CrowdStrike University

CROWDSTRIKE UNIVERSITY

# FALCON 200
# FALCON PLATFORM FOR ADMINISTRATORS

## COURSE OVERVIEW

Stopping breaches with the CrowdStrike Falcon® platform starts with a robust configuration. To ensure your organization is effectively protected, *FALCON 200: Falcon Platform for Administrators* covers best practice settings for protecting your hosts.

This course is appropriate for those who use the Falcon platform daily and focuses on the installation, configuration and management of the platform. It is intended for technical contributors who will be administrating and using the Falcon platform. During this course, students will install sensors and configure prevention policies, users and groups, and fine-tune detections.

## WHAT YOU WILL LEARN

- Install and deploy the latest OS-specific Falcon sensors in your environment
- Implement best practices to configure policies, users and host groups to ensure your environment is protected
- Utilize Falcon dashboards and reports to determine that your organization's environment includes adequate coverage and that endpoints have the latest sensor updates
- Fine-tune detections with indicators of compromise (IOC) management and exclusions

## PREREQUISITES

- Knowledge of computer networking concepts and protocols, and network security methodologies, privacy principles, cyber threats and vulnerabilities
- Completion of eLearning courses within the Falcon Administrator Learning Path in CSU is recommended
- Familiarity with the Microsoft Windows environment
- Ability to comprehend course curriculum presented in English

## 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 includes a CrowdStrike Falcon platform walkthrough and hands-on exercises on creating groups and policies and installing sensors.

**Take this class if:**

- You are a system administrator or security engineer
- You are preparing for the CrowdStrike Certified Falcon Administrator (CCFA) exam

**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

**FALCON 200 Falcon Platform for Administrators**

## USER MANAGEMENT

- Determine roles required for access to features and functionality in the Falcon console
- Create a new user, delete a user and edit a user

## SENSOR DEPLOYMENT

- Analyze the pre-installation OS/networking requirements prior to installing the Falcon sensor
- Apply appropriate settings to successfully install a Falcon sensor on Windows, Linux and macOS
- Uninstall a sensor
- Use Host Management to verify sensor properties
- Explain the different types of sensor reports and what each report provides
- Recognize issues with the basic configuration requirements in the system environment or Falcon components
- Determine the appropriate sensor update policy settings and related general settings in order to control the update process

## GROUP CREATION

- Determine the appropriate group assignment for endpoints and understand how this impacts the application of policies
- Describe policy types, components, application and workflow
- Define precedence, groups and best practices

## PREVENTION POLICIES

- Determine the appropriate prevention policy settings for endpoints and explain how this impacts security posture

## QUARANTINE FILES

- Apply options required to manage quarantine files

## IOC MANAGEMENT

- Assess IOC settings required for customized security posturing and to manage false positives

## EXCLUSIONS

- Interpret business requirements to allow trusted activity, and resolve false positives and performance issues
- Write an effective file exclusion rule using glob syntax
- Apply file pattern exclusions to groups
- Demonstrate how to manage exclusion rules

## CUSTOM IOAS, CONTAINMENT AND FALCON REAL TIME RESPONSE (RTR)

- Create custom indicator of attack (IOA) rules to monitor behavior that is not fundamentally malicious
- Describe what a containment policy does
- Configure an allowlist with appropriate IP addresses while the network is under containment, based on security workflow requirements
- Apply roles and policy settings, and track and review RTR audit logs in order to manage user activity

## FALCON FUSION WORKFLOWS

- Configure custom workflows to notify individuals about policies, detections and incidents