os ativos na DMZ, é necessário configurar o QRadar Vulnerability Manager, usando a ferramenta **Gerenciamento do Sistema e de Licença** na guia Administrador.

Procedimento

1. Na guia **Administrador**, clique em **Gerenciamento do Sistema e de Licença** > **Ações de Implementação** > **Gerenciar Implementação de Vulnerabilidade**.
2. Clique em **Usar Scanner Externo**.
3. No campo **IP do Gateway**, digite um endereço IP externo.

   Restrição: Não é possível varrer ativos externos até que o endereço IP externo esteja configurado. Certifique-se de enviar para a IBM um email com os detalhes do endereço IP externo.
4. Opcional: Caso a rede esteja configurada para usar um servidor proxy, clique em **Ativar Servidor Proxy** e digite os detalhes do servidor.
5. Clique em **Salvar** e, em seguida, clique em **Fechar**.
6. Na barra de ferramentas da guia **Administrador**, clique em **Avançado** > **Implementar Configuração Integral**.
7. Clique em **OK**.

Navegadores da web suportados

Para os recursos em produtos IBM Security QRadar funcionarem corretamente, deve-se usar um navegador da web suportado.

Ao acessar o sistema QRadar, um nome de usuário e uma senha são solicitados. O nome de usuário e a senha devem ser configurados com antecedência pelo administrador.

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

Tabela 1. Navegadores da web suportados para produtos QRadar

Navegador da web	Versões suportadas
Mozilla Firefox	Liberação do Suporte Estendido do Firefox 17.0 Liberação de Suporte Estendido do Firefox 24.0
Microsoft Internet Explorer de 32 bits, com o modo de documento e modo de navegador ativados	9.0 10.0
Google Chrome	A versão atual a partir da data de liberação de produtos IBM Security QRadar V7.2.4

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

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

Procedimento

1. Em seu navegador da web Internet Explorer, pressione F12 para abrir a janela Ferramentas de desenvolvedor.
2. Clique em **Modo de navegador** e selecione a versão de seu navegador da web.
3. Clique em **Modo de documento**.
   - Para o Internet Explorer V9.0, selecione **Padrões do Internet Explorer 9**.
   - Para o Internet Explorer V10.0, selecione **Padrões do Internet Explorer 10**.

Estendendo o período de licença temporária do QRadar Vulnerability Manager

Por padrão, ao instalar o IBM Security QRadar SIEM, é possível ver a guia **Vulnerabilidades** porque há também uma chave de licença temporária instalada. Quando a licença temporária expira, é possível estendê-la por mais quatro semanas.

Procedimento

1. Na guia **Administrador**, clique no ícone **Gerenciador de Vulnerabilidade** na área **Experimentar**.
2. Para aceitar o contrato de licença do usuário final, clique em **OK**.

   Após a conclusão do período de licença estendido, deve-se aguardar seis meses para poder ativar a licença temporária novamente. Para ter acesso permanente ao QRadar Vulnerability Manager, é necessário adquirir uma licença.

Capítulo 3. IBM Security QRadar Vulnerability Manager

O IBM Security QRadar Vulnerability Manager é uma plataforma de varredura de rede que detecta as vulnerabilidades nos aplicativos, sistemas e dispositivos na rede ou no DMZ.

O QRadar Vulnerability Manager usa a inteligência de segurança para ajudá-lo a gerenciar e priorizar as vulnerabilidades na rede. Por exemplo, é possível usar o QRadar Vulnerability Manager para monitor as vulnerabilidades continuamente, melhorar a configuração do recurso e identificar as correções de software. Também é possível priorizar as diferenças de segurança correlacionando dados de vulnerabilidade aos dados de fluxos de rede, de dados do log, de firewall e de sistema de prevenção de intrusão (IPS).

É possível manter a visibilidade em tempo real das vulnerabilidades detectadas pelo scanner do QRadar Vulnerability Manager integrado e por outros scanners de terceiros. Os scanners de terceiros são integrados ao QRadar e incluem IBM Security Endpoint Manager, Guardium, AppScan, Nessus, nCircle e Rapid 7.

A menos que observado o contrário, todas as referências ao QRadar Vulnerability Manager se referem ao IBM Security QRadar Vulnerability Manager. Todas as referências ao QRadar se referem ao IBM Security QRadar SIEM e ao IBM Security QRadar Log Manager e todas as referências ao SiteProtector se referem ao IBM Security SiteProtector.

Varredura de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, a varredura de vulnerabilidade é controlada configurando os perfis de varredura. Cada perfil de varredura especifica os recursos que deseja varrer e o planejamento da varredura.

Processador de Vulnerabilidade

Ao licenciar o QRadar Vulnerability Manager, um processador de vulnerabilidade será implementado automaticamente no console do QRadar. O processador contém um componente de varredura do QRadar Vulnerability Manager.

Opções de Implementação

A Varredura de Vulnerabilidade Pode Ser Implementada de Diferentes Maneiras. Por exemplo, é possível implementar o recurso de varredura em um dispositivo de scanner do host gerenciado do QRadar Vulnerability Manager ou em um host gerenciado do QRadar.

Opções de Configuração

Os administradores podem configurar as varreduras das seguintes maneiras:

- Planejar varreduras a serem executadas em horários convenientes para os recursos de rede.
- Especificar os horários durante o qual as varreduras não têm permissão para serem executadas.

- Especificar os recursos que deseja excluir das varreduras, globalmente ou para cada varredura.
- Configure varreduras de correção autenticadas para os sistemas operacionais Linux, UNIX ou Windows.
- Configurar diferentes protocolos de varredura ou especificar os intervalos de porta que deseja varrer.

Conceitos relacionados:

"Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager" na página 8
Se você tiver uma grande rede e requerer opções flexíveis de varredura, poderá incluir mais scanners na implementação do IBM Security QRadar Vulnerability Manager.

"Opções para Mover o Processador de Vulnerabilidade na Implementação do QRadar Vulnerability Manager" na página 5
Se necessário, é possível mover o processador de vulnerabilidade do console do QRadar para um dispositivo do host gerenciado do QRadar Vulnerability Manager aplicado.

Introdução à varredura de vulnerabilidades

A configuração inicial do sistema IBM Security QRadar Vulnerability Manager para o gerenciamento de rede e de vulnerabilidades requer um planejamento sistemático.

Há três áreas principais a serem consideradas ao usar o QRadar Vulnerability Manager para a varredura de vulnerabilidades:

- O tipo de varredura a ser executada e com que frequência executar.
- O número de scanners a serem implementados e o número de ativos a serem verificados simultaneamente.
- Como gerenciar as vulnerabilidades descobertas.

Tipos de varredura

O IBM Security QRadar Vulnerability Manager fornece vários tipos padrão de políticas de varredura. Também é possível definir suas próprias varreduras a partir de modelos.

A seguir estão os modelos usados com mais frequência:

Varredura descoberta
: Descobre ativos de rede. Em seguida, verifica as portas para identificar características de ativos chave, como o sistema operacional, tipo de dispositivo e serviços que são fornecidos pelo ativo. As vulnerabilidades não são verificadas.

Varredura completa
: Descobre ativos de rede que usam um intervalo de portas de varredura rápida. Executa uma varredura de porta que pode ser configurada pelo usuário e uma varredura não autenticada dos serviços descobertos, como FTP, web, SSH e banco de dados. Caso sejam fornecidas credenciais, é executada uma varredura autenticada.

Varredura de correção
: Examina a rede para descobrir ativos e, em seguida, executa uma varredura de porta rápida e uma varredura de credenciais dos recursos.

Varreduras de descoberta

Uma varredura de descoberta é uma varredura leve sem credenciais. Ela examina um espaço de endereço em busca de endereços IP ativos e, em seguida, verifica suas portas. Ela executa consultas DNS e NetBIOS para descobrir qual sistema operacional é executado pelos ativos, quais os serviços abertos fornecidos e todos os nomes de rede a eles designados.

Geralmente, as varreduras de descoberta são executadas com frequência. Normalmente, elas são executadas semanalmente, para garantir boa visibilidade dos ativos de rede e das informações do ativo, como nomes de ativos, sistema operacional e serviços abertos, para usuários SIEM e SOC.

Varreduras integrais

Uma varredura integral executa o conjunto completo de testes do QRadar Vulnerability Manager.

Uma varredura integral tem estas fases:

1. Uma varredura de descoberta
2. Verificações sem credenciais. Verifica serviços que não requerem credenciais, por exemplo, leitura de banners e respostas para informações de versão, vencimento do certificado SSL, teste de contas padrão, teste de respostas para as vulnerabilidades.
3. Verificações com credenciais. O QRadar Vulnerability Manager efetua logon no ativo e reúne o inventário de aplicativos instalados e configurações necessárias e mostra (ou oculta) vulnerabilidades, conforme adequado. As varreduras de credenciais são preferíveis a varreduras sem credenciais. As varreduras sem credenciais fornecem uma visão geral útil da postura de vulnerabilidade da rede. No entanto, as varreduras com credenciais são essenciais para um programa abrangente e eficiente de gerenciamento de vulnerabilidades.

Nota: Às vezes, as varreduras integrais podem bloquear algumas contas de administração, por exemplo, SQL Server, quando o QRadar Vulnerability Manager testa várias credenciais padrão nessas contas.

Varreduras de correção

É possível usar as varreduras de correções para determinar quais correções e produtos estão instalados ou ausentes na rede.

Uma varredura de correção tem duas fases principais:

- Uma varredura de descoberta
- Verificações sem credenciais

As varreduras de correções são executadas de forma mais rápida e têm menos impacto sobre a rede e os ativos que estão sendo verificados, porque não executam verificações sem credenciais.

Quando fizer a varredura

A seguir, é mostrado um cronograma típico para cada tipo de varredura:

- Varredura de descoberta – Execução semanal
- Varredura de Correções – Execução a cada 1–4 semanas

- Varredura integral – Execução a cada 2-3 meses

Conceitos relacionados:

"Planejamento de Varredura" na página 32
No IBM Security QRadar Vulnerability Manager, é possível planejar as datas e horas nas quais é conveniente varrer os recursos de rede para as vulnerabilidades conhecidas.

Capítulo 5, "Varredura de Vulnerabilidade", na página 27
No IBM Security QRadar Vulnerability Manager, toda a varredura de rede é controlada pelos perfis de varredura que você criar. É possível criar vários perfis de varredura e configurar cada perfil de forma diferente dependendo dos requisitos específicos de sua rede.

"Políticas de Varredura" na página 55
Uma política de varredura fornece um local central para a configuração de requisitos de varredura específicos.

Tarefas relacionadas:

"Criando um Perfil de Varredura" na página 27
No IBM Security QRadar Vulnerability Manager, configure perfis de varredura para especificar como e quando os recursos de rede são digitalizados para vulnerabilidades.

Implementações de scanner remoto

É possível implementar um número ilimitado de scanners remotos em uma rede.

Ao designar uma implementação de scanner remoto, considere os seguintes fatores:

- O número de ativos a serem verificados.
- A conectividade de rede entre o IBM Security QRadar Vulnerability Manager e os ativos por ele verificados.
- A largura da banda da rede necessária.
- A necessidade de usar a varredura dinâmica.
- Quantas Placas da Interface de Rede (NICs) devem ser usadas em um scanner.

Scanners e ativos

Inicialmente, não há limite no número de ativos que um scanner pode verificar. Cada scanner tem uma largura de banda e as solicitações de verificação são enfileiradas quando essa largura de banda é atingida.

Quanto mais ativos um scanner tiver que verificar, mais tempo levará a varredura. Por exemplo, a implementação de scanners para verificar até 4.000-5.000 ativos resulta em tempos de varredura aceitáveis (2-3 dias, no máximo).

Conectividade do scanner e do ativo

Em geral, deve-se evitar fazer varreduras através de firewalls e sobre conexões WAN de baixa largura de banda.

As diretrizes a seguir são úteis:

- Mantenha a carga nos firewalls baixa.
- Reduza o risco de interferência do firewall na varredura. Por exemplo, não permita que o firewall bloqueie portas que são necessárias para a execução da varredura.
- Certifique-se de que as varreduras sejam executadas o mais rápido possível.

- Certifique-se de que a baixa conectividade da WAN não afete negativamente as varreduras.

Configurações de limite da largura da banda

É possível configurar a largura da banda da rede por perfil de varredura no IBM Security QRadar Vulnerability Manager.

Ao aumentar a largura da banda da rede por perfil de varredura, o QRadar Vulnerability Manager verifica mais ferramentas de vulnerabilidade em paralelo e, portanto, as varreduras são executadas mais rapidamente. É possível configurar o limite da largura da banda na página Configuração do Perfil de Varredura. As seguintes opções estão disponíveis:

Opção	Configuração do limite da largura da banda
Baixo	100 Kbps
Médio	1.000 Kbps (padrão)
Alto	5.000 Kbps
Completo	Máximo da rede

Caso você esteja fazendo a varredura em um número limitado de links de largura da banda da rede, não aumente a largura da banda da rede para mais de 1.000 Kbps. Como regra, ao fazer uma varredura de correção com uma configuração **Médio**, o QRadar Vulnerability Manager faz a varredura de correção de 10 ativos em paralelo. Com uma configuração **Alto**, ele verifica 50 ativos em paralelo.

Conceitos relacionados:

"Detalhes do Perfil de Varredura" na página 31
No IBM Security QRadar Vulnerability Manager, é possível descrever sua varredura, selecionar o scanner a ser utilizado e escolher entre uma série de opções de política de varredura.

Tarefas relacionadas:

"Criando um Perfil de Varredura" na página 27
No IBM Security QRadar Vulnerability Manager, configure perfis de varredura para especificar como e quando os recursos de rede são digitalizados para vulnerabilidades.

Varredura dinâmica

Na varredura dinâmica, o IBM Security QRadar Vulnerability Manager seleciona um scanner, com base no endereço IP a ser verificado.

A varredura dinâmica reduz o número de tarefas de varredura que devem ser configuradas. Por exemplo, se você implementar 10 scanners do QRadar Vulnerability Manager e não utilizar a varredura dinâmica, deverá configurar 10 tarefas de varredura individuais. Deve-se configurar um scanner por tarefa de varredura. Ao usar a varredura dinâmica, é possível configurar uma única tarefa de varredura para usar todos os 10 scanners, associando intervalos de CIDR com cada scanner. O QRadar Vulnerability Manager seleciona o scanner adequado para cada endereço IP que está sendo verificado.

A varredura dinâmica é mais útil ao implementar vários scanners. Se houver, por exemplo, mais de 5 scanners, a varredura dinâmica pode economizar tempo. Como regra, não ative a varredura dinâmica ao fazer a configuração inicial das

varreduras de teste. É possível alternar para a varredura dinâmica quando você estiver satisfeito com os tempos e resultados de varredura.

Conceitos relacionados:

"Varreduras de Vulnerabilidade Dinâmica" na página 53
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura para usar determinados scanners de vulnerabilidade para intervalos de CIDR específicos de sua rede. Por exemplo, os scanners podem ter acesso apenas a determinadas áreas da rede.

Tarefas relacionadas:

"Criando um Perfil de Varredura" na página 27
No IBM Security QRadar Vulnerability Manager, configure perfis de varredura para especificar como e quando os recursos de rede são digitalizados para vulnerabilidades.

Placas da Interface de Rede em scanners

No IBM Security QRadar Vulnerability Manager a varredura não é dependente das Placas da Interface de Rede (NICs) que estão configuradas no dispositivo de scanner.

É possível configurar várias NICs, embora geralmente sejam configuradas de 4-5 NICs. O QRadar Vulnerability Manager usa protocolos TCP/IP padrão para verificar qualquer dispositivo que tenha um endereço IP. Caso sejam definidas várias NICs, a varredura segue a configuração de rede padrão em um dispositivo.

Visão geral do gerenciamento de vulnerabilidade

O IBM Security QRadar Vulnerability Manager fornece um processo para gerenciar as vulnerabilidades baseadas na designação de proprietários de ativos.

É possível configurar proprietários de Ativos na página Designação de Vulnerabilidade da guia **Vulnerabilidades** ou usando uma API. Após a designação dos ativos, todas as vulnerabilidades descobertas nos ativos serão designadas a esses usuários ou grupos com uma data de vencimento baseada no nível de risco das vulnerabilidades em questão. Na página Designação de Vulnerabilidade também é possível configurar datas de vencimento e níveis de risco. Assim, é possível configurar relatórios de remediação a serem enviados para esses usuários periodicamente. Use os relatórios de remediação para destacar as seguintes ações:

- As correções a serem instaladas.
- As etapas a serem executadas para correção da vulnerabilidade.
- Os ativos que têm vulnerabilidades vencidas.
- Novas vulnerabilidades descobertas desde a última varredura.

Os relatórios de correção padrão estão disponíveis na guia **Email** da página Configuração do Perfil de Varredura. É possível criar relatórios de cliente extra, usando as procuras do QRadar Vulnerability Manager. Use uma ampla variedade de critérios de procura, para assegurar-se de que os relatórios se concentrem nas atividades de correção de vulnerabilidades necessárias para atender suas necessidades comerciais e de conformidade específicas.

Para facilitar a criação de relatórios de correção, o QRadar Vulnerability Manager pode criar automaticamente relatórios de Vulnerabilidades de ativos e Vulnerabilidades para cada proprietário de ativos, a partir de uma única definição de relatório.

Ao verificar novamente os ativos, as vulnerabilidades corrigidas são automaticamente detectadas e sinalizadas como corrigidas. Elas são removidas dos relatórios e visualizações, a menos que seja explicitamente configurado de outra forma. As vulnerabilidades corrigidas anteriormente que forem detectadas novamente serão automaticamente reabertas.

Conceitos relacionados:

Capítulo 10, "Relatórios de Vulnerabilidade", na página 85
No IBM Security QRadar Vulnerability Manager, é possível gerar ou editar um relatório existente ou usar o assistente de relatório para criar, planejar e distribuir um novo relatório.

Tarefas relacionadas:

"Designando um usuário técnico como proprietário de grupos de recursos" na página 81
No IBM Security QRadar Vulnerability Manager, é possível configurar grupos de ativos e automaticamente designar suas vulnerabilidades para usuários técnicos.

"Configurando os tempos de correção para as vulnerabilidades em ativos designados" na página 83
No IBM Security QRadar Vulnerability Manager, é possível configurar os tempos de correção para diferentes tipos de vulnerabilidades.

"Enviando E-mail aos Proprietários de Ativos Quando Varreduras de Vulnerabilidade Começarem e Pararem" na página 63
Envie um e-mail aos responsáveis técnicos configurados para alertá-los sobre o planejamento de varredura. Também é possível enviar por e-mail relatórios aos proprietários de ativo.

"Procurando Dados de Vulnerabilidade" na página 66
No IBM Security QRadar Vulnerability Manager, é possível identificar vulnerabilidades importantes procurando os dados de vulnerabilidade.

Painel de Gerenciamento de Vulnerabilidades

É possível exibir informações de vulnerabilidade no painel de QRadar.

O IBM Security QRadar Vulnerability Manager é distribuído com um painel de vulnerabilidade padrão, para que seja possível visualizar rapidamente o risco para sua organização.

É possível criar um novo painel, gerenciar os painéis existentes e modificar as configurações de exibição de cada item do painel de vulnerabilidade.

Para obter mais informações sobre os painéis, consulte o *Guia de Usuários* para o produto.

Revisando Dados de Vulnerabilidade No Painel De Gerenciamento de Vulnerabilidades Padrão

É possível exibir informações de gerenciamento de vulnerabilidades no painel do QRadar.

O painel de gerenciamento de vulnerabilidades padrão contém informações de risco, vulnerabilidade e varredura.

É possível configurar seu próprio painel para conter elementos diferentes, como procuras salvas.

Procedimento

1. Clique na guia **Painel**.
2. Na barra de ferramentas, na lista **Mostrar Painel**, selecione **Gerenciamento de Vulnerabilidades**.

Criando Um Painel Customizado de Gerenciamento de Vulnerabilidades

No QRadar é possível criar um painel de gerenciamento de vulnerabilidades customizado para seus requisitos.

Procedimento

1. Clique na guia **Painel**.
2. Na barra de ferramentas, clique em **Novo Painel**.
3. Digite um nome e descrição para seu painel de vulnerabilidade.
4. Clique em **OK**.
5. Opcional: Na barra de ferramentas, selecione **Incluir Item** > **Gerenciamento de Vulnerabilidades** e escolha uma das opções a seguir:
   - Se desejar mostrar procuras salvas padrão no painel, selecione **Procuras de Vulnerabilidade**.
   - Se desejar mostrar links de website para informações de segurança e vulnerabilidade, selecione **Notícias de Segurança**, **Recomendações de Segurança** ou **Vulnerabilidades Mais Recentes Publicadas**.
   - Se desejar mostrar informações sobre varreduras concluídas ou em execução, selecione **Varreduras Concluídas** ou **Varreduras em Andamento**.

Tarefas relacionadas:

"Salvando Seus Critérios de Procura de Vulnerabilidade" na página 70
No IBM Security QRadar Vulnerability Manager, é possível salvar os critérios de procura de vulnerabilidade para uso futuro.

Criando um painel para conformidade de correção

Crie um painel que mostre a correção mais efetiva a ser usada para corrigir as vulnerabilidades localizadas na rede.

Procedimento

1. Clique na guia **Painel**.
2. Na barra de ferramentas, clique em **Novo Painel**.
3. Digite um nome e descrição para seu painel de vulnerabilidade.
4. Clique em **OK**.
5. Na barra de ferramentas, selecione **Incluir item** > **Gerenciamento de vulnerabilidade** > **Procuras de vulnerabilidade** e escolha a procura salva padrão que deseja mostrar em seu painel.
6. No cabeçalho do novo item do painel, clique no ícone amarelo **Configurações**.
7. Selecione **Correção** na lista **Grupo por** e selecione uma das opções a seguir na lista **Gráfico por**:
   - Se desejar ver em quantos ativos precisa-se aplicar a correção, selecione **Contagem de ativo**.
   - Se deseja ver a pontuação de risco acumulativa por correção, selecione **Pontuação de risco**.

- Se desejar ver o número de vulnerabilidades cobertas por uma correção, selecione **Contagem de vulnerabilidade**.

8. Clique em **Salvar**.
9. Para visualizar os detalhes de vulnerabilidade na página **Gerenciar vulnerabilidades** > **Por vulnerabilidade**, na guia **Vulnerabilidades**, clique no link **Visualizar por vulnerabilidade** na parte inferior do item do painel.

Capítulo 4. Integrações do Software de Segurança

O IBM Security QRadar Vulnerability Manager se integra com outros produtos de segurança para ajudá-lo a gerenciar e priorizar os riscos de segurança.

Integração do IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager

O IBM Security QRadar Vulnerability Manager se integra ao QRadar Risk Manager para ajudá-lo a priorizar os riscos e vulnerabilidades na rede.

O QRadar Risk Manager é instalado como um dispositivo separado e, em seguida, é incluído no console do QRadar SIEM como um host gerenciado, usando a ferramenta **Gerenciamento de Sistema e de Licença** na guia Administrador.

Para obter mais informações sobre como instalar o QRadar Risk Manager, consulte o *Guia de Instalação do IBM Security QRadar Risk Manager*.

Políticas de Risco e Priorização de Vulnerabilidade

É possível integrar-se ao QRadar Vulnerability Manager QRadar Risk Manager, definindo e monitorando as políticas de risco de ativo ou de vulnerabilidade.

Se transmitir ou falhar as políticas de risco definidas no QRadar Risk Manager, as pontuações de risco de vulnerabilidade no QRadar Vulnerability Manager serão ajustadas. Os níveis de ajuste dependem das políticas de risco na organização.

Ao ajustar as pontuações de risco de vulnerabilidade no QRadar Vulnerability Manager, os administradores poderão executar as tarefas a seguir:

- Ganhar visibilidade imediata das vulnerabilidades que falharam uma política de risco.

  Por exemplo, novas informações podem ser exibidas no painel do QRadar ou enviadas usando o email.
- Priorizar novamente as vulnerabilidades que requerem atenção imediata.

  Por exemplo, um administrador pode usar a **Pontuação de Risco** para identificar rapidamente as vulnerabilidades de alto risco.

Se você aplicar as políticas de risco em um nível de ativo no QRadar Risk Manager, todas as vulnerabilidades neste ativo terão as pontuações de riscos ajustadas.

Para obter mais informações sobre como criar e monitorar políticas de riscos, consulte *Guia do Usuário do IBM Security QRadar Risk Manager*.

Tarefas relacionadas:

"Priorizando Vulnerabilidades de Alto Risco Aplicando Políticas de Risco" na página 74
No IBM Security QRadar Vulnerability Manager, é possível alertar os administradores para vulnerabilidades de risco mais alto, aplicando políticas de riscos à vulnerabilidades.

Integração do IBM Security Endpoint Manager

O IBM Security QRadar Vulnerability Manager se integra ao IBM Security Endpoint Manager para ajudar a filtrar e priorizar as vulnerabilidades que podem ser corrigidas.

Componentes de Integração

Uma integração típica do QRadar Vulnerability Manager IBM Security Endpoint Manager consiste nos seguintes componentes:

- Um console do IBM Security QRadar.
- Uma instalação licenciada do QRadar Vulnerability Manager.
- Uma instalação de servidor IBM Security Endpoint Manager.
- Uma instalação do agente do IBM Security Endpoint Manager em cada um dos destinos de varredura na rede.

Correção de Vulnerabilidade

Caso o IBM Security Endpoint Manager tenha sido instalado e integrado, o QRadar Vulnerability Manager fornecerá informações diferentes para ajudá-lo a corrigir as vulnerabilidades.

- Se o IBM Security Endpoint Manager não estiver instalado, o QRadar Vulnerability Manager fornecerá informações sobre as vulnerabilidades para as quais há uma correção disponível.

  O QRadar Vulnerability Manager mantém uma lista de informações de correção de vulnerabilidades. As informações de correção são correlacionadas com relação ao catálogo de vulnerabilidade conhecido.

  Usando o recurso de procura do QRadar Vulnerability Manager, é possível identificar vulnerabilidades que têm uma correção disponível.

- Se o IBM Security Endpoint Manager não estiver instalado, o QRadar Vulnerability Manager também fornecerá detalhes específicos sobre o processo de correção de vulnerabilidades. Por exemplo, uma correção pode ser planejada ou um ativo pode já estar corrigido.

  O servidor IBM Security Endpoint Manager reúne informações de correção de cada um dos agentes do IBM Security Endpoint Manager. As informações de status de correção são transmitidas ao QRadar Vulnerability Manager em intervalos de tempo pré-configurados.

  Usando o recurso de procura do QRadar Vulnerability Manager, é possível identificar rapidamente aquelas vulnerabilidades planejadas a serem corrigidas ou as que já estão corrigidas.

Tarefas relacionadas:

"Identificando o Status da Correção das Vulnerabilidades" na página 76
No IBM Security QRadar Vulnerability Manager, é possível identificar o status da correção das suas vulnerabilidades.

Configurando o SSL para integração do IBM Security Endpoint Manager

É possível configurar a criptografia SSL (secure socket layer) para integrar o QRadar Vulnerability Manager ao IBM Security Endpoint Manager.

Procedimento

1. Para fazer download do certificado de chave pública, abra o navegador da web e digite `https://IP address/webreports`.

   Lembre-se: O *IP address* é o endereço IP do servidor IBM Security Endpoint Manager.
2. Clique em **Adicionar Exceção**.
3. Na janela Incluir Exceção de Segurança , clique em **Visualizar**.
4. Clique na guia **Detalhes** e clique em **Exportar**.
5. No campo **Nome do arquivo**, digite `iemserver_cert.der`
6. No campo **Salvar como tipo**, selecione **X.509 Certificate (DER)**.
7. Clique em **Salvar**.
8. Copie o certificado de chave pública no console do QRadar.
9. Opcional: Para criar um armazenamento confiável do QRadar Vulnerability Manager
   a. Ao usar o SSH, efetue login no console do IBM Security QRadar SIEM como o usuário raiz.
   b. Digite o comando a seguir:

      ```
      keytool -keystore /opt/qvm/iem/truststore.jks -genkey -alias iem.
      ```
   c. Nos prompts, digite as informações apropriadas para criar o armazenamento confiável.
10. Para importar o certificado de chave pública para o armazenamento confiável, digite o comando a seguir:

    ```
    keytool -importcert -file iemserver_cert.der -keystore truststore.jks
    -storepass <your truststore password> -alias iem_crt_der
    ```
11. No prompt **Confiar neste certificado?**, digite **Sim**.

Integrando o IBM Security QRadar Vulnerability Manager ao IBM Security Endpoint Manager

É possível integrar o IBM Security QRadar Vulnerability Manager ao IBM Security Endpoint Manager.

Antes de Iniciar

Os componentes a seguir devem ser instalados na rede:

- Um servidor IBM Security Endpoint Manager.
- Um agente IBM Security Endpoint Manager em cada ativo verificado na rede.

Caso você utilize a criptografia SSL (secure socket layer), certifique-se de configurar o SSL (secure socket layer) para integração do IBM Security Endpoint Manager.

Procedimento

1. Ao usar o SSH, efetue login no console do IBM Security QRadar SIEM como o usuário raiz.
2. Altere o diretório para o local a seguir:

   ```
   /opt/qvm/iem
   ```
3. Para configurar o adaptador do IBM Security Endpoint Manager para o QRadar Vulnerability Manager, digite os seguintes comandos:

a. Digite `./iem-setup-webreports.pl`
b. Digite o *Endereço IP* do servidor IBM Security Endpoint Manager.
c. Digite o *Nome de usuário* do servidor IBM Security Endpoint Manager.
d. Digite a *Senha* do servidor IBM Security Endpoint Manager.

4. Opcional: No prompt **Usar Criptografia SSL?**, digite a resposta apropriada.

   Importante: Se você digitar `Sim`, em seguida, assegure-se de que as condições de pré-requisito sejam atendidas.
5. Digite o local do armazenamento confiável.
6. Digite a senha do armazenamento confiável.

Integração do IBM Security SiteProtector

O QRadar Vulnerability Manager se integra ao IBM Security SiteProtector para ajudar a conduzir a política do sistema de prevenção de intrusão (IPS).

Ao configurar o IBM Security SiteProtector, as vulnerabilidades detectadas pelas varreduras são automaticamente encaminhadas para o SiteProtector.

O IBM Security SiteProtector recebe dados de vulnerabilidade das varreduras do QRadar Vulnerability Manager que são executadas apenas após a configuração da integração.

Conectando-se ao IBM Security SiteProtector

É possível encaminhar dados de vulnerabilidade para o IBM Security SiteProtector para ajudar a conduzir a política do sistema de prevenção de intrusão (IPS).

Procedimento

1. Na guia **Administrador**, clique em **Gerenciamento do Sistema e de Licença** > **Ações de Implementação** > **Gerenciar Implementação de Vulnerabilidade**.
2. Clique em **Usar SiteProtector**.
3. No campo **Endereço IP do SiteProtector**, digite o endereço IP do servidor do gerenciador de agentes do IBM Security SiteProtector.
4. Clique em **Salvar** e, em seguida, clique em **Fechar**.
5. Na barra de ferramentas da guia **Administrador**, clique em **Avançado** > **Implementar Configuração Integral**.
6. Clique em **OK**.

O que Fazer Depois

Verifique os ativos de rede para determinar se os dados de vulnerabilidade serão exibidos na instalação do IBM Security SiteProtector.

Capítulo 5. Varredura de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, toda a varredura de rede é controlada pelos perfis de varredura que você criar. É possível criar vários perfis de varredura e configurar cada perfil de forma diferente dependendo dos requisitos específicos de sua rede.

Perfis de Varredura

Use perfis de varredura para executar as seguintes tarefas:

- Especifique os nós de rede, domínios ou domínios virtuais que deseja varrer.
- Especifique os recursos de rede que deseja excluir das varreduras.
- Criar janelas operacionais, que definem os horários em que as varreduras podem ser executadas.
- Executar manualmente perfis de varredura ou planejar uma varredura para ser executada em uma data futura.
- Executar, pausar, retomar, cancelar ou excluir uma única ou várias varreduras.
- Use credenciais centralizadas para executar sistemas operacionais Windows, UNIX ou Linux.
- Varra os recursos de uma procura de recursos salva.

Conceitos relacionados:

"Conjuntos de Credenciais Centralizadas" na página 40
Ao executar varreduras autenticadas, é possível usar uma lista central que armazene as credenciais de login dos sistemas operacionais Linux, UNIX ou Windows. O administrador do sistema deve configurar a lista de credenciais.

Criando um Perfil de Varredura

No IBM Security QRadar Vulnerability Manager, configure perfis de varredura para especificar como e quando os recursos de rede são digitalizados para vulnerabilidades.

Sobre Esta Tarefa

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrador** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Além disso, também é possível definir as seguintes configurações opcionais.

   - Caso mais scanners tenham sido incluídos na implementação do QRadar Vulnerability Manager, selecione um scanner na lista **Servidor de Varredura**. Essa etapa é desnecessária se você deseja usar a varredura dinâmica.
   - Para ativar esse perfil para varredura on demand, clique na caixa de seleção **Varredura On Demand Ativada**.

     Ao selecionar essa opção, o perfil é disponibilizado para ser usado se você desejar acionar uma varredura em resposta a um evento de regra

customizada. Ela também permite a varredura de vulnerabilidades on demand, usando o menu ativado pelo botão direito do mouse na página Ativos.

- Para especificar qual scanner deve ser usado para cada intervalo de CIDR, clique na caixa de seleção **Seleção de servidor dinâmico**.

  Caso você tenha configurado domínios na janela **Administrador** > **Gerenciamento de Domínio**, é possível selecionar um na lista **Domínios**. São verificados apenas os ativos dentro do domínio selecionado.
- Para varrer sua rede usando um conjunto predefinido de critérios de varredura, selecione um tipo de varredura na lista **Políticas de Varredura**.
- Se você tiver configurado credenciais centralizadas para ativos, clique na caixa de seleção **Usar Credenciais Centralizadas**. Para obter informações adicionais, consulte o *IBM Security QRadar SIEM Administration Guide*.

4. Clique em **Salvar**.

Conceitos relacionados:

"Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager" na página 8
Se você tiver uma grande rede e requerer opções flexíveis de varredura, poderá incluir mais scanners na implementação do IBM Security QRadar Vulnerability Manager.

"Políticas de Varredura" na página 55
Uma política de varredura fornece um local central para a configuração de requisitos de varredura específicos.

"Varreduras de Vulnerabilidade Dinâmica" na página 53
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura para usar determinados scanners de vulnerabilidade para intervalos de CIDR específicos de sua rede. Por exemplo, os scanners podem ter acesso apenas a determinadas áreas da rede.

Tarefas relacionadas:

"Associando Scanners de Vulnerabilidades com Intervalos de CIDR" na página 54
No IBM Security QRadar Vulnerability Manager, para executar varredura dinâmica, deve-se associar os scanners de vulnerabilidade com diferentes segmentos de sua rede.

"Varrendo novamente um ativo usando a opção do menu ativado pelo botão direito do mouse" na página 30
No IBM Security QRadar Vulnerability Manager, é possível varrer novamente rapidamente um ativo, usando a opção ativada pelo botão direito do mouse.

"Configurando uma política de varredura para gerenciar varreduras de vulnerabilidades" na página 56
No IBM Security QRadar Vulnerability Manager, é possível configurar uma política de varredura para controlar as varreduras de vulnerabilidades.

Criando um perfil de varredura de scanner externo

No IBM Security QRadar Vulnerability Manager, é possível configurar perfis de varredura para usarem um scanner hospedado para verificar ativos em sua DMZ.

Antes de Iniciar

O QRadar Vulnerability Manager deve ser configurado com um scanner hospedado. Para obter mais informações, consulte "Varrendo os Recursos na sua DMZ" na página 11.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrador** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para criar um perfil de scanner externo, também é necessário seguir as etapas restantes neste procedimento.
4. Selecione um scanner externo na lista **Servidor de varredura**.
5. Selecione **Varredura integral** ou **Varredura da web** na lista **Políticas de varredura**.
6. Clique na guia **Domínio e aplicativo da web**. No painel **Webs virtuais**, insira as informações de domínio e de endereço IP dos websites e aplicativos que você deseja varrer.
7. Clique em **Salvar**.

Criando um perfil de referência

Para criar varreduras de conformidade do Center for Internet Security, é necessário configurar perfis de referência. Use as varreduras de conformidade do CIS para testar a conformidade de referência do CIS do Windows e do Red Hat Enterprise Linux.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrador** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir Referência**.
4. Se desejar usar credenciais centralizadas predefinidas, selecione a caixa de seleção **Usar credenciais centralizadas**.

   As credenciais usadas para fazer varreduras nos sistemas operacionais Linux devem ter privilégios de administrador. As credenciais usadas para varreduras nos sistemas operacionais Windows devem ter privilégios de administrador.
5. Caso você não esteja usando a varredura dinâmica, selecione um scanner QRadar Vulnerability Manager na lista **Servidor de Varredura**.
6. Para ativar a varredura dinâmica, clique na caixa de seleção **Seleção de servidor dinâmico**.

   Caso você tenha configurado domínios na janela **Administrador** > **Gerenciamento de Domínio**, é possível selecionar um domínio na lista **Domínios**. São verificados apenas os ativos que estão dentro dos intervalos e domínios de CIDR que estão configurados para seus scanners.
7. Na guia **Quando varrer**, configure o planejamento de execução, o horário de início da varredura e quaisquer janelas operacionais predefinidas.
8. Na guia **Email**, defina as informações sobre essa varredura a serem enviadas e para quem elas devem ser enviadas.
9. Se não estiver usando as credenciais centralizadas, inclua as credenciais que a varredura requer na guia **Credenciais adicionais**.

   As credenciais usadas para fazer varreduras nos sistemas operacionais Linux devem ter privilégios de administrador. As credenciais usadas para varreduras nos sistemas operacionais Windows devem ter privilégios de administrador.

10. Clique em **Salvar**.

Conceitos relacionados:

"Conjuntos de Credenciais Centralizadas" na página 40
Ao executar varreduras autenticadas, é possível usar uma lista central que armazene as credenciais de login dos sistemas operacionais Linux, UNIX ou Windows. O administrador do sistema deve configurar a lista de credenciais.

Executando perfis de varredura manualmente

No IBM Security QRadar Vulnerability Manager é possível executar um ou mais perfis de varredura manualmente.

Também é possível planejar varreduras para executar em uma data e hora futuras. Para obter mais informações, consulte "Planejamento de Varredura" na página 32.

Antes de Iniciar

Assegure-se de que um processador de vulnerabilidade esteja implementado. Para obter mais informações, consulte "Verificando Se Um Processsador de Vulnerabilidade Está Implementado" na página 7.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Na página Perfis de Varredura, marque a caixa de seleção nas linhas designadas para os perfis de varredura a serem executados.

   Nota: Para localizar os perfis de varredura a serem executados, use o campo **Nome** da barra de ferramentas para filtrar por nome os perfis de varredura.
4. Na barra de ferramentas, clique em **Executar**.

   Por padrão, as varreduras concluem uma varredura rápida usando o Protocolo de Controle de Transmissão (TCP) e o Protocolo UDP (UDP). Uma varredura rápida inclui a maioria das portas no intervalo de 1 a 1024.

Conceitos relacionados:

"Detalhes do Perfil de Varredura" na página 31
No IBM Security QRadar Vulnerability Manager, é possível descrever sua varredura, selecionar o scanner a ser utilizado e escolher entre uma série de opções de política de varredura.

Tarefas relacionadas:

"Gerenciando os Resultados da Varredura" na página 60
No IBM Security QRadar Vulnerability Manager, na página Resultados da Varredura, é possível gerenciar os resultados da varredura e gerenciar as varreduras que estão em execução.

Varrendo novamente um ativo usando a opção do menu ativado pelo botão direito do mouse

No IBM Security QRadar Vulnerability Manager, é possível varrer novamente rapidamente um ativo, usando a opção ativada pelo botão direito do mouse.

A opção de varredura ativada pelo botão direito do mouse também está disponível na guia Ofensas do QRadar e na visualização de ativo de sub-rede do QRadar Risk Manager.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades** > **Por Ativo**.
3. Na página Por Ativo, identifique o ativo que deseja varrer novamente.
4. Clique com o botão direito do mouse no **Endereço IP** e selecione **Executar Varredura de Vulnerabilidade**.
5. Na janela Executar Varredura de Vulnerabilidade, selecione o perfil de varredura a ser usado quando o ativo for varrido novamente.

   O processo de varredura requer um perfil de varredura. O perfil de varredura determinará as opções de configuração de varredura usadas quando a varredura for executada.

   Para visualizar um perfil de varredura na janela Executar Varredura de Vulnerabilidade, marque a caixa de seleção **Varredura On Demand Ativada** na guia **Detalhes** na página Configuração do Perfil de Varredura.

   Importante: O perfil de varredura selecionado pode ser associado a diversos destinos de varredura ou intervalos de endereços IP. No entanto, ao usar a opção de clicar com o botão direito, apenas o ativo selecionado será digitalizado.
6. Clique em **Nova Varredura**.
7. Clique em **Fechar Janela**.
8. Para revisar o andamento da varredura de clique com o botão direito do mouse, na área de janela de navegação, clique em **Resultados da Varredura**.

   As varreduras de clique com o botão direito do mouse são identificadas pelo prefixo **RC:**.

Conceitos relacionados:

"Vulnerabilidades de ativo" na página 71
No IBM Security QRadar Vulnerability Manager, é possível exibir os dados de vulnerabilidade de resumo agrupados para cada recurso varrido.

Detalhes do Perfil de Varredura

No IBM Security QRadar Vulnerability Manager, é possível descrever sua varredura, selecionar o scanner a ser utilizado e escolher entre uma série de opções de política de varredura.

Os detalhes do perfil de varredura são especificados na guia **Detalhes**, na página Configuração do Perfil de Varredura.

Consulte principalmente as seguintes opções:

Tabela 2. Opções de Configuração de Detalhes do Perfil de Varredura

Opções	Descrição
Utilizar Credenciais Centralizadas	Especifica que o perfil utiliza credenciais predefinidas. As credenciais centralizadas são definidas na janela **Administrador** > **Configuração do Sistema** > **Credenciais Centralizadas**.
Servidor de Varredura	O scanner selecionado depende da configuração de rede. Por exemplo, para varrer os recursos DMZ, selecione um scanner que possui acesso a essa área da rede. O servidor de varredura **Controlador** é implementado com o processador de vulnerabilidade no console do QRadar ou no host gerenciado do QRadar Vulnerability Manager. **Restrição:** É possível ter apenas 1 processador de vulnerabilidade na implementação. Entretanto, é possível implementar diversos scanners nos dispositivos de scanner do host gerenciado do QRadar Vulnerability Manager dedicado ou nos hosts gerenciados do QRadar.

Tabela 2. Opções de Configuração de Detalhes do Perfil de Varredura (continuação)

Opções	Descrição
Varredura On Demand	Ativa a varredura on demand de ativos para o perfil. Use o menu ativado pelo botão direito do mouse na página Ativos para executar a varredura de vulnerabilidades on demand. Ao selecionar essa opção, o perfil também é disponibilizado para ser usado se você desejar acionar uma varredura em resposta a um evento de regra customizada. Com a ativação da varredura on demand, a varredura dinâmica também é ativada.
Seleção de servidor dinâmico	Especifica se deseja usar um scanner de vulnerabilidade separado para cada intervalo de CIDR varrido. Durante uma varredura, o QRadar Vulnerability Manager distribui automaticamente a atividade de varredura para o scanner correto para cada intervalo de CIDR que você especificar. Caso você tenha configurado domínios na janela Gerenciamento de Domínios da guia **Administrador**, também é possível selecionar o domínio a ser verificado.
Limite de Largura da Banda	A largura da banda da varredura. A configuração padrão é média. **Importante:** Se você selecionar um valor maior de 1000 kbps, poderá afetar o desempenho da rede.
Políticas de Varredura	Os critérios de varredura pré-configurada sobre portas e protocolos. Para obter mais informações, consulte "Políticas de Varredura" na página 55.

Conceitos relacionados:

"Varreduras de Vulnerabilidade Dinâmica" na página 53
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura para usar determinados scanners de vulnerabilidade para intervalos de CIDR específicos de sua rede. Por exemplo, os scanners podem ter acesso apenas a determinadas áreas da rede.

"Políticas de Varredura" na página 55
Uma política de varredura fornece um local central para a configuração de requisitos de varredura específicos.

Planejamento de Varredura

No IBM Security QRadar Vulnerability Manager, é possível planejar as datas e horas nas quais é conveniente varrer os recursos de rede para as vulnerabilidades conhecidas.

O planejamento de varredura é controlado usando a área de janela **Quando Varrer**, na página Configuração do Perfil de Varredura.

Um perfil de varredura configurado com uma configuração manual deve ser executado manualmente. No entanto, os perfis de varredura que não estão configurados como varreduras manuais, também podem ser executados manualmente.

Ao selecionar um planejamento de varredura, é possível refinar ainda mais seu planejamento configurando um intervalo de varredura permitido.

Tarefas relacionadas:

"Configurando um Intervalo de Varredura Permitido" na página 51
No IBM Security QRadar Vulnerability Manager, é possível criar uma janela operacional para especificar os horários que uma varredura pode ser executada.

"Revisando suas Varreduras Planejadas em Formato da Agenda" na página 34
No IBM Security QRadar Vulnerability Manager, o calendário de varredura planejado fornece um local central em que é possível revisar informações sobre varreduras planejadas.

Varrendo Domínios Mensalmente

No IBM Security QRadar Vulnerability Manager, é possível configurar um perfil de varredura para varrer os domínios na rede todo mês.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para configurar varreduras mensais, também é necessário seguir as etapas restantes neste procedimento.
4. Clique na área de janela **Quando Varrer**.
5. Na lista **Executar Planejamento**, selecione **Mensal**.
6. No campo **Horário de Início**, selecione uma data e hora de início para a varredura.
7. No campo **Dia do mês**, selecione um dia de cada mês no qual a varredura será executada.
8. Clique na guia **Domínio e aplicativo da web**.
9. No campo **Domínios**, digite a URL do ativo a ser verificado e clique em (**>**).
10. Clique em **Salvar**.
11. Opcional: Durante e após a varredura, é possível monitorar o progresso da varredura e revisar as varreduras concluídas.

Planejando Varreduras de Novos Recursos Não Digitalizados

No IBM Security QRadar Vulnerability Manager, é possível configurar varreduras planejadas de ativos de rede descobertos recentemente, não digitalizados.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Perfis de Ativos**, em seguida, na barra de ferramentas, clique em **Procura** > **Nova Procura**.
3. Para especificar ativos descobertos recentemente, não digitalizados, conclua as etapas a seguir no painel **Parâmetros de Procura**:
   a. Selecione **Dias Desde a Localização do Ativo**, **Menos de 2** e, em seguida, clique em **Incluir Filtro**.
   b. Selecione **Dias Desde a Varredura do Ativo Mais de 2**, em seguida, clique em **Incluir Filtro**.
   c. Clique em **Procurar**.
4. Na barra de ferramentas, clique em **Salvar Critérios** e conclua as opções a seguir:
   a. No campo **Inserir o Nome desta Procura**, digite o nome da procura de ativo.
   b. Clique em **Incluir em Minhas Procuras Rápidas**.
   c. Clique em **Compartilhar com Todos**.
   d. Clique em **OK**.
5. Clique na guia **Vulnerabilidades**.

6. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
7. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para planejar varreduras para ativos não verificados, também é necessário seguir as etapas restantes neste procedimento.
8. Na área de janela Incluir Procuras Salvas, selecione a procura de ativo salva na lista **Procuras Salvas Disponíveis** e clique em (>).
9. Clique na área de janela **Quando Varrer** e na lista **Executar Planejamento**, selecione **Semanal**.
10. Nos campos **Horário de Início**, digite ou selecione a data e hora na qual deseja executar a varredura em cada dia selecionado da semana.
11. Marque as caixas de seleção para os dias da semana que deseja executar a varredura.
12. Clique em **Salvar**.

    Para obter mais informações sobre como usar a guia **Ativos** e salvar as procuras de ativo, consulte o *Guia de Usuários* para o produto.

Tarefas relacionadas:

"Procurando Dados de Vulnerabilidade" na página 66
No IBM Security QRadar Vulnerability Manager, é possível identificar vulnerabilidades importantes procurando os dados de vulnerabilidade.

Revisando suas Varreduras Planejadas em Formato da Agenda

No IBM Security QRadar Vulnerability Manager, o calendário de varredura planejado fornece um local central em que é possível revisar informações sobre varreduras planejadas.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrativo** > **Varreduras Planejadas**.
3. Opcional: Passe o mouse sobre a varredura planejada para exibir informações sobre a varredura planejada.

   Por exemplo, é possível mostrar o tempo que uma varredura levou para ser concluída.
4. Opcional: Clique duas vezes em uma varredura planejada para editar o perfil da varredura.

Destinos e Exclusões de Varredura de Rede

No IBM Security QRadar Vulnerability Manager, é possível fornecer informações sobre os recursos, domínios ou webs virtuais na rede que deseja varrer.

Use a guia **Detalhes** na página Configuração do Perfil de Varredura para especificar os ativos de rede a serem verificados.

É possível excluir um host específico ou intervalo de hosts que nunca deve ser digitalizado. Por exemplo, é possível restringir uma varredura de ser executada em

servidores críticos que estão hospedando os aplicativos de produção. Você também pode desejar configurar a varredura para destinar apenas áreas específicas da rede.

O QRadar Vulnerability Manager se integra ao QRadar fornecendo a opção de varrer ativos que fazem parte de uma procura salva de ativo.

Destinos de varredura

É possível especificar os destinos de varredura definindo um intervalo de CIDR, um endereço IP, um intervalo de endereços IP ou uma combinação dos três.

Varredura de Domínio

É possível incluir domínios no perfil de varredura para testar transferências de zona de DNS em cada um dos domínios especificados.

Um host pode usar a transferência de zona de DNS para solicitar e receber uma transferência de zona completa para um domínio. A transferência de zona é um problema de segurança, porque os dados de DNS é usado para decifrar a topologia da rede. Os dados contidos em uma transferência de zona de DNS são sensíveis e, portanto, qualquer exposição dos dados pode ser considerada como uma vulnerabilidade. As informações obtidas podem ser usadas para exploração maliciosa, como envenenamento ou spoofing de DNS.

Varreduras que Usaram Procuras Salvas de Recurso

É possível varrer os recursos e endereços IP associados a uma procura salva de ativo do QRadar.

As procuras salvas são exibidas na seção **Procuras Salvas do Ativo** da guia **Detalhes**.

Para obter mais informações sobre como salvar uma procura de ativo, consulte o *Guia de Usuários* para o produto.

Excluir Destinos de Varredura de Rede

Na seção **Ativos Excluídos** da guia **Domínio e Aplicativo da Web**, é possível especificar os endereços IP, intervalos de endereços IP ou intervalos de CIDR para os ativos que não devem ser verificados. Por exemplo, se desejar evitar a varredura de um servidor altamente carregado, instável ou sensível, exclua estes ativos.

Ao configurar uma exclusão de varredura em uma configuração de perfil de varredura, a exclusão se aplicará apenas ao perfil de varredura.

Webs Virtuais

É possível configurar um perfil de varredura para varrer URLs diferentes que são hospedadas no mesmo endereço IP.

Ao varrer uma web virtual, o QRadar Vulnerability Manager verificará cada página da web para a injeção de SQL e as vulnerabilidades de scripts de site cruzado.

Tarefas relacionadas:

"Varrendo Intervalos de CIDR com Diferentes Scanners de Vulnerabilidade" na página 54
No IBM Security QRadar Vulnerability Manager, é possível varrer áreas da rede com diferentes scanners de vulnerabilidade.

"Excluindo Recursos de todas as Varreduras"
No IBM Security QRadar Vulnerability Manager, as exclusões de varredura especificam os recursos na rede que não são digitalizadas.

"Planejando Varreduras de Novos Recursos Não Digitalizados" na página 33
No IBM Security QRadar Vulnerability Manager, é possível configurar varreduras planejadas de ativos de rede descobertos recentemente, não digitalizados.

"Varrendo Domínios Mensalmente" na página 33
No IBM Security QRadar Vulnerability Manager, é possível configurar um perfil de varredura para varrer os domínios na rede todo mês.

Excluindo Recursos de todas as Varreduras

No IBM Security QRadar Vulnerability Manager, as exclusões de varredura especificam os recursos na rede que não são digitalizadas.

Sobre Esta Tarefa

Exclusões de varredura se aplicam a todas as configurações de perfil de varredura e podem ser usadas para excluir uma atividade de varredura de servidores instáveis ou sensíveis. Use o campo **Endereços IP** na página Exclusão de Varredura para inserir os endereços IP, intervalos de endereços IP ou intervalos de CIDR a serem excluídos de todas as varreduras. Para acessar a página Exclusão de Varredura:

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrativo** > **Exclusões de Varredura**.
3. Na barra de ferramentas, selecione **Ações** > **Incluir**.

   Nota: Também é possível usar a seção **Ativos Excluídos** da guia **Vulnerabilidades** > **Administrativo** > **Perfis de Varredura** > **Incluir** > **Domínio e Aplicativo da Web** para excluir ativos de um perfil de varredura específico.

Gerenciando Exclusões de Varredura

No IBM Security QRadar Vulnerability Manager é possível atualizar, excluir ou imprimir exclusões de varredura.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrativo** > **Exclusões de Varredura**.
3. Na lista na página Exclusões de Varreduras, clique na **Exclusão de Varredura** que deseja modificar.
4. Na barra de ferramentas, selecione uma opção no menu **Ações**.
5. Dependendo da seleção, siga as instruções na tela para concluir esta tarefa.

Protocolos e Portas de Varredura

No IBM Security QRadar Vulnerability Manager, é possível escolher diferentes protocolos de varredura e vários intervalos de porta de varredura.

Use a área de janela **Como Varrer** na página Configuração do Perfil de Varredura para especificar os protocolos de varredura e as portas que deseja varrer.

É possível configurar os protocolos de porta do perfil de varredura usando as opções a seguir:

Tabela 3. Opções de Protocolo e Porta de Varredura

Protocol	Descrição
TCP e UDP	O protocolo de varredura padrão que varre portas comuns no intervalo de 1 a 1024. **Lembre-se:** Comparados com outros protocolos de varredura, o TCP e o UDP podem gerar mais atividade de rede.
TCP	Os protocolos de varredura mais comuns. Quando a varredura TCP for combinada com a varredura do intervalo IP, você poderá localizar um host que está executando serviços propensos a vulnerabilidades. O intervalo de portas padrão é 1 - 65535.
SYN	Envia um pacote a todas as portas especificadas. Se o destino estiver atendendo, ele responderá com um SYN e ACK (Reconhecimento). Se o destino não estiver atendendo, ele responderá com um RST (reconfiguração). Normalmente, a porta de destino é fechada e um RST é retornado. O intervalo de portas padrão é 1 - 65535.
ACK	Semelhante ao SYN, mas nesse caso um sinalizador ACK está configurado. A varredura ACK não determina se a porta está aberta ou fechada, mas testa se a porta é filtrada ou não filtrada. Testar a porta será útil ao analisar a existência de um firewall e seus conjuntos de regras. A filtragem de pacotes simples permite conexões estabelecidas (pacotes com o conjunto de bits ACK), considerando que um firewall stateful mais sofisticado não pode permitir. O intervalo de portas padrão é 1-65535.
FIN	Um pacote TCP usado para terminar uma conexão ou pode ser usado como um método para identificar portas abertas. FIN envia os pacotes de erro a uma porta e espera que as portas de atendimento abertas enviem de volta mensagens de erro diferentes das portas fechadas. O scanner envia um pacote FIN, que pode fechar uma conexão aberta. As portas fechadas respondem a um pacote FIN com um RST. As portas abertas ignoram o pacote em questão. O intervalo de portas padrão é 1 - 65535.

Varrendo Um Intervalo de Portas Completas

No IBM Security QRadar Vulnerability Manager, é possível varrer o intervalo de portas completas nos ativos especificados.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para varrer um intervalo de portas completo, também é necessário seguir as etapas restantes neste procedimento.
4. Clique na guia **Como Varrer**.
5. No campo **Protocolo**, aceite os valores padrão de **TCP & UDP**.
6. No campo **Intervalo**, digite **1-65535**.

   Restrição: Os intervalos de portas devem ser configurados na ordem, separados por traços, delimitados por vírgulas, consecutivos, crescente e sem sobreposições. Diversos intervalos de portas devem ser separados por uma vírgula. Por exemplo, os seguintes exemplos mostram os delimitadores usados para inserir os intervalos de portas: (1-1024, 1055, 2000-65535).
7. No campo **Tempo Limite (m)**, digite o tempo, em minutos, após o qual você deseja que a varredura seja cancelada se nenhum resultado de varredura for descoberto.

Importante: É possível digitar qualquer valor no intervalo de 1 a 500. Assegure-se de não inserir um tempo muito curto, caso contrário a varredura da porta poderá não detectar todas as portas em execução. Os resultados de varredura são descobertos antes de o período de tempo limite ser exibido.

8. Clique em **Salvar**.
9. Na página Perfis de Varredura, clique em **Executar**.

Varrendo Recursos com Portas Abertas

No IBM Security QRadar Vulnerability Manager, é possível configurar um perfil de varredura para varrer ativos com portas abertas.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Perfis de Ativos**, em seguida, na barra de ferramentas, clique em **Procura** > **Nova Procura**.
3. Para especificar ativos com portas abertas, configure as opções a seguir na área de janela **Parâmetros de Procura**:
   a. Selecione **Ativos com Porta Aberta**, **Iguais a Qualquer Um dos 80** e clique em **Incluir Filtro**.
   b. Selecione **Ativos com Porta Aberta**, **Iguais a Qualquer Um dos 8080** e clique em **Incluir Filtro**.
   c. Clique em **Procurar**.
4. Na barra de ferramentas, clique em **Salvar Critérios** e configure as opções a seguir:
   a. No campo **Inserir o Nome desta Procura**, digite o nome da procura de ativo.
   b. Clique em **Incluir em Minhas Procuras Rápidas**.
   c. Clique em **Compartilhar com Todos** e clique em **OK**.
5. Clique na guia **Vulnerabilidades**.
6. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
7. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para varrer ativos com portas abertas, também é necessário seguir as etapas restantes neste procedimento.
8. Na guia **Detalhes**, selecione a procura de ativo salva na lista **Procuras Salvas Disponíveis** e clique em **>**.

   Ao incluir uma procura salva de ativo no perfil de varredura, os recursos e os endereços IP associados à procura salva serão digitalizados.
9. Clique na área de janela **Quando Varrer** e na lista **Executar Planejamento**, selecione **Manual**.
10. Clique na área de janela **O que Varrer**.
11. Clique em **Salvar**.

    Para obter mais informações sobre como salvar uma procura de ativo, consulte o *Guia de Usuários* para o produto.

O que Fazer Depois

Execute as etapas no procedimento, “Executando perfis de varredura manualmente” na página 30.

Varreduras de Correção Autenticadas

No IBM Security QRadar Vulnerability Manager, é possível varrer nomes de comunidades e executar varreduras de correção autenticadas para os sistemas operacionais Windows, Linux e UNIX.

nomes da comunidade SNMP

É possível varrer os ativos da rede usando os nomes da comunidade do SNMP.

Quando você varre os ativos, o QRadar Vulnerability Manager é autenticado usando os serviços SNMP localizados e conclui uma varredura de vulnerabilidade mais detalhada.

Varreduras de correção do Windows

Para varrer os sistemas operacionais Windows em busca de correções ausentes, o acesso de registro remoto e a interface de gerenciamento do Windows (WMI) devem estar ativados. Caso a sua varredura de correção do Windows retorne problemas de conectividade do WMI, deve-se configurar seus sistemas Windows.

Para ler dados WMI em um servidor remoto, você deve ativar as conexões entre o console do QRadar e o servidor que está sendo monitorando. Se o servidor estiver usando um firewall do Windows, você deverá configurar o sistema para ativar as solicitações remotas do WMI.

Caso esteja usando uma conta de não administrador para monitorar o servidor Windows, deve-se ativar a conta para interagir com o Modelo de Objeto Componente Distribuído (DCOM).

Se a ferramenta de varredura de correção não puder se conectar a um ativo do Windows, um ícone de aviso amarelo triangular será exibido ao lado do ativo nos resultados da varredura. A vulnerabilidade a seguir é aumentada: `Erro nas verificações locais`.

Proteja a varredura autenticada do sistema operacional Linux

Para varrer sistemas operacionais Linux usando autenticação segura, é possível configurar criptografia de chave pública entre seu console ou o host gerenciado e seus destinos de varredura.

Quando a autenticação segura é configurada, não é necessário especificar uma senha do sistema operacional Linux em seu perfil de varredura.

Você deve configurar a autenticação de chave pública em cada sistema operacional Linux que desejar varrer.

Caso você mova o processador de vulnerabilidade para um dispositivo do processador de vulnerabilidade dedicado, deve-se configurar novamente a autenticação segura entre o dispositivo do processador de vulnerabilidade dedicado e o destino de varredura.

Se a ferramenta de varredura de correção não puder se conectar a um ativo do Linux, um ícone de aviso amarelo triangular será exibido ao lado do ativo nos resultados da varredura. A vulnerabilidade a seguir é aumentada: `Varredura de correção SSH - Logon com falha`.

Tarefas relacionadas:

"Configurando a autenticação de chave pública do sistema operacional Linux" na página 41
Para verificar sistemas operacionais Linux usando a autenticação de chave pública segura, é necessário configurar o console ou o host gerenciado do IBM Security QRadar e o ativo a ser verificado. Quando a autenticação está configurada, é possível fazer a varredura autenticada, especificando um nome de usuário do sistema operacional Linux e não especificando uma senha. O QRadar suporta `rsa` e `dsa` para a geração da chave SSH.

"Configurando Uma Varredura Autenticada dos Sistemas Operacionais Linux ou UNIX" na página 42
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura de autenticação dos sistemas operacionais Linux ou UNIX que estão na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

"Configurando uma varredura autenticada do sistema operacional Windows" na página 44
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura dos sistemas operacionais Windows instalados na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

Conjuntos de Credenciais Centralizadas

Ao executar varreduras autenticadas, é possível usar uma lista central que armazene as credenciais de login dos sistemas operacionais Linux, UNIX ou Windows. O administrador do sistema deve configurar a lista de credenciais.

Um administrador pode especificar credenciais para os dispositivos de rede SNMP e os sistemas operacionais Linux, UNIX ou Windows. Portanto, um usuário que seja responsável por configurar um perfil de varredura não precisa conhecer as credenciais de cada recurso que é varrido. Além disso, se as credenciais de um recurso mudarem, as credenciais poderão ser modificadas centralmente, em vez de se atualizar o perfil de varredura.

Tarefas relacionadas:

"Configurando Uma Varredura Autenticada dos Sistemas Operacionais Linux ou UNIX" na página 42
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura de autenticação dos sistemas operacionais Linux ou UNIX que estão na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

"Configurando uma varredura autenticada do sistema operacional Windows" na página 44
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura dos sistemas operacionais Windows instalados na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

“Criando um perfil de referência” na página 29
Para criar varreduras de conformidade do Center for Internet Security, é necessário configurar perfis de referência. Use as varreduras de conformidade do CIS para testar a conformidade de referência do CIS do Windows e do Red Hat Enterprise Linux.

Configurando um Conjunto de Credenciais

No IBM Security QRadar Vulnerability Manager, é possível criar um conjunto de credenciais para os recursos na rede. Durante uma varredura, se uma ferramenta de varredura solicitar as credenciais de um sistema operacional Linux, UNIX ou Windows, as credenciais serão automaticamente transmitidas do conjunto de credenciais para a ferramenta de varredura.

Procedimento

1. Clique na guia **Admin**.
2. Na área de janela **Configuração do Sistema**, clique em **Credenciais Centralizadas**.
3. Na janela Credenciais Centralizadas, na barra de ferramentas, clique em **Incluir**.

   Para configurar um conjunto de credenciais, o único campo obrigatório na janela Conjunto de Credenciais é o campo **Nome**.
4. Na janela Conjunto de Credenciais, clique na guia **Ativos**.
5. Digite um intervalo de CIDR para os recursos para os quais deseja especificar credenciais e clique em **Incluir**.
6. Opcional: Clique nas guias **Linux/Unix, Windows ou Network Devices (SNMP)**, em seguida, digite as credenciais.
7. Clique em **Salvar**.

Configurando a autenticação de chave pública do sistema operacional Linux

Para verificar sistemas operacionais Linux usando a autenticação de chave pública segura, é necessário configurar o console ou o host gerenciado do IBM Security QRadar e o ativo a ser verificado. Quando a autenticação está configurada, é possível fazer a varredura autenticada, especificando um nome de usuário do sistema operacional Linux e não especificando uma senha. O QRadar suporta `rsa` e `dsa` para a geração da chave SSH.

Antes de Iniciar

Você deve configurar sua chave pública no dispositivo em que seu processador de vulnerabilidade está instalado. Para obter mais informações, consulte “Verificando Se Um Processsador de Vulnerabilidade Está Implementado” na página 7.

Procedimento

1. Usando SSH, efetue login no console do QRadar ou no host gerenciado como usuário raiz.
2. Gere um par de chaves públicas DSA digitando o seguinte comando:

   ```
   su -m -c 'ssh-keygen -t dsa' qvmuser
   ```
3. Aceite o arquivo padrão, pressionando **Enter**.
4. Aceite a passphrase padrão para a chave DSA, pressionando a tecla **Enter**.
5. Pressione a tecla **Enter** novamente para confirmar.

6. Copie a chave pública no destino de varredura digitando o seguinte comando:

   ```
   ssh-copy-id -i /home/qvmuser/.ssh/id_dsa.pub root@<IP address>
   ```

   Altere <*IP address*> para o endereço IP do destino de varredura.
7. Digite a passphrase para o destino de varredura.
8. Verifique se a conta *qvmuser* no console pode fazer SSH para o destino de varredura sem uma passphrase, digitando o seguinte comando:

   ```
   su -m -c 'ssh -o StrictHostKeyChecking=no root@<IP address> ls' qvmuser
   ```

   Altere <*IP address*> para o endereço IP do destino de varredura.

   É exibida uma lista dos arquivos que estão no diretório inicial do usuário raiz no destino de varredura.

O que Fazer Depois

Crie um perfil de varredura no QRadar Vulnerability Manager com um nome de usuário *root*, sem especificar uma senha e execute uma varredura de correção.

Tarefas relacionadas:

"Configurando Uma Varredura Autenticada dos Sistemas Operacionais Linux ou UNIX"
No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura de autenticação dos sistemas operacionais Linux ou UNIX que estão na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

Configurando Uma Varredura Autenticada dos Sistemas Operacionais Linux ou UNIX

No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura de autenticação dos sistemas operacionais Linux ou UNIX que estão na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

Antes de Iniciar

Para varrer usando uma lista de credenciais, você deve, primeiramente, definir uma lista central das credenciais requeridas pelos seus sistemas operacionais. Para obter mais informações, consulte "Configurando um Conjunto de Credenciais" na página 41.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para configurar uma varredura autenticada, também é necessário seguir as etapas restantes neste procedimento.
4. Opcional: Clique em **Usar Credenciais Centralizadas** para varrer os sistemas operacionais Linux ou UNIX.

   Se um conjunto de credenciais não for configurado e você não especificar manualmente as credenciais, as ferramentas de varredura executarão, mas nenhuma credencial será transmitida.

Caso haja um conjunto de credenciais para os hosts que estão sendo verificados, as credenciais que forem especificadas manualmente na guia **Credenciais Adicionais** substituirão o conjunto de credenciais.

5. Clique na guia **Quando Varrer**.
6. Na lista **Executar Planejamento**, selecione **Manual**.
7. Clique na guia **Credenciais Adicionais**.
8. Na área **Varredura de Correção do Linux/Unix**, digite o nome de usuário e a senha dos hosts do Linux ou UNIX a serem verificados e clique em **>**.

   Uma senha não é requerida, se você tiver configurado a autenticação de chave pública entre seu console e seu destino de varredura.
9. Clique em **Salvar**.
10. Na página Perfis de Varredura, clique em **Executar**.

Conceitos relacionados:

"Conjuntos de Credenciais Centralizadas" na página 40
Ao executar varreduras autenticadas, é possível usar uma lista central que armazene as credenciais de login dos sistemas operacionais Linux, UNIX ou Windows. O administrador do sistema deve configurar a lista de credenciais.

Tarefas relacionadas:

"Configurando um Conjunto de Credenciais" na página 41
No IBM Security QRadar Vulnerability Manager, é possível criar um conjunto de credenciais para os recursos na rede. Durante uma varredura, se uma ferramenta de varredura solicitar as credenciais de um sistema operacional Linux, UNIX ou Windows, as credenciais serão automaticamente transmitidas do conjunto de credenciais para a ferramenta de varredura.

"Configurando a autenticação de chave pública do sistema operacional Linux" na página 41
Para verificar sistemas operacionais Linux usando a autenticação de chave pública segura, é necessário configurar o console ou o host gerenciado do IBM Security QRadar e o ativo a ser verificado. Quando a autenticação está configurada, é possível fazer a varredura autenticada, especificando um nome de usuário do sistema operacional Linux e não especificando uma senha. O QRadar suporta `rsa` e `dsa` para a geração da chave SSH.

Ativando permissões para as varreduras de correção do Linux ou do UNIX

Contas do usuário não raiz devem ter as permissões para executar os comandos que o QRadar Vulnerability Manager requer para varrer os computadores Linux e UNIX em busca de correções.

Sobre Esta Tarefa

Para designar as permissões relevantes para a varredura de correção do Linux ou do UNIX, use o procedimento a seguir:

Procedimento

1. SSH para o ativo.
2. Execute os comandos `uname` a seguir:

```
uname -m
uname -n
uname -s
```

```
uname -r
uname -v
uname -p
uname -a
```

3. Dependendo do seu sistema operacional, execute os comandos a seguir:

Sistema operacional	Comandos

Linux	Leia os conteúdos dos arquivos a seguir que forem relevantes para sua distribuição:
	• /etc/redhat-release
	• /etc/SuSE-release
	• /etc/debian-version
	• /etc/slackware-version
	• /etc/mandrake-version
	• /etc/gentoo-version
	Por exemplo, no Red Hat Enterprise Linux, use os comandos:
	`ls /etc/redhat-releasecat`
	`/etc/redhat-release`
	`rpm -qa --qf '%{NAME}--%{VERSION}---%{RELEASE}`
	`|%{EPOCH}--%{ARCH}---%{FILENAMES}--%{SIGPGP}---%{SIGGPG}\n'`
	`rpm -qa --qf '%{NAME}-%{VERSION}-%{RELEASE}|%{EPOCH}\n'`

Solaris	`/usr/bin/svcs -a`
	`/usr/bin/pkginfo -x | awk '{ if ( NR % 2 ) { prev = \$1 }`
	`else { print prev\" \"\$0 } }'`
	`/usr/bin/showrev -p`
	`/usr/sbin/patchadd -p`
	`/usr/bin/isainfo -b`
	`/usr/bin/isainfo -k`
	`/usr/bin/isainfo -n`
	`/usr/bin/isainfo -v`

HP-UX	`/usr/sbin/swlist -l fileset -a revision` `/usr/sbin/swlist -l patch`
AIX	`oslevel -r` `lslpp -Lc`
ESX	`vmware -vesxupdate query --all` `. /etc/profile ; /sbin/esxupdate query –all`

Configurando uma varredura autenticada do sistema operacional Windows

No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura dos sistemas operacionais Windows instalados na rede. É possível especificar manualmente as credenciais no perfil de varredura ou usar um conjunto de credenciais.

Se a varredura for executada sem privilégios administrativos, o QRadar Vulnerability Manager varrerá o registro remoto para cada instalação no sistema operacional Windows.

A varredura sem privilégios administrativos está incompleta, propensa a positivos falsos e não cobre muitos aplicativos de terceiros.

Antes de Iniciar

O QRadar Vulnerability Manager usa protocolos de acesso remoto do sistema operacional Windows padrão ativados, por padrão, na maioria das janelas de implementação.

Se os resultados da varredura do Windows retornarem uma vulnerabilidade de erro de verificações locais, que indica problemas de conectividade do Windows Management Interface (WMI), você deverá configurar os sistemas Windows.

Para obter mais informações sobre a conectividade do Windows, consulte:

- "Ativando Acesso de Registro Remoto para Recursos no Sistema Operacional Windows" na página 47.
- "Configurando a Instrumentação de Gerenciamento do Windows" na página 47.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para configurar uma varredura autenticada do sistema operacional Windows, siga as etapas restantes neste procedimento.
4. Opcional: Clique em **Usar Credenciais Centralizadas** para varrer os sistemas operacionais Windows.

   Para que as ferramentas de varredura que requerem credenciais possam ser executadas, é necessário configurar um conjunto de credenciais ou especificar credenciais manualmente para os hosts.

   Caso haja um conjunto de credenciais para os hosts que estão sendo verificados, as credenciais que forem especificadas manualmente na guia **Credenciais Adicionais** substituirão o conjunto de credenciais.
5. Clique na área de janela **Quando Varrer**.
6. Na lista **Executar Planejamento**, selecione **Manual**.
7. Clique na área **Credenciais Adicionais**.
8. Na área **Varredura de Correção do Windows**, digite o **Domínio**, **Nome de Usuário** e **Senha** para os hosts do Windows a serem verificados e clique em (>).
9. Clique em **Salvar**.
10. Na página Perfis de Varredura, clique em **Executar**.

Conceitos relacionados:

"Conjuntos de Credenciais Centralizadas" na página 40
Ao executar varreduras autenticadas, é possível usar uma lista central que armazene as credenciais de login dos sistemas operacionais Linux, UNIX ou Windows. O administrador do sistema deve configurar a lista de credenciais.

"Varreduras de Correção Autenticadas" na página 39
No IBM Security QRadar Vulnerability Manager, é possível varrer nomes de comunidades e executar varreduras de correção autenticadas para os sistemas operacionais Windows, Linux e UNIX.

Varredura de correção do Windows

A *varredura de correção do Windows* é um método baseado em rede autenticado usado para interrogar o computador de destino quanto a atualizações e correções ausentes relacionadas à segurança.

A varredura de correção do Windows requer acesso a três serviços do Windows principais:

- Registro remoto
- WMI
- Compartilhamentos administrativos

É possível varrer computadores em busca de correções do Windows sem usar a WMI e os Compartilhamentos administrativos, mas os resultados não serão completos e estarão propensos a positivos falsos.

Use senhas complexas. No entanto, alguns caracteres especiais podem causar problemas. Limite os caracteres especiais a números, pontos-finais, vírgulas, pontos e vírgulas, aspas, sinais de porcentagem e espaços.

Registro remoto

O serviço de Registro remoto deve estar ativado, iniciado e acessível a partir do dispositivo de scanner do QRadar Vulnerability Manager e do usuário de varredura configurado usado no perfil de varredura.

Se o registro remoto não puder ser acessado, a varredura de correção do Windows falhará completamente.

Se o QRadar Vulnerability Manager não puder acessar o registro remoto, os resultados da varredura registrarão o erro a seguir:

```
Erro de verificações locais – O serviço de Registro remoto não está sendo
executado
```

No QRadar Vulnerability Manager versão 7.2.3 e mais recente, um ícone de triângulo amarelo é exibido próximo ao ativo nos resultados da varredura.

O status do serviço de registro remoto pode ser verificado no **Painel de controle administrativo** sob **Serviços**. Assegure-se de que os serviços dependentes a seguir estejam iniciados:

- Chamada de procedimento remoto (RPC)
- Ativador do processo de servidor DCOM
- Gerenciador de EndPoint RPC

O QRadar Vulnerability Manager pode acessar o registro remoto sobre o NetBIOS clássico (portas 135, 137, 139) ou o NetBIOS sobre TCP mais recente (na porta 445). Firewalls pessoais ou de rede que bloqueiam acesso a um desses protocolos evitam o acesso às varreduras de correção do Windows.

Por padrão, as contas do usuário administrativo têm acesso ao registro remoto. As contas do usuário não administrativo não têm acesso ao registro remoto. Deve-se configurar o acesso.

Ativando Acesso de Registro Remoto para Recursos no Sistema Operacional Windows

Para varrer os sistemas baseados no Windows, é necessário configurar o registro.

Procedimento

1. Efetue login no sistema baseado no Windows.
2. Clique em **Iniciar**.
3. No campo **Procurar Programas e Arquivos**, digite **Serviços** e pressione Enter.
4. Na janela Serviços, localize o serviço **Registro Remoto**.
5. Clique com o botão direito no serviço **Registro Remoto** e clique em **Iniciar**.
6. Feche a janela Serviços.

Designando permissões mínimas de registro remoto

Por padrão, as contas do usuário administrativo têm acesso ao registro remoto. As contas do usuário não administrativo não têm acesso ao registro remoto. Deve-se configurar o acesso.

Procedimento

1. No computador Windows de destino, crie ou designe um Usuário Global ou Local (por exemplo, "QVM_scan_user") e designe acesso somente leitura ao Registro para a conta do usuário não administrativo.
2. Efetue logon no seu computador Windows usando uma conta que tenha privilégios de administrador. Clique em **Iniciar** > **Executar**.
3. Digite `regedit`.
4. Clique em **OK**.
5. Acesse a chave:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurePipeServers \winreg.

   As permissões associadas a essa chave de registro controlam quais usuários ou qual grupo podem acessar o registro remotamente a partir da rede.
6. Destaque a chave **winreg** e execute uma das etapas a seguir:
   - No Windows XP ou mais recente, clique em **Editar** > **Permissões**.
   - No Windows 2000, clique em **Segurança** > **Permissões**.
7. Dê acesso somente leitura à conta "QVM_scan_user" designada.

   No Windows XP, a configuração *ForceGuest* será ativada por padrão quando estiver no modo de grupo de trabalho. Essa configuração pode causar problemas de acesso para conexões WMI e acesso de compartilhamentos, outros serviços DCOM e serviços RPC. Não é possível desativar a configuração *ForceGuest* em computadores Windows XP Home.

Configurando a Instrumentação de Gerenciamento do Windows

O QRadar Vulnerability Manager usa a Instrumentação de Gerenciamento do Windows (WMI) para localizar e identificar versões dos arquivos .exe e .dll instalados nos ativos de destino verificados.

Sobre Esta Tarefa

Sem as informações fornecidas pela WMI, muitos aplicativos de terceiros seriam ignorados. Positivos falsos que são detectados durante a varredura de registro (usando o serviço de registro remoto) não podem ser identificados ou removidos pelo QRadar Vulnerability Manager.

A WMI é instalada em todos os sistemas operacionais Windows modernos, como Windows Vista, Windows 2008, Windows 2012, Windows 7, Windows 8 e Windows 8.1).

As solicitações de WMI remotas devem estar ativadas e acessíveis pelo usuário de varredura nos ativos varridos. Se a WMI não estiver disponível, o erro a seguir será relatado nos resultados da varredura:

```
Erro de verificações locais – Não é possível consultar o Sistema de
arquivos remoto serviceMount da WMI
```

No QRadar Vulnerability Manager versão 7.2.3 e mais recente, um ícone de aviso de triângulo amarelo aparece próximo ao ativo nos resultados da varredura.

Se sua varredura de correção não for bem-sucedida, execute as etapas a seguir.

Procedimento

1. No servidor de destino, acesse **Painel de controle** > **Ferramentas administrativas** > **Gerenciamento de computadores**.
2. Expanda **Serviços e aplicativos**.
3. Clique com o botão direito em **Controle de WMI** e em **Propriedades**.
4. Clique na guia **Segurança**.
5. Clique em **Segurança**.
6. Opcional: Se necessário, inclua o usuário de monitoramento e clique na caixa de seleção **Ativação remota** para o usuário ou o grupo que solicita dados de WMI. Para incluir um usuário ou grupo de monitoramento:
   a. Clique em **Incluir**.
   b. No campo **Inserir os nomes de objetos a serem selecionados**, digite o nome do grupo ou nome de usuário.
   c. Clique em **OK**.
7. Clique em **Avançado** e aplique isso à raiz e aos subnamespaces.

   Nota: Em alguns casos, talvez também seja necessário configurar o firewall do Windows e as configurações do DCOM.

   Se você tiver problemas de WMI, poderá instalar as ferramentas Administrativas de WMI a partir do website da Microsoft .

   As ferramentas incluem um navegador de WMI que o ajuda a se conectar a uma máquina remota e navegar pelas informações de WMI. Essas ferramentas o ajudam a isolar quaisquer problemas de conectividade em um ambiente mais direto e mais simples.

Permitir solicitações de WMI por um firewall do Windows

Para ler os dados de WMI em um servidor remoto, uma conexão deve ser feita a partir do seu computador de gerenciamento (quando o software de monitoramento estiver instalado) ao servidor que está sendo monitorado. Caso o servidor de destino esteja executando o Firewall do Windows (também chamado de Firewall de Conexão de Internet) instalado nos computadores Windows XP e Windows 2003, deve-se configurar o firewall para permitir a passagem de solicitações de WMI remotas.

Para configurar o Firewall do Windows para permitir solicitações de WMI remotas, abra um prompt de comandos e insira o comando a seguir:

```
netsh firewall set service RemoteAdmin enable
```

Configurando permissões mínimas do DCOM

Para se conectar a um computador remoto usando a WMI, deve-se assegurar que as configurações do DCOM e as configurações de segurança de namespace de WMI corretas estejam ativadas para a conexão.

Sobre Esta Tarefa

Para conceder permissões de ativação e inicialização remotas do DCOM para um usuário ou um grupo, realize estas etapas.

Procedimento

1. Clique em **Iniciar** > **Executar**, digite `DCOMCNFG` e clique em **OK**.
2. Na caixa de diálogo **Serviços do componente**, expanda **Serviços do componente**, expanda **Computadores** e clique com o botão direito em **Meu computador** e em **Propriedades**.
3. Na caixa de diálogo **Propriedades do meu computador**, clique na guia **Segurança COM**.
4. Sob **Permissões de ativação e inicialização**, clique em **Editar limites**.
5. Na caixa de diálogo **Permissão de inicialização**, se seu nome ou grupo não aparecer na lista **Nomes de usuário ou grupos**, siga estas etapas:
   a. Na caixa de diálogo **Permissão de inicialização**, clique em **Incluir**.
   b. Na caixa de diálogo **Selecionar usuários, computadores ou grupos**, inclua seu nome e o grupo na caixa **Inserir os nomes de objeto a serem selecionados** e clique em **OK**.
6. Na caixa de diálogo **Permissão de inicialização**, selecione seu usuário e grupo na caixa **Nomes de usuário ou grupo**.
7. Na coluna **Permitir** sob **Permissões para o usuário**, selecione **Inicialização remota**, selecione **Ativação remota** e clique em **OK**.

Configurando permissões de acesso remoto do DCOM

Deve-se conceder permissões de acesso remoto do DCOM para determinados usuários e grupos.

Sobre Esta Tarefa

Caso o Computador A esteja se conectando remotamente ao Computador B, é possível configurar essas permissões no Computador B a fim de permitir que um usuário ou grupo que não faça parte do grupo de Administradores no Computador B se conecte ao Computador B.

Procedimento

1. Clique em **Iniciar** > **Executar**, digite `DCOMCNFG` e clique em **OK**.
2. Na caixa de diálogo **Serviços do componente**, expanda **Serviços do componente**, expanda **Computadores** e clique com o botão direito em **Meu computador** e em **Propriedades**.
3. Na caixa de diálogo **Propriedades do meu computador**, clique na guia **Segurança COM**.
4. Sob **Permissões de acesso**, clique em **Editar limites**.
5. Na caixa de diálogo **Permissão de acesso**, selecione o nome **LOGON ANÔNIMO** na caixa **Nomes de usuário ou grupo**. Na coluna **Permitir** sob **Permissões para o usuário**, selecione **Acesso remoto** e clique em **OK**.

Compartilhamentos administrativos

Todos os computadores Windows têm compartilhamentos administrativos, ativados por `\\machinename\driveletter$`, especialmente quando eles fazem parte de um domínio.

O QRadar Vulnerability Manager usa compartilhamentos administrativos para detectar vulnerabilidades no conjunto limitado de aplicativos a seguir:

- Mozilla Firefox
- Mozilla Thunderbird
- Java FX
- Apache Archiva
- Apache Continuum
- Preferências do Google Chrome

Os compartilhamentos administrativos não são visíveis a usuários não administrativos, e algumas organizações desativam os compartilhamentos administrativos ou usam contas do usuário não administrativo para a varredura. Se os compartilhamentos administrativos não estiverem acessíveis, o QRadar Vulnerability Manager poderá ignorar vulnerabilidades nos produtos na lista anterior ou produzir positivos falsos. De modo geral, os testes de vulnerabilidade do QRadar Vulnerability Manager usam compartilhamentos administrativos somente como último recurso e usam varreduras de registro e WMI.

Ativando compartilhamentos administrativos

No Windows Vista ou mais recente, os compartilhamentos administrativos serão desativados por padrão quando estiverem no modo de “grupo de trabalho”.

Sobre Esta Tarefa

Ative compartilhamentos administrativos usando estas etapas:

Procedimento

1. Clique em **Iniciar** > **Executar** e digite `regedit`.
2. Acesse a chave: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Clique com o botão direito em **Controle de WMI** e em **Propriedades**.
4. Inclua um novo DWORD chamado: `LocalAccountTokenFilterPolicy`
5. Configure o valor como 1.

Desativando compartilhamentos administrativos

Algumas organizações não desejam ativar compartilhamentos administrativos. No entanto, ao ativar o serviço de registro remoto, o serviço do servidor será iniciado e os compartilhamentos administrativos serão ativados.

Sobre Esta Tarefa

Para desativar compartilhamentos administrativos, modifique a chave de registro a seguir:

Procedimento

1. Clique em **Iniciar** > **Executar** e digite `regedit`.
2. Acesse a chave: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer**

3. Configure o parâmetro **AutoShareWks** como 0.

   Nota: Essa ação não desativa o compartilhamento IPC$. Embora esse compartilhamento não seja usado para acessar os arquivos diretamente, assegure-se de que o acesso anônimo a esse compartilhamento esteja desativado. Como alternativa, é possível remover o compartilhamento IPC$ completamente excluindo-o na inicialização usando o comando a seguir:

   ```
   net share IPC$ /delete
   ```

   Use esse método para remover os compartilhamentos C$ e D$ também.

Configurando um Intervalo de Varredura Permitido

No IBM Security QRadar Vulnerability Manager, é possível criar uma janela operacional para especificar os horários que uma varredura pode ser executada.

Sobre Esta Tarefa

Se uma varredura não for concluída dentro da janela operacional, ela será pausada e continuará quando a janela operacional for reaberta. Para configurar uma janela operacional:

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Administrador** > **Janela Operacional**.
3. Na barra de ferramentas, clique em **Ações** > **Incluir**.
4. Insira um nome para a janela operacional no campo **Nome**.
5. Escolha um planejamento de janela operacional na lista **Planejamento**.
6. Opcional: Selecione os horários em que a varredura é permitida.
7. Opcional: Selecione seu fuso horário.
8. Se você selecionou **Semanalmente** na lista **Planejamento**, clique nas caixas de seleção dos dias da semana desejados na área **Semanalmente**.
9. Se você selecionou **Mensalmente** na lista **Planejamento**, selecione um dia na lista **Dia do Mês**.
10. Clique em **Salvar**.

O que Fazer Depois

As janelas operacionais podem ser associadas a perfis de varredura usando a guia **Quando Varrer** na página Configuração do Perfil de Varredura.

Se duas janelas operacionais forem designadas a um perfil de varredura, o perfil de varredura será executado na intersecção de tempo das janelas operacionais. Por exemplo, ao configurar duas janelas operacionais diárias para os períodos de 1h a 6h e de 5h a 9h, a varredura será executada apenas entre as 5h e as 6h. Se as janelas operacionais não estiverem configuradas com planejamentos de horário sobrepostos, as varreduras não serão executadas.

Varrendo Durante Horários Permitidos

No IBM Security QRadar Vulnerability Manager, é possível planejar uma varredura dos recursos de rede em horários permitidos, usando uma janela operacional.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Janela Operacional**.
3. Na barra de ferramentas, selecione **Ações** > **Incluir**.
4. Digite um nome para a janela operacional, em seguida, configure um intervalo de tempo permitido e clique em **Salvar**.
5. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
6. Na barra de ferramentas, clique em **Incluir**.

   Ao criar um perfil de varredura, os únicos campos obrigatórios são **Nome** e **Endereços IP** na guia **Detalhes** da página Configuração do Perfil de Varredura. Para configurar a varredura durante horários permitidos, também é necessário seguir as etapas restantes neste procedimento.
7. Clique na guia **Quando Varrer**.
8. Na lista **Executar Planejamento**, selecione **Diário**.
9. Nos campos **Horário de Início**, digite ou selecione a data e hora na qual deseja executar a varredura a cada dia.
10. Na área de janela **Janelas Operacionais**, selecione a janela operacional na lista e clique em (>).
11. Clique em **Salvar**.

Gerenciando Janelas Operacionais

No IBM Security QRadar Vulnerability Manager, é possível editar, excluir e imprimir janelas operacionais.

Lembre-se: É possível editar uma janela operacional enquanto ela estiver associada a um perfil de varredura.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Janela Operacional**.
3. Selecione a janela operacional que deseja editar.
4. Na barra de ferramentas, selecione uma opção no menu **Ações**.
5. Siga as instruções na interface com o usuário.

   Restrição: Não é possível excluir uma janela operacional associada a um perfil de varredura. Você deve primeiro desconectar a janela operacional do perfil de varredura.

Desconectando Uma Janela Operacional

Se desejar excluir uma janela operacional associada a um perfil de varredura, você deverá desconectar a janela operacional do perfil de varredura.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Selecione o perfil de varredura que deseja editar.

4. Na barra de ferramentas, clique em **Editar**.
5. Clique na área de janela **Quando Varrer**.
6. Selecione a opção relevante na lista **Executar Planejamento**, conforme necessário.
7. No campo **Nome**, selecione a janela operacional a ser desconectada e clique em (<).
8. Clique em **Salvar**.

Varreduras de Vulnerabilidade Dinâmica

No IBM Security QRadar Vulnerability Manager, é possível configurar uma varredura para usar determinados scanners de vulnerabilidade para intervalos de CIDR específicos de sua rede. Por exemplo, os scanners podem ter acesso apenas a determinadas áreas da rede.

Durante uma varredura, o QRadar Vulnerability Manager determina que scanner usar para cada CIDR, endereço IP ou intervalo de IPs especificado no perfil de varredura.

Varredura dinâmica e domínios

Caso você tenha configurado domínios na janela Gerenciamento de Domínio na guia **Administrador**, é possível associar scanners aos domínios incluídos.

Por exemplo, é possível associar diferentes scanners individualmente com um domínio diferente, ou com diferentes intervalos de CIDR dentro do mesmo domínio. O QRadar verifica dinamicamente os intervalos de CIDR configurados que contêm os endereços IP especificados em todos os domínios que estão associados com scanners no sistema. Os ativos com o mesmo endereço IP em diferentes domínios são verificados individualmente, se o intervalo de CIDR de cada domínio incluir esse endereço IP. Se um endereço IP não estiver dentro de um intervalo de CIDR configurado para um domínio de scanner, o QRadar verificará o domínio que está configurado para o scanner do Controlador para o ativo.

Configurando a varredura dinâmica

Para usar *varredura dinâmica*, você deve executar as seguintes ações:

1. Incluir scanners de vulnerabilidade na implementação do QRadar Vulnerability Manager. Para obter mais informações, consulte “Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager” na página 8.
2. Associe os scanners de vulnerabilidade aos intervalos de CIDR e domínios.
3. Configure uma varredura de vários intervalos de CIDR e ative a **Seleção de servidor dinâmico** na guia **Detalhes** da página Configuração do Perfil de Varredura.

Conceitos relacionados:

“Varredura dinâmica” na página 17
Na varredura dinâmica, o IBM Security QRadar Vulnerability Manager seleciona um scanner, com base no endereço IP a ser verificado.

“Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager” na página 8
Se você tiver uma grande rede e requerer opções flexíveis de varredura, poderá incluir mais scanners na implementação do IBM Security QRadar Vulnerability Manager.

"Detalhes do Perfil de Varredura" na página 31
No IBM Security QRadar Vulnerability Manager, é possível descrever sua varredura, selecionar o scanner a ser utilizado e escolher entre uma série de opções de política de varredura.

Associando Scanners de Vulnerabilidades com Intervalos de CIDR

No IBM Security QRadar Vulnerability Manager, para executar varredura dinâmica, deve-se associar os scanners de vulnerabilidade com diferentes segmentos de sua rede.

Antes de Iniciar

Deve-se incluir scanners de vulnerabilidade extras em sua implementação. Para obter mais informações, consulte "Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager" na página 8.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Scanners**.

   Atenção: Por padrão, o scanner Controller é exibido. O scanner Controller é parte do processador do QRadar Vulnerability Manager que é implementado no QRadar Console ou em um dispositivo de processamento dedicado do QRadar Vulnerability Manager. É possível designar um intervalo de CIDR ao scanner Controller, mas você deve implementar scanners extras para usar a varredura dinâmica.
3. Clique em um scanner na página **Scanners**.
4. Na barra de ferramentas, clique em **Editar**.

   Restrição: Não é possível editar o nome do scanner. Para editar um nome do scanner, clique em **Administrador** > **Gerenciamento de Sistema e de Licença** > **Ações de Implementação** > **Gerenciar Implementação de Vulnerabilidade**.
5. No campo **CIDR**, digite um intervalo de CIDR ou diversos intervalos de CIDR separados por vírgulas.
6. Clique em **Salvar**.

Conceitos relacionados:

"Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager" na página 8
Se você tiver uma grande rede e requerer opções flexíveis de varredura, poderá incluir mais scanners na implementação do IBM Security QRadar Vulnerability Manager.

Varrendo Intervalos de CIDR com Diferentes Scanners de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível varrer áreas da rede com diferentes scanners de vulnerabilidade.

Antes de Iniciar

Você deve configurar os intervalos de CIDR de rede para usar os diferentes scanners de vulnerabilidade na implementação do QRadar Vulnerability Manager.

Para obter mais informações, consulte “Opções para Incluir Scanners na Implementação do QRadar Vulnerability Manager” na página 8.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Perfis de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.
4. Clique na caixa de seleção **Seleção de Servidor Dinâmico**.

   Caso você tenha configurado domínios na janela **Administrador** > **Gerenciamento de Domínio**, é possível selecionar um domínio na lista **Domínios**. São verificados apenas os ativos dentro do domínio selecionado.
5. Opcional: Incluir mais intervalos de CIDR.
6. Clique em **Salvar**.
7. Clique na caixa de seleção na linha designada para a varredura na página Perfis de Varredura e clique em **Executar**.

Políticas de Varredura

Uma política de varredura fornece um local central para a configuração de requisitos de varredura específicos.

É possível usar políticas de varredura para especificar tipos de varredura, portas e vulnerabilidades a serem verificadas e ferramentas de varredura a serem usadas. No IBM Security QRadar Vulnerability Manager, uma *política de varredura* é associada com um perfil de varredura e é usada para controlar uma varredura de vulnerabilidade. Use a lista **Políticas de Varredura** na guia **Detalhes** da página Configuração do Perfil de Varredura para associar uma política de varredura a um perfil de varredura.

É possível criar uma nova política de varredura ou copiar e modificar uma política pré-configurada distribuída com o QRadar Vulnerability Manager.

Políticas de Varredura Pré-configuradas

As políticas de varredura pré-configuradas a seguir são distribuídas com o QRadar Vulnerability Manager:

- Varredura completa
- Varredura descoberta
- Varredura do banco de dados
- Varredura de correção
- Varredura PCI
- Varredura da web

Uma descrição de cada política de varredura pré-configurada é exibida na página Políticas de Varredura.

Tarefas relacionadas:

“Modificando Uma Política de Varredura Pré-configurada” na página 56
No IBM Security QRadar Vulnerability Manager, é possível copiar uma política de varredura pré-configurada e modificar a política para seus requisitos exatos de varredura.

"Configurando uma política de varredura para gerenciar varreduras de vulnerabilidades"
No IBM Security QRadar Vulnerability Manager, é possível configurar uma política de varredura para controlar as varreduras de vulnerabilidades.

Modificando Uma Política de Varredura Pré-configurada

No IBM Security QRadar Vulnerability Manager, é possível copiar uma política de varredura pré-configurada e modificar a política para seus requisitos exatos de varredura.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Políticas de Varreduras**.
3. Na página Políticas de Varredura, clique em uma política de varredura pré-configurada.
4. Na barra de ferramentas, clique em **Editar**.
5. Clique em **Copiar**.
6. Na janela Copiar política de varredura, digite um novo nome no campo **Nome** e clique em **OK**.
7. Clique na cópia da política de varredura e na barra de ferramentas e clique em **Editar**.
8. No campo **Descrição**, digite novas informações sobre a política de varredura.

   Importante: Se você modificar a nova política de varredura, deverá atualizar as informações na descrição.
9. Para modificar a política de varredura, use as guias **Varredura de Porta**, **Vulnerabilidades**, **Grupos de Ferramentas** ou **Ferramentas**.

   Restrição: Dependendo do **Tipo de Varredura** selecionado, não é possível usar todas as guias na janela Política de Varredura.

Configurando uma política de varredura para gerenciar varreduras de vulnerabilidades

No IBM Security QRadar Vulnerability Manager, é possível configurar uma política de varredura para controlar as varreduras de vulnerabilidades.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Administrativo** > **Políticas de Varreduras**.
3. Na barra de ferramentas, clique em **Incluir**.
4. Digite o nome e a descrição de sua política de varredura.

   Para configurar uma política de varredura, os únicos campos obrigatórios na janela Nova Política de Varredura são **Nome** e **Descrição**.
5. Na lista **Tipo de Varredura**, selecione o tipo de varredura no qual a política de varredura será baseada.
6. Para incluir vulnerabilidades específicas em sua política de varredura, execute as seguintes etapas:
   a. Na janela Nova Política de Varredura, clique na caixa de seleção **Correção**.

b. Clique na guia **Vulnerabilidades**.
c. Clique em **Incluir**.

   Por padrão, todas as vulnerabilidades descobertas no ano passado são exibidas.
d. Filtrar a lista de vulnerabilidades.
e. Clique nas vulnerabilidades que deseja incluir em sua política de varredura e clique em **Enviar** na barra de ferramentas.

7. Para incluir ou excluir grupos de ferramentas a partir de uma política de varredura sem credenciais ou integral, clique na guia **Grupo de Ferramentas**.
8. Para incluir ou excluir ferramentas a partir de uma política de varredura sem credenciais ou integral, clique na guia **Ferramentas**.

   Importante:

   Se você não modificar as ferramentas ou grupos de ferramenta e tiver selecionado a opção **Completa** como seu tipo de varredura, todas as ferramentas e grupos de ferramentas associados a uma varredura completa estarão incluídos na política de varredura.
9. Clique em **Salvar**.

Capítulo 6. Investigações de Varredura de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível investigar recursos do resumo e dados de vulnerabilidade para cada varredura.

Para investigar varreduras de vulnerabilidade, execute as seguintes tarefas:

- Construir e salvar critérios de procura de vulnerabilidade complexa.
- Investigar níveis de risco de exploração em um nível de rede, ativo e vulnerabilidade.
- Priorizar os processos de correção de vulnerabilidade.

Resultados da varredura

É possível usar a página Resultados da Varredura para investigar as informações a seguir:

- O progresso de uma varredura e as ferramentas de varredura que estão enfileiradas e em execução.
- O status de uma varredura. Por exemplo, uma varredura com um status de **Interrompido** indica que a varredura foi concluída com sucesso ou cancelada.
- O grau de risco associado a cada perfil de varredura concluído. O risco é indicado pela coluna **Pontuação** e mostra a pontuação total de Common Vulnerability Scoring System (CVSS) para o perfil de varredura concluído.
- O número total de recursos que foram localizados pela varredura.
- O número total de vulnerabilidades descobertas pelo perfil de varredura concluído.
- O número total de serviços abertos descobertos pelo perfil de varredura concluído.

Contagens de Vulnerabilidade

A página Resultados da Varredura mostra **Vulnerabilidades** e **Instâncias de Vulnerabilidades**.

- A coluna **Vulnerabilidades** mostra o número total de vulnerabilidades exclusivas que foram descobertas em todos os recursos varridos.
- Quando você varre diversos ativos, a mesma vulnerabilidade pode estar presente em ativos diferentes. Portanto, a coluna **Instâncias de Vulnerabilidade** mostra o número total de vulnerabilidades que foram descobertas em todos os recursos varridos.

Procurando Resultados da Procura

No IBM Security QRadar Vulnerability Manager, é possível procurar e filtrar os resultados da varredura.

Por exemplo, você pode querer identificar varreduras recentes, varreduras em um endereço IP específico ou varreduras que identificaram uma vulnerabilidade específica.

Sobre Esta Tarefa

Use o campo **Nome** na guia **Vulnerabilidades** para procurar resultados pelo nome do perfil de varredura. Para usar um critério mais avançado na procura, faça o seguinte:

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Resultados da Varredura**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.

   Para procurar os resultados de sua varredura, não há campos obrigatórios. Todos os parâmetros são opcionais.
4. Para mostrar resultados de varreduras que foram concluídas dentro de um número recente de dias, digite um valor no campo **Varredura executada nos últimos dias**.
5. Para mostrar resultados de varredura para uma vulnerabilidade específica, clique em **Navegar** no campo **Contém Vulnerabilidade**.
6. Para mostrar resultados de varredura para varreduras que foram apenas planejadas, clique em **Excluir varredura sob demanda**.
7. Clique em **Procurar**.

Conceitos relacionados:

"Planejamento de Varredura" na página 32
No IBM Security QRadar Vulnerability Manager, é possível planejar as datas e horas nas quais é conveniente varrer os recursos de rede para as vulnerabilidades conhecidas.

Incluindo títulos de colunas em procuras de ativos

Limite as procuras de ativos com filtros que incluam perfis de ativos customizados, nome, contagem de vulnerabilidade e pontuação de risco.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Perfis de Ativos**, em seguida, na barra de ferramentas, clique em **Procura** > **Nova Procura**.
3. No campo que contém os nomes de colunas, no campo à esquerda, clique nos títulos de colunas que você deseja incluir em sua procura e clique no botão de seta para mover os títulos selecionados para o campo à direita.
4. Clique nos botões para cima e para baixo para alterar a prioridade dos títulos de colunas selecionados.
5. Quando o campo à direita contiver todos os cabeçalhos de coluna em que você deseja procurar, clique em **Procurar**.

Gerenciando os Resultados da Varredura

No IBM Security QRadar Vulnerability Manager, na página Resultados da Varredura, é possível gerenciar os resultados da varredura e gerenciar as varreduras que estão em execução.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Resultados da Varredura**.

3. Opcional: Caso você deseje executar novamente varreduras que foram concluídas, marque a caixa de seleção nas linhas designadas para as varreduras e clique em **Executar**.

   Uma varredura concluída possui um status de **Interrompido**.
4. Opcional: Para excluir varreduras concluídas:
   a. Na página Resultados da Varredura, marque a caixa de seleção nas linhas designadas para os resultados de varredura a serem excluídos.
   b. Na barra de ferramentas, clique em **Excluir**.

      Se você excluir um conjunto de resultados da varredura, nenhum aviso será exibido. Os resultados da varredura serão excluídos imediatamente.

      Lembre-se: Quando você exclui um conjunto de resultados de varredura, nem os dados de varredura do modelo de ativos do QRadar nem o perfil de varredura são excluídos.
5. Opcional: Para cancelar uma varredura que está em execução:
   a. Na página Resultados da Varredura, marque a caixa de seleção nas linhas designadas para as varreduras a serem canceladas.
   b. Na barra de ferramentas, clique em **Cancelar**.

      É possível cancelar uma varredura que possui um status de **Em Execução** ou **Pausado**. Após cancelar uma varredura, o status da varredura será **Interrompido**.

Níveis de Risco do Recurso e Categorias de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível investigar o nível de risco de exploração dos ativos verificados, na página Ativos de Resultados da Varredura.

A página Ativos de Resultados da Varredura fornece um resumo de riscos de vulnerabilidades para cada um dos ativos que foram verificados por meio da execução de um perfil de varredura.

Pontuação de risco

Cada vulnerabilidade que é detectada em sua rede tem uma pontuação de risco que é calculada usando a pontuação base Common Vulnerability Scoring System (CVSS). Uma contagem de alto risco fornece uma indicação do potencial para a exploração de vulnerabilidade.

Na página Ativos de Resultados da Varredura, a coluna **Pontuação** é uma acumulação da pontuação de risco para cada vulnerabilidade em um ativo. O valor acumulado fornece uma indicação do nível de risco associado a cada ativo.

Para identificar rapidamente os recursos com mais risco de exploração de vulnerabilidade, clique no título da coluna **Pontuação** para classificar seus ativos por nível de risco.

Categorias e Contagens de Vulnerabilidade

A página Ativos de Resultados da Varredura mostra o número total de vulnerabilidades e serviços abertos descobertos em cada ativo verificado.

Para identificar os recursos com o número mais alto de vulnerabilidades, clique no título da coluna **Instâncias de Vulnerabilidade** para ordenar seus ativos.

As colunas **Alto**, **Médio**, **Baixo** e **Aviso** agrupam todas as vulnerabilidades de acordo com seu risco.

As colunas **% de Aprovação da Verificação de Políticas** e **% de Falha da Verificação de Políticas** exibem a porcentagem de verificações de políticas que o ativo aprovou ou falhou na varredura de referências. Clique nos valores nessas colunas para ver mais informações sobre as verificações de políticas aprovadas ou com falha na página Verificações de Políticas de Resultados da Varredura.

Dados de Recurso, Vulnerabilidade e Serviços Abertos

No IBM Security QRadar Vulnerability Manager, a página Detalhes do Ativo de Resultados de Varredura mostra dados sobre ativos, vulnerabilidades e serviços abertos.

Usando as opções na barra de ferramentas, é possível se alternar entre a visualização de vulnerabilidades e serviços abertos.

A página Detalhes do Ativo de Resultados da Varredura fornece as seguintes informações:

- Informações de resumo sobre o ativo varrido, incluindo o sistema operacional e o grupo de rede.
- Uma lista das vulnerabilidades ou serviços abertos que foram descobertos no ativo varrido.
- Várias maneiras de categorizar e ordenar sua lista de vulnerabilidades ou serviços abertos, por exemplo, **Risco**, **Severidade** e **Pontuação**.
- Uma maneira rápida de visualizar informações de vulnerabilidade e serviços abertos. Na barra de ferramentas, clique em **Vulnerabilidades** ou **Serviços Abertos**.
- Uma maneira fácil de visualizar informações detalhadas sobre o ativo varrido. Na barra de ferramentas, clique em **Detalhes do Ativo**.
- Um método alternativo de criar uma exceção de vulnerabilidade. Na barra de ferramentas, clique em **Ações** > **Exceção**.

O ícone de cuidado indica que a varredura falhou. Passe o mouse sobre o ícone para obter detalhes adicionais.

Para obter mais informações sobre a janela Detalhes do Ativo, consulte o *Guia do Usuário* do produto.

Conceitos relacionados:

Capítulo 8, “Regras de Exceção de Vulnerabilidade”, na página 79
No IBM Security QRadar Vulnerability Manager, é possível configurar regras de exceção para minimizar o número de vulnerabilidades positivo falso.

Visualizando o Status de Downloads de Correção de Ativo

Visualize se um ativo possui um download de correção pendente. Se houver downloads pendentes, o ativo terá todas as correções disponíveis.

Procedimento

1. Procure o ativo para o qual você deseja confirmar o status da correção.
2. Clique no endereço IP do ativo para abrir a janela **Detalhes do Ativo**.
3. Clique em **Detalhes** > **Propriedades** para abrir a janela **Propriedades do Ativo**.

4. Clique na seta **Correções do Windows**.
5. Visualize o status da correção na coluna **Pendente**.
   - Verdadeiro - o ativo possui correções pendentes para download.
   - Falso - o ativo não possui downloads de correção pendentes.

Severidade de PCI e Risco de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível revisar o risco e a gravidade de payment card industry (PCI) para cada vulnerabilidade localizada por uma varredura.

É possível revisar as informações a seguir:

- O nível de risco associado a cada vulnerabilidade.
- O número de ativos em sua rede na qual uma vulnerabilidade específica foi localizada.

Para investigar uma vulnerabilidade, é possível clicar no link de uma vulnerabilidade na coluna **Vulnerabilidade**.

Enviando E-mail aos Proprietários de Ativos Quando Varreduras de Vulnerabilidade Começarem e Pararem

Envie um e-mail aos responsáveis técnicos configurados para alertá-los sobre o planejamento de varredura. Também é possível enviar por e-mail relatórios aos proprietários de ativo.

Antes de Iniciar

Configure o servidor de correio do sistema e responsáveis técnicos de ativos. Para obter informações adicionais, consulte o *IBM Security QRadar SIEM Administration Guide*.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Clique em **Administrativo** > **Perfis de Varreduras**.
3. Na linha designada para a varredura a ser editada, marque a caixa de seleção e clique em **Editar** na barra de ferramentas.
4. Na área **O que Enviar por Email** da guia **Email**, marque as caixas de seleção adequadas.
5. Caso você tenha marcado a caixa de seleção **Relatórios**, no campo **Relatórios Disponíveis**, selecione os relatórios a serem enviados por email e clique na seta para mover os relatórios para o campo **Relatórios Selecionados**.

   Os relatórios podem ser grandes. Confirme se os relatórios enviados não foram rejeitados pelo provedor de e-mail do destinatário.
6. Na área **O Que Enviar por E-mail**, selecione os destinatários que você deseja que receba os e-mails:
   - Para enviar um e-mail aos responsáveis técnicos dos ativos digitalizados, marque a caixa de seleção **Responsáveis Técnicos**. Responsáveis técnicos recebem e-mail sobre seus ativos apenas.
   - Para inserir ou selecionar endereços de e-mail no campo, marque a caixa de seleção **Endereços Para**. Selecione emails e clique em **Incluir-me** para enviar

aos destinatários de email selecionados. Os endereços de e-mail inseridos recebem e-mails e relatórios sobre todos os ativos digitalizados.

7. Clique em **Salvar**.

Capítulo 7. Gerenciamento das Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível gerenciar, procurar e filtrar dados de vulnerabilidade para ajudá-lo a focar nas vulnerabilidades que representam o maior risco à organização.

Os dados de vulnerabilidade exibidos são baseados nas informações de status de vulnerabilidade que são mantidas no modelo de ativo do QRadar. Estas informações incluem as vulnerabilidades que são localizadas pelo scanner do QRadar Vulnerability Manager e as vulnerabilidades que são importadas dos produtos externos de varredura.

Gerencie as vulnerabilidades para fornecer as informações a seguir:

- Uma visualização de rede da variação da vulnerabilidade atual.
- Identificar as vulnerabilidades que apresentam o maior risco à organização e designar as vulnerabilidades aos usuários do QRadar para correção.
- Estabelecer o quão amplamente a rede é impactada pelas vulnerabilidades e exibir as informações detalhadas sobre os recursos de rede que contêm as vulnerabilidades.
- Decidir quais vulnerabilidades representam menos riscos à organização e criar exceções de vulnerabilidade.
- Exibir informações históricas sobre as vulnerabilidades na rede.
- Exibir dados de vulnerabilidade por rede, ativo, vulnerabilidade, serviço aberto ou instância de vulnerabilidade.

Investigando Pontuações de Risco de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível investigar pontuações de risco de vulnerabilidade e entender como cada pontuação é calculada.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Opcional: Clique na coluna **Pontuação de Risco** para classificar as vulnerabilidades por risco.
4. Para investigar a pontuação de risco, passe o mouse sobre uma pontuação de risco de vulnerabilidade.

Detalhes de Pontuação de Risco

No IBM Security QRadar Vulnerability Manager, as pontuações de risco de vulnerabilidade fornecem uma indicação do risco que uma vulnerabilidade representa para a organização.

Usando o IBM Security QRadar Risk Manager, é possível configurar políticas que ajustam pontuações de risco de vulnerabilidade e chamam a atenção para as tarefas de correção importantes.

Pontuação de Risco

A **Pontuação de Risco** fornece o contexto de rede específico usando métricas de base, temporais e ambientais do Common Vulnerability Scoring System (CVSS).

Quando o QRadar Risk Manager não estiver licenciado, a coluna **Pontuação de Risco** mostrará a pontuação da métrica ambiental do CVSS com um valor máximo de 10.

Subpontuação de Explorabilidade

A explorabilidade é calculada como um subconjunto da pontuação de base do CVSS, usando os elementos a seguir:

- O Vetor de Acesso fornece uma indicação de risco baseada na distância, por exemplo, local, rede adjacente ou rede, de um intruso.
- A Complexidade de Acesso fornece uma indicação de risco baseada na complexidade do ataque. Quanto mais baixa a complexidade maior o risco.
- A Autenticação fornece uma indicação de risco baseada em tentativas de autenticação. Quanto menos tentativas maior o risco.

Ajustes de Risco

Se o IBM Security QRadar Risk Manager for instalado e você tiver configurado políticas de risco de vulnerabilidade, os ajustes de riscos serão listados. Os ajustes aumentam ou diminuem o risco geral associado a uma vulnerabilidade.

Conceitos relacionados:

"Integração do IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager" na página 23
O IBM Security QRadar Vulnerability Manager se integra ao QRadar Risk Manager para ajudá-lo a priorizar os riscos e vulnerabilidades na rede.

Tarefas relacionadas:

"Priorizando Vulnerabilidades de Alto Risco Aplicando Políticas de Risco" na página 74
No IBM Security QRadar Vulnerability Manager, é possível alertar os administradores para vulnerabilidades de risco mais alto, aplicando políticas de riscos à vulnerabilidades.

Procurando Dados de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível identificar vulnerabilidades importantes procurando os dados de vulnerabilidade.

O QRadar Vulnerability Manager fornece vários métodos para procurar os dados. É possível procurar por rede, ativo, serviço aberto ou vulnerabilidade.

As procuras salvas padrão fornecem um método rápido de identificar o risco para a organização. Procuras salvas são exibidas no campo **Procuras Salvas Disponíveis** na página Procura do Gerenciador de Vulnerabilidade.

Antes de Iniciar

Você deve criar um perfil de varredura e varrer seus ativos de rede.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.
4. Se quiser carregar uma procura salva, execute as etapas a seguir:
   a. Opcional: Selecione um grupo da lista **Grupo**.
   b. Opcional: No campo **Digitar Procura Salva**, digite a procura salva que deseja carregar.
   c. Na lista **Procuras Salvas Disponíveis**, selecione uma procura salva e clique em **Carregar**.
   d. Clique em **Procurar**.
5. Se quiser criar uma nova procura, execute as etapas a seguir na área de janela Parâmetros de Procura:
   a. Na **primeira lista**, selecione o parâmetro que deseja usar.
   b. Na **segunda lista**, selecione um modificador de procura. Os modificadores que estão disponíveis dependem do parâmetro de procura selecionado.
   c. Na **terceira lista**, digite ou selecione as informações específicas relacionadas ao parâmetro de procura.
   d. Clique em **Incluir filtro**.

   Por exemplo, para enviar um email das vulnerabilidades designadas para um usuário técnico, selecione **Contato do Proprietário Técnico** e forneça um endereço de email que esteja configurado na página Designação de Vulnerabilidade.
6. Clique em **Procurar**.
7. Opcional: Na barra de ferramentas, clique em **Salvar Critérios de Procura**.

   Importante: Os relatórios de vulnerabilidades usam informações de procura salvas. Se você desejar criar um relatório com um email para um usuário técnico, você deverá salvar seus critérios de procura.

Conceitos relacionados:

"Parâmetros de Procura de Vulnerabilidade" na página 68
No IBM Security QRadar Vulnerability Manager, é possível procurar os dados de vulnerabilidade e salvar as procuras para uso posterior.

Procuras rápidas de vulnerabilidade

Procure vulnerabilidades digitando uma sequência de procura de texto que usa palavras ou frases simples.

No IBM Security QRadar Vulnerability Manager, é possível usar procuras rápidas para filtrar vulnerabilidades nas páginas Minhas Vulnerabilidades Designadas e Gerenciar Vulnerabilidades.

Use a lista **Procuras Rápidas** para fazer uma procura de vulnerabilidades pré-configurada.

Use o campo **Filtro Rápido** para criar seus próprios filtros de vulnerabilidade. Clique em **Salvar Critérios de Procura** para incluir seus filtros rápidos de vulnerabilidade na lista **Procuras Rápidas**.

Tabela 4. Diretrizes de sintaxe do filtro rápido de vulnerabilidade

Descrição	Exemplo

Inclua qualquer texto simples que você espera encontrar em título de vulnerabilidade, descrição, solução, interesse, tipo de ID de referência ou valor do ID de referência.	`2012-3764`
	
	`MS203`
	
	`java`

Para procurar apenas o texto no título da vulnerabilidade, inclua **:A** na sequência de texto da procura	`PHP:A`
Para procurar apenas o texto na descrição da vulnerabilidade, inclua **:B** na sequência de texto da procura	`cross-site scripting:B`
Para procurar apenas o texto no tipo de referência de vulnerabilidade externa, inclua **:C** na sequência de texto da procura	`RedHat RHSA:C`
Incluir caracteres curinga. O termo de procura não pode começar com um curinga.	`SSLv*`

Agrupar termos com operadores lógicos: **AND**, **OR** e **NOT** (ou **!**). Para serem reconhecidos como operadores lógicos e não como termos de procura, os operadores devem estar em letras maiúsculas.	`PHP AND Traversal`
	
	`XSS:A OR cross-site scripting:A`
	
	`!MySQL`
	
	`NOT MySQL`

Tarefas relacionadas:

"Salvando Seus Critérios de Procura de Vulnerabilidade" na página 70
No IBM Security QRadar Vulnerability Manager, é possível salvar os critérios de procura de vulnerabilidade para uso futuro.

Parâmetros de Procura de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível procurar os dados de vulnerabilidade e salvar as procuras para uso posterior.

A tabela a seguir não é uma lista completa de parâmetros de procura de vulnerabilidade, mas um subconjunto das opções disponíveis.

Selecione qualquer um dos parâmetros para procurar e exibir dados de vulnerabilidade.

Tabela 5. Parâmetros de Procura de Vulnerabilidade

Opção	Descrição
Complexidade de Acesso	A complexidade do ataque que é necessária para explorar uma vulnerabilidade.
Vetor de Acesso	O local de rede a partir do qual uma vulnerabilidade pode ser explorada.
Procura salva de ativo	O host, endereço IP ou intervalo de endereços IP associados a uma procura salva de ativo. Para obter mais informações sobre como salvar as procuras de ativo, consulte o *Guia de Usuários* para o produto.
Ativos com Serviço Aberto	Recursos que possuem serviços abertos específicos. Por exemplo, HTTP, FTP e SMTP.
Autenticação	O número de vezes que um invasor deve ser autenticado em relação a um destino para explorar uma vulnerabilidade.
Impacto da Disponibilidade	O nível que a disponibilidade do recurso poderá ser comprometida, se uma vulnerabilidade for explorada.

Tabela 5. Parâmetros de Procura de Vulnerabilidade (continuação)

Opção	Descrição
Impacto de Confidencialidade	O nível de informações confidenciais que poderão ser obtidas, se uma vulnerabilidade for explorada.
Dias desde a localização do ativo	O número decorrido de dias desde a descoberta do ativo com a vulnerabilidade na rede. Os recursos podem ser descobertos por uma varredura ativa ou passivamente usando as análise de fluxo ou log.
Dias desde o tráfego do serviço associado de vulnerabilidade	Exibe as vulnerabilidades em ativos com o tráfego de camada 7 associado a/de um ativo, com base no número de dias decorrido desde que o tráfego foi detectado.
Domínio	Caso você tenha configurado o IBM Security QRadar para sistemas com vários domínios, use essa opção para especificar o domínio no qual você deseja procurar vulnerabilidades.
Por Serviço Aberto	Use este parâmetro para procurar vulnerabilidades que estão associadas a serviços abertos específicos, como HTTP, FTP e SMTP.
Tipo de Referência Externa	Vulnerabilidades que possuem um fixlet do Endpoint Manager associado. Usando esse parâmetro, é possível mostrar apenas as vulnerabilidades, sem uma correção disponível.
Impacto	O impacto potencial à organização. Por exemplo, perda de controle de acesso, tempo de inatividade e perda de reputação.
Incluir avisos antecipados	As vulnerabilidades publicadas recentemente que são detectadas na rede, sem executar a varredura adicional.
Incluir exceções de vulnerabilidade	Aquelas vulnerabilidades com uma regra de exceção aplicada.
Impacto da Integridade	O nível ao qual a integridade do sistema poderá ser comprometida, se uma vulnerabilidade for explorada.
Incluir apenas ativos com risco	As vulnerabilidades que passam ou falham políticas de riscos específicos que são definidas e monitoradas no IBM Security QRadar Risk Manager. **Nota:** Deve-se monitorar pelo menos uma pergunta na página Monitor de Política na guia **Riscos** para usar esse parâmetro de procura.
Incluir apenas ativos com risco transmitido	Vulnerabilidades aprovadas em políticas de risco específicas que são definidas e monitoradas no QRadar Risk Manager.
Incluir apenas avisos antecipados	Use este parâmetro para incluir apenas as vulnerabilidades publicadas recentemente que são detectadas na rede, sem executar a varredura adicional na procura.
Incluir apenas Exceções de Vulnerabilidade	Use este parâmetro para incluir apenas as vulnerabilidades com uma regra de exceção aplicada na procura.
Vencido por Dias	Use este parâmetro para procurar as vulnerabilidades que estão vencidas para correção por um determinado número de dias.
Status da Correção	Use este parâmetro para filtrar as vulnerabilidades por status da correção. Para obter mais informações, consulte "Identificando o Status da Correção das Vulnerabilidades" na página 76.
Gravidade de PCI	Use este parâmetro para procurar vulnerabilidade pelo nível de Gravidade de PCI (Alto, Médio ou Baixo) designado pelo serviço de conformidade de PCI. As vulnerabilidades que recebem um nível de Gravidade de PCI Alto ou Médio falham na conformidade de PCI.
Procura Rápida	É possível procurar vulnerabilidades de um título, descrição, solução e ID de referência externa. No campo **Procura Rápida**, é possível usar os operadores AND, OR e NOT e colchetes.
Risco	Use este parâmetro para procurar vulnerabilidades por nível de risco (Alto, Médio, Baixo, Aviso).
Não designado	Use este parâmetro para procurar vulnerabilidades que não têm um usuário designado para corrigi-las.
Referência Externa de Vulnerabilidade	As vulnerabilidades que são baseadas em uma lista de IDs de vulnerabilidade importados, por exemplo ID de CVE. Para obter mais informações sobre Conjuntos de Referências, consulte o *Guia de Administração* para o produto.
Vulnerabilidade possui uma correção virtual do fornecedor	As vulnerabilidades que podem ser corrigidas por um sistema de prevenção de intrusão.
Estado de vulnerabilidade	O status da vulnerabilidade desde a última varredura da rede ou ativos de rede específicos. Por exemplo, ao varrer ativos, as vulnerabilidades descobertas são, Novo, Preexistente, Corrigido ou Existente.
Vulnerabilidade com risco	Use este parâmetro para filtrar as vulnerabilidades pelos resultados da política de riscos. Deve-se monitorar pelo menos uma pergunta na página Monitor de Política na guia **Riscos** para usar esse parâmetro de procura.

Salvando Seus Critérios de Procura de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível salvar os critérios de procura de vulnerabilidade para uso futuro.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura** e conclua a procura dos dados.
4. Na barra de ferramentas, clique em **Salvar Critérios de Procura**.
5. Na janela Salvar Critérios de Procura, digite um nome reconhecível para a procura salva.
6. Opcional: Para incluir a procura salva na lista **Procuras Rápidas**, na barra de ferramentas, clique em **Incluir em Minhas Procuras Rápidas**.
7. Opcional: Para compartilhar os critérios de procura salva com todos os usuários do QRadar, clique em **Compartilhar com Todos**.
8. Opcional: Para colocar a procura salva em um grupo, clique em um grupo ou em **Gerenciar Grupos** para criar um novo grupo.

   Para obter mais informações sobre como gerenciar grupos de procuras, consulte o *Guia de Administração* para o produto.
9. Opcional: Se você desejar mostrar os resultados da procura salva ao clicar em qualquer uma das páginas Gerenciar Vulnerabilidades na área de janela de navegação, clique em **Configurar Como Padrão**.
10. Clique em **OK**.

Excluindo Critérios de Procura de Vulnerabilidade Salva

No IBM Security QRadar Vulnerability Manager, é possível excluir os critérios de procura de vulnerabilidade salva.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Gerenciar Vulnerabilidades** > **Por Rede**
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.
4. Na página Busca do Gerenciador de Vulnerabilidade, na lista **Procuras Salvas Disponíveis**, selecione a procura salva que deseja excluir.
5. Clique em **Excluir**.
6. Clique em **OK**.

Instâncias de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível exibir as vulnerabilidades em cada um dos recursos varridos de sua rede. Cada vulnerabilidade pode ser listada várias vezes porque a vulnerabilidade existe em vários de seus ativos.

Se você configurar scanners de avaliação de vulnerabilidades (VA) de terceiros, usando a guia **Admin** do QRadar, as vulnerabilidades que forem detectadas serão automaticamente exibidas na página Por Instâncias de Vulnerabilidade.

Para obter mais informações sobre scanners VA, consulte o *Guia de Administração* do seu produto.

A página Por Instâncias de Vulnerabilidade fornece as seguintes informações:

- Uma visualização de cada vulnerabilidade que foi detectada pela varredura de seus ativos de rede.
- O risco que cada vulnerabilidade apresenta para o Payment Card Industry (PCI).
- O risco que uma vulnerabilidade apresenta para sua organização. Clique na coluna **Pontuação de Risco** para identificar as vulnerabilidades de mais alto risco.
- O nome ou endereço de email do usuário designado para corrigir a vulnerabilidade.
- O número de dias em que a vulnerabilidade deve ser corrigida.

Conceitos relacionados:

"Detalhes de Pontuação de Risco" na página 65
No IBM Security QRadar Vulnerability Manager, as pontuações de risco de vulnerabilidade fornecem uma indicação do risco que uma vulnerabilidade representa para a organização.

Vulnerabilidades de Rede

No IBM Security QRadar Vulnerability Manager, é possível revisar os dados de vulnerabilidade agrupados por rede.

A página Por Rede fornece as informações a seguir:

- Uma pontuação de risco acumulada baseada nas vulnerabilidades detectadas em cada uma de suas redes.
- O número de ativos, vulnerabilidades e serviços abertos para cada rede.
- O número de vulnerabilidades designadas para um usuário técnico e que estão vencidas para correção.

Vulnerabilidades de ativo

No IBM Security QRadar Vulnerability Manager, é possível exibir os dados de vulnerabilidade de resumo agrupados para cada recurso varrido.

É possível usar a página Por Recurso para priorizar as tarefas de correção para recursos de sua organização que apresentem maior risco.

A página Por Ativo fornece as informações a seguir:

- Uma pontuação de risco acumulada baseada nas vulnerabilidades detectadas em cada um de seus ativos.

  Clique na coluna **Pontuação de Risco** para classificar seus ativos por seu risco.
- O número de vulnerabilidades de recursos designadas para um usuário técnico e que estão vencidas para correção.

Vulnerabilidades de Serviço Aberto

No IBM Security QRadar Vulnerability Manager, é possível exibir dados de vulnerabilidade agrupados por serviço aberto.

A página Por Serviço Aberto mostra uma pontuação de risco acumulada e uma contagem de vulnerabilidade para cada serviço de sua rede inteira.

Investigando o Histórico de uma Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível exibir informações úteis sobre o histórico de uma vulnerabilidade.

Por exemplo, é possível investigar informações sobre como a pontuação de risco de uma vulnerabilidade foi calculada. Também é possível revisar informações sobre quando uma vulnerabilidade foi descoberta pela primeira vez e a varredura que foi usada para descobrir a vulnerabilidade.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Opcional: Procure os dados de vulnerabilidade.
4. Clique na vulnerabilidade que deseja investigar.
5. Na barra de ferramentas, selecione **Ações** > **Histórico**.

Tarefas relacionadas:

"Procurando Dados de Vulnerabilidade" na página 66
No IBM Security QRadar Vulnerability Manager, é possível identificar vulnerabilidades importantes procurando os dados de vulnerabilidade.

Reduzindo o Número de Vulnerabilidades Positivas Falsas

No IBM Security QRadar Vulnerability Manager, é possível criar regras de exceção automaticamente para as vulnerabilidades associadas a um tipo específico de servidor.

Ao configurar os tipos de servidor, o QRadar Vulnerability Manager criará regras de exceção e reduzirá automaticamente as vulnerabilidades retornadas pela procura de dados.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, selecione **Descoberta de Servidor**.
3. Para criar automaticamente regras de exceção positivas falsas para as vulnerabilidades nos tipos de servidores específicos, na lista **Tipo de Servidor**, selecione uma das opções a seguir:
   - Servidores FTP
   - Servidores do Sistema de Nomes de Domínio
   - Servidores de Correio
   - Servidores da Web

   Pode demorar alguns minutos para o campo **Portas** ser atualizado.
4. Opcional: Na lista **Rede**, selecione a rede para os servidores.
5. Clique em **Descobrir Servidores**.
6. Na área de janela Servidores Correspondentes, selecione os servidores nos quais as regras de exceção de vulnerabilidade são criadas.
7. Clique em **Aprovar Servidores Selecionados**.

Resultados

Dependendo da seleção do tipo de servidor as vulnerabilidades a seguir serão automaticamente configuradas como regras de exceção positivas falsas:

Tabela 6. Vulnerabilidades do Tipo de Servidor

Tipo de Servidor	Vulnerability
Servidores FTP	**Servidor FTP Presente**
Servidores do Sistema de Nomes de Domínio	**O Servidor do Sistema de Nomes de Domínio Está em Execução**
Servidores de Correio	**Servidor SMTP Detectado**
Servidores da Web	**O Serviço da Web Está em Execução**

Investigando Vulnerabilidades e Recursos de Alto Risco

Em IBM Security QRadar Vulnerability Manager, é possível investigar as vulnerabilidades de alto risco que podem ser suscetíveis à exploração.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na página Por Instâncias de Vulnerabilidade, clique no título da coluna **Pontuação de Risco** para classificar as vulnerabilidades por pontuação de risco.
4. Passe o mouse sobre o campo **Pontuação de risco** para investigar as métricas de CVSS usadas para derivar a pontuação de risco.
5. Identifique a vulnerabilidade que tem a pontuação mais alta e clique no link **Vulnerabilidade**.
6. Na janela Detalhes de vulnerabilidade, investigue a vulnerabilidade:
   a. Para visualizar o website do IBM Security Systems, clique no link **X-Force**.
   b. Clique no link **CVE** para visualizar o website do National Vulnerability Database.

      O website do IBM Security Systems e o National Vulnerability Database fornecem informações de correção e detalhes sobre como uma vulnerabilidade pode afetar a organização.
   c. Para abrir a janela Corrigindo para a vulnerabilidade, clique no link **Detalhes de plug-in**. Use as guias para descobrir a Definição Oval, a Base de Conhecimento do Windows ou informações de recomendação do UNIX sobre a disponibilidade. Esse recurso fornece informações sobre como o QRadar Vulnerability Manager verifica os detalhes de vulnerabilidade durante uma varredura de correção. É possível usá-lo para identificar por que uma vulnerabilidade aumentou ou não em um ativo.
   d. A caixa de texto **Solução** contém informações detalhadas sobre como corrigir uma vulnerabilidade.

Conceitos relacionados:

"Detalhes de Pontuação de Risco" na página 65
No IBM Security QRadar Vulnerability Manager, as pontuações de risco de vulnerabilidade fornecem uma indicação do risco que uma vulnerabilidade representa para a organização.

Priorizando Vulnerabilidades de Alto Risco Aplicando Políticas de Risco

No IBM Security QRadar Vulnerability Manager, é possível alertar os administradores para vulnerabilidades de risco mais alto, aplicando políticas de riscos à vulnerabilidades.

Ao aplicar uma política de risco, a pontuação de risco de uma vulnerabilidade será ajustada, permitindo aos administradores priorizar com mais precisão as vulnerabilidades que requerem atenção imediata.

Neste exemplo, a pontuação de risco de vulnerabilidade é automaticamente aumentada por um fator de porcentagem para qualquer vulnerabilidade que permanecer ativa na rede após 40 dias.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na barra de ferramentas, clique em **Procura** > **Nova Procura**.
4. Na área de janela Parâmetros de Procura, configure os filtros a seguir:
   a. **Iguais de Alto Risco**
   b. **Dias desde a descoberta das vulnerabilidades, maior ou igual a 40**
5. Clique em **Procura** e, em seguida, na barra de ferramentas, clique em **Salvar Critérios de Procura**.

   Digite um nome de procura salva identificável no QRadar Risk Manager.
6. Clique na guia **Riscos**.
7. Na área de janela de navegação, clique em **Monitor de Política**.
8. Na barra de ferramentas, clique em **Ações** > **Novo**.
9. No campo **O Que Deseja para Nomear Esta Pergunta**, digite um nome.
10. No campo **Quais Testes Deseja Incluir na Pergunta**, clique em **são suscetíveis às vulnerabilidades contidas em procuras salvas de vulnerabilidade**.
11. No campo **Localizar Recursos Que**, clique no parâmetro sublinhado em **são suscetíveis às vulnerabilidades contidas em procuras salvas de vulnerabilidade**.
12. Identifique a procura salva da vulnerabilidade de alto risco do QRadar Vulnerability Manager, clique em **Incluir**, em seguida, clique em **OK**.
13. Clique em **Salvar Pergunta**.
14. Na área de janela Perguntas, selecione a pergunta na lista e, na barra de ferramentas, clique em **Monitor**.

    Restrição: O campo **Descrição do Evento** é obrigatório.
15. Clique em **Enviar Eventos Aprovados na Pergunta**.
16. No campo **Ajustes de Pontuação de Vulnerabilidade**, digite um valor de porcentagem de ajuste de risco no campo **Ajuste de Pontuação de Vulnerabilidade de Porcentagem na Falha da Pergunta**.
17. Clique em **Aplicar Ajuste a Todas as Vulnerabilidades em Um Ativo**, em seguida, clique em **Salvar Monitor**.

O que Fazer Depois

Na guia **Vulnerabilidades**, é possível procurar as vulnerabilidades de alto risco e priorizá-las

Conceitos relacionados:

"Integração do IBM Security QRadar Risk Manager e IBM Security QRadar Vulnerability Manager" na página 23
O IBM Security QRadar Vulnerability Manager se integra ao QRadar Risk Manager para ajudá-lo a priorizar os riscos e vulnerabilidades na rede.

Tarefas relacionadas:

"Salvando Seus Critérios de Procura de Vulnerabilidade" na página 70
No IBM Security QRadar Vulnerability Manager, é possível salvar os critérios de procura de vulnerabilidade para uso futuro.

Configurando Cores de Exibição Customizadas para Pontuações de Risco

Configure códigos de cor customizados para pontuações de risco do IBM Security QRadar Vulnerability Manager para visualizar pontuações de risco com códigos de cor nas interfaces do QRadar Vulnerability Manager.

Procedimento

1. No IBM Security QRadar, selecione **Vulnerabilidades** > **Atribuição de Vulnerabilidade** > **Preferências de Risco**.
2. Na coluna **Maior que ou igual a**, insira o valor mínimo da pontuação de risco para Alto, Médio, Baixo e Aviso.
3. Na coluna **Cor**, selecione ou defina uma cor para representar pontuações de risco Alta, Média, Baixa e Aviso.

Identificando vulnerabilidades com uma correção do IBM Security Endpoint Manager

No IBM Security QRadar Vulnerability Manager, é possível identificar as vulnerabilidades que têm uma correção disponível.

Após identificar as vulnerabilidades que têm uma correção disponível, é possível investigar informações detalhadas sobre a correção na janela Detalhes da Vulnerabilidade.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**
4. Na área de janela Parâmetros de Procura configure as opções a seguir:
   a. Na **primeira lista** selecione **Referência de Tipo Externa**.
   b. Na **segunda lista** selecione **Iguais**.
   c. Na **terceira lista** selecione **Correção do IBM Endpoint Manager**.
   d. Clique em **Incluir filtro**.
   e. Clique em **Procurar**.

      A página Por Instâncias de Vulnerabilidade mostra as vulnerabilidades que têm uma correção disponível.

5. Opcional: Solicite as vulnerabilidades de acordo com sua importância, clicando no título da coluna **Pontuação de Risco**.
6. Opcional: Para investigar informações de correção para uma vulnerabilidade, clique em um link de vulnerabilidade na coluna **Vulnerabilidade**.
7. Opcional: Na janela Detalhes da Vulnerabilidade, role para a parte inferior da janela para visualizar as informações de correção de vulnerabilidade.

   O **ID do Site** e o **ID do Fixlet** são identificadores exclusivos usados para a aplicação de correções de vulnerabilidades, usando o IBM Security Endpoint Manager.

   A coluna **Base** indica uma referência exclusiva que você pode usar para acessar mais informações sobre uma base de conhecimento.

Identificando o Status da Correção das Vulnerabilidades

No IBM Security QRadar Vulnerability Manager, é possível identificar o status da correção das suas vulnerabilidades.

Filtrando as vulnerabilidades corrigidas, é possível priorizar seus esforços de correção nas vulnerabilidades mais críticas na organização.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.
4. Na **primeira lista** na área de janela Parâmetros de Procura, selecione **Status da Correção**.
5. Na **segunda lista**, selecione um modificador de procura.
6. Para filtrar as vulnerabilidades de acordo com seu status da correção, selecione uma das opções a seguir na terceira lista:

Opção	Descrição
Downloads Pendentes	Selecione esta opção para mostrar as vulnerabilidades que são planejadas para serem corrigidas
Reinício Pendente	Selecione esta opção para mostrar as vulnerabilidades corrigidas após a reinicialização do ativo digitalizado
Fixos(as)	Selecione esta opção para mostrar as vulnerabilidades corrigidas pelo IBM Security Endpoint Manager

7. Clique em **Incluir filtro**.
8. Clique em **Procurar**.

Conceitos relacionados:

"Integração do IBM Security Endpoint Manager" na página 24
O IBM Security QRadar Vulnerability Manager se integra ao IBM Security Endpoint Manager para ajudar a filtrar e priorizar as vulnerabilidades que podem ser corrigidas.

Removendo dados de vulnerabilidade indesejados

Use a funcionalidade de limpeza de vulnerabilidades do QRadar Vulnerability Manager para remover dados de vulnerabilidade antigos do modelo de ativo.

Sobre Esta Tarefa

Todos os cenários a seguir podem deixar dados de vulnerabilidade indesejados:

- Mudança do tipo de scanner
- Ativos descontinuados
- Mudança do endereço IP
- Varreduras imprecisas ou de teste

Importante: Depois de removidos, os dados de vulnerabilidade de um tipo de ativo ou scanner não podem ser recuperados.

Procedimento

Existem duas opções para a remoção de dados de vulnerabilidade indesejados:

- Use a opção **Ações** > **Limpar Vulnerabilidades (Todos)** na página Ativos para remover todos os dados de vulnerabilidade para um tipo de scanner selecionado.
- Use a opção **Ações** > **Limpar Vulnerabilidades (Ativo)** na página Detalhes do Ativo para remover todos os dados de vulnerabilidade para um ativo específico com um tipo de scanner selecionado.

Configurando períodos de retenção de dados de vulnerabilidade

É possível configurar o período de retenção para dados de tendências de vulnerabilidade e os resultados da varredura na janela Configuração do Gerenciador de Perfis de Ativo.

Sobre Esta Tarefa

Use as regras de configuração na seção **Retenção de Vulnerabilidade do QVM** da janela Configuração do Gerenciador de Perfis de Ativo para definir por quanto tempo o IBM Security QRadar Vulnerability Manager deve reter dados de tendências de vulnerabilidade e os resultados da varredura.

Procedimento

1. Clique em **Administrador** > **Configuração do Gerenciador de Perfis de Ativo**.
2. Na seção **Retenção de Vulnerabilidade do QVM** da janela Configuração do Gerenciador de Perfis de Ativo, insira valores nos seguintes campos:

Regra	Descrição	Valor Padrão
Dados de Relatórios de Tendências de Vulnerabilidade (em Dias)	Configura quantos dias o QRadar Vulnerability Manager deve reter dados de tendências de vulnerabilidade para serem usados em relatórios diários de vulnerabilidade.	14 dias

Regra	Descrição	Valor Padrão
Dados de Relatórios de Tendências de Vulnerabilidade (em Semanas)	Configura por quantas semanas o QRadar Vulnerability Manager deve reter dados de tendências de vulnerabilidade para serem usados em relatórios semanais de vulnerabilidade.	14 semanas
Dados de Relatórios de Tendências de Vulnerabilidade (em Meses)	Configura por quantos meses o QRadar Vulnerability Manager deve reter dados de tendências de vulnerabilidade para serem usados em relatórios mensais de vulnerabilidade.	14 meses
Limpar Resultados de Varredura Após Período (em Dias)	Use esta regra com **Limpar Resultados de Varredura Após Período (em Ciclos de Execução)** para configurar os limites de retenção para os dados de resultados de varreduras. Configura o número de dias que o QRadar Vulnerability Manager retém dados após a aplicação da regra de limitação **Limpar Resultados de Varredura Após Período (em Ciclos de Execução)**.	30 dias
Limpar Resultados de Varredura Após Período (em Ciclos de Execução)	Use esta regra com **Limpar Resultados de Varredura Após Período (em Dias)** para configurar os limites de retenção para os dados de resultados de varreduras. Configura quantas versões de dados de resultados de varredura são retidas pelo QRadar Vulnerability Manager. Esta regra tem precedência sobre o valor configurado em **Limpar Resultados de Varredura Após Período (em Dias)**. Para os valores padrão para as regras **Limpar Resultados de Varredura Após Período (em Dias)** e **Limpar Resultados de Varredura Após Período (em Ciclos de Execução)**: • O QRadar Vulnerability Manager retém os dados de resultados de varreduras para os 3 ciclos de execução mais recentes. Ele também retém outras versões dos resultados de varreduras executadas dentro do limite de 30 dias. • Se algum dos 3 ciclos de execução mais recentes tiver ocorrido além do limite de 30 dias, o QRadar Vulnerability Manager retém os dados de resultados de varreduras desses ciclos de execução.	3 ciclos de execução

3. Clique em **Salvar**.

Capítulo 8. Regras de Exceção de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível configurar regras de exceção para minimizar o número de vulnerabilidades positivo falso.

Quando se aplica regras de exceção às vulnerabilidades, você reduz o número de vulnerabilidades exibidas nos resultados da procura.

Se você criar uma exceção de vulnerabilidade, a vulnerabilidade não será removida do QRadar Vulnerability Manager.

Visualizando Regras de Exceção

Para exibir exceções de vulnerabilidade, é possível procurar seus dados de vulnerabilidade usando filtros de procura.

Para visualizar as regras de exceção, clique na guia **Vulnerabilidades** e, em seguida, clique em **Exceção de Vulnerabilidade** na área de janela de navegação.

Tarefas relacionadas:

"Reduzindo o Número de Vulnerabilidades Positivas Falsas" na página 72
No IBM Security QRadar Vulnerability Manager, é possível criar regras de exceção automaticamente para as vulnerabilidades associadas a um tipo específico de servidor.

Aplicando uma Regra de Exceção de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível aplicar manualmente uma regra de exceção de vulnerabilidade a uma vulnerabilidade que você decidir que não representa uma ameaça significante.

Se você aplicar uma regra de exceção, a vulnerabilidade não será mais exibida nos resultados da procura do QRadar Vulnerability Manager. Entretanto, a vulnerabilidade não será removida do QRadar Vulnerability Manager.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades** > **Por Rede**.
3. Opcional: Procure os dados de vulnerabilidade. Na barra de ferramentas, clique em **Procura** > **Nova Procura**.
4. Clique no link da coluna **Instâncias de Vulnerabilidade**.
5. Selecione a vulnerabilidade para a qual deseja criar uma regra de exceção.
6. Na barra de ferramentas, selecione **Ações** > **Exceção**.

   Para aplicar uma regra de exceção de vulnerabilidade, o único campo obrigatório é a caixa de texto **Comentário**. Todos os outros parâmetros são opcionais.
7. Opcional: Na janela Manter Regra de Exceção, escolha uma das seguintes opções:
   - Digite uma data em que a exceção de vulnerabilidade deve expirar.

- Se a exceção de vulnerabilidade não deve expirar nunca, clique em **Nunca Expira**.

8. Na seção Notas da janela Manter Regra de Exceção, digite o texto na caixa de texto**Comentários**.
9. Clique em **Salvar**.

Tarefas relacionadas:

"Procurando Dados de Vulnerabilidade" na página 66
No IBM Security QRadar Vulnerability Manager, é possível identificar vulnerabilidades importantes procurando os dados de vulnerabilidade.

Gerenciando Uma Regra de Exceção de Vulnerabilidade

Se você receber novas informações sobre uma vulnerabilidade, poderá atualizar ou remover uma regra de exceção de vulnerabilidade existente.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Exceção de Vulnerabilidade**.
3. Clique na vulnerabilidade que deseja gerenciar.
4. Na barra de ferramentas, selecione uma opção no menu **Ações**.

   Importante: Se você excluir uma regra de exceção de vulnerabilidade, nenhum aviso será exibido. A vulnerabilidade será excluída imediatamente.
5. Clique em **Salvar**.

Procurando Exceções de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível procurar os dados de vulnerabilidade e filtrar os resultados da procura para exibir exceções vulnerabilidade.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Gerenciar Vulnerabilidades** > **Por Ativo**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.
4. Para filtrar os dados de vulnerabilidade para incluir exceções vulnerabilidade na área de janela Parâmetros de Procura, selecione uma das opções a seguir:
   - Incluir exceções de vulnerabilidade

     Exibe todas as vulnerabilidades, incluindo as vulnerabilidades com uma regra de exceção aplicados a elas.
   - Incluir apenas exceções de vulnerabilidade

     Exibe apenas as vulnerabilidades com uma regra de exceção aplicadas a ela.
5. Clique em **Incluir filtro**.
6. Clique em **Procurar**.

Capítulo 9. Correção de Vulnerabilidade

No QRadar Vulnerability Manager, é possível designar vulnerabilidades para um usuário técnico para correção.

É possível designar vulnerabilidades para seu usuário técnico usando dois métodos.

- Designar vulnerabilidades individuais a um usuário técnico para correção.
- Designe um usuário técnico como o proprietário de grupos de recursos

Tarefas relacionadas:

"Configurando os tempos de correção para as vulnerabilidades em ativos designados" na página 83
No IBM Security QRadar Vulnerability Manager, é possível configurar os tempos de correção para diferentes tipos de vulnerabilidades.

Designando vulnerabilidades individuais para um usuário técnico para correção

No IBM Security QRadar Vulnerability Manager, é possível designar vulnerabilidades individuais para um usuário do QRadar para correção.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Gerenciar Vulnerabilidades**.
3. Opcional: Procure os dados de vulnerabilidade.
4. Selecione a vulnerabilidade que deseja designar para correção.
5. Na barra de ferramentas, clique em **Ações** > **Designar/Editar**.
6. Selecione um usuário técnico da lista **Usuário Designado**.

   Designe usuários técnicos na página Designação de Vulnerabilidade. Para obter mais informações, consulte "Designando um usuário técnico como proprietário de grupos de recursos".
7. Opcional: Na lista **Data de Vencimento**, selecione uma data futura em que a vulnerabilidade deverá ser corrigida.

   Se você não selecionar uma data, a **Data de Vencimento** será configurada como a data atual.
8. Opcional: No campo **Notas**, digite informações úteis sobre o motivo para a designação de vulnerabilidade.
9. Clique em **Salvar**.

Designando um usuário técnico como proprietário de grupos de recursos

No IBM Security QRadar Vulnerability Manager, é possível configurar grupos de ativos e automaticamente designar suas vulnerabilidades para usuários técnicos.

Após designar um usuário técnico e varrer os recursos, todas as vulnerabilidades nos ativos serão designadas para o usuário técnico para correção.

Os tempos de correção para as vulnerabilidades podem ser configurados, dependendo de seu risco ou gravidade.

Caso um novo ativo seja incluído na rede e esteja contido no grupo de ativos de um usuário técnico, as vulnerabilidades do ativo serão automaticamente designadas para o usuário técnico.

É possível enviar relatórios por email automaticamente para seus usuários técnicos com os detalhes das vulnerabilidades que eles são responsáveis por corrigir.

Antes de Iniciar

Se desejar configurar um grupo de ativos identificados por uma procura salva de ativos, você deverá procurar seus ativos e salvar os resultados.

Para obter mais informações sobre a procura de ativos e salvamento dos resultados, consulte o *Guia do Usuário* de seu produto.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Designação de Vulnerabilidade**.
3. Na barra de ferramentas, clique em **Incluir**.
4. Digite um nome, endereço de email e intervalo de CIDR.

   Para designar automaticamente um usuário técnico na janela Novo Proprietário do Ativo, os únicos campos obrigatórios serão **Nome**, **Email** e **CIDR**.
5. Caso você tenha configurado o IBM Security QRadar para vários domínios, selecione o domínio relevante na lista **Domínios**.
6. Para filtrar a lista de ativos em seu intervalo de CIDR por nome de ativo, digite uma sequência de texto no campo **Filtro do Nome do Ativo**.
7. Para filtrar a lista de ativos em seu intervalo de CIDR por sistema operacional, digite uma sequência de texto no campo **Filtro de S.O.**.
8. Opcional: Clique em **Procura de Ativos** para designar o usuário técnico para os recursos associados com uma procura de ativos salva.
9. Clique em **Salvar**.
10. Opcional: Na barra de ferramentas, clique em **Horários de Correção**.

    É possível configurar o tempo de correção para cada tipo de vulnerabilidade, dependendo de seu risco e gravidade.

    Por exemplo, talvez seja necessário corrigir vulnerabilidades de alto risco dentro de 5 dias.
11. Opcional: Na barra de ferramentas, clique em **Planejamento**.

    Por padrão, o contato do usuário técnico para seus ativos é atualizado a cada 24 horas.

    Novos ativos incluídos em sua implementação e que estão dentro do intervalo de CIDR que você especificou são atualizados automaticamente com o contato técnico especificado.

    Importante: O planejamento se aplica às associações que você fez entre os usuários técnicos e grupos de recursos.
12. Opcional: Clique em **Atualizar Agora** para configurar imediatamente o proprietário de seus ativos.

Dependendo do tamanho de sua implementação, talvez demore um pouco mais de tempo para a atualização de seus ativos.

13. Clique em **Salvar**.

    Quaisquer vulnerabilidades já designadas ao usuário técnico para correção serão atualizadas com o novo usuário técnico.

14. Se as vulnerabilidades não foram designadas anteriormente a um usuário técnico, você deverá varrer os recursos que designou ao usuário técnico.

    Importante: A varredura de ativos assegura que todas as vulnerabilidades designadas a um usuário técnico existam no ativo.

Configurando os tempos de correção para as vulnerabilidades em ativos designados

No IBM Security QRadar Vulnerability Manager, é possível configurar os tempos de correção para diferentes tipos de vulnerabilidades.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Designação de Vulnerabilidade**.
3. Selecione uma designação a partir da lista Proprietários do Ativo.
4. Na barra de ferramentas, clique em **Horários de Correção**.
5. Atualize os tempos de correção para as vulnerabilidades que são baseadas em seu risco e gravidade.
6. Clique em **Salvar**.

Capítulo 10. Relatórios de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível gerar ou editar um relatório existente ou usar o assistente de relatório para criar, planejar e distribuir um novo relatório.

O QRadar Vulnerability Manager contém vários relatórios padrão.

O assistente de relatório fornece um guia passo a passo sobre como projetar, planejar e gerar relatórios.

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

Enviando emails para usuários técnicos com suas vulnerabilidades designadas que requerem correção

Ao designar vulnerabilidades para um usuário técnico para correção, é possível gerar um relatório que é enviado por email para o usuário técnico.

O email contém informações sobre as vulnerabilidades que o usuário técnico deve corrigir.

Gerando relatórios de conformidade PCI

É possível gerar um relatório de conformidade para seus recursos PCI (segmento de cartões de pagamento).

O relatório de conformidade demonstra que você tomou todas as precauções de segurança necessárias para proteger seus recursos críticos.

Executando Um Relatório do QRadar Vulnerability Manager Padrão

No IBM Security QRadar Vulnerability Manager, é possível executar um relatório de gerenciamento de vulnerabilidades padrão.

Procedimento

1. Clique na guia **Relatórios**.
2. Na lista de relatórios, clique no relatório que deseja executar.

   Por exemplo, você pode desejar mostrar um relatório de visão geral da vulnerabilidade para os últimos sete dias.
3. Na barra de ferramentas, selecione **Ações** > **Executar Relatório**, em seguida, clique em **OK**.
4. Para visualizar o relatório concluído em um formato PDF, clique no ícone na coluna **Formatos**.

Enviando emails com relatórios de vulnerabilidades designadas para usuários técnicos

No IBM Security QRadar Vulnerability Manager, é possível enviar um relatório de vulnerabilidades designadas para o contato técnico de cada recurso.

Um relatório enviado por email lembra seus administradores de que as vulnerabilidades estão designadas para eles e requerem correção. Os relatório podem ser planejados mensalmente, semanalmente, diariamente ou de hora em hora.

Antes de Iniciar

Deve-se concluir as tarefas a seguir:

1. Designe um usuário técnico como o proprietário dos grupos de recursos. Para obter informações adicionais, consulte "Designando um usuário técnico como proprietário de grupos de recursos" na página 81
2. Varra os recursos que você designou para o proprietário técnico.
3. Crie e salve uma procura de vulnerabilidade que use o parâmetro **Contato do Proprietário Técnico** como uma entrada. Para obter informações adicionais, consulte "Procurando Dados de Vulnerabilidade" na página 66

Procedimento

1. Clique na guia **Relatórios**.
2. Na barra de ferramentas, selecione **Ações** > **Criar**.
3. Clique em **Semanal** e, em seguida, clique em **Avançar**.
4. Clique no layout do relatório integral que é exibido na seção esquerda superior do assistente de relatório e clique em **Avançar**.
5. Digite um **Título do Relatório**.
6. Na lista **Tipo de Gráfico**, selecione **Vulnerabilidades do Ativo** e digite um **Título do Gráfico**.
7. Opcional: Se um proprietário de contato técnico for responsável por mais de cinco ativos e você desejar enviar todas as informações do ativo por email, aumente o valor na lista **Limitar Recursos até o Máximo**.

   Lembre-se: Usando a guia **Ativos**, você deverá assegurar que o mesmo proprietário de contato técnico seja designado a cada ativo aos quais ele é responsável.
8. No campo **Tipo de Gráfico**, selecione **AggregateTable**.

   Se você selecionar qualquer valor diferente de **AggregateTable**, o relatório não gerará um sub-relatório de vulnerabilidade.
9. Na área de janela de conteúdo Conteúdo do Gráfico, clique em **Procura a Ser Usada** e selecione a procura de vulnerabilidade do contato técnico salvo e, em seguida, clique em **Salvar Detalhes do Contêiner**.
10. Clique em **Avançar** e selecione o tipo de saída de relatório.
11. Na seção de distribuição de relatório do assistente de relatório, clique em **Diversos Relatórios**.
12. Clique em **Todos os Proprietários de Recursos**.
13. Opcional: Clique em **Carregar proprietários do recurso** para exibir toda a lista de detalhes de contato dos usuários técnicos.

    É possível remover todos os usuários técnicos para os quais você não deseje enviar um email com uma lista de vulnerabilidades designadas.
14. Na lista Relatórios, selecione o relatório criado e, na barra de ferramentas, selecione **Ações** > **Executar Relatório**.

Tarefas relacionadas:

"Designando um usuário técnico como proprietário de grupos de recursos" na página 81
No IBM Security QRadar Vulnerability Manager, é possível configurar grupos de ativos e automaticamente designar suas vulnerabilidades para usuários técnicos.

"Procurando Dados de Vulnerabilidade" na página 66
No IBM Security QRadar Vulnerability Manager, é possível identificar vulnerabilidades importantes procurando os dados de vulnerabilidade.

Gerando relatórios de conformidade PCI

No IBM Security QRadar Vulnerability Manager, é possível gerar um relatório de conformidade para seus recursos de PCI (segmento de cartões de pagamento). Por exemplo, gere um relatório para os recursos que armazenam cartões de crédito ou outras informações financeiras confidenciais.

O relatório de conformidade demonstra que você tomou todas as precauções necessárias de segurança para proteger seus recursos.

Procedimento

1. Execute uma varredura de PCI para os recursos de sua rede que armazenam ou processam informações PCI.

   Para obter mais informações, consulte "Criando um Perfil de Varredura" na página 27.
2. Atualize os planos de conformidade de recursos e as declarações de software.

   Seu plano de conformidade e as declarações de software são exibidas na seção de notas especiais do resumo executivo.

   Para obter mais informações, consulte os padrões de segurança PCI para fornecedores de software aprovados.
3. Crie e execute um relatório de conformidade PCI para os recursos que você varreu.

Tarefas relacionadas:

"Criando um Perfil de Varredura" na página 27
No IBM Security QRadar Vulnerability Manager, configure perfis de varredura para especificar como e quando os recursos de rede são digitalizados para vulnerabilidades.

Atualizando os planos de conformidade de recursos e as declarações de software

No IBM Security QRadar Vulnerability Manager, se você desejar gerar um relatório de conformidade PCI para seus recursos, você deverá concluir os atestados para cada recurso.

Seu atestado de conformidade é exibido em seu relatório de conformidade PCI.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Perfis de Ativos**.
3. Na página Recursos, selecione o recurso para o qual deseja fornecer um atestado.
4. Na barra de ferramentas, clique em **Editar Ativo**.
5. Na janela Editar Perfil do Recurso, clique na área de janela **CVSS, Peso e Conformidade**.

6. Complete os campos a seguir. Use a ajuda instantânea se precisar de assistência:
   - Plano de Conformidade
   - Notas de Conformidade
   - Declaração de Notas de Conformidade
   - Descrição de Notas de Conformidade
   - Conformidade fora da Razão de Escopo
7. Clique em **Salvar**.

Criando um relatório de conformidade PCI

No IBM Security QRadar Vulnerability Manager, é possível criar e executar um relatório de conformidade PCI.

O relatório de conformidade PCI demonstra que seus ativos envolvidos em atividades PCI estão em conformidade com precauções de segurança que evitam ataque externo.

Antes de Iniciar

Assegure-se de ter executado uma varredura de conformidade PCI.

Procedimento

1. Clique na guia **Relatórios**.
2. Na barra de ferramentas, selecione **Ações** > **Criar**.
3. Clique em **Semanal** e, em seguida, clique em **Avançar**.
4. Clique no layout do relatório integral que é exibido na seção esquerda superior do assistente de relatório e clique em **Avançar**.
5. Digite um **Título do Relatório**.
6. Na lista **Tipo de Gráfico**, selecione **Conformidade de Vulnerabilidade** e digite um **Título de Gráfico**.
7. Na lista **Perfil de Varredura**, selecione o perfil de varredura para os recursos varridos.

   Atenção: Se nenhum perfil de varredura for exibido, você deverá criar e executar uma varredura PCI dos recursos de sua rede que armazenam ou processam informações PCI.
8. Na lista **Resultado de Varredura**, selecione a versão do perfil de varredura que você deseja usar.

   Lembre-se: Para fornecer evidência de sua conformidade, você deve selecionar a opção **Mais Recente** na lista **Resultado de Varredura**. Também é possível gerar um relatório de conformidade usando um perfil de varredura que tenha sido executado em uma data anterior.
9. Na lista **Tipo de Relatório**, selecione um tipo de relatório.

   Se você selecionar **Resumo Executivo**, **Detalhes de Vulnerabilidade** ou uma combinação de ambos, o atestado será anexado automaticamente a seu relatório de conformidade PCI.
10. Complete as informações nas áreas de janela **Informações do Cliente de Varredura** e **Informações do Fornecedor de Varredura Aprovado**.

Importante: Você deve incluir um nome no campo **Empresa** para as duas áreas de janela, pois essas informações são exibidas na seção de atestado do relatório.

11. Clique em **Salvar Detalhes do Contêiner** e, em seguida, clique em **Avançar**.
12. Use o Assistente de Relatório para concluir o relatório de conformidade PCI.

Resultados

O relatório é exibido na lista de relatórios e é gerado automaticamente.

Incluindo títulos de colunas em procuras de ativos

Limite as procuras de ativos com filtros que incluam perfis de ativos customizados, nome, contagem de vulnerabilidade e pontuação de risco.

Procedimento

1. Clique na guia **Ativos**.
2. Na área de janela de navegação, clique em **Perfis de Ativos**, em seguida, na barra de ferramentas, clique em **Procura** > **Nova Procura**.
3. No campo que contém os nomes de colunas, no campo à esquerda, clique nos títulos de colunas que você deseja incluir em sua procura e clique no botão de seta para mover os títulos selecionados para o campo à direita.
4. Clique nos botões para cima e para baixo para alterar a prioridade dos títulos de colunas selecionados.
5. Quando o campo à direita contiver todos os cabeçalhos de coluna em que você deseja procurar, clique em **Procurar**.

Capítulo 11. Pesquisa de Vulnerabilidade, Notícias e Recomendações

É possível usar o IBM Security QRadar Vulnerability Manager para ficar ciente do nível de ameaça de vulnerabilidade e gerenciar a segurança na organização.

Uma biblioteca de vulnerabilidade contém vulnerabilidades comuns que são reunidas de uma lista de fontes externas. O recurso externo mais significativo é o National Vulnerability Database (NVD). É possível pesquisar vulnerabilidades específicas usando inúmeros critérios, por exemplo, fornecedor, produto e intervalo de data. Você pode ter interesse em vulnerabilidades específicas que existem em produtos ou serviços que são usados em sua empresa.

O QRadar Vulnerability Manager também fornece uma lista de artigos e recomendações de notícias relacionados à segurança, reunidos de uma lista externa de recursos e fornecedores. Artigos e recomendações são uma fonte útil de informações de segurança em todo o mundo. Artigos também lhe ajudam a se manter atualizado sobre os atuais riscos de segurança.

Visualizando Informações Detalhadas sobre Vulnerabilidades Publicadas

No IBM Security QRadar Vulnerability Manager, é possível exibir informações detalhadas de vulnerabilidade.

Usando a página Pesquisar Vulnerabilidades, é possível investigar as métricas CVSS e acessar informações de pesquisa e desenvolvimento do IBM X-Force.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, selecione **Pesquisar** > **Vulnerabilidades**.
3. Opcional: Se nenhuma vulnerabilidade for exibida, selecione um intervalo de tempo alternativo na lista **Visualizar vulnerabilidades de**.
4. Opcional: Para procurar as vulnerabilidades, na barra de ferramentas, selecione **Procura** > **Nova Procura**.
5. Identifique a vulnerabilidade que deseja investigar.
6. Clique no link de vulnerabilidade na coluna **Nome da Vulnerabilidade**.

Tomando Conhecimento de Desenvolvimentos de Segurança Global

No IBM Security QRadar Vulnerability Manager, é possível visualizar notícias de segurança de todo o mundo para ajudar a mantê-lo atualizado sobre os desenvolvimentos de segurança atuais.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Pesquisar** > **Notícias**.
3. Se nenhum artigo de notícias for exibido, selecione um intervalo de tempo alternativo na lista **Visualizar notícias de**.

4. Para procurar os artigos de notícias, na barra de ferramentas, selecione **Procura** > **Nova Procura**.
5. Identifique o artigo de notícias sobre o qual deseja saber mais.
6. Clique no link do artigo de notícias na coluna **Título do Artigo**.

Visualizando Recomendações de Segurança dos Fornecedores de Vulnerabilidade

No IBM Security QRadar Vulnerability Manager, é possível visualizar as recomendações de vulnerabilidade que são emitidas por fornecedores de software. Use informações de recomendação para lhe ajudar a identificar os riscos em sua tecnologia e a entender as implicações do risco.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em **Pesquisar** > **Recomendações**.
3. Se nenhuma recomendação for exibida, selecione um intervalo de tempo alternativo na lista **Visualizar recomendações de**.
4. Se desejar procurar as recomendações de segurança, na barra de ferramentas, selecione **Procura** > **Nova Procura**.
5. Clique no link da recomendação e na coluna **Recomendação**.

   Cada recomendação de segurança pode incluir referências de vulnerabilidade, soluções e soluções alternativas.

Procurando Vulnerabilidades, Notícias e Recomendações

No IBM Security QRadar Vulnerability Manager, é possível procurar as notícias e recomendações mais recentes de vulnerabilidade que são emitidas por fornecedores de software.

Procedimento

1. Clique na guia **Vulnerabilidades**.
2. Na área de janela de navegação, clique em uma das opções a seguir:
   - **Pesquisar** > **Vulnerabilidades**.
   - **Pesquisar** > **Notícias**.
   - **Pesquisar** > **Recomendações**.
3. Na barra de ferramentas, selecione **Procura** > **Nova Procura**.
4. Digite uma frase de procura no campo **Frase**.
5. Se estiver procurando itens de notícias, selecione uma fonte de notícias na lista **Origem**.
6. Na área **Por Intervalo de Data**, especifique o período de data para as notícias ou recomendações de seu interesse.
7. Caso você esteja procurando uma vulnerabilidade publicada, especifique um fornecedor, produto e versão na área **Por Produto**.
8. Se estiver procurando uma vulnerabilidade publicada, especifique um ID de CVE, de Vulnerabilidade ou de OSVDB na área **Por ID**.

Feeds de notícias

Use os itens do painel **Feeds RSS** para ver as mais recentes notícias de segurança, recomendações, informações de vulnerabilidade publicadas e atualizações sobre as varreduras do IBM que estão concluídas ou em andamento.

Os itens do painel **Feeds RSS** giram os 10 itens de notícias e resultados de varredura mais recentes, para que não seja necessário procurar informações nas páginas Procura ou Resultados da Varredura na guia **Vulnerabilidades**.

Na guia **Painel**, use o menu **Incluir Item** > **Relatórios** > **Feeds RSS** para incluir feeds RSS em seu painel.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

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

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

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

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão

incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
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 o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

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

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos

incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos de marca comercial da IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial (® ou ™), estes símbolos indicarão marcas comerciais dos Estados Unidos ou de direito consuetudinário de propriedade da IBM no momento em que estas informações foram publicadas. Estas marcas comerciais também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atual de marcas comerciais da IBM está disponível na web em Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

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

Linux é uma marca comercial de Linus Torvalds nos Estados Unidos e/ou em outros países.

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

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

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

Considerações Sobre a Política de Privacidade

Produtos de software IBM, incluindo soluções de software como um serviço (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir que você colete informações pessoalmente identificáveis. Se esta Oferta de Software usar cookies para coletar as informações pessoalmente identificáveis, as informações específicas sobre o uso de cookies desta oferta serão apresentadas a seguir.

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

Se as configurações implementadas para esta Oferta de Software fornecerem a capacidade de coletar, como cliente, informações pessoalmente identificáveis dos

usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico a respeito das leis aplicáveis⌂a essa coleta de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy, a Declaração de privacidade online da IBM em http://www.ibm.com/privacy/details, a seção intitulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de software como serviço e de produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.

Glossário

Este glossário fornece termos e definições para software e produtos do IBM Security QRadar Vulnerability Manager.

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 para um termo relacionado ou contrastante.

Para obter outros termos e definições, consulte o Website de terminologia IBM (abre em uma nova janela).

"A" "B" "C" "D" "H" "I" na página 100 "L" na página 100 "N" na página 100 "P" na página 100 "R" na página 100 "S" na página 101 "T" na página 101 "U" na página 101 "V" na página 101

A

Alta disponibilidade (HA)
Relativo a um sistema em cluster que é reconfigurado quando as falhas do nó ou do daemon ocorrerem de forma que as cargas de trabalho possam ser redistribuídas para os nós restantes no cluster.

ativo Um objeto gerenciável que é implementado ou que pretende-se que seja implementado em um ambiente operacional.

B

banco de dados de vulnerabilidade nacional (NVD)
Um repositório de dados de gerenciamento de vulnerabilidades baseados nos padrões dos Estados Unidos.

C

CDP Consulte potencial de dano indireto.

CIDR Consulte Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
Um método para incluir endereços (IP) Internet Protocol de classe C. Os endereços são oferecidos aos Provedores de Serviço da Internet (ISPs) para uso de seus clientes. Os endereços CIDR reduzem o tamanho das tabelas de roteamento e tornam mais endereços IP disponíveis nas organizações.

cliente
Um programa de software ou de computador que solicita serviços de um servidor.

Common Vulnerability Scoring System (CVSS)
Um sistema de pontuação pela qual a gravidade de uma vulnerabilidade é medida.

console
Uma interface baseada na web a partir da qual um operador pode controlar e observar a operação do sistema.

crime Uma mensagem enviada ou um evento gerado em resposta a uma condição monitorada. Por exemplo, uma ofensa fornecerá informações se uma política foi violada ou se a rede está sofrendo um ataque.

criptografia
Em segurança do computador, o processo de dados de transformação para uma forma ininteligível de tal maneira que os dados originais não possam ser obtidos ou só possam ser obtidos usando um processo de decriptografia.

CVSS Consulte Common Vulnerability Scoring System.

D

DNS Consulte Sistema de Nomes de Domínio.

H

HA Consulte alta disponibilidade.

I

Internet Protocol (IP)
Um protocolo que roteia dados por meio de uma rede ou redes interconectadas. Este protocolo atua como um intermediário entre as camadas de protocolo superiores e a rede física. Consulte também Protocolo de Controle de Transmissões.

IP Consulte Internet Protocol.

J

janela operacional
Um período de tempo configurado dentro do qual a execução de uma varredura é permitida.

L

lista de exclusão de varredura
Uma lista de ativos, grupos de redes e intervalos de CIDR que não são ignorados pelas varreduras.

N

nível de severidade de PCI
O nível de risco que uma vulnerabilidade representa ao Payment Card Industry.

NVD Consulte banco de dados de vulnerabilidade nacional.

P

Payment Card Industry Data Security Standard (PCI DSS)
Um padrão mundial de segurança de informações montado pelo Payment Card Industry Security Standards Council (PCI SSC). A norma foi criada para ajudar as organizações que processam pagamentos com cartão, para evitar fraudes de cartão de crédito, por meio de controles aumentados em torno de dados e de sua exposição para comprometerem-se. A norma aplica-se a todas as organizações que suspendem, processam ou passam informações do proprietário do cartão para qualquer marca do cartão com o logotipo de uma das marcas de cartão.

PCI DSS
Consulte Payment Card Industry Data Security Standard.

perfil de varredura
As informações de configuração que especificam como e quando os recursos em uma rede são digitalizados para as vulnerabilidades.

potencial de dano indireto (CDP)
Uma medida do impacto potencial de uma vulnerabilidade explorada em um ativo físico ou em uma organização.

processo de correção
Um processo de designação, rastreamento e correção de vulnerabilidades que foram identificadas em um ativo.

Protocolo de Controle de Transmissões (TCP)
Um protocolo de comunicação usado na Internet e em todas as redes que seguem os padrões da Internet Engineering Task Force (IETF) para protocolo de interligação de redes. O TCP oferece um protocolo confiável de host a host em redes de comunicação através da comutação de pacotes e em sistemas interconectados dessas redes. Consulte também Internet Protocol.

Protocolo Simples de Gerenciamento de Rede (SNMP)
Um conjunto de protocolos para sistemas de monitoramento e dispositivos em redes complexas. Informações sobre os dispositivos gerenciados são definidas e armazenadas em um Management Information Base (MIB).

Protocolo UDP (UDP)
Um Protocolo da Internet que fornece serviço de datagrama não confiável, sem conexão. Permite que um programa de aplicativo em uma máquina ou processo envie um datagrama a um programa de aplicativo em outra máquina ou processo.

R

recomendação
Um documento que contém informações e análise sobre uma ameaça ou vulnerabilidade.

regra de positivo falso
Uma regra específica às vulnerabilidades

de baixo risco que minimiza o volume de vulnerabilidades gerenciadas.

S

Sistema de Nomes de Domínio (DNS)
O sistema de banco de dados distribuído que mapeia os nomes de domínio para endereços IP.

SNMP
Consulte Protocolo Simples de Gerenciamento de Rede.

T

TCP Consulte Protocolo de Controle de Transmissões.

Transferência de Zona de DNS
Uma transação que replica um banco de dados de Domain Name System (DNS).

U

UDP Consulte Protocolo UDP.

V

varredura on demand
Uma varredura executada apenas quando iniciada pelo usuário. Os tipos de varreduras incluem varreduras completas, varreduras de descoberta, varreduras de correções, varreduras de PCI, varreduras de banco de dados e varreduras da web.

vulnerabilidade
Uma exposição de segurança em um sistema operacional, software do sistema ou componente de software de aplicativo.

Índice Remissivo

W