Security by Design für Softwarearchitekten

Bedrohungen mit STRIDE analysieren, Sicherheitsrisiken bewerten und Architekturentscheidungen absichern

Beginn:
11.10.2027 - 09:00 Uhr

Ende:
12.10.2027 - 17:00 Uhr

Dauer:
2,0 Tage

Flex: Ostfildern oder Online

Veranstaltungsnr.: **36524.00.001**

Leitung

Frank Gräfe, M.Sc.

Präsenz oder Online
EUR 1.390,00
(MwSt.-frei)
Mitgliederpreis
EUR 1.251,00
(MwSt.-frei)

in Zusammenarbeit mit:

GESELLSCHAFT FÜR INFORMATIK

BESCHREIBUNG







Wie sicher ist eine Softwarearchitektur, wenn KI-Agenten eigenständig Code verändern, APIs aufrufen und Deployments über CI/CD-Pipelines auslösen? Vernetzte Anwendungen, Cloud-Dienste und automatisierte Prozesse schaffen zusätzliche Angriffsflächen, während unklare Vertrauensgrenzen und weitreichende Berechtigungen Sicherheitsrisiken erhöhen. Security by Design setzt deshalb bereits bei Architekturentscheidungen an und bildet einen Schwerpunkt im **TAE-Lernpfad Softwarearchitektur**.

Ziel der Weiterbildung
In dieser zweitägigen Weiterbildung erarbeiten Sie eine strukturierte Vorgehensweise, um Sicherheitsanforderungen frühzeitig in die Softwarearchitektur zu integrieren. Anhand eines durchgängigen Fallbeispiels mit einem KI-Assistenten und einer automatisierten CI/CD-Pipeline untersuchen Sie typische Angriffsflächen. Als Bestandteil des **TAE-Lernpfads Softwarearchitektur** vertieft das Seminar die sicherheitsorientierte Bewertung und Gestaltung von Softwarearchitekturen.

Nach der Weiterbildung können Sie:

- Schutzbedarf und Vertrauensgrenzen in vernetzten Softwarearchitekturen systematisch identifizieren.
- Bedrohungen mithilfe von Threat Modeling und STRIDE strukturiert analysieren.
- Klassische und KI-spezifische Sicherheitsrisiken anhand ihrer Auswirkungen priorisieren.
- Geeignete Sicherheitsmaßnahmen auswählen und Architekturentscheidungen als Architecture Decision Records (ADR) dokumentieren.
- Überprüfbare Sicherheitsanforderungen für Architektur- und Entwicklungsprozesse formulieren.

Nutzen der Weiterbildung

Die Weiterbildung erhöht die Sicherheit bei Architekturentscheidungen und unterstützt den frühzeitigen Umgang mit sicherheitskritischen Entwurfsproblemen. Dadurch lassen sich aufwendige nachträgliche Anpassungen reduzieren und Abstimmungen zwischen Architektur, Entwicklung und IT-Sicherheit gezielter gestalten. Ein persönlicher 30-Tage-Plan erleichtert die Übertragung der Ergebnisse in laufende Projekte.

PROGRAMM

Montag., 11. Oktober und Dienstag, 12. Oktober 2027
von 9:00 Uhr bis 17:00 Uhr (inkl. Pausen)

1. Security by Design – Grundlagen und Sicherheitsprinzipien

- Bedeutung von Security by Design und Secure by Default
- Sicherheitsziele: Vertraulichkeit, Integrität und Verfügbarkeit
- Bedrohungen, Schwachstellen und Risiken unterscheiden
- Sicherheitsanforderungen als Bestandteil des Architekturprozesses
- Zielkonflikte zwischen Sicherheit, Performance, Usability und Kosten

2. Schutzbedarfsanalyse und Systemmodellierung

- Schutzwürdige Werte (Assets) und kritische Systemkomponenten identifizieren
- Schutzbedarf systematisch ermitteln und dokumentieren
- Datenflussdiagramme und Vertrauensgrenzen erstellen
- Sicherheitsrelevante Schnittstellen und Abhängigkeiten erkennen
- Praxisübung: Schutzbedarfsanalyse einer vernetzten Softwareanwendung

3. Threat Modeling und Risikobewertung

- Threat Modeling als Methode zur systematischen Bedrohungsanalyse
- STRIDE: Bedrohungskategorien erkennen und anwenden
- Angreifermodelle und Missbrauchsszenarien entwickeln
- KI-spezifische Bedrohungen: Prompt Injection und übermäßige Agentenberechtigungen
- Risiken bewerten und priorisieren
- Praxisübung: Bedrohungsanalyse und Erstellung eines Risikoregisters

4. Sichere Softwarearchitekturen gestalten

- Sicherheitsprinzipien: Least Privilege, Defense in Depth, Fail Secure und Zero Trust
- Authentifizierung, Autorisierung und sichere Identitätsverwaltung
- Sicherheitsmechanismen: OAuth 2.0, OpenID Connect, mTLS und Secrets Management
- Sicherheitsanforderungen an APIs, Dienste und automatisierte Prozesse
- Architekturvarianten vergleichen und Sicherheitsmaßnahmen auswählen
- Restrisiken bewerten und Verantwortlichkeiten festlegen
- Praxisübung: Sicherheitsentscheidungen entwickeln und als Architecture Decision Records (ADR) dokumentieren

5. Sicherheitsanforderungen überprüfen und im Entwicklungsprozess verankern

- Überprüfbare Sicherheitsanforderungen formulieren
- Missbrauchsfälle (Misuse Cases) als Grundlage für Sicherheitsprüfungen
- Security Reviews und Bewertung von Architekturentscheidungen
- Sicherheitsanforderungen in Definition of Done und Entwicklungsprozesse integrieren
- Threat Modeling bei Architekturänderungen aktualisieren
- Security im Software-Lebenszyklus: Schwachstellenmanagement, Software-Lieferkette und sichere Updates
- Praxisübung: Gegenseitiges Architektur- und Security-Review

6. Vertiefung: Security by Design in industriellen Anwendungen

- Übertragung einer bestehenden Softwarearchitektur auf eine industrielle Edge-Umgebung
- Veränderte Schutzbedarfe, Bedrohungen und Risiken erkennen
- Besonderheiten beim Einsatz von KI-generiertem Steuerungscode
- Sicherheitsanforderungen an Freigabeprozesse und produktive Steuerungssysteme
- Einordnung von IEC 62443 und Maschinenverordnung
- Praxisübung: Delta-Analyse und Bewertung notwendiger Architekturänderungen

7. Praxistransfer – Security by Design in eigenen Projekten anwenden

- Eigene Softwarearchitektur oder bereitgestelltes Fallbeispiel strukturiert betrachten
- Schutzbedarf, kritische Datenflüsse und Vertrauensgrenzen identifizieren
- Wesentliche Bedrohungen und Risiken priorisieren
- Erste Sicherheitsmaßnahmen und Architekturentscheidungen ableiten
- Prüfmöglichkeiten und Restrisiken berücksichtigen
- Kollegialer Austausch und Feedback zu den entwickelten Ansätzen
- Persönlichen 30-Tage-Plan zur Umsetzung im Berufsalltag erstellen

Hinweis:
Die Übungen erfolgen anhand abstrahierter, anonymisierter oder bereitgestellter Fallbeispiele. Vertrauliche Unternehmens- und Projektdaten müssen nicht offengelegt werden. Ziel ist die methodische Anwendung und Entwicklung erster Verbesserungsansätze, nicht die vollständige Ausarbeitung eines projektspezifischen Sicherheitskonzepts.

TEILNEHMER:INNENKREIS

Die Weiterbildung richtet sich an Softwarearchitekten, Solution Architects, Senior

Softwareentwickler, Software Engineers und Technical Leads. Sie ist auch interessant für Cloud- und Backend-Entwickler mit Architekturverantwortung, Embedded-Softwareentwickler, Systemarchitekten sowie IT-Security-Fachkräfte mit Bezug zur Softwareentwicklung.

Als Bestandteil des **TAE-Lernpfads Softwarearchitektur** eignet sich das Seminar insbesondere für Fachkräfte, die ihre Architekturkompetenz um systematische Sicherheitsanalysen und sicherheitsorientierte Entwurfsentscheidungen erweitern möchten.

Hinweis: Grundkenntnisse der Softwarearchitektur sowie praktische Erfahrung mit verteilten oder vernetzten Anwendungen werden vorausgesetzt. Spezielle Security-Kenntnisse, Programmierarbeiten während des Seminars oder Kenntnisse der industriellen Steuerungstechnik sind nicht erforderlich.

REFERENT:INNEN

Frank Gräfe, M.Sc.

Frank Gräfe, M.Sc. ist Software Engineer mit über zehn Jahren Erfahrung in der professionellen Softwareentwicklung. Seit 2018 entwickelt er bei Festo mit C# und .NET Software für Anwendungen in Automatisierung und Robotik. Als Dozent an der DHBW Stuttgart vermittelt er zudem C#/.NET, objektorientierte Softwareentwicklung, Concurrent Programming sowie moderne Entwicklungspraktiken wie Clean Code und Test Driven Development. In seinen Schulungen verbindet er fundiertes Fachwissen mit langjähriger industrieller Praxiserfahrung.

Weitere Veranstaltungen

Aufbau Softwarearchitektur - Systeme gezielt modernisieren

VERANSTALTUNGSORT UND HOTEL

Technische Akademie Esslingen
An der Akademie 5
73760 Ostfildern



Anfahrt
Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.

Hotelübernachtung benötigt?

Über den nachfolgenden Link finden Sie nahegelegene Hotels in direkter Umgebung zu TAE-Konditionen:

Hotelbuchung

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet Verpflegung (vor Ort) sowie ausführliche Unterlagen.

Preis:
Die Teilnahmegebühr beträgt:
1.390,00 € (MwSt.-frei) vor Ort
1.390,00 € (MwSt.-frei) pro Teilnehmer live online

Fördermöglichkeiten:
Bei einem Großteil unserer Veranstaltungen profitieren Sie von 45 % Zuschuss aus der ESF-Fachkursförderung.
Bisher sind diese Mittel für den vorliegenden Kurs nicht bewilligt. Dies kann verschiedene Gründe haben. Wir empfehlen Ihnen daher, Kontakt mit unserer Anmeldung aufzunehmen. Diese gibt Ihnen gerne Auskunft über die Förderfähigkeit der Veranstaltung.

Weitere Bundesland-spezifische Fördermöglichkeiten finden Sie hier.

Inhouse Durchführung:
Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles Inhouse-Training an.

IMMER TOP!

Unser Qualitätsversprechen



Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?