Umbrella Greylists und Grey Domains verstehen

Inhalt

Einleitung

In diesem Dokument werden Graulisten und Grauzonen-Domänen in Cisco Umbrella beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Umbrella bietet eine Funktion, mit der über Umbrella Intelligent Proxy Anfragen nach URLs, potenziell schädlichen Dateien und Domänennamen, die mit bestimmten nicht kategorisierten Domänen verbunden sind, proxybasiert werden können.

Graue Domänen

Der intelligente Proxy vermeidet alle vorab identifizierten Domains, die sicher und/oder schädlich sind. Es gibt jedoch bestimmte Domänen, die riskant sein können. Diese Domänen sind zwar nicht schädlich, können aber die Erstellung und/oder das Hosting schädlicher Subdomänen und Inhalte ermöglichen, die den Domäneninhabern unbekannt sind. Daher werden diese "grauen" Domänen

als riskante Domänen gekennzeichnet, da sie sowohl sichere als auch schädliche Subdomänen/Inhalte hosten können. Diese nicht kategorisierten Sites können beliebte Sites wie Filesharing-Dienste umfassen.

Greylist

Die Greylist ist eine Liste risikobehafteter grauer Domänen, die der intelligente Proxy abfängt und als Proxies identifiziert, um festzustellen, ob sie tatsächlich schädlich sind oder nicht. Es handelt sich um eine dynamische Liste von Grauzonen, die unser Sicherheitsteam überwacht.

Beispiele: "examplegrey.com" ist eine Domäne, die es Benutzern ermöglicht, ihre eigenen Inhalte zu hosten. Während die Domäne selbst sicher sein könnte, kann ein böswilliger Akteur schädliche Inhalte/Subdomänen wie "examplegrey.com/malicious" hosten. Gleichzeitig können auch andere nicht schädliche Inhalte als "examplegrey.com/safe" gehostet werden. Wenn Sie examplegrey.com in der Greylist lassen, können Sie die schädlichen Inhalte ("examplegrey.com/malicious") blockieren, während Sie den sicheren Inhalt ("examplegrey.com/safe") zulassen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.