Integrazione di ZeroFOX con Umbrella

Sommario

Introduzione

Questo documento descrive come integrare ZeroFOX Enterprise con Umbrella in modo che gli eventi di sicurezza possano essere applicati ai client protetti da Umbrella.

Panoramica di ZeroFOX Enterprise e Cisco Umbrella Integration

Integrando ZeroFOX Enterprise con Cisco Umbrella, gli addetti alla sicurezza e gli amministratori possono estendere la protezione contro le minacce basate sui social media di oggi a notebook, tablet o telefoni in roaming, fornendo al contempo un altro livello di imposizione a una rete aziendale distribuita.

Integrazione di Cisco Umbrella e ZeroFox: Come funziona?

ZeroFOX Enterprise invia a Cisco Umbrella per l'applicazione globale tutte le minacce che trova, come le cyber-minacce basate sui social media, tra cui malware mirato, phishing, social engineering, impersonazioni e altre attività fraudolente o dannose.

Umbrella convalida quindi la minaccia per garantire che possa essere aggiunta a una policy. Se

viene confermato che le informazioni di ZeroFOX rappresentano una minaccia, l'indirizzo di dominio viene aggiunto all'Elenco destinazioni ZeroFOX come parte di un'impostazione di protezione che può essere applicata a qualsiasi criterio Umbrella. Tale criterio viene applicato immediatamente a qualsiasi richiesta effettuata dai dispositivi assegnati a tale criterio.

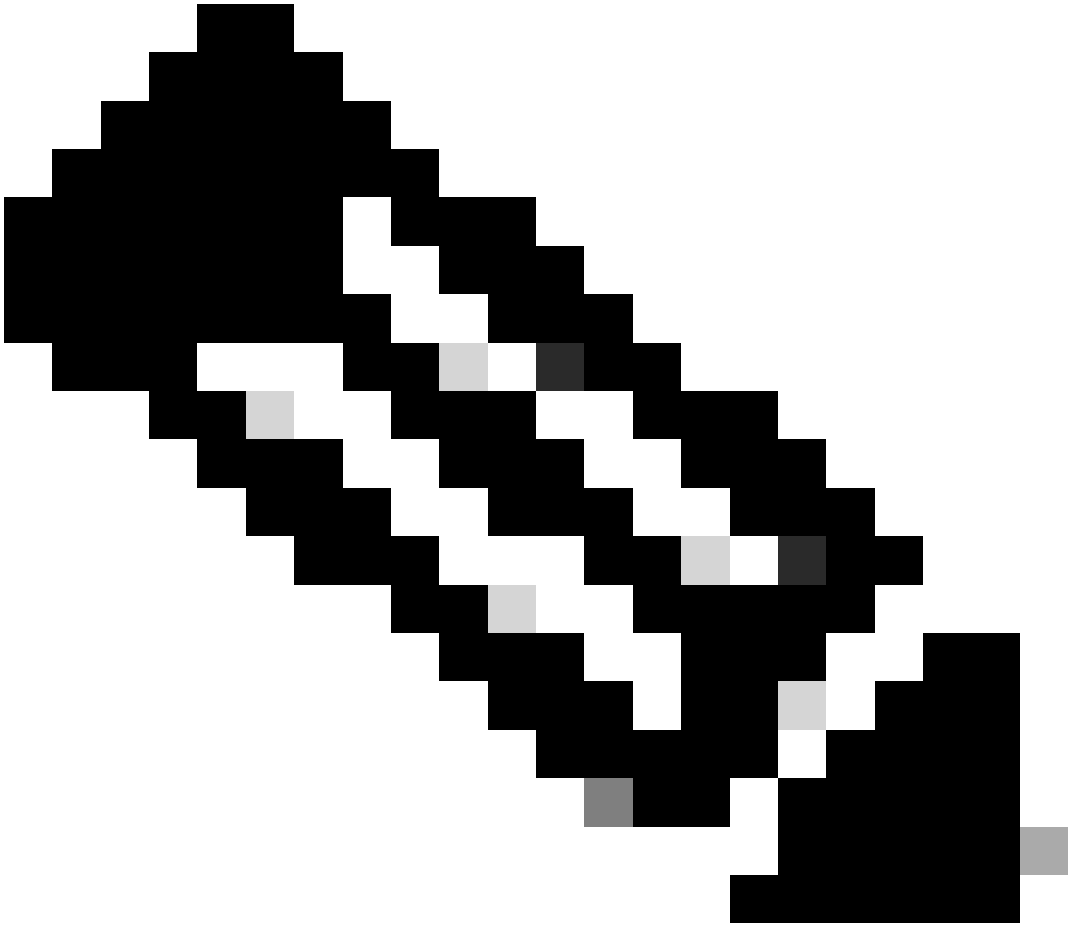
In futuro, Cisco Umbrella analizza automaticamente gli avvisi ZeroFOX e aggiunge siti dannosi all'Elenco destinazioni ZeroFOX, estendendo l'intelligence ZeroFOX a tutti gli utenti e i dispositivi remoti e fornendo un altro livello di imposizione alla rete aziendale.

A tale scopo, è sufficiente eseguire le seguenti semplici operazioni di configurazione:

1. Abilitare l'integrazione in Umbrella per generare un token API.
2. Incollare il token API nell'account ZeroFOX.
3. Impostare ZeroFOX in modo che venga bloccato nelle impostazioni di protezione per i criteri desiderati

Prerequisiti

- Diritti amministrativi di ZeroFOX Enterprise
- Diritti amministrativi dashboard ombrello
- Il dashboard Umbrella deve avere l'integrazione ZeroFOX abilitata



Nota: L'integrazione ZeroFOX è inclusa solo nel pacchetto Umbrella Platform. Se non disponi del pacchetto della piattaforma e desideri un'integrazione ZeroFOX, contatta il tuo rappresentante Cisco Umbrella. Se disponete del pacchetto della piattaforma ma non vedete ZeroFOX come un'integrazione per il vostro dashboard, contattate il supporto Umbrella.

Importante: Nonostante Umbrella faccia del suo meglio per convalidare e consentire i domini che sono noti per essere generalmente sicuri (ad esempio, Google e Salesforce), per evitare interruzioni indesiderate, si consiglia di aggiungere qualsiasi dominio che non si desidera bloccare all'Elenco globale dei domini consentiti o ad altri elenchi di destinazione in base ai propri criteri.

Alcuni esempi:

- Home page dell'organizzazione. Ad esempio, mydomain.com.
- Domini che rappresentano i servizi forniti e che possono avere record interni ed esterni. Ad esempio, mail.myservicedomain.com e portal.myotherservicedomain.com.
- Le applicazioni cloud meno note dipendono in modo significativo dal fatto che Umbrella non

può essere a conoscenza o includere nella convalida automatica dei domini. Ad esempio, localcloudservice.com.

L'elenco globale degli indirizzi consentiti si trova in Policies > Destination Lists in Umbrella. Per ulteriori informazioni, vedere la documentazione: Gestisci elenchi di destinazione

Passaggio 1: Generazione token API e script Umbrella

Per comunicare con l'appliance ThreatQ, è necessario innanzitutto individuare l'URL univoco in Umbrella.

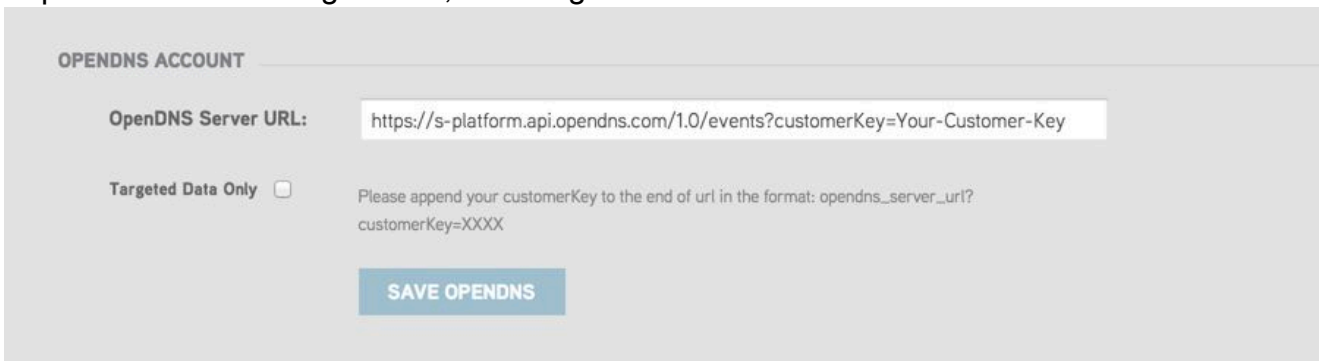
1. Accedere al dashboard Umbrella come amministratore, selezionare Impostazioni > Integrazioni e fare clic su "ZeroFOX" nella tabella per espanderlo.
2. Selezionare Attiva, quindi fare clic su Salva. In questo modo viene generato un URL univoco con il codice cliente.

Poiché l'URL è necessario in un secondo momento durante la configurazione di ZeroFOX, copiare l'URL e accedere al dashboard ThreatQ.

Passaggio 2: Impostazione del dashboard aziendale ZeroFOX per inviare informazioni a Umbrella

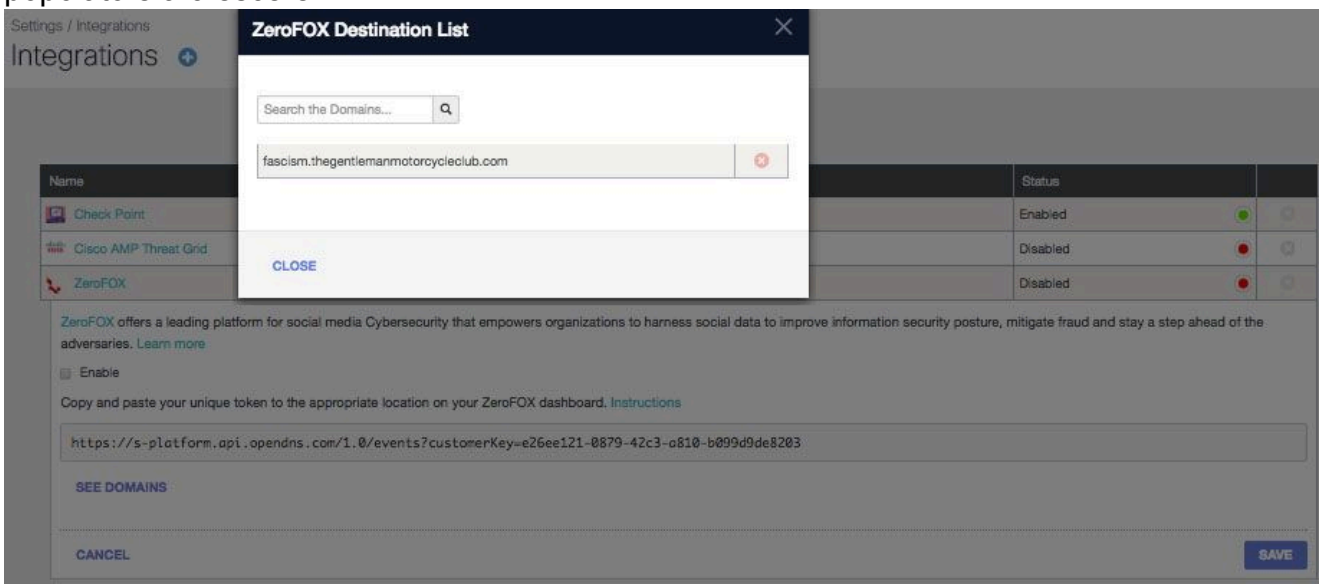
Il passaggio successivo consiste nell'aggiungere l'URL copiato nel passaggio 1 al dashboard ZeroFOX.

1. Fate clic sull'icona a forma di ingranaggio nel quadro comandi di Zerofox, quindi selezionate Impostazioni account.
2. Scorrere l'elenco di integrazione fino a visualizzare le informazioni sull'account OpenDNS e incollare l'URL da Umbrella nel campo URL server OpenDNS.
3. Al primo avvio dell'integrazione, si consiglia di selezionare Solo dati di destinazione.



Passaggio 3: Imposta eventi ZeroFOX da bloccare in Umbrella

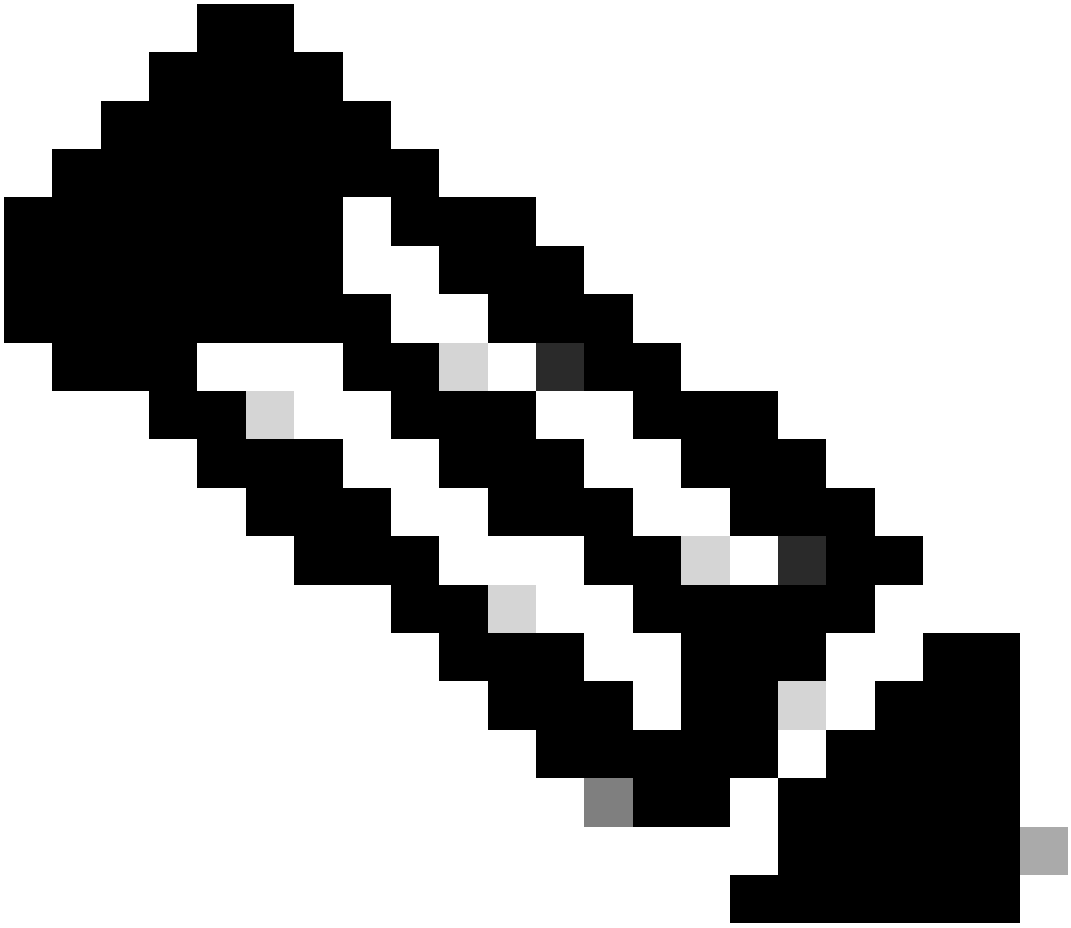
1. Accedere di nuovo al dashboard Umbrella come amministratore.
2. Passare a Impostazioni > Integrazioni e fare clic su "ZeroFOX" nella tabella per espanderla.
3. Fare clic su Vedere domini.
   In questo modo si espande un elenco di domini che include le ultime ore di eventi dell'account ZeroFOX. Da quel momento in poi, un elenco ricercabile inizia a essere popolato e a crescere.



Il passo successivo è osservare e controllare gli eventi aggiunti alla nuova categoria di sicurezza ZeroFOX.

Osservazione degli eventi aggiunti alla categoria di protezione ZeroFOX in modalità di controllo

Gli eventi di ZeroFOX Enterprise iniziano a popolare un elenco di destinazioni specifico che può essere applicato ai criteri come categoria di protezione ZeroFOX. Per impostazione predefinita, l'elenco di destinazione e la categoria di protezione sono in modalità di controllo e non vengono applicati ad alcun criterio e non comportano modifiche ai criteri Umbrella esistenti.



Nota: La modalità di controllo può essere attivata per il tempo necessario in base al profilo di distribuzione e alla configurazione di rete.

Esamina elenco di destinazione

Puoi controllare l'Elenco destinazioni di ZeroFox in qualsiasi momento.

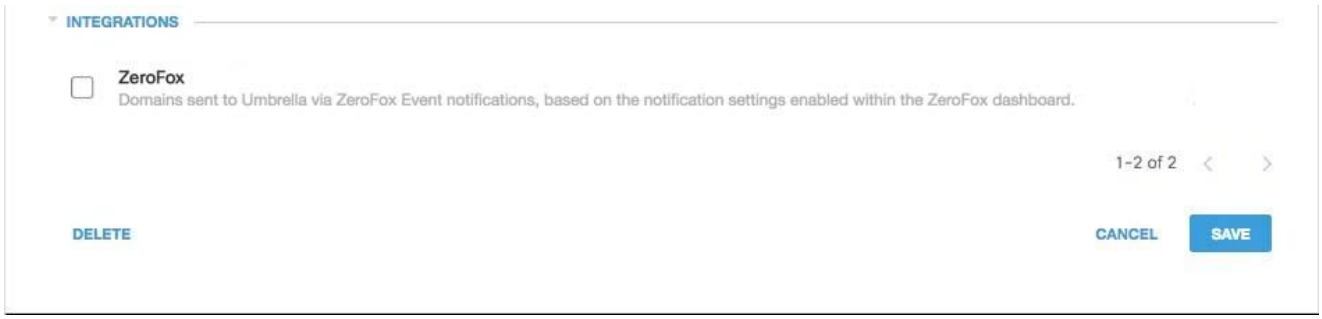
1. Passare a Impostazioni > Integrazioni.
2. Espandere "ZeroFOX" nella tabella e fare clic su Vedere Domini.

Rivedere le impostazioni di protezione per un criterio

È possibile rivedere in qualsiasi momento le impostazioni di protezione che possono essere attivate per un criterio.

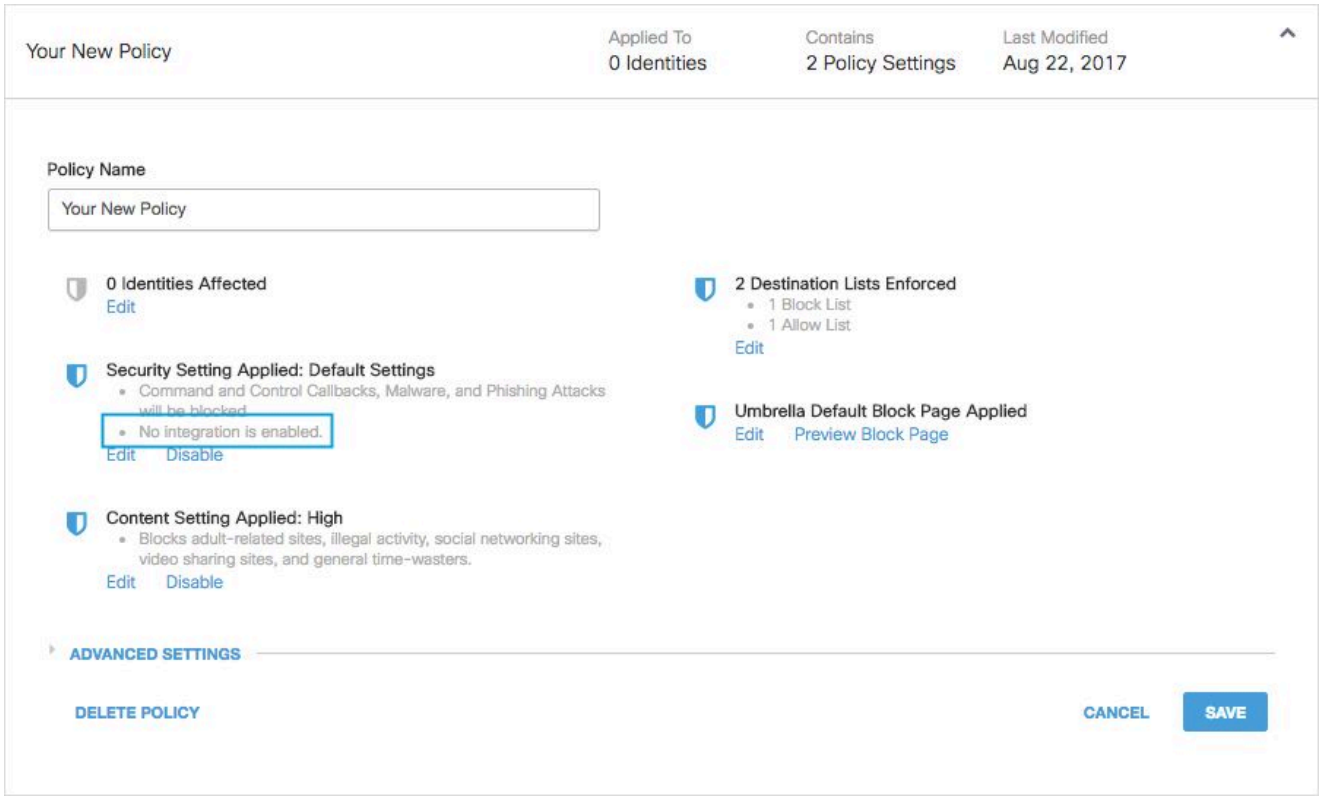
1. Passare a Criteri > Impostazioni protezione.
2. Fare clic su un'impostazione di protezione nella tabella per espanderla e scorrere fino a

Integrations per individuare l'impostazione ZeroFOX.



115014041606

È inoltre possibile esaminare le informazioni sull'integrazione tramite la pagina Riepilogo impostazioni di protezione.

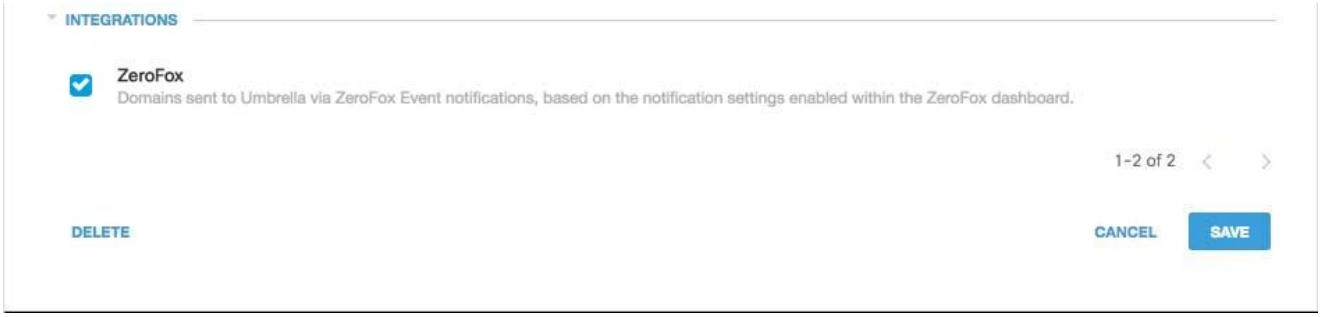


25464154913556

Applicazione delle impostazioni di protezione ZeroFOX in modalità di blocco a un criterio per client gestiti

Quando sei pronto a far applicare queste minacce di sicurezza aggiuntive da parte dei client gestiti da Umbrella, è sufficiente modificare l'impostazione di sicurezza su un criterio esistente, o creare un nuovo criterio che si trovi più in alto rispetto al tuo criterio predefinito per assicurarti che venga applicato prima.

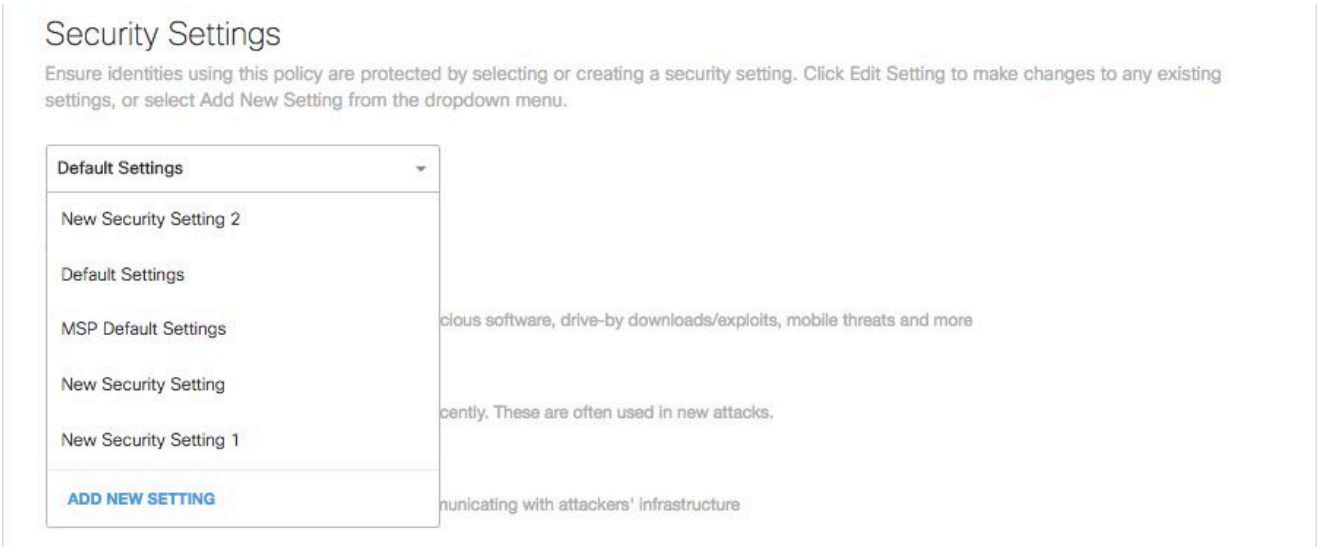
1. Passare a Policy > Security Settings (Policy > Impostazioni di protezione) e in Integrations (Integrazioni), selezionare ZeroFOX e fare clic su Save (Salva).



115014042806

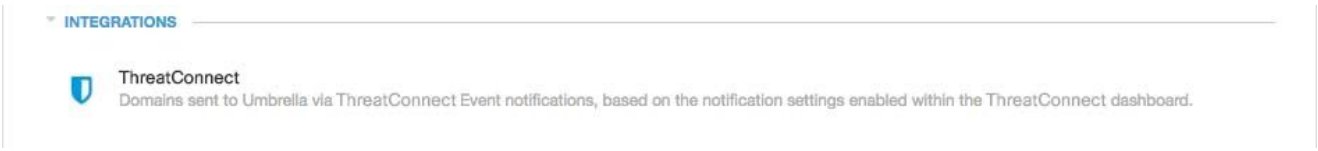
Successivamente, nella Creazione guidata criteri, aggiungere un'impostazione di protezione al criterio che si sta modificando:

1. Passare a Criteri > Elenco criteri.
2. Espandere un criterio e fare clic su Modifica in Impostazioni di protezione applicate.
3. Nella casella di riepilogo a discesa Impostazioni protezione, selezionare un'impostazione di protezione che includa l'impostazione ThreatConnect.



25464147943700

L'icona dello scudo sotto Integrations viene aggiornata in blu.



25464147957652

4. Fare clic su Imposta e ritorna.

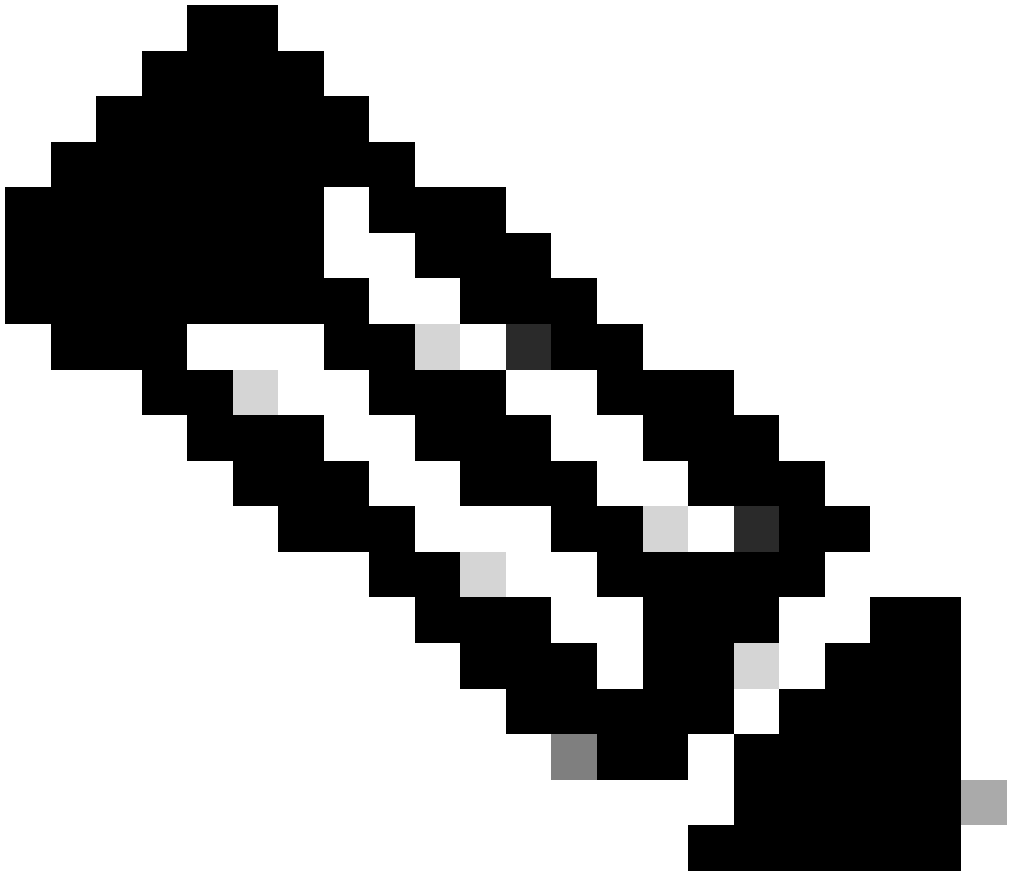
I domini ZeroFOX contenuti nell'impostazione di protezione per ZeroFOX vengono bloccati per le identità che utilizzano tale criterio.

Segnalazione degli eventi ZeroFOX in Umbrella

Segnalazione di eventi di protezione ZeroFOX

L'Elenco destinazioni ZeroFOX è una delle categorie di protezione per le quali è possibile creare un report. La maggior parte o tutti i report utilizzano le categorie di protezione come filtro. Ad esempio, è possibile filtrare le categorie di protezione per visualizzare solo le attività correlate a ZeroFOX.

1. Passare a Report > Ricerca attività e in Categorie di sicurezza selezionare ZeroFOX per filtrare il report in modo da visualizzare solo la categoria di sicurezza per ZeroFOX.



Nota: Se l'integrazione ZeroFOX è disattivata, non viene visualizzata nel filtro Categorie di sicurezza.

115014043046

2. Fare clic su Apply (Applica).

Segnalazione dell'aggiunta di domini all'elenco di destinazione ZeroFOX

Il registro di controllo di Umbrella Admin include gli eventi dell'account ZeroFOX quando aggiunge domini all'elenco di destinazione.

Il registro di controllo di Umbrella Admin è disponibile in Reporting > Registro di controllo di amministrazione. Per segnalare quando un dominio è stato aggiunto, filtrare per includere solo le modifiche ZeroFOX applicando un filtro a Identities & Settings per l'Elenco destinazioni ZeroFox.

Una volta eseguito il report, verrà visualizzato un elenco delle modifiche apportate quando è stato aggiunto l'Elenco destinazioni ZeroFOX dall'integrazione.

Gestione di rilevamenti indesiderati o falsi positivi

Gestione di un elenco di indirizzi consentiti per il rilevamento di elementi indesiderati

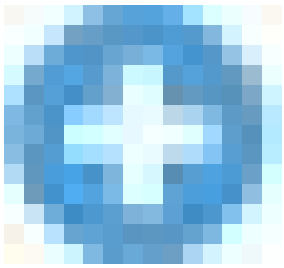
Anche se improbabile, è possibile che i domini aggiunti automaticamente da ZeroFOX possano attivare un blocco indesiderato che impedirebbe agli utenti di accedere a determinati siti web. In una situazione come questa, si consiglia di aggiungere i domini a un elenco degli indirizzi consentiti, che ha la precedenza su tutti gli altri tipi di elenchi di blocco, incluse le impostazioni di protezione. Un elenco Consenti ha la precedenza su un elenco Blocca quando un dominio è presente in entrambi.

Ci sono due ragioni per cui questo approccio è preferibile. In primo luogo, nel caso in cui l'accessorio ZeroFOX dovesse aggiungere nuovamente il dominio dopo la rimozione, l'elenco degli oggetti autorizzati impedisce che ciò provochi ulteriori problemi. In secondo luogo, l'elenco degli accessi mostra una registrazione cronologica di domini problematici che possono essere utilizzati per le indagini forensi o le relazioni di audit.

Per impostazione predefinita, esiste un elenco di indirizzi consentiti globale che viene applicato a tutti i criteri. L'aggiunta di un dominio all'elenco globale degli indirizzi consentiti comporta che il dominio sia consentito in tutti i criteri.

Se l'impostazione di protezione ZeroFOX in modalità blocco viene applicata solo a un sottoinsieme delle identità Umbrella gestite, ad esempio solo a computer mobili e dispositivi mobili mobili, è possibile creare un elenco Consenti specifico per tali identità o criteri.

Per creare un elenco Consenti:

1. Selezionare Criteri > Elenchi di destinazione, quindi fare clic sul pulsante 

   25464155856404

   Aggiungi icona.
2. Selezionare Consenti, quindi aggiungere il dominio all'elenco.
3. Fare clic su Save (Salva).

Una volta salvato l'elenco di destinazione, è possibile aggiungerlo a un criterio esistente che copre i client interessati dal blocco indesiderato.

Eliminazione di domini dall'elenco di destinazione ZeroFOX

Esiste un

(Elimina) accanto a ciascun nome di dominio nell'Elenco destinazioni ZeroFOX. L'eliminazione dei domini consente di pulire l'Elenco destinazioni ZeroFOX in caso di rilevamento indesiderato.

Tuttavia, l'eliminazione non è permanente se ZeroFOX rinvia il dominio ad Umbrella.

Per eliminare un dominio:

1. Passare a Impostazioni > Integrazioni, quindi fare clic su "ZeroFOX" per espanderlo.
2. Fare clic su Vedere domini.
3. Cercare il nome di dominio da eliminare.
4. Fare clic sull'icona Elimina.

5. Fare clic su Close (Chiudi).
6. Fare clic su Save (Salva).

Nel caso di un rilevamento indesiderato o di un falso positivo, si consiglia di creare immediatamente un elenco degli accessi consentiti in Umbrella e quindi di correggere il falso positivo in ZeroFOX. In seguito, è possibile rimuovere il dominio dall'Elenco destinazioni ZeroFOX.

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).