Integration von ThreatConnect mit Umbrella

Inhalt

Einleitung

In diesem Dokument wird die Integration von ThreatConnect in Cisco Umbrella beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ThreatConnect-Dashboard mit Zugriff zur Aktualisierung der URL für Integrationen
- Administratorrechte für Umbrella Dashboard
- Für das Umbrella Dashboard muss die ThreatConnect-Integration aktiviert sein.

Verwendete Komponenten

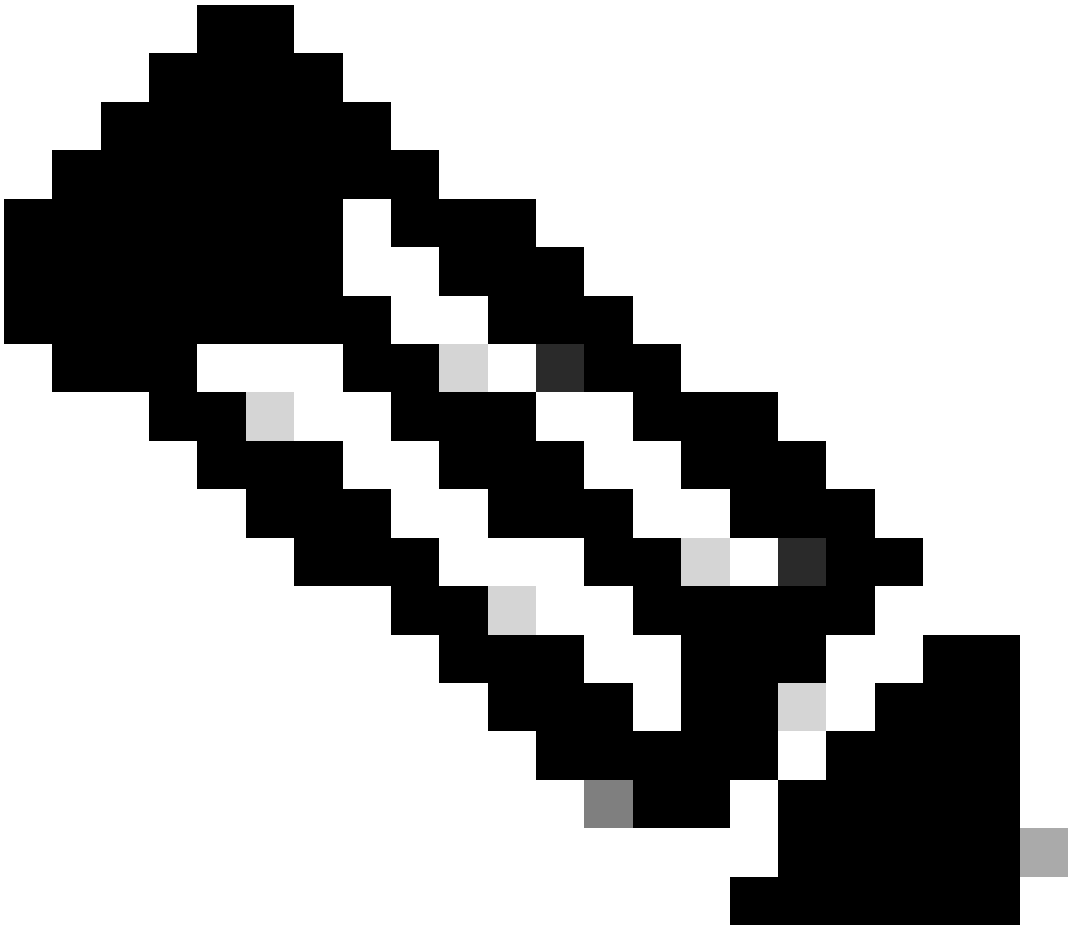
Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

ThreatConnect und Cisco Umbrella Integration - Überblick

Durch die Integration von ThreatConnect mit Cisco Umbrella können Sicherheitsbeauftragte und Administratoren jetzt den Schutz vor komplexen Bedrohungen auf mobile Laptops, Tablets oder Telefone ausdehnen und gleichzeitig eine weitere Durchsetzungsebene für ein verteiltes Unternehmensnetzwerk bereitstellen.

In diesem Leitfaden wird erläutert, wie ThreatConnect für die Kommunikation mit Umbrella konfiguriert wird, damit Sicherheitsereignisse aus dem ThreatConnect-TIPP in Richtlinien integriert werden, die auf Clients angewendet werden können, die durch Ihren Cisco Umbrella-Schutz geschützt sind.

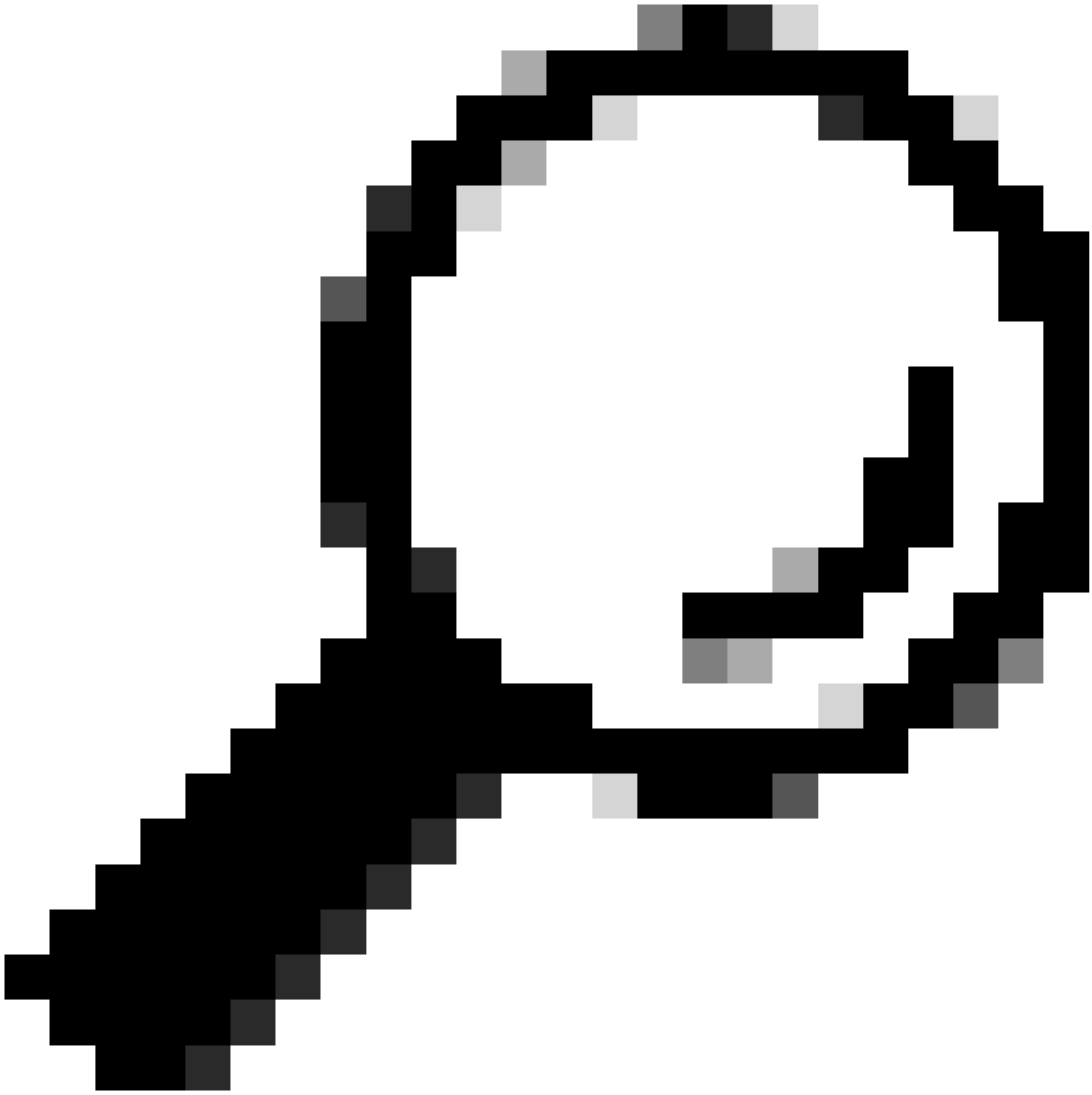


Anmerkung: Die ThreatConnect-Integration ist nur in einem bestimmten Cisco Umbrella-Paket enthalten. Wenn Sie nicht über ein Paket verfügen, das diese Integration enthält, wenden Sie sich an Ihren Cisco Umbrella-Vertreter, um es zu erhalten. Wenn Sie über das richtige Paket verfügen, ThreatConnect aber nicht als Integrationslösung für Ihr Dashboard angezeigt wird, wenden Sie sich an den Cisco Umbrella Support.

Die ThreatConnect-Plattform sendet zunächst die gefundenen Cyber Threat Intelligence, z. B. Domains, die Malware hosten, Befehle und Kontrolle für Botnet- oder Phishing-Websites, an Umbrella.

Umbrella validiert die Bedrohung, um sicherzustellen, dass sie einer Richtlinie hinzugefügt werden kann. Wenn sich bestätigt, dass die Informationen von ThreatConnect eine Bedrohung darstellen, wird die Domänenadresse im Rahmen einer Sicherheitseinstellung, die auf eine beliebige Umbrella-Richtlinie angewendet werden kann, der Liste der ThreatConnect-Ziele hinzugefügt. Diese Richtlinie wird sofort auf alle Anforderungen angewendet, die von Geräten mithilfe von Richtlinien mit der ThreatConnect-Zielliste gestellt werden.

In Zukunft analysiert Umbrella automatisch ThreatConnect-Warnungen und fügt bösartige Websites zur ThreatConnect-Zielliste hinzu. Dadurch wird der Schutz durch ThreatConnect auf alle Remote-Benutzer und -Geräte ausgeweitet und eine weitere Durchsetzungsebene für Ihr Unternehmensnetzwerk geschaffen.



Tipp: Während Umbrella sich bemüht, bekanntermaßen sichere Domains zu validieren und zuzulassen (z. B. Google und Salesforce), um unerwünschte Unterbrechungen zu vermeiden, schlägt Umbrella vor, Domains, die Sie nicht blockieren möchten, der globalen Zulassungsliste oder anderen Ziellisten gemäß Ihrer Richtlinie hinzuzufügen. Beispiele:

- Die Startseite für Ihre Organisation. Beispiel: mydomain.com.
- Domänen, die von Ihnen bereitgestellte Dienste darstellen und sowohl interne als auch externe Datensätze enthalten können. Beispielsweise mail.myservicedomain.com und portal.myotherservicedomain.com.
- Weniger bekannte Cloud-Anwendungen, von denen Sie stark abhängig sind, die Umbrella jedoch nicht kennt oder in die automatische Domänenvalidierung einbezieht. Beispiel: localcloudservice.com.

Die globale Zulassungsliste finden Sie unter Richtlinien > Ziellisten in Umbrella. Weitere Informationen finden Sie in der Dokumentation: Ziellisten verwalten

Konfigurieren des Umbrella Dashboards zum Empfangen von Ereignissen von ThreatConnect

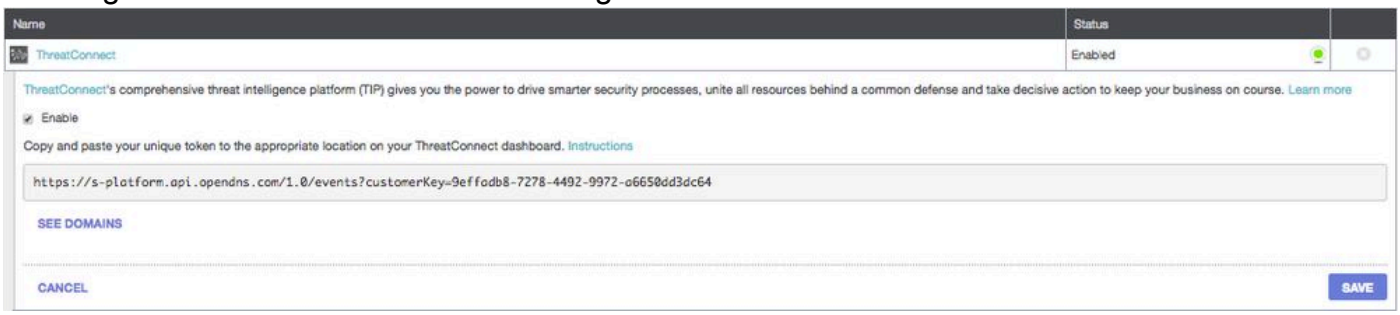
Suchen Sie zunächst in Umbrella nach Ihrer eindeutigen URL, mit der die ThreatQ-Appliance kommunizieren kann:

1. Melden Sie sich bei Ihrem Umbrella Dashboard an.

2. Navigieren Sie zu Richtlinien > Integrationen.

3. Wählen Sie in der Tabelle ThreatConnect aus, um die Liste zu erweitern.

4. Wählen Sie Aktivieren und dann Speichern. Dadurch wird eine eindeutige, spezifische URL für Ihre Organisation innerhalb von Umbrella generiert.



Sie benötigen die URL weiter unten in diesem Artikel, wenn Sie ThreatConnect so konfigurieren, dass Daten an Umbrella gesendet werden.

Konfigurieren von ThreatConnect für die Kommunikation mit Umbrella

Um Datenverkehr von ThreatConnect an Umbrella zu senden, müssen Sie ThreatConnect mit den URL-Informationen konfigurieren, die im ersten Abschnitt dieses Artikels generiert werden:

1. Melden Sie sich bei Ihrem ThreatConnect-Dashboard an.

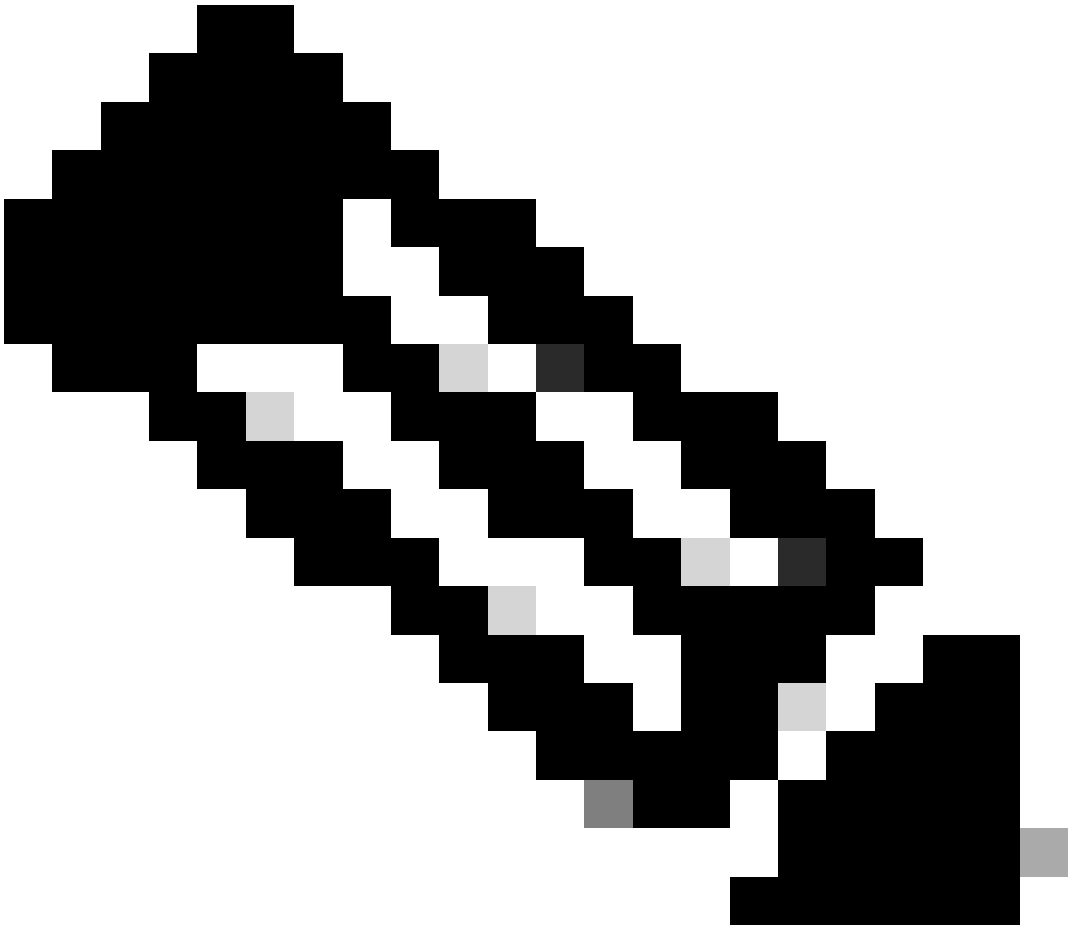
2. Fügen Sie die URL in den entsprechenden Bereich mit Umbrella zu verbinden.

Die genauen Anweisungen variieren, und Umbrella empfiehlt, sich an den ThreatConnect-Support zu wenden, wenn Sie sich nicht sicher sind, wie oder wo Sie API-Integrationen in ThreatConnect konfigurieren möchten.

Beobachtung von Ereignissen, die der Sicherheitskategorie von ThreatConnect im Überwachungsmodus hinzugefügt wurden

Mit der Zeit können Ereignisse aus Ihrem ThreatConnect-Dashboard beginnen, eine bestimmte Zielliste auszufüllen, die als ThreatConnect-Sicherheitskategorie auf Richtlinien angewendet werden kann. Die Zielliste und die Sicherheitskategorie befinden sich standardmäßig im

Überwachungsmodus, d. h., sie werden nicht auf Richtlinien angewendet und führen nicht zu Änderungen an Ihren vorhandenen Umbrella-Richtlinien.



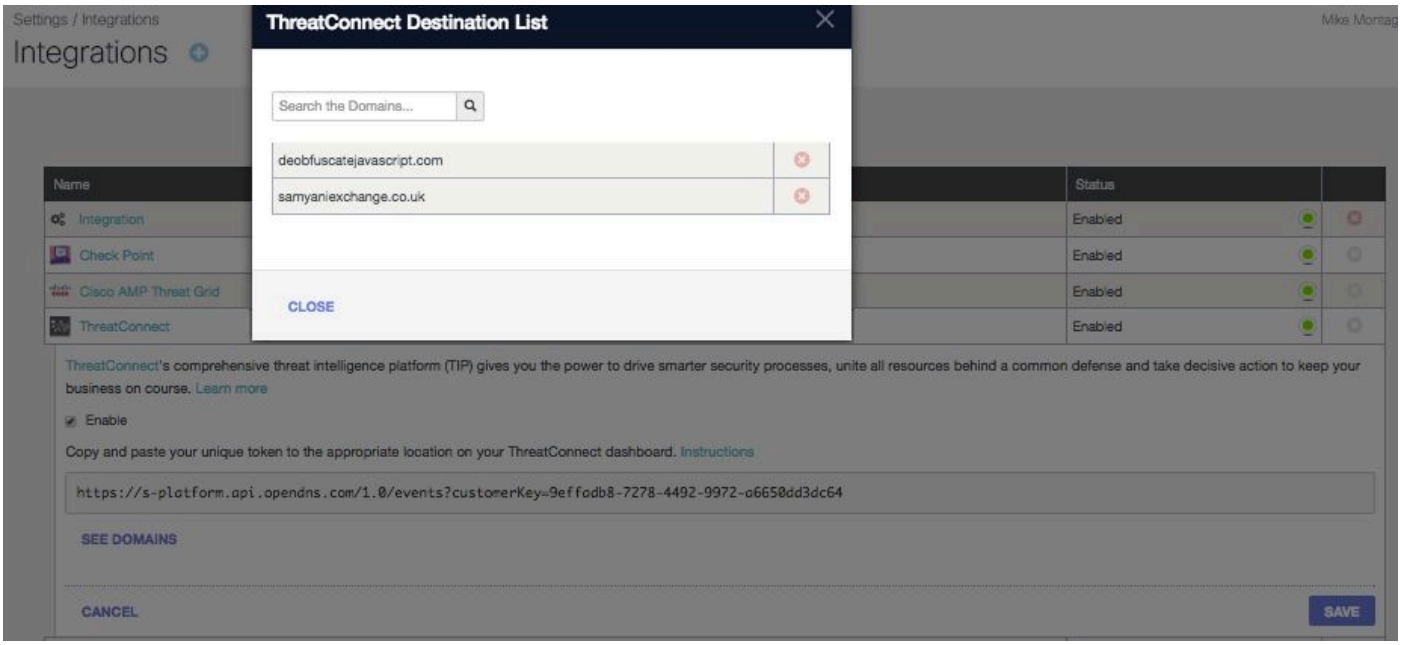
> Anmerkung: Der Überwachungsmodus kann je nach Bereitstellungsprofil und Netzwerkkonfiguration so lange aktiviert werden, wie dies erforderlich ist.

Zielliste überprüfen

Sie können die ThreatConnect-Zielliste in Umbrella jederzeit einsehen:

1. Navigieren Sie im Umbrella Dashboard zu Policies > Integrations (Richtlinien > Integrationen).

2. Erweitern Sie in der Tabelle ThreatConnect, und wählen Sie Domains anzeigen aus.



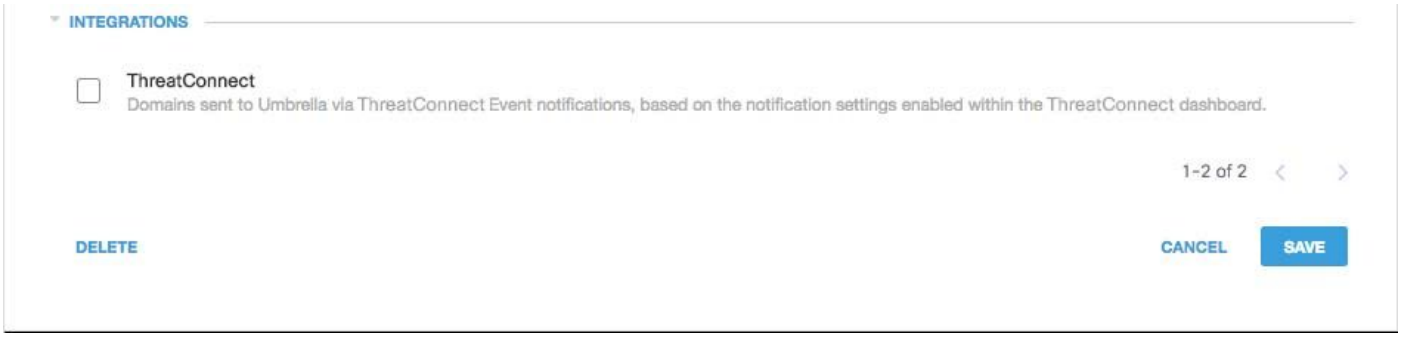
Sicherheitseinstellungen für eine Richtlinie überprüfen

Sie können die Sicherheitseinstellungen, die für eine Richtlinie aktiviert werden können, jederzeit überprüfen:

1. Navigieren Sie im Umbrella Dashboard zu Richtlinien > Sicherheitseinstellungen.

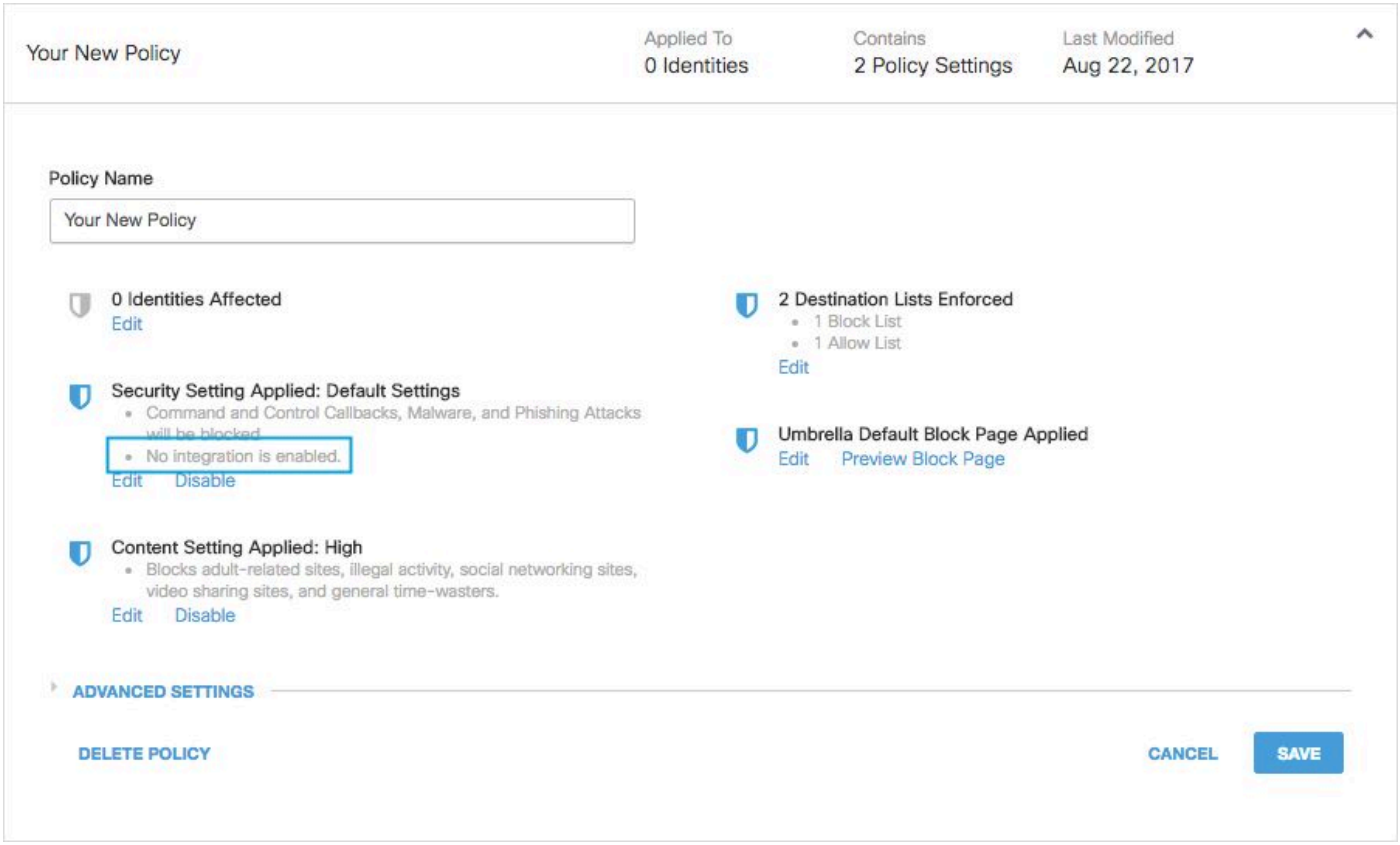
2. Wählen Sie eine Sicherheitseinstellung in der Tabelle aus, um sie zu erweitern.

3. Navigieren Sie zu Integrations, um die ThreatConnect-Einstellung zu finden.



115014036566

4. Sie können die Integrationsinformationen auch auf der Seite Sicherheitseinstellungsübersicht überprüfen.



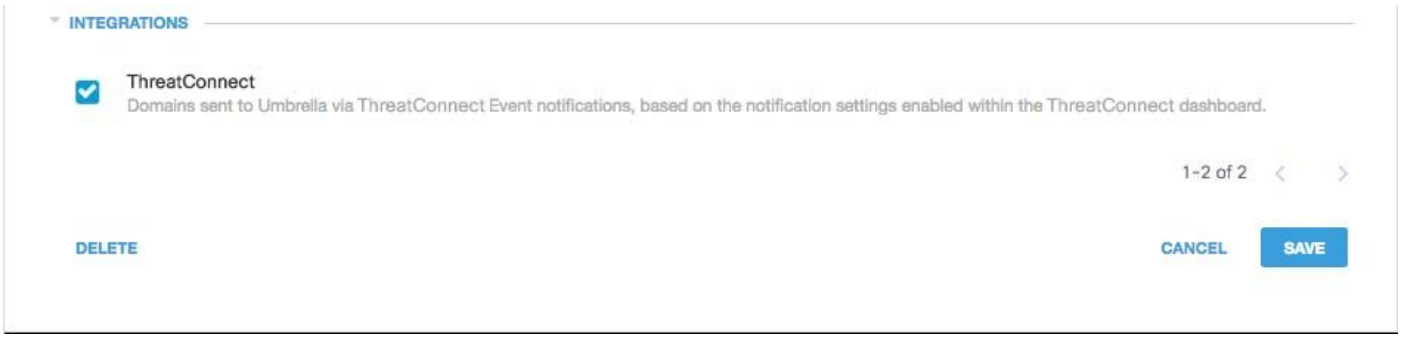
25464103885972

Anwenden der ThreatConnect-Sicherheitseinstellungen im Blockmodus auf eine Richtlinie für verwaltete Clients

Wenn Sie bereit sind, diese zusätzlichen Sicherheitsbedrohungen von Clients durchzusetzen, die von Umbrella verwaltet werden, ändern Sie einfach die Sicherheitseinstellung in einer vorhandenen Richtlinie, oder erstellen Sie eine neue Richtlinie, die über Ihrer Standardrichtlinie liegt, um sicherzustellen, dass sie zuerst durchgesetzt wird:

1. Navigieren Sie zu Richtlinien > Sicherheitseinstellungen.

2. Wählen Sie unter Integrationen die Option ThreatConnect und dann Speichern.



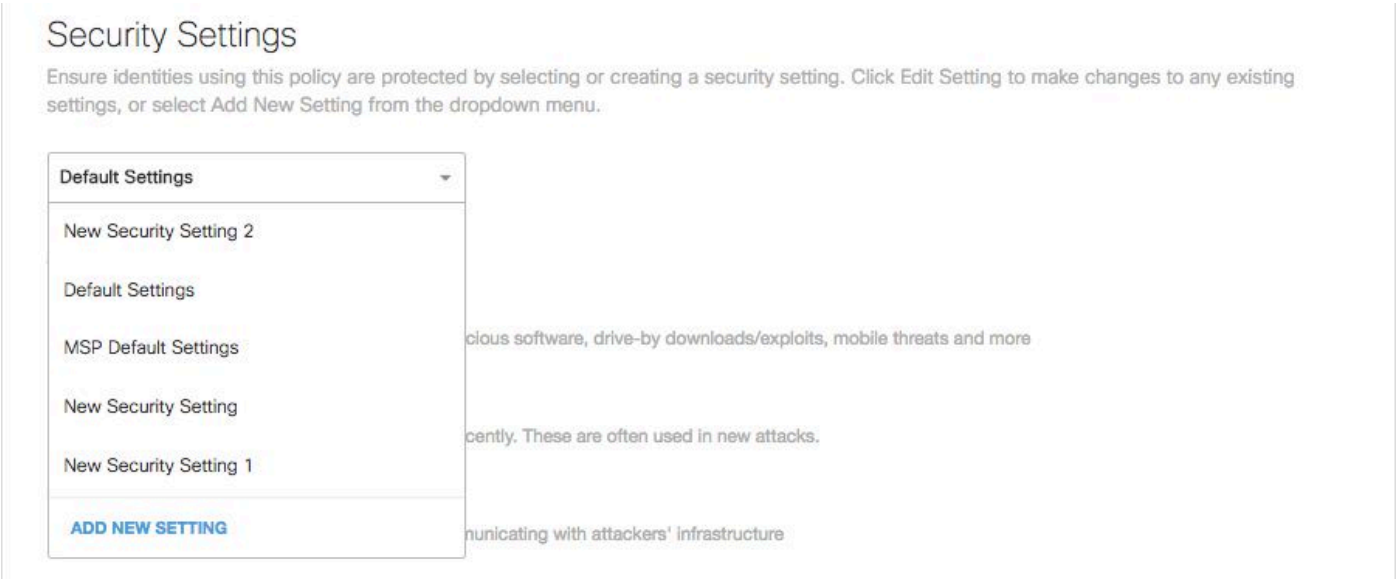
115014203703

Fügen Sie anschließend im Richtlinien-Assistenten eine Sicherheitseinstellung zu der Richtlinie hinzu, die Sie bearbeiten:

1. Navigieren Sie zu Richtlinien > Richtlinienliste.

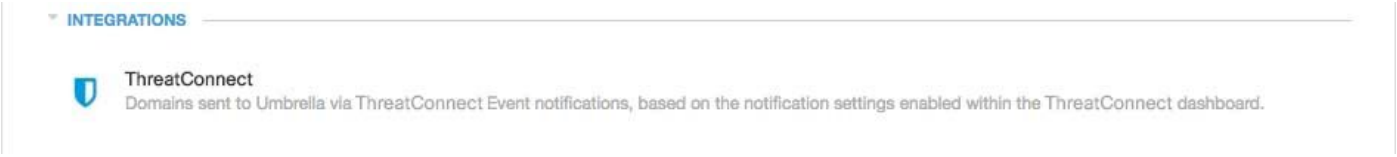
2. Erweitern Sie eine Richtlinie. Wählen Sie unter Sicherheitseinstellung angewendet die Option Bearbeiten aus.

3. Wählen Sie in der Dropdown-Liste Sicherheitseinstellungen eine Sicherheitseinstellung aus, die die ThreatConnect-Einstellung enthält.



25464103908884

Das Schildsymbol unter Integrationen wird blau angezeigt.



115014037666

4. Wählen Sie Festlegen und Zurücksenden.

Die in den Sicherheitseinstellungen für ThreatConnect enthaltenen ThreatConnect-Domänen werden dann mithilfe der Richtlinie für Identitäten gesperrt.

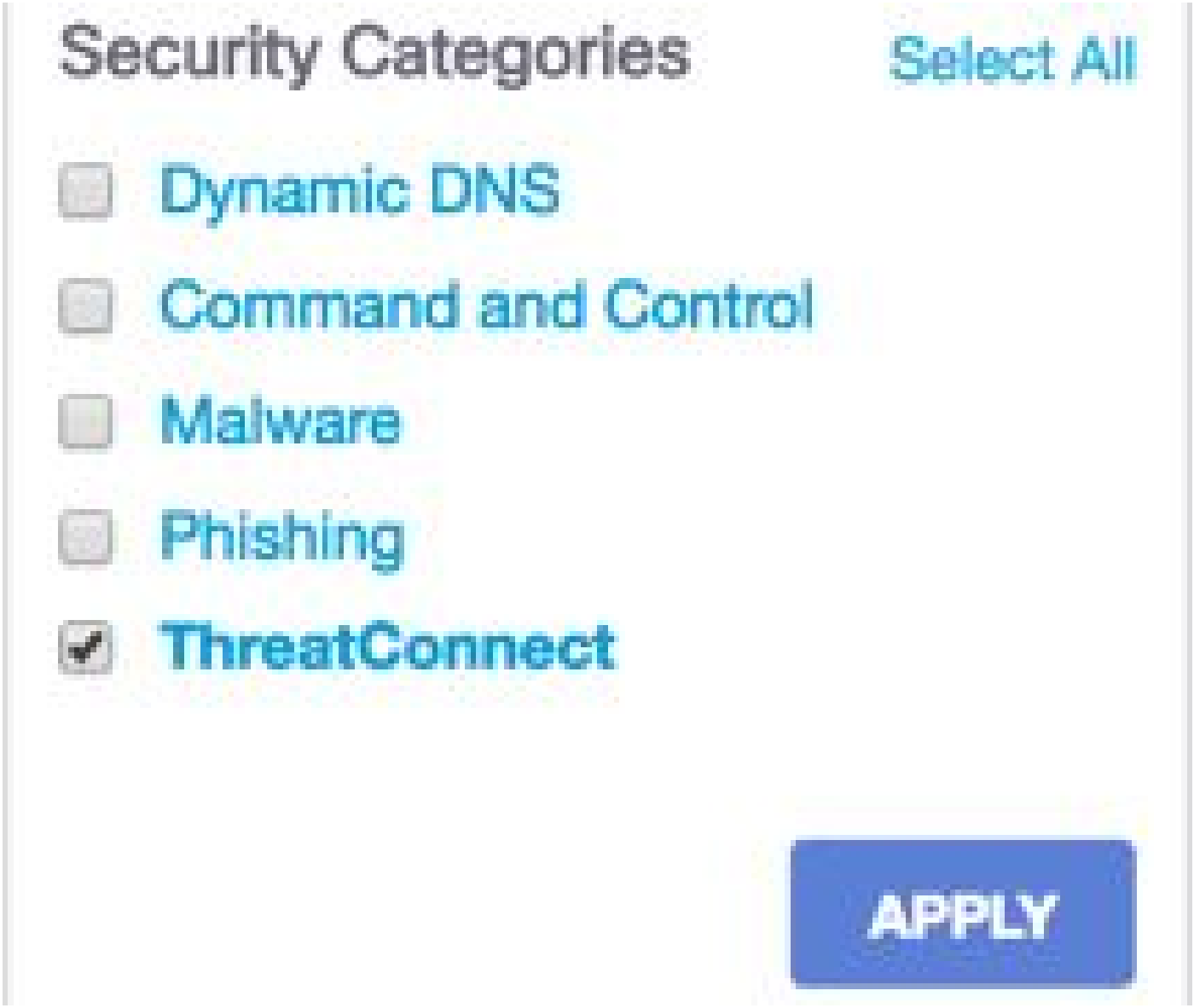
Berichte in Umbrella für ThreatConnect-Ereignisse

Berichte zu ThreatConnect-Sicherheitsereignissen

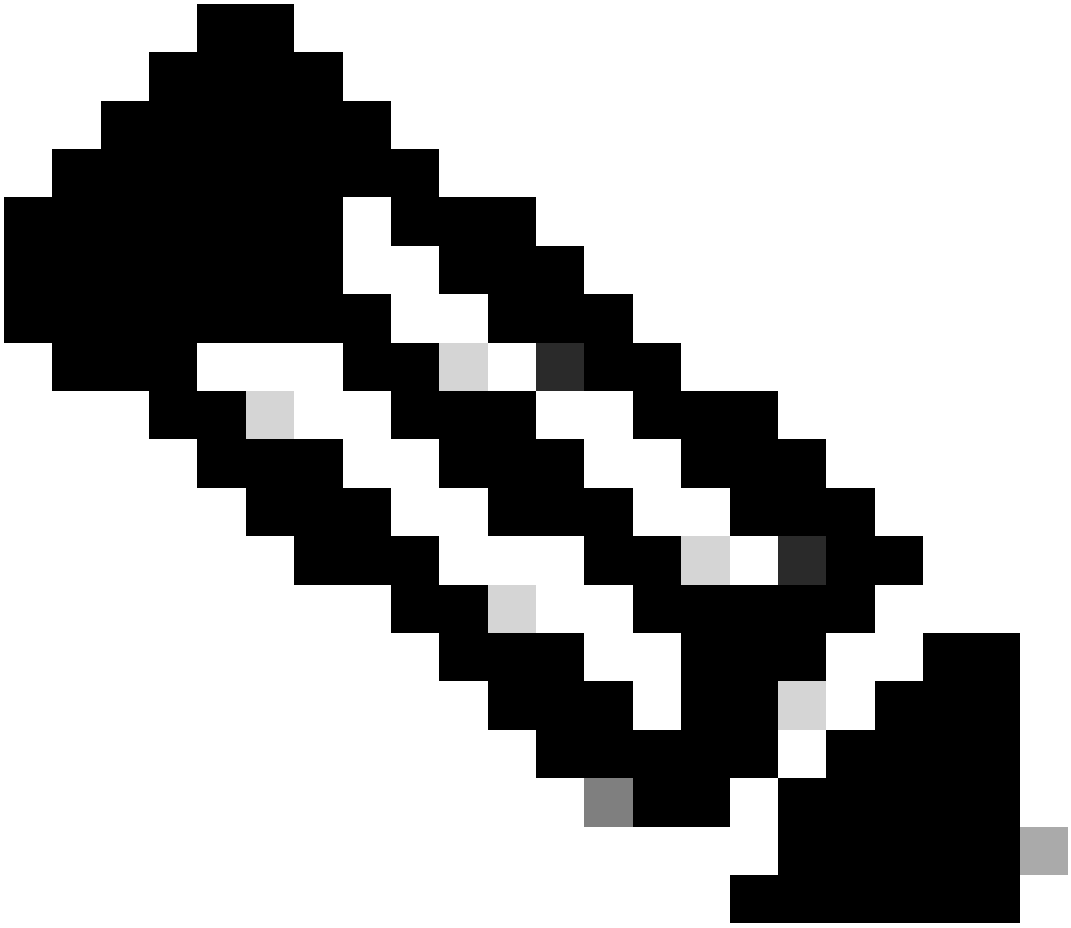
Die ThreatConnect-Zielliste ist eine der Sicherheitskategorielisten, über die Sie Berichte erstellen können. Die meisten oder alle Berichte verwenden die Sicherheitskategorien als Filter. Sie können beispielsweise Sicherheitskategorien filtern, sodass nur die mit ThreatConnect zusammenhängenden Aktivitäten angezeigt werden:

1. Navigieren Sie zu Auswertung > Aktivitätssuche.

2. Wählen Sie unter Sicherheitskategorien die Option ThreatConnect aus, um den Bericht so zu filtern, dass nur die Sicherheitskategorie für ThreatConnect angezeigt wird.



115014206603



Anmerkung: Wenn die ThreatConnect-Integration deaktiviert ist, wird sie nicht im Filter "Sicherheitskategorien" angezeigt.

3. Wählen Sie Anwenden.

Melden beim Hinzufügen von Domänen zur ThreatConnect-Zielliste

Das Admin-Audit-Protokoll enthält Ereignisse vom ThreatConnect-Dashboard, wenn Domänen zur Zielliste hinzugefügt werden. Ein Benutzer mit dem Namen "ThreatConnect-Konto", der auch mit dem ThreatConnect-Logo versehen ist, generiert die Ereignisse. Zu diesen Ereignissen gehören die hinzugefügte Domäne und der Zeitpunkt, zu dem sie hinzugefügt wurde.

Sie können Filter anwenden, um nur Änderungen an ThreatConnect aufzunehmen, indem Sie einen Filter für den Benutzer "ThreatConnect-Konto" anwenden.

Umgang mit unerwünschten Erkennungen oder Fehlalarmen

Zulassungslisten

Obwohl unwahrscheinlich, ist es möglich, dass Domänen, die automatisch von ThreatConnect hinzugefügt werden, eine unerwünschte Blockierung auslösen können, die Benutzer am Zugriff auf bestimmte Websites hindert. In einer solchen Situation empfiehlt Umbrella, die Domäne(n) einer Zulassungsliste hinzuzufügen, die Vorrang vor allen anderen Typen von Blocklisten hat, einschließlich der Sicherheitseinstellungen.

Es gibt zwei Gründe, warum dieser Ansatz vorzuziehen ist:

- Wenn das ThreatConnect-Dashboard die Domäne nach dem Entfernen erneut hinzugefügt hat, schützt die Zulassungsliste vor weiteren Problemen.
- Darüber hinaus zeigt die Zulassungsliste einen Verlaufsdatensatz problematischer Domänen an, die für forensische Untersuchungen oder Auditberichte verwendet werden können.

Standardmäßig gibt es eine globale Zulassungsliste, die auf alle Richtlinien angewendet wird. Durch Hinzufügen einer Domäne zur globalen Zulassungsliste wird die Domäne in allen Richtlinien zugelassen.

Wenn die Sicherheitseinstellung ThreatConnect im Blockmodus nur auf eine Teilmenge Ihrer verwalteten Umbrella-Identitäten angewendet wird (z. B. nur auf Roaming-Computer und mobile Geräte), können Sie eine spezifische Zulassungsliste für diese Identitäten oder Richtlinien erstellen.

So erstellen Sie eine Zulassungsliste:

1. Navigieren Sie zu Richtlinien > Ziellisten, und wählen Sie das Symbol Hinzufügen (+) aus.

2. Wählen Sie Zulassen und fügen Sie Ihre Domäne zur Liste hinzu.

3. Wählen Sie Speichern.

Nachdem die Zielliste gespeichert wurde, können Sie sie einer vorhandenen Richtlinie hinzufügen, die die Clients abdeckt, die von dem unerwünschten Block betroffen sind.

Löschen von Domänen aus der ThreatConnect-Zielliste

Neben jedem Domänennamen in der ThreatConnect-Zielliste befindet sich ein Symbol zum Löschen. Beim Löschen von Domänen können Sie die Liste der ThreatConnect-Ziele bereinigen, wenn eine unerwünschte Erkennung auftritt. Der Löschvorgang ist jedoch nicht permanent, wenn das ThreatConnect-Dashboard die Domäne erneut an Umbrella sendet.

So löschen Sie eine Domäne:

1. Navigieren Sie zu Richtlinien > Integrationen.

2. Wählen Sie ThreatConnect aus, um es zu erweitern.

3. Wählen Sie Siehe Domänen.

4. Suchen Sie nach dem Domänennamen, den Sie löschen möchten.

5. Wählen Sie das Symbol Löschen.

6. Wählen Sie Schließen und dann Speichern.

Im Fall einer unerwünschten Erkennung oder eines Fehlalarms empfiehlt Umbrella, sofort eine Zulassungsliste in Umbrella zu erstellen und anschließend das Fehlalarmen im ThreatConnect-Dashboard zu beheben. Später können Sie die Domäne aus der ThreatConnect-Zielliste entfernen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.