

DevSecOps

Ziel und Nutzen

Nach diesem Kurs wirst du Sicherheit erfolgreich in deine DevOps-Prozesse integrieren und eine umfassende DevSecOps-Kultur etablieren können. Du erwirbst praktische Fertigkeiten zur Implementierung automatisierter Sicherheitstests, Container-Scanning und Vulnerability Management. Von Static Code Analysis über SBOM-Generierung bis hin zu Kubernetes Policy Management - du lernst, Sicherheit als integralen Bestandteil deiner CI/CD-Pipelines zu implementieren.

Durch praxisnahe Übungen und realistische Szenarien entwickelst du die Kompetenz, sichere Container-Images zu erstellen, Deployment-Konfigurationen zu scannen und automatisierte Security Issue Tracking zu implementieren. Du beherrschst den Shift-Left-Ansatz und kannst sowohl traditionelle als auch moderne Sicherheitstools effektiv einsetzen.

Zielpublikum

Dieser Kurs richtet sich an DevOps Engineers, Software-Entwickler, Systemadministratoren und Security Engineers, die Sicherheit erfolgreich in ihre CI/CD-Pipelines integrieren möchten.

Inhalt

Workshop bei [Letsboot](#).

In diesem Workshop lernst du, wie du Sicherheit nahtlos in deine DevOps-Prozesse integrierst und eine umfassende DevSecOps-Kultur in deinem Team etablierst. Du wirst praktische Techniken zur Automatisierung von Sicherheitstests, Container-Scanning und Vulnerability Management kennenlernen.

Dank hands-on Übungen und realen Szenarien entwickelst du die Fähigkeit, sichere CI/CD-Pipelines zu implementieren und Sicherheitsrisiken frühzeitig zu erkennen.

Wir beginnen mit den DevSecOps-Grundlagen und vertiefen uns dann in fortgeschrittene Themen wie Container-Sicherheit, Policy Management und automatisierte Compliance-Checks.

Voraussetzungen

Grundlegende Kenntnisse in DevOps-Praktiken und CI/CD-Pipelines.

Erfahrung mit Git, Docker und grundlegende Linux-Kenntnisse.

Laptop mit lokalen Installationsrechten empfohlen.