CONCEPT

Open Source Intelligence (OSINT) for Corporate Investigations and Due Diligence

Open Source Intelligence (OSINT) for Corporate Investigations and Due Diligence

Introduction:

Open source intelligence OSINT now informs counterparty vetting, fraud inquiries and threat assessments, yet much of it is gathered through unplanned searching, captured as screenshots without provenance and reported with no grading of how reliable each source is. The result is findings that cannot be repeated, defended or safely shared. This Core Concept course builds a disciplined OSINT method for corporate investigations and due diligence, from collection requirements and lawful boundaries to verification, researcher security and reporting. Participants work on realistic case files and leave with an OSINT Collection Plan and Intelligence Report Pack.

Course Objectives:

- Translate an investigation or due diligence question into collection requirements, a lawful basis and a scoped OSINT research plan
- Apply the principles of the Berkeley Protocol to the collection, preservation and verification of publicly available online information
- Trace company ownership, directors and corporate history through public registries, filings, court records and media archives
- Examine domains, websites and hosting records at a defensive level to attribute online assets to the organisations behind them
- Verify images, videos and claimed locations and grade every source for reliability before findings are relied upon
- Produce an OSINT Collection Plan and Intelligence Report Pack that another investigator can review and repeat

Target Audience:

- Corporate investigators who handle fraud, misconduct and integrity inquiries using public information
- Due diligence analysts who vet counterparties, suppliers, partners and acquisition targets
- Compliance and risk staff who screen third parties for adverse media and reputational exposure
- Security and threat intelligence analysts who monitor threats to the organisation, its brand and its assets
- Internal audit and fraud examination staff who gather background information during reviews

Course Outline:

Day 1: OSINT Foundations and the Intelligence Cycle

- Intelligence Cycle Stages: Direction, Collection, Processing, Analysis and Dissemination
- Open Source Categories: Media, Government Data, Grey Literature and Commercial Datasets
- OSINT Use Cases in Fraud, Integrity Vetting and Threat Assessment
- Lawful Basis, Privacy Impact and Proportionality Screening Checklist
- OSINT Maturity Self-Assessment of Current Research Practice

Day 2: Professional Standards and Collection Planning

- Berkeley Protocol Professional, Methodological and Ethical Principles
- Berkeley Protocol Investigation Phases: Online Inquiry to Investigative Analysis
- Collection Requirements Matrix and Priority Intelligence Questions
- Research Scope Boundaries: Public Data, Access Controls and Terms of Service
- OSINT Research Plan Template with Keywords, Sources and Stop Criteria

Day 3: Search, Corporate Records and Online Infrastructure

- Advanced Search Operators, Web Archives and Cached Page Retrieval
- Company Registry, Filings and Beneficial Ownership Record Tracing
- Court Records, Sanctions Lists and Adverse Media Screening Workflow
- WHOIS, DNS and Certificate Transparency Lookups for Domain Attribution
- Social Media Research on Organisational Accounts and Public Posts

Day 4: Verification, Disinformation and Researcher Security

- Reverse Image Search, Metadata Review and Image Provenance Checks
- Geolocation and Chronolocation of Images and Video
- Detecting Manipulated Media, AI-Generated Content and Coordinated Disinformation
- Source Reliability and Information Credibility Grading Matrix
- Researcher Operational Security: Attribution Risk, Isolated Browsing and Wellbeing

Day 5: Case Files and the Intelligence Report Pack

- Evidence Capture Log: Hashing, Timestamps and Web Page Preservation
- Supplier Due Diligence Case Study: Hidden Ownership and Red Flags
- Brand Impersonation Case Study: Lookalike Domains and Fraudulent Pages
- OSINT Collection Plan and Intelligence Report Pack Drafting
- Peer Review Panel and Findings Defence

Skills You Will Gain:

- Collection Requirements Planning
- Corporate Ownership Tracing
- Domain Attribution Analysis
- Image and Location Verification
- Source Reliability Grading
- Researcher Operational Security
- Online Evidence Preservation
- Intelligence Report Writing

Why Attend This Course:

- Return with an OSINT Collection Plan and Intelligence Report Pack tested on supplier vetting and brand impersonation cases
- Answer due diligence questions faster by knowing which public records hold ownership, litigation and adverse media data
- Present findings that reviewers, lawyers and decision makers can trace back to a preserved and graded source
- Compare research practice with investigators and analysts from finance, energy, telecoms and public service

Conclusion:

Public information is only useful to an organisation when it is collected with purpose, gathered lawfully and verified before anyone acts on it. This course moves from the intelligence cycle and legal boundaries, through collection planning and the Berkeley Protocol, to search, corporate records, domain research, verification and researcher security. The final day applies that method to realistic case files and produces an OSINT Collection Plan and Intelligence Report Pack that participants use to run their next inquiry to a repeatable and defensible standard.