



Softwaresicherheit im automobilen Entwicklungsprozess

Step by step zu mehr Sicherheit

Das Seminar vermittelt grundlegende Sicherheitsaspekte der Softwareentwicklung. Teilnehmende lernen, Sicherheitsanforderungen frühzeitig zu berücksichtigen, Bedrohungen zu analysieren und Risiken zu bewerten. Praxisnahe Workshops helfen, Implementierungsschwachstellen zu erkennen und Schutzmaßnahmen umzusetzen.

Grundlagen, Methoden und Werkzeuge für sichere Softwareentwicklung

Das Seminar bietet eine umfassende Einführung in die Sicherheitsaspekte der Softwareentwicklung. Angesichts der zunehmenden Komplexität und Vernetzung moderner Systeme ist es unerlässlich, Sicherheitsbelange von Beginn an in jedem Entwicklungsschritt zu berücksichtigen.

Teilnehmende erhalten einen Überblick über aktuelle Vorgehensmodelle, Methoden und Werkzeuge, die für die Entwicklung sicherer

Software im gesamten Lebenszyklus eingesetzt werden können. Dabei werden sowohl Security Requirements als auch Bedrohungsanalysen betrachtet, um potenzielle Risiken frühzeitig zu identifizieren und zu bewerten.

Die Schulung wird von erfahrenen Dozenten mit fundiertem Hintergrund in der IT-Sicherheitsforschung geleitet, die neben theoretischem Wissen auch Einblicke in aktuelle Forschungsergebnisse bieten.

Kursdetails auf einen Blick

- Für **Software-Architekten*innen, Fachexpert*innen, Projektleiter*innen**
- **Inhouse Training**
- Dauer: **2 oder 4 Tage**
- Format: **Präsenz oder Online**
- Kosten: 1.200,00 Euro (USt.-befreit gem. § 4 Nr. 22a UStG)

Praxisorientierte Schulung zur sicheren Software-Implementierung

Ein zentraler Bestandteil des Seminars ist die sichere Implementierung von Software. Teilnehmende lernen, typische Implementierungsschwachstellen zu erkennen und zu vermeiden. Zudem werden sie mit gängigen Angriffstechniken vertraut gemacht, um entsprechende Gegenmaßnahmen entwickeln zu können. Workshops ermöglichen es, die erworbenen Kenntnisse anhand von Beispielprojekten anzuwenden und zu vertiefen. Durch diese praxisnahe Herangehensweise wird das Verständnis für die Entwicklung sicherer Software gestärkt und die Fähigkeit zur Umsetzung in Projekten gefördert.

Das Seminar richtet sich an Software-Architektinnen und -Architekten sowie Software-Ingenieurinnen und -Ingenieure, die ihre Kenntnisse im Bereich der Softwaresicherheit erweitern möchten.

Auch Fachexpertinnen und -experten sowie technische (Projekt-)Leiterinnen und -Leiter in Entwicklungsprojekten profitieren von den vermittelten Inhalten. Vorausgesetzt werden Grundkenntnisse der Softwaretechnik, insbesondere in den Bereichen Softwareentwicklungsprozesse, Anforderungsanalyse, Softwaredesign und Softwaretest.

Nach dem Seminar können Sie:

- **Sicherheitsbelange** in allen Phasen berücksichtigen.
- Wesentliche **Bedrohungen identifizieren** und abwehren.
- Hauptsächliche **Sicherheitslücken** in Software vermeiden, erkennen und beheben.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/Software-Engineering>

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

Tag 1

- Übersicht über die Entwicklung sicherer Software, Vorgehensmodelle, Reifegradmodelle und Standards
- Risiko- und Anforderungsanalyse
- Workshop Requirements: Strukturanalyse mit DFD, Bedrohungsanalyse mit STRIDE, Risk Modeling, Requirements Specification
- Secure Design: Prinzipien und Entwurfsmuster

Tag 2

- Sichere Implementierung: Angriffsflächen am Beispiel Automotive
- Typische Implementierungsschwachstellen und Gegenmaßnahmen, Seitenkanalangriffe
- Workshop Implementierung: Finden und Vermeiden von Programmierfehlern
- Testen von Schutzkonzepten

Zugangsvoraussetzung:

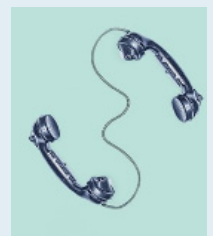
Grundkenntnisse der Softwaretechnik (Software Engineering):

Softwareentwicklungsprozesse, Anforderungsanalyse, Softwaredesign, Nachvollziehen von C-Programmbeispielen, Softwaretest

Fachlicher Ansprechpartner am Fraunhofer AISEC

Albert Stark
Tel. +49 89 3229986-1038
albert.stark@aisec.fraunhofer.de

Fraunhofer AISEC
Herrmann-Brenner-Platz 1
92637 Weiden i.d.OPf.



Lernlabor
Cybersicherheit