CLD101 - CLOUD SECURITY FUNDAMENTALS

Course Learning Objectives

Describe what cloud computing is and its advantages. Discover what are the common cloud delivery and deployment models. Learn about the attack vectors associated with cloud computing. Differentiate between various attacks that could be targeting your cloud application.

Apply cloud security design principles when developing cloud-based applications. Utilize sound cloud security testing techniques. Recognize the security risks and concerns with adopting cloud computing.

Description

This course aims to teach you about common security concerns surrounding cloud-based applications and to some extent, cloud providers.

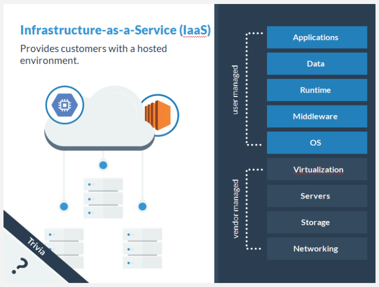
You will also learn about best practices and security concepts involved when creating applications for the cloud, all the way from requirements to deployment.

Audience

Cloud application developers

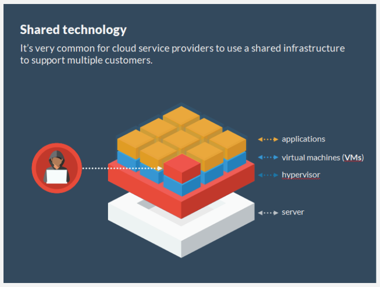
Time Required

Tailored learning - 60 minutes total



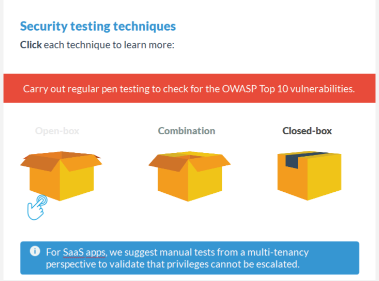
Infrastructure-as-a-Service (IaaS)

Provides customers with a hosted environment.



Shared technology

It's very common for cloud service providers to use a shared infrastructure to support multiple customers.



Security testing techniques

Click each technique to learn more:

Carry out regular pen testing to check for the OWASP Top 10 vulnerabilities.

For SaaS apps, we suggest manual tests from a multi-tenancy perspective to validate that privileges cannot be escalated.

Security Compass

CLD101 - CLOUD SECURITY FUNDAMENTALS

Course Outline

1. Introduction to Cloud Computing

- What is cloud computing?
- Why cloud?
- Cloud delivery models
- Software-as-a-Service
- Platform-as-a-Service
- Infrastructure-as-a-Service
- Cloud deployment models
- Cloud-based applications
- Characteristics of cloud-based applications
- Security concerns

4. Security Concerns and Challenges

- Standards and compliance
- Cloud standards working group
- Case study: Google apps
- Privacy compliance
- Privacy policy
- Access control and identity management
- Enterprise identity provider
- Identity management-as-a-service
- Encryption and key management
- Software-based protections
- VM architecture

2. Security Objectives

- Cloud security objective
- Confidentiality
- Integrity
- Availability
- Cloud attack vectors
- Insecure APIs
- Shared technology
- Cloud service providers
- Cloud users
- Attacks associated with cloud-based applications
- Availability based attacks
- Data security based attacks
- Network security based attacks
- Identity management based attacks

3. Secure SDLC

- Cloud application security requirements
- Authentication and identification
- Authorization
- Auditing
- Cloud security design principles
- Weakest link
- Least privilege
- Separation of duties
- Defense in depth
- Fail safe
- Economy of mechanism
- Complete mediation
- Open design
- Least common mechanism
- Psychological acceptability
- Leveraging existing components
- Secure development practices
- Choosing a language
- Coding practices
- Managing user input
- Handling data
- Cloud application security testing
- Security test plan
- Security testing techniques
- Cloud application secure deployment

Security Compass