

FALCON 300

Falcon Administrator Optimization and Automation

Course Overview

Managing the CrowdStrike Falcon® platform in enterprise environments requires more than foundational knowledge — it demands the ability to optimize performance, automate operations, and troubleshoot complex issues at scale.

This advanced course builds on core administrative skills to help experienced practitioners design scalable architectures, streamline administrative workflows, and maintain platform health across distributed environments.

Learners will develop practical expertise in policy optimization, Falcon Real Time Response (RTR), API-driven automation using PSFalcon, and workflow orchestration with CrowdStrike Falcon® Fusion SOAR. Through hands-on exercises and scenario-based learning, participants will apply operational best practices to improve efficiency, reduce manual effort, and strengthen their Falcon deployment.

What You Will Learn

In this course, you will learn how to:

- » Apply daily Falcon administration workflows to monitor host health, manage sensor functionality, and maintain accurate endpoint visibility
- » Configure and optimize policies to balance detection effectiveness and system performance across different workloads
- » Use Falcon RTR to investigate, validate, and remediate endpoint issues at scale

1-day program | 2 credits

This instructor-led course combines guided walkthroughs, real-world scenarios, and hands-on exercises to help experienced Falcon administrators operate efficiently at enterprise scale.

Take this class if you are: an experienced Falcon administrator, senior security engineer, or platform owner responsible for managing large or complex Falcon environments

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.

- » Automate Falcon administrative workflows using Falcon Fusion SOAR, APIs, and PSFalcon
- » Monitor endpoint health and platform performance using Falcon data and operational metrics
- » Troubleshoot sensor, policy, and communication issues across distributed environments
- » Implement scalable architecture strategies and phased deployments
- » Generate automated reporting and integrate Falcon with enterprise system

Recommended Prerequisites

- » Completion of FALCON 200 or equivalent experience
- » Minimum of 6 months of hands-on Falcon administration experience
- » Active Falcon environment with deployed sensors
- » Recommended: **CrowdStrike Certified Falcon Administrator (CCFA)** certification

Requirements

- » Broadband internet connection, web browser, microphone, and speakers
- » Recommended: Dual monitors and headset

Class Material

Course materials will be available in CrowdStrike University on the day of class.

Topics

Daily Falcon Administration Workflows

- » Manage Reduced Functionality Mode (RFM) and restore sensor functionality
- » Monitor host health using last-seen data and platform health indicators
- » Identify unmanaged endpoints and maintain accurate inventory
- » Use query-based workflows to identify issues and schedule recurring administrative tasks

Policy Optimization and Performance Tuning

- » Configure policies for varied workloads, including servers, workstations, and containers
- » Optimize machine learning (ML) settings to balance detection and performance
- » Implement and validate exclusion strategies across policy types
- » Tune policy configurations to support operational efficiency at scale

Scalable Architecture and Environment Customization

- » Design host grouping strategies for enterprise environments
- » Configure advanced policy types, including content update and host retention policies
- » Plan and execute phased deployment, rollout, and rollback strategies

Falcon Real Time Response (RTR) for Administrative Operations

- » Use Falcon RTR to remotely troubleshoot endpoint and sensor issues
- » Validate custom indicators of compromise (IOCs), indicators of attack (IOAs), and exclusions
- » Perform remediation actions across distributed endpoints
- » Support administrative workflows through secure remote access

APIs and PSFalcon

- » Understand Falcon API fundamentals and permission scopes
- » Authenticate and execute administrative actions using PSFalcon
- » Identify automation opportunities to reduce manual effort
- » Apply best practices for scripting, logging, and error handling
- » Automate tasks such as sensor reinstallation and reporting

Falcon Fusion SOAR

- » Build workflows to enforce policy governance and prevent unauthorized changes
- » Configure alerts for administrative and configuration changes
- » Automate repetitive administrative and operational tasks
- » Integrate Falcon workflows with external systems

Operational Excellence and Advanced Troubleshooting

- » Troubleshoot sensor communication and performance issues
- » Analyze policy impact on endpoint performance and behavior
- » Monitor platform health and implement proactive remediation strategies
- » Use audit logs and activity tracking for visibility and compliance
- » Build custom dashboards and generate reports for operational insight
- » Integrate third-party tools to extend Falcon capabilities

