

Know-how to go

Sicherheit in der Softwareentwicklung

Security by Design – Sicherheit im gesamten Softwareentwicklungsprozess

Nina Malkomes

Nina Malkomes



- Fachliche Schwerpunkte: Agile Skalierung & Transformation, Einführung und Gestaltung von DevOps-Prozessen
- Planung, Steuerung und Durchführung von IT-Projekten sowie Erfahrung im Programmmanagement
- Aktuelles Projekt: Konzeption und Einführung einer CI/CD-Landschaft in eine bestehende IT-Infrastruktur inklusive Toolauswahl unter Berücksichtigung von DevOps-Ansätzen

Ausgangslage & Motivation



Situation

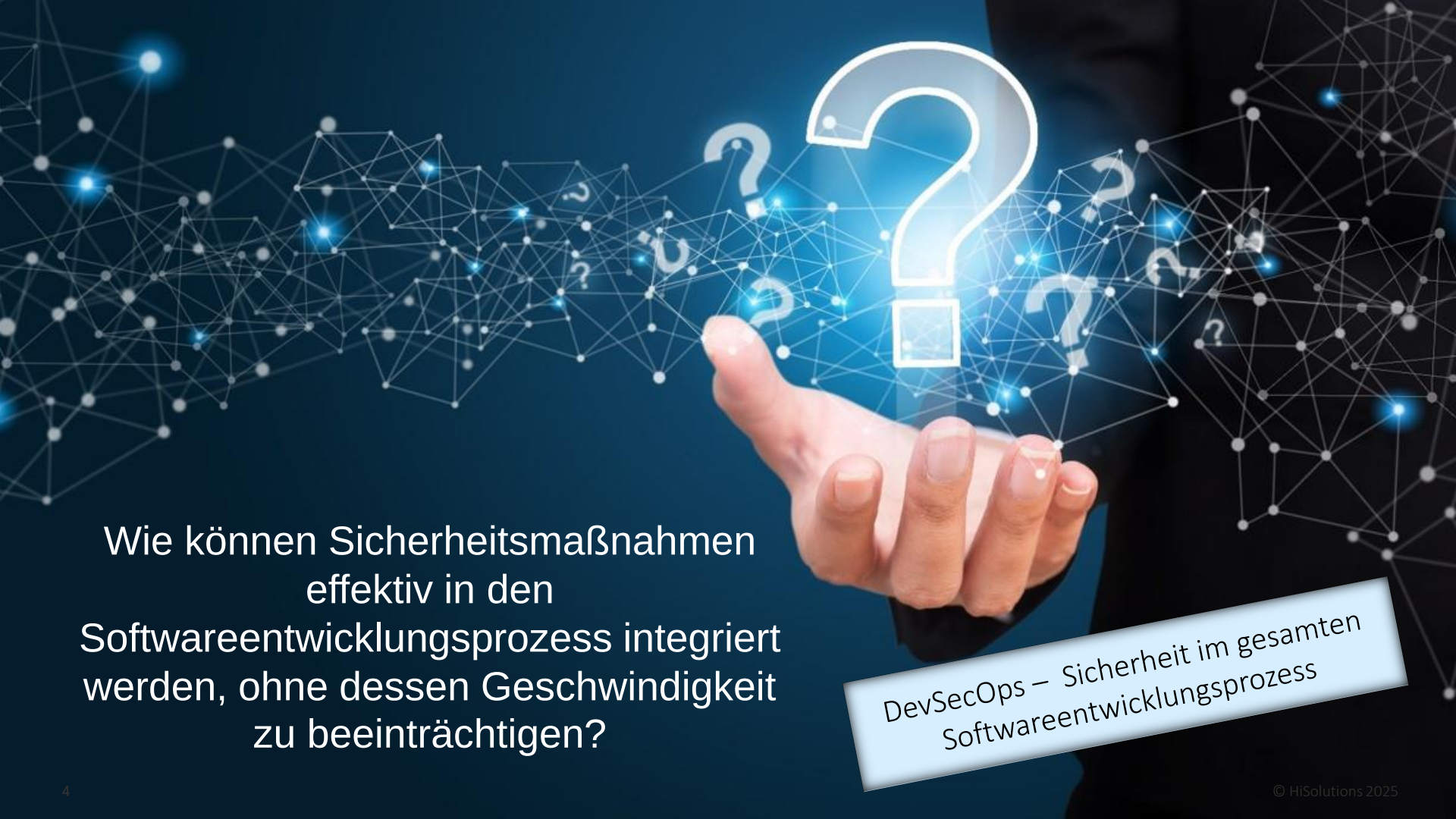
Das Thema Sicherheit in der Softwareentwicklung beschäftigt aufgrund der aktuellen Lage so gut wie jede IT-Organisation.



Complication

Viele Organisationen stehen vor großen Herausforderungen, frühzeitige Sicherheitsmaßnahmen in ihren Softwareentwicklungsprozess zu integrieren:

- Software wird immer öfter Zielscheibe von Cyberangriffen
- Anwendung von Open-Source-Bibliotheken und unbekannte Abhängigkeiten
- Schnelle Entwicklungs- und Release-Zyklen erfordern einen hohen Automatisierungsgrad
- Mangel an automatisierten (und manuellen) Sicherheitstests
- Sicherheit wird oft als nachträglicher Schritt betrachtet



Wie können Sicherheitsmaßnahmen
effektiv in den
Softwareentwicklungsprozess integriert
werden, ohne dessen Geschwindigkeit
zu beeinträchtigen?

DevSecOps – Sicherheit im gesamten
Softwareentwicklungsprozess

DevSecOps ebnet die Grundlage für sichere Softwareentwicklung

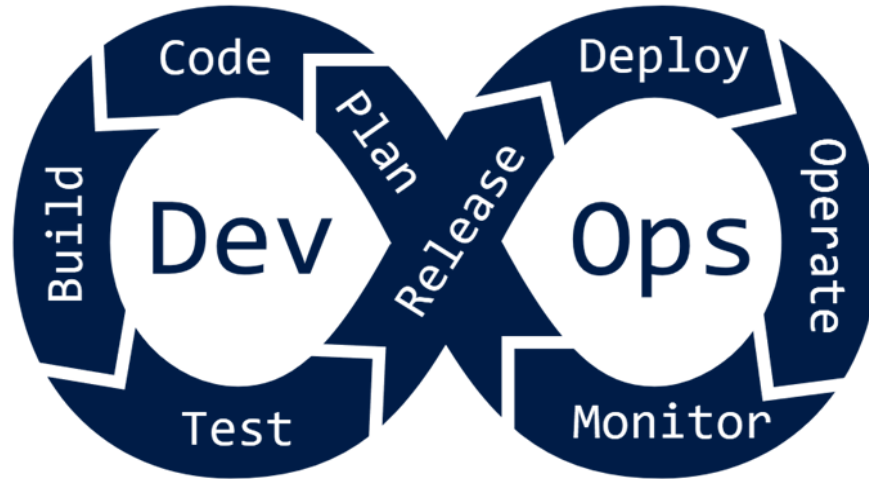


DevSecOps umfasst einen ganzheitlichen Ansatz in der Softwareentwicklung, der Sicherheit als integralen Bestandteil des Entwicklungs- und Betriebsprozesses betrachtet.

Zielsetzung:

-  Sicherheit in der Softwareentwicklung risikoorientiert und kontinuierlich verbessern
-  Mit einem ganzheitlichen Ansatz, sowohl technisch als auch organisatorisch, die vorhandenen Risiken geeignet mitigieren
-  Definition von Regeln, Methoden und Automatisierung, mit denen sich Sicherheit von Anfang an sicherstellen lässt

Softwareentwicklung meets DevSecOps



Automatische
Sicherheitsscans

Collaboration
zwischen
Teams

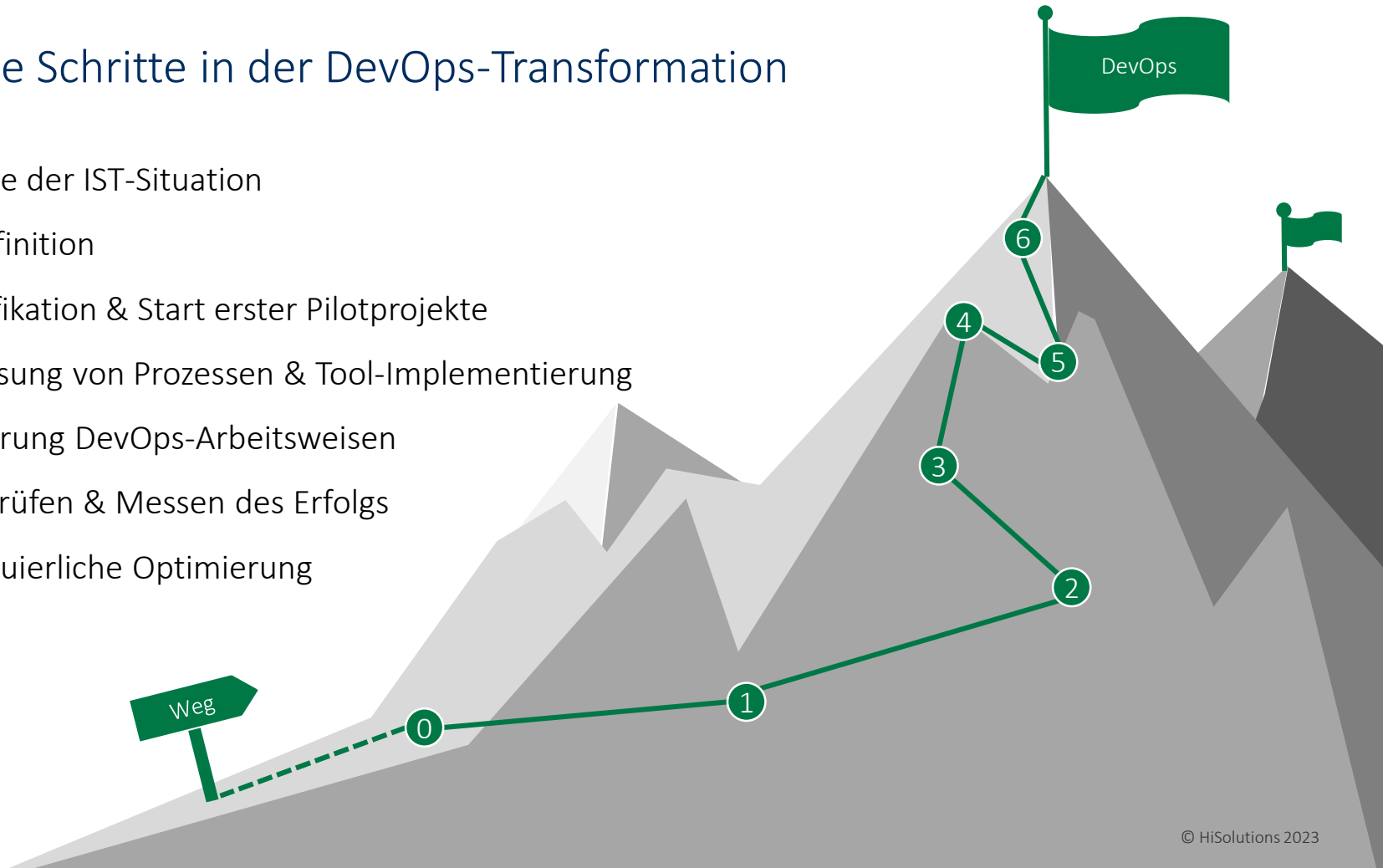
Shift-Left
Security

Continuous Monitoring
& Incident Response

Kontinuierliche
Einbindung
von Security

Typische Schritte in der DevOps-Transformation

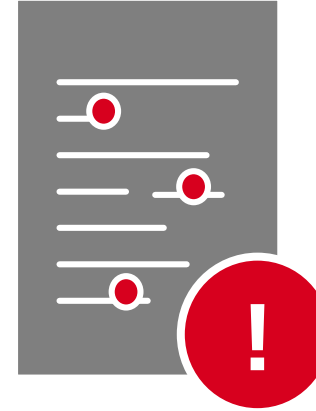
- 0 Analyse der IST-Situation
- 1 Zieldefinition
- 2 Identifikation & Start erster Pilotprojekte
- 3 Anpassung von Prozessen & Tool-Implementierung
- 4 Einführung DevOps-Arbeitsweisen
- 5 Überprüfen & Messen des Erfolgs
- 6 Kontinuierliche Optimierung



Dos and Don'ts in der Transformation



- Einen Scope festlegen
- Technische Schulden vor dem Start begleichen
- Maximale Teamgrößen festlegen
- Mit Prototypen & Experimenten arbeiten



- Eine DevOps-Transformation on Top zu anderen Themen starten
- Eine „Big Bang“-Transformation starten
- Feste Teams vorgeben
- Lange Freigabeprozesse & viele Restriktionen

Compliance & Kultur



Sicherheitsvorgaben

Automatisierte Security Scans

Security by Design

Automatisierung als Standard: Reduktion manueller Prozesse

Continuous Learning

Security Awareness als fester Bestandteil

Regulatorische Vorgaben nach Branche

DevSecOps in unserem Alltag & Ausblick

DevSecOps in unseren Projekten

- Cross-funktionale Teams mit Expertise aus verschiedenen Bereichen
- Security Awareness in allen Beratungsteams

Coming soon (in den nächsten Vorträgen):

Einblicke entlang des Softwareentwicklungsprozesses mit den Themen **DevSecOps, Softwareentwicklung, Umgang mit Security-Themen**

... beleuchtet aus unterschiedlichen Ecken:

- Anforderungsanalyse & Design
- Implementierung & Testing
- Betrieb & Wartung

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com