Integration von ZeroFOX in Umbrella

Inhalt

Einleitung

Dieses Dokument beschreibt, wie ZeroFOX Enterprise mit Umbrella integriert werden kann, damit die Sicherheitsereignisse auf die durch Umbrella geschützten Clients angewendet werden können.

ZeroFOX Enterprise und Cisco Umbrella Integration - Überblick

Durch die Integration von ZeroFOX Enterprise mit Cisco Umbrella können Sicherheitsbeauftragte und Administratoren den Schutz vor aktuellen Social Media-basierten Bedrohungen auf mobile Laptops, Tablets oder Telefone ausdehnen und gleichzeitig eine weitere Durchsetzungsebene für ein verteiltes Unternehmensnetzwerk bereitstellen.

Cisco Umbrella- und ZeroFox-Integration: Wie funktioniert es?

ZeroFOX Enterprise leitet alle gefundenen Bedrohungen, wie z. B. Social Media-basierte Cyber-Bedrohungen, wie zielgerichtete Malware, Phishing, Social Engineering, Identitätswechsel und andere betrügerische oder bösartige Aktivitäten, an Cisco Umbrella weiter, um diese weltweit durchzusetzen.

Umbrella validiert die Bedrohung, um sicherzustellen, dass sie einer Richtlinie hinzugefügt werden kann. Wenn die Informationen von ZeroFOX als Bedrohung bestätigt werden, wird die Domain-Adresse der ZeroFOX-Zielliste als Teil einer Sicherheitseinstellung hinzugefügt, die auf jede Umbrella-Richtlinie angewendet werden kann. Diese Richtlinie wird sofort auf alle Anforderungen angewendet, die von Geräten gestellt werden, die dieser Richtlinie zugewiesen sind.

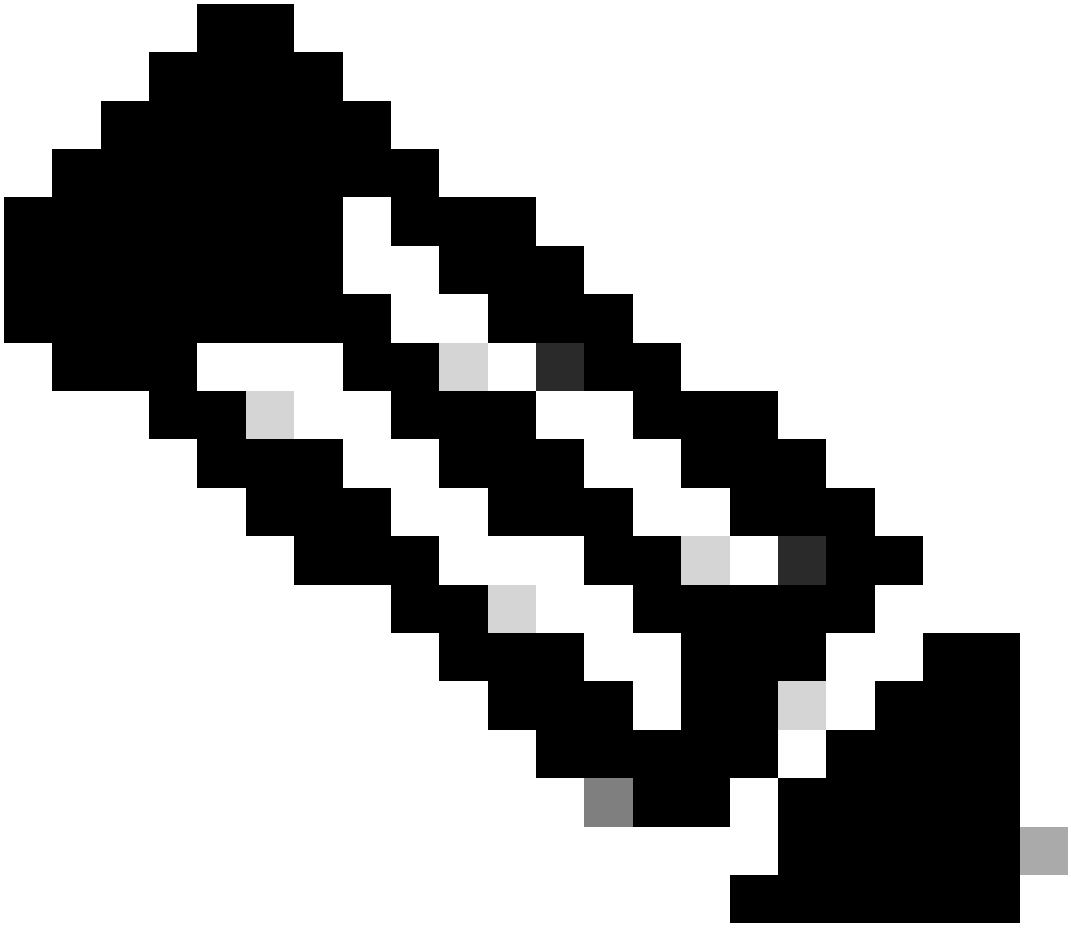
In Zukunft parst Cisco Umbrella automatisch ZeroFOX-Warnungen und fügt bösartige Websites zur ZeroFOX-Zielliste hinzu. So wird die ZeroFOX-Intelligenz auf alle Remote-Benutzer und -Geräte ausgeweitet und eine weitere Ebene der Durchsetzung für Ihr Unternehmensnetzwerk bereitgestellt.

Dies wird durch die folgenden einfachen Einrichtungsschritte erreicht:

1. Aktivieren Sie die Integration in Umbrella, um ein API-Token zu generieren.
2. Fügen Sie dieses API-Token in Ihr ZeroFOX-Konto ein.
3. Setzen Sie ZeroFOX so, dass es unter den Sicherheitseinstellungen für die gewünschten Richtlinien blockiert wird.

Voraussetzungen

- ZeroFOX Enterprise Administratorrechte
- Administratorrechte für Umbrella Dashboard
- Für das Umbrella Dashboard muss die ZeroFOX-Integration aktiviert sein.



Anmerkung: Die ZeroFOX-Integration ist nur im Umbrella Platform-Paket enthalten. Wenn Sie nicht über das Plattform-Paket verfügen und eine ZeroFOX-Integration wünschen, wenden Sie sich an Ihren Cisco Umbrella-Vertreter. Wenn Sie das Plattform-Paket haben, aber ZeroFOX nicht als Integration für Ihr Dashboard sehen, wenden Sie sich bitte an den Umbrella Support.

Wichtig: Während Umbrella sich bemüht, bekanntermaßen sichere Domains (z. B. Google und Salesforce) zu validieren und zuzulassen, um unerwünschte Unterbrechungen zu vermeiden, schlagen wir vor, Domains, die nicht blockiert werden sollen, 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.

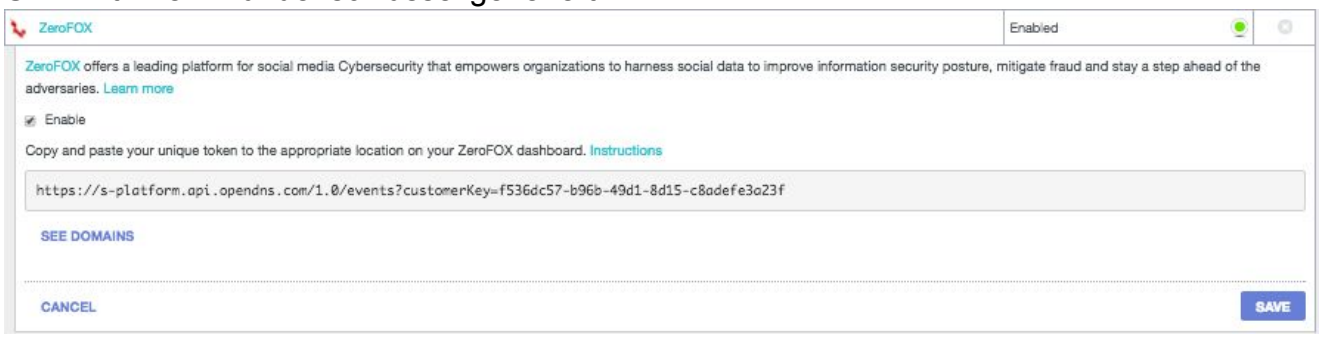
- Weniger bekannte Cloud-Anwendungen, von denen Sie stark abhängig sind, dass Umbrella diese nicht kennen oder in ihre automatische Domänenvalidierung einbeziehen kann. Beispiel: localcloudservice.com.

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

Schritt 1: Generierung von Umbrella-Skripts und API-Token

Suchen Sie zunächst in Umbrella Ihre eindeutige URL für die ThreatQ-Appliance, mit der Sie kommunizieren können.

1. Melden Sie sich als Administrator bei Ihrem Umbrella Dashboard an, navigieren Sie zu Einstellungen > Integrationen und klicken Sie in der Tabelle auf "ZeroFOX", um es zu erweitern.
2. Aktivieren Sie Aktivieren, und klicken Sie dann auf Speichern. Dadurch wird eine eindeutige URL mit Ihrem Kundenschlüssel generiert.

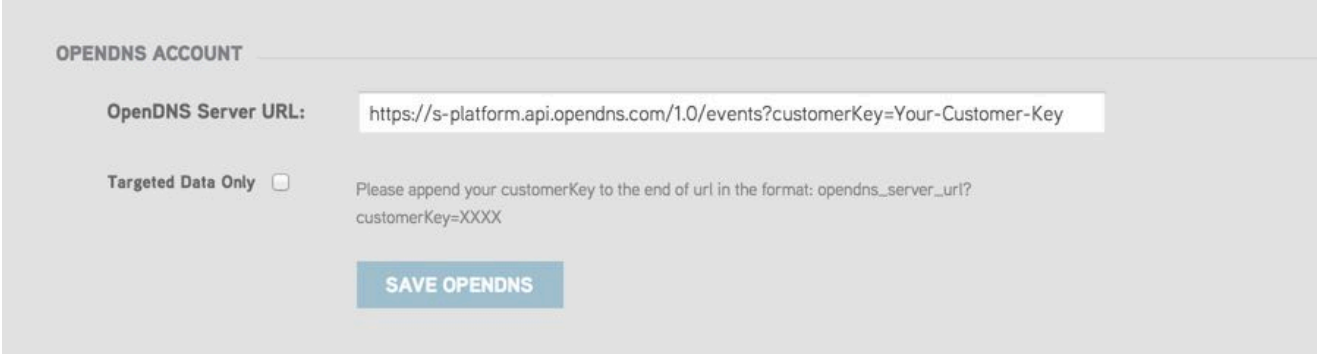


   Sie benötigen die URL später, wenn Sie ZeroFOX konfigurieren. Kopieren Sie die URL, und gehen Sie zu Ihrem ThreatQ-Dashboard.

Phase 2: Einrichten Ihres ZeroFOX Enterprise-Dashboards zum Senden von Informationen an Umbrella

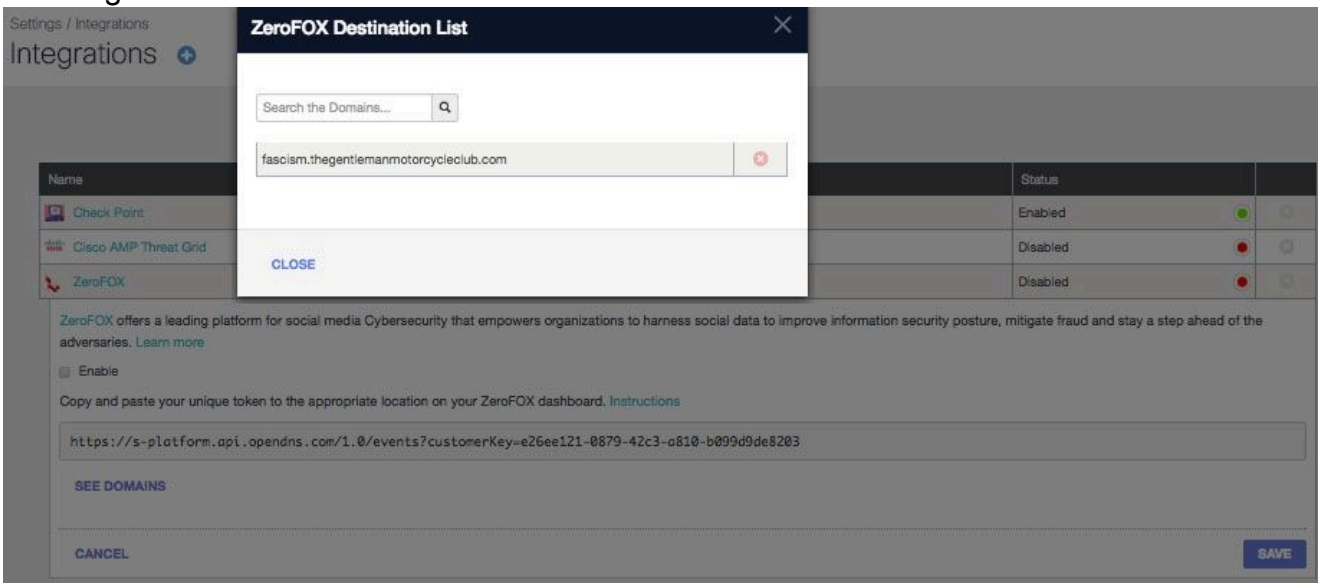
Im nächsten Schritt fügen Sie die URL, die Sie in Schritt eins kopiert haben, dem ZeroFOX Dashboard hinzu.

1. Klicken Sie auf das Zahnrad-Symbol im Zerofox-Dashboard, und wählen Sie dann Kontoeinstellungen aus.
2. Blättern Sie in der Integrationsliste nach unten, bis Sie die OpenDNS-Kontoinformationen sehen, und fügen Sie die URL von Umbrella in das Feld OpenDNS Server URL ein.
3. Nach der ersten Aktivierung der Integration empfehlen wir, die Option Nur Zieldaten zu aktivieren.



Schritt 3: Einrichtung von ZeroFOX-Ereignissen, die innerhalb von Umbrella blockiert werden sollen

1. Melden Sie sich als Administrator wieder bei Ihrem Umbrella Dashboard an.
2. Navigieren Sie zu Einstellungen > Integrationen und klicken Sie auf "ZeroFOX" in der Tabelle, um es zu erweitern.
3. Klicken Sie auf Domains anzeigen.
   Damit wird eine Liste von Domains erweitert, die die letzten Stunden an Ereignissen von Ihrem ZeroFOX-Konto umfasst. Ab diesem Zeitpunkt wird eine durchsuchbare Liste mit Suchergebnissen erweitert.

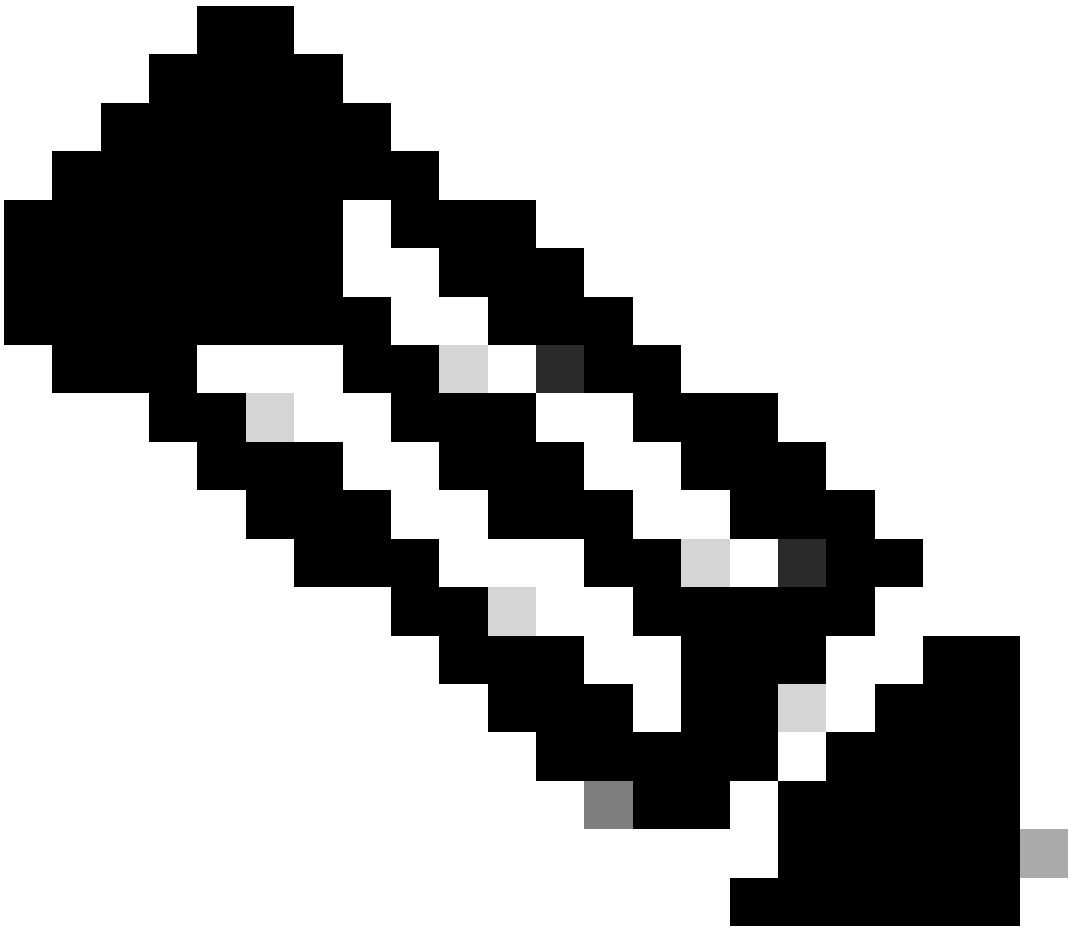


Der nächste Schritt ist, die Ereignisse zu beobachten und zu überprüfen, die zu Ihrer neuen ZeroFOX Sicherheitskategorie hinzugefügt wurden.

Beobachtung von Ereignissen, die der ZeroFOX-Sicherheitskategorie im Überwachungsmodus hinzugefügt wurden

Die Ereignisse von ZeroFOX Enterprise beginnen, eine bestimmte Zielliste auszufüllen, die als ZeroFOX-Sicherheitskategorie auf Richtlinien angewendet werden kann. Die Zielliste und die Sicherheitskategorie befinden sich standardmäßig im Überwachungsmodus und werden nicht auf Richtlinien angewendet. Dies führt 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

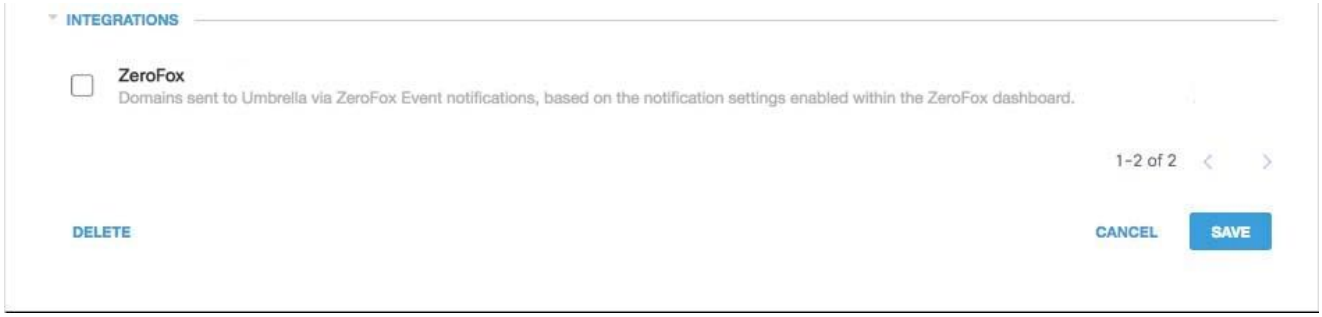
Sie können die ZeroFox Zielliste jederzeit einsehen.

1. Navigieren Sie zu Einstellungen > Integrationen.
2. Erweitern Sie "ZeroFOX" in der Tabelle und klicken Sie auf Domains anzeigen.

Sicherheitseinstellungen für eine Richtlinie überprüfen

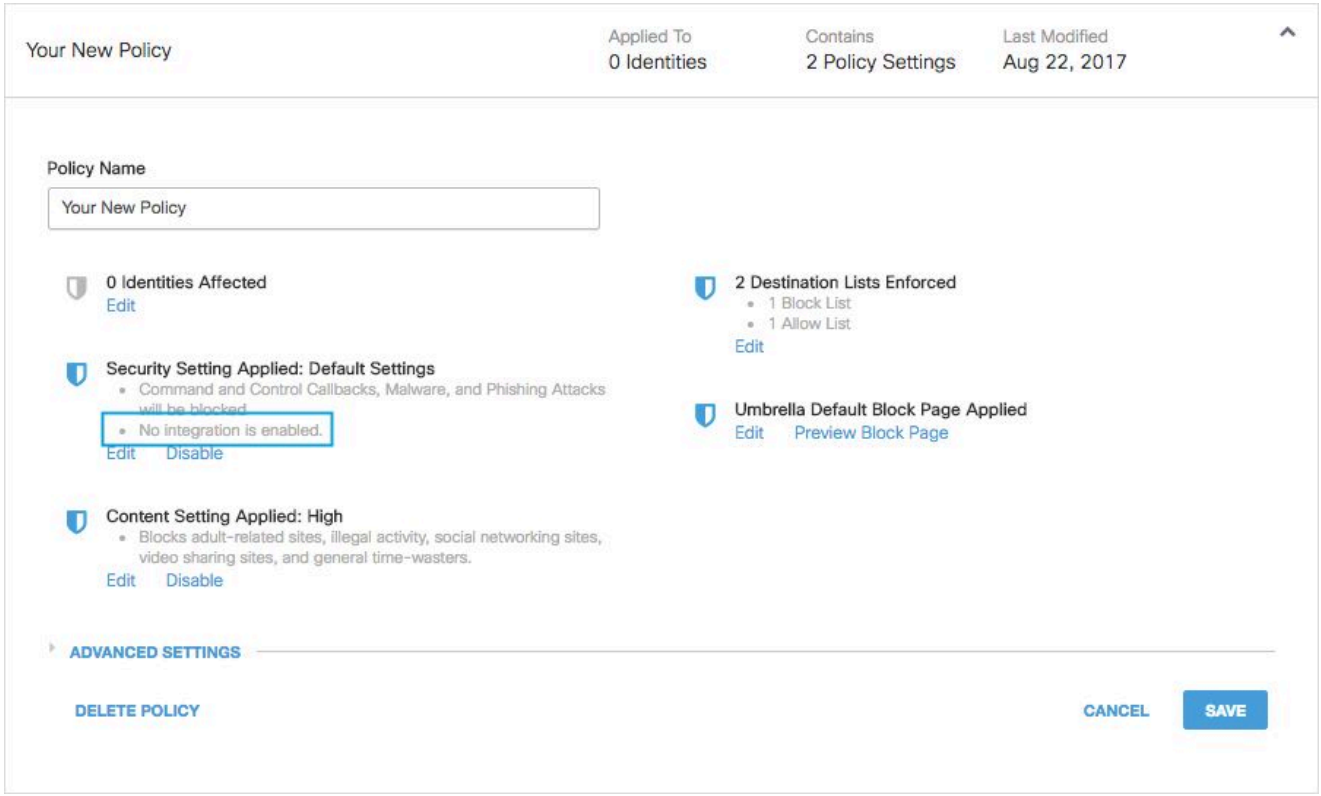
Sie können die Sicherheitseinstellungen, die für eine Richtlinie aktiviert werden können, jederzeit überprüfen.

1. Navigieren Sie zu Richtlinien > Sicherheitseinstellungen.
2. Klicken Sie auf eine Sicherheitseinstellung in der Tabelle, um sie zu erweitern, und blättern Sie zu Integrations, um die Einstellung ZeroFOX zu finden.



115014041606

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



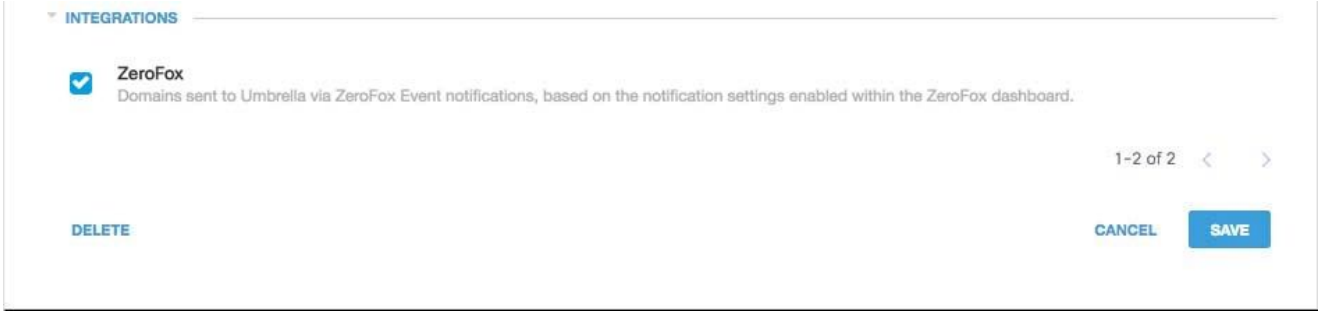
25464154913556

Anwenden der ZeroFOX-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 höher als Ihre

Standardrichtlinie ist, um sicherzustellen, dass sie zuerst durchgesetzt wird.

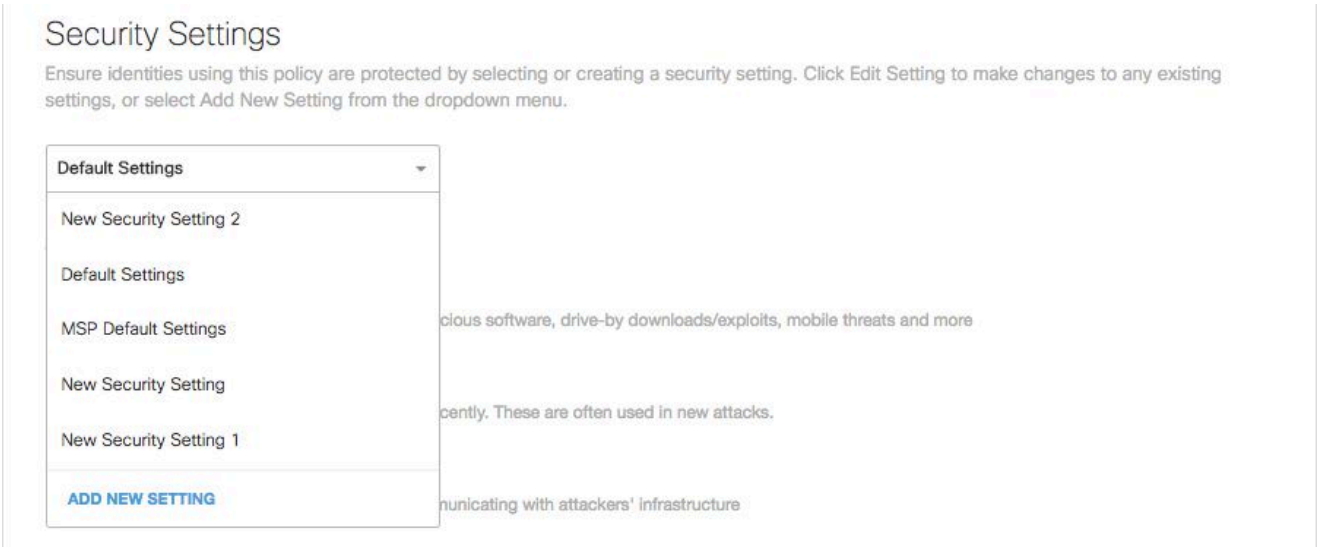
1. Navigieren Sie zu Policies > Security Settings, und aktivieren Sie unter Integrations die Option ZeroFOX, und klicken Sie auf Save.



115014042806

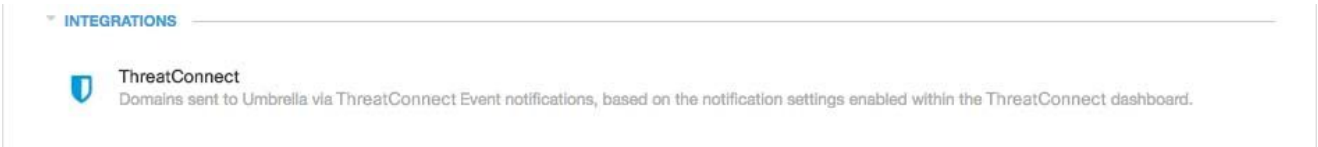
Fügen Sie anschließend im Richtlinien-Assistenten eine Sicherheitseinstellung zu der Richtlinie hinzu, die Sie bearbeiten:

1. Navigieren Sie zu Richtlinien > Richtlinienliste.
2. Erweitern Sie eine Richtlinie, und klicken Sie unter "Sicherheitseinstellung angewendet" auf Bearbeiten.
3. Wählen Sie im Pulldown-Menü Sicherheitseinstellungen eine Sicherheitseinstellung aus, die auch die Einstellung ThreatConnect enthält.



25464147943700

Das Schildsymbol unter Integrationen wird blau angezeigt.



25464147957652

4. Klicken Sie auf Festlegen und Zurücksenden.

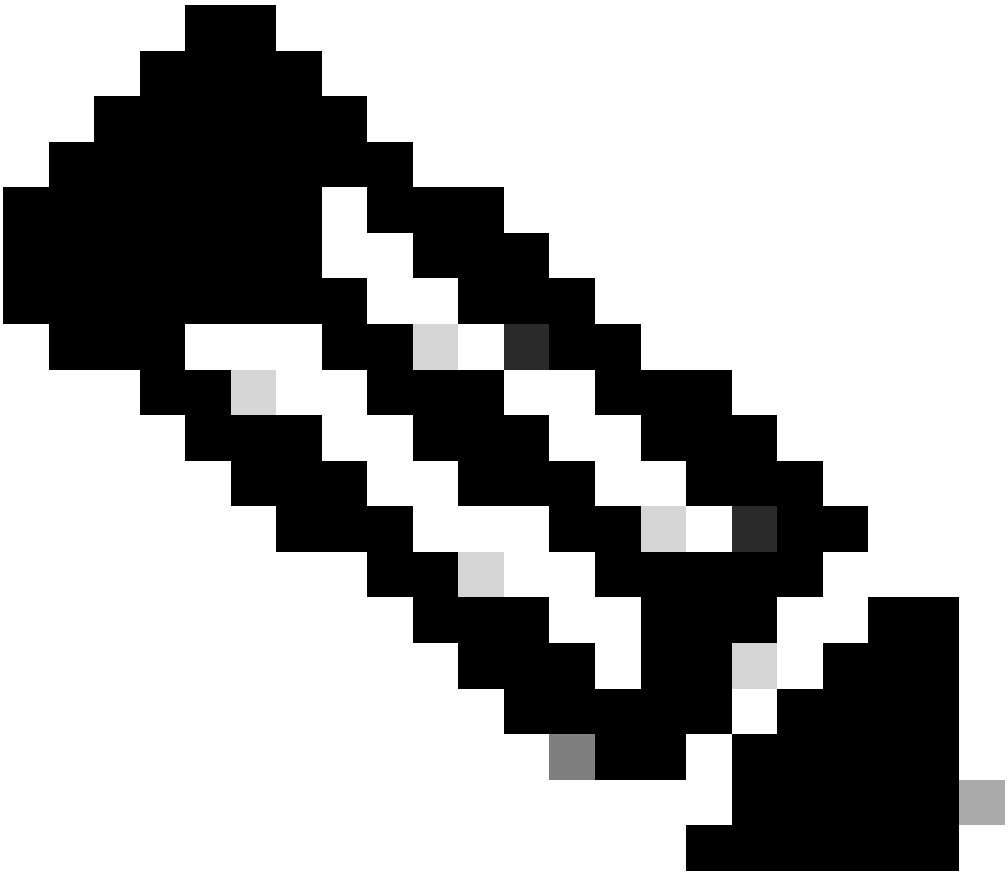
ZeroFOX-Domänen, die in den Sicherheitseinstellungen für ZeroFOX enthalten sind, werden für diese Identitäten gesperrt, die diese Richtlinie verwenden.

Reporting in Umbrella für ZeroFOX Events

Berichte zu ZeroFOX Security-Ereignissen

Die ZeroFOX-Zielliste ist eine der Sicherheitskategorielisten, über die Sie berichten können. Die meisten oder alle Berichte verwenden die Sicherheitskategorien als Filter. Sie können beispielsweise Sicherheitskategorien filtern, sodass nur Aktivitäten im Zusammenhang mit ZeroFOX angezeigt werden.

1. Navigieren Sie zu Reporting > Activity Search, und wählen Sie unter Security Categories die Option ZeroFOX aus, um den Bericht so zu filtern, dass nur die Sicherheitskategorie für ZeroFOX angezeigt wird.



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

115014043046

2. Klicken Sie auf Apply (Anwenden).

Melden beim Hinzufügen von Domänen zur ZeroFOX-Zielliste

Das Umbrella Admin Audit-Protokoll enthält Ereignisse von Ihrem ZeroFOX-Konto, da es der Zielliste Domänen hinzufügt.

Das Umbrella Admin Audit log (Umbrella-Administratorüberwachungsprotokoll) finden Sie unter Reporting > Admin Audit Log (Berichte > Administratorüberwachungsprotokoll). Um einen Bericht darüber zu erstellen, wann eine Domäne hinzugefügt wurde, filtern Sie, um nur ZeroFOX-Änderungen einzubeziehen, indem Sie einen Filter auf Identitäten & Einstellungen für die ZeroFox-Zielliste anwenden.

Nach dem Ausführen des Berichts wird eine Liste der Änderungen angezeigt, die beim Hinzufügen der ZeroFOX-Zielliste aus der Integration vorgenommen wurden.

Umgang mit unerwünschten Erkennungen oder Fehlalarmen

Verwalten einer Zulassungsliste für die unerwünschte Erkennung

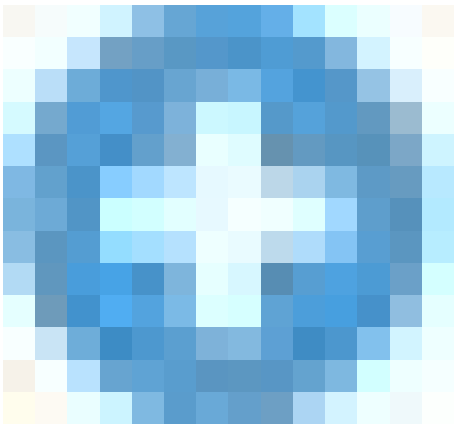
Obwohl unwahrscheinlich, ist es möglich, dass Domains, die automatisch von ZeroFOX hinzugefügt werden, eine unerwünschte Blockierung auslösen, die Benutzer am Zugriff auf bestimmte Websites hindern würde. In einer solchen Situation empfehlen wir, die Domäne(n) einer Zulassungsliste hinzuzufügen, die Vorrang vor allen anderen Blocklistenarten hat, einschließlich Sicherheitseinstellungen. Eine Zulassungsliste hat Vorrang vor einer Sperrliste, wenn eine Domäne in beiden vorhanden ist.

Es gibt zwei Gründe, warum dieser Ansatz vorzuziehen ist. Erstens, falls die ZeroFOX-Appliance die Domäne nach dem Entfernen erneut hinzufügen sollte, schützt die Zulassungsliste davor, weitere Probleme zu verursachen. 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 Nullfox-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.

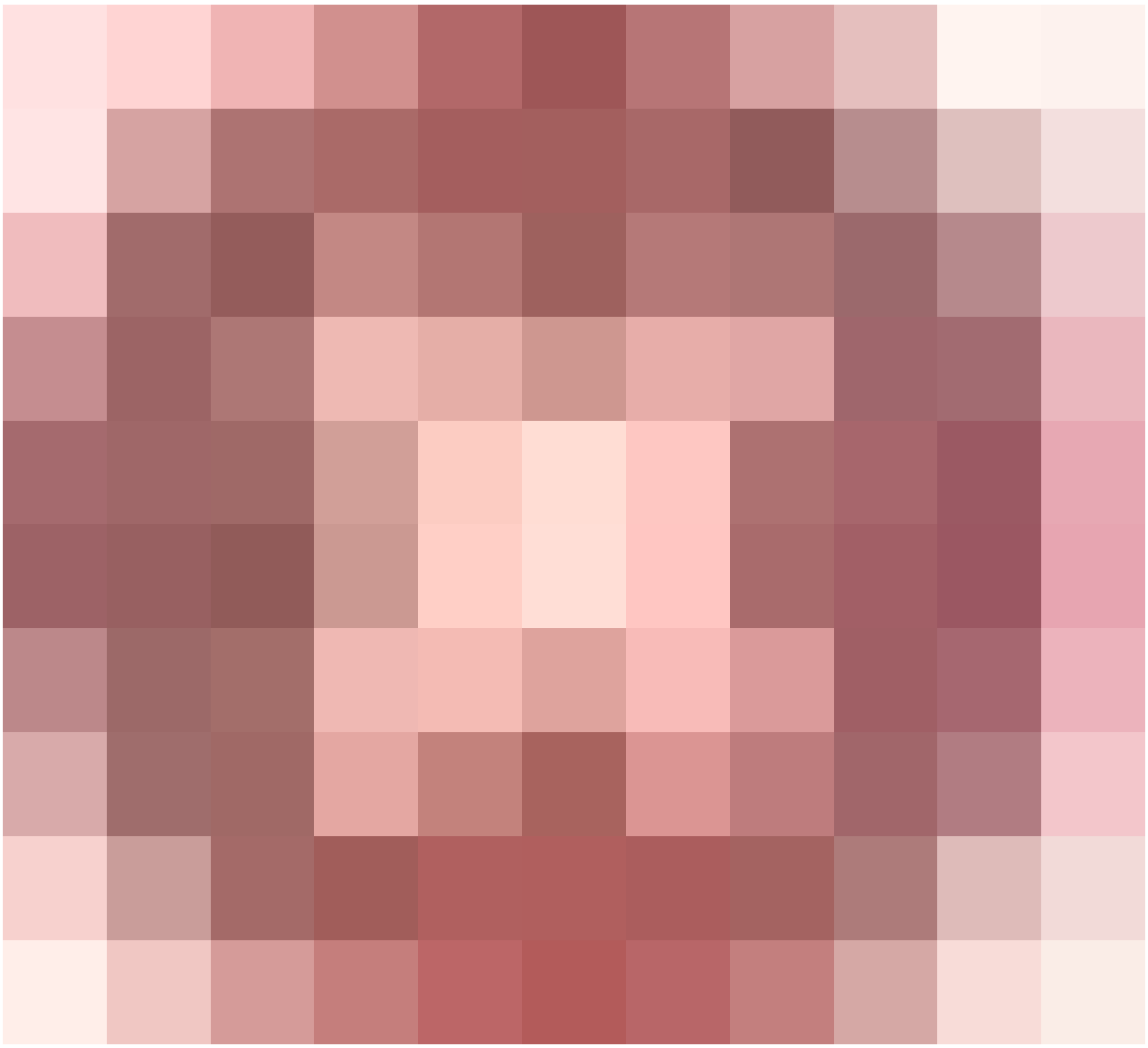
So erstellen Sie eine Zulassungsliste:

1. Navigieren Sie zu Richtlinien > Ziellisten, und klicken Sie auf 

Symbol hinzufügen
2. Wählen Sie Zulassen aus, und fügen Sie Ihre Domäne zur Liste hinzu.
3. Klicken Sie auf 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 ZeroFOX-Zielliste

Es gibt eine  (Delete)-Symbol neben jedem Domänennamen in der ZeroFOX-Zielliste. Durch das Löschen von Domänen können Sie die ZeroFOX-Zielliste im Falle einer unerwünschten Erkennung bereinigen.

Der Löschvorgang ist jedoch nicht dauerhaft, wenn ZeroFOX die Domain erneut an Umbrella sendet.

So löschen Sie eine Domäne:

1. Navigieren Sie zu Einstellungen > Integrationen, und klicken Sie dann auf "ZeroFOX", um es zu erweitern.
2. Klicken Sie auf Domains anzeigen.
3. Suchen Sie nach dem Domänennamen, den Sie löschen möchten.
4. Klicken Sie auf das Symbol Löschen.

5. Klicken Sie auf Close (Schließen).
6. Klicken Sie auf Speichern.

Im Falle einer unerwünschten Erkennung oder eines Fehlalarms empfehlen wir, sofort eine Zulassungsliste in Umbrella zu erstellen und dann das Fehlalarmproblem innerhalb von ZeroFOX zu beheben. Später können Sie die Domäne aus der ZeroFOX-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.