Comment corriger les e-mails à partir de CTR

Contenu

Introduction
Informations générales
Components Used
Configuration
Vérification
Étape 1. Accédez au portail CTR en fonction de l'accès aux serveurs disponibles et examinez
Étape 2. Examinez les messages transmis qui semblent malveillants ou dangereux à l'aide des observables pris en charge. Les observables peuvent être recherchés selon les critères suivants, comme l'illustre l'image :
2.1 Exemple d'enquête et d'enquête sur la PI ci-dessous, comme le montrent les images :
2.2 Voici ce que vous recevez dans votre boîte de réception avant que le message ne soit corrigé, comme l'illustre l'image :
2.3 En cliquant sur « ID de message Cisco », sélectionnez dans les options de menu l'une des actions résolues prises en charge, comme illustré dans l'image :
2.4 Dans cet exemple, « Initiate Forward » est sélectionné et une fenêtre contextuelle Success apparaît dans le coin inférieur droit, comme l'illustre l'image :
2.5 Dans l'ESA, vous pouvez voir les journaux suivants sous « mail_logs » qui montrent que la correction « CTR » démarre, l'action sélectionnée et l'état final.
2.6 L'instruction "[Message Remediated]" apparaît en avant-plan dans l'objet du message, comme l'illustre l'image :
2.7 L'adresse e-mail que vous saisissez lors de la configuration du module ESA/SMA est celle qui reçoit les e-mails corrigés lors de la sélection de l'option « Transfert » ou « Transfert/Suppression », comme illustré sur l'image :
2.8 Enfin, si vous regardez les détails du suivi des messages de la nouvelle interface du ESA/SMA, vous pouvez voir les mêmes journaux obtenus dans les « mail_logs » et « Last State » que « Remediated », comme le montre l'image :

Introduction

Ce document décrit comment corriger les e-mails provenant de Cisco Threat Response (CTR).

Informations générales

L'enquête CTR a été mise à jour pour prendre en charge la correction des messages à la demande. L'administrateur peut rechercher des e-mails spécifiques à partir de boîtes aux lettres utilisateur O365 et OnPrem Exchange et y remédier via un dispositif de sécurité de la messagerie électronique (ESA) ou un dispositif de gestion de la sécurité (SMA).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Compte CTR
- Cisco Security Services Exchange
- ESA AsycnOs 14.0.1-033

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.

> **Note**: La correction des recherches et des courriers est prise en charge dans les déploiements hybrides O365, Exchange 2016 et 2019 et dans les déploiements Exchange sur site 2013 uniquement.

Configuration

1. Configurer les paramètres de compte dans l'ESA
2. Configurer le profil chaîné et mapper le ou les domaines au profil de compte
3. Intégrer CTR à ESA ou SMA

Vérification

Vous pouvez rechercher les observables dans le portail CTR et sélectionner le message à corriger en procédant comme suit :

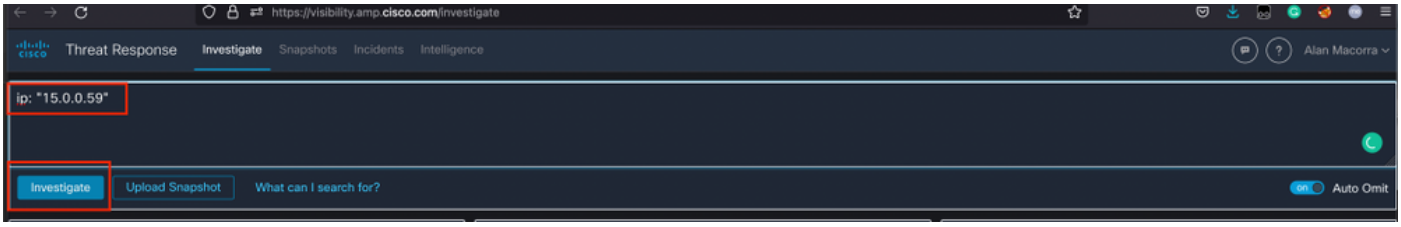
Étape 1. Accédez au portail CTR en fonction de l'accès aux serveurs disponibles et examinez

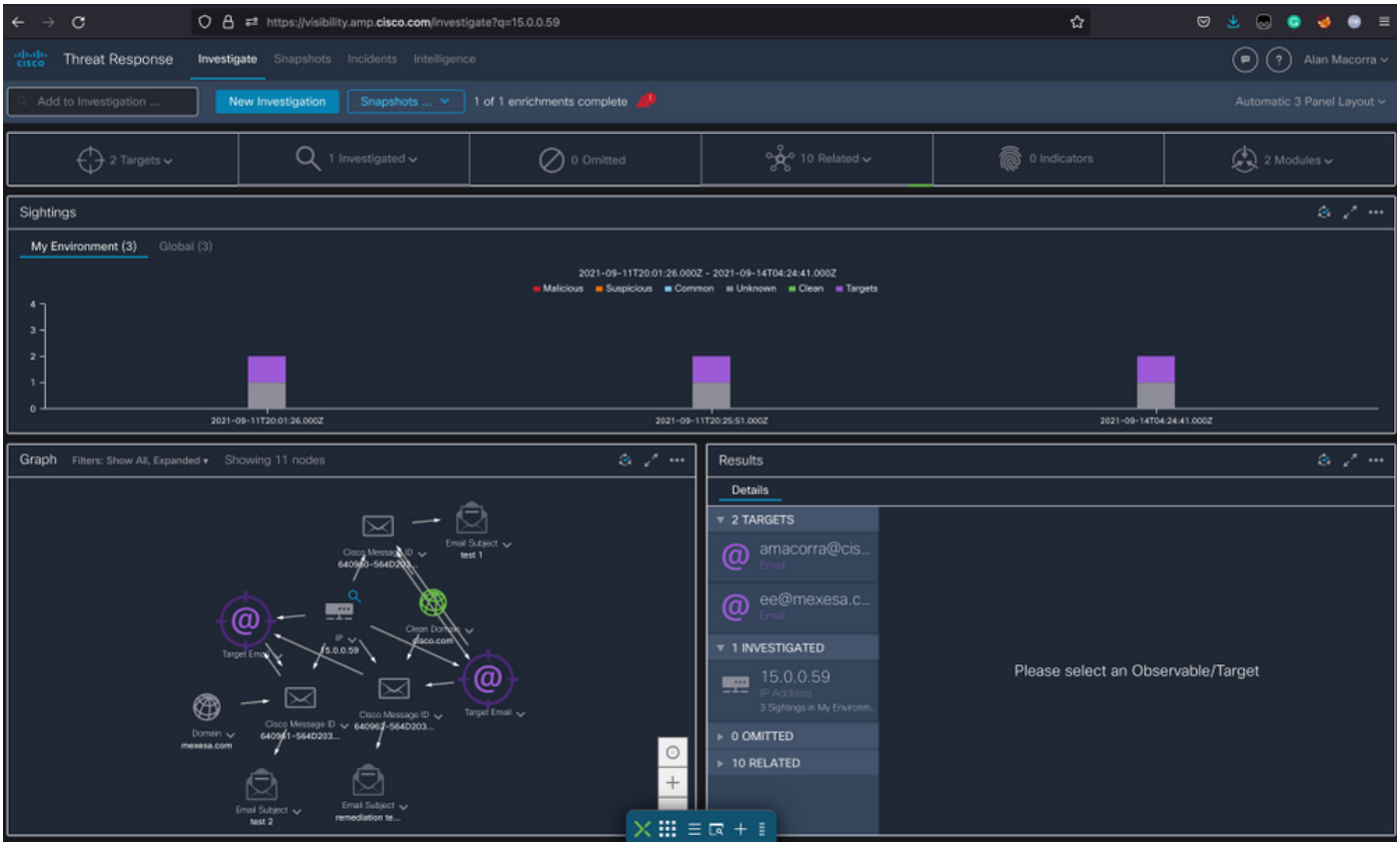
- États-Unis https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- UE https://visibility.eu.amp.cisco.com/investigate

Étape 2. Examinez les messages transmis qui semblent malveillants ou dangereux à l'aide des observables pris en charge. Les observables peuvent être recherchés selon les critères suivants, comme l'illustre l'image :

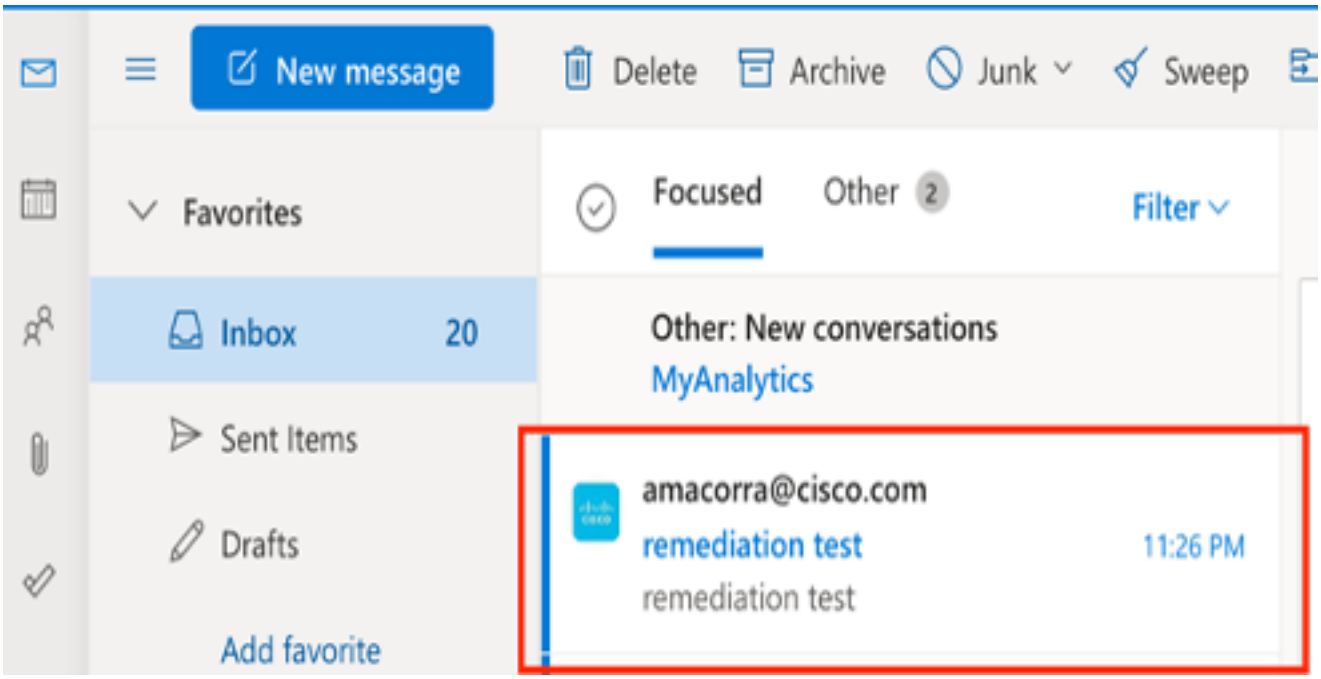
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

2.1 Exemple d'enquête et d'enquête sur la PI ci-dessous, comme le montrent les images :

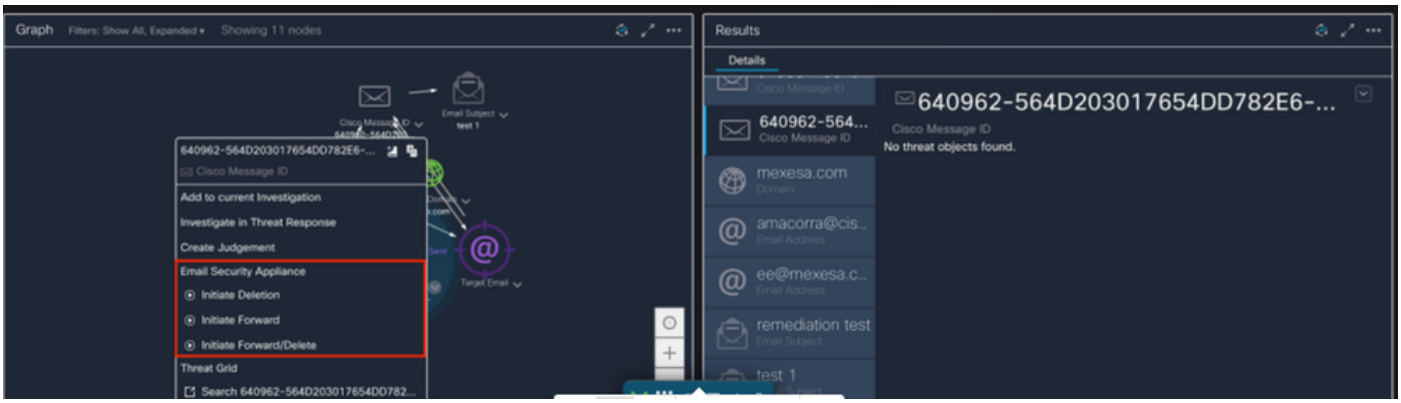




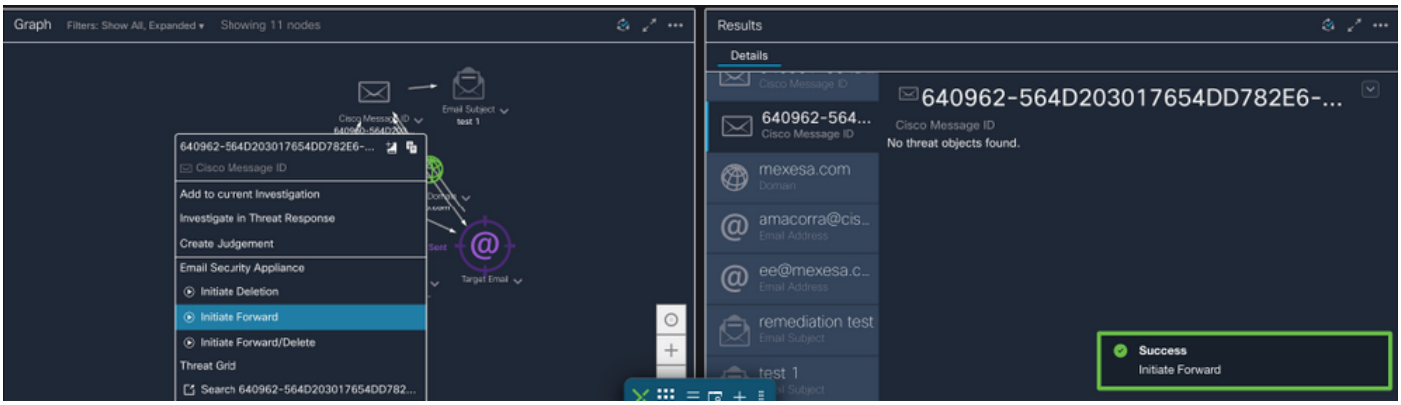
2.2 Voici ce que vous recevez dans votre boîte de réception avant que le message ne soit corrigé, comme l'illustre l'image :



2.3 En cliquant sur « ID de message Cisco », sélectionnez dans les options de menu l'une des actions résolues prises en charge, comme illustré dans l'image :



2.4 Dans cet exemple, « Initiate Forward » est sélectionné et une fenêtre contextuelle Success apparaît dans le coin inférieur droit, comme l'illustre l'image :

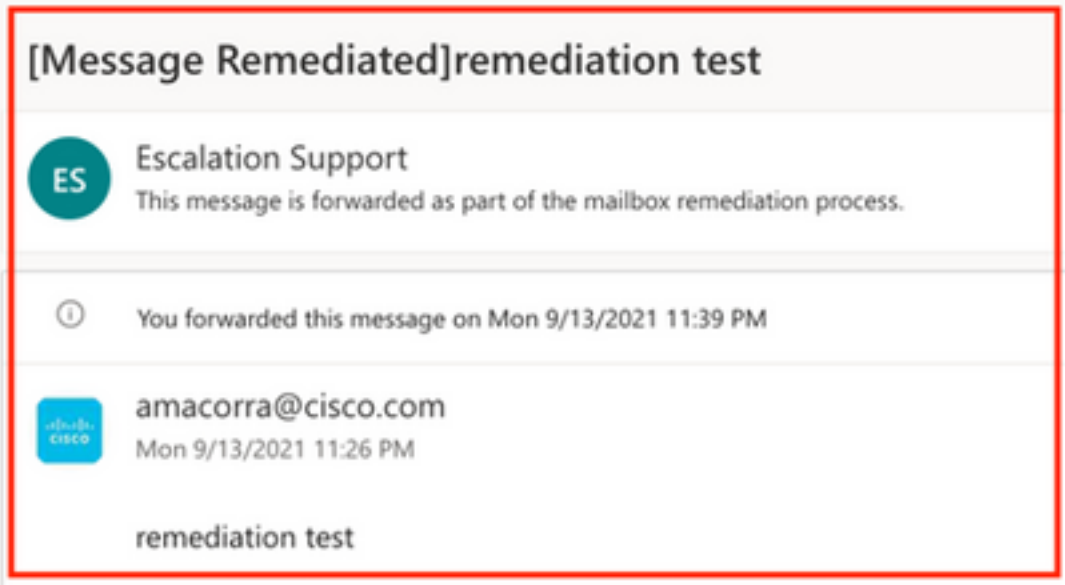


2.5 Dans l'ESA, vous pouvez voir les journaux suivants sous « mail_logs » qui montrent que la correction « CTR » démarre, l'action sélectionnée et l'état final.

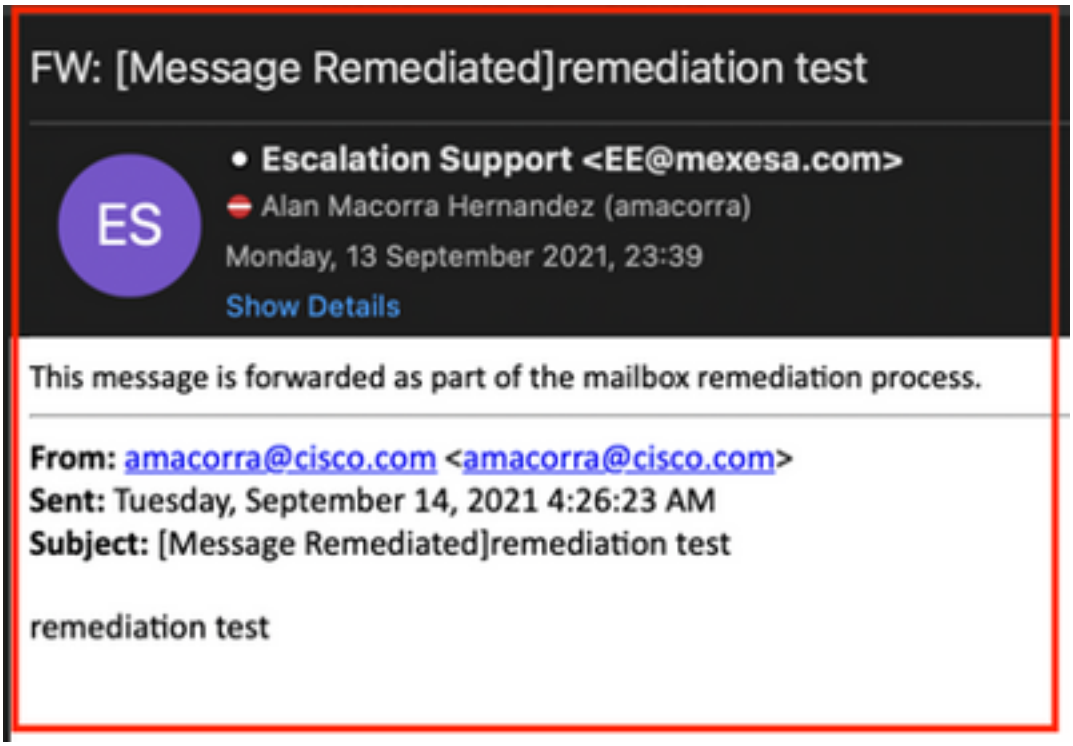
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for
recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'. Remediation status:
Remediated.
```

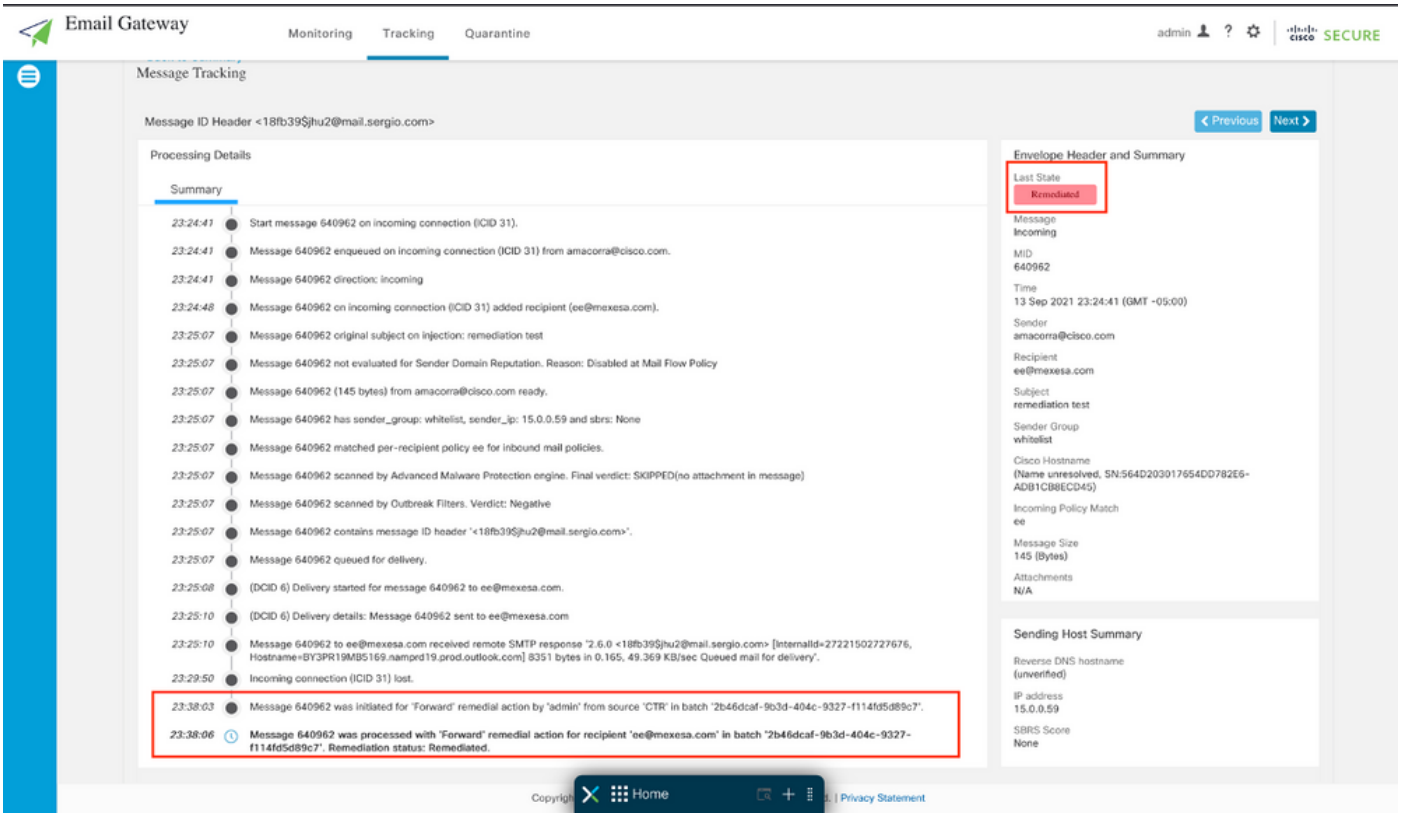
2.6 L'instruction "[Message Remediated]" apparaît en avant-plan dans l'objet du message, comme l'illustre l'image :



2.7 L'adresse e-mail que vous saisissez lors de la configuration du module ESA/SMA est celle qui reçoit les e-mails corrigés lors de la sélection de l'option « Transfert » ou « Transfert/Suppression », comme illustré sur l'image :



2.8 Enfin, si vous regardez les détails du suivi des messages de la nouvelle interface du ESA/SMA, vous pouvez voir les mêmes journaux obtenus dans les « mail_logs » et « Last State » que « Remediated », comme le montre l'image :



Note: Plusieurs correctifs peuvent se produire, si vous configurez dans votre ESA/SMA la fonctionnalité à rechercher et à corriger, vous pouvez corriger le même message à partir de CTR et aussi de ESA/SMA. Cela peut vous permettre de transférer le même message à une adresse de messagerie différente de celle configurée dans le module d'intégration.