



carmasec

security. done. right.



carmasec

security. done. right.

DevSecOps & Security Automation: Agile Sicherheit und pragmatische Lösungsansätze

Carsten Marmulla

Bochum, 27.03.2019

Agenda

- Wer sind wir? Was können wir?
- Status Quo
- Digitale Transformation
- Paradigmenwechsel
- Agile Security
- Lösungsansätze
- Fazit

Wer sind wir?



- Gegründet **2018**
- Standorte: **Essen** und **Köln**
- Fokus: Cyber Security **Advisory, Consulting** und **Research**
- Branchenerfahrung: **Telekommunikation, Informationstechnologie,**
Logistik, Finanzdienstleistungen, Gesundheitswesen, Energie, u.a.

Wer sind wir?



Carsten Marmulla
Managing Partner
Senior Trusted Advisor

Standort Essen

carsten.marmulla@carmasec.com

Projekt- und Beratungserfahrung: >20 Jahre

Themenschwerpunkte:

- Information Security Management
- IT Service Management
- IT Governance/Risk/Compliance Management
- Data Privacy und Data Protection

Zertifizierungen:

Certified Information Security Manager (CISM), ISO 27001 Auditor, ITIL v3, COBIT 5 Practitioner, PRINCE2 Practitioner, Professional Scrum Master



Jan Sudmeyer
Managing Partner
Senior Trusted Advisor

Standort Köln

jan.sudmeyer@carmasec.com

Projekt- und Beratungserfahrung: >10 Jahre

Themenschwerpunkte:

- Projekt- und Information Security Management
- Risk Assessments, Security Architecture, Security Engineering
- Data Privacy und Data Protection
- Fraud Management, Sicherheits- und Notfallmanagement

Zertifizierungen:

Certified Information Systems Security Professional (CISSP), ISO 27001 Foundation, ITIL v3, COBIT 5 Foundation, PRINCE 2 Practitioner

Was können wir?

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.

*„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

Status Quo



INNOVATION



Status Quo

Sleeping Positions



- Unternehmen unterliegen globalem Wettbewerbsdruck
- Innovative Technologieansätze versprechen...
 - Effizienzgewinne,
 - höhere Umsetzungsgeschwindigkeit,
 - Kostenreduktion,
 - neue (datengetriebene) Geschäftsmodelle.

- In erster Linie:
 - Gesamtheitlicher Veränderungsprozess (Change Management)
- Primär zu definieren:
 - Zweck (Motivation) und
 - Ziel (Erwartung)
- Nicht ausschließlich Technologiewandel

Paradigmenwechsel

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

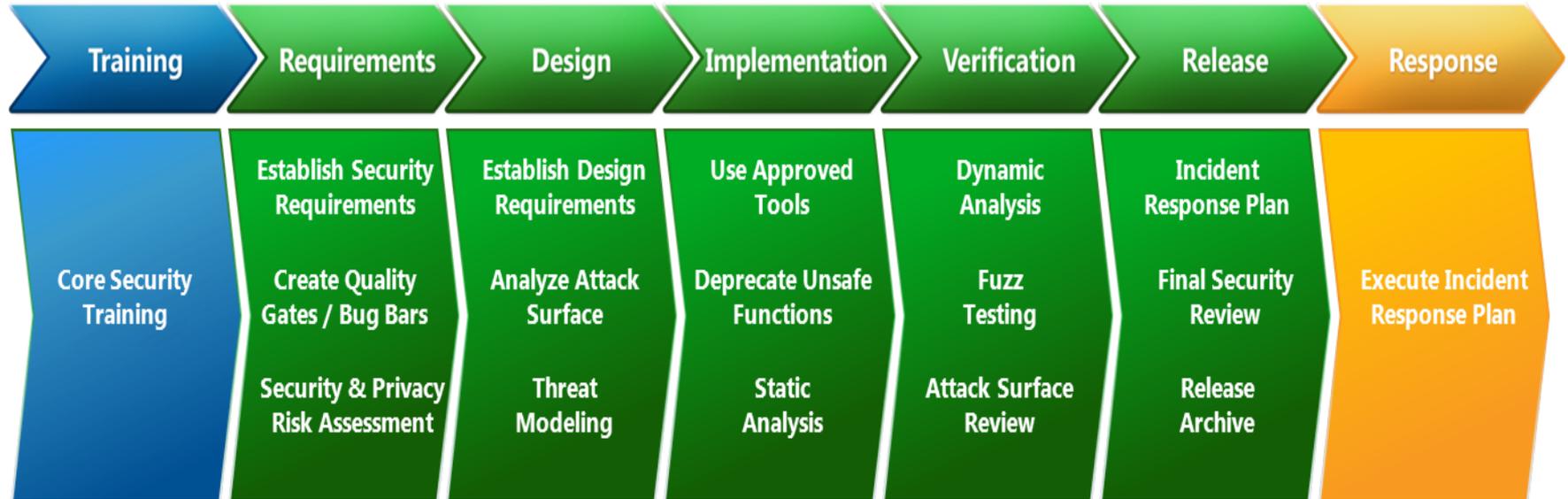
„Heutezutage ist alles Code.“

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

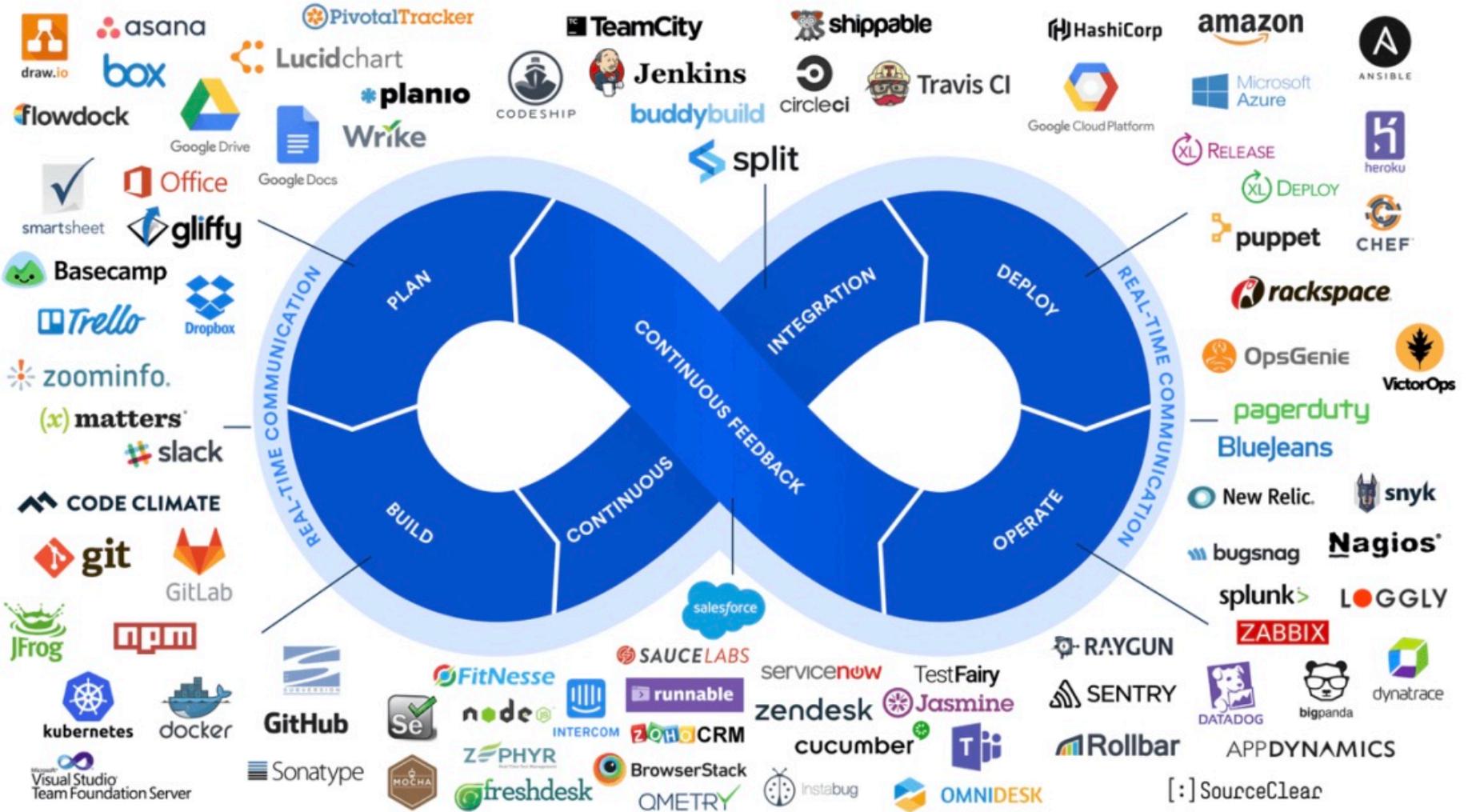
- Was bedeutet das für “Security“?
 - Geschwindigkeitsanforderung steigt
 - Perimetersicherheit funktioniert nicht mehr (uneingeschränkt)
 - Penetrationstests helfen nicht mehr
 - Prozesse müssen flexibel und dynamisch werden
 - Bewegliche Zielarchitektur (volatile Infrastruktur, „moving target“)
 -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

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

Lösungsansätze



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



Lösungsansätze



Lösungsansätze

<u>BIZ</u>	<u>DEV</u>	<u>OPS</u>
<ul style="list-style-type: none">• Functional Requirements• User Stories	<ul style="list-style-type: none">• Infrastructure as Code• Continuous Integration• Continuous Deployment• Agile Development Methods (Scrum, Kanban, Agile, ...)• Test Cases, Acceptance Criteria, Test Automation	<ul style="list-style-type: none">• IT Service Operations (see ITIL), Infrastructure Management• Logging & Monitoring, Utilization & Capacity Management• Patch Management• Decommissioning
<u>SEC</u>		
<ul style="list-style-type: none">• Compliance Requirements• Security Measures & Controls• Security by design• Privacy by design	<ul style="list-style-type: none">• Development Guidelines, Secure Development, Awareness• Security Test Cases & AC• Security Test Automation (SAST/DAST, Code Audit, ...)• Hardening Infrastructure Artifacts• Secure Software Development Lifecycle Management	<ul style="list-style-type: none">• Continuous Security Monitoring• Periodic Security Testing & Vulnerability Management• Infrastructure hardening• Security Incident & Event Management• Secure Software Development Lifecycle Management

- Verwendung von anerkannten „Best Practices“ und „Blueprints“
- Frühzeitiges Aufsetzen einer „Governance“
- Nutzung von Kontrollen zur Effizienzmessung
- Standardisierung und Automatisierung
- Management von Sicherheit ist ein kontinuierlicher Prozess
- **DAS WICHTIGSTE: KEINE ZEIT VERLIEREN UND HEUTE STARTEN**

*„If everything seems under control,
you're not going fast enough.”*

—

Mario Andretti



carmasec

carmasec Limited & Co. KG
Ruhrallee 185
45136 Essen
Germany

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