E-mails van CTR verhelpen

Inhoud

Inleiding Achtergrondinformatie Gebruikte componenten Configureren Verificatie Stap 1. Toegang tot het CTR-portal op basis van de toegang tot beschikbare servers en onderzoek Stap 2. Onderzoek de geleverde berichten die kwaadaardig of bedreigend lijken te zijn door gebruik te maken van de ondersteunde wachtwoorden. De waarnemingen kunnen aan de hand van de volgende criteria worden bezocht, zoals in de afbeelding wordt getoond: 2.1 Onderstaand een voorbeeld van een onderzoek en onderzoek in het kader van het OT, zoals blijkt uit de beelden:

2.2 Dit krijgt u in uw inbox voordat het bericht wordt hersteld, zoals in de afbeelding wordt getoond:

2.3 Selecteer in het menu-opties een van de ondersteunde bewerkingsacties zoals in de afbeelding:

2.4 In dit voorbeeld wordt "Vooruit openen" geselecteerd en verschijnt een Success pop-upvenster in de rechterbenedenhoek, zoals in de afbeelding:

2.5 In het ESA, kunt u de volgende logbestanden zien onder "mail_logs" die laten zien dat het "CTR"-herstel start, de geselecteerde actie en de definitieve status.

2.6 Het bericht "[Bericht geremedieerd]" wordt in het bericht voorgedrukt, zoals in de afbeelding weergegeven:

2.7 Het e-mailadres dat u typt bij het configureren van de ESA/SMA-module, is het emailadres dat u ontvangt wanneer u de optie "Voorwaarts" of "Voorwaarts/Verwijderen" selecteert, zoals in de afbeelding wordt weergegeven:

2.8 Ten slotte, als je kijkt naar de informatie-tracking details van de nieuwe interface van de ESA/SMA, dan zie je dezelfde logbestanden die zijn verkregen in "mail logs" en "Laatste Staat" als "Geremedieerd", zoals in de afbeelding getoond wordt:

Inleiding

Dit document beschrijft hoe u e-mails van Cisco Threat Response (CTR) kunt verbeteren.

Achtergrondinformatie

Het CTR-onderzoek is bijgewerkt om de correctie van OnDemand Mail te ondersteunen. Admin kan specifieke e-mails van O365 en OnPrem Exchange-gebruikersmailboxen doorzoeken en deze herstellen door een e-mail security applicatie (ESA) of security Management-applicatie (SMA).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CTR-account
- Cisco Security Services exchange
- ESR AS 14.0.1-033

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Opmerking: Zoeken en mailverbetering wordt alleen ondersteund in O365, Exchange 2016 & 2019 Hybrid-implementaties en On-Prem 2013 Exchange implementaties.

Configureren

- 1. Accountinstellingen instellen in de ESA
- 2. Geketend profiel configureren en de domein(en) in kaart brengen naar het accountprofiel
- 3. Integreren met CTR of ESA of SMA

Verificatie

U kunt de observeermiddelen in het CTR-portal onderzoeken en het bericht voor herstel selecteren in de volgende stappen:

Stap 1. Toegang tot het CTR-portal op basis van de toegang tot beschikbare servers en onderzoek

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

Stap 2. Onderzoek de geleverde berichten die kwaadaardig of bedreigend lijken te zijn door gebruik te maken van de ondersteunde wachtwoorden. De waarnemingen kunnen aan de hand van de volgende criteria worden bezocht, zoals in de afbeelding wordt getoond:

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 Onderstaand een voorbeeld van een onderzoek en onderzoek in het kader van het OT, zoals blijkt uit de beelden:

$\leftarrow \rightarrow \mathbf{G}$	C O A ≠ https://visibility.amp.cisco.com/investigate			ជ	🗢 🕹 🗟 🥥 曼 ≡
threat Response					🔎 🕐 Alan Macorra 🗸
ip: "15.0.0.59"					
					•
Investigate Upload Snaps	shot What can I search for?				🚾 Auto Omit
				····	
$\leftarrow \rightarrow \mathbf{G}$	O A	tigate?q=15.0.0.59		습	☺ ৬
cisco Threat Response	Investigate Snapshots Incidents Intelligen				🗭 ? Alan Macorra 🗸
Add to Investigation		1 of 1 enrichments complete 🔑			
2 Targets ~	Q 1 Investigated ~	0 Omitted	ార్లి 10 Related 🗸	0 Indicators	2 Modules 🗸
Sightings					8 / ···
My Environment (3) Global (
		2021-09-11T20:01:26.000 Malicious Suspicious Comm	Z - 2021-09-14T04:24:41.000Z mon == Unknown == Clean == Targets		
4					
2 -	-		_	-	-
1					
	2021-09-11120.01:26.000Z	0.01.26.000Z 2021-09-11120-25:51.000Z		2021-09-14T04:24:41.000Z	
Graph Filters: Show All, Expanded		8 / ···	Results		8.2 ···
	,	<u> </u>	Details		
			V 2 TARGETS		
	Cisco Messara (0 , 640940-5640200 ,	lest 1	@ amacorra@cis		
			@ ee@mexesa.c		
	Cost Dorte				
	Target Emoly		15.0.0.59	Please select an Obs	ervable/Target
6		Target Email -	3 Sightings in My Environm		
D. mex	Cisco Message ID ~ 640961-5640203 esa.com		▶ 0 OMITTED		
	ð Ø	+	▶ 10 RELATED		
	Ernal Subject V test 2 remediation te				

2.2 Dit krijgt u in uw inbox voordat het bericht wordt hersteld, zoals in de afbeelding wordt getoond:



2.3 Selecteer in het menu-opties een van de ondersteunde bewerkingsacties zoals in de afbeelding:



2.4 In dit voorbeeld wordt "Vooruit openen" geselecteerd en verschijnt een Success pop-upvenster in de rechterbenedenhoek, zoals in de afbeelding:

Graph Filters: Show All, Expanded + Showing 11 nodes	ø / …	Results	& / ···
		Details	
- 🖂	- 🛛	Cisco Message ID	
Cmp Messar A0 Super Supe		640962-564 Cisco Message ID	Cisco Message ID No threat objects found.
Cisco Message ID	R	mexesa.com	
Add to current Investigation	~ ftf~	Doman 🛛	
Investigate in Threat Response		amacorra@cis	
Create Judgement	Sent + @ +	Email Address	
Email Security Appliance		ee@mexesa.c	
 Initiate Deletion 	→ target Email →	Email Address	
 Initiate Forward 	0	remediation test	
 Initiate Forward/Delete 		Email Subject	Success
Threat Grid		🚔 test 1	Initiate Forward
Search 640962-564D203017654DD782		Subject	

2.5 In het ESA, kunt u de volgende logbestanden zien onder "mail_logs" die laten zien dat het "CTR"-herstel start, de geselecteerde actie en de definitieve status.

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 Het bericht "[Bericht geremedieerd]" wordt in het bericht voorgedrukt, zoals in de afbeelding weergegeven:



2.7 Het e-mailadres dat u typt bij het configureren van de ESA/SMA-module, is het emailadres dat u ontvangt wanneer u de optie "Voorwaarts" of "Voorwaarts/Verwijderen" selecteert, zoals in de afbeelding wordt weergegeven:

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 Ten slotte, als je kijkt naar de informatie-tracking details van de nieuwe interface van de ESA/SMA, dan zie je dezelfde logbestanden die zijn verkregen in "mail_logs" en "Laatste Staat" als "Geremedieerd", zoals in de afbeelding getoond wordt:

\triangleleft	Email Gateway	Monitoring Tracking Quarantine	admin 🚣 ? 🌣 🔤 🐮 SECURE				
⊜	Message Tracking						
	Message ID Hea	der <18fb39\$jhu2@mail.sergio.com>	✓ Previous Next >				
	Processing Det	aits	Envelope Header and Summary				
	Summary		Last State Krmediated				
	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 640962				
	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	ee@mexesa.com				
	23:25:07	Message 640962 (145 bytes) from amacorra@clsco.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.	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\$jhu2@mail.sergio.com>'.	Message Size				
	23:25:07	Message 640962 queued for delivery.	145 (Bytes) Attachments				
	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	Sending Host Summary				
	23:25:10	Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18fb39\$/hu2@mail.sergio.com> [internalid=27221502727676, Hostname=BY3PR19M85169.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 '2b46dtaf-9b3d-404c-9327-f114fd5d89c7'.	IP address 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				
		copyrigh 🗙 III Home 🖙 + II all Privacy Statement					

Opmerking: Er kunnen verschillende corrigerende maatregelen worden genomen. Als u de functie in uw ESA/SMA instelt om te zoeken en te verbeteren, dan kunt u hetzelfde bericht corrigeren vanaf CTR en ook via ESA/SMA. Hierdoor kunt u hetzelfde bericht doorsturen naar een ander e-mailadres dan het bericht dat in de <u>integratiemodule</u> is ingesteld.