carmasec

security. done. right.

DevSecOps & Security Automation:

Agile Sicherheit und pragmatische Lösungsansätze

Carsten Marmulla

Bochum, 22.02.2019

Agenda

carmasec

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

Wer sind wir?

carmasec

- 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

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?

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.

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

—

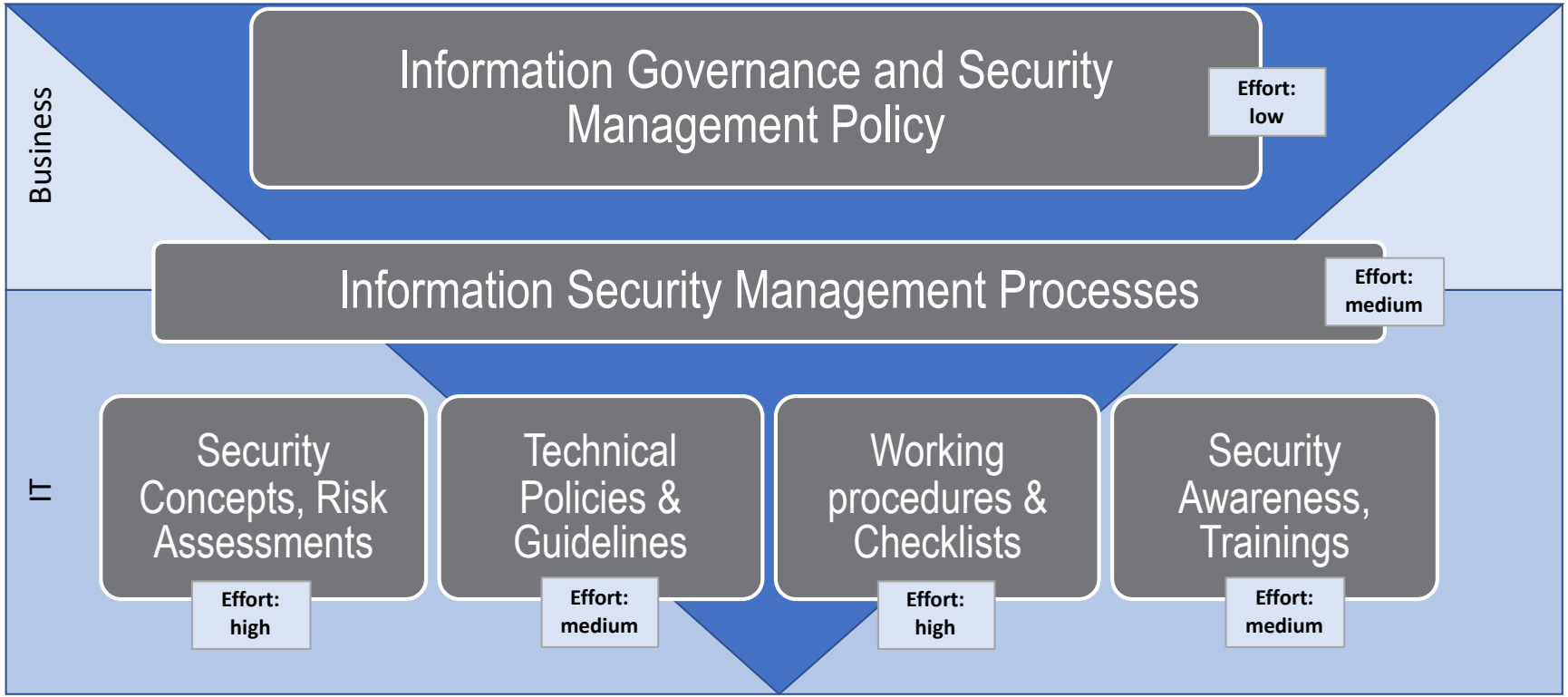
John T. Chambers

Status Quo

carmasec

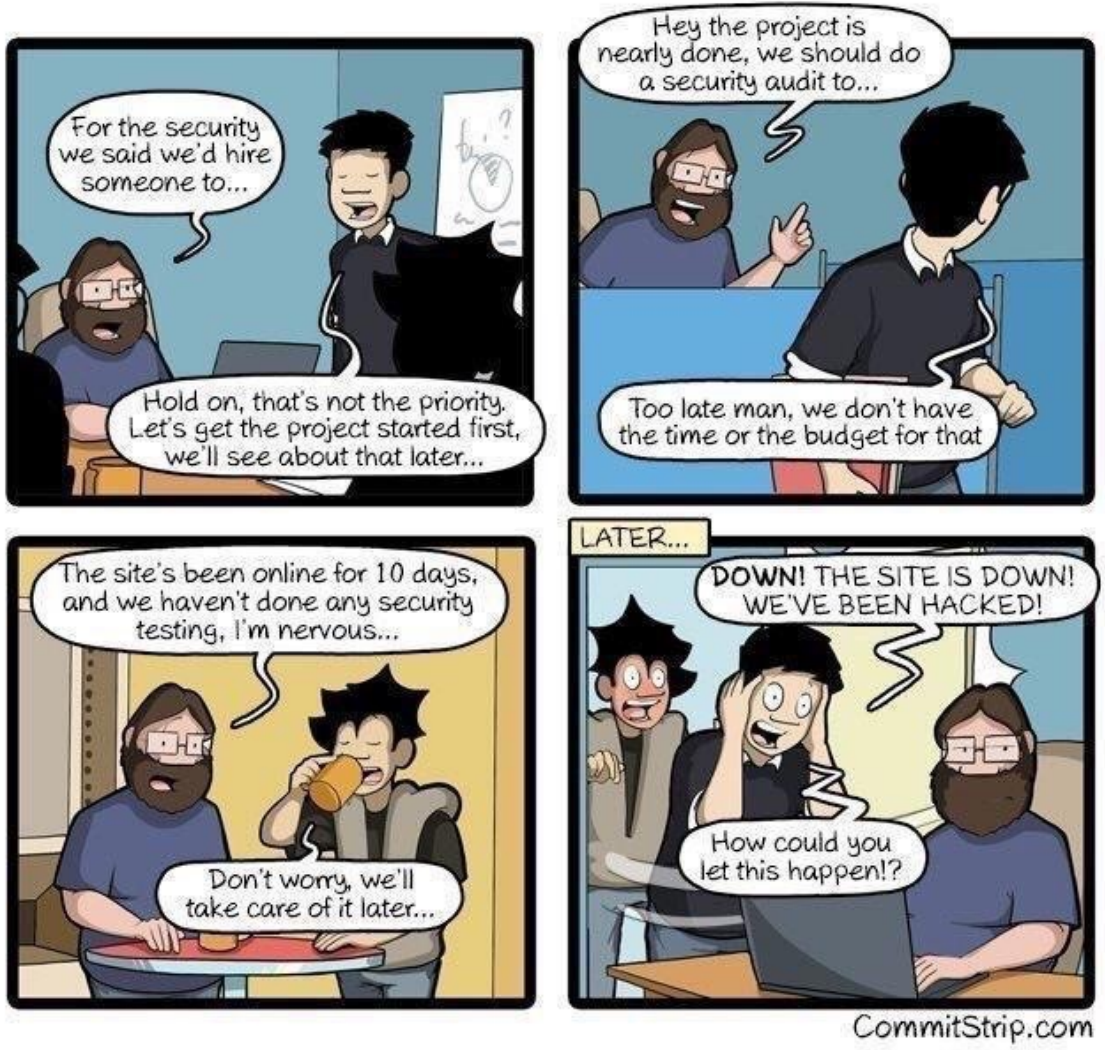
INNOVATION

Status Quo


Business
IT
Information Governance and Security Management Policy
Effort: low
Information Security Management Processes
Effort: medium
Security Concepts, Risk Assessments
Effort: high
Technical Policies & Guidelines
Effort: medium
Working procedures & Checklists
Effort: high
Security Awareness, Trainings
Effort: medium

Status Quo

	Typ 1: „Skript-Kid“	Typ 2: „Hacktivist“	Typ 3: „Cybercrime“	Typ 4: „Nachrichtendienste“
Motivation	• „Ruhm & Ehre“ • Zeigen, was man kann • Spiel & Spaß	• Politische Meinungs-äußerung / Protest	• Betrug • Erpressung • Geldwäsche	• Spionage • Sabotage
Ressourcen	• Zumeist Einzeltäter oder kleinere Gruppen	• Gut organisierte Gruppen • Hohe Arbeitsteiligkeit • Weltweite Verteilung	• Gut organisierte Gruppen • Hohe Arbeitsteilung • Weltweite Verteilung • Große Finanzmittel verfügbar	• Staatlich gelenkt • Extrem hohe Finanzmittel zur Verfügung
Beispiele	• Verunstalten von Internetseiten • Meldungen von Schwachstellen in Webseiten an die Presse • ...	• DDoS gegen Banken, die Wikileaks Konten gesperrt hatten • Anonymous-Angriffe gegen Unternehmen • ...	• APTs • Phishing-E-Mails • DDoS auf Online-shops/Onlinewetten • SPAM • ...	• Stuxnet (Iranisches Atomprogramm) • Red October (Regierungen im Ostblock) • ...
Aufwand Prävention/ Abwehr	Niedrig bis mittel	Mittel	Hoch	Sehr Hoch
	Primärer Fokus			**Sekundärer Fokus**


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

Status Quo

Digitale Transformation

carmasec

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

Digitale Transformation

carmasec

- In erster Linie:

  Gesamtheitlicher Veränderungsprozess (Change Management)

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

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

Paradigmenwechsel

carmasec

„Heutezutage ist alles Code.“

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

Agile Security

carmasec

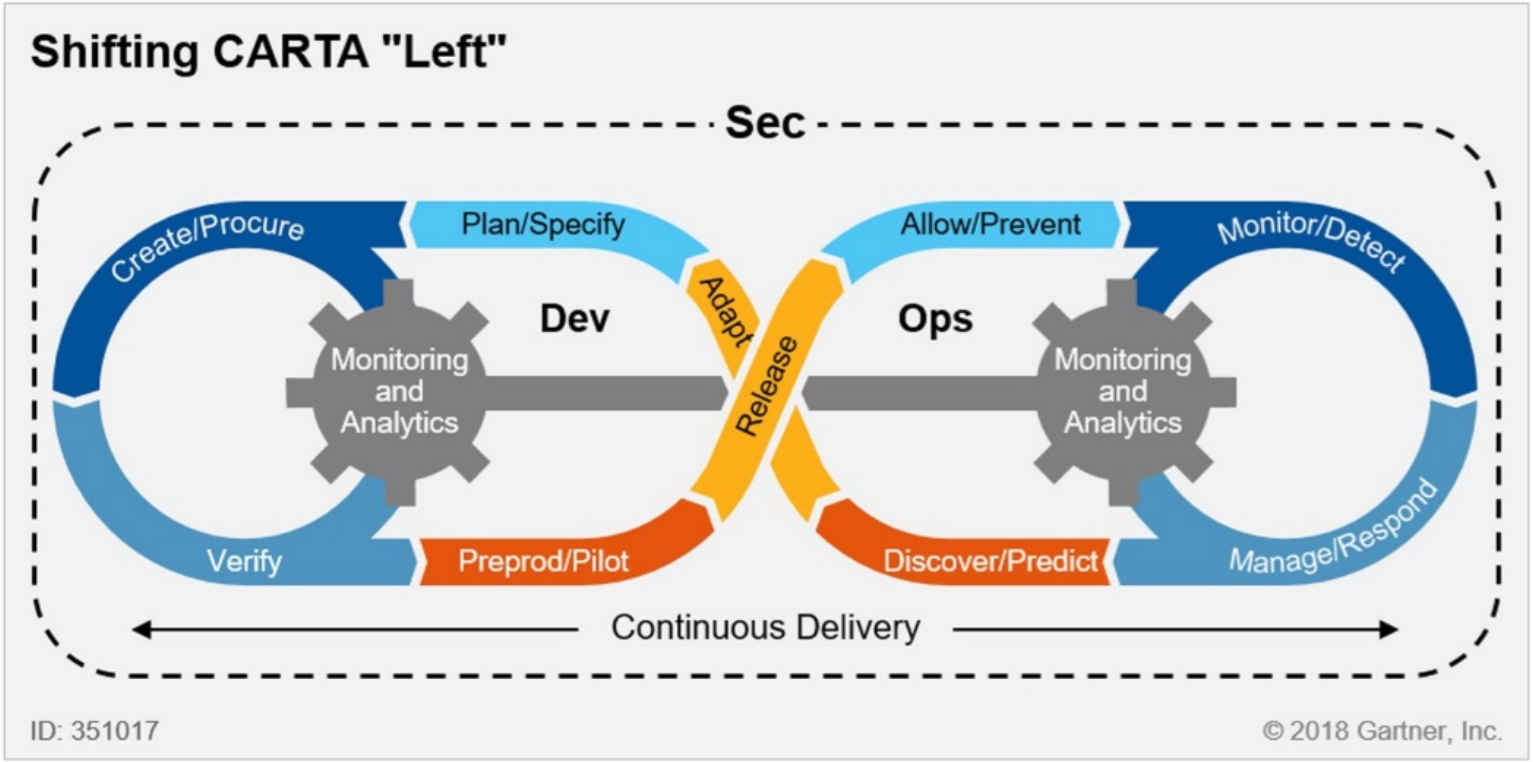
- Was bedeutet das für “Security“?
  - Geschwindigkeitsanforderung steigt
  - Perimetersicherheit funktioniert nicht mehr (uneingeschränkt)
  - Penetrationstests helfen nicht mehr
  - Prozesse müssen flexibel und dynamisch werden
  - Bewegliche Zielarchitektur (volatile Infrastruktur, „moving target“)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

Lösungsansätze

carmasec

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

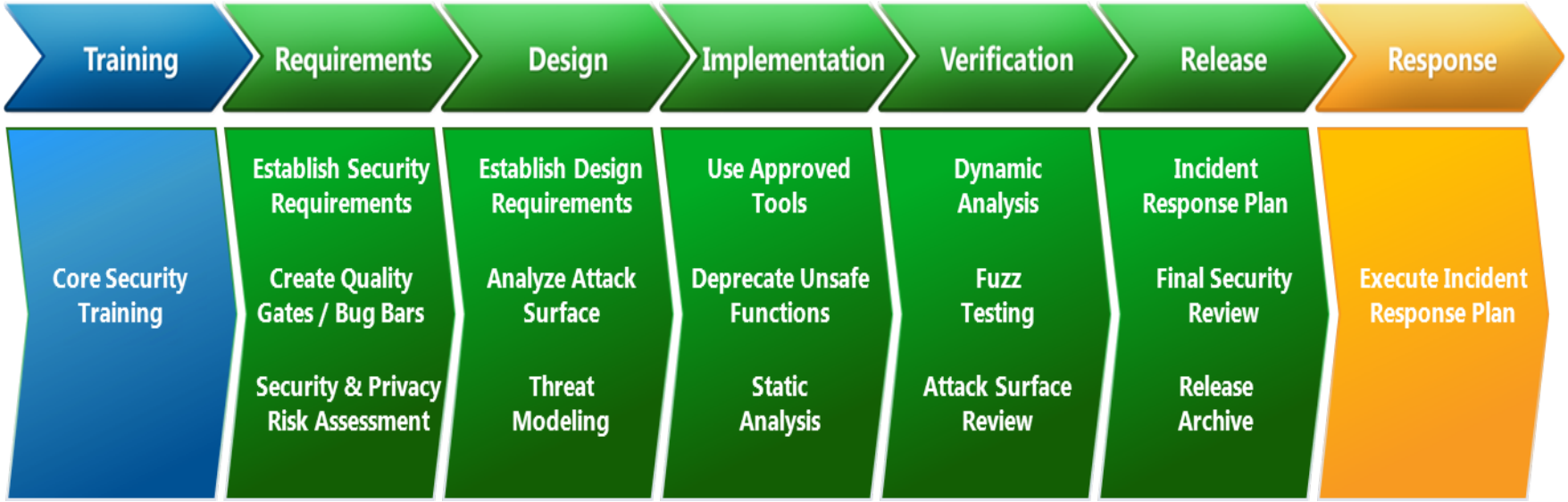
Figure 4. Shifting CARTA "Left" Into DevSecOps (Dev/Build) and Procurement (Buy)



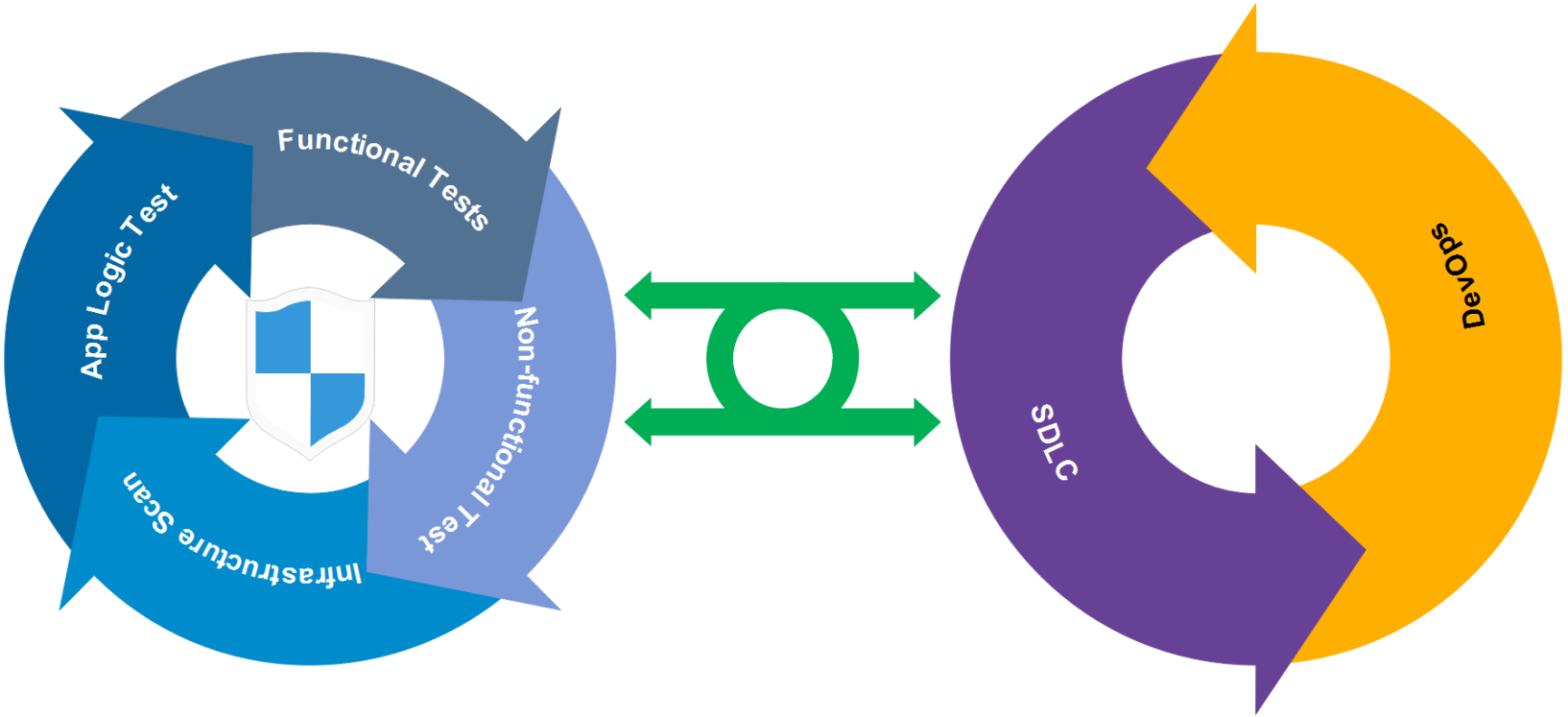
Source: Gartner (October 2018)

Lösungsansätze

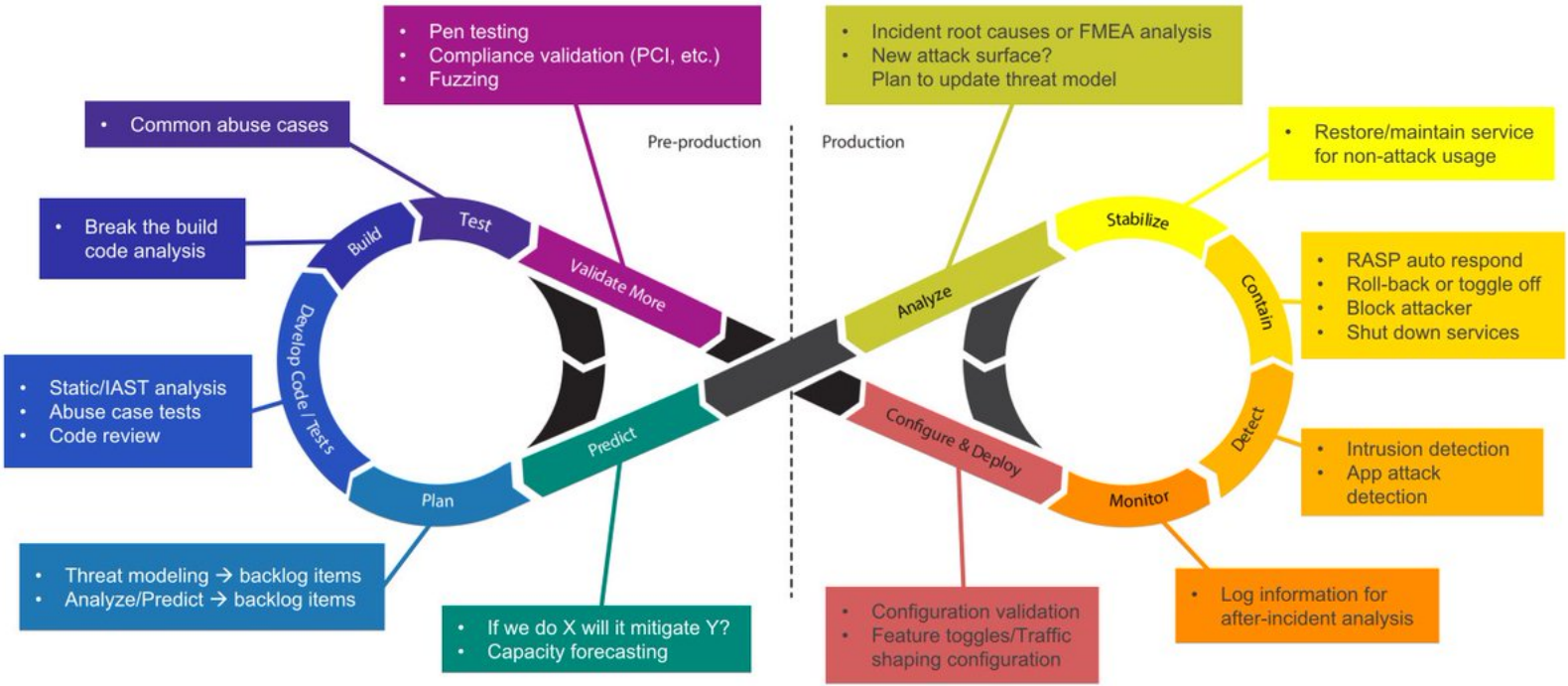
carmasec

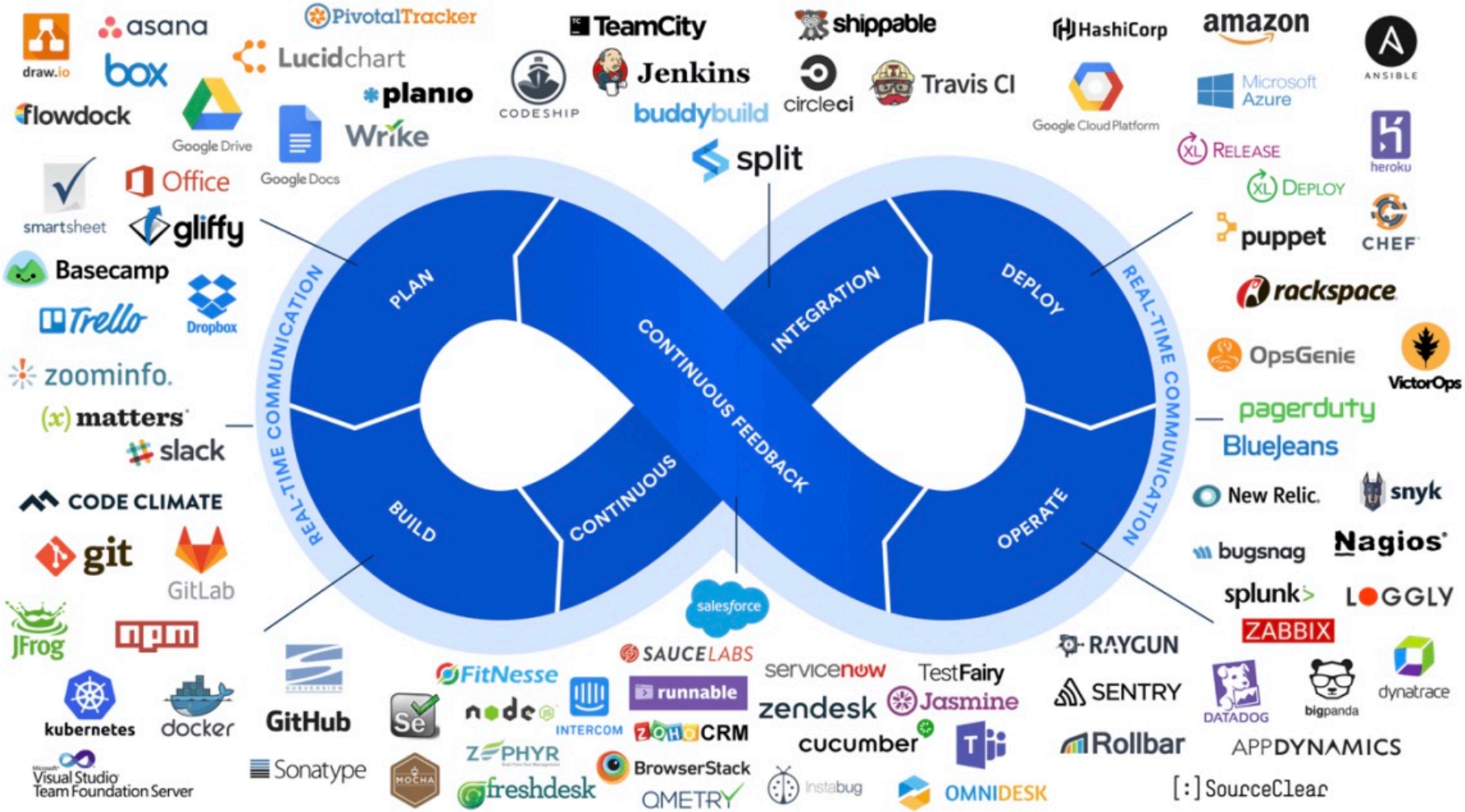


Lösungsansätze



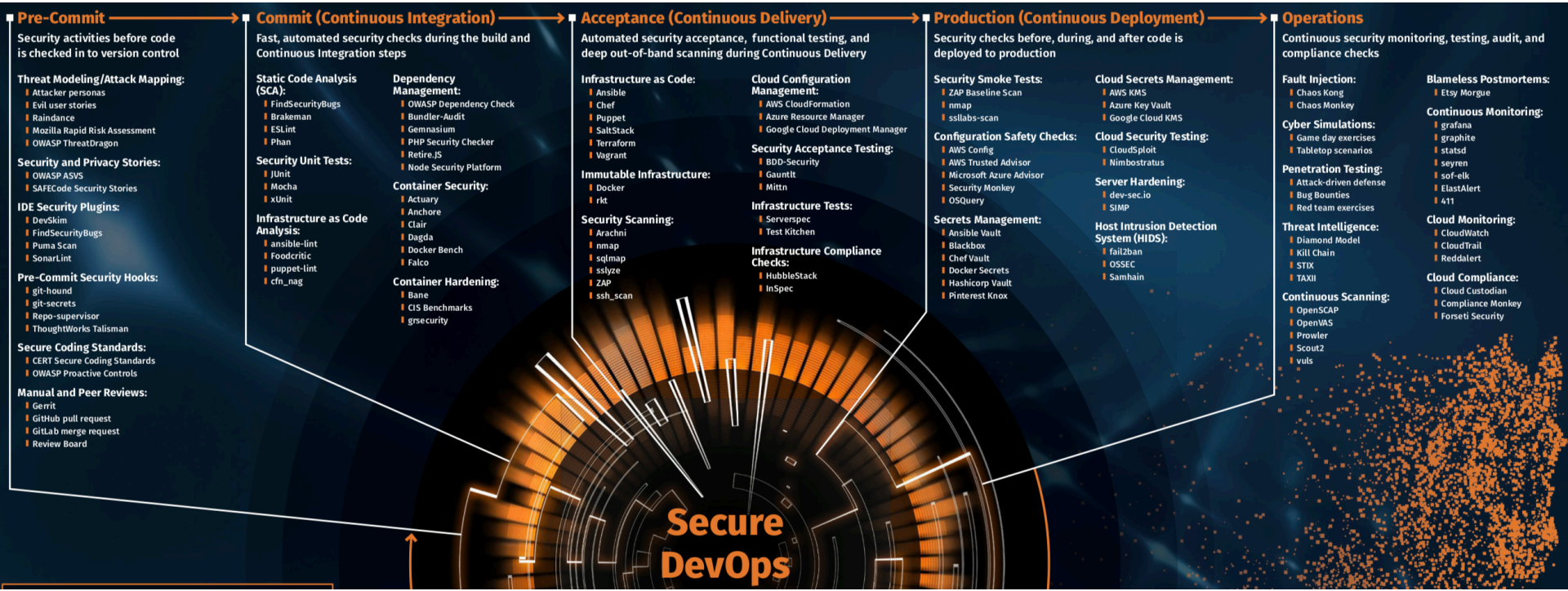
Lösungsansätze




draw.io
asana
PivotalTracker
TeamCity
shippable
HashiCorp
amazon
box
Lucidchart
Jenkins
Travis CI
ANSIBLE
planio
CODESHIP
circleci
flowdock
Google Drive
buddybuild
Microsoft Azure
Google Cloud Platform
Wrike
Google Docs
split
RELEASE
heroku
Office
DEPLOY
smartsheet
gliffy
puppet
CHEF
Basecamp
rackspace
Trello
Dropbox
OpsGenie
VictorOps
zoominfo.
matters
pagerduty
slack
BlueJeans
CODE CLIMATE
New Relic.
snyk
git
GitLab
bugsnag
Nagios
splunk>
LOGGLY
JFrog
npm
ZABBIX
RAYGUN
kubernetes
docker
GitHub
FitNesse
SAUCELABS
servicenow
TestFairy
SENTRY
DATADOG
bigpanda
dynatrace
runnable
zendesk
Jasmine
INTERCOM
ZOHO CRM
cucumber
Rollbar
APPDYNAMICS
ZEPHYR
BrowserStack
Visual Studio Team Foundation Server
Sonatype
freshdesk
QMETRY
Instabug
OMNIDESK
[:]SourceClear
PLAN
CONTINUOUS
INTEGRATION
DEPLOY
BUILD
OPERATE
CONTINUOUS FEEDBACK
REAL-TIME COMMUNICATION
REAL-TIME COMMUNICATION
salesforce

Lösungsansätze

carmasec



Lösungsansätze

carmasec

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

Lösungsansätze

carmasec

- 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

Lösungsansätze

- 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