

IBM Security QRadar Incident Forensics  
Versão 7.3.0

*Guia do Usuário*



**Nota**

Antes de usar estas informações e o produto que ela suporta, leia as informações em “Avisos” na página 43.

**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.

© Copyright IBM Corporation 2014, 2017.

---

# Índice

<b>Introdução ao uso do IBM Security QRadar Incident Forensics . . . . .</b>	<b>v</b>
<b>Capítulo 1. O que há de novo para os usuários no QRadar Incident Forensics V7.3.0 . . .</b>	<b>1</b>
<b>Capítulo 2. Investigações de segurança . . . . .</b>	<b>3</b>
Investigações de segurança de rede . . . . .	4
Paciente zero: identificar a fonte de um ataque . . . . .	4
Sistemas comprometidos . . . . .	5
Os dados vazaram para entidades desautorizadas . . . . .	5
Investigações de análise de funcionário . . . . .	6
Uso indevido de acesso. . . . .	6
Conluio . . . . .	7
Sabotagem . . . . .	8
Investigações de abuso e fraude . . . . .	8
Transações desautorizadas . . . . .	8
Alocação não sancionada de recursos . . . . .	9
Desvios de protocolo e evasão de controles legais . . . . .	10
Investigações de coleção de evidências . . . . .	10
Confiança na identificação de ameaças . . . . .	10
Refinando as práticas de segurança . . . . .	11
Avaliações de risco . . . . .	12
<b>Capítulo 3. Iniciando com investigações forenses . . . . .</b>	<b>13</b>
QRadar Incident Forensicsprocuras e marcadores. . . . .	14
Procura de documentos e investigação . . . . .	15
Recuperação forense . . . . .	15
Casos forenses . . . . .	16
Coleções . . . . .	16
Fazendo upload de arquivos pcap e documentos de sistemas externos para casos forenses . . . . .	17
Consultas no repositório forense . . . . .	18
Termos de consulta de formato livre . . . . .	18
Tags de metadados . . . . .	19
Combinações booleanas . . . . .	20
Ferramenta do gerador de consultas . . . . .	21
Ferramenta de filtro de consulta . . . . .	22
Resultados para filtros ativos . . . . .	22
Os filtros de procura para a ferramenta de filtro de consulta . . . . .	22
Limitando o número de documentos retornados em uma procura . . . . .	23
Anotações do documento. . . . .	23
<b>Capítulo 4. Ferramentas de investigação . . . . .</b>	<b>25</b>
Visualização de rede e documento. . . . .	25
Inspecionando tráfego de rede e documentos em um bloco de tempo . . . . .	26
Ferramenta pesquisadora . . . . .	26
Visualização de documento reconstruída. . . . .	27
Conteúdo do documento extraído . . . . .	27
Exportação de documentos no QRadar Incident Forensics . . . . .	27
Exportando documentos como arquivos pcap . . . . .	27
Impressão digital . . . . .	28
Investigando relacionamentos para controlar trilhas de identidade . . . . .	29
Ferramenta Visualizar . . . . .	30
Visualizando relações e associações . . . . .	30
Análise de artefato para conteúdo suspeito ou malicioso . . . . .	31
Analisando arquivos para conteúdo integrado e atividade maliciosa . . . . .	35

Analisando as imagens para ameaças ocultas ou atividade suspeita. . . . .	36
Analisando links com conexões e relações . . . . .	36
Executando uma recuperação a partir de uma página Atributos do documento. . . . .	37
<b>Capítulo 5. Investigando o tráfego de rede para um endereço IP . . . . .</b>	<b>39</b>
BPF customizado . . . . .	40
<b>Avisos . . . . .</b>	<b>43</b>
Marcas comerciais . . . . .	45
Termos e condições para a documentação do produto . . . . .	45
Declaração de privacidade on-line da IBM . . . . .	46
<b>Glossário . . . . .</b>	<b>47</b>
A. . . . .	47
C. . . . .	47
D. . . . .	47
F. . . . .	47
H. . . . .	47
I. . . . .	48
M. . . . .	48
O. . . . .	48
P. . . . .	48
R. . . . .	48
S. . . . .	48
T. . . . .	48
V. . . . .	49
<b>Índice Remissivo . . . . .</b>	<b>51</b>

---

# Introdução ao uso do IBM Security QRadar Incident Forensics

Este guia contém informações sobre a investigação dos incidentes de segurança usando o IBM® Security QRadar Incident Forensics.

## Público desejado

Os investigadores extraem informações do tráfego de rede e dos documentos no repositório forense. Essas informações são usadas na investigação dos incidentes de segurança.

## 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](http://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. A IBM 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 melhorar seu ambiente de segurança e dados. Mais especificamente, o IBM Security QRadar Incident Forensics foi projetado para ajudar as empresas a investigar e entender melhor o que aconteceu em incidentes de segurança de rede. A ferramenta permite que as empresas indexem e procurem dados de pacote de rede capturados (PCAPs) e inclui um recurso que pode reconstruir esses dados para seu formato original. Esse recurso de reconstrução pode reconstruir dados e arquivos, incluindo mensagens de email, arquivo e anexos de figura, telefonemas VoIP e websites. Informações adicionais sobre os recursos e as funções do Programa e como eles podem ser configurados estão contidas nos manuais e em outra documentação que acompanha o Programa. O uso deste Programa pode envolver diversas leis ou regulamentos. Incluindo aqueles relacionados a privacidade, proteção de dados, emprego, comunicações eletrônicas e armazenamento. O IBM Security QRadar Incident Forensics pode ser usado somente para fins lícitos e de forma legal. O Cliente concorda em usar este Programa de acordo com, e assume toda a responsabilidade pelo cumprimento das leis, dos regulamentos e das políticas aplicáveis. O licenciado declara que irá obter ou obteve quaisquer consentimentos, permissões ou licenças necessários para ativar o uso legal do IBM Security QRadar Incident Forensics.

---

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

O IBM Security QRadar Incident Forensics V7.3.0 introduz a seleção de dispositivo Packet Capture (PCAP) para os usuários que estão executando uma recuperação.

### **A seleção do dispositivo PCAP disponível para uma recuperação do QRadar Incident Forensics**

Para ver somente o tráfego dos dispositivos PCAP em sua implementação ao executar uma recuperação do QRadar Incident Forensics, escolha **Dispositivo de captura customizado**.

 Saiba mais sobre a seleção de dispositivo PCAP..





---

## Capítulo 2. Investigações de segurança

Com o IBM Security QRadar Incident Forensics, é possível detectar ameaças emergentes, determinar a causa raiz e evitar recorrências. Usando ferramentas forenses, é possível focar rapidamente sua análise em quem iniciou a ameaça, como fizeram isso e o que foi comprometido.

Como um investigador forense, é possível reconstituir as ações passo a passo dos criminosos cibernéticos e reconstruir os dados de rede brutos que estão relacionados a um incidente de segurança.

Primeiramente, quando sua organização souber de uma ameaça ou de um potencial risco de segurança ou violação de conformidade, você configura objetivos para avaliar o escopo, identificar as entidades que estão envolvidas e entender as motivações.

É possível usar as ferramentas no IBM Security QRadar Incident Forensics em cenários específicos nos diferentes tipos de investigações, como segurança de rede, análise de funcionário, fraude e abuso e coleta de evidências.

1. Recuperar e reconstruir sessões de rede para e a partir de um endereço IP.
2. A partir dos incidentes que são criados, será possível consultar as categorias de atributos para reunir evidência.

Ao criar uma recuperação, um incidente será criado.

3. Use os filtros de procura para recuperar somente as informações que interessam.
4. Dependendo do tipo de investigação, escolha a ferramenta forense que fornece a evidência necessária.

### Conteúdo suspeito

É possível usar a procura para procurar por qualquer elemento contextual ou identificador conhecido sobre o invasor ou incidente. Se você usar a palavra-chave na procura, o conteúdo suspeito será retornado. Algum conteúdo suspeito pode ser relevante para a investigação.

### Transformação de dados

A transformação de dados é alcançada fazendo com que o conteúdo retornado pelo resultado da procura apareça como um hotlink. Por exemplo, se você procurar "Tom", os resultados podem incluir emails que Tom escreveu, os bate-papos de Tom e informações contextuais adicionais. Ao clicar para visualizar um email, todo ativo ou entidade, como anexos ou IDs de computadores que Tom usou, aparecem como links. Um investigador pode usar esses links para uma rápida investigação.

### Impressão digital

Use a Impressão digital para examinar os dados e mapear o relacionamento entre entidades, como endereços IP, nomes e endereços MAC com base na frequência. É possível selecionar um ou mais resultados para visualizar a frequência e direção do relacionamento.

## Pesquisador

Use o Pesquisador para ver uma linha de tempo das atividades para que seja possível reconstituir um ataque. O pesquisador reconstrói a sessão e classifica os documentos em ordem de tempo.

## Filtragem de conteúdo

Use a filtragem de conteúdo para olhar para um subconjunto de categorias de conteúdo, como Correio da Web, Pornografia, para ajudá-lo a remover o ruído ou conteúdo irrelevante durante a procura.

---

## Investigações de segurança de rede

É possível usar o QRadar Incident Forensics para detectar e investigar atividades maliciosas destinadas a ativos críticos. É possível usar as ferramentas forenses integradas para ajudá-lo a corrigir uma violação de segurança de rede e evitar que isso ocorra novamente.

Use as ferramentas investigativas do QRadar Incident Forensics para ajudá-lo a descobrir como o evento ocorreu, minimizar seu impacto e fazer tudo o que puder para evitar outra violação.

## Paciente zero: identificar a fonte de um ataque

Neste cenário, uma organização é alertada de uma violação suspeita. O objetivo é localizar o ponto inicial de um ataque para isolar a fonte. A organização deve colocar em quarentena as entidades comprometidas para evitar a propagação do ataque para outras partes da organização.

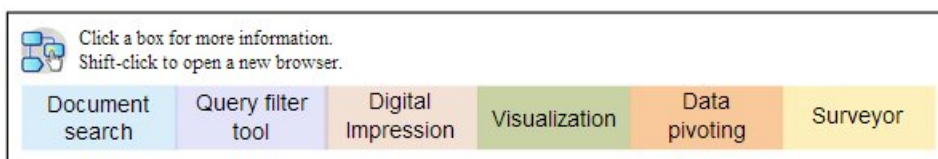
### Objetivos

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Determinar o tipo de ataque.
- Identificar o ponto de entrada inicial da ameaça.
- Obter detalhes sobre a carga útil maliciosa.
- Entender como a carga útil maliciosa foi disseminada além do ponto de entrada.

### Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar atributos sintomáticos que estão associados à carga útil maliciosa.
2. Use categorias de conteúdo para filtrar o conteúdo que não seja relevante para a investigação.
3. Examine o conteúdo suspeito sinalizado pelo produto.

4. Use as Impressões digitais e visualizações para explorar relacionamentos de extensão da carga útil maliciosa, do perpetrador ou do destino.
5. Use a transformação de dados e siga as ligações de dados para identificar o paciente zero.
6. Use o Pesquisador para ver uma linha de tempo das atividades para que seja possível reconstituir um ataque.

## Sistemas comprometidos

Neste cenário, uma organização é alertada que um ou mais de seus sistemas foram comprometidos por uma técnica avançada de ciberataque, tal como water hole, phishing, força bruta ou injeção de SQL.

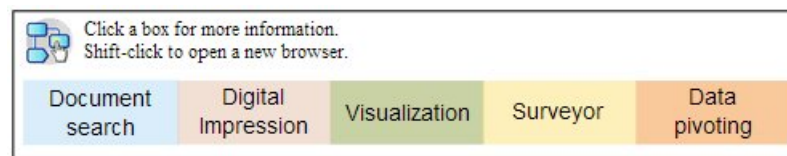
### Objetivos

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Determinar a extensão dos comprometimentos na organização.
- Entender o tipo de risco operacional do comprometimento em cada sistema.
- Descobrir quaisquer ações periféricas que o ataque inicial realizou para contornar as atividades de limpeza e de detecção.

### Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar carga útil maliciosa ou ativo comprometido.
2. Examine o conteúdo suspeito sinalizado pelo produto.
3. Use as Impressões Digitais e as Visualizações para explorar relacionamentos de entidade que resultam de sistemas comprometidos.
4. Use o Pesquisador para ver uma linha de tempo das atividades para que seja possível reconstituir um ataque.
5. Descubra inconsistências ou interações suspeitas nas categorias de dados usando procura de formato livre, transformação de dados e conteúdo suspeito.

## Os dados vazaram para entidades desautorizadas

Neste cenário, uma organização é alertada de que os dados sensíveis vazaram para entidades desautorizadas dentro de sua organização ou para partes externas.

### Objetivo

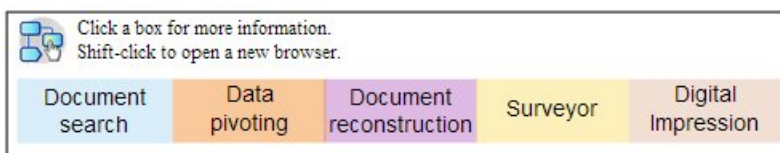
Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Determinar a natureza e a quantidade dos dados que vazaram.
- Entender as técnicas que foram empregadas.
- Descobrir os perpetradores.

- Identificar a origem do vazamento.

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar identificadores dos dados que vazaram.
2. Examine o conteúdo suspeito sinalizado pelo produto.
3. Revise toda a extensão dos dados que vazaram ou em vazamento revisando a reconstrução de dados.
4. Use Impressão digital e visualizações para explorar todos os relacionamentos das entidades envolvidas.
5. Use o Pesquisador para ver uma linha de tempo das atividades para que seja possível reconstituir um ataque.
6. Use procura de formato livre para descobrir as motivações para o vazamento de dados.
7. Use a transformação de dados para localizar as ligações para outros dados que, possivelmente, vazaram.

---

## Investigações de análise de funcionário

Use o QRadar Incident Forensics para detectar conluio, sabotagem e uso indevido de acesso. Identifique o perpetrador, identifique os colaboradores, identifique os sistemas comprometidos e as perdas de dados do documento.

### Uso indevido de acesso

Neste cenário, uma organização é alertada que um ou mais de seus funcionários estão fazendo uso indevido das credenciais ou são usados como um proxy para acessar sistemas e dados sensíveis para atividades desautorizadas.

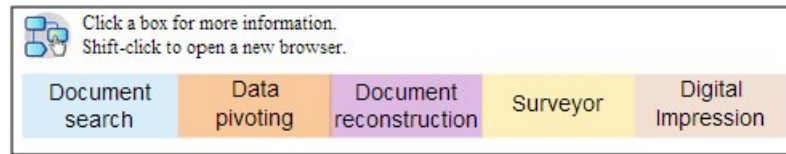
#### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Determinar a identidade do usuário.
- Resolver quem ou o que está empregando a identidade para atividades desautorizadas.
- Entender o objetivo do uso indevido do acesso.
- Avaliar se a entidade possui mais entidades que também possam ser utilizadas de maneira indevida.

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar identidades que estão acessando dados ou sistemas sensíveis.
2. Resolva quais dessas tentativas de acesso são suspeitas examinando o conteúdo suspeito, realizando procuras de formato livre, transformando dados e filtrando conteúdo.
3. Visualize a reconstrução de dados para o conteúdo que está sendo acessado.
4. Reconstitua quaisquer padrões de acesso e avalie a frequência no Pesquisador.
5. Use a Impressão digital para revelar os aliases usados por uma única entidade.

## Conluio

Neste cenário, uma organização é alertada que uma ou mais partes interessadas estão agindo em conluio entre si ou com partes externas em atividades que prejudicam a organização.

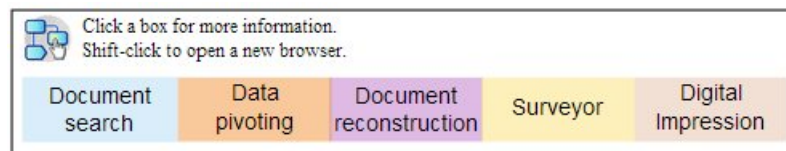
### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Determinar as entidades que agem em conluio.
- Entender a natureza e os padrões das interações entre os colaboradores.
- Descobrir o conteúdo que sustenta o esquema.
- Revelar a duração do esquema para entender o escopo do risco.

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar os identificadores das entidades envolvidas.
2. Examine o conteúdo suspeito sinalizado pelo produto.
3. Use Impressão digital, visualizações e filtros de conteúdo para identificar relacionamentos que possam ser suspeitos.
4. Use o Pesquisador para rastrear as atividades das entidades envolvidas para obter o conteúdo das interações.
5. Descubrir as motivações do conluio ao revisar os documentos reconstruídos.
6. Usa procura de formato livre e transformação de dados para localizar o início das atividades de conluio.

## Sabotagem

Neste cenário, uma organização é alertada de que uma ou mais partes interessadas estão tentando interromper as operações. A parte interessada pode estar sendo usada como um proxy.

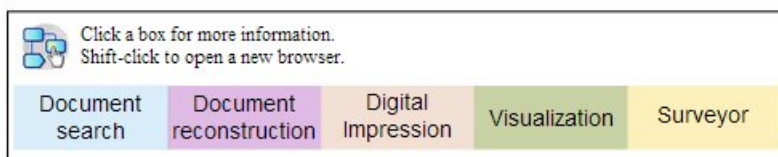
### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Identificar o sabotador.
- Entender as técnicas que foram empregadas pelo sabotador.
- Avaliar o impacto e o escopo da interrupção.
- Identificar as vulnerabilidades que foram exploradas pelo sabotador

### Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar os sintomas da sabotagem.
2. Examine o conteúdo suspeito sinalizado pelo produto.
3. Use a navegação visual, Impressão digital e filtragem de conteúdo para explorar os sintomas e detectar os identificadores do sabotador.
4. Use o Pesquisador para rastrear as atividades do sabotador.
5. Use a reconstrução de dados para descobrir as funções e motivações do sabotador.
6. Use a reconstrução de dados para revisar o conteúdo usado pelo sabotador.
7. Use a procura de formato livre, o Pesquisador e o conteúdo suspeito para exibir os sistemas comprometidos e os procedimentos que permitiram a sabotagem.

---

## Investigações de abuso e fraude

Use o QRadar Incident Forensics para localizar transações desautorizadas, alocação não sancionada de recursos, desvios de protocolo e evasão de controles legais.

### Transações desautorizadas

Neste cenário, uma organização é alertada de que transações desautorizadas estão provocando um impacto financeiro negativo nas operações de negócios.

#### Objetivo

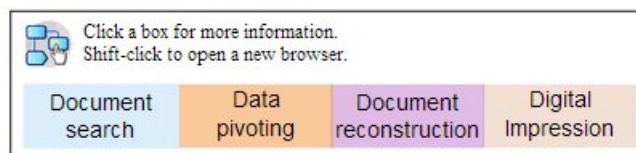
Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Localizar as transações desautorizadas.
- Identificar as entidades que estão envolvidas e são responsáveis pelas transações desautorizadas.
- Entender a frequência e as tendências das transações desautorizadas.

- Avaliar o escopo de risco das transações desautorizadas.

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar quaisquer transações suspeitas ou inconsistentes.
2. Use procura de formato livre e transformação de dados para procurar repetições dessas transações.
3. Use transformações de dados e Impressão digital para descobrir entidades associadas às transações suspeitas.
4. Descubra o conteúdo das transações para revelar o valor quantitativo ao revisar documentos reconstruídos.

## Alocação não sancionada de recursos

Neste cenário, uma organização suspeita de alocação não sancionada de recursos, o que está causando um impacto financeiro negativo nas operações de negócios.

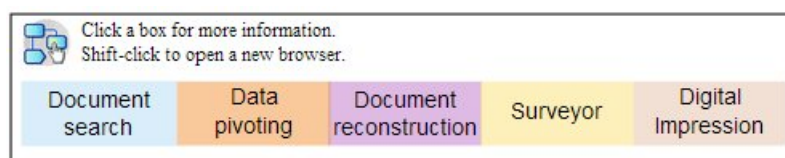
### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Localizar a alocação inadequada dos recursos.
- Identificar as entidades envolvidas e responsáveis pela alocação inadequada de recursos.
- Entender as motivações da alocação não sancionada de recursos.
- Avaliar o tamanho e escopo dos recursos alocados inadequadamente.

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para comunicações associadas aos recursos alocados.
2. Use procura de formato livre, transformação de dados e Impressão digital para localizar identificadores de entidades que estão realizando a alocação não sancionada de recursos.
3. Processe o conteúdo das interações que estão envolvidas para avaliar os motivos ao revisar os documentos reconstruídos e ao usar as visualizações.
4. Use o Pesquisador para reconstituir as atividades de alocação para entender a quantidade de recursos alocados inadequadamente.

## Desvios de protocolo e evasão de controles legais

Neste cenário, uma organização é alertada de que os negócios, os protocolos de TI e os controles legais foram contornados, o que resulta em um impacto financeiro negativo.

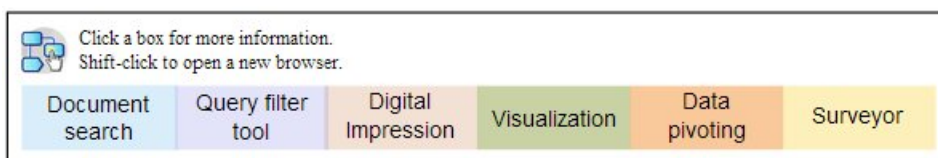
### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Avaliar quais protocolos ou controles legais foram evadidos.
- Identificar as entidades que se encaixam nesse comportamento.
- Entender as motivações dessas entidades.
- Avaliar a difusão desse mau comportamento.

### Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar processos de negócios controlados por protocolos ou controles.
2. Use procura de formato livre, transformação de dados e reconstrução de dados para referências cruzadas com a documentação que descreve os protocolos e os controles legais.
3. Use filtragem de conteúdo, procura de formato livre para descobrir as instâncias específicas em que ocorreram as evasões de protocolos/controles.
4. Use Impressão digital, visualizações, transformação de dados e filtragem de conteúdo para localizar os identificadores de entidade associados.
5. Use o Pesquisador para reconstituir as atividades das entidades para explorar as possíveis motivações.

---

## Investigações de coleção de evidências

Use o QRadar Incident Forensics para acessar o risco de vulnerabilidades na organização, quantificar a confiança na identificação de ameaças ou perpetradores e refinar as práticas de segurança.

### Confiança na identificação de ameaças

Neste cenário, uma organização é alertada sobre uma determinada ameaça, exploração ou vulnerabilidade. Para justificar os esforços de correção que possam priorizar operações normais de negócios, eles desejam quantificar um intervalo de confiança para qualquer risco associado.

### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

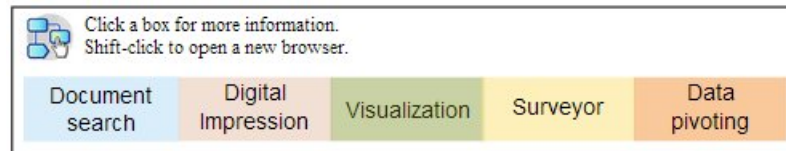
- Validar a possibilidade do risco de segurança.



- Determinar se existe evidência do risco de segurança.
- Avaliar a amplitude e o impacto monetário do risco de segurança.
- Entender a natureza do risco de segurança

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre, conteúdo suspeito e tabela de dados dinâmicos para procurar a ameaça, exploração ou vulnerabilidade usando as possíveis entidades de destino como ponto de início.
2. Use procura de formato livre e transformação de dados para compilar as ocorrências.
3. Use procura de formato livre para documentos de referência cruzada que podem fornecer referência ao impacto.
4. Use a Impressão digital e as visualizações para identificar as entidades afetadas.
5. Use o Pesquisador para analisar as atividades associadas à ameaça ou ao perpetrador.

## Refinando as práticas de segurança

A detecção de comportamentos novos e de risco motiva uma organização a avaliar se as práticas de segurança existentes são suficientes. Nesse cenário, uma organização procura qualificar a eficácia de suas regras de segurança para os riscos enfrentados.

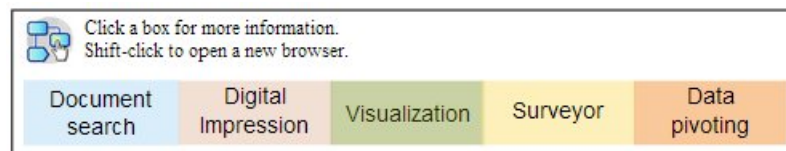
### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Reconhecer comportamentos novos ou de risco.
- Avaliar a eficácia das regras de segurança existentes.
- Entender as falhas na segurança que surgem devido a operações dinâmicas.
- Avaliar a eficácia das práticas de segurança propostas.

## Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use a procura de formato livre para procurar comportamentos novos ou de risco, tais como usuários móveis e serviços baseados em nuvem, usando conhecimento organizacional e de domínio.

2. Examine o conteúdo suspeito e use o Pesquisador para fazer referência cruzada desses comportamentos com regras ou práticas de segurança existentes.
3. Use a procura de formato livre, o Pesquisador, a reconstrução de conteúdo e a visualização para analisar alertas das regras de segurança para frequência de positivos falsos.
4. Use a procura de formato livre, o Pesquisador, a reconstrução de conteúdo, a transformação de dados e a visualização para descobrir negativos falsos que não são detectados pelas regras ou práticas de segurança existentes.

## Avaliações de risco

Neste cenário, um boletim de segurança que esboça determinadas vulnerabilidades, explorações ou comportamentos maliciosos avisa o que uma organização pode fazer para avaliar o risco. A avaliação de risco determina se a organização está suscetível ou se já está comprometida.

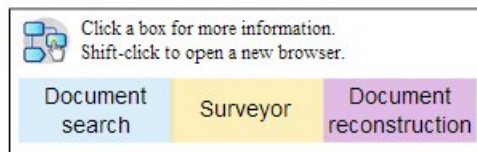
### Objetivo

Para resolver o problema nestas investigações, a organização possui os seguintes objetivos:

- Avaliar a presença de vulnerabilidades identificadas na organização.
- Detectar a presença maliciosa de partes externas.
- Descobrir a evidência de qualquer comprometimento.
- Determinar se a organização é vítima de uma exploração.
- Determinar a identidade do usuário.

### Investigação

Use as ferramentas da guia **Forense** para ajudá-lo na investigação.



1. Use procura de formato livre para procurar por traços ou vulnerabilidades, explorações ou outros comportamentos maliciosos que são especificados no boletim de segurança.
2. Use procura de formato livre para pesquisar referências cruzadas ou outros dados para derivar indicadores.
3. Use o Pesquisador para investigar interações que, possivelmente, exploraram as vulnerabilidades que foram identificadas.
4. Examine o conteúdo suspeito sinalizado pelo produto.
5. Revise o conteúdo que suporta interações de riscos em potencial usando a reconstrução de dados.
6. Use o Pesquisador para reconstituir as atividades de entidades de risco em potencial.

---

## Capítulo 3. Iniciando com investigações forenses

Para iniciar com investigações forenses no IBM Security QRadar Incident Forensics, use o menu **Iniciação Rápida** para navegar e filtrar dados que estão no repositório forense. Essa barra de ativação contém consultas de sumarização predefinidas que você pode usar para iniciar uma procura ou obter relacionamentos para uma entidade.

Para iniciar, siga estas diretrizes:

1. Inicie uma recuperação forense ou procure a partir de uma ofensa na guia **Ofensas**.
  - Se você clicar com o botão direito em um ofensa ou em qualquer endereço IP e executar uma recuperação forense, a investigação recuperará os dados de captura brutos para os intervalos de tempo especificados a partir do dispositivo de captura, extrairá e reconstruirá os documentos e, em seguida, incluirá os resultados no repositório forense.
  - Se você clicar com o botão direito do mouse em uma ofensa ou em qualquer endereço IP e executar uma procura forense, o repositório forense será filtrado e nele será procurado aquele endereço IP. Os resultados serão, então, mostrados na grade principal na guia **Forense**. É possível refinar sua procura construindo consultas.

Quando o QRadar Incident Forensics recebe uma solicitação de procura, ele processa os dados de captura de pacote e os coloca de volta no formato em que foram enviados para o destinatário-alvo. Documentos do Microsoft Word, por exemplo, são recuperados como arquivos do Word. Chamadas de telefone com voz-via-IP são recuperadas como arquivos de áudio. Os arquivos recuperados são então indexados usando conteúdo de metadados e de arquivo para que possam ser procurados.

2. Na guia **Forensics**, clique em **Iniciação Rápida**.

Depois de executar uma recuperação ou procura, em vez de fazer procuras de forma livre e construir suas próprias consultas, você poderá iniciar rapidamente sua investigação usando consultas predefinidas a partir do menu **Iniciação Rápida** na guia **Forensics**. Por exemplo, você pode ver a categoria **Conteúdo Suspeito** e executar uma das consultas como **alerta de entidade**. *Conteúdo suspeito* baseia-se em um conjunto definido de regras no conteúdo que mostra atividade maliciosa. Uma sinalização *alerta de entidade* sinaliza uma possível entidade maliciosa que está envolvida na violação de uma política de segurança.

A categorização de conteúdo e os recursos de filtragem ajudam a reduzir o volume de dados retornados

3. Na **Grade**, selecione documentos a verificar.

O QRadar Incident Forensics retorna resultados da procura priorizados. Da mesma forma que a otimização do mecanismo de procura prioriza sites em uma procura da Internet, as ocorrências mais frequentes aparecem no topo da lista.

Você pode começar a transformar os dados clicando em links e procurando os metadados que estão associados ao documento. Os recursos para transformar dados fornecem várias visualizações de procura e sumarizações de dados.

4. Para investigar relacionamentos entre todas as ações e incidente de segurança, na visualização de documento, selecione um link e clique com o botão direito do mouse em **Obter relacionamentos para**.

Depois de investigar atributos, filtre as informações que você reúne ao conectar entidades.

5. Clique em **Impressões Digitais** para seguir a trilha de identidade e obter um conjunto compilado de associações.

Uma impressão digital é um índice de metadados que pode ajudar a identificar invasores suspeitos ou agentes suspeitos seguindo trilhas de usuários maliciosos. Na construção desses relacionamentos, o QRadar Incident Forensics usa dados de origens de rede como endereços IP, endereços MAC e portas e protocolos TCP. Ele pode localizar informações como IDs de bate-papo e pode ler informações como identificação de autor de processamento de texto ou de aplicativos de planilha. Uma impressão digital pode ajudar a descobrir associações vinculando a identidade da entidade para identificar informações para outros usuários ou entidades.

---

## QRadar Incident Forensicsprocuras e marcadores

Os investigadores usam o IBM Security QRadar Incident Forensics para extrair dados relevantes do tráfego de rede e de documentos.

### Procurando e marcando registros

Para permitir a atividade forense intuitiva, o QRadar Incident Forensics recupera dados do pacote e alimenta outro conteúdo. Essa tecnologia oferece exploração de dados orientada à procura, reconstrução de sessão e inteligência forense para ajudar nas investigações de incidentes de segurança.

Os investigadores concentram suas investigações em ações de alta granularidade em primeiro lugar e, em seguida, fazem ajustes finos nas descobertas para transformá-las em um conjunto de resultados finais relevante. Uma abordagem simples e de alto nível é procurar e marcar muitos registros primeiro. Em seguida, focar nos registros marcados para identificar um conjunto final de registros. Determinar que material é relevante para ajustar as consultas para incluir ou excluir itens. Usar o material para comprovar uma hipótese.

À medida que novas oportunidades são desenvolvidas, é possível acompanhá-las usando outros métodos. É possível usar ferramentas de visualização e de análise para avaliar manual e automaticamente se os resultados são relevantes. É possível também usar consultas variadas para obter um aspecto diferente do mesmo problema.

### Processando resultados marcados

Ao localizar resultados significativos para a investigação, é possível marcar os resultados para uma inspeção mais profunda e uma determinação final. Marque mais do que você pensa que precisa. Se tiver dúvida, marque. Você deseja eliminar o material irrelevante e focar no que acredita ser relevante.

Depois de marcar um conjunto de resultados que você pensa ser relevante, poderá fazer ajustes finos na sua inspeção.

1. Inspeccione cada documento marcado por meio das ferramentas de visualização e de análise.

2. Anexe notas do caso aos documentos e tome as decisões finais sobre cada documento a respeito de sua relevância para o caso.
3. Se um registro não for relevante, remova o marcador.  
No processo de investigação, você identificou o material relevante no repositório e agora tem um conjunto relevante de registros marcados.
4. Imprima, exporte ou processe os registros relevantes.

---

## Procura de documentos e investigação

Os investigadores procuram documentos que são relevantes para uma pista ou hipótese sobre como um incidente de segurança ocorreu.

### Procuras

Em vez de examinar manualmente em meio a massas de documentos, a maioria dos quais não relacionada ao caso, os investigadores usam o repositório forense para extrair documentos que satisfaçam às características de interesse. Por exemplo, um documento que ocorreu dentro de um determinado período de tempo, pertence a um tópico de interesse, ou um documento que é enviado ou recebido por um invasor suspeito.

As procuras podem ser específicas. Por exemplo, "localizar a sequência de caracteres exata "Mission Alpha"" é específica. Como alternativa, as procuras podem ser gerais. Por exemplo, "localizar todos os números de previdência social onde quer que existam no repositório" é mais geral.

A procura pode ser simples e baseada apenas em um critério. Os resultados da procura complexa devem satisfazer a diversas condições. Por exemplo, localizar todos os emails entre dois invasores suspeitos sobre um tópico e excluir emails que contenham anexos, é uma procura complexa. O propósito de uma procura é reduzir de maneira rápida e precisa os registros para um conjunto de trabalhos gerenciáveis. Com um conjunto menor de documentos a serem inspecionados pelo investigador, os documentos possuem maior probabilidade de serem relevantes ao caso.

---


## Recuperação forense

Para recuperar dados brutos de captura de pacote a partir de dispositivos de captura de pacote, execute uma tarefa de recuperação forense em um ou mais endereços IP ou portas.

### Executando uma recuperação em um endereço IP ou porta

Execute uma recuperação forense para recuperar os dados brutos de captura a partir do dispositivo de captura. É possível executar uma recuperação em vários endereços IP ou portas. Se um endereço IP ou porta não for inserido, todo o tráfego UDP e TCP será recuperado. Se vários endereços IP ou portas forem inseridos, você deverá usar uma vírgula para separá-los.

Execute uma recuperação forense clicando com o botão direito em um endereço IP

ou porta no QRadar ou selecionando o ícone **Executar recuperação**  na guia Forense.

**Restrição:** Como regra, é possível inserir cerca de 7 endereços IPv4 e 7 portas ou no máximo 255 caracteres por vez. Os campos **Endereço IP** e **Porta** são combinados com outras frases para criar uma sequência de filtros. A sequência de filtros não pode ter mais de 255 caracteres

## Executar novamente a recuperação

Na guia Forense, use a opção executar novamente a recuperação na grade de resultados para executar uma recuperação criada anteriormente. Por exemplo, se os resultados retornarem dados incompletos, você executará novamente a recuperação forense para incluir endereços IP diferentes ou para mudar o prazo especificado na tarefa de recuperação da execução anterior.

Para executar novamente a tarefa de recuperação forense anterior, clique em **Executar novamente esta recuperação forense**. Ao executar novamente uma tarefa de recuperação, a página Recuperação forense contém valores executados anteriormente. É possível executar uma recuperação idêntica novamente ou mudar os valores gerados automaticamente.

Será possível executar novamente uma recuperação somente quando a tarefa estiver concluída; tiver um status de concluída, cancelada ou com falha.

---

## Casos forenses

Casos são contêineres lógicos para sua coleção de arquivos importados de documento e captura de pacote.

Os casos são criados por administradores ou investigadores que têm privilégios para criar casos. Os administradores criam e designam casos aos investigadores. Os investigadores podem criar um novo caso ao recuperarem dados de captura de pacote de um endereço IP no IBM Security QRadar.

### Tarefas relacionadas:

“Fazendo upload de arquivos pcap e documentos de sistemas externos para casos forenses” na página 17

É possível fazer upload de dados externos em casos específicos.

---

## Coleções

Use coleções para agrupar dados relacionados de uma fonte específica, como um arquivo de dados de captura de pacote (pcap), PDF ou fluxo de rede.

As coleções são usadas para identificar e gerenciar grupos de dados relacionados. É possível excluir rapidamente os dados do grupo na coleção quando a investigação é concluída.

As coleções são criadas por administradores ou investigadores. Os administradores criam as coleções para carregar manualmente os dados para o IBM Security QRadar Incident Forensics. Os administradores também incluem coleções em casos. Os investigadores podem criar uma nova coleção quando iniciam a recuperação de dados de captura de pacote de um endereço IP no IBM Security QRadar.

Considere as regras a seguir para coleções e nomes de coleções:

- Nomes de coleções devem ser exclusivos.
- Casos incluem uma ou mais coleções.
- Coleções podem ser incluídas em vários casos.

- Os resultados da procura retornam dados duplicados quando um investigador possui dois casos com a mesma coleção.
- Se um nome de coleção não for exclusivo quando um novo pcap for transferido por upload, a coleção original será excluída antes que ocorra o upload do novo pcap.

## Fazendo upload de arquivos pcap e documentos de sistemas externos para casos forenses

É possível fazer upload de dados externos em casos específicos.

### Antes de Iniciar

Um administrador deve ativar permissões FTP seguras para o usuário que deseja fazer upload de arquivos externos.

### Sobre Esta Tarefa

O IBM Security QRadar Incident Forensics pode importar dados de um diretório acessível de qualquer diretório acessível que esteja na rede. Os dados podem estar em diversos formatos, incluindo, entre outros, os seguintes formatos:

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

É possível fazer upload de vários arquivos para um caso.

**Restrição:** O nome do caso deve ser exclusivo. Não é possível criar um caso que tenha o mesmo nome de um caso existente.

### Procedimento

1. No cliente FTP, execute as seguintes etapas:
  - a. Assegure que a 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 use o nome de usuário do QRadar Incident Forensics e a senha que foram criados.
2. Conecte-se ao servidor do QRadar Incident Forensics e crie um novo diretório.
3. Para FTP e arquivos pcap de armazenamento, no diretório criado por você para o caso, crie um diretório denominado `singles` e arraste os arquivos pcap para esse diretório.
4. Para FTP e para armazenar outros tipos de arquivos que não sejam arquivos pcap, no diretório criado por você para o caso, crie um diretório denominado `import` e arraste os arquivos para esse diretório.
5. Para reiniciar o servidor FTP, digite o comando a seguir:  
`etc/init.d/vsftpd restart`
6. Para reiniciar o servidor que move os arquivos da área de upload para o diretório do QRadar Incident Forensics, digite o comando a seguir:

## Resultados

É possível ver seu caso em uma das ferramentas na guia **Forense**.

---

## Consultas no repositório forense

Os investigadores especificam as características dos documentos que eles estão interessados em recuperar junto ao banco de dados forense. Várias consultas são usadas para localizar um conjunto de documentos para uma investigação.

Diversas consultas e inspeção manual de um pequeno conjunto de documentos é superior a examinar no repositório inteiro. As ideias para consultas subsequentes e consultas refinadas muitas vezes são geradas durante a inspeção de um documento irrelevante.

Quantidade maior e especificidade dos termos de consulta resultam em conjuntos de resultados de maior relevância. Seu objetivo é definir o máximo que se sabe sobre os resultados que você deseja e ser altamente específico quando possível. Qualquer número de termos de consulta pode ser inserido nos critérios de procura. Separe os termos com um espaço ou com um operador booleano. Os termos que são separados apenas com um espaço sugerem um operador OR lógico booleano. Um operador OR significa que encontrar qualquer um dos termos é igualmente desejável. Os resultados que atendem à maioria dos termos de procura são colocados no início da lista para indicar a intensidade da correspondência com os termos de consulta.

Um critério de procura único também é referido como um termo de consulta. As procuras geralmente envolvem mais de um termo de consulta. O conjunto de termos de consulta para uma única procura também é referido como uma sequência de consulta. Tornar-se especialista em formular consultas requer prática, mas não é difícil. Apenas envolve alguns termos de consulta e aprendizagem de como criar e negar os termos em combinações que dão a você aquilo que você deseja. Como as sequências de consulta são salvas no QRadar Incident Forensics, é possível fazer ajustes finos constantes em suas procuras à medida que você conhece melhor os dados.

### Tarefas relacionadas:

“Visualizando relações e associações” na página 30

Use a janela Visualizar para examinar as relações entre atributos em documentos recuperados. Por exemplo, você pode inspecionar os endereços de email que se comunicaram com um endereço de email específico.

## Termos de consulta de formato livre

Os investigadores procuram correspondências exatas de sequência de caracteres, inserindo os termos de consulta diretamente no campo de critérios de procura na guia **Forense**. É possível usar consultas de palavra única ou várias.

A tabela a seguir descreve o tipo de consultas de procura que podem ser usadas.

*Tabela 1. Tipos de consultas de formato livre*

Tipo de consulta de procura	Descrição	Exemplo
Consulta de palavra única	Procura um termo nos documentos.	puppies



Tabela 1. Tipos de consultas de formato livre (continuação)

Tipo de consulta de procura	Descrição	Exemplo
Consulta única com curinga	Procura uma correspondência para um ou mais caracteres no meio ou no final de um termo de consulta. <b>Restrição:</b> Os caracteres curinga não podem ser usados como o primeiro caractere de uma procura.	te?t test* te*t
Consulta de várias palavras	Especifica que os resultados da procura são retornados na ordem de relevância do termo de consulta. Os documentos que contêm ambos os termos de consulta são listados primeiro, seguido pelos documentos que contêm apenas um dos termos de consulta. Os documentos que contêm apenas um termo de consulta são classificados de acordo com o número de ocorrências do termo de consulta individual.	free puppies
Consulta de várias palavras com aspas duplas	Corresponde à sequência exata. Os documentos que contêm ambas as palavras, mas não nesta ordem e nesta proximidade não são retornados como resultados. Efetivamente, as aspas duplas tornam essas duas palavras em uma única sequência ou termo de consulta. Para o mecanismo de procura, elas não são vistas mais como duas palavras separadas.	"free puppies"
Consulta de várias palavras que usa o operador AND	Especifica que ambos os termos de consulta devem estar presentes no documento para que resultem em uma correspondência. Os termos de consulta podem estar em qualquer ordem e não é necessário que estejam próximos um do outro.	free AND puppies

## Tags de metadados

Entidades comuns são marcadas para permitir que os investigadores recuperem rapidamente conjuntos de resultados exatos de documentos relevantes.

Muitos campos de metadados podem ser usados no índice Incident Forensic, dependendo do tipo de sessão, documento ou protocolo.

Quando você especifica um nome de tag de metadados, ele deve ser exato e existir no repositório forense.

A tabela a seguir lista os tipos de procuras de tag de metadados.

Tabela 2. Procuras de tag de metadados

Tipo de procura de tag de metadados	Formato	Exemplo
Padrão	MetadataTag:<value>	ApplicationProtocol:http
Curinga	MetadataTag:*	CreditCardNumber:*

Tabela 2. Procuras de tag de metadados (continuação)

Tipo de procura de tag de metadados	Formato	Exemplo
Intervalo	MetadataTag:[<start value> TO <end value>	Duration:[30 TO 56]

**Conceitos relacionados:**

“Anotações do documento” na página 23

Os investigadores marcam os documentos e incluem notas neles para controlar as ideias e a lógica sobre documentos em seus casos.

## Combinações booleanas

Vários termos de consulta podem ser utilizados juntos com o uso de operadores booleanos simples para criar sequências de consulta altamente direcionadas. Formadas corretamente, essas sequências de consulta podem retornar resultados que correspondem exatamente ao que um investigador está procurando.

Os operadores booleanos básicos são AND, OR, NOT e (). O operador AND especifica que ambos os termos de consulta devem corresponder no documento. O operador OR especifica que um dos termos de consulta pode ser encontrado em um documento. O operador NOT nega ou remove os resultados, que correspondem aos termos de consulta que são negados. O operador () agrupa os termos de consulta e os valores para aplicar funções a um conjunto, aplicar diversos valores a uma única função ou para esclarecimento de sintaxe.

Os operadores booleanos devem estar em letras maiúsculas.

A tabela a seguir lista os operadores booleanos e um exemplo de sequência de consulta.

Tabela 3. Operadores booleanos para sequências de consulta

Operador booleano	Sequência de consulta de exemplo	Explicação do exemplo
AND	TcpPort:80 AND Protocol:http	Dois termos de consulta são usados para localizar todo o tráfego da web padrão. Se o teste da web ocorresse na Porta 8080, ele não seria uma correspondência, já que ambos os termos de consulta não seriam verdadeiros.
OR	Collection:yahoo* OR Collection:cnn* OR Collection:msn*	Três termos de consulta são usados para limitar os resultados aos resultados das coleções de documentos do Yahoo, da CNN e do MSN no repositório forense.
NOT	ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)	Procura o tráfego com o uso da porta não padrão. O primeiro termo de consulta procura o tráfego HTTP padrão e o segundo elimina todo o tráfego que está usando portas HTTP aceitas.

Tabela 3. Operadores booleanos para sequências de consulta (continuação)

Operador booleano	Sequência de consulta de exemplo	Explicação do exemplo
()	(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)  NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)	Essas consultas usam parênteses efetivamente para alcançar objetivos complexos. Sem os parênteses, elas são mais longas e mais complexas de serem formuladas e depuradas.

## Ferramenta do gerador de consultas

Use a ferramenta do gerador de consultas para criar procuras ou gerenciar procuras salvas.

A ferramenta do gerador de consultas orienta graficamente os investigadores pelo processo de criação de procuras avançadas que usam listas categorizadas de termos de consulta com exemplos.

Tabela 4. Parâmetros para a ferramenta do gerador de consultas

Parâmetro	Descrição
Selecionar categoria	Filtra a lista de tags de metadados disponíveis na lista <b>Selecionar campo</b> .
Selecionar campo	As tags de metadados usadas para identificar as informações no repositório forense.
Exemplo de consulta	Executa a consulta que está no campo <b>Entrada de consulta</b> e relata o número de resultados.
Novo	Substitui uma consulta existente pela nova consulta quando você clica em <b>Inserir consulta</b> .
AND	Combina uma nova consulta com a consulta existente quando você clica em <b>Inserir consulta</b> . Os documentos devem corresponder a ambos os termos da consulta.
OR	Combina a nova consulta com a consulta existente quando você clica em <b>Inserir consulta</b> . Os documentos devem corresponder a um dos termos.

Os investigadores podem salvar e organizar as procuras em pastas no sistema de arquivos, que permite o compartilhamento entre investigadores. Os investigadores usam as descrições ou os nomes das consultas salvas para fins de referência, gerenciamento e entendimento.

A função **Usar consulta** na guia **Consulta** é usada para enviar uma consulta salva para o campo **Entrada de critérios de procura** para execução.

Os investigadores usam a lista de consulta anterior para localizar consultas executadas anteriormente e tornar a executá-las selecionando a consulta desejada e clicando em **Inserir consulta**.

## Ferramenta de filtro de consulta

A ferramenta de filtro de consulta usa os dados ativos para fornecer dicas visuais de construção de filtros persistentes.

O filtro de consulta é um filtro de plano de fundo persistente que reduz o conjunto de documentos ativos que está sendo interrogado pela sequência de consultas. Ao usar um filtro, o conjunto de documentos disponíveis é reduzido sem sobrecarregar a sequência de consultas com termos de consulta estáticos. Conseqüentemente, será obtido mais controle sobre a sequência de consultas.

O filtro de consulta é um bom lugar para iniciar uma investigação por causa de suas listas de tipo de filtro dependentes do caso, atualização dinâmica e resumo de resultados em tempo real. As listas de tipo de filtro são preenchidas com todos os valores encontrados nos casos que estão disponíveis para você. Você pode ver rapidamente quais dados estão contidos nos casos que possui. Selecionar ou limpar os itens da lista de tipos de filtro atualiza automaticamente o resumo de resultados. É possível ver facilmente a eficácia do filtro e o quanto de um conjunto de documentos permanece quando você utiliza o filtro.

Não é aconselhável ajustar o filtro de consulta padrão para consultas que você deseja reutilizar. Para as consultas que deseja manter, crie um novo filtro de consulta. Se você tiver modificado o filtro de consulta padrão, reconfigure-o quando tiver terminado para evitar a exclusão incorreta de documentos de futuras consultas de procura.

### Resultados para filtros ativos

Os investigadores visualizam os resultados de filtros ativos na seção de resumo de resultados na ferramenta de filtro de consulta.

Conforme o filtro é alterado, o resumo é alterado para exibir a contagem total de documentos e a contagem de documentos disponíveis. A contagem total de documentos é o número de documentos disponíveis para o investigador antes de o filtro ser aplicado. A contagem de documentos disponíveis é o número de documentos disponíveis após o filtro ser aplicado. Os investigadores usam essas contagens para avaliar a eficácia do filtro e ajustar adequadamente a maneira de construí-lo.

### Os filtros de procura para a ferramenta de filtro de consulta

Os investigadores filtram os dados de seus casos designados. Os dados são separados em grupos por tipo de filtro, por exemplo, endereço IP ou endereço MAC.

Usando a alternância de ação lógica, o investigador pode incluir ou excluir itens selecionados na lista.

Cada grupo de filtros de procura tem uma alternância de ação lógica que pode ser configurada para incluir ou excluir os itens que são selecionados na lista. Quando configurado para incluir, os itens na lista são associados a um AND lógico, o que significa que cada documento disponível contém todos os itens selecionados. Quando configurado para excluir, um OR lógico é usado, significando que cada documento disponível não contém nenhum dos itens selecionados.

Os investigadores podem usar o grupo **UserQuery** para formular suas próprias sequências de consultas a serem incluídas no filtro.

## Limitando o número de documentos retornados em uma procura

Você pode incluir filtros em suas consultas do IBM Security QRadar Incident Forensics para limitar o número ou o tipo de documentos que vê na página de resultados da procura.

### Procedimento

1. Na guia **Forensics**, clique no ícone **Filtros de Consulta**.  
Os dados são separados em grupos por tipo de filtro.
2. Na janela **Filtros de Procura**, para cada tipo de filtro, escolha se irá incluir os documentos nos resultados da procura clicando em **Incluir** ou **Excluir**.
3. Para localizar um item em um grupo de filtros, siga estas etapas:
  - a. Na coluna **Tipo de Filtro**, expanda um grupo de filtros.
  - b. Na janela **Procurar**, selecione os critérios e clique em **Localizar**.  
Ao procurar um registro no grupo de filtros **Categoria da Web**, todos os campos de categoria correspondentes são exibidos. Por exemplo, quando você procura **Categoria da Web igual bate-papo, Bate-papo** e categorias relacionadas, como **Sistema de Mensagens Instantâneas, Correio da Web/Sistema de Mensagens Unificado, Mecanismos de Procura/Catálogos da Web/Portais** e **Nuvem** são exibidas.

---

## Anotações do documento

Os investigadores marcam os documentos e incluem notas neles para controlar as ideias e a lógica sobre documentos em seus casos.

Os documentos podem ser marcados na tela de resultados principal e na ferramenta pesquisadora, na grade cronológica que exibe a sequência de documentos que são trocados durante uma interação. Como as consultas e investigações podem ser complexas, os investigadores marcam todos os registros, incluindo documentos de menor interesse. O uso de um marcador elimina a necessidade de recriar consultas complexas e linhas de investigação. As anotações podem ser criadas após um registro ser marcado.

Durante uma investigação, há momentos em que você deseja seguir dois ou mais caminhos. Use a função de navegador para duplicar a guia em que você está no momento. A duplicação da guia ajuda a evitar ter de voltar e seguir os caminhos adicionais ou a lembrar como chegar ao ponto de ramificação. É possível duplicar a guia atual quantas vezes for necessário. Siga cada caminho diferente em uma guia diferente e marque os documentos relevantes ao longo do caminho. É possível incluir uma nota que designe o caminho que levou a cada documento marcado.

As notas representam uma maneira de gravar pensamentos enquanto você investiga. Elas podem ser removidas apenas por um administrador. Elas são marcadas com o ID do usuário do investigador e o registro de data e hora em que foi inserida. Quando os documentos são exportados, as notas são geradas com o documento reconstruído e seus atributos.

### Conceitos relacionados:

“Tags de metadados” na página 19

Entidades comuns são marcadas para permitir que os investigadores recuperem rapidamente conjuntos de resultados exatos de documentos relevantes.



---

## Capítulo 4. Ferramentas de investigação

Os investigadores usam o Pesquisador, as Impressões digitais e as ferramentas de Exportar e Visualizar para gerenciar dados de maneiras diferentes.

A página de resultados da procura é a página padrão na guia **Forense**. Os resultados da procura estão disponíveis no guia **Grade**. Os investigadores usam os resultados da procura na grade para procurar rapidamente e acessar documentos. Na guia **Grade**, use as ferramentas Pesquisador, Impressões digitais, Exportar e Visualizar para avançar na investigação.

### Indicador de linha

O indicador de linha fornece um identificador exclusivo para cada documento que é retornado em um conjunto de resultados. Use o indicador de linha para enviar um documento e todos os documentos relacionados necessários para a ferramenta de Visualização reconstruída.

### Ordem da linha

É possível classificar as linhas que são exibidas na grade. Como o número total de resultados pode ser maior que o número de resultados exibido na grade, não é possível classificar todo o conjunto de resultados.

### Indicador de documentos visualizados

O indicador de documentos visualizados é um pequeno círculo que alterna entre vermelho e verde para indicar se um investigador visualizou um documento.

### Seleção de documento

Os investigadores usam o seletor de documentos exibidos para escolher o número de documentos que são exibidos na grade de resultados. É possível usar **SELECIONAR TODOS** para enviar os documentos para uma função subsequente e é possível enviar vários documentos para processamento ou visualização. Ao selecionar os documentos usando o seletor de documentos exibidos, todos os documentos são selecionados e não apenas os documentos que estão presentes na grade.

---

## Visualização de rede e documento

Os investigadores usam a ferramenta de visualização para detectar padrões, entender onde ocorre maior tráfego de rede e congestionamento de documentos durante um período especificado e visualizar conteúdo suspeito. Por exemplo, os investigadores podem visualizar padrões de tráfego de rede, como servidores que são acessados depois do expediente da empresa.

A ferramenta VGrid está dividido em blocos de tempo. Conteúdo suspeito, como tráfego de rede ou documentos, é representado por um retângulo vermelho na grade. Um retângulo verde representa conteúdo regular. Um bloco colorido brilhante indica mais tráfego. Quanto maior a saturação da cor, maior a quantidade de tráfego. O brilho de um bloco de tempo é relativo aos dados atuais exibidos na

ferramenta VGrid. Por exemplo, um bloco de tempo colorido brilhante fica mais escuro à medida que diferentes blocos de tempo são carregados com mais dados.

Os investigadores podem visualizar os tipos de tráfego de rede e o número de documentos para cada bloco de tempo que tem o conteúdo.

## Inspecionando tráfego de rede e documentos em um bloco de tempo

Os investigadores podem desejar examinar documentos individuais, websites navegados ou emails enviados dentro de um bloco de tempo específico.

### Procedimento

1. Na guia **Forensics**, selecione a guia **VGrid**.
2. Use uma das opções a seguir para inspecionar conteúdo em um bloco de tempo:
  - Para visualizar tipos de tráfego de rede e número de documentos, passe o mouse sobre o bloco de tempo.
  - Para procurar conteúdo no bloco de tempo, selecione um ou mais blocos de tempo. Clique com o botão direito e selecione **Procurar blocos de tempo selecionados**.
  - Para visualizar a sequência de eventos, selecione o bloco de tempo e, em seguida, selecione **Pesquisador**.
  - Para visualizar o conteúdo, selecione um bloco de tempo e, em seguida, selecione **Visualizar**.

---

## Ferramenta pesquisadora

Use a ferramenta Pesquisadora para visualizar uma sequência de eventos em um incidente de segurança conforme eles ocorreram.

Essa ferramenta é usada pelos investigadores para ver o que invasores suspeitos visualizaram e suas ações. A ferramenta pesquisadora representa a sequência cronológica de atividades em um incidente de segurança em um visualizador parecido com filme. Como o Pesquisador é orientado a tempo, a seleção de um único documento na tela de resultados não mostra muito. Se poucos documentos forem selecionados, expanda o raio de tempo em torno dos documentos selecionados na guia **Atributos**. Expandir o tempo clicando no link **Mostrar contexto**.

Use a guia **Atributos** para exibir informações de certificado e metadados. Você clica com o botão direito em um endereço IP ou porta para filtrar por eventos ou clica com o botão direito em um endereço MAC para filtrar por eventos e ativos.

É possível filtrar suas consultas por horário do caso, protocolo e endereço IP.

Você usa a guia **Lista** para ver uma lista cronológica de documentos que foram enviados e recebidos.

Números de ID de documento verdes indicam que um documento foi revisado por um investigador, enquanto documentos com números de ID vermelhos não foram revisados.



## Visualização de documento reconstruída

A guia **Visualizar** mostra uma visualização reconstruída do documento que está selecionada no lado esquerdo da tela na visualização Lista.

Essa poderosa combinação de sequenciamento à esquerda e reconstrução à direita torna possível ver o que os invasores suspeitos viram ou fizeram na rede. Além dos documentos visíveis que percorreram a rede, o Pesquisador também mostra os bastidores de handshakes entre computadores e as trocas de certificados que ocorreram.

### Tarefas relacionadas:

Capítulo 5, “Investigando o tráfego de rede para um endereço IP”, na página 39  
Para obter visibilidade do conteúdo relevante nas conversas que ocorreram durante um incidente de segurança, é possível recuperar e reconstruir o tráfego de rede que está associado a um endereço IP. Também é possível procurar através dos casos existentes relacionados com um endereço IP.

## Conteúdo do documento extraído

A guia **Texto** mostra o conteúdo que é extraído do documento. O conteúdo do documento não é formatado.

Esse texto é do indexador do mecanismo de procura.

---

## Exportação de documentos no QRadar Incident Forensics

No IBM Security QRadar Incident Forensics, todos os documentos exportados, exceto os documentos pcap exportados, incluem o documento reconstruído, o texto bruto do documento, os atributos e as notas anexadas ao documento.

Quando os documentos pcap são exportados, nenhuma reconstrução é feita. Por exemplo, ao exportar uma página da web, tudo que o navegador transferiu por download durante a conexão principal é transferido por download. Normalmente, a maioria do conteúdo de texto é transferida por download durante a conexão principal. No entanto, a maioria dos navegadores modernos usam conexões múltiplas para fazer o download de mais itens, como folhas de estilo e imagens, que não fazem parte da exportação. Ao exportar, o conteúdo pcap a princípio não é reconstruído.

Outro exemplo, são os protocolos complexos, como FTP e VOIP, onde há um comando principal e uma conexão de controle e uma conexão de dados separada. Se você exportar os arquivos pcap para uma chamada VOIP ou um download por FTP, os dados não serão reconstruídos e você poderá obter resultados inesperados.

## Exportando documentos como arquivos pcap

É possível exportar documentos como arquivos pcap a partir de vários dispositivos IBM Security QRadar Incident Forensics e IBM Security QRadar Packet Capture.

**Restrição:** O conteúdo exportado para o formato pcap não é reconstruído.

### Procedimento

1. Para exportar dados dos documentos selecionados, na grade de recuperação na guia **Forensics**, selecione as caixas de seleção próximas aos documentos e, em seguida, clique em **Exportar**.

É possível selecionar no máximo 25 documentos para exportar para o formato pcap.

2. A partir da lista **Selecionar tipo de exportação**, clique em **PCAP**.
3. Após todos os documentos de um host QRadar Incident Forensics serem exportados, será possível clicar em **Download**.
4. Se a exportação de um documento falhar, exporte o documento novamente clicando na mensagem **FAIL**.

## Resultados

Se um único arquivo pcap for exportado, o arquivo pcap será transferido por download. Se mais que um arquivo pcap for exportado, os arquivos pcap serão montados em um arquivo compactado (.zip) e o arquivo compactado será transferido por download.

Cada documento armazena o endereço IP do host QRadar Incident Forensics e o endereço IP do dispositivo QRadar Packet Capture do qual o documento é proveniente originalmente. Se você remover um host QRadar Incident Forensics ou mover um QRadar Packet Capture, talvez não consiga fazer uma exportação.

---

## Impressão digital

Uma *impressão digital* é um conjunto compilado de associações e relacionamentos que identificam um trilha de identidade. Os relacionamentos de rede de reconstrução de impressão digital ajudam a revelar a identidade de uma entidade invasora, como ela se comunica e com quem se comunica.

Use a ferramenta de Impressão digital para responder rapidamente estas importantes perguntas:

- O que se sabe sobre esse invasor suspeito, computador ou endereço IP?
- Com quem esse invasor suspeito conversou?
- Quem está em sua rede de contatos?
- O invasor suspeito está tentando disfarçar sua identidade?

## Identificadores online

Identificadores online, como endereços de email, endereços Skype, endereços MAC, IDs de bate-papo, IDs de mídia social ou IDs do Twitter são utilizados para identificar entidades ou pessoas. Entidades ou pessoas conhecidas que são localizadas no tráfego de rede e nos documentos são identificadas automaticamente.

O IBM Security QRadar Incident Forensics correlaciona os identificadores de tag que interagem entre si para produzir uma impressão digital.

Os relacionamentos da coleção em relatórios de impressão digital representam uma presença eletrônica coletada continuamente que está associada a um invasor, a uma entidade de rede relacionada ou a qualquer termo de metadados de impressão digital. Os investigadores podem clicar em qualquer identificador de impressão digital de tag que está associado a um documento. O relatório de impressão digital resultante é listado em formato tabular e organizado por tipo de identificador.

## Obtendo informações de relacionamento

Um relatório de impressão digital mostra as interações entre um *identificador central* e todos os outros identificadores. Um *identificador central* é o identificador online que é a fonte de interesse em um incidente de segurança.

O identificador principal em muitas categorias geralmente é a identidade do identificador central nesse tipo de identificador ou categoria. Por exemplo, se o identificador for um endereço MAC, o endereço de email que tiver a maioria das interações provavelmente pertencerá ao invasor suspeito que possui o computador. No entanto, se os endereços IP forem designados dinamicamente, você também deverá investigar os endereços IP designados durante um intervalo de tempo.

As correlações entre outras categorias e o identificador central normalmente são menos fortes. Antes de decidir agir com base na impressão digital, valide os dados com fontes independentes. Use a ferramenta de Impressão digital para expandir o raio de uma investigação até os invasores e entidades mais suspeitos.

## Investigando relacionamentos para controlar trilhas de identidade

A impressão digital reconstrói relacionamentos de rede para ajudar a identificar uma entidade de ataque e outras entidades com as quais ela se comunica.

A ferramenta de Impressões digitais mostra a distribuição de frequência de eventos correlatos. A ferramenta mostra relacionamentos entre entidades e conta as relações. Quanto mais alta a contagem, mais forte é o relacionamento. Por exemplo, se você visualizar os relacionamentos entre um endereço de email e outras entidades, é possível ver quem está se comunicando com quem. É possível visualizar os endereços IP que estão associados ao endereço email, os endereços IP visitados pelo suspeito e os outros nomes que estão associados ao endereço de email.

Em implementações distribuídas, você tem a opção de ver os relacionamentos de um nó em sua organização.

### Procedimento

1. Selecione um resultado na lista de documentos na grade de recuperação e clique na guia **Impressão digital**.

2. Na lista, selecione um item que você deseja explorar.

Por padrão, o relatório de impressão digital é listado em formato tabular, que é organizado por tipo de identificador. Todos os identificadores que interagem com o identificador central são exibidos. Os identificadores da interação são organizados por tipo de identificador e classificados por frequência de interação.

3. Se você vir um identificador de interesse, selecione-o.

Identificadores são hyperlinks e você pode usá-los como identificador central de outro relatório. Outra guia é criada e o novo identificador central é exibido. Você pode ver com quem um determinado invasor suspeito interage e, em seguida, com quem as interações do suspeito interagem. É possível expandir o raio de uma investigação para mais invasores e entidades suspeitos com os quais eles interagem.

4. Para examinar outro host, selecione o endereço IP na lista **Selecionar host remoto**.

Em instalações distribuídas, você pode escolher o host QRadar Incident Forensics e, em seguida, visualizar a impressão digital. A visualização padrão é o host primário, mas você pode selecionar qualquer host secundário que esteja associado ao host QRadar Incident Forensics.

5. Para ver uma visualização de associações e relacionamentos das interações do identificador central com outros identificadores, clique na guia **Visualizar dados**.

---

## Ferramenta Visualizar

É possível explorar associações e relacionamentos visualmente em vários atributos e categorias de dados.

Use a janela Visualizar para examinar um mapa relacional de metadados de uma, duas ou uma grande seleção de documentos. Quando seleções grandes de documentos são usadas, o investigador obtém uma visão abrangente dos relacionamentos de metadados e da frequência relativa. Os investigadores podem então seguir esses caminhos para avançar na investigação de um incidente de proteção.

A visualização dos documentos selecionados pode ser facilmente reconstruída com uma relação diferente, alterando uma ou ambas as relações.

A visualização mostra cada relação que está contida nos documentos selecionados e mostra a frequência da relação. Cada nó representa uma parte distinta de metadados que está sendo relacionada dos documentos selecionados. O tamanho transmite a frequência relativa quando comparado com outros nós. Links mostram as conexões que são encontradas entre as partes distintas de metadados e transmitem a frequência por meio do tamanho. Os investigadores podem usar os nós com o objetivo de identificar possíveis vias para investigação adicional.

### Visualizando relações e associações

Use a janela Visualizar para examinar as relações entre atributos em documentos recuperados. Por exemplo, você pode inspecionar os endereços de email que se comunicaram com um endereço de email específico.

#### Procedimento

1. Na grade de recuperação, clique nas caixas de seleção dos documentos que você deseja investigar e clique em **Visualizar**.
2. Selecione o layout, o número de documentos a serem exibidos e as relações entre os atributos que você deseja ver e clique em atualizar.
3. Utilize os controles de zoom para ver mais ou menos detalhes da imagem.
4. Para executar uma nova procura ou modificar o filtro ativo, clique com o botão direito em um nó.

No menu sensível ao contexto, você pode trazer essa parte de metadados de volta para executar uma nova procura. Também é possível modificar o filtro ativo para incluir ou excluir os metadados.

**Restrição:** É possível visualizar até 9999 documentos por vez em uma janela Visualizar.

---

## **Análise de artefato para conteúdo suspeito ou malicioso**

Como um analista de segurança, será possível verificar as ameaças que evitaram a detecção, analisando artefatos reconstruídos, como arquivos e imagens. Para entender as conexões entre colaboradores e artefatos, também é possível investigar os links para e a partir desses arquivos e imagens.

### **Exemplo - usando a análise de artefato para localizar a origem de um ataque (paciente zero)**

John é um analista de segurança nas indústrias Replay. Vários sistemas são infectados apesar de todas as medidas de segurança no lugar. Após identificar e colocar esses sistemas em quarentena, John precisará descobrir como esses sistemas se infectaram e se outros ativos estão comprometidos da mesma forma.

### **Recuperação de pacote de um endereço IP**

Com início nos endereços IP e o prazo aproximado envolvido, John pode usar o QRadar Incident Forensics para recuperar os dados relevantes do pacote.

## Forensics Recovery

**IP Address:**   
**Port:**   
**Case:** case1   
**Collection:**   
**Start Date:** 1/26/2017  2:23 PM   
**End Date:** 1/26/2017  3:23 PM   
**Tags:**

**Advanced Options**

**Enable Custom BPF**

**Enable Custom Capture Devices**

Figura 1. Recuperação de um endereço IP

## Análise de arquivo

Verificando o conteúdo executável, John inicia, usando os recursos de análise do arquivo incluídos no QRadar Incident Forensics. Agora ele pode ver uma lista de todos os arquivos, quantas vezes eles foram enviados, se eles continham scripts ou arquivos integrados e seus escores de entropia. John vê rapidamente um arquivo de imagem que o QRadar Incident Forensics sinalizou como conteúdo suspeito e como tendo um script integrado.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa99e 4.93731	
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dc2e494f0d68b9d1 5.74523	
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd95f 5.38451	

Figura 2. Atributos de análise do arquivo

O *score de entropia do arquivo*, que mede a aleatoriedade dos dados e é usado para localizar malware criptografado, e a distribuição de entropia também mostra

claramente que uma parte do arquivo não é o que ele deveria ser. Uma análise adicional prova que este arquivo contém uma nova forma de malware que passou pelas medidas de segurança existentes sem ser detectado e foi responsável pelos sistemas infectados.

No seguinte diagrama, a entropia é usada como um indicador da variabilidade de bits por byte. Como cada caractere em uma unidade de dados consiste em 1 byte, o valor de entropia indicará a variação de caracteres e a compressibilidade da unidade de dados. As variações nos valores de entropia no arquivo podem indicar que o conteúdo suspeito está oculto nos arquivos. Por exemplo, os valores altos de entropia podem ser uma indicação de que os dados são armazenados criptografados e compactados e os valores inferiores podem indicar que, em tempo de execução, a carga útil é descriptografada e armazenada em diferentes seções.

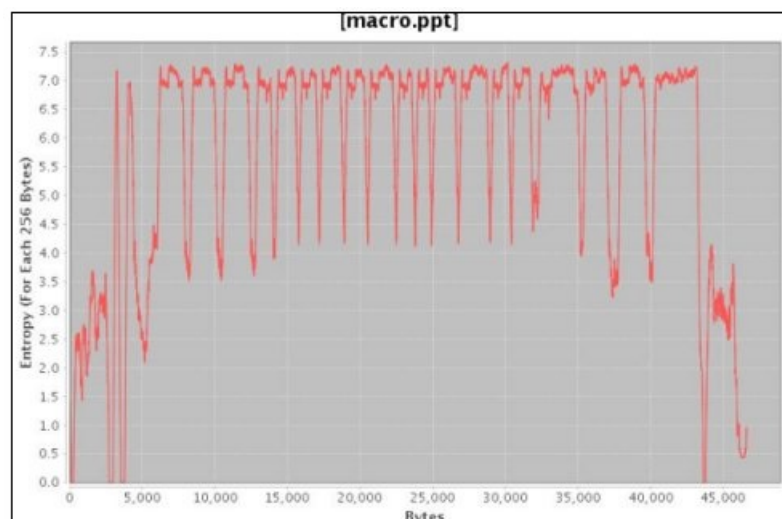


Figura 3. Exemplo de gráfico de entropia do arquivo que mostra scripts integrados

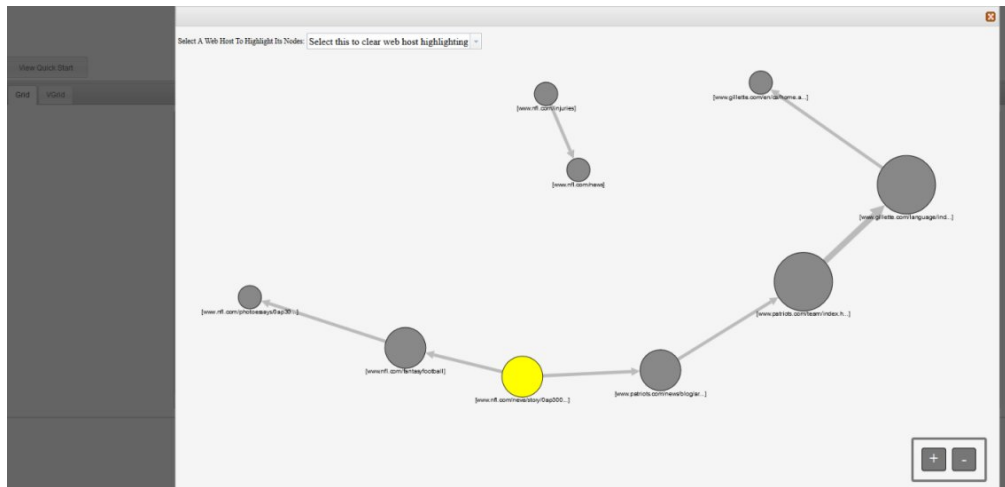
John agora precisa entender de onde veio esse arquivo e quem mais pode tê-lo. John usa o QRadar Incident Forensics para localizar rapidamente o servidor da web que forneceu o arquivo de imagem infectado. A página da web em questão é popular por transmitir as notícias mais atuais do time NFL favorito de todos e está comprometida. Mesmo que o site contivesse muitas imagens, John localizou apenas uma imagem anteriormente usando a análise do arquivo que continha o malware integrado.

### **Análise de link para visualizar a comunicação do website**

Para determinar como outros sistemas podem ser afetados, John usa a análise de link para visualizar rapidamente todos os websites que foram visualizados e apesar da grande quantidade de tráfego nos websites para as empresas as quais a Replay fez negócio, um pequeno subconjunto de acessos podem claramente ser vistos no host infectado da web. John analisa estes links para ver quais outros servidores em sua rede foram usados para acessar esse host da web.

Em sua investigação, John usa os nós no gráfico, que representam as páginas da web e as setas entre os nós representam as relações ou as transações entre as páginas da web para avaliar rapidamente os padrões de tráfego e ver como os documentos foram percorridos. Quanto maior o nó, mais links o documento terá

em seu caminho e quanto maior a seta de link, mais vezes o link foi usado.



Sendo um site popular de notícias da NFL, não foi surpreendente ver que vários outros servidores estavam em contato com esse host da web e foram afetados potencialmente.

### Análise de imagem

Para limitar quais servidores transferiram por download o arquivo de imagem malicioso, John alterna para a análise de imagem e pode ver rapidamente todos os arquivos de imagem que foram enviados ou recebidos.

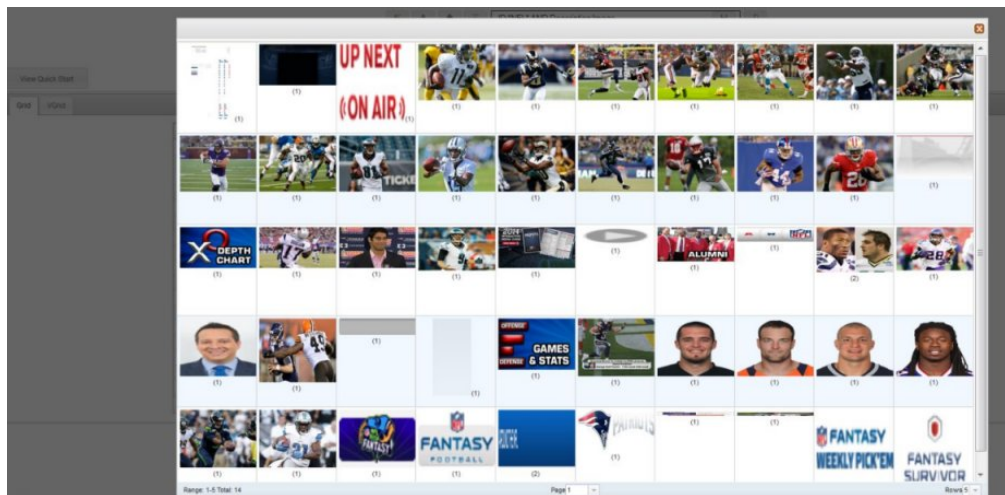


Figura 4. Exemplo de análise de imagem e distribuição de imagem

John confirma rapidamente que todos os seus servidores infectados e 2 servidores que ele desconhecia acessaram o arquivo de imagem comprometido.

John também determina que vários dos outros servidores que acessaram o mesmo website não fizeram o download do arquivo infectado. John agora tem as informações que ele precisa para colocar em quarentena esses 2 servidores extras e criar um novo hash de arquivo do arquivo infectado que as Indústrias Replay podem fazer o upload e compartilhar com os outros no IBM X-Force Exchange.



## Analisando arquivos para conteúdo integrado e atividade maliciosa

Para investigar ameaças ocultas em arquivos, é possível ver os valores de entropia do arquivo, fazer o download dos scripts ou arquivos integrados para análise posterior e visualizar o documento e seus atributos.

Como os intrusos podem ofuscar o conteúdo dos arquivos binários nos arquivos de contêiner, será possível usar a análise de arquivo em IBM Security QRadar Incident Forensics para examinar se os arquivos contêm scripts integrados ou outro conteúdo binário.

*Entropia de arquivo* mede a aleatoriedade dos dados em um arquivo e é usada para determinar se um arquivo contém dados ocultos ou scripts suspeitos. A escala de aleatoriedade é de 0, não aleatória, a 8, totalmente aleatória, como um arquivo criptografado. Quanto mais uma unidade pode ser compactada, menor o valor de entropia; quanto menos uma unidade pode ser compactada, maior o valor da entropia.

No seguinte diagrama, a entropia é usada como um indicador da variabilidade de bits por byte. Como cada caractere em uma unidade de dados consiste em 1 byte, o valor de entropia indicará a variação de caracteres e a compressibilidade da unidade de dados. As variações nos valores de entropia no arquivo podem indicar que o conteúdo suspeito está oculto nos arquivos. Por exemplo, os valores altos de entropia podem ser uma indicação de que os dados são armazenados criptografados e compactados e os valores inferiores podem indicar que, em tempo de execução, a carga útil é descriptografada e armazenada em diferentes seções.

### Procedimento

1. Na guia **Forensics**, selecione um ou mais arquivos recuperados na visualização **Grade**.
2. No menu de ferramentas investigativas na parte superior da grade, clique em **Análise do arquivo**.  
Nos resultados, cada linha da grade contém dados de análise para um documento, por exemplo, o nome do arquivo, a descrição, se o conteúdo suspeito é detectado e os valores de entropia.
3. Para classificar os arquivos por um atributo específico, como entropia, clique no título da coluna associada.
4. Na lista de arquivos, clique com botão direito em um arquivo para obter uma investigação adicional
  - Para revisar o documento e seus atributos, clique em **Exibir documento**.
  - Para revisar um gráfico de entropia e verificar se um script ou arquivo integrado pode conter malware, clique em **Exibir entropia**.

É possível usar valores de entropia como uma indicação de que o arquivo pode ter um conteúdo malicioso. Por exemplo, arquivos de texto ASCII são de forma típica altamente compactáveis e têm valores baixos de entropia. Os dados criptografados geralmente não são compactáveis e geralmente têm um valor alto de entropia. Malware está frequentemente compactado e oculto em arquivos e imagens.

- Para fazer o download de arquivos integrados, clique em **Extrair arquivos integrados** e selecione os arquivos para o download.

Esta opção está disponível somente para documentos com os scripts ou arquivos integrados. Os arquivos são transferidos por download para o local

de download do navegador da web. Cuidado para não abrir scripts potencialmente prejudiciais em um ambiente desprotegido.

## Analizando as imagens para ameaças ocultas ou atividade suspeita

As imagens visualizadas são classificadas por tamanho e relevância com um número de frequência entre parênteses. Esta análise poderá ser útil, quando um empregado que estiver usando os recursos da empresa olhar para imagens inapropriadas, restritas ou proibidas. Por exemplo, as imagens podem estar relacionadas a aviões, certos edifícios ou locais que são alvos de violações de segurança.

Com a análise de imagem, é possível visualizar as imagens mais relevantes de um ou mais documentos em um ou mais arquivos de capturas de pacotes em uma exibição em vez de ser forçado a abrir cada documento e visualizar as imagens.

### Procedimento

1. Na guia **Forensics**, na visualização **Grade**, selecione um ou mais documentos que contenham imagens na descrição.
2. No menu de ferramentas investigativas na parte superior da grade, clique em **Análise de imagem**.

Nos resultados, as versões miniaturas de todas as imagens contidas nos documentos são exibidas em ordem de relevância. O número entre parênteses ao lado da imagem indica o número de instâncias da imagem no documento. Se você colocar o cursor sobre uma imagem miniatura, ela ficará maior.

3. Clique com o botão direito em uma imagem para obter uma investigação adicional

- Para revisar a imagem e seus atributos, clique em **Exibir documento**.
- Para revisar um gráfico de entropia e verificar se uma imagem pode conter malware, clique em **Exibir entropia**.

É possível usar valores de entropia como uma indicação de que o arquivo pode ter um conteúdo malicioso. Por exemplo, arquivos de imagem de bitmap e arquivos de texto ASCII são de forma típica altamente compactáveis e têm valores baixos de entropia. Os dados criptografados geralmente não são compactáveis e geralmente têm um valor alto de entropia. Malware está frequentemente compactado e oculto em arquivos e imagens.

## Analizando links com conexões e relações

Na análise de link, os links mostram o compartilhamento entre os websites que foram visualizados. Durante as investigações de incidentes de segurança, será possível ver rapidamente onde há sobreposição e como as pessoas estão se comunicando.

Por exemplo, se você acha que esse grupo de perpetradores está colaborando, mas não tem certeza de como, será possível olhar para um conjunto de documentos de um número de usuários e usar a análise de link para mostrar as páginas comuns da web. É possível investigar websites específicos.

### Procedimento

1. Na guia **Forensics**, selecione um ou mais páginas da web na visualização **Grade**.

2. No menu de ferramentas investigativas na parte superior da grade, clique em **Análise de link**.

Se houver uma relação entre os websites, um gráfico de cytoscape mostrará as páginas da web como círculos (nós) e links para e a partir das páginas da web como setas. Quanto maior o nó, mais links o documento terá em seu caminho e quanto maior a seta de link, mais vezes o link foi usado. Os nós selecionados são amarelos.

3. Para investigar a comunicação de um host da web específico, na lista **Selecionar host da web**, selecione o host da web.

Os nós que representam as páginas da web do host da web selecionado são destacados como círculos cinza escuro.

4. Para aumentar ou diminuir o tamanho dos círculos (nós) e as setas, use os controles para aumentar o zoom (+) ou diminuir o zoom (-).

Também é possível rolar acima ou para baixo na roda do mouse para aumentar ou diminuir o tamanho dos nós e das setas.

5. Para mover um ou mais nós, clique e arraste os nós.

É possível mover o gráfico inteiro clicando em qualquer lugar no plano de fundo e, em seguida, segurando e arrastando.

---

## Executando uma recuperação a partir de uma página Atributos do documento

Quando visualizar a guia **Atributos** de um documento, será possível executar uma recuperação de um endereço IP ou porta.

### Procedimento

1. A partir da página Procura na guia **Forense**, execute uma procura.
2. Na lista de documentos retornados, clique em um para abri-lo.
3. Clique na guia **Atributos**.
4. Clique em um endereço IP ou porta.
5. No menu, clique em **Executar uma recuperação de**.



---

## Capítulo 5. Investigando o tráfego de rede para um endereço IP

Para obter visibilidade do conteúdo relevante nas conversas que ocorreram durante um incidente de segurança, é possível recuperar e reconstruir o tráfego de rede que está associado a um endereço IP. Também é possível procurar através dos casos existentes relacionados com um endereço IP.

Quando o tráfego de rede é reconstruído a partir de um endereço IP, um incidente é criado. Os investigadores podem visualizar uma sequência de eventos do incidente de segurança ou visualizar os documentos no incidente.

O IBM Security QRadar Incident Forensics indexa todos os dados de rede disponíveis, dados do arquivo, metadados e caracteres de texto que estão em cada arquivo recuperado.

Em implementações distribuídas, diversos dispositivos de captura e hosts QRadar Incident Forensics capturam e processam dados. Você pode visualizar resultados agregados de recuperação de incidente ou resultados por host e dispositivo de captura.

### Procedimento

1. Para criar um caso e obter dados dos dispositivos de captura de pacote, no QRadar, clique com o botão direito em um endereço IP e, em seguida, selecione

**Executar recuperação forense** ou clique no ícone de recuperação forense  .


- a. Configure os parâmetros de recuperação forense, usando as informações a seguir:

*Tabela 5. Parâmetros para recuperação forense*

Parâmetro	Descrição
Endereços IP	Use o comando para separar vários endereços IP. Se nenhum endereço IP ou porta for inserido, o TCP ou UDP padrão será usado.
SOAP	Use vírgulas para separar várias portas.
Caso	O nome do caso deve ser exclusivo.
Coleção	Os dados recuperados são agrupados em uma coleção e associados ao caso. O nome da coleção deve ser exclusivo. Se o nome da coleção existir no caso, a coleção original será excluída.
Tags	Opcional. Usado para recuperar rapidamente os conjuntos de resultados exatos de documentos relevantes. Use uma vírgula para separar várias tags. Use somente caracteres alfanuméricos; caracteres especiais não são permitidos.
Ativar BPF (Berkeley Packet Filter) customizado	Disponível para usuários administradores. Marcar a caixa de seleção ativa um campo de entrada BPF em que você especifica um endereço IP e uma porta.
Ativar dispositivos de captura customizados	Disponível para usuários administradores. Marcar a caixa de seleção gera a lista de dispositivos PCAP em sua implementação. Selecione um ou mais dispositivos para ver o tráfego somente desses dispositivos.

- b. Clique em **OK** e, em seguida, clique na guia Forensics.

**Resolução de problemas:** Se você vir uma mensagem dizendo que você não tem permissão para recuperar dados, assegure-se de que seu perfil de segurança tenha acesso ao endereço IP. Em algumas instâncias, se você tiver usado um caractere # no campo **Tags**, você poderá ver a mensagem.

- c. Clique no ícone de incidentes  para visualizar os incidentes. Expanda ou reduza o conteúdo ao navegar por uma hierarquia.
  - d. Para visualizar os documentos no incidente, clique em **Ir para os resultados da página da procura**.
  - e. Para visualizar uma seqüência de eventos do incidente, clique em **Ir para os resultados da página do pesquisador**.
  - f. Para remover ou cancelar um incidente específico, clique em **Excluir ou cancelar este incidente**.
  - g. Para executar novamente a tarefa de recuperação forense anterior, clique em **Executar novamente esta recuperação forense**. Por exemplo, se os resultados retornarem dados incompletos, você executará novamente a recuperação forense para incluir endereços IP diferentes ou para mudar o prazo especificado na tarefa de recuperação da execução anterior.
2. Para procurar casos existentes no QRadar, clique com o botão direito em um endereço IP e clique em **Executar procura forense**.
    - a. Na guia **Forense**, clique no ícone de incidentes.
    - b. Para investigar uma agregação das atividades que estão associadas a um incidente, destaque um caso passando o mouse sobre ele e, em seguida, clique no ícone de procura.
    - c. Para investigar as atividades por host QRadar Incident Forensics e dispositivo de captura em implementações distribuídas, expanda a entrada **Caso** e, em seguida, expanda a entrada **Coleção**.
    - d. Para visualizar uma lista cronológica de interações em um incidente, destaque a coleção passando o mouse sobre ela e, em seguida, clique no ícone Pesquisador.

**Conceitos relacionados:**

“Visualização de documento reconstruída” na página 27

A guia **Visualizar** mostra uma visualização reconstruída do documento que está selecionada no lado esquerdo da tela na visualização Lista.

---

## BPF customizado

Para ver somente determinados tipos de tráfego ao executar uma recuperação forense, é possível escolher criar um Berkeley Packet Filter (BPF) customizado.

Na Recuperação forense, marcar a caixa de seleção ativa um campo de entrada BPF no qual você especifica um filtro BPF que filtra o tráfego de rede.

Use a sintaxe de BPF para especificar os filtros BPF. Uma expressão consiste em uma ou mais primitivas. As primitivas são referências a um ou mais campos em um cabeçalho de protocolo de rede. Por exemplo, host, porta, porta tcp são todos primitivas. É possível construir expressões complexas de filtro usando os operadores AND, OR e NOT.

Estes são exemplos de filtros:

```
host 10.0.0.1
port 80
tcp port 80 and host 10.0.0.1
host 10.0.0.1 or host 10.0.0.2 or port 80 or port 443
```

Para criar um BPF customizado, deve-se ter acesso à função de usuário Administrador. Todos os usuários não administradores têm acesso somente leitura do campo de texto BPF. Os usuários administradores podem inserir qualquer expressão de BPF.

**Restrição:** A recuperação forense se aplicará à entrada BPF fornecida. Se os resultados da recuperação não forem conforme esperado, verifique a entrada de recuperação e o BPF para assegurar que os critérios estejam corretos.

Mesmo quando não usado pelo BPF customizado, o campo BPF sempre tem o conteúdo dos campos **Endereço IP** ou **Porta**. Se nenhum endereço IP ou porta for inserido, o BPF customizado usará o TCP ou UDP padrão.





---

## 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.

Estas informações podem incluir imprecisões técnicas ou erros tipográficos. São feitas mudanças periódicas nas informações aqui contidas; tais mudanças 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  
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.

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 dos revendedores 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](http://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](http://www.ibm.com/legal/copytrade.shtml).

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 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 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>.

---

## Glossário

Este glossário fornece termos e definições para IBM Security QRadar Incident Forensics software e produtos.

As seguintes referências cruzadas são usadas nesse glossário:

- *Consulte* o encaminha de um termo não preferencial para o termo preferencial ou de uma abreviação para sua forma por extenso.
- *Consulte também* o encaminha para um termo relacionado ou contrastante.

Para outros termos e definições, consulte o website IBM Terminology (abre em uma nova janela).

“A” “C” “D” “F” “H” “I” na página 48 “M” na página 48 “O” na página 48 “P” na página 48 “R” na página 48 “S” na página 48 “T” na página 48 “V” na página 49

---

### A

#### **anomalia**

Um desvio do comportamento esperado da rede.

#### **ataque**

Qualquer tentativa realizada por uma pessoa desautorizada de comprometer a operação de um programa de software ou sistema de rede. Consulte também invasor.

---

### C

**caso** As informações que estão contidas dentro de um banco de dados que pertence a uma investigação particular.

#### **categoria**

Um conjunto de itens que são agrupados de acordo com uma descrição específica ou classificação. As categorias podem ser de níveis diferentes de informações em uma dimensão.

#### **coleção**

Um conjunto nomeado de dados distinto que é associado a um caso. Por exemplo, um conjunto ordenado de pacotes de rede capturados.

#### **conversa**

Um fluxo de dados reconstruído de modo forense entre dois ou mais terminais de rede. Por exemplo, uma conversa de rede social.

#### **criptografia**

Na segurança do computador, o processo de transformação de dados em uma forma ininteligível, de tal maneira que os dados originais, quer não pode ser obtido ou só pode ser obtida por meio de um processo de decifração.

---

### D

#### **desdobrando**

O processo pelo qual os dados de captura de pacote são descompilados para que todos os dados ingeridos sejam produzidos como um relatório de resultados.

#### **dispositivo de captura**

Consulte dispositivo de captura do pacote.

#### **dispositivo de captura de pacote**

Um dispositivo independente que intercepta e registra dados de tráfego.

---

### F

#### **ferramenta do pesquisador**

Uma ferramenta que exibe a sequência cronológica de atividades em um incidente de segurança em um visualizador.

---

### H

#### **hipótese**

Uma explicação proposta para um incidente que é baseada nas evidências disponíveis coletadas em um caso. Uma hipótese deve ser testável e falsificável.

---

## I

### **Identifica**

Uma coleta de atributos de uma origem de dados que representa uma pessoa, organização, lugar ou item.

### **identificador de centralização**

O item de categoria com o qual todos os outros identificadores interagiram. O identificador de centralização é o item central em uma investigação.

### **impressão digital**

Um relatório composto de identificadores de tag relacionados uns com os outros em um caso individual.

### **incidente**

Consulte incidente de segurança.

### **incidente de segurança**

Um evento no qual as operações de rede normal são violadas, comprometidas ou atacadas.

### **informações de captura de pacote**

As informações de dados de tráfego que são coletadas por um dispositivo de captura.

### **inspetor de domínio**

Um inspetor especializado que é designado para desconstruir e extrair dados forenses de websites de domínio específico, como Facebook ou Gmail.

### **inspetor de protocolo**

Um inspetor especializado que é projetado para extrair dados forenses de protocolos de rede, como HTTP ou FTP.

### **invasor**

Um usuário (humano ou programa de computador) que tente causar danos a um sistema de informações ou acessar informações não destinadas ao acesso geral. Consulte também ataque.

### **investigador forense**

O usuário que extrai os dados relevantes do tráfego de rede e documentos no repositório forense.

---

## M

### **mapa relacional de metadados**

Um mapa que exhibe metadados relacionados de documentos de caso.

## metadados

Dados que descrevem as características dos dados; dados descritivos.

---

## O

**ofensa** Uma mensagem enviada ou um evento gerado em resposta a uma condição monitorada. Por exemplo, uma ofensa fornecerá informações sobre se uma política tiver sido infringida ou a rede está sofrendo um ataque.

### **Operador booleano**

Uma função integrada que especifica uma operação lógica de AND, OR ou NOT quando os conjuntos de operações são avaliados. Os operadores booleanos são &&, || e !.

---

## P

### **presença eletrônica coletada continuamente**

Uma identidade online do invasor como uma coleção de impressões digitais que estão vinculadas.

---

## R

### **registro de fluxo**

Um registro de uma conversa entre dois hosts.

### **relacionamento de impressão digital**

Um relacionamento entre identificadores de tag relacionados a um caso.

---

## S

### **superfluxo**

Um fluxo único que é composto por diversos fluxos com propriedades semelhantes para aumentar a capacidade de processamento ao reduzir as restrições de armazenamento.

---

## T

### **tarifa de recuperação**

Um processo que recupera dados de captura consultados e os encaminha para o dispositivo de desdobramento para ingestão.

### **tráfego**

Na comunicação de dados, a quantidade

de dados transmitidos que passa de um ponto em particular em um caminho.

**tráfego de rede alimentado**

Tráfego de rede capturado que foi processado pelo processo de desdobramento forense.

**trilha** Impressões digitais que conectam indivíduos envolvidos em um caso a indivíduos de fora do caso.

**trilha de navegação**

Um elemento da interface da web que exibe a posição do usuário dentro de um site. Em geral, são vários hyperlinks que aparecem na parte superior ou inferior da página. Esses links indicam as páginas que foram visualizadas e permite ao usuário navegar de volta ao local de início.

---

**V**

**vulnerabilidade**

Uma exposição de segurança em um sistema operacional, software do sistema ou componente de software de aplicativo.





---

# Índice Remissivo

## A

anotações 23  
arquivos  
fazendo upload usando FTP 17

## B

blocos de tempo 26

## C

consulta 21  
critérios de procura 21

## G

gerador de consultas 21  
glossário 47

## I

impressão digital  
visão geral 28  
investigação de endereço IP 39

## N

novos recursos, 1

## O

o que há de novo  
usuários da versão 7.2.7 1

## P

padrões 25

## T

tag de metadados 19

## V

visualizações 25







Impresso no Brasil