CrowdStrike University

CST 330
CREATING INTELLIGENCE WITH FALCON

COURSE OVERVIEW

This course introduces the doctrinal concepts of gathering and analyzing information to create intelligence products. It includes cyber threat intelligence methodologies but is more broadly focused on general intelligence doctrine. This is an introductory-level intelligence course and is appropriate for techies and non-techies alike who have little or no experience in intelligence functions and production. This course is intended for managers, report writers, intelligence consumers and analysts of all types.

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 intelligence reporting and data from various Falcon applications
- Relate basic intelligence processes and concepts to technical data
- Justify proposed security changes to an environment based on own intelligence analysis
- Support your organization's overall security posture by contributing customized, high-level cyber threat reporting

This instructor-led course introduces the doctrinal concepts of gathering and analyzing information to create intelligence products. It includes multiple hands-on labs that allow students to apply what they have learned.

2-day program | 4 credits

Registration

For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires four (4) 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 330 Creating Intelligence with Falcon

INTRODUCTION

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

CROWDSTRIKE FALCON

- Falcon applications
- Falcon intelligence
  - Review of each Falcon Intelligence module
- Student exercise
  - Discover detection in Insight and follow links to associated intelligence reporting

INTELLIGENCE 101

- Concepts of intelligence
  - Contrasting information from intelligence
  - Intel as a process, product and organization
  - Introduction to tactical, operational and strategic intelligence
  - Goals of an intelligence program
  - Various types of intelligence
- Characteristics of effective intelligence
  - Attributes of effective intelligence
  - Intelligence frameworks
  - Creating a flexible framework
  - High-order intel program capabilities
- The intelligence process
  - The intelligence cycle & process
  - Key considerations of an intel framework
- Intelligence consumers
  - Various levels of consumers
  - Consumer level-appropriate reporting
- Intelligence reach
  - External collaboration
  - Intel sharing platforms
  - CrowdStrike® intelligence

INTEL REQUIREMENTS

- Requirements process
- Framing the intel problem
- Introduction to structured argumentation
- Forming a requirement hierarchy
- Student exercise
  - Group exercise to create standing and ad-hoc requirements

INTEL COLLECTION

- Selecting sources of information
- Collection aggregation and storage
- Legalities of collection
- Timing of collection
- Student exercise
  - Group exercise to identify and gather sources of information

INTEL ANALYSIS

- Concept of exactness
- Types of analysis
- The analytic process
- Analytic views and models
- Traits of a good analyst
- Student exercise
  - Individual and group tasks to analyze collected information

INTEL PRODUCTION

- Echelons of reporting
- Proper report formatting
- The reporting framework
- Challenges of production
- Student exercise
  - Individual and group tasks to report on collected and analyzed information/intelligence

FRAMEWORK VALIDATION

- Intelligence framework concepts
- Intelligence validation
- Framework validation
- Student exercise
  - Group discussion and validation of student-built intel framework

FALCON SPOTLIGHT & FALCON INTELLIGENCE

- Introduction to Falcon Spotlight and Falcon Intelligence