Schnelle Prüfung von Nicht-Antworten-Umbrella Security-Anfragen

Inhalt

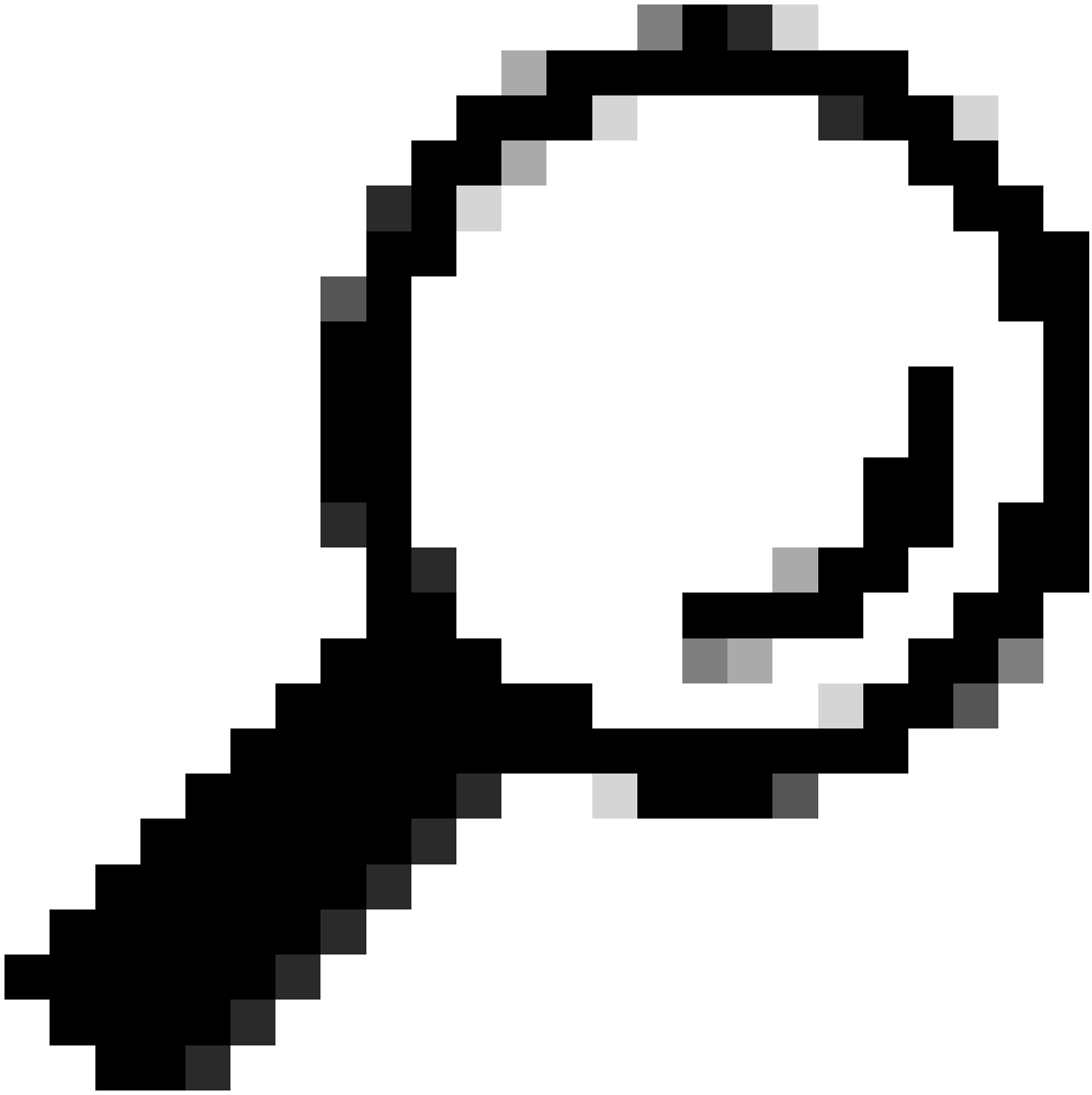
Einleitung

In diesem Dokument wird beschrieben, wie Umbrella Sicherheitsüberprüfungsanfragen schnell und ohne Antwort einreichen kann.

Überblick

Das Umbrella Support Team stellt eine neue Möglichkeit zur schnellen Bearbeitung der Einsendung von Sicherheitsüberprüfungen vor. Das menschliche Support-Team wird dabei komplett übersprungen. So sparen Sie bis zu zwei Tage Zeit.

Zu den unterstützten Einsendungen gehört die Anforderung, aus Sicherheitsgründen zu blockieren. Anfragen zum Hinzufügen neuer Sicherheitsblöcke können mehrere Domänen einreichen.



Tipp: Anfragen zur Freigabe einer Domain, zur Überprüfung von Fehlalarmen oder zur Überprüfung von Content-Kategorisierungen wie Pornografie werden derzeit nicht akzeptiert. Dies schließt die Kategorie "Geparkte Domänen" ein. Diese Anfragen müssen an die Talos Intelligence gesendet werden. Weitere Informationen finden Sie im Artikel "How To: Reichen Sie einen Talos Kategorisierungsantrag" ein, um Anweisungen zu erhalten.

Senden Sie eine E-Mail im festen Format an umbrella-research-noreply@cisco.com, um die Prüfung abzuschicken.

Falls dieses automatisierte System ausfällt - erstellen Sie bitte ein Support-Ticket bei Cisco Umbrella, und unser Support-Team bearbeitet Ihre Überprüfungsanfrage innerhalb der Standardreaktionszeit.

Übermittlungsformat

Antworten werden nicht in einem bestimmten Format eingereicht. Beiträge, die diesem Format nicht entsprechen, werden mit einer einzigen Antwort zurückgewiesen, die Hinweise darauf enthält, was zu klären ist. Weitere Antworten werden nicht akzeptiert. Einzelheiten zu möglichen Antworten finden Sie im nächsten Abschnitt unten. Nur an die Adresse umbrella-research-noreply@cisco.com gesendete Nachrichten werden verarbeitet.

Eingaben werden mit folgenden Formaten akzeptiert:

Postanschrift (anklickbarer Link): umbrella-research-noreply@cisco.com

Zentrale Domäne:

```
Domain: domain.comRequest: blockComments: Include background information or attribution and rationale h
```

Mehrere Domänen:

```
Domaincsv: domain.com, moredomains.com,moredomain.comRequest: blockComments: Include background informa
Comments: (Additional comments are supported - must start with comments:)Desired: malware
```

Oder

```
Domaincsv: domain.com, moredomains.com,moredomain.com
moredomains.com, evenmoredomains.com, stillmoredomains.com,
afewmoredomains.com
enddomains:Request: blockComments: Include background information or attribution and rationale here
more comments are supported (and optional). Include additional comment lines
here. End with
endcomments:Desired: malware
```

Felder:

Domäne: Dies ist die Domäne, die zur Überprüfung gesendet wird. Dies enthält nur den Domain-Namen selbst und nichts mehr in dieser Zeile.

Deaktivieren Sie die Domäne, wenn Sie befürchten, dass Filter für ausgehende E-Mails diese Übermittlung stören könnten. Folgende Formate werden akzeptiert:

domain[..]com

DomänenSVV: Dies ist die Liste der Domänen, die zur Überprüfung eingesendet werden. Wenn

mehrere Domänen übermittelt werden, gilt Folgendes für die Domäne: werden ignoriert. Dieses Feld wird nur für den Anforderungstypblock verwendet.

Anforderung: Handelt es sich hierbei um eine Übermittlung, in der gefordert wird, dass die Domäne einer zu sperrenden (blockierenden) Sicherheitsklassifizierung hinzugefügt wird?

Akzeptierter Wert für Anforderung:

- blockieren

Kommentare: Fügen Sie Hintergrundinformationen wie Phishing- oder Malware-Link-Details oder Informationen hinzu, die unser Forschungsteam zur Überprüfung der Domain verwendet.

Kommentare können auch De-Fanged-URLs enthalten, die mit der eingesendeten Domäne in Zusammenhang stehen, aber stellen Sie sicher, dass Sie auch das "" ändern. auch. Beispiele:

hxxp://domain[.]com/badstuff.exe

hxxps://domain[.]com/badstuff.exe

Gewünscht: Dieses Feld bestätigt das gewünschte Ergebnis der Einreichung. Geben Sie einen der akzeptierten Werte für die gewünschte Klassifizierung an.

Akzeptierte Werte für Gewünscht:

- Malware
- Phishing
- Botnet

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.