CrowdStrike University

CTI 346
STRUCTURED ANALYTIC TECHNIQUES FOR CYBER ANALYSTS

COURSE OVERVIEW

This course introduces the five core categories of structured analysis and incorporates individual structured analytic tools. Structured analytic techniques are scientifically-derived tools that analysts can use to abstract their biases out of their own analysis and can also be used to gain insight into the meaning and value of large sets of information. Through the use of these techniques, the analyst is able to provide better accuracy, relevancy and substance to their intelligence reporting.

PREREQUISITES

Experience at a national-level intelligence organization or successful completion of CTI 330: Creating Intelligence with Falcon.

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

- Comprehend course curriculum presented in English
- Completion of FHT 100 & FALCON 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:

- Discuss and compare the five core groups of structured analytic techniques and their varied uses
- Apply structured analytic tools to sets of unstructured data to create intelligence

1-day program | 2 credits

This instructor-led course introduces the five core categories of structured analysis and incorporates hands-on exercises of the individual structured analytic tools to allow students to apply what they have learned.

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

CTI 346 Structured Analytic Techniques for Cyber Analysts

INTRODUCTION

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

INTEL OVERVIEW (REVIEW)

- Review of Intel 101 (CTI 330)

STRUCTURED ANALYSIS OVERVIEW

- (Re) Introduction to Structured Analysis
- Grouping of techniques
  - By method/use-case
  - By collaborative effort
  - By complexity
- Structured argumentation
- Habits of a "master thinker"

ORGANIZING TECHNIQUES

- Sorting tools
- Chronologies and timelines
- Link charts and diagrams
- Matrices

IMAGINATIVE THINKING

- Brainstorming
- Outside-In-thinking
- Red Team analysis
- Alternative futures analysis
- Counterfactual reasoning
- Morphological reasoning

DECISION MAKING

- Event mapping
- Event tree
- Subjective probability
- Weighted ranking
- Argument mapping

DIAGNOSTIC TECHNIQUES

- Key assumption check
- Quality of information check
- Indicators or signpost of change
- Analysis of competing hypotheses
- Adversary intentions matrix

CONTRARIAN TECHNIQUES

- Devil's advocacy
- Team A/Team B
- High-impact/low probability
- What if?

CONCLUSION