Updated 05/07/2024

Sign up

OSINT and Counter OSINT training

2 days (14 hours)

Presentation

Our OSINT (Open Source Intelligence) training course will give you the method and tools to succeed in your search for public information.

With the emergence of the Internet, the volume of data available has exploded. The ability to collect, process and analyze this data has become a rare skill. Indeed, it is essential to be on the lookout for the latest news or weak signals to gain a competitive edge.

By following our training course, you will learn the basics of data retrieval.
open-source, legislation on data collection, social and ethical impacts, and various monitoring tools.

You'll learn all about the essential tasks involved in Open Source Intelligence, including how to collect open-source data using intelligence tools, how to comply with legal and ethical standards, and how to ensure that data is properly analyzed.

We'll also teach you how to protect yourself against OSINT attacks. This part will teach you good security practices and how to protect your privacy.

Objectives

- Understanding OSINT and its importance
- Understanding the social and ethical challenges of Open Source Intelligence
- Securing your data with OSINT

Target audience

- Data scientists
- Data analysts
- Project Managers
- Intelligence analysts
- Business analysts

Prerequisites

No prerequisites.

OSINT and Counter OSINT training program

DAY 1: Introduction to OSINT

- What is Open Source Intelligence / OSINT?
- OSINT objectives
- OSINT's main users

OSINT ethics

- Social impact - Avoiding illegal collection
- Ethical principles - Respect for privacy

Case studies

- OSINT usage examples - Shodan - HaveIbeenpwnd
- OSINT protection application examples - Threat identification

OSINT data collection

- Media monitoring (Interviews, News)
- Article follow-up (Academic Research, Journalism)
- Report follow-up (NGOs, governments, police and justice services, international agencies)
- Internet monitoring (websites, forums, social networks)
- Geospatial tracking (GEOINT)
- Tools: Recon-ng, Maltego, Maps...

DAY 2: OSINT data analysis

- Analytical techniques - Case study: Sentiment analysis on Twitter
- Data visualization

Protection against OSINT

- OSINT threat assessment - Risk assessment
- Upstream and downstream OSINT countermeasures (VPN, Wireshark, etc.)

Information security

- Security threats - Social engineering and phishing
- Security practices - Two-factor authentication

Privacy policy

- Online privacy
- Privacy tools - Email encryption (Signal, ProtonMail and best practices)

Complementary module (+1 day) : Competitive analysis and dashboards

OSINT strategies

- Why establish an OSINT strategy?
- Strategy creation process

Competitive analysis

- Why is competitive analysis important?
- How do you perform an OSINT competitive analysis?
- The best tools

Creating OSINT dashboards

- Introduction
- The different elements
- Criteria for a good OSINT dashboard
- Introducing the best tools

Advanced protection against OSINT

- Advanced techniques to protect your information
- Case study: How can organizations protect themselves against OSINT data collection?
- Simulation scenarios to apply acquired skills
- Analysis of results

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.