Course : Safety in cyberspace

Seminar - 3d - 21h00 - Ref. SCE
Price : 2990 CHF E.T.

4,4 / 5

Cybercrime is a growing threat to society, and cybercriminals act from anywhere to attack corporate infrastructures through cyberspace. This training course will show you how to meet corporate security requirements and integrate security into the architecture of an information system. You will be presented with a detailed analysis of threats and means of intrusion, as well as an overview of the main security measures available on the market.

Teaching objectives

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

- Understanding the evolution of criminals in cyberspace
- Understanding security in the cloud
- Secure client workstations and applications
- Understanding the principles of cryptography
- Learn how to manage IS security supervision

Intended audience

Anyone wishing to learn the fundamentals of IS security.

Prerequisites

Completion of the training course "Fundamentals of IS security".

Course schedule

1 Cyberspace and information security

- Principles of security: defense in depth, security policy.
- Fundamental concepts: risk, asset, threat...
- Risk management methods (ISO 27005, EBIOS, MEHARI). Overview of ISO 2700x standards.
- The evolution of cybercrime. Identifying threat agents.
- New threats (APT, spear phishing, watering hole, exploit kit, etc.).
- Software security flaws.
- The course of a cyber attack (NIST).
- 0day vulnerabilities, 0day exploits and exploitation kits.

PARTICIPANTS

Anyone wishing to learn the fundamentals of IS security.

PREREQUISITES

Completion of the training course "Fundamentals of IS security".

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.

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.

2 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.

3 Client workstation security

- Threats to client workstations.
- The role of the personal firewall and its limitations.
- Anti-virus/anti-spyware software.
- Security patches on client workstations.
- Secure removable devices.
- Checking customer compliance with NAC solutions.
- Browser and plug-in vulnerabilities.

4 The basics of cryptography

- The main constraints on use and legislation in France and around the world.
- Cryptographic techniques.
- Public key and symmetrical algorithms.
- Hash functions.
- Public key architectures.
- NSA and GCHQ cryptanalysis programs.

5 The user authentication process

- Biometric authentication and legal aspects.
- Challenge/response authentication.
- Password theft techniques, brute force, secret entropy.
- Strong authentication.
- Smart card authentication and X509 client certificate.
- The "3A" architecture: concept of SSO, Kerberos.
- IAM platforms.
- Identity federation via social network APIs.
- Identity federation for the enterprise and the cloud.

6 Exchange security

- SSL Crypto API and evolutions from SSL v2 to TLS v1.3.
- Attacks on SSL/TLS protocols and HTTPS flows.
- Hardware key containment, FIPS-140-3 certified.
- Easily assess the security of an HTTPS server.
- The IPsec standard, AH and ESP modes, IKE and key management.
- Overcoming problems between IPSec and NAT.
- SSL VPNs. What's the advantage over IPSec?
- SSH and OpenSSH for secure remote administration.
- On-the-fly flow decryption: legal aspects.

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.

7 Security for wireless networks and mobile devices

- Specific WiFi attacks. How to detect Rogue AP?
- Terminal safety mechanisms.
- WEP vulnerabilities. RC4 algorithm weaknesses.
- Risk description.
- IEEE 802.11i security standard. WLAN architecture.
- User and terminal authentication.
- WiFi authentication in the enterprise.
- Audit tools, free software, aircrack-ng, Netstumbler, WifiScanner...
- Threats and attacks on mobility.
- iOS, Android, Windows mobile: strengths and weaknesses.
- Viruses and malicious code on cell phones.
- MDM and EMM solutions for fleet management.

8 Software security

- Web and mobile applications: what are the differences in terms of security?
- The main risks according to OWASP.
- Focus on XSS, CSRF, SQL injection and session hijacking attacks.
- The main secure development methods.
- Security clauses in development contracts.
- Application firewall or WAF.
- How do you assess an application's security level?

9 The concepts of Security by Design and Privacy by Design

- Safety in design.
- The Security by Design approach to security assurance.
- The 7 fundamental principles of Privacy by Design.
- Privacy taken into account throughout the process.

10 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.

Dates and locations

REMOTE CLASS
2026 : 16 Mar., 15 June, 28 Sep., 30 Nov.