Sottomissione rapida richieste di revisione della sicurezza Umbrella senza risposta

Sommario

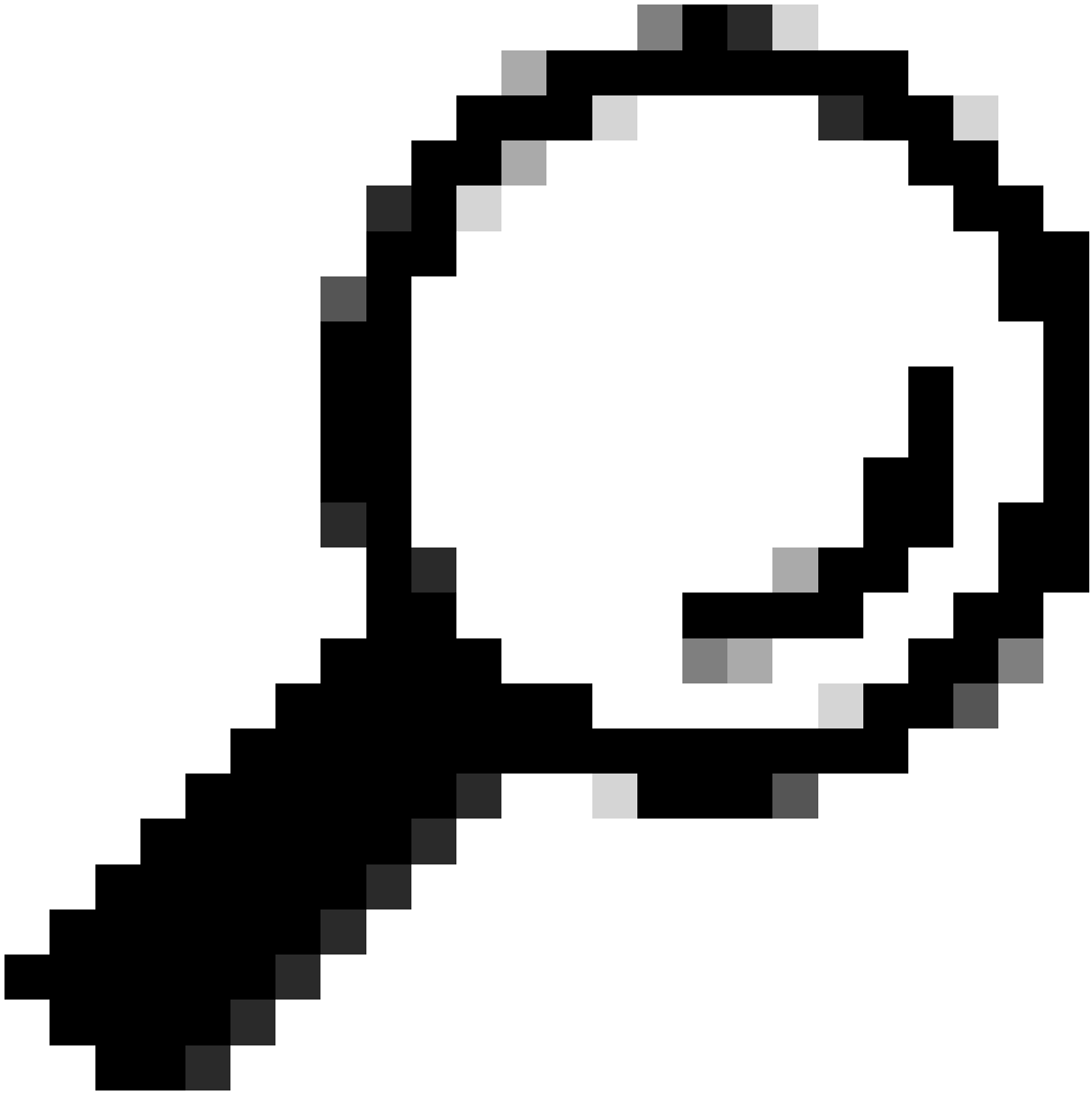
Introduzione

Questo documento descrive come inviare rapide richieste di revisione della sicurezza Umbrella senza risposta.

Panoramica

Il team di supporto Umbrella sta introducendo un nuovo modo per elaborare rapidamente la richiesta di revisione della sicurezza ignorando completamente il team di supporto umano, risparmiando fino a giorni di tempo dalla timeline del processo.

Gli invii supportati includono la richiesta di blocco per un motivo di sicurezza. Per le richieste di aggiunta di nuovi blocchi di protezione sono consentiti più invii di dominio.



Suggerimento: Le richieste di sbloccare un dominio, rivedere i falsi positivi o rivedere la categorizzazione dei contenuti come la pornografia non sono accettate in questo momento. È inclusa la categoria Domini in attesa. Queste richieste devono essere inviate all'intelligence Talos. Vedere l'articolo "Procedura: Invia una richiesta di categorizzazione Talos" per istruzioni.

Per inviare la revisione, inviare un'e-mail a umbrella-research-noreply@cisco.com con il formato fisso.

In caso di guasto di questo sistema automatizzato, aprite una richiesta di assistenza in Cisco Umbrella e il nostro team di assistenza risponde alla richiesta di revisione nei tempi di risposta standard.

Formato di invio

Nessun invio di risposta si basa su un formato di invio specifico. Gli inoltri che non soddisfano questo formato vengono rifiutati con una singola risposta contenente indicazioni su cosa risolvere. Non sono accettate altre risposte. Per ulteriori informazioni sulle possibili risposte, vedere la sezione successiva. Vengono elaborati solo i messaggi inviati all'indirizzo umbrella-research-noreply@cisco.com.

Gli invii vengono accettati nei seguenti formati:

Indirizzo (collegamento selezionabile): umbrella-research-noreply@cisco.com

Dominio singolo:

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

Più domini:

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

o

```
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
```

Campi:

Dominio: Dominio inviato per la revisione. Contiene solo il nome di dominio stesso e niente di più in questa riga.

Se si è preoccupati che i filtri della posta in uscita possano interferire con questo invio, disattivare la fang del dominio. Il formato accettato è il seguente:

dominio[.]com

Domini: Elenco dei domini inviati per la revisione. Se si inviano più domini, il dominio: vengono

ignorati. Questo campo viene utilizzato solo con il blocco del tipo di richiesta.

Richiesta: Si tratta di un inoltro che richiede l'aggiunta del dominio a una classificazione di protezione da bloccare (blocco)?

Valore accettato per la richiesta:

- Block (Blocca)

Commenti: Includere informazioni di base, inclusi i dettagli relativi al collegamento di phishing o malware o le informazioni utilizzate dal team di ricerca per esaminare il dominio.

I commenti possono contenere anche URL de-Fanged relativi al dominio inviato, ma accertarsi di modificare anche il "." anche. Esempi:

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

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

Desiderato: Questo campo conferma il risultato desiderato dell'invio. Fornire uno dei valori accettati per la classificazione desiderata.

Valori accettati per Desiderato:

- malware
- phishing
- botnet

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).