Publication date : 02/13/2025

Course : CTI (Cyber Threat Intelligence), level 2

Practical course - 3d - 21h00 - Ref. CYJ
Price : 2460 € E.T.

NEW

This advanced training program in Cyber Threat Intelligence (CTI) aims to deepen the knowledge of cybersecurity professionals wishing to master advanced cyber threat analysis methodologies (techniques for collecting, correlating and exploiting threat intelligence).

Teaching objectives

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

- ✓ Analyze and correlate indicators of compromise (IOCs) and tactics, techniques and procedures (TTPs)
- ✓ Develop OpenCTI to optimize CTI workflows
- ✓ Use STIX and TAXII to represent threat information
- ✓ Master advanced techniques for collecting and evaluating cyberthreat intelligence

Intended audience

Security managers and architects. System and network technicians and administrators, CTI analysts, SOC experts, auditors and pentesters.

Prerequisites

Knowledge equivalent to that provided by the course "CTI (Cyber Threat Intelligence), level 1" (ref. CYI).

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, CTI analysts, SOC experts, auditors and pentesters.

PREREQUISITES

Knowledge equivalent to that provided by the course "CTI (Cyber Threat Intelligence), level 1" (ref. CYI).

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 CTI (Cyber Threat Intelligence)

- A reminder of the fundamentals of CTI.
- Cybersecurity intelligence models (Pyramid of Pain, Diamond Model, Cyber Kill Chain, ATT&CK Framework).
- Advanced analysis of an attack campaign.

2 Threat analysis and correlation

- In-depth cyber-threat analysis techniques.
- Advanced use of CTI tools (MISP, OpenCTI, Threat Intelligence Platforms).
- Investigation of an APT group.
- Methodology for correlating and contextualizing IOCs and TTPs.
- Development of usable threat indicators.

3 Exploiting and integrating intelligence into operations

- Integration of CTI intelligence into SOCs and CSIRTs.
- CTI intelligence automation and orchestration.
- Incident response based on CTI data.
- Communication strategies and information sharing (STIX/TAXII, ISACs).
- Crisis management and decision-making.

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 : 18 Mar., 10 June, 21 Sep., 14 Dec.

PARIS LA DÉFENSE
2026 : 11 Mar., 3 June, 14 Sep., 7 Dec.