Intégrer ZeroFOX à Umbrella

Table des matières

Introduction

Présentation de ZeroFOX Enterprise et de Cisco Umbrella Integration

Intégration Cisco Umbrella et ZeroFox : Comment cela fonctionne-t-il?

- Conditions préalables
- Étape 1 : Génération de jetons de script et API Umbrella
- Étape 2 : Configurer votre tableau de bord ZeroFOX Enterprise pour envoyer des informations à Umbrella
- Étape 3 : Configuration des événements ZeroFOX à bloquer dans Umbrella

Observation des événements ajoutés à la catégorie de sécurité ZeroFOX en mode audit

- Vérifier la liste de destinations
- Vérifier les paramètres de sécurité d'une stratégie

Application des paramètres de sécurité ZeroFOX en mode blocage à une stratégie pour les clients gérés

Reporting dans Umbrella pour les événements ZeroFOX

- Génération de rapports sur les événements de sécurité ZeroFOX
- Signalement lorsque des domaines ont été ajoutés à la liste de destinations ZeroFOX

Gestion des détections indésirables ou des faux positifs

- Gestion d'une liste verte pour la détection indésirable
- Suppression de domaines de la liste de destinations ZeroFOX

Introduction

Ce document décrit comment intégrer ZeroFOX Enterprise avec Umbrella afin que les événements de sécurité puissent être appliqués aux clients protégés par Umbrella.

Présentation de ZeroFOX Enterprise et de Cisco Umbrella Integration

En intégrant ZeroFOX Enterprise à Cisco Umbrella, les responsables de la sécurité et les administrateurs peuvent étendre la protection contre les menaces actuelles basées sur les médias sociaux aux ordinateurs portables, tablettes ou téléphones itinérants, tout en fournissant une couche supplémentaire d'application à un réseau d'entreprise distribué.

Intégration Cisco Umbrella et ZeroFox : Comment cela fonctionne-t-il?

ZeroFOX Enterprise transmet toutes les menaces détectées, telles que les cybermenaces basées

sur les médias sociaux, y compris les programmes malveillants ciblés, le phishing, l'ingénierie sociale, les usurpations d'identité et autres activités frauduleuses ou malveillantes, à Cisco Umbrella pour une application globale.

Umbrella valide ensuite la menace pour s'assurer qu'elle peut être ajoutée à une stratégie. S'il est confirmé que les informations de ZeroFOX constituent une menace, l'adresse de domaine est ajoutée à la liste de destinations ZeroFOX dans le cadre d'un paramètre de sécurité qui peut être appliqué à n'importe quelle stratégie Umbrella. Cette stratégie est immédiatement appliquée à toutes les requêtes effectuées à partir des périphériques affectés à cette stratégie.

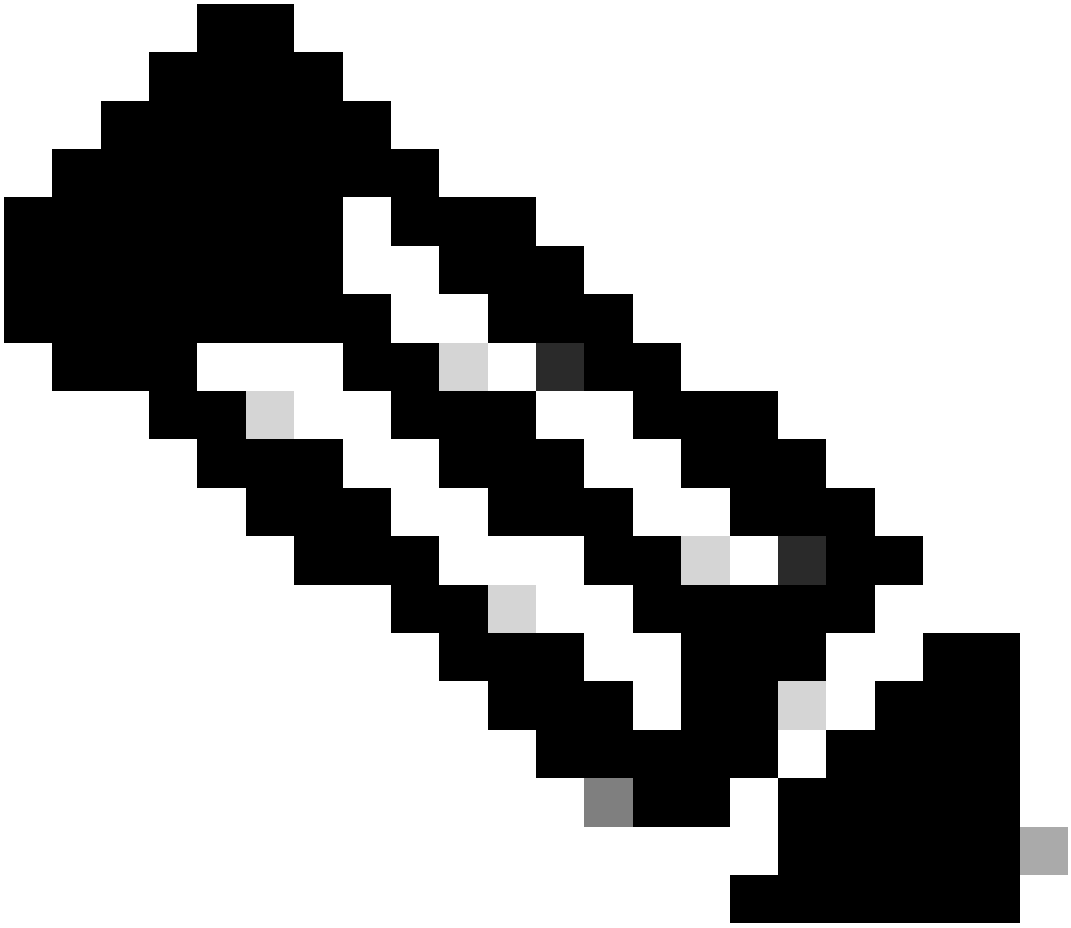
Cisco Umbrella analyse automatiquement les alertes ZeroFOX et ajoute des sites malveillants à la liste de destinations ZeroFOX. Il étend ainsi l'intelligence ZeroFOX à tous les utilisateurs et périphériques distants et fournit une autre couche d'application à votre réseau d'entreprise.

Pour ce faire, suivez ces étapes de configuration simples :

1. Activez l'intégration dans Umbrella pour générer un jeton API.
2. Collez ce jeton API dans votre compte ZeroFOX.
3. Configurez ZeroFOX pour qu'il bloque sous les paramètres de sécurité de la ou des stratégies souhaitées

Conditions préalables

- Droits d'administration de ZeroFOX Enterprise
- Droits administratifs du tableau de bord parapluie
- L'intégration ZeroFOX doit être activée sur le tableau de bord Umbrella



Remarque : L'intégration ZeroFOX est uniquement incluse dans le package Umbrella Platform. Si vous ne disposez pas de l'offre plate-forme et souhaitez bénéficier de l'intégration ZeroFOX, contactez votre représentant Cisco Umbrella. Si vous disposez du package Plate-forme mais que vous ne voyez pas ZeroFOX comme une intégration pour votre tableau de bord, veuillez contacter le support Umbrella.

Important : Alors qu'Umbrella fait de son mieux pour valider et autoriser les domaines qui sont généralement sûrs (par exemple, Google et Salesforce), pour éviter toute interruption indésirable, nous vous suggérons d'ajouter tous les domaines que vous ne voulez pas bloquer à la liste verte globale ou à d'autres listes de destinations conformément à votre politique.

Exemples :

- Page d'accueil de votre organisation. Par exemple, mydomain.com.
- Domaines représentant des services que vous fournissez et pouvant avoir des enregistrements internes et externes. Par exemple, mail.myservicedomain.com et portal.myotherservicedomain.com.

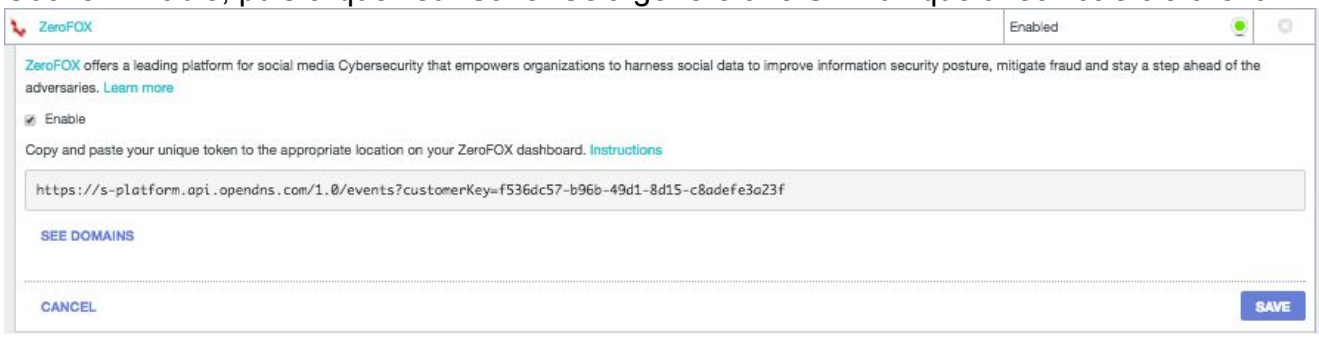
- Les applications cloud moins connues dont vous dépendez fortement et qu'Umbrella ne peut pas connaître ou inclure dans leur validation de domaine automatique. Par exemple, localcloudservice.com.

La liste verte globale se trouve dans Politiques > Listes de destinations dans Umbrella. Pour plus d'informations, consultez notre documentation : Gérer les listes de destinations

Étape 1 : Génération de jetons de script et API Umbrella

Commencez par rechercher votre URL unique dans Umbrella pour que l'appliance ThreatQ communique avec.

1. Connectez-vous à votre tableau de bord Umbrella en tant qu'administrateur, accédez à Paramètres > Intégrations et cliquez sur « ZeroFOX » dans le tableau pour le développer.
2. Cochez Enable, puis cliquez sur Save. Cela génère une URL unique avec votre clé client.

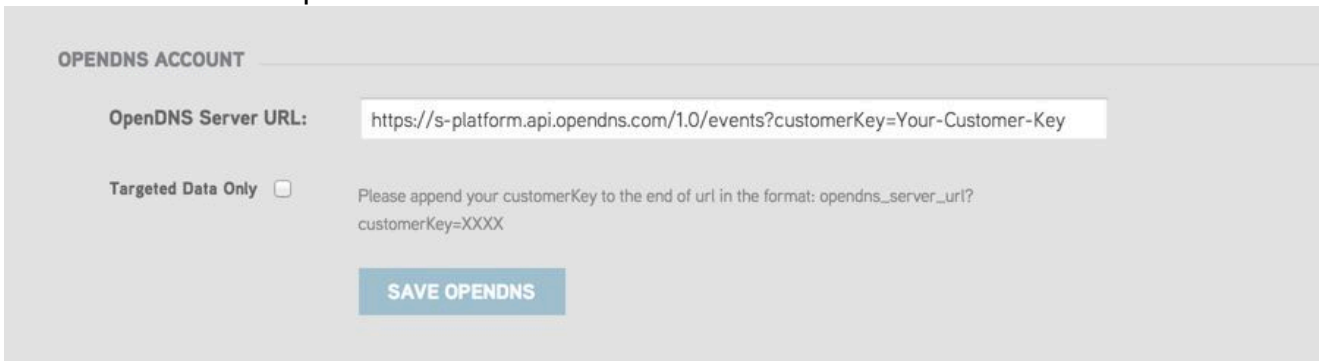


   Vous aurez besoin de l'URL ultérieurement lorsque vous configurerez ZeroFOX. Copiez l'URL et accédez à votre tableau de bord ThreatQ.

Étape 2 : Configurer votre tableau de bord ZeroFOX Enterprise pour envoyer des informations à Umbrella

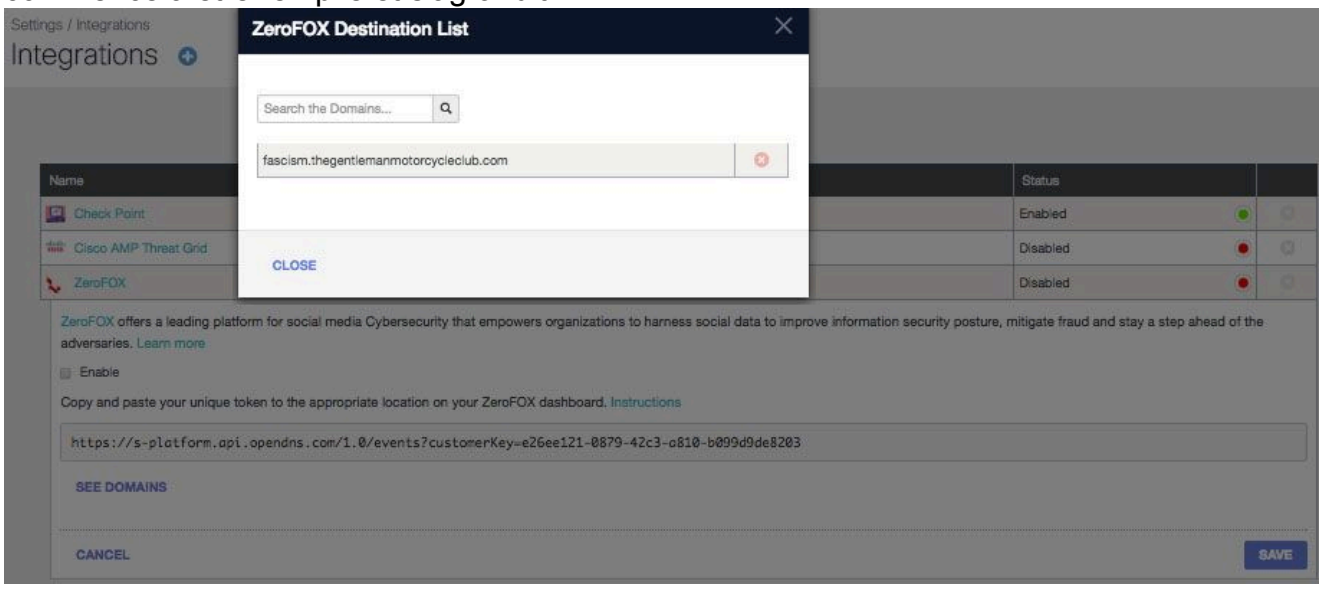
L'étape suivante consiste à ajouter l'URL que vous avez copiée à l'étape 1 au tableau de bord ZeroFOX.

1. Cliquez sur l'icône d'engrenage dans le tableau de bord Zerofox, puis sélectionnez Paramètres du compte.
2. Faites défiler la liste d'intégration jusqu'à ce que vous voyiez les informations de compte OpenDNS et collez l'URL d'Umbrella dans le champ OpenDNS Server URL.
3. Lors de la première activation de l'intégration, nous vous recommandons de sélectionner Données ciblées uniquement.



Étape 3 : Configuration des événements ZeroFOX à bloquer dans Umbrella

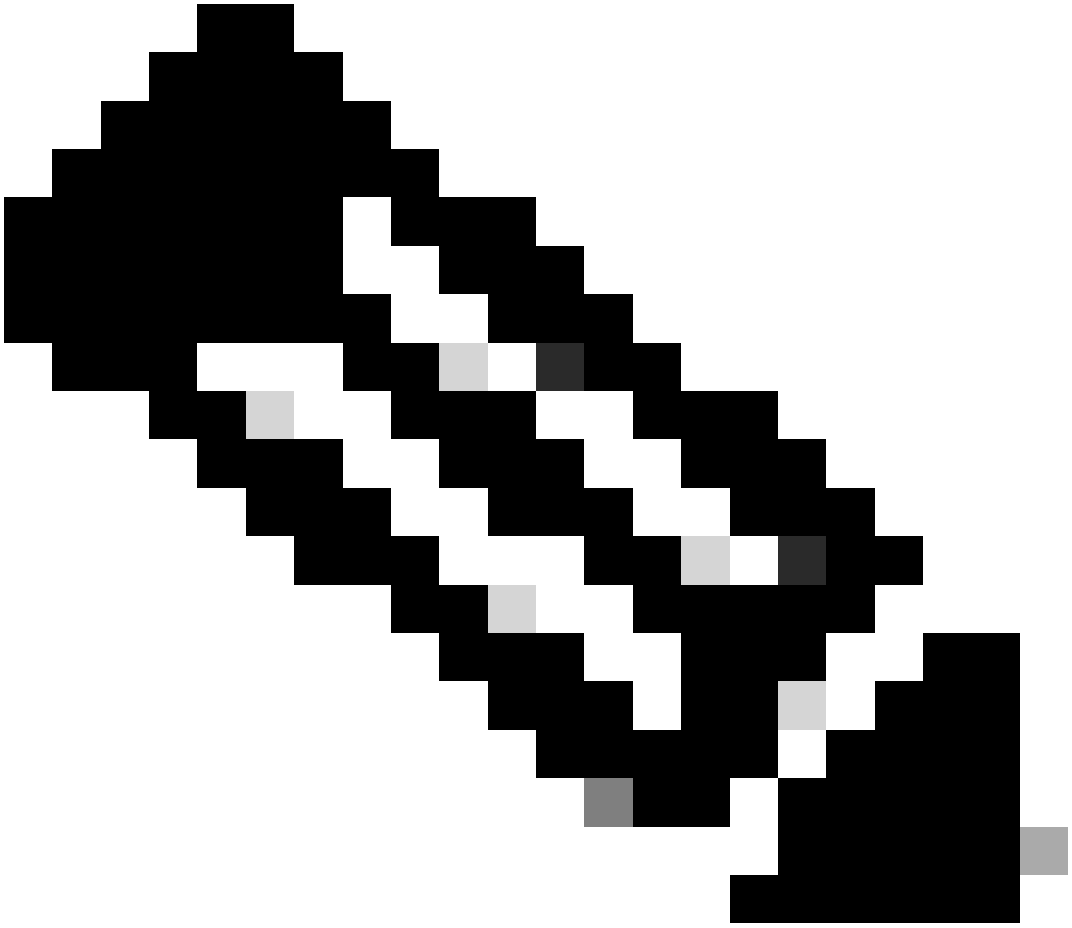
1. Reconnectez-vous à votre tableau de bord Umbrella en tant qu'administrateur.
2. Accédez à Paramètres > Intégrations et cliquez sur "ZeroFOX" dans le tableau pour le développer.
3. Cliquez sur Voir domaines.
   Cette opération permet d'étendre la liste des domaines qui comprend les dernières heures d'événements de votre compte ZeroFOX. À partir de ce moment, une liste consultable commence à être remplie et s'agrandit.



L'étape suivante consiste à observer et à auditer les événements ajoutés à votre nouvelle catégorie de sécurité ZeroFOX.

Observation des événements ajoutés à la catégorie de sécurité ZeroFOX en mode audit

Les événements de ZeroFOX Enterprise commencent à remplir une liste de destination spécifique qui peut être appliquée aux stratégies en tant que catégorie de sécurité ZeroFOX. Par défaut, la liste de destinataires et la catégorie de sécurité sont en mode Audit et ne sont appliquées à aucune stratégie. Elles n'entraînent aucune modification de vos stratégies Umbrella existantes.



Remarque : Le mode audit peut être activé pendant la durée nécessaire, en fonction de votre profil de déploiement et de la configuration du réseau.

Vérifier la liste de destinations

Vous pouvez consulter la liste de destinations ZeroFox à tout moment.

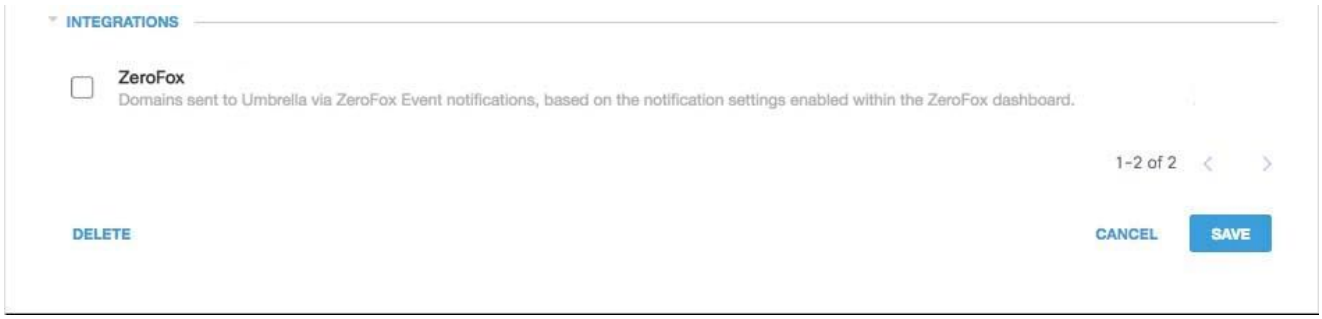
1. Accédez à Paramètres > Intégrations.
2. Développez « ZeroFOX » dans le tableau et cliquez sur Voir domaines.

Vérifier les paramètres de sécurité d'une stratégie

Vous pouvez vérifier à tout moment le paramètre de sécurité qui peut être activé pour une stratégie.

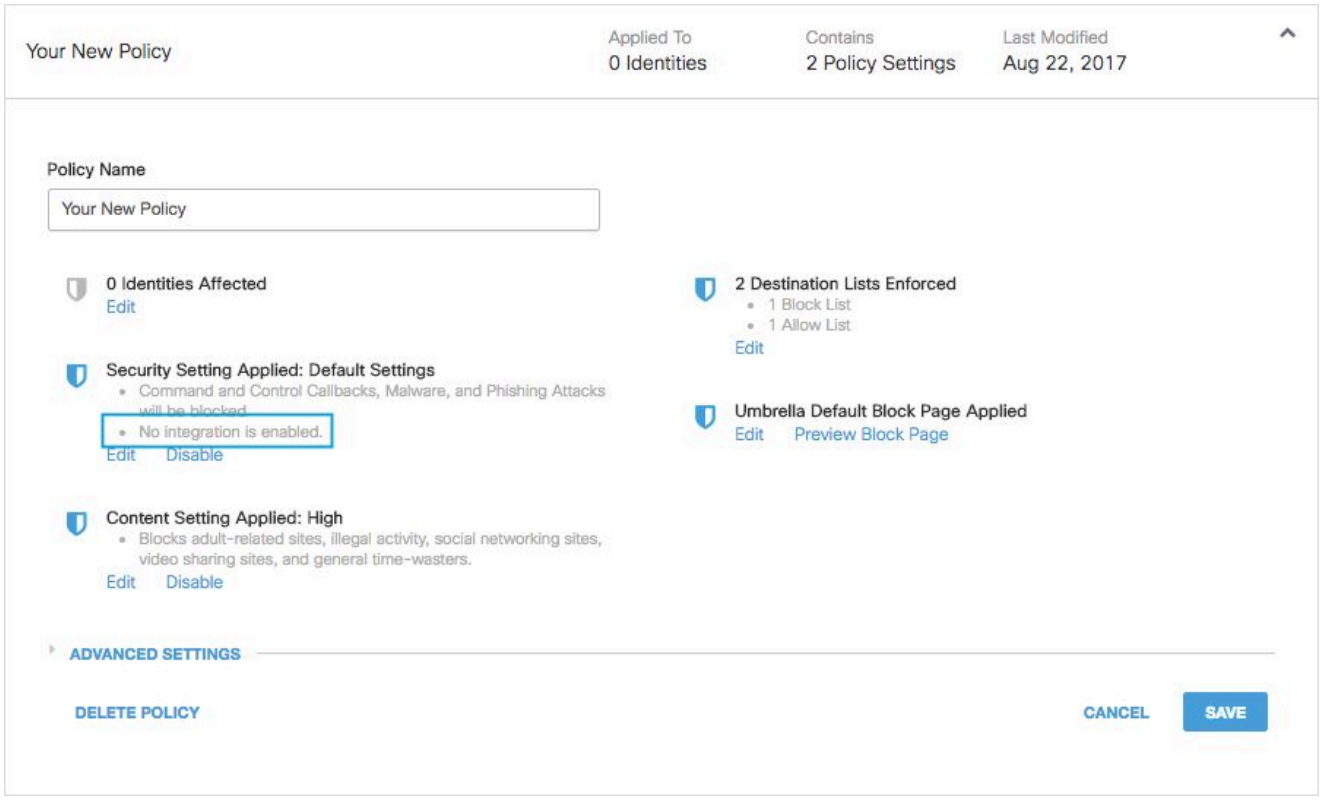
1. Accédez à Stratégies > Paramètres de sécurité.
2. Cliquez sur un paramètre de sécurité dans le tableau pour le développer et faites défiler

jusqu'à Integrations pour localiser le paramètre ZeroFOX.



115014041606

Vous pouvez également consulter les informations d'intégration via la page Récapitulatif des paramètres de sécurité.

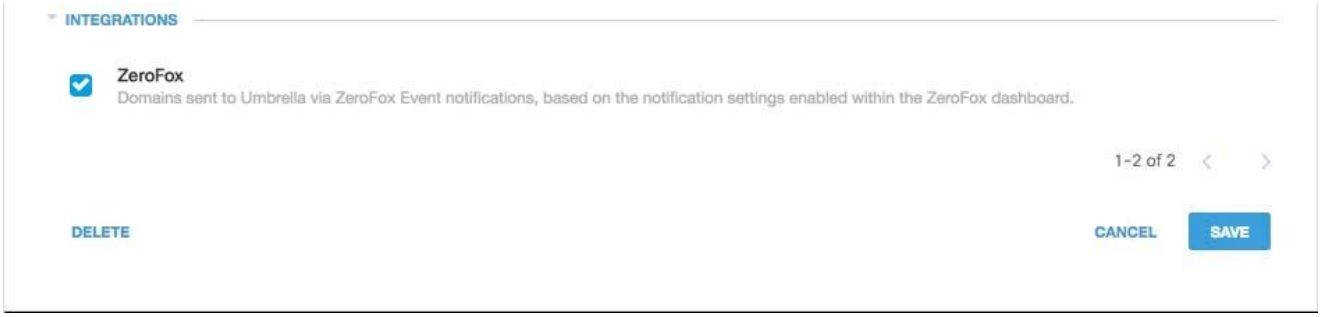


25464154913556

Application des paramètres de sécurité ZeroFOX en mode blocage à une stratégie pour les clients gérés

Une fois que vous êtes prêt à faire appliquer ces menaces de sécurité supplémentaires par les clients gérés par Umbrella, il vous suffit de modifier le paramètre de sécurité sur une stratégie existante ou de créer une nouvelle stratégie plus élevée que votre stratégie par défaut pour vous assurer qu'elle est appliquée en premier.

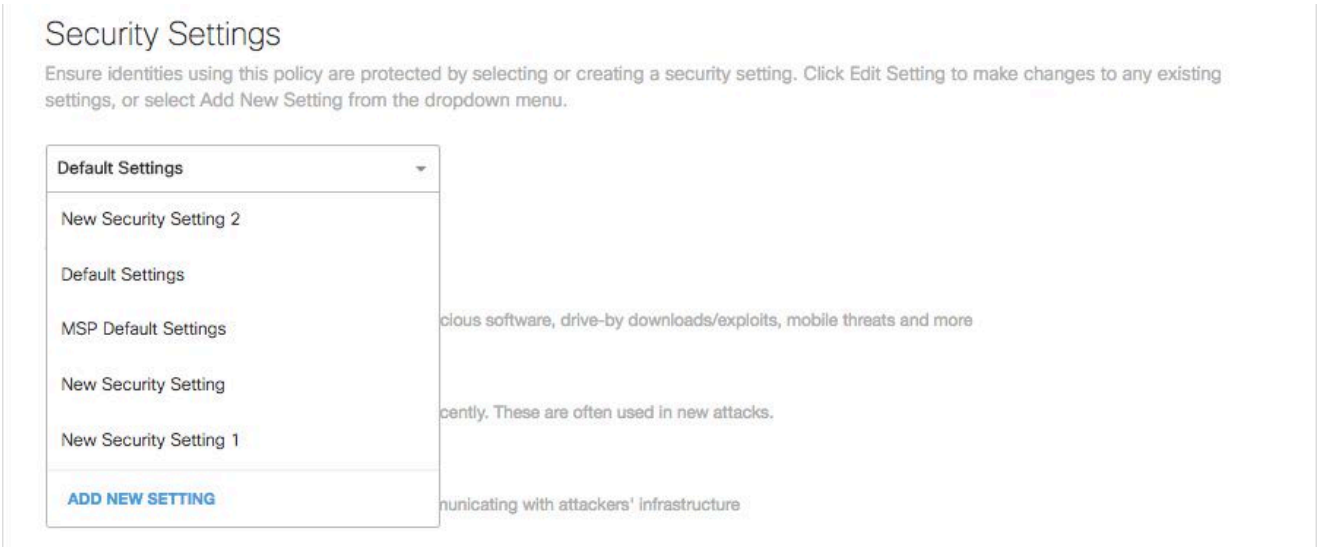
1. Accédez à Policies > Security Settings et sous Integrations, cochez ZeroFOX et cliquez sur Save.



115014042806

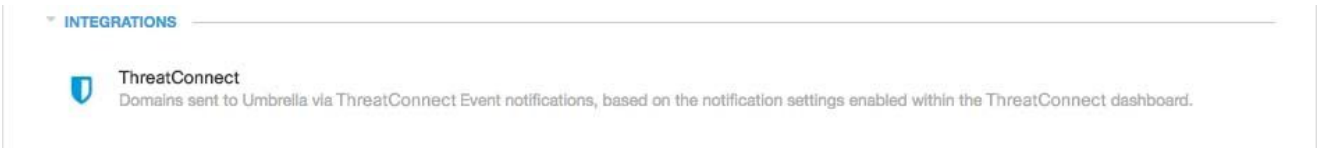
Ensuite, dans l'Assistant Stratégie, ajoutez un paramètre de sécurité à la stratégie que vous modifiez :

1. Accédez à Politiques > Liste des politiques.
2. Développez une stratégie et cliquez sur Edit sous Security Setting Applied.
3. Dans le menu déroulant Security Settings, sélectionnez un paramètre de sécurité qui inclut le paramètre ThreatConnect.



25464147943700

L'icône en forme de bouclier sous Intégrations devient bleue.



25464147957652

4. Cliquez sur Set & Return.

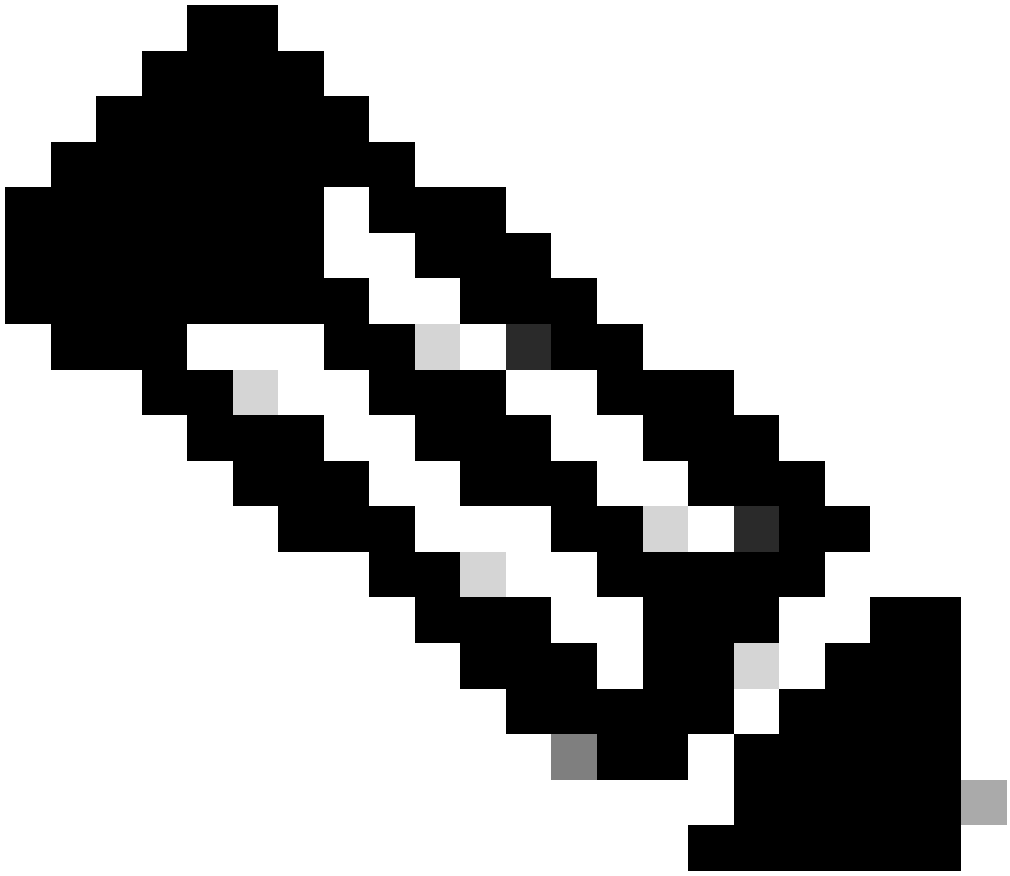
Les domaines ZeroFOX contenus dans le paramètre de sécurité de ZeroFOX sont bloqués pour les identités utilisant cette stratégie.

Reporting dans Umbrella pour les événements ZeroFOX

Génération de rapports sur les événements de sécurité ZeroFOX

La liste de destinations ZeroFOX est l'une des listes de catégories de sécurité sur lesquelles vous pouvez générer des rapports. La plupart ou la totalité des rapports utilisent les catégories de sécurité comme filtre. Par exemple, vous pouvez filtrer les catégories de sécurité pour afficher uniquement l'activité liée à ZeroFOX.

1. Accédez à Reporting > Activity Search et sous Security Categories sélectionnez ZeroFOX pour filtrer le rapport afin d'afficher uniquement la catégorie de sécurité pour ZeroFOX.



Remarque : Si l'intégration ZeroFOX est désactivée, elle n'apparaît pas dans le filtre Catégories de sécurité.

115014043046

2. Cliquez sur Apply.

Signalement lorsque des domaines ont été ajoutés à la liste de destinations ZeroFOX

Le journal d'audit d'admin Umbrella inclut les événements de votre compte ZeroFOX lorsqu'il ajoute des domaines à la liste de destination.

Le journal d'audit d'admin Umbrella se trouve dans Reporting > Journal d'audit d'admin. Afin d'indiquer quand un domaine a été ajouté, filtrez pour inclure uniquement les modifications ZeroFOX en appliquant un filtre aux Identités et paramètres pour la liste de destinations ZeroFOX.

Une fois que vous avez exécuté le rapport, vous voyez une liste des modifications apportées lorsque la liste de destinations ZeroFOX a été ajoutée à à partir de l'intégration.

Gestion des détections indésirables ou des faux positifs

Gestion d'une liste verte pour la détection indésirable

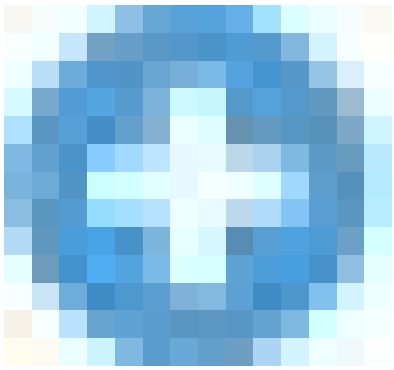
Bien que peu probable, il est possible que les domaines ajoutés automatiquement par ZeroFOX puissent déclencher un blocage indésirable qui empêcherait les utilisateurs d'accéder à des sites Web particuliers. Dans une situation comme celle-ci, nous vous recommandons d'ajouter le ou les domaines à une liste d'autorisation, qui est prioritaire sur tous les autres types de listes de blocage, y compris les paramètres de sécurité. Une liste verte est prioritaire sur une liste rouge lorsqu'un domaine est présent dans les deux.

Cette approche est préférable pour deux raisons. Tout d'abord, si l'appliance ZeroFOX devait ajouter à nouveau le domaine après sa suppression, la liste d'autorisation protège contre ce problème, ce qui provoquerait d'autres problèmes. Deuxièmement, la liste verte affiche un historique des domaines problématiques pouvant être utilisés pour des rapports d'investigation ou d'audit.

Par défaut, une liste verte globale est appliquée à toutes les stratégies. L'ajout d'un domaine à la liste verte globale entraîne l'autorisation du domaine dans toutes les stratégies.

Si le paramètre de sécurité ZeroFOX en mode bloc est appliqué uniquement à un sous-ensemble de vos identités Umbrella gérées (par exemple, il est appliqué uniquement aux ordinateurs et périphériques mobiles itinérants), vous pouvez créer une liste d'autorisation spécifique pour ces identités ou stratégies.

Pour créer une liste verte :

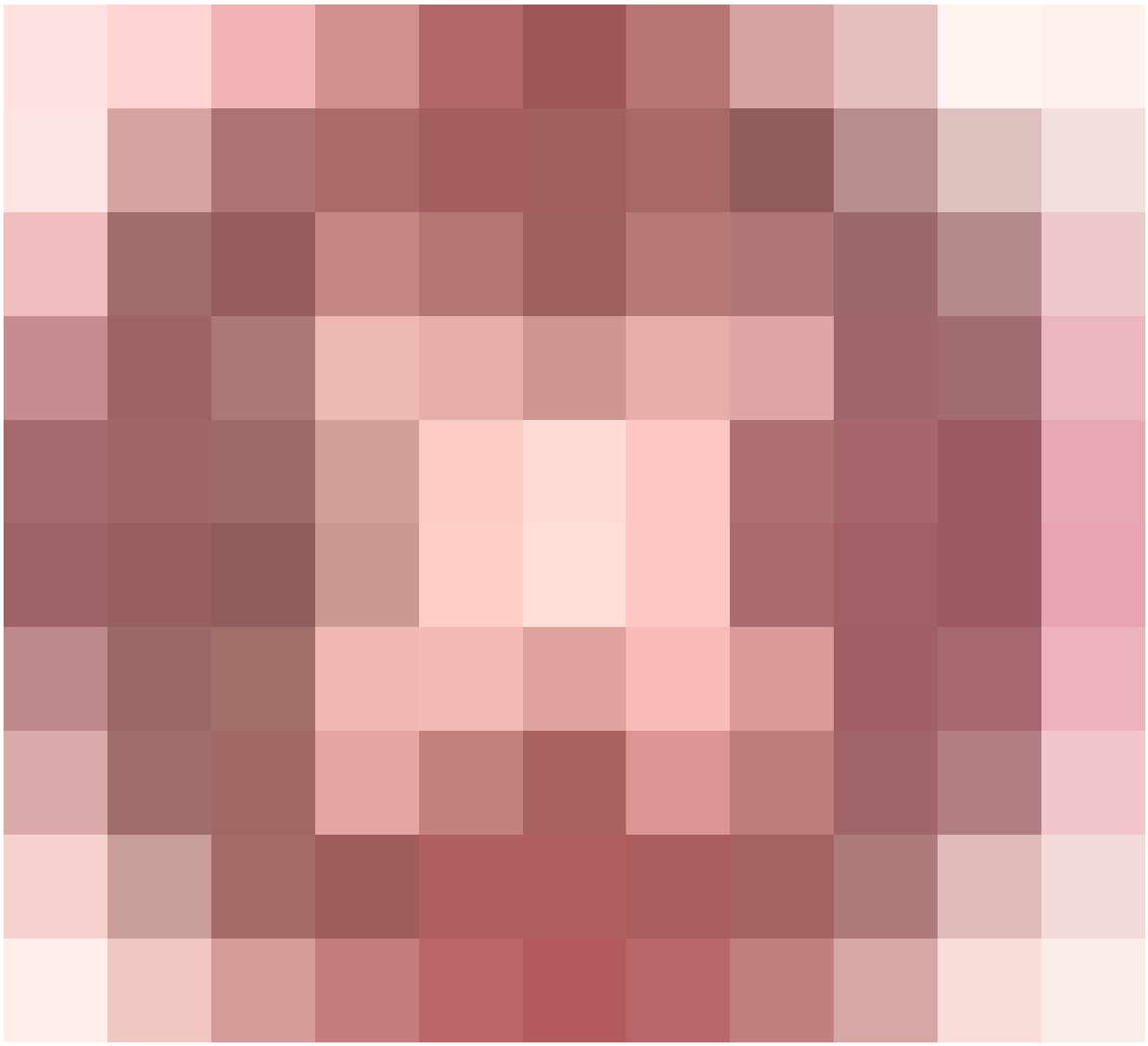
1. Accédez à Policies > Destination Lists, puis cliquez sur le bouton 

   25464155856404

   Ajouter une icône.
2. Sélectionnez Allow, et ajoutez votre domaine à la liste.
3. Cliquez sur Save.

Une fois la liste de destinations enregistrée, vous pouvez l'ajouter à une stratégie existante couvrant les clients qui ont été affectés par le blocage indésirable.

Suppression de domaines de la liste de destinations ZeroFOX

Il y a un  (Supprimer) en regard de chaque nom de domaine dans la liste de destinations ZeroFOX. La suppression de domaines vous permet de nettoyer la liste de destinations ZeroFOX en cas de détection indésirable.

Cependant, la suppression n'est pas permanente si ZeroFOX renvoie le domaine à Umbrella.

Pour supprimer un domaine :

1. Accédez à Paramètres > Intégrations, puis cliquez sur "ZeroFOX" pour le développer.
2. Cliquez sur Voir domaines.
3. Recherchez le nom de domaine que vous souhaitez supprimer.
4. Cliquez sur l'icône Supprimer.

5. Cliquez sur Fermer.
6. Cliquez sur Save.

Dans le cas d'une détection indésirable ou d'un faux positif, nous vous recommandons de créer immédiatement une liste d'autorisation dans Umbrella, puis de corriger le faux positif dans ZeroFOX. Vous pourrez ensuite supprimer le domaine de la liste de destinations ZeroFOX.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.