Course : Cybersecurity, Adversary Emulation

emulate the opponent to simulate advanced attacks

Practical course - 2d - 14h00 - Ref. RTA

Price : 1630 CHF E.T.

NEW

Adversary emulation is a cybersecurity assessment method that replicates the tactics, techniques and procedures (TTPs) of real-world threat actors in order to assess and improve an organization's security defenses. This training will enable you to simulate real-world attacks, understand adversarial techniques, and test your detection and response capabilities in a controlled environment.

Teaching objectives

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

- Understanding the strategic benefits of adversary emulation
- Using Atomic Red Team in a MITRE ATT&CK approach
- Deploy a realistic scenario with Caldera and/or Atomic Red Team
- Interpreting results, detecting and reinforcing defensive posture

Intended audience

SOC analysts, blue teamers, pentesters, red teamers, security managers, security administrators.

Prerequisites

Good knowledge of IS security, networks and systems.

Course schedule

1 Adversary Emulation 101

- Definitions and key concepts.
- Emulation, simulation and pentesting: comparison and why emulate?
- Proactive defensive posture, aligned with real threats.

PARTICIPANTS

SOC analysts, blue teamers, pentesters, red teamers, security managers, security administrators.

PREREQUISITES

Good knowledge of IS security, networks and systems.

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.

2 Discover MITRE ATT&CK

- Introducing the MITRE ATT&CK and D3FEND matrices.
- Tools for emulating tactics, techniques and procedures (TTP).

Hands-on work
Identify the TTPs of an APT group.

3 Atomic Red Team

- Presentation of Atomic Red Team, Atomic CLI, Invoke-Atomic.
- How to use a test, adapt it, and create one.

Hands-on work
Simple TTP tests (e.g. exfiltration, persistence, recognition).

4 Creating an emulated attack mini-campaign with Atomic Red Team

- Build a mini-attack campaign.
- Run tests with Atomic CLI or Invoke-Atomic.
- Observation of logs and impacts on the target machine.

Hands-on work
Build an attack campaign and observe traces and impacts on the target machine.

5 Atomic Red Team TTP detection and correlation

- Which logs, which Sigma, YARA, or EDR detection rules?
- Implementation of collection, correlation and investigation tools to track down malicious activity.

Hands-on work
Detection of TTPs generated by Atomic RedTeam.

6 Caldera

- Opponent emulation platform: Caldera.
- Presentation and difference with ART: agents, automatic sequences.
- Demonstration and implementation of an automated scenario.

Hands-on work
Setting up agents and running a Caldera scenario.

7 AI and cybercriminals

- Use of AI by attackers (polymorphic scripts, GPT in the attack).
- Emerging threats (LLM poisoning, AI jailbreak, social engineering 2.0).
- Adapting adversary emulation to augmented threats.

8 Purple Team Challenge

- How to integrate Atomic Red Team into a security pipeline.
- Best practices for enriching SOC use cases.
- Resources, community projects, ready-to-use scenarios.

Hands-on work
Offensive/defensive simulation: one team attacks, the other detects, review of results, scoring based on MITRE.

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 : 19 Mar., 9 June, 24 Sep., 17 Dec.