

Open-Source Intelligence (OSINT)

Learn to gather, analyse and report open-source intelligence across the web, social media, dark web and multimedia sources.

40 Hours

DURATION

12

MODULES

48

TOPICS

COURSE OVERVIEW

This course covers the fundamentals, methodologies and legal considerations of open-source intelligence, and how to set up a secure OSINT lab using virtual machines and anonymity tools. It then addresses search engine and Google dorking techniques, social media intelligence, email and username investigations, and website and domain intelligence. Further modules examine dark web investigations, geolocation and image analysis, video and audio analysis, and people and identity investigations. The course concludes with OSINT for cyber threat intelligence and with reporting and operational security practices.

WHO THIS COURSE IS FOR

OSINT Investigators

Threat Intelligence Analysts

Cybersecurity Analysts

Incident Responders

Digital Forensics Investigators

Security Researchers

LEARNING OBJECTIVES

- Explain OSINT scope, methodologies and legal considerations
- Configure a secure OSINT lab using virtual machines and anonymity tools
- Apply advanced search engine and Google dorking techniques
- Analyse social media platforms for intelligence and network mapping
- Investigate email addresses and username footprints across platforms
- Perform WHOIS lookups and domain and infrastructure reconnaissance
- Access and investigate dark web marketplaces and forums securely
- Identify threat actors and support cyber threat intelligence with OSINT

12 Modules, 48 Topics

01

Introduction to Open-Source Intelligence (OSINT)

TOPICS

- What is OSINT? Scope and Applications
- OSINT vs. Threat Intelligence vs. Reconnaissance
- Ethical and Legal Considerations in OSINT
- OSINT Methodologies and Frameworks (OSINT Framework, IntelTechniques)

02

Setting Up an OSINT Lab

TOPICS

- Configuring a Secure OSINT Environment
- Using Virtual Machines (Kali Linux, Tails, Whonix)
- Privacy and Anonymity Tools (VPNs, Tor, ProxyChains)
- Essential OSINT Browser Extensions and Plugins

03

Search Engine OSINT & Advanced Google Dorking

TOPICS

- Effective Search Engine Techniques (Google, Bing, Yandex, DuckDuckGo)
- Google Hacking Database (GHDB) for Advanced Queries
- Extracting Data from Cached and Archived Pages (Wayback Machine)
- Searching Hidden and Non-Indexed Content

04

Social Media Intelligence (SOCMINT)

TOPICS

- Investigating Social Media Platforms (Facebook, Twitter, LinkedIn, Instagram)
- Extracting Metadata from Posts and Profiles
- Automated Social Media Data Collection
- Analyzing Social Connections and Network Mapping

05

Email and Username OSINT

TOPICS

- Investigating Email Addresses
- Tracing Username Footprints Across Platforms
- Email Header Analysis for Source Tracking
- Identifying Fake or Disposable Email Addresses

06

Website & Domain Intelligence

TOPICS

- WHOIS Lookups and DNS Reconnaissance
- Investigating Subdomains and Server Infrastructure
- Web Technology Fingerprinting (Wappalyzer, WhatWeb)
- Monitoring Website Changes and Leaks (Wayback Machine, Visualping)

07

Dark Web and Deep Web OSINT

TOPICS

- Understanding the Dark Web and Deep Web
- Accessing .onion Sites Securely Using Tor
- Investigating Dark Web Marketplaces and Forums
- Dark Web Search Engines and Information Gathering

08

Geolocation and Image OSINT

TOPICS

- Reverse Image Search Techniques
- Extracting Metadata from Images
- Geolocation Using OpenStreetMap, Google Earth, and Sentinel Hub
- Satellite and Aerial Imagery for OSINT Investigations

09

Video and Audio Analysis in OSINT

TOPICS

- Extracting Metadata from Videos and Audio Files
- Reverse Searching Video Frames
- Identifying Background Noises and Locations from Audio Sources
- Fact-Checking and Verifying Multimedia Content

10

People and Identity Investigations

TOPICS

- Investigating Public Records and Data Breaches
- Tracking Online Identities and Digital Footprints
- Analyzing Behavioral Patterns and Social Engineering Risks
- Gathering Intelligence on Threat Actors

11

OSINT for Cyber Threat Intelligence (CTI)

TOPICS

- Identifying Cyber Threat Actors and Groups
- Monitoring Data Breaches and Leaks
- Investigating Malware and Cybercrime Activities (VirusTotal)
- OSINT for Incident Response and Threat Hunting

12

Reporting and Operational Security (OPSEC) in OSINT

TOPICS

Organizing and Documenting OSINT Findings · Creating Actionable OSINT Reports · Ensuring Investigator Anonymity and OPSEC · Automating OSINT Collection

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com