Empêcher les appareils CrowdStrike d'une détection

Publié: 2023-09-30

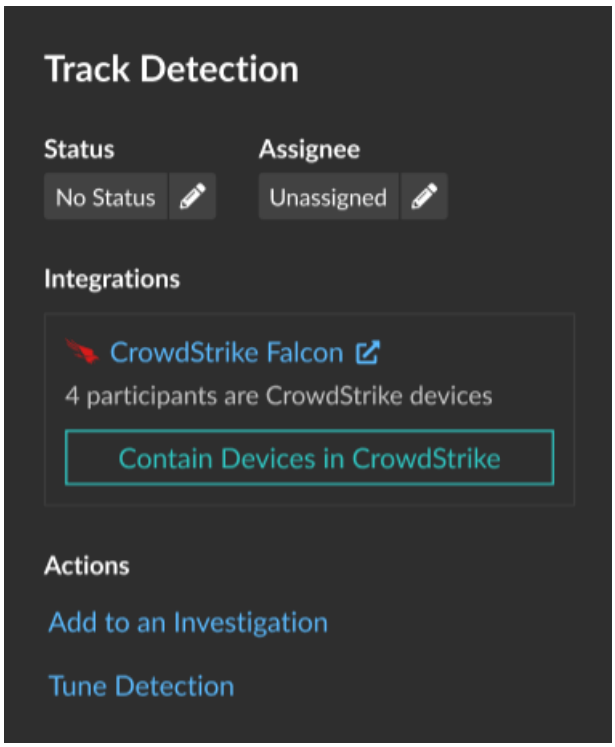
Vous pouvez initier le confinement des appareils CrowdStrike participant à une détection de sécurité. Le confinement empêche les appareils d'établir des connexions avec d'autres appareils de votre réseau.

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.

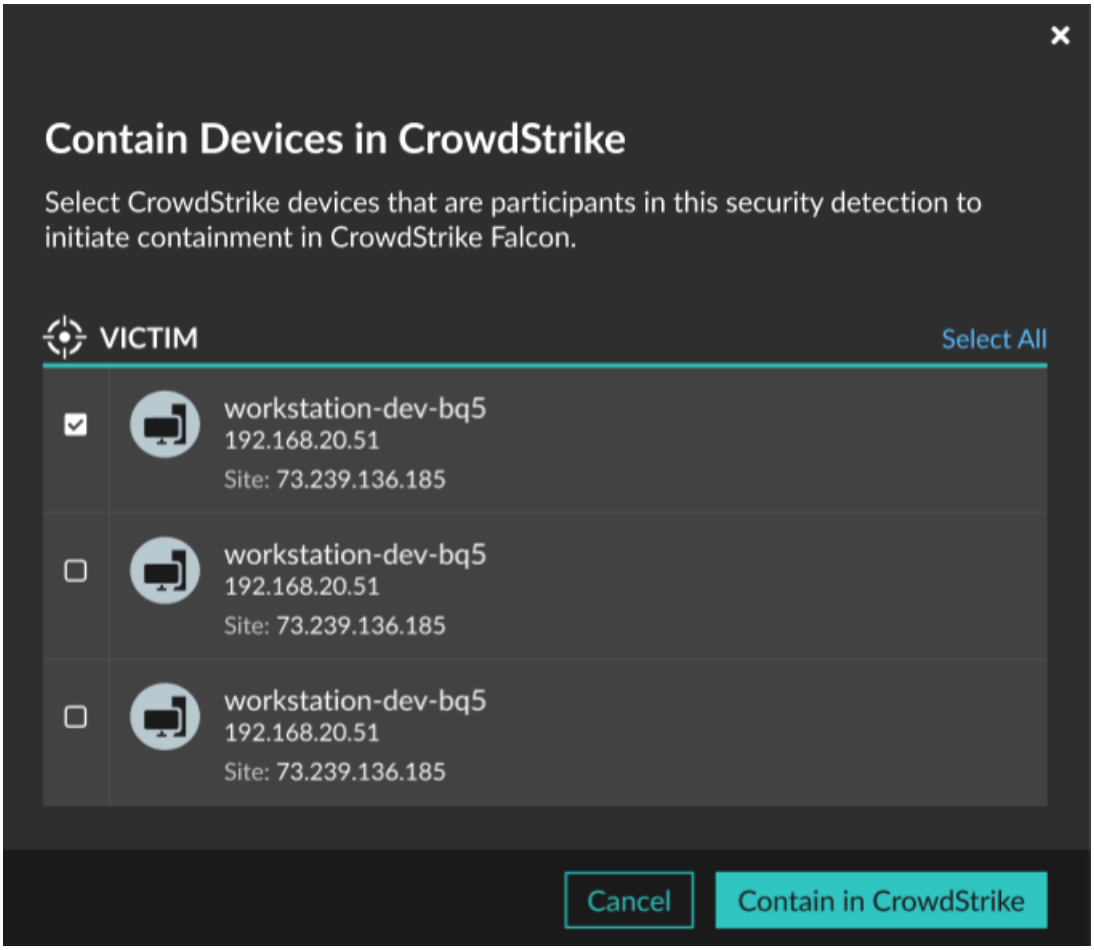
Avant de commencer

- Le confinement des appareils doit être activé pour Intégration à CrowdStrike.
- Les utilisateurs doivent avoir accès au module NDR et disposer d'un nombre d'écriture limité privilèges 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**.
3. 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.



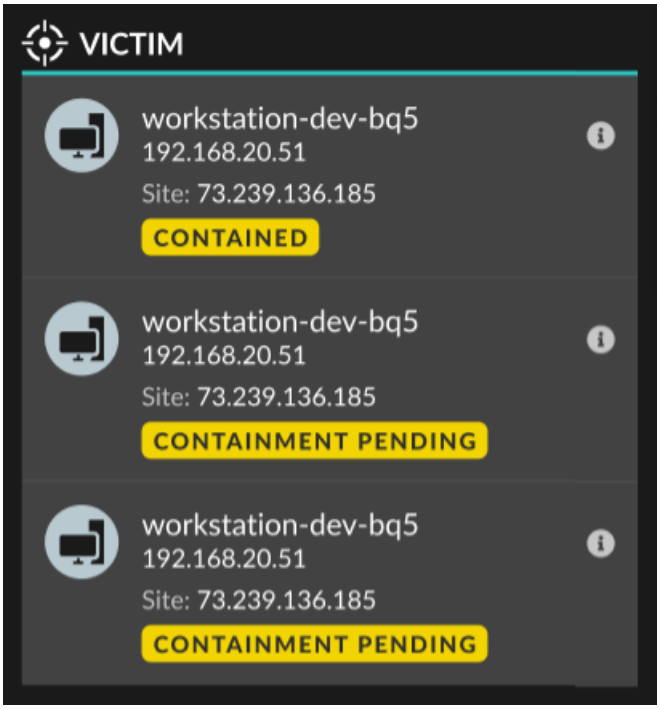
4. Cliquez **Contenir les appareils dans CrowdStrike**.
   La boîte de dialogue affiche les appareils CrowdStrike associés à la détection.



5. 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.



- 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.