CrowdStrike-Geräte aus einer Erkennung eindämmen

Veröffentlicht: 2024-02-16

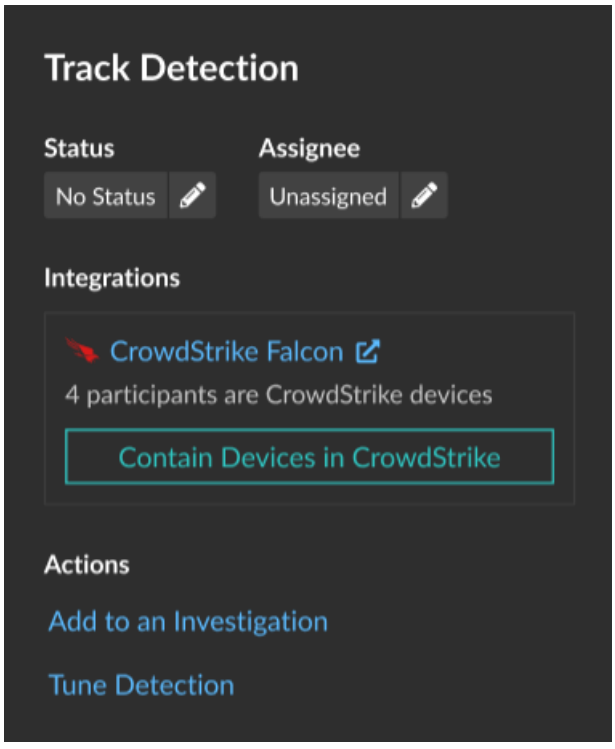
Sie können die Eindämmung von CrowdStrike-Geräten einleiten, die an einer Sicherheitserkennung Erkennung sind. Containment verhindert, dass Geräte Verbindungen zu anderen Geräten in Ihrem Netzwerk herstellen.

Nachdem Sie die Eindämmung anhand einer Erkennung eingeleitet haben, wird eine Anfrage an CrowdStrike Falcon gestellt, um die Geräte einzudämmen, und neben dem Teilnehmer wird der Status Eindämmung ausstehend angezeigt. Der Status wird erst dann auf Enthalten aktualisiert, wenn das ExtraHop-System eine Antwort von CrowdStrike erhalten hat.

Bevor Sie beginnen

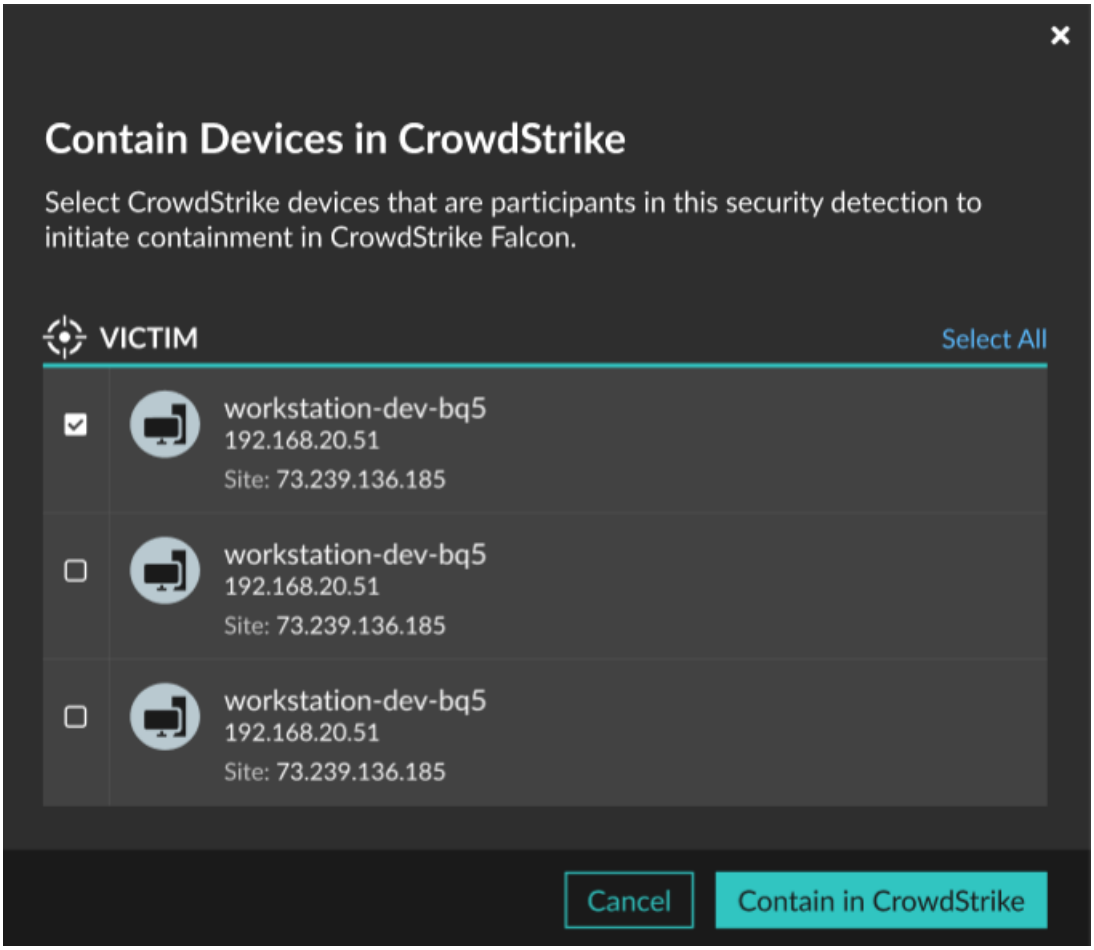
- Device Containment muss aktiviert sein für CrowdStrike-Integration.
- Benutzern muss Zugriff auf das NDR-Modul gewährt werden und sie müssen über eingeschränkte Schreibmöglichkeiten verfügen Privilegien oder höher, um die Aufgaben in diesem Handbuch zu erledigen.

1. <extrahop-hostname-or-IP-address>Melden Sie sich über https://beim ExtraHop-System an.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken Sie auf einen Erkennungstitel, um die Seite mit den Erkennungsdetails anzuzeigen. Die Anzahl der CrowdStrike-Geräte, die an der Erkennung beteiligt sind, wird im Abschnitt Integrationen unter Track Detection angezeigt.



4. klicken **Geräte in CrowdStrike enthalten**.
Im Dialogfeld werden die CrowdStrike-Geräte angezeigt, die mit der Erkennung verknüpft sind.

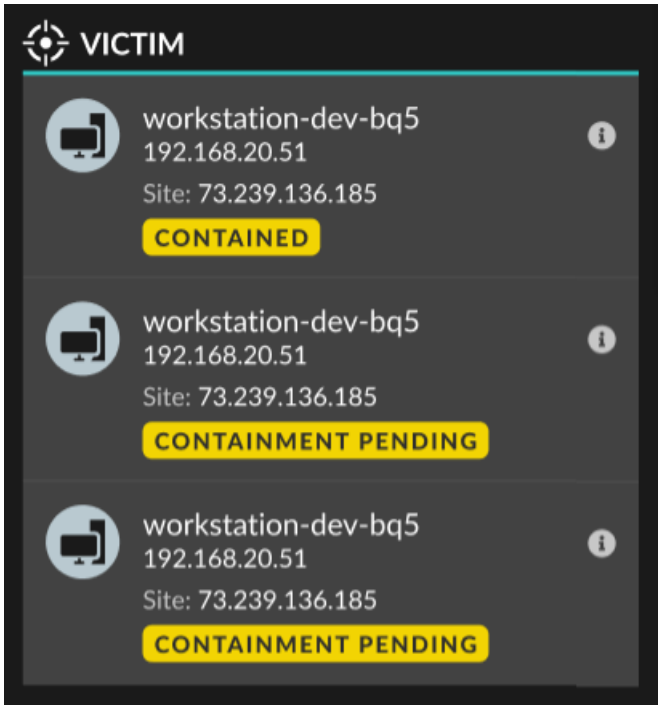
© 2024ExtraHop Networks, Inc. Alle Rechte vorbehalten.



5. Wählen Sie die Geräte aus, die Sie enthalten möchten, und klicken Sie auf **In CrowdStrike enthalten**. Eine Anfrage wird an CrowdStrike gesendet und neben jedem ausgewählten Teilnehmer wird der Status Containment Pending angezeigt.

Nächste Schritte

- Überprüfen Sie die Geräteeinhausung, indem Sie den Status anhand der Erkennungsdetails überprüfen. Der Containment-Status erscheint auch in der Eigenschaften Gerät.



- Versuchen Sie erneut, ein Gerät zu enthalten. Der Status „Eindämmung steht noch aus“ wird nicht mehr angezeigt, wenn eine Eindämmungsanfrage an CrowdStrike abgelehnt wird oder abläuft.
- Befreien Sie ein Gerät über die CrowdStrike Falcon-Konsole aus dem Container. Klicken Sie im Bereich Integrationen unter Track Detection auf **CrowdStrike Falcon** um die Konsole in einem neuen Tab zu öffnen. Der Containment-Status wird nicht mehr angezeigt, nachdem das ExtraHop-System eine Antwort von CrowdStrike erhalten hat.