Empêcher les appareils CrowdStrike d'une détection

Publié: 2024-08-08

Vous pouvez initier le confinement des appareils CrowdStrike participant à une détection de sécurité. Le confinement empêche les appareils d'établir des connexions avec d'autres appareils de votre réseau.

Une fois que vous avez initié le confinement à la suite d'une détection, une demande est envoyée à CrowdStrike Falçon pour contenir les appareils et le statut Containment Pending apparaît à côté du participant. Le statut est mis à jour à Contained uniquement lorsque le système ExtraHop reçoit une réponse de CrowdStrike.

Avant de commencer

- Le confinement des appareils doit être activé pour Intégration à CrowdStrike Z.
- Les utilisateurs doivent avoir accès au module NDR et disposer d'un nombre d'écriture limité privilèges
 d' ou supérieur pour effectuer les tâches décrites dans ce guide.
- 1. <extrahop-hostname-or-IP-address>Connectez-vous au système ExtraHop via https://.
- 2. En haut de la page, cliquez sur Détections.
- Cliquez sur le titre d'une détection pour afficher la page détaillée de la détection. Le nombre d'appareils CrowdStrike participant à la détection apparaît dans la section Intégrations sous Track Detection.

Track Detection						
Status		Assignee				
No Status	ø	Unassigned	ø			
Integrations						
CrowdStrike Falcon ^[2] 4 participants are CrowdStrike devices						
Contain Devices in CrowdStrike						
Actions						
Add to an Investigation						
Tune Dete	ection					

4. Cliquez Contenir les appareils dans CrowdStrike.

La boîte de dialogue affiche les appareils CrowdStrike associés à la détection.

Cor Selec initiat	Contain Devices in CrowdStrike Select CrowdStrike devices that are participants in this security detection to initiate containment in CrowdStrike Falcon.						
(∲) \	/ІСТІМ				Select All		
>	•	workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185					
0	•	workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185					
D		workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185					
			Cancel	Contain in Crov	vdStrike		

 Sélectionnez les appareils que vous souhaitez contenir et cliquez sur Contenu dans CrowdStrike. Une demande est envoyée à CrowdStrike et le statut Containment Pending apparaît à côté de chaque participant sélectionné.

Prochaines étapes

• Vérifiez le confinement de l'équipement en vérifiant son état à partir des détails de détection. L'état du confinement apparaît également dans propriétés de l'équipement .

🔶 VIСТІМ				
	workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185 CONTAINED	•		
	workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185 CONTAINMENT PENDING	0		
Ð	workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185 CONTAINMENT PENDING	•		

- Réessayez de contenir un équipement. Le statut Containment Pending n'apparaît plus lorsqu' une demande de confinement adressée à CrowdStrike est refusée ou expire.
- Libérez un équipement du confinement depuis la console CrowdStrike Falçon. Dans la section Intégrations, sous Détection des pistes, cliquez sur **CrowdStrike Falçon** pour ouvrir la console dans un nouvel onglet. L'état du confinement n'apparaît plus une fois que le système ExtraHop reçoit une réponse de CrowdStrike.