SC470-EN Secure Development Principles

Kurzbeschreibung:

The **SC470-EN Secure Development Principles** workshop teaches you the theoretical principles of secure software development in a professional environment.

In addition to robust architecture, the focus is on business and threat modeling as well as risk handling. You will learn about all the building blocks of the secure development lifecycle: requirement gathering, secure design, secure implementation, secure testing and deployment. Specifically, the topics of business and project requirements, threat modeling and secure design will be covered.

The workshop places particular emphasis on current concepts, which are explored in depth using numerous interactive practical examples. This gives participants the opportunity to actively contribute their own experiences and requirements. By the end of the workshop, participants will have gained a solid understanding of secure software development in a professional environment and will be able to plan robust and secure applications and support their implementation.

The course is part of the "qSkills Secure Software Quadrant", which consists of:

- SC460 Secure Architecture and Design
- SC470 Secure Development Principles
- SC475 OWASP Security Champion
- SC480 Secure Operations

Zielgruppe:

The **SC470-EN Secure Development Principles** training is ideal for:

- Software project managers / product owners
- Business analysts / requirements engineers
- IT consultants
- Junior software/cloud architects
- Junior software developers

Voraussetzungen:

In order to be able to follow the course content and pace of learning in the **SC470-EN Secure Development Principles** workshop, professional experience in software development is helpful. Programming knowledge is not a prerequisite.

Sonstiges:

Dauer: 4 Tage

Preis: 2850 Euro plus Mwst.

Ziele:

The **SC470-EN Secure Development Principles** course provides:

- Identify vulnerabilities in concepts and architectures
- Identify business critical assets
- Develop and describe attack vectors

Inhalte/Agenda:

- **Introduction**
  - What is secure coding and what is it not
  - Terminology and concept of training
- **Requirement Gathering**
  - Business requirements (business area, processes, assets, etc.)
  - Project requirements (code maturity, internal functionality requirements, budget, legal requirements, etc.)
  - Threat model (protection goals, identification of attack vectors, risk management, mitigation strategies)
- **Secure Design**
  - Secure Design Principles (Bugchains, Security by Design, Viega's and Graw's Principle)
  - Robust Architecture (Application Components, The Dependency Rule, Service Mesh)
  - Robust Technology Design (Development Considerations, Supply Chain Considerations)
- **Secure Implementation**
  - OWASP Top 10, CWE, Best Practices
  - Authentication (Identification & Authentication, Broken Access Control)
  - Processing (Input Parsing, Injection)
  - Storage (Software & Data Integrity, Cryptographic Failures, Logging & Monitoring Failures)
- **Testing**
  - Automated Testing (Test Cases, Test Setups, Tools)
  - Penetration Testing (Concept, Methods, Tools)
  - Chaos Engineering (Concept, Resilience, Case Study)
- **Deployment & Maintenance**
  - Launch (Release Strategies, Hypercare)
  - Longterm Support (Change Management, Feature Requests, Future Proof)
  - Disaster Recovery (Backups, Supply Chain, Business Continuity)
- **Learning progress review / exam**