IBM Security QRadar Incident Forensics
Versão 7.3.0

Guia de Administração

Nota

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

Informações do produto

Este documento aplica-se ao IBM QRadar Security Intelligence Platform V7.3.0 e às liberações subsequentes, a não ser que seja substituído por uma versão atualizada.

Índice

Introdução à administração do IBM Security QRadar Incident Forensics v

Capítulo 1. O que há de novo para os administradores no QRadar Incident Forensics V7.3.0 1

Capítulo 2. Fluxo de trabalho de administração e acesso de usuário a recursos do Forensics 3

Capítulo 3. Gerenciamento do servidor 5
Definições de configuração do servidor 5
Filtros de inspetor de protocolo e domínio 5
Filtro de categoria da web 6
Tipos de protocolos e de documentos suportados 7

Capítulo 4. Gerenciamento de caso 9
Criando casos 9
Fazendo upload de arquivos para casos 10

Capítulo 5. Designando casos a usuários 11
Importando manualmente arquivos em um caso forense 11
Permitindo aos usuários transferir por FTP arquivos pcap e documentos de sistemas externos para casos forenses 12
Decriptografando tráfego SSL e TLS no QRadar Incident Forensics 14

Capítulo 6. Ações planejadas no QRadar Incident Forensics 17
Planejando ações para hosts do QRadar Incident Forensics 17

Capítulo 7. Gerenciando conteúdo suspeito 19
Importando regras de Yara 20
Excluindo regras de Yara 20

Capítulo 8. Auditando o usuário e o uso do sistema no QRadar Incident Forensics . . 23

Capítulo 9. Investigar ameaças com o QRadar Network Insights 25
Investigações de ameaças em tempo real com o QRadar Network Insights 25
Implementações do QRadar Network Insights 26
Requisitos de configuração do QRadar Network Insights 27
Configurando formato do QFlow Collector 27
Configurando um DTLS em um host gerenciado do QRadar Network Insights 27
Níveis de inspeção de fluxo do QRadar Network Insights 28
Definindo as Configurações do QRadar Network Insights 30
Detecção de ameaças com o QRadar Network Insights 30

Avisos 33
Marcas comerciais 35
Termos e condições para a documentação do produto 35
Declaração de privacidade on-line da IBM 36

Introdução à administração do IBM Security QRadar Incident Forensics

Informações sobre administração do IBM® Security QRadar Incident Forensics.

Público desejado

Os administradores criam, mantém e operam um recurso de investigação ativo para que usuários, chamados investigadores, possam concentrar-se na investigação de incidentes de segurança, ou casos, e na exploração de dados.

Documentação técnica

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

Para obter informações sobre como acessar documentação técnica adicional na biblioteca de produtos do QRadar, consulte Nota técnica sobre como acessar a documentação do IBM Security (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Entrando em contato com o suporte ao cliente

Para obter informações sobre como entrar em contato com o suporte ao cliente, consulte Nota técnica de suporte e download (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaração de boas práticas de segurança

A segurança do sistema de TI envolve a proteção de sistemas e as informações através da prevenção, detecção e resposta para acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em alteração, destruição, desapropriação ou mal uso de informações ou pode resultar em danos ou mau uso dos sistemas, incluindo seu uso em ataques a outros sistemas. Nenhum produto ou sistema de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança individual pode ser completamente eficaz na prevenção do acesso ou uso impróprio. AIBM sistemas, produtos e serviços são projetados para fazerem parte de uma abordagem de segurança abrangente legal, que envolverá necessariamente procedimentos operacionais adicionais, podendo requerer outros sistemas, produtos ou serviços para que sejam mais eficientes. A IBM NÃO GARANTE QUE OS SISTEMAS, PRODUTOS OU SERVIÇOS ESTEJAM IMUNES OU TORNAM A SUA EMPRESA IMUNE CONTRA CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PESSOA.

Observe que:

O uso desse programa pode implicar em várias leis ou regulamentações, incluindo aquelas relacionadas à privacidade, proteção de dados, emprego, e armazenamento e comunicações eletrônicas. O IBM Security QRadar pode ser usado apenas para propósitos legais e de maneira legal. O cliente concorda em usar este Programa de acordo com leis, regulamentos e políticas e assume toda a responsabilidade pelo

seu cumprimento. O licenciado declara que obterá ou obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar.

Nota

O IBM Security QRadar Incident Forensics foi projetado para ajudar as empresas a melhorarem seu ambiente e dados de segurança. Mais especificamente, o IBM Security QRadar Incident Forensics foi projetado para ajudar as empresas a investigarem e entenderem melhor o que aconteceu nos incidentes de segurança de rede. A ferramenta permite que as empresas indexem e procurem dados capturados do pacote de rede (PCAPs) e incluam um recurso que possa reconstruir esses dados novamente em sua forma original. Esse recurso de reconstrução pode reconstruir dados e arquivos, incluindo mensagens de email, anexos de arquivo e figuras, telefonemas VoIP e websites. Informações adicionais sobre os recursos e funções do Programa e como podem ser configurados estão contidas nos manuais e em outra documentação que acompanha o Programa. O uso desse Programa pode implicar em várias leis ou regulamentos, incluindo aqueles relacionados à privacidade, proteção de dados, emprego e comunicações e armazenamento eletrônico. O IBM Security QRadar Incident Forensics pode ser usado apenas para propósitos legais e de forma legal. O cliente concorda em usar este Programa conforme as leis, os regulamentos e as políticas aplicáveis, assumindo toda a responsabilidade em seu cumprimento. O Licenciado declara que obterá ou que obteve quaisquer consentimentos, permissões ou licenças necessárias para permitir o uso legal do IBM Security QRadar Incident Forensics.

Capítulo 1. O que há de novo para os administradores no QRadar Incident Forensics V7.3.0

O IBM QRadar Network Insights V7.3.0 introduz uma opção adicional para o formato do QFlow.

Opção TLV disponível para QRadar Network Insights

Use os QFlow Collectors para exportar dados para o QFlow Processor em formato TLV (tab-length-value). Para novas instalações do IBM Security QRadar ou upgrades do QRadar que não possuam um dispositivo QRadar Network Insights como parte de sua implementação, escolha o formato `TLV` no menu **Formato do QFlow**.

 Saiba mais sobre o formato TLV...

Capítulo 2. Fluxo de trabalho de administração e acesso de usuário a recursos do Forensics

Após o IBM Security QRadar Incident Forensics ser instalado e configurado, um administrador poderá solucionar problemas, manter e monitorar o sistema e suas operações e gerenciar o acesso do usuário a casos.

Deve-se ter privilégios administrativos para ver as ferramentas de administração do QRadar Incident Forensics.

Exemplo: fluxo de trabalho de administração

O diagrama a seguir mostra um fluxo de trabalho de amostra para a administração do QRadar Incident Forensics.

1. Use o Gerenciamento do servidor para filtrar categorias da web e tráfego que não deseja monitorar.
2. Use as Permissões de usuário do Forensics para designar casos a investigadores.
3. Use o Gerenciamento de caso para criar e excluir casos e importar conteúdo externo no sistema.
4. Use as Ações planejadas para planejar a manutenção, como a exclusão de documentos antigos, ajustar o banco de dados e reconfigurar o servidor do QRadar Incident Forensics.

Funções de usuário

Para incluir contas do usuário, você deve primeiro criar perfis de segurança para atender aos requisitos de acesso específicos de seus usuários. Para obter mais informações sobre a configuração de perfis de segurança, consulte *Guia de Administração do IBM Security QRadar*.

Na ferramenta Funções de usuário na guia **Administrador** do QRadar, é possível designar as funções de usuário a seguir:

Administrador
Os usuários podem visualizar e acessar todos os casos designados a usuários e todos os incidentes e recebem automaticamente acesso integral ao QRadar Incident Forensics.

Forensics
Os usuários podem ver e acessar a guia **Forensics**, mas não podem criar casos.

Criar casos no Incident Forensics
Os usuários podem criar automaticamente casos forenses.

Capítulo 3. Gerenciamento do servidor

Os administradores podem solucionar problemas, fazer a manutenção e monitorar o sistema IBM Security QRadar Incident Forensics e suas operações.

Para monitorar ou alterar as configurações do servidor ou visualizar os usuários registrados no sistema, abra a ferramenta Gerenciamento do servidor:

1. Efetue logon no QRadar como um administrador.
2. Clique na guia **Administrador**.
3. Na seção **Forensics** na área de janela principal, clique em **Gerenciamento do servidor**.

Definições de configuração do servidor

Use as configurações do servidor na ferramenta Gerenciamento do Servidor do IBM Security QRadar Incident Forensics para configurar as definições de sistema que afetam todos os hosts gerenciados. Depois de mudar uma configuração, você deve implementar suas mudanças usando o menu **Implementar Mudanças** na guia **Administrador**.

Limpar histórico de procura no logout
O histórico de procura será limpo quando os usuários efetuarem logout. A procura limpa aplica-se à lista de históricos de consulta no Auxiliar de consulta e ao último usuário no campo **Entrada dos critérios de procura** na página Procura e resultados.

Número padrão de nós para visualizar
O número máximo de nós que a ferramenta Visualizar mostra. É possível configurar o número de nós a renderizar após os nós serem renderizados pela primeira vez. Ajustar a contagem de nós renderizados afeta apenas essa instância da ferramenta Visualizar.

Filtros de inspetor de protocolo e domínio

É possível excluir certos tipos de tráfego de investigações desativando os inspetores de protocolo ou domínio na ferramenta Gerenciamento do servidor. Use a opção **Filtro do Inspetor**.

Os inspetores de protocolo e domínio processam dados de tráfego de rede alimentados e tentam identificar e indexar os dados de uma maneira significativa. A identificação e a indexação desses dados fornece aos investigadores mais controle para localizar as informações.

Conforme os dados de tráfego de rede são alimentados e os protocolos são identificados, os dados são inspecionados ainda mais pelo inspetor de protocolo apropriado. Os dados de tráfego de rede que são identificados pelo inspetor de protocolo HTTP são inspecionados e indexados ainda mais pelos inspetores de domínio.

Inspetores de protocolo
Os inspetores de protocolo podem identificar o protocolo, como HTTP, POP3, FTP e telnet. É possível excluir inspetores de protocolo. Quando os inspetores são excluídos, quaisquer dados de tráfego de rede associados ao

inspetor ainda serão alimentados, mas o tráfego será identificado e indexado apenas em um nível genérico.

Inspetores de domínio
Os inspetores de domínio inspecionam websites específicos. É possível excluir inspetores de domínio. Ao excluir inspetores de domínio, quaisquer dados de tráfego de rede HTTP associados ao inspetor ainda serão alimentados, mas o tráfego será identificado e indexado apenas no nível HTTP. Para que os inspetores de domínio fiquem ativos, o inspetor de protocolo HTTP também deve estar ativo.

Por padrão, todos os filtros são ativados e você pode ver o tráfego de todos os protocolos. A única exceção é o tráfego SIP (Session Initiation Protocol). Esse protocolo de configuração de chamada, que opera na camada do aplicativo, é desativado por padrão.

Lembre-se: Quando você muda a configuração de filtros do inspetor, a nova configuração é aplicada a cada novo caso que é criado. Os inspetores que são ativados influenciam os documentos que são criados para um caso e os investigadores perdem a capacidade de procurar certos inspetores. Os usuários não sabem quais inspetores são aplicados a um caso.

Qualquer protocolo que não seja processado por um inspetor é categorizado como desconhecido.

Filtro de categoria da web

É possível escolher os tipos de páginas da web e servidores da web que são reconhecidos usando filtros de categoria da web.

Por exemplo, é possível excluir tipos específicos de tráfego de rede HTTP das investigações. Quando os dados de tráfego de rede HTTP forem alimentados, os dados serão categorizados e os documentos resultantes serão agrupados.

Os administradores podem filtrar dados de tráfego de rede HTTP para evitar que os dados sejam alimentados.

Para excluir ou filtrar tráfego, para uma categoria ou grupo, desligue a categoria ou grupo na ferramenta Gerenciamento do servidor.

A categorização, o agrupamento e a filtragem da web afetam os dados de tráfego de rede HTTP durante a alimentação e não têm efeito nos dados que já estão no sistema.

Quando um filtro de grupo for configurado para excluir dados, os dados de tráfego de rede HTTP associados a categorias nesse grupo serão filtrados durante o consumo, independentemente das configurações de filtros de categoria associados.

Exemplo: O que acontece quando você usa um filtro de categoria da web para excluir tráfego?

Você decide excluir tráfego que contém dados dos sites de notícias ou revistas.

1. Na guia **Administrador**, em QRadar, clique em **Gerenciamento de Servidor**.
2. Clique em **Filtro de Categoria da Web** e em **Desativar** ao lado do filtro **Notícias / Revistas**.
3. Clique filtro **Correio da web / Sistema de Mensagens Unificado** e em **Ativar**.

Agora, quando um usuário investiga tráfego consumido na guia **Forensics**, ele vê que um tráfego que contém os dados **Notícias / Revistas** e **Correio da web/ Sistema de Mensagens Unificado** não é consumido, embora o filtro **Correio da web / Sistema de Mensagens Unificado** esteja ativado.

Tipos de protocolos e de documentos suportados

O IBM Security QRadar Incident Forensics captura o conteúdo nos pacotes de fluxo de rede e indexa e processa a carga útil e os metadados.

A lista a seguir descreve os protocolos suportados que o QRadar Incident Forensics pode processar:

- AIM
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- IMAP
- IRC
- Jabber
- Myspace
- NFS
- SIP
- NetBIOS
- Oracle
- POP3
- SMB (Versão 1)
  - Lanman 2.1
  - NT 0.12
- SMTP
- SPDY
- TLS (SSL)
- SSH
- Telnet
- Yahoo Messenger
- MySQL

A lista a seguir descreve os domínios de suporte (websites) e os idiomas suportados para o domínio que o QRadar Incident Forensics pode processar:

- AOL (Acessível, Básico, Padrão) (EN)
- Charter (EN)
- Facebook (Móvel, Desktop) (AR,CN,DE,EN,ES,FR,RU)
- Gmail (Clássico, Padrão) (AR,CN,DE,EN,ES,FR,RU)
- Hotmail (AR,CN,DE,EN,ES,FR,RU)
- LinkedIn (DE,EN,ES,FR,RU)
- MailCom (CN,EN,ES,FR,RU)
- MailRu (RU)

- Maktoob (AR,EN)
- Myspace (EN)
- QQMail (EN,CN)
- Twitter (EN)
- YAHOO Mail (Padrão, Clássico) (EN)
- YAHOO Note (EN)
- YouTube (AR,CN,DE,EN,ES,FR,RU)
- Comcast (Zimbra) (EN)

A lista a seguir descreve os formatos de documento suportados que o QRadar Incident Forensics pode processar:

- Linguagem de marcação de hipertexto
- XML e formatos derivados
- Formatos de documentos Microsoft Office
- Formato OpenDocument
- Portable Document Format
- Formato de publicação eletrônica
- Formato Rich Text
- Formatos de compactação e empacotamento
- Formatos de texto
- Formatos de áudio
- Formatos de imagem
- Formatos de vídeo
- Archives e arquivos de classe Java™
- Formato mbox

Detecção de aplicativo QFlow

A detecção de aplicativo QFlow é usada quando nenhum outro inspetor pode detectar um aplicativo, sessão ou protocolo. A detecção de aplicativo QFlow inspeciona os primeiros 64 bytes de um pacote para uma assinatura e tenta identificar o aplicativo da assinatura e da porta. Alguns exemplos de aplicativos, sessões ou protocolos que a detecção de aplicativo QFlow pode ser capaz de identificar incluem, entre outros, os itens a seguir.

- BitTorrent
- Blubster
- CitrixICA
- Google Talk
- Gnucleuslan
- Gnutella
- GSS-SPNEGO
- NTLMMSSP
- OpenNap
- AtivadorPeer
- Piolet
- UpdateDaemon
- VNC

Capítulo 4. Gerenciamento de caso

Como um administrador, é possível gerenciar casos e coleções usando o Gerenciamento de Caso. É possível criar casos para coleções de documentos ou arquivos de captura de pacote (pcap) e também importar arquivos externos para o sistema IBM Security QRadar Incident Forensics.

Ajustando gerenciamento de caso

Para ajudar a ajustar o gerenciamento de caso, é possível usar a opção **Limpar**. Para dados de *fluxo pcap*, que são uma série de arquivos pcap que estão logicamente relacionados para formar um arquivo pcap grande, é possível forçar que dados armazenados em buffer sejam gravados no disco. A opção **Liberação** força os hosts do QRadar Incident Forensics a gravar fluxos não finalizados no disco, que, por sua vez, ajuda a procurar esses fluxos em um estágio anterior.

Gráficos de distribuição

Se planejar excluir um caso, será possível usar visualmente os gráficos para revisar rapidamente o conteúdo do caso. É possível revisar o tipo de arquivos, os protocolos e os domínios que estão no caso.

Fazendo upload de arquivos pcap para hosts gerenciados

Você pode fazer upload manualmente de dados pcap a partir de fontes externas. Você pode especificar qual host gerenciado do QRadar Incident Forensics fará upload dos dados para processamento. Por exemplo, se você tiver três hosts gerenciados e três arquivos pcap, poderá fazer o upload de cada um para um host gerenciado diferente. Para arquivos pcap maiores, use FTP.

Criando casos

Casos são contêineres lógicos para sua coleção de arquivos de documentos e de pcap importados. É possível usar um único caso para todos os arquivos pcap ou criar diversos casos. Os casos podem ser restringidos a usuários específicos.

Procedimento

1. Na guia **Administrador**, selecione **Gerenciamento de caso**.
2. Clique em **Incluir novo caso**.
3. No campo **Nome do caso**, digite um nome exclusivo.

   Restrição: Nomes de casos não podem conter espaços.
4. Clique em **Salvar**.

Resultados

Um novo diretório que é baseado no nome do caso é criado: `/case_input/<case_name>`. Esse diretório é usado para importar os arquivos pcap.

Fazendo upload de arquivos para casos

Como um administrador, você pode fazer upload de arquivos e documentos de captura de pacote (pcap) externos, como planilhas, arquivos de textos e arquivos de imagens, para o Gerenciamento de Caso do IBM Security QRadar Incident Forensics.

Os tipos de arquivo a seguir são suportados:

- Linguagem de marcação de hipertexto
- XML e formatos derivados
- Formatos de documentos Microsoft Office
- Formato OpenDocument
- Portable Document Format
- Formato de publicação eletrônica
- Formato Rich Text
- Formatos de compactação e empacotamento
- Formatos de texto
- Formatos de áudio
- Formatos de imagem
- Formatos de vídeo
- Arquivos e archives de classe Java
- O formato mbox

O Gerenciamento de caso restringe o número de arquivos que é possível incluir em um caso e o tamanho máximo do arquivo.

Procedimento

1. Na guia **Administrador**, na seção **Forensics**, clique em **Gerenciamento de Caso**.
2. Selecione um caso.
   - Para incluir arquivos externos em um caso existente, selecione o caso na lista **Casos**.
   - Para incluir arquivos em um novo caso, clique em **Incluir novo caso**.

     Restrição: Nomes de casos não podem conter espaços.
3. Na lista **Upload para Host**, selecione o host gerenciado que você deseja para processar os arquivos.
4. Para incluir arquivos pcap ou outros tipos de documentos, escolha um dos métodos a seguir:
   - Clique em **Incluir files**, selecione os arquivos e clique em **Iniciar upload**.
   - Arraste os arquivos para a caixa de upload.

   Após o upload estar completo, os arquivos serão listados na lista **Coleções**.

Capítulo 5. Designando casos a usuários

Como um administrador, você concede acesso a dados forenses aos usuários, designa casos aos usuários e configuram permissões de usuário, como acesso FTP. Os usuários não podem ver dados até que sejam designados a um caso e possam ver apenas os dados dos casos aos quais estão designados.

Tenha cuidado ao designar casos a usuários não administradores que têm aceso restrito a redes. Eles podem ver documentos que são dos endereços IP aos quais normalmente não têm acesso. Por exemplo, se você designar um usuário não administrador para um caso que contém informações de recursos financeiros ou humanos, ele poderá ver os dados quando o investigar.

Sobre Esta Tarefa

Os administradores podem executar as tarefas a seguir:

- Designar diversos usuários a um caso.
- Remover um caso de um usuário.
- Visualizar e acessar todos os casos designados a um usuário.

Os usuários podem ver apenas os casos explicitamente designados a eles.

Procedimento

1. Na guia **Administrador**, clique em **Permissões de usuário do Forensics**.
2. Na lista **Usuários**, selecione um usuário.
3. Na lista de casos na lista **Disponível**, selecione um ou mais casos e clique na seta (>) para mover os casos para a lista **Designado**.

   Dica: Por padrão, um usuário com privilégios administrativos está designado a todos os casos. A seta esquerda (<) e a seta direita (>) não são exibidas.

Importando manualmente arquivos em um caso forense

Diferente da ferramenta Gerenciamento de caso, não há restrições no tamanho do arquivo ou no número de arquivos ao importar arquivos manualmente. É possível criar manualmente um caso e copiar arquivos para ele ou copiar arquivos manualmente para um caso existente.

Por exemplo, é possível usar o comando **scp** para copiar arquivos com segurança de outro host para o diretório `/opt/ibm/forensics/case_input/case_input/` no host IBM Security QRadar Incident Forensics.

Antes de Iniciar

Faça uma cópia de backup dos arquivos importados. Após o arquivo ser importado e processado, o arquivo original será excluído.

Procedimento

1. Use SSH para efetuar login no QRadar Incident Forensics como um usuário-raiz.

2. Para criar um novo caso, acesse /opt/ibm/forensics/case_input e digite o comando a seguir:

   mkdir /opt/ibm/forensics/case_input/<*case_name*>

3. Para copiar arquivos para um caso, use um arquivo, o comando **scp** ou outro programa de transferência de arquivo para copiar os arquivos para o diretório que corresponde ao tipo de arquivo.

   A tabela a seguir lista a estrutura de diretório para os arquivos importados.

Tabela 1. Estrutura de diretório dos arquivos de caso

Diretório	Descrição
/opt/ibm/forensics/case_input/<*case_name*>	O diretório que é usado para importar uma série ou fluxo conectado de arquivos pcap.
/opt/ibm/forensics/case_input/<*case_name*>/singles	O diretório que é usado para importar arquivos pcap individuais.
/opt/ibm/forensics/case_input/case_input/<*case_name*>/import	O diretório que é usado para importar um único arquivo de um tipo que não pcap, por exemplo, documentos Microsoft Word, PDFs do Adobe Acrobat, arquivos de textos e imagens.

Importante: Se um hífen for usado em um nome de arquivo, ele será alterado para um sublinhado quando o arquivo for importado.

Resultados

Após uma importação bem-sucedida, seu nome de arquivo automaticamente aparecerá na janela Coleções do caso que você criou.

Permitindo aos usuários transferir por FTP arquivos pcap e documentos de sistemas externos para casos forenses

Para fazer upload de dados externos para incluir em casos específicos, os administradores podem conceder permissões seguras de FTP a usuários e gerenciar o caso ao qual os dados estão associados. Usuários podem selecionar qual host do IBM Security QRadar Incident Forensics processa a solicitação FTP.

Para mudar uma senha depois que o acesso FTP é ativado, deve-se desativar o acesso FTP e salvar o usuário e, em seguida, reativar o acesso FTP e inserir a nova senha.

Antes de Iniciar

Assegure-se de criar ou designar funções para investigações forenses na ferramenta Funções de Usuário na guia **Administrador**.

Por padrão, o arquivo /etc/vsftpd/vsftpd.conf é configurado para que cinco portas fiquem abertas: 55100-55104. Você pode mudar o intervalo de portas editando o arquivo /etc/vsftpd/vsftpd.conf e mudando os valores das configurações pasv_min_port e pasv_max_port para o intervalo de portas que deseja. Você deve implementar suas mudanças de configuração clicando em **Implementar Mudanças** na guia **Administrador**.

Nota: Os clientes FTP devem suportar o TLS v1.2 (arquivo `vsftpd.conf`). A lista a seguir descreve o mínimo das versões do cliente FTP que são suportadas:

- WinSCP 5.7
- FileZilla 3.9.0.6

Sobre Esta Tarefa

O IBM Security QRadar Incident Forensics pode importar dados de qualquer diretório acessível que esteja na rede. Os dados podem estar em vários formatos, incluindo, mas não se limitando aos formatos a seguir:

- Arquivos de formato PCAP padrão de origens externas
- Documentos, como arquivos de texto, arquivos PDF, planilhas e apresentações
- Arquivos de imagem
- Dados de fluxo de aplicativos
- Dados de fluxo de origens PCAP externas

Os usuários podem fazer upload de diversos arquivos para um caso e um administrador pode conceder a diversos usuários o acesso ao caso.

Restrição: O nome do caso deve ser exclusivo. Um único usuário está associado a um caso, portanto, dois usuários não podem criar um caso que tenha o mesmo nome.

Procedimento

1. Em **Administrador**, clique em **Permissões de usuário do Forensics**.
2. Na lista **Usuários**, selecione um usuário.
3. Na área de janela **Editar usuário**, selecione a caixa de seleção **Ativar acesso FTP**.
4. Insira e confirme a senha FTP para o usuário.
5. Para salvar as mudanças nas permissões, clique em **Salvar usuário**.
6. No cliente FTP, execute as etapas a seguir:
   a. Assegure-se de que Segurança da Camada de Transporte (TLS) esteja selecionada como o protocolo.
   b. Inclua o endereço IP do host do QRadar Incident Forensics.
   c. Crie um logon que usa o nome de usuário e senha do QRadar Incident Forensics que foi criado.
7. Conecte-se ao servidor do QRadar Incident Forensics e crie um novo diretório.
8. Para executar FTP e armazenar arquivos pcap, sob o diretório que você criou para o caso, crie um diretório que é chamado `singles` e arraste os arquivos pcap para esse diretório.
9. Para executar FTP e armazenar outros tipos de arquivos que não sejam arquivos pcap, sob o diretório que você criou para o caso, crie um diretório que é chamado `import` e arraste os arquivos para esse diretório.
10. Para reiniciar o servidor FTP, digite o comando a seguir:
    ```
    etc/init.d/vsftpd restart
    ```
11. Para reiniciar o servidor que move os arquivos da área de upload para o diretório QRadar Incident Forensics, digite o comando a seguir:
    ```
    /etc/init.d/ftpmonitor restart
    ```

Resultados

Um administrador vê os dados que são transferidos por upload no Gerenciamento de caso. Um usuário pode ver seu caso em uma das ferramentas na guia **Forensics**.

Decriptografando tráfego SSL e TLS no QRadar Incident Forensics

Para localizar ameaças ocultas, o IBM Security QRadar Incident Forensics pode decriptografar o tráfego SSL. Se você fornecer a chave privada e o endereço IP do servidor ou uma chave de sessão do navegador e algumas informações de sessão, o inspetor de protocolo poderá decriptografar o tráfego SSL.

Se a chave de sessão for gerada a partir de sites externos ou gerada por outro navegador, o inspetor de protocolo não poderá decriptografar o tráfego SSL de uma sessão de navegador.

Restrição: O mecanismo de troca de chave `Diffie Hellman` não será suportado quando o tráfego criptografado for decriptografado por meio de uma chave privada. Ao usar uma chave privada, outros métodos de troca de chave, como RSA, serão suportados.

A restrição `Diffie Hellman` não se aplicará quando o tráfego for decriptografado com informações que estiverem localizadas em um keylog.

Sobre Esta Tarefa

A decriptografia é suportada para os protocolos a seguir:

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

Os arquivos de log de chave são gerados pelos navegadores Chrome, Firefox e Opera com a variável de ambiente SSLKEYLOGFILE. Os formatos de chave a seguir são suportados para a chave de sessão SSLKEYLOGFILE:

- RSA
- DH

Procedimento

1. Use SSH para efetuar login no host primário do QRadar Incident Forensics como o usuário-raiz.
2. Revise o local das chaves no arquivo `/opt/qradar/forensics.conf`.

   ```
   <sslkeys
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

3. Copie as chaves no diretório que está especificado no arquivo `/opt/qradar/forensics.conf`.
   - Para chaves privadas, copie a chave no diretório `/opt/ibm/forensics/decapper/keys`.

     Exemplo:

     ```
     <keys>
      <key file=" /opt/ibm/forensics/decapper/keys/key_name">
     ```

```
    <address> 1.2.3.4</address>
    <range> 1.2.3.0-1.2.3.255</range>
  </key></keys>
```

- Para arquivos de log de chave que são gerados pelo navegador, copie os arquivos de log de chave no diretório `/opt/ibm/forensics/decapper/keylogs/default`.

Se alterar os subdiretórios nos diretórios `/opt/ibm/forensics/decapper/keys` ou `/opt/ibm/forensics/decapper/keylogs`, você deverá reiniciar o serviço de decapper.

Para reiniciar o serviço decapper, digite o comando a seguir: `service decapper restart`

Capítulo 6. Ações planejadas no QRadar Incident Forensics

É possível planejar a manutenção, como a exclusão de documentos antigos, ajuste o banco de dados e reconfiguração do servidor IBM Security QRadar Incident Forensics.

Se houver muitos documentos, ações planejadas, como a exclusão de documentos antigos, pode demorar a concluir. Se desejar excluir um caso inteiro, use a ferramenta Gerenciamento de caso.

Excluindo documentos

Os administradores podem excluir documentos desatualizados que se baseiam nos registros de data e hora da rede do documento.

É possível excluir documentos, que incluem pcap e outros tipos de arquivo, de um caso ou do servidor. A exclusão de documentos desatualizados ajuda a manter a velocidade ao procurar documentos.

Caso de liberação

Para ajudar a ajustar o gerenciamento de caso, é possível usar a opção **Caso de liberação**. Para dados de *fluxo pcap*, que são uma série de arquivos pcap que estão logicamente relacionados para formar um arquivo pcap grande, é possível forçar dados armazenados em buffer para que sejam gravados no disco. A opção **Caso de liberação** força os hosts do QRadar Incident Forensics a gravar fluxos não finalizados no disco, que, por sua vez, ajuda a procurar esses fluxos em um estágio anterior.

Otimizando o banco de dados

Os administradores podem otimizar o banco de dados para reorganizar o índice do mecanismo de procura em segmentos e remover documentos excluídos.

A ação planejada **Otimizar banco de dados** é semelhante a um comando **`defrag`**.

Ao otimizar o banco de dados, um novo índice é construído. Após o índice ser construído, o novo índice substituirá o índice antigo. Como existem dois índices até que o índice antigo seja substituído, o comando optimize index requer o dobro da quantia de espaço em disco rígido.

Antes de otimizar seu banco de dados, você deverá assegurar que o tamanho de seu índice não exceda 50% do espaço disponível em seu disco rígido.

Planejando ações para hosts do QRadar Incident Forensics

É possível planejar tarefas de manutenção nos hosts do IBM Security QRadar Incident Forensics.

É possível planejar estas tarefas:

- Construir um novo índice para os casos atualmente disponíveis.
- Remover (*idade limite ultrapassada*) documentos que você não deseja reter após um período de tempo especificado.

- Forçar a gravação de dados no disco.

Procedimento

1. Na guia **Administrador**, na seção **Forensics**, clique em **Planejar ações**.
2. Clique em **Incluir Nova Ação**.
3. Na lista **Selecionar ação**, selecione uma ação e especifique as configurações.
   - Para contruir um novo índice para os casos atuais, selecione **Otimizar índice**.

     O novo índice requer cerca do dobro de espaço do índice existente. Certifique-se de ter o espaço adequado.
   - Para excluir documentos que têm um registro de data e hora de rede mais antigo do que a idade especificada, selecione **Documentos com idade limite ultrapassada**.

     Os índices também são removidos quando você exclui os documentos.
   - Para gravar fluxos não finalizados no disco, selecione **Caso de liberação**.
4. Clique em **Salvar**.
5. Para executar, editar ou excluir a ação, selecione a ação para a lista **Ações** e clique em **executar**, **editar** ou **excluir**.

Capítulo 7. Gerenciando conteúdo suspeito

Como um administrador, é possível sinalizar conteúdo suspeito usando o recurso Gerenciamento de conteúdo suspeito.

Regras de Yara

Para sinalizar conteúdo suspeito nos arquivos que são localizados no tráfego de rede do QRadar Incident Forensics, é possível importar e usar regras de Yara existentes para especificar as regras customizadas que são executadas nos arquivos.

Cada regra de Yara inicia com a regra de palavra-chave seguida por um identificador de regra. Regras de Yara são compostas de duas seções:

1. Definição de sequência: na seção de definição de sequências, especifique as sequências que farão parte da regra. Cada sequência usa um identificador que consiste em um símbolo de dólar ($) seguido por uma sequência de caracteres alfanuméricos que são separados por sublinhados.
2. Condição: na seção de condição, defina a lógica da regra. Essa seção deve conter uma expressão booleana que defina as condições nas quais um arquivo satisfaz a regra.

O exemplo a seguir mostra uma regra de Yara simples:

```
rule simple_forensics : qradar
{
    meta:
        description = "This rule will look for str1 at an offsets of 25 bytes
                       into the file."
    sequências:
        $str1 = "pattern of interest"

    condition:
        $a at 25
}
```

O exemplo a seguir mostra uma regra de Yara mais complexa:

```
rule ibm_forensics : qradar
{
    meta:
        description = "This rule will flag content that contains the hex
                       sequence as well as str1 at least 3 times."

    sequências:
        $hex1 = {4D 2B 68 00 ?? 14 99 F9 B? 00 30 C1 8D}
        $str1 = "IBM Security!"


    condition:
        $hex1 and (#str1 > 3)
}
```

Quando a regra de Yara é transferida por upload, o removedor de proteção usa regras que são especificadas quando ele localiza um arquivo em uma recuperação ou um upload de PCAP. Se conteúdo correspondente for localizado, um campo **SuspectContent** será incluído sob a guia **Atributos** para um documento. O campo **SuspectContent** é preenchido com um nome de regra de Yara e quaisquer tags identificadas pela regra.

Restrição: A implementação dos módulos Yara não está atualmente disponível.

Importando regras de Yara

É possível importar suas regras de Yara existentes no IBM Security QRadar Incident Forensics e usá-las para corresponder e sinalizar conteúdo malicioso. Mais de uma regra de Yara pode existir em um arquivo importado.

Procedimento

1. Na guia **Administrador**, selecione **Gerenciamento de conteúdo suspeito**.
2. Clique em **Selecionar arquivo**.
3. Na janela Upload de arquivo, procure o arquivo que deseja importar e clique em **Abrir**.

   Importante: Nomes de regra de Yara devem ser exclusivos.

Resultados

Você verá uma mensagem quando a regra de Yara tiver sido importada com êxito.

O que Fazer Depois

Regras de Yara recentemente importadas não serão aplicadas retroativamente. Após importar as regras de Yara, deve-se executar uma implementação completa para as mudanças entrarem em vigor.

Excluindo regras de Yara

É possível excluir todas as regras de Yara existentes do IBM Security QRadar Incident Forensics. Faça upload de um arquivo que contenha uma única regra vazia para desligar as regras de Yara.

Antes de Iniciar

Procedimento

1. Para criar um novo arquivo que contenha uma única regra vazia, use as etapas a seguir:
   a. Copie a regra a seguir em um editor de texto da sua escolha:

      ```
      rule empty
      {
       condition:
                 falso
      }
      ```

   b. Salve como um arquivo de texto.
2. Na guia **Administrador**, selecione **Gerenciamento de conteúdo suspeito**.
3. Clique em **Selecionar arquivo**.
4. Na janela Upload de arquivo, procure o arquivo que você criou na Etapa 1 e clique em **Abrir**.
5. Clique em **Salvar**.

Resultados

A regra única sempre retorna um resultado **`false`**, que a permite passar o validador. A regra única exclui todas as regras existentes e é inserida no banco de

dados. A regra única nunca sinaliza conteúdo como suspeito.

Capítulo 8. Auditando o usuário e o uso do sistema no QRadar Incident Forensics

Os logs de auditoria são registros cronológicos que identificam contas de usuários que estão associadas ao acesso de dados. Esses logs podem detectar o acesso incomum ou não autorizado e podem identificar problemas como tarefas com falhas.

As atividades a seguir geram eventos de log de auditoria:

- Criar caso
- Designar caso
- Excluir caso
- Excluir coleta
- Todas as consultas do usuário
- Visualização do documento
- Exportar documento

Restrição: A criação de log para criar eventos de coleta não é suportada.

Procedimento

1. Use SSH para efetuar logon no QRadar Console ou QRadar Incident Forensics Standalone como administrador.
2. Acesse o diretório `/var/log/audit`.
3. Abra o arquivo `audit.log` em um editor, como vi, para revisar o conteúdo ou use o comando **`grep`** para procurar uma entrada específica.

Capítulo 9. Investigar ameaças com o QRadar Network Insights

Use o IBM QRadar Network Insights para analisar seus dados da rede em tempo real para que seja possível examinar o comportamento de ameaça em sua rede.

O QRadar Network Insights é uma solução de análise de ameaça de rede que detecta rápida e facilmente ameaças internas, exfiltração de dados e atividade de malware. Os indicadores de ameaças essenciais são reunidos e rastreados com visibilidade integral por meio do tráfego de rede.

Investigações de ameaças em tempo real com o QRadar Network Insights

O IBM QRadar Network Insights fornece análise em tempo real de dados da rede e um nível avançado de detecção de ameaça e análise.

As ameaças avançadas de cybersegurança estão cada vez mais difíceis de se detectar e evitar. A atividade maliciosa geralmente é disfarçada de uso normal, o que permite que as ameaças se movam e se comuniquem entre redes para realizar seus objetivos. Por exemplo, o malware se transforma para evitar detecção baseada em assinatura e as técnicas de engenharia social, como phishing, são efetivas ao abrir a porta para esses ataques.

Capacidade de pesquisa

O recurso de procura do QRadar Network Insights localiza e extrai indicadores importantes dos dados de pacote, por exemplo, informações de fluxo, metadados, conteúdo extraído e conteúdo suspeito. É possível usar o conteúdo extraído para análise retrospectiva de longo prazo.

Integração com o IBM Security QRadar Incident Forensics

O QRadar Network Insights registra atividades do aplicativo, captura artefatos e identifica ativos, aplicativos e usuários que participam das comunicações de rede. O QRadar Network Insights é totalmente integrado ao IBM Security QRadar Incident Forensics para investigações de incidente de postagem e atividades de busca de ameaça. O QRadar Incident Forensics e o IBM QRadar Network Packet Capture capturam, reconstroem e reproduzem toda a conversa, mas o QRadar Network Insights fornece a detecção de incidentes e informa se itens suspeitos ou tópicos de interesse foram discutidos a qualquer momento durante a conversa.

O conteúdo suspeito pode se originar de uma ampla variedade de fontes, como malware, portas não padrão, expressão regular ou regras Yara.

Valor de fluxos

Os fluxos fornecem o QRadar com visibilidade entre a atividade de rede porque permitem a detecção de ativos quando os dispositivos se conectam a uma rede. Com o QRadar Network Insights, é possível correlacionar os dados de fluxo a dados do evento para detectar ameaças que não podem ser identificadas por logs sozinhos. O IBM Security QRadar QFlow Collector fornece fluxos de rede e

também reconhece aplicativos de camada 7 e é possível capturar o início das sessões. O QRadar Network Insights revela ameaças anteriormente ocultas e comportamentos maliciosos.

Conceitos relacionados:

"Níveis de inspeção de fluxo do QRadar Network Insights" na página 28
Para melhorar o desempenho, deve-se escolher a taxa de fluxo apropriada que é necessária ao configurar o **Nível de inspeção de fluxo**.

Implementações do QRadar Network Insights

O IBM QRadar Network Insights é um host gerenciado que você anexa ao console do QRadar.

Para uma implementação do QRadar Network Insights, deve-se selecionar a opção de dispositivo `6200` durante a instalação. Para obter mais informações sobre instalar o dispositivo QRadar Network Insights, consulte o *IBM Security QRadar Incident Forensics Installation Guide*.

Para uma implementação do QRadar Network Insights, é necessário alocar uma licença para a opção de dispositivo `6200`. O QRadar Network Insights requer uma licença separada para o dispositivo `6200`, mas não é necessária uma licença do QRadar Network Insights no console do QRadar.

Relacionamento de dispositivo do QRadar Network Insights com o IBM Security QRadar Incident Forensics

É possível implementar o QRadar Network Insights separadamente da implementação do IBM Security QRadar Incident Forensics Processor. O QRadar Network Insights requer somente uma conexão com o console do QRadar e não requer uma conexão com o dispositivo do QRadar Incident Forensics.

Dispositivo QRadar Network Insights

O dispositivo QRadar Network Insights 1920 é acompanhado de duas placas de rede de terceira geração. As placas de rede são grampeadas diretamente à rede para ajudar na inspeção de pacote em tempo real.

O recurso de encaminhamento de fluxo configurável permite o balanceamento de carga entre múltiplos dispositivos. A configuração de hardware ajuda no processamento de memória para permitir a análise em tempo real dos dados da rede.

Tabela 2. Especificações de placa de rede

Dispositivo 1920	Descrição
`Servidor`	X3650 M5
`CPU`	2 x E5-2680 v4 14C 2,4 GHz 35 MB 2400 MHz 120 W
`RAM`	8 x 16 GB
`HDD`	SSD 2 x 200 GB
`ServeRAID`	M1215
`Placas de E/S`	Intel X520 2P 10 GbE + 2 x 10 G SR 2 x NT40E3 4P 40 G + 2 x 10 G SR + 2 x 10 G LR
`P/S`	2 x 900 W

Requisitos de configuração do QRadar Network Insights

Após instalar o IBM QRadar Network Insights e anexá-lo ao QRadar Console como um host gerenciado, deve-se configurar seu dispositivo antes de poder começar a usá-lo para investigar ameaças em sua rede. O dispositivo QRadar Network Insights lê os pacotes brutos por meio de um grampo de rede ou porta de span e, em seguida, gera pacotes IPFIX. Os pacotes IPFIX são enviados para o processo do QFlow no QRadar Console.

Configurando formato do QFlow Collector

Como um gerente de um cluster de host gerenciado do QRadar, é possível escolher o formato que seu QFlow Collectors usa para exportar dados para o QFlow Processor: TLV ou Carga útil.

Antes de Iniciar

Assegure que os requisitos a seguir sejam atendidos:

__ • Instale um QRadar Console com um QRadar Network Insights anexo como um host gerenciado.

__ • Execute uma implementação integral após anexar o IBM QRadar Network Insights como um host gerenciado.

Procedimento

1. Efetue login no QRadar: `https://IP_Address_QRadar`

   O nome de usuário padrão é `admin`. A senha é aquela da conta do usuário raiz.
2. Clique na guia **Administrador**.
3. Na área de janela de navegação, clique em **System Settings**.
4. Clique no menu **Configurações do QFlow** e escolha o formato do QFlow.

Tabela 3. Opções de formato do QFlow

Formato do QFlow	Descrição
`TLV`	Configuração de formato do QFlow padrão. Escolha **TLV** (tab-length-value) para novas instalações ou para upgrades que não possuam um dispositivo do QRadar Network Insights como parte de sua implementação.
`Payload`	Escolha **Carga útil** para upgrades que possuam um dispositivo do QRadar Network Insights como parte de sua implementação. Isso significa que a implementação pode continuar trabalhando como estava.

5. Clique em **Salvar**.
6. Na barra de menus da guia **Administrador**, clique em **Implementar configuração integral** e confirme as mudanças.
7. Atualize seu navegador da web para visualizar a guia **Forense**.

Configurando um DTLS em um host gerenciado do QRadar Network Insights

Para evitar espionagem do tráfego de rede e grampo, deve-se configurar o Datagram Transport Layer Security (DTLS) em um host gerenciado do QRadar Network Insights. Deve-se configurar uma fonte de fluxo primeiro.

Procedimento

1. Inclua o QRadar Network Insights como um host gerenciado:
   a. Clique na guia **Administrador**.

b. Na área de janela de navegação, clique em **Sistema e gerenciamento de licença** na seção **Configuração do sistema**.
c. Selecione o host gerenciado do QRadar Network Insights. O tipo de dispositivo é `6200`.
d. Clique no ícone **Ações de implementação** e selecione **Incluir host**.
e. Quando solicitado, insira o endereço IP e a senha raiz do host gerenciado do QRadar Network Insights e clique em **Incluir**.

2. Para configurar uma fonte de fluxo, use as etapas a seguir:
a. Efetue login no QRadar como administrador.
b. Clique na guia **Administrador**.
c. Na área de janela de navegação, clique em **Fontes de fluxo** na seção **Fluxos**.
d. Clique no ícone **Incluir** .
e. Especifique um **Nome de fonte de fluxo** descritivo.
f. Selecione um **Coletor de fluxo de destino** ou aceite o valor fornecido.
g. Selecione **Netflow v.1/v.5/v.7/v.9/IPFIX** como o **Tipo de fonte de fluxo**.
h. Insira um valor para a **Porta de monitoramento** ou aceite o valor fornecido.
i. Selecione `DTLS` na lista **Protocolo de link**.
j. Clique em **Salvar**.
k. Na barra de menus da guia **Administrador**, clique em **Implementar configuração integral** e confirme as mudanças.
l. Atualize seu navegador da web.

3. Para configurar a comunicação do DTLS, use as etapas a seguir:

Nota: Se você mudar o QRadar Flow Collector ou a fonte de fluxo de qualquer host gerenciado do QRadar Network Insights em sua implementação, deverá executar o script de configuração do DTLS novamente.
a. Clique no ícone **Ações de implementação** e selecione **Editar conexão de host**.
b. Na página Modificar QRadar Network Insights, selecione QRadar Flow Collector e a fonte de fluxo.
c. Clique em **Salvar**.
d. Feche a página Sistema e gerenciamento de licença.
e. Na guia **Administrador**, clique no ícone **Implementar mudanças**.
f. Use o **SSH** para efetuar login como o usuário raiz no QRadar Console.
g. Execute este comando para configurar o certificado do DTLS:
`python /opt/qradar/bin/qflow_dtls_cert_setup.py`
h. Efetue login no QRadar como administrador.
i. Na guia **Admin**, selecione **Avançado** > **Implementar configuração integral**.

Níveis de inspeção de fluxo do QRadar Network Insights

Para melhorar o desempenho, deve-se escolher a taxa de fluxo apropriada que é necessária ao configurar o **Nível de inspeção de fluxo**.

A taxa de fluxo está relacionada aos níveis de visibilidade por meio do conteúdo disponível, como origem, destino, protocolo e tipos de arquivos específicos.

Os níveis de inspeção de fluxo são acumulativos, portanto, cada nível leva as propriedades do nível anterior.

Flows

Os fluxos são o nível mais baixo de inspeção. Os fluxos são detectados por 5 tuplas e o número de bytes e pacotes que estão fluindo em cada direção são contados. Este tipo de informação é semelhante ao que você obtém de um roteador ou comutador de rede que não executa uma inspeção abrangente de pacote. Esse nível suporta a largura da banda mais alta, mas gera a menor quantia de informações de fluxo.

Os atributos que o QRadar Network Insights gera usando o nível de inspeção de fluxo são: valores de 5 tuplas, um ID de fluxo, contagens de pacote e octetos em cada direção e horários de início e término de fluxo.

Fluxos enriquecidos

Cada fluxo é identificado e inspecionado por um dos inspetores de protocolo ou domínio e muitos tipos de atributos podem ser gerados por meio dessa inspeção.

A lista a seguir descreve os atributos que o QRadar Network Insights gera usando o nível de inspeção de fluxos enriquecidos:

- Valores de metadados HTTP - incluindo categorização de URLs
- ID de aplicativo e ação
- Informações do arquivo (nome, tamanho, hash)
- Nomes de usuário de origem e de destinatário
- Valores de conteúdo suspeito limitado

Fluxos enriquecidos do conteúdo

Os fluxos enriquecidos do conteúdo são a configuração padrão e o nível mais alto de inspeção. Todos os atributos que o nível de fluxos enriquecidos faz e também varre e inspeciona o conteúdo dos arquivos que localiza. Isso resulta em uma determinação de tipo de conteúdo mais precisa e pode produzir mais valores de conteúdo suspeito originados na inspeção do conteúdo do arquivo.

A lista a seguir descreve os atributos que o QRadar Network Insights gera usando o nível de inspeção de fluxos enriquecidos de conteúdo:

- Informações Pessoais
- Dados confidenciais
- Scripts integrados
- Redirecionamentos
- Conteúdo suspeito baseado em conteúdo configurável

Tabela 4. Considerações sobre o desempenho

Configuração de nível de inspeção de fluxo	**Desempenho**
`Fluxos`	10 Gbps
`Fluxos enriquecidos`	Aproximadamente 10 Gbps. O desempenho varia dependendo da configuração de nível de inspeção, da procura, dos critérios de extração e dos dados da rede.
`Fluxos enriquecidos de conteúdo (Avançado)`	Aproximadamente 3,5 Gbps. O desempenho de 10 Gbps é acessível com múltiplos dispositivos.

Conceitos relacionados:

"Investigações de ameaças em tempo real com o QRadar Network Insights" na página 25
O IBM QRadar Network Insights fornece análise em tempo real de dados da rede e um nível avançado de detecção de ameaça e análise.

Definindo as Configurações do QRadar Network Insights

Para melhorar o desempenho, configure os níveis de fluxos que os dispositivos do QRadar Network Insights em suas implementações produzem. Cada nível de inspeção fornece visibilidade mais profunda e extrai mais conteúdo.

Procedimento

1. Efetue login no QRadar como administrador.
2. Clique na guia **Administrador**.
3. Na área de janela de navegação, clique em **System Settings**.
4. Clique no menu **Configurações do Network Insights**.
5. No **Nível de inspeção de fluxo**, selecione a taxa de fluxo que é necessária. Use a tabela a seguir para entender os níveis de inspeção de fluxo:

Tabela 5. Níveis de inspeção de fluxo

Nível de inspeção de fluxo	Descrição
`Fluxos`	Nível mais baixo de inspeção. Os fluxos são detectados por 5 tuplas e o número de bytes e pacotes que estão fluindo em cada direção são contados.
`Fluxos enriquecidos`	Cada fluxo é identificado e inspecionado por um dos inspetores de protocolo ou domínio e muitos tipos de atributos podem ser gerados por meio dessa inspeção.
`Fluxos enriquecidos de conteúdo`	A configuração padrão. O nível mais alto de inspeção. Faz tudo que os níveis de Fluxos enriquecidos fazem, mas também varre e inspeciona o conteúdo dos arquivos que ele localiza.

6. Clique em **Salvar**.
7. Na barra de menus da guia **Administrador**, clique em **Implementar configuração integral**.
8. Atualize seu navegador da web.

O que Fazer Depois

Implemente o host gerenciado pelo QRadar Incident Forensics Processor.

Detecção de ameaças com o QRadar Network Insights

Para visibilidade em tempo real para a atividade de ameaça em sua rede, use QRadar Network Insights para detectar indicadores de ataques cibernéticos e sua atividade maliciosa.

Fazendo download do conteúdo do QRadar Network Insights

Você faz download do conteúdo do QRadar Network Insights (extensão) por meio do IBM Security App Exchange (http://exchange.xforce.ibmcloud.com/hub/extension/522bf1095f047b0b37225d8efc5d4877). Você usa a ferramenta **Gerenciamento de extensões** para instalá-los.

Para obter informações sobre o uso da ferramenta **Gerenciamento de extensões**, consulte o *IBM Security QRadar Administration Guide*.

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

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.

Quaisquer 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 nesses websites não fazem parte dos materiais deste produto IBM e o uso desses websites é de total 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
Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Av. Pasteur, 138/146 - Botafogo
Rio de Janeiro, RJ
Estados Unidos

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.

Os dados de desempenho e os exemplos dos clientes citados são apresentados para fins ilustrativos apenas. Resultados reais de desempenho podem variar dependendo de configurações específicas e condições operacionais.

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.

As declarações relacionadas a direção ou intenção futuros da IBM estão sujeitas a alteração ou retirada sem aviso prévio e representam metas e objetivos apenas.

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 esses nomes são fictícios e qualquer semelhança com empresas ou pessoas reais é mera coincidência.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas comerciais da International Business Machines Corp., registradas em muitas jurisdições no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou outras empresas. Uma lista atual das marcas comerciais da IBM está disponível na web em "Informações de marca comercial e copyright" em www.ibm.com/legal/copytrade.shtml.

Adobe, o logotipo Adobe, PostScript e o logotipo PostScript são marcas registradas ou marcas comerciais da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

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

Termos e condições para a documentação do produto

Permissões para o uso dessas publicações são concedidas de acordo com os seguintes termos e condições.

Aplicabilidade

Esses termos e condições estão completando quaisquer termos para uso do website IBM.

Uso pessoal

Você pode reproduzir estas publicações para seu uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou fazer trabalho derivado dessas publicações, ou qualquer parte delas, sem o consentimento expresso da IBM.

Uso Comercial

É possível reproduzir, distribuir e exibir essas publicações unicamente dentro de sua empresa, contanto que todos os avisos do proprietário sejam preservados. Não é permitido criar trabalhos derivados destas publicações, ou reproduzir, distribuir ou exibir estas publicações ou qualquer porção das mesmas fora de sua empresa, sem o consentimento expresso da IBM.

Direitas

Exceto conforme expressamente concedido nessa permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, às publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contida neste.

A IBM reserva-se o direito de retirar as permissões concedidas neste documento sempre que, a seu critério, o uso das publicações for prejudicial ao seu interesse ou, conforme determinado pela IBM, as instruções acima não estiverem sendo seguidas da maneira adequada.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto se elas estiverem totalmente em conformidade com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentações de exportação dos Estados Unidos.

A IBM NÃO SE RESPONSABILIZA PELO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM" E SEM GARANTIA DE QUALQUER TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E DE ADEQUAÇÃO PARA UM PROPÓSITO ESPECÍFICO.

Declaração de privacidade on-line da IBM

Os produtos do software IBM, incluindo as soluções de software como serviço, (“Ofertas de software”) podem usar cookies ou outras tecnologias para coletar informações do uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitas 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 informações pessoais identificáveis, informações específicas sobre o uso de cookies desta oferta serão estabelecidas 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 e a Declaração de privacidade online da IBM em http://www.ibm.com/privacy/details, a seção intitulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de software como serviço e de produtos de software IBM” em http://www.ibm.com/software/info/product-privacy.

Impresso no Brasil