

Seminar , 2 day(s)
Ref : OUD

Participants

CIOs, CISOs, security managers, project managers, consultants, administrators.

Pre-requisites

Basic knowledge on computing is required.

Next sessions

Cloud Computing Security

OBJECTIVES

How can you ensure the security of information that's spread out in the cloud? This seminar gives a full overview of this critical issue for remote storage. Once it is complete, participants will have gained the essential knowledge to take the Cloud Security Alliance's CCSK certification test.

1) Introduction to Cloud Computing security

2) Virtual environment security

3) Secure network access to the Cloud

4) Work of the Cloud Security Alliance (CSA)

5) Cloud Computing security according to ENISA

6) NIST recommendations for security

7) Testing Cloud security

8) Legal aspects

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.

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.