MANDIANT

DATASHEET

CYBER INTELLIGENCE FOUNDATIONS

Your doorway to the field of cyber intelligence

HIGHLIGHTS

Learners completing this course will be able to:

- Define cyber intelligence and articulate the roles, impacts and value of a CTI function
- Recognize how intelligence analysts convert raw threat data derived from technical artifacts into actionable intelligence
- Interpret and assess intelligence reporting claims of attribution
- Explain the concepts and interactions between cyber key terrain, cyber security intelligence, quality assessments, indicators of compromise and threat modeling
- Use frameworks such as MITRE, the Intelligence Lifecycle and the Diamond Model in analysis

This three-day foundational course provides learners with a wide-ranging introduction to cyber intelligence roles, frameworks, tradecraft and organizational value.

The course shows learners how intelligence can drive value across many different use cases in different ways. It gives learners a high-level programmatic overview of intelligence, including team composition, the organizational role of cyber threat intelligence (CTI) and stakeholder analysis.

Learners will explore basic practitioner skills such as developing raw data into minimally viable intelligence, interpreting cyber artifacts, and leveraging the intelligence cycle to compose original intelligence products. Basic attribution techniques are introduced.

Concepts introduced in Cyber Intelligence Foundations are reinforced and explored in depth during subsequent intelligence training courses. Users who complete this course are eligible to receive up to 40 CPE credits.

Prerequisites. None

Who should attend. This is a foundational level course for practitioners, consumers or anyone else looking to get started with cyber intelligence.

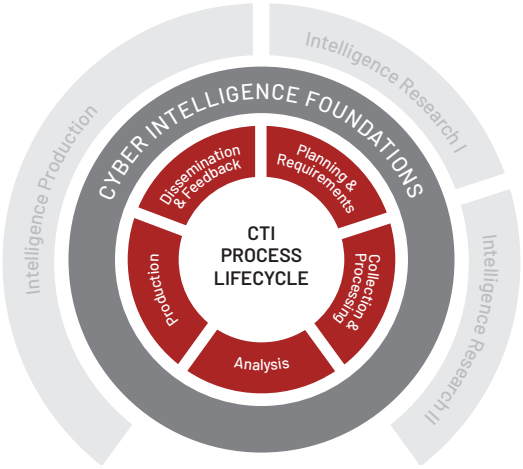

FIGURE 1. Cyber Intelligence Foundations supports all phases of the Intelligence Lifecycle.

TABLE 1. Course includes seven modules.

Module	Topics*
Introduction to Cyber Threat Intelligence	Definition of cyber threat intelligence, different collaborative roles (SOC, NOC, VAT, IR and others), levels of intelligence, threat modeling
The Analyst's Toolkit	Dual Process Theory (intuitive, analytic), Wason selection task, ambiguity effect, types of bias (such as confirmation and conservatism), groupthink, failure to consider visibility, source reliability/fidelity, failure to account for human action, estimative language
Cyber Artifacts	Cyber key terrain, file-based, network-based, host-based, binary, backdoor, botnet, downloader, dropper, ransomware, infostealer, rootkit, worm, compile, file hash, strings, packer, obfuscation, compression, IOCs in modeling
Developing Raw Data into Minimally Viable Intelligence	Development of source data, threat documentation, colors (blue, red, green, yellow), ANB charts, Common Operating Picture (COP), Analyst's Notebook, Maltego, SharePoint, MediaWiki, Anchor Node, FQDN, Pyramid of Pain
How Intelligence Teams Work with Malware	Production systems, AirDrop, USB, SecureFile, static analysis, dynamic analysis, hashing, strings, sandboxing
Writing Intelligence Products	Technical writing, knowing your audience, critical thinking for establishing audience, review procedures, BLUF, AIMS
Establishing Attribution	Basic modeling techniques, levels of attribution, natural language, nodes and edges, graph database

*Lists are not comprehensive.

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

Instructor-Led	On-Demand
Onsite **Duration:** 3 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:** None.	**Duration:** 40 hours (typical). Includes a single two-hour teacher-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 (6 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