Certificate in Open-Source Intelligence (OSINT) Fundamentals

Why Attend

- Open-Source Intelligence (OSINT) can provide organizations with an insight into their digital footprint by utilizing the Internet to determine if any part of their organization or staff members are exposed; and thereby expedite decision making as part of their risk management process.
- On this three-day National Cyber Security Center (NCSC) certified training course, participants will gain an understanding of what OSINT is and how to utilize it. Moreover, participants will learn how to efficiently collect, monitor, and analyze OSINT findings and present these to stakeholders.
- Upon completion of the course, participants will have a solid foundation in the field of OSINT and will have real-world confidence in this discipline with an ability to carry out effective OSINT investigations. Participants will have the opportunity to earn an NCSC Certified Training Course Completion Certificate that is valid for 3 years.

Course Methodology

- This course uses a combination of presentations, group discussions, case studies and exercises based on real life situations.

Course Objectives

By the end of the course, participants will be able to:

- Identify definitions, meanings and the use of concepts and terms that are used in the OSINT field
- Analyze their organization's intelligence requirements
- Develop an understanding of the intelligence lifecycle and the individual components contained within it
- Apply advanced search engine techniques to optimize search results
- Develop an awareness of some of the more common geolocation services available and how to exploit data from imagery for OSINT purposes
- Explain the digital footprint that is left when using the Internet, the dangers associated, and how proper tradecraft can protect against counter surveillance
- Comply with legal requirements and counter OSINT bias

Target Audience

- This course is suitable for OSINT Investigators, Cyber Threat Intelligence Analysts, Financial Crimes Investigators, Human Resources Personnel, Insurance Investigators, Intelligence Personnel, Law Enforcement, Private Investigators and all Security Awareness Staff. It is also suitable for those in the IT field looking for an introduction to OSINT.

Target Competencies

- Legal Research
- Privacy Laws
- Data Protection
- Intelligence and Analysis
- Secure Operations and Incident Management

Overview of Open-Source (OSINT) Intelligence

- Identify definitions, meanings, and use of concepts and terms, that are used in the OSINT world
- The need for, and the benefits of, OSINT

Intelligence Requirements

- The organization's intelligence requirements
- Where to find intelligence requirements

The Intelligence Lifecycle

- The intelligence lifecycle and the individual components contained within it
- The intelligence lifecycle requirements

Leveraging the Internet

- How search engines work
- The value of data online
- Analysis of high-profile data breaches
- Using advanced search engine techniques and features to optimize search results

Imagery Exploitation

- Introduction to how geolocation works
- Common geolocation services available, and how to exploit data from imagery for OSINT purposes
- Protecting organization assets from imagery or geolocation services

OSINT Tradecraft

- The digital footprint, the dangers associated, and protection against counter surveillance
- Legal compliance and counter OSINT bias