Contain CrowdStrike devices from a detection

Published: 2022-12-29

You can initiate containment of CrowdStrike devices that are participants in a security detection. Containment prevents devices from establishing connections to other devices on your network.

After you initiate containment from a detection, a request is made to CrowdStrike Falcon to contain the devices and a Containment Pending status appears next to the participant. The status is updated to Contained only after the ExtraHop system receives a response from CrowdStrike.

Before you begin

- Device containment must be enabled for the CrowdStrike integration Z.
- Users must be granted access through the Detections Access Control global policy 🛽 and have limitedwrite privileges 🗗 or higher to complete the tasks in this guide.
- 1. Log in to the ExtraHop system through https://<extrahop-hostname-or-IP-address>.
- 2. At the top of the page, click **Detections**.
- Click a detection title to view the detection detail page. The number of CrowdStrike devices that are participants in the detection appear in the Integrations section under Track Detection.

Track Detection								
Status		Assignee						
No Status	ø	Unassigned	A					
Integration	Integrations							
 CrowdStrike Falcon I 4 participants are CrowdStrike devices 								
Con	Contain Devices in CrowdStrike							
Actions								
Add to an Investigation								
Tune Dete	ection							

4. Click Contain Devices in CrowdStrike.

The dialog box displays the CrowdStrike devices associated with the detection.

Cor	utain [Devices in Crowd	Strike		~			
Selec	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						
O	•	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						
			Cancel	Contain in Crov	vdStrike			

 Select the devices you want to contain and click Contain in CrowdStrike. A request is sent to CrowdStrike and the Containment Pending status appears next to each selected participant.

Next steps

• Verify device containment by checking the status from the detection details. The containment status also appears in the device properties **Z**.

•	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	6			
•	workstation-dev-bq5 192.168.20.51 Site: 73.239.136.185 CONTAINMENT PENDING	0			

- Retry containing a device. The Containment Pending status no longer appears when a containment request to CrowdStrike is denied or expires.
- Release a device from containment from the CrowdStrike Falcon console. From the Integrations section under Track Detection, click **CrowdStrike Falcon** to open the console in a new tab. The containment status no longer appears after the ExtraHop system receives a response from CrowdStrike.