Cyber For Linguist Course Syllabus (C4L)

This 40-hour, five (5) day course educates linguists and other relevant occupations on basic cyber, networking, information technology, and cyber threat intelligence concepts. This course integrates additional support functions into the cyber domain and it's everchanging environment

Through hands-on exercises and team collaboration, C4L 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

- Ability to recognize the difference between cyber related and intelligence support tasks
- Introduction to digital network components and networking concepts
- Introduction to the cyber threat landscape
- Ability to recognize types of operating systems
- Introduction to cyber threat types and intelligence processes
- Understanding of researching techniques
- Introduction to vulnerabilities and cyber hygiene concepts
- Introduction to malware and ransomware
- Exposure to geo-tagging
- Exposure to industry standard and open source tooling

Module 1

- Introduction to terms and acronyms
- Introduction to digital networking components
- Introduction to network types and network traffic
- Familiarization of types of attacks
- Understanding of spam and phishing

Module 2

- Ability to recognize operating systems between desktop and mobile devices
- Introduction to cyber threat types and advanced persistent threats (APTs)
- Introduction to Cyber Kill Chain ®, Tactics, Techniques, and Procedures (TTPs), and Indicators of Compromise (IOCs)
- Exposure to researching techniques
- Exposure to MITRE ATT&CK concepts

Module 3

- Introduction to vulnerabilities and critical vulnerabilities and exploits (CVEs)
- Exposer to Patching and updating concepts
- Understanding of defense in depth
- Ability to apply basic cyber hygiene concepts
- Introduction to malware and Ransomware
- Introduction to the anatomy of scammers and phishing

Module 4

- Exposure to geo-tagging
- Exposure to industry standard and open-source tools
- Practical application of tools

Module 5

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

Students will Need

Access to 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