JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Open Source Intelligence (OSINT) Investigations Course

12 – 23 September 2027
Kuala Lumpur

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Open Source Intelligence (OSINT) Investigations Course

Ref: 499_18418 **Date:** 12 – 23 September 2027 **Location:** Kuala Lumpur **Fees:** 8000 GBP

Open Source Intelligence OSINT Investigations is an advanced 2-week training course for security analysts, investigators and corporate intelligence officers who turn publicly available information into verified findings, ending with an Open Source Threat Assessment. Protest movements, fraud networks and hostile actors now leave traces across social platforms, imagery and public records, and decision makers expect evidence rather than rumour. Jupiter Prime Training offers this course to practitioners who already research subjects online.

Why Open Source Intelligence OSINT Investigations Matters Now

Three pressures shape open source investigations today: the sheer volume of social media, imagery and registry data that must be filtered quickly, manipulated and synthetic content that can mislead an unwary analyst, and executives, legal advisers and security managers who need findings they can defend. An organisation that runs OSINT well spots threats to sites, staff and events early and screens partners with confidence, while one that runs it badly acts on false leads or breaches privacy expectations. The course is structured around the intelligence cycle of direction, collection, processing, analysis and dissemination, with structured analytic techniques for judgement.

Who Gains Most from Open Source Intelligence OSINT Investigations

- Security analysts who monitor threats to sites, executives and events
- Investigators who research individuals, companies and networks behind incidents
- Corporate intelligence officers who brief leaders on emerging risks
- Due diligence specialists who screen partners, suppliers and acquisitions
- Protective security planners who need early warning before travel or events

A corporate security function that sends its analysts, investigators and due diligence specialists together gains most, because they can agree one collection discipline, one verification standard and one reporting format across every inquiry.

Open Source Intelligence OSINT Investigations Capabilities

Participants move from ad hoc searching to disciplined collection, verification and reasoned judgement that stands up when challenged.

- Design collection plans from intelligence requirements set by decision makers — security leaders prioritising questions
- Apply advanced search operators, archives and public records to locate relevant material — investigators building case files
- Test the authenticity of images, video and accounts through geolocation and metadata checks — analysts rejecting manipulated content
- Assess source reliability and information credibility before drawing conclusions — legal and compliance advisers
- Specify safe research environments and attribution management — protecting investigators and the organisation
- Communicate findings with confidence levels in concise intelligence products — executives deciding on protective action

Key Open Source Intelligence OSINT Investigations Terms

- Open source intelligence OSINT — intelligence produced from publicly available information that is collected, verified and analysed to answer a specific question.
- Intelligence cycle — the repeating sequence of direction, collection, processing, analysis and dissemination that turns questions into usable intelligence.
- Geolocation — confirming where an image or video was captured by matching visible features to maps, satellite imagery and street-level views.
- Source reliability grading — a rating of how dependable a source has proved, kept separate from how credible a single item appears.
- Attribution management — measures that stop investigated subjects from identifying who is researching them or why.
- Intelligence requirement — a clearly stated question from a decision maker that directs what collection and analysis must answer.

Open Source Intelligence OSINT Investigations Day by Day

Day 1: The OSINT Landscape

- Intelligence Cycle Stages — Linking Collection to Decision Needs
- Intelligence Requirements Writing — Turning Concerns Into Answerable Questions
- OSINT Versus Cyber Threat Intelligence — Defining the Investigative Scope
- Information Environment Mapping — Locating Where Relevant Traces Appear
- Legal and Ethical Boundaries — Respecting Privacy and Platform Terms

Day 2: Safe Research Environments

- Attribution Management Methods — Protecting Investigator Identity
- Research Personas and Their Limits — Weighing Access Against Risk
- Isolated Browsing Environments — Separating Casework From Personal Use
- Evidence Capture and Hashing — Preserving Pages Before They Change
- Case Logging Standards — Recording Every Search and Source

Day 3: Advanced Search and Archives

- Search Operators and Query Building — Narrowing Results Precisely
- Web Archives and Cached Pages — Recovering Deleted Material
- Public Records and Corporate Registries — Tracing Ownership and Directors
- Document Metadata Extraction — Revealing Authors, Dates and Tools
- Multilingual Searching — Reaching Sources Beyond One Language

Day 4: Social Media Intelligence

- Account and Network Mapping — Revealing Links Between Profiles
- Hashtag and Keyword Monitoring — Tracking Mobilisation Around Sites and Events
- Sock Puppet and Bot Indicators — Spotting Coordinated Inauthentic Activity
- Timeline Reconstruction From Posts — Ordering Events Accurately
- Platform Data Limits — Judging What Each Network Reveals

Day 5: Imagery and Geolocation

- Visual Clue Extraction — Reading Signs, Terrain and Architecture
- Satellite and Street-Level Imagery Comparison — Confirming Locations
- Chronolocation Using Shadows and Weather — Estimating When Images Were Taken
- Reverse Image Searching — Finding Earlier Copies and Origins
- Video Frame Analysis — Verifying Footage of Incidents

Day 6: Verification and Disinformation

- Source Reliability and Credibility Grading — Separating Source From Claim
- Manipulated and Synthetic Media Indicators — Detecting Altered Content
- Cross-Corroboration Methods — Requiring Independent Confirmation
- Disinformation Campaign Patterns — Recognising Coordinated Narratives
- Verification Logs — Recording How Each Fact Was Confirmed

Day 7: Investigating People and Organisations

- Subject Profiling Workflows — Building Lawful Background Pictures
- Due Diligence Research on Partners — Screening Suppliers and Agents
- Network and Link Charting — Visualising Relationships Between Entities
- Adverse Media Screening — Finding Reputational Red Flags
- Physical Footprint Mapping — Linking Organisations to Sites and Assets

Day 8: Threat Monitoring for Security

- Threat Indicator Libraries — Defining What Triggers Escalation
- Event and Travel Security Monitoring — Watching Locations Before Visits
- Protest and Unrest Tracking — Anticipating Disruption at Facilities
- Executive Exposure Reviews — Reducing Personal Information Online
- Alert Thresholds and Escalation Routes — Getting Warnings to Responders

Day 9: Analysis and Intelligence Reporting

- Structured Analytic Techniques — Testing Competing Hypotheses
- Estimative Language and Confidence Levels — Expressing Uncertainty Clearly
- Intelligence Product Formats — Choosing Briefs, Alerts and Assessments
- Visualisation of Findings — Using Maps, Timelines and Link Charts
- Dissemination and Handling Rules — Protecting Sensitive Sources

Day 10: Practising the Open Source Threat Assessment

- Applying Intelligence Requirements — Scoping a Live Security Question
- Applying Collection and Search Methods — Gathering Relevant Material
- Applying Verification and Geolocation — Confirming Key Facts
- Applying Structured Analysis — Weighing Hypotheses and Confidence
- Open Source Threat Assessment — Presenting Findings, Confidence and Recommendations

Applying Open Source Intelligence OSINT Investigations After the Course

- Lead an open source exposure review of senior executives, recording personal information that raises risk and agreeing removal or mitigation steps.
- Run a collection and verification exercise on a planned event or site, producing a short alert product with confidence levels for the security manager.

Open Source Intelligence OSINT Investigations Questions FAQ

What is open source intelligence OSINT investigations and why does it matter now?

Open source intelligence OSINT investigations turn publicly available information into verified findings about threats, people and organisations. It matters now because relevant traces are abundant online but mixed with manipulated content that misleads careless analysts.

Which roles gain most from open source intelligence OSINT investigations training?

Security analysts, investigators and corporate intelligence officers gain most from open source intelligence OSINT investigations training, along with due diligence specialists.

How does open source intelligence OSINT investigations differ from a cyber threat intelligence course?

Open source intelligence OSINT investigations focuses on people, organisations, sites and events using public information. A cyber threat intelligence course focuses on malware, network indicators and attacker infrastructure targeting digital systems.

What do you bring back from open source intelligence OSINT investigations training?

You bring back an Open Source Threat Assessment on a real security question. It records requirements, verified findings, confidence levels and recommended protective actions.

Open Source Intelligence OSINT Investigations: The Way Forward

The Open Source Threat Assessment first informs whether a site, event or executive needs added protective measures. Security managers, investigators and protective planners use it to align monitoring and response. After its first use, revisit the collection plan against what proved reliable, whether for an energy facility or a large public event, so future inquiries spend effort where verification succeeds.