Course : Big Data, data security

Practical course - 2d - 14h00 - Ref. SBD
Price : 1680 CHF E.T.

À l'issue de la formation, le participant est capable d'initier une politique de sécurisation des données par une approche technique et légale du sujet. Elle permet de comprendre les enjeux de la sécurité dans les environnements Big Data, d'identifier les risques majeurs et d'y répondre avec des solutions concrètes.

Teaching objectives

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

- ✓ Understanding complex data qualification
- ✓ Identify the main risks affecting massive data processing solutions
- ✓ Understanding the legal framework (CNIL and PLA - Privacy Level Agreement)
- ✓ Know the main basic technical solutions to protect against risks
- ✓ Implement a security policy to deal with risks, threats and attacks

Intended audience

Security and IS consultants, system administrators.

Prerequisites

Notions of application architectures. Good knowledge of network and system security, Hadoop platforms.

Course schedule

PARTICIPANTS

Security and IS consultants, system administrators.

PREREQUISITES

Notions of application architectures. Good knowledge of network and system security, Hadoop platforms.

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.

1 Risks and threats

- Introduction to security. Key external information sources (ANSSI, CLUSIF, ENISA, etc.).
- The current state of IT security.
- IT security vocabulary.
- DICT/P classification: Availability, Integrity, Confidentiality and Traceability/Proof.
- Attacks "lower layers". Security on Hadoop. Intelligence gathering.
- TCP/IP protocol strengths and weaknesses. HTTP: an exposed protocol (SQL injection, Cross Site Scripting, etc.).
- Illustration of ARP and IP Spoofing attacks, TCPSYNflood, smurf, etc.
- Denial of service and distributed denial of service. DNS: Dan Kaminsky attack. Application attacks.

Hands-on work

Install and use the Wireshark network analyzer. Implementing an application attack.

2 Security architectures

- Which architectures for which needs?
- Secure addressing plan: RFC 1918. Address translation (FTP as an example).
- The role of demilitarized zones (DMZs). Examples of architectures.
- Secure architecture through virtualization.
- Firewall: the cornerstone of security, firewalls and virtual environments.
- Proxy server and application relay. Proxy or firewall: competition or complementarity?
- Technological evolution of firewalls (Appliance, VPN, IPS, UTM, etc.).
- Reverse proxy, content filtering, caching and authentication. SMTP relay: a must?

Hands-on work

Implementation of a proxy cache/authentication.

3 Verify system integrity

- Operating principles.
- What products are available?
- Introducing Tripwire or AIDE (Advanced Intrusion Detection Environment).
- Vulnerability auditing.
- Vulnerability management principles, methods and organizations.
- Reference site and overview of auditing tools.
- Definition of a security policy.
- Study and implementation of Nessus (status, operation, evolution).

Hands-on work

Audit network and server vulnerabilities using Nessus and Nmap. Website vulnerability audit.

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.

4 Legal violations of automatic data processing systems

- Reminder, definition of automatic data processing system (ADPS).
- Risks for massive data processing solutions.
- Types of breaches, European context, the LCEN law. The RGPD regulation, CNIL, PLA.
- What are the legal risks for the company, its managers and CISOs?

Dates and locations

REMOTE CLASS
2026 : 18 June, 19 Nov.