

# **Data Security for Developers**

### **Audience Course Data Security for Developers**

The course Data Security for Developers is intended for developers who want to learn what data security risks there are and how you can arm yourself against them.

#### **Prerequisites Course Data Security for Developers**

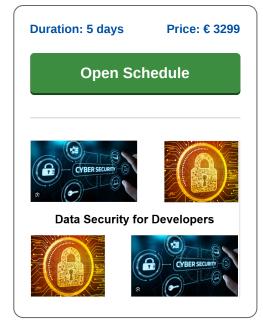
To participate in the course Data Security for Developers, experience with software development is required. Experience with object-oriented programming in C#, Python or Java is beneficial for understanding.

#### **Realization Training Data Security for Developers**

The course Data Security for Developers has a hands-on character. The theory is treated on the basis of presentation slides and is interchanged with practical exercises.

#### **Certification Course Data Security for Developers**

After successfully completing the training, the attendants receive a certificate of participation in the course Data Security for Developers.



## **Content Course Data Security for Developers**

The course Data Security for Developers covers the most common risks in securing data and how you can arm yourself against them. Attention is paid to data protection, securing communication, configuring access control and using authentication methods. Standards such as the General Data Protection Regulation (GDPR) are discussed as well.

#### **Intro Data Security**

The course starts with a discussion and explanation of the main concepts that play a role in Data Security such as authentication, access control, encryption, confidentiality, integrity, as well as backup and recovery.

#### **Secure Communication**

Subsequently setting up secure connections over Secure Sockets Layers (SSL) is treated. The creation of client and server certificates and the role of certificate authorities is covered.

#### **Encryption**

Then the different types of encryption are explained such as symmetric, asymmetric and hash encryption. And various encryption algorithms such as RSA and ECC are considered.

#### Web App Risks

Next attention is paid to typical security risks that play a role in web applications. The prevention of cross site scripting, SQL injection, cross site request forgery and session hijacking are debated then.

The safe regulation of access control by means of key management systems, secure password storage and two factor authentication are also on the program of the course. The importance of role-based and permission-based authorization is treated as well.

#### **Updates, Monitoring and Logging**

Next the importance of keeping systems and applications secure by applying updates is covered. And the importance of monitoring, logging and incident responding is discussed also.

#### **Securing Apps and APIs**

Finally attention is paid to keeping Apps and APIs secure by testing endpoints for data leakage and security flaws. Various standards for data regulation such as GDPR, CCPA, PCI DSS and HIPAA are also treated then.

Locations

Houten, Amsterdam, Rotterdam, Eindhoven, Zwolle, Online



# **Modules Course Data Security for Developers**

Module 1 : Intro Data Security	Module 2 : Secure Communication	Module 3 : Secure Data at Rest
Access Controls	Secure Sockets Layer (SSL)	Asymmetric Encryption
Authentication	Private and Public Key	Symmetric Encryption
Backups and Recovery	SSL Certificates	Hash Encryption
Data Erasure	Creating Certificates	Encryption Algorithms
Data Masking	CSR's	RSA algorithm
Data Resiliency	Client and Server Certificates	ECC algorithm
Encryption	Chain of Trust	Using standard encryption
Confidentiality	Trusted certificate authorities (CAs)	Encoding and obfuscation
Integrity	Transport Layer Security	Digital Signing
Availability	Verify network connections	Salt Function
Cookie Theft	Verify metadata in HTTP headers	Protect against Malware
Module 4 : Web App Risks	Module 5 : Keys and Passwords	Module 6 : Access Controls
Cross Site Scripting	Key management systems	Role Base Security
Prevent Untrusted Data	Assigning Keys	Lattice Based Access Control
Social Engineering	Revoking Keys	Separate Roles and Functions
SQL Injection	Rotating Keys	Role Assignment
Escaping User Input	Deleting Keys	Role Authorization
Prepared Statements	Secure passwords storage	Permission Authorization
URL Rewriting	Avoid embedding in code	Role Hierarchies
Cross-Site Request Forgery	Two factor Authentication	Mandatory Access Control
Session Hijacking	Provide Two Factor option	Discretionary Access Control
Session Fixation	Remove vendor-supplied defaults	Removing access and privileges
Module 7 : Updates and Patches	Module 8 : Monitor and Log	Module 9 : Securing Apps and API's
Addressing Security Vulnerabilities	Event Recording	Basic app security practices
Applying Patches	Log Monitoring	Assessing permissions and data needs
Keeping Systems Updated	Tracing Sending Data	Aligning data access to purpose of use
Checking Distributions	Tracing Storing Data	Testing APIs for data leakage
Use Trusted Network Locations	Monitoring Transfers	Testing endpoints for data leakage
Emails and Attachments	Ensure system stability	Testing transmissions third parties
Manual Updates	Incident Responding	Scanning app and code
Automatic Updates	Improving Compliance	Searching security flaws
Updating Core libraries	Identify security breaches	Regularly test security systems
Module 10 : Data Security Regulations		
	]	
GDPR, CCPA, PCI DSS and HIPAA		
GDPR, CCPA, PCI DSS and HIPAA General Data Protection Regulation		

Sarbanes-Oxley (SOX) PCI Data Security Standard

ISO 27001