SC470 Secure Development Principles

Kurzbeschreibung:

Softwareentwickler und -architekten lernen die Grundlagen sicherer Softwareentwicklung im professionellen Umfeld. Vermittelt werden Business- und Threatmodellierung, Risikobehandlung sowie alle Bausteine des Secure Development Lifecycle von Anforderungsanalyse über Design und Implementierung bis zu Testing und Deployment. Zahlreiche interaktive Praxisbeispiele vertiefen das Verständnis und fördern die aktive Einbindung eigener Erfahrungen.

Zielgruppe:

Das Training **SC470 Secure Development Principles** ist ideal geeignet für:

- Software Projektmanager / Product Owner
- Business Analysten / Requirements Engineers
- IT Consultants/Berater
- Junior Software-/Cloudarchitekten
- Junior Softwareentwickler

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **SC470 Secure Development Principles** gut folgen zu können, ist Berufserfahrung in der Softwareentwicklung hilfreich. Programmierkenntnisse sind keine Voraussetzung.

Sonstiges:

Dauer: 4 Tage

Preis: 2850 Euro plus Mwst.

Ziele:

Der Kurs **SC470 Secure Development Principles** bietet:

- Erkennen von Schwachstellen in Konzepten und Architekturen
- Identifizieren von Business-kritischen Assets
- Entwickeln und Beschreiben von Angriffs-Vektoren

Inhalte/Agenda:

- **Einleitung**
  - ◊ Was ist Secure Coding und was ist es nicht?
  - ◊ Begrifflichkeiten und Konzept der Schulung
  - ◊
- **Requirement Gathering**
  - ◊ Business Requirements (Geschäftsfeld, Prozesse, Assets usw.)
  - ◊ Project Requirements (Code-Reife, interne Funktionalitätsanforderungen, Budget, gesetzliche Anforderungen usw.)
  - ◊ Threat Model (Schutz-Ziele, Identifikation von Angriffs-Vektoren, Risk Management, Mitigation Strategien)
  - ◊
- **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)
  - ◊ Desaster Recovery (Backups, Supply Chain, Business Continuity)
  - ◊
- **Lernstandskontrolle / Prüfung**