CrowdStrike University

CROWDSTRIKE UNIVERSITY

# FALCON 202
# INVESTIGATING AND QUERYING EVENT DATA WITH FALCON EDR

## COURSE OVERVIEW

*FALCON 202: Investigating and Querying Event Data with Falcon EDR* is an intermediate-level course for those who use CrowdStrike Falcon® Insight XDR to detect, investigate and respond to incidents using proactive investigation techniques. During this course, learners will perform search queries, apply custom searches, use reports to assist with hunts and create commands to investigate events and find attacker activity.

This course provides an understanding of concepts and skills necessary for using Falcon Insight to detect, investigate and respond to incidents with proactive investigation techniques.

## WHAT YOU WILL LEARN

- Perform proactive search queries in the Falcon platform using the automated queries and reports
- Recall basic CrowdStrike Query Language (CQL) syntax
- Discover new events using custom queries

## PREREQUISITES

- Intermediate knowledge of cybersecurity incident investigation and the incident lifecycle
- Completion of eLearning courses within the Threat Hunter Learning Path in CSU is recommended
- Completion of FALCON 201 or familiarity with CrowdStrike Falcon® and detection analysis
- Familiarity with the Microsoft Windows environment
- Ability to comprehend 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 best practices and hands-on exercises on using the Falcon platform for incident detection with proactive hunting methods.

**Take this class if:**

- You are a cyber defense incident responder, security analyst, SOC analyst or threat analyst
- You are preparing for the CrowdStrike Certified Falcon Responder (CCFR) or 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.

# FALCON 202 Investigating and Querying Event Data with Falcon EDR

## ANALYST INVESTIGATION METHODOLOGIES

- Explain what threat hunting means
- Explain what incident reponse is
- Describe pursuit methodologies, including real-time, retrospective and retroactive

## INDICATORS OF COMPROMISE AND INDICATORS OF ATTACK

- Explain what information is available in the various searches, reports and timelines in the Falcon platform
- Use automated query tools in the Falcon platform to perform single item and bulk item searches

## CUSTOM QUERIES

- Describe general use cases for event searching
- Explain what information is in the Events Data Dictionary
- Describe the process relationship of Target/Parent/Context
- Perform a basic Search Processing Language (SPL) query
- Explain and demonstrate data output format functions using query pipelines

## DATA ANALYSIS TECHNIQUES

- Explain what the “stats count by” command does and demonstrate how it can be used for statistical analysis
- Use Cluster to group results that are alike
- Perform analysis to determine normal activity for the environment

## EVENT SEARCH QUERY REPORTS

- Locate built-in hunting reports and explain what they provide
- Use hunting and visibility reports in the Falcon platform

## INVESTIGATING WITH FALCON INSIGHT

- Explain how the rename command is used in a query related to associated event data
- Use the rename command, in operator and subsearch during event queries
- Convert and format Unix times to UTC readable times
- Use the join command to combine process events with associated event types
- Use Enhanced Attacker Execution Profiling (EAEP) events to find attacker activity
- Explore removable device events