如何修正來自CTR的電子郵件

目錄

簡介
背景資訊
採用元件
設定
驗證
步驟1.根據訪問可用伺服器的情況訪問CTR門戶並進行調查
步驟2.使用支援的觀察量調檢視似惡意或威脅的已傳送郵件。可觀察量可以通過以下標準進行搜尋，如圖所示：
2.1以下IP調查和調查的示例，如下圖所示：
2.2以下是在郵件補救之前您收件箱中獲得的內容，如下圖所示：
2.3按一下「Cisco Message ID」（思科消息ID）後，從選單選項中選擇任何支援的修正操作，如下圖所示：
2.4在本例中，「Initiate Forward」被選中，並在右下角出現「Success」彈出視窗，如下圖所示：
2.5在ESA中，您可以看到「mail_logs」下的以下日誌，其中顯示「CTR」補救已啟動、已選擇的操作和最終狀態。
2.6語句「[Message Remediated]」顯示在消息主題的前面，如下圖所示：
2.7在配置ESA/SMA模組時鍵入的電子郵件地址是在選擇「轉發」或「轉發/刪除」選項時接收修正電子郵件的地址，如下圖所示：
2.8最後，如果您檢視ESA/SMA新介面的郵件跟蹤詳細資訊，您會看到「mail_logs」和「Last State」中獲取的日誌與「Remediated」相同，如下圖所示：

簡介

本文說明如何修正來自思科威脅回應(CTR)的電子郵件。

背景資訊

已更新CTR調查以支援按需郵件補救。管理員可以搜尋來自O365和OnPrem Exchange使用者郵箱的特定電子郵件，並通過郵件安全裝置(ESA)或安全管理裝置(SMA)對其進行補救。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CTR帳戶
- 思科安全服務交換
- ESA AsycnOs 14.0.1-033

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

附註：僅支援O365、Exchange 2016和2019混合部署以及本地2013 Exchange部署中的搜尋和郵件補救。

設定

1. 在ESA中配置帳戶設定
2. 配置鏈結配置檔案並將域對映到帳戶配置檔案
3. 將CTR與ESA或SMA整合

驗證

您可以調查CTR門戶中的可觀察量，並使用以下步驟選擇用於補救的消息：

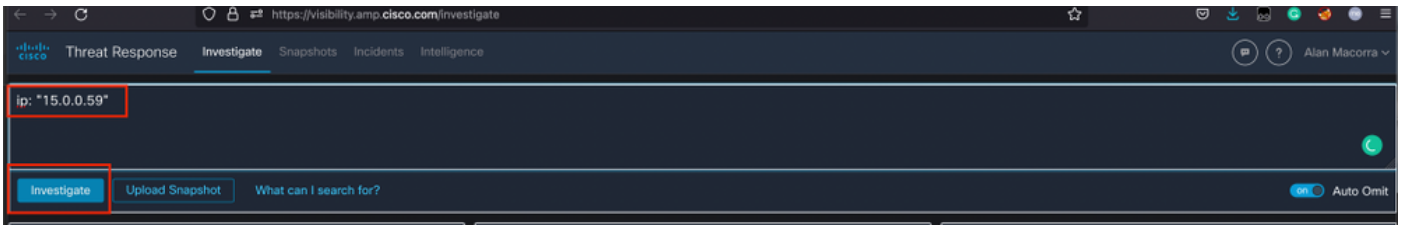
步驟1.根據訪問可用伺服器的情況訪問CTR門戶並進行調查

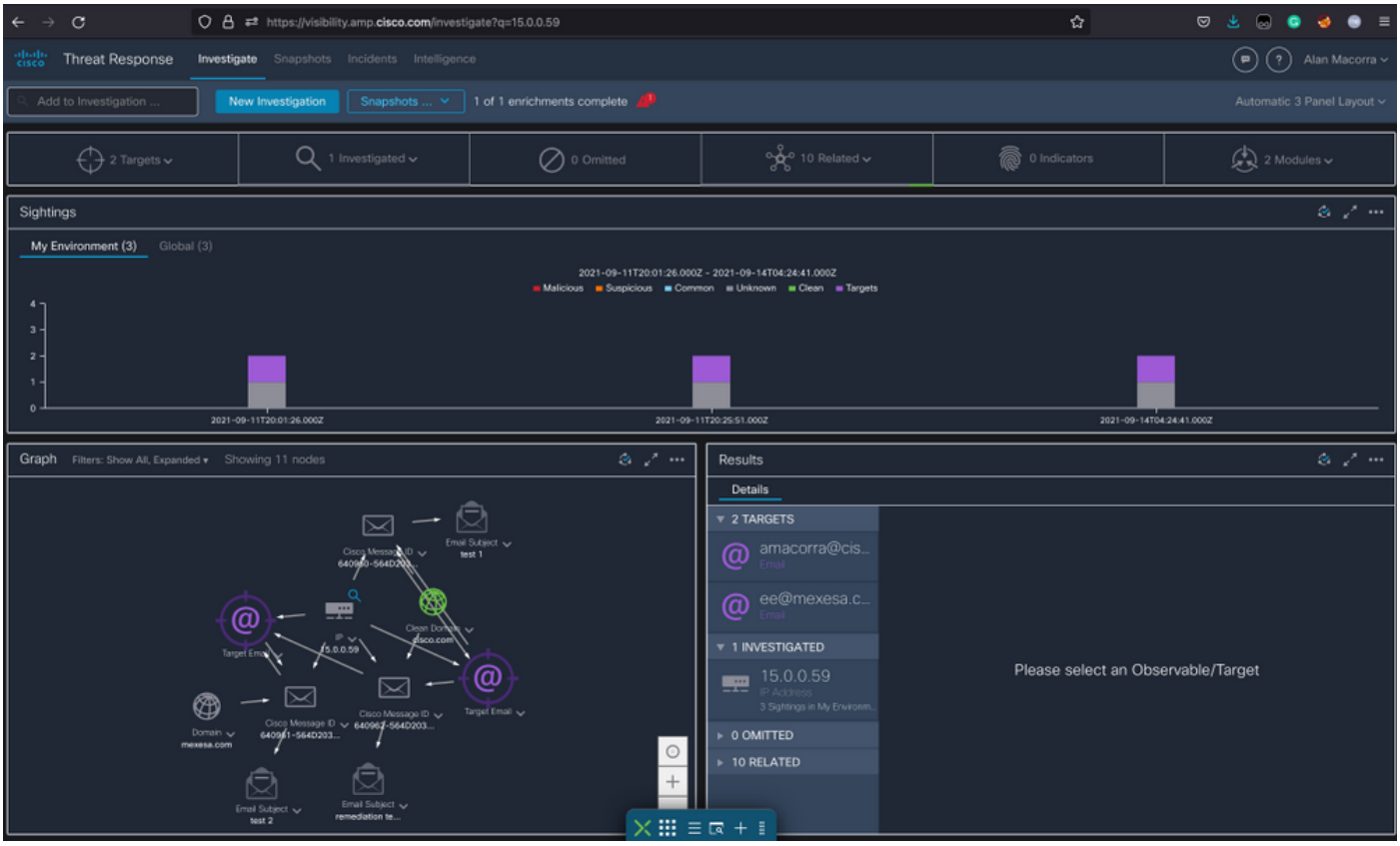
- US https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- 歐盟https://visibility.eu.amp.cisco.com/investigate

步驟2.使用支援的觀察量調檢視似惡意或威脅的已傳送郵件。可觀察量可以通過以下標準進行搜尋，如圖所示：

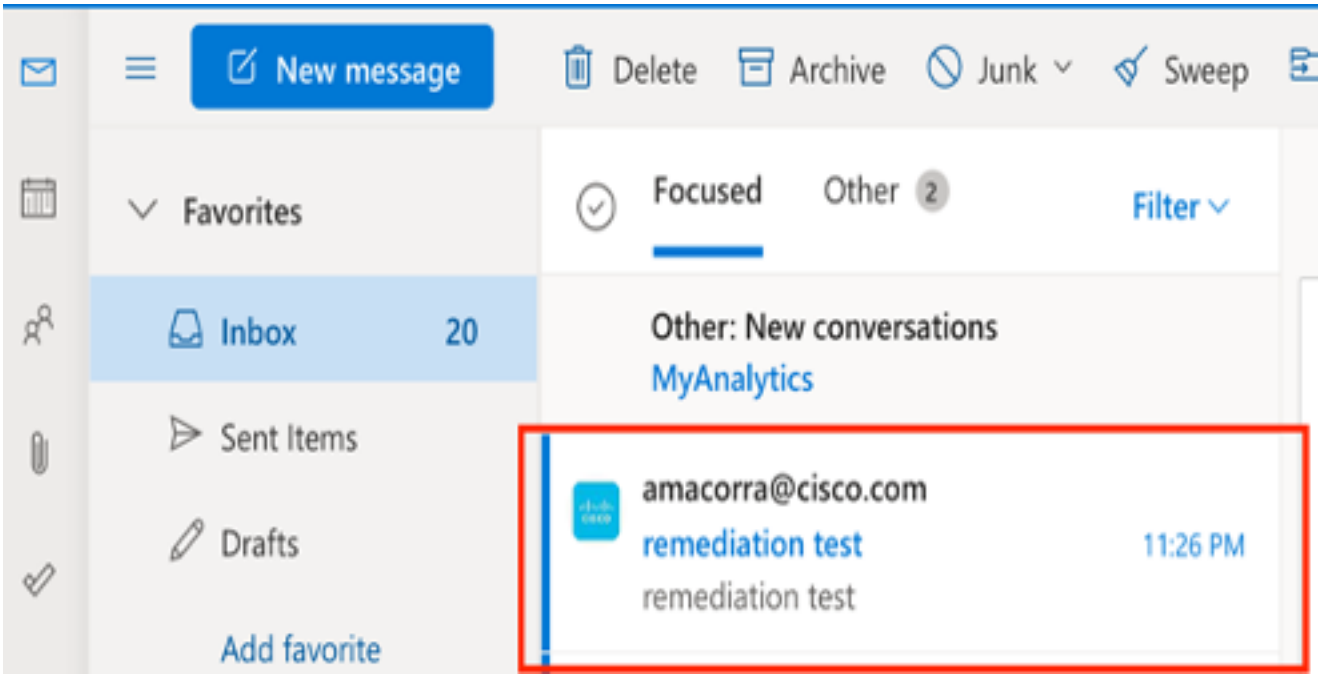
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

2.1以下IP調查和調查的示例，如下圖所示：

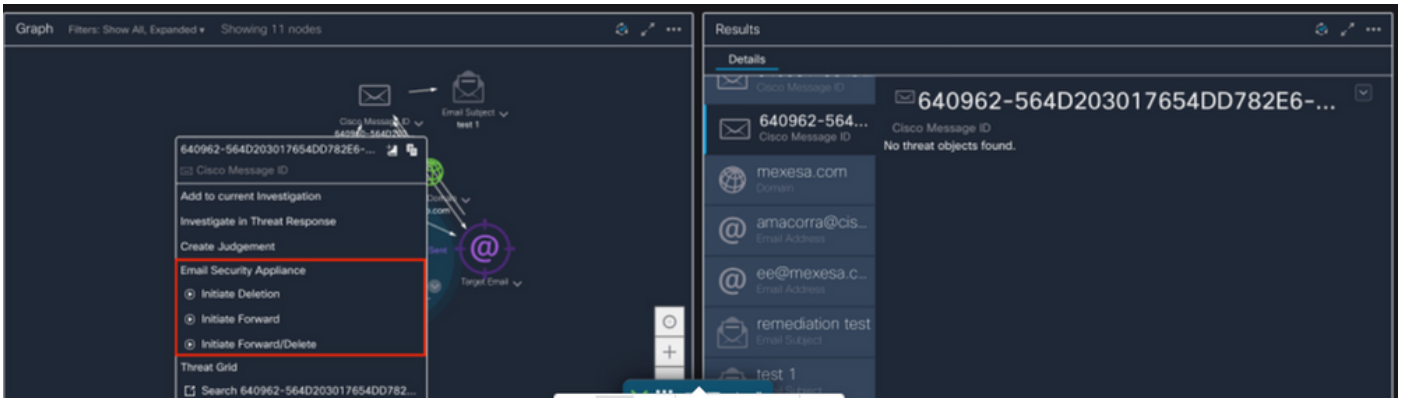




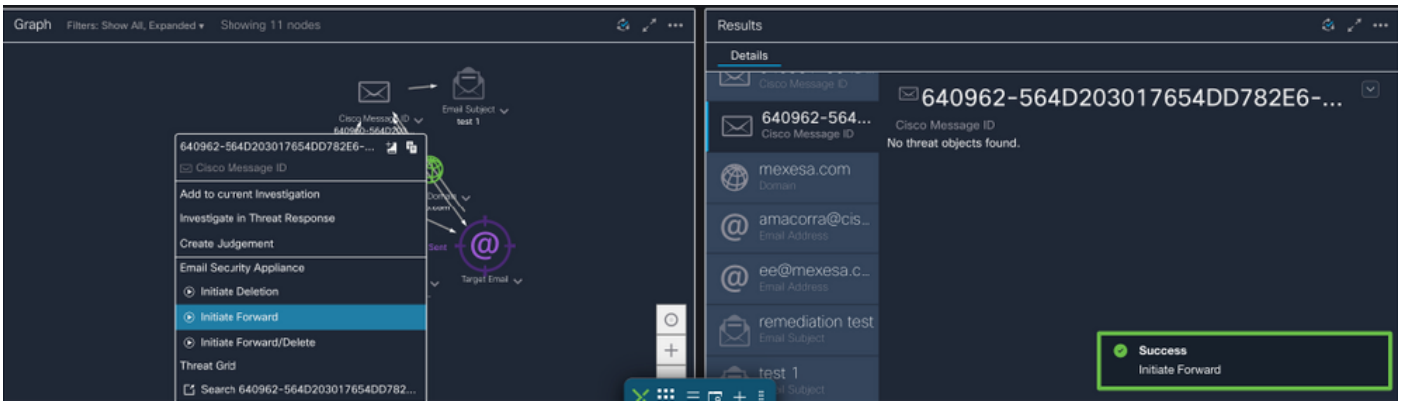
2.2以下是在郵件補救之前您收件箱中獲得的內容，如下圖所示：



2.3按一下「Cisco Message ID」（思科消息ID）後，從選單選項中選擇任何支援的修正操作，如下圖所示：



2.4在本例中，「Initiate Forward」被選中，並在右下角出現「Success」彈出視窗，如下圖所示：

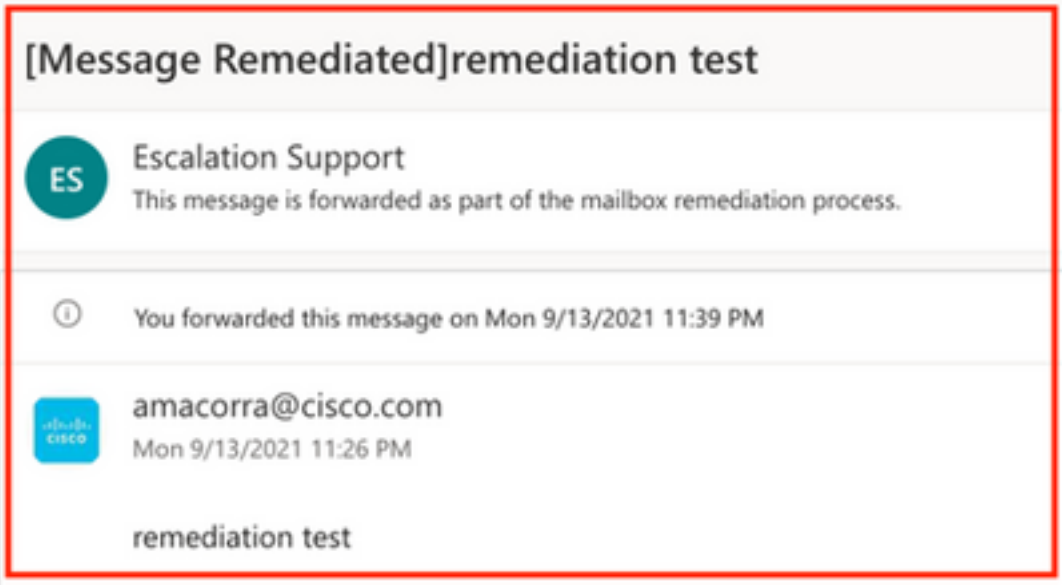


2.5在ESA中，您可以看到「mail_logs」下的以下日誌，其中顯示「CTR」補救已啟動、已選擇的操作和最終狀態。

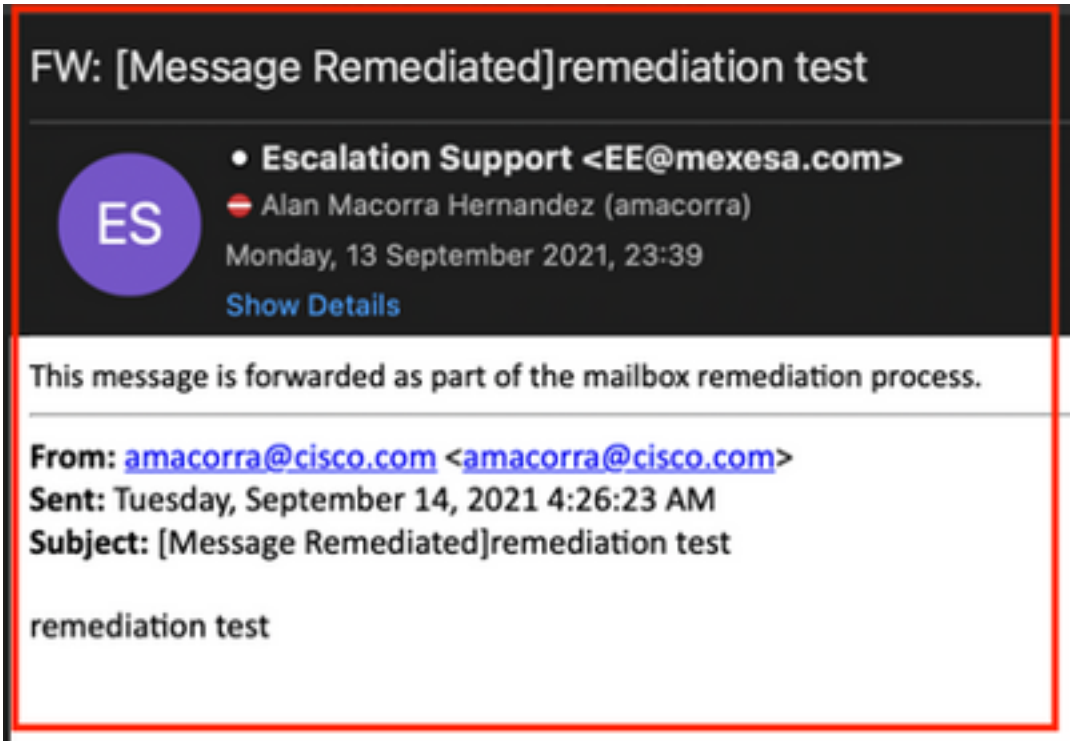
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

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.
```

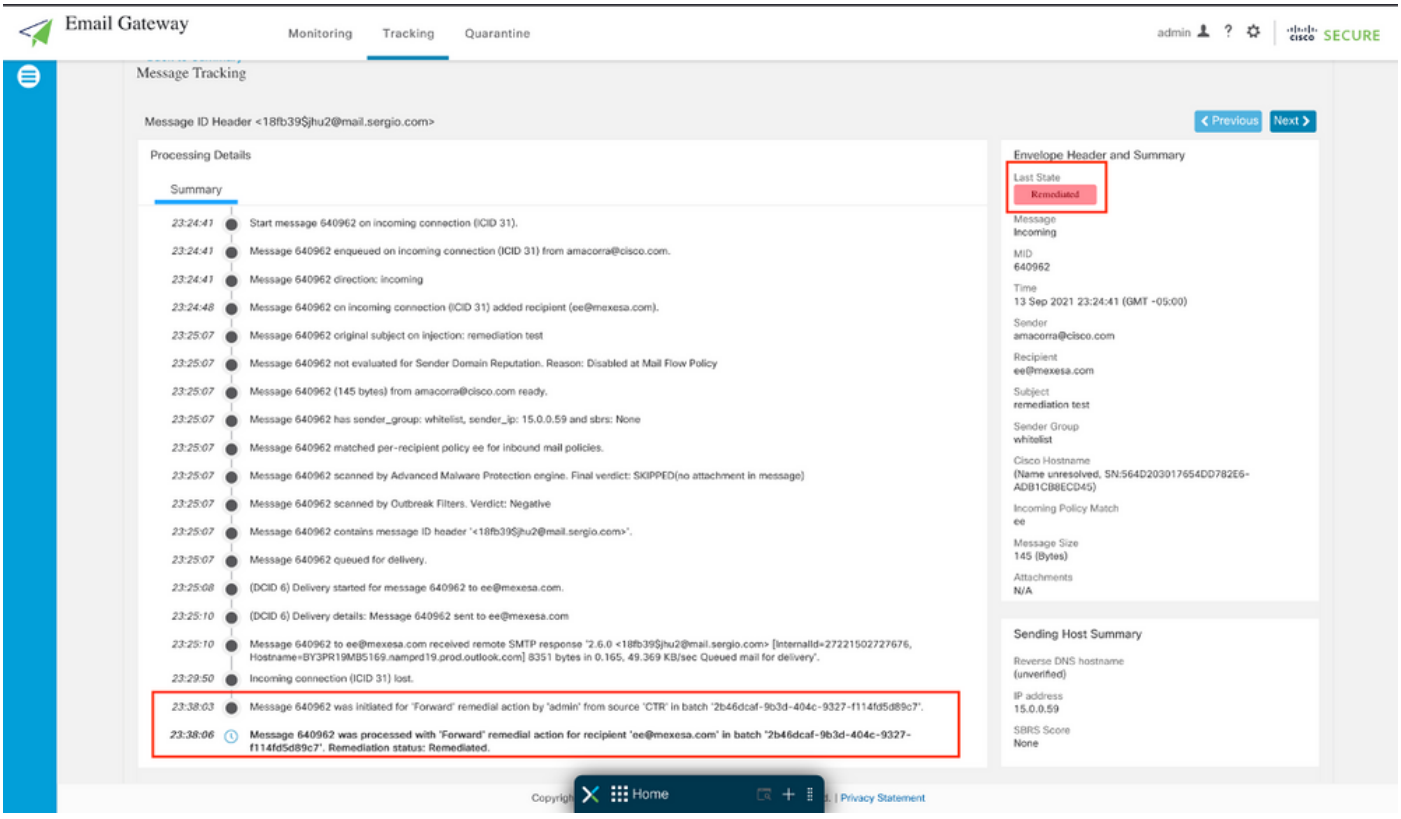
2.6語句「[Message Remediated]」顯示在消息主題的前面，如下圖所示：



2.7在配置ESA/SMA模組時鍵入的電子郵件地址是在選擇「轉發」或「轉發/刪除」選項時接收修正電子郵件的地址，如下圖所示：



2.8最後，如果您檢視ESA/SMA新介面的郵件跟蹤詳細資訊，您會看到「mail_logs」和「Last State」中獲取的日誌與「Remediated」相同，如下圖所示：



附註：可能會發生多個補救，如果您在ESA/SMA中配置搜尋和補救功能，則可以從CTR和ESA/SMA補救同一消息。這允許您將同一郵件轉發到與整合模組中配置的郵件地址不同的郵件地址。