

Cloud Security - Concepts and Challenges

Duration: 1 day

Audience: Professionnel TI

Who is this training for?

Any manager, architect, analyst or developer who wants to gain the knowledge to understand the concepts, threats, risks and challenges associated with cloud security.

Training objectives

- Describe cloud service models (IaaS, PaaS, and SaaS) and explain their commonalities and differences.
- Explain the impact of cloud service models on key elements of organizational security (data management, user management).
- Explain the cloud security issues associated with the roles of the information technology function (Architecture, Development, Operations).
- List the threats and risks associated with the different themes.

Summary

Cloud computing has become a very important element of organizational risk due to the exposure of organizations to security issues. As a result, cloud security is a high-demand area of information technology. In this training, beyond the technological explanations of the security elements, several themes related to this security will be addressed. We will talk about issues, risk, compliance and governance. Cloud security is seen globally and approached with very localized actions to guarantee a better seal of information technology functions, and therefore of organizational functions. At the end of this training, you will have a more complete and pragmatic vision of the cloud security elements to be taken into account in your development or operation work in an information technology context.

Course outline

Chapter 1: Introduction to Cloud Security

- Introduction to the basics of cloud security.

- Cybersecurity versus Cloud Security.

Chapter 2: Cloud Computing Models

- Cloud Service Models (IaaS, PaaS, SaaS).
- Cloud services management model.
- Quizzes.

Chapter 3: The principles of technological security

- Risk. •
- Compliance.
- Cost.
- Confidentiality.
- Governance.
- Quizzes.

Chapter 4: Data and Cloud Security

- Classification.
- Encryptions.
- Identification.
- Quizzes.

Chapter 5: Users and Cloud Security

- Directory Management.
- Password management.
- Authorization and authentication.
- Quizzes.

Chapter 6: Technology Architecture and Cloud Security

- Physical Security.
-

Network security.

- Platform security.
- Product safety.
- Quizzes.

Chapter 7: Software Development and Cloud Security

- Security Requirements.
- Code and intrusion.
- Security testing.
- Principles of DevSecOps.
- Quizzes.

Chapter 8: Cloud Operations and Security

- Security Incident Management.
- Monitoring and observability.
- Forensics.
- Quizzes.

Chapter 9: Conclusion

- Reminder of the threats.
- Reminder of the principles to be followed.
- Cloud security certifications.
- Group discussion.

Approach and methodology

The pedagogical approach combines practical explanations, group discussions and quizzes.

Prerequisites

Basic knowledge of information technology.

Recommendations

- Basic understanding of IT environments (infrastructure, applications, data)
- General notions of networking and cybersecurity (asset)
- Basic knowledge of or interest in cloud technologies (Azure, AWS, etc.)
- Sensitivity to data protection, privacy and compliance issues Interest in risk management and IT governance

Accreditations

Training recognized by the Barreau du Québec for the purposes of mandatory continuing education for a duration of 7 hours.