Integrated Threat Analysis Course Syllabus (ITAC)

This 40-hour, five (5) day course prepares mutli-disciplined intelligence analysts and private industry to understand, operate, and successfully contribute to cyber defense, offense, all hazards analysis, and decision making. Our goal is to promote a more efficient integration between mission operation and analyst by honing intelligence analysts' skills in the cyber domain.

Through hands-on exercises and team collaboration, ITAC students will explore use-cases from around the world to practice effective tradecraft and be prepared to operate immediately.

Contact Information

Contact: 443-620-TEAM (8326) Option #2 **or** training@teamworxsecurity.com

Course Description and Course Goals

- Introduction to and comparison of traditional operations to cyber operations
- Introduction to intelligence life cycles
- Integration of intelligence processes to scenarios
- Ability to read and understand network diagrams
- Ability to communicate network diagram key terrain
- Introduction to the Joint Dynamic Targeting Cycles
- Introduction to threat actors, techniques, and tools
- Ability to recognize threat actors and TTPs
- Introduction to structured analytical techniques
- Practice in researching and validating resources for use in analysis
- Ability to communicate actions taken into written report or verbal discussion

Module 1

- Review of Cyber Threat Intelligence
- Exposure to Titles and Authorities
- Understanding of threat types based on motives and targets
- Application of identifying threat types based on TTPs
- Understanding and identification of IOCs
- Introduction of network devices and protocols

Module 2

- Introduction to attack types through real world examples
- Understanding of the Defense in Depth Model
- Practical application of technical jargon translation to easily recognizable language
- Introduction to Cyber Threat Intelligence tradecraft and tools

Module 3

- Review of Intelligence Life Cycles
- Practical application of Intelligence Life Cycles through case study
- Introduction to the Joint and Dynamic Targeting Cycles
- Practical application of the Dynamic Targeting cycle through case study
- Understanding of Structured Analytical Techniques
- Practice in analytical report writing and presentation

Module 4

- Review of online best practices for secure research
- Introduction to malware analysis and MATRIX Demo
- Demonstrate mastery of course concepts through a comprehensive capstone exercise

Module 5

- Apply hands-on learning acquired during the preceding four days, showcasing practical application and integration of acquired knowledge
- Presentation Skills and public speaking

Students will Need

A computer with internet access. Students are welcome to bring any other note taking materials they wish. (some handouts will be provided)

Grading

This course is based on participation within daily discussions and group activities. Students **MUST** be present to do so.

Course Schedule

Course schedules can vary based on customer needs.

Five (5) Day Course Schedule Expectations:

- Daily start time will be 0900 (9 a.m.)
- Daily end time will be between 1600 (4 p.m.) and 1730 (5:30 p.m.)
- Daily lunch break time will be between 1130 to 1300 (1:00 p.m.)
- Daily schedule may flex based on how quickly students are understanding concepts and questions