Contenir des dispositifs CrowdStrike à partir d'une détection

Publié: 2023-09-19

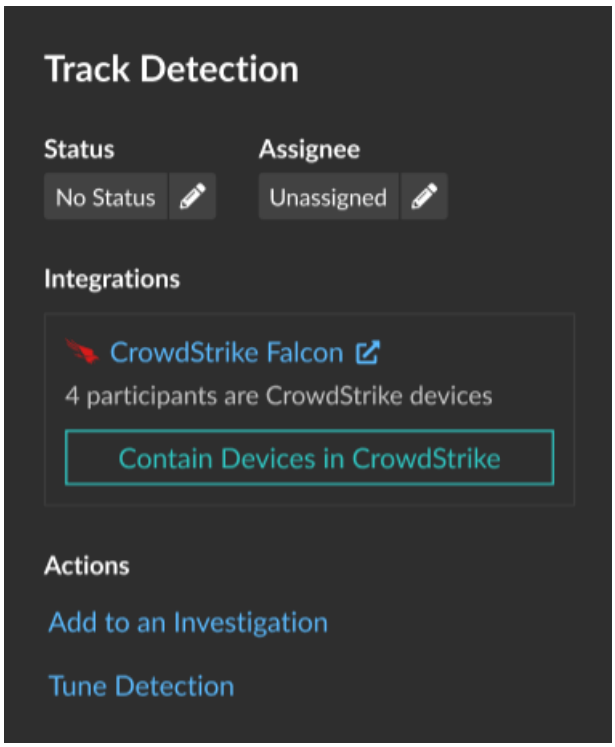
Vous pouvez lancer le confinement des dispositifs CrowdStrike qui participent à une détection de sécurité. Le confinement empêche les dispositifs d'établir des connexions avec d'autres dispositifs sur votre réseau.

Après avoir initié le confinement à partir d'une détection, une demande est faite à CrowdStrike Falcon pour confiner les appareils et un statut de confinement en attente apparaît à côté du participant. L'état est mis à jour et devient Confiné uniquement lorsque le système ExtraHop reçoit une réponse de CrowdStrike.

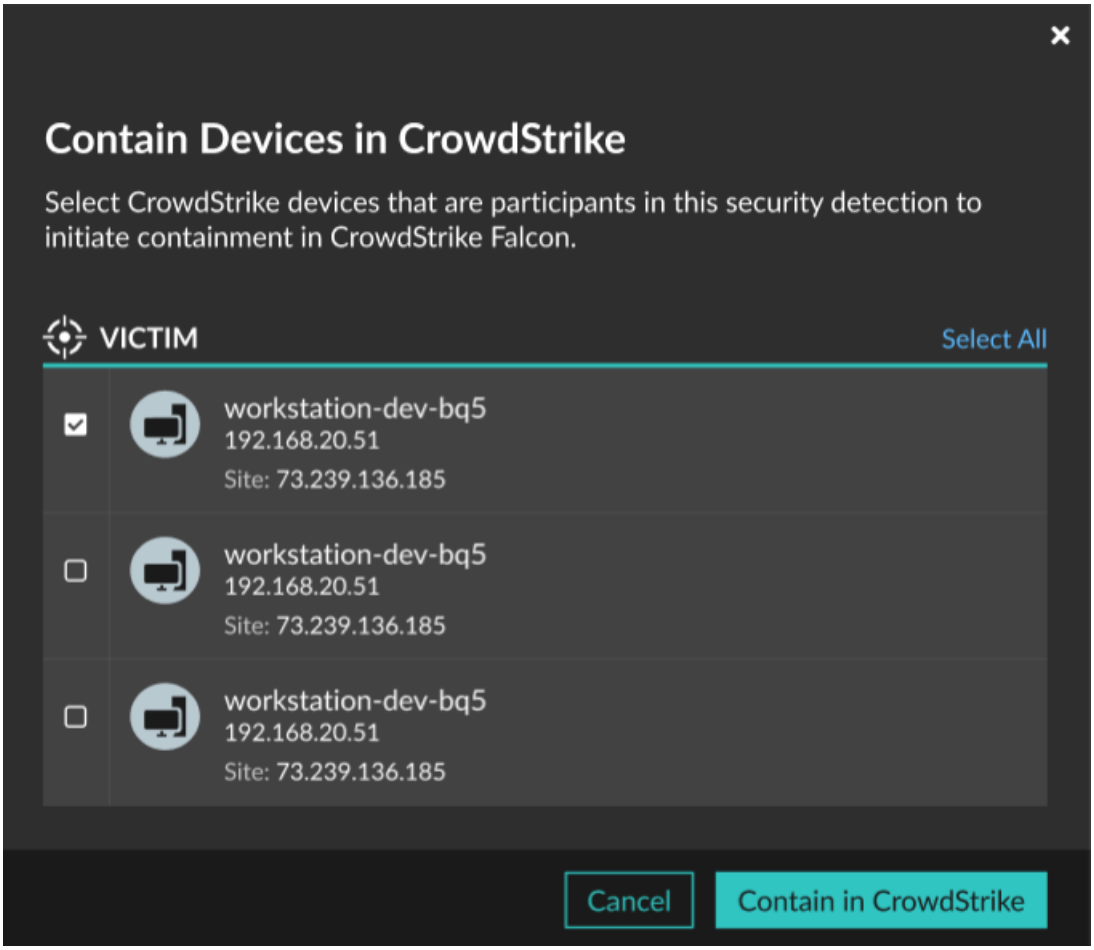
Avant de commencer

- Le confinement des appareils doit être activé pour l'intégration de CrowdStrike.
- Les utilisateurs doivent être autorisés à accéder au système par le biais de la stratégie globale de contrôle d'accès aux détections et disposer de privilèges d'écriture limités ou supérieurs pour effectuer les tâches décrites dans ce guide.

1. Connectez-vous au système ExtraHop via https://<extrahop-hostname-or-IP-address>.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez sur le titre d'une détection pour afficher la page des détails de la détection.
   Le nombre de dispositifs CrowdStrike qui participent à la détection apparaît dans la section Intégrations sous Suivi de la détection.



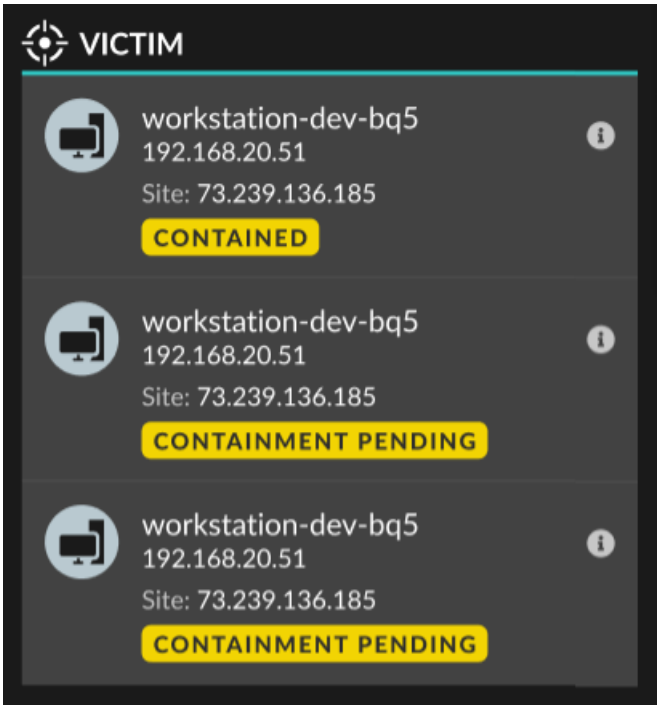
4. Cliquez sur **Container les dispositifs dans CrowdStrike**.
   La boîte de dialogue affiche les dispositifs CrowdStrike associés à la détection.



5. Sélectionnez les appareils que vous souhaitez contenir et cliquez sur **Container dans CrowdStrike**. Une demande est envoyée à CrowdStrike et l'état Containment Pending apparaît à côté de chaque participant sélectionné.

Prochaines étapes

- Vérifiez le confinement du dispositif en contrôlant l'état à partir des détails de la détection. L'état de confinement apparaît également dans les propriétés du dispositif.



- Réessayez de contenir un dispositif. L'état de confinement en attente n'apparaît plus lorsqu'une demande de confinement adressée à CrowdStrike est refusée ou expire.
- Libérer un appareil du confinement à partir de la console CrowdStrike Falcon. Dans la section Intégrations sous Détection de traces, cliquez sur **CrowdStrike Falcon** pour ouvrir la console dans un nouvel onglet. L'état de confinement n'apparaît plus lorsque le système ExtraHop reçoit une réponse de CrowdStrike.