Intégration de ThreatConnect à Umbrella

Table des matières

Introduction

Ce document décrit comment intégrer ThreatConnect à Cisco Umbrella.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Tableau de bord ThreatConnect permettant de mettre à jour l'URL pour les intégrations
- Droits administratifs du tableau de bord parapluie
- L'intégration ThreatConnect doit être activée sur le tableau de bord Umbrella.

Composants utilisés

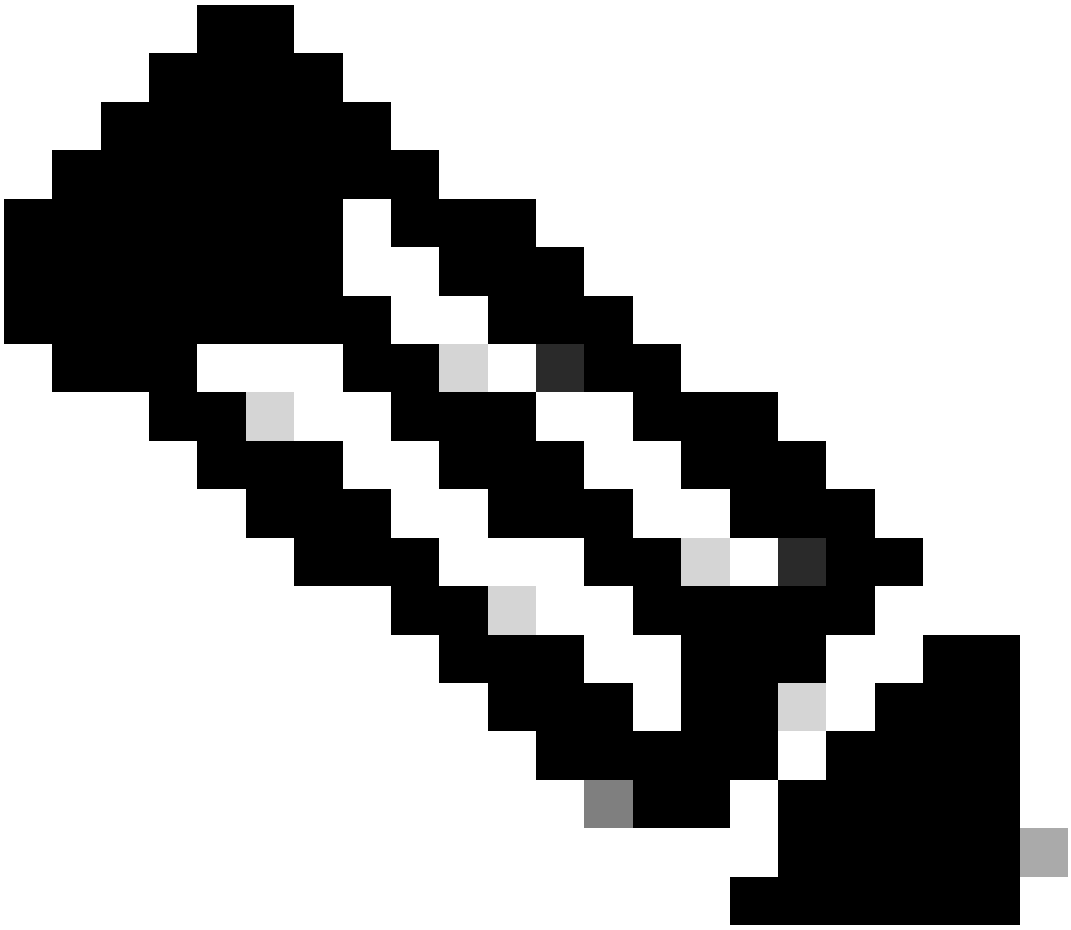
Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Présentation de ThreatConnect et de Cisco Umbrella Integration

En intégrant ThreatConnect à Cisco Umbrella, les responsables de la sécurité et les administrateurs peuvent désormais étendre la protection contre les menaces avancées sur les ordinateurs portables, les tablettes ou les téléphones itinérants, tout en fournissant une couche supplémentaire d'application à un réseau d'entreprise distribué.

Ce guide explique comment configurer ThreatConnect pour communiquer avec Umbrella afin que les événements de sécurité du conseil ThreatConnect soient intégrés dans des politiques qui peuvent être appliquées aux clients protégés par votre Cisco Umbrella.



Remarque : L'intégration de ThreatConnect n'est incluse que dans un certain package Cisco Umbrella. Si vous ne disposez pas d'un package incluant cette intégration,

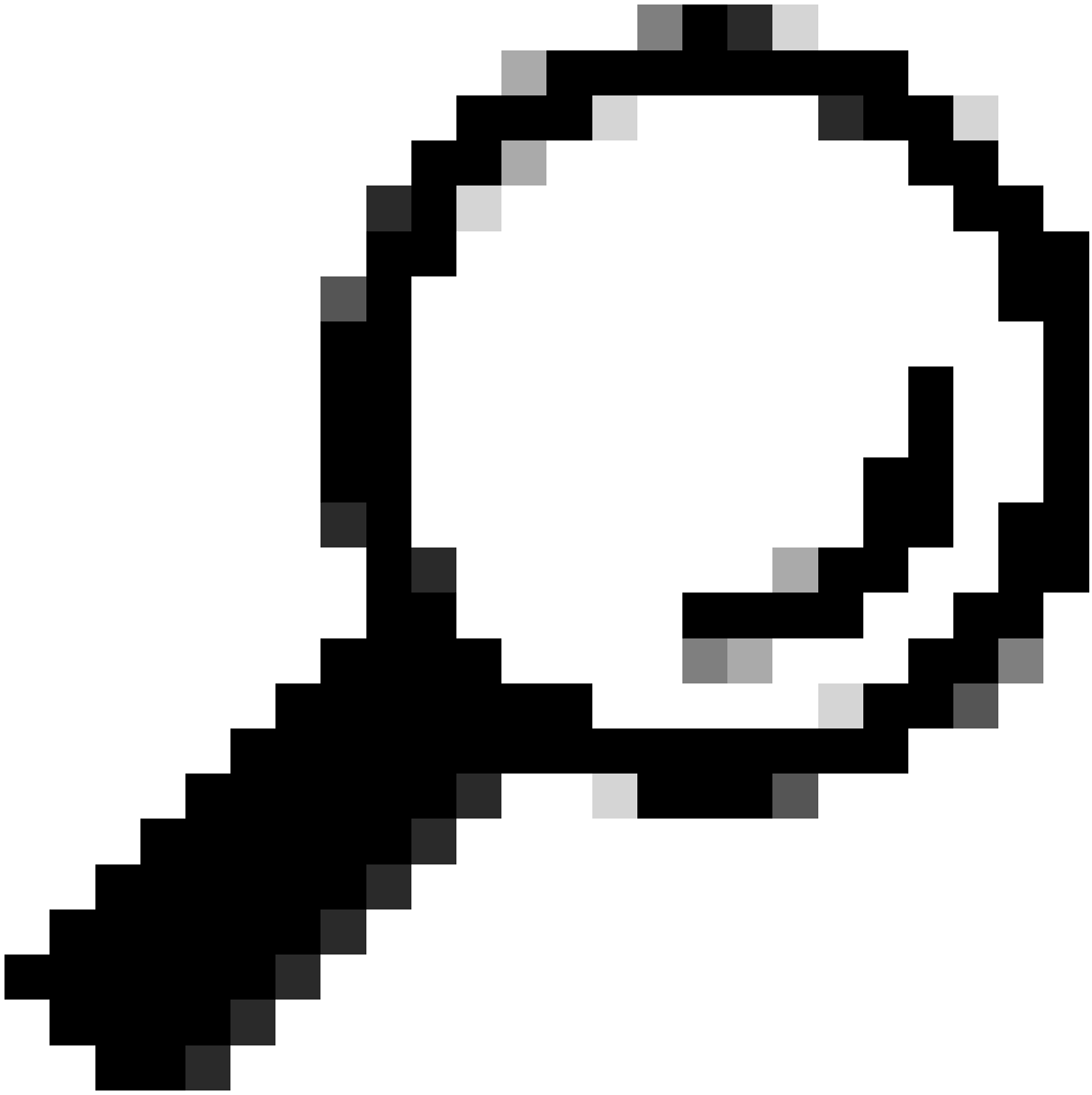
---

contactez votre représentant Cisco Umbrella pour l'obtenir. Si vous disposez du package correct mais que ThreatConnect n'apparaît pas comme une intégration pour votre tableau de bord, veuillez contacter l'assistance Cisco Umbrella.

La plate-forme ThreatConnect envoie d'abord à Umbrella l'intelligence des cybermenaces qu'elle a trouvée, comme les domaines hébergeant des programmes malveillants, la commande et le contrôle des sites de botnets ou d'hameçonnage.

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

Par la suite, Umbrella analyse automatiquement les alertes ThreatConnect et ajoute des sites malveillants à la liste de destinations ThreatConnect, étendant ainsi la protection ThreatConnect à tous les utilisateurs et périphériques distants et fournissant une couche supplémentaire d'application à votre réseau d'entreprise.



Conseil : Tandis qu'Umbrella fait de son mieux pour valider et autoriser les domaines généralement sûrs (par exemple, Google et Salesforce), pour éviter toute interruption indésirable, Umbrella suggère d'ajouter tous les domaines que vous ne voulez pas être bloqués à la liste verte globale ou 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.
- Applications cloud moins connues dont vous dépendez fortement, mais dont Umbrella n'est pas conscient ou n'inclut pas la validation automatique de domaine. Par exemple, localcloudservice.com.

La liste verte globale se trouve dans Politiques > Listes de destinations dans Umbrella.

Reportez-vous à la documentation pour plus d'informations : [Gérer les listes de destinations]

Configurer le tableau de bord Umbrella pour recevoir les événements de ThreatConnect

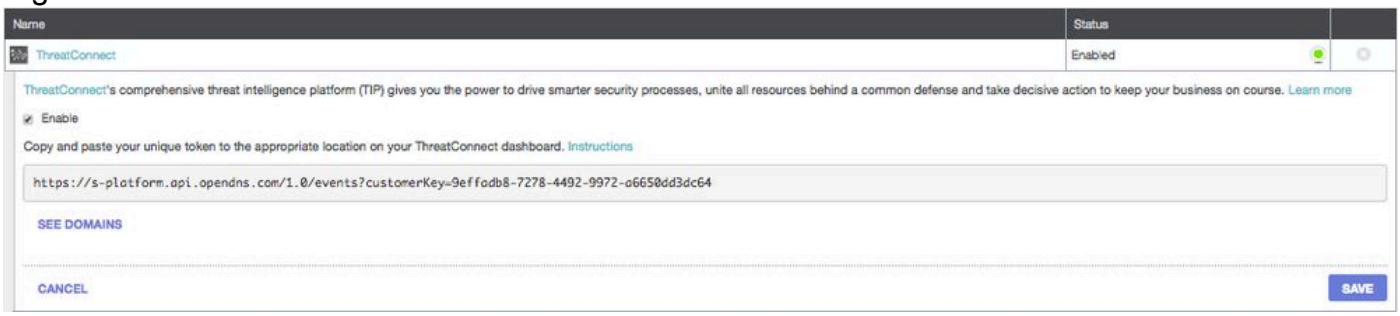
Commencez par rechercher votre URL unique dans Umbrella pour que l'appliance ThreatQ communique avec :

1. Connectez-vous à votre tableau de bord Umbrella.

2. Accédez à Politiques > Intégrations.

3. Dans le tableau, sélectionnez ThreatConnect pour le développer.

4. Sélectionnez Activer, puis Enregistrer. Cela génère une URL unique et spécifique pour votre organisation dans Umbrella.



Vous aurez besoin de l'URL plus loin dans cet article lorsque vous configurerez ThreatConnect pour envoyer des données à Umbrella.

Configurer ThreatConnect pour communiquer avec Umbrella

Pour commencer à envoyer du trafic de ThreatConnect vers Umbrella, vous devez configurer ThreatConnect avec les informations d'URL générées dans la première section de cet article :

1. Connectez-vous à votre tableau de bord ThreatConnect.

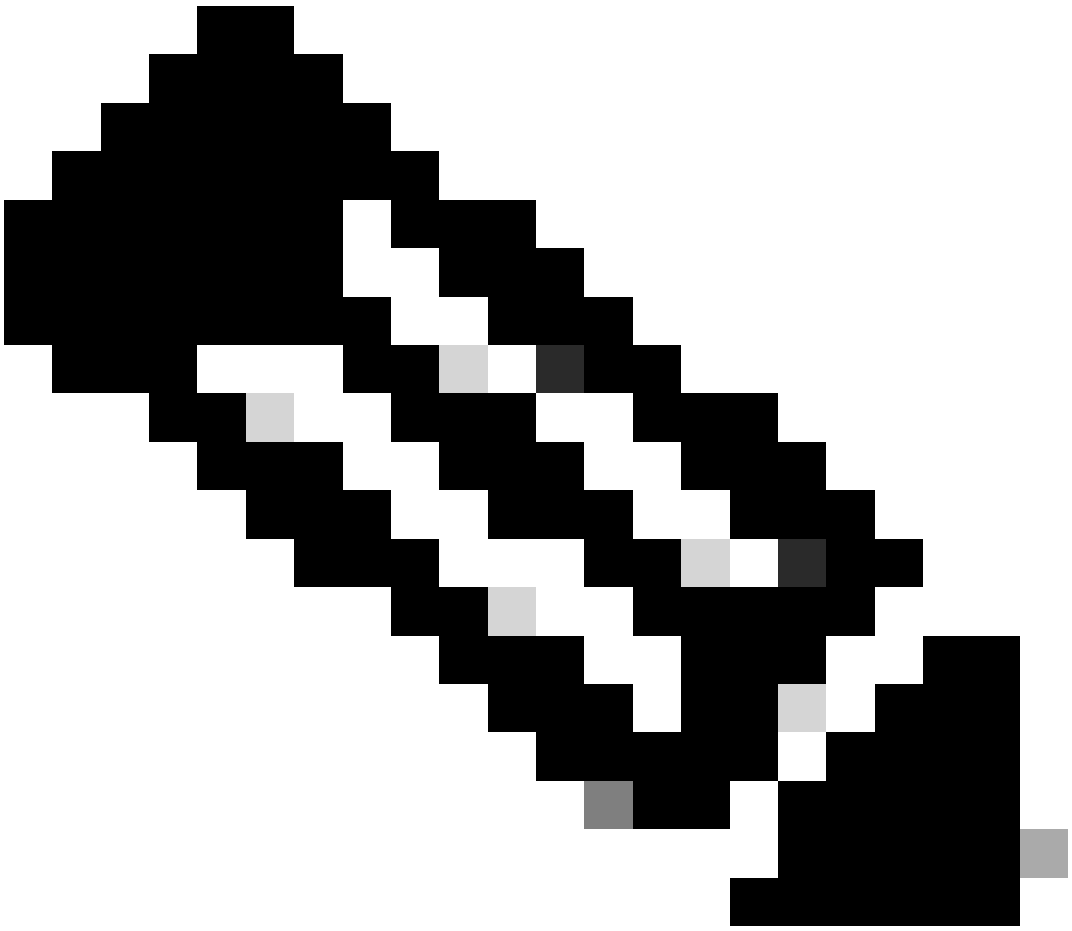
2. Ajoutez l'URL dans la zone appropriée pour vous connecter à Umbrella.

Les instructions précises varient, et Umbrella suggère de contacter le support ThreatConnect si vous n'êtes pas certain de la manière ou de l'endroit de configurer les intégrations d'API dans ThreatConnect.

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

Au fil du temps, les événements de votre tableau de bord ThreatConnect peuvent commencer à

remplir une liste de destinations spécifique qui peut être appliquée aux stratégies en tant que catégorie de sécurité ThreatConnect. Par défaut, la liste de destinataires et la catégorie de sécurité sont en mode Audit, ce qui signifie qu'elles ne sont pas appliquées aux stratégies et n'entraînent aucune modification de vos stratégies Umbrella existantes.



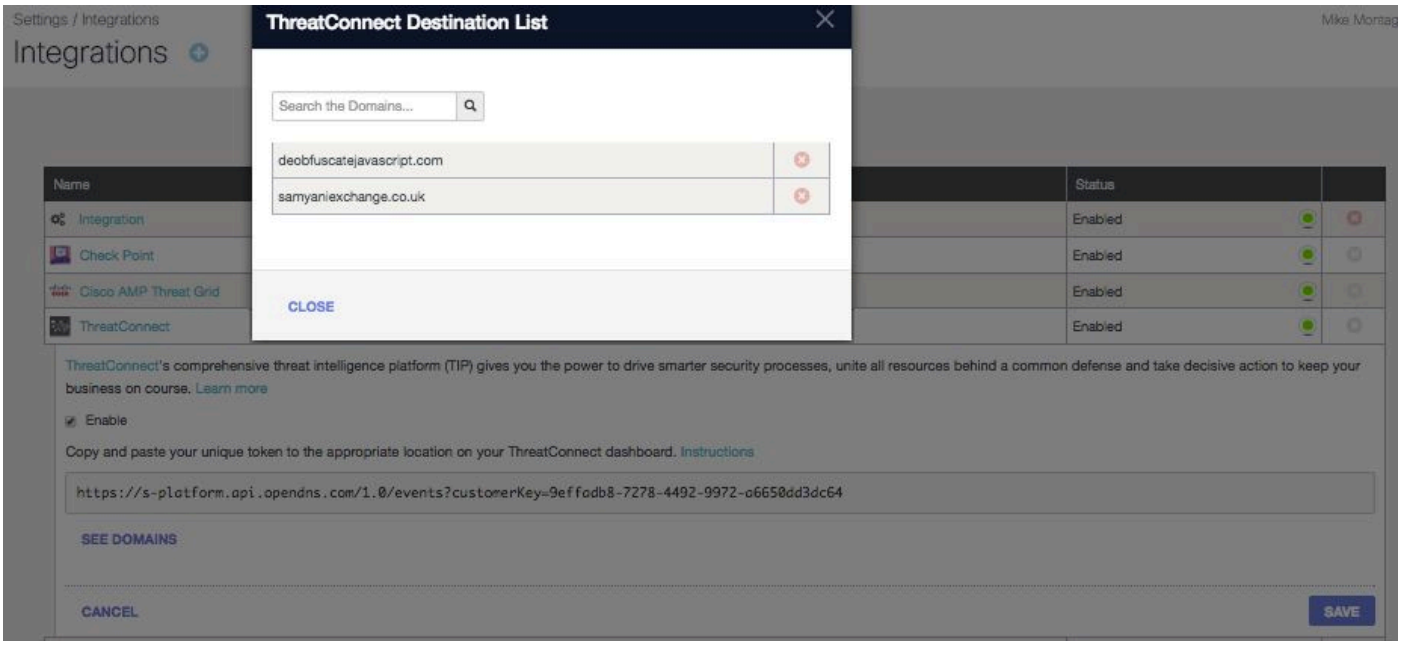
> Remarque : Le mode audit peut être activé pendant la durée nécessaire, en fonction de votre profil de déploiement et de la configuration du réseau.

Vérifier la liste de destinations

Vous pouvez consulter la liste de destinations ThreatConnect dans Umbrella à tout moment :

1. Dans le tableau de bord Umbrella, accédez à Politiques > Intégrations.

2. Dans le tableau, développez ThreatConnect et sélectionnez Voir domaines.



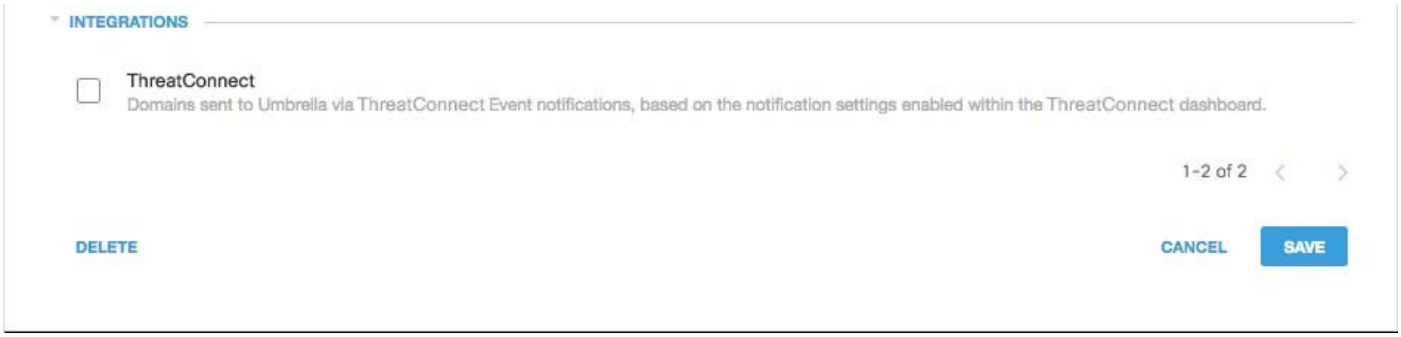
Vérifier les paramètres de sécurité d'une stratégie

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

1. Dans le tableau de bord Umbrella, accédez à Politiques > Paramètres de sécurité.

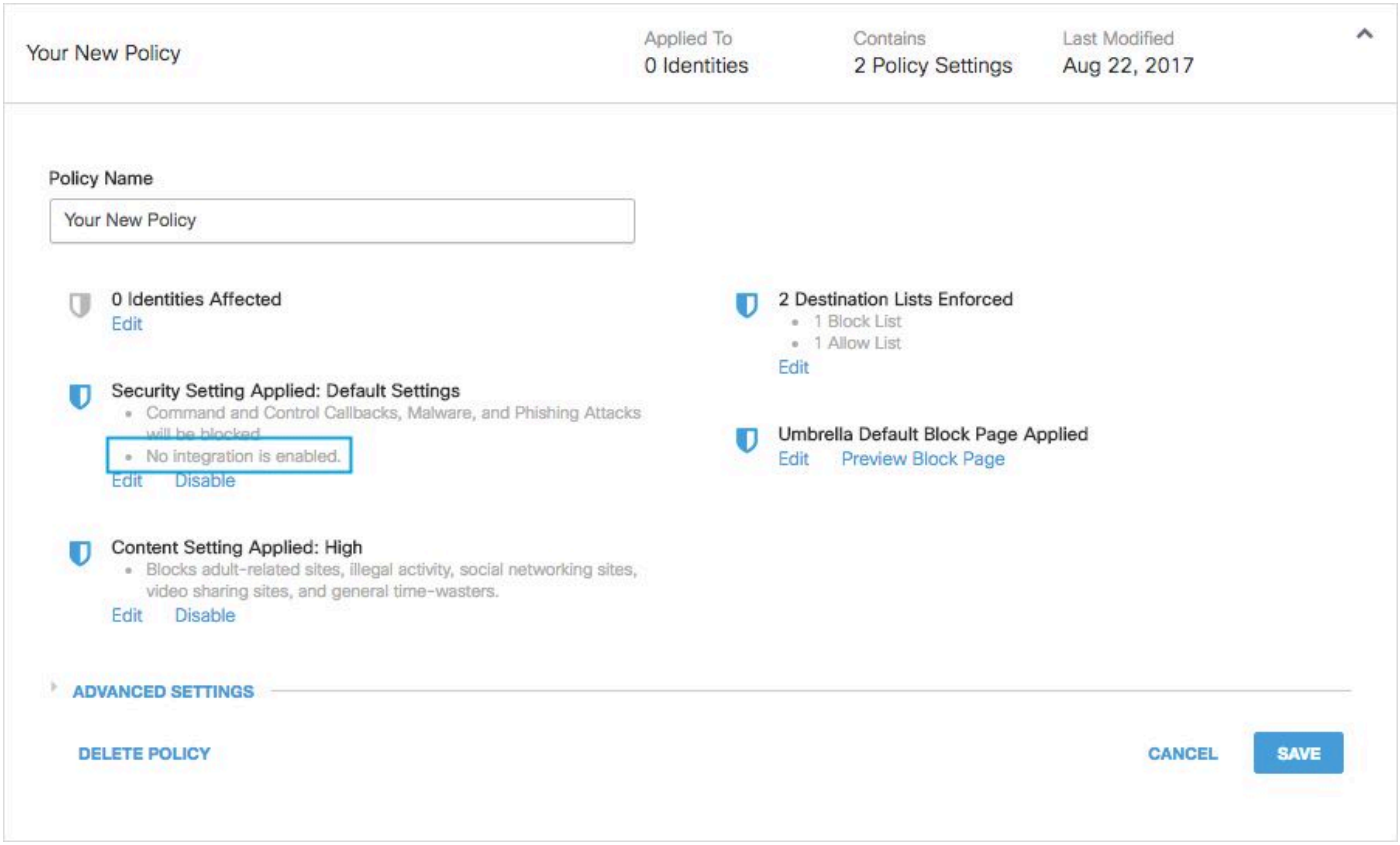
2. Sélectionnez un paramètre de sécurité dans la table pour le développer.

3. Faites défiler jusqu'à Integrations pour localiser le paramètre ThreatConnect.



115014036566

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



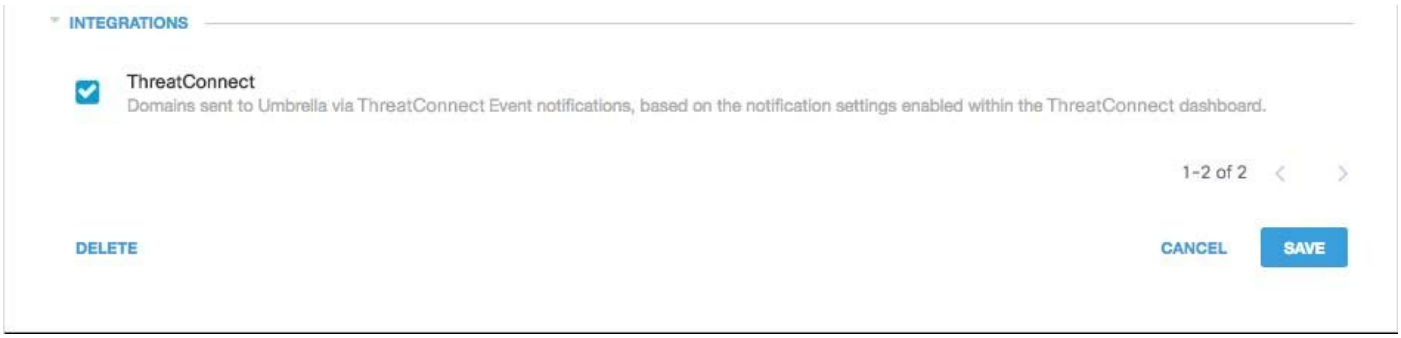
25464103885972

Application des paramètres de sécurité ThreatConnect 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 qui se trouve au-dessus de votre stratégie par défaut pour vous assurer qu'elle est appliquée en premier :

1. Accédez à Stratégies > Paramètres de sécurité.

2. Sous Intégrations, sélectionnez ThreatConnect, puis sélectionnez Enregistrer.



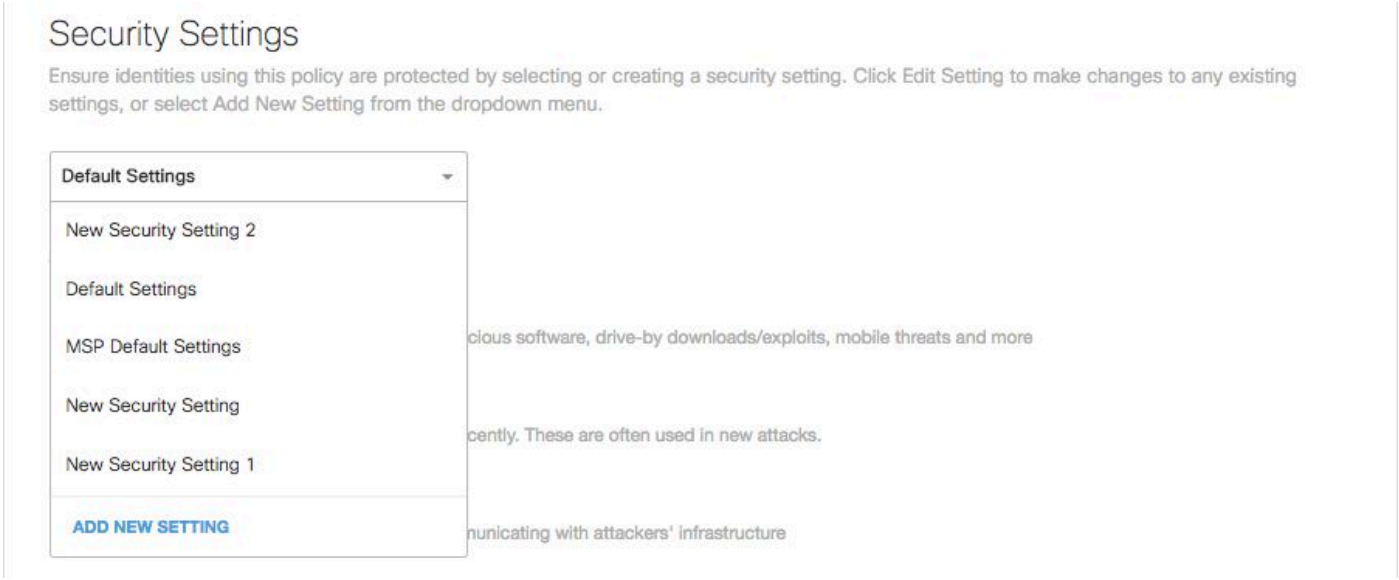
115014203703

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

1. Accédez à Politiques > Liste des politiques.

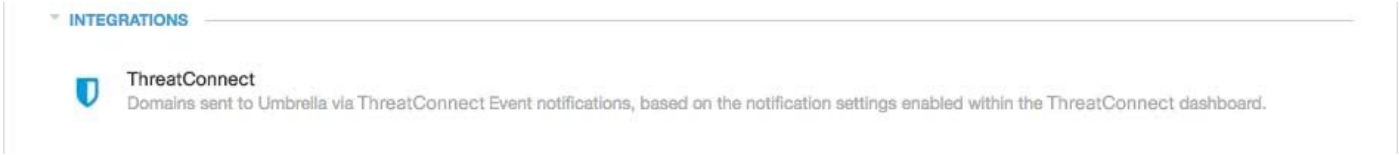
2. Élargissez une stratégie. Sous Paramètres de sécurité appliqués, sélectionnez Modifier.

3. Dans la liste déroulante Paramètres de sécurité, sélectionnez un paramètre de sécurité qui inclut le paramètre ThreatConnect.



25464103908884

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



115014037666

4. Sélectionnez Set & Return.

Les domaines ThreatConnect contenus dans le paramètre de sécurité de ThreatConnect sont ensuite bloqués pour les identités utilisant la stratégie.

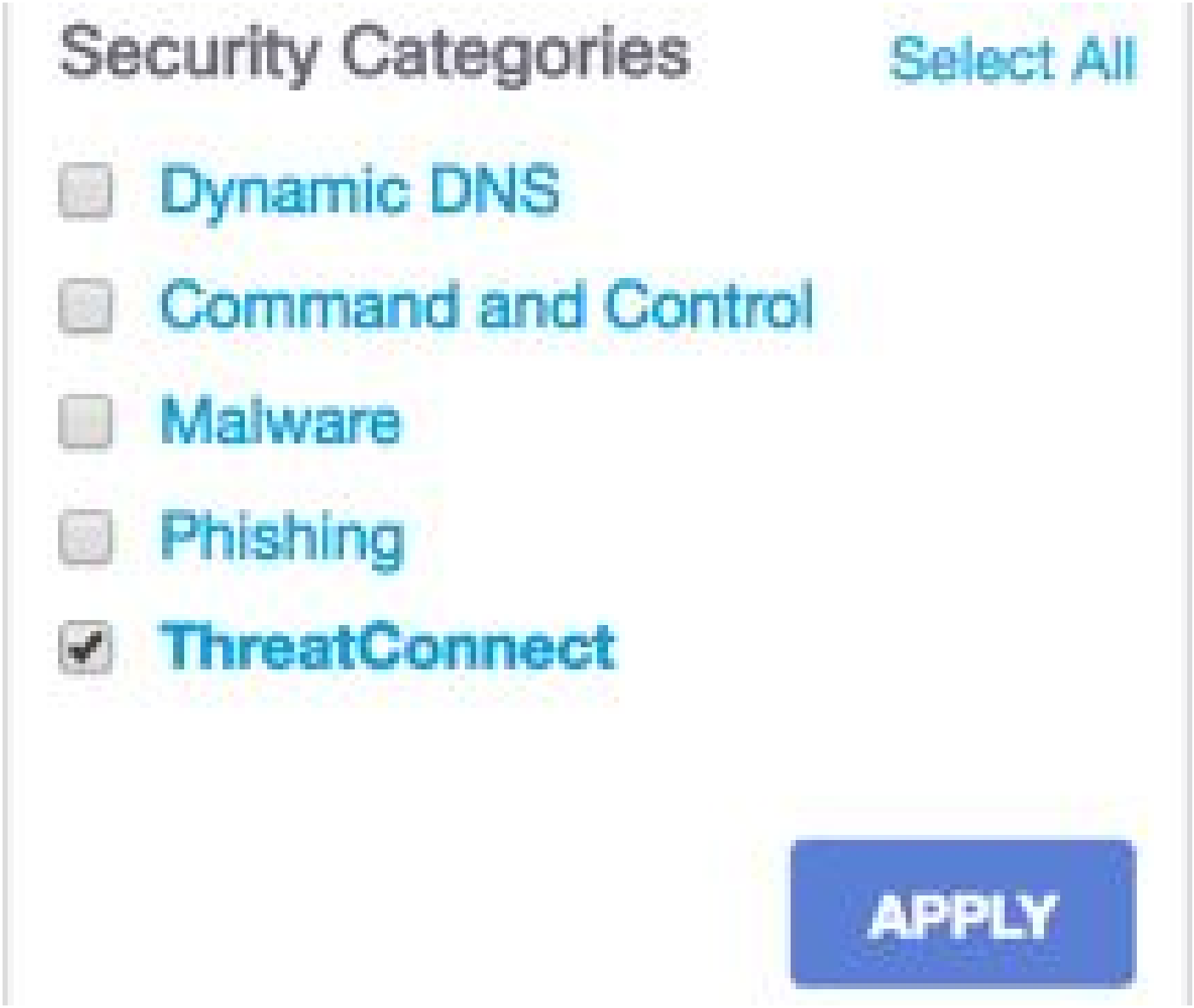
Création de rapports dans Umbrella pour les événements ThreatConnect

Création de rapports sur les événements de sécurité ThreatConnect

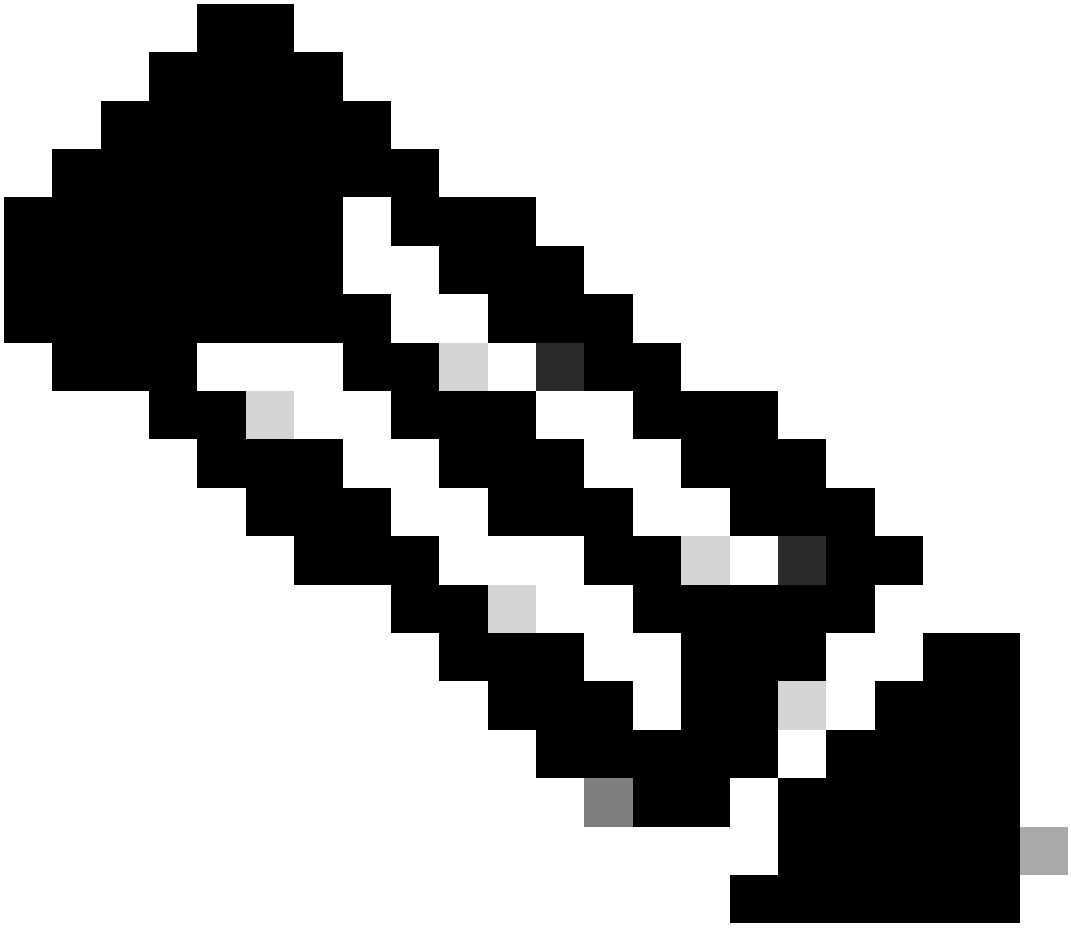
La liste de destinations ThreatConnect est l'une des listes de catégories de sécurité sur lesquelles vous pouvez générer des rapports. La plupart ou la totalité des rapports utilisent les catégories de sécurité comme filtre. Par exemple, vous pouvez filtrer les catégories de sécurité pour afficher uniquement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

1. Accédez à Reporting > Activity Search.

2. Sous Catégories de sécurité, sélectionnez ThreatConnect pour filtrer le rapport afin d'afficher uniquement la catégorie de sécurité pour ThreatConnect.



115014206603



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

3. Sélectionnez Appliquer.

Création de rapports lorsque des domaines ont été ajoutés à la liste de destinations ThreatConnect

Le journal d'audit d'administration inclut les événements du tableau de bord ThreatConnect lorsqu'il ajoute des domaines à la liste de destination. Un utilisateur nommé « Compte ThreatConnect », qui porte également le logo ThreatConnect, génère les événements. Ces événements incluent le domaine qui a été ajouté et l'heure à laquelle il a été ajouté.

Vous pouvez filtrer pour inclure uniquement les modifications ThreatConnect en appliquant un filtre pour l'utilisateur « Compte ThreatConnect ».

Gestion des détections indésirables ou des faux positifs

Listes d’autorisation

Bien que peu probable, il est possible que les domaines ajoutés automatiquement par ThreatConnect déclenchent un blocage indésirable qui empêcherait les utilisateurs d'accéder à des sites Web particuliers. Dans une situation comme celle-ci, Umbrella recommande 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.

Cette approche est préférable pour deux raisons :

- Tout d'abord, si le tableau de bord ThreatConnect a ajouté à nouveau le domaine après sa suppression, la liste d'autorisation prévient que cela entraîne d'autres problèmes.
- En outre, la liste verte affiche un historique des domaines problématiques pouvant être utilisés pour des analyses ou des rapports 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 ThreatConnect 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 Politiques > Listes de destinations et sélectionnez l'icône Ajouter (+).

2. Sélectionnez Autoriser et ajoutez votre domaine à la liste.

3. Sélectionnez Enregistrer.

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 ThreatConnect

Une icône Supprimer apparaît en regard de chaque nom de domaine dans la liste de destinations ThreatConnect. La suppression de domaines vous permet de nettoyer la liste de destinations ThreatConnect en cas de détection indésirable. Toutefois, la suppression n'est pas permanente si le tableau de bord ThreatConnect renvoie le domaine à Umbrella.

Pour supprimer un domaine :

1. Accédez à Politiques > Intégrations.

2. Sélectionnez ThreatConnect pour le développer.

3. Sélectionnez Voir Domaines.

4. Recherchez le nom de domaine que vous souhaitez supprimer.

5. Cliquez sur l'icône Supprimer.

6. Sélectionnez Fermer, puis Enregistrer.

Dans le cas d'une détection indésirable ou d'un faux positif, Umbrella recommande de créer immédiatement une liste d'autorisation dans Umbrella, puis de corriger le faux positif dans le tableau de bord ThreatConnect. Vous pourrez ensuite supprimer le domaine de la liste de destinations ThreatConnect.

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.