

Sicherer Software Entwicklungsprozess – SDLC Fundamentals

In Kooperation mit dem SBA

Kick-start your Secure Software Development Lifecycle

- Softwaresicherheit ganzheitlich und steuerbar
- Sicherheit als Treiber für Softwarequalität
- OWASP SAMM – Reifegradmodell für Software-Security-Assurance
- Gängige Schwachstellenklassen und ihre automatisierte Testbarkeit

Inhalt

Die folgenden Themen werden beleuchtet:

- Einführung: Warum SDLC?
- Die wichtigsten Begriffe
- Anforderungsanalyse mit Sicherheitsfokus
- Gängige Anforderungen am Beispiel der DSGVO
- Sicheres Design und sichere Architektur
- Bedrohungsmodellierung (Threat Modeling)
- Security Design Patterns, die gängige Sicherheitsprobleme lösen
- Grundlegende Secure Coding Practices
- Sicherheit im Build- und Deploymentprozess
- Übersicht über Testarten mit Sicherheitsbezug
- Arten automatisierter Werkzeuge (SAST, DAST, IAST, Dependency-Checks)
- Die Vor- und Nachteile der jeweiligen Werkzeuge
- Gängige Schwachstellenklassen und ihre automatisierte Testbarkeit
- Schwachstellenmanagement
- Logging und Monitoring
- Incident-Management
- Konfigurationsmanagement
- Softwaresicherheit steuerbar und nachvollziehbar machen
- Weiterbildung und Guidance
- Compliance

Jeder der Teilbereiche (Governance, Design, Implementierung, Verifikation, Betrieb) wird wie folgt durchgenommen:

- Einführendes Beispiel aus der Praxis
- Theoretische Konzepte angereichert mit Beispielen
- Häufige Fallstricke bei der Anwendung
- Berührungspunkte mit dem OWASP SAMM
- Entwickler:innen-Checkliste für erste Aktivitäten
- Kurzes Quiz zum Thema

Kursziele

Wollten Sie immer schon wissen, wie man das Thema Softwaresicherheit ganzheitlich und steuerbar angeht? Würden Sie gerne Gesetzen und Regularien vorgehen, auch getrieben von Ihrer Kundschaft? Oder wollen Sie einfach das Thema Sicherheit als Treiber für Softwarequalität im Allgemeinen verwenden? Dann ist dieses eintägige Einführungstraining das Richtige für Sie. In diesem Training wird das Thema Softwaresicherheit aus verschiedenen Perspektiven beleuchtet, und zwar von Governancethemen bis hin zu technologielastrigen Themen wie Design, Entwicklung, Testen und Betrieb. Die Inhalte sind am OWASP SAMM ausgerichtet, einem Reifegradmodell für Software Security Assurance. Nutzen Sie dieses Training für einen Schnellstart Ihres sicheren Softwareentwicklungsprozesses, um das nächste Level der Softwaresicherheit zu erreichen und um das Vorhaben auch Stakeholdern darlegen zu können.

Zielgruppen

Dieser Kurs richtet sich an alle Personen, die in den Softwareentwicklungsprozess involviert sind.

- SoftwareentwicklerInnen
- IT-Projektverantwortliche
- CISOs
- SoftwaretesterInnen
- Scrum Masters
- Software-ArchitektInnen
- CTOs

Referenten

Andreas Boll is senior information security consultant at SBA Research.

Consulting Area: Andreas' consulting activities are focused on the technical aspects of information security.

He frequently conducts penetration tests on a wide range of computer systems, including:

- Web application security
- Mobile app security
- Infrastructure security
- Source Code Audits
- Architecture Review



Mathias Tausig is information security consultant at SBA Research.

Consulting Area: Mathias' consulting activities are focusing on web application penetration testing, threat modeling and teaching activities, mainly in the areas of Application Security and Secure Software Development. He is a regular speaker at security- and Open Source focused conferences (e.g. sec4dev, Linuxwochen, RIOT-OS Summit, CCC Easterhegg, Heise DevSec).

