CROWDSTRIKE

CST 351 – OPEN SOURCE INTELLIGENCE TECHNIQUES WITH FALCON

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 one-day instructor-led course introduces the concepts and methodologies needed to successfully extract indicators and artifacts from the CrowdStrike Falcon application and conduct further Open Source Intelligence (OSINT) gathering as part of a larger intelligence reporting effort. It will offer hands-on training that will cover the basic concepts of secure online access and can help you protect your collection efforts. In addition, we will introduce numerous tools and techniques to enhance your reporting with openly accessible information from the Internet.

PREREQUISITES

There are no prerequisites for this course. A general knowledge of intelligence disciplines, network architectures, and Internet technologies is recommended.

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

- Completion of FHT 100 & FHT 101 course material in CrowdStrike University (or experience using CS Falcon)
- Able to understand course curriculum presented in English
- Perform basic operations on a personal computer
- Be familiar with the 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 end-point to the Internet
    - Understand and use proxies, VPNs, etc.
    - Understand and use virtual machines, including custom cloud-based machines
- Conduct Open Source Intelligence (OSINT) gathering on the Internet
    - Understand the Domain Name System (DNS) and IP registration
    - Define attacker network hierarchy and geolocation
    - Understand and exploit information from online information aggregators
    - Use OSINT tools such as Recon-NG, theHarvester, Shodan, and Maltego
    - Understand and utilize 'Google Dorking' for efficient searching

The course includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

REGISTRATION

For a list of scheduled courses and registration access, please log into 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.

INTRODUCTION

- Who we are
- Who you are
- Admin items
- Course Overview/Agenda

INTRO 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 End-Point
- Securing the Toolset
- Securing the Connection

OSINT STARTING POINTS

- CrowdStrike Falcon Application Overview
- Falcon Intelligence Reports & Feeds
- Indicators
- Detections
- Malware Analysis

OSINT TOOLS & SITES

- MISP
- Google Dorking
- Domain Name System
- IP Geolocation
- Dump Sites
- DarkNets
- Data Mining
    - Recon-NG
    - theHarvester
    - Datasploit
    - Maltego
- Information Aggregators

CONCLUSION