

FALCON 201:

Falcon Platform for Responders

Course Overview:

The CrowdStrike Falcon® platform empowers incident responders and security analysts with advanced detection, investigation, and response capabilities. This technical course provides hands-on experience with real-world scenarios, teaching participants how to effectively analyze security incidents using an analytical process. Participants will learn to navigate Falcon's comprehensive feature set while developing crucial skills in detection analysis and incident investigation.

The course emphasizes a systematic approach to incident response, ensuring analysts can effectively utilize Falcon's powerful detection and investigation tools to uncover, analyze, and respond to potential threats within their environment. This structured approach helps security teams streamline their investigation workflows and make informed decisions about potential security incidents.

What You Will Learn:

In this course, you will learn how to:

- » Analyze and interpret CrowdStrike Falcon endpoint detection data to identify security incidents and execute recommended detection analysis processes
- » Examine Falcon Investigate, CrowdStrike Counter Adversary Operations, and CrowdStrike Charlotte AI™ capabilities
- » Implement proper detection workflow procedures using endpoint security tools
- » Conduct comprehensive security event analysis using Falcon's timeline and search functionalities
- » Investigate real-world attack scenarios using Falcon's advanced detection and analysis capabilities
- » Execute targeted event searches using process relationships and event actions
- » Apply best practices for threat identification, analysis, and response using Falcon platform tools

1-day program | 2 credits

This instructor-led course includes various walkthroughs and hands-on learner exercises

Who should take this course:

- A cyber defense incident responder
- A security analyst
- Anyone preparing for the CrowdStrike Certified Falcon Responder (CCFR) or CrowdStrike Certified Falcon Hunter (CCFH) 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.

Recommended Prerequisites

- » Fundamental knowledge of computer networking concepts and protocols, network security methodologies, privacy principles, cyber threats, and vulnerabilities
- » Intermediate knowledge of incident response and handling methodologies
- » Familiarity with the Microsoft Windows environment
- » Completion of eLearning courses within the Falcon Incident Responder Learning Path in CrowdStrike University

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.

Topics

Falcon Detection Analysis Fundamentals

- » Identify and interpret key components of Falcon detection data
- » Execute the recommended detection analysis process within the Falcon platform
- » Distinguish between different types of security incidents using Falcon detection indicators
- » Apply systematic approaches to detection triage and prioritization

Advanced Investigation Tools and AI Integration

- » Navigate and utilize the Falcon Investigate interface and core functionalities
- » Examine CrowdStrike Counter Adversary Operations data on known adversaries
- » Integrate AI-powered insights into investigation workflows

Detection Workflow and Dashboard Management

- » Implement recommended detection workflow procedures using endpoint security tools
- » Organize detection data effectively for streamlined analysis and reporting
- » Apply best practices for data visualization and investigation logging procedures

Timeline Analysis and Event Search Techniques

- » Analyze security events using Falcon's process timeline functionality
- » Navigate and interpret host timeline data for comprehensive incident analysis
- » Execute advanced searches using Falcon Investigate user search tools and filters
- » Correlate events across multiple timelines to identify attack patterns
- » Apply timeline analysis techniques to reconstruct incident sequences

Real-World Attack Scenario Investigation

- » Investigate comprehensive real-world attack scenarios using Falcon's detection capabilities
- » Identify and analyze advanced threat behaviors and attack methodologies
- » Apply systematic investigation approaches to complex multi-stage attacks
- » Execute thorough threat behavior analysis using Falcon's advanced detection features
- » Correlate multiple indicators of compromise across extended attack timelines

Advanced Event Search and Process Analysis

- » Perform targeted event searches using process relationships and dependencies
- » Execute searches based on specific event actions and behavioral indicators
- » Apply advanced filtering techniques to isolate relevant security events
- » Analyze process execution chains and parent-child relationships effectively
- » Implement search optimization strategies for large-scale investigations



