Comprendre l'API Umbrella Enforcement pour les intégrations personnalisées

Table des matières

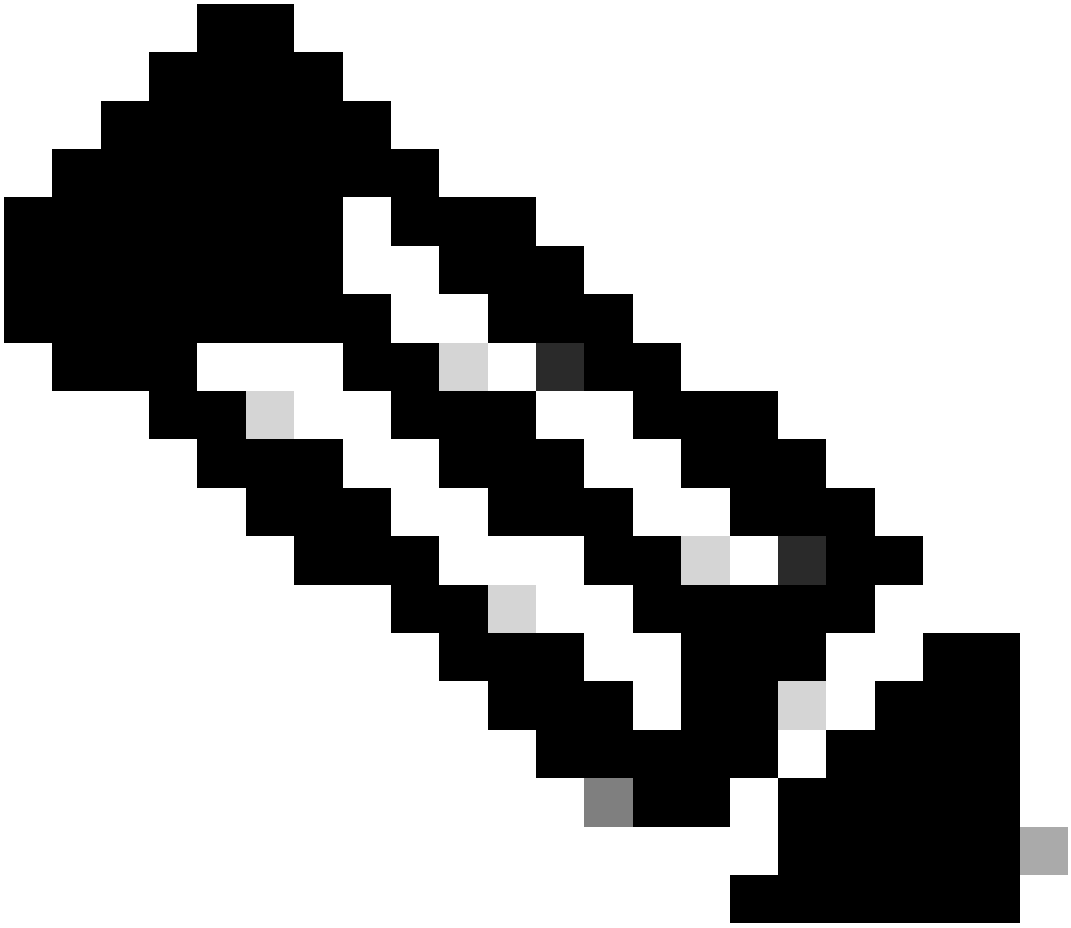
Introduction

Ce document décrit l'API Umbrella Enforcement pour les intégrations personnalisées.

Qu'est-ce que l'API Umbrella Enforcement ?

L'API Umbrella Enforcement permet aux partenaires et aux clients disposant de leurs propres environnements SIEM/TIP (Threat Intelligence Platform) d'injecter des événements et/ou des informations sur les menaces dans leur environnement Umbrella. Ces événements sont alors instantanément convertis en visibilité et en application qui peuvent s'étendre au-delà du périmètre et donc de la portée des systèmes susceptibles d'avoir généré ces événements ou des informations sur les menaces.

L'API d'application peut ingérer des événements au format d'événement générique décrit dans cette documentation d'API et peut prendre en charge les fonctions ADD, DELETE ou LIST.



Remarque : Si vous ne disposez pas de l'API Umbrella Enforcement pour les intégrations personnalisées dans votre tableau de bord Umbrella et que vous souhaitez y accéder, contactez votre représentant Cisco Umbrella.

Pourquoi l'utiliserais-je ?

Il se peut que vous traitiez, gériez et organisiez déjà votre propre système et vos propres processus de renseignements sur les menaces, ce qui vous incite à prendre des mesures sur les domaines identifiés comme malveillants ou suspects. Dans ce cas, une fois qu'une décision a été prise qu'un événement doit être traité (par exemple, converti en protection), plutôt que d'ajouter manuellement la protection à Umbrella à des fins d'application, vous pouvez utiliser l'API d'application pour automatiser ce processus et appliquer instantanément la protection en fonction des domaines associés à l'événement.

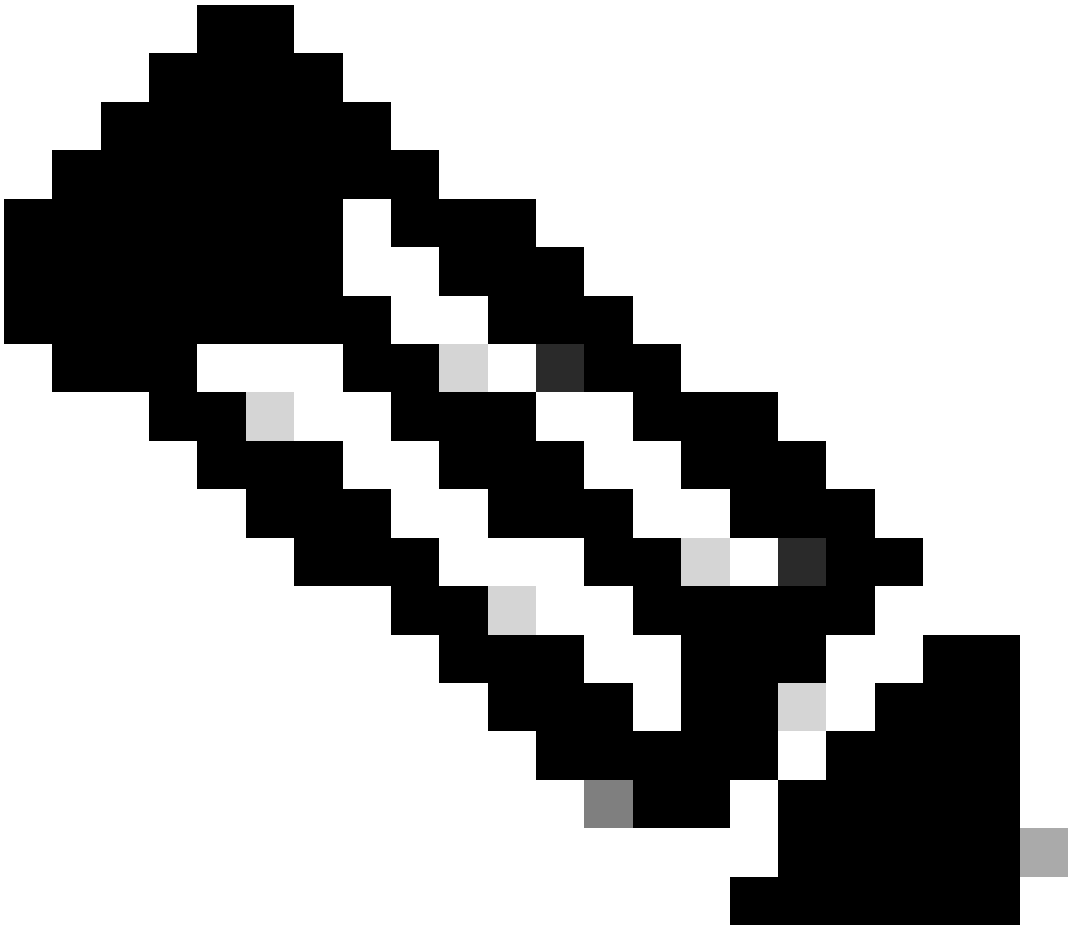
Cela permet à votre équipe de sécurité de concentrer son temps et ses efforts sur les investigations plutôt que sur la configuration en cours d'Umbrella. Elle permet à votre équipe de

sécurité de conserver ses outils et processus au lieu de devoir accéder au tableau de bord Umbrella pour mettre à jour les listes de destinations. En substance, vous pouvez créer une liste de destinations dans Umbrella à partir d'une source externe que vous gérez directement via l'API, puis choisir de bloquer ces destinations pour les identités dans Umbrella.

Comment L'Utiliserais-Je ?

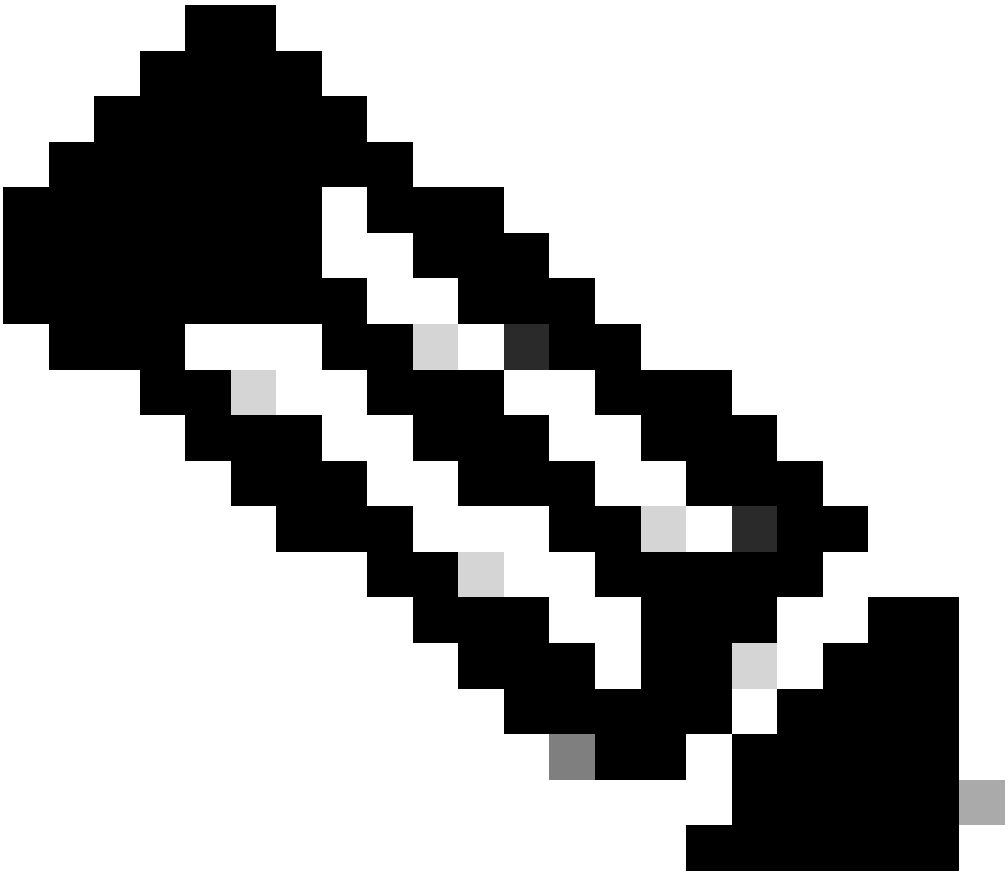
AJOUTER un événement à l'API d'application

Une fois qu'un événement a été ajouté, l'application tente d'extraire des domaines de l'événement.



Remarque : La prise en charge des adresses IP et des URL sera ajoutée ultérieurement.

- Un événement peut contenir n'importe quelle quantité de détails d'événement d'origine que vous souhaitez, mais doit respecter les spécifications décrites dans la documentation de l'API.



Remarque : La prise en charge des détails des événements de surfaçage dans le tableau de bord Umbrella peut être ajoutée ultérieurement.

- Si un domaine est extrait, il est validé par le graphique de sécurité Cisco Umbrella pour s'assurer qu'il ne s'agit pas d'un domaine valide connu susceptible d'entraîner des faux positifs ou déjà considéré comme malveillant par le graphique de sécurité Cisco Umbrella.
- S'il est validé (par exemple, s'il est inconnu et peut être bloqué en toute sécurité), il est ajouté à une liste de destinataires associée à cette intégration personnalisée et apparaît dans le tableau de bord Umbrella comme une catégorie de sécurité personnalisée.
- La catégorie de sécurité personnalisée peut être bloquée ou autorisée par stratégie, pour permettre l'application active ou l'« audit » passif des demandes suspectes.

LIST domaines pour une liste d'API d'application

- Si votre flux de travail inclut le déblocage des domaines qui ont été bloqués en raison d'événements précédemment injectés, une requête LIST fournit tous les domaines actuellement inclus dans la liste de destination associée à cette intégration.

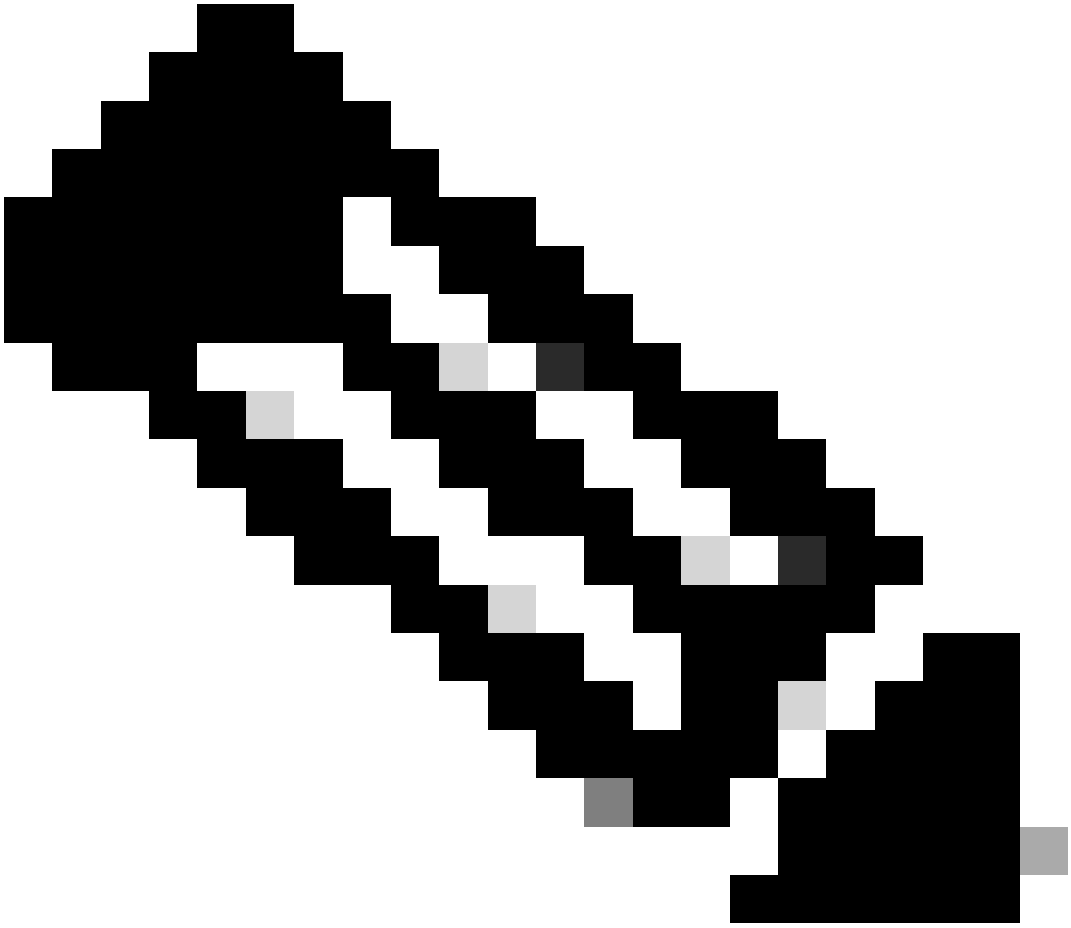
SUPPRIMER le domaine de la liste API d'application

- Si votre flux de travail inclut le déblocage de domaines qui ont été bloqués en raison d'événements précédemment injectés, une demande DELETE vous permet de supprimer un domaine de la liste de destinations associée à cette intégration.
- Si une demande DNS entrante provenant de l'une de vos identités Umbrella est destinée à un domaine dans la liste de destination d'intégration personnalisée, elle est bloquée ou autorisée en fonction du paramètre de sécurité de l'intégration personnalisée associé à la stratégie qui l'a déclenchée.
- Les résultats sont consignés avec tous les autres événements Umbrella, accessibles via la recherche d'activité ou via Amazon S3 à l'aide de l'intégration S3. Ainsi, le trafic associé à l'intégration personnalisée peut éventuellement être réintégré dans votre SIEM/TIP et la boucle de rétroaction fermée.

Procédure pas à pas d'utilisation de l'API Application

Étape 1 : Créez votre intégration personnalisée

Vous pouvez avoir jusqu'à 10 intégrations personnalisées à la fois.



Remarque : Si l'organisation est une organisation enfant d'un MSP, MSSP ou MOC Umbrella, les intégrations personnalisées partagées à partir du niveau de la console s'affichent avant les intégrations créées au niveau de l'organisation enfant.

1. Dans Umbrella, accédez à Politiques > Composants de stratégie > Intégrations et cliquez sur Ajouter.
2. Ajoutez un nom pour l'intégration personnalisée et cliquez sur Créer.
3. Développez votre nouvelle intégration personnalisée, cochez Enable, copiez l'URL d'intégration, puis cliquez sur Save.

Étape 2 : Créez votre ou vos scripts personnalisés.

1. Reportez-vous aux exemples de scripts generate_event et delete_domain dans l'annexe de ce document ou utilisez la documentation de l'API pour créer vos propres scripts afin de générer les demandes correctement formatées pour générer des événements, ou pour supprimer ou répertorier des domaines. Vous voudrez utiliser l'URL d'intégration

personnalisée dans ces scripts à l'avenir.

Étape 3 : Injecter un exemple d'événement

1. Utilisez le script que vous avez créé pour injecter un événement dans votre intégration personnalisée. Dans notre exemple, nous avons ajouté un événement contenant le domaine « creditcards.com ».

Étape 4 : Vérifiez la liste de destinations dans le tableau de bord Umbrella

1. Revenez à Paramètres > Intégrations et dans le tableau développez votre intégration personnalisée.
2. Cliquez sur Voir domaines. Une liste des domaines ajoutés pouvant faire l'objet d'une recherche s'affiche et votre exemple d'événement de l'étape 4 figure maintenant dans la liste.

Étape 5 : Consultez le journal d'audit Admin.

1. Vous pouvez également vérifier l'activité associée à votre intégration personnalisée en consultant le journal d'audit d'administration.
2. Accédez à Reporting > Admin Audit Log.
3. Sous Filtres, entrez le nom de votre intégration personnalisée dans Filtrer par identités et paramètres, puis cliquez sur Exécuter le filtre.

Lorsque vous développez l'entrée, vous voyez maintenant l'événement qui a entraîné l'ajout de votre exemple d'événement (creditcards.com) à votre intégration personnalisée.

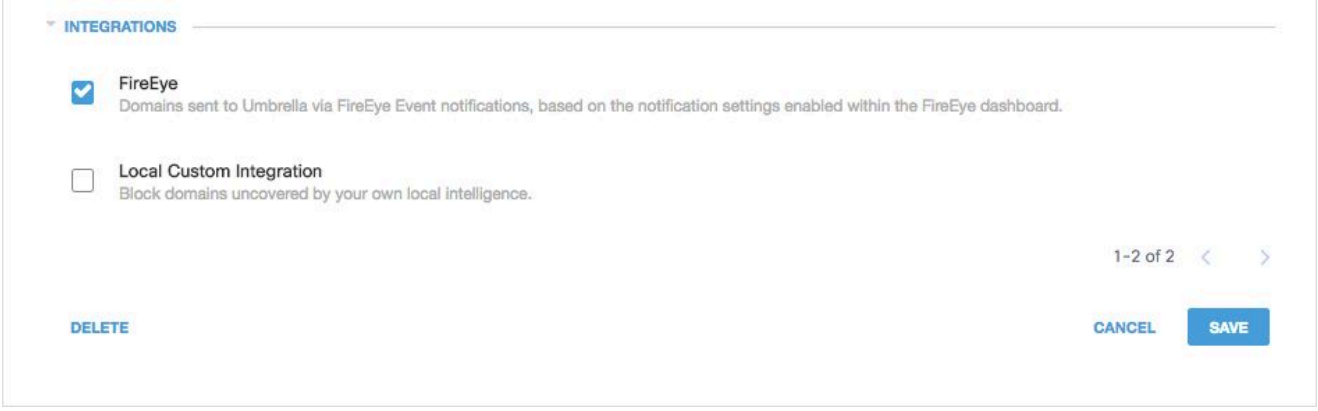
Étape facultative : Répertorier ou supprimer des domaines

Vous pouvez également effectuer un test pour vous assurer que vous êtes en mesure d'énumérer les domaines dans votre intégration personnalisée et de supprimer les domaines au cas où vous ne souhaiteriez plus appliquer contre le domaine ou l'avoir dans votre intégration. Suivez les étapes décrites dans la documentation de l'API pour répertorier et supprimer des domaines.

Configuration des paramètres de sécurité

Maintenant que vous avez validé que vous pouvez injecter des événements (et éventuellement lister et supprimer des domaines), vous pouvez configurer ce que vous voulez qu'il advienne aux requêtes DNS de vos identités qui sont destinées à des domaines dans la catégorie de sécurité de votre intégration personnalisée.

1. Accédez à Policies > Security Settings et sous Integrations, vérifiez votre intégration activée (dans cet exemple, FireEye) et cliquez sur Save.

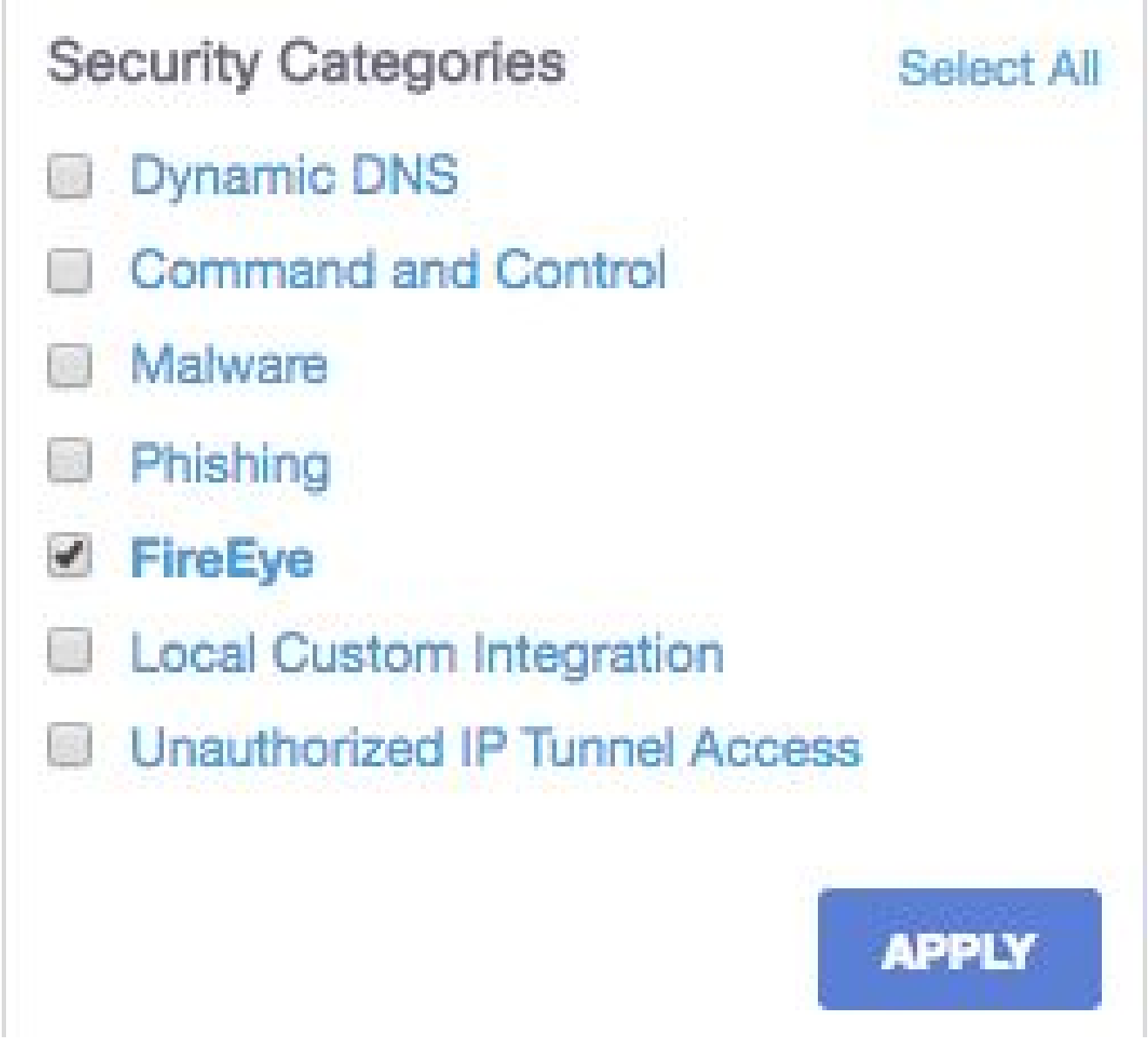


115014145103

Afficher les rapports pour votre intégration personnalisée

Générez des requêtes DNS à partir de l'une de vos identités (par exemple, Réseaux ou Ordinateurs itinérants) destinées au domaine dans votre intégration personnalisée (« creditcards.com » dans notre exemple). Du point de vue du client, vous voyez maintenant le résultat de blocage ou d'autorisation approprié selon la façon dont vous avez configuré vos paramètres de sécurité.

1. Accédez à Reporting > Activity Search et sous Security Categories sélectionnez votre intégration personnalisée (dans cet exemple FireEye) pour filtrer le rapport afin d'afficher uniquement la catégorie de sécurité pour FireEye.

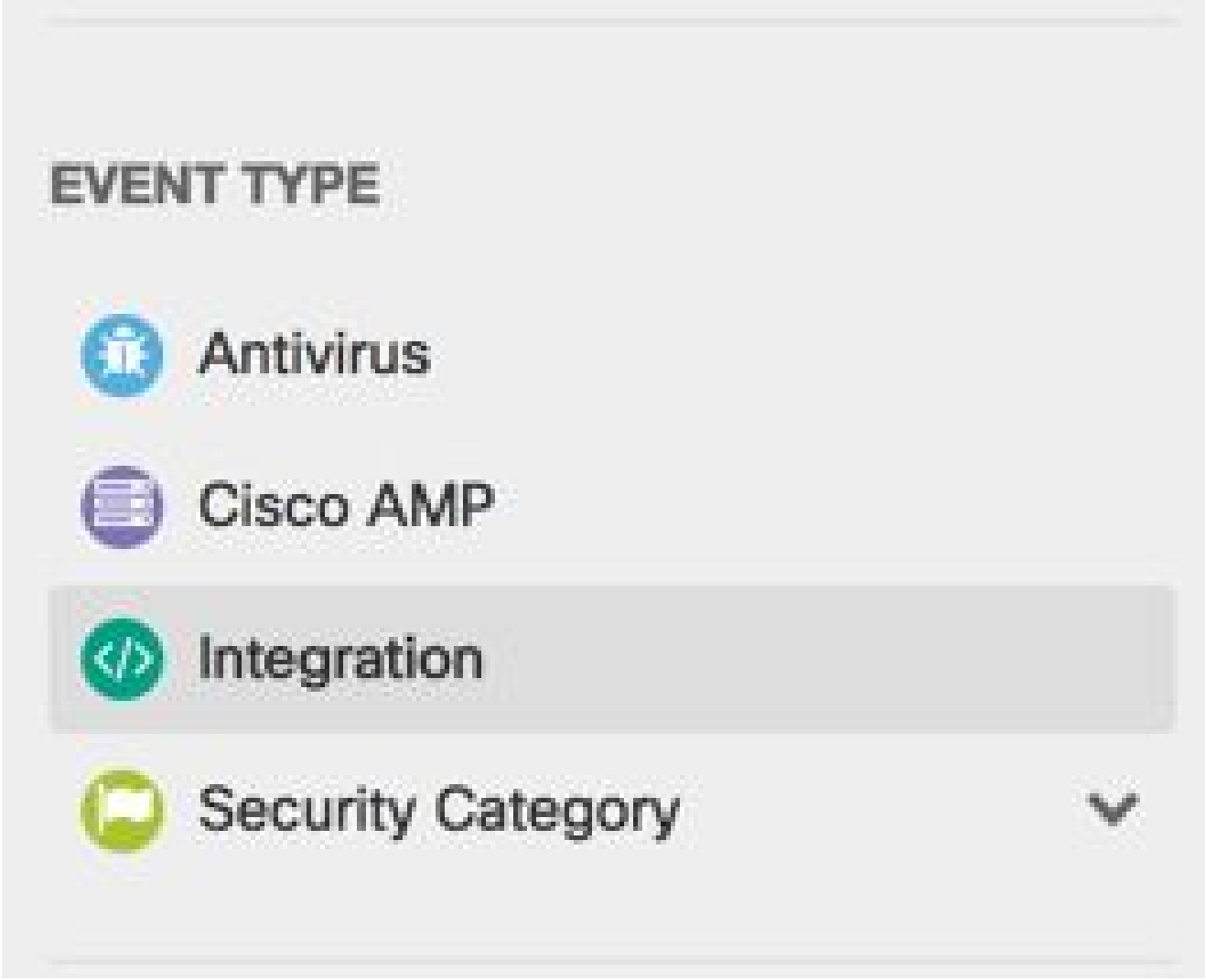


115013981706

2. Cliquez sur Apply pour voir l'activité pour la période sélectionnée dans le rapport.

Vous pouvez également afficher le rapport Volume d'activité pour voir les rapports de capture instantanée ou de tendance au fil du temps, y compris vos intégrations personnalisées.

1. Accédez à Reporting > Security Activity Volume.
2. Sous Event Type, sélectionnez Integration.



115013982286

Configurer votre intégration S3 pour le stockage et la consommation des journaux (facultatif)

Si vous souhaitez ensuite réinjecter vos journaux Umbrella contenant toutes les requêtes pour votre environnement dans votre environnement SIEM/TIP, vous pouvez le faire en utilisant notre intégration S3, qui vous permet de diffuser vos événements d'activité DNS en retour.

Annexe : Exemples de scripts

Ces scripts Perl fournissent des conseils sur la façon de générer un événement pour votre intégration personnalisée. Remplacez la valeur customerKey de votre intégration dans les deux scripts. Notez que ces scripts sont fournis à titre d'exemples et qu'une personnalisation ou des mises à jour peuvent être nécessaires.

generate_event.pl :

```
#!/usr/bin/perl -w

# Custom integration - ADD EVENT URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/events?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $json_blob = "{
    \"alertTime\" : \"2013-02-08T11:14:26.0Z\",
    \"deviceId\" : \"ba6a59f4-e692-4724-ba36-c28132c761de\",
    \"deviceVersion\" : \"13.7a\",
    \"dstDomain\" : \"$domain\",
    \"dstUrl\" : \"http://$domain/a-bad-url\",
    \"eventTime\" : \"2013-02-08T09:30:26.0Z\",
    \"protocolVersion\" : \"1.0a\",
    \"providerName\" : \"Security Platform\"
}";

my $curl_request = "curl '" . $cust_key . "' -v -X POST -H 'Content-Type: application/json' -d '" . $js

my $results = exec($curl_request);
```

delete_domain.pl :

```
#!/usr/bin/perl -w

# Custom integration - DELETE URL

my $cust_key = 'https://s-platform.api.opendns.com/1.0/domains?customerKey=XXXXXXXX-XXXX-XXXX-XXXX-XXXX

die "Usage: $0 - Please supply a domain\n" if @ARGV < 1;
my $domain = $ARGV[0];

my $curl_request = "curl '" . $cust_key . "&where[name]=" . $domain . "' -v -i -g -X DELETE -H 'Content
my $results = exec($curl_request);
```

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.