Key Terrain Analysis Course Syllabus – Operational Technology (KTAC-OT)

This 32-hour, four (4) day course teaches technical and non-technical operators and analysts how to identify, define, document, and guide efforts of decision makers within cyber key terrain and the operational technology environments. Students will become intimate with operational technology terrain and the importance of each device and its capability to be a part of key terrain. Through hands-on exercises and team collaboration, KTAC-OT 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 Key Terrain basics as defined in Joint Publications
- Understanding of the differences between Information Technology (IT) and Operational Technology (OT)
- Ability to recognize and identify Key Terrain-Cyber, IT and OT
- Ability to recognize and identify IT versus OT network traffic
- Understanding of the appropriate tools for each network
- Ability to use Key Terrain-Cyber understanding to influence decision makers
- Understanding of the ever changing and evolving nature of cyber terrain
- Culminating exercise to apply above goals

Module 1

- Pre-Assessment
- Introduction to key terms and acronyms
- Introduction to guiding policies and doctrine
- Understanding of policies and doctrine applied to tradecraft
- Introduction to and application of key terrain markings
- Historical background of key terrain or terrain advantage
- Review of key terrain tracking responsibilities
- Application of key terrain identification using real world scenarios

Module 2

- Review of necessary key terms and acronyms
- Understanding Information Technology (IT) versus Operational Technology (OT)
- Introduction to the Purdue Model
- Understanding identification of OT Key Terrain-Cyber
- IT versus OT network tool discussion
- Demonstrate identifying ICS/SCADA network traffic
- Demonstrate understanding of IT versus OT network Traffic
- End of day Key Terrain discussion

Module 3

- Review of necessary key terms and acronyms
- Defining IT versus OT capabilities and use cases
- Introduction to information technology and operational technology convergence
- Review of IT tools used for OT networks
- Demonstrate use of GrassMarlin (OT specific tooling)
- Historical review of attacks on OT based systems
- Application of OT Key Terrain-Cyber identification
- End of day Key Terrain discussion

Module 4

- Show positive knowledge transference through capstone exercise
- Practical application of research, evaluation, and analysis of data
- Practical application of briefing skills and public speaking

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.

Four (4) 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