Publication date : 01/02/2024

Course : Cybercrime and cyberwar, issues and challenges

Seminar - 2d - 14h00 - Ref. BYR
Price : 2170 CHF E.T.

3,9 / 5

Cybercrime is a growing threat to society. Cybercriminals act from anywhere to attack corporate infrastructures. The question addressed in this course is not whether your organization will be attacked, but how to prepare for, detect, anticipate and manage cyber crises.

Teaching objectives

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

- Know the dangers and identify the sources of threats
- Understanding risks and safety issues
- Detecting intrusions and reacting to malicious acts
- Organize an effective, useful and graduated response
- Crisis planning for cyberwarfare

Intended audience

CISO, ISS function, general management, IT department, legal experts.

Prerequisites

No special knowledge required.

Practical details

Teaching methods

Masterly presentation with real and recent safety facts and incidents and case law in France and Europe.

Course schedule

PARTICIPANTS

CISO, ISS function, general management, IT department, legal experts.

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 Cybercrime in the news

- Sensitive data: cyber theft, espionage.
- New East/West cold war, USA/China.
- Worldwide service denials.
- Organized hackers, the role of intelligence agencies.
- News: malware, bots/botnets, ransomware.
- APT (Advanced Persistant treat), CB violations, skimming.

2 Detecting intrusions

- Management of traces, evidence and recordings.
- Detect abnormal activity, report an incident.
- Security event analysis and correlation (SIEM).
- Relevance of the SOC (Security Operation Center).
- Automate incident management.
- Intrusion testing, an essential anticipatory measure.
- Use a specialized incident detection company.

3 Organizing the response

- Searching for and collecting evidence.
- Declare an incident, prepare your crisis communication.
- Role of CERTs.
- Crisis unit: organization, crisis management.
- Vulnerability and patch management.

4 State order in the face of cybercrime

- Cybercrime (France, Europe): what repressive measures are needed?
- Role of ANSSI (France) and ENISA (Europe).
- Evidence management: admissibility, collection on the Internet.
- European Network and Information Security Directive (2018).
- European "cyber security Act" regulation (2019).
- Military Programming Act (2016).
- Role of states and Europe: laws, directives and regulations.

5 OIV / OSE best practices

- Cybersecurity governance: roles, responsibilities, business line involvement in risk management.
- Defense in depth: access control policy, management of privileged accounts.
- Cybersecurity incident management: detection policy, response.

6 Maintaining safety

- Vulnerability management policy, treatment (patching).
- Sensitive areas: update management.
- Declaration of attacks suffered.
- Mandatory certified service providers (PDIS, PRIS).
- Security audit by ANSSI, use of certified auditors (PASSI, LPM).

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 : 17 Mar., 9 June, 15 Sep., 10 Dec.