Détecter et empêcher l'usurpation de messagerie

Table des matières

Introduction

Ce document décrit comment détecter et empêcher l'usurpation d'adresse e-mail lors de l'utilisation de Cisco Secure Email.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- E-mail sécurisé Cisco

Composants utilisés

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.

À propos de ce document

Ce document s'adresse aux clients Cisco, aux partenaires de distribution Cisco et aux ingénieurs Cisco qui déploient la messagerie sécurisée Cisco. Ce document couvre :

- En quoi consiste l'usurpation de messagerie ?
- Workflow de défense contre l'usurpation
- Que pouvez-vous faire de plus avec la prévention contre l'usurpation ?

En quoi consiste la mystification des e-mails

L'usurpation d'e-mail est une falsification d'en-tête d'e-mail dont le message semble provenir d'une personne ou d'une source autre que la source réelle. L'usurpation d'adresse e-mail est utilisée dans les campagnes d'hameçonnage et de spam, car les gens sont plus susceptibles d'ouvrir un e-mail lorsqu'ils pensent qu'une source légitime et fiable l'a envoyé. Pour plus d'informations sur l'usurpation, veuillez vous référer à Qu'est-ce que l'usurpation d'adresse e-mail et Comment le détecter.

L'usurpation d'adresse e-mail appartient aux catégories suivantes :

Catégorie	Description	Cible principale
Usurpation directe de domaine	Empruntez l'identité d'un domaine similaire dans le champ Envelope From en tant que domaine du destinataire.	Employés
Déception de nom d'affichage	L'en-tête De affiche un expéditeur légitime avec le nom de cadre d'une organisation. Elles sont également appelées « compromission de la messagerie professionnelle » (BEC).	Employés
Emprunt d'identité	L'en-tête De affiche un expéditeur légitime avec le nom commercial d'une organisation bien connue.	Clients/partenaires
Attaque basée sur des URL de phishing	Un e-mail avec une URL qui tente de voler des données sensibles ou des informations de connexion de la victime. Un faux e-mail provenant d'une banque vous demandant de cliquer sur un lien et de vérifier les détails de votre compte est un exemple d'attaque par hameçonnage basé sur une URL.	Employés/partenaires
Attaque de	La valeur d'en-tête Enveloppe de ou De affiche une	Employés/partenaires

domaine de type Cousin ou Apparence	adresse d'expéditeur similaire qui se fait passer pour une adresse réelle pour contourner les inspections SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting and Conformance).	
Reprise de compte / Compte compromis	Obtenez un accès non autorisé à un compte de messagerie réel appartenant à quelqu'un, puis envoyez des e-mails à d'autres victimes en tant que propriétaire légitime du compte de messagerie.	Tout le monde

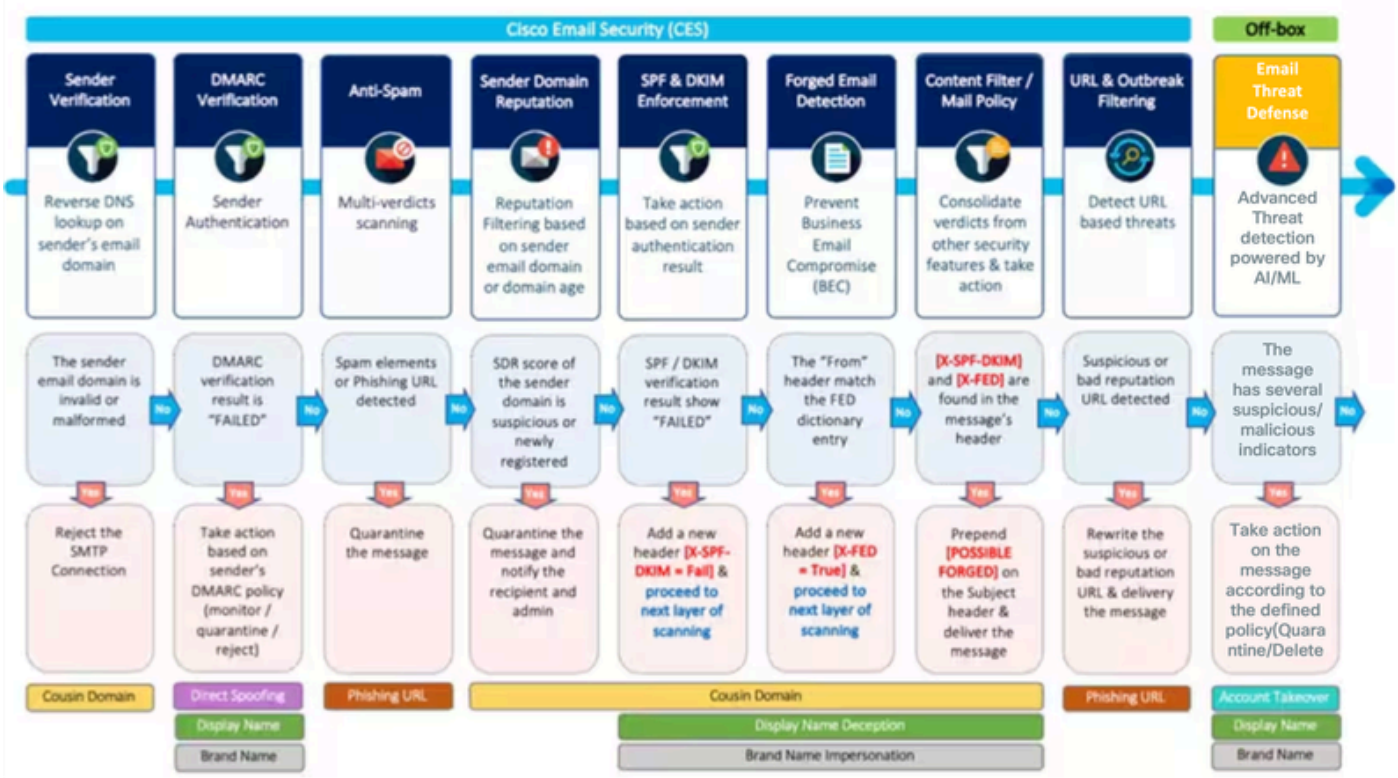
La première catégorie concerne les abus du nom de domaine du propriétaire dans la valeur Envelope From de l'en-tête Internet d'un e-mail. Cisco Secure Email peut remédier à cette attaque en utilisant la vérification DNS (Domain Name Server) de l'expéditeur pour autoriser uniquement les expéditeurs légitimes. Le même résultat peut être obtenu globalement à l'aide de la vérification DMARC, DKIM et SPF.

Cependant, les autres catégories ne violent que partiellement la partie domaine de l'adresse e-mail de l'expéditeur. Par conséquent, il n'est pas facile d'être dissuadé lorsque vous utilisez des enregistrements de texte DNS ou la vérification de l'expéditeur seulement. Idéalement, il serait préférable de combiner certaines fonctionnalités de sécurisation de la messagerie électronique de Cisco et Cisco Secure Email Threat Defense (ETD) pour lutter contre ces menaces avancées. Comme vous le savez, l'administration et la configuration des fonctions de sécurisation de la messagerie électronique Cisco peuvent varier d'une entreprise à l'autre, et une application incorrecte peut entraîner un taux élevé de faux positifs. Par conséquent, il est essentiel de comprendre les besoins de l'entreprise et d'adapter les fonctionnalités.

Workflow de défense contre l'usurpation

Les fonctionnalités de sécurité qui répondent aux meilleures pratiques de surveillance, d'avertissement et d'application contre les attaques par mystification sont présentées dans le schéma (Image 1). Les détails de chaque fonction sont fournis dans ce document. La meilleure pratique consiste à adopter une approche de défense approfondie pour détecter l'usurpation d'adresse e-mail. Les pirates peuvent modifier leurs méthodes à l'encontre d'une entreprise au fil du temps. Un administrateur doit donc surveiller les modifications et vérifier les avertissements et l'application appropriés.

Image 1. Pipeline Cisco Secure Email Spoof Defense

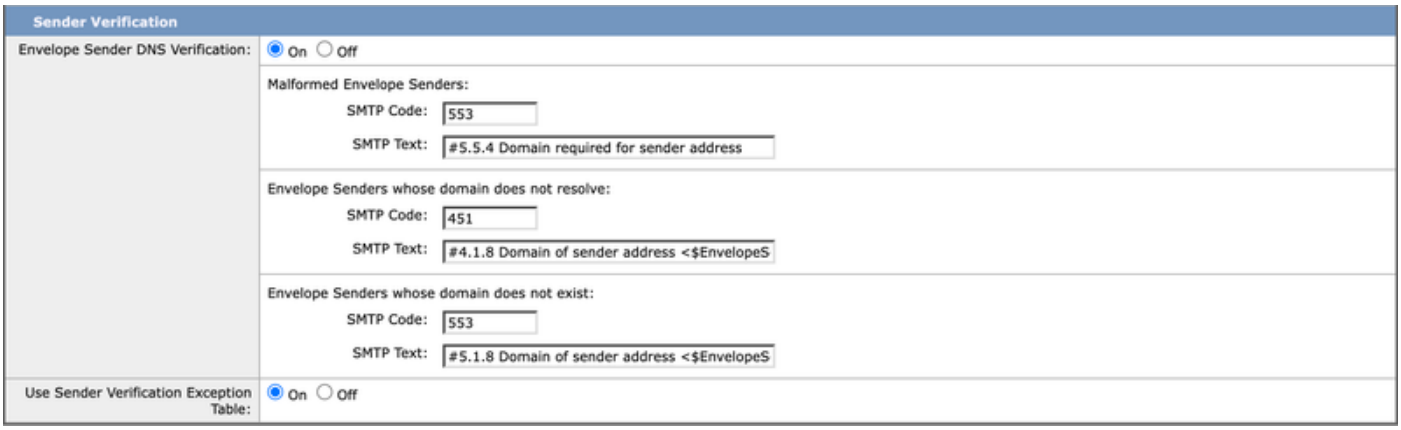


Couche 1 : contrôle de validité du domaine de l'expéditeur

La vérification de l'expéditeur est un moyen plus simple d'empêcher l'envoi d'e-mails à partir d'un domaine de messagerie fictif, tel que l'usurpation de domaine cousin (par exemple, c1sc0.com est l'imposteur de cisco.com). Cisco Secure Email effectue une requête d'enregistrement MX pour le domaine de l'adresse e-mail de l'expéditeur et effectue une recherche d'enregistrement A sur l'enregistrement MX pendant la conversation SMTP. Si la requête DNS renvoie NXDOMAIN, elle peut considérer le domaine comme inexistant. Il est courant que les pirates falsifient les informations de l'expéditeur de l'enveloppe afin que l'e-mail d'un expéditeur non vérifié soit accepté et traité. Cisco Secure Email peut rejeter tous les messages entrants qui échouent au contrôle de vérification qui utilise cette fonctionnalité, sauf si le domaine ou l'adresse IP de l'expéditeur est ajouté au préalable dans la table des exceptions.

Meilleure pratique : configurez Cisco Secure Email pour rejeter la conversation SMTP si le domaine de messagerie du champ de l'expéditeur de l'enveloppe n'est pas valide. Autoriser uniquement les expéditeurs légitimes en configurant la stratégie de flux de messagerie, la vérification des expéditeurs et la table des exceptions (facultatif). Pour plus d'informations, consultez Protection contre les usurpations avec vérification de l'expéditeur.

Image 2. Section Vérification de l'expéditeur dans la stratégie de flux de messagerie par défaut



Couche 2 : vérification de l'en-tête From à l'aide de DMARC

La vérification DMARC est une fonctionnalité beaucoup plus puissante pour lutter contre l'usurpation de domaine direct, et inclut également les attaques par nom d'affichage et par usurpation d'identité de marque. DMARC associe les informations authentifiées avec SPF ou DKIM (source ou signature de domaine d'envoi) avec ce qui est présenté au destinataire final dans l'en-tête De et vérifie que les identificateurs SPF et DKIM sont alignés sur l'identificateur d'en-tête DE.

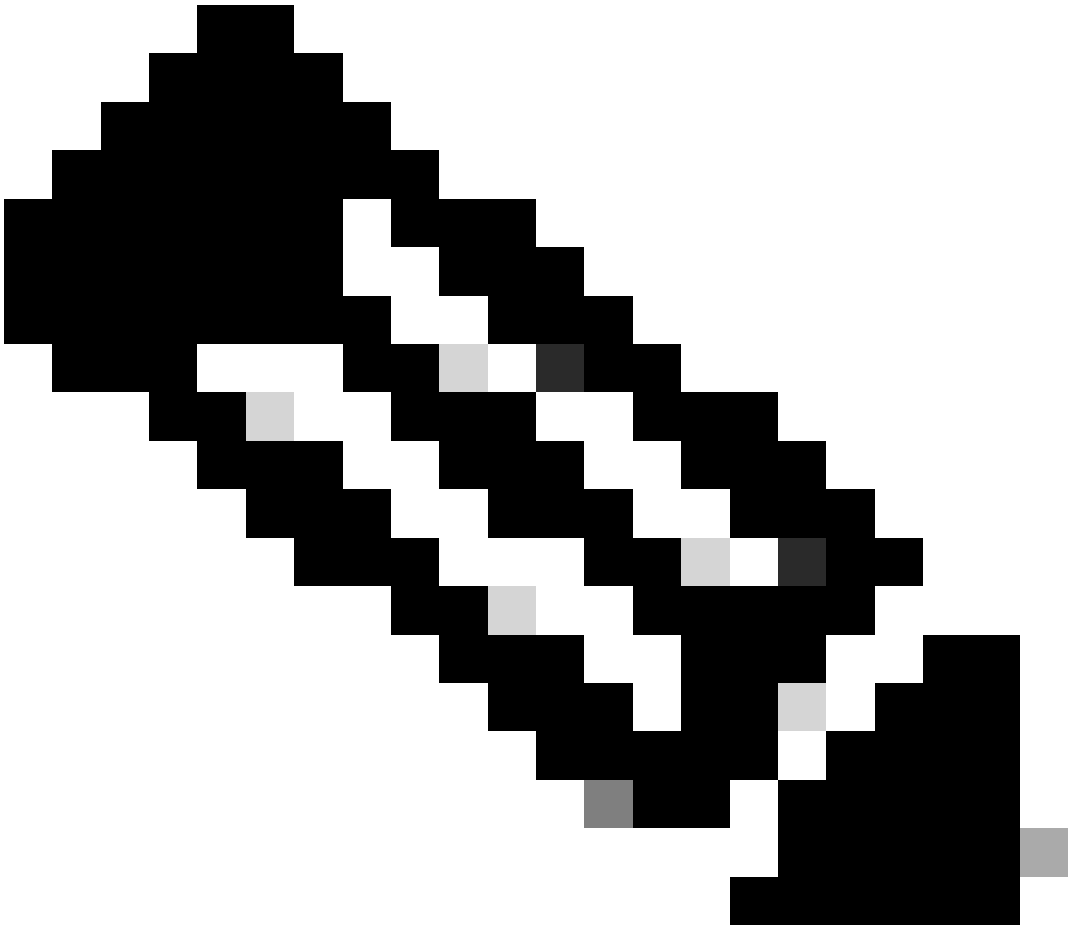
Pour réussir la vérification DMARC, un e-mail entrant doit passer au moins l'un de ces mécanismes d'authentification. En outre, Cisco Secure Email permet également à l'administrateur de définir un profil de vérification DMARC pour remplacer les stratégies DMARC du propriétaire de domaine et envoyer des rapports agrégés (RUA) et des rapports d'échec/analyse (RUF) aux propriétaires de domaine. Cela permet de renforcer leurs déploiements d'authentification en retour.

Meilleure pratique : modifiez le profil DMARC par défaut qui utilise les actions de stratégie DMARC conseillées par l'expéditeur. En outre, les paramètres globaux de la vérification DMARC doivent être modifiés pour permettre la génération correcte de rapports. Une fois le profil correctement configuré, le service de vérification DMARC doit être activé dans la stratégie par défaut Politiques de flux de messagerie.

Image 3. Profil de vérification DMARC

Create DMARC Verification Profile

Profile Name:	DEFAULT
Message Action when the Policy in DMARC Record is Reject:	○ No Action ○ Quarantine to: ACCOUNT_TAKEOVER (centralized) ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC unauthenticated mai
Message Action when the Policy in DMARC Record is Quarantine:	○ No Action ◉ Quarantine to: Policy (centralized)
Message Action for Temporary Failure:	◉ Accept ○ Reject SMTP Code: 451 SMTP Response: #4.7.1 Unable to perform DMARC v
Message Action for Permanent Failure:	○ Accept ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC verification failed.



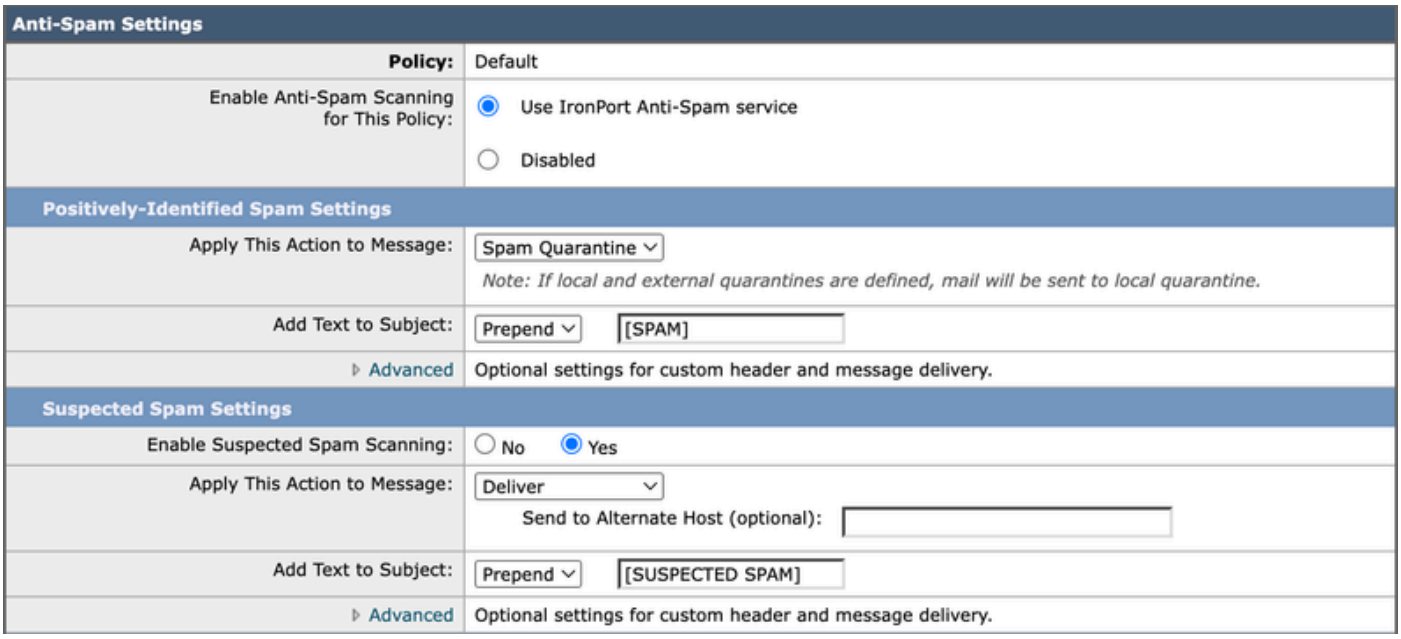
Remarque : DMARC doit être mis en oeuvre en envoyant le propriétaire du domaine conjointement avec un outil de surveillance de domaine, tel que Cisco Domain Protection. Lorsqu'elle est correctement mise en oeuvre, l'application DMARC dans Cisco Secure Email permet de se protéger contre les e-mails d'hameçonnage envoyés aux employés par des expéditeurs ou des domaines non autorisés. Pour plus d'informations sur Cisco Domain Protection, consultez le lien suivant : Cisco Secure Email Domain Protection At-A-Glance.

Couche 3 : Empêcher les spammeurs d'envoyer des e-mails usurpés

Les attaques par mystification peuvent être une autre forme courante de campagne de spam. Par conséquent, l'activation de la protection antispam est essentielle pour identifier efficacement les e-mails frauduleux contenant des éléments de spam/phishing et les bloquer de manière positive. L'antispam, associé à d'autres actions basées sur les meilleures pratiques décrites en détail dans ce document, offre les meilleurs résultats sans perdre d'e-mails légitimes.

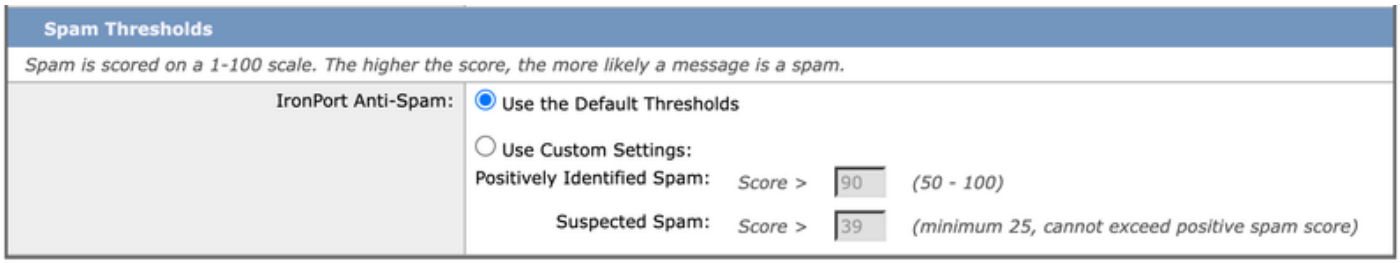
Meilleure pratique : activez l'analyse antispam dans la stratégie de messagerie par défaut et définissez une action de quarantaine pour identifier les paramètres de spam de manière positive. Augmenter la taille minimale d'analyse des messages de spam à au moins 2 millions au niveau mondial.

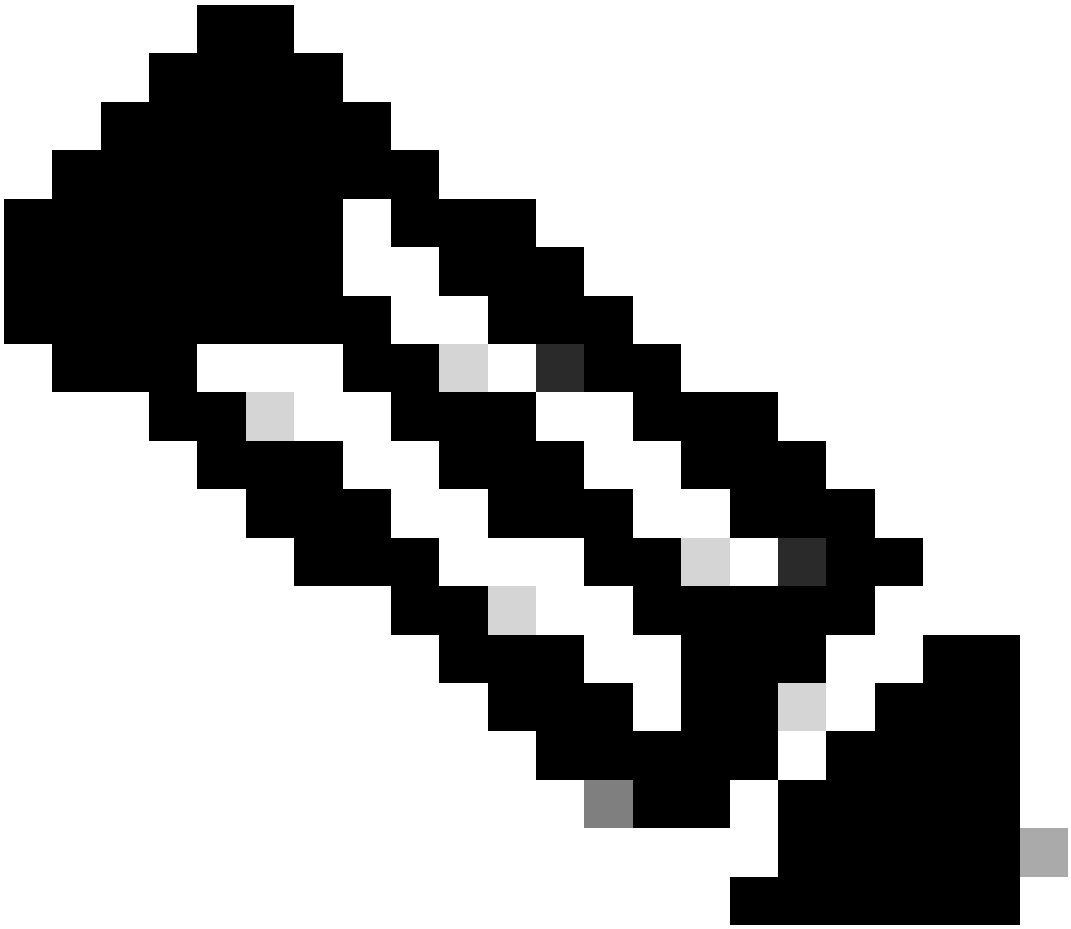
Image 4. Paramètre antispam de la stratégie de messagerie par défaut



Le seuil de spam peut être ajusté pour le spam avéré et le spam suspecté afin d'augmenter ou de diminuer la sensibilité (Image 5). Toutefois, Cisco déconseille à l'administrateur d'effectuer cette opération et d'utiliser uniquement les seuils par défaut comme référence, sauf indication contraire de Cisco.

Image 5. Paramètre des seuils antispam dans la stratégie de messagerie par défaut





Remarque : Cisco Secure Email propose un moteur d'analyse multipoint intelligente (IMS) qui fournit différentes combinaisons du moteur antispam pour augmenter les taux d'interception du spam (taux d'interception le plus agressif).

Couche 4 : identification des expéditeurs malveillants via le domaine de messagerie

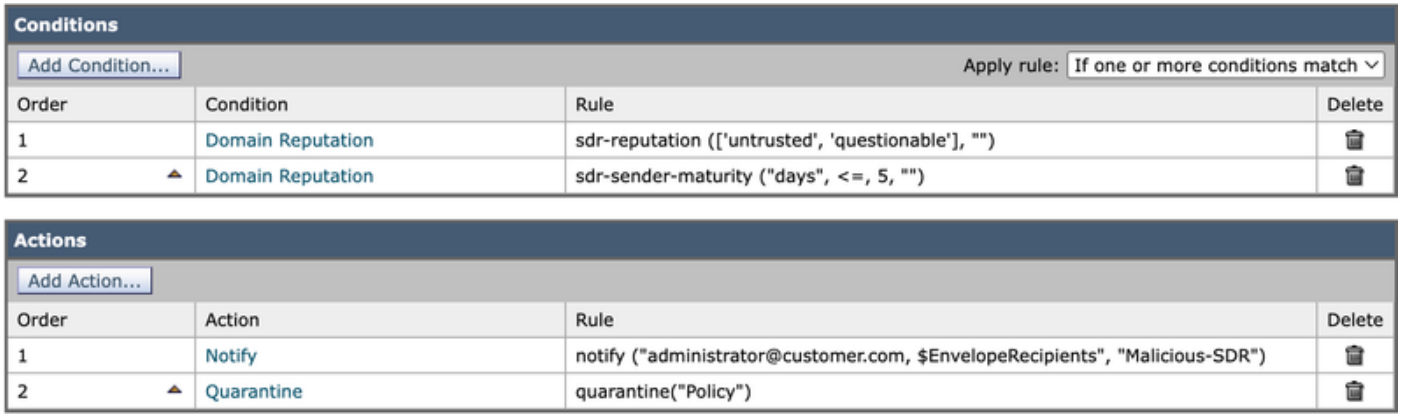
Cisco Talos Sender Domain Reputation (SDR) est un service cloud qui fournit un verdict de réputation pour les e-mails en fonction des domaines de l'enveloppe et de l'en-tête de l'e-mail. L'analyse de réputation basée sur le domaine permet d'augmenter le taux d'interception du spam en allant au-delà de la réputation des adresses IP partagées, de l'hébergement ou des

fournisseurs d'infrastructure. Au lieu de cela, il dérive des verdicts basés sur des fonctionnalités associées aux noms de domaine complets (FQDN) et d'autres informations d'expéditeur dans la conversation SMTP (Simple Mail Transfer Protocol) et les en-têtes de message.

La maturité de l'expéditeur est une fonctionnalité essentielle pour établir la réputation de l'expéditeur. La maturité de l'expéditeur est automatiquement générée pour la classification du spam en fonction de plusieurs sources d'informations et peut différer de l'âge du domaine basé sur Whois. La maturité de l'expéditeur est limitée à 30 jours. Au-delà de cette limite, un domaine est considéré comme arrivé à maturité en tant qu'expéditeur d'e-mail et aucun autre détail n'est fourni.

Meilleure pratique : créez un filtre de contenu entrant qui capture le domaine d'envoi dans lequel le verdict de réputation SDR tombe sous Non approuvé/contestable ou la maturité de l'expéditeur est inférieure ou égale à 5 jours. L'action recommandée consiste à mettre le message en quarantaine et à en informer l'administrateur de la sécurité de la messagerie et le destinataire d'origine. Pour plus d'informations sur la configuration de SDR, consultez la vidéo Cisco sur Cisco Email Security Update (Version 12.0) : Sender Domain Reputation (SDR)

Image 6. Filtre de contenu pour la réputation SDR et l'âge du domaine avec actions de notification et de quarantaine.

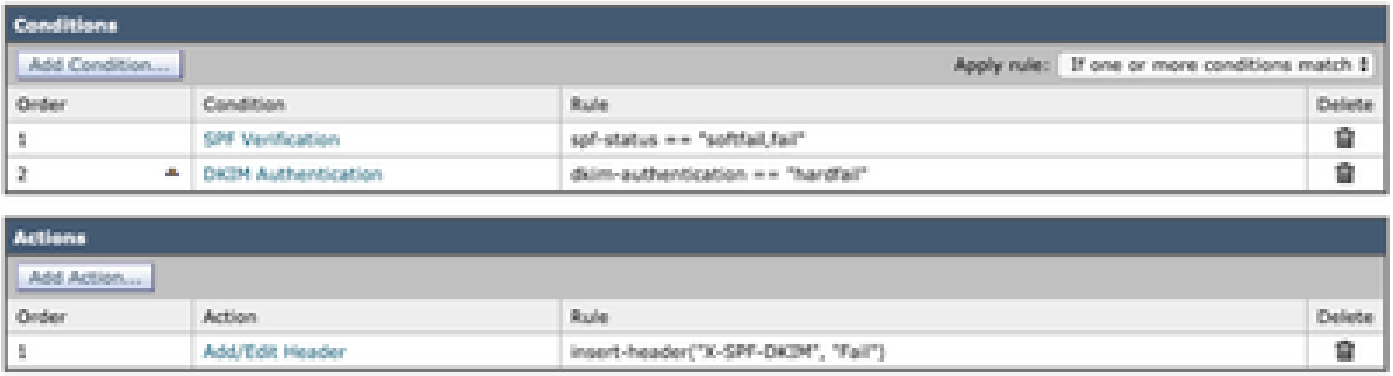


Couche 5 : réduction des faux positifs grâce aux résultats de la vérification SPF ou DKIM

Il est impératif d'appliquer la vérification SPF ou DKIM (les deux ou l'une d'entre elles) pour créer plusieurs couches de détection des e-mails frauduleux pour la plupart des types d'attaque. Au lieu d'entreprendre une action finale (telle que la suppression ou la quarantaine), Cisco recommande d'ajouter un nouvel en-tête tel que [X-SPF-DKIM] sur le message qui échoue à la vérification SPF ou DKIM et de coopérer avec la fonctionnalité de détection des e-mails falsifiés (FED), qui est traitée ultérieurement, en faveur d'un taux d'interception amélioré des e-mails frauduleux.

Meilleure pratique : créez un filtre de contenu qui inspecte les résultats de vérification SPF ou DKIM de chaque message entrant ayant traversé les inspections précédentes. Ajoutez un nouvel en-tête X (par exemple, X-SPF-DKIM=Fail) au message dont la vérification SPF ou DKIM échoue et qui est transmis à la couche d'analyse suivante : détection des e-mails falsifiés (FED).

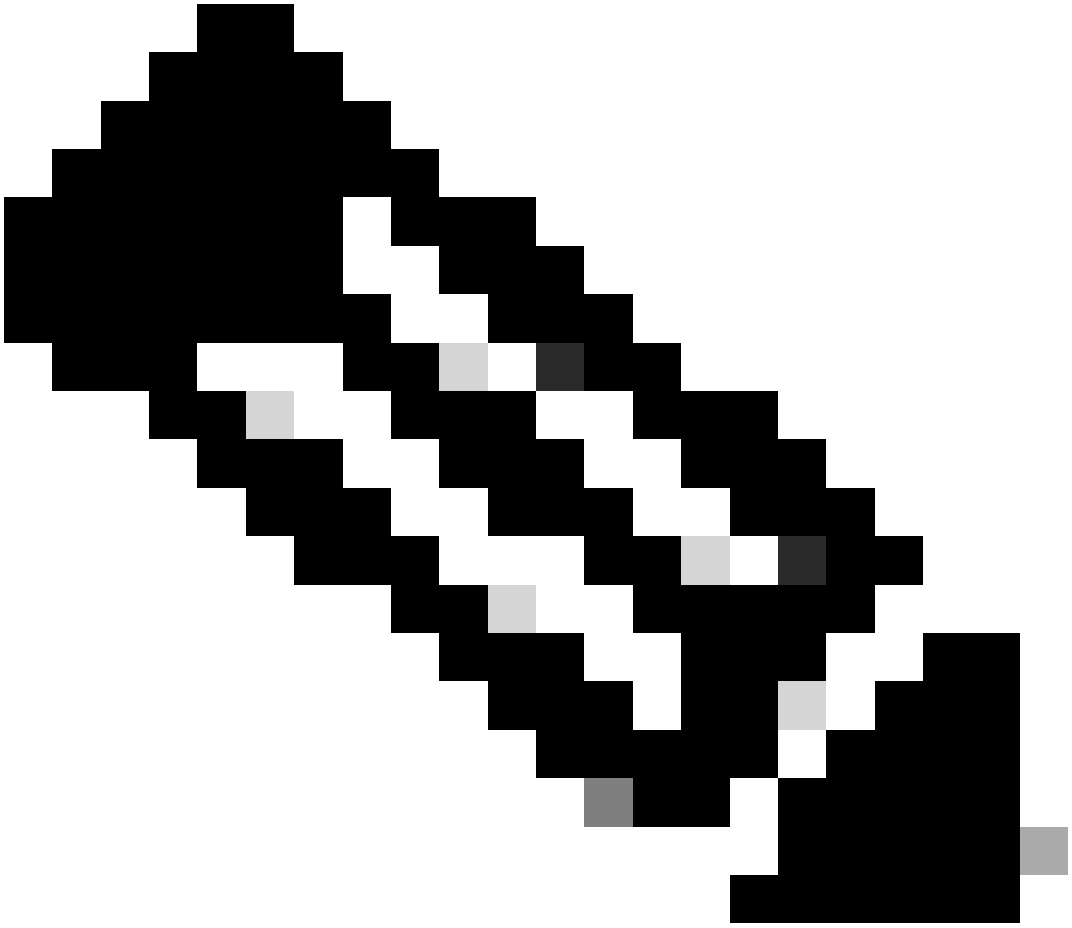
Image 7. Filtre de contenu qui inspecte les messages dont les résultats SPF ou DKIM ont échoué



Couche 6 : détection des messages avec un nom d'expéditeur potentiellement falsifié

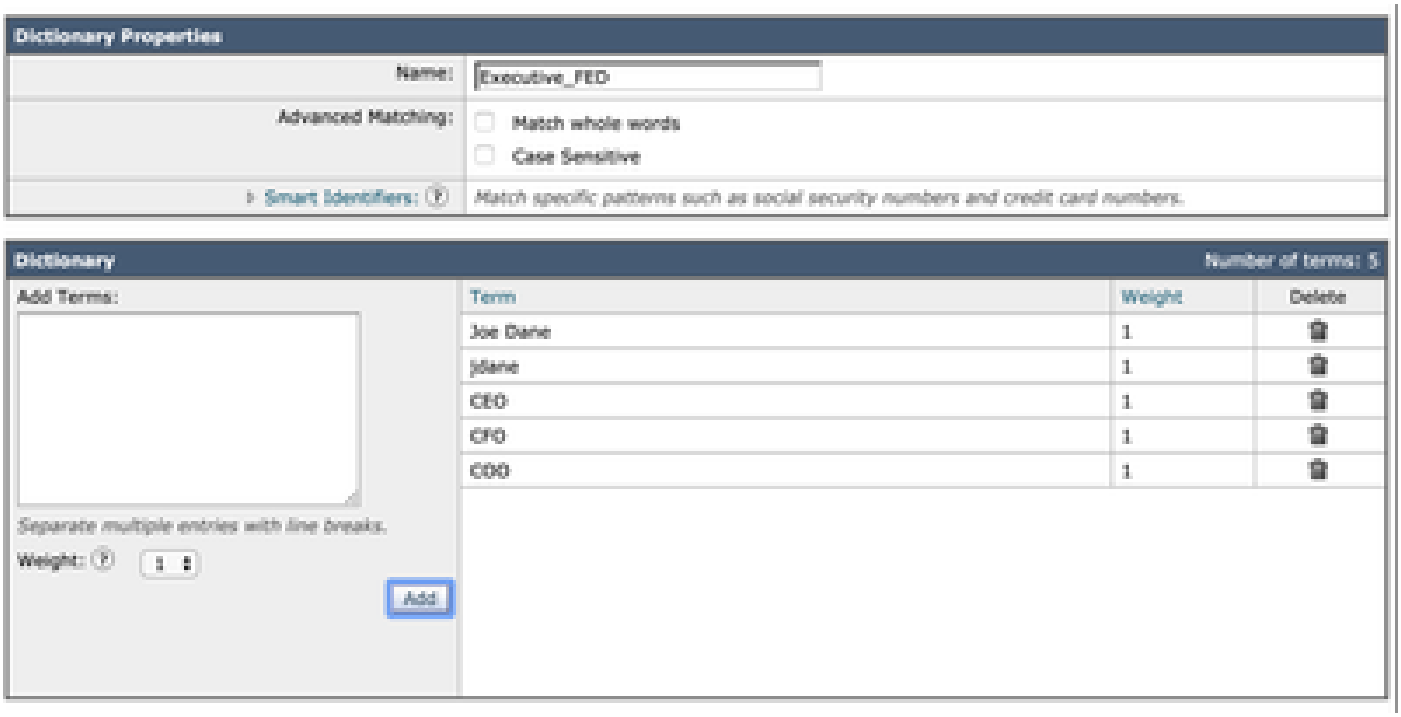
En complément des vérifications SPF, DKIM et DMARC, la détection des e-mails falsifiés (FED) est une autre ligne de défense essentielle contre l'usurpation d'adresse e-mail. Le FED est idéal pour remédier aux attaques par usurpation qui utilisent la valeur From dans le corps du message. Étant donné que vous connaissez déjà les noms des cadres supérieurs au sein de l'entreprise, vous pouvez créer un dictionnaire de ces noms et le référencer avec la condition FED dans les filtres de contenu. En outre, en plus des noms de dirigeants, vous pouvez créer un dictionnaire de domaines cousins ou de domaines similaires basé sur votre domaine en utilisant DNSTWIST (DNSTWIT) pour le comparer à l'usurpation de domaine de même type.

Meilleure pratique : identifiez les utilisateurs de votre organisation dont les messages sont susceptibles d'être falsifiés. Créez un dictionnaire personnalisé qui tient compte des cadres. Pour chaque nom de cadre, le dictionnaire doit inclure le nom d'utilisateur et tous les noms d'utilisateur possibles comme termes (Image 8). Une fois le dictionnaire terminé, utilisez la détection des e-mails falsifiés dans le filtre de contenu pour faire correspondre la valeur De des messages entrants avec ces entrées du dictionnaire.



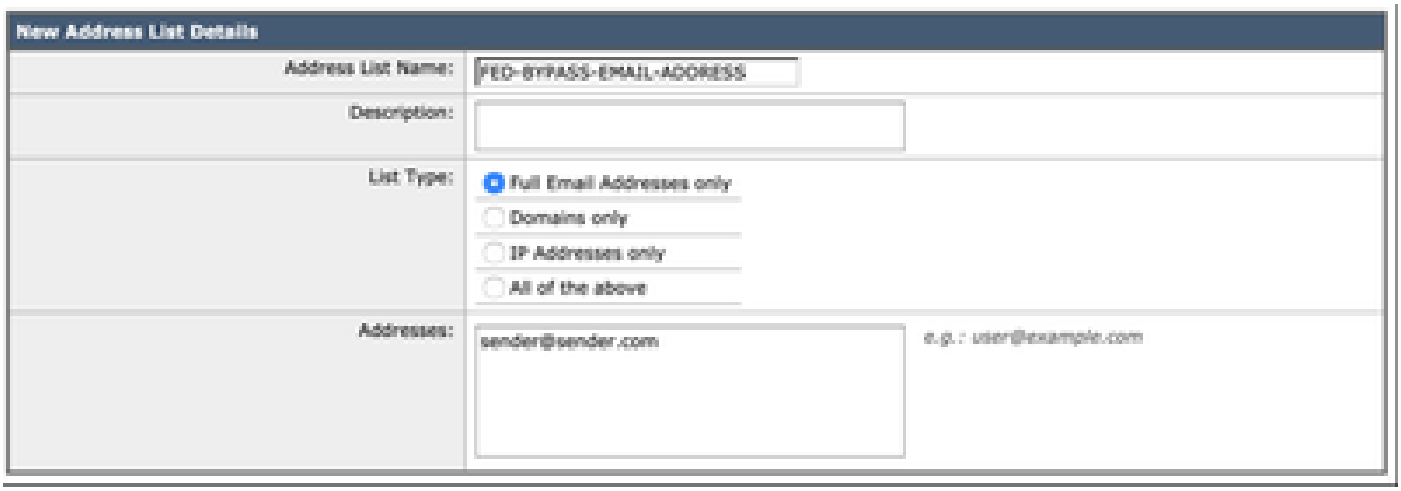
Remarque : étant donné que la plupart des domaines ne sont pas des permutations enregistrées, la vérification de l'expéditeur DNS les protège. Si vous choisissez d'utiliser des entrées de dictionnaire, ne prêtez attention qu'aux domaines enregistrés et veillez à ne pas dépasser 500 à 600 entrées par dictionnaire.

Image 8. Répertoire personnalisé pour la détection des e-mails falsifiés



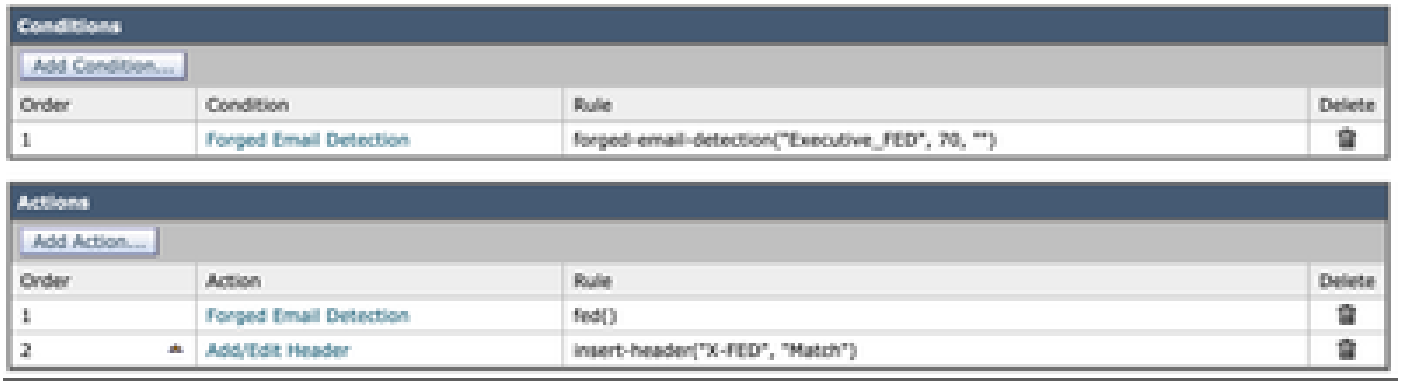
Il est facultatif d'ajouter une condition d'exception pour votre domaine de messagerie électronique dans l'Envelope Send pour contourner l'inspection FED. Il est également possible de créer une liste d'adresses personnalisée pour contourner l'inspection FED et obtenir une liste d'adresses électroniques affichées dans l'en-tête du formulaire (image 9).

Image 9. Créer une liste d'adresses pour contourner l'inspection FED



Appliquez l'action propriétaire Détection des e-mails falsifiés pour supprimer la valeur De et vérifier l'adresse e-mail réelle de l'expéditeur de l'enveloppe dans la boîte de réception du message. Ensuite, plutôt que d'appliquer une action finale, ajoutez un nouvel en-tête X (par exemple, X-FED=Match) sur le message qui correspond à la condition et continuez à transmettre le message à la couche d'inspection suivante (Image 10).

Image 10. Paramètre de filtre de contenu recommandé pour FED

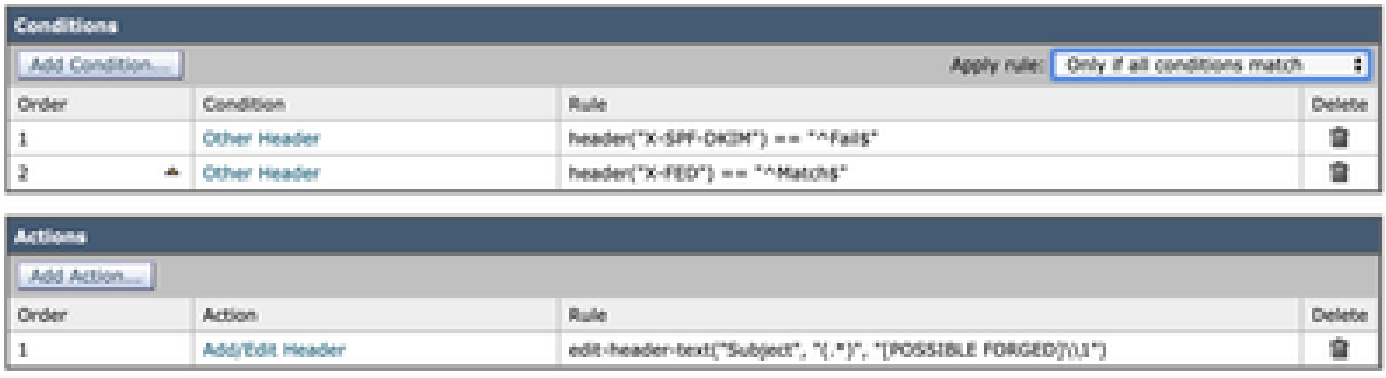


Couche 7 : e-mail d'usurpation identifié positivement

L'identification d'une véritable campagne d'usurpation est plus efficace en référençant d'autres verdicts à partir de diverses fonctions de sécurité dans le pipeline, telles que les informations d'en-tête X produites par SPF/ DKIM Enforcemen et FE. Par exemple, les administrateurs peuvent créer un filtre de contenu pour identifier les messages ajoutés avec les deux nouveaux en-têtes X en raison de l'échec des résultats de vérification SPF / DKIM (X-SPF-DKIM=Fail) et dont l'en-tête From correspond aux entrées du dictionnaire FED (X-FED=Match).

L'action recommandée peut consister soit à mettre le message en quarantaine et à le notifier au destinataire, soit à continuer de remettre le message d'origine mais en ajoutant des mots [POSSIBLE FAUX] à la ligne d'objet comme avertissement au destinataire, comme illustré (Image 11).

Image 11. Combiner tous les en-têtes X en une seule règle (finale)



Couche 8 : Protection contre les URL d'hameçonnage

La protection contre les liens d'hameçonnage est intégrée à l'URL et au filtrage des attaques de la messagerie sécurisée Cisco. Les menaces combinées combinent les messages d'usurpation et d'hameçonnage pour donner l'impression que la cible est plus légitime. L'activation du filtrage des attaques est essentielle pour détecter, analyser et stopper ces menaces en temps réel. Il est intéressant de savoir que la réputation des URL est évaluée dans le moteur antispam et peut être utilisée dans le cadre de la décision de détection du spam. Si le moteur antispam n'arrête pas le message avec l'URL comme spam, il est évalué par le filtrage des URL et des attaques dans la dernière partie du pipeline de sécurité.

Recommandation : créez une règle de filtre de contenu qui bloque une URL avec un score de réputation malveillante et redirige l'URL avec un score de réputation neutre vers Cisco Security Proxy (Image 12). Activez les filtres contre les attaques en activant la modification des messages. La réécriture d'URL permet à Cisco Security Proxy d'analyser les URL suspectes (Image 13). Pour plus d'informations, consultez : Configurer le filtrage des URL pour la passerelle de messagerie sécurisée et la passerelle cloud

Image 12. Filtre de contenu pour la réputation des URL

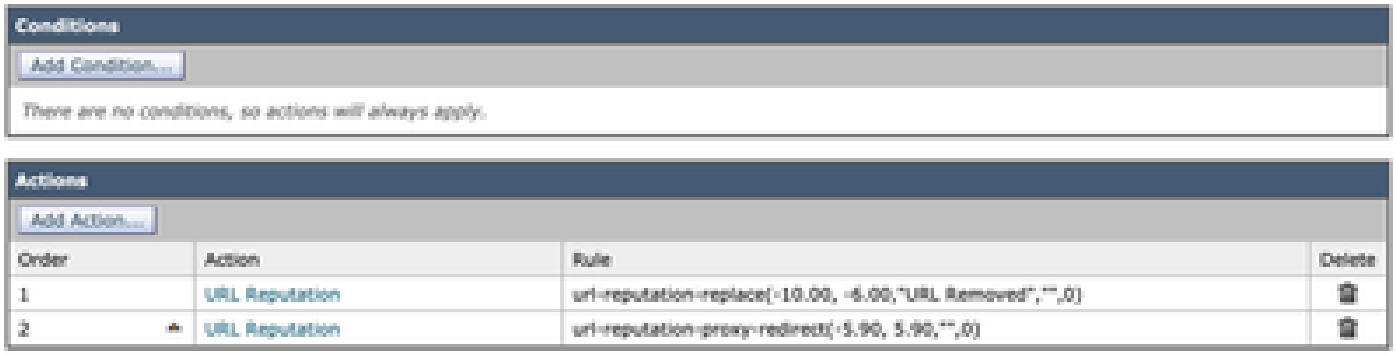
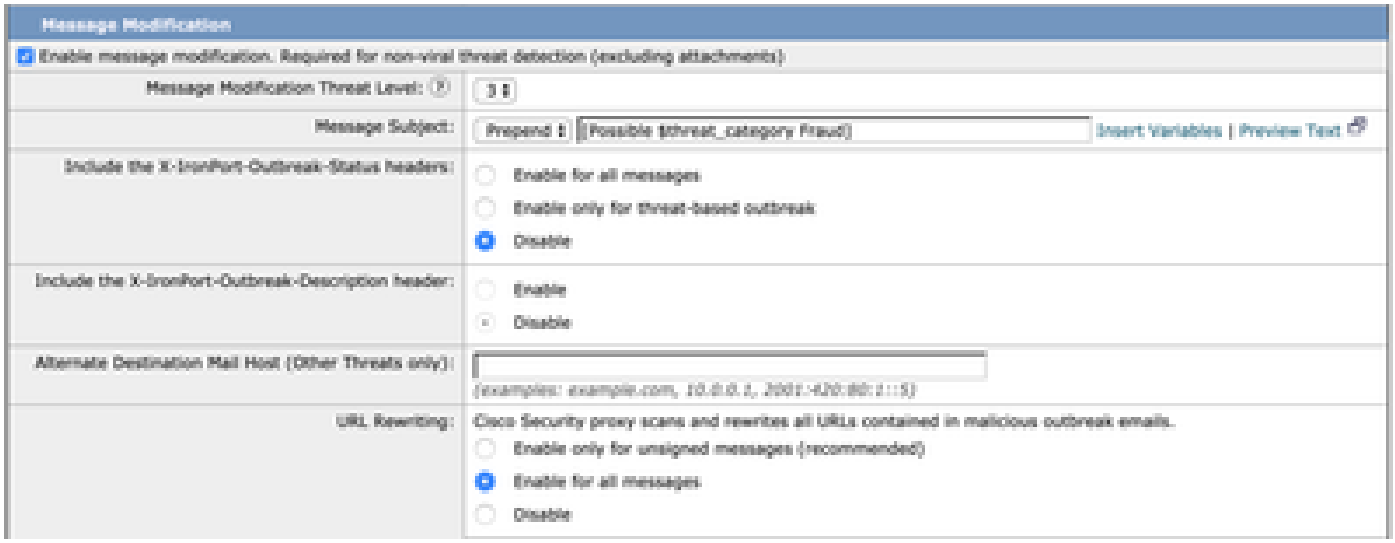


Image 13. Activer la réécriture d'URL dans le filtrage des attaques



Couche 9 : augmentez la capacité de détection d'usurpation avec Cisco Secure Email Threat Defense (ETD)

Cisco propose Email Threat Defense, une solution cloud native qui tire parti de l'intelligence supérieure de Cisco Talos en matière de menaces. Il dispose d'une architecture API pour des temps de réponse plus rapides, une visibilité complète sur les e-mails, y compris les e-mails internes, une vue de conversation pour de meilleures informations contextuelles et des outils de correction automatique ou manuelle des menaces qui se cachent dans les boîtes aux lettres Microsoft 365. Consultez la fiche technique Cisco Secure Email Threat Defense pour plus d'informations.

Cisco Secure Email Threat Defense combat le phishing grâce à l'authentification de l'expéditeur et aux fonctionnalités de détection BEC. Il intègre des moteurs d'apprentissage automatique et

d'intelligence artificielle qui combinent la modélisation locale de l'identité et des relations avec l'analyse des comportements en temps réel pour se protéger contre les menaces basées sur la tromperie d'identité. Il modélise le comportement de confiance des e-mails au sein des entreprises et entre les individus. La solution Email Threat Defense offre notamment les avantages suivants :

- Détectez les menaces connues, émergentes et ciblées grâce à des fonctionnalités avancées de détection des menaces.
- Identifiez les techniques malveillantes et identifiez le contexte des risques métiers spécifiques.
- Recherchez rapidement les menaces dangereuses et corrigez-les en temps réel.
- Utilisez la télémétrie des menaces consultable pour classer les menaces et identifier les parties de votre entreprise les plus vulnérables aux attaques.

Figure 14. Cisco Secure Email Threat Defense fournit des informations sur la manière dont votre entreprise est ciblée.

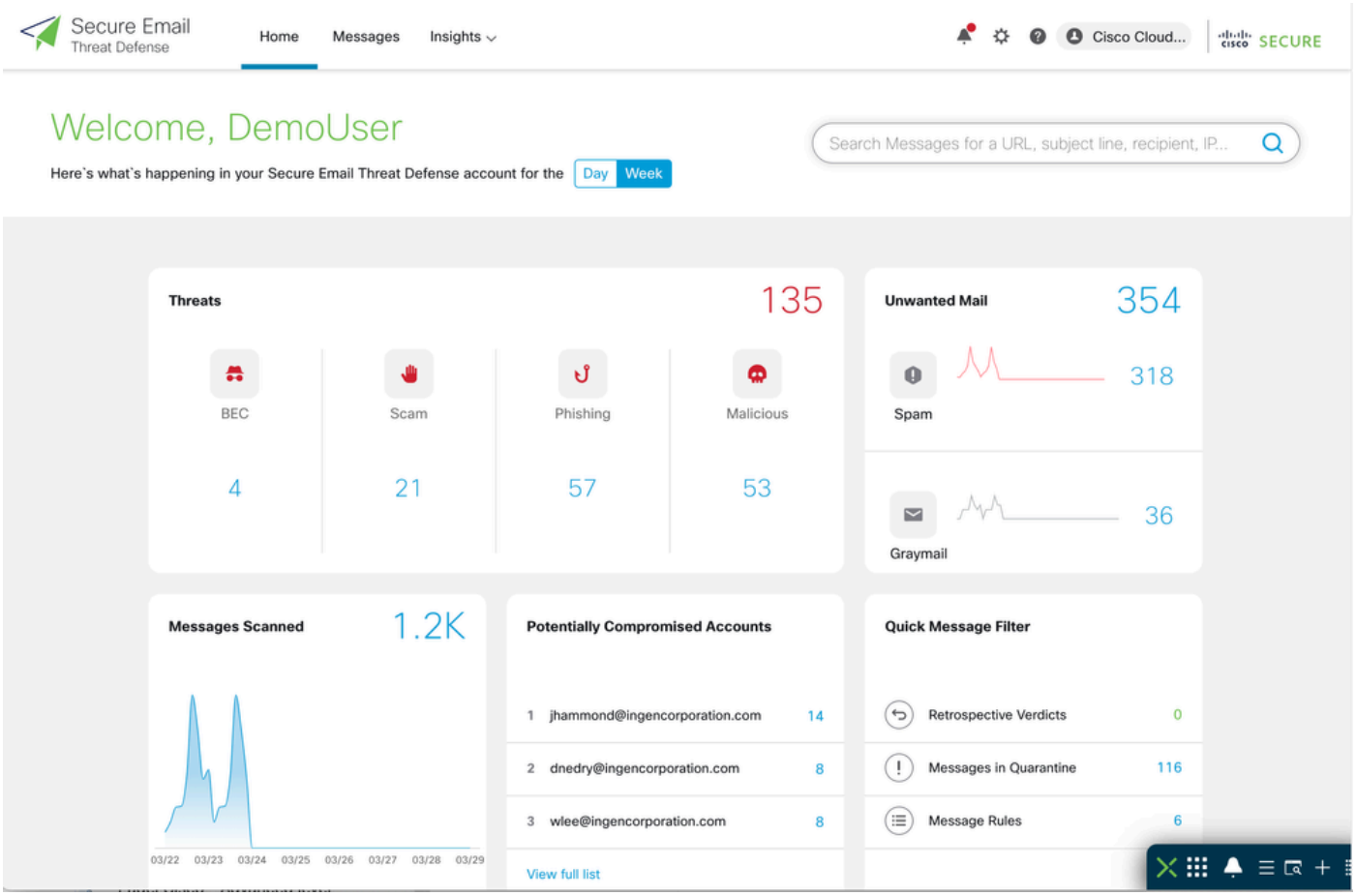
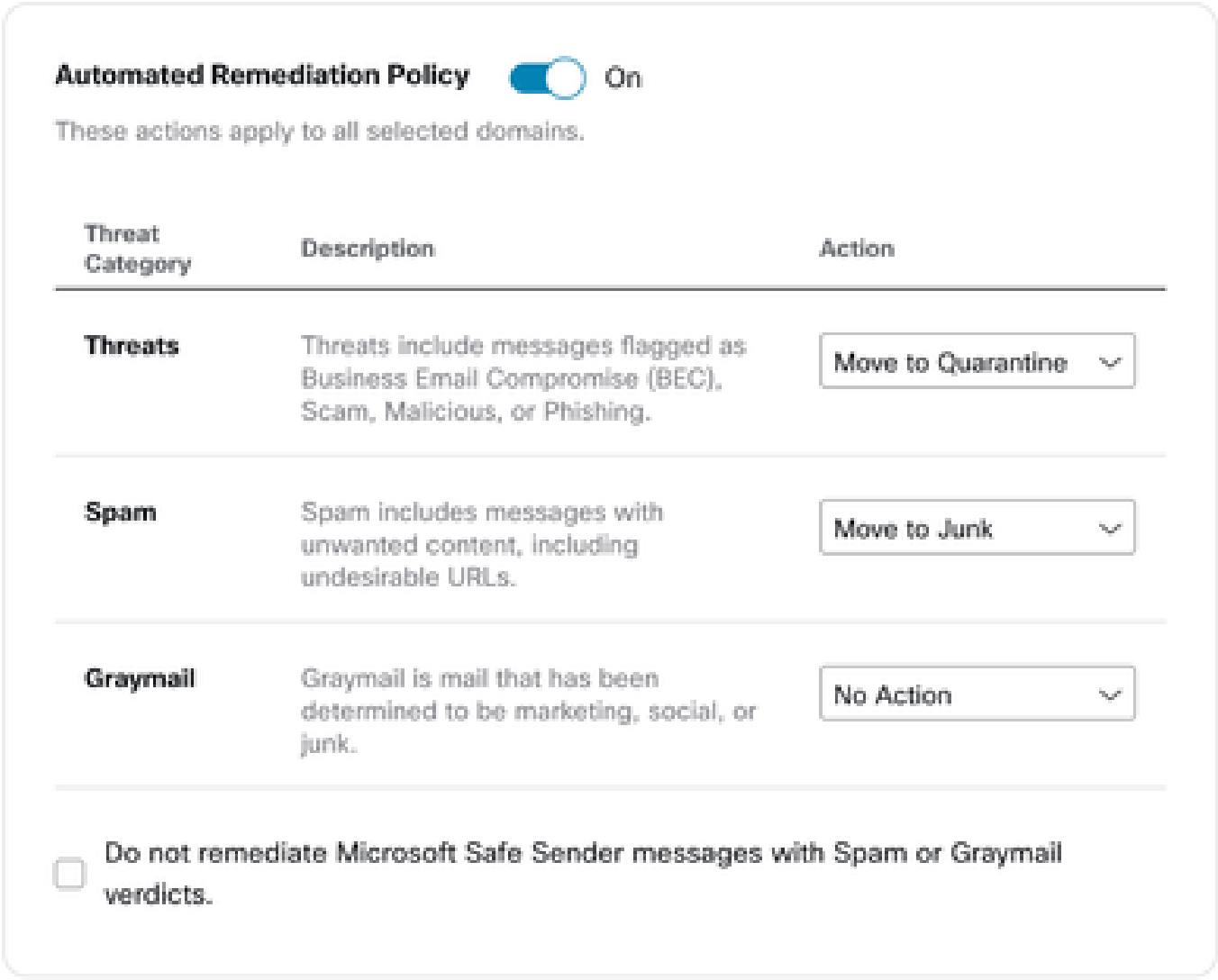


Image 15. Le paramètre de stratégie Cisco Email Threat Defense détermine automatiquement si le message correspond à la catégorie de menace sélectionnée



Que pouvez-vous faire de plus avec la prévention contre l'usurpation

De nombreuses usurpations peuvent être corrigées avec quelques précautions simples qui incluent, sans s'y limiter :

- Limitez l'accès aux domaines répertoriés dans la table d'accès aux hôtes (HAT) à un très petit nombre de partenaires commerciaux.
- Suivez et mettez à jour en permanence les membres du groupe d'expéditeurs SPOOF_ALLOW si vous en avez créé un et suivez les instructions du lien Méthodes conseillées.
- Activez la détection de messages gris et placez-les également dans la quarantaine du spam.

Mais plus important encore, activez SPF, DKIM et DMARC et mettez-les en oeuvre de manière appropriée. Cependant, les directives sur la publication des enregistrements SPF, DKIM et DMARC sortent du cadre de ce document. Pour cela, reportez-vous au livre blanc suivant : Meilleures pratiques d'authentification des e-mails : méthodes optimales de déploiement de SPF, DKIM et DMARC.

Comprendre le défi que représente la résolution des attaques par e-mail telles que les campagnes d'usurpation d'identité décrites ici. Si vous avez des questions sur la mise en oeuvre de ces meilleures pratiques, contactez l'assistance technique Cisco et créez un dossier. Vous pouvez également contacter votre équipe de compte Cisco pour obtenir des conseils sur la solution et la conception. Pour plus d'informations sur Cisco Secure Email, consultez le site Web Cisco Secure Email.

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.