Understand why Domains Are Marked as Newly Seen in Umbrella

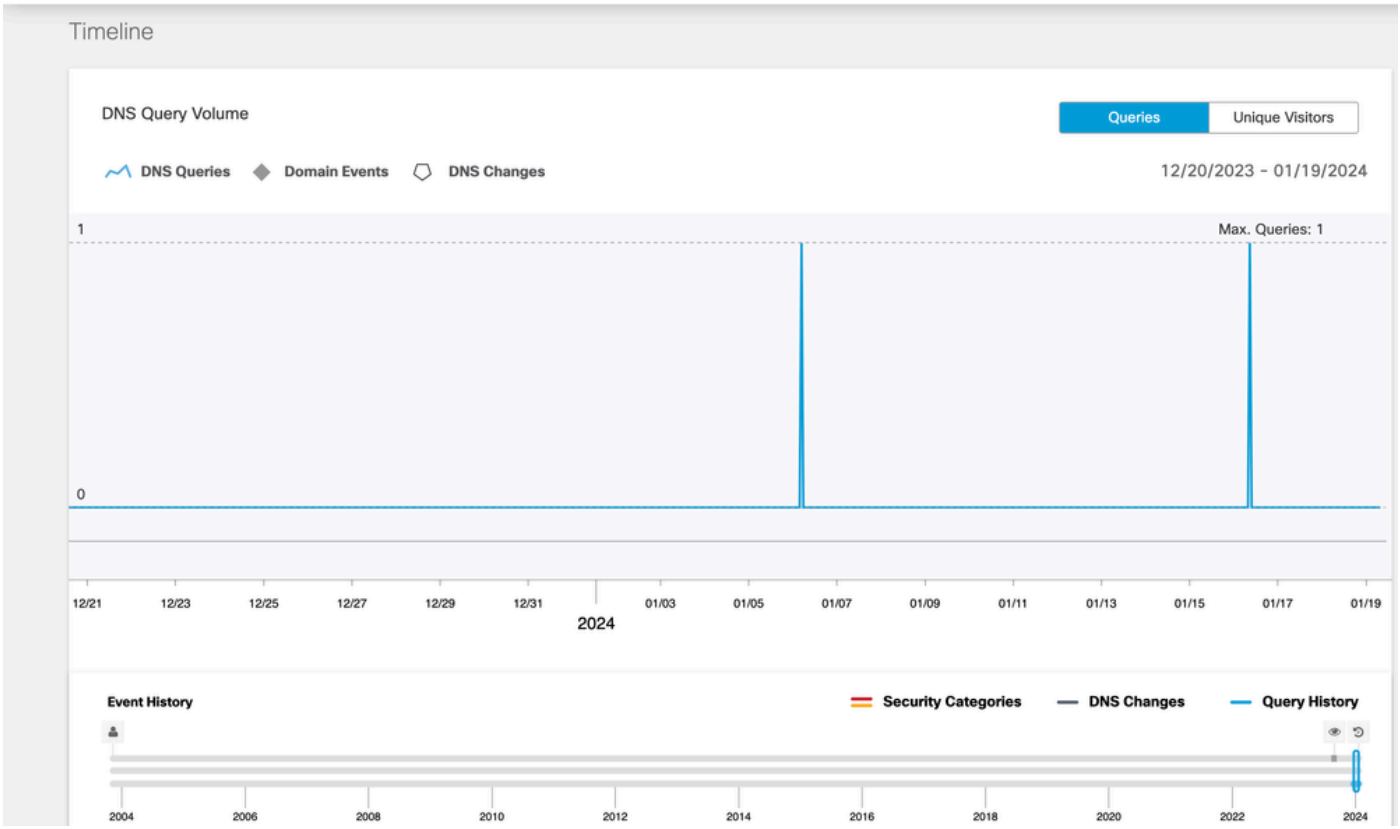
Contents

Introduction

This document describes why domains can be marked as newly seen in Umbrella, even if they have previously been categorized.

Overview

A domain can be granted access before you realize it has been categorized as a Newly Seen Domain (NSD). Due to the extensive scale of the Umbrella DNS logs, domains are not processed in the same system dedicated to identifying newly seen domains. Instead, we use sample data to categorize most of the new domains in a timely manner. However, for domains with very low query volumes, their categorization can be delayed because these queries do not appear in the sampled dataset. To determine if a domain has very low volume, you can use the **Investigate > Smart Search** feature in your Umbrella dashboard. Blocking NSDs can cause disruption, as an NSD does not necessarily indicate malicious activity.



False positive alert generated for Newly Seen Domains

Domains that have already been categorized can suddenly be marked as an NSD. Newly seen domains are discovered by memorizing the DNS queries previously ran by our customers in a database. If a domain does not exist in the NSD database, it is marked as newly seen. However, the query logs used to build the NSD database is heavily sampled and it can falsely mark a domain as newly seen even if the domain has been in use for awhile. For example, if the domain "www.example.com" was already in use but recently marked newly seen, it is possible that it was missed in previous samples and marked the domain as an NSD.