SORINTEQ

ADVANCED OPEN SOURCE INTELLIGENCE (OSINT) & INTERNET INTELLIGENCE INVESTIGATION (I3)

Specialist training for Government and commercial sectors

- 7 Day Programme
- Specialist Training for Law Enforcement
- All Training Equipment Provided
- In Association With the University of Buckingham

Contact Us

0333 0063248

Sorinteq Academy

SORINTEQ

Course Overview

Internet Intelligence & Investigation (I3) enables professionals to harvest a rich source of accurate and timely data left by individuals, organisations, and threat actors within the digitally connected world. This is the third course in Sorinteq's I3 suite of OSINT training and is designed to take learners to an Advanced level of capability.

The fusion of advanced OSINT with conventional investigative methods provides organisations with a powerful tool for intelligence gathering, due diligence, corporate investigations, fraud enquiries, threat monitoring, and strategic decision-making.

The Advanced Open Source Intelligence Course is designed for experienced and technically competent professionals who are already operationally active in investigative or intelligence-gathering roles and who require higher-level technical capability to deal with increasingly sophisticated online subjects and complex digital environments.

This course builds on the skills taught in our Intermediate I3 Programme and develops enhanced technical capability, particularly in the use of code-based tools, APIs, advanced digital tradecraft, and analytical techniques that significantly improve the effectiveness of internet-based investigations.

The programme is delivered as a 7-day blended course, consisting of:

- 2 Days Virtual Pre-Course Learning
- 5 Days Classroom-Based Practical Delivery

This structure allows learners to complete foundation preparation remotely before progressing into intensive operational classroom delivery.

Who is the course for?

This course is designed for experienced professionals working in investigative, intelligence, and due diligence roles across the commercial sector, including:

- Corporate investigators
- Fraud and financial crime teams
- Due diligence and compliance professionals
- Corporate intelligence analysts
- Cyber security and cyber threat teams
- Corporate security and protective intelligence teams
- Risk and reputational threat management professionals
- Investigators supporting litigation, insider risk, and strategic intelligence functions

Participants should already have strong OSINT experience or have completed Sorinteq's Intermediate I3 Course.

This programme is intended for technically confident practitioners who want to move beyond standard investigative approaches and operate at a significantly higher capability level.

SORINTEQ

Course Content

Phase One – Pre-Course Remote Learning (2 Days Virtual)
Learners complete structured remote preparation before attending the classroom phase.
Including:

API Fundamentals and Data Handling
- Understanding APIs and data extraction opportunities
- Authentication and access considerations
- Data structure and handling principles

Introduction to Web Scraping
- Collection opportunities from public online sources
- Data extraction methodologies
- Practical preparation for large-scale research

OSINT Operational Security Fundamentals
- Digital footprint management
- Secure research environments
- Protecting investigators and organisations from exposure

Phase Two – Classroom Delivery (5 Days)
Practical, advanced operational training delivered in either virtual or physical classroom format.
Including:

API Overview and Usage
- Practical application of APIs in investigations
- Data enrichment and automation opportunities

Pattern Detection in LLMs
- Identifying structured behaviours and anomalies
- Understanding AI-generated content environments

Visualisation of Complex Networks
- Mapping relationships between people, organisations, infrastructure, and events

Identifying Disinformation and BOT Activity
- Coordinated behaviour detection
- Online manipulation and influence operations

Forensic Linguistic Considerations in OSINT
- Authorship analysis
- Is the same actor operating multiple accounts?
- Language-based attribution opportunities

Advanced Personal Security Measures
- Protecting operational staff and organisational identity

Detection of Adversary Counter-OSINT Activity
- Recognising deception, monitoring, and anti-investigative behaviour

AI in OSINT Support – Good and Bad
- Practical use of AI in investigations
- Risks, validation, and evidential defensibility

Intelligence Recovery from Secure Communication Platforms
- Understanding investigative opportunities within hardened communications environments

SORINTEQ

Final Exercise Phase
Interactive Live Capture The Flag (CTF) Investigation
Learners apply all skills taught during the programme within a realistic live investigative scenario.
Including:

- Full operational investigation using Sorinteq's virtual platform
- Real-world intelligence collection and analysis
- Multi-source attribution and technical investigation
- Decision-making under operational pressure
- Final structured debrief and performance review

All elements taught throughout the course will be tested within a realistic commercial investigative environment.

Aims and Objectives of the Course

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

- Use advanced command-line techniques to support OSINT investigations
- Utilise APIs to develop and enhance research capabilities
- Conduct effective and scalable web scraping for intelligence collection
- Apply advanced Digital Operational Security (OpSec) principles
- Build comprehensive Digital Fingerprints of targets and organisations
- Conduct infrastructure mapping and technical relationship analysis
- Identify patterns and anomalies within Large Language Model (LLM) data environments
- Visualise complex digital networks and investigative relationships
- Identify disinformation campaigns, coordinated inauthentic behaviour, and BOT activity
- Apply forensic linguistic thinking to authorship analysis and attribution
- Understand how Artificial Intelligence can enhance investigative capability
- Identify intelligence and evidential opportunities from secure communication platforms and hardened environments

Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations worldwide.
Our Advanced OSINT programmes are designed for professionals who need more than basic internet research—they need advanced capability that creates real operational value.
This course provides learners with the technical confidence, investigative tradecraft, and strategic awareness required to operate effectively against sophisticated digital targets and complex organisational challenges.
For further enquiries please email info@sorinteq.com or call Sorinteq on +44 (0)333 0063248.
Sorinteq provide all necessary training equipment including laptop computers, internet connectivity, mobile devices and training material.