TeamWorx SECURITY
INTELLIGENT WORKFORCE TECHNOLOGY

Key Terrain Analysis Course (KTAC) Syllabus

This 40-hour, five (5) day instructor led course that teaches the technical and non-technical operator and analyst how to define, identify, document, and guide efforts of decision makers within cyber key terrain.

Our courses are primarily designed for the Department of Defense intelligence analyst but also meet the training and mission needs of any analyst. Our goal is to promote a more efficient integration between mission operation and analyst.

Contact Information

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

Course Description and Course Goals

- This course is designed and created for the Intel Analyst role that is an already integrated member to cyber operations
- Will include a pre-assessment and capstone evaluation
- Fluid understanding of kinetic key terrain based on Joint Publication
- Comparison of non-kinetic (cyber) key terrain to identified kinetic key terrain
- Clear scenario-based learning surrounding key terrain aspect culminating in a 4-hour capstone event
- Utilization of real world network topology and symbology to identify and guide decision makers understanding of key terrain options and understanding
- Understanding of the ever changing and evolving nature of cyber terrain
- Delivering tactical information requirements through Operational and Strategic Operations
- Review of current threats within the cyber domain, breaches, and threat frameworks and understanding how to apply key terrain evaluations to them
- Wholistic hands-on review of a recent malware/ransomware event, including the reverse engineering and forensics point of view, to obtain an appreciation for malware analysis and achieve the ability to tell the story of malware threats in reports and briefings
- Students will gain a spectrum of understanding behind adversarial actions and dive deep into thinking like the adversary
- Students will be able to speak knowledgably to and understand network and cyber terminology and produce clear and concise statements for decision makers
- Students will come away with a repeatable foundation for success in future scenarios

Students will Need

- Note taking materials (notepad, pen, pencil, etc.)
- Access to a computer with internet access (video conferencing capabilities, TeamWorx Security will utilize a conferencing platform that meets the students' needs if remote.)

Grading

This course is based on participation within daily discussions, and group activities. In most cases, discussions are based on assigned homework from the night prior. Therefore, homework counts towards the grading and completion of the course. With the requirement for grading based on participation, the student **MUST** be present to do so. Additionally, the course will wrap with a 4-hour, scenario based cyber key terrain analysis to be presented by the teams to the instructors.

Assignments and Homework

- Homework will include reading assignments to spark conversation during morning sessions.
- Homework assignments will require students to apply skills learned throughout the course to reports in Hive-IQ through provided accounts.
- Capstone event will be an assigned team event and require participation to receive a certificate.

Course Schedule

Course schedules can vary based on customer needs.

Five (5) Day Course Schedule Expectations:

- Daily start time will be 0800 (8 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 ebb and flow based on how quickly students are understanding concepts and questions