Publication date : 07/15/2024

Course : Introductory Cybersecurity Course

Practical course - 10d - 70h00 - Ref. BCS
Price : 6870 CHF E.T.

BEST

At the end of the course, the learner will be able to apply the fundamental principles, standards and tools of IT security in an operational context.

Teaching objectives

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

- A global vision of cybersecurity and its environment (challenges, ecosystem...)
- Learn about the various cybersecurity guidelines, standards and tools
- Understanding cybersecurity professions
- Know the legal obligations related to cybersecurity
- Understand the main risks and threats as well as protective measures
- Identify best practices in IT security

Intended audience

Anyone wishing to learn the fundamentals of IT security and/or move into cybersecurity professions (technicians, system and network administrators).

Prerequisites

General knowledge of information systems and familiarity with the ANSSI security hygiene guide.

Composition de la formation

Introduction to computer security

Ref. ISI - 1 day ★ 4 / 5

Safety in cyberspace

Ref. SCE - 3 days ★ 4 / 5

PARTICIPANTS

Anyone wishing to learn the fundamentals of IT security and/or move into cybersecurity professions (technicians, system and network administrators).

PREREQUISITES

General knowledge of information systems and familiarity with the ANSSI security hygiene guide.

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.

Course schedule

1 Threats and risks

- What is IT security?
- How can negligence create catastrophe?
- Everyone's responsibilities.
- IS architecture and potential vulnerabilities.
- Corporate networks (local, remote, Internet).
- Wireless networks and mobility. Risky applications: Web, messaging...
- Database and file system. Threats and risks.
- The sociology of pirates. Underground networks. Motivations.

2 Workstation safety

- Confidentiality, signature and integrity. Encryption constraints.
- The different cryptographic elements. Windows, Linux or MAC OS: which is the most secure?
- Managing sensitive data. Laptop issues.
- The different threats on the client workstation ? Understanding malicious code.
- How do you manage security vulnerabilities?
- USB ports. The role of the client firewall.

3 The authentication process

- Access controls: authentication and authorization.
- The importance of authentication.
- The traditional password.
- Certificate and token authentication.
- Remote connection via the Internet.
- What is a VPN?
- Why use strong authentication?

4 The safety audit process

- A continuous, comprehensive process.
- Audit categories, from organizational audits to penetration testing.
- 19011 best practices applied to safety.
- How to create an internal audit program? How do you qualify your auditors?
- Comparative contributions, recursive approach, human implications.
- Safety awareness: who? Who? Who?
- Definitions of Morality/Deontology/Ethics.
- The safety charter, its legal existence, content and validation.

5 The emergency plan and the cost of safety

- Risk coverage and continuity strategy.
- The importance of emergency, continuity, recovery and crisis management plans, PCA/PRA, PSI, RTO/RPO.
- Develop a continuity plan and integrate it into a quality approach.
- How to define safety budgets.
- Definition of Return On Security Investment (ROSI).
- Cost evaluation techniques, different calculation methods, Total Cost of Ownership (TCO).
- The Anglo-Saxon concept of the "Payback Period".

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.

6 Firewalls, virtualization and cloud computing

- Proxy servers, reverse proxy, address masking.
- Firewall-based perimeter protection.
- The differences between UTM, enterprise, NG and NG-v2 firewalls.
- Intrusion Prevention System (IPS) and IPS NG products.
- DMZ (demilitarized zone) solutions.
- Vulnerabilities in virtualization.
- The risks associated with Cloud Computing according to ANSSI, ENISA and CSA.
- The Cloud Control Matrix and its use in evaluating Cloud providers.

7 Safety supervision

- Safety dashboards.
- Security audits and penetration tests.
- Legal aspects of penetration testing.
- IDS probes, VDS scanner, WASS.
- How to respond effectively to attacks?
- Record evidence.
- Implement a SIEM solution.
- ANSSI labels (PASSI, PDIS & PRIS) for outsourcing.
- What to do in the event of an intrusion
- Judicial expertise: the role of a judicial expert (criminal or civil).
- Private legal expertise.

8 Web attacks

- OWASP: organization, chapters, Top10, manuals, tools.
- Discover the infrastructure and associated technologies, strengths and weaknesses.
- Client side: clickjacking, CSRF, cookie theft, XSS, components (Flash, Java). New vectors.
- Server side: authentication, session theft, injections (SQL, LDAP, files, commands).
- Inclusion of local and remote files, cryptographic attacks and vectors.
- Evasion and bypassing protection: WAF bypass techniques, for example.
- Burp Suite tools, ZAP, Sqlmap, BeEF.

Role-playing
Presentation and familiarization with environments and tools.
Implementation of various Web attacks in real-life conditions on the server and client sides.

9 Detecting intrusions

- Operating principles and detection methods.
- Market players, overview of systems and applications.
- Network (Nmap) and application (Web applications) scanners.
- IDS (Intrusion Detection System).
- The advantages of these technologies, and their limitations.
- How do you place them in your enterprise architecture?
- Market overview, detailed SNORT study.

Role-playing
Presentation and familiarization with environments and tools. Installation, configuration and implementation of SNORT, writing attack signatures.

10 Information gathering

- Heterogeneous sources. What is a safety event?
- Security Event Information Management (SIEM). Events collected from the IS.
- Equipment system logs (firewalls, routers, servers, databases, etc.).
- Passive collection in listening mode and active collection.

Role-playing
Log analysis procedure. Geolocating an address. Correlating logs from different sources, visualizing, sorting and searching for rules.

Dates and locations

REMOTE CLASS
2026 : 5 Mar., 4 June, 17 Sep., 19 Nov.