

AGIL ABER SICHER!

[https://andifalk.github.io/
agil-aber-sicher-heise-devsec-2018/presentation/index.html](https://andifalk.github.io/agil-aber-sicher-heise-devsec-2018/presentation/index.html)

// heise
devSec()



ANDREAS FALK

Novatec Consulting GmbH

andreas.falk@novatec-gmbh.de / @andifalk (Twitter)

<https://www.novatec-gmbh.de/beratung/agile-security>



UNSERE SOFTWARE IST DOCH SICHER ?

Kritische Sicherheitslücke gefährdet Milliarden WhatsApp-Nutzer UPDATE



Stand: 10.10.2018 10:43 Uhr – Jürgen Schmidt



(Bild: arivera)

Eine Sicherheitslücke in WhatsApp ermöglicht es, ein Smartphone mit einem einzigen Video-Call zu kapern. Potentiell betroffen sind Milliarden WhatsApp-Nutzer.

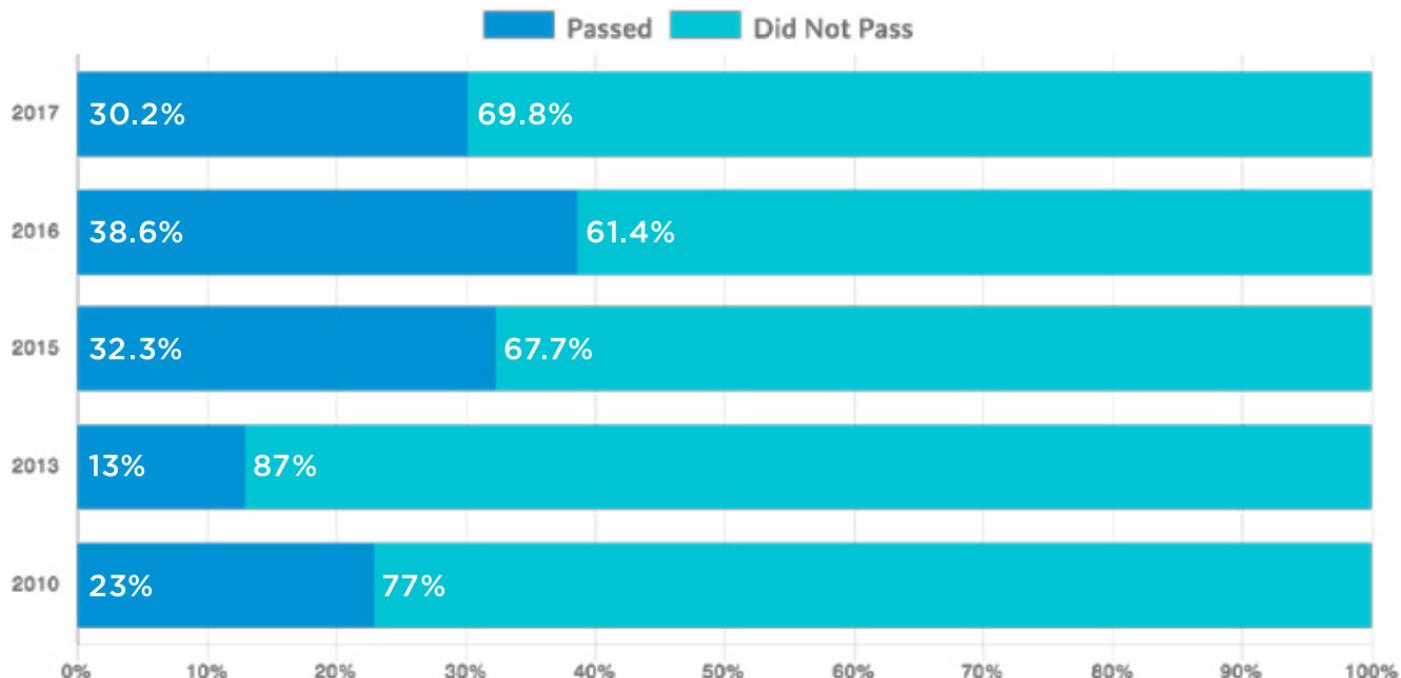
Quelle: [heise.de](https://www.heise.de)

STATE OF SOFTWARE SECURITY REPORT 2017

(VERACODE)

OWASP TOP 10 POLICY PASS RATE

Percentage of
Applications Passing
on First Scan



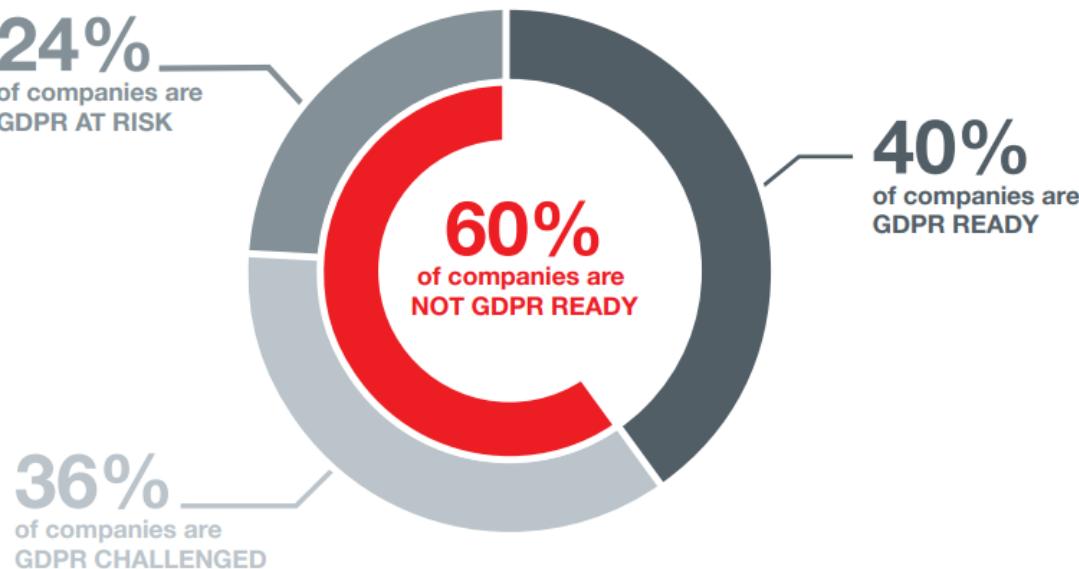
Quelle: veracode.com

**SECURITY IST
NICHT MEIN JOB !?**

EU DATENSCHUTZ GRUNDVERORDNUNG

Seit Mai 2018 geltendes Recht!

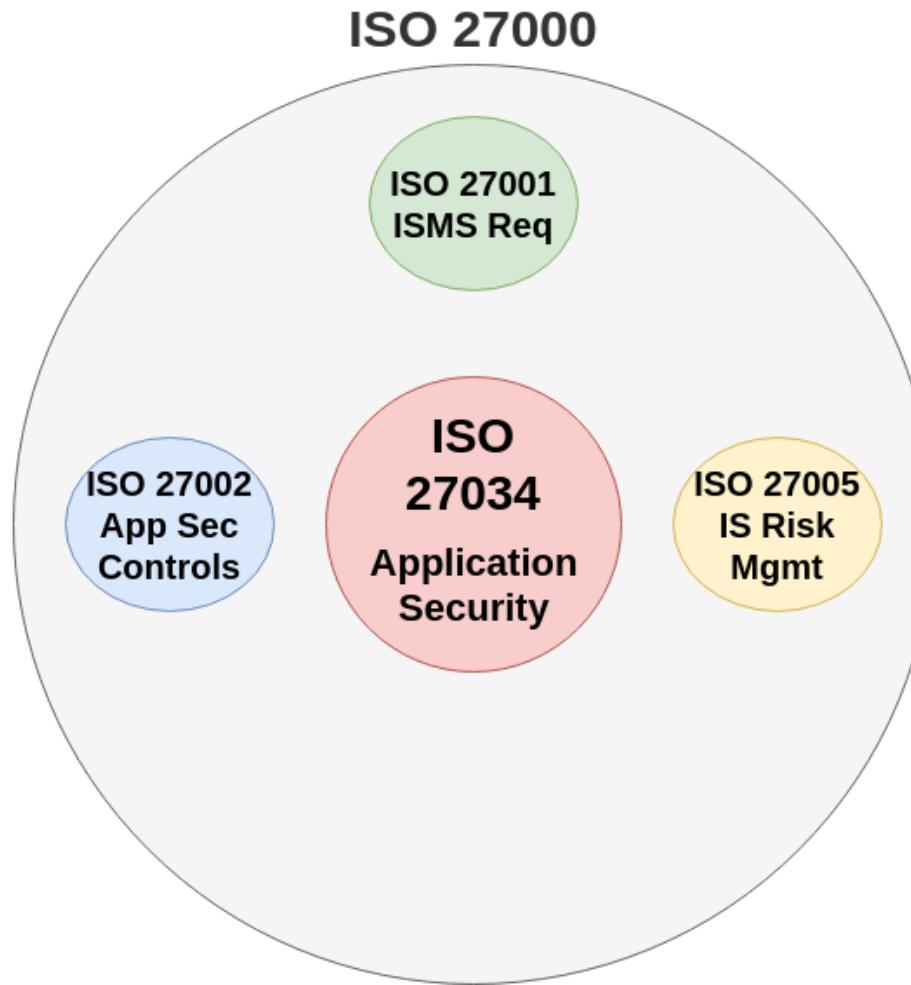
GDPR READINESS



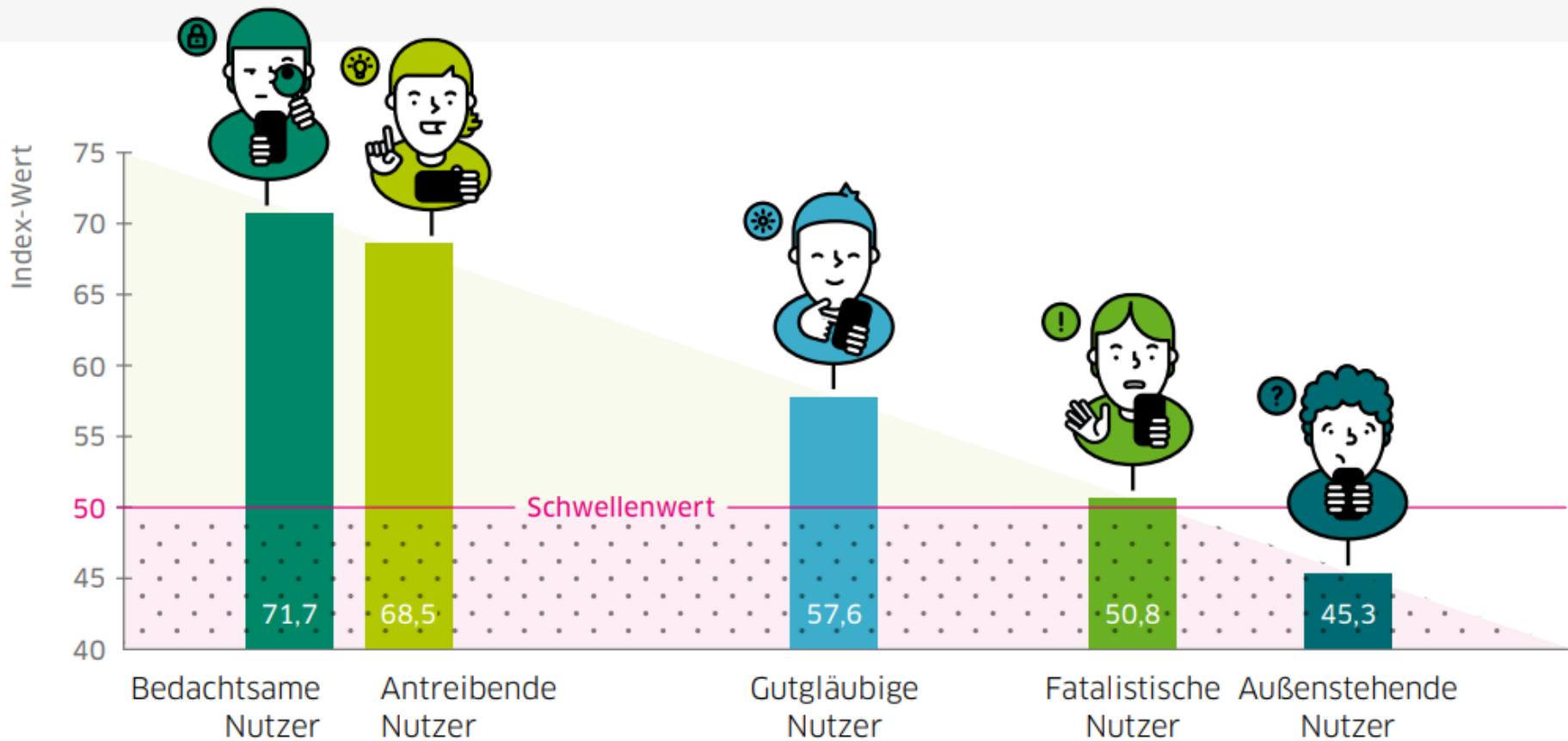
Quelle: [GDPR's Missing Link Report \(senzing.com/gdpr\)](https://senzing.com/gdpr)

ISO 27034

Neuer Standard für Anwendungssicherheit

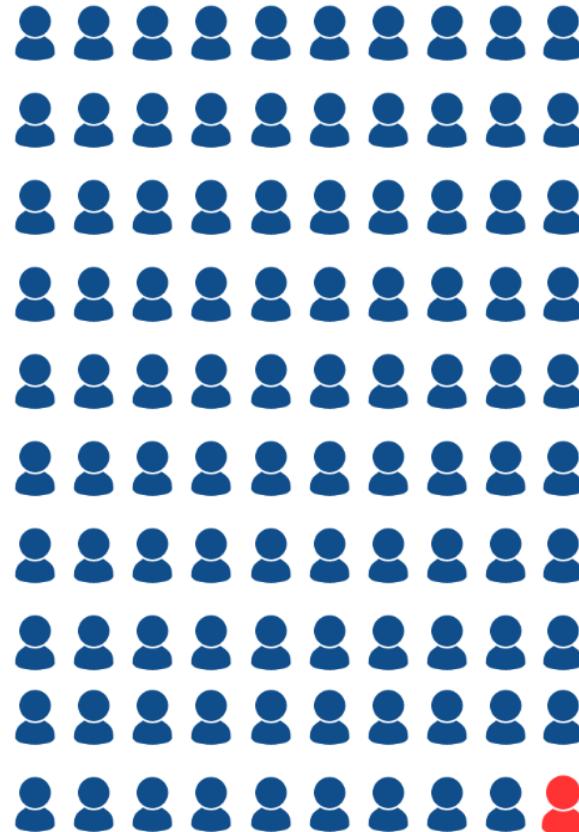


NUTZERVERHALTEN



Quelle: Deutschland sicher im Netz (DsiN): Sicherheitsindex 2018

1 SECURITY-PROFESSIONAL FÜR 100 ENTWICKLER

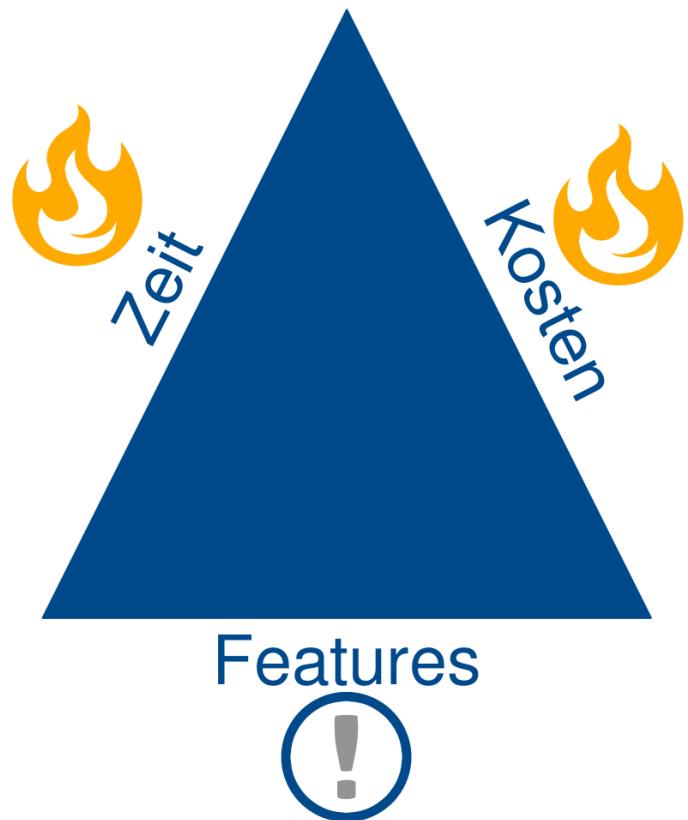


Quelle: sonatype.com/devops-survey-report

SICHERHEIT

IM PROJEKTALLTAG

WIR HABEN DOCH KEINE ZEIT



- X Dokumentation
- X Security / Tests
- ✓ Features!

HACKER FINDEN UNS NICHT !

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#)[Getting Started](#)

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

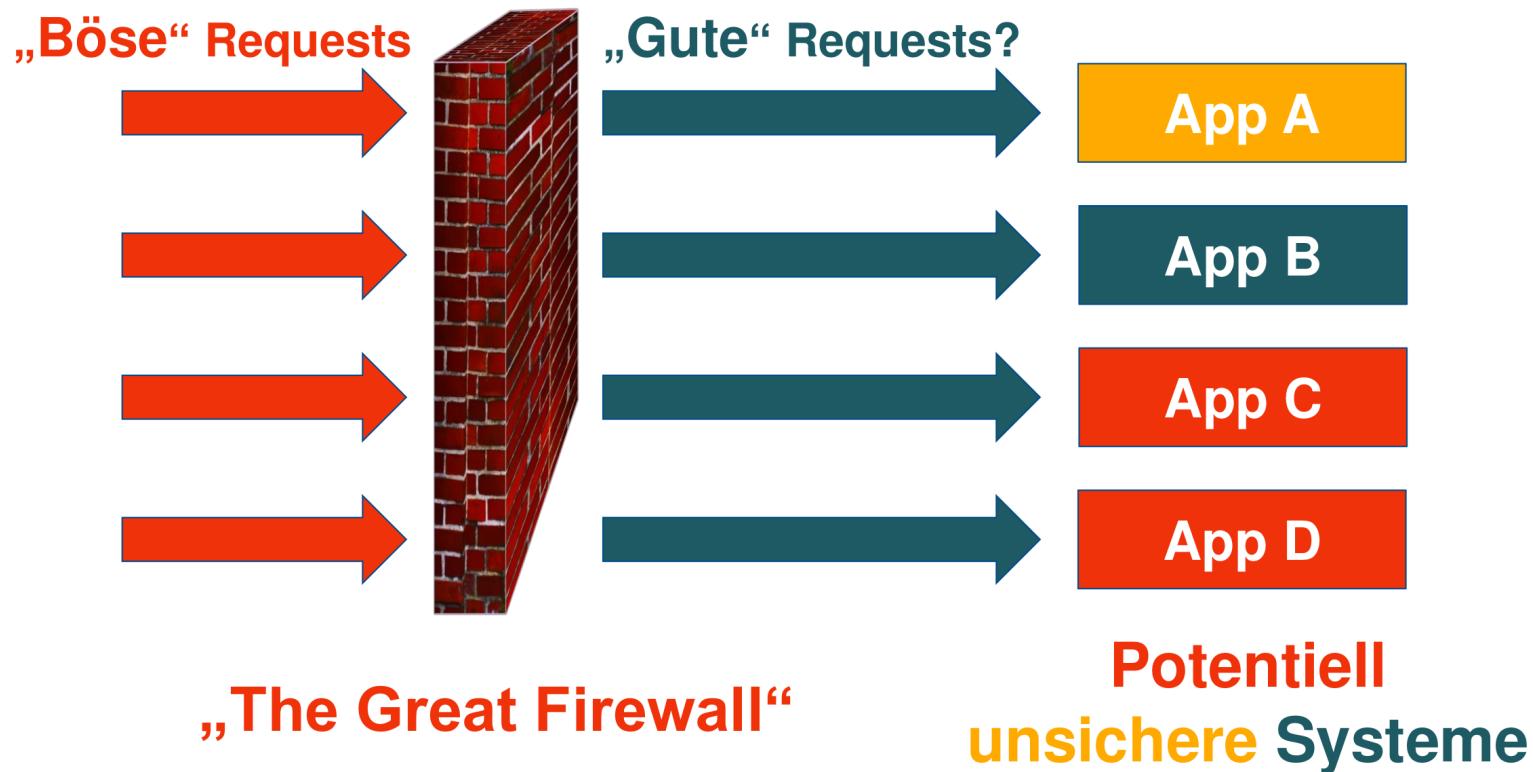


Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Quelle: shodan.io

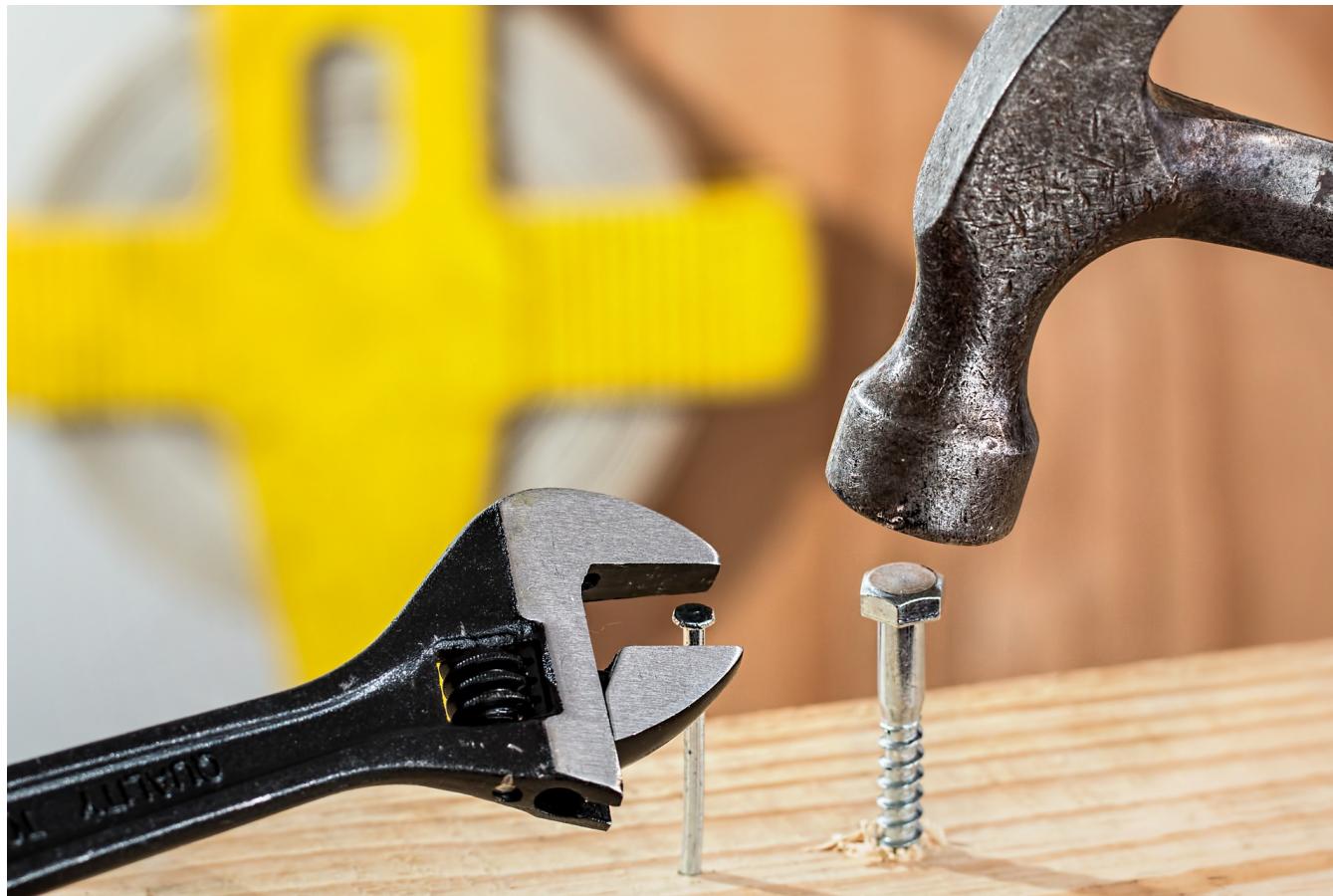
WIR HABEN DOCH EINE FIREWALL!



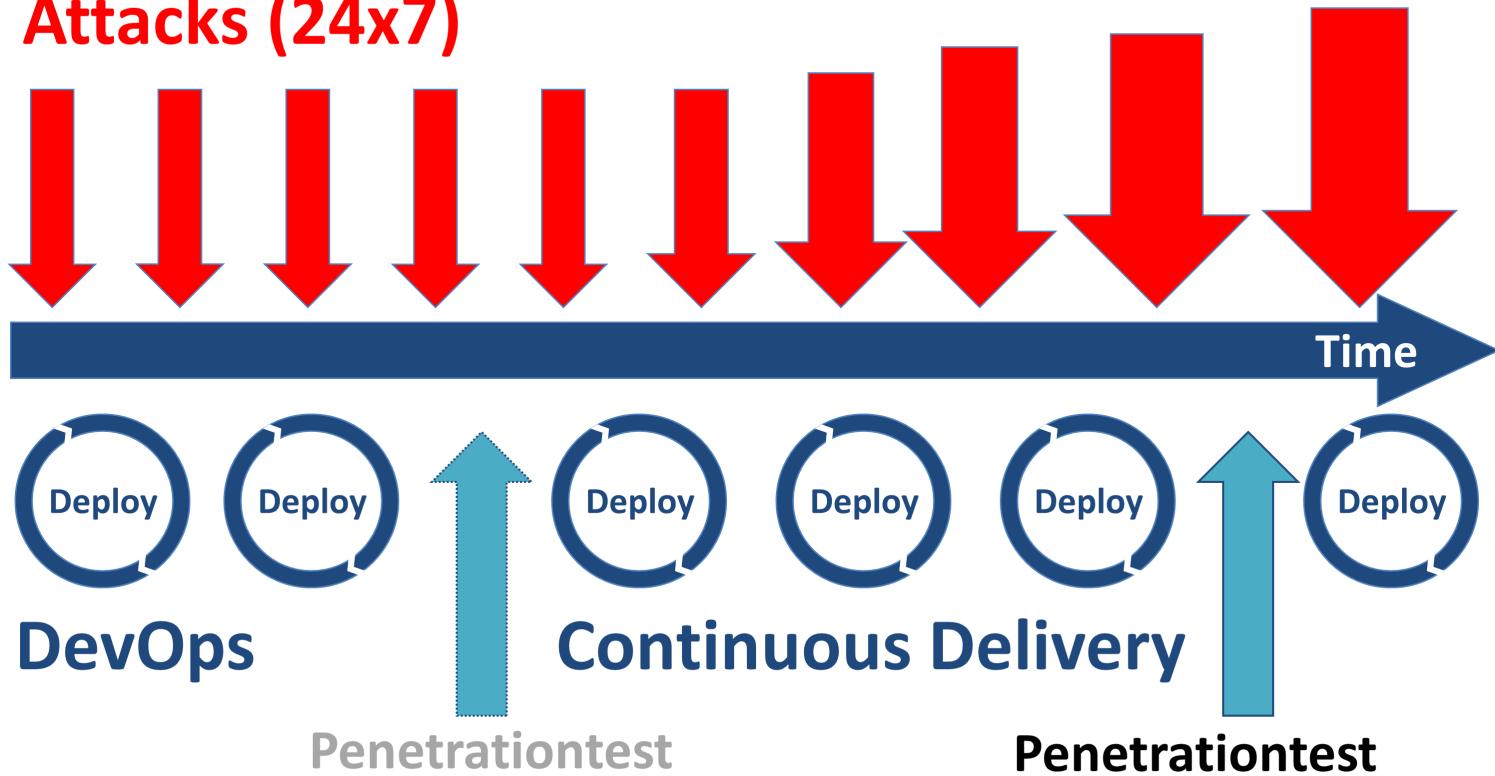
Niemals dem internen Netzwerk blind vertrauen!

PEN-TEST KURZ VOR “GOING LIVE”

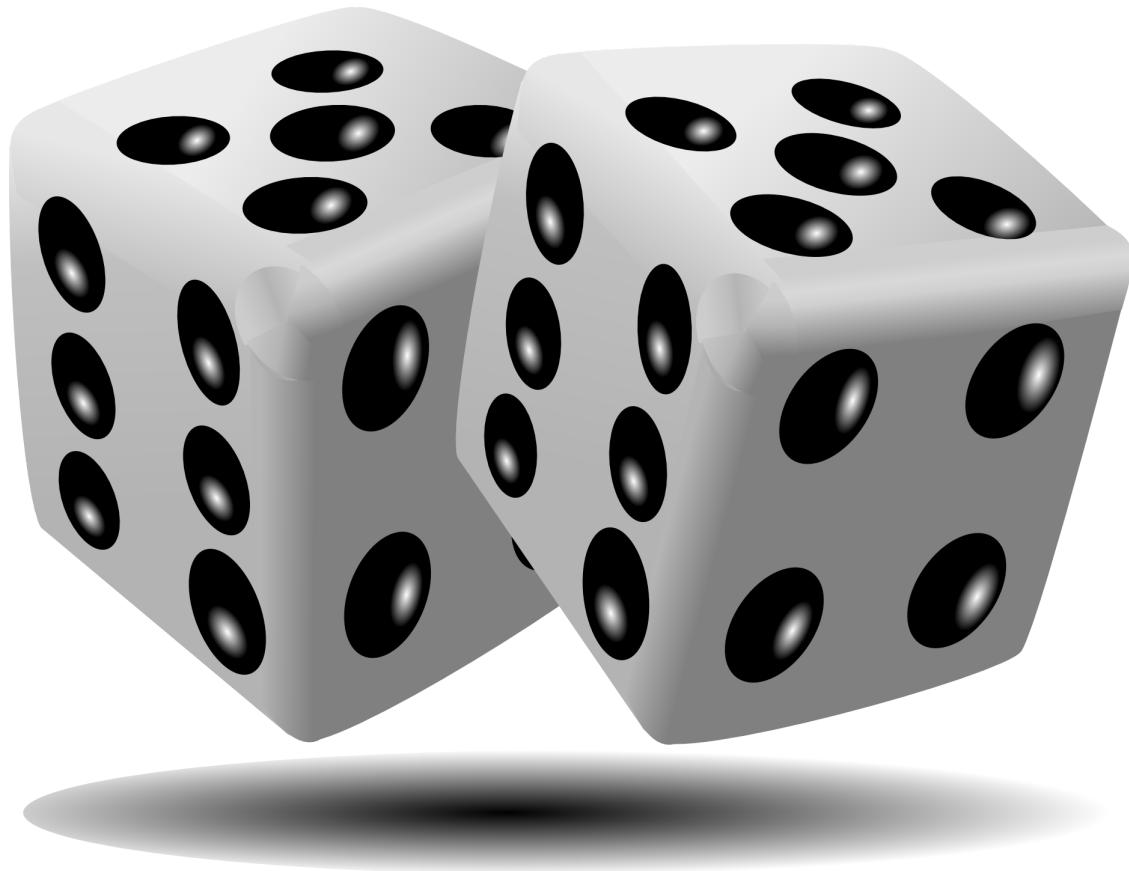
“Wir testen die Sicherheit in die Software hinein”



Attacks (24x7)



WEITER SO ?



WAS NUN ?



TECHNOLOGY STACKS



Applications



kubernetes



Istio

PaaS



Terraform



Cloud Foundry

Cloud Provider



CI/CD



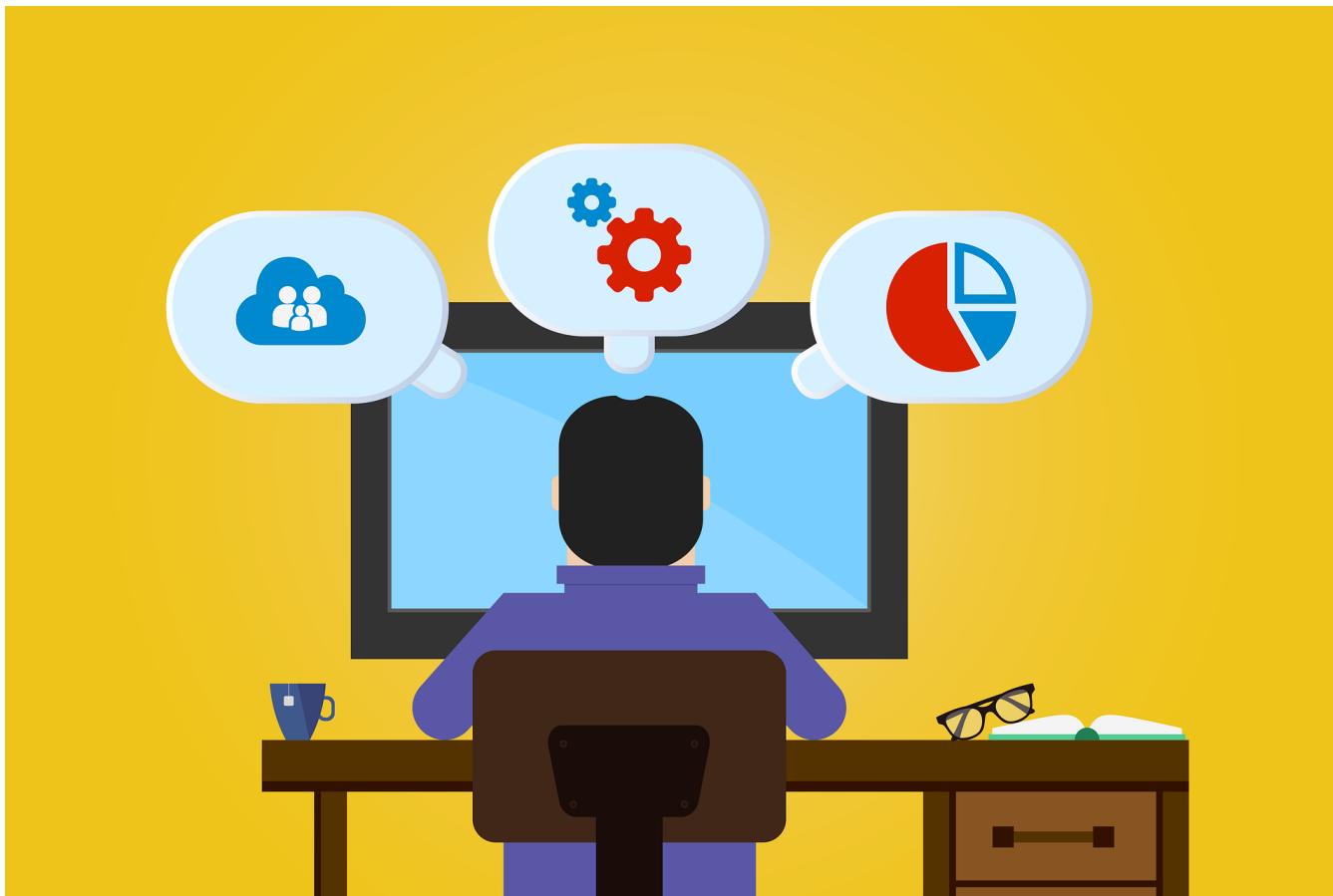
Jenkins



**JFrog
ARTIFACTORY**

Sonatype

SOLL DAS ALLES NUN DER ENTWICKLER MACHEN?



ROTATE, REPAIR, REPAVE

“What if every server inside my data center had a maximum lifetime of two hours? This approach would frustrate malware writers...”

Justin Smith (Chief Security Officer at Pivotal)

Rotate, Repair, Repave (<https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave>)

VERTRAULICHE DATEN

Azure Key Vault

AWS Secrets Manager

Google Cloud HSM

CloudFoundry CredHub

Hashicorp Vault



SICHERE FRAMEWORKS UND TOOLS

Angular 2 should implement security features on-par with Angular 1. This is a tracking issue for all implementation work.

The basic idea is to implement automatic, secure escaping for all values that can reach the DOM by whitelisting known to be safe patterns, comparable to Angular 1's `$sce` service. By default, with no specific action for developers, Angular apps must be secure. To support all use cases, allow users to explicitly bypass security checks for specific values (`sanitizer.bypassSecurityTrust...`).

This follows the [OWASP recommendations on XSS prevention](#).



Password Encoding Upgrades

User's can implement `UserDetailsService` and expose it as a `@Bean` and on authentication success Spring Security's `DaoAuthenticationProvider` will:

- Check to see if the password storage mechanism needs updated using the new `PasswordEncoder.upgradeEncoding` method. For example, if it is encoded in sha256, then by default Spring Security would advise it is upgraded to BCrypt.
- If the password encoding needs to be upgraded, it will encode the password using the current `PasswordEncoder`
- The `UserDetails` and new password will be passed to the `UserDetailsService` so it can be saved with the upgraded password encoding.



Secure

Automatically secure your services through managed authentication, authorization, and encryption of communication between services.



kubernetes

MEHR TRANSPARENZ

Spring Project Vulnerability Reports Published

 ENGINEERING



ROSSEN STOYANCHEV



OCTOBER 16, 2018



0 COMMENTS

The following CVEs have been published today:

1. [CVE-2018-15756](#) for Spring Framework 5.1.1, 5.0.10, and 4.3.20.
2. [CVE-2018-15758](#) for Spring Security OAuth 2.3.3, 2.2.2, 2.1.2, and 2.0.15.

Please, review the information, including affected project versions, in the CVE reports and upgrade immediately.

Spring Boot Users:

Spring Boot 2.0.6 and 1.5.17, released earlier today, contain the fixes for the above vulnerabilities.

<https://spring.io/blog/2018/10/16/spring-project-vulnerability-reports-published>



Agile Praktiken (Scrum, Kanban, XP)

Architektur, Programmiersprachen, Patterns

Unit-, Integration-, E2E-Testing, Monitoring

Authentifizierung, Authz, SQL Injections, XSS, ...

Secret Management, Datenschutz, Verschlüsselung

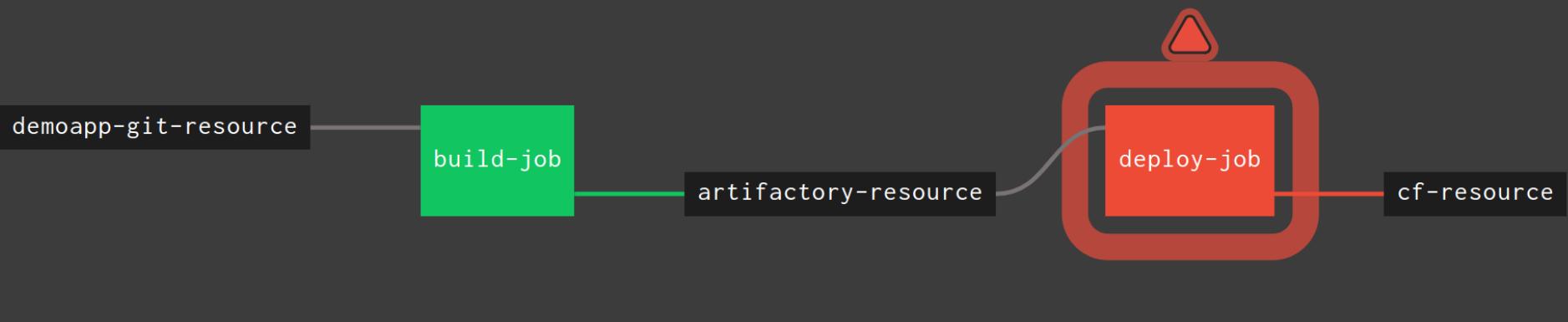
ABSICHERUNG DER CI/CD-PIPELINE

Keine Credentials in VCS (Git, SVN, ...)

Credentials in Jenkins, Concourse,... sicher ablegen

Jenkins & Co regelmäßig aktualisieren

Test Code ist kein 2.Klasse Code



SECDEVOPS

DEVSECOPS

DEVOPSSEC

SECDEVOPS

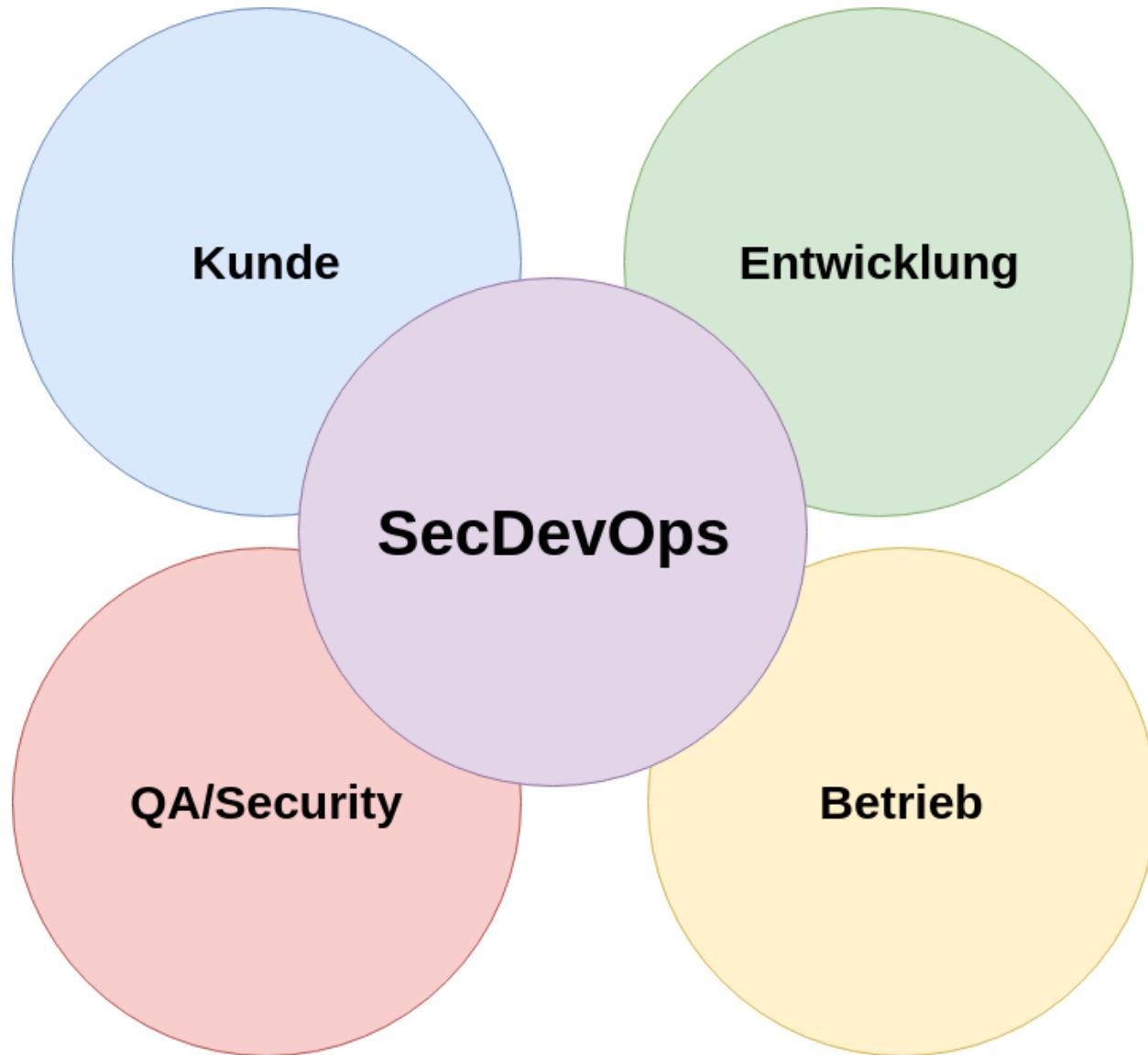
DEVOPSSEC

SECDEVOPS

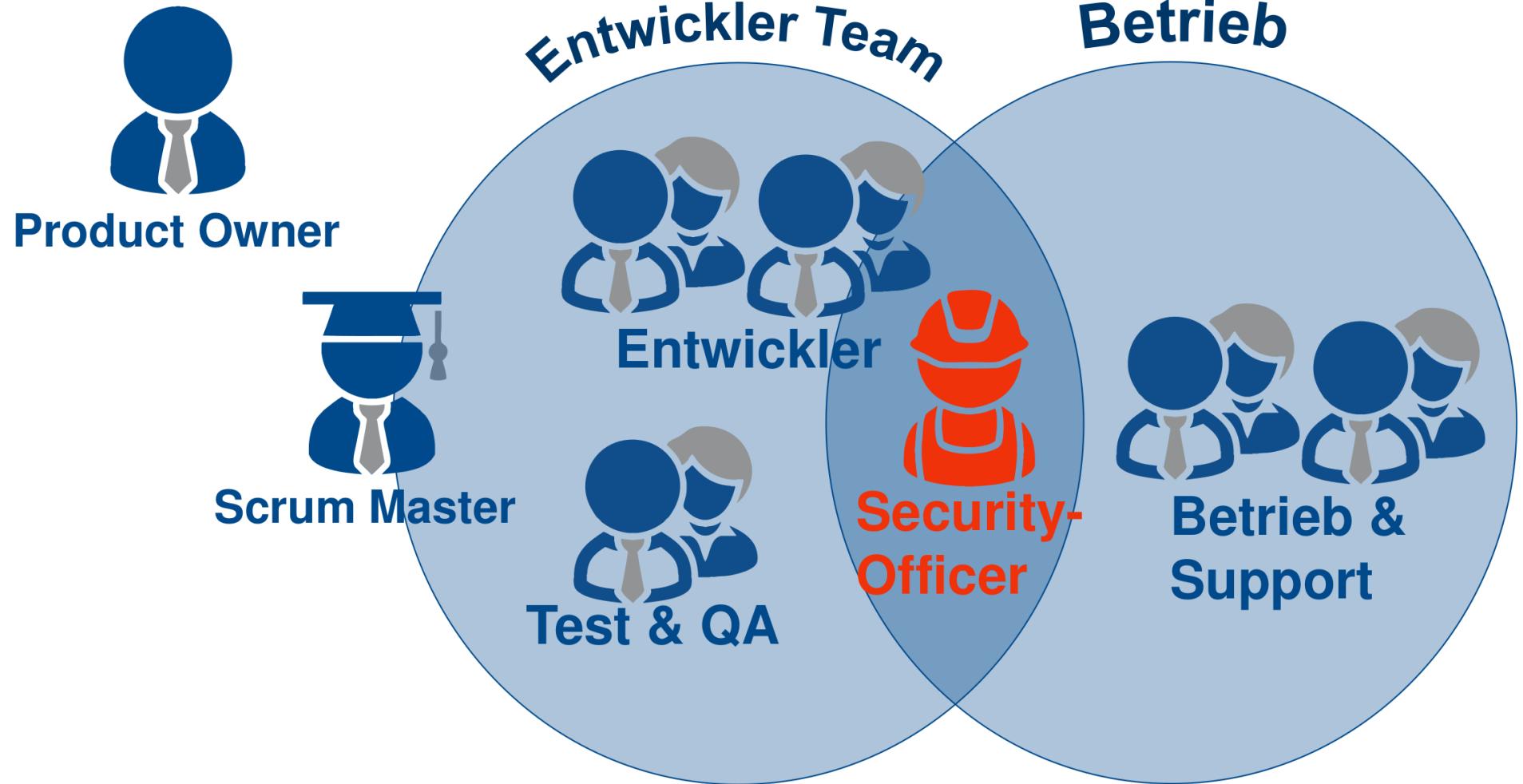
SECDEVOPS

“SHIFT LEFT”

ES GEHT NUR GEMEINSAM



SECURITY OFFICER/CHAMPION



SICHERE ENTWICKLUNGS- PROZESSE ?

Agile

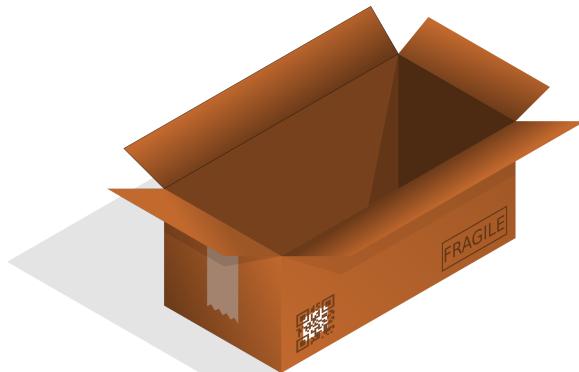


Waterfall

SCRUM GUIDE

“Das Entwicklungsteam besteht aus Profis, die am Ende eines jeden Sprints ein fertiges (*Done*) Inkrement übergeben, welches potenziell auslieferbar ist.”

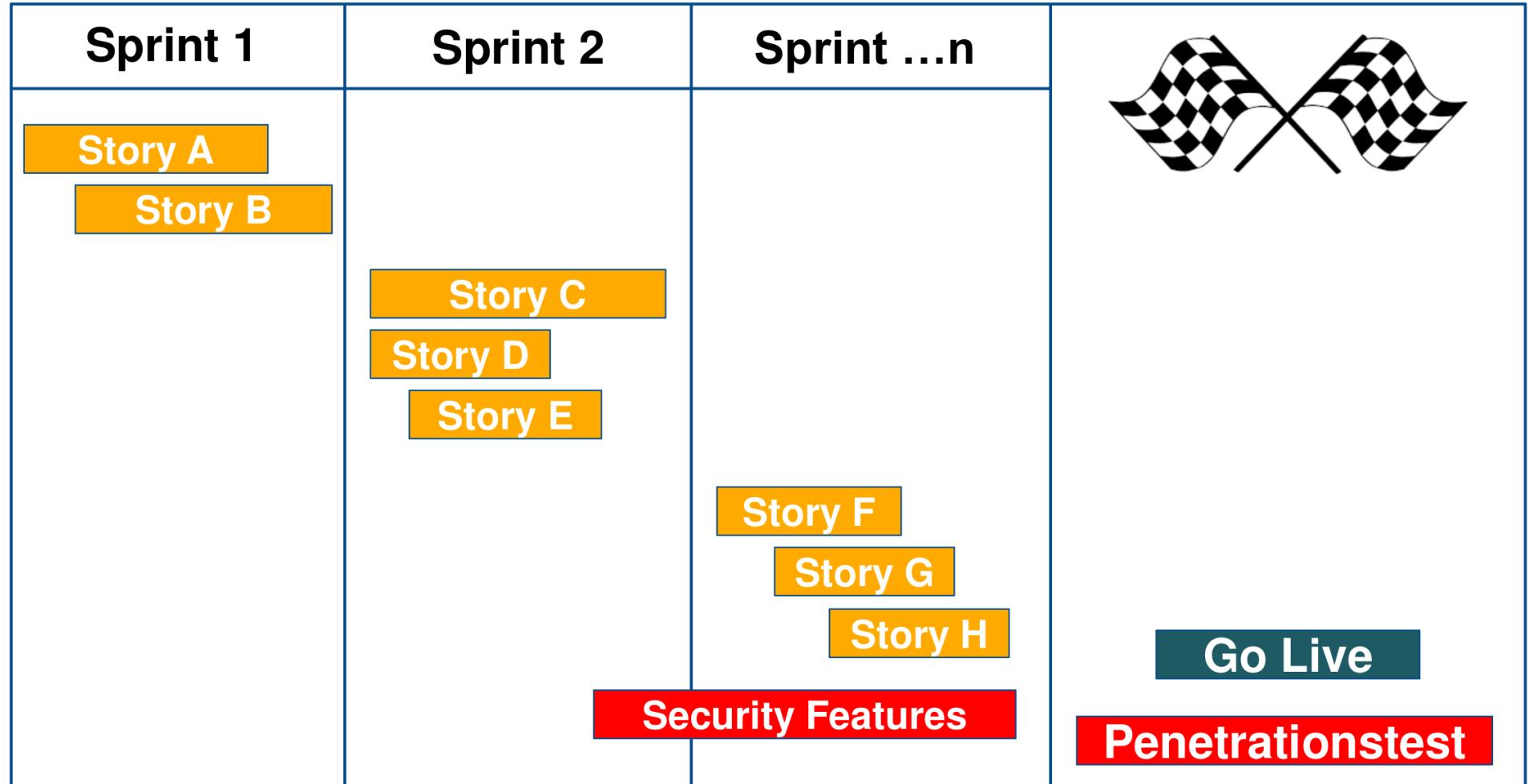
Quelle: www.scrumguides.org



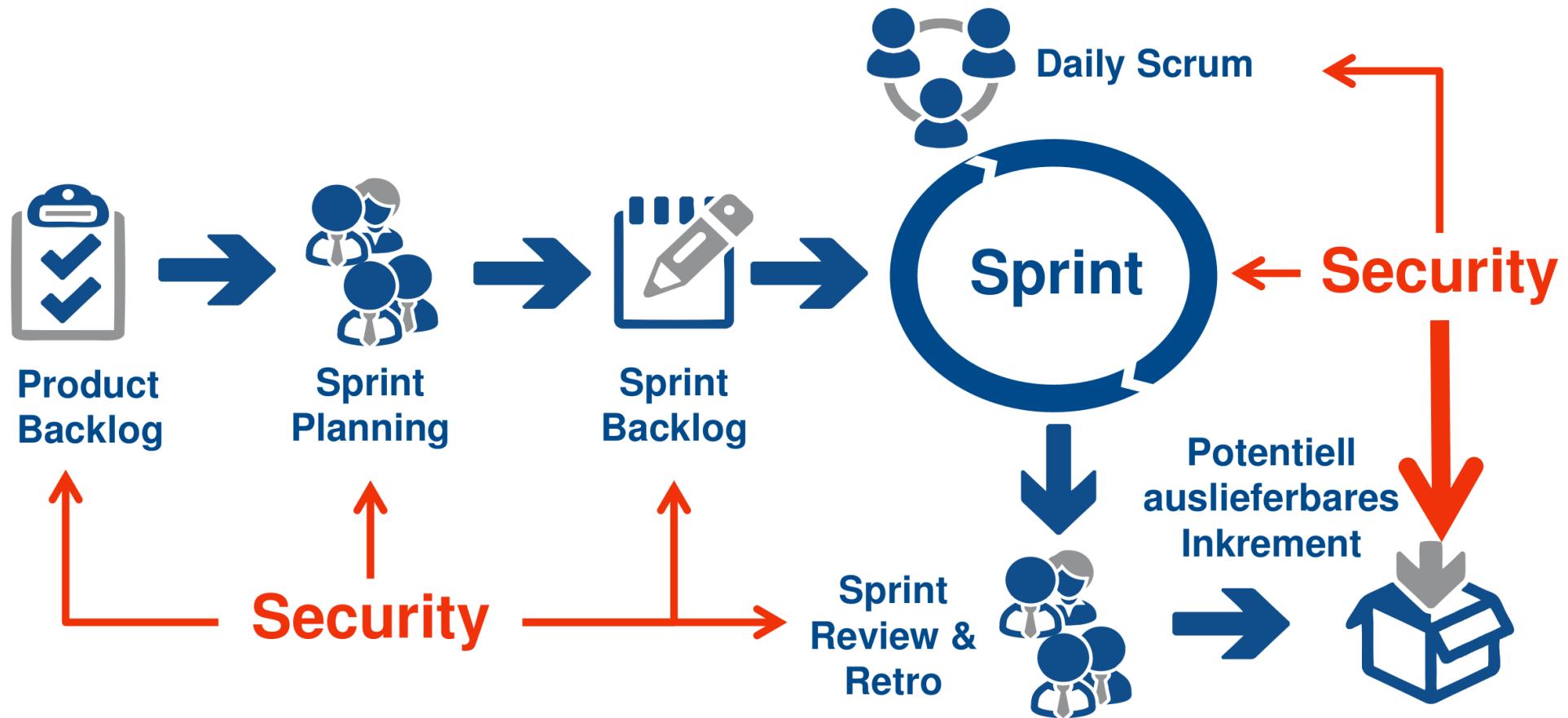
POTENTIELL UNSICHER AUSLIEFERN ?



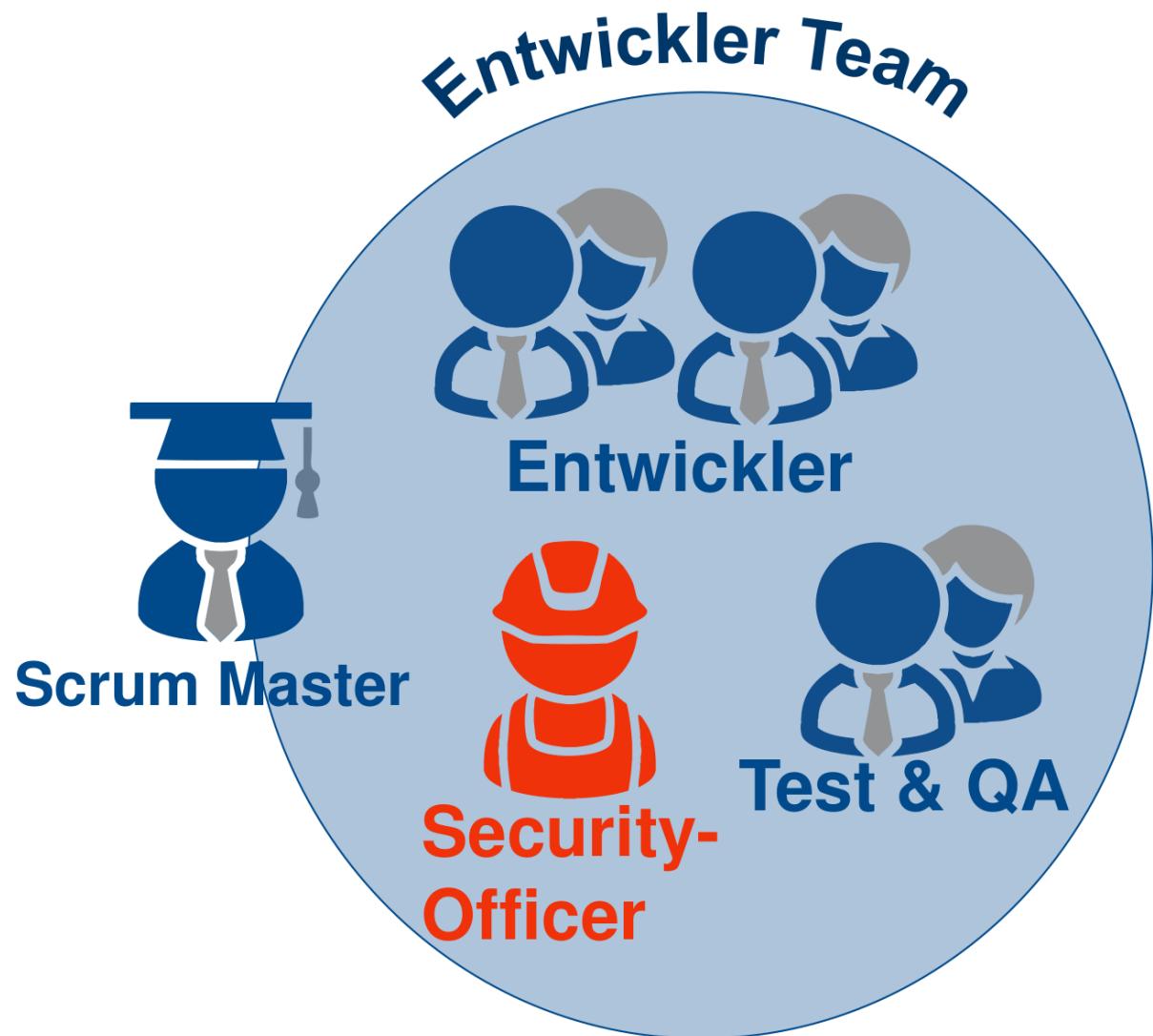
AUSGANGSLAGE: SECURITY != AGIL!



SECURITY IN SCRUM



SECURITY OFFICER/CHAMPION



SECURITY TRAININGS

Product Owner



- Sicherheits-Risiken
- Datenschutz-Risiken
- Threat Modeling
- **AbUser Stories (*Evil Stories*)**

THREAT MODELING IST AUCH AGIL

Produktiv Code erstellen

Security-Tests → Grün!

Test Driven Development (TDD)

Zuerst die Security Tests

Security Testfälle und AbUser Stories

Absicherung gegen Bedrohungen

Festlegung Software-Architektur

User Stories, UML Diagramme

Threat Model

Als

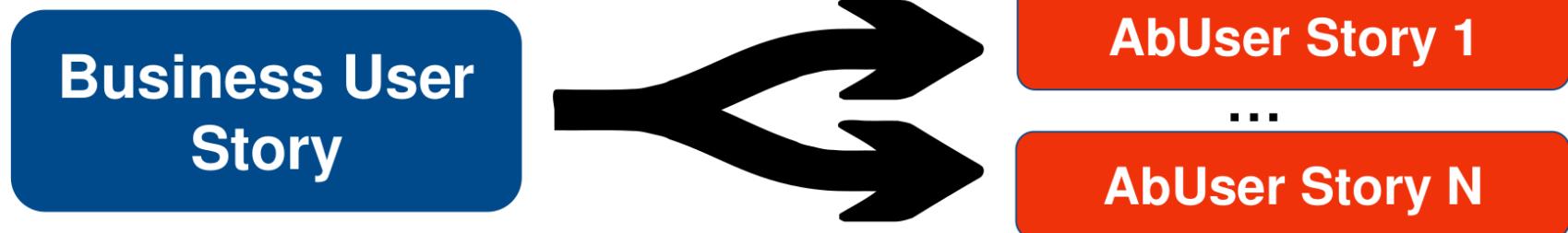
Diskussions-Basis

Identifikation und Vermeidung von Bedrohungen

„Elevation of privilege“ Spiel



ABUSER STORIES



Als Kunde möchte ich Produkte auswählen und zum Warenkorb hinzufügen um diese zu kaufen.

Als Angreifer möchte ich Anfragen so manipulieren um Preise der Produkte im Warenkorb zu ändern.

SECURITY TRAININGS

Development Team



- Threat Modeling
- Secure Design Patterns
- Security Code Reviews
- Security Testing
- Security Dojos

OPEN WEB APPLICATION SECURITY PROJECT



<https://www.owasp.org>

OWASP TOP PROJEKTE

OWASP Top 10

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.]

<https://github.com/OWASP/Top10>

Application Security Verification Standard

<https://github.com/OWASP/ASVS>

Pro Active Controls

https://www.owasp.org/index.php/OWASP_Proactive_Controls

SECURITY DOJO'S JUICE SHOP

The screenshot shows the OWASP Juice Shop v6.3.0 application interface. At the top, there is a navigation bar with links for Login, English, Search, Contact Us, and Score Board. A green success message box displays: "You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)". Below the navigation is a "Score Board" section with a progress bar indicating 2% completion. Under "Difficulty", there are five categories: ★ (1/9 solved), ★★ (0/8 solved), ★★★ (0/21 solved), ★★★★ (0/9 solved), and ★★★★★ (0/6 solved). The main content area is titled "★" and contains a table of challenges:

Name	Description	Status
Admin Section	Access the administration section of the store.	unsolved
Confidential Document	Access a confidential document.	unsolved
Deprecated Interface	Use a deprecated B2B interface that was not properly shut down.	unsolved
Error Handling	Provoke an error that is not very gracefully handled.	unsolved
Five-Star Feedback	Get rid of all 5-star customer feedback.	unsolved
Redirects Tier 1	Let us redirect you to a donation site that went out of business.	unsolved
Score Board	Find the carefully hidden 'Score Board' page.	solved
XSS Tier 1	Perform a <i>reflected</i> XSS attack with <code><script>alert("XSS1")</script></code> .	unsolved
Zero Stars	Give a devastating zero-star feedback to the store.	unsolved

<https://github.com/bkimminich/juice-shop>

SLACK SECURITY CHAMPIONS

Novatec Consult... Andreas Falk

Jump to...

All Threads

Channels

- # bmw-performance-cg
- # ca-aqe
- # ca-aqe-alm
- 🔒 ca-aqe-lead
- # cop-cloud-automation
- # cop-kafka
- # cop-kotlin
- # cop-linux
- # cop-security-champs**
- # cop-software-design
- # cop-topic-leads
- # feedback_website
- # hardrockcafe
- # novasummit-speaker
- # novasummit2018
- # novatec
- # novatec-online
- 🔒 security-group
- # we-go-serverless

#cop-security-champs

☆ | 89 | 0 | For everyone who has questions about Software- or IT-S...



Search



Monday, June 18th

Monday, June 25th



09:02

@all Welcome @mwa to the security group!

We just found out at the Sommerfest that @mwa studied IT security and has experiences with pentesting and is interested in the topic!



09:03

Good morning everybody!

Wednesday, July 25th



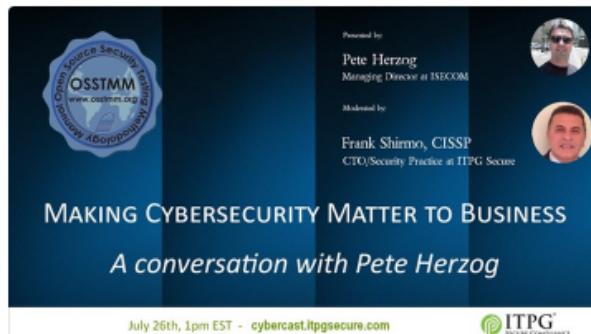
08:39

Guten Morgen Zusammen, falls jemand Interesse hat <https://www.brighttalk.com/webcast/14987/324971>

B brighttalk.com

Making Cybersecurity Matter to Business - A conversation with Pete Herzog

In early 2000, the Open Source Security Testing Methodology Manual (OSSTMM) was released with the primary objective of improving how the enterprise conducted security testing. Key sections of this met... (305 KB) ▾





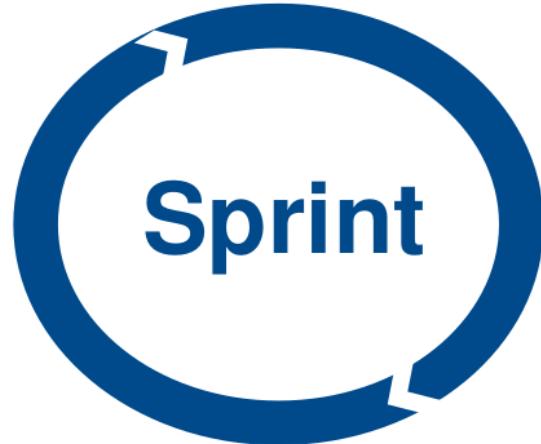
Product Backlog

- Threat Model Refinement
- **Ab**User Stories erstellen
- Security Features mit hoher Prio
- Akzeptanzkriterien für Sicherheit



Sprint Planning

- Detaillierung Threat Model
- Akzeptanzkriterien für Sicherheit
- Security Patterns diskutieren
- Security Testfälle



- Secure Design / Coding
- Pairing mit Security-Officer/Champion
- Security-Aware DoD
- Security Code Reviews
- Security Testing

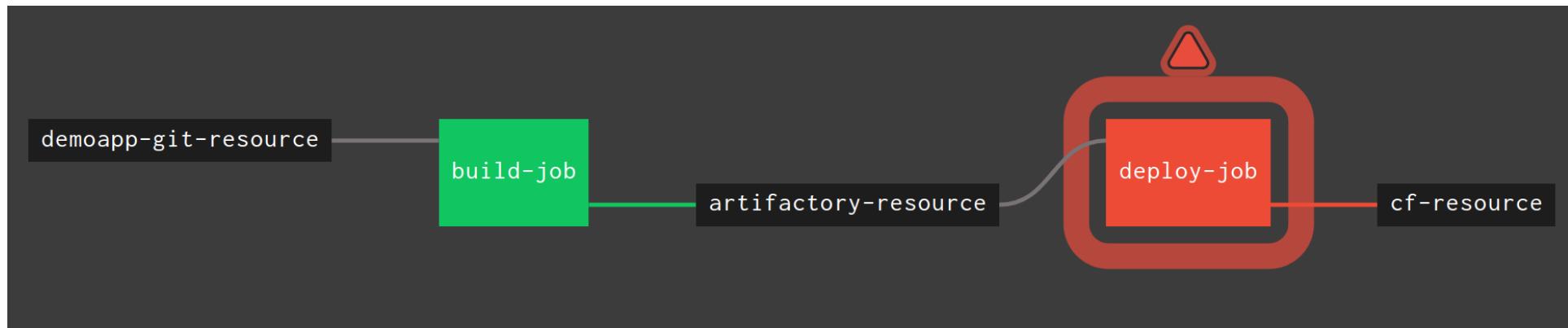
ENTWICKLER SECURITY TESTS

BEVOR EIN ANGREIFER “TESTET”

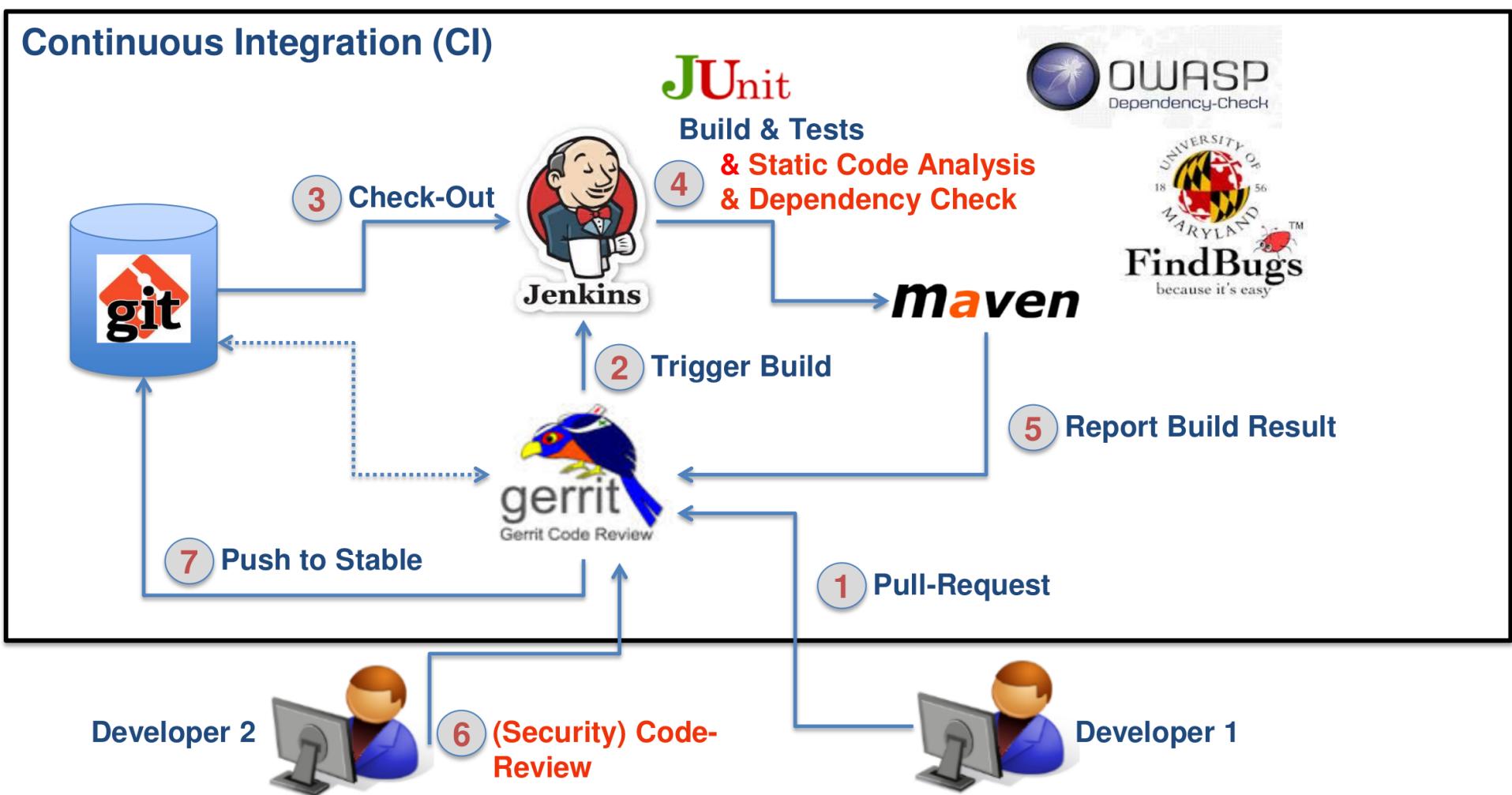
- Security Unit/Integrationstests
- OWASP ZAP
- Burp Suite Free Edition
- SQLMap

CI/CD PIPELINES

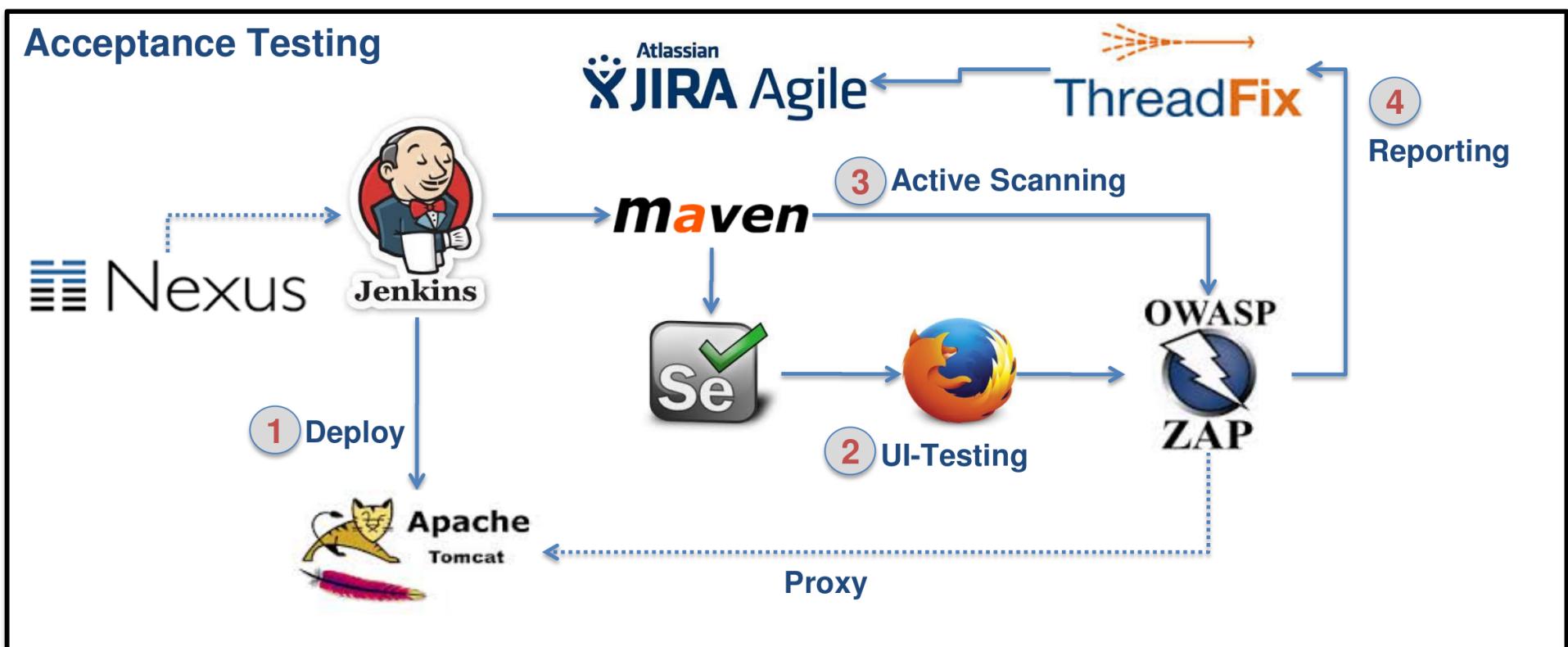
Continuous Delivery/Deployment ermöglicht
schnelle Reaktion mit Security-Fixes



CI COMMIT-STAGE MIT STATISCHER ANALYSE (SAST)



CI SECURITY-STAGE MIT DYNAMISCHER ANALYSE (DAST)

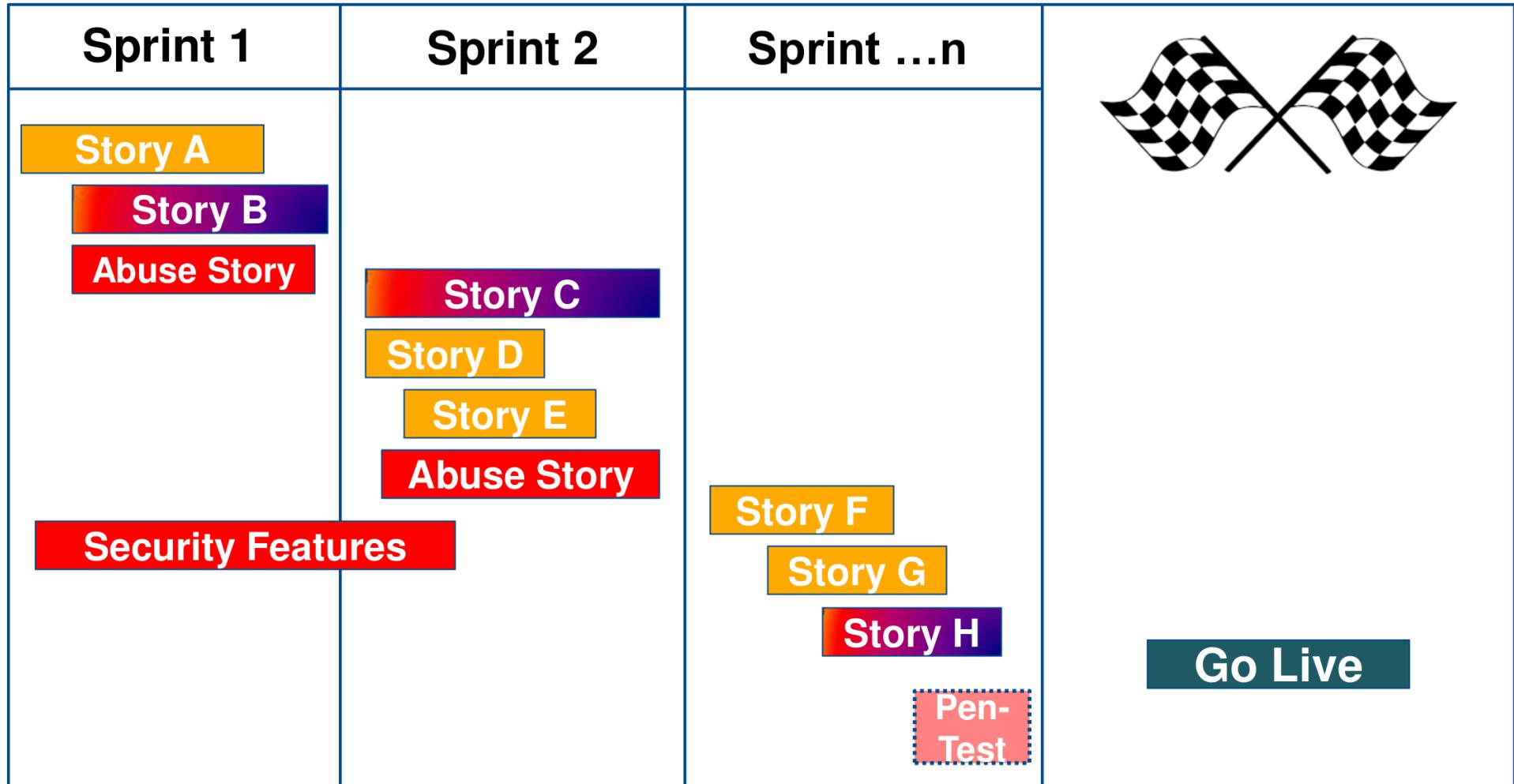




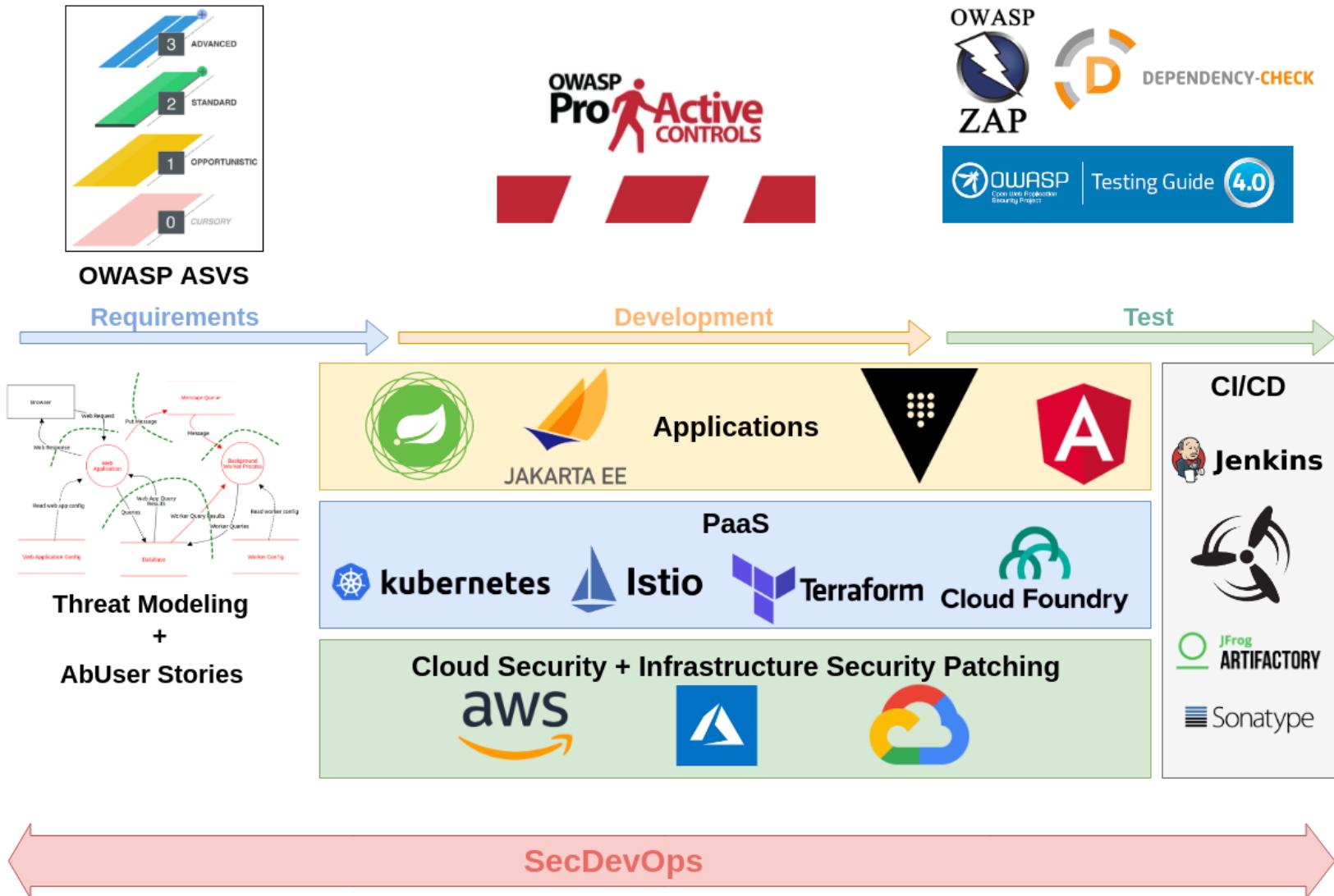
Sprint Review & Retro

- Transparenz der Security gegenüber Stakeholdern
- Inspect & Adapt aller Security-Aktivitäten

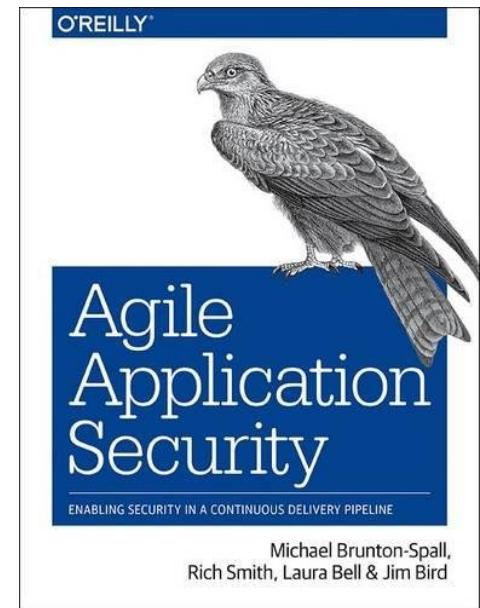
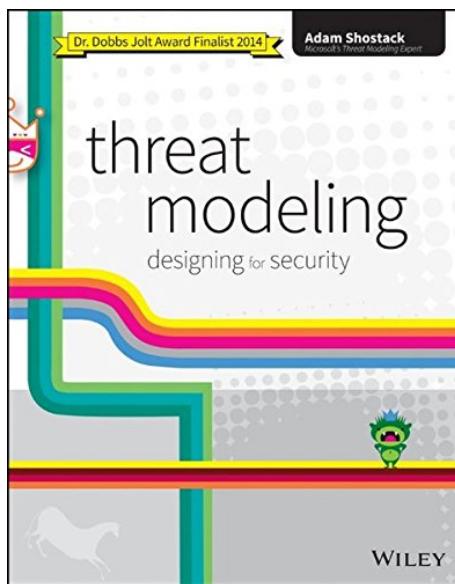
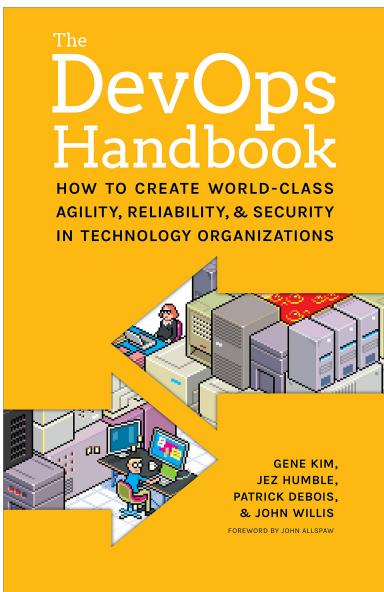
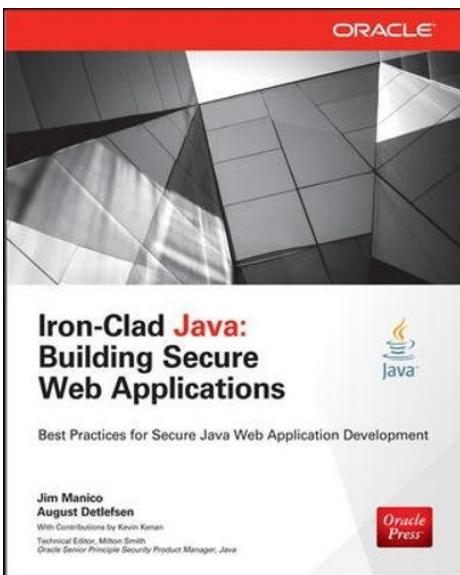
IDEALZUSTAND: SECURITY == AGIL!



THE BIG PICTURE



BOOK REFERENCES



Q&A

<https://www.novatec-gmbh.de/beratung/agile-security>

<https://blog.novatec-gmbh.de>

andreas.falk@novatec-gmbh.de
@andifalk



IT-Tage 2018 (Frankfurt)
12.12.2018

[Continuous Delivery-Pipelines mit Concourse CI](#)

ONLINE REFERENCES

- [Shodan.io](#)
- [Verzeichnis der ISO 27034 Teile](#)
- [Deutschland sicher im Netz \(DsiN\): Sicherheitsindex 2018](#)
- [OWASP Top 10 2017 \(<https://github.com/OWASP/Top10>\)](#)
- [Application Security Verification Standard \(<https://github.com/OWASP/ASVS>\)](#)
- [Pro Active Controls
\(\[https://www.owasp.org/index.php/OWASP_Proactive_Controls\]\(https://www.owasp.org/index.php/OWASP_Proactive_Controls\)\)](#)
- <https://docs.microsoft.com/de-de/azure/security/azure-security-threat-modeling-tool>
- <https://github.com/bkimminich/juice-shop>
- [Rotate, Repair, Repave \(<https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave>\)](https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave)

All images used are from [Pixabay](#) and are published under [Creative Commons CC0 license](#).

All used logos are trademarks of respective companies