Intégrer ThreatQ à Umbrella

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Présentation de ThreatQ et de Cisco Umbrella Integration

Fonctionnalité d'intégration

Génération de jetons de script et API Umbrella

Comment configurer ThreatQ pour communiquer avec Umbrella

- Observation des événements ajoutés à la catégorie de sécurité ThreatQ en mode audit
- Vérifier la liste de destinations
- Vérifier les paramètres de sécurité d'une stratégie

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

Création de rapports dans Umbrella pour les événements ThreatQ

- Génération de rapports sur les événements de sécurité ThreatQ
- Signalement de l'ajout de domaines à la liste de destinations ThreatQ

Gestion des détections indésirables ou des faux positifs

- Listes d'autorisation
- Suppression de domaines de la liste de destinations ThreatQ

Introduction

Ce document décrit comment intégrer ThreatQ à Cisco Umbrella.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Un tableau de bord ThreatQ avec accès pour mettre à jour l'URL pour les intégrations
- Droits administratifs du tableau de bord parapluie
- L'intégration ThreatQ doit être activée sur le tableau de bord Umbrella.

Composants utilisés

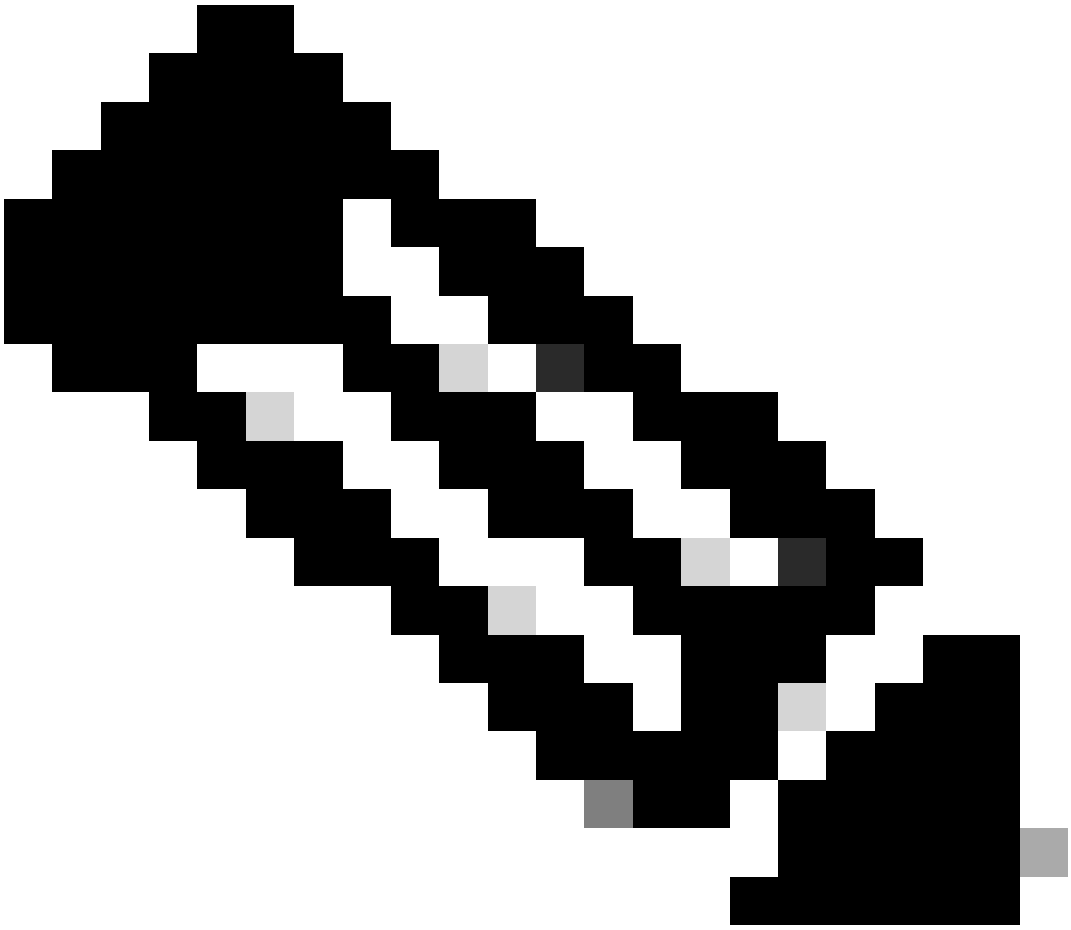
Les informations contenues dans ce document sont basées sur Cisco Umbrella.

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 ThreatQ et de Cisco Umbrella Integration

En intégrant ThreatQ 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 ThreatQ pour communiquer avec Umbrella afin que les événements de sécurité du conseil ThreatQ soient intégrés dans des politiques pouvant être appliquées aux clients protégés par Cisco Umbrella.



Remarque : L'intégration ThreatQ n'est incluse que dans certains packages Cisco Umbrella. Si vous ne disposez pas de la solution requise et souhaitez intégrer ThreatQ,

---

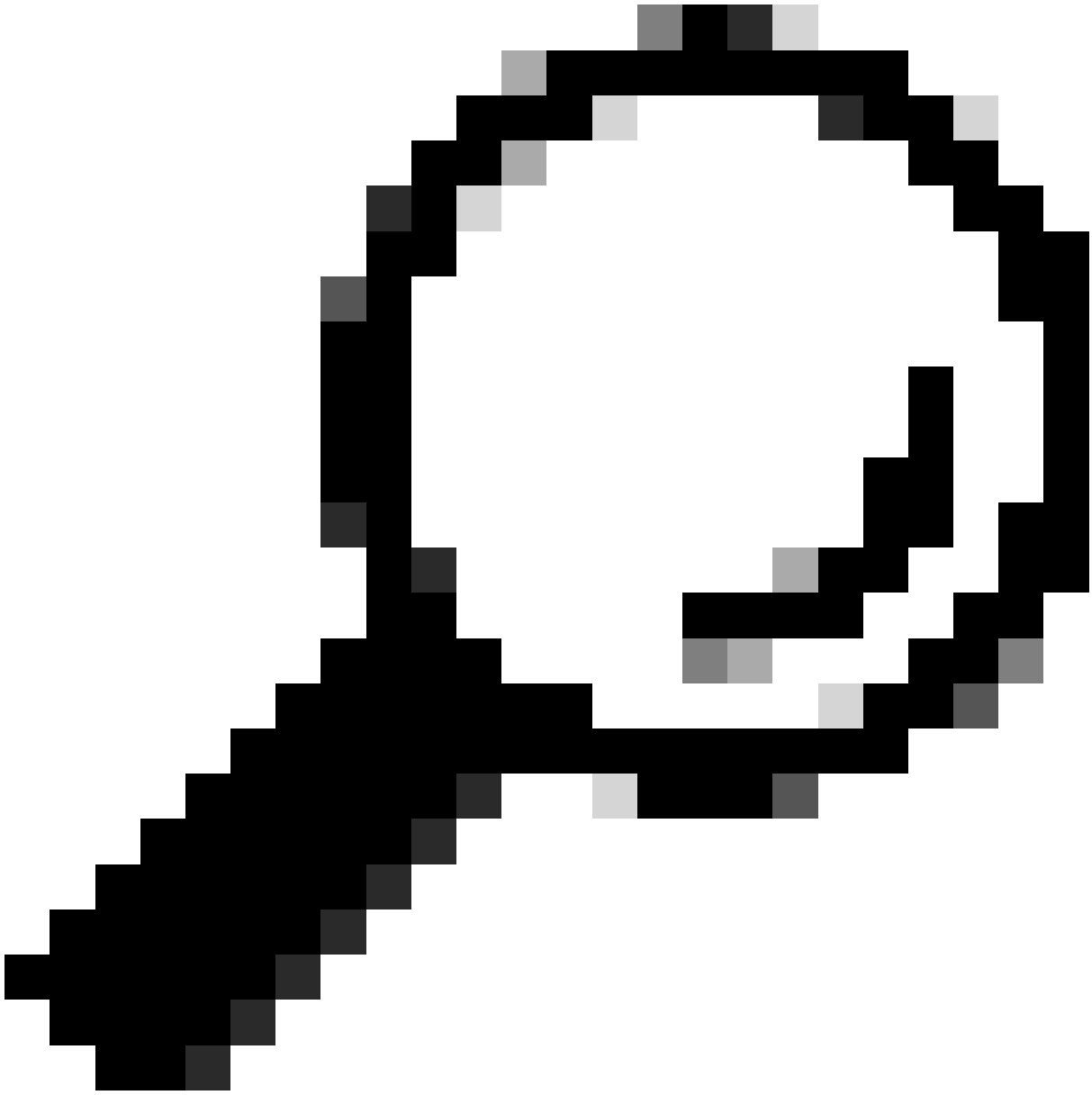
contactez votre représentant Cisco Umbrella. Si vous disposez du package Cisco Umbrella approprié mais que ThreatQ n'apparaît pas comme une intégration pour votre tableau de bord, contactez l'assistance Cisco Umbrella.

Fonctionnalité d'intégration

La plate-forme ThreatQ envoie d'abord à Umbrella les informations sur les cybermenaces qu'elle a détectées, telles que 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 ThreatQ constituent une menace, l'adresse de domaine est ajoutée à la liste de destinations ThreatQ 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 ThreatQ.

Par la suite, Umbrella analyse automatiquement les alertes ThreatQ et ajoute les sites malveillants à la liste de destinations ThreatQ. Cela étend la protection ThreatQ à tous les utilisateurs et périphériques distants et fournit une autre couche d'application à votre réseau d'entreprise.



Conseil : Alors que Cisco Umbrella fait de son mieux pour valider et autoriser les domaines généralement sûrs (par exemple, Google et Salesforce), pour éviter les interruptions indésirables, nous vous suggérons d'ajouter des domaines que vous ne souhaitez jamais avoir bloqués à la liste verte globale ou à d'autres listes de destinations conformément à votre politique. Exemples :

- La page d'accueil de votre entreprise
- 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 et dont Cisco Umbrella ne tient pas compte dans la validation automatique des domaines. Par exemple, « localcloudservice.com ».

Ces domaines peuvent être ajoutés à la liste verte globale, qui se trouve sous Politiques >

Listes de destinations dans Cisco Umbrella.

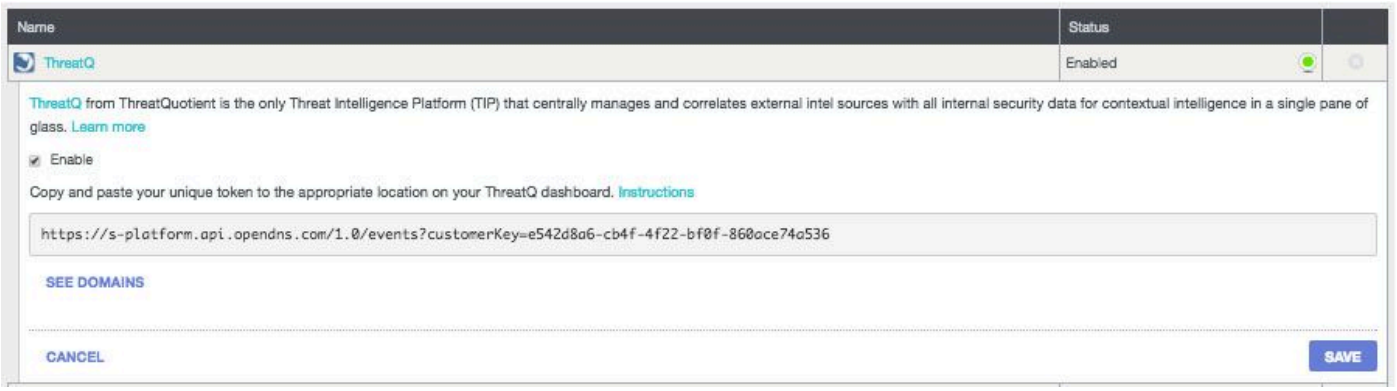
Génération de jetons de script et API Umbrella

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

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

2. Accédez à Paramètres > Intégrations et sélectionnez ThreatQ dans le tableau pour le développer.

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



Vous aurez besoin de l'URL ultérieurement lorsque vous configurerez ThreatQ pour envoyer des données à Umbrella. Copiez l'URL et accédez à votre tableau de bord ThreatQ.

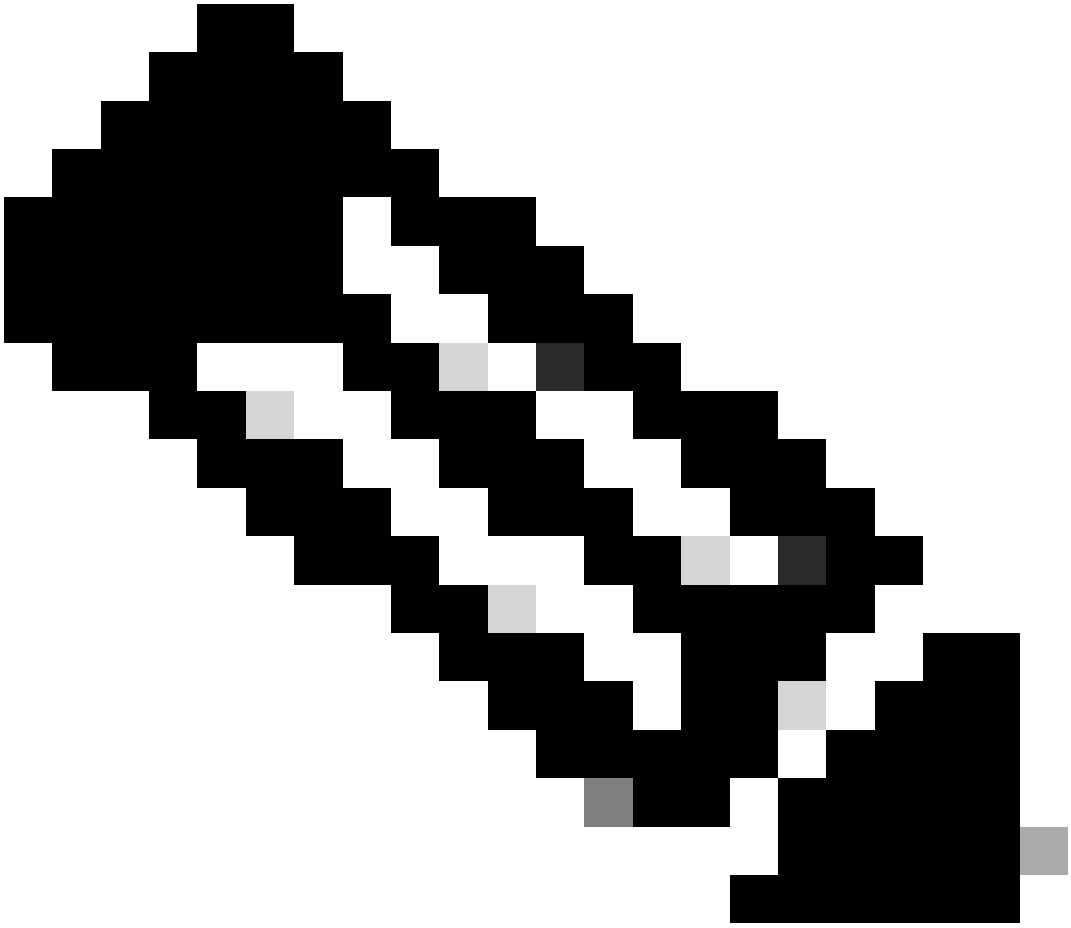
Comment configurer ThreatQ pour communiquer avec Umbrella

Connectez-vous à votre tableau de bord ThreatQ et ajoutez l'URL dans la zone appropriée pour vous connecter à Umbrella.

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

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

Au fil du temps, les événements de votre tableau de bord ThreatQ commencent à remplir une liste de destinations spécifique qui peut être appliquée aux stratégies en tant que catégorie de sécurité ThreatQ. Par défaut, la liste de destinataires et la catégorie de sécurité sont en mode Audit, ce qui signifie qu'elles ne sont appliquées à aucune stratégie et ne peuvent pas entraîner de modification de vos stratégies Umbrella existantes.



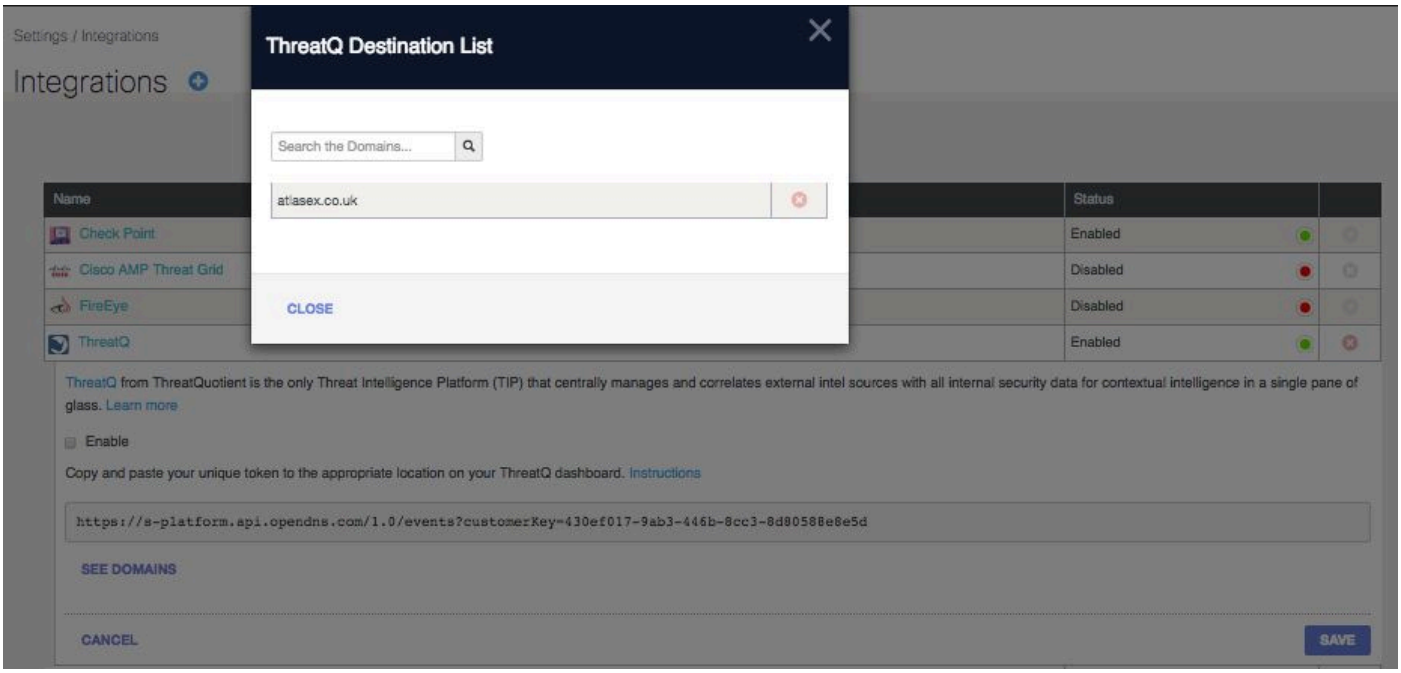
Remarque : Le mode audit peut être activé pendant la durée nécessaire, en fonction de votre profil de déploiement et de la configuration du réseau.

Vérifier la liste de destinations

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

1. Accédez à Paramètres > Intégrations.

2. Développez ThreatQ dans le tableau et sélectionnez Voir Domaines.



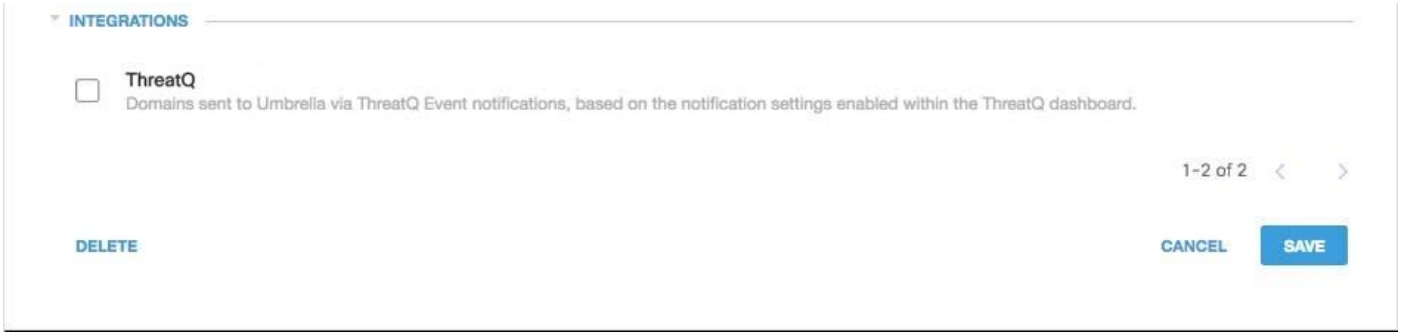
Vérifier les paramètres de sécurité d'une stratégie

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

1. Accédez à Stratégies > Paramètres de sécurité.

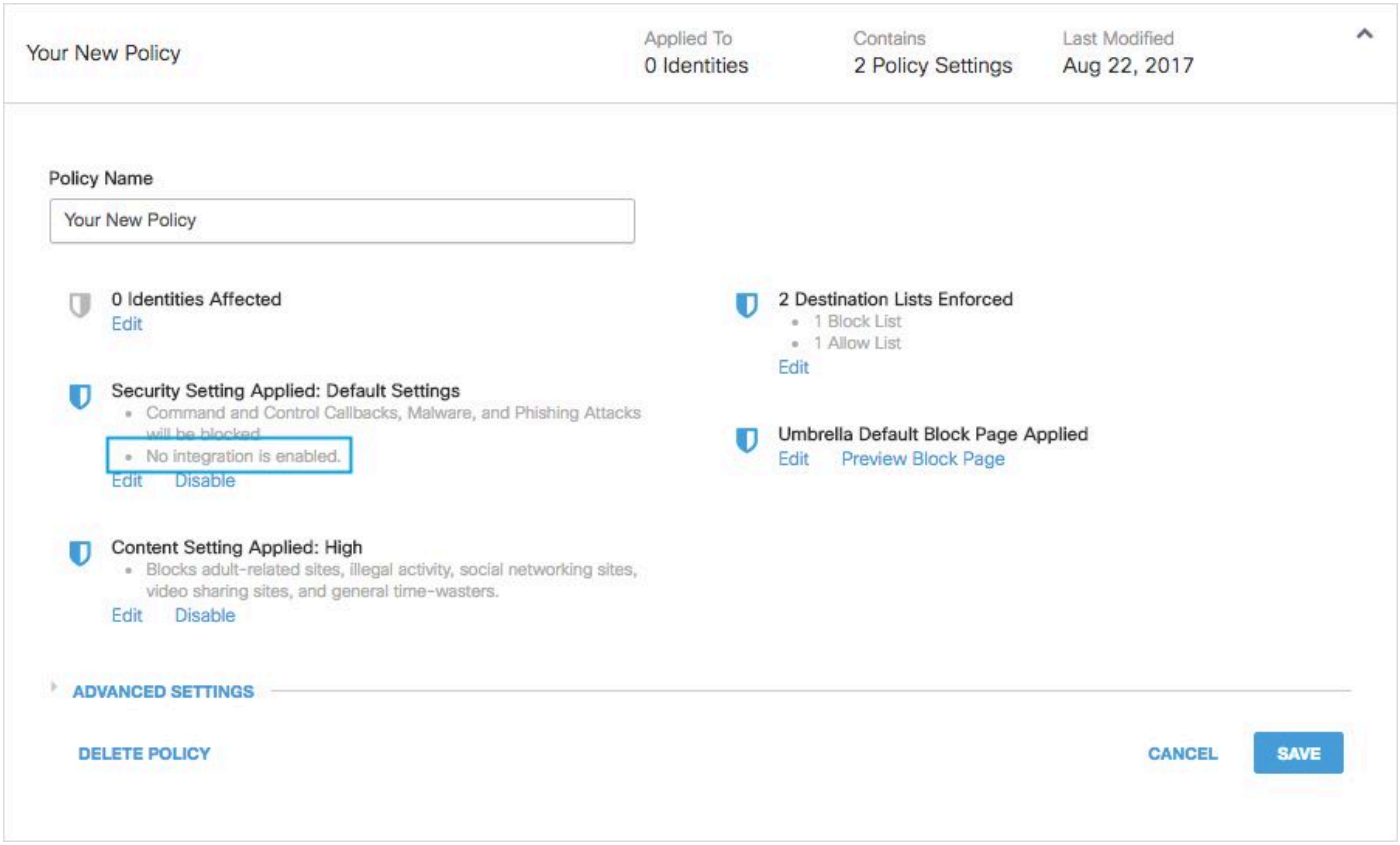
2. Sélectionnez un paramètre de sécurité dans la table pour le développer.

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



115014040286

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



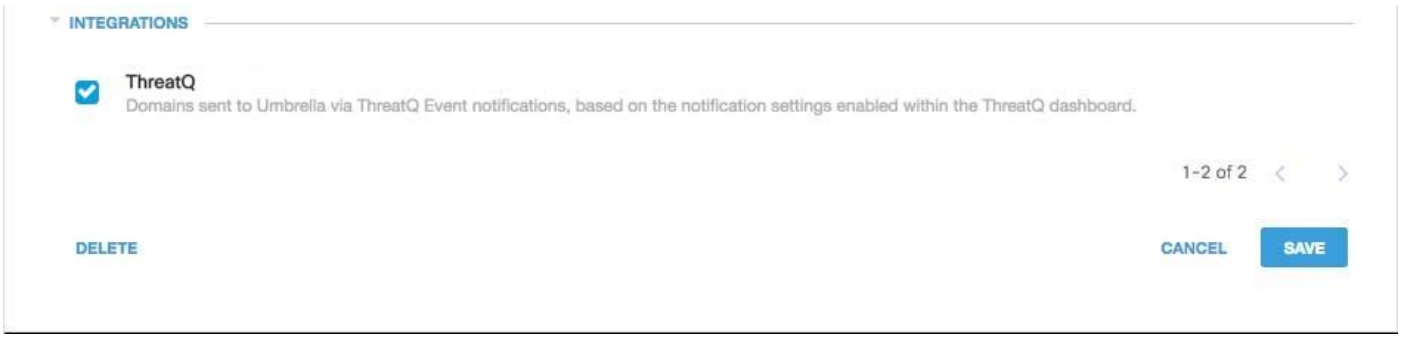
25464141748116

Application des paramètres de sécurité ThreatQ 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, vous pouvez modifier le paramètre de sécurité sur une stratégie existante ou créer une nouvelle stratégie qui se trouve plus haut que votre stratégie par défaut pour vous assurer qu'elle est appliquée en premier :

1.Accédez à Politiques > Paramètres de sécurité.

2. Sous Intégrations, sélectionnez ThreatQ et Enregistrer.



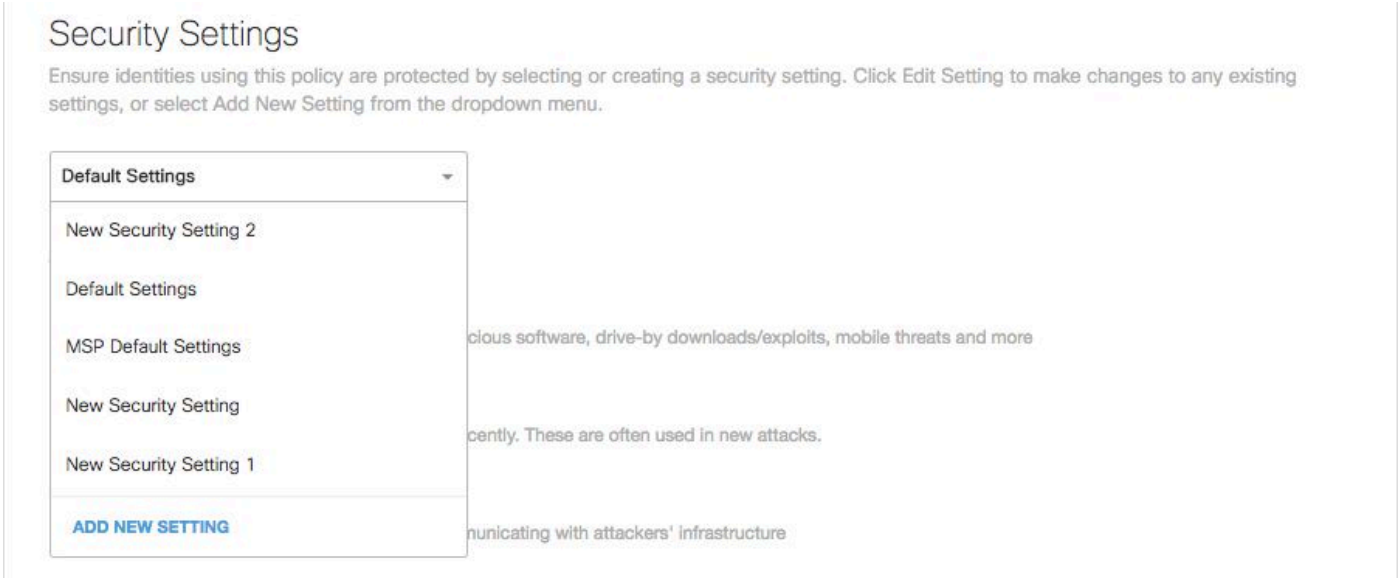
115014207403

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

1. Accédez à Politiques > Liste des politiques.

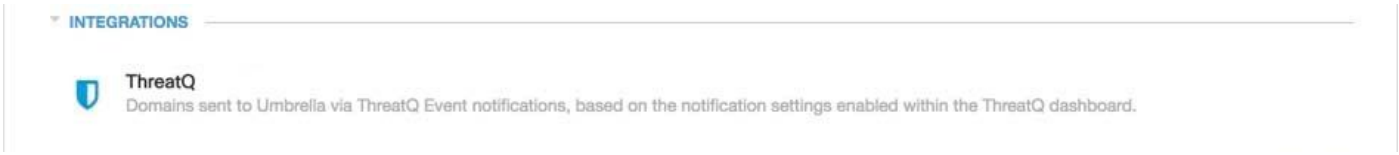
2. Développez une stratégie et sélectionnez Modifier sous Paramètres de sécurité appliqués.

3. Dans le menu déroulant Paramètres de sécurité, sélectionnez un paramètre de sécurité qui inclut le paramètre ThreatQ.



25464141787668

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



115014040506

4. Sélectionnez Set & Return.

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

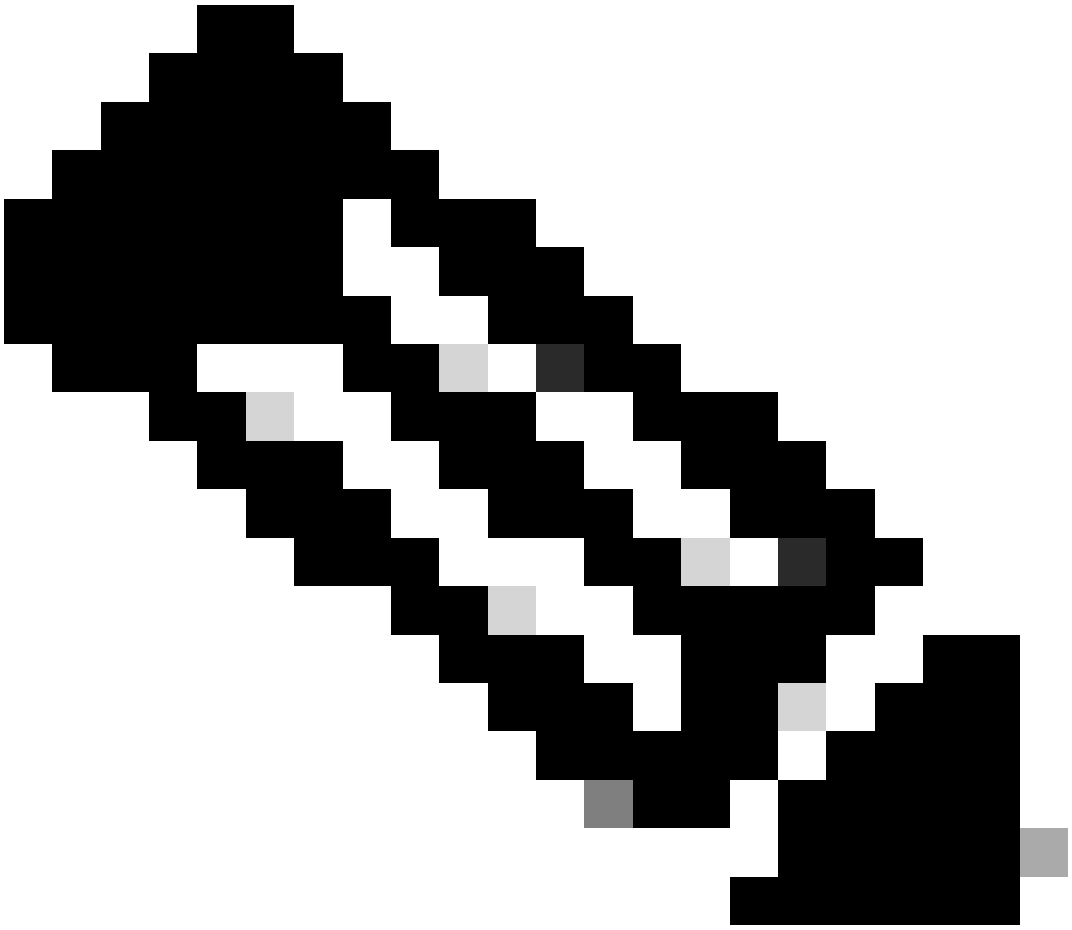
Création de rapports dans Umbrella pour les événements ThreatQ

Génération de rapports sur les événements de sécurité ThreatQ

La liste de destinations ThreatQ 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 les activités liées à ThreatQ.

1. Accédez à Reporting > Activity Search.

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



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

115014207603

3. Sélectionnez Appliquer.

Signalement de l'ajout de domaines à la liste de destinations ThreatQ

Le journal d'audit d'admin Umbrella inclut les événements du tableau de bord ThreatQ lors de l'ajout de domaines à la liste de destinations. Un utilisateur nommé « Compte ThreatQ », qui porte également le logo ThreatQ, génère les événements. Ces événements incluent le domaine qui a été ajouté et l'heure à laquelle il a été ajouté. Le journal d'audit d'admin Umbrella est disponible à l'adresse Reporting > Admin Audit Log.

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

Gestion des détections indésirables ou des faux positifs

Listes d’autorisation

Bien qu'improbable, il est possible que les domaines ajoutés automatiquement par ThreatQ déclenchent un blocage indésirable qui peut empêcher 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 ThreatQ devait rajouter le domaine après sa suppression, la liste verte prévient que cela entraîne d'autres problèmes.
- Ensuite, 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 ThreatQ 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 ThreatQ

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

Pour supprimer un domaine :

1. Accédez à Paramètres > Intégrations, puis sélectionnez ThreatQ pour le développer.

2. Sélectionnez Voir Domaines.

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

4. Cliquez sur l'icône Supprimer.

5. Sélectionnez Fermer.

6. Sélectionnez 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 ThreatQ. Vous pourrez ensuite supprimer le domaine de la liste de destinations ThreatQ.

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.