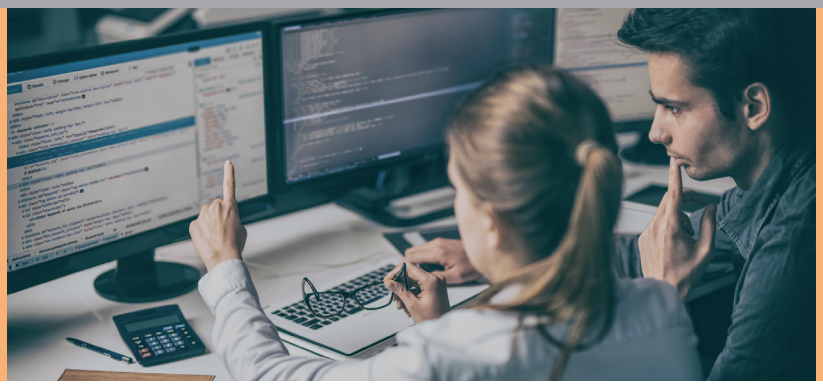
Fraunhofer
ACADEMY

SEMINAR
15. – 17.1.2018
21. – 23.2.2018
14. – 16.3.2018
11. – 14.5.2018



IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …

… Angreifer und deren Motivation klassifizieren.
… Bedrohungen gegenüber der Software sowie der Entwicklung identifizieren.
… Risiken gegenüber der Software priorisieren und adressieren.
… Maßnahmen von den Risiken ableiten, bewerten und implementieren.

Dieses Seminar bietet Ihnen …

…einen passgenauen Mix aus Theorie und Praxis.
… viele Beispiele und anwendbares Wissen.
… Übungen zum vermittelten Inhalt an realitätsnahen Fallbeispielen, damit Sie Ihr Wissen direkt im Unternehmen einsetzen können.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/cybersicherheit-sse

SECURE SOFTWARE ENGINEERING

Ganzheitliche Absicherung der Software-Entwicklung

Die Herausforderung: Softwaresysteme vor Angriffen schützen

IT-Systeme steuern heute alle zentralen und oft sicherheitskritischen Funktionen in städtischen Infrastrukturen, Autos, Bahnen, Fabriken oder Flugzeugen. Dies bedeutet ein enormes Bedrohungspotenzial in allen Arten von Anwendungen und Applikationen. Damit diese jederzeit funktionieren und vor Angriffen geschützt sind, muss die Systemqualität durchgehend gewährleistet werden. Hierfür ist es nötig, den gesamten Softwareentwicklungsprozess abzusichern und die Qualität stetig zu optimieren.

Die Lösung: Qualität und Sicherheit in der Softwareentwicklung herstellen

Für eine ganzheitliche Absicherung und Verbesserung der Qualität softwarebasierter Systeme und das Erkennen von Sicherheitslücken sind alle Software-Verantwortlichen gefragt: sowohl Architekten als auch Planer und Entwickler. Dafür müssen sie die Perspektive potenzieller Angreifer, ihre Motive und Methoden, aber auch die Sicht der Kunden kennen und berücksichtigen. Dieser Perspektivenwechsel bildet ein zentrales Element des Seminars »Secure Software Engineering«. Neben Motivation und Grundlagen der sicheren Softwareentwicklung liegt ein weiterer Schwerpunkt auf Secure Design, Coding sowie Software Security Tests.Darüber hinaus werden ein Ausblick in alle sicherheitsrelevanten Tasks des Lebenszyklus der Software gegeben sowie die unterschiedlichen Herausforderungen in verschiedenen Entwicklungsmethoden – etwa Agile oder Wasserfall-Entwicklung sowie die Integration in DevOps diskutiert.

INFORMATIONEN IM ÜBERBLICK

Kurs: Secure Software Engineering
Empfohlen sind:
- Erfahrung in der Software-Entwicklung sowie deren Methoden
- Kenntnisse zu Technologien wie Tomcat und Datenbanken
- Grundkenntnisse zur Programmiersprache Java

Dauer: 3 Tage in Präsenz
Kurssprache: Deutsch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort:
Brandenburg an der Havel
Termin: 15.–17.1., 14.–16.3. Brandenburg; 21.–23.2., 11.–14.5. Berlin
Kosten: 1800 €
Veranstaltet durch:

Technische Hochschule Brandenburg
University of Applied Sciences
Fachbereich Wirtschaft

UNSERE REFERENTEN

Marcel Niefindt
Doktorrand im Bereich Secure Software Engineering der TH Brandenburg sowie Manager Cyber Risk & Software Quality bei Deloitte

Sandro Hartenstein
Dozent für Secure System LifeCycle Management an der TH Brandenburg sowie freier IT-Security Analyst und Berater

Die Inhalte: Entwicklung, Testen und Warten von sicherer Software

Grundlagen sicherer Software
- Angreifer: Typ, Potenzial, Motivation
- Schutzziele: Unternehmenswerte, Compliance

Entwicklungsmethoden sicherer Software

Bedrohungsmodellierung
- Angriffsvektoren
- Risikoanalyse
- Maßnahmen
- Controls (Wirksamkeit)

Sicherer Software-Entwurf und Programmierung
- Schritte und Möglichkeiten für eine sichere Software-Architektur
- Vorgehen und Wege für sicheres Programmieren

Security Testing
- Besonderheiten von Sicherheitstests
- Penetrationtests

Wartung sicherer Software
- Response-Prozesse
- Security Incidents Handling (CERT)
- Kommunikationsstrategien

Die Zielgruppe: Alle Software-Verantwortlichen

Software-Architekten, Software-Entwickler, Software-Planer

Die Lernziele: Sichere Software umsetzen

Die Teilnehmenden verstehen Methoden und Techniken, um sichere Software zu entwerfen und in eigenen Projekten zu implementieren

Das Lernlabor Cybersicherheit: Weiterbildung für die IT-Sicherheitsexperten von morgen

Das Lernlabor Cybersicherheit ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT-Infrastruktur.

HABEN SIE NOCH FRAGEN ZU…

… sicherer Software-Entwicklung?

Marcel Niefindt | TH Brandenburg
marcel.niefindt@th-brandenburg.de

… Anmeldung, Organisation oder weiteren Angeboten?

Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de