CrowdStrike University

CROWDSTRIKE UNIVERSITY

FHT 240
INVESTIGATING AND MITIGATING THREATS WITH REAL TIME RESPONSE

COURSE OVERVIEW

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). This course explains how to use Falcon RTR query information from hosts, put and run files and scripts, and perform administrative functions related to roles and permissions.

WHAT YOU WILL LEARN

- Perform the administrative tasks required to use Falcon RTR
- Work with processes, memory and files on a host
- Work with Windows event logs and the Windows registry
- Obtain network and system information
- Perform script-related tasks

PREREQUISITES

- Completion of all FHT 100-level course material
- Completion of the FAICON 201 course or familiarity with the CrowdStrike Falcon® platform and detection analysis
- Intermediate knowledge of cybersecurity incident investigation and the incident lifecycle
- Familiarity with CrowdStrike Falcon® OverWatch™ best practices (FALCON 201 course)
- Ability to comprehend course curriculum presented in English
- Familiarity 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 allows learners to use Falcon RTR to remotely perform the tasks that a responder would do if they were physically present at an endpoint.

Take this class if:
You are a cyber defense incident responder, security analyst, SOC analyst or threat analyst

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.

Last Update: Nov 22, 2023

CrowdStrike University

FHT 240 Investigating and Mitigating Threats with Real Time Response

INTRODUCTION TO FALCON RTR

- About Falcon RTR
- Requirements
- Policies and roles
- Documentation
- Connecting to the host

GENERAL FALCON RTR USAGE

- Administrative commands
- Host navigation with Falcon RTR

RETRIEVING ARTIFACTS

- Manipulating files
- Viewing and editing the registry
- Viewing Windows event logs
- Obtaining network information
- Working with processes
- Dumping memory (full and process)
- Interacting with Windows Updates

CUSTOM SCRIPTS

- Writing custom scripts
- Running custom scripts
- Response scripts and files
- Overview of automating Falcon RTR

SESSION LOGS

- Audit logs
- Custom scripts logs
- Put file logs

During this course, students will discuss and explore all commands available in Falcon RTR and utilize those commands where appropriate in hands-on labs.