carmasec

security. done. right.


# DevSecOps & Security Automation:

## Agile Sicherheit und pragmatische Lösungsansätze

**Carsten Marmulla**

Internet Security Days, Phantasialand Brühl, 26.09.2019

# Steckbrief Referent

***Carsten Marmulla***

*Managing Partner &*
*Senior Trusted Advisor*

**Skills und Themenschwerpunkte**:

- 20 Jahre IT-Branchenerfahrung (Projekt-management- und IT-Beratungserfahrung)
- Zertifizierungen: Certified Information Security Manager (CISM), ITIL v3, ISO 27001 Auditor (ISMS), COBIT-Practitioner, PRINCE2-Practitioner, ...
- Informationssicherheitsmanagement (ISO 27001, BSI IT-Grundschutz)
- IT-Servicemanagement gemäß ITIL v3
- IT-Sicherheit & Datenschutz
- IT-GRC: IT-Governance, IT-Risikomanagement, IT-Compliance

**Projekterfahrungen (Auszug):**

- Aufbau und Optimierung von IT-Servicemanagementprozessen
- Erstellung von Sicherheitskonzepten; Schutzbedarfsfeststellungen; Organisatorische Reifegradermittlung; Durchführung von Schwachstellen-/ Risiko- und Business Impact Analysen (BIA); Identifizierung und Steuerung der Maßnahmen
- Definition von Prozessen für Informations-, IT-Sicherheit sowie Datenschutz, Erstellung von Informationssicherheitsrichtlinien, Festlegung, Einführung und Kontrolle der Sicherheitspolitik und Sicherheitsstrategie
- Konzeption, Aufbau und Einführung von Managementsystemen für Informationssicherheit gemäß ISO 27001 und Zertifizierungsvorbereitung; Konzeption und Implementierung von Kennzahlensystemen (KPI)
- Optimierung der IT-Wertschöpfung im Rahmen der IT-Governance (COBIT); Überprüfung der Einhaltung der IT-Compliance und der Datenschutzanforderungen

**Referenzkunden (Auszug)**:

- Deutsche Post AG
- Postbank Systems AG
- Vodafone Group Services GmbH
- Deutsche Telekom AG
- Vodafone D2 GmbH
- DeTeAccounting GmbH
- Fresenius Netcare GmbH
- TÜV Rheinland AG
- OXEA GmbH
- Grünenthal GmbH
- ProActiv Service GmbH (Talanx)
- Hochtief Concessions GmbH

# Leistungsangebot

carmasec

**Information Security Management**
Wegweisende Konzepte auf Basis langjähriger Expertise und Best-Practise.

**Security Automation**
Automatisierte Lösungen für das Security Management in agilen Entwicklungsprozessen und im Incident Response.

**Data Privacy Protection**
Evaluation relevanter Datenschutzvorgaben und Sicherstellung der Compliance (z.B. BDSG und DSGVO).

**Governance, Risk, Compliance**
Beratung des Managements im GRC Kontext auf Basis der spezifischen Anforderungen.

**Agile Security**
Integration des agilen Software Development Lifecycle in das vorhandene Security Management (Secure SDLC).

**Cyber Resilience**
Schutz vor Cyber Attacken und Steigerung der Widerstandskraft gegen Angriffe auf die Informationssicherheit.

**Business Continuity**
Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs nach Security Incidents.

**DevSecOps**
Transformation zu DevSecOps durch geräuschlose Integration von Security Controls in die DevOps und CI/CD Pipeline.

**Security Research**
Evaluation aktueller Security Entwicklungen und neuartiger Angriffsszenarien sowie Ableitung von Abwehrstrategien.

carmasec

*„There are only two types of companies:*
*those, that have been hacked,*
*and those, who don’t know,*
*they have been hacked.“*

—

*John T. Chambers*

# DevSecOps – warum eigentlich?

carmasec

- Unternehmen unterliegen globalem Wettbewerbsdruck
- Innovative Technologieansätze im Rahmen der Digitalen Transformation versprechen...
  - Effizienzgewinne,
  - höhere Umsetzungsgeschwindigkeit,
  - Kostenreduktion,
  - neue (datengetriebene) Geschäftsmodelle.

# DevSecOps – warum eigentlich?

carmasec

- Digitale Transformation ist in erster Linie:

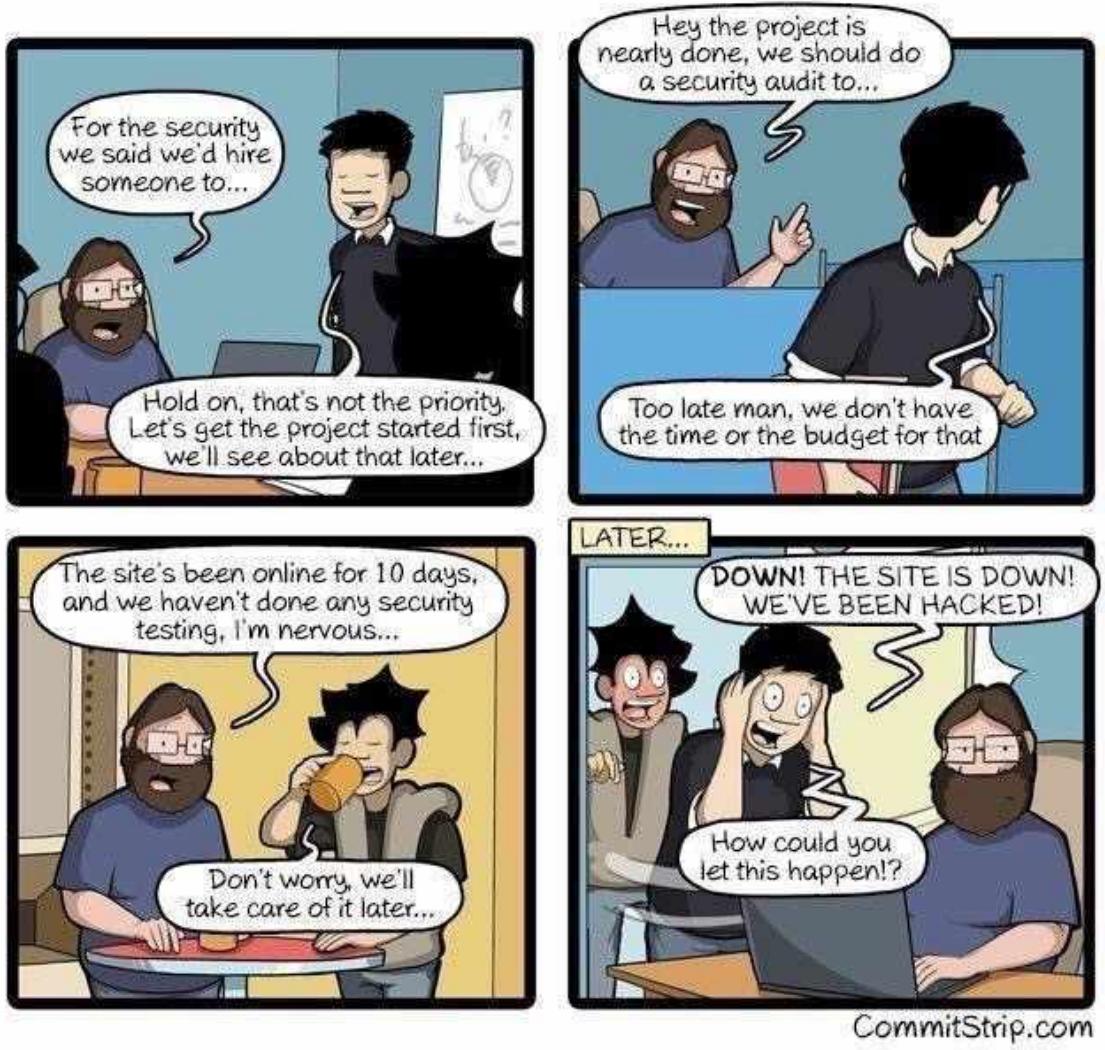
  Gesamtheitlicher Veränderungsprozess (Change Management)

- Primär zu definieren:
  - Zweck (Motivation) und
  - Ziel (Erwartung)
- Nicht ausschließlich Technologiewandel

# DevSecOps – Status Quo?

carmasec

# INNOVATION?


For the security we said we'd hire someone to...
Hold on, that's not the priority. Let's get the project started first, we'll see about that later...
Hey the project is nearly done, we should do a security audit to...
Too late man, we don't have the time or the budget for that
The site's been online for 10 days, and we haven't done any security testing, I'm nervous...
Don't worry, we'll take care of it later...
LATER...
DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!
How could you let this happen!?
CommitStrip.com

carmasec

# DevSecOps – Status Quo

carmasec

# DevSecOps – Paradigmenwechsel

carmasec

1. Infrastrukturwandel:

   „On-Premise“ (Rechenzentrum) → Cloud Services

2. Entwicklungs- und Releasemethodik:

   Klassische Releaseplanung → Agile Methoden

3. Änderung der „Enterprise Architecture“:

   Multi-Tier-Architekturen → Microservices / Container / Serverless

# DevSecOps – Paradigmenwechsel

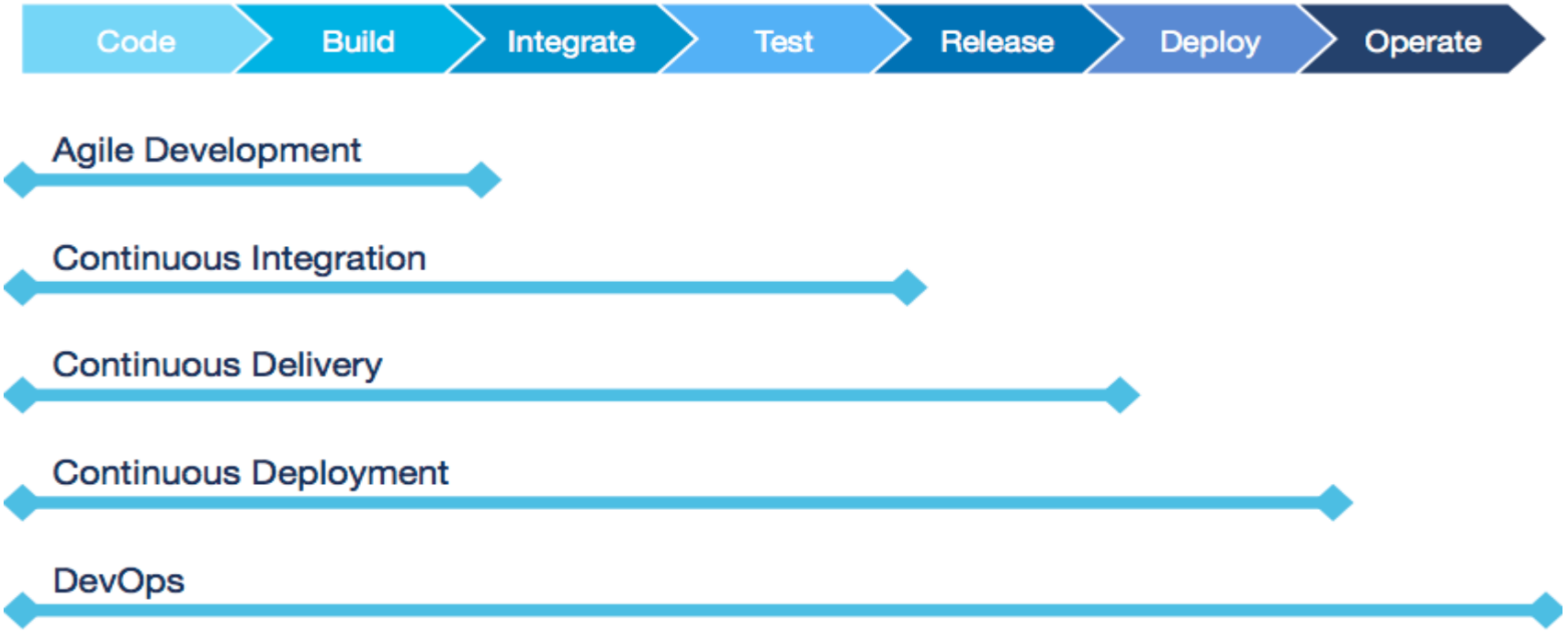
carmasec

## „Heutezutage ist alles Code.“

- Software-defined networking (inkl. Switches, Gateways/Firewalls)
- Software-defined storage
- ...
- „Infrastructure as Code“ (e.g. Terraform)

# Dev(Sec)Ops – Wo ist die Sicherheit?

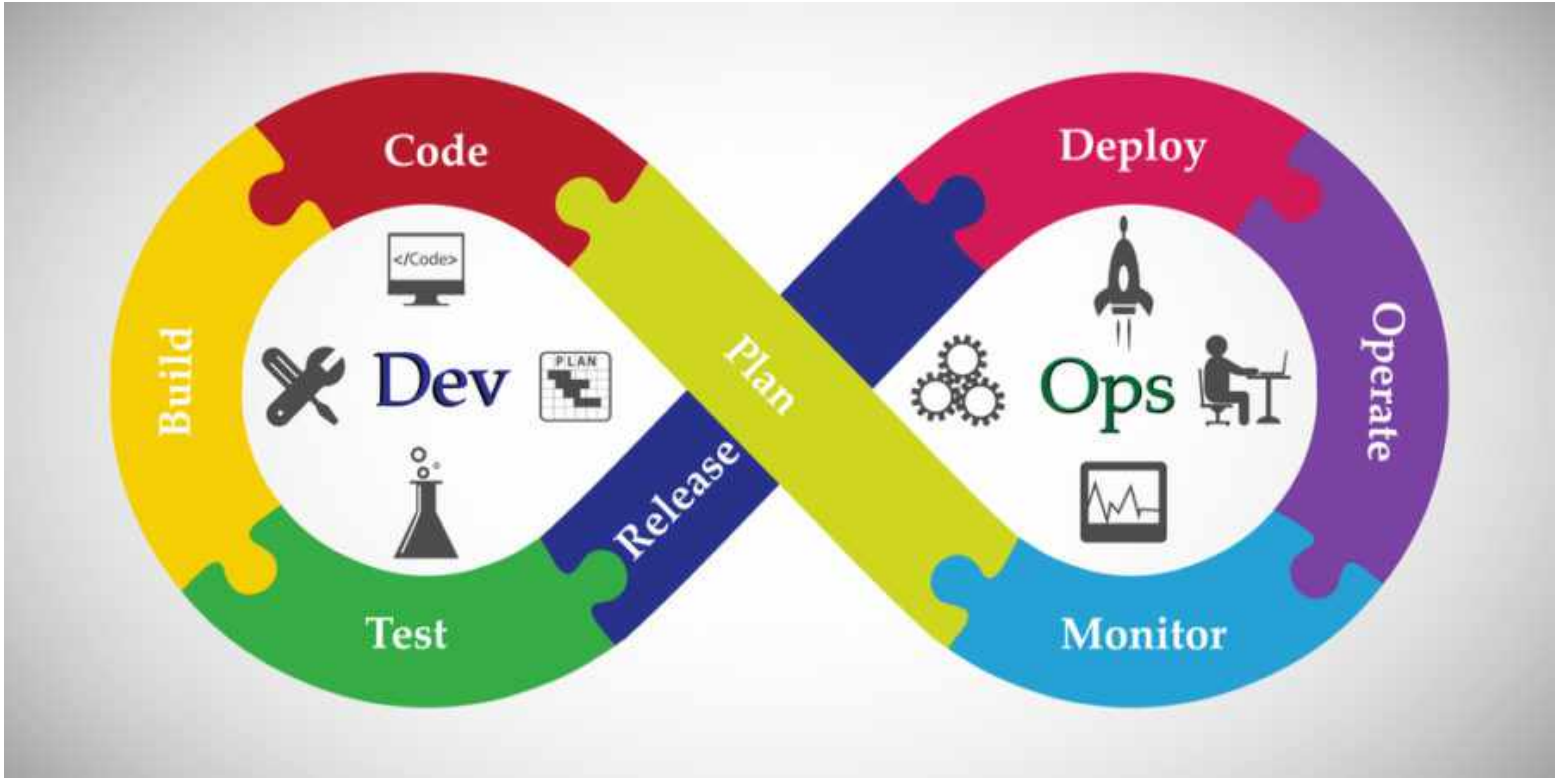
carmasec




Quelle: http://skillslane.com/continuous-integration-delivery-deployment/

# Dev(Sec)Ops – Wo ist die Sicherheit?

carmasec




Quelle: https://www.tigera.io/wp-content/uploads/2018/12/shutterstock_1213223074-900x.jpg

carmasec

*“With great power comes great responsibility!“*

—

*Voltaire*

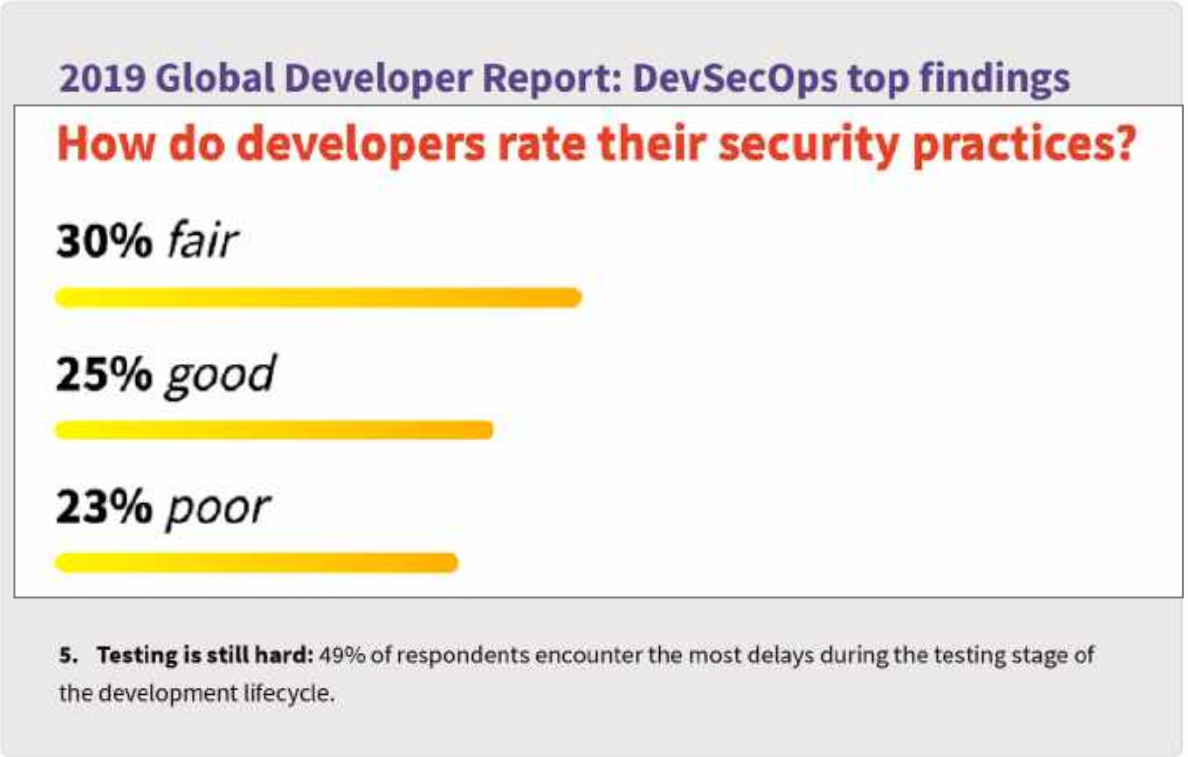
# DevSecOps – Agile Security

carmasec

- Was bedeutet das für “Security“?
  - Geschwindigkeitsanforderung steigt
  - Perimetersicherheit funktioniert nicht mehr (uneingeschränkt)
  - Penetrationstests allein helfen nicht mehr
  - Prozesse müssen flexibel und dynamisch werden
  - Bewegliche Zielarchitektur (volatile Infrastruktur, „moving target“)
  - Klassisches „Patch Management“ uneffizient
  - Standardisierung und Automatisierung notwendig

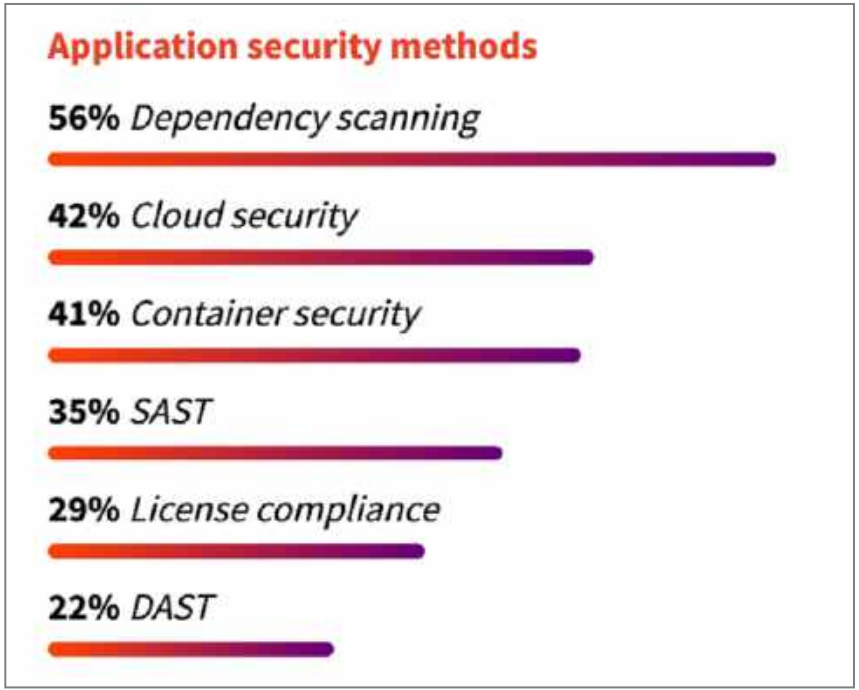
# DevSecOps – GitLab Global Developer Report

carmasec




Quelle: https://about.gitlab.com/developer-survey/2019/

# DevSecOps – GitLab Global Developer Report




Quelle: https://about.gitlab.com/developer-survey/2019/

# DevSecOps – OWASP Top 10 (2013 vs. 2017)

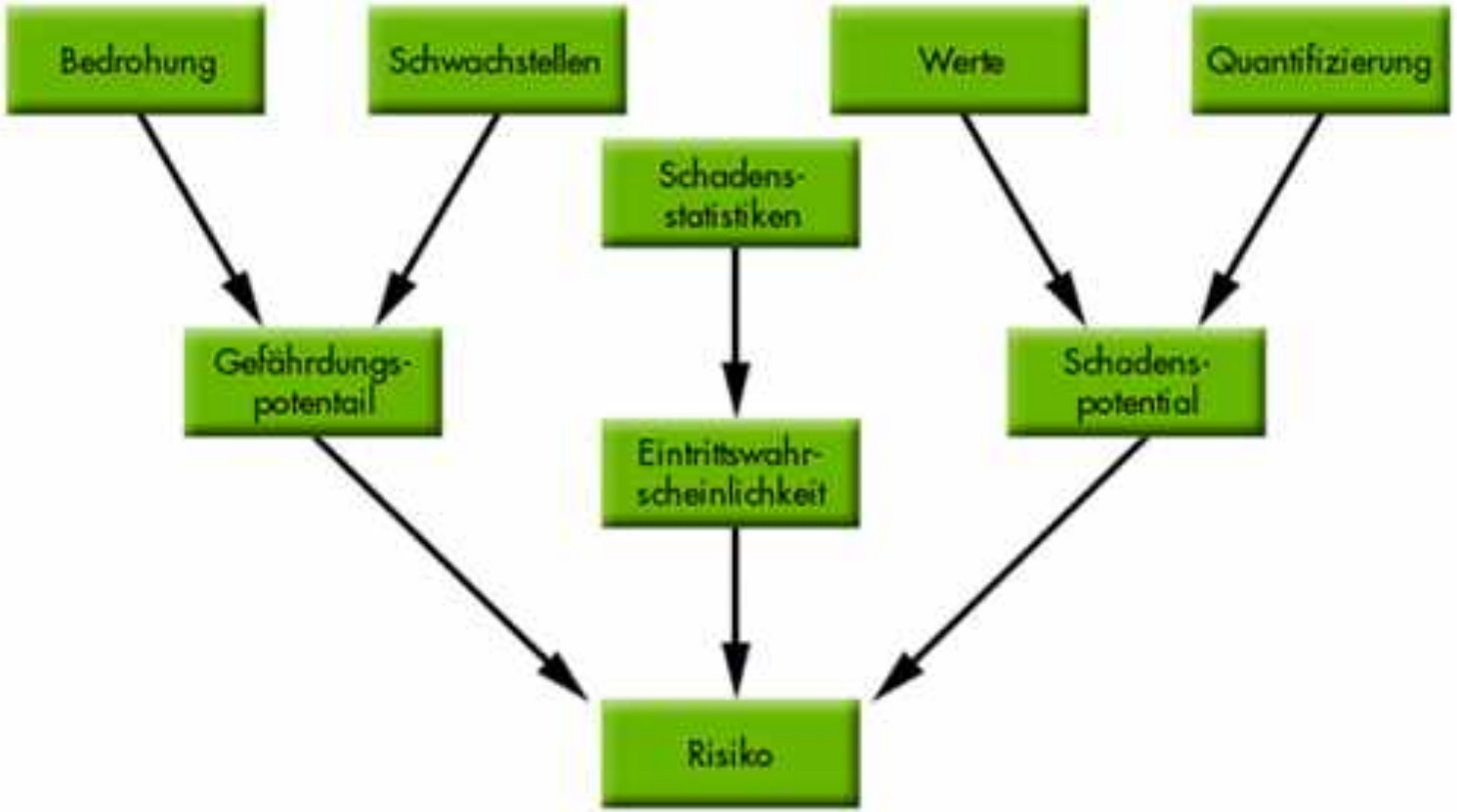
carmasec

| OWASP Top 10 - 2013 | → | OWASP Top 10 - 2017 |
|---|---|---|
| A1 – Injection | → | A1:2017-Injection |
| A2 – Broken Authentication and Session Management | → | A2:2017-Broken Authentication |
| A3 – Cross-Site Scripting (XSS) | ↘ | A3:2017-Sensitive Data Exposure |
| A4 – Insecure Direct Object References [Merged+A7] | U | A4:2017-XML External Entities (XXE) [NEW] |
| A5 – Security Misconfiguration | ↘ | A5:2017-Broken Access Control [Merged] |
| A6 – Sensitive Data Exposure | ↗ | A6:2017-Security Misconfiguration |
| A7 – Missing Function Level Access Contr [Merged+A4] | U | A7:2017-Cross-Site Scripting (XSS) |
| A8 – Cross-Site Request Forgery (CSRF) | ☒ | A8:2017-Insecure Deserialization [NEW, Community] |
| A9 – Using Components with Known Vulnerabilities | → | A9:2017-Using Components with Known Vulnerabilities |
| A10 – Unvalidated Redirects and Forwards | ☒ | A10:2017-Insufficient Logging&Monitoring [NEW,Comm.] |

Quelle: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

# DevSecOps – Was ist eigentlich ein Risiko?

carmasec



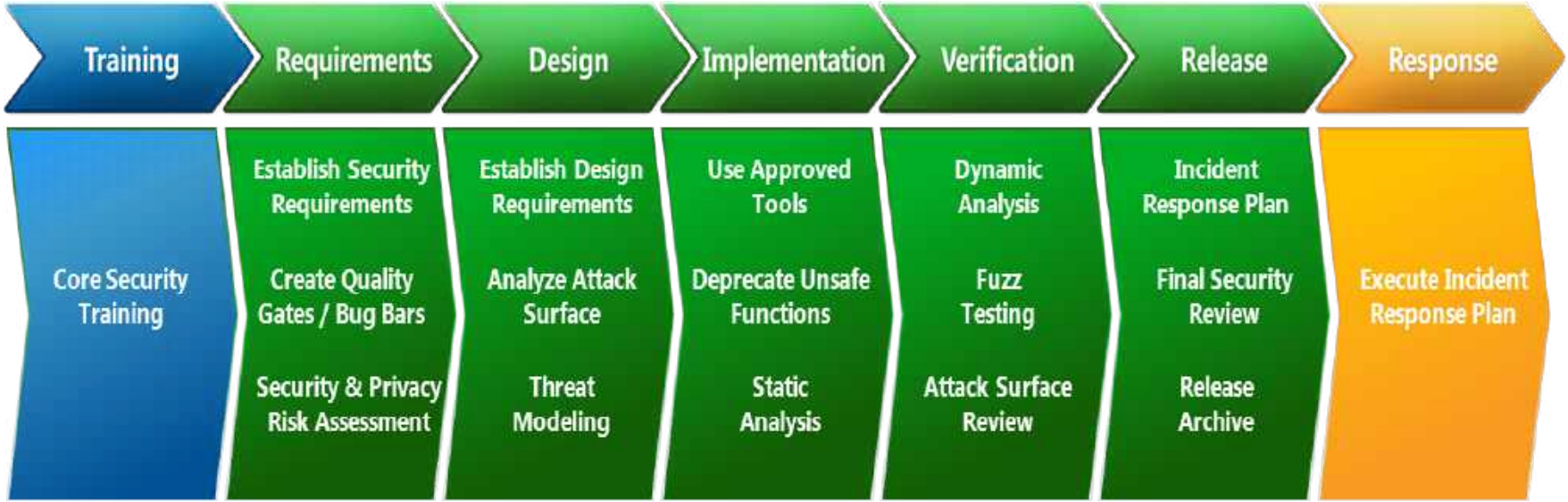
# DevSecOps – Methodik

carmasec

- „Shift Left“-Ansatz
- Dev(Sec)Ops-Methodik
- Statische/Dynamische Code Analyse (SAST/DAST)
- (Secure) Software Development Lifecycle (SDLC/SSDLC)
- Continuous Security Monitoring
- Security Orchestration, Automation & Response (SOAR)
- ...

# DevSecOps – Methodik

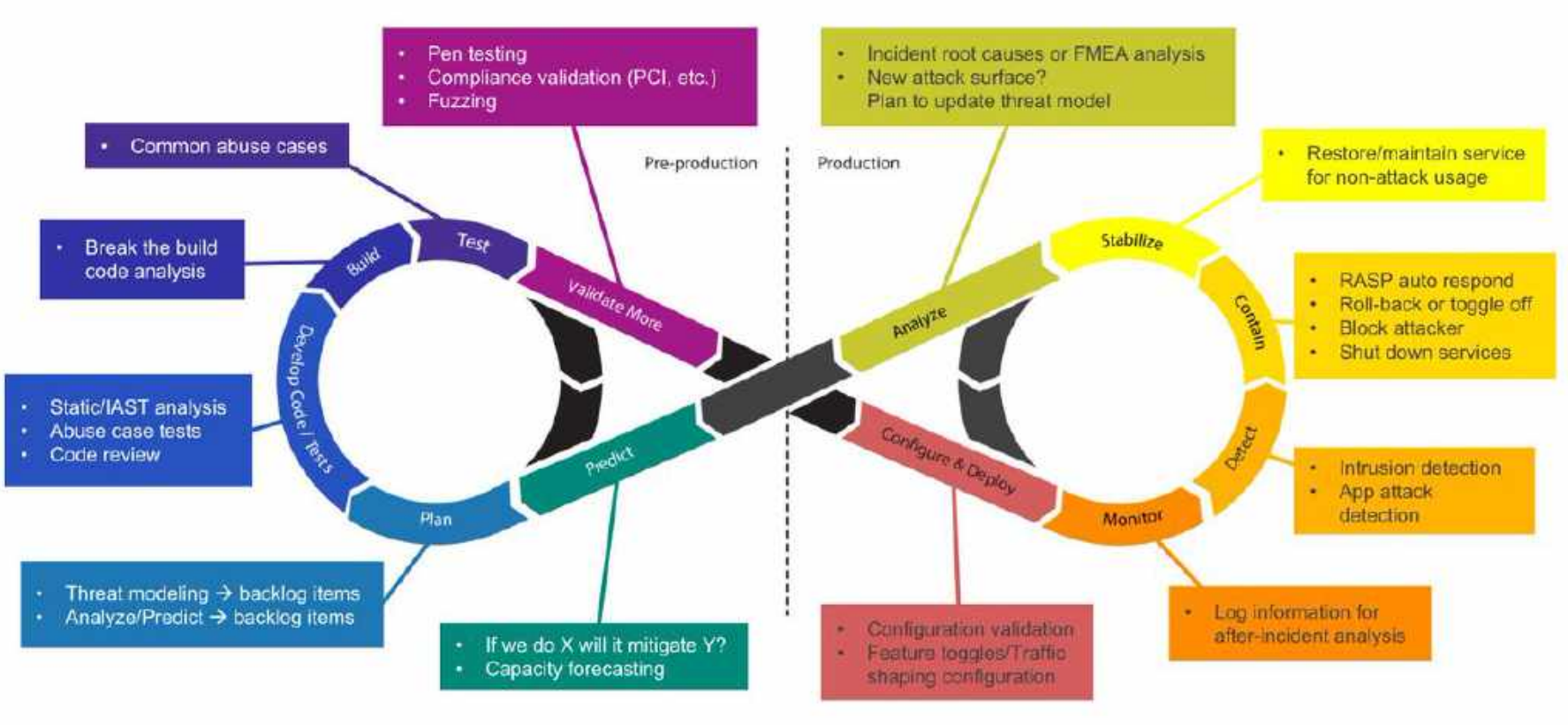
carmasec




Quelle: https://www.microsoft.com/en-us/securityengineering/sdl/

# DevSecOps – Methodik

carmasec



carmasec

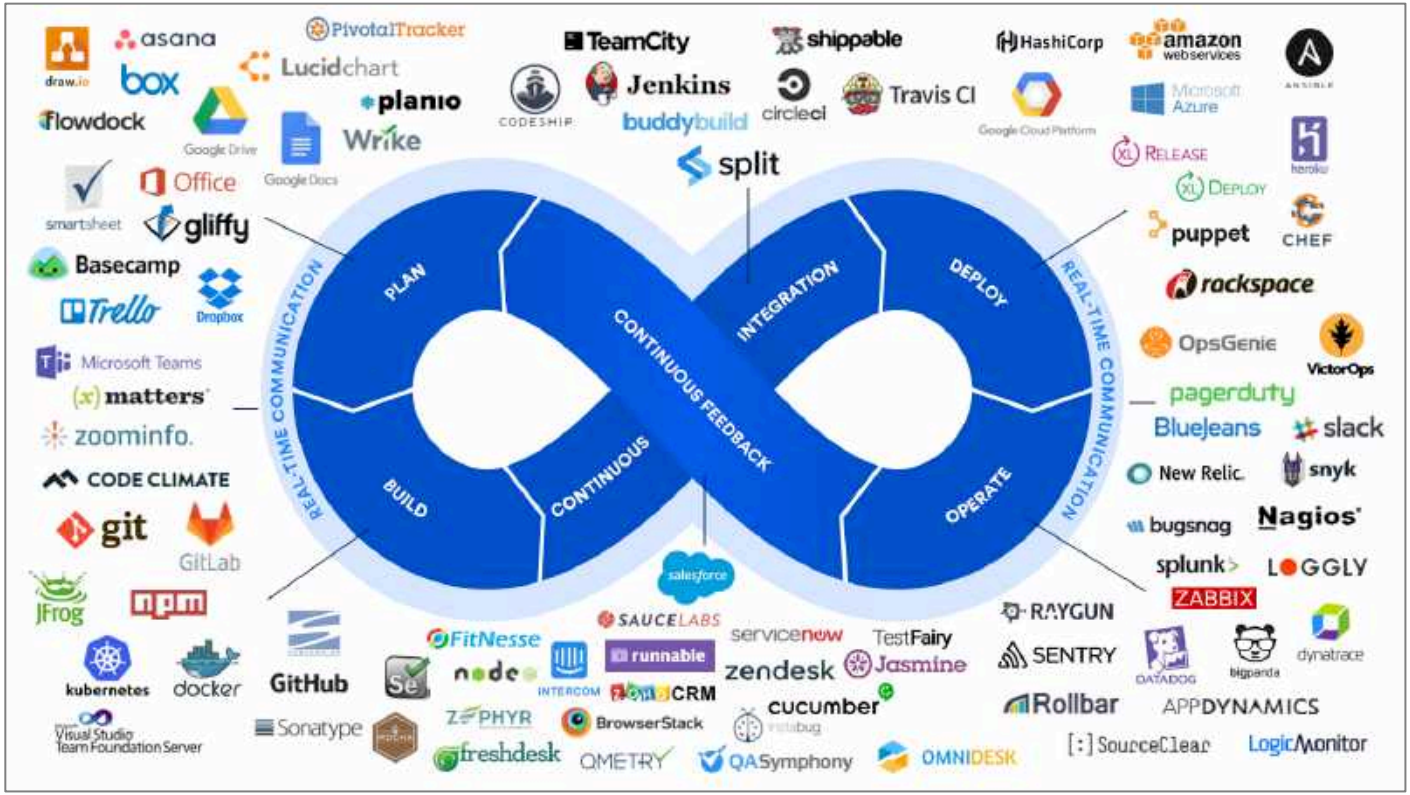
*“If you think that technology can solve your security problems, then you don´t understand the problems and you don´t understand the technology.”*

—

*Bruce Schneier*

# DevSecOps – A fool with a tool, ...?

carmasec




Quelle: https://marketplace.atlassian.com/categories/devops

# DevSecOps – A fool with a tool, ...?

carmasec


Quelle: https://www.sans.org/security-resources/posters/secure-devops-toolchain-swat-checklist/60/download

# DevSecOps – Lösungsansätze

carmasec

| BIZ | DEV | OPS |
|---|---|---|
| • Functional Requirements<br>• User Stories | • Infrastructure as Code<br>• Continuous Integration<br>• Continuous Deployment<br>• Agile Development Methods (Scrum, Kanban, Agile, ...)<br>• Test Cases, Acceptance Criteria, Test Automation | • IT Service Operations (see ITIL), Infrastructure Management<br>• Logging & Monitoring, Utilization & Capacity Management<br>• Patch Management<br>• Decommisioning |
| **SEC** | | |
| • Compliance Requirements<br>• Security Measures & Controls<br>• Security by design<br>• Privacy by design | • Development Guidelines, Secure Development, Awareness<br>• Security Test Cases & AC<br>• Security Test Automation (SAST/DAST, Code Audit, ...)<br>• Hardening Infrastructure Artifacts<br>• Secure Software Development Lifecycle Management | • Continuous Security Monitoring<br>• Periodic Security Testing & Vulnerability Management<br>• Infrastructure hardening<br>• Security Incident & Event Management<br>• Secure Software Development Lifecycle Management |

# DevSecOps – Lösungsansätze

carmasec

- Verwendung von anerkannten „Best Practices“ und „Blueprints“
- Sicherheits- und Risikobewusstsein bei **allen Beteiligten**
- **Frühzeitiges Aufsetzen** einer „Governance“ (Prozesse, Kontrollen)
- Nutzung von Kontrollen zur Effizienzmessung und **Wirksamkeit**
- **Standardisierung** und **Automatisierung**
- Management von Sicherheit ist ein kontinuierlicher Prozess
- **DAS WICHTIGSTE: KEINE ZEIT VERLIEREN UND HEUTE STARTEN**


Melden Sie sich für unseren Newsletter an: www.carmasec.com/newsletter

carmasec Ltd. & Co. KG
Ruhrallee 185
45136 Essen
Germany

Telefon: +49 (0) 201 426 385 900
Fax: +49 (0) 201 426 385 909
Web: www.carmasec.com
Email: contact@carmasec.com