Painel do Umbrella: Novo recurso e inspeção de arquivo

Contents

Introdução

Este documento descreve o novo painel do Umbrella.

Notou algo diferente no painel do seu Umbrella? Bem, estamos felizes em anunciar que estamos começando o processo de mover as pessoas para um novo conjunto de recursos incríveis do Umbrella. O primeiro recurso que apresentamos é a inspeção de arquivos. A inspeção de arquivos verifica os arquivos que suas identidades baixam para ver se contêm código mal-intencionado e bloqueia-os, caso contenham.

Para ajudá-lo a aproveitar esse novo recurso, também lançamos relatórios de segurança novos e atualizados e uma nova experiência de criação de política. Esse recurso é um dos vários que planejamos para versões futuras, criados com base no avanço de nossa infraestrutura de Proxy Inteligente para oferecer ainda mais segurança baseada em nuvem para nossos usuários.

Esses recursos estão sendo implementados em pequenos incrementos para nossos clientes. Se você recebeu um alerta em seu painel sobre esses recursos, você os tem! E se você quiser ser um dos primeiros a adotar esses recursos, entre em contato com umbrella-support@cisco.com.

O recurso de inspeção de arquivos está disponível apenas para clientes com os pacotes Umbrella Insights ou Umbrella Platform. Clique aqui para ler mais sobre os pacotes e entre em contato com seu representante de conta da Cisco se tiver alguma dúvida.

Ótimo, como posso aproveitar a inspeção de arquivos?

O assistente de política permite habilitar a Inspeção de arquivo na página de resumo ou ao criar uma nova política.

No lado de relatórios, a seção de navegação de relatórios do painel Umbrella foi atualizada para que você possa localizar facilmente nossos relatórios novos e atualizados. Vamos ver como habilitar o recurso e conferir alguns relatórios.

Ativando a Inspeção de Arquivos

A inspeção de arquivos é um recurso do Proxy Inteligente que amplia seu escopo e funcionalidade, adicionando a capacidade de verificar arquivos em busca de conteúdo mal-intencionado hospedado em domínios suspeitos. Um domínio suspeito não é confiável nem é conhecido por ser mal-intencionado e está listado em nossa "lista cinza" de domínios.

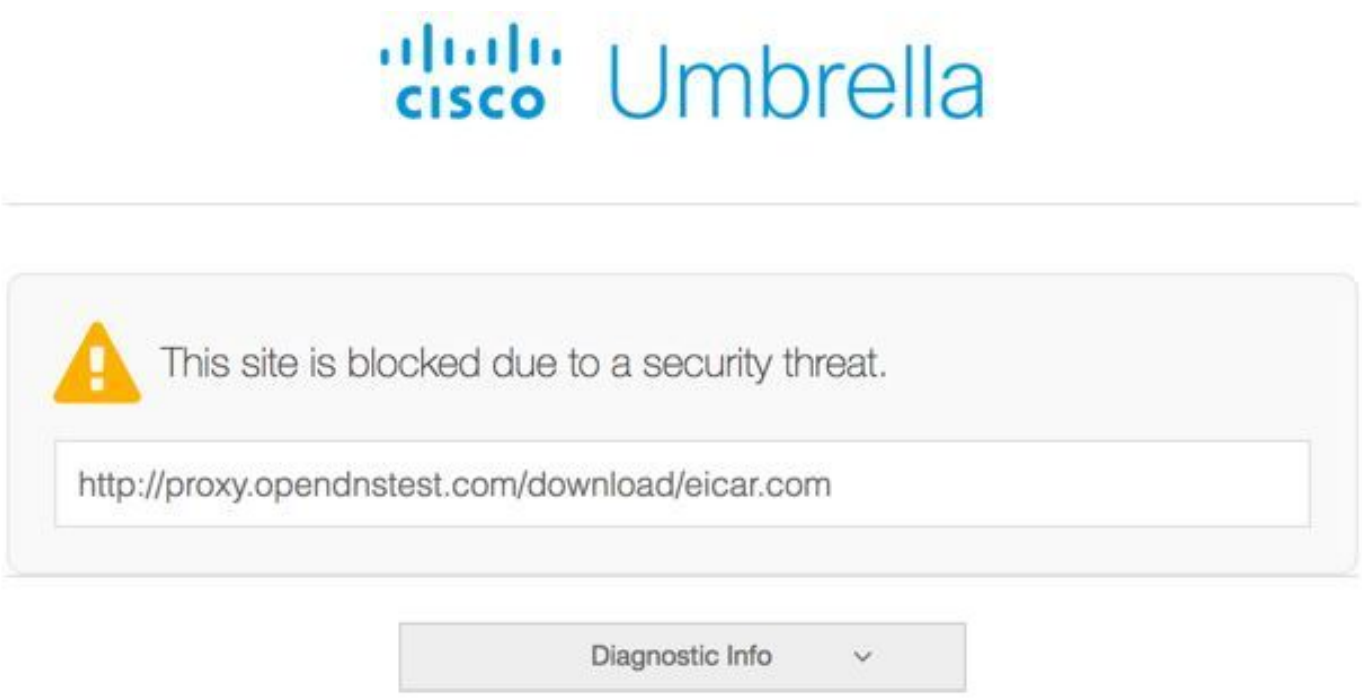
Com o assistente de política do Umbrella, a inspeção de arquivos é fácil de implementar. Navegue até Policies > Policy List (Políticas > Lista de políticas) e expanda uma política ou clique no ícone + (Add) (Adicionar) para criar uma nova política. No assistente de política, certifique-se de que a Inspeção de arquivos esteja ativada na página de resumo ou, em uma nova política, certifique-se de verificar Inspecionar arquivos depois de ativar o Proxy inteligente (em Configurações avançadas). A documentação completa deste recurso pode ser encontrada aqui: https://docs.umbrella.com/deployment-umbrella/docs/file-inspection

Recomendamos habilitar a Descriptografia SSL para aproveitar ao máximo esse recurso.

Testando Inspeção de Arquivo

De um dispositivo que foi registrado em uma política com a Inspeção de arquivos habilitada:

1. Procure em http://proxy.opendnstest.com/download/eicar.com.
2. Uma página de bloqueio como esta aparece:



Relatórios para Inspeção de Arquivos

Como parte da ajuda para fornecer mais visibilidade sobre o que foi bloqueado (bem como

quando, por que e como), atualizamos alguns relatórios no Umbrella, incluindo um relatório de Atividade de Segurança renovado:

- O Relatório de visão geral sobre segurança
  Fornece um instantâneo fácil de ler da atividade da rede por meio de gráficos. Você pode ver rapidamente o que está acontecendo com suas identidades e seu tráfego, ilustrando onde os problemas podem estar ocorrendo. Saiba mais sobre isso aqui.

- O Relatório de atividades de segurança
  Destaca eventos de segurança sinalizados, mas não necessariamente bloqueados, pela inteligência de ameaças do Umbrella. Isso inclui eventos de segurança filtrados por meio do Proxy Inteligente e da inspeção de arquivos. Este relatório é especialmente importante para mostrar o que foi bloqueado, por que e como. Saiba mais sobre isso aqui.

- Relatório Pesquisa de atividades
  Ajuda você a encontrar o resultado de cada solicitação DNS, URL e IP de suas várias identidades, ordenadas por data e hora decrescentes. Este relatório lista todas as atividades no Umbrella para o período de tempo selecionado e, usando filtros, você pode refinar sua pesquisa para ver apenas o que deseja ver. Saiba mais sobre isso aqui.

E com nossa navegação recém-atualizada, esses relatórios também são fáceis de acessar! Basta expandir o painel do menu à esquerda e ir para qualquer relatório diretamente de qualquer outro lugar no painel.

Como posso fazer com que você saiba o que eu penso?

Adoraríamos saber o que você acha desses novos recursos. Se tiver dúvidas ou comentários, gostaríamos de saber o que você tem a dizer! Envie seus comentários para umbrella-support@cisco.com e inclua o máximo de detalhes possível. Por exemplo, capturas de tela, o navegador que você está usando, seu SO e o cenário no qual você está usando esses recursos.

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.