Dashboard Umbrella: Nuova funzionalità e ispezione dei file

Sommario

Introduzione

Bene, come posso sfruttare l'ispezione fuori sede?

- Abilitazione dell'ispezione dei file
- Verifica dell'ispezione dei file

Creazione di rapporti per l'ispezione dei file

Come posso farle sapere cosa penso?

Introduzione

Questo documento descrive il nuovo dashboard Umbrella.

Hai notato qualcosa di diverso nel tuo dashboard Umbrella? Beh, siamo lieti di annunciare che stiamo iniziando il processo di trasferimento delle persone verso una nuova serie di fantastiche caratteristiche dell'Umbrella. La prima funzionalità che stiamo introducendo è l'ispezione dei file. L'ispezione dei file consente di analizzare i file scaricati dall'utente per verificare se contengono codice dannoso e, in caso affermativo, di bloccarli.

Per consentire ai clienti di trarre vantaggio da questa nuova funzionalità, sono stati inoltre pubblicati nuovi e aggiornati report sulla sicurezza e una nuova esperienza nella creazione di criteri. Questa funzionalità è una delle numerose pianificate per le versioni future, create sulla base dell'avanzamento dell'infrastruttura dei proxy intelligenti per offrire agli utenti una sicurezza ancora maggiore basata su cloud.

Queste funzioni vengono implementate a piccoli incrementi per i nostri clienti. Se nel dashboard è visualizzato un avviso relativo a queste funzionalità, significa che sono disponibili. Per essere i primi a utilizzare 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. Fare clic qui per ulteriori informazioni sui pacchetti e contattare il rappresentante commerciale Cisco per qualsiasi domanda.

Bene, come posso sfruttare il controllo dei file?

La Creazione guidata criteri consente di attivare l'ispezione dei file dalla pagina di riepilogo o durante la creazione di un nuovo criterio.

Sul lato dei report, la sezione di navigazione dei report del dashboard Umbrella è stata aggiornata per consentire di trovare facilmente i report nuovi e aggiornati. Verrà ora illustrato come attivare la funzionalità e come estrarre alcuni report.

Abilitazione dell'ispezione dei 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 è noto come dannoso ed è incluso nella lista grigia dei domini.

Con la procedura guidata Umbrella policy, l'ispezione dei file è facile da implementare. È sufficiente selezionare Criteri > Elenco criteri ed espandere un criterio oppure fare clic sull'icona + (Aggiungi) per creare un nuovo criterio. Nella Creazione guidata criteri, assicurarsi che l'opzione Controllo file sia abilitata nella pagina di riepilogo oppure, in base a un nuovo criterio, controllare Controlla file dopo aver abilitato il proxy intelligente (in Impostazioni avanzate). La documentazione completa relativa a questa funzione è disponibile qui: https://docs.umbrella.com/deployment-umbrella/docs/file-inspection

Per sfruttare al meglio questa funzionalità, è consigliabile abilitare la decrittografia SSL.

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 la seguente:

Creazione di rapporti per l'ispezione dei file

Per dare maggiore visibilità a ciò che è stato bloccato (così come a quando, perché e come),

abbiamo aggiornato alcuni report in Umbrella, tra cui un report aggiornato sulle attività di sicurezza:

- Report Panoramica sulla protezione
  Fornisce un'istantanea di facile lettura dell'attività di rete tramite grafici e diagrammi. Puoi vedere rapidamente cosa sta succedendo con le tue identità e il loro traffico, illustrando dove potrebbero essersi verificati dei problemi. Ulteriori informazioni qui.

- Report attività di protezione
  Evidenzia gli eventi relativi alla sicurezza contrassegnati, ma non necessariamente bloccati, dall'intelligence delle minacce Umbrella. inclusi gli eventi di sicurezza filtrati tramite il proxy intelligente e l'ispezione dei file. Questa relazione è particolarmente importante per mostrare cosa è stato bloccato, perché e come. Ulteriori informazioni qui.

- Report Ricerca attività
  Consente di trovare il risultato di ogni richiesta DNS, URL e IP dalle varie identità, ordinata in base a data e ora decrescente. Questo report elenca tutte le attività in Umbrella per il periodo di tempo selezionato e, utilizzando i filtri, è possibile limitare la ricerca per vedere solo ciò che si desidera vedere. Ulteriori informazioni qui.

E grazie alla navigazione aggiornata, è facile accedere anche a questi report! È sufficiente espandere il riquadro del menu a sinistra e passare a qualsiasi report direttamente da qualsiasi altro punto del dashboard.

Come posso farle sapere cosa penso?

Vorremmo conoscere la tua opinione sulle nuove caratteristiche. Per qualsiasi domanda o commento, ti invitiamo a rispondere! 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).