Comprendre la catégorie de sécurité potentiellement dangereuse dans Umbrella

Table des matières

Introduction

Ce document décrit la catégorie Sécurité potentiellement dangereuse dans Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Les clients parapluie ont différents niveaux de tolérance au risque en matière de sécurité. Selon le secteur et le type de travail que vous effectuez, il peut être avantageux de surveiller et de bloquer de manière proactive les activités potentiellement dangereuses. Le nouveau paramètre de sécurité « Potentially Harmful » se trouve sous Prevent à côté d'autres paramètres de sécurité et est défini sur Allow par défaut :

Potentially Harmful Domains

Domains that exhibit suspicious behavior and may be part of an attack.

115011476788

Détails

Potentially Harmful est une catégorie de sécurité qui contient des domaines susceptibles d'être malveillants. Il est différent des catégories de « programmes malveillants » d'Umbrella, car Umbrella les classe avec un niveau de confiance inférieur quant à savoir s'ils sont réellement malveillants. Une autre façon de formuler est que ces domaines sont considérés comme suspects selon nos analystes de recherche et les algorithmes que nous utilisons pour déterminer globalement, mais pas nécessairement connu pour être malveillant.

L'utilisation de cette catégorie dépend de votre tolérance au risque de bloquer des domaines potentiellement bons. Si vous disposez d'un environnement hautement sécurisé, il s'agit d'une bonne catégorie à bloquer et si votre environnement est plus souple, vous pouvez simplement autoriser et surveiller.

Si vous n'êtes pas sûr de savoir lequel de ces problèmes vous concerne, vous pouvez surveiller les activités qui sont confirmées comme « potentiellement dangereuses » dans vos rapports. La disponibilité de cette catégorie peut fournir une granularité supplémentaire dans la classification du trafic, en augmentant la visibilité et en fournissant une meilleure protection et en améliorant la réponse aux incidents. Par exemple, si vous pensez qu'une machine est infectée par un programme malveillant, l'examen des domaines potentiellement dangereux qu'elle a visités peut vous aider à mieux évaluer le niveau de compromission.

Umbrella détermine ce qui est « potentiellement dangereux » en pesant plusieurs facteurs qui indiquent que, bien que le domaine ne soit pas clairement malveillant, il pourrait constituer une menace. Par exemple, il existe différents types de services de tunnellisation DNS. Certains de ces services entrent dans les catégories des VPN bénins, malveillants et de tunneling DNS, mais certains sont plus flous et ne rentrent dans aucune de ces catégories. Si le cas d'utilisation du tunneling est inconnu et suspect, la destination peut être classée dans la catégorie Potentiellement dangereux.

Un autre exemple vient du modèle de rang Spike d'Umbrella. Le modèle de classement Spike d'Umbrella exploite des quantités massives de données de requête DNS et détecte les domaines qui ont des pics dans leurs modèles de requête DNS en utilisant le graphique d'onde sonore. Le trafic qui atteint le niveau le plus élevé dans le domaine de rang de pic peut automatiquement être classé comme malveillant, et le trafic qui est plus faible sur le seuil peut tomber dans la catégorie Potentiellement Nocif.

Pour signaler les détections indésirables dans l'une de ces catégories :

- Veuillez envoyer toutes les demandes de catégorisation de données à Cisco Talos via l'assistance Talos.
- Pour connaître les étapes générales à suivre pour envoyer des demandes à Cisco Talos, consultez Comment : Soumettre Une Demande De Catégorisation.

Pour la catégorie Potentiellement Dangereux, Umbrella ne la reclasse pas comme sûre sans prendre l'assurance que le domaine est absolument légitime.

Les deux catégories peuvent être filtrées dans vos rapports comme n'importe quelle autre catégorie de sécurité.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.