MINISTRY OF DIGITAL

CyberGuru
CYBER SECURITY PROFESSIONAL DEVELOPMENT

CyberSecurity MALAYSIA

OPEN SOURCE INTELLIGENCE (OSINT)

Level: Fundamental | **Duration:** 2 days

With the rapidly increasing amount of information that reside on the internet due to digital transformation, managing digital security & privacy of Personally Identifiable Information (PII) of organisations and individuals has become more difficult, as more digital footprints are left on the internet can be backtracked/traced to reveal private/ sensitive information.

As these sensitive, and at times confidential information are on the internet, the information are considered open source; or publicly available and are easily searched by anyone, including cyber criminals and law enforcement agencies for investigation purposes.

The main objective of this training is to combine digital security and privacy awareness by integration of certain domains/clauses under the ISO 27001:2013 (Information Security Management System), its extension relating to privacy; ISO/IEC 27701:2019 (Privacy Information Management System) international standard and Open Source Intelligence (OSINT) techniques as a risk assessment technique for additional security controls (for risk identification, management/mitigation) of information privacy.

The integration aims to raise awareness and expose participants to the concept of data privacy by looking at different perspectives; from both a malicious threat actor and a data protection officer (DPO)/ auditor/investigation officer, journalist, academician/students or researcher.

Participants will be trained on Open Source Intelligence techniques, methodologies and using specific tools to find, gather and analyse Personally Identifiable Information (PII) sources from the Internet that pose risks to an individual or organisation based on the specific requirements and controls specified in the ISO 27001:2013 (ISMS), ISO 27701:2019 (PIMS) international standards for the purpose of collecting evidence for an audit, research or investigations.

Whether you are just getting started in information security or cybersecurity, OSINT plays an important role in various types of investigations and research purposes; from counterterrorism and crime investigations, auditing, job candidate background search to academic research.

Objectives

1. This training will focus is on two different aspects of OSINT; the first being from an investigations perspective and the other from a normal user of the Internet – giving exposure to participants the numerous ways that criminals steal your personal information and explains how they benefit from the data obtained. The presentation includes live demonstrations of how you and your family are likely to be attacked and the easy steps which anyone can take to prevent becoming a victim.
2. You will learn real-world applicable skills that are utilized by law enforcement, military intelligence, private investigators, loss prevention, cyber defenders and attackers all use to help aid in their investigations.
3. Participants will be taught the theoretical aspects of OSINT; the definition, framework, objectives, users, advantages and disadvantages, legal aspects and shown real world case scenarios of crime investigations and research done with OSINT.
4. The goal is to create an industry-leading body of knowledge and skillsets standards that can be taught, tested and validated so you can be successful in your career regardless if you are in law enforcement, intelligence, loss prevention, private investigations, information security, or cybersecurity.

Target Participants

Participants can be from various backgrounds who are interested in enhancing their skills in information gathering and analysis of publicly available data found on the Internet. Possible candidates include who are interested in knowing more about their data and how they are used on the Internet by looking at data from the perspective of a cybercriminal and investigator in the aspect of privacy and digital security.

Entry/Enabling Requirements

- Intermediate computer user and internet literate.
- Familiar with social media networking sites/platforms.
- Analytical and creative thinker.

Career pathway

- Journalist – Investigative journalism specialising in fact-checking and open-source intelligence.
- Private investigators
- Law enforcement investigation officers
- Academia – (students,tutors,lecturers/researchers) for research/ studies/assignments
- Non profit/NGOs
- Human Resources
- Data Protection Officers

Modules

Know your Internet – Understanding surface web, deep web & dark web

- Participants will learn and understand the differences of surface web, deep web and the dark web in the perspective of data/information and security.
- Learn the definition and types of Personally Identifiable Information (PII) and Digital Footprints that can be found on the web; how it can be searched and where it can be found.

Cyber/Web Intelligence Framework

- Participants will learn the overall intelligence framework and the define the differences of each intelligence channel such as HUMINT, SOCMINT, IMINT and OSINT.
- Focus of the course will be data/information gathering on the Internet with Open Source Intelligence (OSINT) and its sub branch, Social Media Intelligence (SOCMINT) for specifically searching, analysing and validation of PII on social media:
  - OSINT Definition
    - » Legal & Ethical considerations of OSINT in international & Malaysian law
    - » What OSINT is not – comparing OSINT to doxing
    - » Real world OSINT users – participants will learn about the real world users of OSINT
    - » The different modes of open source intelligence – HUMINT, IMINT/GEOINT, SIGINT and MASINT
  - Advantages/Disadvantages & Scenarios where OSINT can/is used
  - The Framework – Using the OSINT framework as a guideline to start investigations/research
  - Cycle/Process – identifying the process/cycle involved in information gathering with OSINT.

Create an OSINT process

- Defining the target, scope & objectives – participants will learn to identify target/subject, define the search scope and the objectives using the OSINT framework and process as a guideline.

Understand the data collection life cycle

- Participants will be taught to identify and analyse and differentiate data/information that can be of use in an investigation/research.
- Searching for in-depth data/information through pivoting methods
- Analyse links between data and correlate to form a stronger evidence/link to the target/subject.

Conduct OSINT investigations in support of a wide range of customers

- Participants will learn methods to identify the method of investigation/search for different types of customers from different backgrounds; law enforcement, marketing, human resources, academia

Create a secure platform for data collection

- Creation of a secure platform for data/information gathering with Virtual Machines
- Participants will learn to setup and use specific tools and methods to collect data on a subject/target

Capture and record data

- Methods and tools used to capture and record data/information gathered on the web will be taught to participants for intelligence reporting.

Harvest web data

- Participants will be taught on how to harvest open source web data for specific purposes using special techniques and tools

Perform searches for people

- People-specific search methods for PII vulnerabilities tracking using digital footprints search methods

Access social media data (SOCMINT)

- Social Media Intelligence data collection methods and tools

Collect data from the dark web

- Data/information gathering on cryptocurrency wallets

<u>Practical & Hands-on</u>

- Identification of Personally Identifiable Information (PII)
- Identification of types of digital footprints; and how it can be backtracked and correlated to PII using search, information (intelligence) gathering and analysis techniques of OSINT.
- Installation and usage techniques of privacy based browser, browser extensions, search engines and services to search and gather information (intelligence) and expose websites that tracks visitors/users with ad-tracking/analytics therefore exposing private/sensitive information.
- Collect open source intelligence/information from specific social media platform using a combination of OSINT and non OSINT tools. Students are then taught on the types of data that can be collected, analyse and finesse the information collected into actionable intelligence/information in the form of an intelligence report.
- Students will be taught on analysis and reporting techniques based on the information (intelligence) gathered and the various ways it can be misused, traced to Personally Identifiable Information of an individual/organisation and how it can impact/severity of data privacy.

For additional information, please visit www.cyberguru.my. You can also contact us at training@cybersecurity.my or call at 03 8800 7999

CyberSecurity Malaysia,
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia

Tel: +603 8800 7999 **Fax:** +603 8008 7000
Email: info@cybersecurity.my
Customer Service Hotline: 1 300 88 2999
Website: www.cybersecurity.my