Configurer la passerelle de messagerie sécurisée pour utiliser la quarantaine Microsoft et la notification de quarantaine Microsoft

Table des matières

Introduction

Ce document décrit les étapes de configuration requises pour intégrer Cisco Secure Email (CES) à la quarantaine Microsoft 365.

Aperçu

Dans une infrastructure de messagerie moderne, plusieurs couches de sécurité sont souvent mises en oeuvre, ce qui entraîne la mise en quarantaine des e-mails par différents systèmes. Pour rationaliser l'expérience utilisateur et améliorer la cohérence des notifications, il est avantageux de centraliser la gestion de la quarantaine sur une plate-forme unique. Ce guide explique comment rediriger les messages indésirables, tels que les courriers indésirables et les messages grisâtres, identifiés par Cisco CES vers la quarantaine des utilisateurs Microsoft 365.

Conditions préalables

Pour effectuer cette configuration, assurez-vous que vous disposez des éléments suivants :

1. Un locataire actif dans Cisco Secure Email Gateway
2. Un locataire actif dans Microsoft Exchange Online.
3. Accès aux services Microsoft 365 (O365)
4. Une licence Microsoft 365 Defender (requise pour configurer les stratégies de quarantaine et les notifications)

Configuration de Microsoft 365 (O365)

Commencez par configurer Microsoft 365 pour recevoir et gérer les messages mis en quarantaine.

Activer les notifications de quarantaine dans Microsoft Exchange en ligne

Vous pouvez vous reporter à la documentation officielle de Microsoft pour configurer les notifications utilisateur pour les messages mis en quarantaine :
Configuration de la notification de quarantaine Microsoft

Créer une règle de flux de messagerie

Une fois les notifications activées, configurez une règle qui redirige les messages marqués par Cisco Secure Email Gateway vers la quarantaine hébergée de Microsoft.

1. Ouvrez le Centre d'administration Microsoft Exchange.
2. Dans le menu de gauche, allez à Flux de messages → Règles.
3. Cliquez sur Add a rule, puis sélectionnez Create a new rule.
4. Définissez le nom de la règle sur : Règle de quarantaine CSE.
5. Sous Apply this rule if, sélectionnez The message header, puis choisissez matches text patterns.
6. Dans le nom de l'en-tête, saisissez : X-CSE-Quarantine, et définissez la valeur pour qu'elle corresponde : vrai.
7. Sous Effectuer les opérations suivantes, choisissez Rediriger le message vers, puis sélectionnez Quarantaine hébergée.
8. Enregistrez la configuration.
9. Après l'enregistrement, assurez-vous que la règle est activée.

Dans l'image, vous pouvez voir à quoi ressemble la règle.

CSE Quarantine

Edit rule conditions Edit rule settings

Status: Disabled

Enable or disable rule

Enabled

Updating the rule status, please wait...

Rule settings

Rule name
CSE Quarantine

Mode
Enforce

Severity
Not specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
1

For rule processing errors
Ignore

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Deliver the message to the hosted quarantine.

Rule comments

Règle Microsoft

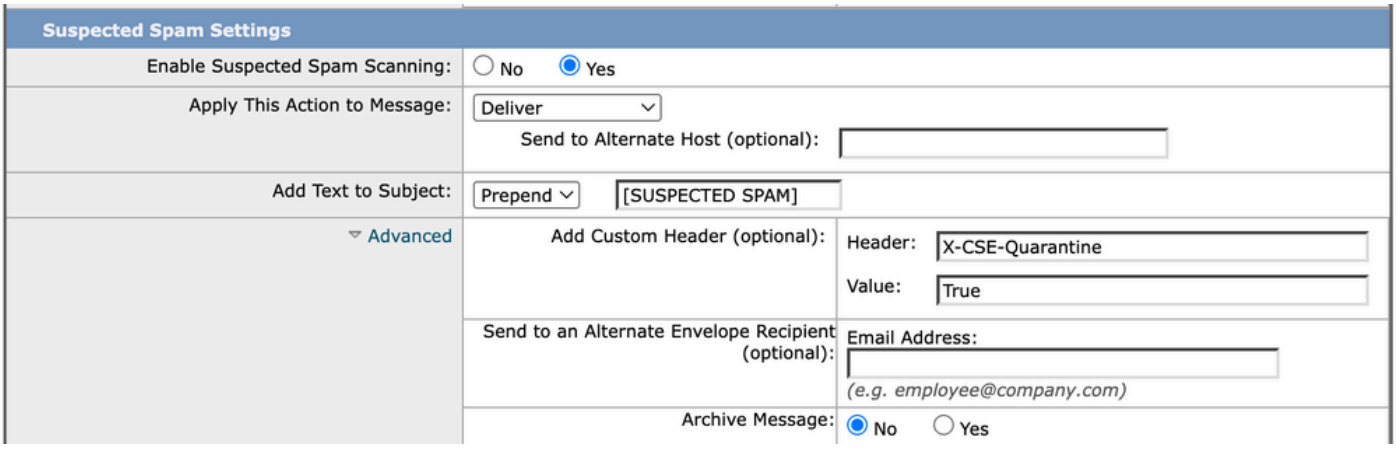
Configurer la messagerie sécurisée Cisco

Dans Cisco CES, vous pouvez ajouter un en-tête personnalisé (X-CSE-Quarantine : true) à tout message que nous souhaitons rediriger vers la quarantaine de Microsoft.

Ces messages peuvent être marqués par n'importe quel filtre ou moteur de contenu dans CES. Dans cet exemple, nous le configurons pour les messages de spam suspecté.

1. Ouvrez la console Cisco Secure Email Management.
2. Accédez à Politiques de messagerie → Politiques de messages entrants.
3. Modifiez les stratégies que vous souhaitez modifier (par exemple, sélectionnez la stratégie par défaut).
4. Cliquez sur les paramètres de spam pour la stratégie sélectionnée.
5. Sous Suspect Spam, remplacez l'action Quarantaine par Remettre.
6. Cliquez sur Avancé et ajoutez un en-tête personnalisé :
    - Nom d'en-tête : X-CSE-Quarantine
    - Valeur: true (même valeur utilisée dans la règle Microsoft)
7. Cliquez sur Submit, puis sur Commit Changes pour appliquer la configuration.

Dans l'image, vous pouvez voir à quoi ressemble la configuration.

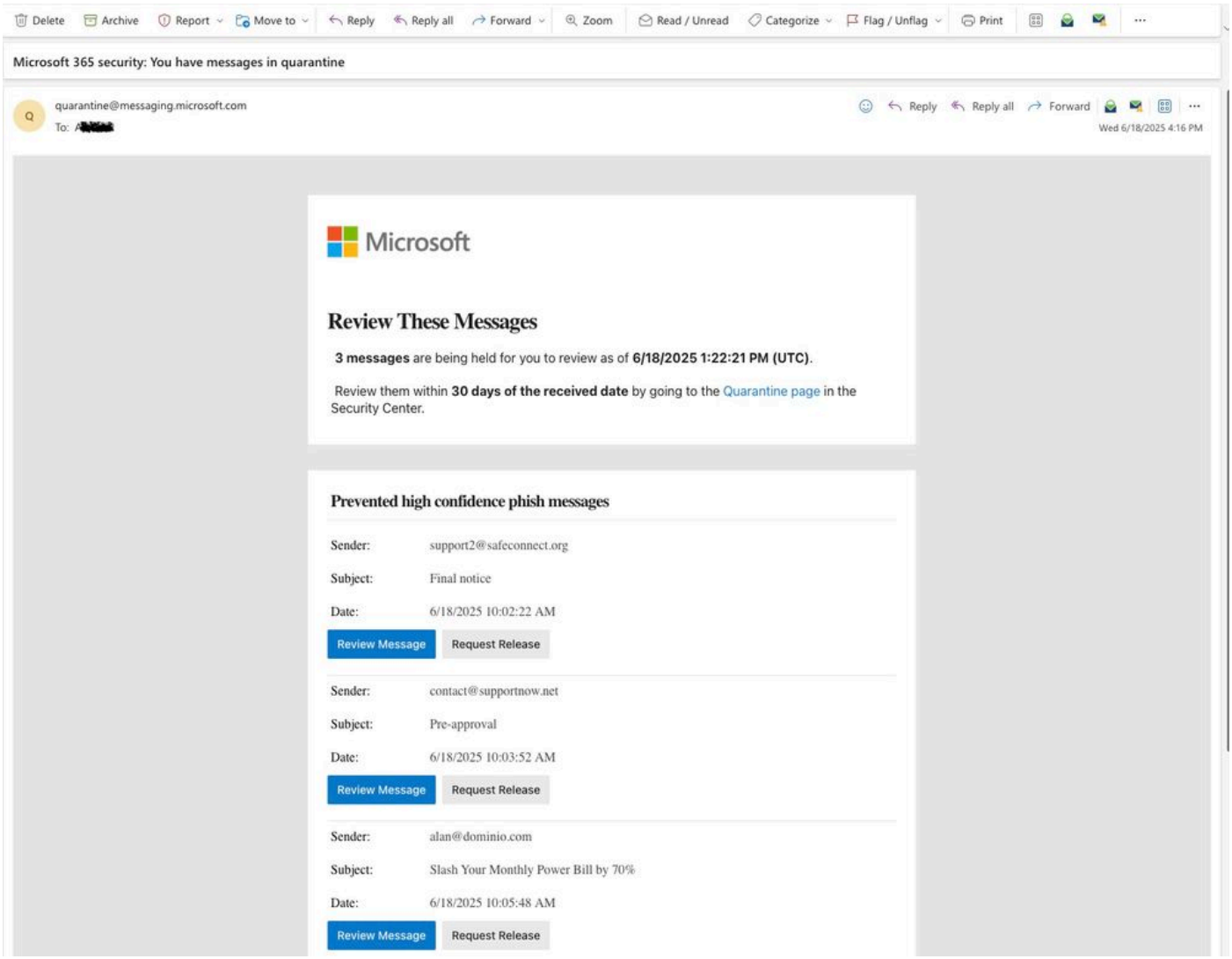


configuration CES

Vérifier

À partir de ce moment, les e-mails identifiés par Cisco CES comme des spams potentiels seront marqués avec l'en-tête personnalisé. Microsoft 365 détecte cette balise et redirige le message vers la quarantaine de l'utilisateur.

Les utilisateurs qui vont recevoir des notifications de quarantaine selon la configuration Microsoft 365.



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.