CrowdStrike University

FHT 201
INTERMEDIATE FALCON PLATFORM FOR RESPONDERS

COURSE OVERVIEW

This course instructs intermediate responders in the best use of CrowdStrike® Falcon for incident triage. The course is appropriate for those who use the Falcon platform on a day-to-day basis to detect, investigate and respond to incidents. Positions might include security analyst, SOC analyst, security engineer, IT security operations manager, security administrator, endpoint security administrator or channel sales engineer.

PREREQUISITES

To obtain the maximum benefit from this class, you should meet the following requirements:

- Completion of the 100-level courses in CrowdStrike University
- Comprehend course curriculum presented in English
- Perform basic operations on a personal computer
- Have intermediate knowledge of cyber security incident investigation and lifecycle
- Be familiar with Microsoft Windows environment

CLASS MATERIAL

Once registered for the course, associated materials may be downloaded from CrowdStrike University.

LEARNING OBJECTIVES

Students who complete this course should be able to:

- Use the key features of the Falcon platform applications
- Analyze detections and ascertain true or false positive findings
- Apply a standard analytic process to detection triage
- Describe the data available in the Insight application
- Use Insight to continue analysis beyond a detection
- Perform limited discovery of additional events beyond a detection

This instructor-led course covers the best use of the Falcon platform for incident triage and includes multiple practical labs for learners to apply what they've learned.

1-day program | 2 credits

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.

CrowdStrike University

FHT 201 Intermediate Falcon Platform for Responders

INTRODUCTION

- Who we are
- Who you are
- Administrative items
- Course overview/agenda

DETECTION ANALYSIS

- Detections application
- MITRE ATT&CK framework
- Analytical process
- Analyst workflows
- Student exercise
  - Practicing the detection workflow

EVENT DISCOVERY

- Investigate application overview

EVENT ACTIONS/WORKFLOWS

- Student exercises
  - Pivoting workflows
  - Credential theft

REAL WORLD ANALYSIS

- Student exercises
  - Social engineering & ransomware detections
  - Performing a hash search

HANDLING NOISE/FALSE POSITIVES

- Student exercises
  - False positives
  - Encoded PowerShell commands

REPORTING

- Detections
- Exporting process data
- Student exercises
  - Reports and dashboards
  - Lateral movement

PROACTIVE INVESTIGATIONS/HUNTING 101

- Bulk IP Search
- Bulk Domain Search
- Student exercise
  - Analyzing third-party intelligence

FINAL EXERCISES

- Students practice investigating a reverse shell detection
- Additional scenarios as time allows