CrowdStrike University

FALCON 201
FALCON PLATFORM FOR RESPONDERS

COURSE OVERVIEW

FALCON 201: Falcon Platform for Responders instructs learners on best practices for using CrowdStrike Falcon® Insight. This course provides the knowledge and skills necessary for incident responders or security analysts who use the Falcon platform to detect, investigate and respond to incidents. During this course, learners will analyze real-world scenarios for detections and incidents using a standard analytical process.

WHAT YOU WILL LEARN

- Analyze detections and ascertain true or false positive findings
- Apply a standard analytic process to detection triage
- Use the data available within Falcon Insight to continue analysis beyond a detection
- Perform limited discovery of additional events beyond a detection

PREREQUISITES

- Knowledge of computer networking concepts and protocols, network security methodologies, privacy principles, cyber threats and vulnerabilities
- Knowledge of incident response and handling methodologies
- Completion of eLearning courses within the Falcon Responder Learning Path in CSU 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 covers the best use of the Falcon platform for incident triage and includes multiple practical labs for learners to detect, investigate and respond to incidents.

Take this class if:

- You are a cyber defense incident responder or security 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.

Last Update: Nov 22, 2023

UNDERSTANDING DETECTION ANALYSIS

- Explain what information and information sources related to Endpoint Detections are available in the Falcon platform
- Explain what information the MITRE ATT&CK® framework provides
- Use best practices to determine which tools in the Falcon platform can help to investigate a detection

DETECTION ANALYSIS PROCESS

- Use information within the Falcon platform to provide context to a detection
- Analyze process relationships using the information contained in the Full Detection Details
- Interpret the data contained in various query results

EVENT DISCOVERY

- Perform an Event Search from a detection and refine a search using event actions
- Describe the process relationship
- Demonstrate how to get to a Process Explorer from an Event Search

PROCESS AND HOST TIMELINES

- Explain what information a process timeline, host timeline and user search provides
- Generate a process timeline
- Pivot from a detection to a process timeline

REAL-WORLD SCENARIOS

- Use Falcon Insight to analyze a masquerading detection and an indicator of attack (IOA)-based detection

DEALING WITH NOISE

- Use detection filtering and grouping to reduce noise
- Describe what the Block, Block and Hide Detection, Detect Only, Allow and No Action policies do
- Explain the effects of allowlisting and blocklisting
- Explain the effects of machine learning exclusion rules and sensor visibility exclusions

DETECTION REPORTING

- Export detection and process data from Full Detection Details for further review
- Describe what information is in the Detection Activity Report, Executive Summary Dashboard and Detection Resolution Dashboard

PROACTIVE INVESTIGATIONS

- Triage a non-Falcon indicator of compromise (IOC) in the Falcon platform
- Explain what information an IP search, Hash Executions search and a Bulk Domain search provide

INCIDENTS

- Analyze a Falcon incident containing lateral movement
- Compare the differences between analyzing Incidents and Detections