Cyber Series Course 1: Cyber Intelligence Tradecraft Certification

COURSE DESCRIPTION:

This course provides definitive sections along the intelligence lifecycle that are in-depth, aligned to DoD instructions such as the Joint Publication 2.0, DoDI 3305.13,and 3305.02. Following the intelligence lifecycle, students are required to demonstrate understanding and use of collection methods using defined targets and target case studies, understanding and applying analytic techniques, when and how to use analytic techniques and analytic types. Using direction from Sherman Kent and analytic methods from Richards Heuer, students are presented case studies for analysis, required to use tradecraft methods, and provide written reports in standard analytic format. Students are also required to orally present their deliverables to the class. Students leave this course with the tools, methods, and understanding necessary to enhance intelligence programs.

The course is taught in a crawl, walk, run format. What does that mean? We teach the academics first in classrooms style. We then follow up with a review of the materials in conjunction with case studies and scenarios. The run section of the course follows with case studies taking the student through the cyber intelligence lifecycle from priority intelligence and information requirements, task assignments, potential data sources and focus of analysis, potentially relevant data, examination of tactics, techniques, and procedures (TTPs), TTP use for hunt and detect, reductionism, usable data, structured methods of analysis, credibility and relevance of data, findings, campaign analysis, analytic review, peer review, written briefs and assessments, and dissemination.

OUTLINE:

DAY 1 – Anonymity and Passive Persona setup, Collection Methods and Techniques, Collection Planning, PIRs, Collection Process Flow, Collection Tools and Targeting, Alignment with Hunt and Detect Needs, Ties to CSIRT, TTPs, IoCs, Threat Intelligence, Open Source Intelligence, All-Source Intelligence, Standard Glossary and Taxonomy – 1 Day (Case Study 1)

DAY 2 – Organization, Production, and Structured Analytic Techniques, Adversary Denial and Deception, Use of Techniques, Types of Evidence, Production Management, Critical Thinking, Process Flow, Metrics, Intake forms, and templates (Case Study 2)

DAY 3 – Types and Methods of Analysis, Decomposition, Recomposition, Methods for Fusion, Case Studies in Analysis, Cognitive Bias, Credibility and Reliability of Sources, Confidence Levels, Analysis of Competing Hypothesis, Flow into Hunt, Detect, CSIRT, TTPs, IoCs, Inductive/Abductive/Deductive Reasoning, Historic trending and campaign analysis, Intelligence for organizational resilience (Case Study 3)

DAY 4 & 5 – Case Study 4, Identifying Your Consumers, Stakeholder Identification, and Analysis, Standing Orders from Leadership, Analytic Writing, BLUF, AIMS, Types of Reports, Product Line Mapping / Report Serialization, and Dissemination, Cyber and Threat Intelligence Program Strategic Plan, Goals, Objectives.

NOTE: Students need to bring a laptop. PC based is preferred but Mac will work. Students require administrative access to the laptop and the laptop should not have corporate controls that block installation and access to various websites. All activities performed during the class comply with US law.

All students receive an Amazon Fire 7" Tablet Display WiFi 8GB. Books are pushed to the tablet for classroom use.

Students who complete the course will be certified as Cyber Intelligence Tradecraft Professional.

CEU's Available at Student Request.