Comment corriger les e-mails à partir de CTR

Contenu

Introduction

Informations générales

Components Used

Configuration

Vérification

Étape 1. Accédez au portail CTR en fonction de l'accès aux serveurs disponibles et examinez Étape 2. Examinez les messages transmis qui semblent malveillants ou dangereux à l'aide des observables pris en charge. Les observables peuvent être recherchés selon les critères suivants, comme l'illustre l'image :

2.1 Exemple d'enquête et d'enquête sur la PI ci-dessous, comme le montrent les images :

2.2 Voici ce que vous recevez dans votre boîte de réception avant que le message ne soit corrigé, comme l'illustre l'image :

2.3 En cliquant sur « ID de message Cisco », sélectionnez dans les options de menu l'une des actions résolues prises en charge, comme illustré dans l'image :

2.4 Dans cet exemple, « Initiate Forward » est sélectionné et une fenêtre contextuelle Success apparaît dans le coin inférieur droit, comme l'illustre l'image :

2.5 Dans l'ESA, vous pouvez voir les journaux suivants sous « mail_logs » qui montrent que la correction « CTR » démarre, l'action sélectionnée et l'état final.

2.6 L'instruction "[Message Remediated]" apparaît en avant-plan dans l'objet du message, comme l'illustre l'image :

2.7 L'adresse e-mail que vous saisissez lors de la configuration du module ESA/SMA est celle qui reçoit les e-mails corrigés lors de la sélection de l'option « Transfert » ou « Transfert/Suppression », comme illustré sur l'image :

2.8 Enfin, si vous regardez les détails du suivi des messages de la nouvelle interface du ESA/SMA, vous pouvez voir les mêmes journaux obtenus dans les « mail logs » et « Last State » que « Remediated », comme le montre l'image :

Introduction

Ce document décrit comment corriger les e-mails provenant de Cisco Threat Response (CTR).

Informations générales

L'enquête CTR a été mise à jour pour prendre en charge la correction des messages à la demande. L'administrateur peut rechercher des e-mails spécifiques à partir de boîtes aux lettres utilisateur O365 et OnPrem Exchange et y remédier via un dispositif de sécurité de la messagerie électronique (ESA) ou un dispositif de gestion de la sécurité (SMA).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Compte 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Note: La correction des recherches et des courriers est prise en charge dans les déploiements hybrides O365, Exchange 2016 et 2019 et dans les déploiements Exchange sur site 2013 uniquement.

Configuration

- 1. Configurer les paramètres de compte dans l'ESA
- 2. Configurer le profil chaîné et mapper le ou les domaines au profil de compte
- 3. Intégrer CTR à ESA ou SMA

Vérification

Vous pouvez rechercher les observables dans le portail CTR et sélectionner le message à corriger en procédant comme suit :

Étape 1. Accédez au portail CTR en fonction de l'accès aux serveurs disponibles et examinez

- États-Unis https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- UE https://visibility.eu.amp.cisco.com/investigate

Étape 2. Examinez les messages transmis qui semblent malveillants ou dangereux à l'aide des observables pris en charge. Les observables peuvent être recherchés selon les critères suivants, comme l'illustre l'image :

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 Exemple d'enquête et d'enquête sur la PI ci-dessous, comme le montrent les images :

$\leftarrow \rightarrow G$	○ A ∓² https://visibility.amp. cisco.com /investigate			ជ	
threat Response	e Investigate Snapshots Incidents Intelligence				🗭 ? Alan Macorra ~
ip: "15.0.0.59"					
					٢
Investigate Upload Sna	pshot What can I search for?				👀 Auto Omit
		.		.	
$\leftarrow \ \rightarrow \ G$	O A = https://visibility.amp.cisco.com/invest	tigate?q=15.0.0.59		습	☺ 👱 😞 🥥 🧐 ≡
threat Response	Investigate Snapshots Incidents Intelligen				🔎 ? Alan Macorra ~
 Add to Investigation 	New Investigation Snapshots Y	1 of 1 enrichments complete 🔑			
2 Targets 🗸	Q 1 Investigated ~	0 Omitted	్లోలో 10 Related 🗸	0 Indicators	😥 2 Modules 🗸
Sightings					8 / ···
My Environment (3) Globa					
4-		2021-09-11T20:01:26.0002 Malicious Suspicious Comm	z - 2021-09-14T04:24:41.000Z non ≡ Unknown ≡ Clean ≡ Targets		
3-					
2 -					
.1					
	2021-09-11120.01.26.0002	2021-09-1	1120.25.51.0002	2021-09+1410	24.41.0002
Graph Filters: Show All, Expande		@ / ···	Results		\$ / ···
		Ê,	Details		
		∑ i Subject ↓	amacorra@cis_		
	640940-564D294	lest 1	Emal		
	🍈 – 🚔 🔌		@ ee@mexesa.c		
	Durret French	Ň	▼ 1 INVESTIGATED		
		@	15.0.0.59	Please select an Obse	ervable/Target
		Target Email 🗸	3 Sightings in My Environm		
~	Domain V 640961-5640203 exess.com	0	▶ 0 OMITTED		
		+	▶ 10 RELATED		
	Erral Subject V test 2 remediation te	N			
		/ !!! =			

2.2 Voici ce que vous recevez dans votre boîte de réception avant que le message ne soit corrigé, comme l'illustre l'image :



2.3 En cliquant sur « ID de message Cisco », sélectionnez dans les options de menu l'une des actions résolues prises en charge, comme illustré dans l'image :

Graph Fitters: Show All, Expanded + Showing 11 nodes	8 / ···	Results	6.7 m	
		Details		
<u>∽</u>	- 🛛 🔹	Cisco Message ID	≅640962-564D203017654DD782E6-	
City Manual, City City Manual, City 640962-5640203017565400782E6		640962-564 Cisco Message ID	Cisco Message ID No threat objects found.	
🖂 Cisco Message ID			mexesa.com	
Add to current Investigation		🐭 Domain		
Investigate in Threat Response				@ amacorra@cis
Create Judgement	•••• (@)	Email Address		
Email Security Appliance	Tang front as	ee@mexesa.c		
Initiate Deletion		Ernail Address		
 Initiate Forward 	0	remediation test		
 Initiate Forward/Delete 	+	Email Subject		
Threat Grid	· · · · · · · · · · · · · · · · · · ·	🚖 test 1		
[] Search 640962-564D203017654DD782		al Schinet		

2.4 Dans cet exemple, « Initiate Forward » est sélectionné et une fenêtre contextuelle Success apparaît dans le coin inférieur droit, comme l'illustre l'image :

Graph Filters: Show All, Expanded + Showing 11 nodes	& / ···	Results	& / ···
		Details	
⊠ -	- 🛛	Cisco Message ID	
Cisog Messay (0	Emeil Sutject 🤝 Nest 1	640962-564 Cisco Message ID	Cieco Message ID No threat objects found.
Cisco Message ID	2	mexesa.com	
Add to current Investigation	erte -	Domain	
Investigate in Threat Response		amacorra@cis	
Create Judgement	Sert + @ +	Email Address	
Email Security Appliance		ee@mexesa.c	
 Initiate Deletion 	- arget trial -	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 Dans l'ESA, vous pouvez voir les journaux suivants sous « mail_logs » qui montrent que la correction « CTR » démarre, l'action sélectionnée et l'état 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 L'instruction "[Message Remediated]" apparaît en avant-plan dans l'objet du message, comme l'illustre l'image :



2.7 L'adresse e-mail que vous saisissez lors de la configuration du module ESA/SMA est celle qui reçoit les e-mails corrigés lors de la sélection de l'option « Transfert » ou « Transfert/Suppression », comme illustré sur l'image :

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 Enfin, si vous regardez les détails du suivi des messages de la nouvelle interface du ESA/SMA, vous pouvez voir les mêmes journaux obtenus dans les « mail_logs » et « Last State » que « Remediated », comme le montre l'image :

\triangleleft	Kemail Gateway Monitoring Tracking Quarantine admin 1 ? 🌣 🖞 🖞 SEC			
0	Message Tracki	ng uter e180-30\$34/200mail service.com>	C Previous Next Y	
	message to ne	นขา < เอเมออัปทางสุขาหละออาฟิตรรษทาง		
	Processing De Summary	ails	Envelope Header and Summary Last State Remduted	
	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	Recipient ee@mexesa.com	
	23:25:07	Message 640962 (145 bytes) from amacorra@oisco.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\$jihu2@mail.sergio.com>'.	ee 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	Condition Used Community	
	23:25:10	Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18fb39\$/jbu2@mail.sergio.com> [internalid=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'.	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 X III Home C + I all Privacy Statement		

Note: Plusieurs correctifs peuvent se produire, si vous configurez dans votre ESA/SMA la fonctionnalité à rechercher et à corriger, vous pouvez corriger le même message à partir de CTR et aussi de ESA/SMA. Cela peut vous permettre de transférer le même message à une adresse de messagerie différente de celle configurée dans le <u>module d'intégration</u>.