Installez une stratégie DLP de coutume pour détecter les numéros de sécurité sociale formatés et non formatés

Contenu

Introduction

Ce document décrit comment installer une stratégie DLP de coutume pour détecter les numéros de sécurité sociale formatés et non formatés (SSN) sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Installez une stratégie DLP de coutume pour détecter les numéros de sécurité sociale formatés et non formatés

Par conception l'engine de lecture DLP détecte seulement les numéros de sécurité sociale formatés. C'est dû au haut niveau des faux positifs provoqués par les nombres 9-digit contenus dans les données utilisées par de divers secteurs. Par exemple, la banque aba conduisant des nombres sont 9-digits et déclencheraient en balayant pour un numéro de sécurité sociale non formaté. Comme tel il est recommandé pour éviter de balayer pour les numéros de sécurité sociale non formatés à moins que strictement requis par votre organisation. Si on l'exige que votre organisation balaye pour les numéros de sécurité sociale non formatés, vous pouvez créer une stratégie DLP de coutume en suivant les étapes fournies dans la solution ci-dessous.

AsyncOS fournit l'option de créer votre propre à partir de zéro de stratégie utilisant des classificateurs développés par RSA ou votre organisation. Cette option est considérée avancée et devrait être utilisée seulement dans les rares cas quand les modèles de stratégie de prédéfinis ne répondent pas aux propres exigences de votre environnement de réseau.

Créez une stratégie faite sur commande

1. Àpartir de la GUI : **Stratégies de messagerie > Policy Manager DLP**.
2. Cliquez sur le bouton de **stratégie DLP d'ajouter…**.
3. **La stratégie faite sur commande** choisie au bas de l'écran et cliquent sur Add **à côté de la stratégie faite sur commande.**
4. Écrivez un nom de stratégie DLP. Exemple : *Stratégie faite sur commande SSN*.

Créez un classificateur

La création des classificateurs faits sur commande te donne la grande flexibilité au-dessus des critères balayés dans l'engine DLP. Nous emploierons ceci à notre avantage pour balayer pour SSN formaté et SSN non formaté.

1. Du déroulant assorti satisfait de classificateur, choisi **créez un classificateur** et cliquez sur le bouton d'**ajouter**.
2. Écrivez un nom assorti satisfait de classificateur. Exemple : *SSN tous les formats.*
3. Selon les règles sectionnez, placez la baisse vers le bas des mots ou expression à l'**entité**.
4. Sélectionnez l'entité : **Numéro de sécurité sociale des USA, formaté**.
5. Cliquez sur Add la **règle**.
6. **Entité** de nouveau choisie.
7. Sélectionnez l'entité : **Numéro de sécurité sociale des USA, non formaté**.
8. Cliquez sur **Submit**.

Placez les configurations de sévérité

Les configurations suivantes sont un bon point commençant, toutefois elles sont simplement une instruction pour vous aider et peuvent exiger quelques paramètres de configuration d'étalonnage ou de remplaçant basés sur vos besoins d'organismes.

- **Configurations essentielles de sévérité**
  Action appliquée aux messages : **Quarantaine**
  Cryptage d'enable (vérifié)
  Règle de cryptage : **Toujours cryptage de message d'utilisation**
  Profil de cryptage (sélectionnez votre profil configuré de cryptage du déroulant)
  Objet de message crypté : **$subject**
- **Configurations de à sévérité élevée**
  Action appliquée aux messages : **Livrez**
  Cryptage d'enable (vérifié)
  Règle de cryptage : **Toujours cryptage de message d'utilisation**
  Profil de cryptage (sélectionnez votre profil configuré de cryptage du déroulant)
  Objet de message crypté : **$subject**
- **Configurations moyennes de sévérité**
  Action appliquée aux messages : *Livrez*
  Cryptage d'enable (vérifié)
  Règle de cryptage : **Seulement cryptage de message d'utilisation si le TLS échoue**
  Profil de cryptage (sélectionnez votre profil configuré de cryptage du déroulant)

Objet de message crypté : **$subject**

- **Basses configurations de sévérité**
  Action appliquée aux messages : **Livrez**
  Cryptage d'enable (décoché)

Placez l'échelle de sévérité

De nouveau, les configurations suivantes sont un bon point commençant, toutefois elles sont simplement une instruction pour vous aider et peuvent exiger quelques paramètres de configuration d'étalonnage ou de remplaçant basés sur vos besoins d'organismes.

1. Àla droite du diagramme d'échelle de sévérité, cliquez sur Edit l'**échelle**.
2. Glissez le premier traitement jusqu'à IGNORENT = 0.
3. Glissez le deuxième traitement jusqu'au BAS = 1 à 9.
4. Glissez le troisième traitement jusqu'au SUPPORT = 10 à 50.
5. Glissez le quatrième traitement jusqu'à la HAUTE = 60 à 89.
6. Si vous avez placé ceci correctement, ESSENTIEL automatiquement sera placé 90 à 100.
7. Clic **fait** une fois terminé.

Soumettez et commettez les modifications

Pour mener la création à bonne fin de cette stratégie, cliquez sur le bouton de **soumission**. Cliquez sur les **modifications de validation** se boutonnent dans l'angle supérieur droit du GUI. Vous serez porté à l'écran non engagé de modifications, des **modifications de validation de** clic. Vous devriez ne voir **aucune modification en suspens** dans l'angle supérieur droit du GUI si réussi.

Dernières étapes

Vous devrez maintenant activer la stratégie DLP sur une stratégie de mail sortant dans le cadre des **stratégies de messagerie de Policies->Outgoing de messagerie**. Pour tester en dehors de la production que vous pouvez créer une stratégie sortante faite sur commande avec vous-même a indiqué comme expéditeur et active la stratégie DLP sur cette stratégie de test.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems