Updated on 22/08/2025

Sign up

OSINT training

3 days (21 hours)

Presentation

Our AI-oriented "OSINT" training course will enable you to master the methods and tools needed to effectively exploit information from open sources. OSINT (Open Source Intelligence) has become a strategic asset for cybersecurity teams, and the integration of artificial intelligence now makes it possible to automate, sort and rapidly analyze data to identify the most relevant information.

Our AI-oriented OSINT training course is designed for cybersecurity professionals (CISOs, SOC managers, SOC analysts, cybersecurity consultants). It takes a practical, operational approach, with concrete workshops and case studies to help you put what you've learned into practice right away.

During the course, you will discover the principles and challenges of OSINT, learn to collect, sort and analyze data from open sources, and put into practice the use of AI tools (LLM, SpiderFoot HX, Maltego, 1 TRACE...) to automate and enrich your investigations. You'll be able to conduct a complete OSINT investigation, and deliver an analysis that can be directly used to enhance your organization's security and responsiveness.

At the end of the course, you'll be able to conduct an OSINT 360 investigation, effectively sort and analyze the data collected, and integrate OSINT into an operational framework to enhance your organization's security and responsiveness.

Objectives

- Understand the principles and challenges of OSINT
- Master information gathering tools and techniques
- Collect, sort and analyze data
- Use artificial intelligence (AI) tools to automate, filter and analyze data from open sources
- Integrate OSINT into an operational framework

Target audience

- CISO
- SOC Managers
- SOC analysts
- Cybersecurity consultants
- Anyone responsible for the security of a corporate information system.

Prerequisites

- Basic computer skills
- Notions in data analysis and writing

OUR OSINT IA-ORIENTED TRAINING PROGRAM

[Day 1 - Morning]

Introduction to OSINT and legal framework

- Definition and challenges of OSINT for cybersecurity
- Typology of open sources (Surface Web, Deep Web, Dark Web)
- Limits, ethics and legal aspects (RGPD, legal framework in France/EU)
- OSINT cycle: Planning ? Collection ? Analysis ? Dissemination
- Principles and challenges of OSINT in a cybersecurity and organizational context
- Practical workshop: Mapping open sources relevant to an SOC case (sites, forums, social networks, public databases).

[Day 1 - Afternoon] OSINT

collection methodology

- Drawing up a research plan (hypotheses, keywords, scenarios)
- Advanced search techniques (Google Dorks, alternative engines, metasearch)
- Evidence archiving and preservation (hash, capture tools)
- Mastering information gathering tools and techniques
- Practical exercise: Searching for sensitive information on a fictitious company.

Basic OSINT tools

- Secure browsers and useful extensions
- Collecting information on social networks (Facebook, LinkedIn, Twitter/X, Instagram)
- Metadata (images, documents, PDF files)
- Practical workshop: Extracting and analyzing metadata from a document set.

[Day 2 - Morning]

OSINT on technical infrastructures

- WHOIS, DNS, Shodan, Censys, Hunter.io, LeakLooker
- Exploration of networks and sub-domains
- Mapping exposed infrastructures
- Practical workshop: Identification of exposed services of a fictitious target with Shodan/Censys.

[Day 2 - Afternoon]

OSINT and Threat Intelligence

- Correlation of collected data
- Cross-referencing with databases of leaks and paste sites (HaveIBeenPwned, BreachDirectory)
- Introduction to Maltego and relational graphs
- How to collect, sort and analyze data efficiently
- Practical workshop: Create a target's relational graph from collected data.

Automating data collection with AI and scripting

- Presentation of automation tools (TheHarvester, SpiderFoot HX, recon-ng, 1 TRACE, Maltego)
- Using AI (LLMs, NLP) to filter, categorize and prioritize data
- Advanced case study: filtering a data dump (CSV/JSON) with an LLM and generating a prioritization table
- Discussion: limits, biases and security of data entrusted to AI
- Using artificial intelligence tools to automate, filter and analyze data from open sources
- Practical exercise: Automate an OSINT search and generate a summary with AI.

[Day 3 - Morning]

Integrating OSINT in an operational context

- Role of OSINT in a SOC and for a CISO
- Use cases: internal investigations, threat hunting, competitive intelligence, crisis management (cyber attacks, data leakage)
- OSINT reporting formats and appropriate communication (CISO, GM, SOC teams)
- Integrating OSINT into an operational security framework
- Interoperability: integrating OSINT into a SOC/SIEM/TIP
- Practical exercise: Writing an OSINT mini-report based on real data collection.

[Day 3 - Afternoon] Final

case study

- Implementation of the OSINT method from start to finish:
- Define the problem
- Identify and collect sources
- Sort and analyze data
- Present an operational report
- Case study: OSINT investigation on a fictitious target with final presentation to the group.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT 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 training: 60% hands-on, 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.

Certification

A certificate will be awarded to each trainee who has completed the entire course.