Améliorations à venir de la sécurité Umbrella - Domaines récemment vus

Table des matières

Introduction

Ce document décrit les améliorations de sécurité à venir apportées à la catégorie Nouveaux domaines (NSD) des services Secure Access et Umbrella.

Aperçu

Nous sommes ravis de vous informer d'une importante amélioration apportée à la catégorie Nouveaux domaines (NSD), un aspect clé de nos services d'accès sécurisé et de protection, sous la direction de l'équipe Talos Threat Research.

Que faisons-nous ?

Dans le cadre de nos efforts continus pour renforcer votre sécurité, nous mettons en oeuvre un système mis à jour pour NSD, en passant à la version 2 (NSDv2). Cette nouvelle itération élargit considérablement les données sources, car elle inclut maintenant l'ensemble complet de notre DNS passif qui alimente notre produit Investigate (800B requêtes/jour), une amélioration par rapport à la méthodologie d'échantillonnage statistique des domaines nouvellement vus actuels.

Avec NSDv2, nous avons affiné l'ensemble de données pour mieux refléter les commentaires et l'utilisation des clients, ainsi que l'analyse des données de l'occurrence jusqu'à la condamnation par notre équipe de recherche sur les menaces Talos. Le nouvel algorithme se concentre sur la découverte de nouveaux domaines de niveau enregistré et réduit le « bruit » de plusieurs sous-domaines partageant un parent commun.

Pourquoi faisons-nous cela ?

Nous avons écouté les commentaires des clients et analysé les données montrant comment NSD pourrait retarder la catégorisation des domaines à faible volume, causant des résultats inattendus et des perturbations dans les domaines s'ils connaissaient une augmentation soudaine de la popularité. En outre, les modifications apportées aux domaines à volume élevé peuvent entraîner

des changements inattendus, par exemple lorsqu'un réseau de diffusion de contenu introduit des modifications dans son système d'attribution de noms.

L'équipe Talos Threat Research a développé NSDv2 en collaboration avec Umbrella pour résoudre ces problèmes, fournissant un système plus fiable et plus précis pour identifier les nouveaux domaines.

En quoi cela vous est-il bénéfique ?

L'amélioration de NSDv2 est conçue en tenant compte de votre sécurité et de votre efficacité opérationnelle :

- Détection des menaces améliorée : NSDv2 se targue d'une amélioration d'au moins 45 % du taux d'identification des domaines qui se révèlent ensuite malveillants.
- Diminution des faux positifs : Avec un système de ciblage plus précis, vous subissez moins de perturbations en raison de domaines incorrectement marqués qui sont utilisés régulièrement.
- Performances optimisées : L'ensemble de données rationalisé permet non seulement une publication plus rapide, mais permet également à notre équipe d'assistance de résoudre rapidement les problèmes, le cas échéant.
- « Meilleure pratique » d'application : Cette catégorie est plus cohérente et pertinente et permet un meilleur alignement avec les attentes du secteur et des clients.
- Données de reporting enrichies : Le contexte et la couverture améliorés avec NSDv2 enrichissent les données dans les rapports.
- Prédiction améliorée : Cette mise à jour aide le proxy intelligent à déterminer les domaines à risque qui nécessitent une inspection plus approfondie.
- Aucune interaction client requise : Il s'agit d'une mise à jour de nos pipelines pour une catégorisation dynamique, et ne nécessite aucune migration ou modification de politique pour nos clients. Il s'agit d'une amélioration totalement transparente pour les administrateurs et les utilisateurs finaux.

Les modifications apportées à cette catégorie doivent être déployées le 13 août 2024. Nous vous sommes reconnaissants de la confiance que vous continuez à accorder à nos services et nous sommes impatients de vous apporter ces améliorations importantes en matière 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.