Configurer l'appliance Secure Malware Analytics avec Umbrella

Table des matières

Introduction

Ce document décrit comment configurer et dépanner les intégrations tierces prises en charge avec l'appliance Secure Malware Analytics (anciennement Threat Grid).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Analyse des programmes malveillants sécurisés Cisco
- Cisco Umbrella

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

- Umbrella
- Appliance Secure Malware Analytics

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.

Informations générales

Afin de fournir des informations analytiques supplémentaires d'un échantillon soumis, telles que le score de risque Umbrella, l'appliance Malware Analytics s'intègre à Umbrella via la clé API.

Configuration

> Conseil : dans les opérations de cluster TGA, chaque noeud TGA est configuré individuellement. Si vous ne configurez pas chaque noeud TGA, les résultats peuvent être incohérents.

> Remarque : la source des intégrations provient de l'interface sale de l'appliance ; l'interface sale doit être connectée et l'accès sortant doit être autorisé pour que le fonctionnement soit correct.

Étape 1. Connectez-vous à votre tableau de bord Umbrella et cliquez sur Admin > Licensing dans le menu de navigation de gauche. Votre type de package actuel s'affiche.

Étape 2. Assurez-vous que vous disposez d'une licence SIG https://umbrella.cisco.com/products/umbrella-enterprise-security-packages

Étape 3. Dans votre tableau de bord Umbrella, cliquez sur Investigate > API keys > copy API Access Tokens

Étape 4. Connectez-vous à l'interface Opadmin (Admin) de Malware Analytics Appliance.

Étape 5. Accédez à Configuration > Integrations.

Étape 6. Configurez la TGA avec les jetons d'accès à l'API.

Une fois configuré, cliquez sur Save, puis sur reconfigure.

Étape 7. Utiliser la fonction RASH sur l'appliance client pour effectuer

systemctl —no-block restart tg-supervisor

Étape 8. Testez que votre licence dispose du niveau API approprié :

curl —include —request POST —header "Autorisation : Bearer 12345678910" —data-binary "["cnn.com"]" https://investigate.api.umbrella.com/domains/categorization

> Remarque : vous devez contacter le gestionnaire de compte du client pour obtenir la mise à niveau de licence.
> L'action souhaitée n'a pas pu être effectuée car la licence de niveau 1 n'a pas accès aux terminaux en bloc. Cela nécessite une mise à niveau de licence vers un accès de niveau 2 ou 3.

Étape 1. Soumettez un échantillon d'URL pour analyse.

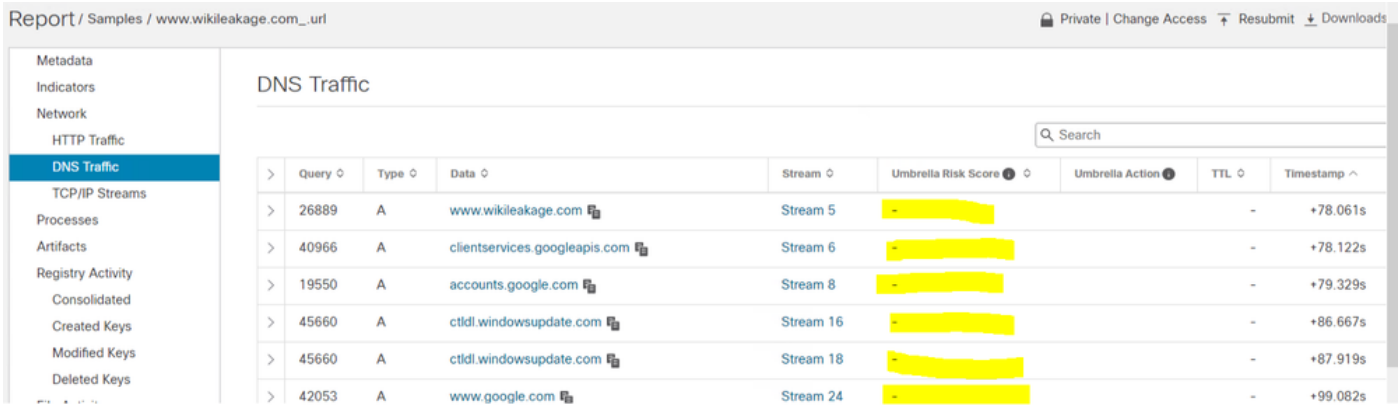
Étape 2. Une fois l'exemple terminé, affichez la fenêtre Samples>DNS traffic .

Étape 3. Accédez à Score des risques parapluie.

Dépannage

1. Le score de risque global n'est pas présenté dans l'exemple d'appliance Malware Analytics sous le trafic DNS

Assurez-vous de ne pas obtenir l'erreur HTTP 403 à l'étape 8. Testez que votre licence dispose du niveau API approprié.

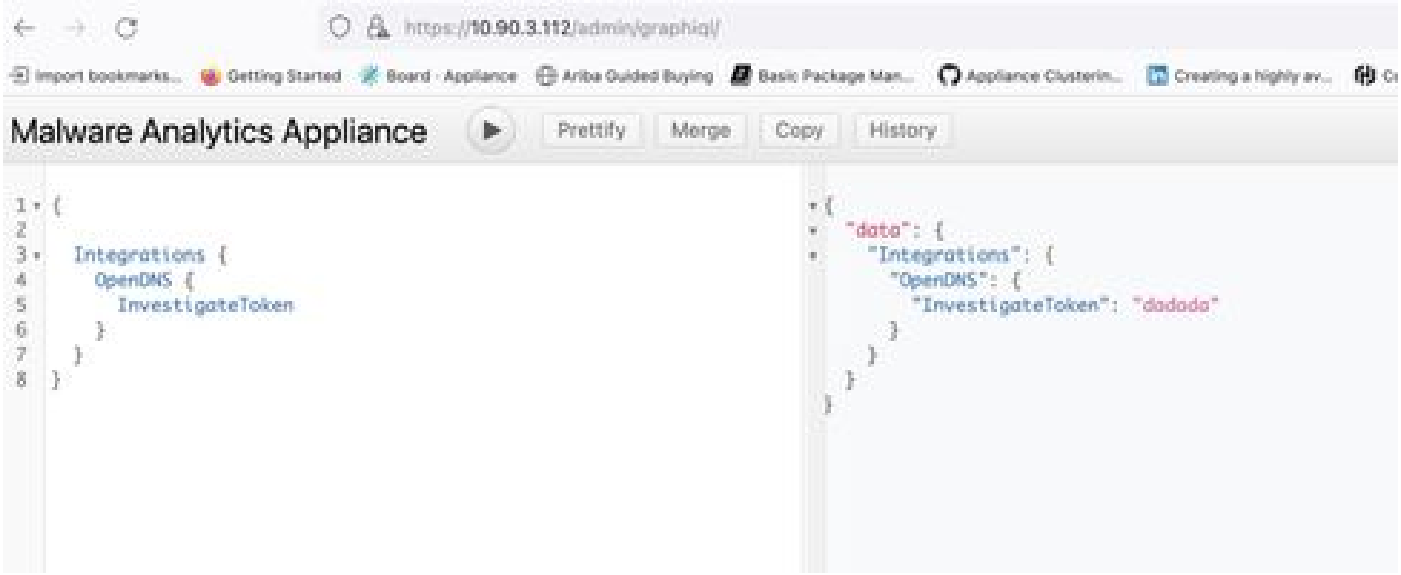


Pour résoudre ce problème, les clients doivent contacter le spécialiste de la sécurité et l'équipe chargée du compte pour mettre à niveau leurs licences Umbrella. Il n'est pas du devoir ou de la responsabilité de GATE d'aider avec licence Umbrella.

2. Le jeton Umbrella n'est pas enregistré dans l'appliance Malware Analytics

Afin de vérifier que le jeton API Umbrella est correctement codé en dur dans l'Appliance, vous pouvez utiliser graphiql pour interroger le fichier de configuration. La réponse doit être le jeton API Umbrella correct obtenu à partir du tableau de bord Umbrella.

> Conseil : Remplacez <IP> par le nom d'hôte correspondant de la TGA, Effacez les valeurs par défaut et tapez exactement ce qui est sur l'écran de gauche, puis appuyez sur le bouton Lire.


https://10.90.3.112/admin/graphiql/
Import bookmarks...
Getting Started
Board · Appliance
Ariba Guided Buying
Basic Package Man...
Appliance Clusterin...
Creating a highly av...
Malware Analytics Appliance
Prettify
Merge
Copy
History
{
Integrations {
OpenDNS {
InvestigateToken
}
}
}
{
"data": {
"Integrations": {
"OpenDNS": {
"InvestigateToken": "dadada"
}
}
}
}

graphiql

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.