IBM Security QRadar Incident Forensics
Versão 7.2.5

Guia de administração

Nota

Antes de usar estas informações e o produto que elas suportam, leia as informações em "Avisos" na página 21.

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

Para obter informações sobre como acessar mais documentação técnica na biblioteca de produtos QRadar, consulte Acessando a Nota Técnica de 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 a 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 proteger sistemas e informações por meio de prevenção, detecção e resposta ao acesso incorreto de dentro e fora de sua empresa. O acesso incorreto pode resultar em informações que são alteradas, destruídas, desapropriadas ou usadas indevidamente ou pode resultar em dano ou uso indevido dos sistemas, inclusive para uso em ataques a outros. 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 IBM são projetados para fazerem parte de uma abordagem de segurança legal abrangente, que envolverá necessariamente procedimentos operacionais adicionais e poderá requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS SÃO IMUNES, OU DEIXARÃO SUA EMPRESA IMUNE, DE CONDUTAS ILEGAIS OU MALICIOSAS DE QUALQUER PARTE.

Observação:

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 pode ser usado somente 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 obteve ou obterá as permissões ou licenças necessárias para possibilitar o uso do IBM Security QRadar dentro da lei.

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 somente para propósitos legais e de maneira 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 obteve todos os consentimentos, permissões ou licenças necessários para permitir seu uso legal do IBM Security QRadar Incident Forensics.

Capítulo 1. O que há de novo para os administradores no QRadar Incident Forensics V7.2.5

O IBM Security QRadar Incident Forensics V7.2.5 introduz o processamento de dados nos hosts gerenciados do QRadar Incident Forensics ou em um host do QRadar Incident Forensics Standalone.

Distribuir processamento de arquivos pcap transferidos por upload manualmente através de hosts do QRadar Incident Forensics

Para distribuir processamento, você pode fazer upload de captura de pacote (arquivos pcap) ou de documentos, como planilhas, imagens, arquivos PDF e muito mais para qualquer host gerenciado que desejar que processe os dados. Você pode também pode fazer upload de arquivos para o host QRadar Incident Forensics Standalone.  Saiba mais...

Arquivos FTP para qualquer host do QRadar Incident Forensics

Como um administrador, você pode permitir que usuários transfiram por FTP arquivos grandes para qualquer host gerenciado do QRadar Incident Forensics. Usuários podem selecionar qual host gerenciado do QRadar Incident Forensics processa os dados. Os usuários também podem transferir por FTP arquivos para o host do QRadar Incident Forensics Standalone.  Saiba mais...

Copiar arquivos manualmente para qualquer host do QRadar Incident Forensics

Diferente da ferramenta Gerenciamento de caso, não há restrições no tamanho do arquivo ou no número de arquivos ao importar arquivos manualmente. É possível usar o comando **scp** para copiar arquivos com segurança de outro host para o diretório `/opt/ibm/forensics/case_input/case_input/` em qualquer host do IBM Security QRadar Incident Forensics.  Saiba mais...

Capítulo 2. Visão geral de administração do QRadar Incident 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.

Dve-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 *IBM Security QRadar SIEM Administration Guide*.

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.

Máximo de download de arquivo (MB)
O tamanho máximo da captura de arquivo que um dispositivo de captura de pacote pode recuperar. Dependendo da densidade do tráfego de rede, você poderá precisar aumentar o limite. Por exemplo, quando há incidentes de segurança na guia **Forensics** e nenhuma recuperação, você poderá tentar aumentar o limite do tamanho do arquivo.

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.

Filtro de categoria da web

É possível excluir tipos específicos de tráfego de rede HTTP das investigações. Quando os dados de tráfego de rede HTTP forem consumidos, 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.

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.

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**.
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.

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.

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**.

     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: ou arraste-os para a caixa de upload.
   - Clique em **Incluir pcaps**, 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**.

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.

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**.

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**.

Capítulo 5. 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.

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.

Capítulo 6. 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 7. 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
- SMTP
- 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 (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

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).

Os termos a seguir são marcas comerciais ou marcas registradas de outras empresas:

Os termos a seguir são marcas comerciais ou marcas registradas de outras empresas:

Adobe e Acrobat e todas as marcas comerciais baseadas em Adobe 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 Sun Microsystems, Inc. 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.

Considerações Sobre a Política de Privacidade

Produtos IBM Software, incluindo soluções de software como 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, 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 informações pessoalmente identificáveis, informações específicas sobre o uso de cookies desta oferta serão apresentadas a seguir.

Dependendo das configurações implementadas, esta Oferta de Software pode usar cookies de sessão que coletam o ID de sessão de cada usuário para propósitos de gerenciamento 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 estes propósitos, consulte a Política de Privacidade da IBM em http://www.ibm.com/privacy e a Declaração de Privacidade Online da IBM na seção http://www.ibm.com/privacy/details titulada “Cookies, web beacons e outras tecnologias” e a “Declaração de privacidade de produtos de software IBM e de software como serviço” em http://www.ibm.com/software/info/product-privacy.