

FHT 200 FALCON PLATFORM FOR ADMINISTRATORS

This one-day instructor-led course instructs new and beginning users on the technical fundamentals of the Falcon Platform. The course is appropriate for those who use the Falcon Platform on a day to day basis, and focuses on the installation, configuration and day-to-day management of the product. This course includes a complete GUI-interface walkthrough.

Please note: there is a self-paced version of this course available in CrowdStrike University. The instructor led version of the course is targeted toward those students who wish to have a live-instructor for the fundamental material.

PREREQUISITES

This hands-on course is intended for technical contributors who will be administrating and using the Falcon Platform.

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

- Perform basic operations on a personal computer
- Have a basic knowledge of cyber security incident investigation and incident lifecycle.
- Be familiar with the Microsoft Windows environment
- 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:

- Navigate through the Falcon GUI
- Identify all Apps within the Falcon Platform
- Understand what specific tasks can be accomplished within the various Apps
- Identify and download the latest OS specific Falcon Sensor
- Install and configure the Falcon Platform

REGISTRATION

For a list of scheduled courses and registration access, please log into 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

Introduction

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

Falcon Interface Walkthrough

- GUI Layout Basics
- Apps Walkthrough
 - Activity App Walkthrough
 - Investigate App Walkthrough
 - Hosts App Walkthrough
 - Configuration App Walkthrough
 - Dashboards App Walkthrough
 - Discover App Walkthrough
 - Intelligence App Walkthrough
 - Users App Walkthrough
 - Support App Walkthrough
 - User Profile Settings

Groups

- Groups overview
 - Management
 - Static and Dynamic assignment
- Deployment Group overview
- Policy Group overview

Prevention Policy

- Settings
- Best Practices

Sensor Update Policy

- Settings
- Best Practices

Containment Policy

- Settings
- Best Practices

Initial Configuration Recommendations

Sensor Installation

- Pre Installation
- Windows Installation
- macOS Installation
- *Nix Installation
- Troubleshooting