

FALCON 202:

Investigating and Querying Event Data with Falcon EDR

Course Overview:

Take your investigative capabilities to the next level with this intermediate-level course focused on proactive threat hunting using CrowdStrike Falcon® Insight XDR. Security professionals progress from understanding event data and reports to building queries, visualizing activity, performing data analysis, and executing end-to-end investigation workflows. The course emphasizes how analysts actually work: correlating events, pivoting across datasets, validating hypotheses, and understanding attacker behavior over time. Through instructor-led walkthroughs and hands-on exercises, participants learn to move from isolated alerts to structured, repeatable investigations.

This course prepares analysts to think critically, ask better questions, and efficiently investigate suspicious activity across hosts, users, processes, and infrastructure.

What You Will Learn:

In this course, you will learn how to:

- » Use pre-built reports, timelines, and searches to initiate investigations
- » Build and refine event queries using CrowdStrike Query Language (CQL)
- » Analyze event data to identify patterns, outliers, and suspicious behavior
- » Apply visualization techniques to understand scope, relationships, and timelines
- » Develop and test threat hunting hypotheses using indicators of attack (IOAs) and indicators of compromise (IOCs)
- » Correlate related events across time, entities, and datasets
- » Pivot intentionally to expand investigations and uncover attacker activity
- » Execute structured investigation workflows from initial signal to conclusion

1-day program | 2 credits

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

Who should take this course: This class is best suited for:

- Cyber defense incident responder
- Security analyst
- SOC analyst
- Threat analyst
- People 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

- » Intermediate knowledge of cybersecurity incident investigation and the incident life cycle
- » Familiarity with the CrowdStrike Falcon platform
- » Familiarity with Microsoft Windows and Linux system logs
- » Prior exposure to logs, alerts, or endpoint telemetry
- » Completion of eLearning courses within the Falcon Threat Hunter Learning Path in CrowdStrike University
- » Completion of FALCON 201 or CQL 201 or familiarity with the CrowdStrike Falcon® platform and detection analysis

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

Event Reports and Timelines

- » Use built-in reports as investigation starting points
- » Analyze host, user, IP, and bulk search reports
- » Review OS-specific sensor reports (Windows, Linux, macOS)
- » Interpret host and process timelines to understand activity sequence
- » Leverage visual investigation tools such as the Remote Access Graph and geo-activity views

Understanding Event Data and Query Foundations

- » Explain event data structure and commonly used fields
- » Navigate the Sensor Events Index and Events Full Reference
- » Apply CrowdStrike Query Language (CQL) fundamentals
- » Describe the purpose and capabilities of Advanced Event Search
- » Build investigation-driven queries to answer specific security questions

Visualizing the Hunt

- » Explain why visualization is critical for large-scale investigations
- » Create and interpret tables, charts, graphs, and Sankey-style views
- » Analyze activity using the Remote Access Graph and Indicator Graph
- » Evaluate geo-location and relationship-based visualizations
- » Transform investigation results into interactive pivots
- » Use visualization to support reporting and communicate findings effectively

Threat Hunting and Incident Response

- » Differentiate threat hunting from incident response workflows
- » Analyze IOAs and IOCs using behavioral context
- » Develop and test threat hunting hypotheses
- » Apply hypothesis-driven pivoting techniques
- » Interpret Automated Leads, including purpose, confidence, severity, and limitations
- » Determine when Automated Leads are appropriate based on operational context

Data Analysis Techniques

- » Analyze IOCs and IOAs within investigation data
- » Differentiate normal and abnormal process relationships
- » Examine parent/child relationships and execution context
- » Identify web shell and persistence behaviors (e.g., Sticky Keys, IIS abuse)
- » Detect patterns of attacker behavior across systems
- » Establish normal activity baselines within an environment

Investigation Workflows and Pivoting

- » Explain correlation concepts using the `correlate()` function
- » Compare `correlate` and `join` to determine appropriate usage
- » Apply pivoting as an analyst mindset rather than a single action
- » Decide when and where to pivot during investigations
- » Avoid tunnel vision and premature closure during analysis
- » Build repeatable, defensible investigation workflows

