

FALCON 240:

Investigating and Mitigating Threats with Falcon Real Time Response

Course Overview

CrowdStrike Falcon® Real Time Response (RTR) provides deep access to systems across the distributed enterprise and enhanced visibility that is necessary to fully understand emerging threats. With Falcon RTR, incident responders are able to directly remediate incidents, which helps 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 Falcon RTR. The course explains use cases and administrative considerations for Falcon RTR and provides hands-on experience remediating threats using a variety of Falcon RTR commands and custom scripts.

What You Will Learn

In this course, you will learn how to:

- » Execute Falcon RTR commands for threat remediation
- » Develop and implement custom scripts for specialized responses
- » Design automated workflows using Falcon RTR custom scripts
- » Monitor and audit Falcon RTR activities
- » Apply administrative best practices for Falcon RTR usage

Recommended Prerequisites

- » Knowledge of basic operations on a personal computer
- » Intermediate knowledge of cybersecurity incident investigation and the incident life cycle
- » Completion of FALCON 140: Real Time Response Fundamentals
- » Completion of SOAR 100: Falcon Fusion SOAR Fundamentals
- » Completion of FALCON 201: Falcon Platform for Responders
- » Familiarity with the Microsoft Windows environment

1-day program | 2 credits

This instructor-led course includes various walkthroughs and hands-on learner exercises

Take this class if you are:
A system responder,
a system integrator,
or preparing for the
CrowdStrike Certified
Falcon Responder (CCFR)
exam

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.

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.

Topics

Technical Capabilities of Falcon RTR

- » Explain Falcon RTR use cases
- » Explain system and CrowdStrike Falcon® platform requirements for Falcon RTR
- » Identify the areas of the Falcon RTR console

Falcon RTR Architecture and Administrative Requirements

- » Explain the connection mechanism and encryption mechanism
- » Set up users with a Falcon RTR role
- » Discuss response policies
- » Access Falcon RTR documentation

Connect to a Host

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

Remediate Threats with Falcon RTR Commands

- » Identify when to use Falcon RTR to respond to a detection or incident
- » Identify a threat
- » Explain the use of commands in Falcon RTR
- » Explain the general command syntax
- » Run Falcon RTR commands

Remediate Threats with Falcon RTR Custom Scripts

- » Identify the three different ways to run a custom script
- » Explain the script capabilities and nuances in Falcon RTR
- » Identify the differences between a script's output in PowerShell vs. Falcon 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

Automated Workflows and Falcon RTR

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

Audit Falcon RTR Activity

- » Identify which roles can see which audit logs
- » Review and export Falcon RTR session audit logs
- » Review and export Falcon "Response scripts and files" audit logs

