Afficher les notes de verdict d'analyse d'image dans mail_logs sur ESA

Table des matières

Introduction

Aperçu

- Types de fichiers pris en charge

Conditions préalables

Limites

Afficher le score du verdict d'un message particulier

- Procédure
- Résultats attendus

Informations connexes

Introduction

Ce document décrit comment afficher le score du verdict d'analyse d'image pour un message sur un ESA exécutant AsyncOS pour la sécurité de la messagerie.

Aperçu

ESA est l'acronyme de Cisco Email Security Appliance. L'analyse d'images nécessite une licence pour pouvoir être activée. Certains messages contiennent des images qu'une entreprise peut analyser à la recherche de contenu inapproprié. L'analyse d'images n'est pas conçue pour compléter ou remplacer les moteurs d'analyse antivirus et antispam. Son objectif est d'imposer une utilisation acceptable en identifiant le contenu inapproprié dans les e-mails.

Après avoir configuré Cisco AsyncOS pour la sécurité de la messagerie pour l'analyse d'images, utilisez les règles de filtre d'analyse d'images pour effectuer des actions sur les e-mails suspects ou inappropriés.

Types de fichiers pris en charge

Image Analysis peut analyser les types de fichiers image joints :

- BMP
- GIF
- OIC
- JPEG
- PCX

- PNG
- TGA
- QUERELLE

L'analyseur d'image utilise des algorithmes qui mesurent la couleur de la peau, la taille du corps et la courbure pour déterminer la probabilité qu'un graphique contienne un contenu inapproprié. Lors de la numérisation de pièces jointes d'image, les empreintes Cisco déterminent le type de fichier et l'analyseur d'image évalue le contenu de l'image. Si une image est incorporée dans un autre fichier, le moteur de numérisation Stellent extrait l'image (par exemple, à partir de documents Word, Excel et PowerPoint). Le verdict d'analyse d'image est calculé pour le message dans son ensemble. Si un message ne contient pas d'image, l'analyse d'image attribue une note de 0 (Nettoyage).

 Remarque : Les images ne peuvent pas être extraites des fichiers PDF.

Conditions préalables

- Licence Image Analysis installée.
- Analyse d'images activée dans Cisco AsyncOS pour la sécurité de la messagerie (AsyncOS).
- Accès à mail_logs (CLI ou GUI) et à l'ID de message (MID) du message à examiner.

Limites

- Le verdict est calculé pour l'ensemble du message ; Les journaux de messagerie signalent les résultats par pièce jointe (par exemple, une pièce jointe ZIP affiche le nom du fichier ZIP et le score maximal d'images qu'il contient).
- Les images ne peuvent pas être extraites des fichiers PDF.

Afficher le score du verdict d'un message particulier

Procédure

1. Identifiez l'ID (MID) du message.
2. Accédez à mail_logs (à partir de l'interface utilisateur graphique ou de l'interface de ligne de commande, selon le déploiement).
3. Recherchez les entrées de journal qui incluent le MID et l'analyse d'image.
4. Notez le nom et le score de la pièce jointe, et si celle-ci est marquée comme non analysable.
5. Vérifiez les lignes de journal suivantes pour l'action effectuée (par exemple, l'action de règle de filtre, la quarantaine ou la suppression).

Résultats attendus

Les entrées du journal indiquent le nom de la pièce jointe, le score de l'analyse d'image et si la

pièce jointe était analysable ou non. Les journaux ne mappent pas directement les scores aux étiquettes de verdict.

Cet exemple montre les entrées liées à l'analyse d'image dans mail_logs :

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
 is unscannable.
Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
 'Unscannable.jpg' score 0 unscannable
Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
 drop-attachments-where-image-verdict filter 'f-001'
Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

Informations connexes

- Guide d'utilisation du courrier électronique AsyncOS
- Coordonnées du service d’assistance Cisco à l’échelle mondiale
- Assistance technique et documentation produit

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.