
Online Investigation Capability: OSINT Collection, Verification and Reporting Training Course

15 – 19 August 2027
Kuala Lumpur





Online Investigation Capability: OSINT Collection, Verification and Reporting Training Course

Ref: 355_22539 Date: 15 – 19 August 2027 Location: Kuala Lumpur Fees: 4000 GBP

Programme Summary

Online investigation capability, covering OSINT collection, verification and reporting, is the subject of this five-day training course for heads of security, investigations and risk intelligence teams at a managerial level, ending in a capability plan for one team. Open source information grows daily, yet teams often collect without a plan, verify unevenly and report without stating confidence. The programme moves from standards and legal limits, through diagnosis of sources and risk, to collection, verification and reporting design, then to a worked plan. Mars Training Centre UK delivers this programme in online investigation capability.

The Business Case

When open source research is run by individuals with no shared method, findings cannot be repeated, evidence is lost and decisions rest on unchecked material. Leaders who set requirements, grade sources and review reports can show how conclusions were reached and protect their investigators.

- Decision Reliability: Improves as sources are graded and findings carry a stated confidence.
- Evidence Loss: Falls as capture and preservation follow one protocol.
- Investigator Exposure: Reduces as safety and legal limits are written into every task.

Principles and Evidence Base

- Berkeley Protocol on Digital Open Source Investigations: Created with the UN Office of the High Commissioner for Human Rights, its international standards for online research frame Sessions 1 to 3.
- Professional, legal and ethical practice: The Protocol's guidance on gathering, analysing and preserving digital information shapes the collection and preservation work in Session 3.
- Investigator safety: The Protocol's measures to protect digital, physical and psychosocial safety inform the safety plan in Session 1.

Intended Participants

- Security heads who commission open source research for threat and incident questions.
- Investigations leaders who rely on online material in cases and reports.
- Risk intelligence managers who run research teams and set quality standards.
- Legal and compliance leads who judge the limits of online collection.

The programme serves corporate security, financial institutions, public agencies and media-facing organisations.



Learning Outcomes

1. Participants will be able to evaluate an organisation's online research practice against recognised international standards for digital open source investigations.
2. Participants will be able to diagnose weaknesses in source selection, reliability and manipulation risk.
3. Participants will be able to construct a collection plan with verification and preservation steps.
4. Participants will be able to appraise open source reports for evidence, confidence and clarity.
5. Participants will be able to design safety, data protection and quality review rules for a research team.
6. Participants will be able to justify a capability plan and its indicators to a head of security.

Programme Structure

Day 1: Online Investigation Principles and Legal Limits

What may an organisation investigate online, and under which standards and limits?

- Berkeley Protocol Standards Review
- OSINT Capability and Role Map
- Legal and Ethical Boundary Statement
- Investigator Safety and Digital Hygiene Plan
- Research Question and Requirement Brief

Day 2: Diagnosing Sources, Platforms and Information Risk

Where is open source information reliable, and where does it mislead?

- Source Landscape Survey
- Platform and Data Type Inventory
- Source Reliability Grading Grid
- Manipulation and Disinformation Risk Check
- Current Research Workflow Audit

Day 3: Designing Collection and Verification

How is open source material collected, checked and preserved so that others can rely on it?

- Collection Plan Template
- Content Verification Checklist
- Image and Location Check Sheet
- Capture and Preservation Protocol
- Provenance and Custody Log



Day 4: Analysis, Reporting and Governance

How does collected material become a report that a decision-maker can use and defend?

- Link and Timeline Analysis Chart
- Confidence and Caveat Statement
- Open Source Report Template
- Quality Review Cycle
- Data Protection and Retention Rule Sheet

Day 5: Applying Online Investigation Capability in One Team

Is the capability plan ready for a head of security to adopt?

- Applying the Session 2 Source Audit to the Chosen Team
- Testing the Session 3 Collection Plan on a Live Question
- Checking the Session 4 Report Against Quality Review
- Setting Capability Indicators for the Team
- Completing the Online Investigation Capability Plan

Methodology

The programme is built around structured exercises on anonymised research tasks from corporate security, financial crime and public safety settings. Participants work in small teams as a research lead, a verifier and a client, and move one question from requirement to report.

- Suggested activity: Grading a set of public sources for reliability and recording the reasons.
- Suggested activity: Verifying one claim by tracing its origin and recording each step.
- Suggested activity: Rewriting a finding so that its confidence and limits are clear.

Capstone Output

Each participant completes an online investigation capability plan for one team. It holds a requirement brief, a source grading approach, a collection and verification protocol, a report standard, safety and data rules and capability indicators. The plan is used to brief a head of security and to set up the team's next tasks.

Frequently Asked Questions

Is online investigation capability suitable for leaders who do not run searches themselves?

Yes. Online investigation capability is set at managerial level and assumes you commission and use research, not that you operate collection tools yourself.



Which standards does online investigation capability rest on in this training?

Online investigation capability rests on the Berkeley Protocol on Digital Open Source Investigations and its guidance on professional, legal and ethical practice and investigator safety.

How is the plan from online investigation capability used at work?

You use the online investigation capability plan to brief a head of security, set collection and verification rules and review the quality of reports.

How does online investigation capability differ from a programme on cyber threat intelligence?

Online investigation capability centres on collecting and verifying public information for investigations, while a cyber threat intelligence programme centres on adversaries and attacks on networks.