Open-Source Analysis Course Syllabus (OSINT)

This 40-hour, five (5) day course is designed for the intelligence analyst role as an integrated capability to operations, specifically tying in open-source and publicly available information. Using the OSINT framework students will learn how to use openly available data to help build threat profiles and pictures.

Through hands-on exercises and team collaboration, OSINT 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 Open Source and Publicly Available Information (PAI)
- Introduction to OSINT landscape and evolving tools
- Ability to demonstrate the use of online safety tools
- Ability to associate threats with open-source tooling and software
- Integration of open source and PAI to cyber domain
- Ability to communicate actions taken into written report or verbal discussion

Module 1

- Introduction to open source and PAI data types
- Understanding of Virtual Private Networks
- Exposure to ‘safe’ browsing techniques
- Introduction to open-source mapping tools
- Comprehension of types of bias when conducting research
- Practice turning analysis into legible reports for publishing
- Exposure to sock puppet accounts

Module 2

- Introduction to open-source research tools
- Practice using open-source research tools
- Comprehension of Google dorking
- Exposure to web archives
- Understanding of geographical tagging

Module 3

- Understanding of The Onion Router (TOR)
- Exposure on how and when to use TOR
- Exploration of Social Media Accounts for PAI data
- Understanding types of username searches
- Exposure to image and video searches
- Comprehension in Geo-Tagging and social media location services

Module 4

- Exposure to Cyber open-sources tools and dashboards
- Practice using phishing resources and repositories
- Exposure to malicious files and malware repositories
- Introduction to Cyber Threat Intelligence (CTI) resources
- Introduction to cyber threat maps
- Exposure to OSINT and PAI communities

Module 5

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

Students will Need

Access to a computer with internet access. Students are also welcome to bring any other note taking means 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