Entenda a categoria de segurança potencialmente prejudicial no Umbrella

Contents

Introdução

Este documento descreve a categoria de segurança Potencialmente Prejudicial no Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

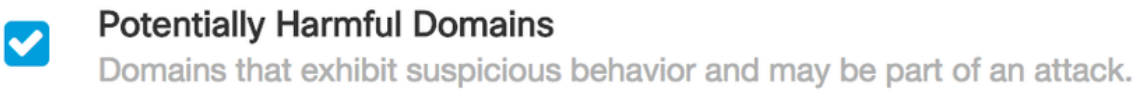
Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

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.

Overview

Os clientes da Umbrella têm diferentes níveis de tolerância a riscos quando se trata de segurança. Dependendo do setor e do tipo de trabalho realizado, pode ser benéfico monitorar e bloquear proativamente atividades potencialmente prejudiciais. A nova configuração de segurança "Potentially Harmful" pode ser encontrada em Prevent ao lado de outras Security Settings e está definida como Allow por padrão:



115011476788

Detalhes

Potencialmente nocivo é uma categoria de segurança que contém domínios que provavelmente serão mal-intencionados. É diferente das categorias de "malware" da Umbrella porque a Umbrella as classificou com um nível menor de confiança sobre se elas são realmente mal-intencionadas. Outra maneira de expressar isso é que esses domínios são considerados suspeitos de acordo com nossos analistas de pesquisa e os algoritmos que usamos para determinar em geral, mas não necessariamente conhecidos como mal-intencionados.

O uso desta categoria depende da sua tolerância ao risco de bloquear domínios potencialmente bons. Se você tiver um ambiente altamente seguro, essa é uma boa categoria para bloquear e, se o seu ambiente estiver mais solto, você poderá simplesmente permitir e monitorar.

Se você não tiver certeza de qual delas você se enquadra, poderá monitorar atividades confirmadas como "Potencialmente Prejudicial" em seus relatórios. Ter essa categoria disponível pode fornecer granularidade adicional na classificação do tráfego, aumentando a visibilidade e oferecendo maior proteção e melhorando a resposta a incidentes. Por exemplo, se você acredita que uma máquina está infectada com malware, dar uma olhada nos domínios potencialmente prejudiciais que ela tem visitado pode ajudá-lo a fazer um melhor trabalho de avaliação do nível de comprometimento.

A Umbrella determina o que é "potencialmente prejudicial", ponderando vários fatores que indicam que, embora o domínio não seja claramente mal-intencionado, ele pode representar uma ameaça. Por exemplo, há vários tipos de serviços de tunelamento DNS. Alguns desses serviços se enquadram nas categorias de VPN de tunelamento benigno, mal-intencionado e DNS, mas alguns são mais incertos e não se enquadram em nenhuma dessas categorias. Se o caso de uso para o tunelamento for desconhecido e suspeito, o destino pode se enquadrar na categoria Potencialmente prejudicial.

Outro exemplo vem do modelo de classificação Spike da Umbrella. O modelo de classificação Spike da Umbrella aproveita grandes quantidades de dados de solicitação DNS e detecta domínios que têm picos em seus padrões de solicitação DNS usando gráficos de onda de som. O tráfego que atinge o nível mais alto no domínio de classificação Spike pode ser classificado automaticamente como mal-intencionado, e o tráfego que está abaixo do limite pode cair na categoria Potencialmente prejudicial.

Para relatar detecções indesejadas em qualquer uma destas categorias:

- Envie todas as solicitações de categorização de dados para o Cisco Talos por meio doTalos

Support.

- Para obter as etapas gerais de envio de solicitações ao Cisco Talos, consulte Como: Enviar Uma Solicitação De Categorização.

Para a categoria Potencialmente Nocivo, a Umbrella não a reclassifica como segura sem garantir que o domínio seja absolutamente legítimo.

Ambas as categorias podem ser filtradas em seus relatórios, como qualquer outra categoria de segurança.

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.