Publication date : 03/01/2024

Course : Cloud Computing Security

Seminar - 2d - 14h00 - Ref. OUD
Price : 2020 CHF E.T.

4,4 / 5

Course schedule

1 Introduction to Cloud Computing security

- Definition of Cloud Computing (NIST, Burton Group).
- Major providers and main faults already observed.
- SecaaS (Security as a Service).
- The keys to a secure architecture in the Cloud.

2 Virtual environment security

- How virtualization helps security.
- Specific threats and vulnerabilities.
- Three security integration models: Virtual DataCenter, Hardware Appliance and Virtual Appliance.
- Virtualization-specific security solutions.

3 Secure network access to the Cloud

- Vulnerabilities and issues in access security.
- Native security in IP v4, IPsec and IP v6.
- Protocols: PPTP, L2TP, IPsec and VPN SSL.
- Access to Cloud via the secure Web (https).
- Vulnerabilities of Cloud clients (PC, tablets, smartphones) and browsers.

4 Work of the Cloud Security Alliance (CSA)

- Security Guidance for Critical Areas of Focus in Cloud Computing.
- The thirteen areas of security. The seven main threats.
- The GRC integrated suite.
- CloudAudit, Cloud Controls Matrix, Consensus Assessments Initiative Questionnaire, Cloud Trust Protocol.
- CCSK certification (Certificate of Cloud Security Knowledge).

5 Cloud Computing security according to ENISA

- Cloud risk assessment and management using the ISO 27005 standard.
- The thirty-five risks identified by ENISA. ENISA recommendations for government Cloud security.

PARTICIPANTS

PREREQUISITES

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.

6 NIST recommendations for security

- Guidelines for security and confidentiality in public cloud computing.
- Analysis of the NIST 800-144 and NIST 800-146 standards.

7 Testing Cloud security

- What security label for suppliers: Cobit, ISO2700x, or ISO 15401 common criteria?
- How do you audit security in the Cloud?
- Cloud-oriented security testing tools (Metasploit & VASTO, openVAS, xStorm, etc.).

8 Legal aspects

- Private cloud to public cloud: Legal consequences. Responsibilities of various players.
- Regulatory compliance (PCI-DSS, CNIL, SOX...).
- Precautions for writing a contract.

Dates and locations

REMOTE CLASS
2026 : 16 June, 16 June, 29 Sep., 29 Sep., 24 Nov., 24 Nov.

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.