

Come correggere le e-mail da CTR

Sommario

[Introduzione](#)

[Premesse](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Passaggio 1. Accedere al portale CTR in base all'accesso ai server disponibili e verificare](#)

[Passaggio 2. Esaminare i messaggi recapitati che sembrano essere dannosi o una minaccia utilizzando gli oggetti osservabili supportati. Gli oggetti osservabili possono essere cercati in base ai seguenti criteri, come mostrato nell'immagine:](#)

[2.1 Di seguito è riportato un esempio di inchiesta e di inchiesta relative al PI, come illustrato nelle immagini:](#)

[2.2 Ecco cosa si ottiene nella casella di posta prima che il messaggio venga corretto, come mostrato nell'immagine:](#)

[2.3 Facendo clic su "ID messaggio Cisco", selezionare dalle opzioni di menu una delle azioni risolte supportate, come mostrato nell'immagine:](#)

[2.4 In questo esempio, viene selezionato "Inizia in avanti" e viene visualizzata una finestra pop-up di successo nell'angolo in basso a destra, come mostrato nell'immagine:](#)

[2.5 Nell'ESA, sotto "mail logs", si possono vedere i seguenti log che mostrano l'avvio della risoluzione "CTR", l'azione selezionata e lo stato finale.](#)

[2.6 L'indicazione "\[Messaggio risolto\]" appare anteposta all'oggetto del messaggio, come mostrato nell'immagine:](#)

[2.7 L'indirizzo e-mail che si digita durante la configurazione del modulo ESA/SMA è quello che riceve le e-mail risolte quando si seleziona l'opzione "Forward" o "Forward/Delete", come mostrato nell'immagine:](#)

[2.8 Infine, se si osservano i dettagli di tracciamento dei messaggi della nuova interfaccia dell'ESA/SMA, si possono vedere gli stessi log ottenuti nei "mail logs" e nell'"Ultimo stato" come "Remediated", come mostrato nell'immagine:](#)

Introduzione

Questo documento descrive come risolvere i problemi relativi alle e-mail di Cisco Threat Response (CTR).

Premesse

L'indagine CTR è stata aggiornata per supportare OnDemand Mail Remediation. L'amministratore può cercare e-mail specifiche dalle caselle di posta degli utenti O365 e OnPrem Exchange e correggerle tramite Email Security Appliance (ESA) o Security Management Appliance (SMA).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Account CTR
- Cisco Security Services Exchange
- ESA AsyncOs 14.0.1-03

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: La ricerca e la risoluzione dei problemi relativi alla posta elettronica sono supportate solo nelle distribuzioni ibride di Exchange 365, Exchange 2016 e 2019 e nelle distribuzioni Exchange locali 2013.

Configurazione

1. [Configurazione delle impostazioni dei conti nell'ESA](#)
2. [Configurare il profilo concatenato e mappare i domini al profilo account](#)
3. [Integrazione di CTR con ESA o SMA](#)

Verifica

È possibile analizzare gli elementi osservabili nel portale CTR e selezionare il messaggio per la risoluzione utilizzando i passaggi seguenti:

Passaggio 1. Accedere al portale CTR in base all'accesso ai server disponibili e verificare

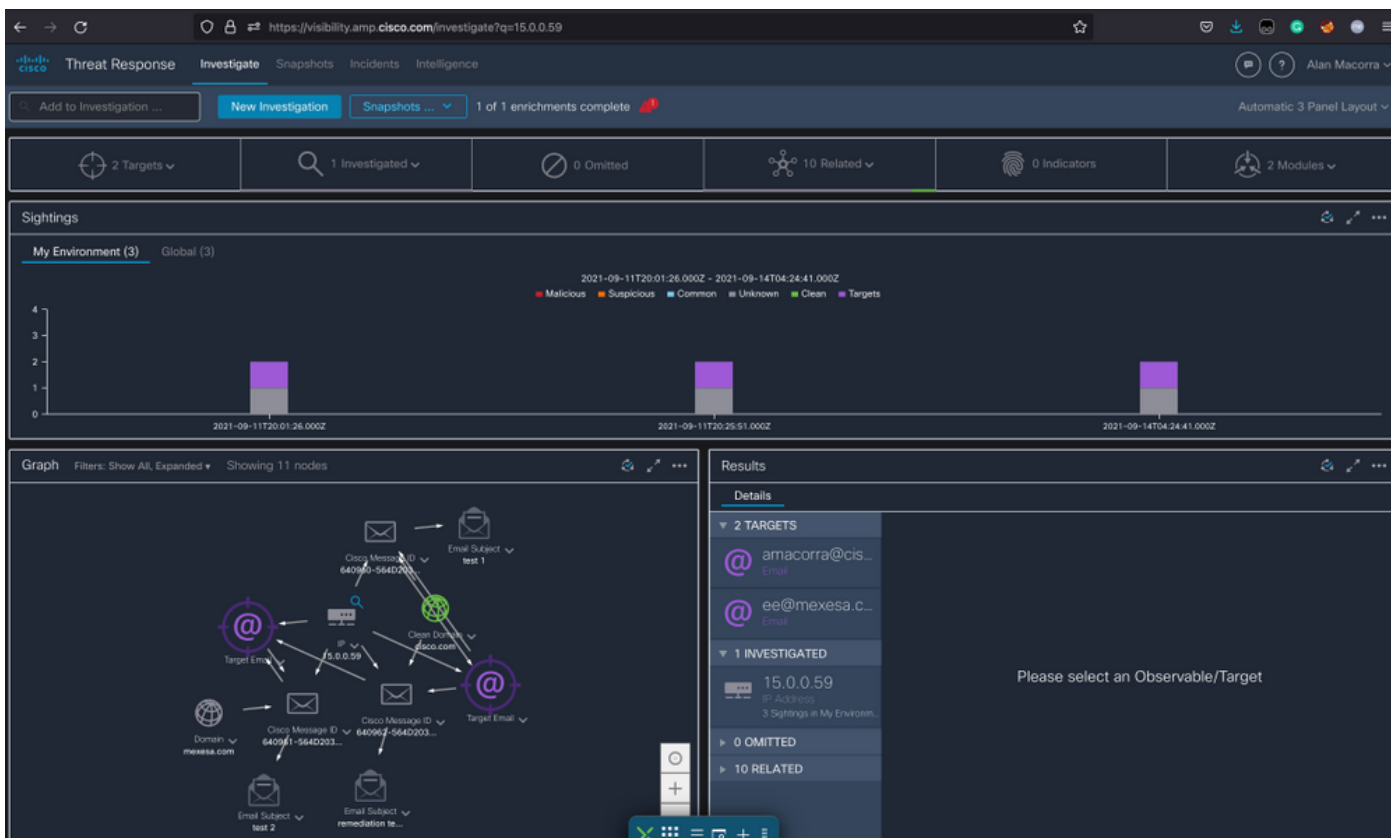
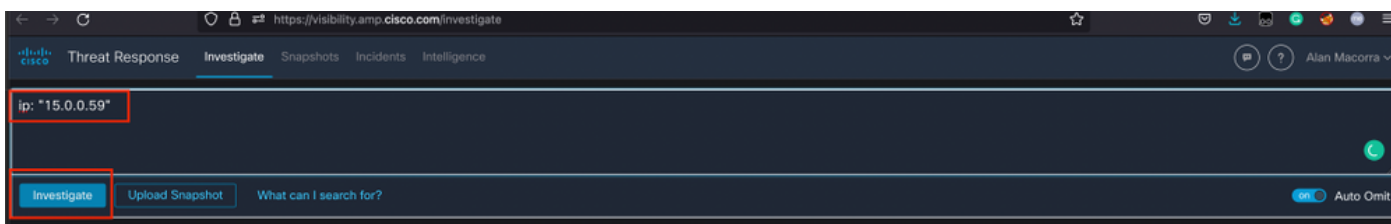
- USA <https://visibility.amp.cisco.com/investigate>
- APJC <https://visibility.apjc.amp.cisco.com/investigate>
- EU <https://visibility.eu.amp.cisco.com/investigate>

Passaggio 2. Esaminare i messaggi recapitati che sembrano essere dannosi o una minaccia utilizzando gli oggetti osservabili supportati. Gli oggetti osservabili possono essere cercati in base ai seguenti criteri, come mostrato nell'immagine:

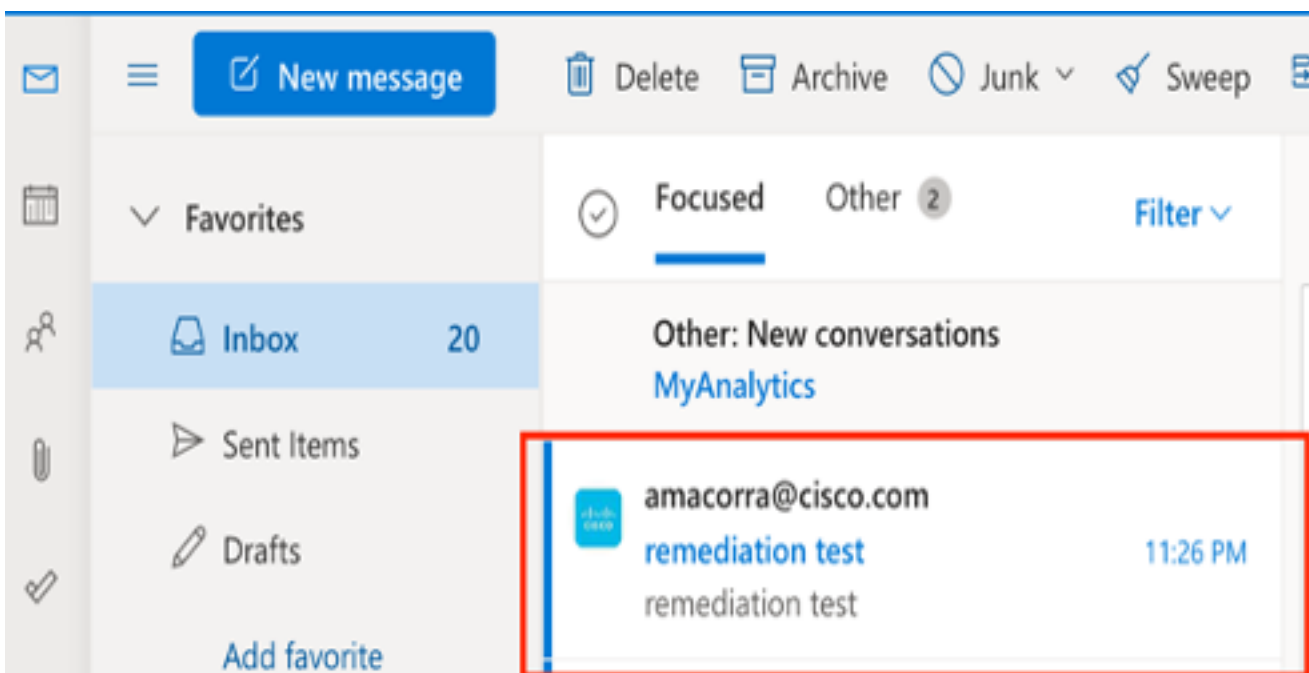
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

2.1 Di seguito è riportato un esempio di inchiesta e di inchiesta relative al PI, come illustrato

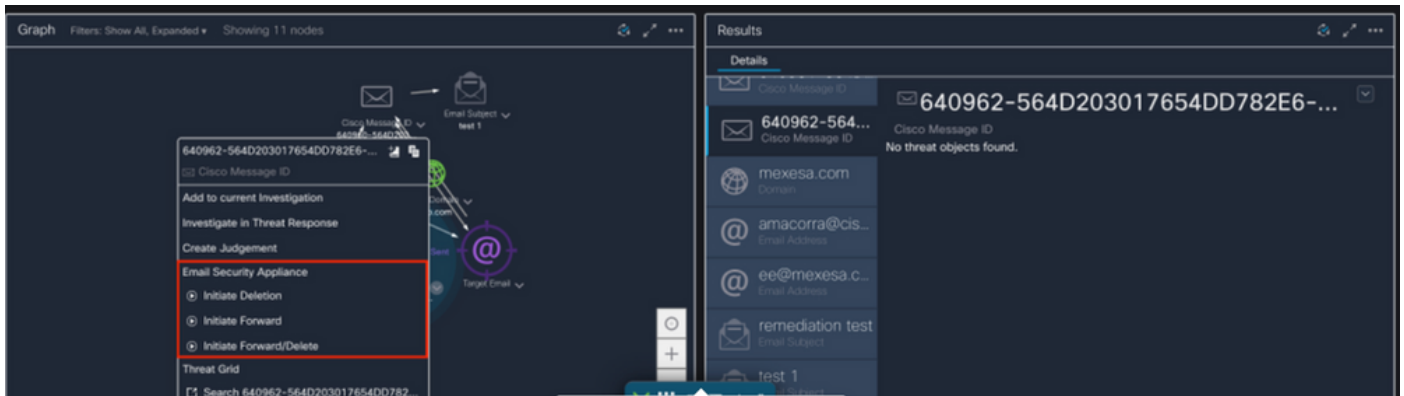
nelle immagini:



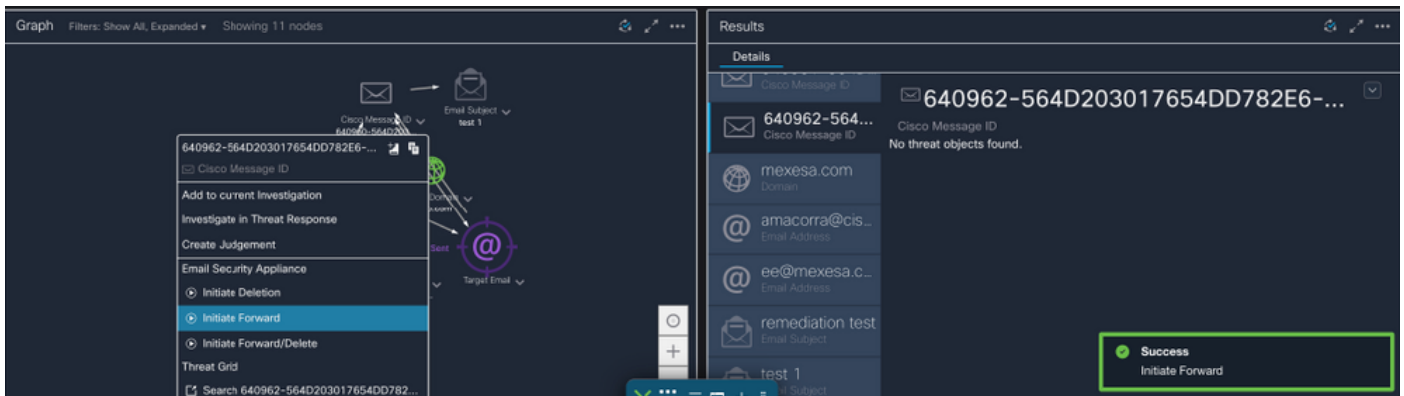
2.2 Ecco cosa si ottiene nella casella di posta prima che il messaggio venga corretto, come mostrato nell'immagine:



2.3 Facendo clic su "ID messaggio Cisco", selezionare dalle opzioni di menu una delle azioni risolte supportate, come mostrato nell'immagine:



2.4 In questo esempio, viene selezionato "Inizia in avanti" e viene visualizzata una finestra pop-up di successo nell'angolo in basso a destra, come mostrato nell'immagine:

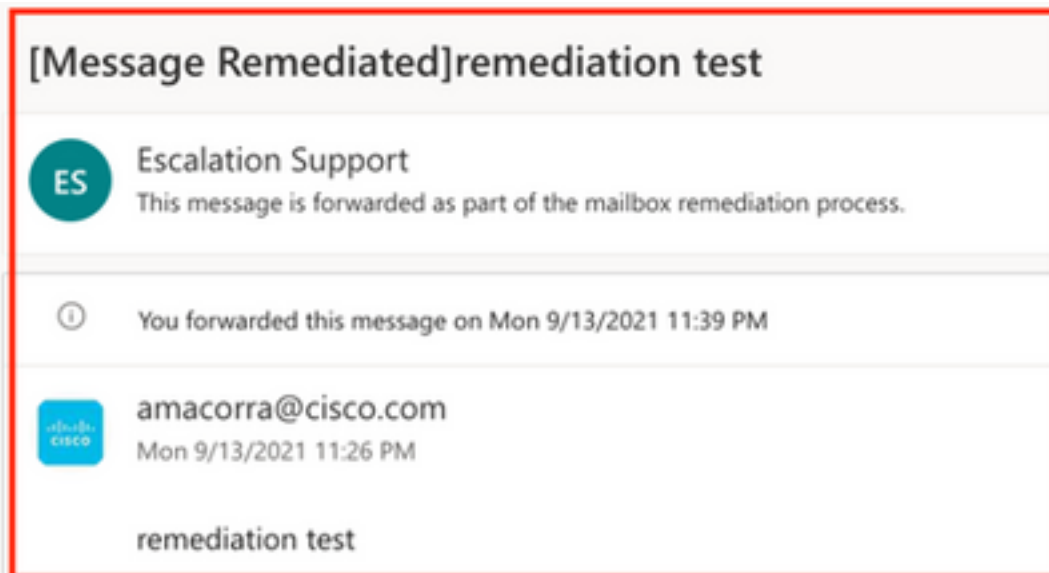


2.5 Nell'ESA, sotto "mail_logs", si possono vedere i seguenti log che mostrano l'avvio della risoluzione "CTR", l'azione selezionata e lo stato finale.

```
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'indicazione "[Messaggio risolto]" appare anteposta all'oggetto del messaggio, come mostrato nell'immagine:



2.7 L'indirizzo e-mail che si digita durante la configurazione del modulo ESA/SMA è quello che riceve le e-mail risolte quando si seleziona l'opzione "Forward" o "Forward/Delete", come mostrato nell'immagine:



2.8 Infine, se si osservano i dettagli di tracciamento dei messaggi della nuova interfaccia dell'ESA/SMA, si possono vedere gli stessi log ottenuti nei "mail_logs" e nell'"Ultimo stato" come "Remediated", come mostrato nell'immagine:

Message Tracking

Message ID Header <18fb395jhu2@mail.sergio.com>

Processing Details

Summary

- 23:24:47 Start message 640962 on incoming connection (ICID 31).
- 23:24:47 Message 640962 enqueued on incoming connection (ICID 31) from amacorra@cisco.com.
- 23:24:47 Message 640962 direction: incoming
- 23:24:48 Message 640962 on incoming connection (ICID 31) added recipient (ee@mexesa.com).
- 23:25:07 Message 640962 original subject on injection: remediation test
- 23:25:07 Message 640962 not evaluated for Sender Domain Reputation. Reason: Disabled at Mail Flow Policy
- 23:25:07 Message 640962 (145 bytes) from amacorra@cisco.com ready.
- 23:25:07 Message 640962 has sender_group: whitelist, sender_ip: 15.0.0.59 and sbrs: None
- 23:25:07 Message 640962 matched per-recipient policy ee for inbound mail policies.
- 23:25:07 Message 640962 scanned by Advanced Malware Protection engine. Final verdict: SKIPPED(no attachment in message)
- 23:25:07 Message 640962 scanned by Outbreak Filters. Verdict: Negative
- 23:25:07 Message 640962 contains message ID header '<18fb395jhu2@mail.sergio.com>'
- 23:25:07 Message 640962 queued for delivery.
- 23:25:08 (DCID 6) Delivery started for message 640962 to ee@mexesa.com.
- 23:25:10 (DCID 6) Delivery details: Message 640962 sent to ee@mexesa.com
- 23:29:10 Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18fb395jhu2@mail.sergio.com> [internalid=27221502727676, Hostname=BY3PR19MBS169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.
- 23:29:50 Incoming connection (ICID 31) lost.
- 23:38:03 Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcdf-9b3d-404c-9327-f114fd5d89c7'.
- 23:38:06 Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcdf-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.

Envelope Header and Summary

Last State
Remediated

Message
Incoming

MID
640962

Time
13 Sep 2021 23:24:41 (GMT -05:00)

Sender
amacorra@cisco.com

Recipient
ee@mexesa.com

Subject
remediation test

Sender Group
whitelist

Cisco Hostname
(Name unresolved, SN:564D203017654DD782E6-AD81CB8ECD45)

Incoming Policy Match
ee

Message Size
145 (Bytes)

Attachments
N/A

Sending Host Summary

Reverse DNS hostname
(unverified)

IP address
15.0.0.59

SIBRS Score
None

Copyright X Home + Privacy Statement

Nota: È possibile che si verifichino diverse correzioni, se si configura in ESA/SMA la funzione di ricerca e correzione, è possibile correggere lo stesso messaggio da CTR e anche da ESA/SMA. In questo modo è possibile inoltrare lo stesso messaggio a un indirizzo e-mail diverso da quello configurato nel [modulo di integrazione](#).