CertNexus Cyber Secure Coder

Sicher entwickeln von Anfang an – Schutz für Ihre Anwendungen durch Security by Design und sichere Programmierung im gesamten

Seminar	4 Termine verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	24 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 29020 | Herstellernummer: CNX-CSC

Stand: 06.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29020

Die Bedeutung von Software-Sicherheit ist enorm – dennoch beschäftigen sich viele Entwicklungsteams erst mit dem Thema Sicherheit, nachdem der Code bereits geschrieben und die Software zur Auslieferung vorbereitet wird. Wie bei allen Aspekten der Softwarequalität gilt auch hier: Um eine erfolgreiche Umsetzung zu gewährleisten, sollten Sicherheits- und Datenschutzaspekte während des gesamten Softwareentwicklungsprozesses berücksichtigt werden.

Dieser Kurs vermittelt einen Ansatz, wie Sicherheits- und Datenschutzaspekte über den gesamten Softwareentwicklungszyklus hinweg behandelt werden können. Sie lernen Sicherheitslücken kennen, die die Sicherheit gefährden, und erfahren, wie Sie diese in Ihren eigenen Projekten erkennen und beheben können. Darüber hinaus lernen Sie allgemeine Strategien zum Umgang mit Sicherheitsmängeln und Fehlkonfigurationen kennen, wie man Software so gestaltet, dass der menschliche Faktor im Bereich Sicherheit berücksichtigt wird, und wie Sicherheit in alle Entwicklungsphasen integriert werden kann.

Nutzen

In diesem Kurs wenden Sie Best Practices in der Softwareentwicklung an, um sichere Software zu entwickeln.

Sie werden:

- den Bedarf an Sicherheit in Ihren Softwareprojekten erkennen.
- Schwachstellen in der Software beseitigen.
- einen Security by Design-Ansatz verwenden, um eine sichere Architektur für Ihre Software zu entwerfen.
- gängige Schutzmaßnahmen implementieren, um Benutzer und Daten zu schützen.
- verschiedene Testmethoden anwenden, um Sicherheitsmängel in Ihrer Software zu finden und zu beheben.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- ausgelieferte Software warten, um eine kontinuierliche Sicherheit zu gewährleisten.

Zielgruppe

Dieser Kurs richtet sich an Softwareentwickler, Tester und Architekten, die Software in verschiedenen Programmiersprachen und auf unterschiedlichen Plattformen – darunter Desktop, Web, Cloud und Mobile – entwerfen und entwickeln und ihre Fähigkeit verbessern möchten, qualitativ hochwertige Software zu liefern, insbesondere in Bezug auf Sicherheit und Datenschutz.

Der Kurs ist auch für Teilnehmende geeignet, die sich auf die Zertifizierungsprüfung **CertNexus Cyber Secure Coder (CSC), Exam CSC-210** vorbereiten möchten.

Voraussetzungen

Dieser Kurs vermittelt Konzepte der sicheren Programmierung, die für viele verschiedene Arten von Softwareentwicklungsprojekten relevant sind. Auch wenn in diesem Kurs Python®, HTML und JavaScript® verwendet werden, um verschiedene Programmierkonzepte zu veranschaulichen, ist keine Erfahrung in diesen Programmiersprachen erforderlich, um von diesem Kurs zu profitieren. Sie sollten jedoch über grundlegende Programmiererfahrung verfügen – sei es in der Entwicklung von Desktop-, Mobile-, Web- oder Cloud-Anwendungen. Logical Operations bietet eine Vielzahl von Kursen zur Softwareentwicklung an, mit denen Sie sich auf diesen Kurs vorbereiten können, zum Beispiel:

- Python® Programming: Introduction
- Python® Programming: Advanced
- HTML5: Content Authoring with New and Advanced Features
- SQL Querying: Fundamentals (Second Edition)

Inhalte des Seminars

Lektion 1: Ermittlung des Sicherheitsbedarfs in Ihren Softwareprojekten

- Thema A: Sicherheitsanforderungen und -erwartungen identifizieren
- Thema B: Faktoren identifizieren, die die Softwaresicherheit untergraben
- Thema C: Schwachstellen in Ihrer Software finden
- Thema D: Informationen über Schwachstellen und Exploits sammeln

Lektion 2: Umgang mit Schwachstellen

- Thema A: Umgang mit Schwachstellen aufgrund von Softwarefehlern und Fehlkonfigurationen

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Thema B: Umgang mit Schwachstellen aufgrund menschlicher Faktoren
- Thema C: Umgang mit Schwachstellen aufgrund von Prozessmängeln

Lektion 3: Sicherheitsorientiertes Design

- Thema A: Allgemeine Prinzipien für sicheres Design anwenden
- Thema B: Software entwerfen, um spezifischen Bedrohungen entgegenzuwirken

Lektion 4: Entwicklung sicherer Software

- Thema A: Best Practices für sicheres Programmieren befolgen
- Thema B: Plattformbedingte Schwachstellen verhindern
- Thema C: Datenschutzbedingte Schwachstellen verhindern

Lektion 5: Umsetzung gängiger Schutzmaßnahmen

- Thema A: Zugriff durch Login und Benutzerrollen beschränken
- Thema B: Daten beim Transport und bei der Speicherung schützen
- Thema C: Fehlerbehandlung und Protokollierung implementieren
- Thema D: Sensible Daten und Funktionen schützen
- Thema E: Datenbankzugriffe absichern

Lektion 6: Testen der Softwaresicherheit

- Thema A: Sicherheitstests durchführen
- Thema B: Code analysieren, um Sicherheitsprobleme zu finden
- Thema C: Automatisierte Testwerkzeuge einsetzen, um Sicherheitsprobleme zu erkennen

Lektion 7: Aufrechterhaltung der Sicherheit in ausgelieferter Software

- Thema A: Anwendungen überwachen und protokollieren zur Unterstützung der Sicherheit
- Thema B: Sicherheit nach der Bereitstellung aufrechterhalten

Anhang A: Zuordnung der Kursinhalte zur Cyber Secure Coder-Zertifizierung (Prüfung CSC-210)

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29020 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.