CrowdStrike University

CROWDSTRIKE
UNIVERSITY

# FALCON 240
# INVESTIGATING AND MITIGATING THREATS WITH REAL TIME RESPONSE

## COURSE OVERVIEW

Real Time Response (RTR)  provides deep access to systems across the distributed enterprise and enhanced visibility that is necessary to fully understand emerging threats. Incident responders are able to directly remediate, which helps to dramatically reduce the time needed to respond to attacks and the likelihood of an attack becoming a costly breach.

This hands-on course is intended for technical contributors who will be performing remediation, host-level response to detections or host investigations with CrowdStrike Falcon® Real Time Response (RTR). The course explains use cases and administrative considerations for Falcon RTR and provides hands-on experience remediating threats using a variety of RTR commands, custom scripts and over the API using PSFalcon.

## WHAT YOU WILL LEARN

- Remediate a threat using Real Time Response commands
- Utilize custom scripts to remediate a threat
- Use PSFalcon to remediate an incident
- Create an automated workflow using RTR custom scripts
- Audit Real Time Response activity

## PREREQUISITES

- Knowledge of basic operations on a personal computer
- Intermediate knowledge of cybersecurity incident investigation and incident lifecycle
- Completion of FALCON 140: Real Time Response Fundamentals
- Completion of FHT 114: Falcon Fusion Fundamentals
- Completion of FALCON 201: Falcon Platform for Responders
- Familiar with the Microsoft Windows environment

## REQUIREMENTS

- Broadband internet connection, web browser, microphone and speakers
- Dual monitors and headset are recommended

## CLASS MATERIAL

Associated materials may be accessed from CrowdStrike University on the day of class.

1-day program | 2 credits

This instructor-led course includes instructor walkthroughs and hands-on learner exercises. You will practice identifying threats as well as the steps to remediate them.

**Take this class if:**
You are a system responder or integrator.

**Registration**
For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires two (2) training credits.  If you do not have access to CrowdStrike University, need to purchase training credits or need more information, please contact sales@crowdstrike.com.

## TECHNICAL CAPABILITIES OF REAL TIME RESPONSE

- Explain the use case of Real time response
- Explain system and Falcon requirements for Real time response
- Identify the areas of the RTR console

## RTR ARCHITECTURE AND ADMINISTRATIVE REQUIREMENTS

- Explain the connection mechanism and encryption mechanism
- Set up users with RTR role
- Discuss Response policies
- Access RTR documentation

## CONNECT TO A HOST

- Identify the different ways to connect to a host
- Connect to a host

## REMEDIATE THREATS WITH RTR COMMANDS

- Identify when to use Real Time Response to respond to a detection or incident
- Identify a threat
- Explain the use of commands in Real time response
- Explain the general command syntax
- Run Real Time Response commands

## REMEDIATE THREATS WITH RTR CUSTOM SCRIPTS

- Identify the three different ways to run a custom script
- Explain the script capabilities and nuances in RTR
- Identify the differences between a script's output in PowerShell vs RTR
- Add a custom script to the repository
- Run a custom script from the repository
- Run a raw custom script
- Edit and save a custom script from the repository

## REMEDIATE THREATS WITH PSFALCON

- Explain what PSFalcon is
- Find devices using filtered search in PSFalcon
- Run saved script on devices using PSFalcon
- Access PSFalcon wiki

## AUTOMATED WORKFLOWS AND RTR

- Define what a Workflow is
- Explain when to use a Workflow
- Identify supported Workflow triggers
- Create a workflow

## AUDIT RTR ACTIVITY

- Identify which roles can see which audit logs
- Review and Export RTR session audit logs
- Review and Export Response scripts & files audit logs