Integration von ThreatQ mit Umbrella

Inhalt

Einleitung

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

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

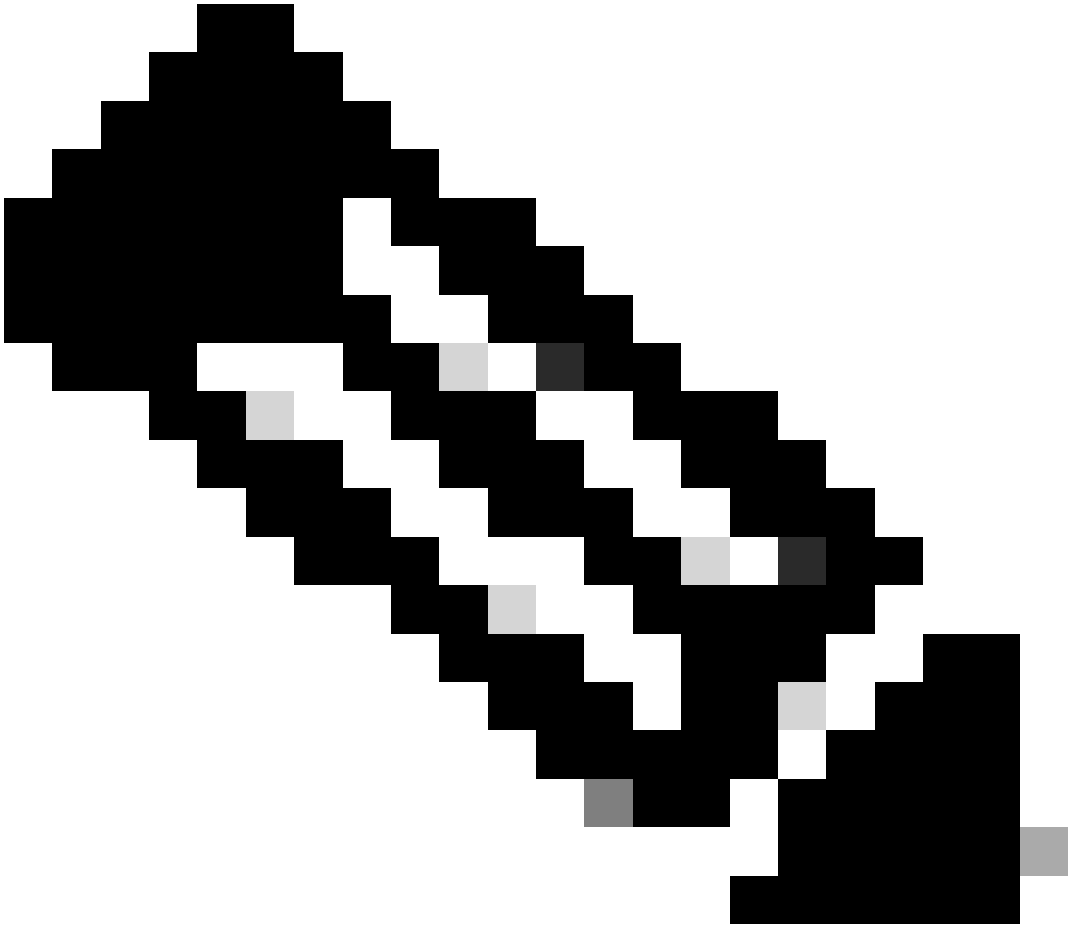
Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

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.

ThreatQ und Cisco Umbrella Integration - Überblick

Durch die Integration von ThreatQ 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 ThreatQ für die Kommunikation mit Umbrella konfiguriert wird, damit Sicherheitsereignisse aus dem ThreatQ-TIPP in Richtlinien integriert werden, die auf Clients angewendet werden können, die durch Cisco Umbrella geschützt sind.



Anmerkung: Die ThreatQ-Integration ist nur in [bestimmten Cisco Umbrella-Paketen]

---

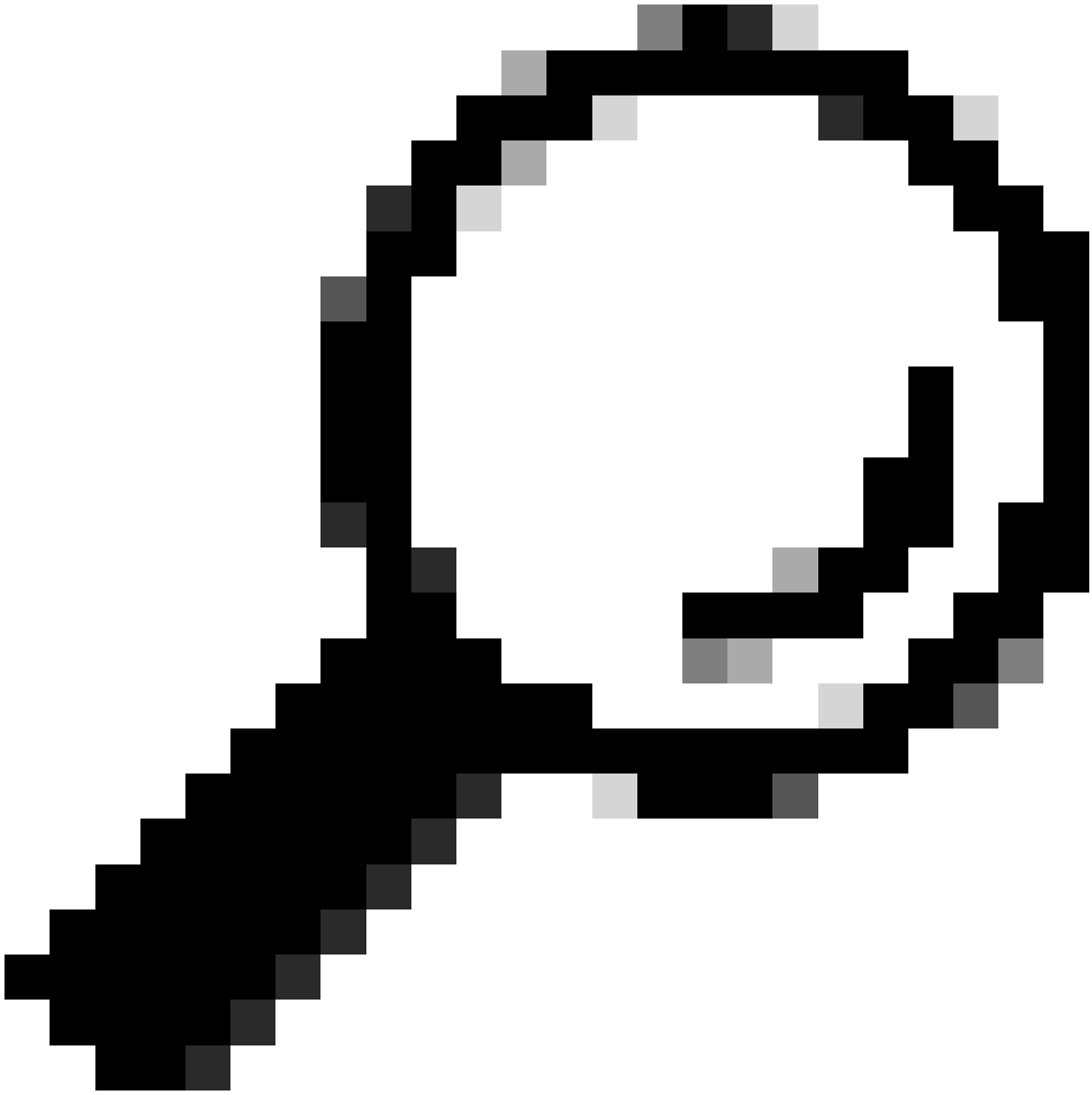
enthalten. Wenn Sie nicht über das erforderliche Paket verfügen und ThreatQ integrieren möchten, wenden Sie sich an Ihren Cisco Umbrella-Vertreter. Wenn Sie über das richtige Cisco Umbrella-Paket verfügen, ThreatQ jedoch nicht als Integration für Ihr Dashboard angezeigt wird, wenden Sie sich an den Cisco Umbrella Support.

Integrationsfunktion

Die ThreatQ-Plattform sendet zunächst die gefundenen Cyber Threat Intelligence-Daten, z. B. Domänen, die Malware hosten, sowie 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 ThreatQ eine Bedrohung darstellen, wird die Domänenadresse im Rahmen einer Sicherheitseinstellung, die auf eine beliebige Umbrella-Richtlinie angewendet werden kann, zur ThreatQ-Zielliste hinzugefügt. Diese Richtlinie wird sofort auf alle Anforderungen angewendet, die von Geräten mithilfe von Richtlinien mit der ThreatQ-Zielliste gestellt werden.

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



Tipp: Während Cisco Umbrella nach besten Kräften versucht, bekanntermaßen sichere Domains (z. B. Google und Salesforce) zu validieren und zuzulassen, empfehlen wir, Domains, die niemals blockiert werden sollen, gemäß Ihrer Richtlinie zur globalen Zulassungsliste oder anderen Ziellisten hinzuzufügen, um unerwünschte Unterbrechungen zu vermeiden. Beispiele:

- Die Startseite Ihres Unternehmens
- Domänen, die von Ihnen bereitgestellte Dienste darstellen und sowohl interne als auch externe Datensätze enthalten können. Beispiel: "mail.myservicedomain.com" und "portal.myotherservicedomain.com".
- Weniger bekannte Cloud-basierte Anwendungen, von denen Cisco Umbrella abhängt, werden nicht automatisch für die Domänenvalidierung validiert. Beispiel: "localcloudservice.com".

Diese Domänen können der globalen Zulassungsliste hinzugefügt werden, die unter

Richtlinien > Ziellisten in Cisco Umbrella zu finden ist.

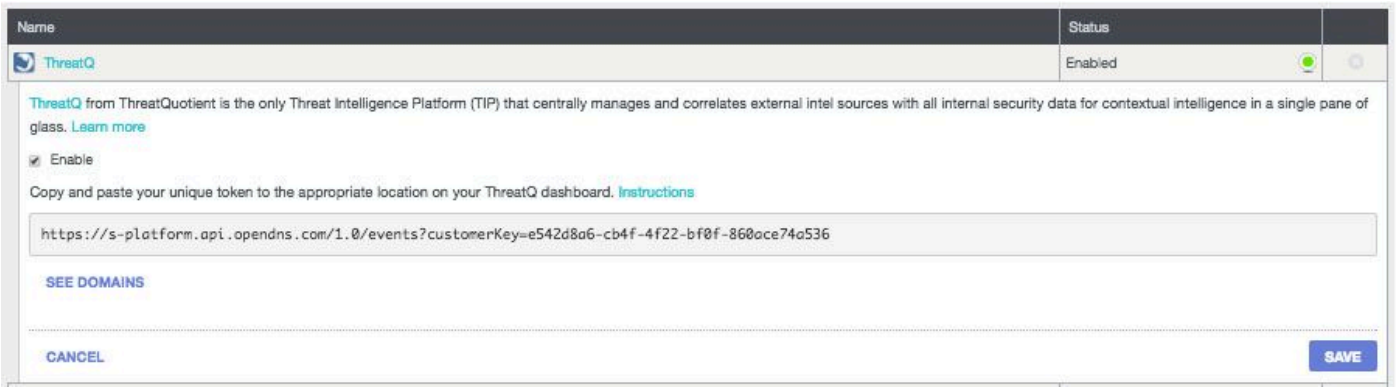
Generierung von Umbrella-Skripts und API-Token

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 Einstellungen > Integrationen, und wählen Sie ThreatQ in der Tabelle aus, um es zu erweitern.

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



Sie benötigen die URL später, wenn Sie ThreatQ zum Senden von Daten an Umbrella konfigurieren. Kopieren Sie die URL, und gehen Sie zu Ihrem ThreatQ-Dashboard.

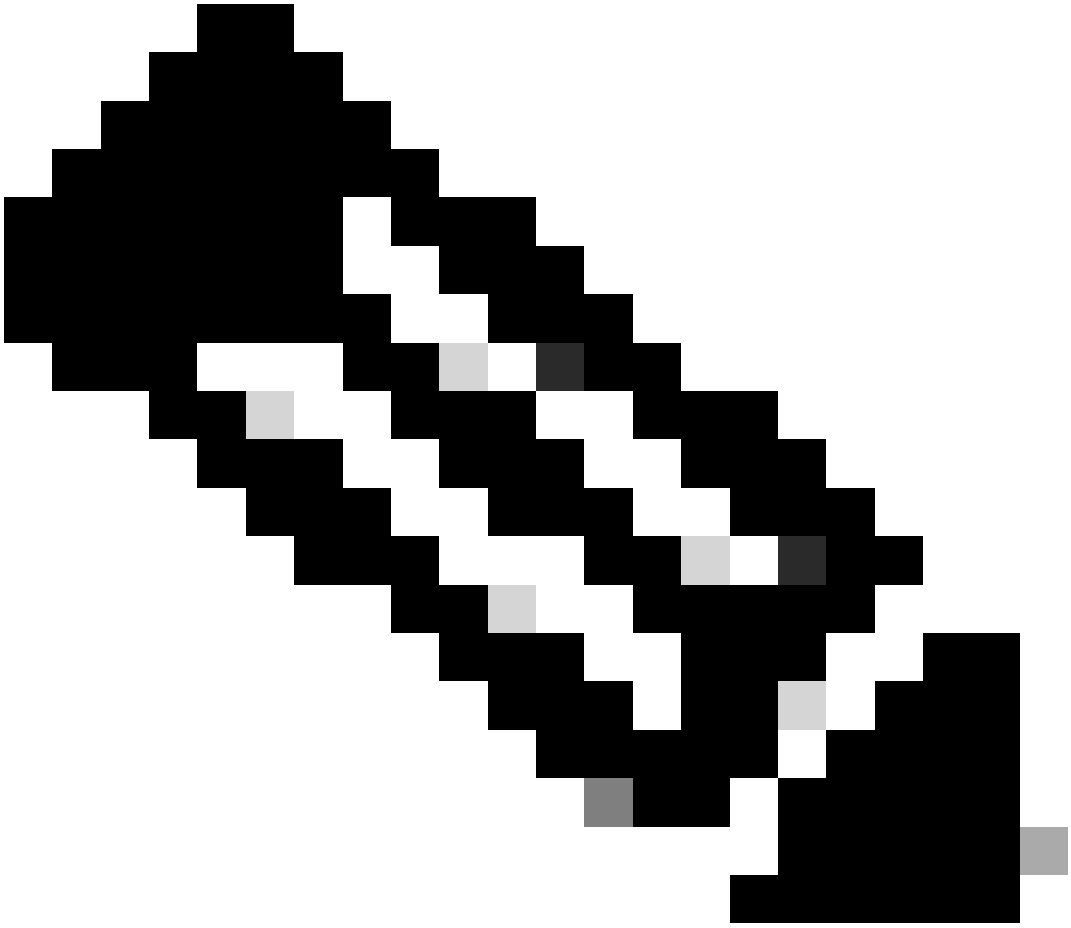
Konfigurieren von ThreatQ für die Kommunikation mit Umbrella

Melden Sie sich bei Ihrem ThreatQ-Dashboard an, und fügen Sie die URL in den entsprechenden Bereich für die Verbindung mit Umbrella hinzu.

Die genauen Anweisungen variieren, und Umbrella empfiehlt, den ThreatQ-Support zu kontaktieren, wenn Sie sich nicht sicher sind, wie oder wo Sie API-Integrationen in ThreatQ konfigurieren sollen.

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

Mit der Zeit füllen Ereignisse aus Ihrem ThreatQ-Dashboard eine bestimmte Zielliste aus, die auf Richtlinien als ThreatQ-Sicherheitskategorie angewendet werden kann. Die Zielliste und die Sicherheitskategorie befinden sich standardmäßig im Überwachungsmodus, d. h., sie werden nicht auf Richtlinien angewendet und können nicht zu Änderungen an Ihren vorhandenen Umbrella-Richtlinien führen.



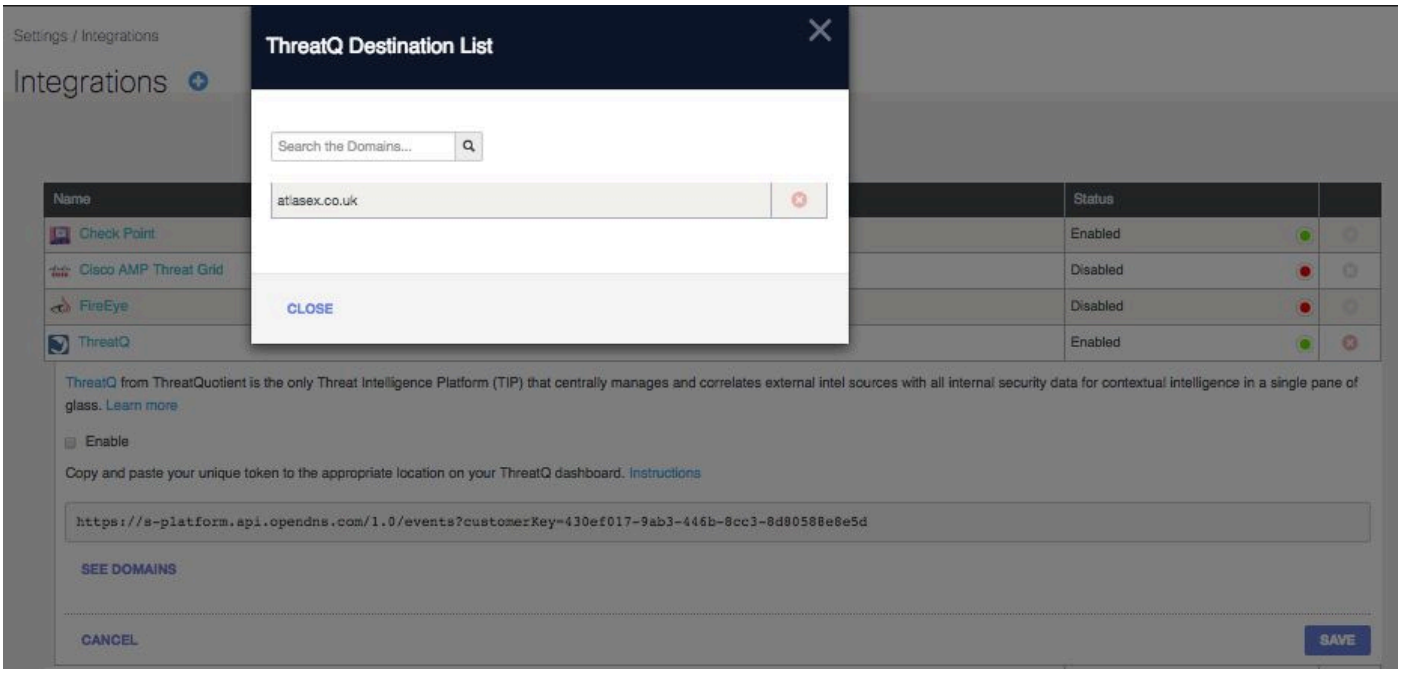
Anmerkung: Der Überwachungsmodus kann je nach Bereitstellungsprofil und Netzwerkkonfiguration so lange aktiviert werden, wie dies erforderlich ist.

Zielliste überprüfen

Sie können die ThreatQ-Zielliste in Umbrella jederzeit einsehen:

1. Navigieren Sie zu Einstellungen > Integrationen.

2. Erweitern Sie ThreatQ in der Tabelle, und wählen Sie Siehe Domänen aus.



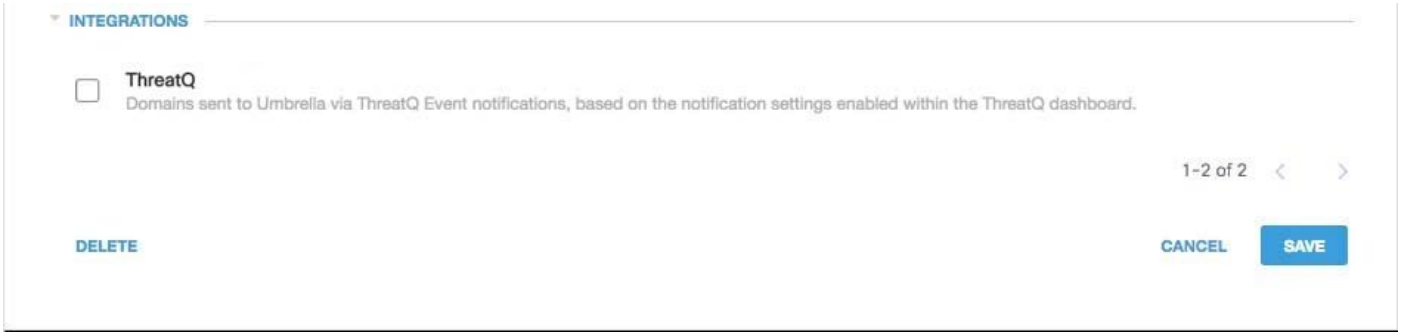
Sicherheitseinstellungen für eine Richtlinie überprüfen

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

1. Navigieren Sie zu Richtlinien > Sicherheitseinstellungen.

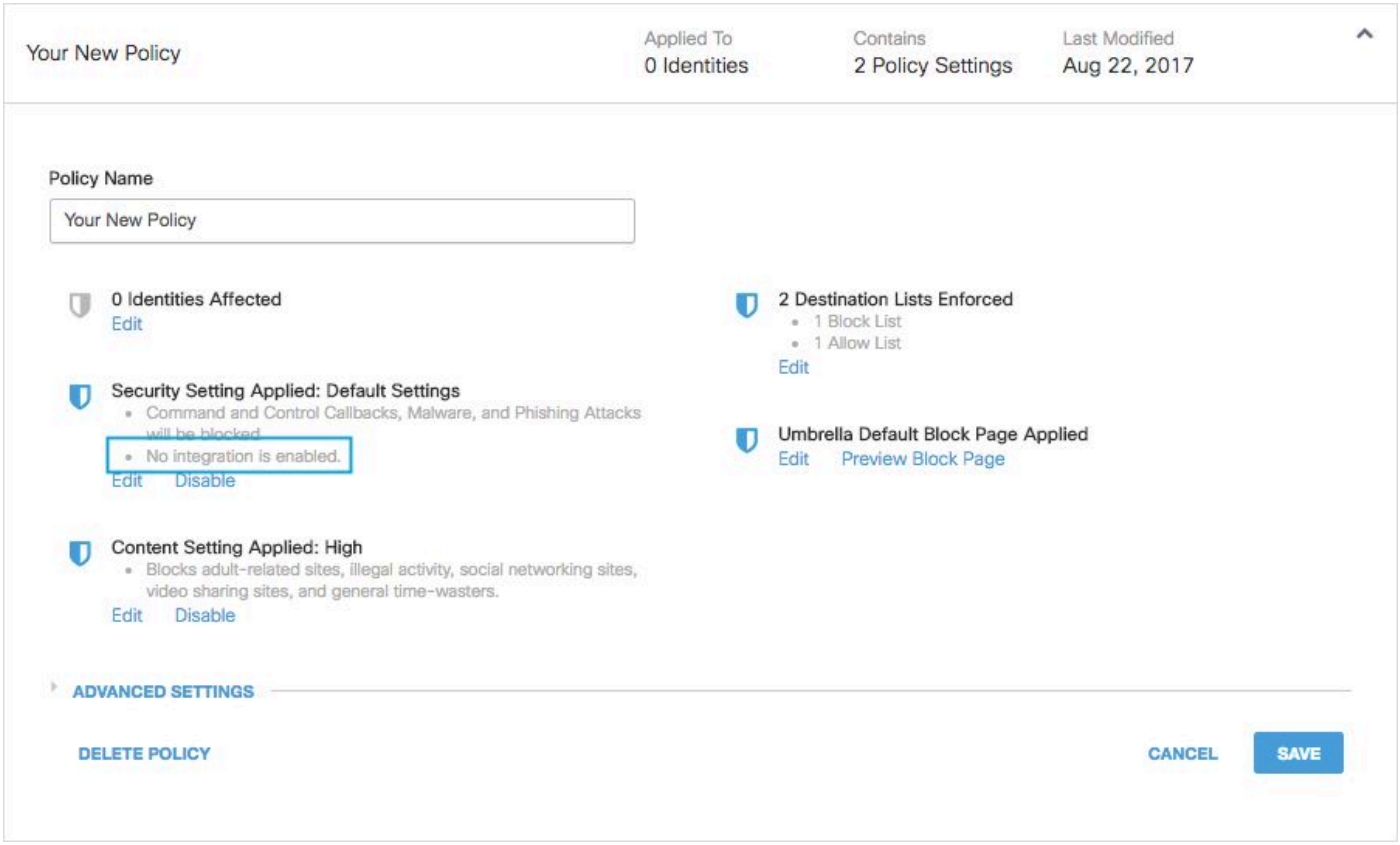
2. Wählen Sie eine Sicherheitseinstellung in der Tabelle aus, um sie zu erweitern.

3. Navigieren Sie zu Integrations, um die Einstellung ThreatQ zu finden.



115014040286

Sie können die Integrationsinformationen auch auf der Seite Übersicht über die Sicherheitseinstellungen überprüfen.



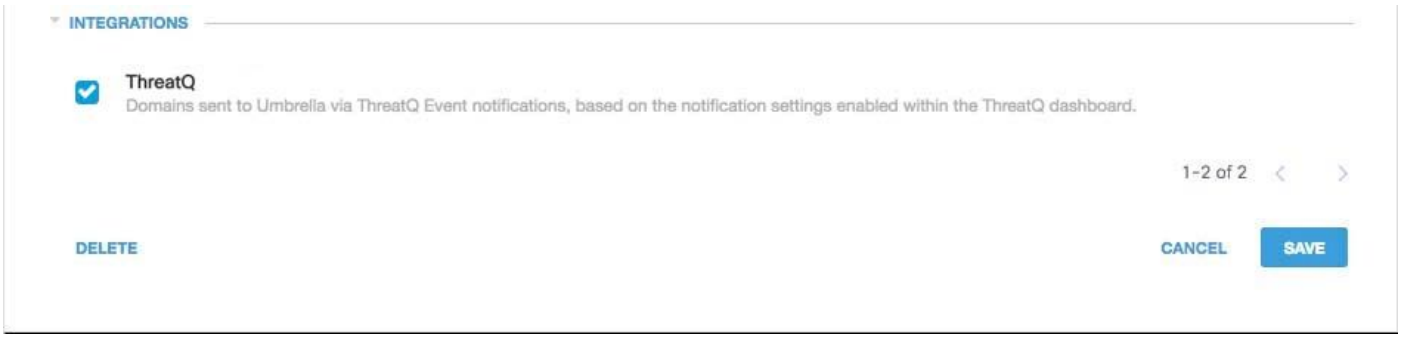
25464141748116

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

Wenn Sie diese zusätzlichen Sicherheitsbedrohungen von Clients erzwungen haben, die von Umbrella verwaltet werden, können Sie die Sicherheitseinstellung einer vorhandenen Richtlinie ändern oder eine neue Richtlinie erstellen, die höher als die Standardrichtlinie ist, um sicherzustellen, dass sie zuerst erzwungen wird:

1.Navigieren Sie zu Richtlinien > Sicherheitseinstellungen.

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



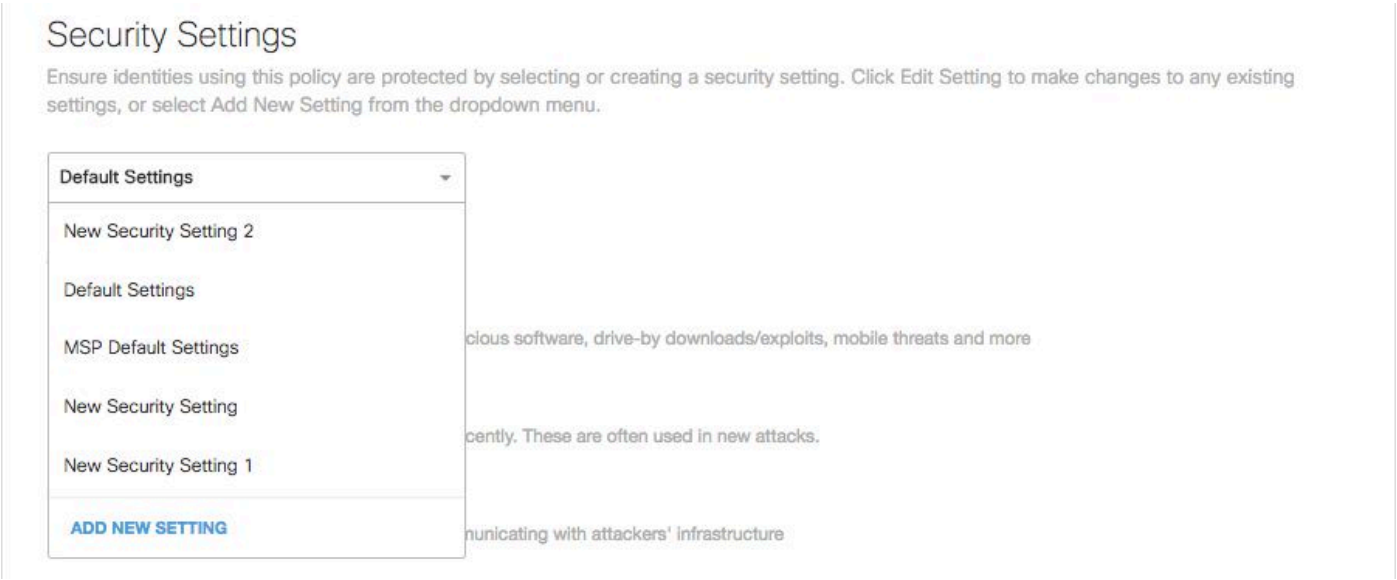
115014207403

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

1. Navigieren Sie zu Richtlinien > Richtlinienliste.

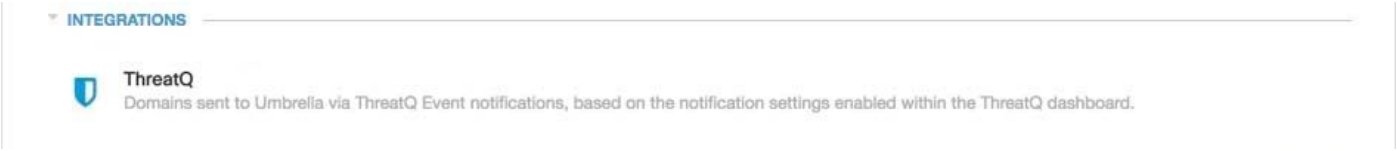
2. Erweitern Sie eine Richtlinie, und wählen Sie unter Sicherheitseinstellung angewendet die Option Bearbeiten aus.

3. Wählen Sie im Pulldown-Menü Sicherheitseinstellungen eine Sicherheitseinstellung aus, die die Einstellung ThreatQ enthält.



25464141787668

Das Schildsymbol unter Integrationen wird auf blau aktualisiert.



115014040506

4. Wählen Sie Festlegen und Zurücksenden.

Die in den Sicherheitseinstellungen für ThreatQ enthaltenen ThreatQ-Domänen werden jetzt für Identitäten mithilfe der Richtlinie blockiert.

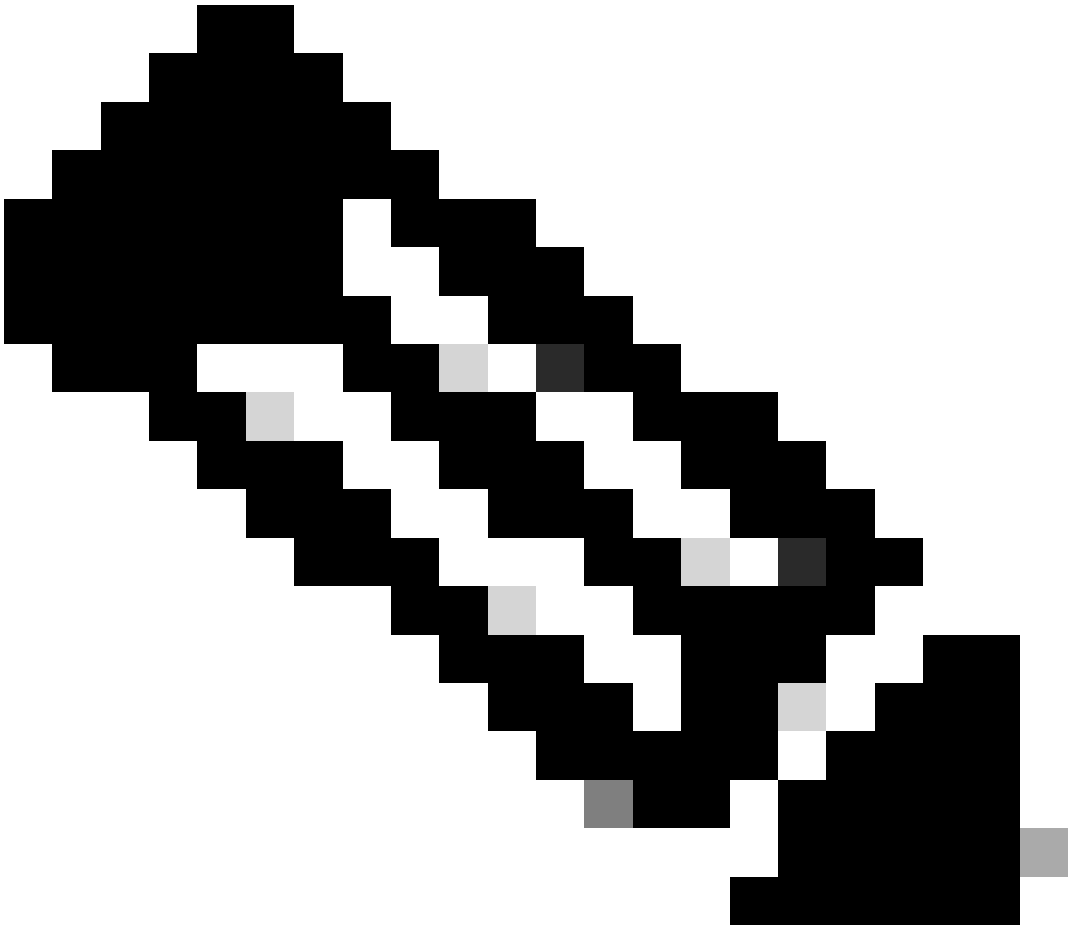
Umbrella-Berichterstellung für ThreatQ-Ereignisse

Berichte zu ThreatQ-Sicherheitsereignissen

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

1. Navigieren Sie zu Auswertung > Aktivitätssuche.

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



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

115014207603

3. Wählen Sie Anwenden.

Melden beim Hinzufügen von Domänen zur ThreatQ-Zielliste

Das Umbrella Admin Audit-Protokoll enthält Ereignisse aus dem ThreatQ Dashboard, wenn es Domänen zur Zielliste hinzufügt. Ein Benutzer mit dem Namen "ThreatQ-Konto", der auch mit dem ThreatQ-Logo versehen ist, generiert die Ereignisse. Zu diesen Ereignissen gehören die hinzugefügte Domäne und der Zeitpunkt, zu dem sie hinzugefügt wurde. Das Umbrella Admin Audit-Protokoll finden Sie unter Reporting > Admin Audit Log.

Sie können Filter anwenden, um nur ThreatQ-Änderungen einzubeziehen, indem Sie einen Filter für den Benutzer des ThreatQ-Kontos anwenden.

Umgang mit unerwünschten Erkennungen oder Fehlalarmen

Zulassungslisten

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

Dieser Ansatz ist aus zwei Gründen vorzuziehen:

- Wenn das ThreatQ-Dashboard die Domäne nach dem Entfernen erneut hinzufügen sollte, schützt die Zulassungsliste vor weiteren Problemen.
- Zweitens zeigt die Zulassungsliste einen Verlaufsdatensatz problematischer Domänen an, die für forensische Untersuchungen oder Prüfberichte 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 ThreatQ-Sicherheitseinstellung 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 Policys > Ziellisten, und wählen Sie das Symbol Hinzufügen aus.

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

3. Wählen Sie Speichern.

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

Löschen von Domänen aus der ThreatQ-Liste

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

So löschen Sie eine Domäne:

1. Navigieren Sie zu Einstellungen > Integrationen, und wählen Sie dann ThreatQ aus, um es zu erweitern.

2. Wählen Sie Siehe Domänen.

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

4. Wählen Sie das Symbol Löschen.

5. Wählen Sie Schließen.

6. Wählen Sie Speichern.

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