Recuperar arquivos colocados em quarentena por endpoint seguro

Contents

Introdução

Este documento descreve como restaurar arquivos que foram colocados em quarentena pelo conector de Ponto de Extremidade Seguro a partir do console do Ponto de Extremidade Seguro.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Console Cisco Secure Endpoint

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Secure Endpoint Console v5.4.2025030619

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

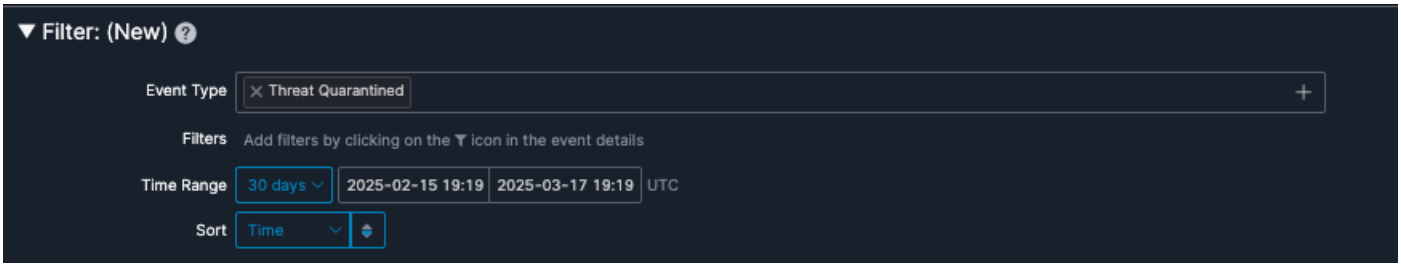
Problema

Os arquivos em quarentena pelo conector Secure Endpoint (SE) podem ser recuperados para análise de arquivos, envios de falsos positivos ou restauração quando o arquivo é considerado seguro. Os administradores podem executar essa ação diretamente no Console de endpoint seguro.

Solução

1. Navegue até a página Eventos no console do SE.

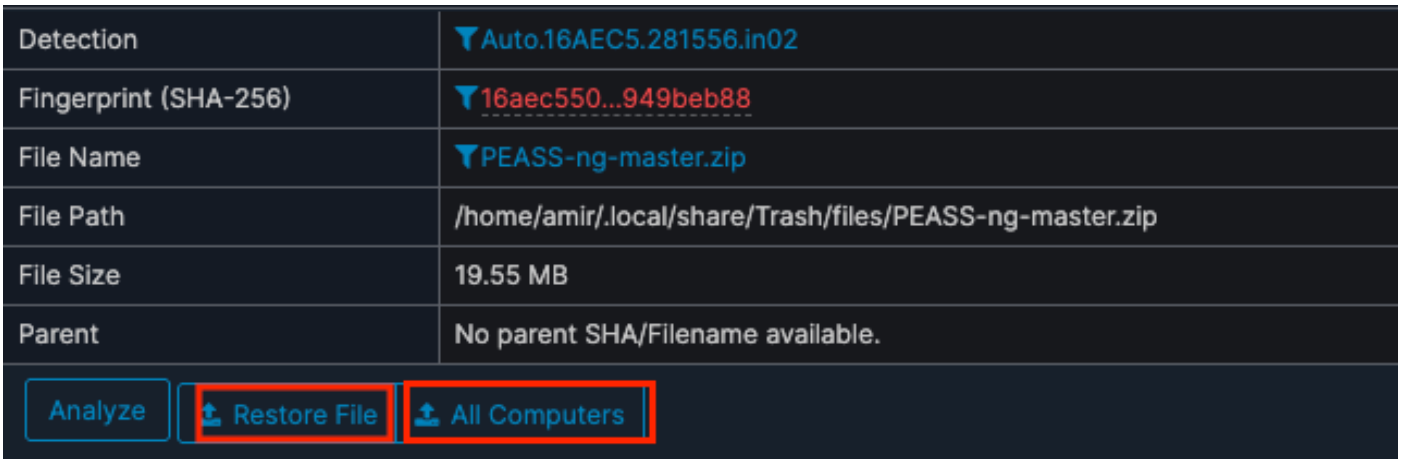
2. Filtre os eventos para mostrar todas as quarentenas bem-sucedidas selecionando o filtro Tipo de Evento = Ameaça em Quarentena.



Tipo de evento em quarentena de ameaça

3. Identifique o evento de detecção associado ao arquivo que você precisa restaurar.

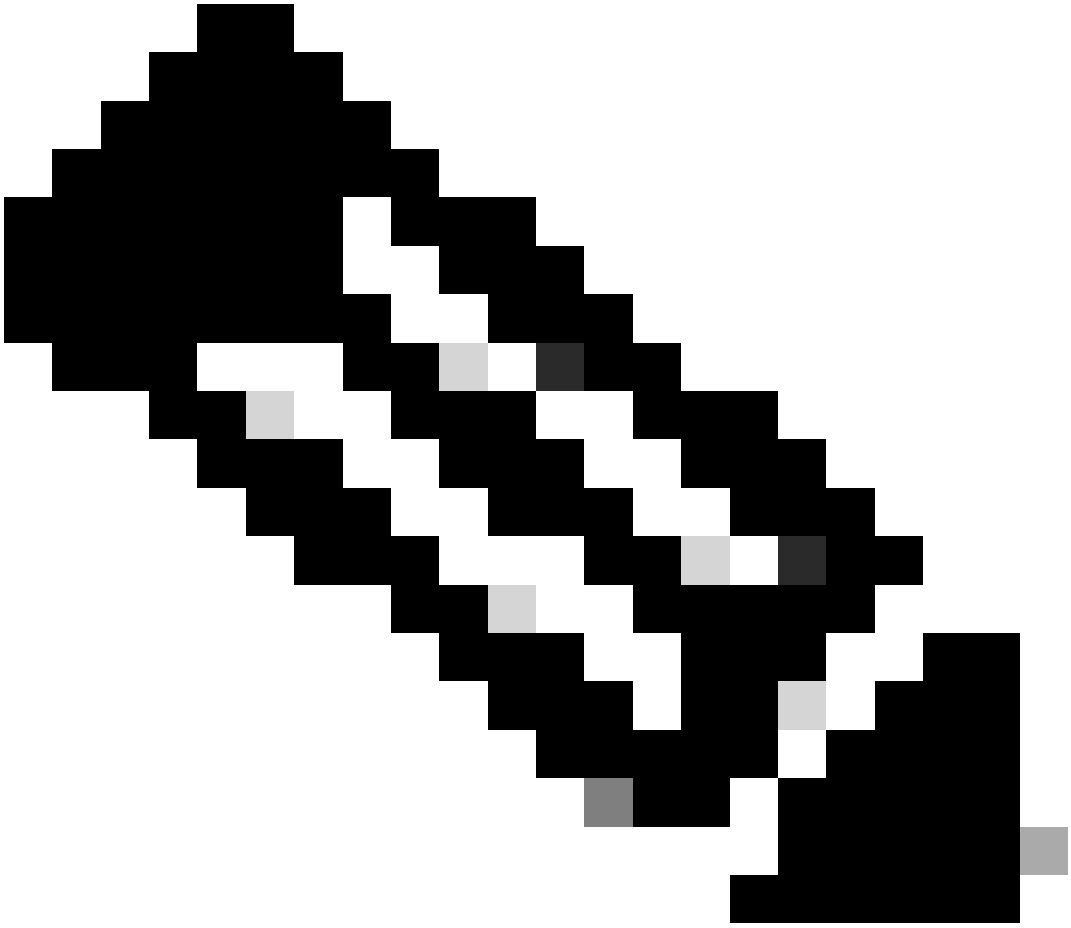
4. Expanda os detalhes do evento para acessar a opção Restaurar Arquivo. Selecionar Restaurar Arquivo restaura o arquivo na máquina afetada. Selecionar Todos os computadores restaura o arquivo em todos os computadores em que ele foi colocado em quarentena.



Opções de Restauração de Arquivo

5. O Intervalo de pulsação é a frequência com que o conector chama para casa para ver se há arquivos a serem restaurados pelo administrador. Os arquivos são restaurados quando os computadores afetados estão online ou quando ocorre o próximo intervalo de pulsação.

6. Se o arquivo for confiável, adicione-o a uma Lista de Permissões para evitar que ele seja colocado em quarentena novamente.



Note: Os arquivos permanecem em quarentena por 30 dias ou quando a pasta de quarentena atinge 100 MB e os arquivos mais antigos são limpos. Os arquivos em quarentena não podem mais ser restaurados após serem limpos.

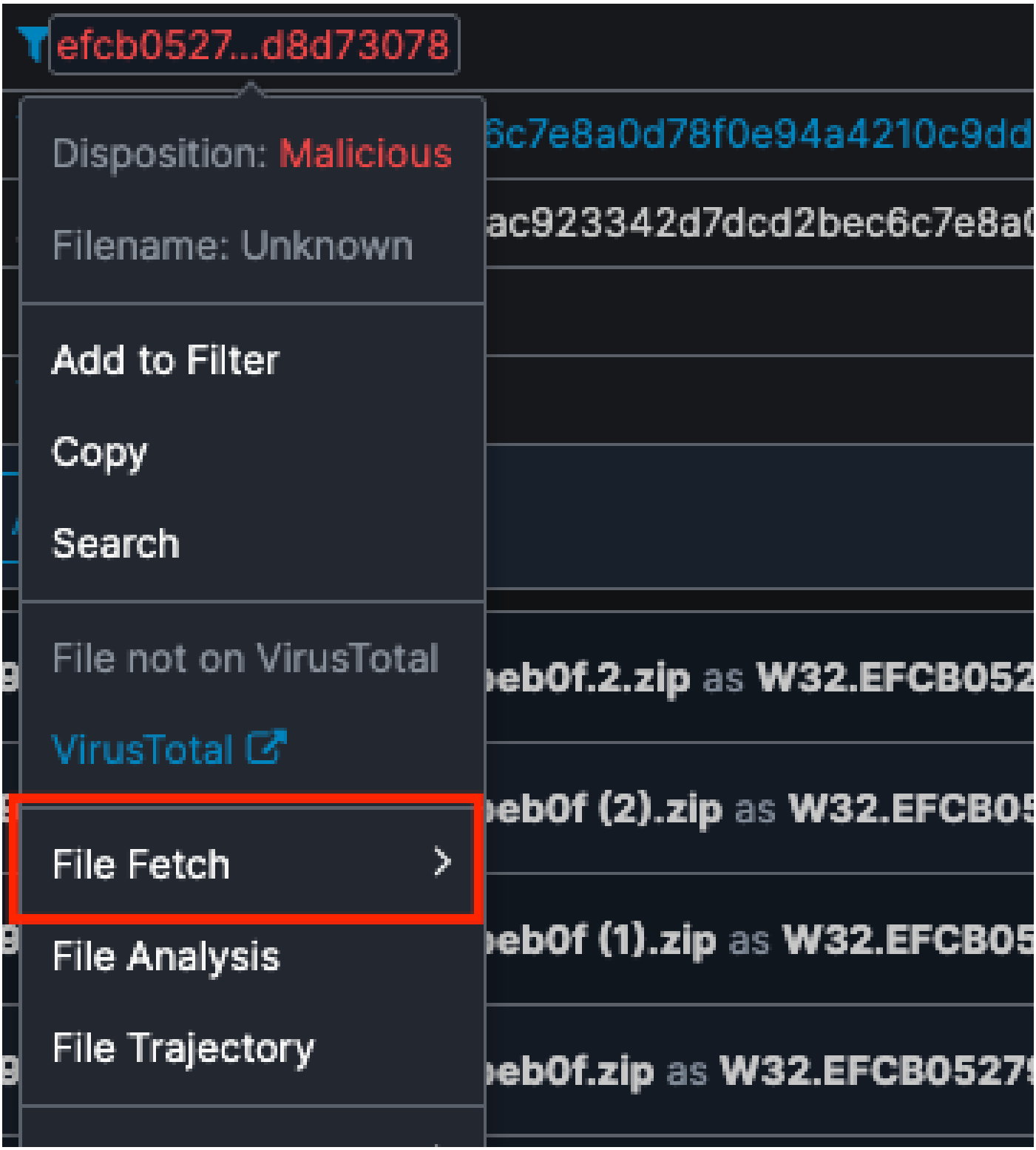
Se você precisar simplesmente baixar um arquivo em quarentena para análise de ameaças ou envios de falsos positivos sem restaurá-lo para seu ambiente, você pode usar o recurso Busca de Arquivo. Etapas para Download de um Arquivo em Quarentena:

1. Navegue até a página Eventos no console do SE.

2. Filtre os eventos para mostrar todas as quarentenas bem-sucedidas selecionando o filtro Tipo de Evento = Ameaça em Quarentena.

3. Identifique o evento de detecção associado ao arquivo que você precisa para Download.

4. Clique no valor SHA-256 do arquivo em quarentena para revelar a opção File Fetch.



Busca de arquivo

Isso fornece o status da busca de arquivos, a opção para iniciar a busca e o acesso para visualizar o arquivo no Repositório de arquivos.

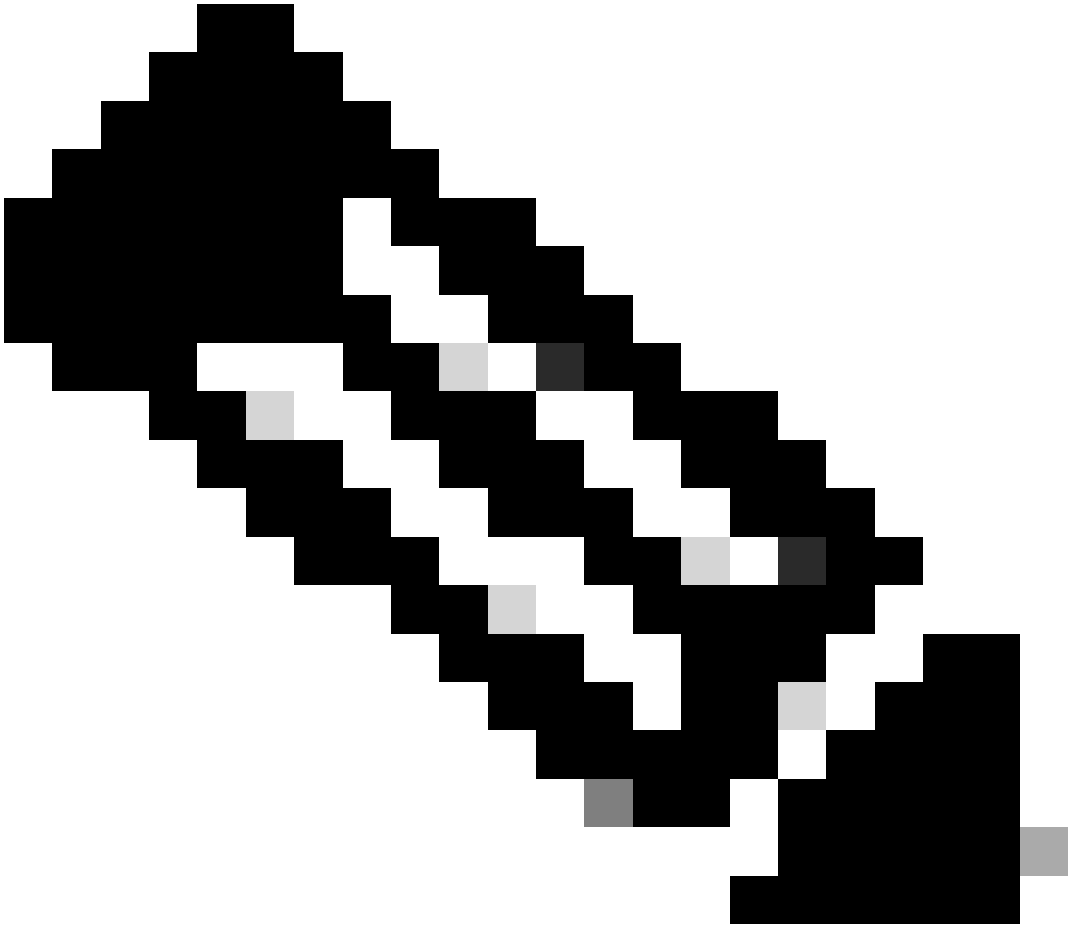
5. Clique em Buscar Arquivo, selecione o Computador do qual deseja recuperar o arquivo e confirme clicando em Buscar.

6. Uma notificação por e-mail é enviada quando o arquivo é carregado no Repositório de arquivos.

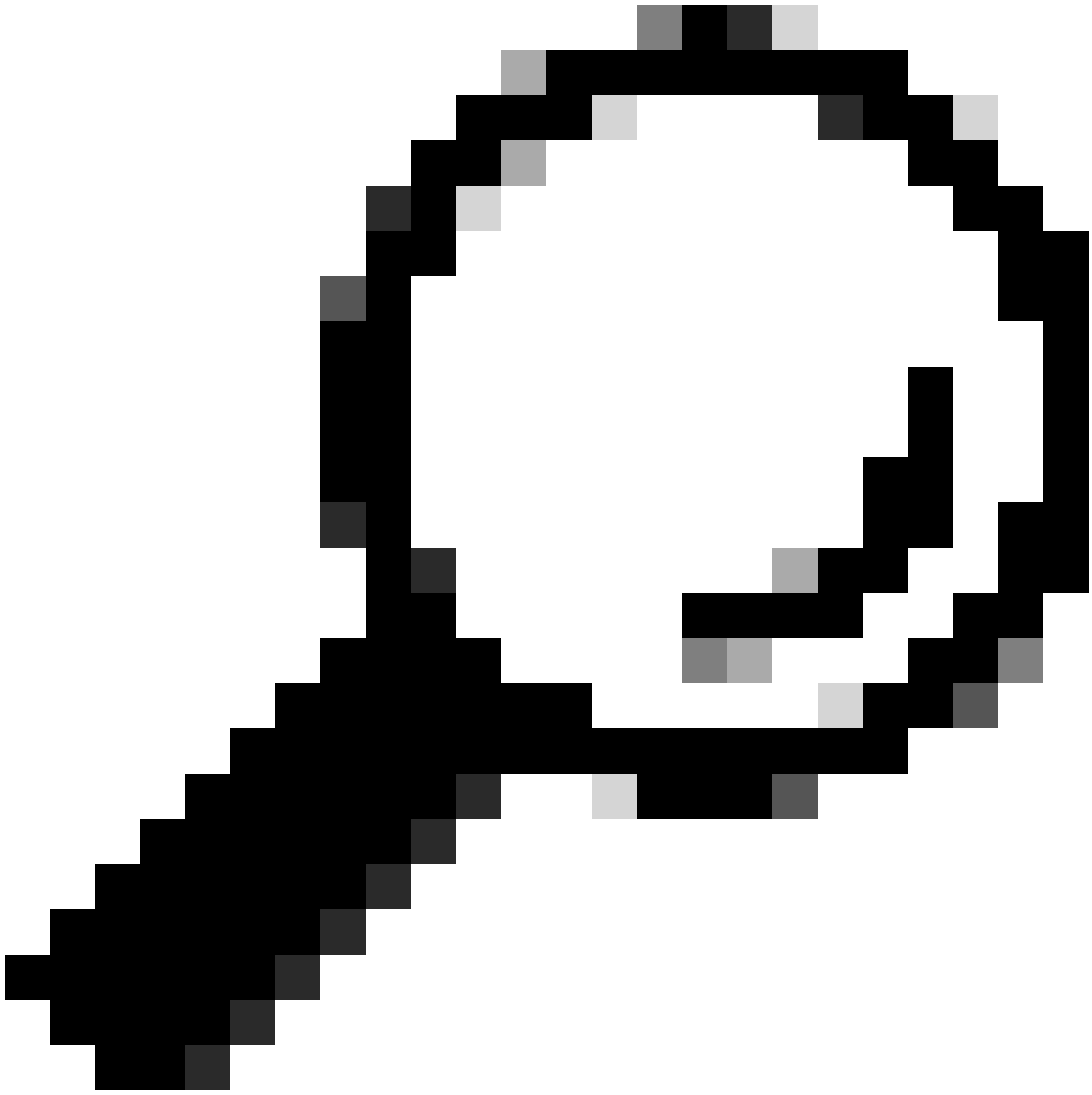
7. Quando o arquivo estiver disponível, você poderá ver o arquivo e a opção para fazer download em Análise> Repositório de Arquivos.

Download do arquivo

Todos os arquivos baixados do Repositório de arquivos são zipados e protegidos por senha.



Note: Para que a Busca de arquivo funcione corretamente, o tráfego de rede deve ser permitido para o servidor de Busca de arquivo apropriado com base na sua região de nuvem: Europa: rff.eu.amp.cisco.com América do Norte: rff.amp.cisco.com APJC: rff.apjc.amp.cisco.com. Além disso, certifique-se de que a 2FA (Two-Fator Authentication, Autenticação de dois fatores) esteja habilitada para a conta do administrador, pois ela é necessária para iniciar com êxito uma solicitação de busca de arquivo.



Tip: Você pode filtrar eventos usando Tipo de evento = Falha na restauração de quarentena e Tipo de evento = Falha na busca de arquivo para identificar falhas e revisar os motivos correspondentes para as operações de restauração e busca de arquivo, respectivamente.

Se você não conseguir restaurar o arquivo usando as etapas descritas, entre em contato com o TAC da Cisco e forneça o arquivo .qrt localizado no diretório C:\Program Files\Cisco\AMP\Quarantine.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.