Course : Red Team, Blue Team: understanding your teams' methods

A clear vision of offensive (Red Team) and defensive (Blue Team) methods

Synthesis course - 1d - 7h00 - Ref. RTB

Price : 630 CHF E.T.

NEW

This one-day training course provides IT managers and executives with a clear vision of offensive (Red Team) and defensive (Blue Team) methods. Through concrete demonstrations and case studies, you'll discover how your teams identify, conduct and counter attacks, so you can better manage your cybersecurity projects.

Teaching objectives

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

- Understanding the role of the Red Team and Blue Team in cybersecurity
- Acquire an overview of the methodologies and tools used by each team
- Learn how to communicate effectively with these teams and evaluate their performance
- Integrate Red Team and Blue Team practices into project management and IT risk management

Intended audience

Managers, IT managers, project managers, security managers, decision-makers who want to better understand the work of their technical teams.

Prerequisites

No special knowledge required.

Course schedule

PARTICIPANTS

Managers, IT managers, project managers, security managers, decision-makers who want to better understand the work of their technical teams.

PREREQUISITES

No special knowledge required.

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 Why Red Team and Blue Team?

- Security principles: defense in depth, cyber risk modeling.
- Risks associated with intrusion, attacks and system protection.
- Why two distinct teams? Red Teams (attack) and Blue Teams (defense).
- _1_ The role of the Red Team: understanding the attack :
- Introduction to penetration testing (pentests).
- Stages of attack: reconnaissance, exploitation, post-exploitation.
- Tools used by Red Teams (e.g. Kali Linux, Metasploit, nmap).
- Attack scenarios and Red Team objectives: network and system security assessment.
- _2_ The role of the Blue Team: understanding the defense :
- Introduction to intrusion detection, monitoring and incident management.
- Incident response stages: detection, analysis, containment, eradication.
- Tools used by Blue Teams (SIEM, firewalls, IDS/IPS systems).
- Blue Teams play a key role in crisis prevention and management.

2 Collaboration between Red Team and Blue Team: Simulation and confrontation

- How Red Team returns help improve Blue Team defenses and vice versa.
- The role of management in managing these interactions.

Demonstration

Examples of exercises in "Red Team vs Blue Team" (Purple Teaming).

3 Understanding methodologies and reports

- What do Red Teams look for in their reports (weaknesses, vulnerabilities exploited, test results)?
- How a Blue Team analyzes an incident and draws up a crisis management report.
- What do managers need to know from technical reports to make strategic decisions?

4 Manage risks and integrate Red and Blue teams into IT projects

- The importance of security testing in the software development cycle (DevSecOps).
- How to integrate the results of Red and Blue Teams into the risk management process.
- Prepare IT projects taking into account penetration testing and proactive defense.

Dates and locations

REMOTE CLASS
2026 : 20 Mar., 19 June, 18 Sep., 11 Dec.

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.