E-mails van CTR verhelpen

Inhoud

Inleiding

Dit document beschrijft hoe u e-mails van Cisco Threat Response (CTR) kunt verbeteren.

Achtergrondinformatie

Het CTR-onderzoek is bijgewerkt om de correctie van OnDemand Mail te ondersteunen. Admin kan specifieke e-mails van O365 en OnPrem Exchange-gebruikersmailboxen doorzoeken en deze herstellen door een e-mail security applicatie (ESA) of security Management-applicatie (SMA).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CTR-account
- Cisco Security Services exchange
- ESR AS 14.0.1-033

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

> **Opmerking:** Zoeken en mailverbetering wordt alleen ondersteund in O365, Exchange 2016 & 2019 Hybrid-implementaties en On-Prem 2013 Exchange implementaties.

Configureren

1. Accountinstellingen instellen in de ESA
2. Geketend profiel configureren en de domein(en) in kaart brengen naar het accountprofiel
3. Integreren met CTR of ESA of SMA

Verificatie

U kunt de observeermiddelen in het CTR-portal onderzoeken en het bericht voor herstel selecteren in de volgende stappen:

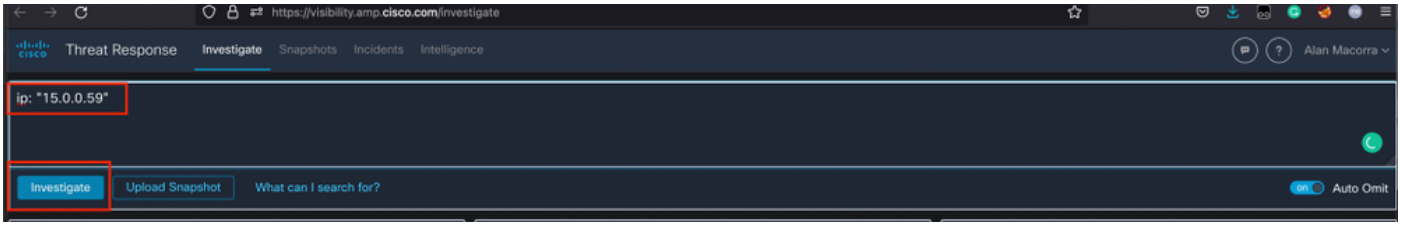
Stap 1. Toegang tot het CTR-portal op basis van de toegang tot beschikbare servers en onderzoek

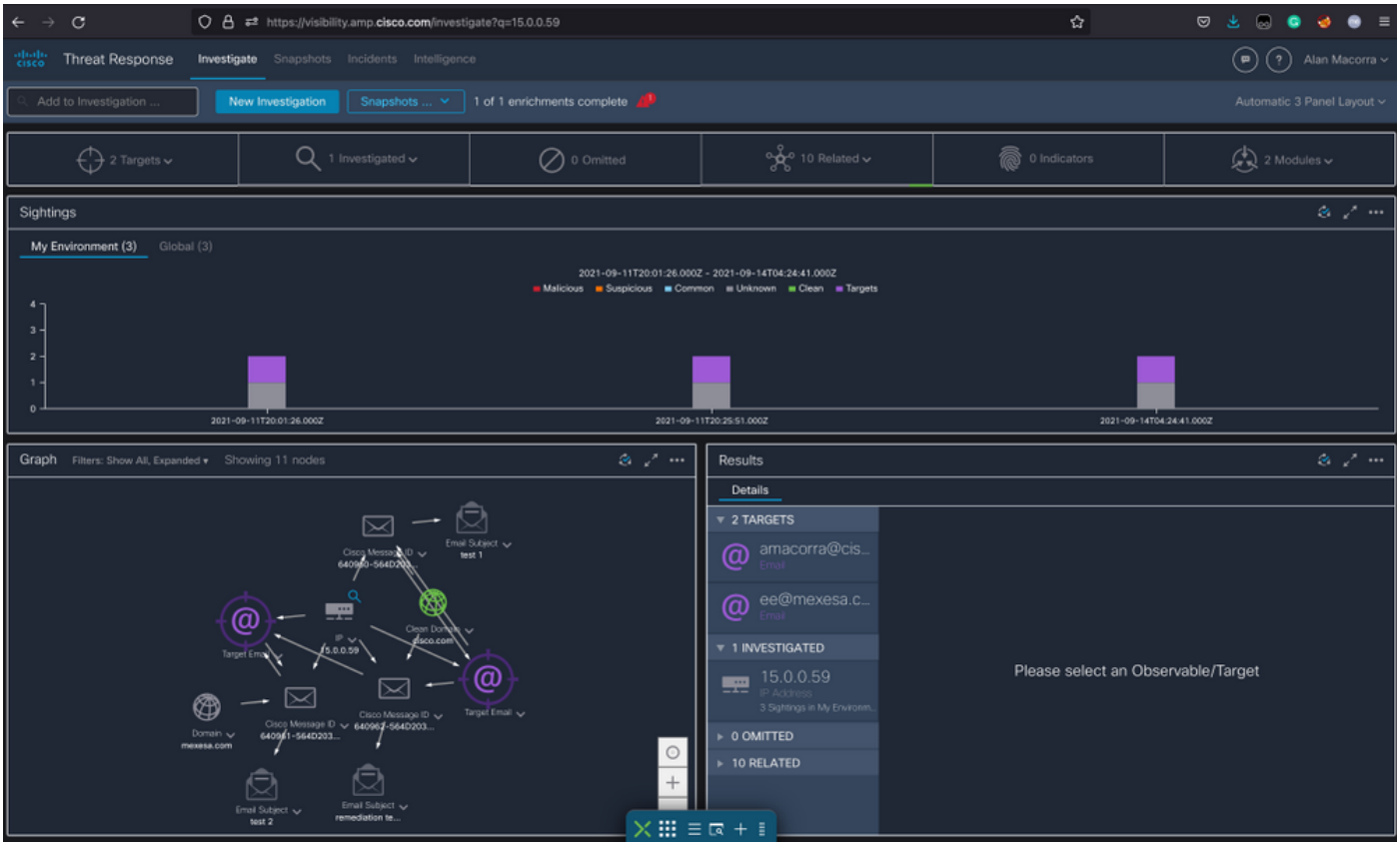
- VS https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- EU https://visibility.eu.amp.cisco.com/investigate

Stap 2. Onderzoek de geleverde berichten die kwaadaardig of bedreigend lijken te zijn door gebruik te maken van de ondersteunde wachtwoorden. De waarnemingen kunnen aan de hand van de volgende criteria worden bezocht, zoals in de afbeelding wordt getoond:

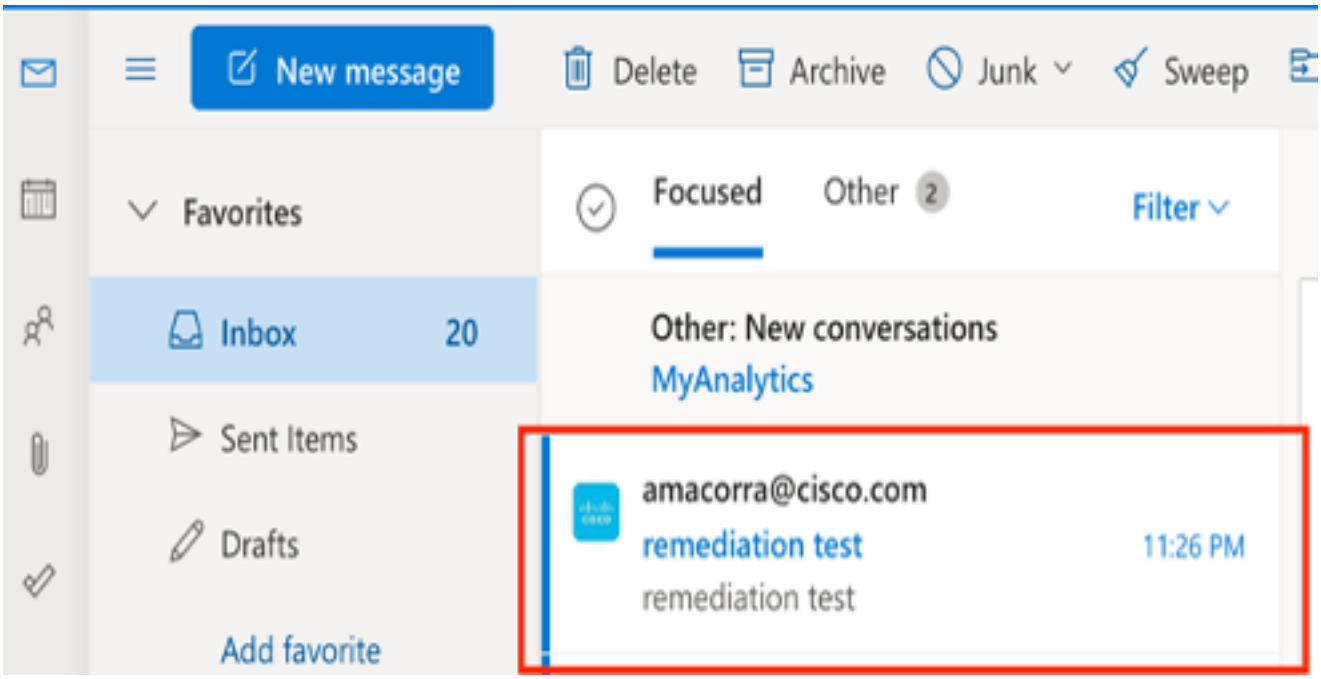
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

2.1 Onderstaand een voorbeeld van een onderzoek en onderzoek in het kader van het OT, zoals blijkt uit de beelden:

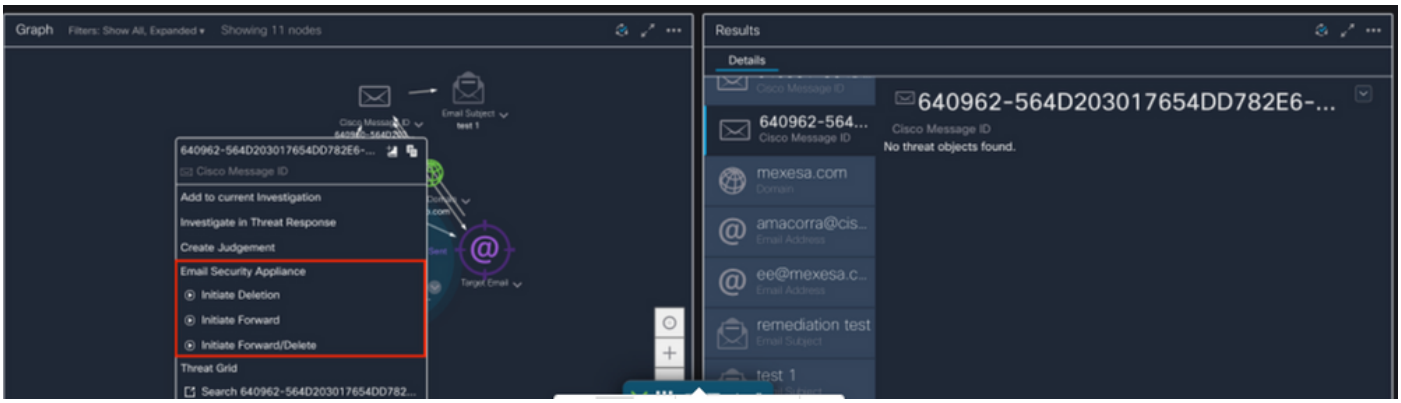




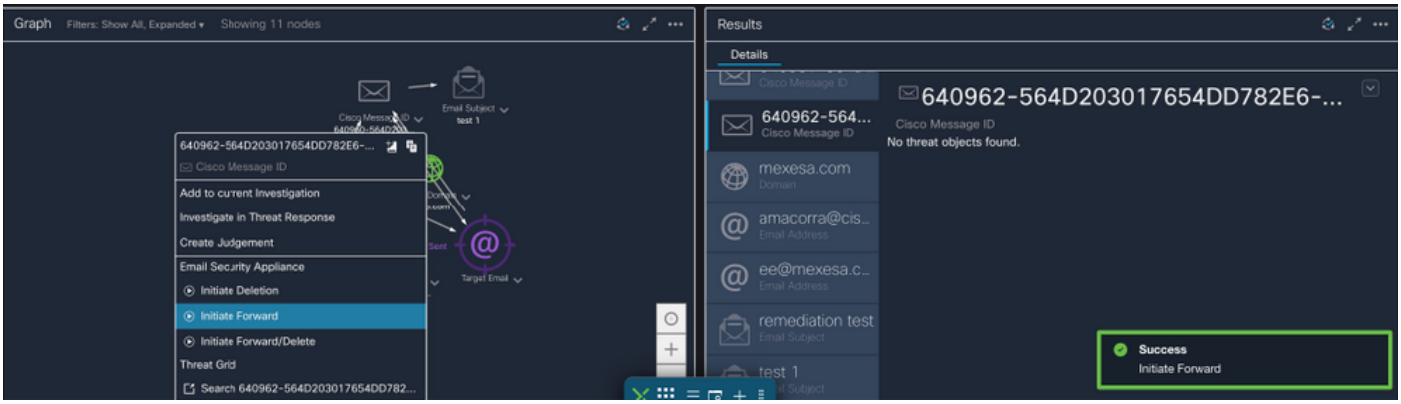
2.2 Dit krijgt u in uw inbox voordat het bericht wordt hersteld, zoals in de afbeelding wordt getoond:



2.3 Selecteer in het menu-opties een van de ondersteunde bewerkingsacties zoals in de afbeelding:



2.4 In dit voorbeeld wordt "Vooruit openen" geselecteerd en verschijnt een Success pop-up-venster in de rechterbenedenhoek, zoals in de afbeelding:

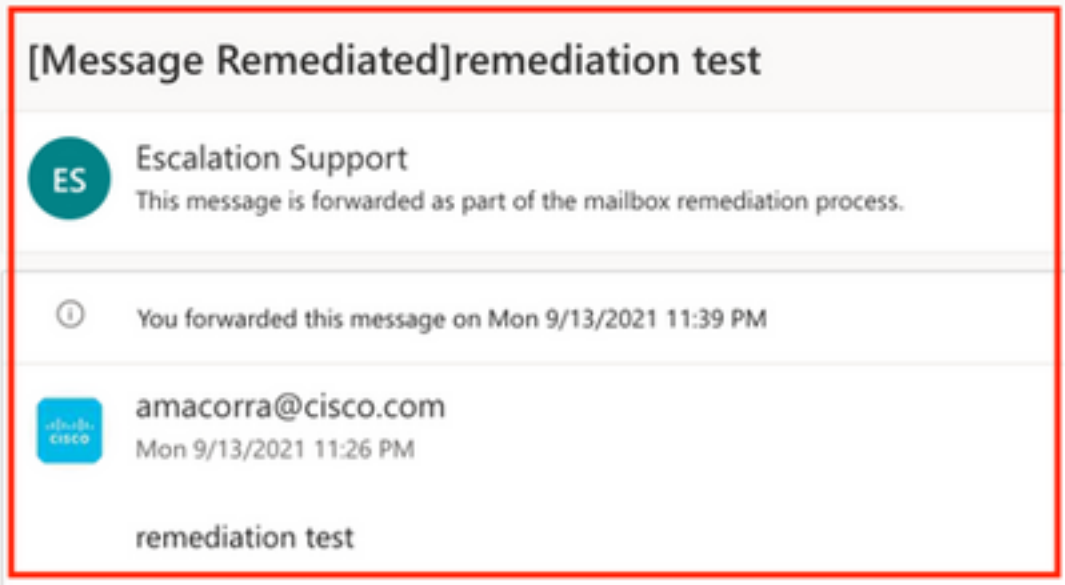


2.5 In het ESA, kunt u de volgende logbestanden zien onder "mail_logs" die laten zien dat het "CTR"-herstel start, de geselecteerde actie en de definitieve status.

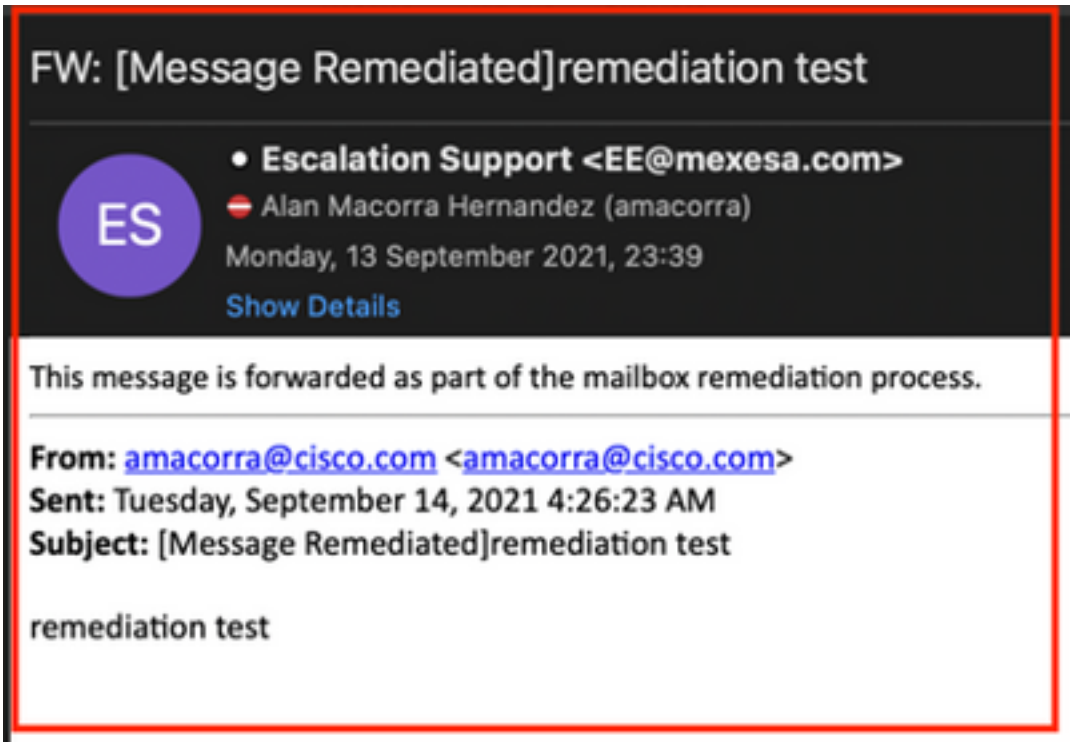
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

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.
```

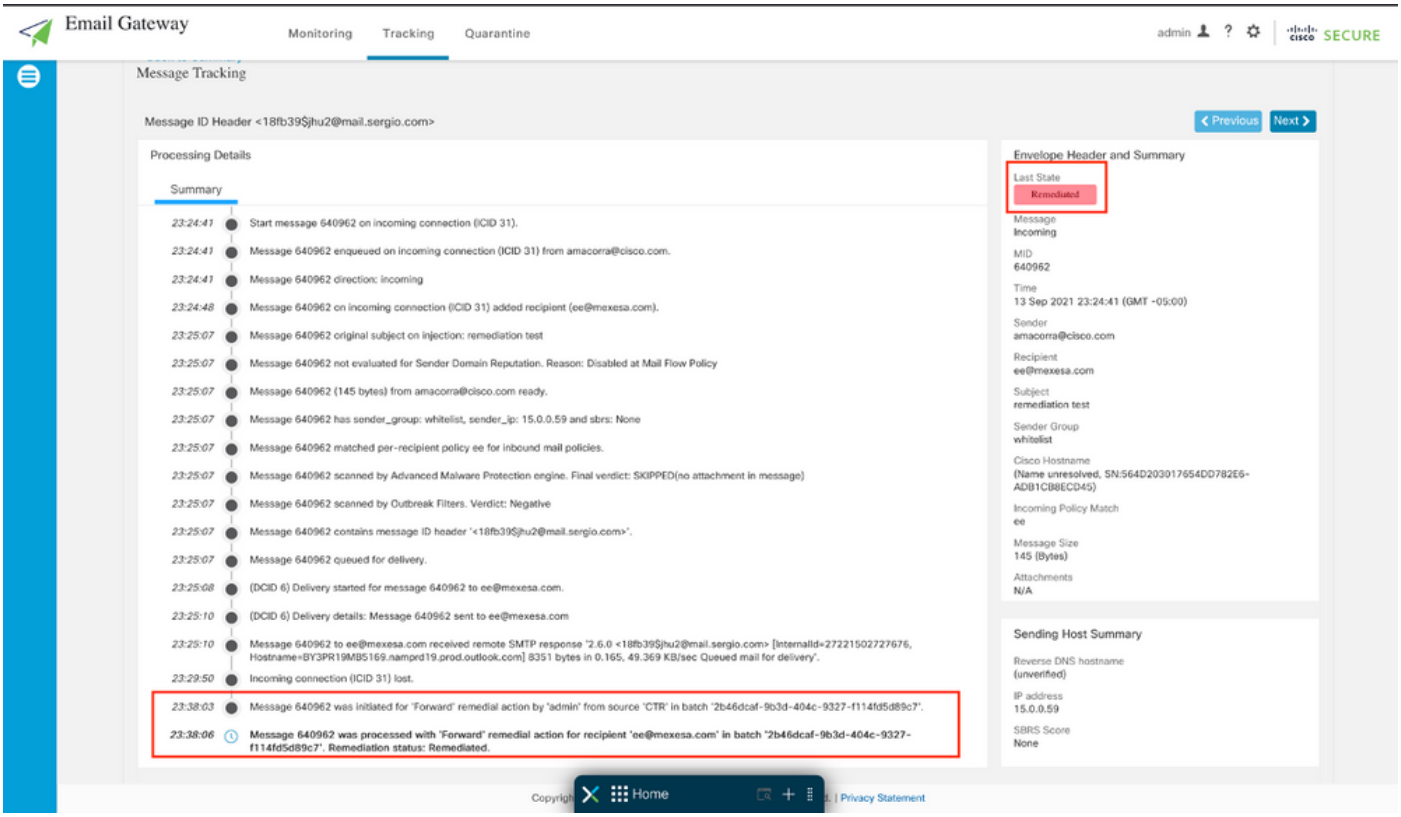
2.6 Het bericht "[Bericht geremedieerd]" wordt in het bericht voorgedrukt, zoals in de afbeelding weergegeven:



2.7 Het e-mailadres dat u typt bij het configureren van de ESA/SMA-module, is het e-mailadres dat u ontvangt wanneer u de optie "Voorwaarts" of "Voorwaarts/Verwijderen" selecteert, zoals in de afbeelding wordt weergegeven:



2.8 Ten slotte, als je kijkt naar de informatie-tracking details van de nieuwe interface van de ESA/SMA, dan zie je dezelfde logbestanden die zijn verkregen in "mail_logs" en "Laatste Staat" als "Geremedieerd", zoals in de afbeelding getoond wordt:



Opmerking: Er kunnen verschillende corrigerende maatregelen worden genomen. Als u de functie in uw ESA/SMA instelt om te zoeken en te verbeteren, dan kunt u hetzelfde bericht corrigeren vanaf CTR en ook via ESA/SMA. Hierdoor kunt u hetzelfde bericht doorsturen naar een ander e-mailadres dan het bericht dat in de integratiemodule is ingesteld.