Integrazione di ThreatConnect con Umbrella

Sommario

Introduzione

Questo documento descrive come integrare ThreatConnect con Cisco Umbrella.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Un dashboard ThreatConnect con accesso per aggiornare l'URL per le integrazioni
- Diritti amministrativi dashboard ombrello
- Per il dashboard Umbrella è necessario abilitare l'integrazione ThreatConnect.

Componenti usati

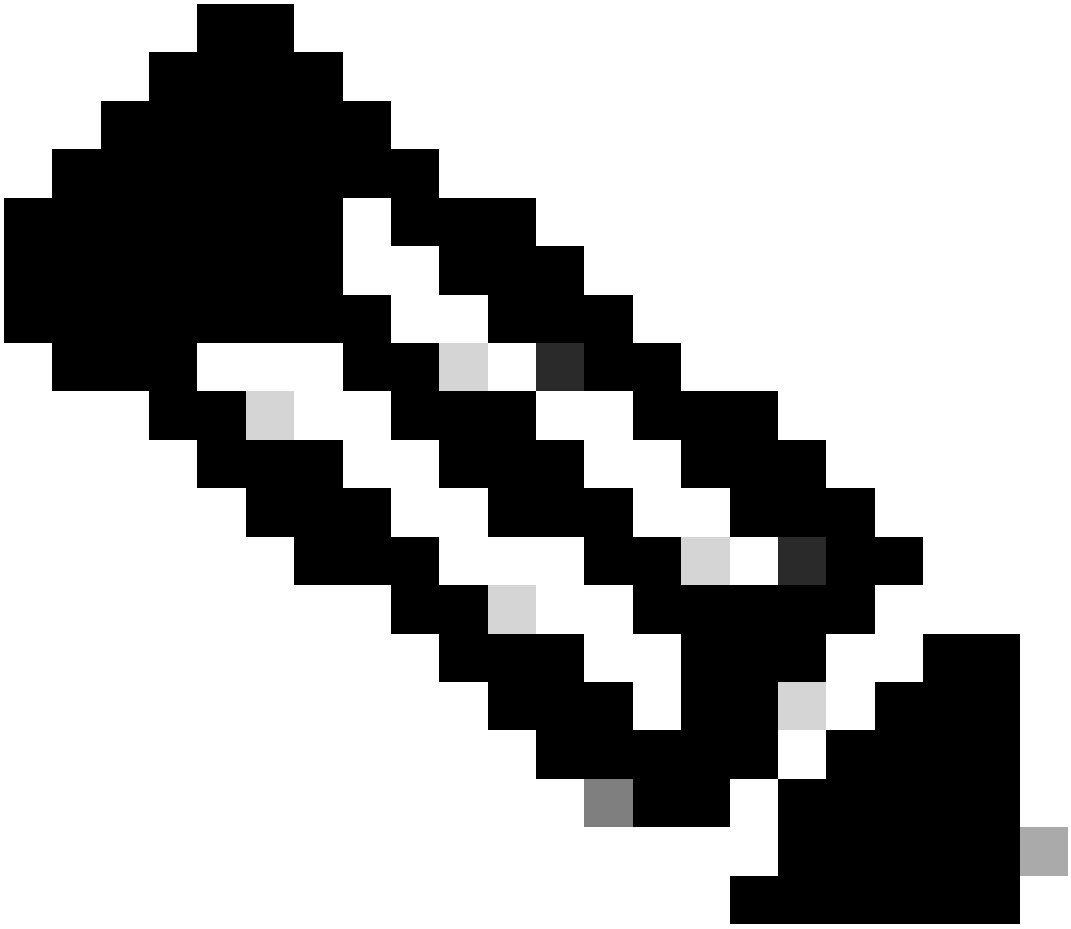
Le informazioni fornite in questo documento si basano su Cisco Umbrella.

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.

Panoramica sull'integrazione di ThreatConnect e Cisco Umbrella

Grazie all'integrazione di ThreatConnect con Cisco Umbrella, gli addetti alla sicurezza e gli amministratori sono ora in grado di estendere la protezione dalle minacce avanzate a notebook, tablet o telefoni in roaming, fornendo inoltre un altro livello di imposizione a una rete aziendale distribuita.

Questa guida illustra come configurare ThreatConnect per comunicare con Umbrella in modo che gli eventi di sicurezza del suggerimento ThreatConnect siano integrati in criteri che possono essere applicati ai client protetti da Cisco Umbrella.



Nota: L'integrazione ThreatConnect è inclusa solo in un determinato pacchetto Cisco

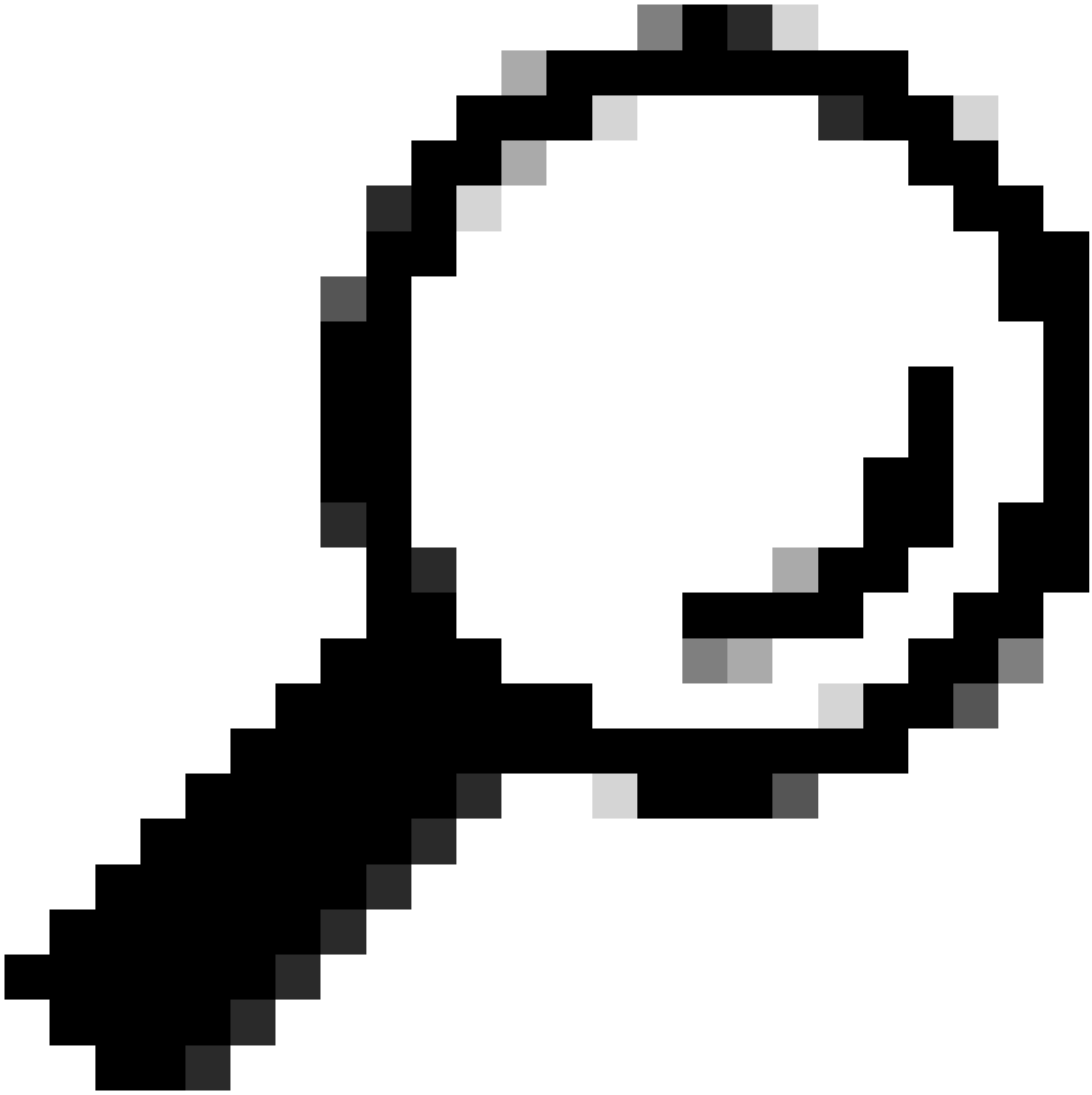
---

Umbrella. Se non disponi di un pacchetto che include questa integrazione, contatta il tuo rappresentante Cisco Umbrella per ottenerlo. Se disponi del pacchetto corretto ma non vedi ThreatConnect come integrazione per il tuo dashboard, contatta il supporto Cisco Umbrella.

La piattaforma ThreatConnect invia prima a Umbrella la Cyber Threat Intelligence che ha trovato, come i domini che ospitano malware, comandi e controllo per botnet o siti di phishing.

Umbrella convalida quindi la minaccia per garantire che possa essere aggiunta a una policy. Se le informazioni di ThreatConnect sono confermate come minacce, l'indirizzo di dominio viene aggiunto all'elenco destinazioni ThreatConnect come parte di un'impostazione di sicurezza che può essere applicata a qualsiasi criterio Umbrella. Questo criterio viene applicato immediatamente a tutte le richieste provenienti dai dispositivi che utilizzano criteri con l'elenco di destinazione ThreatConnect.

In futuro, Umbrella analizza automaticamente gli avvisi ThreatConnect e aggiunge siti dannosi all'elenco destinazioni ThreatConnect, estendendo la protezione ThreatConnect a tutti gli utenti e i dispositivi remoti e fornendo un altro livello di imposizione alla rete aziendale.



Suggerimento: 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 qualsiasi interruzione indesiderata, Umbrella suggerisce di aggiungere qualsiasi dominio che non si vuole essere bloccati all'Elenco globale dei domini consentiti o ad altri elenchi di destinazione secondo i vostri 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.
- Applicazioni cloud meno note da cui l'utente dipende in modo significativo, ma che Umbrella non è a conoscenza o non include nella convalida automatica del dominio. Ad esempio, localcloudservice.com.

L'elenco globale degli indirizzi consentiti si trova in Criteri > Elenchi di destinazione in

Umbrella. Per ulteriori informazioni, vedere la documentazione: Gestisci elenchi di destinazione

Configura il dashboard ombrello per la ricezione di eventi da ThreatConnect

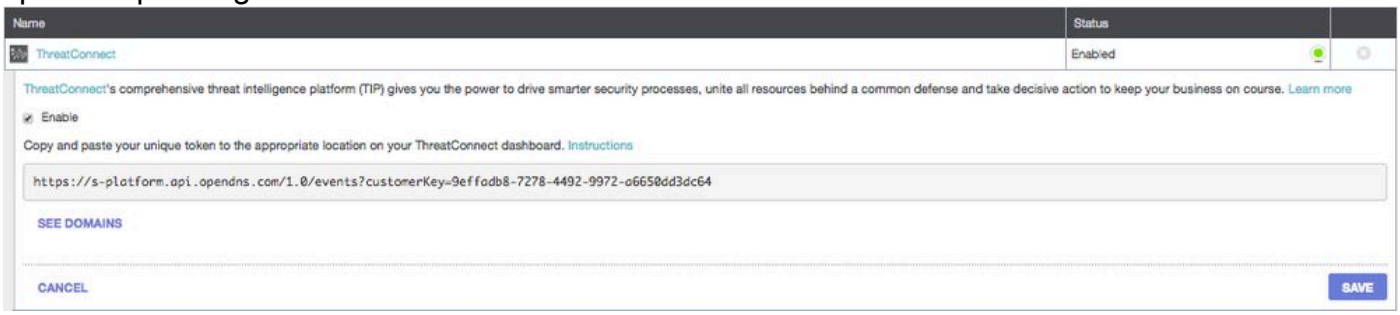
Per comunicare con l'appliance ThreatQ, iniziare a cercare il proprio URL univoco in Umbrella:

1. Accedi al dashboard Umbrella.

2. Passare a Criteri > Integrazioni.

3. Nella tabella, selezionare ThreatConnect per espanderla.

4. Selezionare Abilita, quindi selezionare Salva. In questo modo viene generato un URL univoco e specifico per l'organizzazione in Umbrella.



L'URL è necessario più avanti in questo articolo quando si configura ThreatConnect per l'invio di dati a Umbrella.

Configura ThreatConnect per comunicare con Umbrella

Per iniziare a inviare traffico da ThreatConnect a Umbrella, è necessario configurare ThreatConnect con le informazioni sull'URL generate nella prima sezione di questo articolo:

1. Accedere al dashboard ThreatConnect.

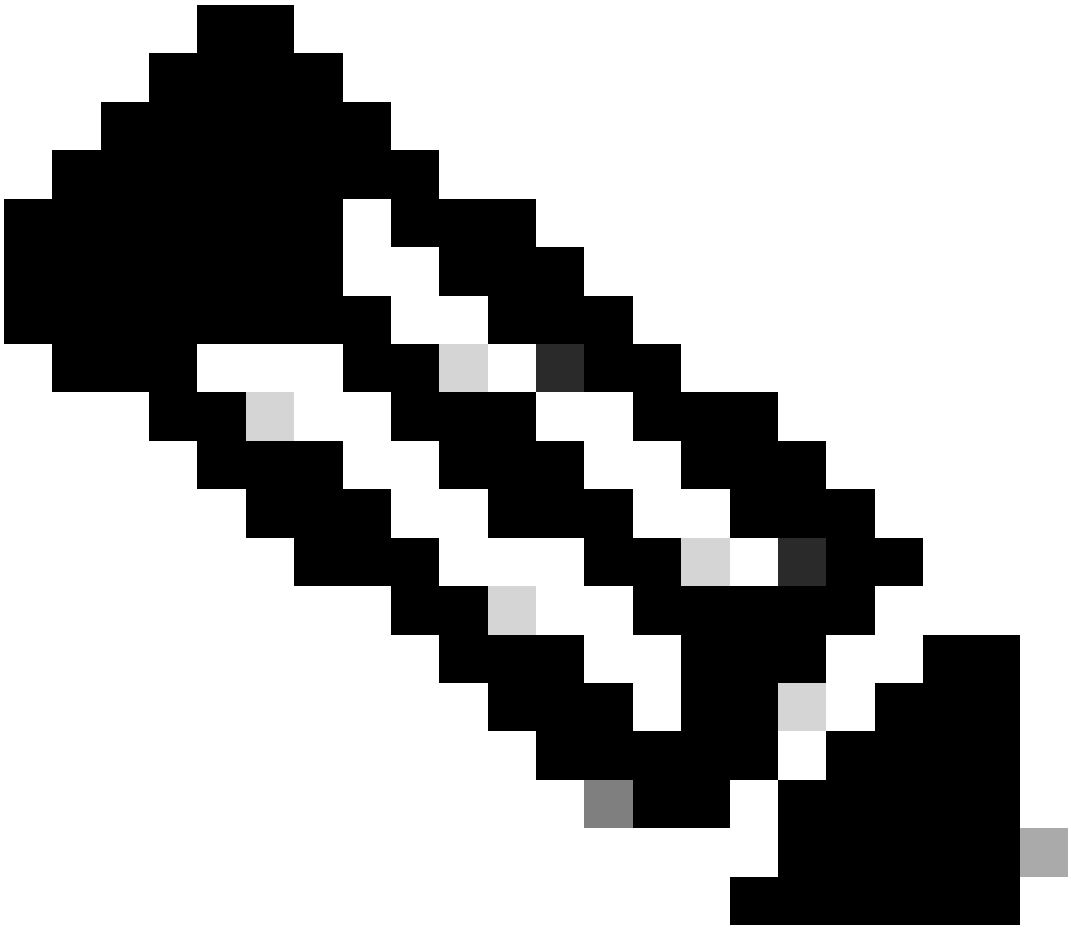
2. Aggiungi l'URL nell'area appropriata per connetterti con Umbrella.

Le istruzioni esatte variano e Umbrella consiglia di contattare il supporto ThreatConnect se non si è certi di come o dove configurare le integrazioni API all'interno di ThreatConnect.

Osservazione degli eventi aggiunti alla categoria di sicurezza ThreatConnect in modalità di controllo

Con il tempo, gli eventi del dashboard ThreatConnect possono iniziare a popolare un elenco di destinazioni specifico che può essere applicato ai criteri come categoria di sicurezza ThreatConnect. Per impostazione predefinita, l'elenco di destinazione e la categoria di protezione

sono in modalità di controllo, ovvero non vengono applicati ai criteri e non comportano modifiche ai criteri Umbrella esistenti.



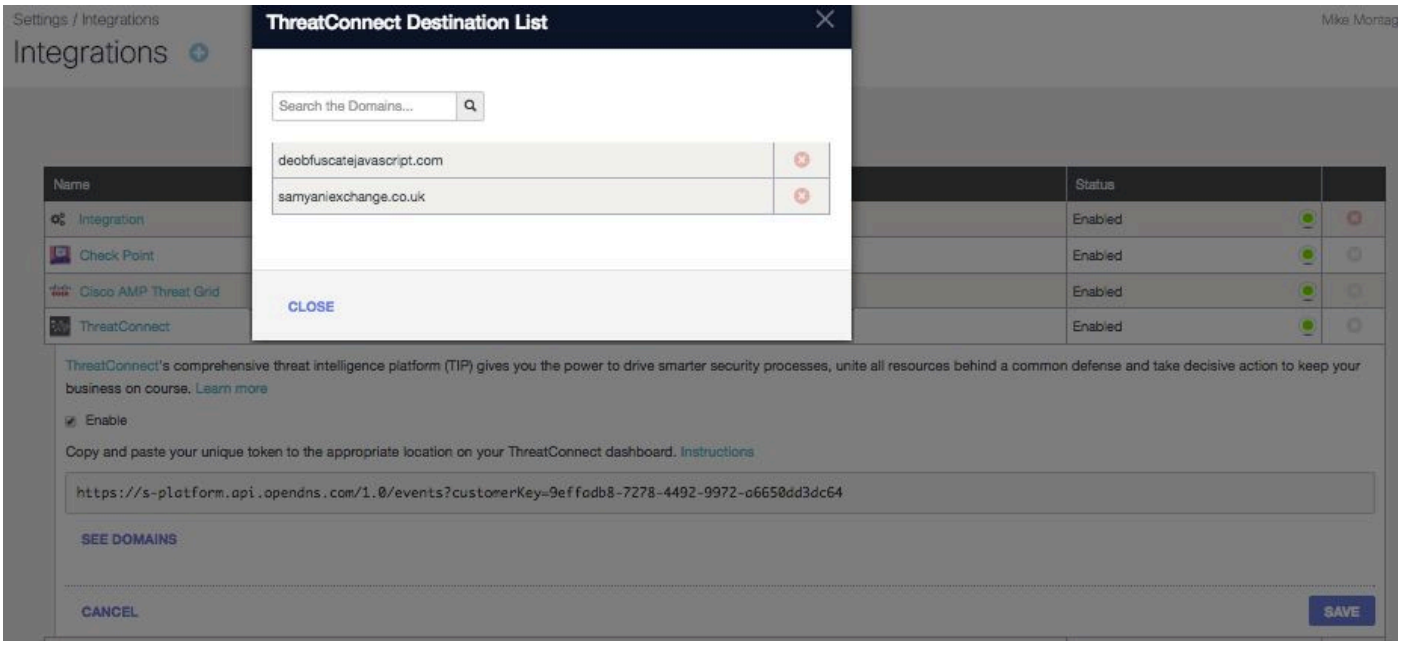
> Nota: La modalità di controllo può essere attivata per il tempo necessario in base al profilo di distribuzione e alla configurazione di rete.

Esamina elenco di destinazione

È possibile consultare l'elenco delle destinazioni ThreatConnect in Umbrella in qualsiasi momento:

1. Nel dashboard Umbrella, passare a Criteri > Integrazioni.

2. Nella tabella, espandere ThreatConnect e selezionare Vedere Domini.



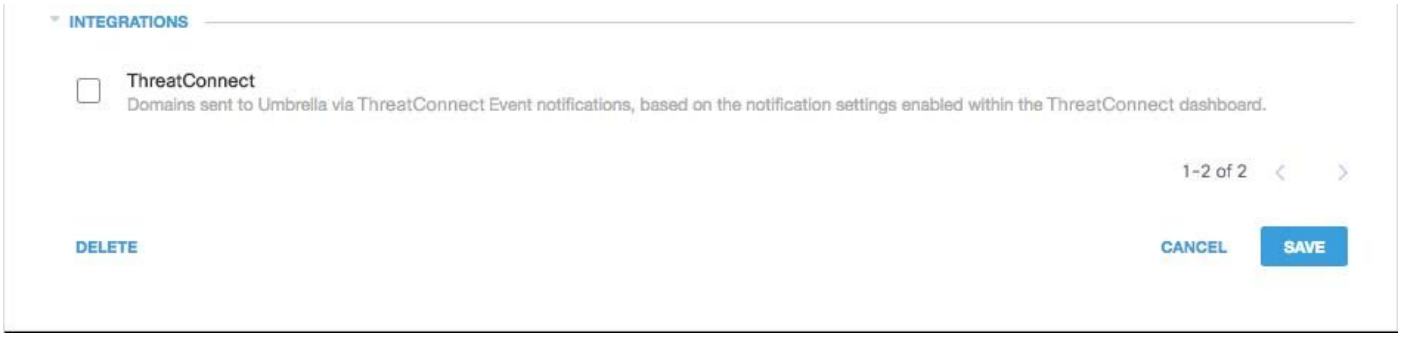
Rivedere le impostazioni di protezione per un criterio

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

1. Nel dashboard Umbrella, passare a Criteri > Impostazioni protezione.

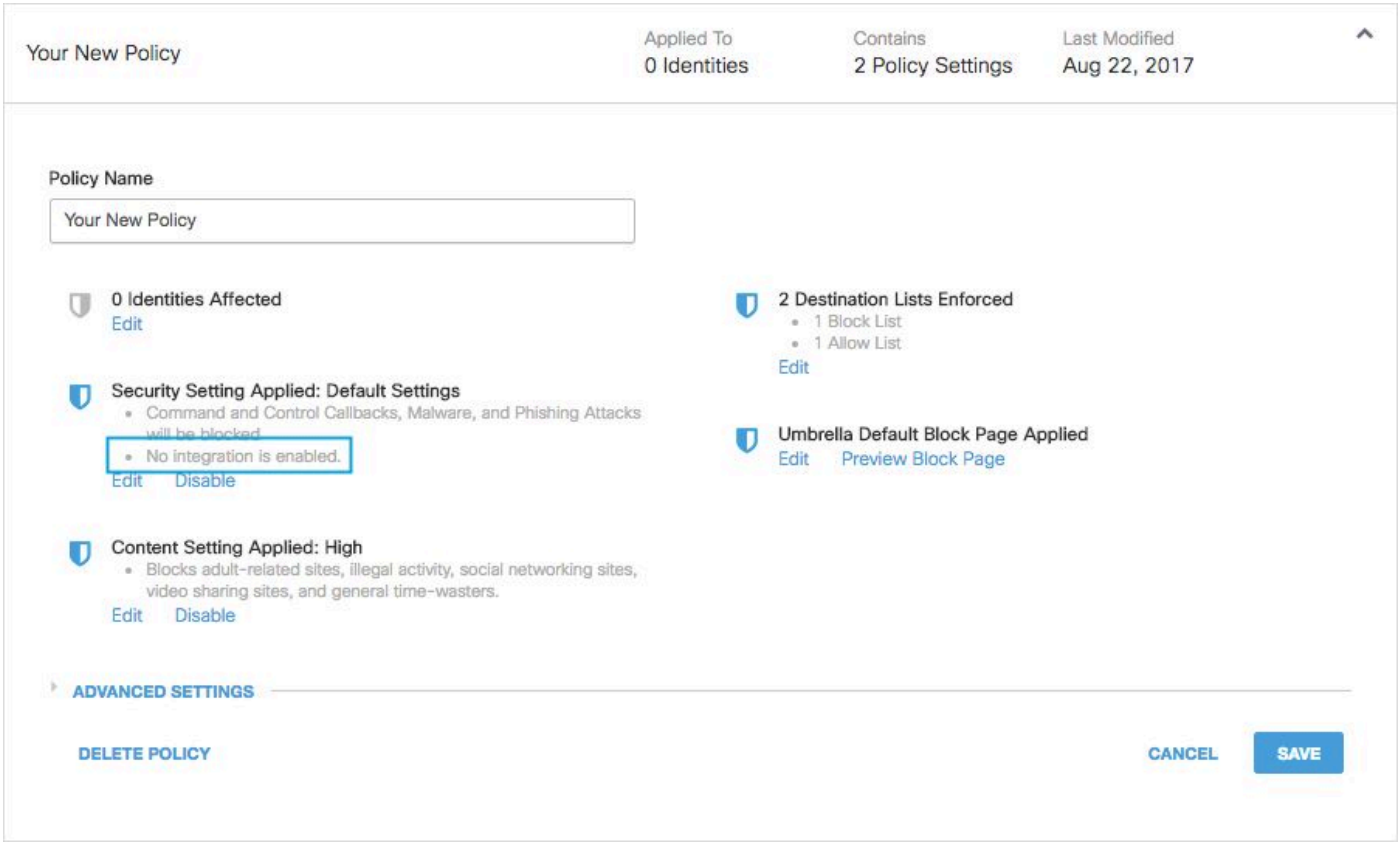
2. Selezionare un'impostazione di protezione nella tabella per espanderla.

3. Scorrere fino a Integrations (Integrazioni) per individuare l'impostazione ThreatConnect.



115014036566

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



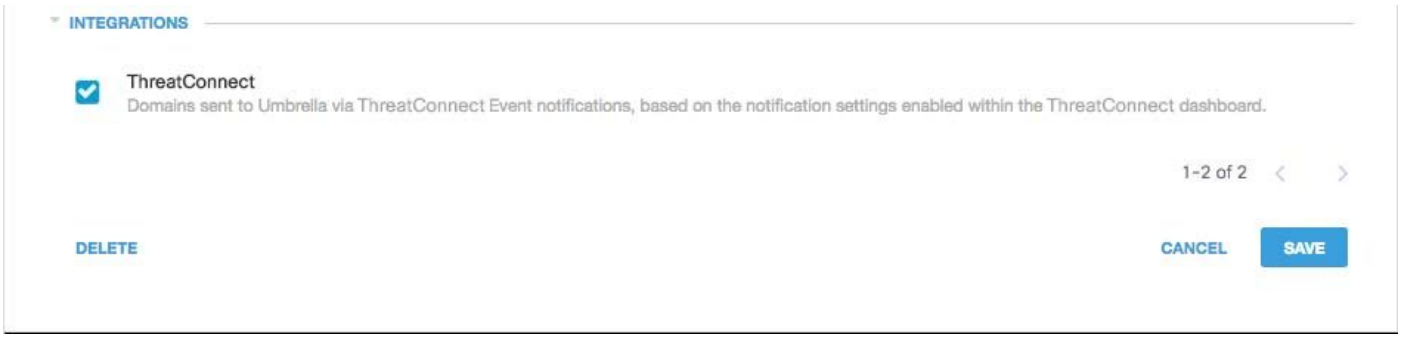
25464103885972

Applicazione delle impostazioni di sicurezza di ThreatConnect in modalità di blocco a un criterio per client gestiti

Quando sei pronto a far applicare queste ulteriori minacce alla sicurezza 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 al di sopra del tuo criterio predefinito per assicurarti che venga applicato per primo:

1. Passare a Criteri > Impostazioni protezione.

2. In Integrazioni, selezionare ThreatConnect, quindi selezionare Salva.



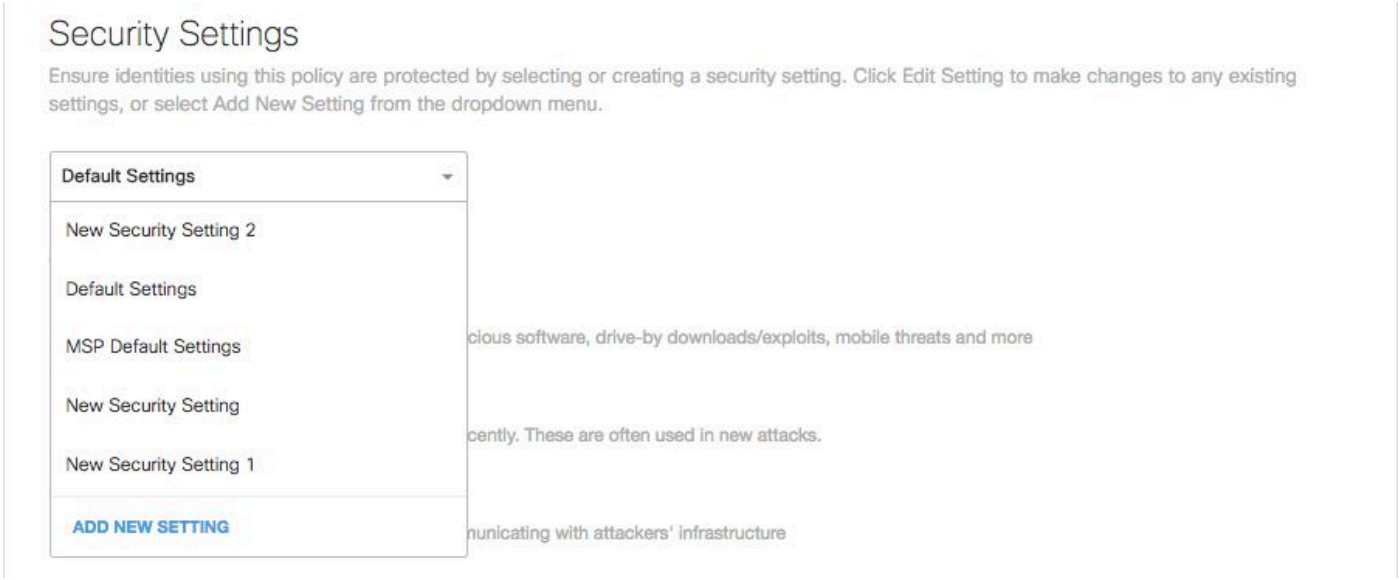
115014203703

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

1. Passare a Criteri > Elenco criteri.

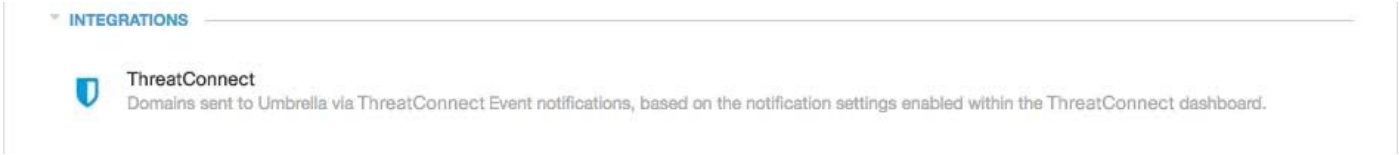
2. Espandere un criterio. In Impostazioni di protezione applicate, selezionare Modifica.

3. Nell'elenco a discesa Security Settings (Impostazioni di protezione), selezionare un'impostazione di protezione che includa l'impostazione ThreatConnect.



25464103908884

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



115014037666

4. Selezionare Set & Return.

I domini ThreatConnect contenuti nell'impostazione di protezione per ThreatConnect vengono quindi bloccati per le identità che utilizzano il criterio.

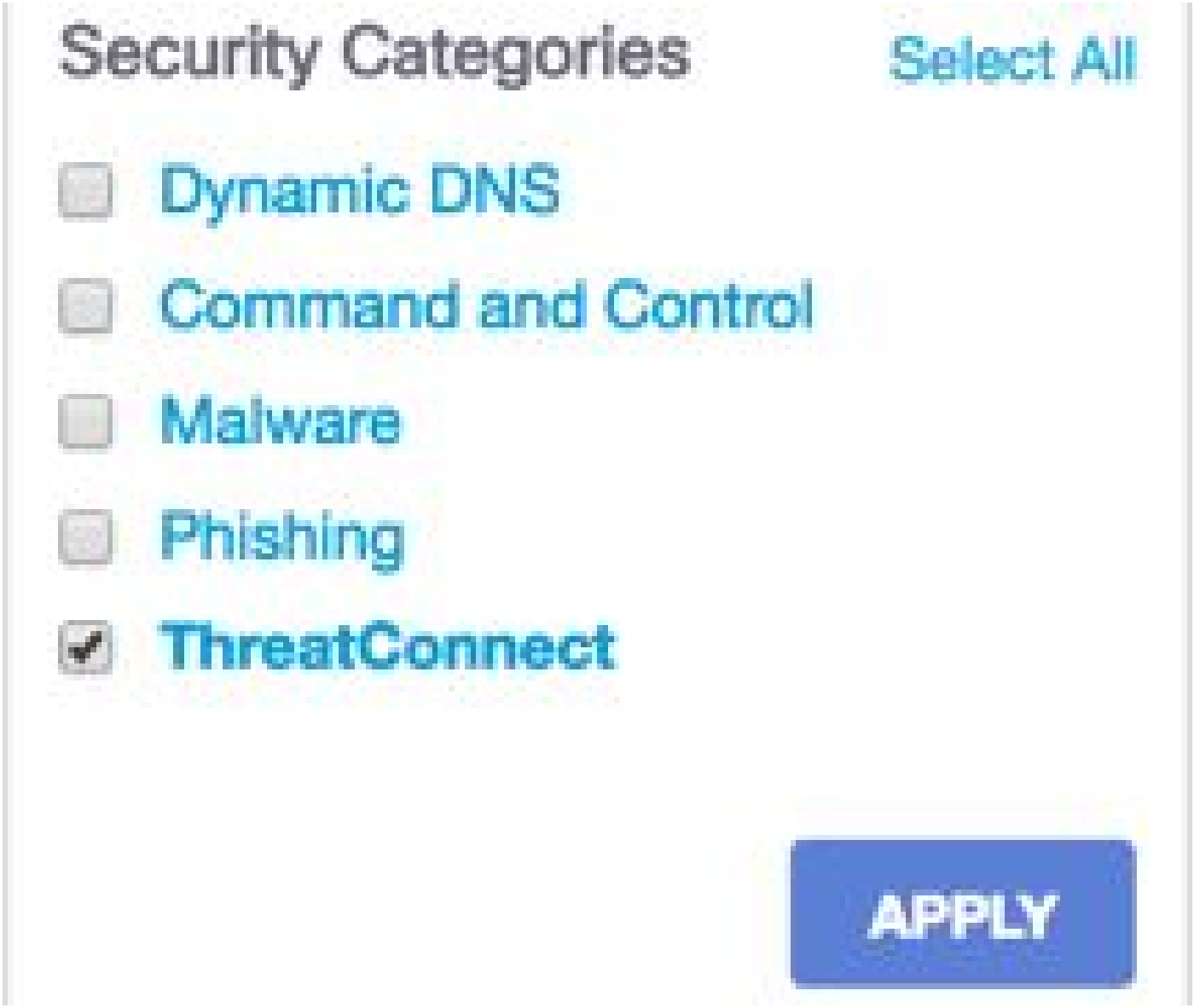
Segnalazione degli eventi di ThreatConnect in Umbrella

Segnalazione di eventi relativi alla sicurezza di ThreatConnect

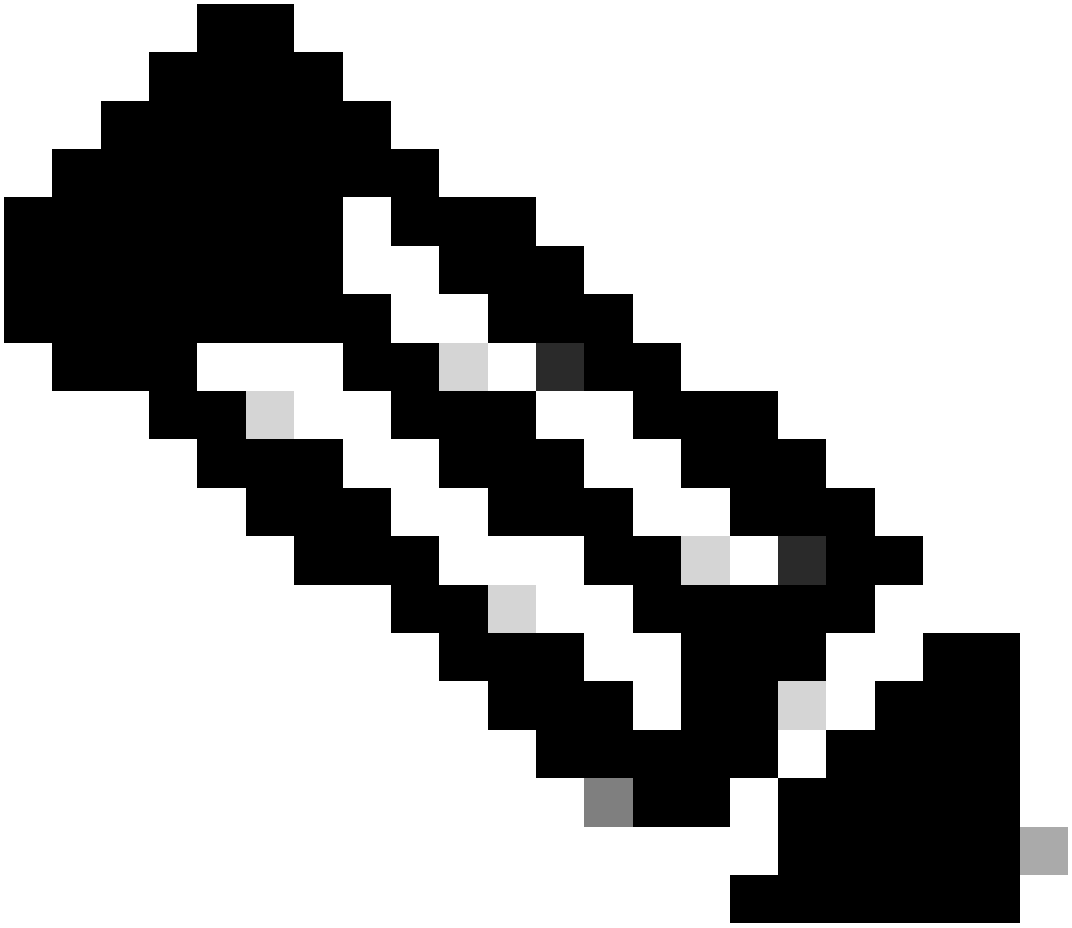
L'elenco delle destinazioni di ThreatConnect è una delle categorie di sicurezza per le quali è possibile creare un report. La maggior parte o tutti i report utilizzano le categorie di protezione come filtro. Ad esempio, è possibile filtrare le categorie di protezione per visualizzare solo le attività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

1. Passare a Reporting > Ricerca attività.

2. In Categorie di sicurezza, selezionare ThreatConnect per filtrare il report in modo da visualizzare solo la categoria di sicurezza per ThreatConnect.



115014206603



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

3. Selezionare Applica.

Segnalazione dell'aggiunta di domini all'elenco destinazioni ThreatConnect

Il registro di controllo Admin include gli eventi dal dashboard ThreatConnect man mano che aggiunge domini all'elenco di destinazione. Gli eventi sono generati da un utente denominato "Account ThreatConnect", anch'esso contrassegnato con il logo ThreatConnect. Tali eventi includono il dominio aggiunto e l'ora in cui è stato aggiunto.

È possibile filtrare per includere solo le modifiche ThreatConnect applicando un filtro per l'utente "ThreatConnect Account".

Gestione di rilevamenti indesiderati o falsi positivi

Elenchi di destinazioni autorizzate

Anche se improbabile, è possibile che i domini aggiunti automaticamente da ThreatConnect possano attivare un blocco indesiderato che impedirebbe agli utenti di accedere a determinati siti Web. In una situazione come questa, Umbrella consiglia di aggiungere i domini a un elenco di indirizzi consentiti, che ha la precedenza su tutti gli altri tipi di elenchi di indirizzi bloccati, incluse le impostazioni di protezione.

Esistono due motivi per cui questo approccio è preferibile:

- In primo luogo, nel caso in cui il dashboard ThreatConnect riaggiunga il dominio dopo che è stato rimosso, l'elenco Consenti protegge da ciò che causa ulteriori problemi.
- Inoltre, l'elenco Consenti mostra una registrazione cronologica di domini problematici che possono essere utilizzati per analisi legali o report 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 ThreatConnect 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. Passare a Criteri > Elenchi di destinazione e selezionare l'icona Aggiungi (+).

2. Selezionare Consenti e aggiungere il dominio all'elenco.

3. Selezionare 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 delle destinazioni ThreatConnect

L'elenco delle destinazioni di ThreatConnect contiene un'icona Delete accanto a ciascun nome di dominio. L'eliminazione dei domini consente di pulire l'elenco delle destinazioni ThreatConnect in caso di rilevamento indesiderato. Tuttavia, l'eliminazione non è permanente se il dashboard ThreatConnect invia nuovamente il dominio a Umbrella.

Per eliminare un dominio:

1. Passare a Criteri > Integrazioni.

2. Selezionare ThreatConnect per espanderlo.

3. Selezionare Vedere Domini.

4. Cercare il nome di dominio che si desidera eliminare.

5. Selezionare l'icona Elimina.

6. Selezionare Chiudi, quindi Salva.

Nel caso di un rilevamento indesiderato o di un falso positivo, Umbrella consiglia di creare immediatamente un elenco degli accessi consentiti in Umbrella e quindi di correggere il falso positivo all'interno del dashboard ThreatConnect. In seguito, è possibile rimuovere il dominio dall'elenco delle destinazioni di ThreatConnect.

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).