CROWDSTRIKE

FHT 201 INTERMEDIATE FALCON PLATFORM FOR RESPONDERS

This one-day instructor-led course instructs intermediate responders in the best use of the Falcon Platform for incident triage. The course is appropriate for those who use the Falcon Platform on a day to day basis, focused on triaging and responding to alerts. It includes practical labs for students to develop hands-on skills.

PREREQUISITES

This hands-on course is intended for technical contributors who use Falcon Insight 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, Channel Sales Engineers

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

- Completion of the FHT100 level course material in CrowdStrike University
- Able to understand course curriculum presented in English
- Perform basic operations on a personal computer
- Have an intermediate knowledge of cyber security incident investigation and incident lifecycle.
- Be familiar with the 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 app
- Use the Insight app to continue analysis beyond a detection
- Perform limited discovery of additional events beyond a detection

The course includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

REGISTRATION

For a list of scheduled courses and registration access, please log into your CrowdStrike University account.
This course requires two 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

INTRODUCTION

- **Who we are**
- **Who you are**
- **Admin items**
- **Course Overview/Agenda**

Detection Analysis

- **Detections App**
  - Filtering
  - Detection Types
  - Prevention Types
- **Analytical Process**
  - Understand the detection
  - Review process tree to understand origin
  - Understand process(es) involved
  - Examine what's normal for this system
  - Examine what's normal for this customer
  - Peer review
- **Analyst Workflows**
  - Assigning a detection
  - Updating detection status
  - Commenting
  - Network Contain
- **Student Exercise**
  - Use the analytical process to review a basic detection

EVENT DISCOVERY

- **Investigate App Overview**
  - What is Event Data
  - ProcessData
  - Context Data
  - Key Event Types
- **Event Actions/workflows**
- **Student Exercise**
  - Working with Event Data and Event Actions
- **Student Exercise**
  - Social Engineering Detections/Ransomware Detections
  - Performing a hash search
- **Student Exercise**
  - PowerShell related detection
  - PowerShell Hunting Reports
- **Student Exercise**
  - False Positives
  - Encoded PowerShell commands

REPORTING

- **Detections**
  - Executive Summary Dashboard
  - Detection Activity Dashboard
  - Detection Resolution Dashboard
  - Detection Activity Report
- **Exporting Process Data**
  - Process Table
  - Process Activity
  - PNG
- **Student Exercise**
- **Student Exercise**
  - Credential Theft
  - NGAV Detections

PROACTIVE INVESTIGATIONS/HUNTING 101

- **Bulk IP Search**
- **Bulk Domain Search**
- **Student Exercise**
  - IP and Domain Searching

FINAL EXCERCISE

- Students work on their own to investigate a complex phishing attack
- Additional scenarios as time allows