CTR에서 이메일을 수정하는 방법

목차

소개
배경 정보
사용되는 구성 요소
구성
확인
1단계. 사용 가능한 서버에 대한 액세스를 기반으로 CTR 포털에 액세스하고
2단계. 지원되는 관찰 가능한 개체를 사용하여 악의적이거나 위협인 것으로 보이는 전달된 메시지를 조사합니다. 이미지에 표시된 대로 다음 기준에 따라 관찰 가능 항목을 검색할 수 있습니다.
2.1 아래 이미지에 표시된 IP 조사 및 조사의 예:
2.2 메시지에 표시된 것처럼 메시지가 수정되기 전에 받은 편지함에 표시되는 내용은 다음과 같습니다.
2.3 "Cisco Message ID(Cisco 메시지 ID)"를 클릭한 다음, 이미지에 표시된 대로 지원되는 교정 작업 중 하나를 메뉴 옵션에서 선택합니다.
2.4 이 예에서는 "Initiate Forward(착신 전환 시작)"가 선택되고 이미지에 표시된 것처럼 오른쪽 하단 모서리에 Success(성공) 팝업 창이 나타납니다.
2.5 ESA의 "mail_logs" 아래에 "CTR" 교정이 시작되며 선택한 작업 및 최종 상태가 표시되는 다음 로그가 표시됩니다.
2.6 메시지 제목 앞에 "[Message Remediated]"라는 문장이 나타납니다(이미지에 표시됨).
2.7 ESA/SMA 모듈을 구성할 때 입력하는 이메일 주소는 이미지에 표시된 대로 "Forward(전달)" 또는 "Forward/Delete(전달/삭제)" 옵션을 선택할 때 교정 이메일을 수신하는 이메일 주소입니다.
2.8 마지막으로, ESA/SMA의 새 인터페이스에 대한 메시지 추적 세부사항을 보면 "mail_logs" 및 "Last State(마지막 상태)"에서 얻은 것과 동일한 로그가 이미지에 표시된 대로 "Remediated(치료)"로 표시됩니다.

소개

이 문서에서는 CTR(Cisco Threat Response)에서 이메일을 교정하는 방법에 대해 설명합니다.

배경 정보

CTR 조사가 온디맨드 메일 교정을 지원하도록 업데이트되었습니다. 관리자는 O365 및 OnPrem Exchange 사용자 사서함에서 특정 이메일을 검색하고 ESA(Email Security Appliance) 또는 SMA(Security Management Appliance)를 통해 수정할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CTR 계정

- Cisco Security Services Exchange
- ESA AsycnOs 14.0.1-033

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

> **참고:** 검색 및 메일 교정은 O365, Exchange 2016 및 2019 하이브리드 배포 및 온프레미스 2013 Exchange 구축에서만 지원됩니다.

구성

1. ESA에서 계정 설정 구성
2. 체인으로 연결된 프로필을 구성하고 도메인을 계정 프로필에 매핑
3. CTR을 ESA 또는 SMA와 통합

확인

CTR 포털에서 관찰 가능 사항을 조사하고 아래 단계를 사용하여 교정할 메시지를 선택할 수 있습니다.

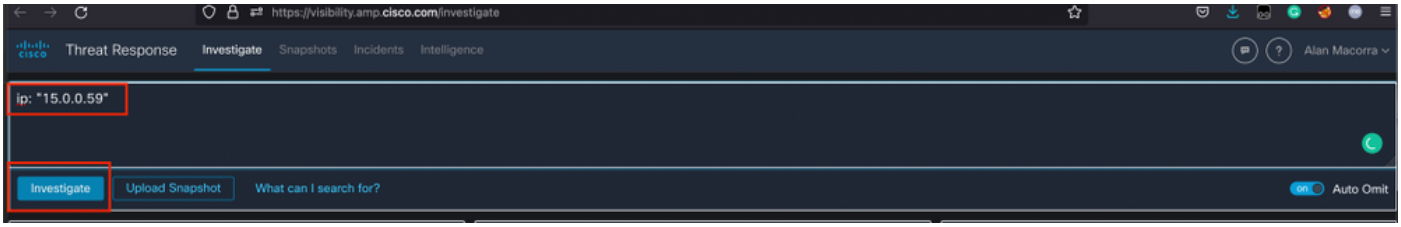
1단계. 사용 가능한 서버에 대한 액세스를 기반으로 CTR 포털에 액세스하고

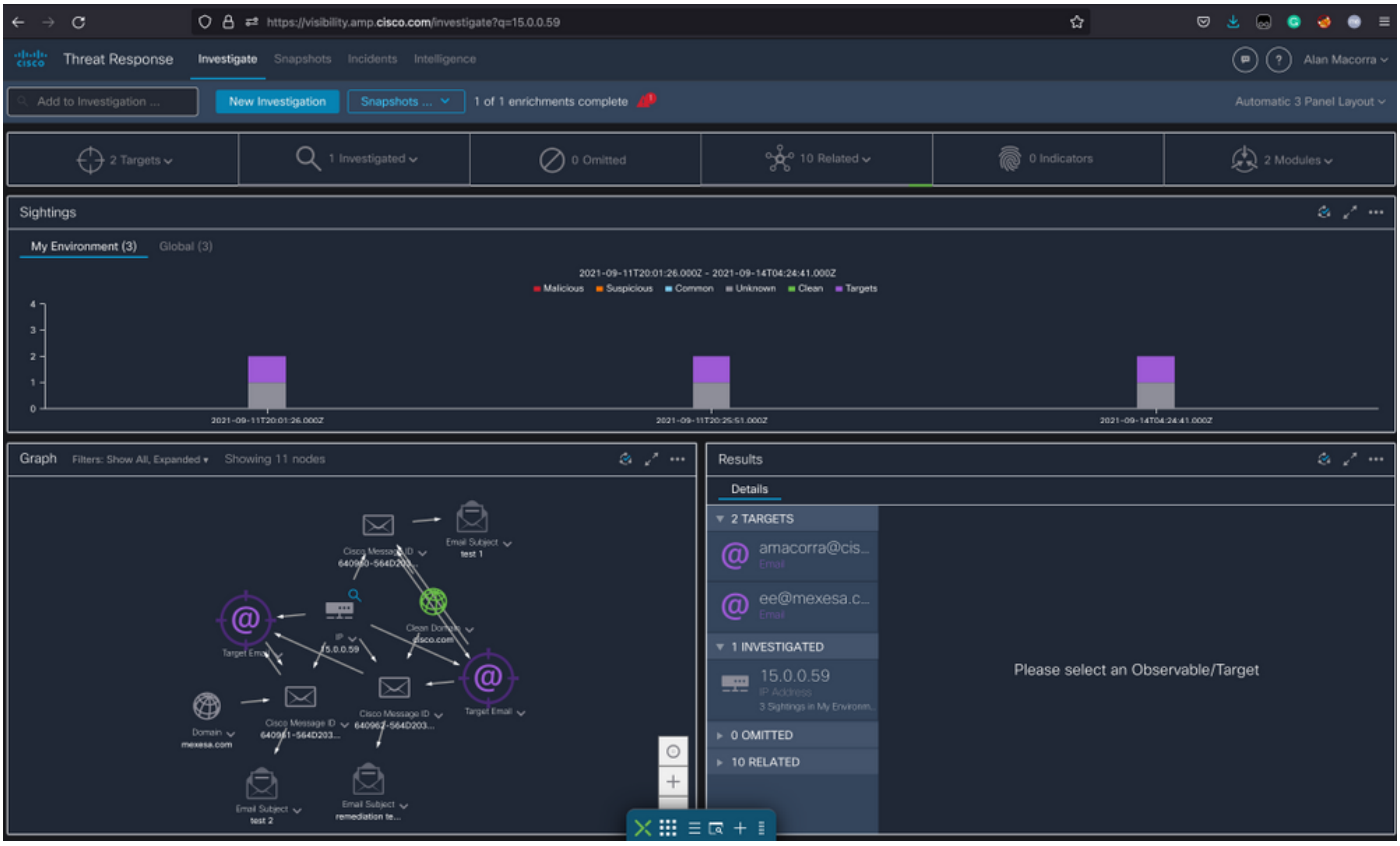
- 미국 https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- EU https://visibility.eu.amp.cisco.com/investigate

2단계. 지원되는 관찰 가능한 개체를 사용하여 악의적이거나 위협인 것으로 보이는 전달된 메시지를 조사합니다. 이미지에 표시된 대로 다음 기준에 따라 관찰 가능 항목을 검색할 수 있습니다.

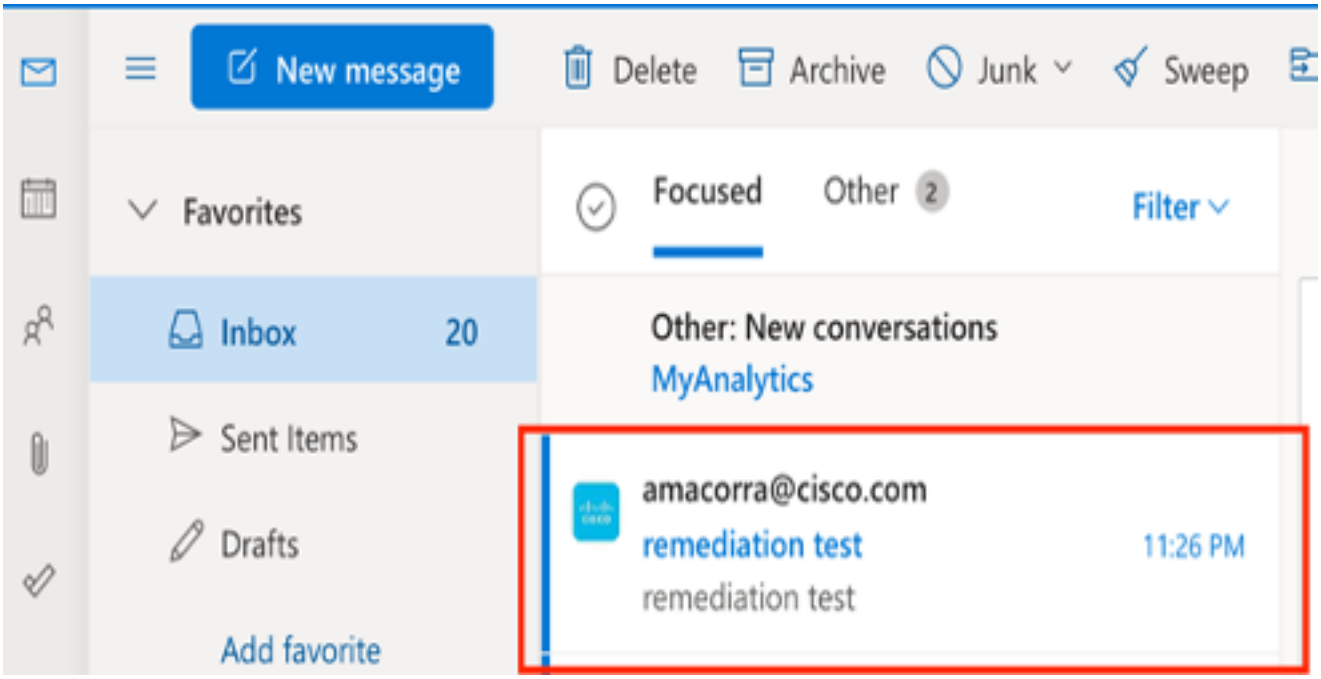
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

2.1 아래 이미지에 표시된 IP 조사 및 조사의 예:

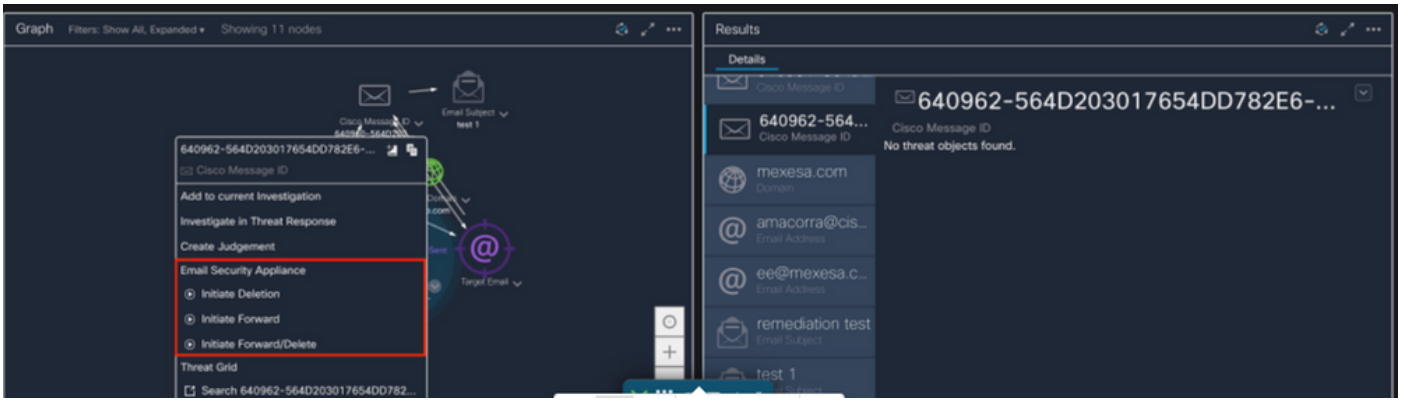




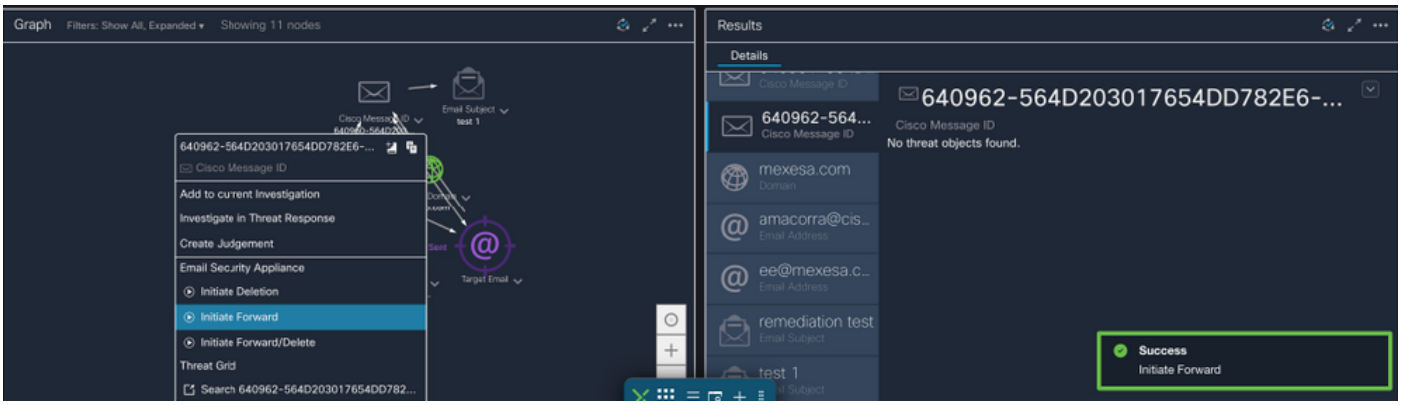
2.2 메시지에 표시된 것처럼 메시지가 수정되기 전에 받은 편지함에 표시되는 내용은 다음과 같습니다.



2.3 "Cisco Message ID(Cisco 메시지 ID)"를 클릭한 다음, 이미지에 표시된 대로 지원되는 교정 작업 중 하나를 메뉴 옵션에서 선택합니다.



2.4 이 예에서는 "Initiate Forward(착신 전환 시작)"가 선택되고 이미지에 표시된 것처럼 오른쪽 하단 모서리에 Success(성공) 팝업 창이 나타납니다.

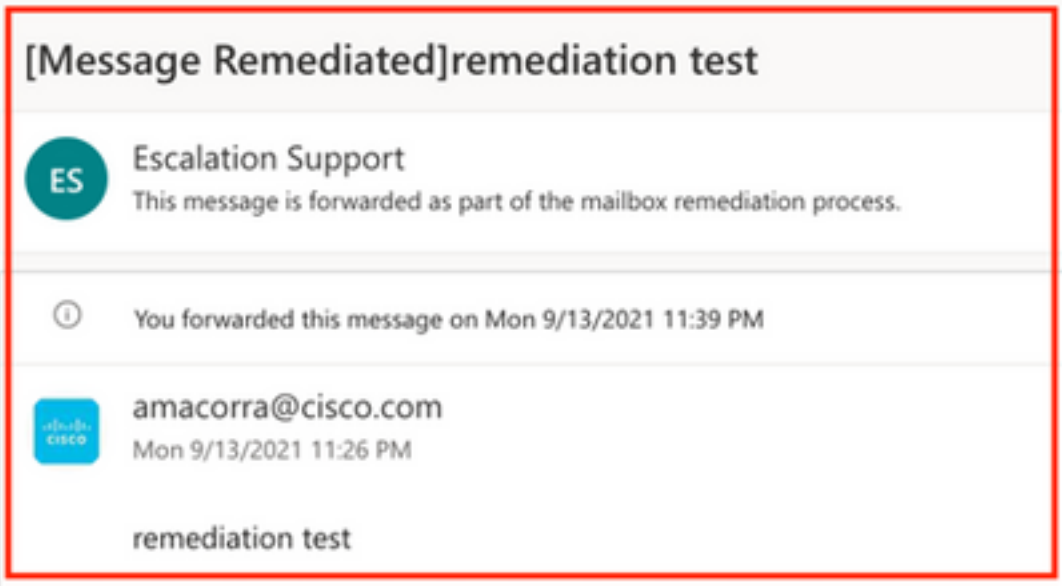


2.5 ESA의 "mail_logs" 아래에 "CTR" 교정이 시작되며 선택한 작업 및 최종 상태가 표시되는 다음 로그가 표시됩니다.

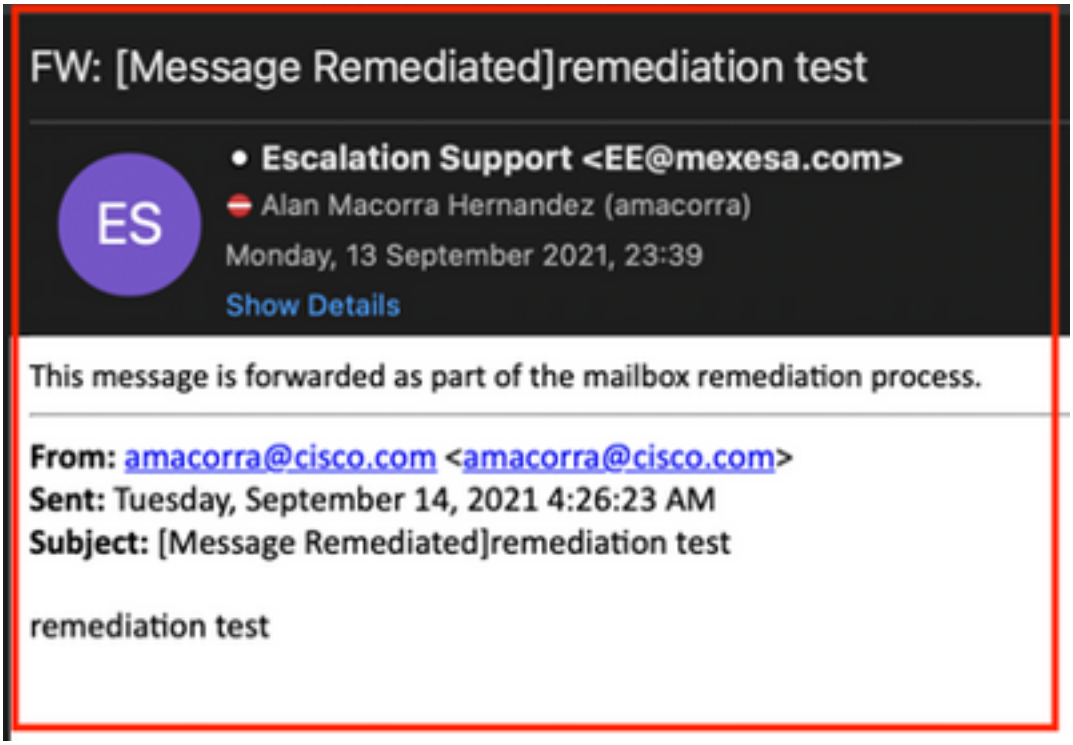
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

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.
```

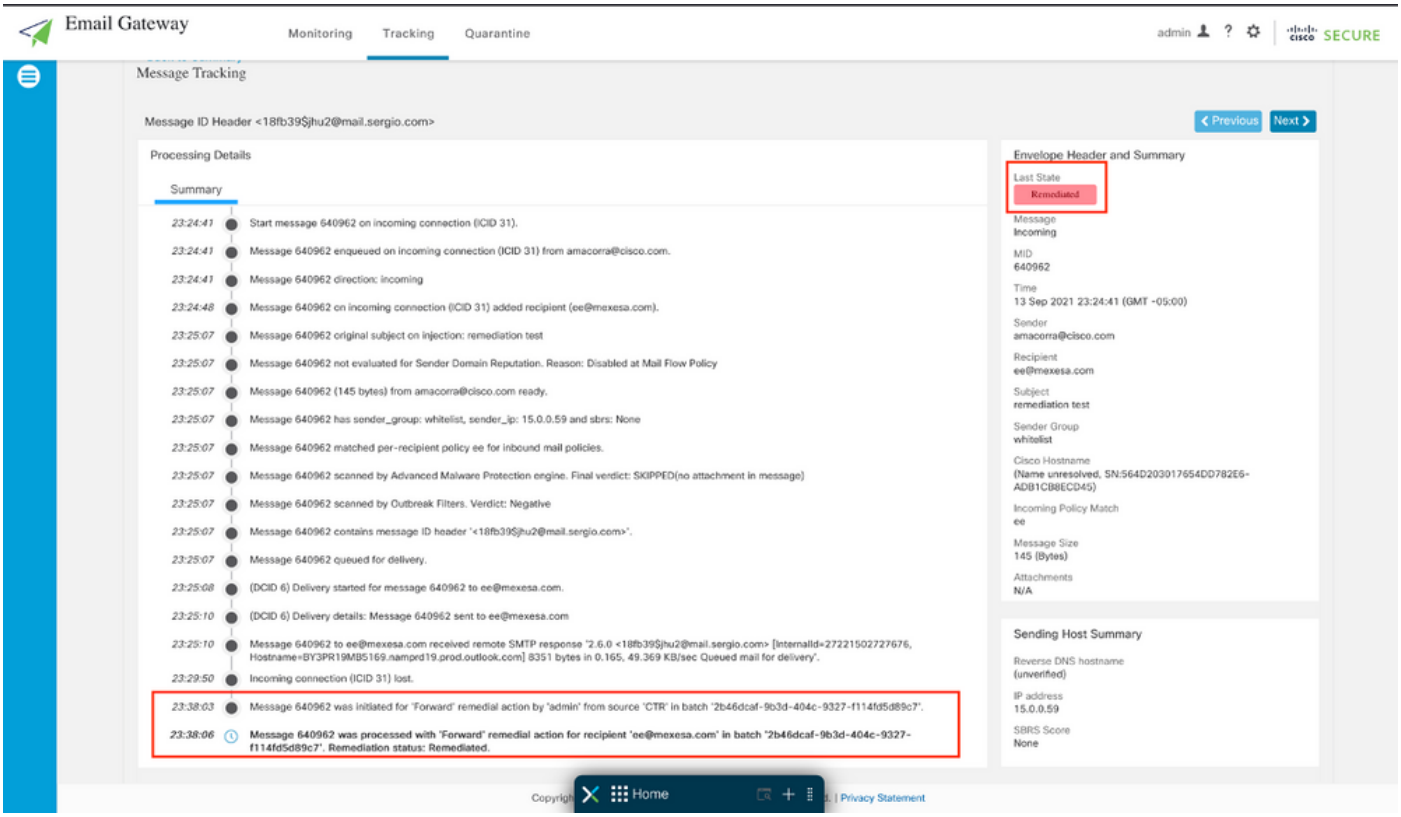
2.6 메시지 제목 앞에 "[Message Remediated]"라는 문장이 나타납니다(이미지에 표시됨).



2.7 ESA/SMA 모듈을 구성할 때 입력하는 이메일 주소는 이미지에 표시된 대로 "Forward(전달)" 또는 "Forward/Delete(전달/삭제)" 옵션을 선택할 때 교정 이메일을 수신하는 이메일 주소입니다.



2.8 마지막으로, ESA/SMA의 새 인터페이스에 대한 메시지 추적 세부사항을 보면 "mail_logs" 및 "Last State(마지막 상태)"에서 얻은 것과 동일한 로그가 이미지에 표시된 대로 "Remediated(치료)"로 표시됩니다.



참고: ESA/SMA에서 검색 및 교정할 기능을 구성하면 CTR과 ESA/SMA에서도 동일한 메시지

를 교정할 수 있습니다. 이렇게 하면 통합 모듈에 구성된 것과 다른 이메일 주소로 동일한 메시지를 전달할 수 있습니다.