Configurer l'intégration de Secure Malware Analytics (anciennement Threat Grid) avec Umbrella

Table des matières

Introduction

Ce document décrit comment intégrer Secure Malware Analytics (anciennement Threat Grid) avec Umbrella.

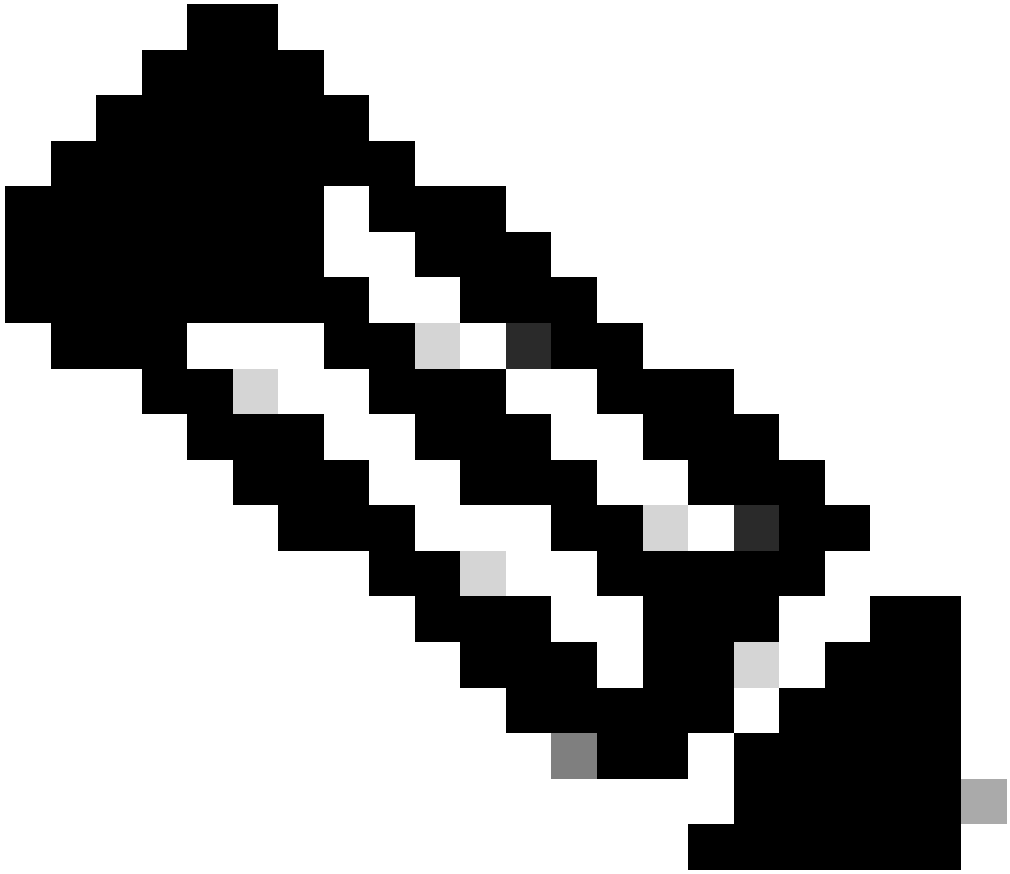
Présentation de l'intégration de Cisco Secure Malware Analytics (Threat Grid) pour Cisco Umbrella

Grâce à l'intégration de Cisco Secure Malware Analytics (anciennement Threat Grid) et de Cisco Umbrella, les équipes de sécurité peuvent désormais étendre leur visibilité et renforcer leur protection contre les menaces avancées actuelles qui pèsent sur les ordinateurs portables, les tablettes ou les téléphones itinérants, tout en offrant une couche supplémentaire d'application à un réseau d'entreprise distribué.

Ce guide explique comment configurer Cisco Secure Malware Analytics (Threat Grid) pour communiquer avec Cisco Umbrella afin que les informations sur les menaces générées par Cisco Secure Malware Analytics (Threat Grid) puissent être automatiquement intégrées dans des politiques qui protègent les clients sous votre Cisco Umbrella.

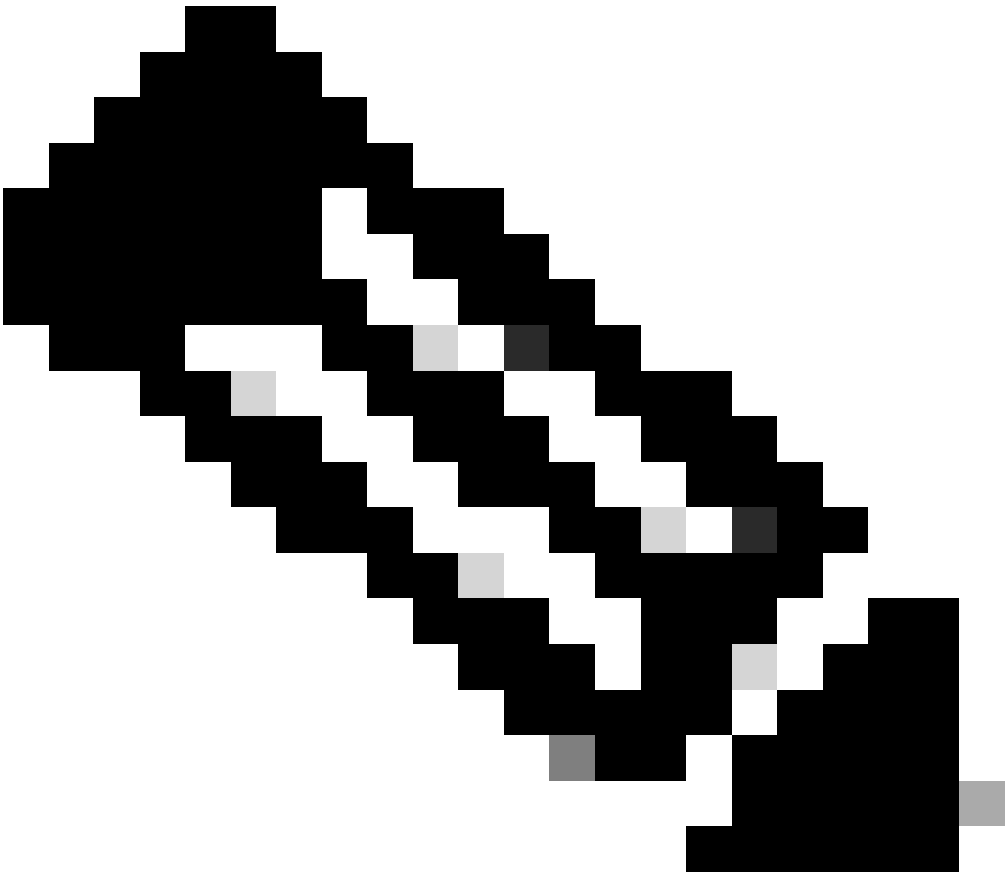
Conditions préalables

- Un tableau de bord fonctionnel Cisco Secure Malware Analytics (Threat Grid) avec accès à la clé API de votre compte.



Remarque : Les appareils et les terminaux Cisco Secure Malware Analytics (Threat Grid) ne sont pas pris en charge pour le moment.

- Droits d'administration de Cisco Umbrella Dashboard.
- L'intégration de Cisco Secure Malware Analytics (Threat Grid) doit être activée sur le tableau de bord Cisco Umbrella.



Remarque : L'intégration de Cisco Secure Malware Analytics (Threat Grid) est uniquement incluse dans les packages Cisco Umbrella tels que DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Si vous ne disposez pas d'un package Cisco Umbrella et souhaitez bénéficier de cette intégration, contactez votre responsable de compte Cisco Umbrella. Si vous disposez d'un package Cisco Umbrella mais que vous ne voyez pas Cisco Secure Malware Analytics (Threat Grid) comme une intégration pour votre tableau de bord, contactez l'assistance Cisco Umbrella.

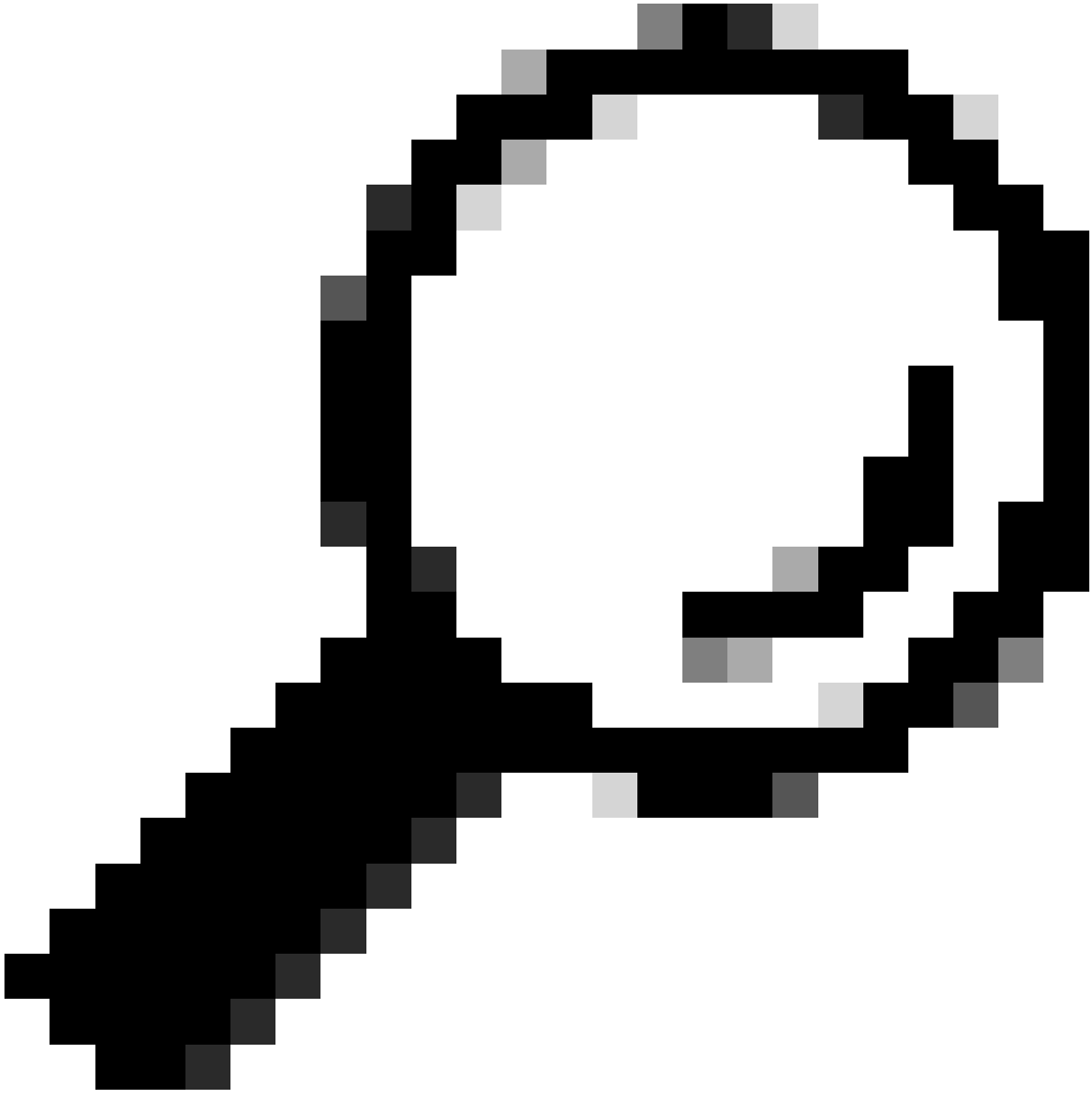
Comment fonctionne cette intégration ?

Cisco Umbrella s'adresse à l'API Cisco Secure Malware Analytics (Threat Grid) et récupère les listes de domaines générées à partir de l'analyse d'échantillons malveillants. Cisco Umbrella importe ensuite cette liste via l'API Cisco Umbrella Enforcement. Cette approche est différente de la façon dont les autres intégrations fonctionnent, car Cisco Umbrella tire parti de l'intelligence des menaces en effectuant des requêtes API vers l'API Cisco Secure Malware Analytics (Threat Grid), plutôt qu'en acceptant des incidents provenant d'autres systèmes qui transmettent l'intelligence

des menaces au service Cisco Umbrella.

Cisco Umbrella valide ensuite la menace pour s'assurer qu'elle peut être ajoutée à votre politique. S'il est confirmé que les informations provenant de Cisco Secure Malware Analytics (Threat Grid) constituent une menace ou qu'il ne s'agit pas d'un domaine valide connu, l'adresse de domaine est ajoutée à la liste de destinations de Cisco Secure Malware Analytics (Threat Grid) dans le cadre d'un paramètre de sécurité pouvant être appliqué à n'importe quelle stratégie Cisco Umbrella. Cette politique est immédiatement appliquée à toutes les requêtes effectuées à partir de périphériques utilisant des politiques exploitant l'intégration de Cisco Secure Malware Analytics (Threat Grid).

Cisco Umbrella extrait deux flux distincts de Cisco Secure Malware Analytics (Threat Grid) : un flux public (global) et un flux client uniquement (privé, spécifique à un seul client).



Conseil : Alors que Cisco Umbrella fait de son mieux pour valider et autoriser les

---

domaines généralement sûrs (par exemple, Google et Salesforce), pour éviter toute interruption indésirable, nous vous suggérons d'ajouter tous les 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 :

- Page d'accueil de votre organisation.
- Domaines représentant des services que vous fournissez qui peuvent 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 dont Cisco Umbrella n'a peut-être pas connaissance ou qu'il n'inclut pas dans leur validation automatique de domaine. Par exemple, « localcloudservice.com ».

Ces domaines doivent être ajoutés à la liste verte globale, qui se trouve sous Politiques > Listes de destinations dans Cisco Umbrella.

Configuration de votre tableau de bord Cisco Umbrella pour obtenir des informations auprès de Cisco Secure Malware Analytics (Threat Grid)

La première étape consiste à rechercher ou à générer la clé API dans votre tableau de bord Cisco Secure Malware Analytics (Threat Grid) :

1. Connectez-vous à votre tableau de bord Cisco Secure Malware Analytics (Threat Grid) et sélectionnez les détails de votre compte.
2. Sous vos détails de compte, une clé API peut déjà être visible si vous en avez déjà créé une. Si ce n'est pas le cas, sélectionnez Générer une nouvelle clé API.

   Votre clé API est alors visible sous Détails utilisateur > Clé API.

Ajoutez ensuite la clé API au tableau de bord Cisco Umbrella pour qu'il puisse extraire les données de Cisco Secure Malware Analytics (Threat Grid) :

1. Connectez-vous à votre tableau de bord Cisco Umbrella en tant qu'administrateur.
2. , accédez à Politiques > Composants de politique > Intégrations et sélectionnez « Cisco AMP Threat Grid » (Cisco Secure Malware Analytics (Threat Grid)) dans le tableau pour le développer.
3. Sélectionnez Enable, collez votre clé API dans la zone API Key, puis sélectionnez Save.

À ce stade, si vous recevez une erreur, il y a probablement un problème avec votre clé API ou les communications entre les services. Vérifiez votre clé API et réessayez, et si elle échoue toujours, contactez le support Cisco Umbrella.

Si vous recevez un message de réussite, cela indique que le service Cisco Umbrella a pu utiliser

la clé API pour établir une connexion initiale à l'API Cisco Secure Malware Analytics (Threat Grid). Le service Cisco Umbrella utilise un intervalle d'interrogation de cinq minutes pour récupérer les données de Cisco Secure Malware Analytics (Threat Grid).

Même après l'intervalle de cinq minutes, si aucune donnée valide ou aucun événement de menace valide ne peut être extrait par le tableau de bord Cisco Umbrella, les informations peuvent ne pas apparaître. Lorsque l'intégration est activée pour la première fois, elle commence simplement par revenir en arrière de cinq minutes pour les flux globaux et les flux d'entreprise uniquement et la première fois qu'elle reçoit des données se situe à l'intervalle de cinq minutes suivant, de sorte que les données peuvent ne pas apparaître immédiatement.

Si la clé API du côté de Cisco Secure Malware Analytics (Threat Grid) était désactivée ou supprimée, l'intégration serait désactivée. Pour restaurer l'intégration, une nouvelle clé API doit être fournie dans le tableau de bord Cisco Umbrella. En cas de dépassement du délai d'attente ou d'erreur de service interne entre Cisco Umbrella et Cisco Secure Malware Analytics (Threat Grid), une exception d'un type différent est déclenchée et l'intégration n'est pas désactivée. Au lieu de cela, les connexions continuent d'être tentées toutes les cinq minutes, comme dans des conditions normales.

Détails techniques

Les requêtes API exactes utilisées pour extraire des informations de Cisco Secure Malware Analytics (Threat Grid) sont répertoriées ci-dessous. Notez que seuls les événements d'un niveau de gravité supérieur à 90, d'un niveau de confiance supérieur à 90 et de type Domaines sont collectés. Dans cet exemple, l'heure est une plage de cinq minutes qui est incrémentée pour la requête suivante. L'`api_key` fourni dans Cisco Umbrella est utilisé à la place de la variable `<key>` :

- Public (flux global) :

  ```
  hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
  ```

- Client uniquement (flux privé) :

  ```
  hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
  ```

ou:

- Public (flux global) :

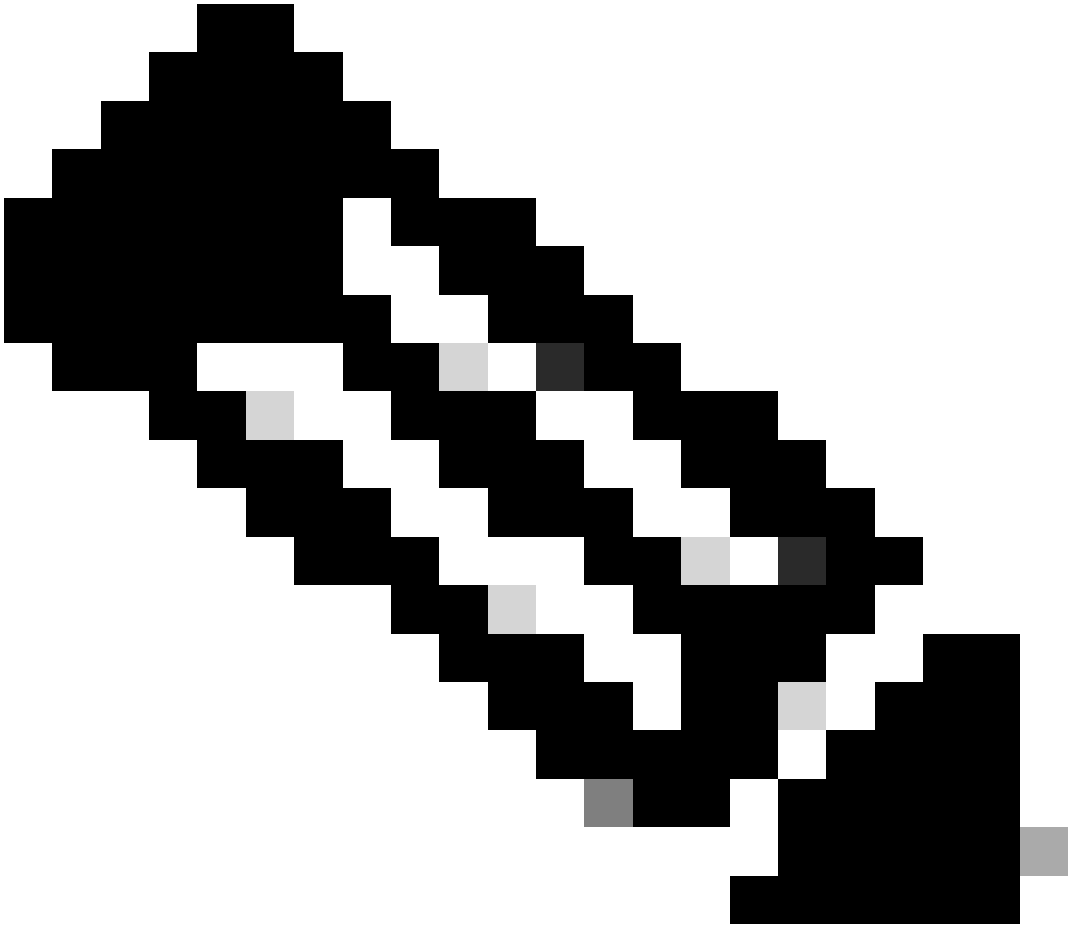
  ```
  hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
  ```

- Client uniquement (flux privé) :

hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=

Observation des événements ajoutés à Cisco Secure Malware Analytics (Threat Grid) en « mode audit »

Au fil du temps, les événements de Cisco Secure Malware Analytics (Threat Grid) commencent à remplir une liste de destinations spécifiques qui peuvent être appliquées à des politiques comme la catégorie Cisco Secure Malware Analytics (Threat Grid). Par défaut, la liste de destination et la catégorie de sécurité sont en « mode audit » et ne sont appliquées à aucune stratégie. Par conséquent, aucune requête n'est bloquée. Cependant, vous pouvez voir quelles requêtes sont associées (et auraient pu être bloquées) par la catégorie de sécurité Cisco AMP Threat Grid.



Remarque : Le « mode audit » peut être activé aussi longtemps que nécessaire, voire

indéfiniment, en fonction de votre profil de déploiement et de la configuration du réseau.

Vérifier la liste de destinations

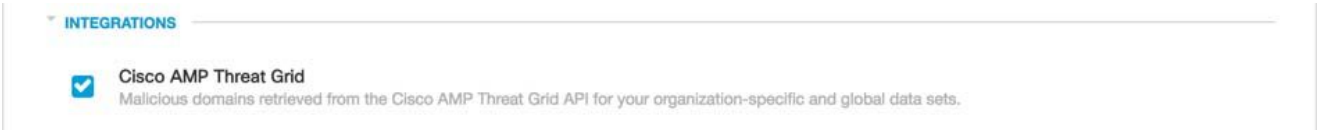
Vous pouvez consulter la liste de destinations Cisco Secure Malware Analytics (Threat Grid)à tout moment.

1. Accédez à Politiques > Composants de la politique > Intégrations.
2. Développez « Cisco AMP Threat Grid » (Cisco Secure Malware Analytics (Threat Grid)) dans le tableau et sélectionnez « Voir Domaines ».

Vérifier les paramètres de sécurité d'une stratégie

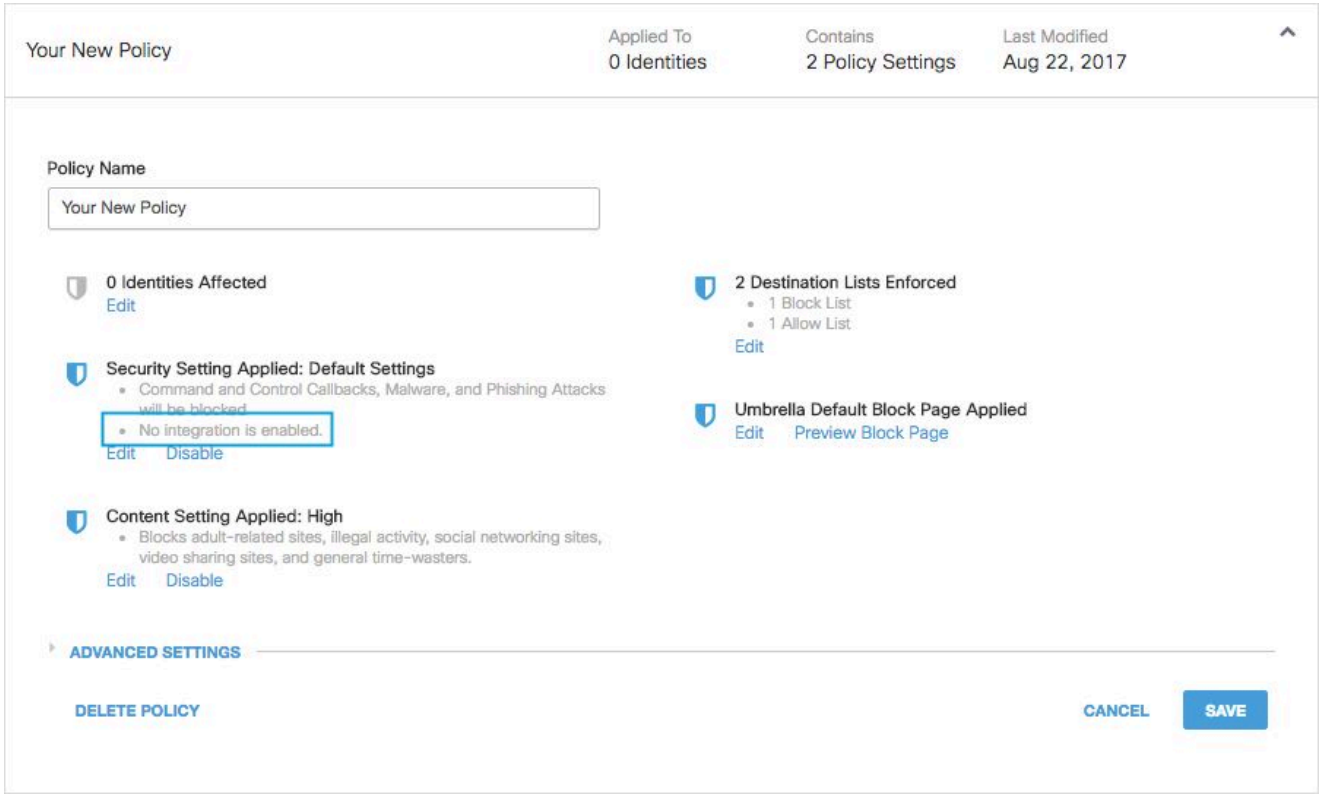
Vous pouvez consulter à tout moment les paramètres de sécurité pouvant être activés pour une stratégie dans Cisco Umbrella :

1. Accédez à Stratégies > Composants de stratégie > Paramètres de sécurité.
2. Cliquez sur un paramètre de sécurité dans le tableau pour le développer.
3. Faites défiler jusqu'à la section Integrations et développez la section pour afficher l'intégration de Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)).
4. Cochez la case correspondant à l'intégration de Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)), puis sélectionnez Save.

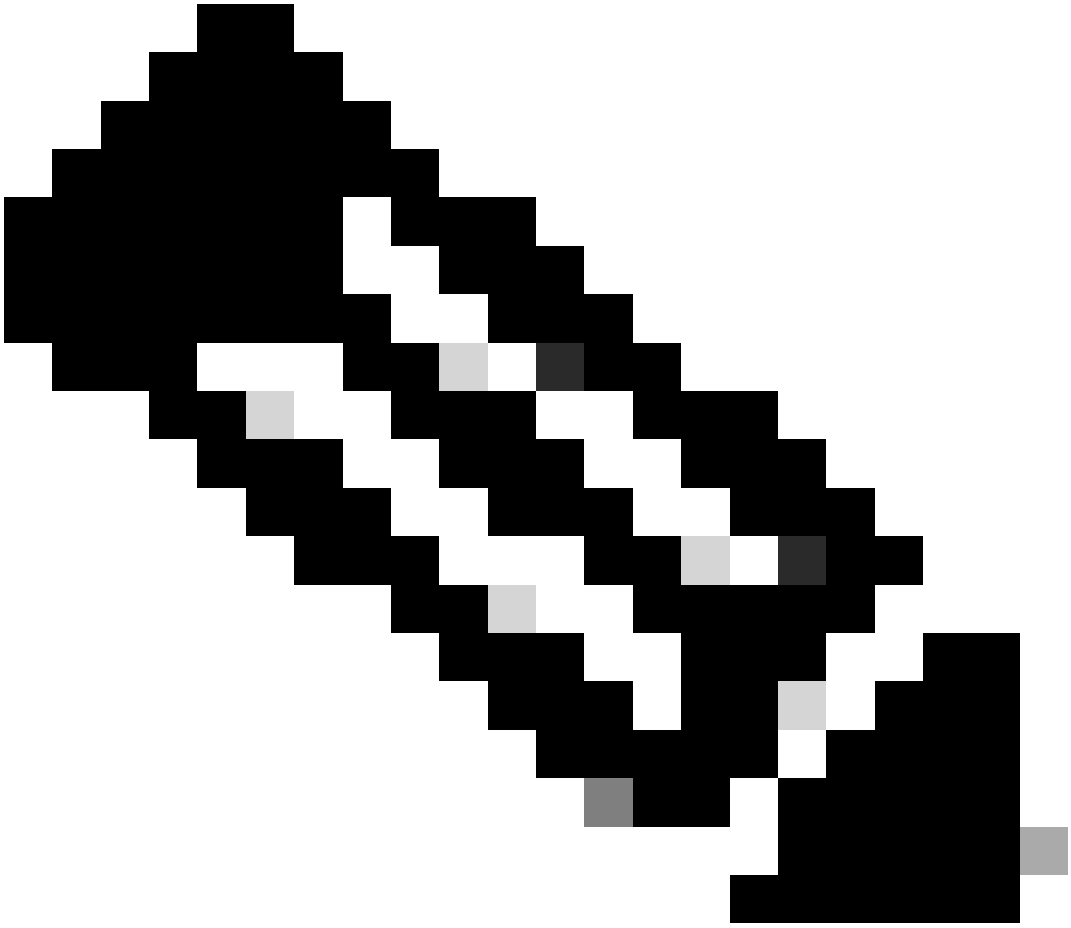


115014151543

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



20993269073556



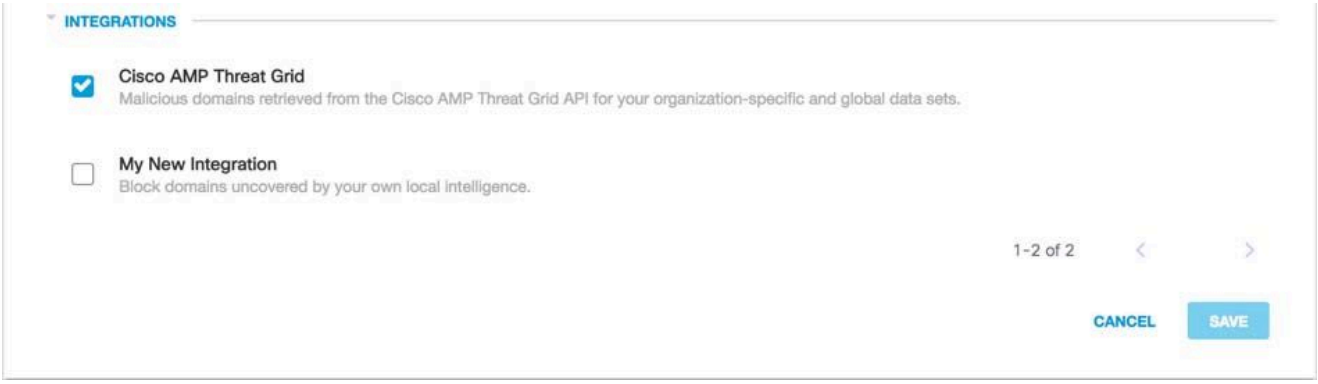
Remarque : L'application des paramètres peut prendre jusqu'à cinq minutes et si de nouveaux événements ne sont pas injectés dans le système Cisco Secure Malware Analytics (Threat Grid), vous ne verrez peut-être pas de nouveaux domaines ajoutés à votre intégration.

Application du paramètre de sécurité Cisco Secure Malware Analytics (Threat Grid) en mode « blocage » à une stratégie pour les clients gérés

Une fois que vous êtes prêt à bloquer ces domaines pour les clients gérés par Cisco Umbrella, modifiez le paramètre de sécurité sur une stratégie existante ou créez 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 Politiques > Composants de la stratégie > Paramètres de sécurité.

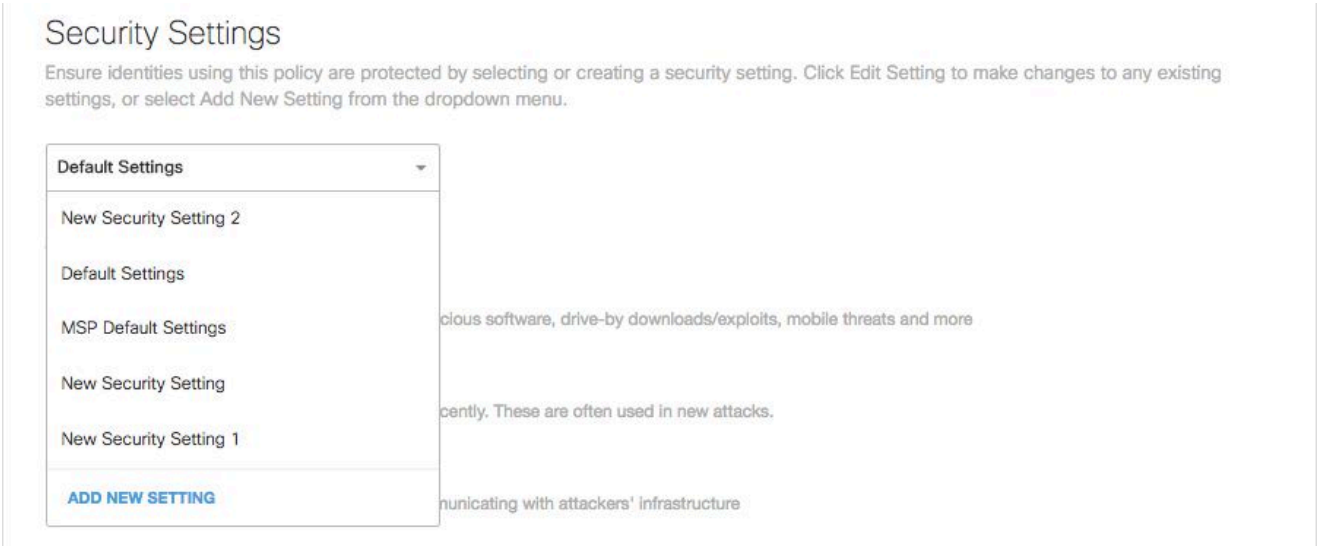
2. Sous Integrations, vérifiez que la case « Cisco AMP Threat Grid » est cochée. Si ce n'est pas le cas, cochez la case et sélectionnez Enregistrer.



115013987086

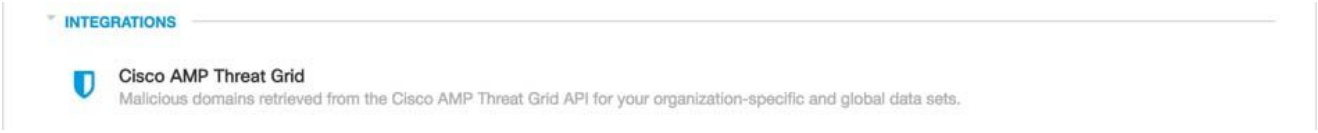
Ensuite, dans l'assistant Cisco Umbrella Policy, ajoutez un paramètre de sécurité à la stratégie que vous modifiez :

1. Accédez à Policies > Management > All Policies.
2. Développez une stratégie et sous Paramètres de sécurité appliqués, puis sélectionnez Modifier.
3. Dans le menu déroulant Security Settings, sélectionnez un paramètre de sécurité qui inclut le paramètre « Cisco AMP Threat Grid ».



20993282642708

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



115013987446

4. Sélectionnez Set & Return.

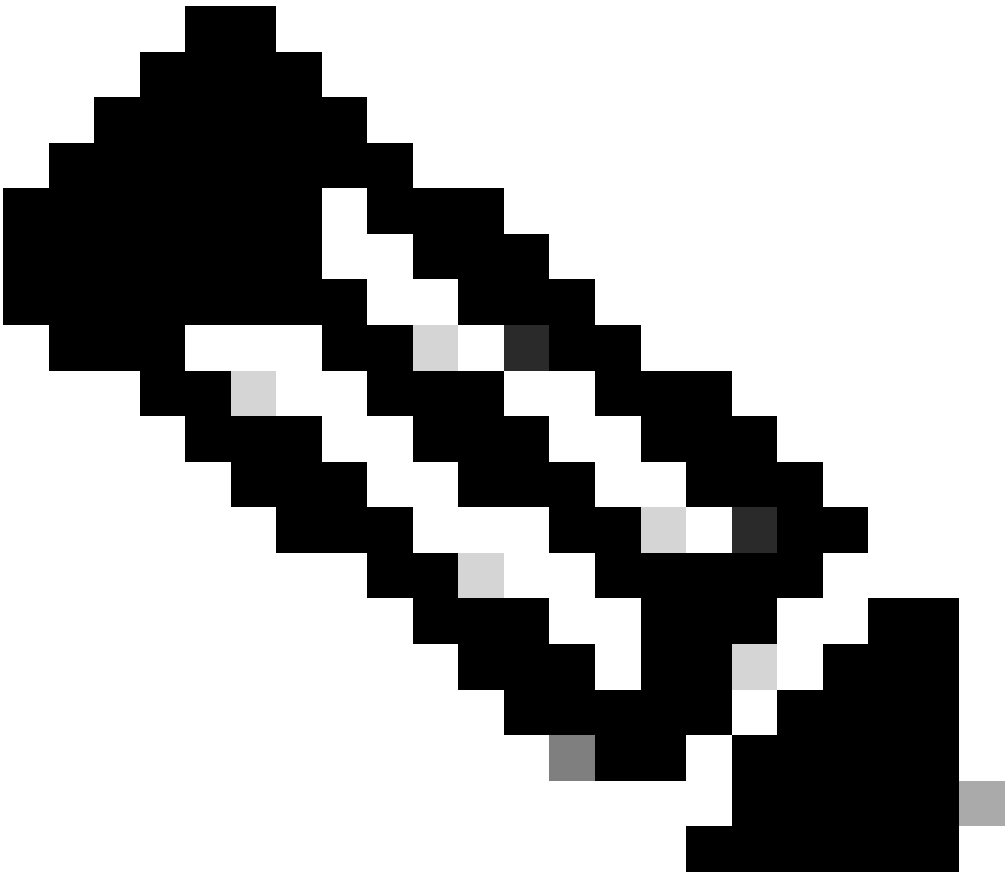
   Les domaines Cisco Secure Malware Analytics (Threat Grid) contenus dans le paramètre de sécurité de Cisco Secure Malware Analytics (Threat Grid) sont bloqués pour les identités utilisant la stratégie.

Création de rapports dans Cisco Umbrella pour les événements Cisco Secure Malware Analytics

Génération de rapports sur les événements de sécurité Cisco Secure Malware Analytics (Threat Grid)

La liste de destinations Cisco Secure Malware Analytics (Threat Grid) 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 Cisco Secure Malware Analytics (Threat Grid).

1. Accédez à Reporting > Core Reports > Activity Search et sous Security Categories sélectionnez « Cisco AMP Threat Grid » (Cisco Secure Malware Analytics (Threat Grid)) pour filtrer le rapport afin d'afficher uniquement la catégorie de sécurité pour Cisco Secure Malware Analytics (Threat Grid).



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

115014210123

2. Sélectionnez Apply.

Création de rapports sur le moment où les domaines ont été ajoutés à la liste de destinations Cisco Secure Malware Analytics (Threat Grid)

Le journal d'audit de Cisco Umbrella Admin inclut les événements du tableau de bord Cisco Secure Malware Analytics (Threat Grid) lors de l'ajout de domaines à la liste de destination. Un utilisateur nommé « Cisco AMP Threat Grid Domain List », également marqué du logo Cisco, génère les événements. Ces événements incluent le domaine qui a été ajouté et l'heure à laquelle il a été ajouté.

La sélection de l'entrée Admin Audit Log la développe pour afficher les détails, y compris le domaine spécifique qui a été ajouté.

Vous pouvez appliquer un filtre pour inclure uniquement les modifications de Cisco Secure Malware Analytics (Threat Grid) en appliquant un filtre pour l'utilisateur « Liste de domaines de

Cisco AMP Threat Grid ».

Gestion des détections indésirables ou des faux positifs

Deux types de détection Cisco Secure Malware Analytics (Threat Grid) et deux solutions

Il existe actuellement deux types de blocs Cisco Secure Malware Analytics (Threat Grid) : Une avec une résolution possible et une seconde avec une résolution actuelle pour une détection indésirable.

1. Entrée dans Global Threat Grid (Public) : Pour l'instant, la seule méthode pour autoriser le domaine est de l'ajouter à votre liste d'autorisation.
2. Flux client uniquement (privé) : peut être traité à l'aide d'une entrée de liste verte ou supprimé de la liste d'intégration d'AMP Threat Grid.

Listes d’autorisation

Bien que peu probable, il est possible que les domaines ajoutés automatiquement par votre intégration Cisco Secure Malware Analytics (Threat Grid) déclenchent une détection indésirable qui empêche vos utilisateurs d'accéder à des sites Web particuliers. Dans une telle situation, nous vous recommandons d'ajouter le ou les domaines à une liste d'autorisation (Stratégies > Listes de destination), qui est prioritaire sur tous les autres types de listes de blocage, y compris les paramètres de sécurité.

Cette approche est privilégiée pour deux raisons. Tout d'abord, si le tableau de bord Cisco Secure Malware Analytics (Threat Grid) devait rajouter 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'analyse 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 Cisco Secure Malware Analytics (Threat Grid) en mode bloc est appliqué uniquement à un sous-ensemble de vos identités Cisco 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 Stratégies > Composants de stratégie > Listes de destination et sélectionnez 

(« Ajouter »).
2. Sélectionnez Allow et ajoutez votre domaine à la liste.

3. Sélectionnez Enregistrer.

Une fois la liste 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 de Cisco Secure Malware Analytics (Threat Grid)

À côté de chaque nom de domaine dans la liste Cisco Secure Malware Analytics (Threat Grid) figure une icône (« Supprimer »). La suppression de domaines vous permet de nettoyer la liste de destinations Cisco Secure Malware Analytics (Threat Grid) en cas de détection indésirable.

La suppression n'est pas permanente si le tableau de bord Cisco Secure Malware Analytics (Threat Grid) renvoyait le domaine à Cisco Umbrella.

1. Accédez à Politiques > Composants de politique > Intégrations et sélectionnez « Cisco AMP Threat Grid » (Cisco Secure Malware Analytics (Threat Grid)) pour le développer.
2. Sélectionnez Voir Domaines.
3. Recherchez le nom de domaine que vous souhaitez supprimer.
4. Sélectionnez l'icône ("Supprimer").
5. Sélectionnez Fermer.
6. Sélectionnez Enregistrer.

En cas de détection indésirable ou de faux positif, nous vous recommandons de créer immédiatement une liste d'autorisation dans Cisco Umbrella, puis de corriger le faux positif dans le tableau de bord Cisco Secure Malware Analytics (Threat Grid). Vous pourrez ensuite supprimer le domaine de la liste de destinations Cisco Secure Malware Analytics (Threat Grid).

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.