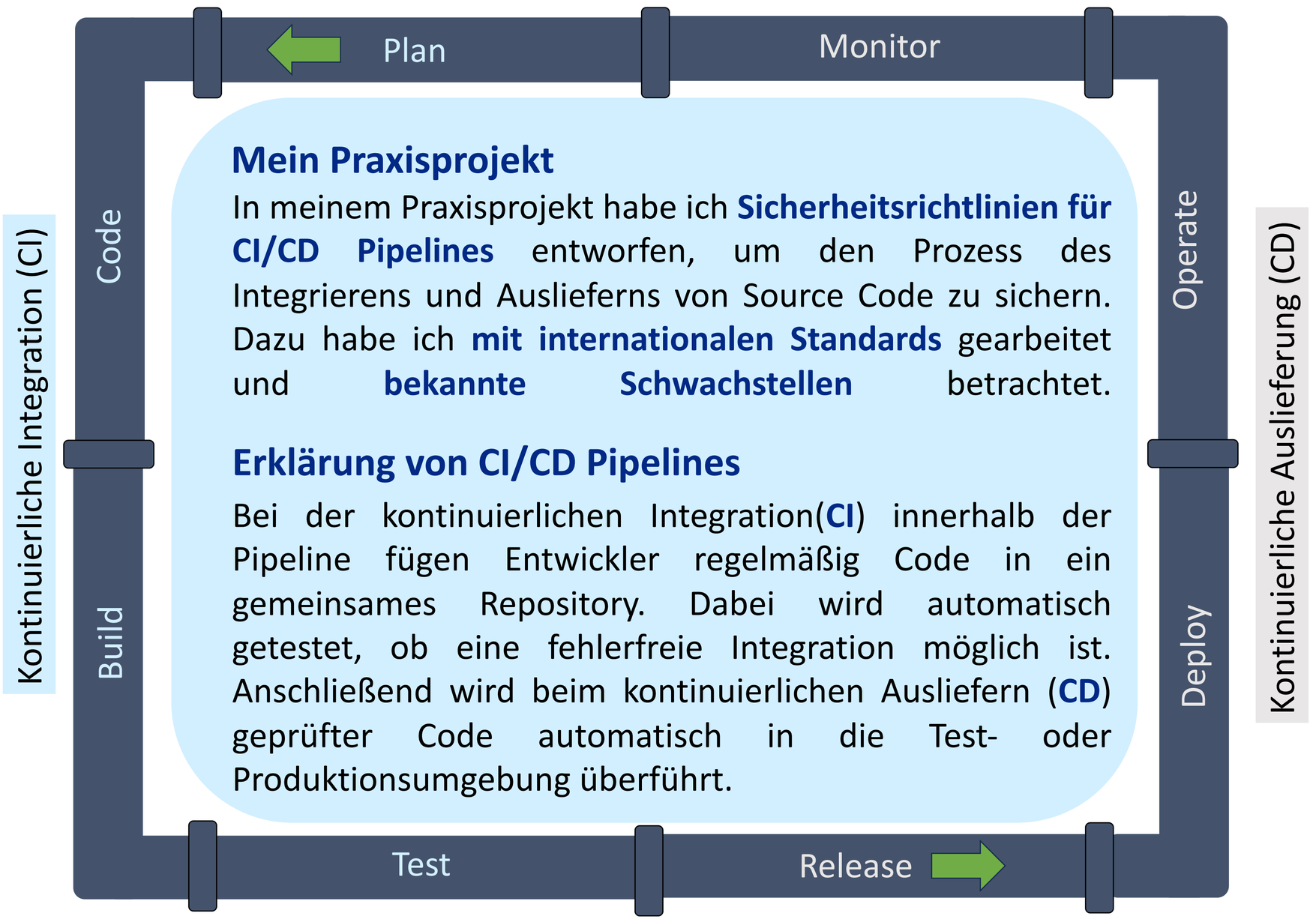
Sicherheitsrichtlinien für CI/CD Pipelines



Mein Praxisprojekt

In meinem Praxisprojekt habe ich **Sicherheitsrichtlinien für CI/CD Pipelines** entworfen, um den Prozess des Integrierens und Auslieferns von Source Code zu sichern. Dazu habe ich **mit internationalen Standards** gearbeitet und **bekannte Schwachstellen** betrachtet.

Erklärung von CI/CD Pipelines

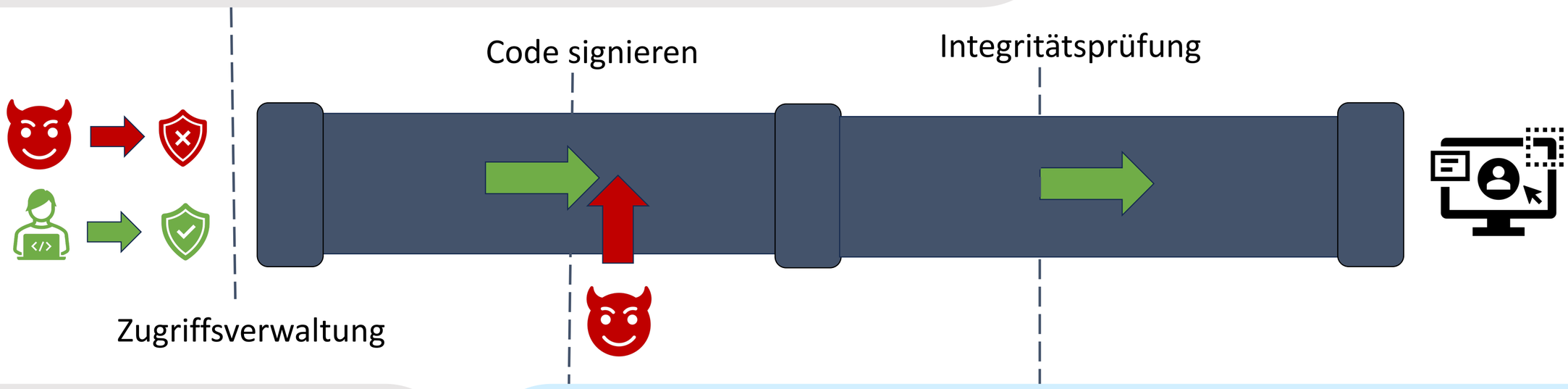
Bei der kontinuierlichen Integration(**CI**) innerhalb der Pipeline fügen Entwickler regelmäßig Code in ein gemeinsames Repository. Dabei wird automatisch getestet, ob eine fehlerfreie Integration möglich ist. Anschließend wird beim kontinuierlichen Ausliefern (**CD**) geprüfter Code automatisch in die Test- oder Produktionsumgebung überführt.

Motivation

CI/CD Pipelines sind weit verbreitet in der Softwareentwicklung. Sie ermöglichen es, Codeänderungen **schnell und zuverlässig** auszuliefern. Doch mit dieser Automatisierung entstehen auch **Sicherheitsrisiken**, die gezielt ausgenutzt werden können – von ungeprüften Code Auslieferungen bis hin zu unsicheren Zugriffskontrollen**.** Um **Angreifern** diese Möglichkeiten **zu verwehren**, ist es wichtig, konkrete Sicherheitsrichtlinien zu formulieren, an die sich Entwicklerteams halten sollten.

Internationale Standards - Beispiel

Aus einem NIST Standard lassen sich unter anderem Richtlinien zur **Zugriffsverwaltung** ableiten. Ein Angriffsszenario, welches dabei verhindert werden soll, könnte sein, dass ein Angreifer versucht, Schadcode in die Pipeline einzuschleusen. Dies könnte er versuchen, indem er den normalen Prozess durchführt, den auch Mitarbeiter durchführen. Eine Zugriffsverwaltung und dazugehörige Identitätsprüfung verhindern einen solchen Angriff.



Projektmanagement

Das Projekt wurde durch ein Sicherheitsteam **initiiert** und wird in Zusammenarbeit mit Entwicklungsteams, welche für die Umsetzung verantwortlich sind, **gesteuert**. Ebenso wird von diesen und weiteren Verantwortlichen die **Qualitätssicherung** gewährleistet.

Bekannte Schwachstellen – Beispiel

Eine der OWASP Top 10 Sicherheitsrisiken für CI/CD ist die fehlende **Überprüfung der Artefakt-Integrität**. Wird ein Artefakt beim Erstellen signiert, kann vor der Ausführung geprüft werden, ob eine gültige Signatur vorliegt. Ist dies der Fall, wurde der Code nicht manipuliert und darf in die Produktion überführt werden. Konkrete Sicherheitsrichtlinien zum Signieren von Code und entsprechender Integritätsprüfung sind daher wichtig.

Mia Fuchs

h_da hochschule darmstadt informatik
member of EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY
SAP

Praxisprojekt 2
Informatik Dual
2025

Gruppe A