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:

<u>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:</u>

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

Èpossibile 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:

$\leftarrow \rightarrow \mathbf{G}$ 0.0	음 루 https://visibility.amp.cisco.com/inves	tigate		ث	☺ 👱 💀 😳 🧕 ≡
"dische Threat Response Investigate Snapshots Incidents Intelligence				🗭 ? Alan Macorra ~	
ip: "15.0.0.59"	ip: *15.0.0.59*				
Investigate Upload Snapshot	What can I search for?				Concentration Auto Omit
← → ♂	}	gate?q=15.0.0.59		ជ	⊌ 2 ⊗ 0 3 0 ≡
Cisco Threat Response Invest	tigate Snapshots Incidents Intelligenc				🗭 💎 Alan Macorra ~
Add to Investigation		1 of 1 enrichments complete 📕			
2 Targets V	Q 1 Investigated ~	0 Omitted	్లళ్లి 10 Related 🗸	0 Indicators	2 Modules 🗸
Sightings					8 / ···
4 - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -		2021-09-11729 01:26.000 Malicious Surpicious Com 2021-09-11 2021-09-1	2 - 2021-09-14T04-24-41.000Z mon = Unknown = Clean = Targets	2821-09-14754	24 41 000Z
Graph Filters: Show All, Expanded • S		@ / ···	Results		s / …
		<u>_</u>	Details		
та Сотпат н пинина сот	Con Messare 10 - Enel Con Con Messare 10 - Enel Con Con Messare 10 - Enel Con Con Messare 10 - Enel States 1 - Enel States	Stated v at 1 englet fund v	2 TARGETS amacorra@cis Enul ee@mexesa.c tinvestigateD Factors Signogs in My Environm. to ReLATED	Please select an Obs	ervable/Target

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

	■ 🗹 New message	🗓 Delete \Xi Archive 🚫 Junk 🗸 🎸 Sweep 🖻
†	\checkmark Favorites	
RR	🖓 Inbox 20	Other: New conversations
0	➢ Sent Items	amacorra@cisco.com
N	🖉 Drafts	remediation test 11:26 PM
	Add favorite	

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

Graph Fitters: Show All, Expanded + Showing 11 nodes	8 / ···	Results	8.7 ···	
		Details		
$\boxtimes \neg \boxtimes$		Cisco Message ID	■640962-564D203017654DD782E6-	
Claco Messa D V Mest 1		640962-564	Cisco Message ID	
640962-564D203017654DD782E6 🛃 🖷		Cisco Message ID	No threat objects found.	
🖂 Cisco Message ID		mexesa.com		
Add to current Investigation	-ff-	<i>A</i> ~	Domain	
Investigate in Threat Response		amacorra@cis		
Create Judgement	(@)	@}	Email Address	
Email Security Appliance		ee@mexesa.c		
Initiate Deletion		Email Address		
 Initiate Forward 	0	remediation test		
 Initiate Forward/Delete 	+	Emeil Subject		
Threat Grid		test 1		
Search 640962-564D203017654DD782		Al Schiert		

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:

FW: [Message Remediated]remediation test			
ES	 Escalation Support <ee@mexesa.com></ee@mexesa.com> Alan Macorra Hernandez (amacorra) Monday, 13 September 2021, 23:39 Show Details 		
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 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:

\triangleleft	Email Gateway	Monitoring Tracking Quarantine	admin 💄 ? 🌣 🔡 SECURE
₿	Message Trackir	g	
	Message ID Hea	ler <18fb39\$jhu2@mail.sergio.com>	< Previous Next >
	Processing Deta	its	Envelope Header and Summary
	Summary		Last State Remediated
	23:24:41	Start message 640962 on incoming connection (ICID 31).	Message
	23:24:41	Message 640962 engueued on incoming connection (ICID 31) from amacorra@cisco.com.	MID
	23:24:41	Message 640962 direction: incoming	640962 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)
	23:25:07	Message 640962 original subject on injection: remediation test	Sender 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 640962 (145 bytes) from amacorra@cisco.com ready.	Subject
	23:25:07	Message 640962 has sender_group: whitelist, sender_jp: 15.0.0.59 and sbrs: None	Sender Group
	23:25:07	Message 640962 matched per-recipient policy ee for inbound mail policies.	whitelist Circe Mesterer
	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\$jhu2@mail.sergio.com>".	Message 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.	N/A
	23:25:10	(DCID 6) Delivery details: Message 640962 sent to ee@mexesa.com	Condian Uses Common
	23:25:10	Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18/b395/bu2@mail.sergio.com> [Internalld=27221502727676, Hostname=BY3PR19MB5169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.	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'.	15.0.0.59
	23:38:06	Message 640962 was processed with "Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327- f114fd5d89c7'. Remediation status: Remediated.	SBRS Score None
		Copyrign 🗙 III Home 🗔 + II s. 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 <u>modulo di integrazione</u>.