CTRからの電子メールの修復方法

内容

概要

このドキュメントでは、Cisco Threat Response(CTR)から電子メールを修復する方法について説明します。

背景説明

CTR調査は、オンデマンドメール修復をサポートするように更新されています。管理者は、O365およびOnPrem Exchangeのユーザメールボックスから特定の電子メールを検索し、Eメールセキュリティアプライアンス(ESA)またはセキュリティ管理アプライアンス(SMA)を介してそれらを修復できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CTRアカウント
- Cisco Security Services Exchange
- ESA AsycnOs 14.0.1-033

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

> **注**：検索とメールの修復は、O365、Exchange 2016および2019ハイブリッド展開、およびオンプレミスの2013 Exchange展開でのみサポートされます。

設定

1. ESAでのアカウント設定
2. チェーンプロファイルの設定とドメインのアカウントプロファイルへのマッピング
3. CTRをESAまたはSMAと統合

確認

CTRポータルで回答を調査し、次の手順を使用して修復のメッセージを選択できます。

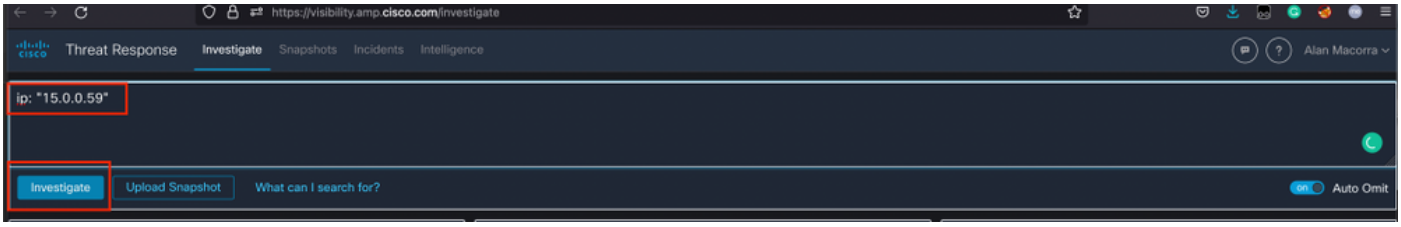
ステップ1：使用可能なサーバへのアクセスに基づいてCTRポータルにアクセスし、

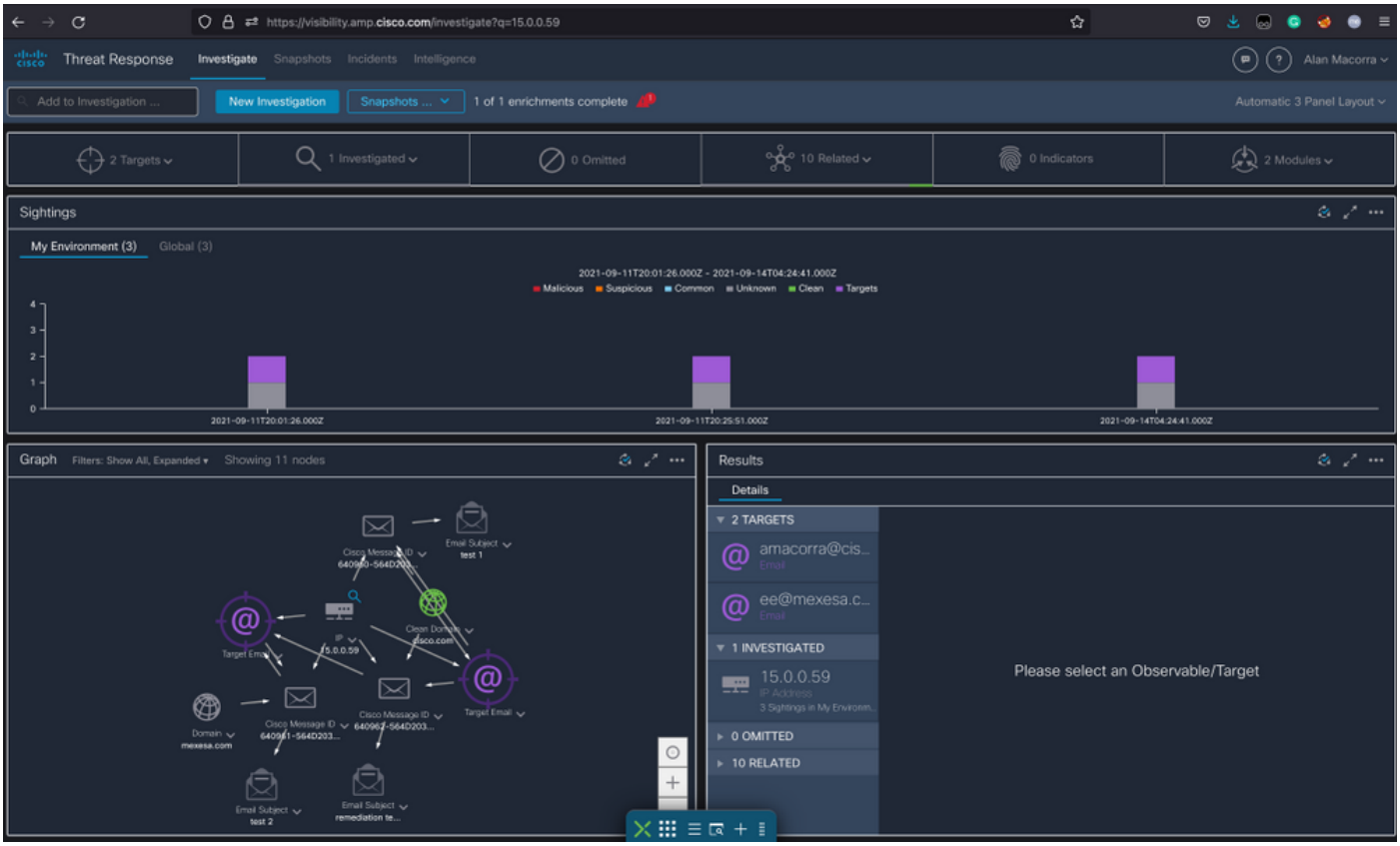
- 米国https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- EU https://visibility.eu.amp.cisco.com/investigate

ステップ2：サポートされている回答を使用して、悪意のあるメッセージや脅威と思われるメッセージを調査します。回答は、図に示すように、次の基準で検索できます。

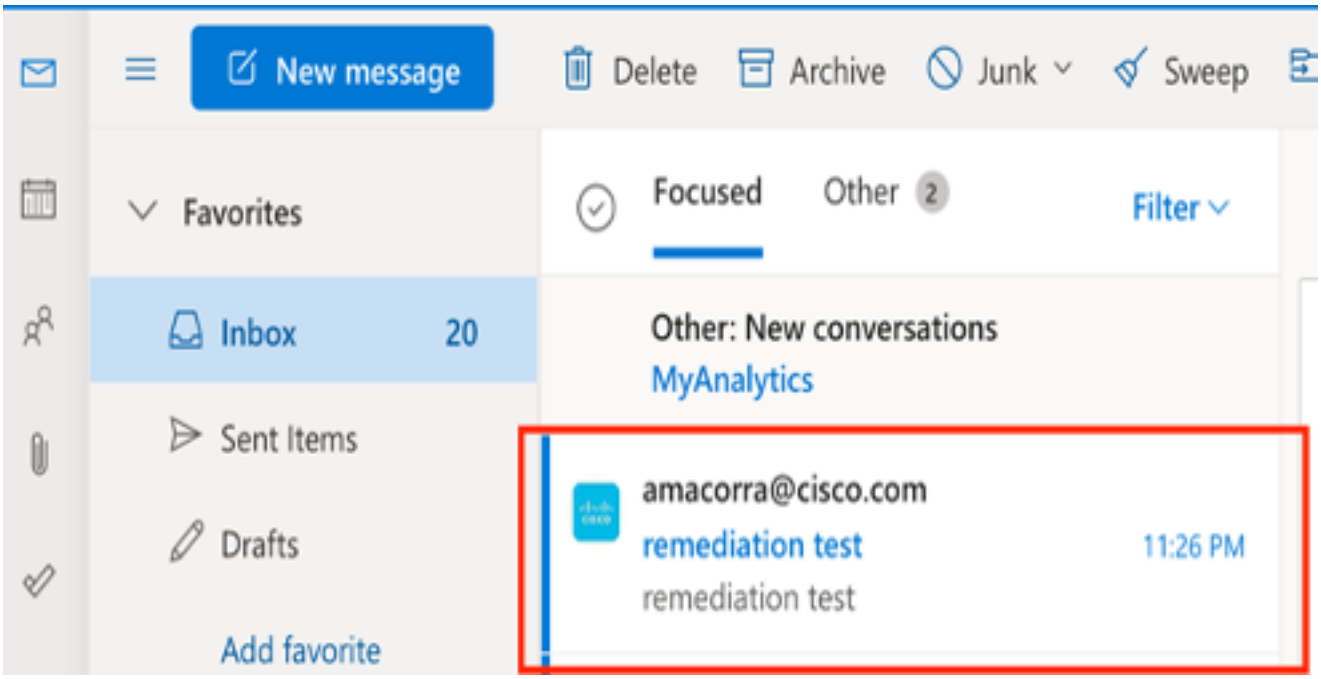
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

2.1次の図に示すように、IP調査と調査の例を示します。

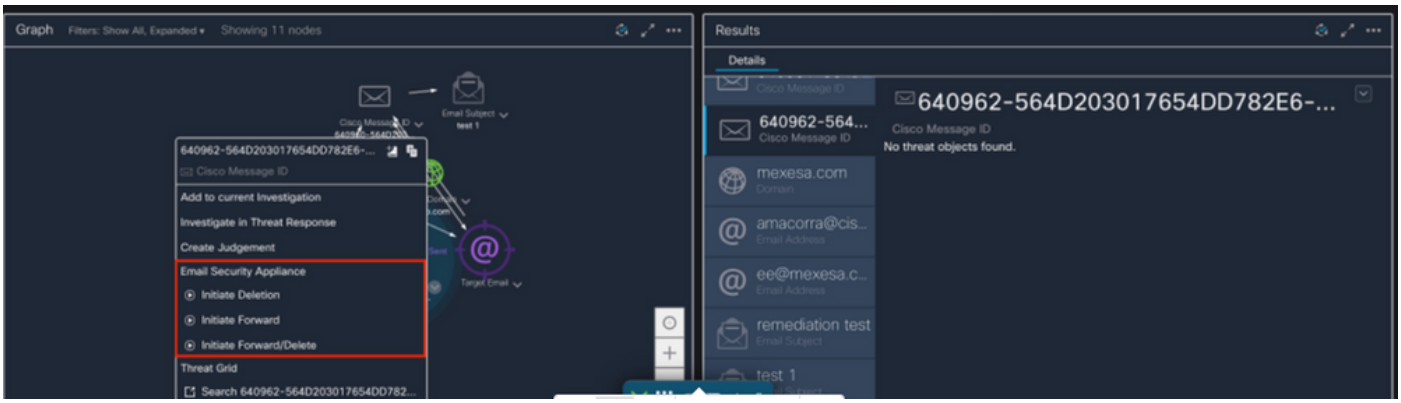




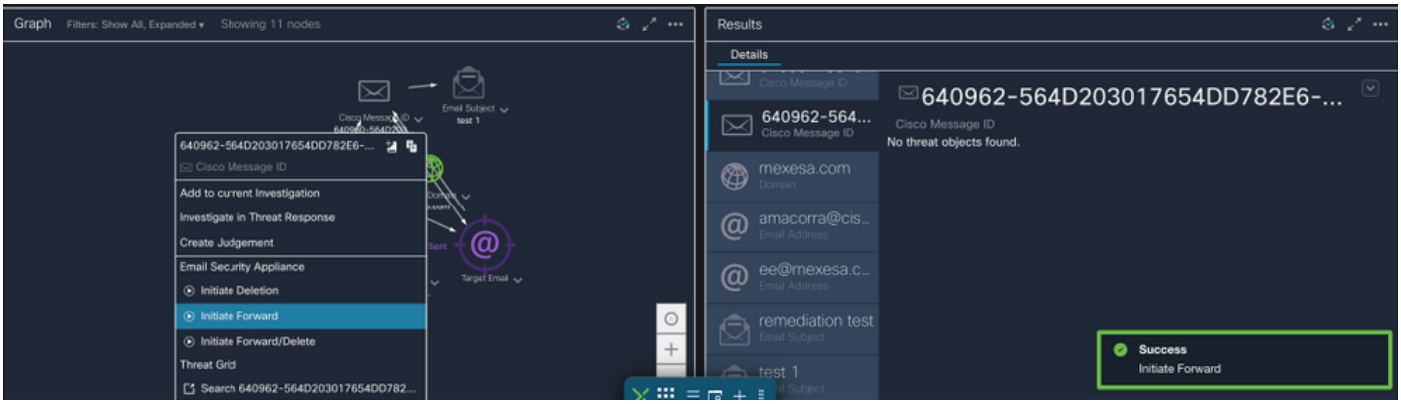
2.2次の図に示すように、メッセージが修復される前に受信トレイに表示されるものは次のとおりです。



2.3 [Cisco Message ID (シスコメッセージID)]をクリックし、次の図に示すように、サポートされている修復アクションのいずれかをメニューオプションから選択します。



2.4この例では、「Initiate Forward」が選択され、図に示すように、右下隅にSuccessポップアップウィンドウが表示されます。

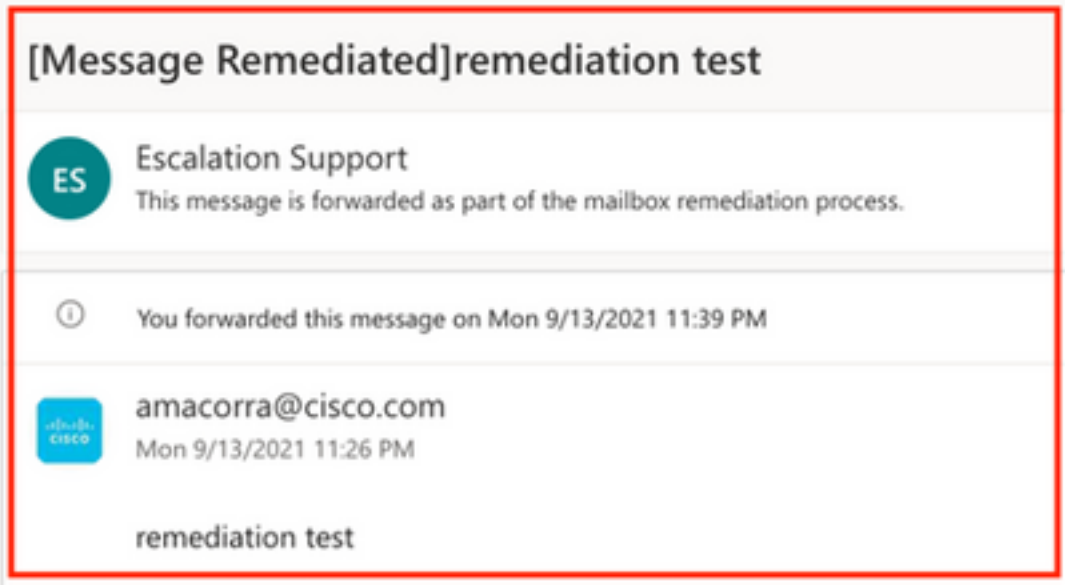


2.5 ESAでは、「mail_logs」の下に、「CTR」修復が開始したこと、選択されたアクション、および最終ステータスを示す次のログが表示されます。

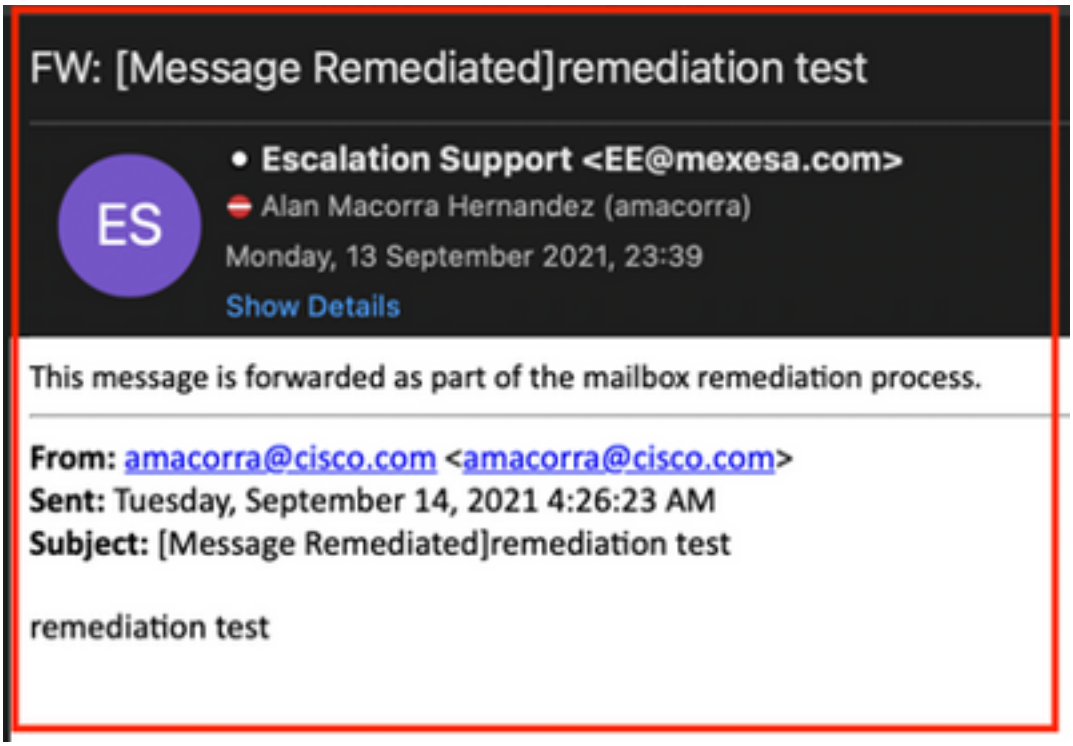
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

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.
```

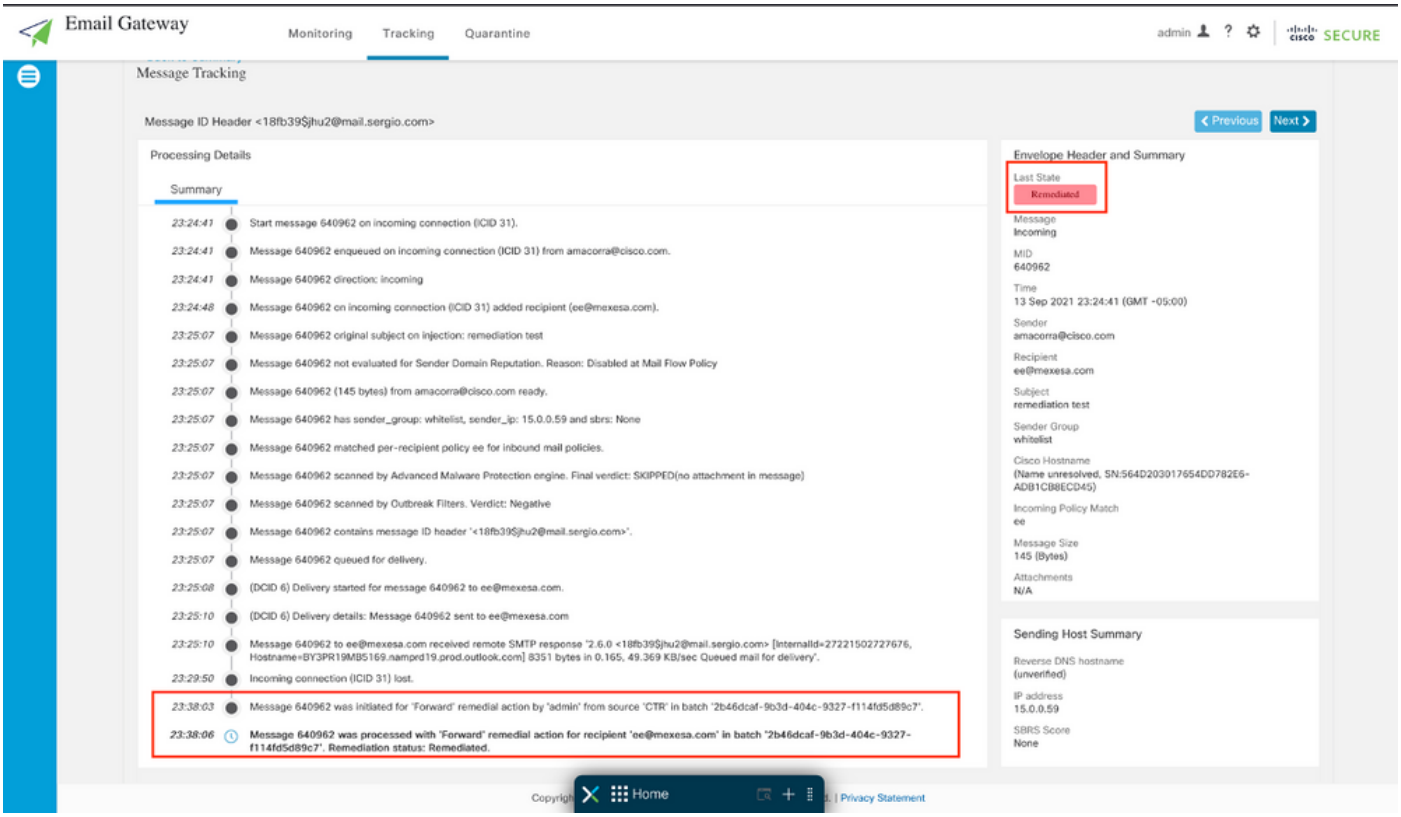
2.6図に示すように、メッセージの件名の前に「[Message Remediated]」という文が表示されます。



2.7 ESA/SMAモジュールを設定するときに入力する電子メールアドレスは、「転送」または「転送/削除」オプションを選択したときに修復された電子メールを受信する電子メールアドレスです（図を参照）。



2.8最後に、ESA/SMAの新しいインターフェイスのメッセージトラッキングの詳細を見ると、図に示すように、「mail_logs」と「Last State」で取得したものと同じログが「Remediated」として表示されます。



注：ESA/SMAで検索と修復の機能を設定すると、CTRとESA/SMAから同じメッセージを修復できます。これにより、統合モジュールで設定した電子メールアドレスとは異なる電子メールアドレスに同じメッセージを転送できます。