CrowdStrike University

CROWDSTRIKE UNIVERSITY

FALCON 302
ADVANCED THREAT HUNTING WITH FALCON

COURSE OVERVIEW

Utilizing CrowdStrike Falcon®, participants will learn to hunt for signs of an adversarial compromise. This course focuses on finding abnormal enterprise activity and searching for related data points, with the goals of finding all impacted hosts and — when possible — identifying the adversary. Students will learn advanced threat hunting techniques to use throughout the entire threat hunting cycle. Topics include initiating hunts, developing search techniques and reporting findings. The course delves into in-depth investigation of Falcon events, the application of common threat models and the use of structured analysis to bridge knowledge gaps.

WHAT YOU WILL LEARN

In this course, you will:

- Conduct proactive and reactive threat hunts to uncover indications of adversarial compromise.
- Develop initial threat hunting findings, employ data contextualization to create lead resolutions and communicate findings through reporting.
- Pivot from hunting triggers through the operationalization of intelligence to uncover new adversary findings.
- Utilize CrowdStrike Query Language to hunt through Falcon process and event data.
- Report findings to affected stakeholders.

PREREQUISITES

- Completion of FALCON 202: Investigating and Querying Event Data With Falcon EDR is strongly recommended
- Intermediate knowledge of cybersecurity incident investigation and the incident life cycle
- Ability to perform basic operations on a personal computer
- Ability to comprehend course curriculum presented in English
- Familiarity with Microsoft Windows environments
- Familiarity with navigating the Falcon platform console

CLASS MATERIAL

Download your Learner Guide and Lab Guide from CrowdStrike University once the class starts.

3-day program | 6 credits

This instructor-led course is based on real-world intrusions and culminates in an expert-curated, realistic capstone project.

Take this class if:

You are a threat hunter, cyber defense incident responder, security analyst, SOC analyst or threat analyst.

Registration

For a list of scheduled courses and registration access, please log into your CrowdStrike University account. This course requires six (6) training credits. If you need to purchase training credits, need more information or do not have access to CrowdStrike University, please contact sales@crowdstrike.com.

DAY 1

Welcome

- Who we are
- Who you are
- Administrative items

Introduction

- Introduction to the exercise scenarios
- Review the Falcon Raptor environment
- Review the CrowdStrike Query Language

Definitions and Concepts

- Find threat hunt leads in Falcon event data
- Differentiate between indicators of attack (IOAs) and indicators of compromise (IOCs)
- Use threat intelligence to build knowledge around existing leads
- Discover typical endpoint events that trigger an enterprise threat hunt
- Act on discovered IOAs, IOCs and anomalies
- Conduct a threat hunt maturity assessment

DAY 2

CrowdStrike SEARCH Methodology

- Summarize CrowdStrike® Falcon OverWatch™ SEARCH (Sense, Enrich, Analyze, Reconstruct, Communicate, Hone) threat hunting methodology
- Analyze the environment for adversary activity using the SEARCH methodology
- Use the CrowdStrike Query Language to enrich understanding of the attack

Tactical Threat Hunting Methodologies

- Learn to how apply various threat hunting methods to an investigation
- Query internal data stores for artifacts found in your environment
- Investigate and research IOAs and IOCs to discover adversarial presence
- Utilize advanced threat hunting techniques as part of routine operations
- Recognize the importance of situational awareness during a threat hunt

DAY 3

Contextual Hunting with Intel Models

- Apply models and frameworks to understand adversary intent and capabilities
- Completely identify tactics, techniques and procedures (TTPs) using the MITRE ATT&CK® framework
- Understand how the MITRE ATT&CK framework is incorporated into the Falcon platform
- Use the MITRE ATT&CK Navigator to intimately understand the attacker's next moves
- Apply morphological analysis with the MITRE ATT&CK framework to kill the attack
- Explore the potential of the cyber kill chain to enhance analysis
- Understand the use of the Diamond Model of Intrusion Analysis

Automating the Threat Hunt

- Understand the use of the Falcon API in threat hunting
- Create custom IOAs and allow the Falcon platform to continually hunt for you
- Automate threat hunting with custom IOCs
- Survey workflow options available in CrowdStrike Falcon® Fusion
- Build scheduled searches to automate hunting

Capstone

- Complete a threat hunt using scenario-based learning
- Refine your understanding of the attack using doctrinal intelligence analysis
- Complete a threat hunt report based on findings from the capstone exercise

This course culminates in a 4-hour, self-paced capstone project. Learners can apply newly acquired skills in a scenario that emulates an attack by a sophisticated adversary.