

Informazioni sulle nuove funzionalità di Umbrella Dashboard

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Nuove caratteristiche](#)

[Come trarre vantaggio da queste funzioni](#)

[Ispezione file](#)

[Verifica dell'ispezione dei file](#)

[Abilitazione del blocco degli URL negli elenchi di destinazione](#)

[Creazione di report](#)

[Invio del feedback Umbrella](#)

Introduzione

Questo documento descrive l'ispezione dei file e il blocco URL personalizzato tramite gli elenchi di destinazione in Umbrella Dashboard.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sul dashboard Umbrella.

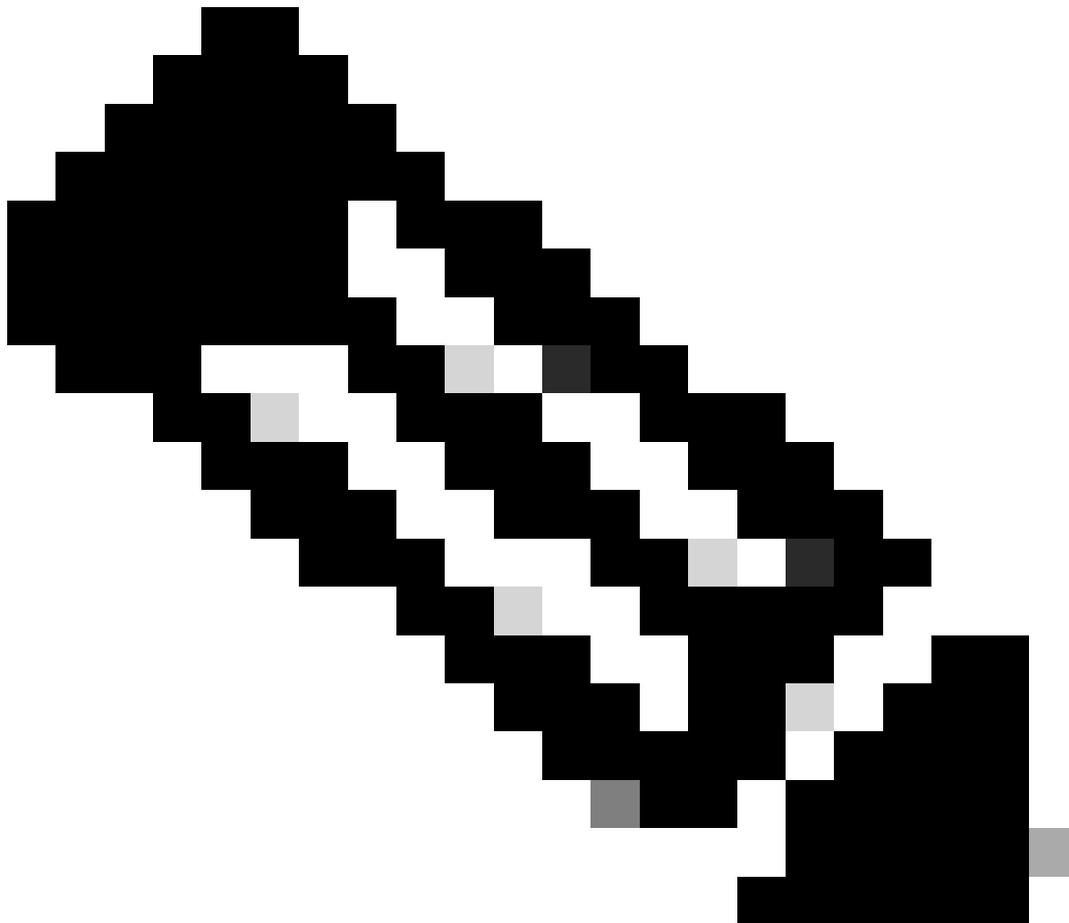
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nuove caratteristiche

Umbrella sta introducendo una nuova serie di funzionalità che migliorano le tue funzionalità. Questa modifica consente di visualizzare due nuove funzionalità nel dashboard in questo momento:

- L'ispezione dei file analizza i file scaricati dalle identità per verificare se contengono codice dannoso e, in caso affermativo, bloccarli.
- Gli URL bloccati personalizzati consentono di bloccare il proprio set di URL in un elenco di destinazione. In questo modo è possibile bloccare pagine specifiche senza bloccare interi domini.

Per trarre vantaggio da questa nuova funzionalità, è possibile utilizzare i report nuovi e aggiornati e una nuova esperienza nella creazione di policy. La funzionalità di ispezione dei file è una delle numerose release pianificate per il futuro, basate sull'avanzamento dell'infrastruttura dei proxy intelligenti per offrire una maggiore sicurezza basata sul cloud.



Nota: Queste funzionalità vengono implementate a piccoli incrementi per i nostri clienti e questi aggiornamenti sono a disponibilità limitata con l'avanzamento di Umbrella con questa release. Se nel dashboard è stato visualizzato un avviso relativo a queste funzionalità, significa che sono disponibili. Per maggiori informazioni su queste funzioni, contattare umbrella-support@cisco.com.

La funzionalità di ispezione dei file è disponibile solo per i clienti con i pacchetti Umbrella Insights o Umbrella Platform. [Ulteriori informazioni sui pacchetti](#) e qualsiasi domanda al rappresentante commerciale Cisco.

Come trarre vantaggio da queste funzioni

L'accesso a queste nuove funzionalità è disponibile in due modi: la procedura guidata consente di abilitare l'ispezione dei file dalla pagina di riepilogo e, attraverso gli elenchi di destinazione, è possibile aggiungere URL personalizzati agli elenchi di destinazione bloccati. Inoltre, il blocco personalizzato degli URL può essere gestito in modo specifico dalla pagina di gestione degli elenchi di destinazione.

Sul lato dei report, la sezione di navigazione report del dashboard Umbrella è stata aggiornata per consentire di trovare facilmente i report nuovi e aggiornati. Ulteriori informazioni in questo articolo su come attivare queste funzionalità e verificare alcuni report.

Ispezione file

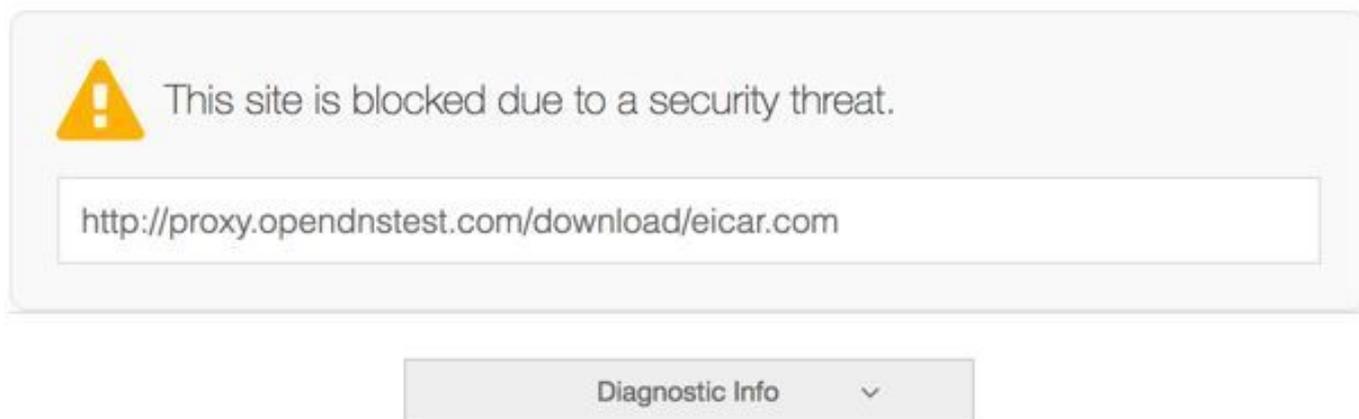
L'ispezione dei file è una funzione del proxy intelligente che ne estende l'ambito e le funzionalità aggiungendo la possibilità di analizzare i file per rilevare contenuti dannosi ospitati in domini sospetti. Un dominio sospetto non è considerato attendibile né dannoso.

Con la procedura guidata Umbrella policy, l'ispezione dei file è facile da implementare. Passare a Criteri > Elenco criteri ed espandere un criterio o selezionare l'icona + (Aggiungi) per creare un nuovo criterio. Nella Creazione guidata criteri, assicurarsi che Ispezione file sia abilitata nella pagina di riepilogo, oppure selezionare Ispezione file da un nuovo criterio dopo aver abilitato il proxy intelligente (in Impostazioni avanzate). [Per ulteriori informazioni, consultare la documentazione completa relativa a questa funzione.](#)

Verifica dell'ispezione dei file

Da un dispositivo registrato in un criterio con Ispezione file abilitata:

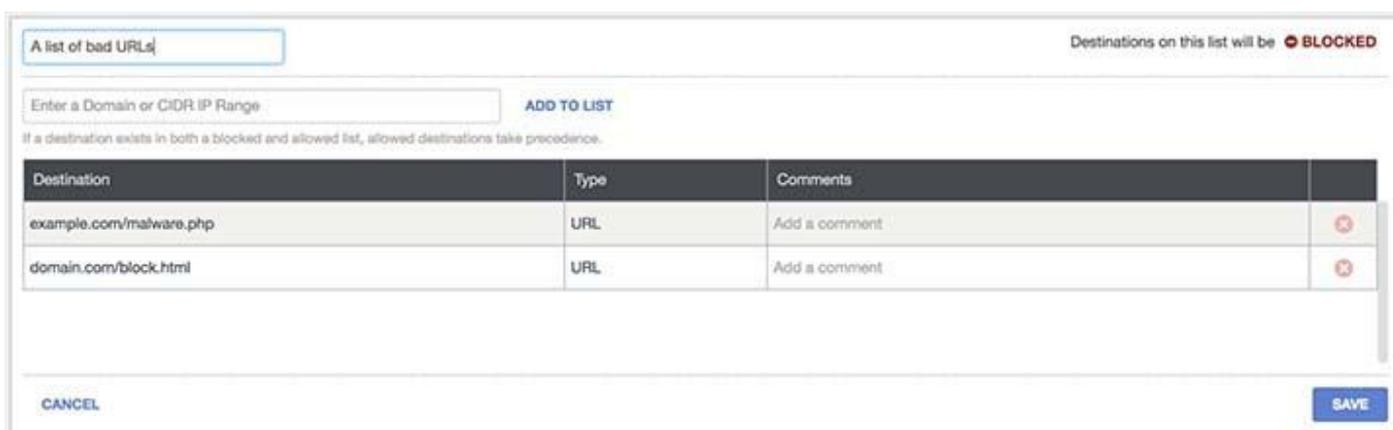
1. Selezionare <http://proxy.opendnstest.com/download/eicar.com>.
2. Viene visualizzata una pagina di blocco come questa schermata.



Pagina Umbrella bloccata

Abilitazione del blocco degli URL negli elenchi di destinazione

Per bloccare un URL, inseriscilo semplicemente in un elenco di destinazioni bloccate o crea un nuovo elenco di destinazioni bloccate solo per gli URL. A tale scopo, selezionare Criteri > Elenchi di destinazione, espandere un elenco di destinazione, aggiungere un URL e quindi selezionare Salva.



Destination	Type	Comments
example.com/malware.php	URL	Add a comment
domain.com/block.html	URL	Add a comment

Elenco destinazioni bloccate ombrello

[Per ulteriori informazioni, consultare la documentazione completa relativa a questa funzione.](#)

Affinché l'infrastruttura Umbrella possa ispezionare un URL per determinare se corrisponde a quelli definiti nell'elenco di destinazioni bloccate, è necessario disporre dei seguenti elementi:

- Il proxy intelligente e la decrittografia SSL devono essere abilitati come parte del criterio. Per

ulteriori informazioni, leggere i [documenti Umbrella](#).

- È necessario installare la CA radice Cisco Umbrella nei computer che utilizzano questo criterio. In questo modo viene garantito che anche le connessioni https siano filtrate. Per ulteriori informazioni, leggere i [documenti Umbrella](#).

È importante specificare correttamente un URL in modo che il contenuto del criterio corrisponda a quello a cui l'utente sta tentando di accedere (e che venga successivamente bloccato). Per ulteriori informazioni sugli URL che è possibile utilizzare o meno, consultare la [sezione sulle procedure relative all'elenco di destinazioni degli URL personalizzati](#).

Creazione di report

Umbrella ora ha dei report nuovi e migliorati:

- Rapporto Panoramica sulla sicurezza: fornisce un'istantanea di facile lettura dell'attività di rete tramite grafici e diagrammi. È possibile visualizzare rapidamente l'attività nelle identità e nel relativo traffico, illustrando le possibili cause dei problemi. Ulteriori informazioni [sono disponibili nei documenti Umbrella](#).
- Il rapporto Attività di sicurezza: evidenzia gli eventi di sicurezza contrassegnati, ma non necessariamente bloccati, da Umbrella threat intelligence. inclusi gli eventi di sicurezza filtrati tramite il proxy intelligente e l'ispezione dei file. Ulteriori informazioni [sono disponibili nei documenti Umbrella](#).
- Rapporto Ricerca attività: consente di trovare il risultato di ogni richiesta DNS, URL e IP dalle varie identità, ordinata in base alla data e all'ora decrescente. Questo report può elencare tutte le attività relative alla sicurezza in Umbrella per il periodo di tempo selezionato e consente di limitare la ricerca utilizzando i filtri per visualizzare solo ciò che si desidera vedere. Ulteriori informazioni [sono disponibili nei documenti Umbrella](#).

Anche queste relazioni sono facili da ottenere.

Invio del feedback Umbrella

A Umbrella piacerebbe sapere cosa ne pensi di queste nuove funzionalità. Qualsiasi domanda o commento avete, Umbrella vuole sentire da voi! Inviare il proprio feedback all'indirizzo umbrella-support@cisco.com e includere il maggior numero di dettagli possibile. Ad esempio, screenshot, il browser in uso, il sistema operativo e lo scenario in cui vengono utilizzate queste funzionalità.

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).