Advanced Threat Analysis Course Syllabus (ATAC)

This 40-hour, five (5) day course teaches multi-disciplined intelligence analysts to hone their understand of networks, cyber terminology, and adversarial actions to successfully contribute to cyber intelligence operations from a fusion perspective.

Through hands-on exercises and team collaboration, ATAC 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 advanced threat modeling
- Ability to recognize treads in analysis
- Understanding of cyber threat framework stages
- Application of Tactics, Techniques, and Procedures (TTPs) based threat hunting
- Understanding of critical thinking, analytic failures, and logical fallacies
- Introduction to research and data collection techniques
- Practical hands-on application of tools and techniques

Module 1

- Review of collection requirements
- Review of Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs)
- Ability to identify and categorize portions of the Pyramid of Pain
- Practical application of the Diamond Model and Threading
- Review of MITRE ATT&CK tooling

Module 2

- Introduction to Cyber Threat Framework Stages
- Comparison of and exposure to Cyber Threat Framework types
- Understanding the Cyber Kill Chain and Threat Framework crosswalk
- Understanding the Diamond Model and Threat Framework crosswalk
- Introduction and application of TTP based threat hunting

Module 3

- Understanding of critical thinking concepts
- Understanding of analytical failures, pitfalls, and tendencies
- Understanding of analytical best practices
- Introduction to logical fallacies
- Understanding relevance in research techniques

Module 4

- Exposure to helpful research tools
- Introduction to research and data collection techniques
- Practical application of collection matrices

Module 5

- Understanding of analysis and production
- Practical application of research, analysis, and reporting
- Show positive knowledge transference through capstone exercise

Students will Need

A computer with internet access. Students are also 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