Dépannage des erreurs de classification et d'analyse pour DLP

Table des matières

Introduction

Informations importantes

Exemples de journal des violations et d'absence de violation

Liste de vérification du dépannage

- Confirmer la version du moteur DLP
- Activer la consignation du contenu correspondant
  - Exemple De Journalisation Du Contenu Correspondant Dans Le Suivi Des Messages
- Vérifier La Configuration Du Comportement D'Analyse
- Revoir La Configuration De L'Échelle De Gravité
- Vérifiez Les Adresses E-Mail Ajoutées Aux Champs Filtrer Les Expéditeurs Et Les Destinataires

Informations connexes

Introduction

Ce document décrit les méthodes courantes de dépannage des erreurs de classification et d'analyse (ou des échecs) liées à DLP sur le ESA.

Informations importantes

Il est essentiel de noter que la prévention contre la perte de données (DLP) sur l'appareil de sécurité de la messagerie électronique Cisco (ESA) est plug-and-play dans le sens où vous pouvez l'activer, créer une stratégie et commencer à rechercher les données sensibles ; cependant, vous devez également être conscient que les meilleurs résultats ne sont obtenus qu'après avoir ajusté DLP pour répondre aux exigences spécifiques de votre entreprise. Cela inclut des éléments tels que les types de stratégies DLP, les détails de correspondance de stratégie, la façon d'ajuster l'échelle de gravité, les filtres et les personnalisations supplémentaires.

Exemples de journal des violations et d'absence de violation

Voici quelques exemples de violations DLP que vous pouvez voir dans les journaux de messagerie et/ou le suivi des messages. La connexion inclut l'horodatage, le niveau de

journalisation, le numéro MID, la violation ou l'absence de violation, la gravité et le facteur de risque, ainsi que la stratégie qui a été mise en correspondance.

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP policy m
```

```
Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy match:
```

Lorsqu'aucune violation n'est détectée, les journaux de messagerie et/ou le suivi des messages consignent simplement DLP no violation.

```
Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation
```

Liste de vérification du dépannage

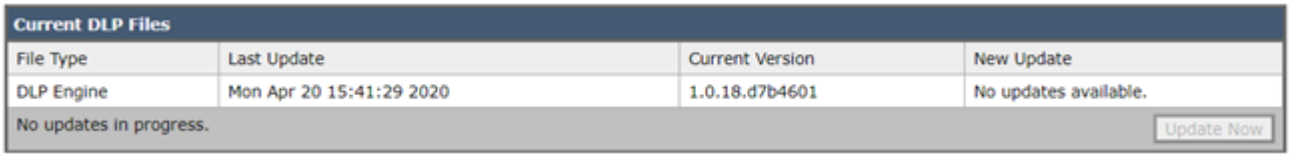
Vous trouverez ci-dessous des éléments courants qui peuvent être révisés lorsque vous traitez de mauvaises classifications DLP ou d'échecs/échecs d'analyse.

Remarque : Cette liste n'est pas exhaustive. Veuillez contacter le centre d'assistance technique de Cisco si vous souhaitez voir un article inclus.

Confirmer la version du moteur DLP

Les mises à jour du moteur DLP ne sont pas automatiques par défaut, il est donc essentiel de vous assurer que vous exécutez la dernière version qui inclut toutes les améliorations récentes ou les corrections de bogues.

Vous pouvez naviguer jusqu'à Prévention de perte de données sous Services de sécurité dans l'interface utilisateur graphique pour confirmer la version actuelle du moteur et pour voir si des mises à jour sont disponibles. Si une mise à jour est disponible, vous pouvez cliquer sur Mettre à jour maintenant pour effectuer la mise à jour.

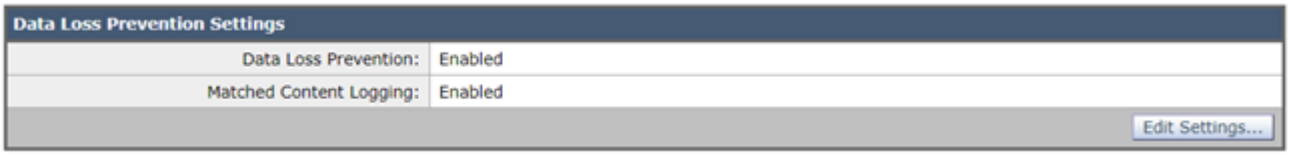


Activer la consignation du contenu correspondant

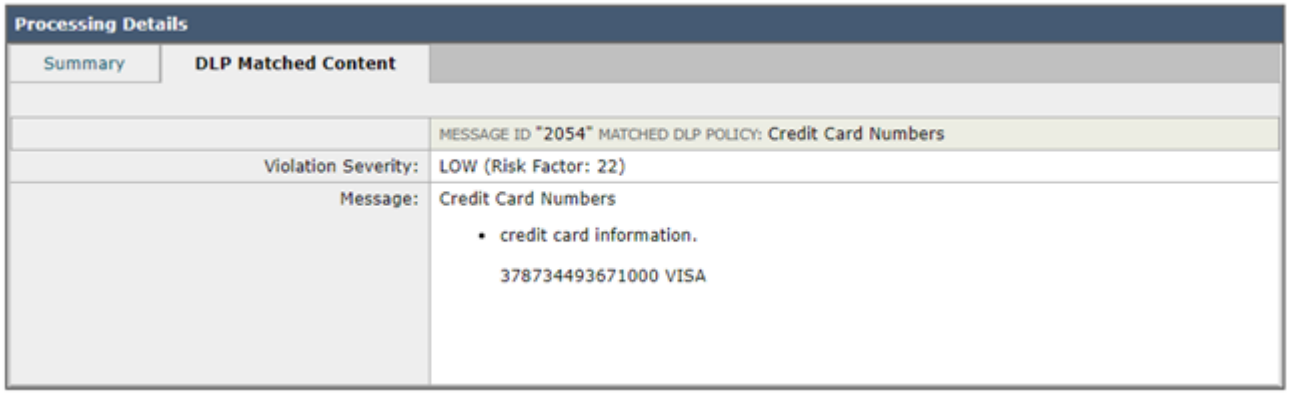
DLP offre la possibilité de consigner le contenu qui ne respecte pas vos stratégies DLP. Ces données peuvent ensuite être affichées dans Suivi des messages pour aider à déterminer le contenu d'un e-mail qui pourrait causer une violation particulière.

⚠ Mise en garde : Il est important de savoir que si ce contenu est activé, il peut inclure des données sensibles telles que des numéros de carte de crédit et de sécurité sociale, et bien plus encore.

Vous pouvez naviguer jusqu'à Prévention de perte de données sous Services de sécurité dans l'interface utilisateur graphique pour voir si la consignation du contenu correspondant est activée.



Exemple De Journalisation Du Contenu Correspondant Dans Le Suivi Des Messages



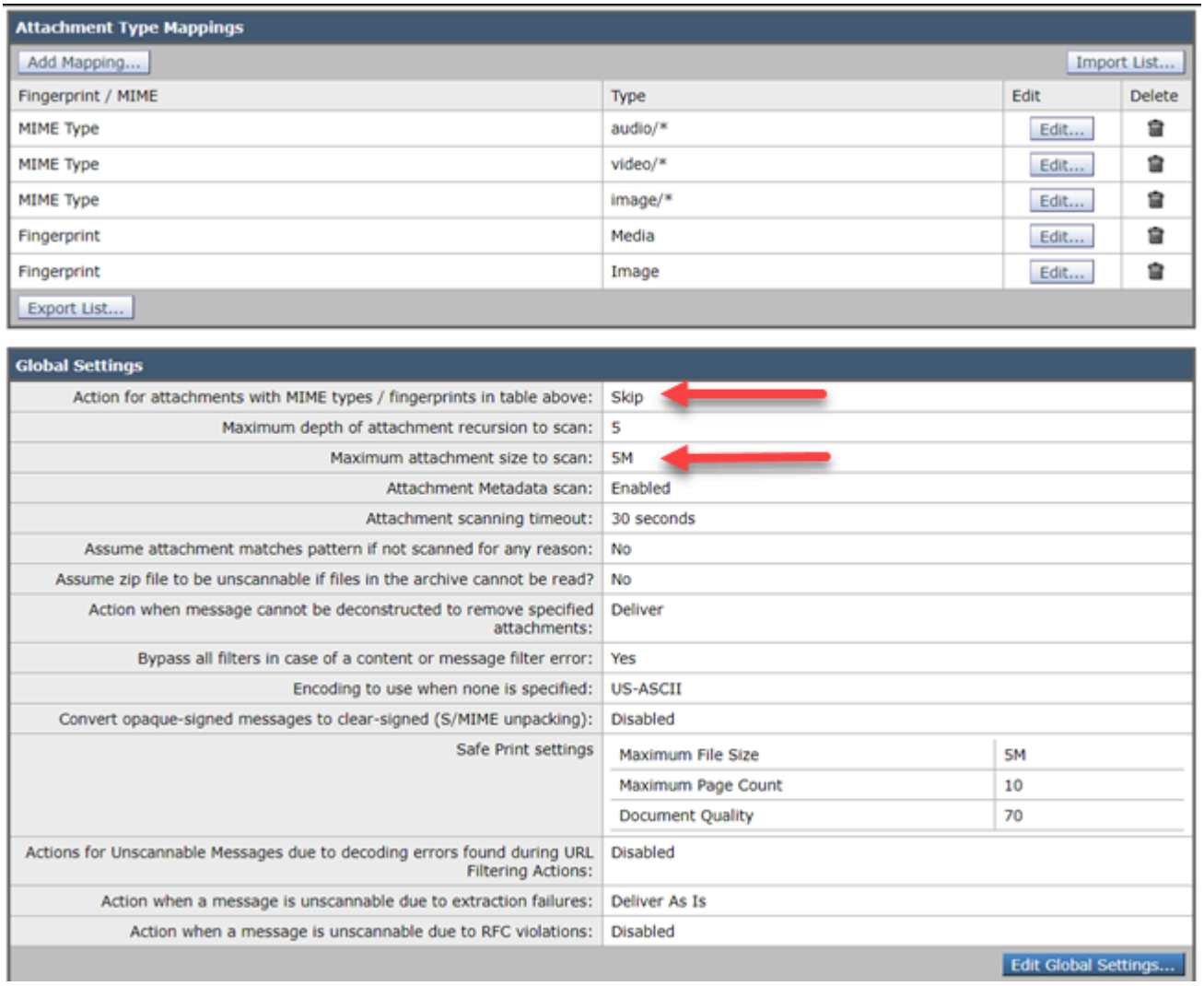
Vérifier La Configuration Du Comportement D'Analyse

La configuration du comportement d'analyse sur l'ESA a également un impact sur la fonctionnalité derrière DLP. Si vous vous référez à l'image ici à titre d'exemple, qui a une taille maximale de

numérisation de pièce jointe configurée de 5 M, tout ce qui est plus grand peut provoquer des balayages DLP manqués. En outre, l'action pour les pièces jointes avec le paramètre de types MIME est un autre élément courant que vous voulez revoir. Cette valeur doit être définie sur la valeur par défaut de Skip afin que les types MIME répertoriés soient ignorés et que tous les autres soient analysés. Si elle est définie sur Scan (Analyser), l'ESA analyse uniquement les types MIME répertoriés dans le tableau.

De même, d'autres paramètres répertoriés ici peuvent avoir un impact sur les analyses DLP et doivent être pris en compte en ce qui concerne le contenu des pièces jointes/e-mails.

Vous pouvez naviguer jusqu'à Comportement d'analyse sous Services de sécurité dans l'interface graphique utilisateur, ou à partir de la commande scanconfig dans l'interface de ligne de commande.



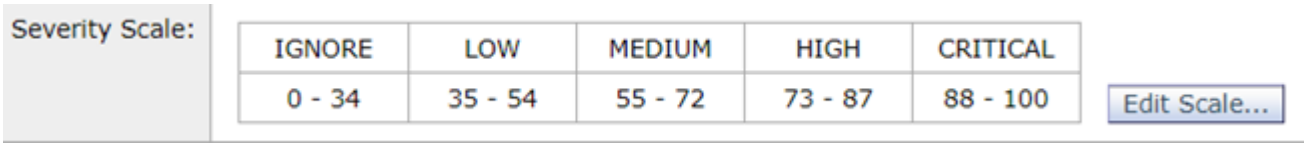
Revoir La Configuration De L'Échelle De Gravité

Les seuils d'échelle de gravité par défaut sont suffisants pour la plupart des environnements ;

toutefois, si vous devez les modifier pour faciliter les correspondances Faux négatif (FN) ou Faux positif (FP), vous pouvez le faire. Vous pouvez également créer une stratégie fictive et la comparer pour vérifier si votre stratégie DLP utilise les seuils par défaut recommandés.

Remarque : les différentes politiques prédéfinies (telles que HIPAA américain et PCI-DSS) ont des échelles différentes

---



Vérifiez Les Adresses E-Mail Ajoutées Aux Champs Filtrer Les Expéditeurs Et Les Destinataires

Vérifiez que toutes les entrées saisies dans l'un de ces champs correspondent à la casse correcte des adresses e-mail de l'expéditeur et/ou du destinataire. Le champ Filtrer les expéditeurs et les destinataires est sensible à la casse. La stratégie DLP ne se déclenche pas si l'adresse e-mail ressemble à "TestEmail@mail.com" dans le client de messagerie et est entrée comme "testemail@mail.com" dans ces champs.



Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final
- En quoi consiste la prévention des pertes de données ?
- Déclencher une violation DLP pour tester une politique HIPAA sur ESA

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.