carmasec

security. done. right.

Everything-as-Code – Anything Secure?

frOSCon 2019

agenda

carmasec

- carmasec
- evolution ::: devops
- evolution ::: architecture & infrastructure
- anything secure?
- what got security to do with it?
- devsecops ::: a fool with a tool
- devsecops ::: in the wild
- missing link

„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

carmasec ::: fakten

- Gegründet 2018
- Standorte: Essen und Köln
- Fokus: Cyber Security Advisory, Consulting und Research
- Branchenerfahrung: Telekommunikation, IT, Logistik, Finanzdienstleister, Health Care, u.a.

carmasec ::: fakten

- Gegründet 2018
- Standorte: Essen und Köln
- Fokus: Cyber Security Advisory, Consulting und Research
- Branchenerfahrung: Telekommunikation, IT, Logistik, Finanzdienstleister, Health Care, u.a.

Was uns antreibt:

Die Faszination und Begeisterung für das Thema Cyber Security

carmasec ::: management

Carsten Marmulla
Managing Partner
Senior Trusted Advisor

Standort Essen
Geboren 1974
+49 151 150 500 59
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
Geboren 1984
+49 175 4820 400
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

carmasec ::: portfolio

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 ::: unsere mission

security.

Wir entwickeln Lösungen, welche die individuellen Anforderungen unserer Kunden berücksichtigen. Ganzheitlich und Ende-zu-Ende.

done.

Wir begleiten unsere Kunden vollumfänglich von der Konzeption bis zum Übergang in den Betrieb. Ein hoher Automatisierungsgrad garantiert nachhaltige und geräuschlose Prozesse.

right.

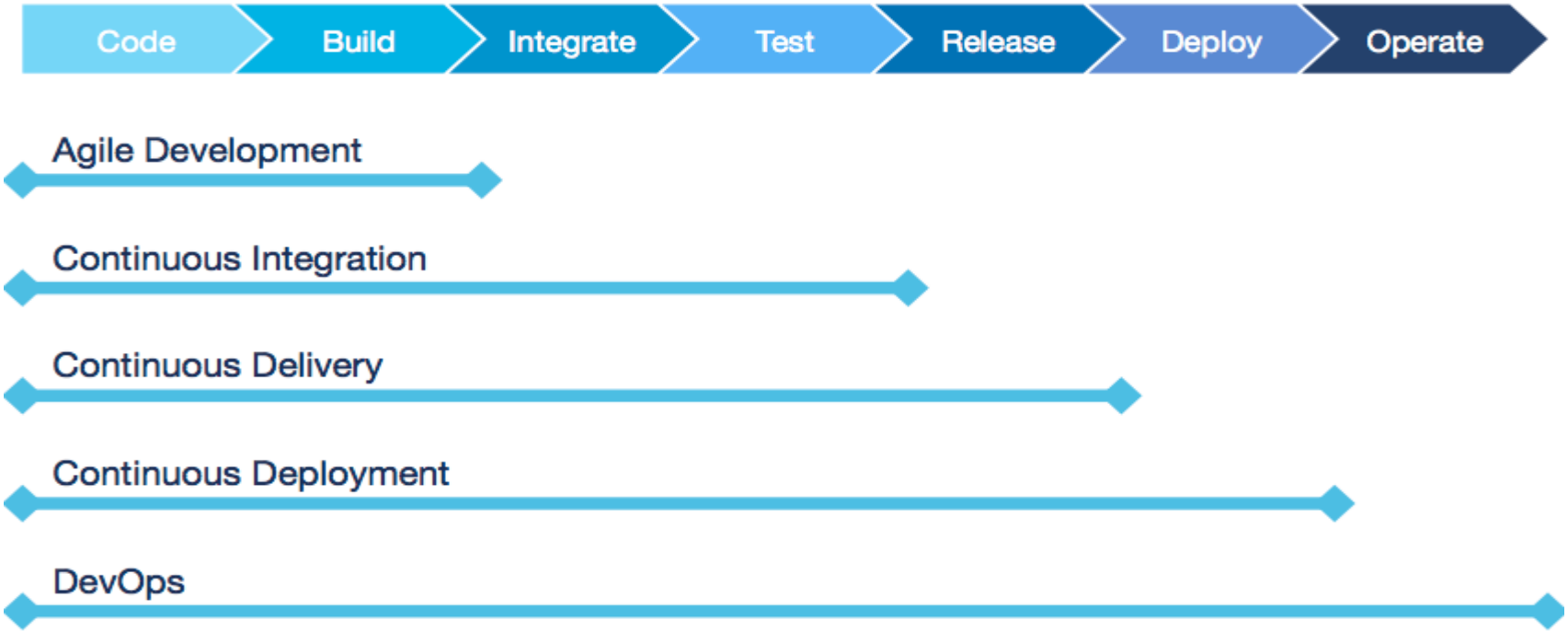
Wir verbinden langjährige Expertise und aktuelle Security Best-Practise um pragmatische Lösungen zu entwickeln die funktionieren.

“Everything is code
and code is law”

—
unknown

evolution ::: devops

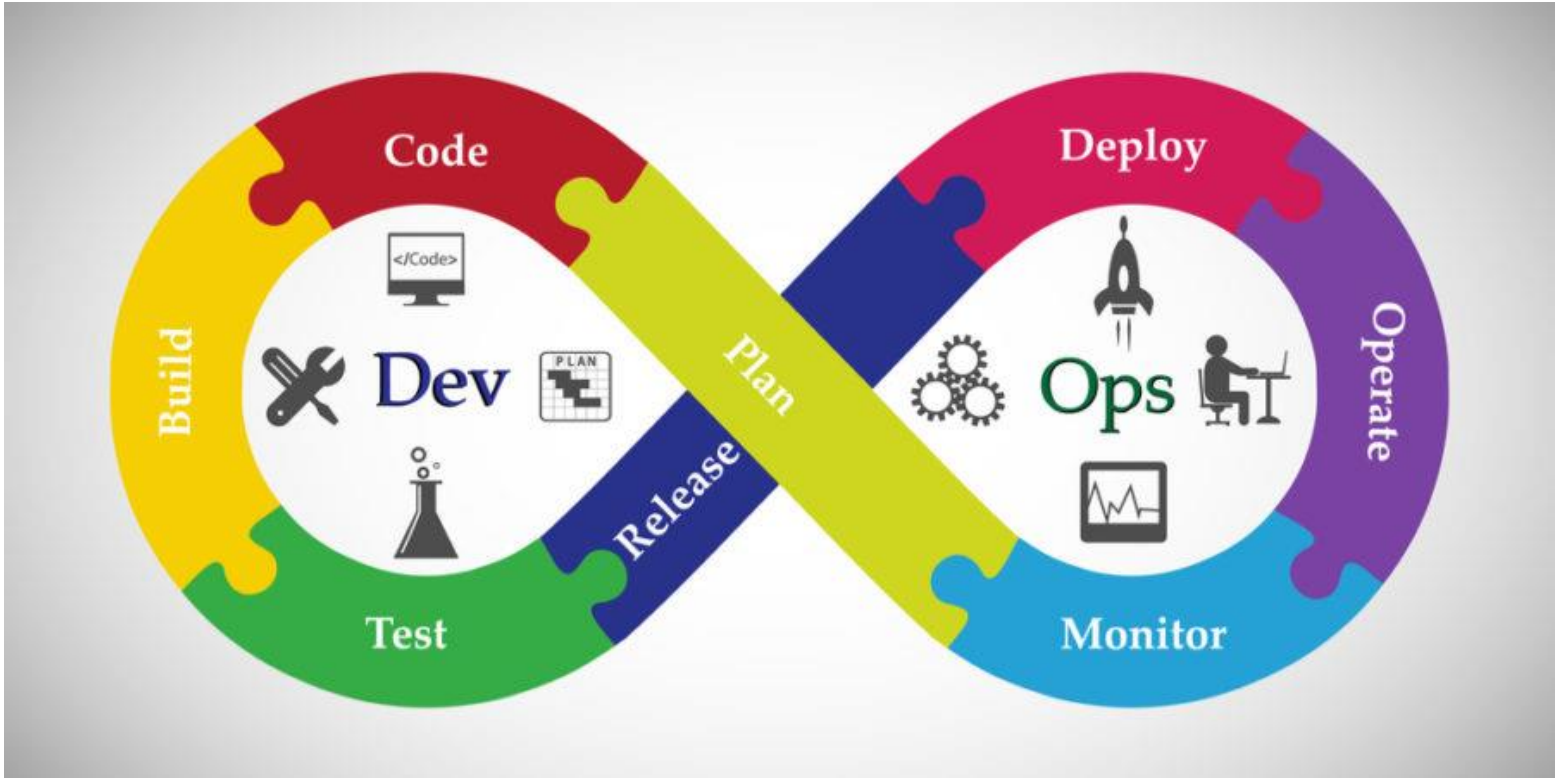
carmasec



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

evolution ::: devops

carmasec



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

evolution ::: architecture & infrastructure

carmasec

Architektur

- Multi -Tier-Architekturen → Microservices, Containerization, Serverless Architecture

evolution ::: architecture & infrastructure

carmasec

Architektur

- Multi-Tier-Architekturen → Microservices, Containerization, Serverless Architecture, …

Infrastruktur

- On-Premise → Cloud
- Hardware → Software Defined Networks (SDN), Software Defined Storage (SDS), Software Defined Infrastructure, Infrastructure-as-Code, …

“With great power comes great responsibility“

—

Voltaire

anything secure?

Wannacry

1,7 Millionen Geräte anfällig für Wannacry

Als Einfallstor für Wannacry sowie für weitere Ransomware-Ableger wie Petya diente eine Schwachstelle in älteren Windows-Betriebssystemen, die durch den Leak von NSA-Hacking-Tools öffentlich bekannt wurde. Dennoch sind dem IT-Sicherheitsexperten Nate Warfield zufolge weltweit noch immer 1,7 Millionen direkt mit dem Internet verbundene Geräte für einen Angriff über diese Sicherheitslücke anfällig. Und das dürfte nur die Spitze des Eisbergs sein. Denn mit den über Shodan gefundenen anfälligen Internetservern sind im schlimmsten Fall jeweils mehrere weitere Geräte mit ähnlichen Schwachstellen verbunden.

Top Countries

1.	United States	401,190
2.	Japan	75,158
3.	Russian Federation	67,109
4.	Germany	47,961
5.	Taiwan	45,865
6.	China	27,766
7.	United Kingdom	22,190
8.	Netherlands	20,491
9.	Singapore	18,931
10.	Hong Kong	18,873

Laut Shodan sind noch Hunderttausende mit dem Internet verbundene Geräte für Wannacry anfällig. (Screenshot: shodan.io)

Quelle: https://t3n.de/news/wannacry-millionen-geraete-sind-immer-noch-fuer-die-ransomware-anfaellig-1162774 (14.05.2019)

anything secure?

OWASP Top 10

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

anything secure?

GitLab Global Developer Report 2019

carmasec

2019 Global Developer Report: DevSecOps top findings

1. **DevOps = better visibility:** Developers, operations team members, and security professionals are 89% more likely to have good insight into what their colleagues are working on when their DevOps model has been in place long term.

2. **Continuous deployment is real:** Almost half — 45% — report continuous code deployment at least somewhere in their organization.

3. **Security is also a work in progress:** 50% agree that security vulnerabilities are mostly discovered by the security team after code is merged and in a test environment.

4. **Remote work supports efficiency:** Remote operations teams are 1.6x more likely to document their work than in-office counterparts.

5. **Testing is still hard:** 49% of respondents encounter the most delays during the testing stage of the development lifecycle.

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

anything secure?

GitLab Global Developer Report 2019

carmasec

2019 Global Developer Report: DevSecOps top findings

1. **DevOps = better visibility:** Developers, operations team members, and security professionals are 89% more likely to have good insight into what their colleagues are working on when their DevOps model has been in place long term.

2. **Continuous deployment is real:** Almost half — 45% — report continuous code deployment at least somewhere in their organization.

3. **Security is also a work in progress:** 50% agree that security vulnerabilities are mostly discovered by the security team after code is merged and in a test environment.

4. **Remote work supports efficiency:** Remote operations teams are 1.6x more likely to document their work than in-office counterparts.

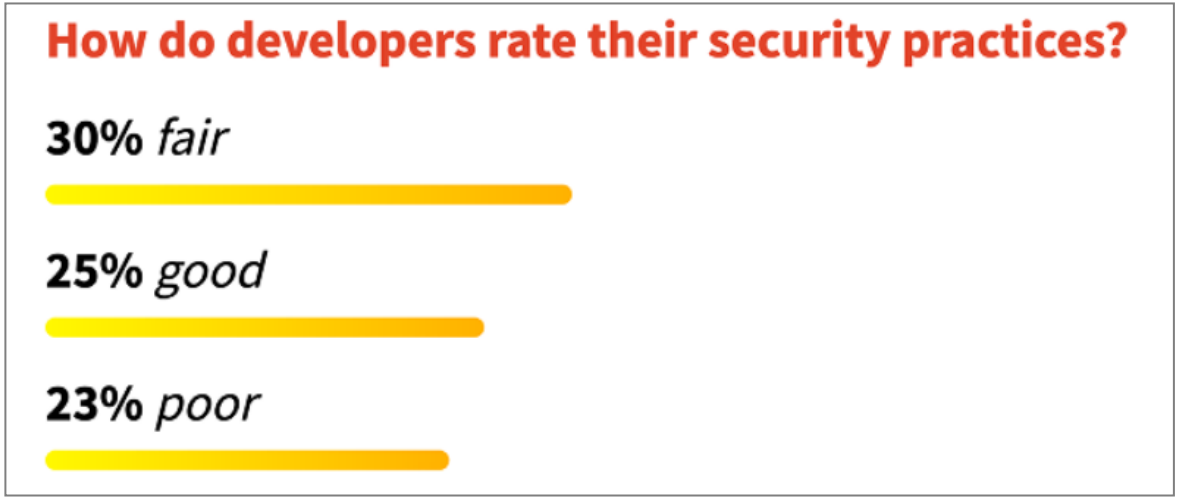
5. **Testing is still hard:** 49% of respondents encounter the most delays during the testing stage of the development lifecycle.

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

anything secure?

GitLab Global Developer Report 2019

carmasec



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

please mind the gap

carmasec

Liebe Entwickler, bitte

- baut besseren, sicheren Code
- kennt und berücksichtigt Security Standards wie CIS und OWASP Guidelines
- verwendet (automatisierte) Security Tools und Controls in allen Phasen des DevSecOps Zyklus
- berücksichtigt nicht-funktionale Anforderungen von Beginn an und fordert diese ein

what got security to do with it?

carmasec

- reine Perimeter Security funktioniert in einer Welt kontinuierlicher Deployments und flexibel skalierender Microservices nicht mehr
- klassische Pentests und Risk Assessments alleine sind zu unflexibel
- Shift-Left bedingt die Übertragung von Verantwortung an Business Verantwortliche und Entwickler welche befähigt werden müssen Risiken zu verstehen und zu managen

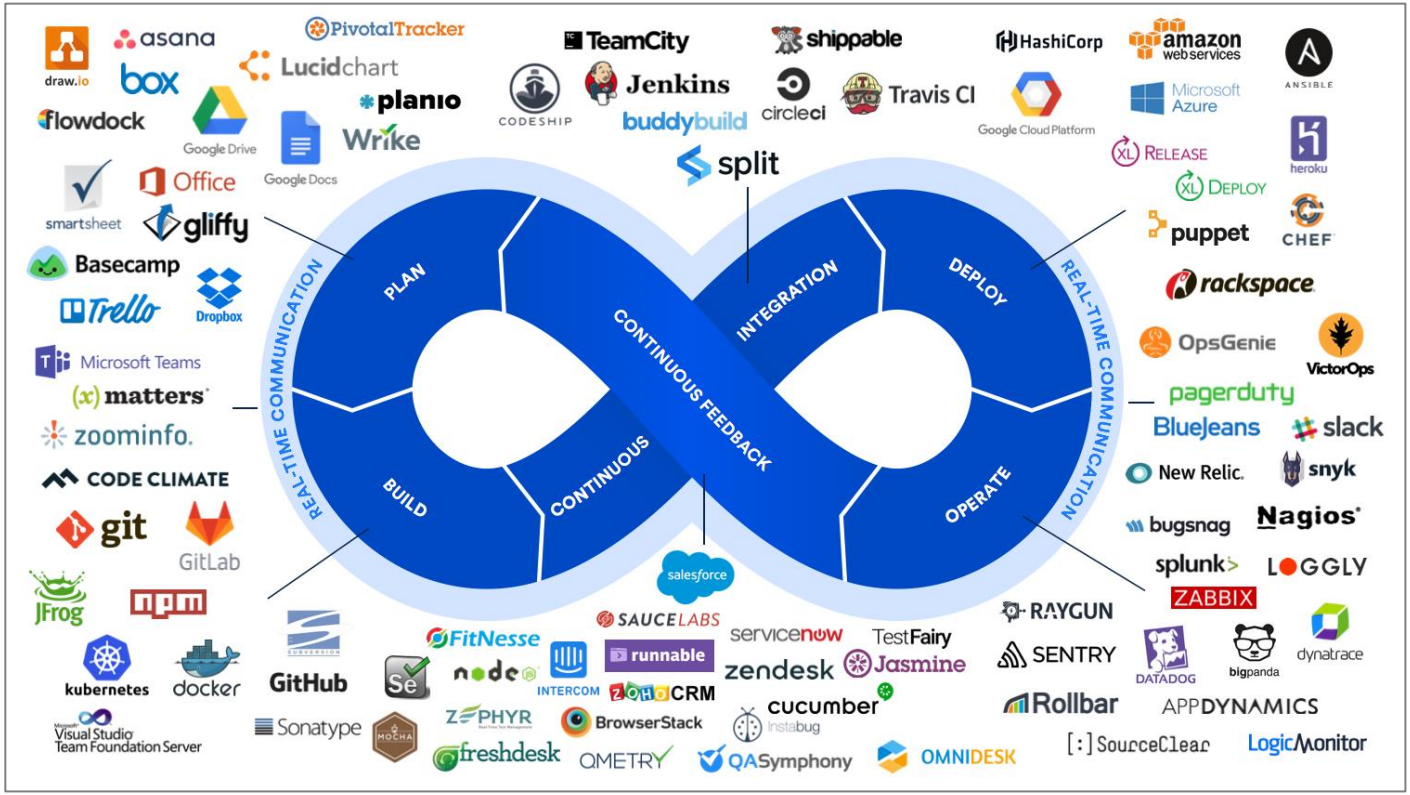
“If you think that technology can solve your security problems,
then you don´t understand the problems
and you don´t understand the technology”

—

Bruce Schneier

devsecops ::: a fool with a tool

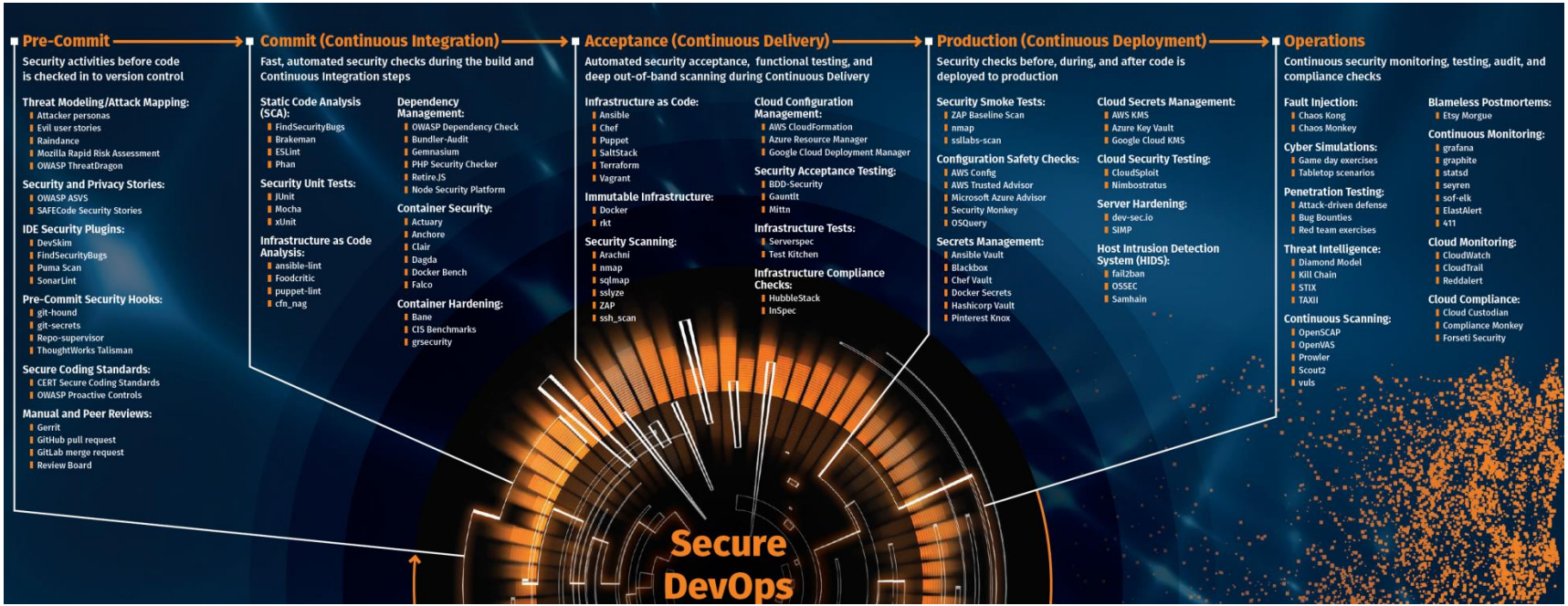
carmasec



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

devsecops ::: a fool with a tool

carmasec

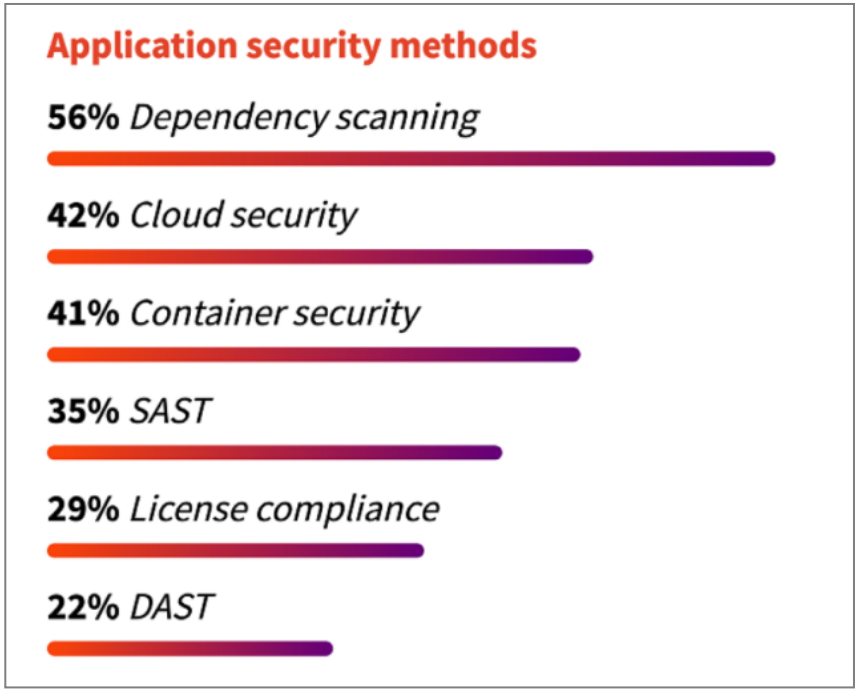


Quelle: https://www.sans.org/security-resources/posters/secure-devops-toolchain-swat-checklist/60/download

devsecops ::: in the wild

GitLab Global Developer Report 2019

carmasec



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

missing link

carmasec

- es existieren diverse Tools, der Marktüberblick und die Integration sind jedoch schwierig
- es besteht die Gefahr der Schaffung von Insellösungen, Tool Abhängigkeiten und Intransparenz
- es bedarf gemeinsamer Lösungen und integrierter Ansätze
- Entwickler selbst müssen in die Entwicklung von Ende-zu-Ende Security Lösungen eingebunden werden bzw. diese selbst mit entwickeln

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