

Como corrigir e-mails do CTR

Contents

[Introduction](#)

[Informações de Apoio](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificação](#)

[Etapa 1. Acesse o portal CTR com base no acesso aos servidores disponíveis e investigue](#)

[Etapa 2. Investigue as mensagens entregues que parecem ser mal-intencionadas ou uma ameaça usando os observáveis compatíveis. Os observadores podem ser pesquisados pelos seguintes critérios, como mostrado na imagem:](#)

[2.1 Um exemplo de um inquérito e de um inquérito por período de inquérito abaixo, como mostrado nas imagens:](#)

[2.2 Aqui está o que você recebe em sua caixa de entrada antes que a mensagem seja remediada, como mostrado na imagem:](#)

[2.3 Ao clicar em "Cisco Message ID", selecione nas opções do menu qualquer uma das ações corrigidas suportadas, conforme mostrado na imagem:](#)

[2.4 Neste exemplo, "Initiate Forward" \(Iniciar encaminhamento\) é selecionado e uma janela pop-up Success \(Êxito\) é exibida no canto inferior direito, como mostrado na imagem:](#)

[2.5 No ESA, você pode ver os seguintes registros em "mail logs" que mostram que a correção "CTR" é iniciada, a ação selecionada e o status final.](#)

[2.6 A instrução "\[Message Remediated\]" aparece anexada no assunto da mensagem, como mostrado na imagem:](#)

[2.7 O endereço de e-mail digitado ao configurar o módulo ESA/SMA é aquele que recebe os e-mails corrigidos ao selecionar a opção "Encaminhar" ou "Encaminhar/Excluir", como mostrado na imagem:](#)

[2.8 Finalmente, se você olhar para os detalhes de rastreamento de mensagens da nova interface do ESA/SMA, poderá ver os mesmos registros obtidos em "mail logs" e "Last State" como "Remediated", como mostrado na imagem:](#)

Introduction

Este documento descreve como corrigir e-mails do Cisco Threat Response (CTR).

Informações de Apoio

A investigação CTR foi atualizada para suportar a correção de correio sob demanda. O administrador pode pesquisar emails específicos de caixas de correio de usuários do O365 e do OnPrem Exchange e corrigi-los por meio de um Email Security Appliance (ESA) ou Security Management Appliance (SMA).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Conta CTR
- Cisco Security Services Exchange
- ESA AsyncOs 14.0.1-033

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Note: A correção de busca e e-mail é suportada em implantações híbridas do O365, do Exchange 2016 e 2019 e apenas em implantações do Exchange no local 2013.

Configurar

1. [Configurar as configurações da conta no ESA](#)
2. [Configure o perfil em cadeia e mapeie os domínios para o perfil da conta](#)
3. [Integrar o CTR com ESA ou SMA](#)

Verificação

Você pode investigar os observáveis no portal CTR e selecionar a mensagem para correção usando as etapas abaixo:

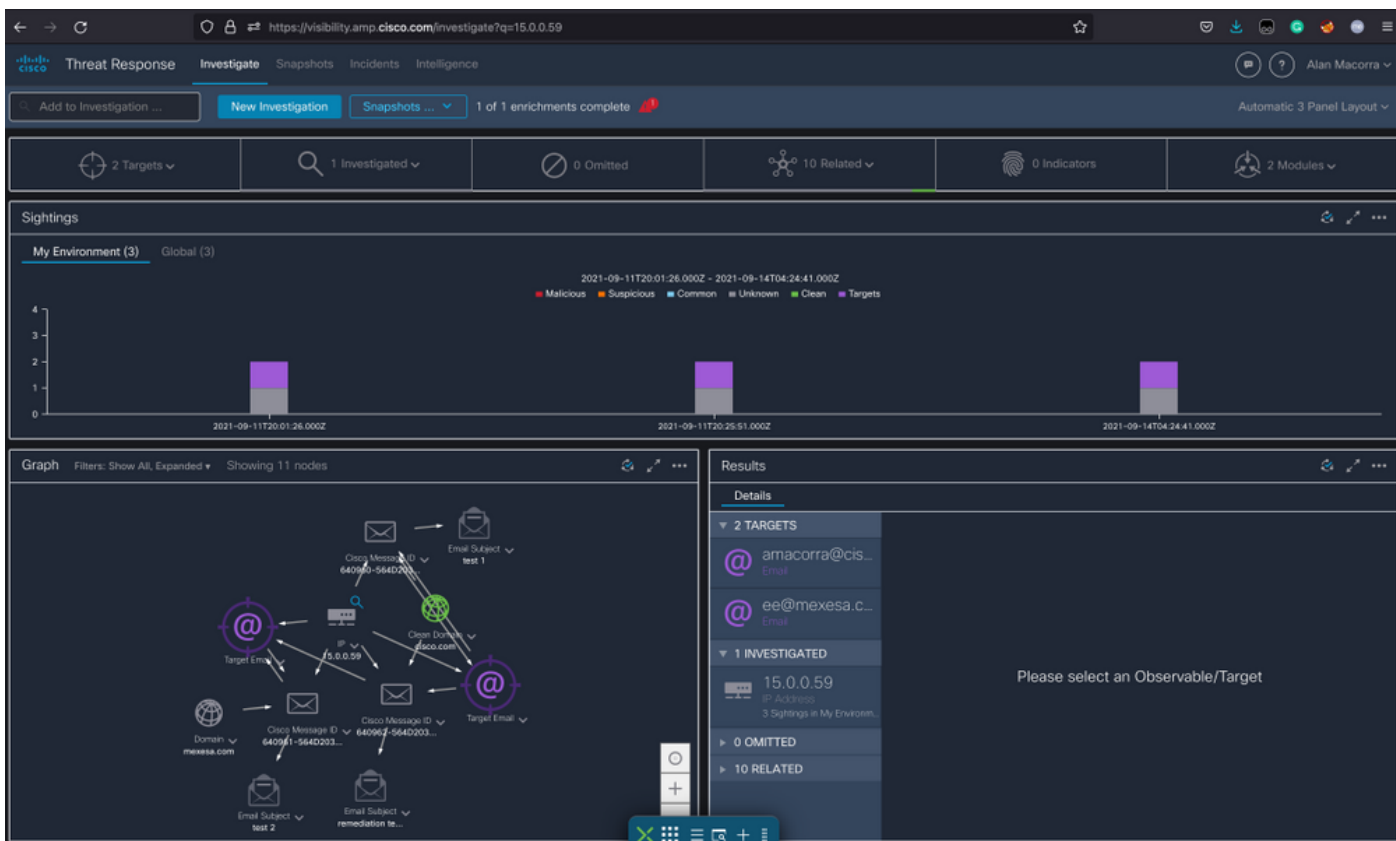
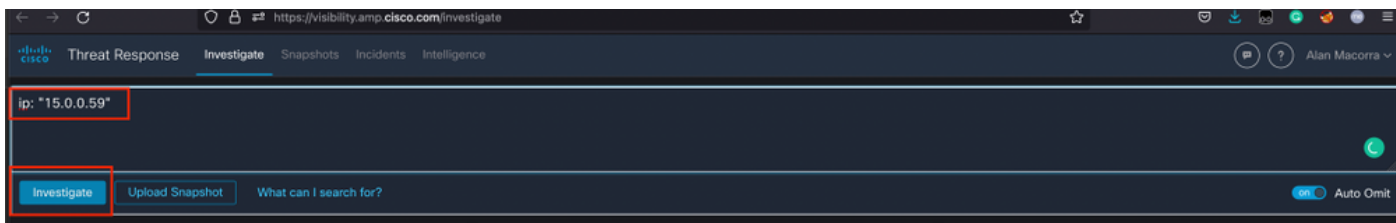
Etapa 1. Acesse o portal CTR com base no acesso aos servidores disponíveis e investigue

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

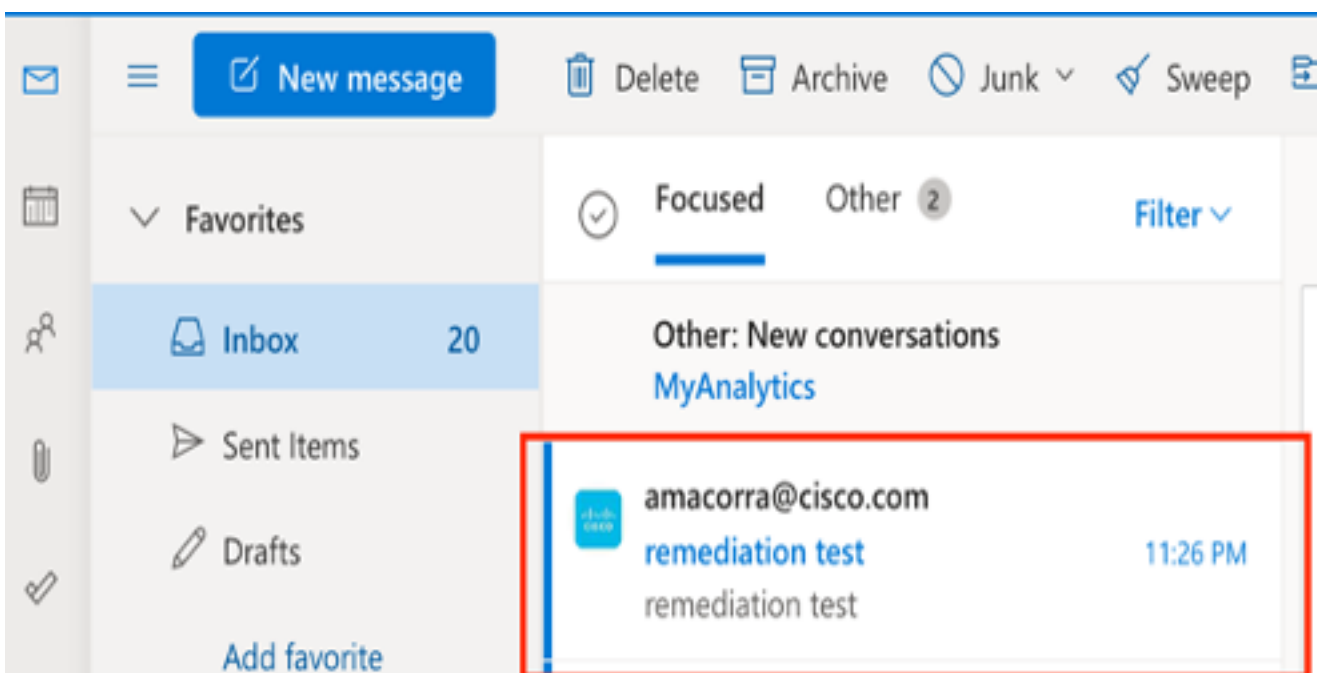
Etapa 2. Investigue as mensagens entregues que parecem ser mal-intencionadas ou uma ameaça usando os observáveis compatíveis. Os observadores podem ser pesquisados pelos seguintes critérios, como mostrado na imagem:

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"

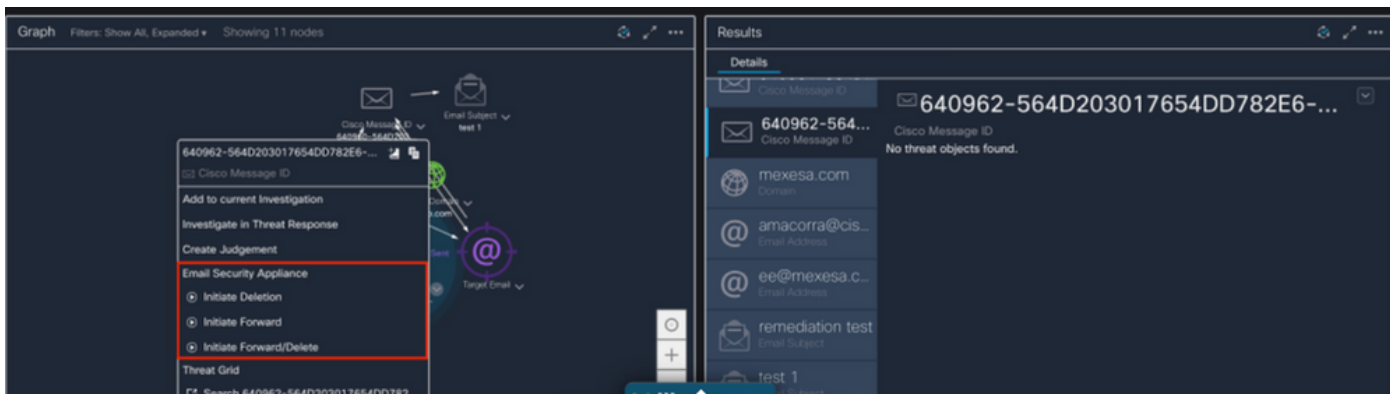
2.1 Um exemplo de um inquérito e de um inquérito por período de inquérito abaixo, como mostrado nas imagens:



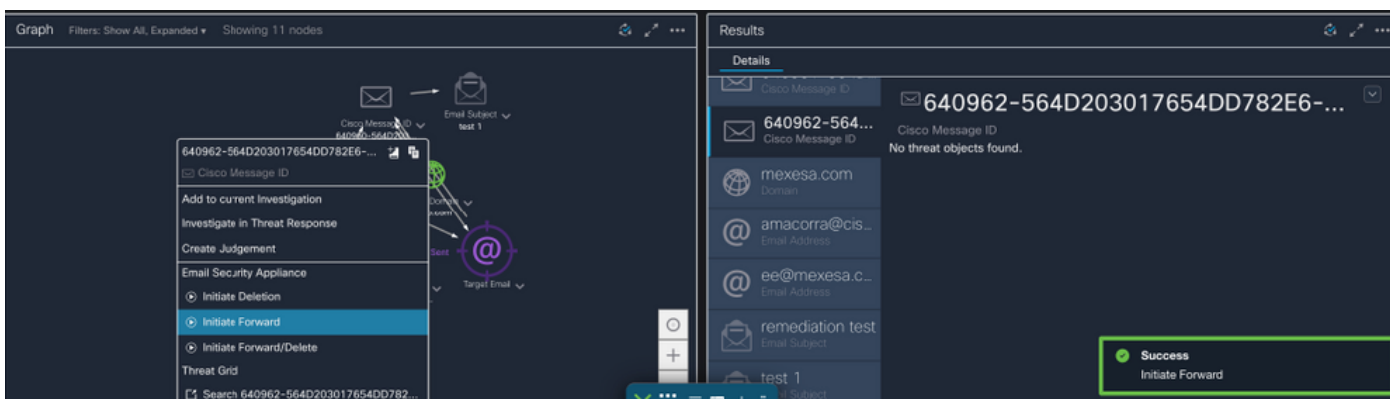
2.2 Aqui está o que você recebe em sua caixa de entrada antes que a mensagem seja remediada, como mostrado na imagem:



2.3 Ao clicar em "Cisco Message ID", selecione nas opções do menu qualquer uma das ações corrigidas suportadas, conforme mostrado na imagem:



2.4 Neste exemplo, "Initiate Forward" (Iniciar encaminhamento) é selecionado e uma janela pop-up Success (Êxito) é exibida no canto inferior direito, como mostrado na imagem:

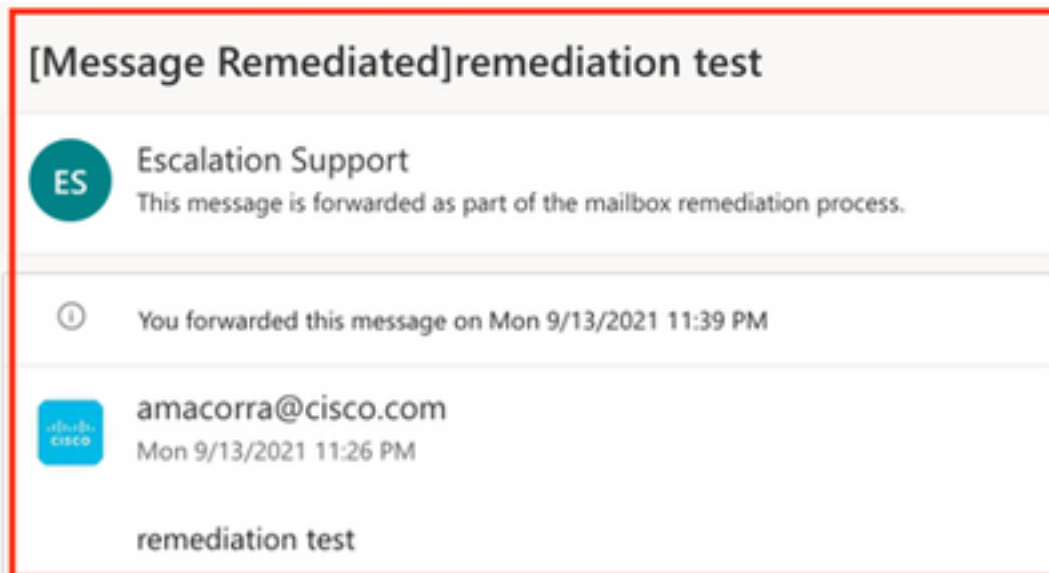


2.5 No ESA, você pode ver os seguintes registros em "mail_logs" que mostram que a correção "CTR" é iniciada, a ação selecionada e o status final.

```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcac-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 '2b46dcac-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.
```

2.6 A instrução "[Message Remediated]" aparece anexada no assunto da mensagem, como mostrado na imagem:



2.7 O endereço de e-mail digitado ao configurar o módulo ESA/SMA é aquele que recebe os e-mails corrigidos ao selecionar a opção "Encaminhar" ou "Encaminhar/Excluir", como mostrado na imagem:



2.8 Finalmente, se você olhar para os detalhes de rastreamento de mensagens da nova interface do ESA/SMA, poderá ver os mesmos registros obtidos em "mail_logs" e "Last State" como "Remediated", como mostrado na imagem:

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

Note: Várias correções podem ocorrer. Se você configurar em seu ESA/SMA o recurso para pesquisar e corrigir, você poderá corrigir a mesma mensagem do CTR e também do ESA/SMA. Isso pode permitir que você encaminhe a mesma mensagem para um endereço de e-mail diferente do configurado no [módulo de integração](#).