CrowdStrike University

CROWDSTRIKE UNIVERSITY

CST 351
OPEN SOURCE INTELLIGENCE TECHNIQUES WITH FALCON

COURSE OVERVIEW

The Falcon Intelligence application contains an enormous number of artifacts and indicators to properly attribute attacks. However, you can still supplement Falcon Intelligence reporting with your own open source information to provide your organization with holistic and customized intelligence reports. This course introduces the concepts and methodologies needed to successfully extract indicators and artifacts from CrowdStrike® Falcon and conduct further Open Source Intelligence (OSINT) gathering as part of a larger intelligence reporting effort. The course will cover the basic concepts of secure online access and can help to protect collection efforts.

PREREQUISITES

To obtain the maximum benefit from this class, you should meet the following requirements:

- Comprehend course curriculum presented in English
- Completion of FHT 100 & FHT 101 course material in CrowdStrike University (or experience using CrowdStrike® Falcon)
- Perform basic operations on a personal computer
- Be familiar with Microsoft Windows environment

CLASS MATERIAL

Once registered for the course, associated materials may be downloaded from CrowdStrike University.

LEARNING OBJECTIVES

Students who complete this course should be able to:

- Retrieve indicators and specified pieces of intelligence from various Falcon applications, including Falcon Intelligence reporting
- Securely connect the collection endpoint to the Internet
- Conduct OSINT gathering on the Internet

This instructor-led course introduces numerous tools and techniques to enhance reporting with openly accessible information from the Internet using multiple hands-on labs that allow students to apply what they learned.

1-day program | 2 credits

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.

CrowdStrike University

CST 351 Open Source Intelligence Techniques with Falcon

INTRODUCTION

- Who we are
- Who you are
- Administrative items
- Course overview/agenda

INTRODUCTION TO INTEL AND OSINT

- OSINT Overview
- Intel 101: Where OSINT fits in
- Answering intelligence requirements
- Forming collection tasks
- Analytic models
  - Diamond Model
  - Cyber Threat Kill-Chain™
  - MITRE ATT&CK framework

CORE CONCEPTS

- Information overlap
- Technical skillsets
- Data pivoting
- Data ownership

MANAGED ATTRIBUTION

- Securing the user
- Securing the endpoint
- Securing the toolset
- Securing the connection

OSINT STARTING POINTS

- CrowdStrike® Falcon Application overview
- Falcon Intelligence reports and feeds
- Indicators
- Detections
- Malware analysis

OSINT TOOLS & SITES

- MISP
- Google dorking
- Domain name system
- IP geolocation
- Dump sites
- DarkNets
- Data mining
- Information aggregators

CONCLUSION