# *Network/Internet Security - Overview*

*Seminar of 3 days - 21h*
*Ref.: SRI - Price 2024: CHF2 890 (excl. taxes)*

## EDUCATIONAL OBJECTIVES

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

Be aware of developments in cybercrime and the challenges it poses

Gain proficiency in the security of the cloud, applications, and client workstations

Understand cryptography concepts

Manage IS security monitoring processes

# THE PROGRAMME

last updated: 07/2021

### 1) Information security and cybercrime

- Security principles: Defense in depth, cyber risk modeling.
- Risk management methods (ISO 27005, EBIOS RM).
- Overview of ISO 2700x standards.
- Evolution of cybercrime.
- New threats (APT, spear phishing, watering hole, crypto-jacking, etc.).
- Security flaws in software.
- Anatomy of a cyberattack (Kill Chain).
- The 0day, 0day Exploit, and exploit kit vulnerabilities.

### 2) Firewall, virtualization and cloud computing

- Perimeter protection based on firewalls and DMZs.
- Differences between UTM, enterprise, NG and NG-v2 firewalls.
- IPS (Intrusion Prevention System) and IPS NG products.
- Vulnerabilities in virtualization.
- Risks associated with Cloud Computing according to CESIN, ENISA, and the CSA.
- CASB solutions to secure data and applications in the cloud.
- The Cloud Controls Matrix and how to use it to evaluate Cloud providers.

### 3) Client workstation security

- Understanding client workstation oriented threats.
- Anti-virus/anti-spyware software.
- How to manage security patches on client workstations.
- Ransomware: preventive and corrective measures.
- How to make removable devices secure.
- Vulnerability of browsers and plug-ins.
- Drive-by download attack.
- Threats via USB keys (BadUSB, rubber ducky, etc.).

### 4) Fundamentals of cryptography

- Cryptographic techniques.
- Public key and symmetric key algorithms.
- Simple, salted and keyed (HMAC) hash functions.
- Public-key infrastructure (PKI).
- CC certification and ANSSI qualification of cryptographic products.

### 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.

### 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.

## 5) Authentication and qualification of users

- Biometric authentication and legal aspects.
- Challenge/response authentication.
- The different attack techniques (brute force, keylogger, credential stuffing, etc.).
- Strong multi-factor authentication (MFA).
- Chip card authentication and X509 client certificate.
- The HOTP and TOTP standards of OATH.
- The UAF and U2F standards of the FIDO (Fast ID Online) alliance.

## 6) Network flow security

- The SSL crypto API and its upgrades from SSL v2 to TLS v1.3.
- Attacks on SSL/TLS protocols.
- Attacks on HTTPS flows.
- Hardware key confinement, FIPS-140-2 certifications.
- The IPsec standard, AH and ESP modes, IKE and key management.
- Overcoming problems between IPSec and NAT.
- The SSL VPNs. What are the benefits compared to IPSec?
- Using SSH and OpenSSH for secure remote administration.
- On-the-fly decryption of flows: Legal aspects.
- Easily evaluating the security of an HTTPS server.

## 7) Wi-Fi security

- Specific Wi-Fi attacks.
- How to detect Rogue APs.
- Terminal security mechanisms.
- KRACK attack on WPA and WPA2.
- Description of the risks.
- The IEEE 802.11i security standard.
- What WPA3 adds and the DragonBlood vulnerabilities.
- User and terminal authentication.
- WiFi authentication within the company.
- Auditing tools, free software, aircrack-ng, Netstumbler, WiFiScanner, etc.

## 8) Smartphone security

- Threats and attacks on mobile devices.
- iOS and Android: strengths and weaknesses.
- Viruses and malicious code on mobile phones.
- MDM and EMM solutions for fleet management.

## 9) Application security

- Applying the principle of defense in depth.
- Web and mobile apps: What security differences are there?
- Main risks according to OWASP.
- Focus on XSS, CSRF, SQL injection, and session hijacking attacks.
- Main methods of secure development.
- What security clauses are there in development contracts?
- The application firewall or WAF.
- How to assess an application's level of security.

## 10) Management and active supervision of security

- Safety audits (scope and frameworks: ISO 27001, GDPR, etc.).
- Intrusion tests (black box, gray box and white box).
- How to effectively respond to attacks.
- Setting up an SIEM solution.
- Should you implement or outsource your Security Operation Center (SOC)?

- SOC 2.0 technologies (CASB, UEBA, Deceptive Security, EDR, SOAR, machine learning, etc.).
- ANSSI labels (PASSI, PDIS & PRIS) for outsourcing.
- Incident response procedures (ISO 27035 and NIST SP 800-61 R2).
- Bug Bounty platforms.

## DATES

Contact us