Comment configurer une stratégie DLP de messagerie dans Cisco Secure Access (SA) et Cisco Email Threat Defense (ETD)

Table des matières

Introduction

Les e-mails restent l'un des canaux les plus courants d'exposition non intentionnelle ou non autorisée des données. Pour aider les entreprises à protéger les informations sensibles partagées par e-mail, Cisco propose des fonctionnalités DLP (Email Data Loss Prevention) grâce à l'intégration de Cisco Secure Access (SA) et de Cisco Email Threat Defense (ETD).

Dans cette architecture, toutes les actions de création, de configuration et d'application des stratégies DLP de messagerie sont effectuées dans Cisco Secure Access. Cisco Email Threat Defense offre une visibilité sur les e-mails et un suivi des messages, tandis que Cisco Secure Access sert de moteur de stratégie pour définir les règles DLP et le comportement d'application.

Cet article explique comment créer une stratégie DLP de messagerie dans Cisco Secure Access, à l'aide d'un modèle DLP prédéfini ou d'un modèle DLP personnalisé.

Conditions préalables

Avant de commencer le processus de configuration, assurez-vous que les conditions suivantes sont remplies :

- Accès administratif : vous devez disposer de privilèges d'administrateur complet pour la console en ligne Cisco Email Threat Defense et la console Cisco Secure Access.
- Abonnements actifs : assurez-vous que vos locataires Email Threat Defense et Secure Access sont actifs et provisionnés.
- Connectivité : l'intégration de l'API entre Email Threat Defense et Secure Access doit être établie.
- Configuration du flux de messagerie : Email Threat Defense doit être correctement déployé en mode Inline pour garantir une inspection active du trafic de messagerie.

Important : Bien que cette solution utilise à la fois Cisco Secure Access et Cisco Email Threat Defense, toutes les étapes de configuration des règles Email DLP décrites dans cet article sont effectuées uniquement dans Cisco Secure Access.

Exigences et composants utilisés

Pour implémenter correctement une stratégie DLP de messagerie, les composants suivants sont utilisés :

- Cisco Email Threat Defense (ETD) : sert de point d'inspection des e-mails. Il capture le trafic

des e-mails sortants et facilite le flux de communication nécessaire au moteur DLP pour effectuer son analyse.
- Cisco Secure Access (SA) : le moteur DLP : il s'agit du composant principal où résident toutes les configurations DLP. Vous utiliserez la console Secure Access pour définir :
    - Identificateurs de données : modèles spécifiques ou types de données sensibles (par exemple, PII, numéros de carte de crédit ou codes de projet internes) que le système doit surveiller.
    - Stratégies DLP : règles qui régissent la manière dont le système doit réagir lorsque des données sensibles sont détectées (par exemple, blocage, chiffrement ou notification).
    - Actions de stratégie : réponses automatisées déclenchées par le moteur DLP, telles que l'interdiction de l'envoi de l'e-mail ou l'application d'un cryptage obligatoire.
- Structure d'intégration : connectivité back-end permettant à ETD de transférer des métadonnées de messagerie électronique au moteur DLP d'accès sécurisé pour l'évaluation des stratégies et leur application ultérieure.

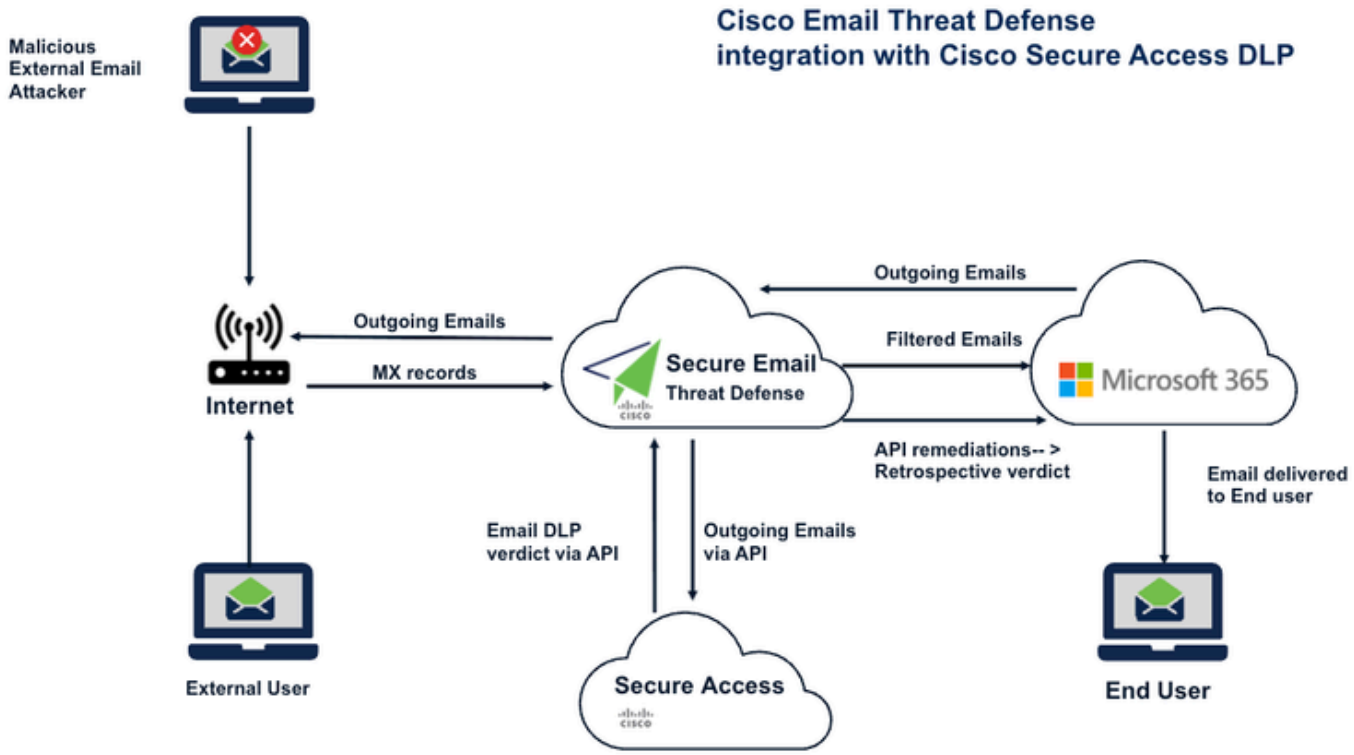
Fonctionnalités de stratégie DLP de messagerie

Lors de la création d'une stratégie DLP de messagerie électronique dans Cisco Secure Access, vous pouvez configurer :

- Nom et description de la règle
- Niveau de gravité
- Classifications de données
- Portée de l'inspection, y compris :
    - Objet du courrier électronique
    - Corps du message
    - Nom de pièce jointe
    - Contenu des pièces jointes
- Contrôles de fichiers, notamment :
    - Étiquettes MIP
    - étiquettes Titus
- Conditions de l'expéditeur
- Conditions du destinataire
- Actions stratégiques :
    - Monitor
    - Block
- Notifications utilisateur facultatives

Diagramme du réseau

Vous trouverez ci-dessous le schéma du réseau illustrant l'intégration de la protection contre les menaces de messagerie électronique sécurisée Cisco avec Cisco Secure Access, ainsi que l'organigramme du trafic.



NOTE: Dans l'image ci-dessus, le serveur Exchange est O365, mais cette configuration DLP peut être effectuée sur n'importe quel serveur Exchange prenant en charge SMTP.

NOTE: Reportez-vous à l'article « Steps to integrated Cisco Email Threat Defense (ETD) with Cisco Secure Access: » (Étapes d'intégration de Cisco Email Threat Defense (ETD) avec Cisco Secure Access :) pour intégrer Cisco Email Threat Defense et Cisco Secure Access via l'API.

Configurer

Configurer une stratégie DLP de messagerie dans Cisco Secure Access

Étape 1: Connectez-vous à Cisco Secure Access

Connectez-vous à la console Cisco Secure Access (SA) à l'aide d'un compte d'administrateur

avec les autorisations requises.

Étape 2: Accédez à Email DLP Rule Creation

Dans le tableau de bord Accès sécurisé, accédez à :

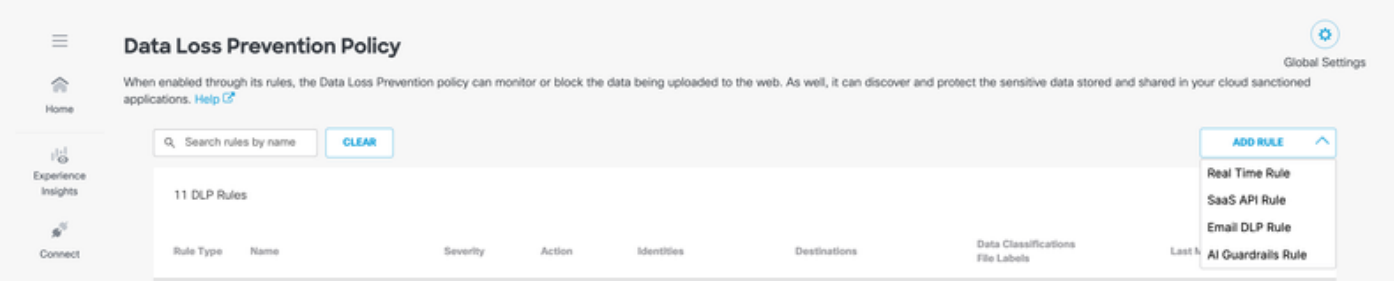
Secure > Policy > Data Loss Prevention Policy > Add Rule > Email DLP Rule

La page Add New Email Rule s'ouvre.

Cisco Secure Access propose deux méthodes pour créer une règle DLP pour les e-mails :

- Créer une règle DLP d'e-mail à l'aide d'un modèle DLP prédéfini
- Créer une règle DLP de messagerie à l'aide d'un modèle DLP personnalisé

Figure 1. Accédez à la création de la règle DLP par e-mail



Option 1: Créer une règle DLP d'e-mail à l'aide d'un modèle DLP prédéfini

Étape 3: Configurer les informations de règle de base

Accédez à la fenêtre ADD RULE > Email DLP Rule,

Dans la fenêtre Ajouter une nouvelle règle d'e-mail, entrez les détails suivants :

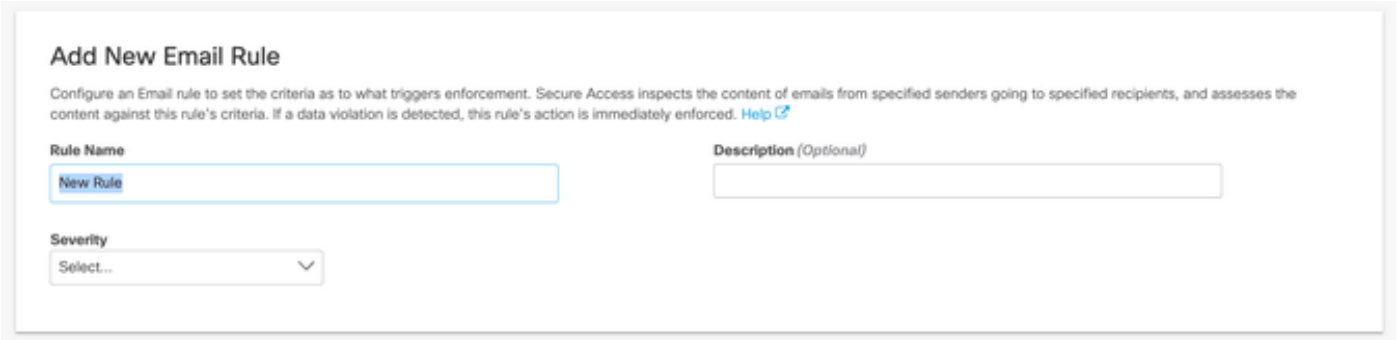
- Nom de règle
  Entrez un nom descriptif pour la règle DLP d'e-mail.

- Description
  Fournissez un bref résumé de l'objectif de la règle.

- Severity (gravité)
  Sélectionnez le niveau de gravité approprié pour la stratégie :

  - Faible
  - Moyen
  - Élevé
  - Critical (critique)

Ces champs permettent de classer les règles d'administration, de création de rapports et de visibilité opérationnelle.



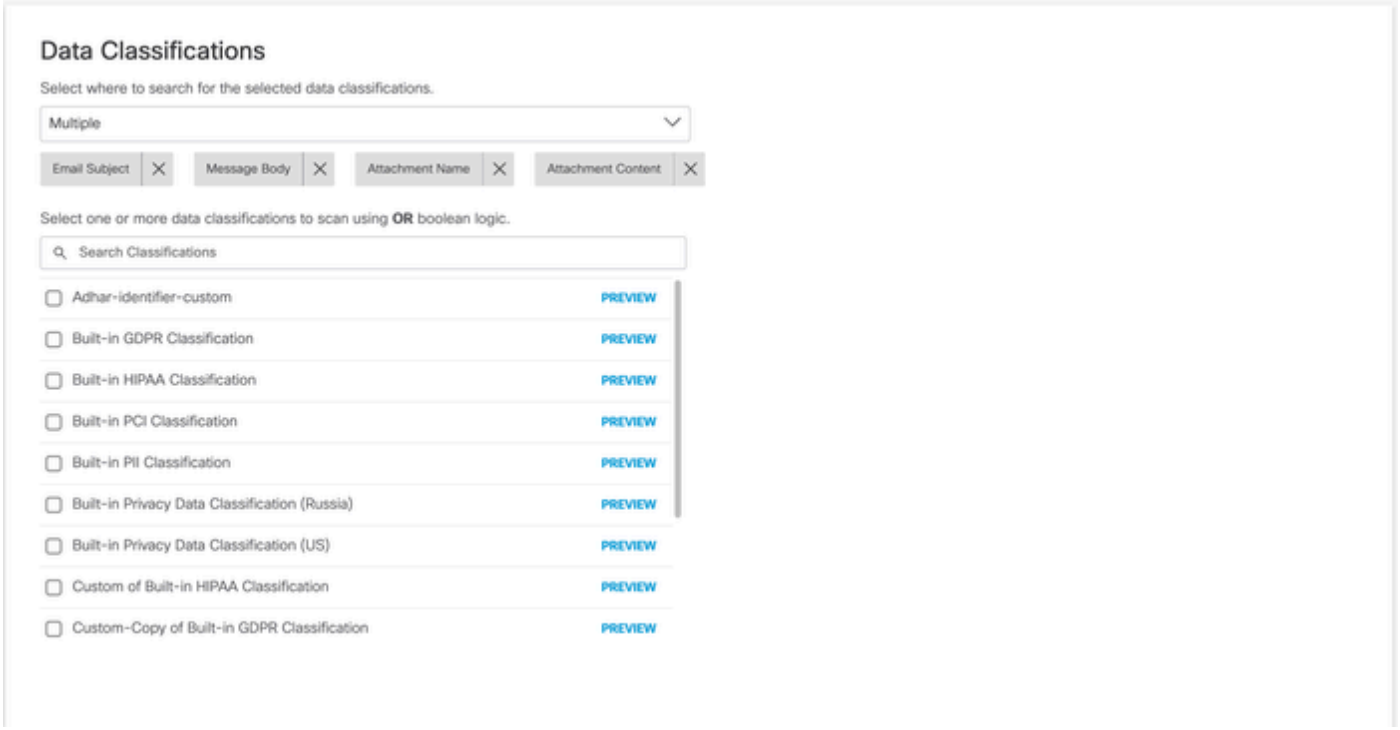
Étape 4: Sélectionner des classifications de données

Sous Data Classifications, sélectionnez le modèle DLP prédéfini qui sera utilisé pour inspecter le contenu des e-mails à la recherche de violations DLP potentielles.

Choisissez ensuite l'emplacement auquel les classifications sélectionnées doivent correspondre. Les sites d'inspection pris en charge incluent :

- Objet du courrier électronique
- Corps du message
- Nom de pièce jointe
- Contenu des pièces jointes

Cela permet à la stratégie d'inspecter à la fois le contenu du message et les pièces jointes à la recherche d'informations sensibles.



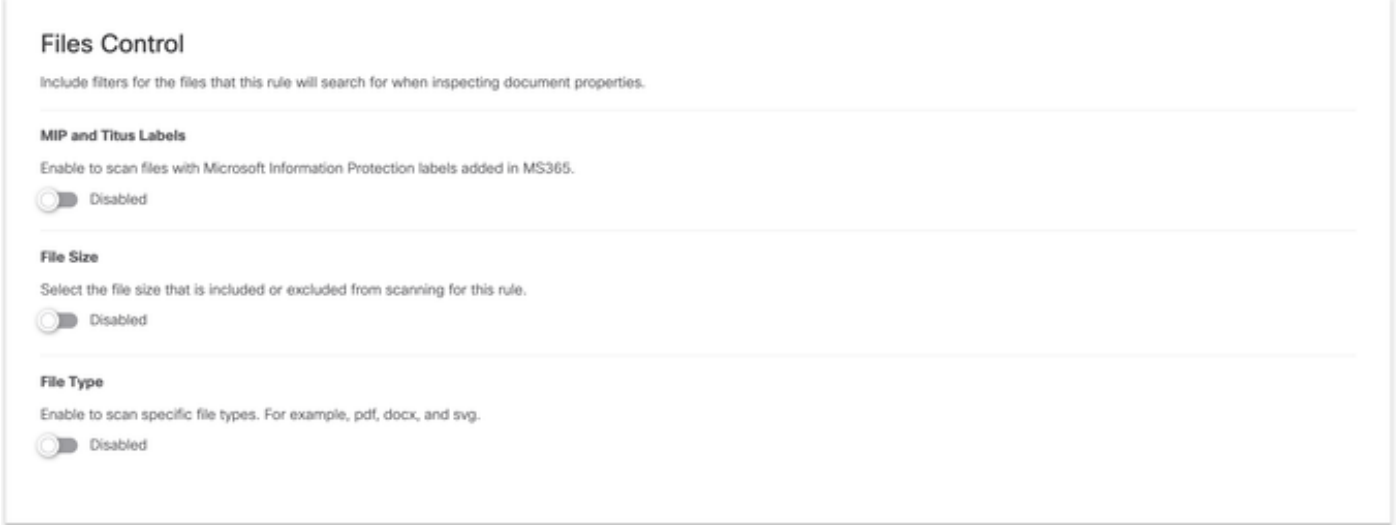
Étape 5: Configurer les contrôles de fichiers

Sous Contrôle des fichiers, configurez les critères d'inspection basés sur des fichiers pour la règle.

Cela inclut la prise en charge de :

- Étiquettes MIP
- étiquettes Titus

Ces paramètres sont utiles lorsque l'application DLP doit prendre en compte les étiquettes de sensibilité ou les métadonnées associées aux fichiers joints.



Étape 6: Définir l'étendue des expéditeurs

Dans la section Expéditeurs, spécifiez les expéditeurs auxquels la stratégie s'applique.

Les options disponibles sont les suivantes :

- Tous les expéditeurs
- Expéditeurs spécifiques
- Exclure des expéditeurs spécifiques

Cela vous permet d'appliquer la règle de manière large ou de la restreindre à des utilisateurs ou des groupes sélectionnés.

Étape 7: Définir l'étendue du destinataire

Dans la section Destinataires, choisissez les utilisateurs ou les groupes qui doivent être inclus ou

exclus de l'évaluation de la stratégie.

Les options disponibles sont les suivantes :

- Inclure tous les utilisateurs
- Inclure des utilisateurs spécifiques
- Exclure des utilisateurs spécifiques

Cela permet d'adapter l'application des stratégies en fonction des destinataires prévus.

Étape 8: Sélectionnez l'action de stratégie

Dans la section Action, choisissez comment Cisco Secure Access doit gérer les e-mails qui sont identifiés comme violant la règle DLP.

Les actions disponibles sont les suivantes :

- Monitor
  L'e-mail est autorisé et l'événement est consigné à des fins de visibilité et de création de rapports.
- Block
  L'e-mail est abandonné pour empêcher la transmission de données sensibles.

Remarque : À l'heure actuelle, les e-mails identifiés positivement peuvent être autorisés via l'action Surveillance ou abandonnés via l'action Bloquer.

Important : Les actions DLP par e-mail ne sont configurées que dans Cisco Secure Access. Si un e-mail est bloqué par l'accès sécurisé, l'événement est également visible dans le suivi des messages Cisco ETD.

Étape 9: Configurer les notifications utilisateur

L'option de notification n'est disponible que pour les destinataires.

Sous Notifications utilisateur, configurez si les utilisateurs doivent être avertis lorsqu'un e-mail correspond à la stratégie DLP.
Il y a une option pour notifier "Actor's Manager" ou un "Custom Recipient". Un « destinataire personnalisé » peut être n'importe qui.

Configurez le modèle de message électronique de Notification par défaut à Notification personnalisée selon vos besoins.

Si cette option est activée, les notifications peuvent aider à sensibiliser les utilisateurs et à réduire les violations répétées des stratégies. Configurez ce paramètre en fonction des exigences opérationnelles et de conformité de votre entreprise.

Étape 9: Configurer les notifications utilisateur

Les notifications aux utilisateurs constituent un outil puissant pour sensibiliser les utilisateurs à la sécurité et garantir la conformité. En alertant les utilisateurs ou les administrateurs lorsqu'un e-mail déclenche une stratégie DLP, vous pouvez immédiatement fournir des commentaires et un contexte sur la violation.

Remarque : Les paramètres de notification sont principalement destinés aux destinataires du courrier électronique et aux parties prenantes désignées.

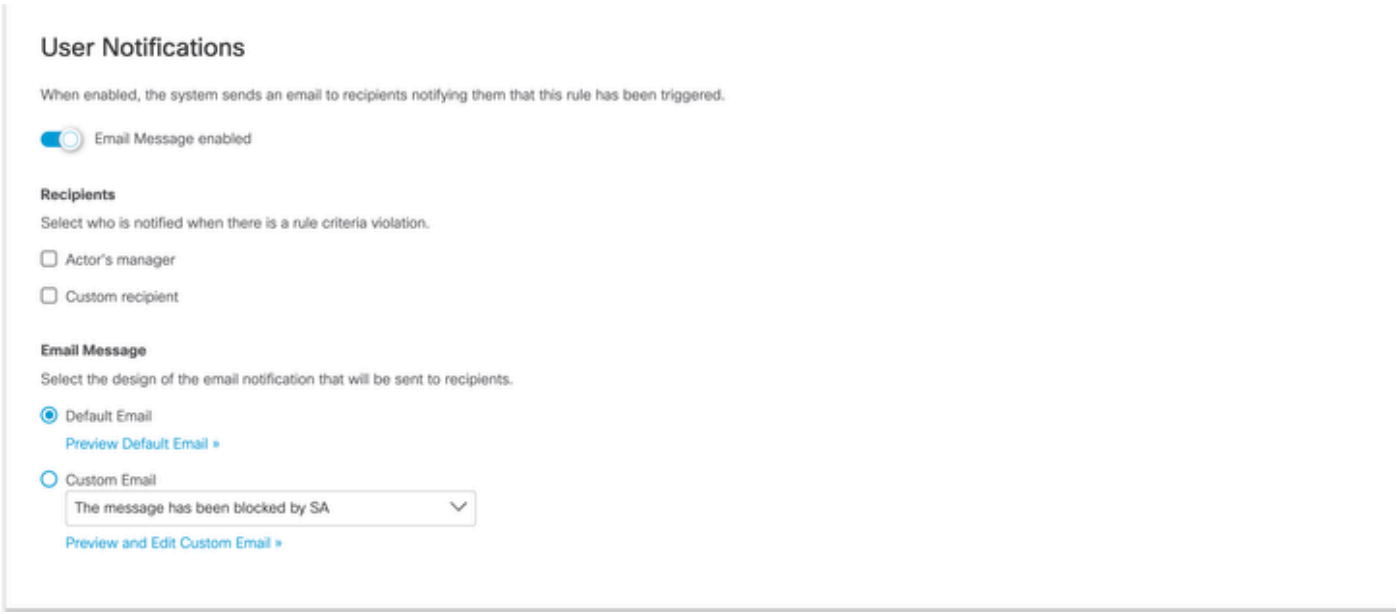
Pour configurer les notifications :

1. Définir les destinataires des notifications : Dans la section Notifications utilisateur, spécifiez qui doit recevoir l'alerte. Vous disposez de deux options principales :
    - Responsable de l'acteur : Envoie la notification directement au responsable de l'utilisateur qui a déclenché la violation de stratégie.

- Destinataire personnalisé : Permet de spécifier n'importe quelle adresse e-mail (par exemple, un centre d'opérations de sécurité ou un responsable de service spécifique).

2. Sélectionner un modèle de message : Vous pouvez choisir entre le modèle de notification par défaut ou une notification personnalisée.
   - Recommandation : Si votre entreprise a des exigences spécifiques en matière de messages de conformité ou de marque interne, utilisez l'option Personnaliser pour personnaliser le corps de l'e-mail afin de fournir des instructions claires et exploitables au destinataire.
3. Vérifier et enregistrer : Une fois les paramètres configurés, assurez-vous qu'ils sont conformes aux politiques de conformité et de fonctionnement de votre entreprise.

Meilleure pratique : L'activation de ces notifications est un moyen efficace de réduire les violations répétées des politiques en informant les utilisateurs en temps réel des procédures de traitement des données sensibles.



Remarque : Les options de notification peuvent varier en fonction de la configuration du service partagé et des paramètres de stratégie.

Étape 10: Vérifier et enregistrer la règle

Après avoir terminé la configuration de la règle :

1. Vérifiez tous les paramètres configurés.
2. Vérifiez que les classifications de données, l'étendue d'inspection, les conditions d'expéditeur et de destinataire et l'action sélectionnées correspondent au comportement de stratégie souhaité.

3. Cliquez sur Enregistrer pour créer la règle Email DLP.

La stratégie DLP pour les e-mails est désormais active dans Cisco Secure Access.

Option 2: Créer une règle DLP d'e-mail à l'aide d'un modèle DLP personnalisé

La création d'un modèle DLP personnalisé comporte deux phases principales : définition d'un identificateur personnalisé et configuration de la classification des données.

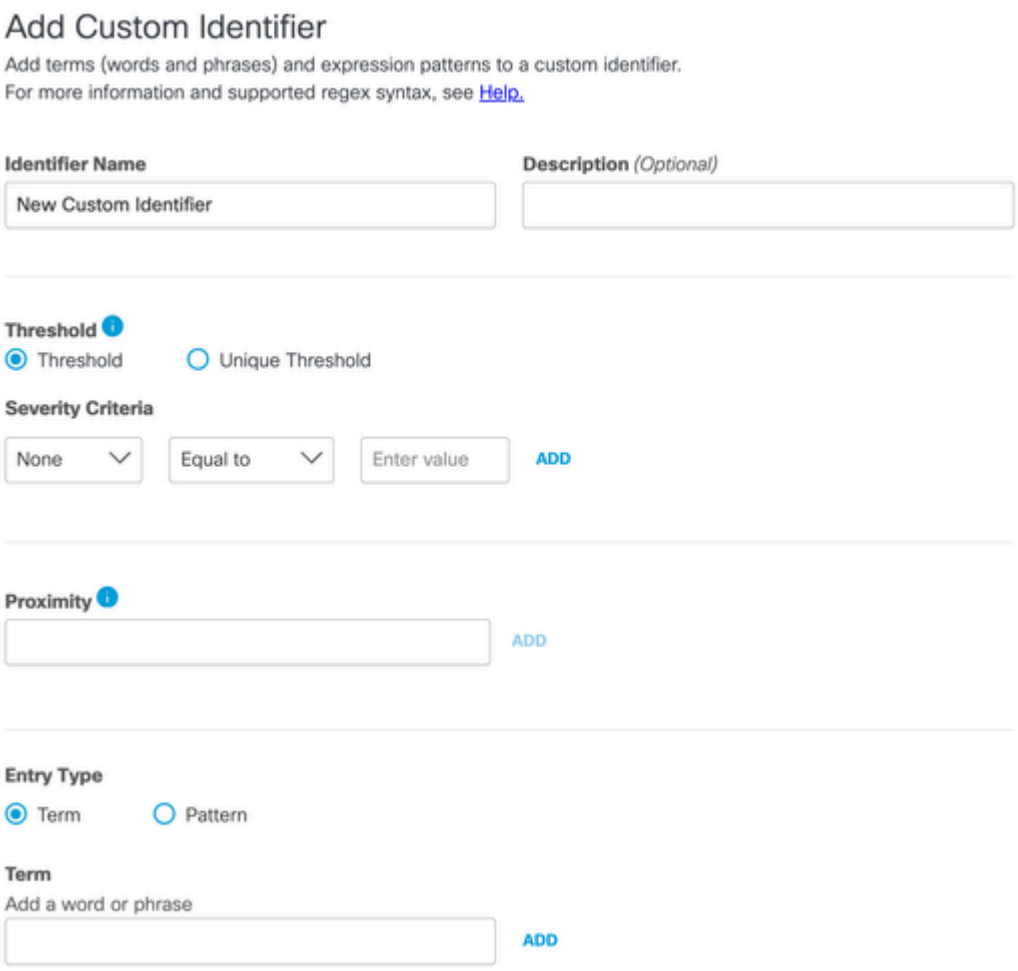
Remarque : Le moteur de classification des données est extrêmement flexible, vous permettant de créer des politiques à l'aide d'un seul identificateur personnalisé ou d'une combinaison d'identificateurs personnalisés et prédéfinis liés par des opérateurs booléens AND/OR.

Étape 11: Créer un identificateur personnalisé

Pour définir un nouveau modèle de données à détecter, procédez comme suit :

1. Connectez-vous au tableau de bord Secure Access.
2. Accédez à Secure > Data Classification.
3. Cliquez sur Ajouter un identificateur personnalisé.
4. Configurez les paramètres suivants dans la fenêtre Ajouter un identificateur personnalisé :

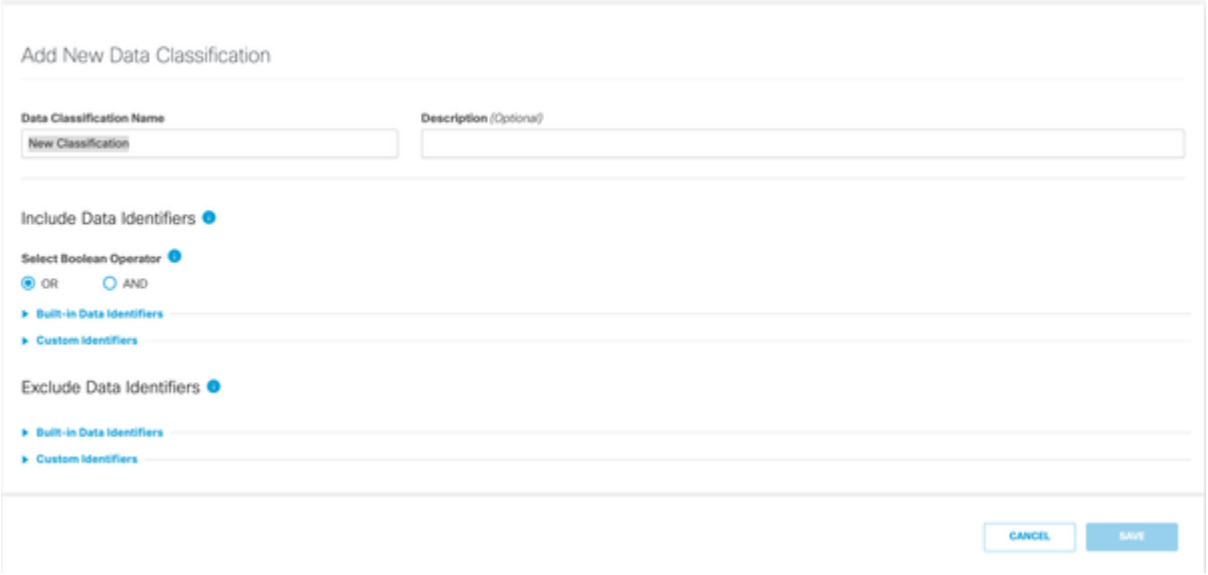
- Nom et description : Fournissez un nom unique et une brève description du type de données que vous souhaitez détecter.
- Seuil :
    - Seuil : Surveille la fréquence totale des données détectées.
    - Seuil unique : Surveille uniquement le nombre d'occurrences uniques des données, en ignorant les doublons.
- Critères de gravité : Attribuez des niveaux de gravité (Très faible, Faible, Moyen, Élevé) en fonction de la fréquence de détection. Vous pouvez les définir à l'aide d'opérateurs de comparaison tels queÉgal à, Supérieur à, Inférieur à ou Plage.
- Proximité : Définissez le seuil de proximité. Cela s'applique à tous les termes et modèles définis dans cet identificateur collectivement, plutôt que par terme individuel.
- Type d'entrée : Définissez la manière dont le système identifie les données :
    - Terme: Un mot ou une expression spécifique.
    - Modèle : Expression régulière (regex) utilisée pour détecter des formats de données spécifiques (numéros de carte de crédit ou codes de projet internes, par exemple).



Étape 12: Configurer la classification des données

Une fois votre identificateur personnalisé enregistré, vous pouvez l'intégrer dans un objet Classification des données :

1. Accédez àSecure > Data Classification > Add (utilisez le bouton situé dans l'angle supérieur droit)
2. Sélectionnez votre nouvel identificateur personnalisé dans la liste disponible.
3. (Facultatif) Combinez votre identificateur personnalisé avec des identificateurs prédéfinis en utilisant la logique AND/OR pour affiner la portée de la détection.
4. Enregistrez la configuration pour la rendre disponible dans vos stratégies DLP de messagerie.
5. Reportez-vous à la capture d'écran ci-dessous pour plus d'informations.
6. Suivez maintenant les mêmes étapes de l'étape 4 à l'étape 10 pour créer une stratégie à l'aide de la classification de données personnalisée.



Cette configuration garantit que votre entreprise peut détecter des informations sensibles adaptées spécifiquement à vos structures de données internes et aux exigences de conformité.

Dépannage

Si la règle Email DLP ne se comporte pas comme prévu, vérifiez les points suivants :

La règle ne correspond pas aux e-mails

- Vérifiez que le modèle de classification de données correct est sélectionné.
- Vérifiez que les emplacements d'inspection appropriés sont activés :
  - Objet du courrier électronique
  - Corps du message
  - Nom de pièce jointe
  - Contenu des pièces jointes
- Assurez-vous que les filtres d'expéditeur et de destinataire n'excluent pas involontairement le message test.

Les e-mails ne sont pas bloqués

- Vérifiez que l'action de la règle est définie sur Blocket non sur Monitor.
- Vérifiez que la règle est enregistrée et activée.
- Assurez-vous que le contenu du courrier électronique correspond aux critères DLP configurés.

Les événements DLP ne sont pas visibles dans ETD

- Vérifiez que Cisco ETD et Cisco Secure Access sont correctement intégrés.
- Vérifiez que l'ETD traite activement le trafic de messagerie électronique concerné.
- Vérifiez si l'événement de stratégie est présent en premier dans Cisco Secure Access.

Aucune correspondance basée sur les pièces jointes n'est détectée

- Vérifiez que le nom et/ou le contenu de la pièce jointe sont sélectionnés dans la portée de l'inspection.
- Vérifiez les paramètres de contrôle de fichier si des étiquettes telles queMIPouTitus font partie de la logique de la règle.

Meilleures pratiques

Tenez compte des meilleures pratiques suivantes lors du déploiement des stratégies DLP pour les e-mails :

- Commencez parMonitormode pour valider le comportement de la stratégie avant d'appliquerBlock.
- Utilisez des noms de règles clairs et descriptifs pour faciliter l'administration.
- Étendez soigneusement les conditions de l'expéditeur et du destinataire afin de réduire les correspondances imprévues.
- Testez avec des données représentatives avant un déploiement général.
- Vérifiez régulièrement le suivi des messages ETD pour valider l'activité des e-mails bloqués ou surveillés.
- Utilisez des modèles personnalisés lorsque des identificateurs de données spécifiques à l'entreprise sont requis.

Résumé

Cisco Secure Access est la plate-forme centrale pour la configuration des stratégies DLP des e-mails dans un déploiement intégré de Cisco Secure Access et de Cisco Email Threat Defense. Tandis qu'ETD fournit la visibilité et le suivi des messages, toutes les fonctions de création de règles DLP, de sélection de classification, d'action d'application et de notification sont configurées dans Secure Access.

En utilisant des modèles DLP prédéfinis ou personnalisés, les administrateurs peuvent inspecter le contenu et les pièces jointes des e-mails, définir l'étendue de l'expéditeur et du destinataire et appliquer des actions de surveillance ou de blocage pour empêcher la perte de données sensibles par e-mail.

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.