Comprendre pourquoi les domaines sont marqués comme récemment vus dans Umbrella

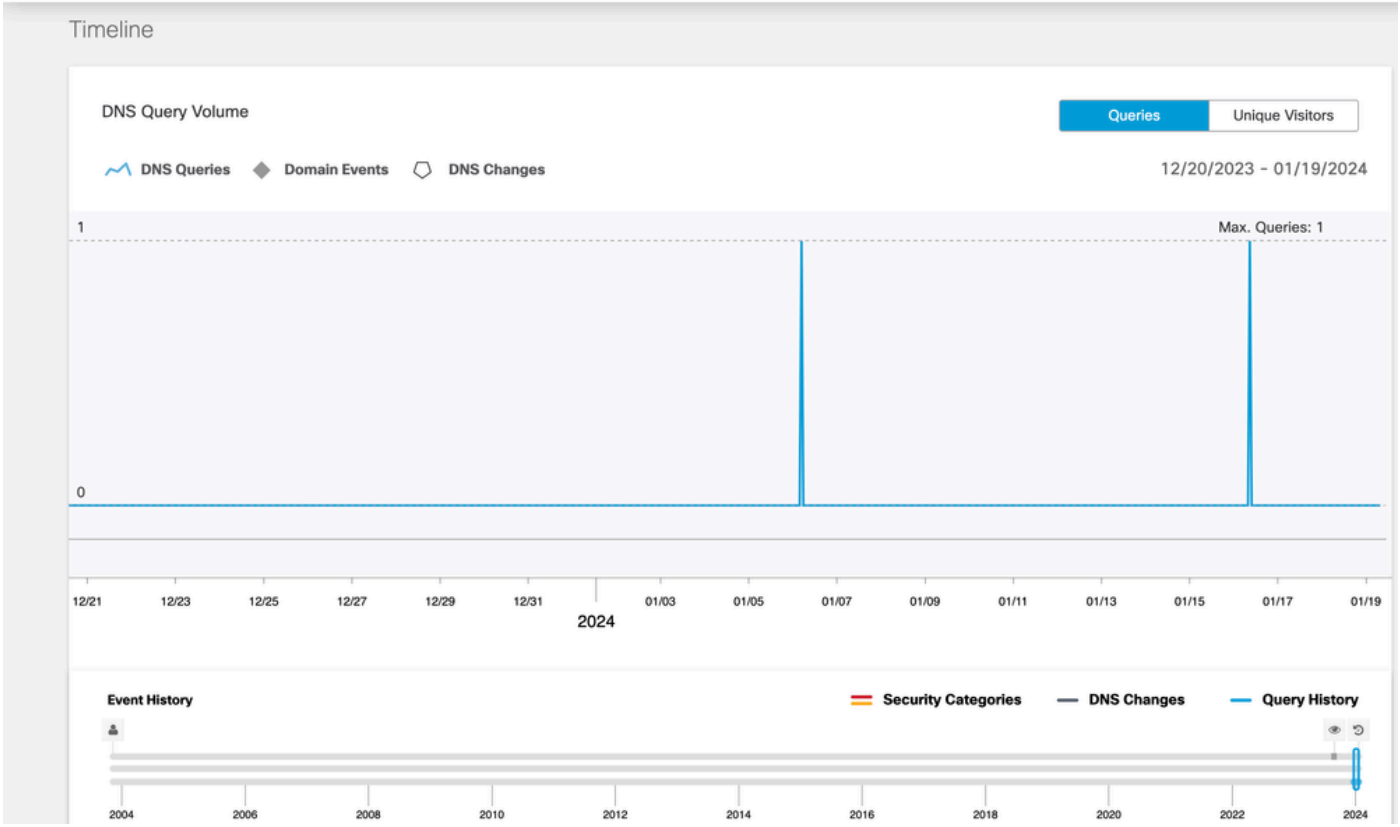
Table des matières

Introduction

Ce document décrit pourquoi les domaines peuvent être marqués comme nouvellement vus dans Umbrella, même s'ils ont déjà été classés.

Aperçu

Vous pouvez accorder l'accès à un domaine avant de vous rendre compte qu'il a été classé en tant que domaine nouvellement vu (NSD). En raison de la grande taille des journaux de DNS Umbrella, les domaines ne sont pas traités dans le même système dédié à l'identification des domaines nouvellement vus. Au lieu de cela, nous utilisons des exemples de données pour catégoriser la plupart des nouveaux domaines en temps opportun. Cependant, pour les domaines avec des volumes de requêtes très faibles, leur catégorisation peut être retardée parce que ces requêtes n'apparaissent pas dans le jeu de données échantillonné. Pour déterminer si un domaine a un volume très faible, vous pouvez utiliser la fonctionnalité Enquêter > Smart Search dans votre tableau de bord Umbrella. Le blocage des NSD peut provoquer des interruptions, car une NSD n'indique pas nécessairement une activité malveillante.



Alerte de faux positif générée pour les domaines récemment vus

Les domaines qui ont déjà été catégorisés peuvent soudainement être marqués comme NSD. Les domaines nouvellement vus sont découverts en mémorisant les requêtes DNS précédemment exécutées par nos clients dans une base de données. Si un domaine n'existe pas dans la base de données NSD, il est marqué comme nouvellement vu. Cependant, les journaux de requêtes utilisés pour construire la base de données NSD sont fortement échantillonnés et peuvent marquer faussement un domaine comme nouvellement vu même si le domaine a été utilisé pendant un certain temps. Par exemple, si le domaine "www.example.com" était déjà utilisé mais récemment marqué comme nouvellement vu, il est possible qu'il ait été manqué dans les échantillons précédents et marqué le domaine comme NSD.

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.