MANDIANT

DATASHEET

INTELLIGENCE RESEARCH II

Open source intelligence (OSINT) tools and techniques

HIGHLIGHTS

Learners completing this course will be able to:

- Configure systems to ensure good operational security (OPSEC) and safety while researching
- Keep detailed case notes and avoid getting lost in their research
- Think critically about when and why to use a particular tool within the context of their research task
- Navigate basic functionalities of several common OSINT tools
- Identify investigation pivot points and artifacts, and how to leverage these to drive their investigations forward

This foundational course shows learners how to identify and develop investigation leads across multiple use cases.

The course helps learners understand the best times and ways to use an open source tool in research and reviews the basic functionalities of such tools. It encourages critical thinking to help learners push research further across several scenarios drawn from frontline experience, including executive-level RFIs, incident response investigations and information operation campaigns.

Lab scenarios require knowledge of tools such as VirusTotal, Alienvault, PassiveTotal and Facebook, and use advanced search engine techniques.

Users who complete this course are eligible to receive up to 16 CPE credits.

Prerequisites. Cyber Intelligence Foundations and Intelligence Research I: Scoping or equivalent knowledge.

Who should attend. This is a foundational level course for cyber practitioners who must safely and efficiently conduct research as part of investigations or in response to RFIs.

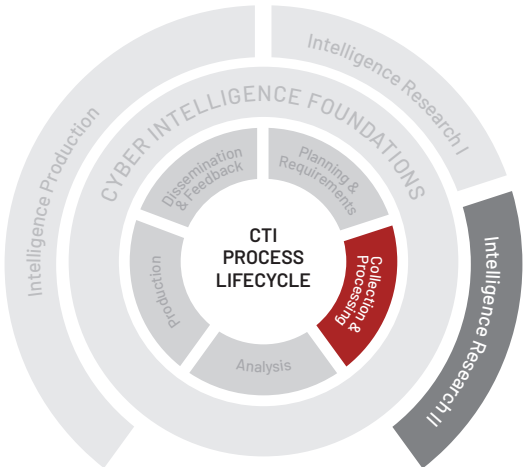

FIGURE 1. Intelligence Research II supports the Collection & Processing phase of the Intelligence Lifecycle.

TABLE 1. Course includes four modules.

Module	Topics
OSINT Overview	Definitions, values/dangers, critical thinking framework (scope, identify/harvest, normalize, enrich, synthesize, report), OODA loop
Getting your Systems Started	OPSEC, PC configuration, toolbars and add-ons, mindmaps, case notes, virtual machines
Tools and Techniques	Virustotal, search engines (Google Dorking, Hacking Database, reverse image search, Censys, Fofa, Dogpile, archives, Shodan), PassiveTotal, DomainTools, social media (APIs, Facebook, Twitter, sock puppets), government documents, deleted data (Wayback Machine, cached pages, screenshots.com), image and video metadata, usernames and aliases (checkuser.org, namechk.com);
Capstone	Conduct research relevant for a scenario tied to potential Triton activity

*Lists are not comprehensive.

TABLE 2. Course accessible in instructor-led (onsite or remote) or on-demand formats.

Instructor-Led	On-Demand
Onsite **Duration:** 2 days (8 hours/day). **Location:** At client-site OR location provided by Mandiant. **Format:** Instructor-facilitated lecture and discussion, hands-on activities emphasizing problem solving and critical thinking. **Technology Requirements:** Computer with reliable internet connection and standard web browser.	**Duration:** 16 hours (typical). Includes a single two-hour instructor-led lab. **Location:** 24x7 online availability for three months from first access. Purchase via mandiant.com and access via training.mandiant.com. Lab enrollment is on a first-come-first-served basis via Mandiant website. **Format:** Materials include videos led by subject matter experts, written materials and multiple choice assessments. **Technology Requirements:** Computer with reliable internet connection and standard web browser.
Remote **Duration:** 4 days (4 hours/day). **Location:** Remote. **Format:** Instructor-facilitated lecture and discussion; hands-on activities emphasizing problem solving and critical thinking. **Technology Requirements:** Computer with reliable internet connection and standard web browser.	

Learn more at **www.mandiant.com/intelligence**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT