Publication date : 02/13/2025

# Course : CTI (Cyber Threat Intelligence), level 1

*Practical course - 3d - 21h00 - Ref. CYI*
*Price : 2210 € E.T.*

★★★★⯪ 4,6 / 5

NEW

This hands-on training course provides cybersecurity professionals with a comprehensive introduction to the fundamentals of threat intelligence. It covers key concepts, threat collection and analysis methodologies, and the use of appropriate tools.

## Teaching objectives

**At the end of the training, the participant will be able to:**

- ✓ Understand the fundamental concepts of Cyber Threat Intelligence and its role in cybersecurity
- ✓ Identify intelligence sources and master threat collection techniques
- ✓ Use threat intelligence tools to better detect and prevent attacks

## Intended audience

Security managers and architects. System and network technicians and administrators, auditors and pentesters.

## Prerequisites

Good knowledge of TCP/IP and corporate network security. Or knowledge equivalent to that provided by the course "System and network security, level 1" (ref. FRW).

## Practical details

**Hands-on work**

A wide range of tools will be deployed by participants.

## Course schedule

### PARTICIPANTS

Security managers and architects. System and network technicians and administrators, auditors and pentesters.

### PREREQUISITES

Good knowledge of TCP/IP and corporate network security. Or knowledge equivalent to that provided by the course "System and network security, level 1" (ref. FRW).

### TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

### ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.

Participants also complete a placement test before and after the course to measure the skills they’ve developed.

### 1 OSINT and CTI

- Open Source and Investigation Principle (OSINT).
- Types of sources: media, social networks, online databases, etc.
- Investigative ethics: respect for privacy, human rights and legality.
- Introduction to the basics of CTI (Cyber Threat Intelligence).
- Nomenclature used in the CTI field.
- Techniques, tactics, procedures and current infrastructures (TTP, ATP, IOC...).
- APT (Advanced Persistent Threat) vs OPSEC (Operational Security).
- Use of tools such as OTX AlienVault, Kaspersky Threat Data Feeds, Shodan, etc.

### 2 CTI tools and techniques

- Threat collection and analysis tools (MISP, OpenCTI, VirusTotal, etc.).
- Methodology for investigating cyberthreats.
- Identification and analysis of indicators of compromise (IOCs).
- Attacker tactics, techniques and procedures (TTP) with MITRE.
- Threat detection and prevention through CTI.
- Use of MISP for IOC management.

### 3 MISP, OpenCTI

- MISP and its features.
- OpenCTI and its features.
- Platform configuration and familiarization.
- Threat management with MISP and OpenCTI.

### 4 Exploiting and communicating intelligence

- Transforming data into actionable intelligence.
- Information sharing and exchange (STIX/TAXII standards).
- Preparation of a CTI intelligence report.
- Responding to an attack using CTI.

**TEACHING AIDS AND TECHNICAL RESOURCES**

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.

• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.

• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

**TERMS AND DEADLINES**

Registration must be completed 24 hours before the start of the training.

**ACCESSIBILITY FOR PEOPLE WITH DISABILITIES**

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

## Dates and locations

**REMOTE CLASS**
2026 : 25 Mar., 17 June, 28 Sep., 14 Dec.

**PARIS LA DÉFENSE**
2026 : 18 Mar., 10 June, 21 Sep., 14 Dec.