Integrazione di ThreatQ con Umbrella

Sommario

Introduzione

Questo documento descrive come integrare ThreatQ con Cisco Umbrella.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Un dashboard ThreatQ con accesso per aggiornare l'URL per le integrazioni
- Diritti amministrativi dashboard ombrello
- Nel dashboard Umbrella deve essere abilitata l'integrazione ThreatQ.

Componenti usati

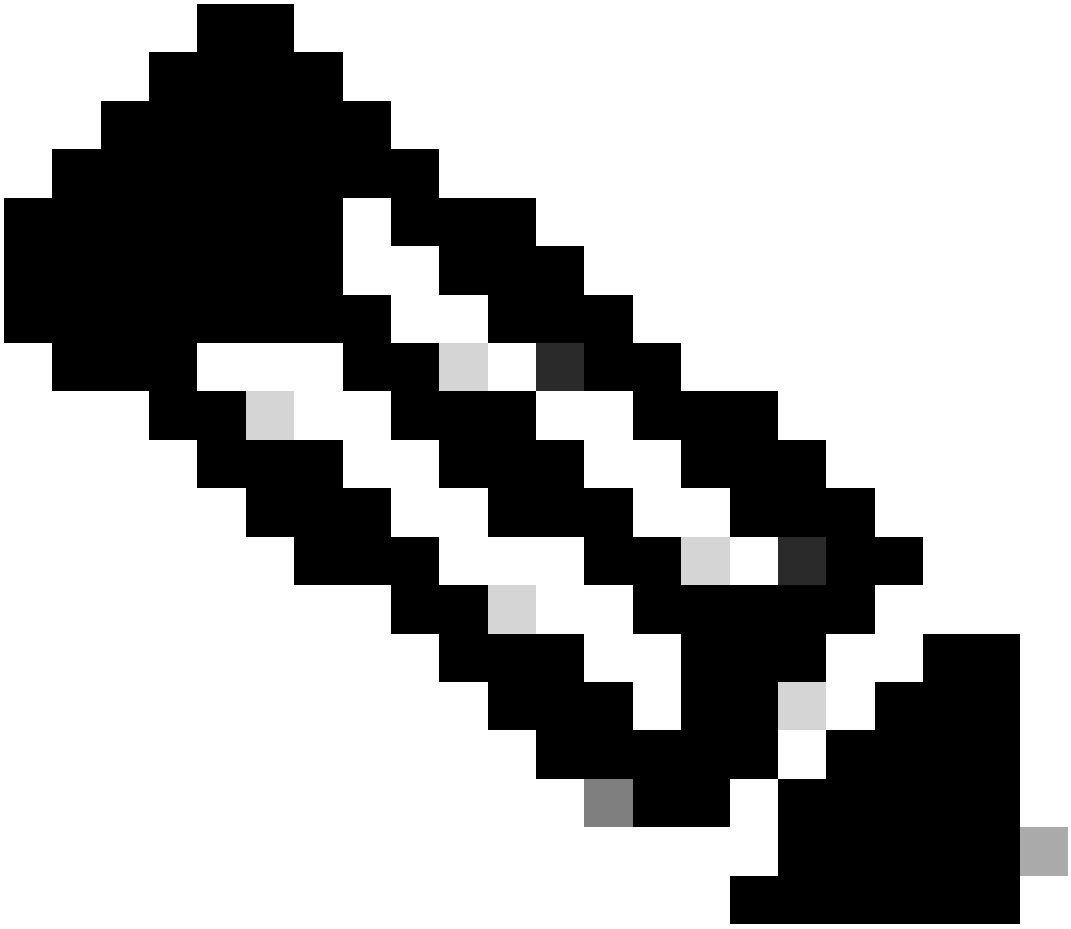
Le informazioni fornite in questo documento si basano su Cisco Umbrella.

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 ThreatQ e Cisco Umbrella

Grazie all'integrazione di ThreatQ 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 al contempo un altro livello di imposizione a una rete aziendale distribuita.

Questa guida descrive come configurare ThreatQ per comunicare con Umbrella in modo che gli eventi di sicurezza del suggerimento ThreatQ siano integrati in policy che possono essere applicate ai client protetti da Cisco Umbrella.



Nota: L'integrazione ThreatQ è inclusa solo in alcuni pacchetti Cisco Umbrella. Se non si

---

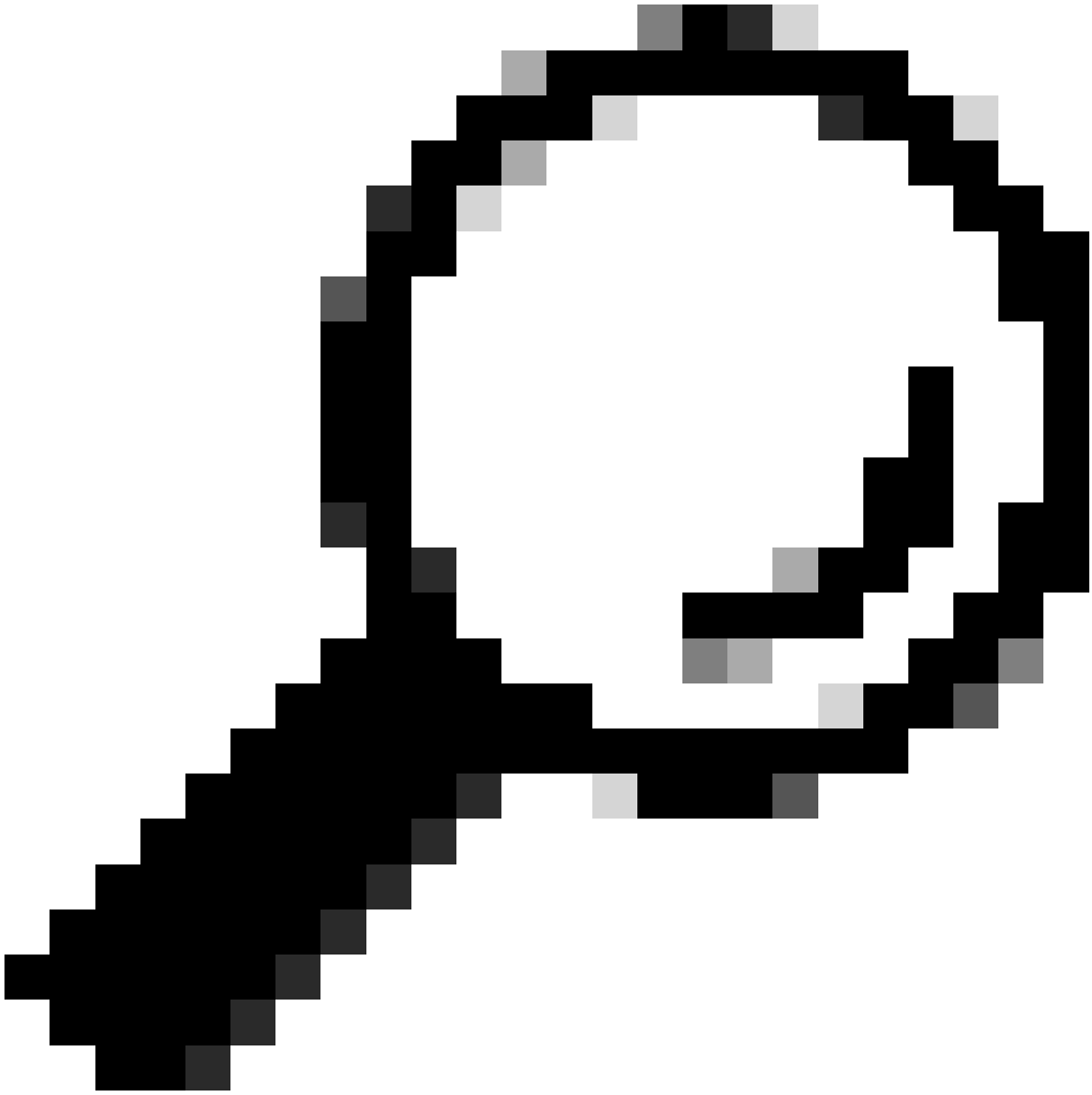
dispone del pacchetto richiesto e si desidera l'integrazione ThreatQ, contattare il rappresentante Cisco Umbrella. Se disponi del pacchetto Cisco Umbrella corretto ma non consideri ThreatQ come un'integrazione per il tuo dashboard, contatta il supporto Cisco Umbrella.

Funzionalità di integrazione

La piattaforma ThreatQ invia prima alla 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 ThreatQ sono confermate come minacce, l'indirizzo del dominio viene aggiunto all'elenco destinazioni ThreatQ 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 ThreatQ.

In futuro, Umbrella analizza automaticamente gli avvisi ThreatQ e aggiunge i siti dannosi all'elenco di destinazione ThreatQ. In questo modo la protezione ThreatQ viene estesa a tutti gli utenti e i dispositivi remoti e viene fornito un ulteriore livello di implementazione alla rete aziendale.



Suggerimento: Mentre Cisco Umbrella cerca il meglio per convalidare e consentire i domini che sono noti per essere generalmente sicuri (ad esempio, Google e Salesforce), per evitare interruzioni indesiderate, ti suggeriamo di aggiungere domini che non vorresti mai aver bloccato all'elenco globale dei siti consentiti o ad altri elenchi di destinazione secondo la tua policy. Alcuni esempi:

- Home page dell'organizzazione
- 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 basate su cloud meno note da cui si dipende non vengono incluse nella convalida automatica del dominio. Ad esempio, "localcloudservice.com".

Questi domini possono essere aggiunti all'elenco globale degli oggetti autorizzati che si trova in Criteri > Elenchi di destinazione in Cisco Umbrella.

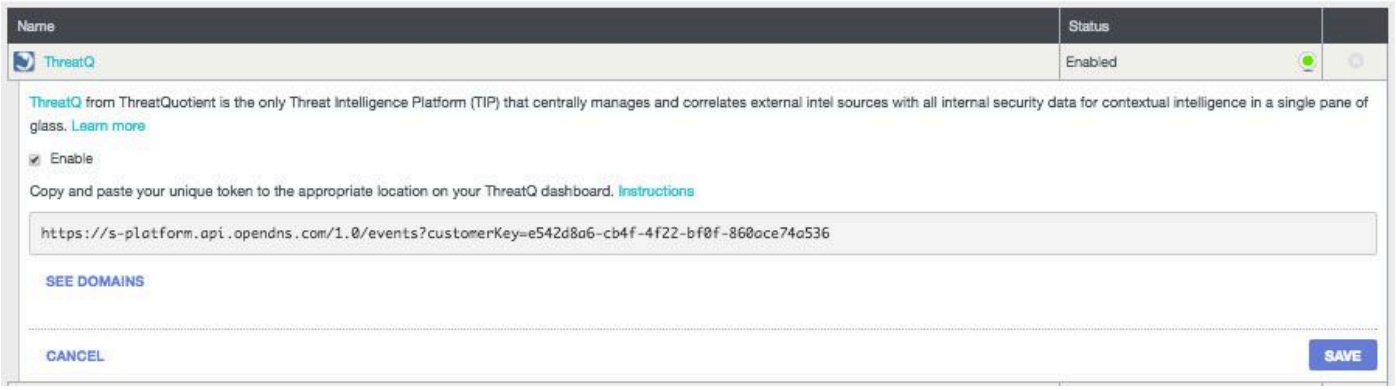
Generazione token API e script Umbrella

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

1. Accedi al dashboard Umbrella.

2. Passare a Impostazioni > Integrazioni e selezionare ThreatQ nella tabella per espanderla.

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



In un secondo momento, quando si configura il ThreatQ per l'invio dei dati a Umbrella, è necessario avere l'URL, quindi copiare l'URL e andare al dashboard ThreatQ.

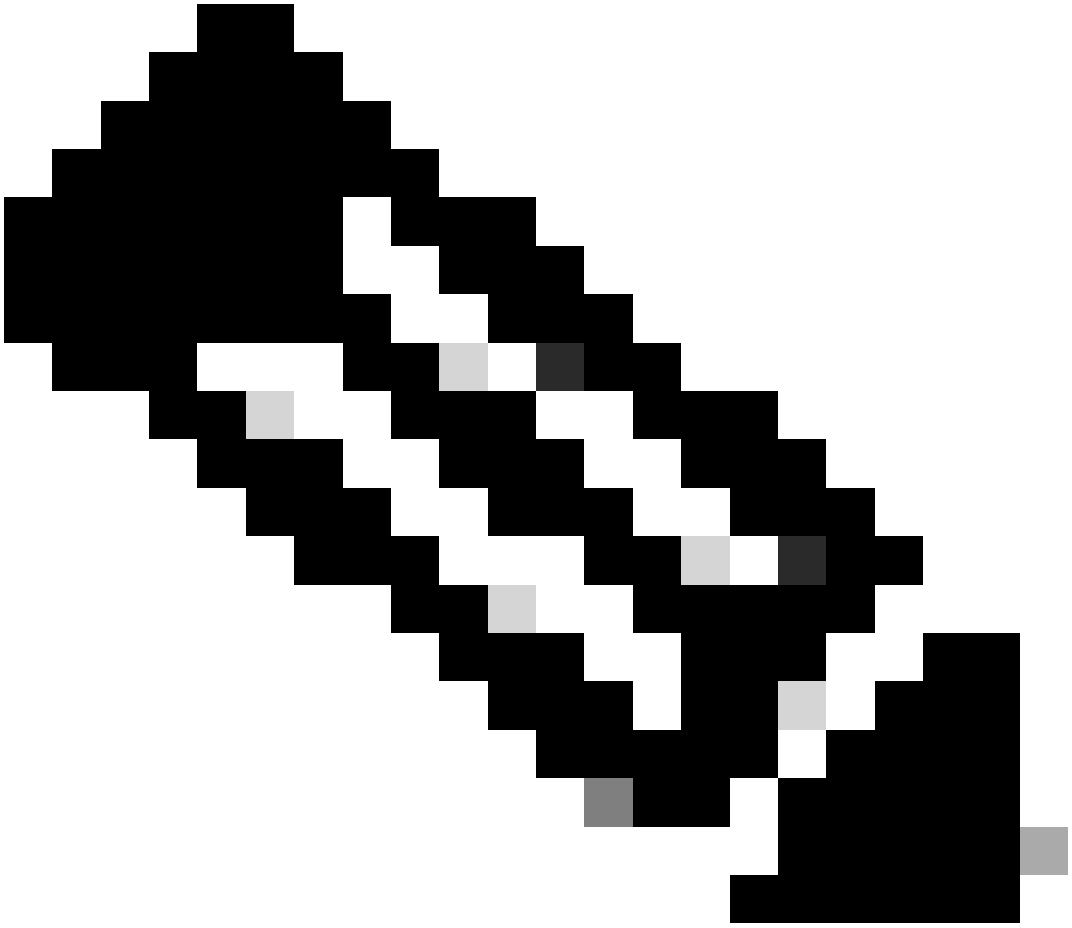
Come configurare ThreatQ per comunicare con Umbrella

Accedere al dashboard ThreatQ e aggiungere l'URL nell'area appropriata per connettersi con Umbrella.

Le istruzioni esatte variano e Umbrella suggerisce di contattare il supporto ThreatQ in caso di dubbi su come o dove configurare le integrazioni API all'interno di ThreatQ.

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

Nel tempo, gli eventi del dashboard ThreatQ iniziano a popolare un elenco di destinazioni specifico che può essere applicato ai criteri come categoria di sicurezza ThreatQ. Per impostazione predefinita, l'elenco di destinazione e la categoria di protezione sono in modalità di controllo, ovvero non vengono applicati ad alcun criterio e non possono comportare modifiche ai criteri Umbrella esistenti.



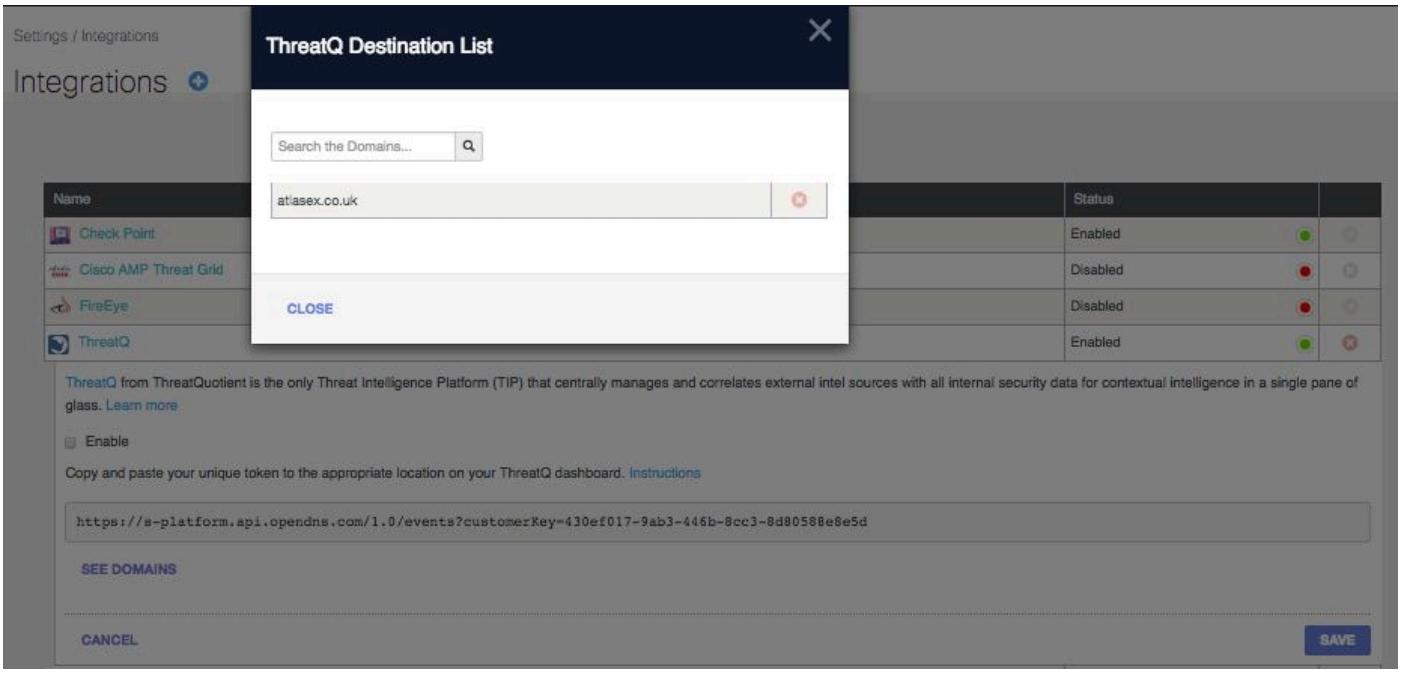
Nota: La modalità di controllo può essere attivata per il tempo necessario in base al profilo di distribuzione e alla configurazione di rete.

Esamina elenco di destinazione

È possibile rivedere l'elenco delle destinazioni ThreatQ in Umbrella in qualsiasi momento:

1. Passare a Impostazioni > Integrazioni.

2. Espandere ThreatQ nella tabella e selezionare Vedere Domini.



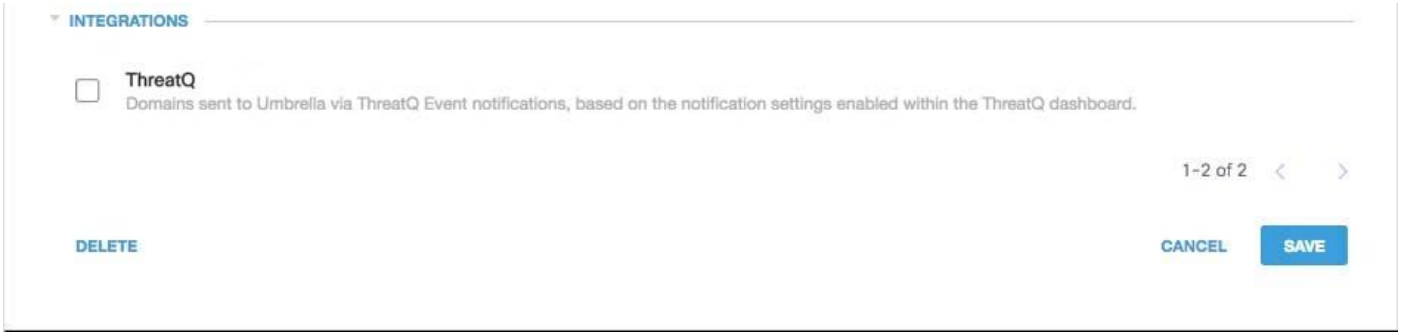
Rivedere le impostazioni di protezione per un criterio

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

1. Passare a Criteri > Impostazioni protezione.

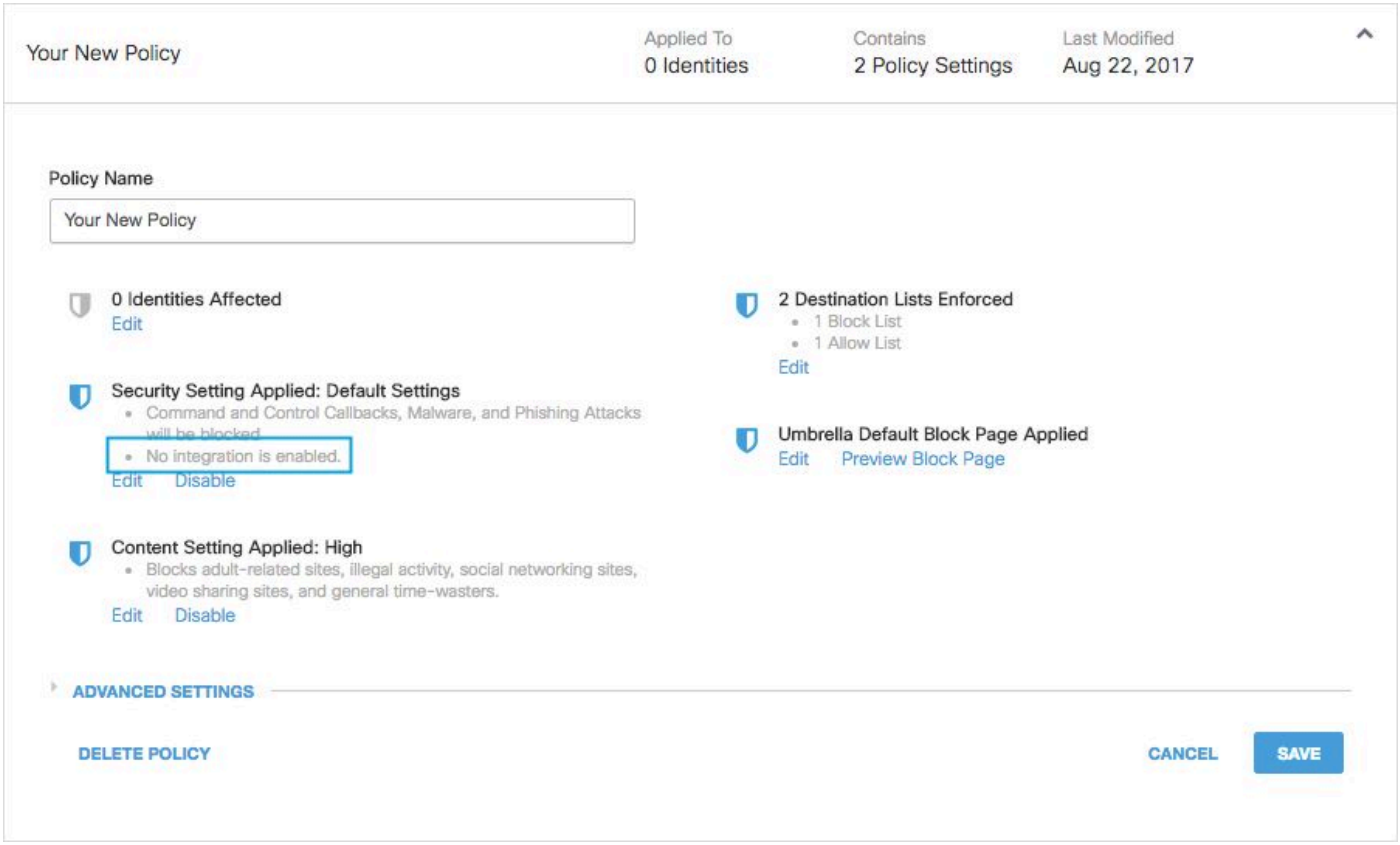
2. Selezionare un'impostazione di protezione nella tabella per espanderla.

3. Scorrere fino a Integrations per individuare l'impostazione ThreatQ.



115014040286

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



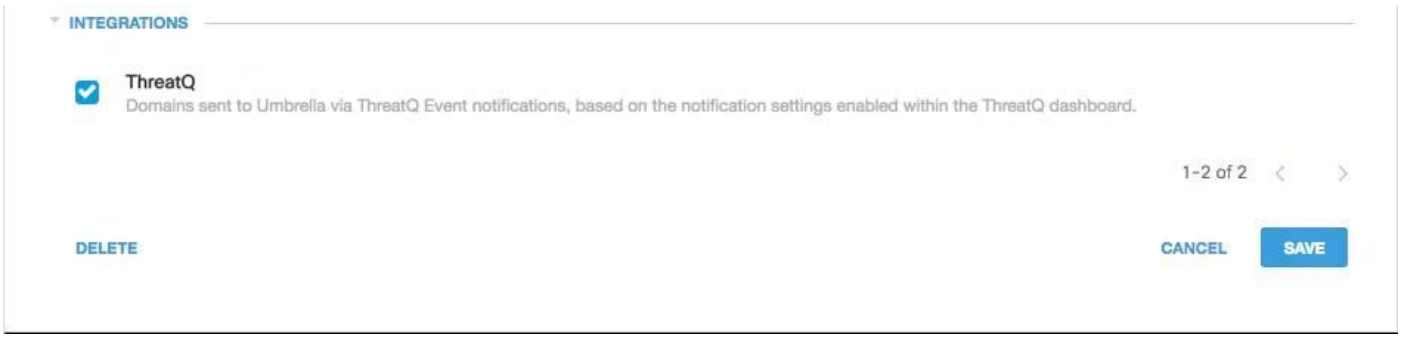
25464141748116

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

Quando sei pronto a far applicare queste minacce di sicurezza aggiuntive ai client gestiti da Umbrella, puoi modificare l'impostazione di sicurezza su un criterio esistente o creare un nuovo criterio che si trovi più in alto del tuo criterio predefinito per assicurarti che venga applicato per primo:

1. Passare a Criteri > Impostazioni protezione.

2. In Integrazioni, selezionare ThreatQ e selezionare Salva.



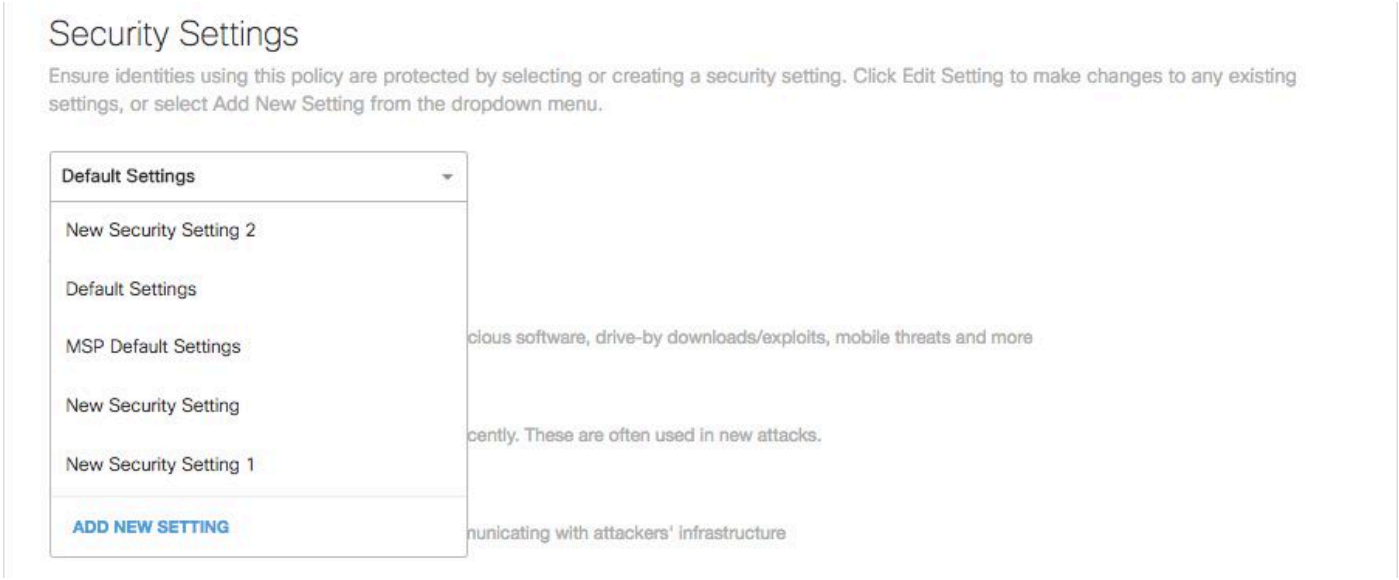
115014207403

Nella Creazione guidata criteri aggiungere quindi un'impostazione di protezione al criterio che si sta modificando:

1. Passare a Criteri > Elenco criteri.

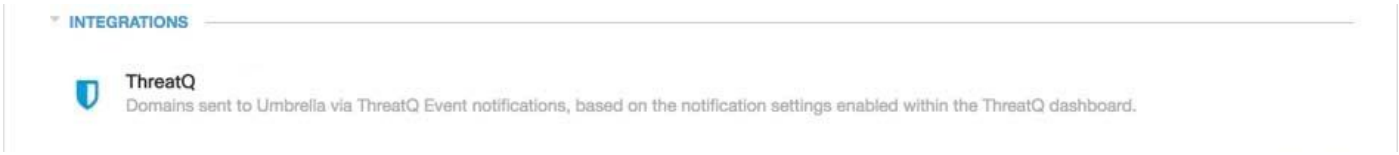
2. Espandere un criterio e selezionare Modifica in Impostazioni di protezione applicate.

3. Nella casella di riepilogo a discesa Security Settings (Impostazioni di protezione), selezionare un'impostazione di protezione che includa ThreatQ.



25464141787668

L'icona a forma di scudo sotto Integrations viene aggiornata in blu.



115014040506

4. Selezionare Set & Return.

I domini ThreatQ contenuti nell'impostazione di protezione per ThreatQ sono ora bloccati per le identità che utilizzano il criterio.

Segnalazione di eventi Umbrella per ThreatQ

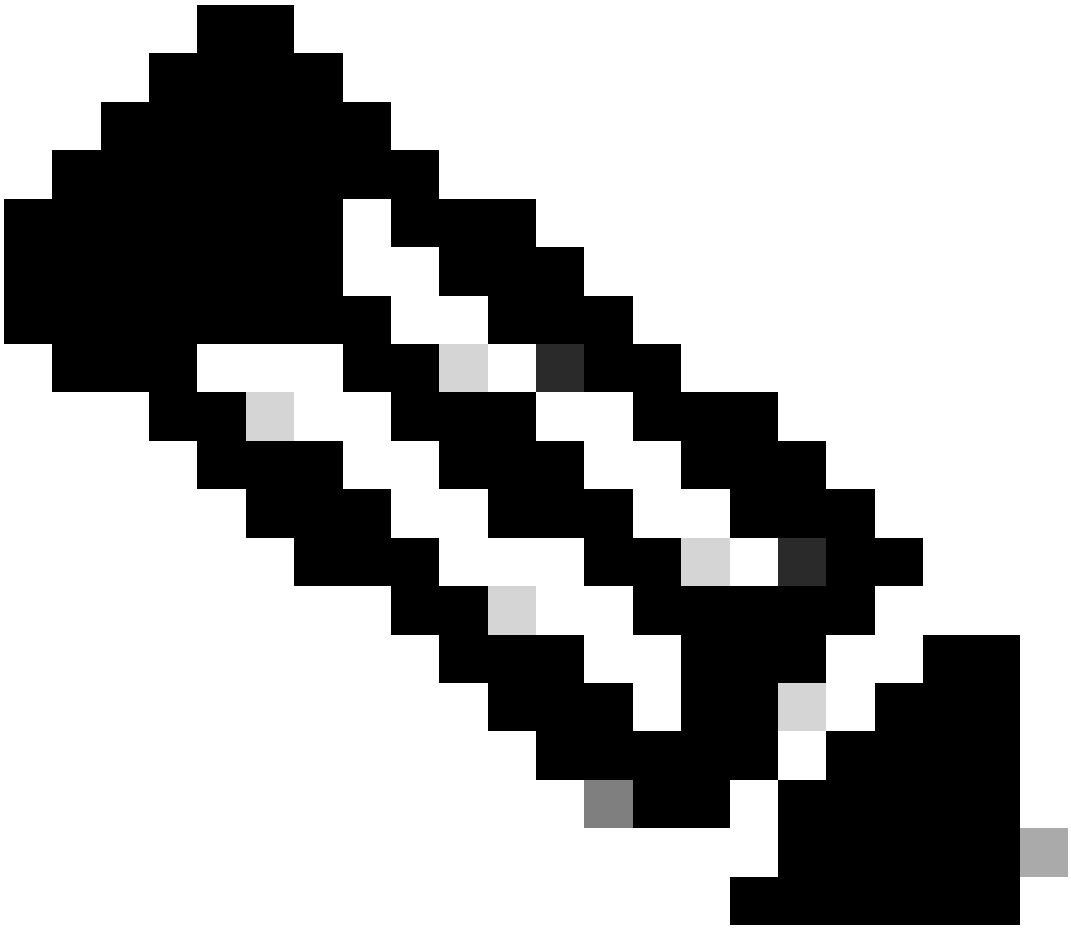
Segnalazione di eventi di sicurezza ThreatQ

L'elenco delle destinazioni ThreatQ è una delle categorie di sicurezza per le quali è possibile creare un rapporto. 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 ThreatQ.

1. Passare a Reporting > Ricerca attività.

2. In Categorie di sicurezza, selezionare ThreatQ per filtrare il rapporto in modo da visualizzare

solo la categoria di sicurezza per ThreatQ.



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

115014207603

3. Selezionare Applica.

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

Il registro di controllo di Umbrella Admin include gli eventi dal dashboard ThreatQ man mano che aggiunge domini all'elenco di destinazione. L'evento viene generato da un utente di nome "ThreatQ Account", anch'esso contrassegnato con il logo ThreatQ. Tali eventi includono il dominio aggiunto e l'ora in cui è stato aggiunto. Il registro di controllo di Umbrella Admin è disponibile in Report > Registro di controllo di amministrazione.

È possibile filtrare per includere solo le modifiche ThreatQ applicando un filtro per l'utente account ThreatQ.

Gestione di rilevamenti indesiderati o falsi positivi

Elenchi di destinazioni autorizzate

Anche se improbabile, è possibile che i domini aggiunti automaticamente da ThreatQ possano attivare un blocco indesiderato che può impedire 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 ThreatQ dovesse aggiungere di nuovo il dominio dopo la rimozione, l'elenco Consenti protegge da quello che causa ulteriori problemi.
- In secondo luogo, l'elenco degli indirizzi consentiti 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 ThreatQ in modalità blocco viene applicata solo a un sottoinsieme delle identità Umbrella gestite (ad esempio, viene applicata solo a computer mobili e dispositivi mobili in roaming), 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 Allow (Consenti), quindi aggiungere il dominio all'elenco.

3. Selezionare Salva.

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

Eliminazione dei domini dall'elenco delle destinazioni ThreatQ

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

Per eliminare un dominio:

1. Passare a Impostazioni > Integrazioni, quindi selezionare ThreatQ per espanderlo.

2. Selezionare Vedere Domini.

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

4. Selezionare l'icona Elimina.

5. Selezionare Chiudi.

6. Selezionare Salva.

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

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).