CROWDSTRIKE

FHT 202 INTERMEDIATE FALCON PLATFORM FOR HUNTERS

This one-day instructor-led course instructs intermediate responders in the best use of the Falcon Platform for incident detection using proactive "hunting" investigation. The course is appropriate for those who use the Falcon Platform to find evidence of incidents that do not raise alerts by other means. 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 Hunt Team members, 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
- Have taken the FHT 201 course or be familiar with the Falcon interface and detection analysis
- Be familiar with the Microsoft Windows environment
- Perform basic operations on a personal computer
- Have an intermediate knowledge of cyber security incident investigation and incident lifecycle.
- Able to understand course curriculum presented in English

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:

- Simulate attacker activity
- Perform proactive search queries in the Falcon Platform using the automated queries and reports
- Understand basic Splunk query syntax
- Discover new events using custom queries
- Describe integration and automation workflow using Falcon Connect

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**

FHT 201 KEY LEARNING CONCEPTS

- **General Analytical Process**
- **App Refresher**
- **Detection Workflow**

REAL WORLD SCENARIOS

- **Exercise - Web Shell Attack**
- **Exercise - Privilege Escalation**

EVENT SEARCHING – AUTOMATED QUERIES

- **Host Search**
- **Hash Search**
- **User Search**
- **Source IP Search**
- **Bulk Hash Search**
- **Bulk Domain Search**
- **Activity Queries**
  - Bulk Destination IP Search
  - Linux Sensor Report
  - Mac Sensor Report
- **Timeline Queries**
  - Host Timeline
  - Process Timeline
- **Hunting and Visibility Reports**
  - Hunting Reports
  - Visibility Reports
- **Sensor Reports**
- **Audit Reports**
- **Exercise – Host Timeline**
- **Exercise –Process Timeline**

EVENT SEARCHING

- **Event Data Overview**
  - Data Types
  - Data Relationships
  - Fields
  - Event Timeline
  - Event Actions
- **Searching 101**
  - Search Syntax
  - Using Fields
  - Sub Searches
  - Formatting Output
  - Patterns
  - Statistics
  - Using the Join Command
- **Exercise – Searching Techniques**
- **Exercise – Sub Searching**

PRACTICAL EXCERCISES

- **Exercise – Using the hunting guide**
- **Exercise – Detecting Outliers**
- **Exercise – Searching for “Patient zero”**
- **Exercise – Using Atomic Indicators**
- **Exercise – Additional queries as time allows**