Comprender la categoría de seguridad potencialmente perjudicial en Umbrella

Contenido

Introducción

En este documento se describe la categoría de seguridad Potencialmente perjudicial de Cisco Umbrella.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

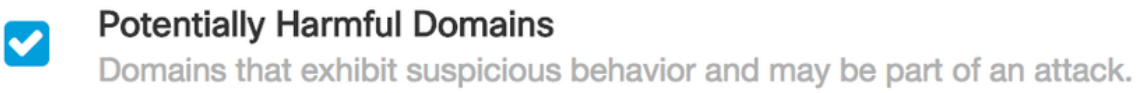
Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Los clientes generales tienen diferentes niveles de tolerancia al riesgo en lo que respecta a la seguridad. Dependiendo del sector y del tipo de trabajo que realice, puede ser beneficioso supervisar y bloquear de forma proactiva las actividades potencialmente dañinas. La nueva configuración de seguridad "Potencialmente perjudicial" se puede encontrar en Prevenir junto a otras configuraciones de seguridad y se establece en Permitir de forma predeterminada:



115011476788

Detalles

Potencialmente perjudicial es una categoría de seguridad que contiene dominios que pueden ser malintencionados. Es diferente de las categorías de "malware" de Umbrella porque Umbrella las clasificó con un nivel de confianza inferior sobre si realmente son maliciosas. Otra forma de expresarlo es que estos dominios se consideran sospechosos según nuestros analistas de investigación y los algoritmos que usamos para determinar en general, pero no necesariamente se sabe que son maliciosos.

El uso de esta categoría depende de su tolerancia al riesgo de bloquear dominios potencialmente buenos. Si tiene un entorno muy seguro, esta es una buena categoría que bloquear y si su entorno es más flexible, puede simplemente permitir y supervisar.

Si no está seguro de a cuál de ellas pertenece, puede supervisar la actividad que se confirma como "Potencialmente perjudicial" en sus informes. La disponibilidad de esta categoría puede proporcionar una granularidad adicional a la hora de clasificar el tráfico, aumentar la visibilidad y ofrecer una mayor protección, así como mejorar la respuesta a incidentes. Por ejemplo, si cree que una máquina está infectada con malware, echar un vistazo a los dominios potencialmente dañinos que ha estado visitando puede ayudarle a evaluar mejor el nivel de riesgo.

Umbrella determina lo que es "potencialmente dañino" sopesando varios factores que indican que aunque el dominio no es claramente malicioso, podría representar una amenaza. Por ejemplo, hay varios tipos de servicios de tunelización DNS. Algunos de estos servicios pertenecen a las categorías de VPN benigna, malintencionada y de túnel DNS, pero algunos son más confusos y no pertenecen a ninguna de estas categorías. Si el caso de uso de la tunelización es desconocido y sospechoso, el destino puede caer en la categoría Potencialmente perjudicial.

Otro ejemplo proviene del modelo de rango Spike de Umbrella. El modelo de rango Spike de Umbrella aprovecha cantidades masivas de datos de solicitudes DNS y detecta dominios que tienen picos en sus patrones de solicitudes DNS mediante gráficos de ondas de sonido. El tráfico que llega a un nivel alto en el dominio de rango de Spike se puede clasificar automáticamente como malicioso, y el tráfico que está por debajo del umbral puede caer en la categoría Potencialmente perjudicial.

Para notificar detecciones no deseadas en cualquiera de estas categorías:

- Envíe todas las solicitudes de categorización de datos a Cisco Talos a [través deTalos Support.]
- Para conocer los pasos generales para enviar solicitudes a Cisco Talos, consulte Cómo:

Envíe Una Solicitud De Categorización.

Para la categoría Potencialmente perjudicial, Umbrella no la vuelve a categorizar como segura sin tener garantías de que el dominio es absolutamente legítimo.

Ambas categorías se pueden filtrar en los informes como cualquier otra categoría de seguridad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).