

Carochan

Captures d'écran TheHive : Ouverture et clôture de dossiers

Analyste : N. Clerbout

Création du Dossier (Case) #1 avec tâches associées :

Case # 1 - Brute Force Attack

Analyst 07/15/24 11:56 3 minutes 1 alert

Sharing (0) | Close | Flag | Merge | Remove

Details

Tasks 6

Observables 3

TTPs

No tasks selected + Add Task Quick Filters

Show Groups Filters 15 per page

Filters

+ Add a filter

List of tasks (6 of 6)

	Group	Task	Date	Assignee	Actions
<input type="checkbox"/>	Not Specified	Analyse des serveurs DC de la zone Europe		Analyst	
<input type="checkbox"/>	Not Specified	Appliquer authentification à plusieurs facteurs		Admin	
<input type="checkbox"/>	default	Compte carter : révocation du token d'authentification + réinitialisation du mot de passe		Admin	
<input type="checkbox"/>	Not Specified	Mise à jour des GPOs relatives aux accès anonymes		Admin	
<input type="checkbox"/>	Not Specified	Revoir configuration du nombre/fréquence de tentatives d'authentification avant blocage du compte		Admin	
<input type="checkbox"/>	Not Specified	Règle Snort : reject tcp 104.244.77.53 any <> \$HOME_NET any (msg: <IP 104.244.77.53 detected>; sid: 1000001; rev: 1)		Admin	

Création du Dossier #2 avec tâches associées :

Case # 2 - Suspicious remote administration of accounts and privileges

Analyst 07/15/24 12:04 5 minutes 2 alerts

Sharing (0) | Close | Flag | Merge | Remove

Details

Tasks 5

Observables 4

TTPs

No tasks selected + Add Task Quick Filters

Show Groups Filters 15 per page

Filters

+ Add a filter

List of tasks (5 of 5)

	Group	Task	Date	Assignee	Actions
<input type="checkbox"/>	Not Specified	Activation de Credential Guard		Admin	
<input type="checkbox"/>	Not Specified	Audit du groupe utilisateurs "Administrators"		Analyst	
<input type="checkbox"/>	Not Specified	Règle Snort : alert tcp 10.11.1.2 any <> \$HOME_NET 88 (msg: <traffic towards port 88 from EU-DMZ>; sid: 1000002; rev: 1)		Admin	
<input type="checkbox"/>	default	Supprimer compte "ext-adm"		Admin	
<input type="checkbox"/>	Not Specified	compte "vagrant" : révocation du token d'authentification, réinitialisation du mot de passe, audit		Admin	

Création du Dossier #3 avec tâches associées :

Case # 3 - SMB scan

Analyst 07/15/24 12:09 2 minutes 1 alert

Sharing (0) | Close Flag Merge Remove

Details

Tasks 3

Observables 10

TTPs

No tasks selected

Add Task

Quick Filters

Show Groups

Filters

15

per page

Filters

Add a filter

List of tasks (3 of 3)

	Group	Task	Date	Assignee	Actions
<input type="checkbox"/>	Not Specified	Configuration de la GPO "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares"		Admin	
<input type="checkbox"/>	default	Déterminer comment l'attaquant a eu accès aux LANs Servers et Utilisateurs de la zone Europe		Analyst	
<input type="checkbox"/>	Not Specified	Revoir la segmentation réseau pour diminuer le nombre d'IP disponibles sur les LANs Servers et Utilisateurs (masques de sous-réseaux)		Admin	

Vue d'ensemble – 3 dossiers ouverts et 3 dossier clos :

Status	# Number	Title	Severity	Details	Assignee	Dates	S. C. U.
<input type="checkbox"/> Open 20 minutes	#1	Multiple authentication failures followed by success. Authentication Failure Bruteforce TOR RDP None	H	Tasks 6 Observables 3 TTPs 0	A	S. 07/15/24 11:56 C. 07/15/24 11:56	
<input type="checkbox"/> Open 12 minutes	#2	Suspicious remote administration of accounts and privileges user creation privileged user 4674 Privileged Object Operation Attempted None	U	Tasks 5 Observables 4 TTPs 0	A	S. 07/15/24 12:04 C. 07/15/24 12:04 U. 07/15/24 12:09	
<input type="checkbox"/> Open 7 minutes	#3	SMB scan Network Scan SMB None	M	Tasks 3 Observables 10 TTPs 0	A	S. 07/15/24 12:09 C. 07/15/24 12:09 U. 07/15/24 12:12	
<input type="checkbox"/> Closed a minute	#4	Malicious e-mail detected spam None (Closed at 07/15/24 12:13 as False Positive)	U	Tasks 0 Observables 2 TTPs 0	A	S. 07/15/24 12:12 C. 07/15/24 12:12 U. 07/15/24 12:13	
<input type="checkbox"/> Closed a few seconds	#5	Massive authentication failures Authentication Failure Bruteforce None (Closed at 07/15/24 12:15 as False Positive)	H	Tasks 0 Observables 2 TTPs 0	A	S. 07/15/24 12:14 C. 07/15/24 12:14 U. 07/15/24 12:15	
<input type="checkbox"/> Closed a few seconds	#6	Nmap scanner detected nmap Network Scanner None (Closed at 07/15/24 12:15 as False Positive)	M	Tasks 0 Observables 3 TTPs 0	A	S. 07/15/24 12:15 C. 07/15/24 12:15 U. 07/15/24 12:15	