Soumettre des demandes d'examen de la sécurité sans réponse rapide

Table des matières

[Introduction](#)

[Aperçu](#)

[Format de soumission](#)

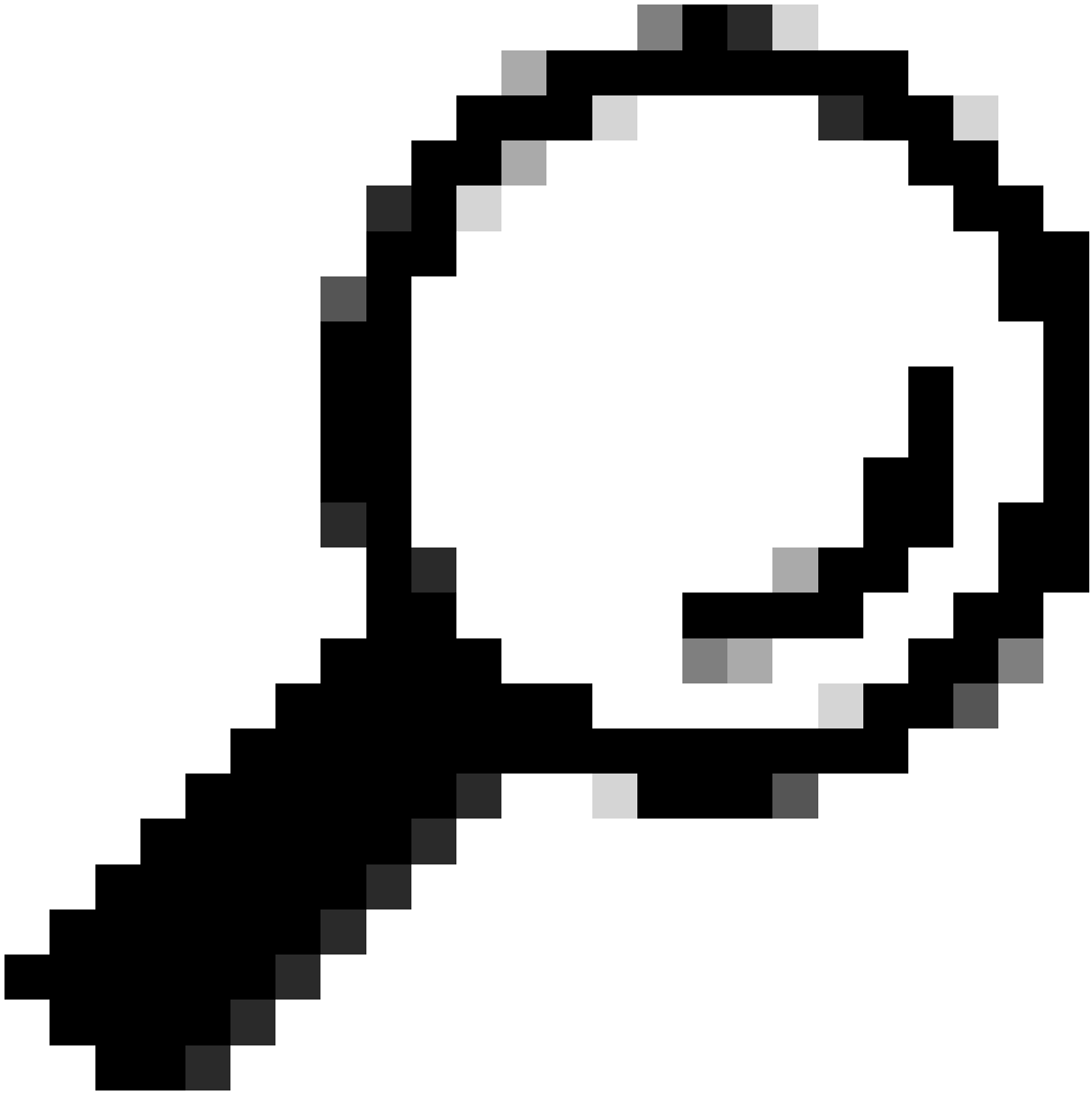
Introduction

Ce document décrit comment soumettre des demandes d'examen de sécurité Umbrella sans réponse rapide.

Aperçu

L'équipe d'assistance Umbrella propose une nouvelle méthode pour traiter rapidement les demandes d'examen de sécurité en ignorant complètement l'équipe d'assistance humaine, ce qui vous permet d'économiser jusqu'à quelques jours sur votre calendrier de traitement.

Les soumissions prises en charge comprennent une demande de blocage pour une raison de sécurité. Les envois de domaines multiples sont autorisés pour les demandes d'ajout de nouveaux blocs de sécurité.



Conseil : Les demandes de déblocage d'un domaine, de vérification des faux positifs ou de vérification de la catégorisation du contenu, comme la pornographie, ne sont pas acceptées pour le moment. Cela inclut la catégorie Domaines parqués. Ces demandes doivent être envoyées à Talos Intelligence. Voir l'article « Comment : Envoyer une demande de catégorisation Talos » pour obtenir des instructions.

Pour envoyer un message pour révision, envoyez un e-mail à l'adresse umbrella-research-noreply@cisco.com avec le format fixe.

En cas de défaillance de ce système automatisé, veuillez ouvrir un dossier d'assistance auprès de Cisco Umbrella et notre équipe d'assistance répond à votre demande d'examen dans le délai de réponse standard.

Format de soumission

Aucune réponse ne repose sur un format de présentation particulier. Les présentations qui ne respectent pas ce format sont rejetées avec une seule réponse et des directives sur ce qu'il faut résoudre. Aucune autre réponse n'est acceptée. Pour plus de détails sur les réponses possibles, voir la section suivante ci-dessous. Seuls les messages envoyés à l'adresse umbrella-research-noreply@cisco.com sont traités.

Les présentations sont acceptées dans les formats suivants :

Adresse postale (lien cliquable) : umbrella-research-noreply@cisco.com

Domaine unique :

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

Plusieurs domaines :

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

ou

```
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
```

Champs :

Domaine : Il s'agit du domaine envoyé pour révision. Il ne contient que le nom de domaine lui-même et rien d'autre sur cette ligne.

Désactivez le domaine si vous craignez que les filtres de messages sortants n'interfèrent avec cet envoi. Les formats acceptés sont les suivants :

domaine[.]com

Domainsv : Il s'agit de la liste des domaines soumis pour révision. Si vous envoyez plusieurs

domaines, le domaine : sont ignorés. Ce champ est uniquement utilisé avec le bloc de type de demande.

Demande : S'agit-il d'un envoi demandant l'ajout du domaine à une classification de sécurité à bloquer (blocage) ?

Valeur acceptée pour la demande :

- block

Commentaires: Inclure toute information de base, y compris les détails de lien de phishing ou de programme malveillant ou les informations que notre équipe de recherche utilise pour examiner le domaine.

Les commentaires peuvent également contenir des URL de suppression de la marque liée au domaine soumis, mais assurez-vous que vous modifiez également le « ». ainsi que. Exemples:

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

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

Souhaité : Ce champ confirme le résultat souhaité de la soumission. Indiquez l'une des valeurs acceptées pour la classification souhaitée.

Valeurs acceptées pour Souhaité :

- programme malveillant
- phishing
- réseau de zombies

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.