Como corrigir e-mails do CTR

Contents

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 AsycnOs 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:

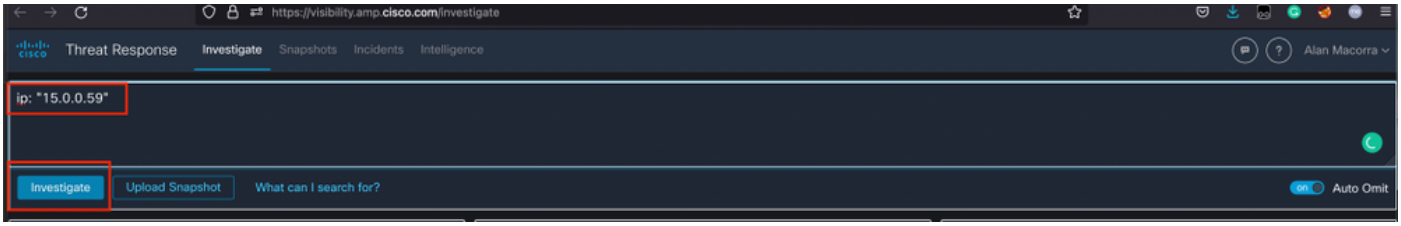
Etapa 1. Acesse o portal CTR com base no acesso aos servidores disponíveis e investigue

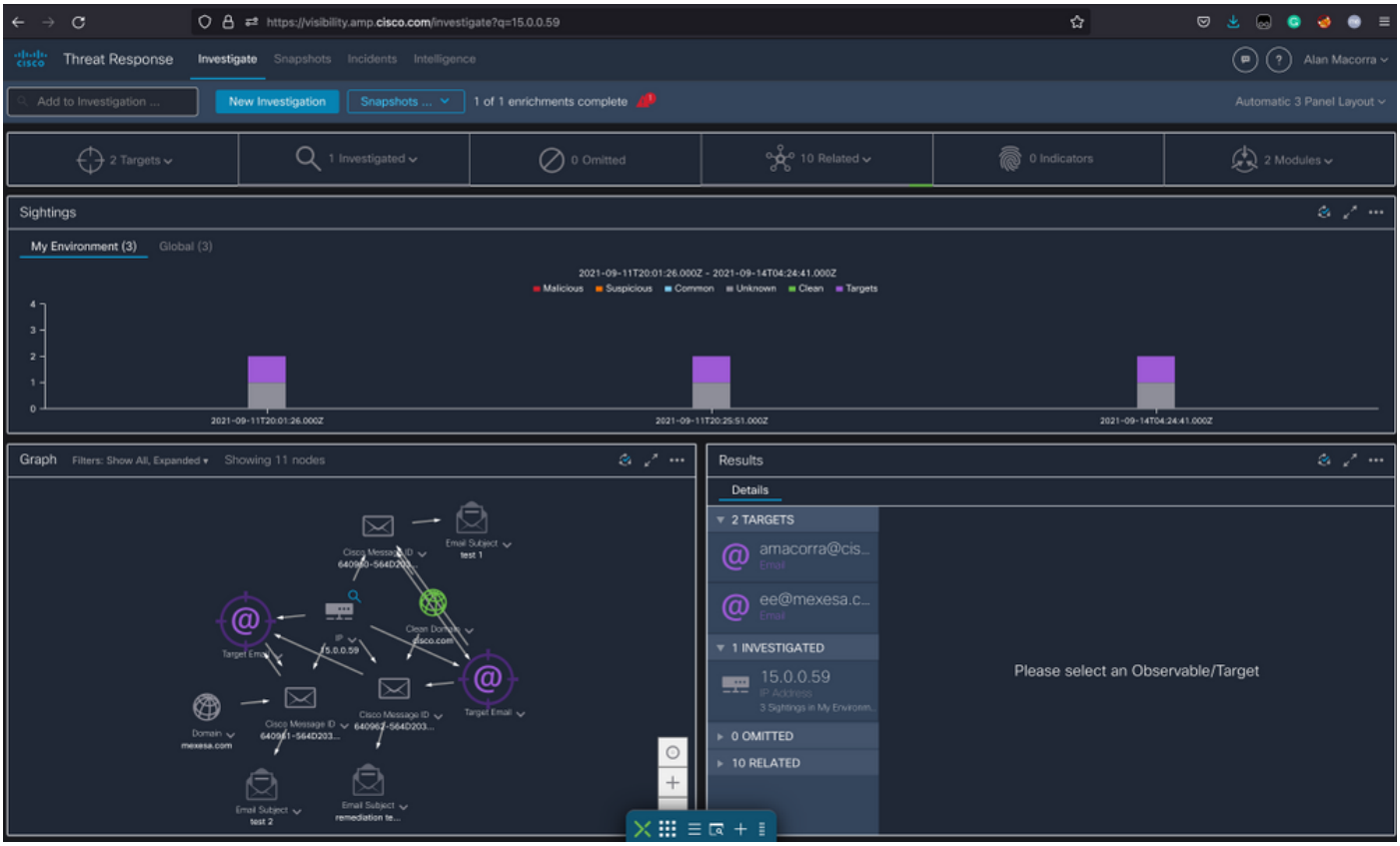
- US https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- EU https://visibility.eu.amp.cisco.com/investigate

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:

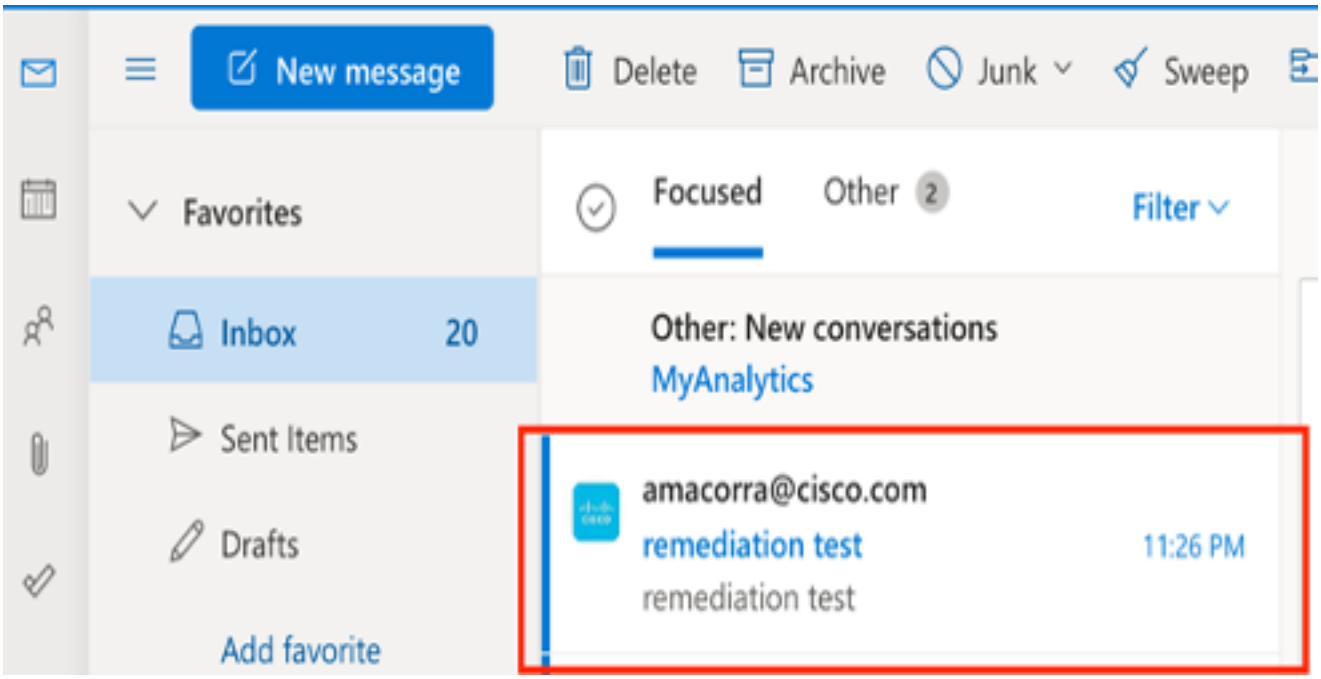
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

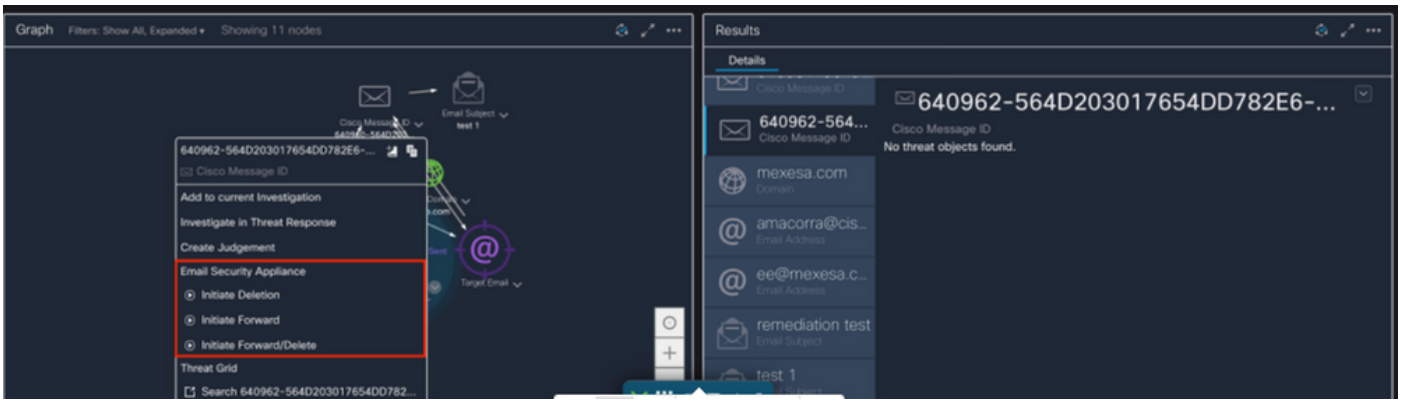




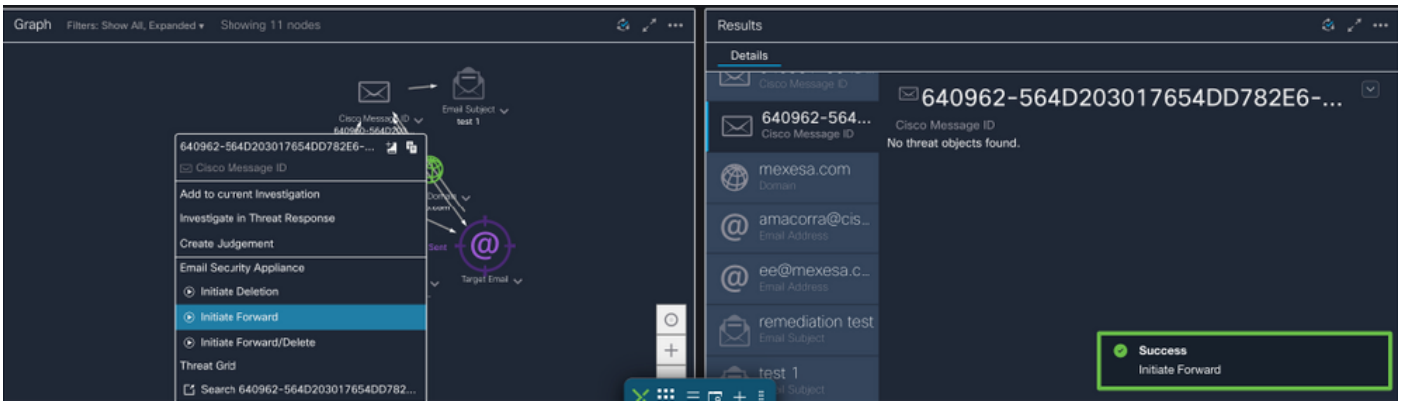
2.2 Aqui está o que você recebe em sua caixa de entrada antes que a mensagem seja remediada, como mostrado na imagem:



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:

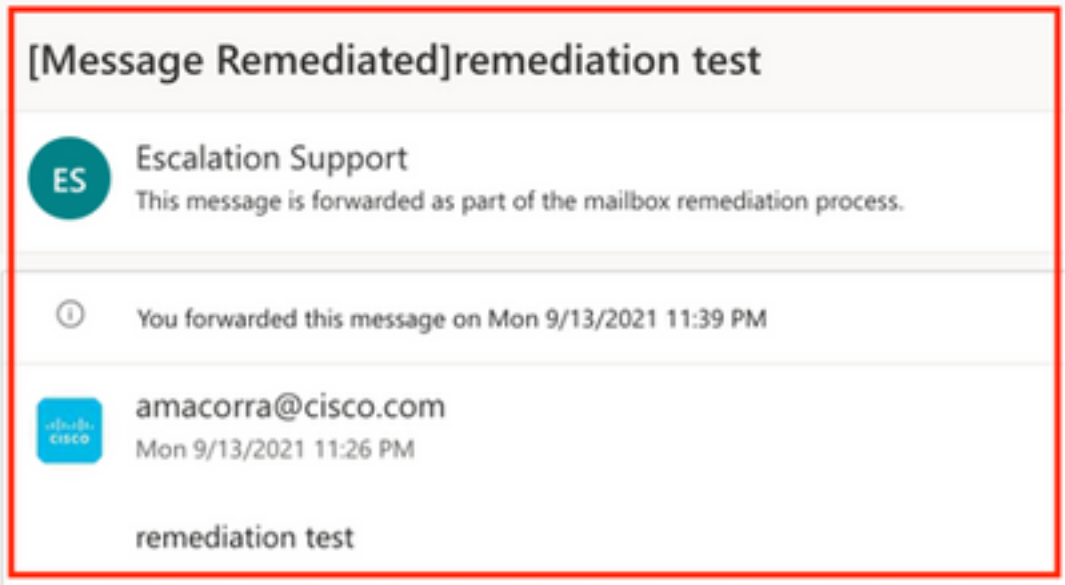


2.5 No ESA, você pode ver os seguintes registros em "mail_logs" que mostram que a correção "CTR" é iniciada, a ação selecionada e o status final.

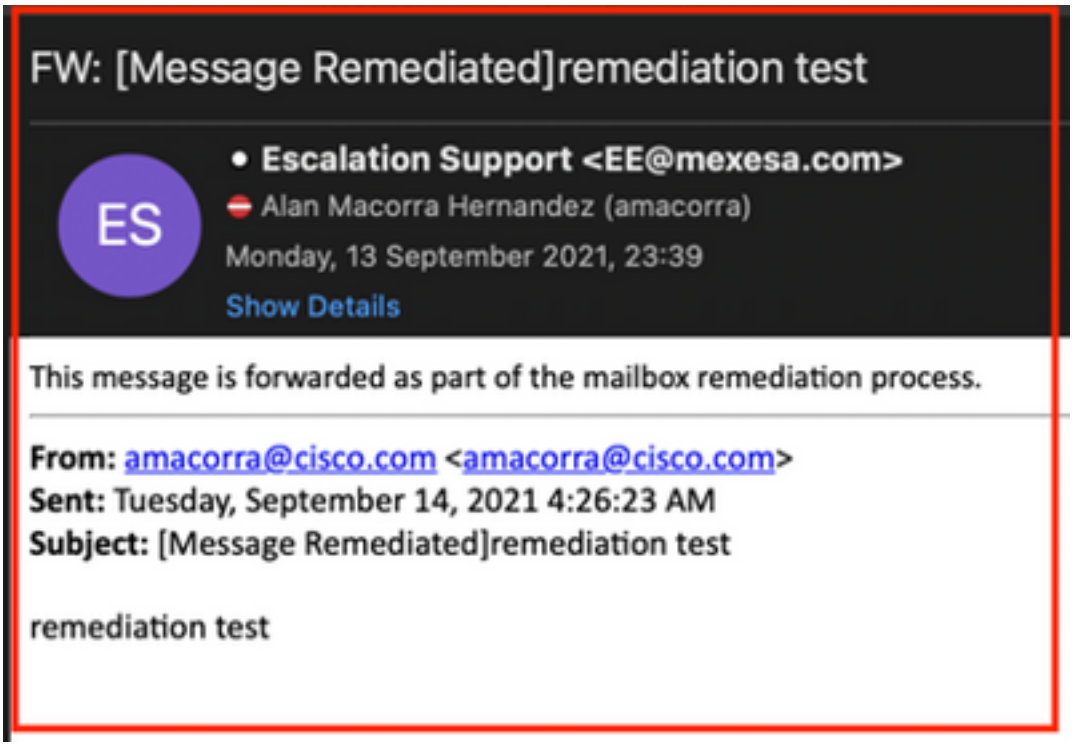
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

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.
```

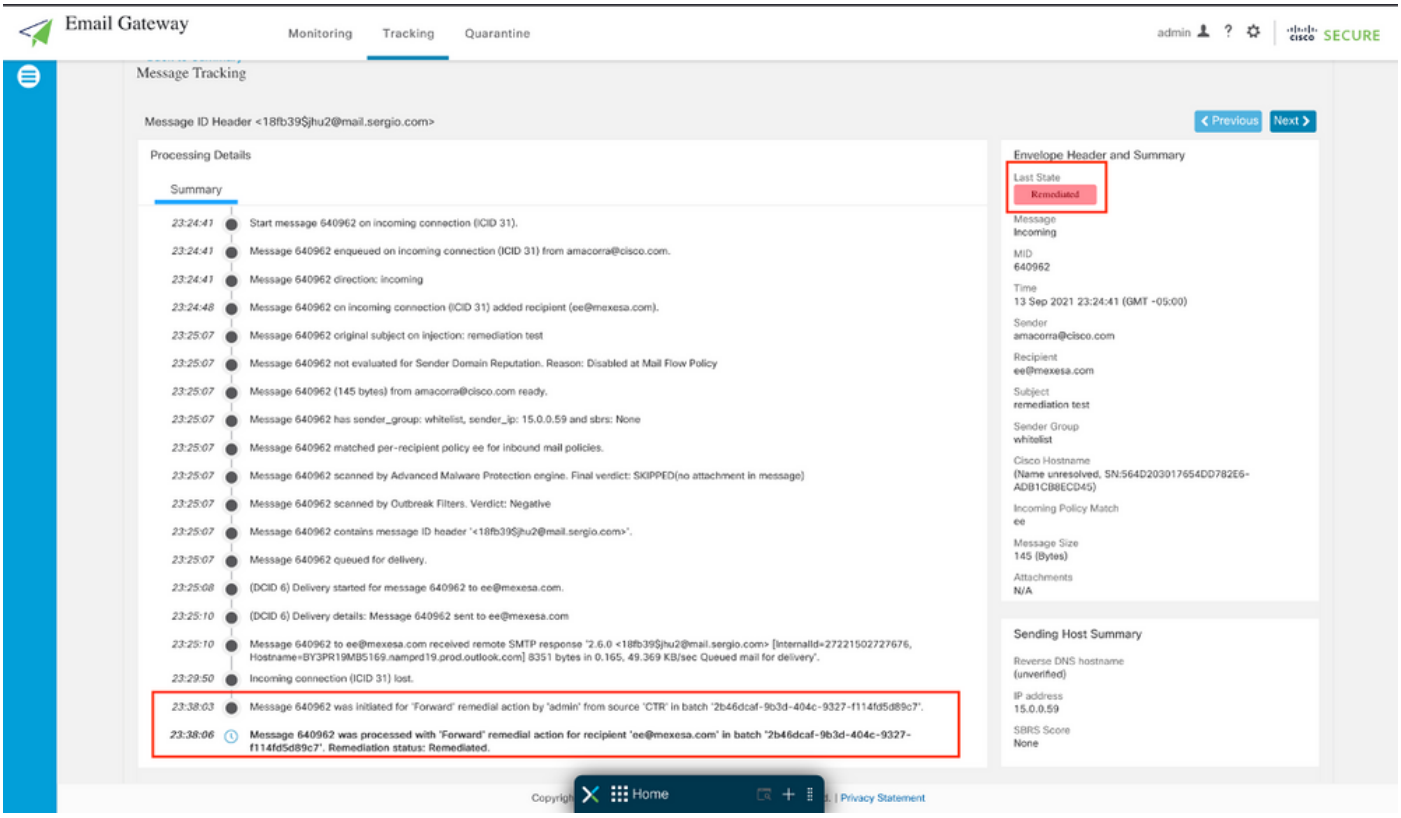
2.6 A instrução "[Message Remediated]" aparece anexada no assunto da mensagem, como mostrado na imagem:



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:



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.