# Como corrigir e-mails do CTR

#### Contents

Introduction

Informações de Apoio

Componentes Utilizados

<u>Configurar</u>

<u>Verificação</u>

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 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 <a href="https://visibility.amp.cisco.com/investigate">https://visibility.amp.cisco.com/investigate</a>
- APJC <a href="https://visibility.apjc.amp.cisco.com/investigate">https://visibility.apjc.amp.cisco.com/investigate</a>
- 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:

$\leftarrow \rightarrow \mathbf{G}$	C A 🕫 https://visibility.amp. <b>cisco.com</b> /investigate			습 🛛 🖻 🛓 😡 🕥 🤘	
threat Response	Response Investigate Snapshots Incidents Intelligence				🗭 🕐 Alan Macorra ~
ip: "15.0.0.59"					
					٢
Investigate Upload Sna	pshot What can I search for?				Auto Omit
		<u> </u>		<u></u>	
← → C	O H ≓ https://visibility.amp.cisco.com/invest	igate?q=15.0.0.59		ជ	
Cisco Threat Response	Investigate Snapshots Incidents Intelligent				(P) (?) Alan Macorra ~
<ul> <li>Add to Investigation</li> </ul>	New Investigation Snapshots Y	1 of 1 enrichments complete 🥔			
2 Targets V	Q 1 Investigated ~	0 Omitted	ာမ္ရွိ 10 Related 🗸	0 Indicators	2 Modules V
Sightings					8 Z ···
My Environment (3) Globa					
		2021-09-11T20:01:26.0002 Malicious Suspicious Comm	Z - 2021-09-14T04:24:41.000Z non ■ Unknown ■ Clean ■ Targets		
3					
2 -					
			ļ		
	2021-09-11T20.01:26.000Z	2021-09-1	1T20:25:51.000Z	2021-09-14T04	124/41.000Z
Graph Filters: Show All, Expande		8.7 ···	Results		
		÷,	Details		
		∑ ISubject ↓	amacorra@cis		
Cost desset (U ~ text 1 640960-5640701.			Email		
	Target Emo	×	▼ 1 INVESTIGATED		
		@	15.0.0.59	Please select an Obse	ervable/Target
	Cisco Message ID Cisco	Target Email 🥪	3 Sightings in My Environm		
m	exess.com	0	► 10 RELATED		
	test 2 remediation te	× ::: =			

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

	■ 🗹 New message	🗓 Delete 🖻 Archive 🚫 Junk 🗸 🚿 Sweep 🚦
Ē	$\checkmark$ Favorites	
RR	🚨 Inbox 20	Other: New conversations
0	▷ Sent Items	amacorra@cisco.com
Ø	🖉 Drafts	remediation test 11:26 PM
	Add favorite	

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:

Graph Filters: Show All, Expanded + Showing 11 nodes	3 / ···	Results	8.7 ···
		Details	
$\boxtimes \rightarrow \boxtimes$	2	Cisco Message ID	⊠640962-564D203017654DD782E6-
Coop Messing of Messin	Bubject ↓ x1	640962-564 Cisco Message ID	Cisco Message ID No threat objects found.
🖂 Cisco Message ID		mexesa.com	
Add to current investigation			
Investigate in Threat Response	<u>+</u>	amacorra@cis	
Create Judgement Sert	@}	Email Address	
Email Security Appliance		ee@mexesa.c	
		Email Address	
<ul> <li>Initiate Forward</li> </ul>	$\circ$	, remediation test	
<ul> <li>Initiate Forward/Delete</li> </ul>	± 1		Success
Threat Grid	· · · ·		Initiate Forward
Search 640962-564D203017654DD782	× = -	J Subject	

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:

FW: [Message Remediated]remediation test			
ES	<ul> <li>Escalation Support <ee@mexesa.com></ee@mexesa.com></li> <li>Alan Macorra Hernandez (amacorra)</li> <li>Monday, 13 September 2021, 23:39</li> <li>Show Details</li> </ul>		
This message is forwarded as part of the mailbox remediation process.			
From: amacorra@cisco.com <amacorra@cisco.com> Sent: Tuesday, September 14, 2021 4:26:23 AM Subject: [Message Remediated]remediation test remediation test</amacorra@cisco.com>			

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:

$\triangleleft$	Kenail Gateway Monitoring Tracking Quarantine admin 1 ? 🌣 🕴					
0	Message Tracking					
	message to ne	กณี - เมาวลว์ในกรณ์แต่แรลเสียวกับแร				
	Processing De Summary	aits	Envelope Header and Summary Last State Reputato			
	23:24:41	Start message 640962 on incoming connection (ICID 31).	Message Incoming			
	23:24:41	Message 640962 enqueued on incoming connection (ICID 31) from amacorra@cisco.com.	MID 640952			
	23:24:41	Message 640962 direction: incoming	Time			
	23:24:48	Message 640962 on incoming connection (ICID 31) added recipient (ee@mexesa.com).	13 Sep 2021 23:24:41 (GMT -05:00) Sender			
	23:25:07	Message 640962 original subject on injection: remediation test	amacorra@cisco.com			
	23:25:07	Message 640962 not evaluated for Sender Domain Reputation. Reason: Disabled at Mail Flow Policy	Recipient ee@mexesa.com			
	23:25:07	Message 540952 (145 bytes) from amacorra@cisco.com ready.	Subject remediation test			
	23:25:07	Message 640962 has sender_group: whitelist, sender_ip: 15.0.0.59 and sbrs: None	Sender Group			
	23:25:07	Message 640962 matched per-recipient policy ee for inbound mail policies.	whitelist Cisco Hostname			
	23:25:07	Message 640962 scanned by Advanced Malware Protection engine. Final verdict: SKIPPED(no attachment in message)	(Name unresolved, SN:564D203017654DD782E6- ADB1CB8ECD45)			
	23:25:07	Message 640962 scanned by Outbreak Filters. Verdict: Negative	Incoming Policy Match			
	23:25:07	Message 640962 contains message ID header '<18fb39\$jbu2@mail.sergio.com>'.	ee Messace Size			
	23:25:07	Message 640962 queued for delivery.	145 (Bytes)			
	23:25:08	(DCID 6) Delivery started for message 640962 to ee@mexesa.com.	Attachments N/A			
	23:25:10	(DCID 6) Delivery details: Message 640962 sent to ee@mexesa.com				
	23:25:10	Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18/b39\$jhu2@mail.sergio.com> [internalid=27221502727676, Hostname-BY3PR19MB5169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.	Sending Host Summary Reverse DNS hostname			
	23:29:50	Incoming connection (ICID 31) lost.	(unverified)			
	23:38:03	Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.	IP address 15.0.0.59			
	23:38:06 (	Message (40962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327- f114fd5d89c7'. Remediation status: Remediated.	SBRS Score None			
		Copyrigh 🗙 III Home 🖙 + II all 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.