SC475 OWASP Security Champion

Kurzbeschreibung:

Der Workshop **SC475 OWASP Security Champion** vermittelt Ihnen die Werkzeuge und Konzepte der sicheren Softwareentwicklung im professionellen Umfeld. Neben dem Härten der eigentlichen Anwendung liegt hier auch ein Fokus auf den modernen Konzepten Supply Chain Management und CI/CD Pipelines. Sie lernen Methoden und Tools kennen, um effizient Schwachstellen in Anwendungen zu identifizieren und zu beheben.

Der Workshop legt besonderen Wert auf praxisnahe Anwendungen, indem zahlreiche Übungen angeboten werden, die es den Teilnehmern ermöglichen, ihr erlerntes Wissen direkt in die Tat umzusetzen und zu festigen. Am Ende des Workshops werden die Teilnehmer ein solides Verständnis für das Härten von Applikationen und den dazugehörigen Prozessen erlangt haben, und können in ihrem Unternehmen als *Security Champion* zum Einsatz kommen.

Der Kurs ist Teil des "qSkills Secure Software Quadrant", bestehend aus:

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

Zielgruppe:

Das Training **SC475 OWASP Security Champion** ist ideal geeignet für:

- Software Entwickler
- DevOps Engineers
- DevSecOps Engineers

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **SC475 OWASP Security Champion** gut folgen zu können, sind allgemeine Programmierkenntnisse und Berufserfahrung als Softwareentwickler notwendig.

Sonstiges:

Dauer: 4 Tage

Preis: 2950 Euro plus Mwst.

Ziele:

Der Kurs **SC475 OWASP Security Champion** bietet:

- Identifizieren und Hardening der Supply Chain
- Hardening von CI/CD Pipelines
- Reaktion auf Security Incidents

Inhalte/Agenda:

- ♦ **Einleitung**
  - ♦ ◊ Vorstellung und Motivation
    ◊ Begrifflichkeiten und Konzept der Schulung
- ♦ ◊
- ♦ **Security Champions**
  - ♦ ◊ OWASP Top 10 und die 3 Big Lies
    ◊ Sisyphos vs Broken Glas
- ♦ ◊
- ♦ **Application Hardening**
  - ♦ ◊ CWE & Design Pattern
    ◊ SAST & DAST
    ◊ Container Hardening
- ♦ ◊
- ♦ **Supply Chain Hardening**
  - ♦ ◊ Discovery and Integration of SBOMs
    ◊ Continuous Vulnerability Detection
    ◊ Centralized Image Artefactories
- ♦ ◊
- ♦ **Pipeline Hardening**
  - ♦ ◊ IaC Security Concepts
    ◊ Qualitygates in CI/CD
    ◊ Response Automation with WAFs
- ♦ ◊
- ♦ **Viele praktische Übungen zu den einzelnen Modulen**
- ♦
- ♦ **Lernstandskontrolle / Prüfung**
  - ♦