


 Entwicklung und Testing
sicherer Software
Online


Informationen im Überblick

 Keine Voraussetzungen

 Führungskräfte (insb.
von Product Ownern und
Entwicklungsteams)

 7 Wochen in Teilzeit
(ca. 23 Stunden), Live-
Online-Sessions jeweils
von 08:30 – 12:30 Uhr

€ 2100,-

 online

Veranstaltet durch



Referenten:



Dr. Stefan Dziwok,
Senior Researcher
am Fraunhofer IEM



Dr. Matthias Becker
Abteilungsleiter am
Fraunhofer IEM



Weitere Infos und
aktuelle Termine
buchen unter:

[www.cybersicherheit.fraunhofer.de/
software_securitytraining_
fuehrungskraefte](http://www.cybersicherheit.fraunhofer.de/software_securitytraining_fuehrungskraefte)

Software Security Training für Führungskräfte

Security als Führungsaufgabe

Sicherheitslücken in Softwareprodukten bedrohen in zunehmendem Maße den Unternehmenserfolg. Trotzdem wird die Verantwortung für Sicherheitsvorfälle häufig allein bei den Entwickler*innen gesehen. Dabei können insbesondere Führungskräfte Security aktiv angehen und in ihrem Verantwortungsbereich systematisch verankern. In diesem Seminar lernen Führungskräfte, wie sie Bedingungen schaffen, die eine sichere Softwareentwicklung ermöglichen und fördern. Sie werden befähigt Risiken zu erkennen und geeignete Maßnahmen im Entwicklungsumfeld einzuleiten.

Inhalte des Seminars

- Sensibilisierung für das Thema Software Security
- Software Security Grundlagen (Terminologie, Schutzziele etc.), Gesetze und Normen, Stakeholder-Management
- Risikoanalyse

- Bereichsentwicklung (u.a. der Kompetenzaufbau ihrer Mitarbeitenden)
- Anwendung in der Praxis via eines Coaching-on-the-Job

Ihr Nutzen

- Nach dem Seminar können Sie die Bedeutung und die Auswirkungen von sicherheitskritischen Vorfällen besser einschätzen.
- Sie können verschiedene Aspekte von Software Security erläutern und sich mit relevanten Stakeholder-Gruppen darüber austauschen.
- Sie sind in der Lage den Ist-Stand in ihrem Bereich zu erfassen und Risiken anhand von verschiedenen Kriterien zu analysieren.
- Sie kennen verschiedene Handlungsoptionen und können konkrete Maßnahmen ergreifen, welche die Software Security steigern.