MANDIANT

DATASHEET

INTELLIGENCE RESEARCH I

Scoping

HIGHLIGHTS

Learners completing this course will be able to:

- Use a structured, repeatable four-step scoping process
- Generate context using various approaches and resources such as the organizational threat profile, key stakeholder analysis and intelligence requirements
- Prepare for collections efforts by developing a research management system
- Assess different kinds of information and sources up front to avoid wasting time on irrelevant or unreliable sources

This one-day foundational course shows learners how to analyze, prioritize and interpret requests for information (RFIs) and create a research plan.

The course provides learners with questioning strategies to uncover stakeholder intent and generate actionable intelligence analysis. It shows learners how to identify and review relevant context such as intelligence requirements, organizational threat profiles and key stakeholder analysis to help them fully interpret implicit and explicit RFIs.

The course walks learners through how to use a research management system to organize research and avoid information overload, and how to assess source relevance and trust to ensure that collections efforts are efficient and focused on the task at hand.

Users who complete this course are eligible to receive up to 8 CPE credits.

Prerequisites. Cyber Intelligence Foundations or equivalent knowledge.

Who should attend. This is a foundational level course for cyber practitioners who must scope and respond to formal and informal requests for information (RFIs).

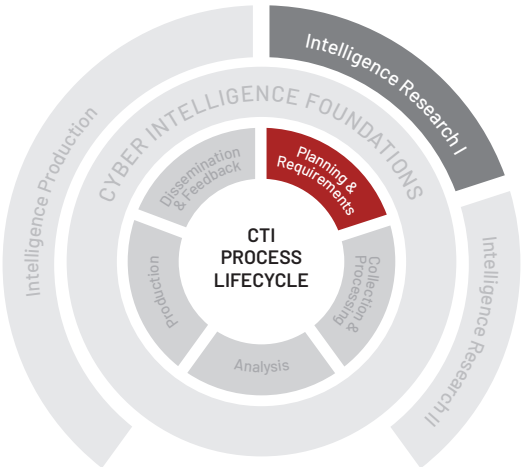

FIGURE 1. Intelligence Research I supports the Planning & Requirements phase of the Intelligence Lifecycle.

TABLE 1. Course includes three modules.

Module	Topics
Organizing Research	Research goals and objectives, research considerations, explicit and Implicit prompts, essential elements of information; four-step research process (prompt, plan, gather, evaluate), intelligence requirements, threat profile, key stakeholder analysis, context, priority
Assessing Information	Interrogating existing holdings, intelligence gaps, knowledge management practices, working knowledge of environment, source types, source characteristics, stakeholder and influence mapping, relevance, trust, Admiralty Code (reliability and credibility), source bias, facts versus opinion versus assessment, estimative language, cognitive bias
Capstone	Outline a research response for a scenario tied to 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:** 1 day (8 hours). **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:** None.	**Duration:** 8 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:** 2 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