AGIL ABER SICHER!

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

NOVATEC

UNSERE SOFTWARE IST DOCH SICHER ?

Kritische Sicherheitslücke gefährdet Milliarden WhatsApp-Nutzer UPDATE

Alert! 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.

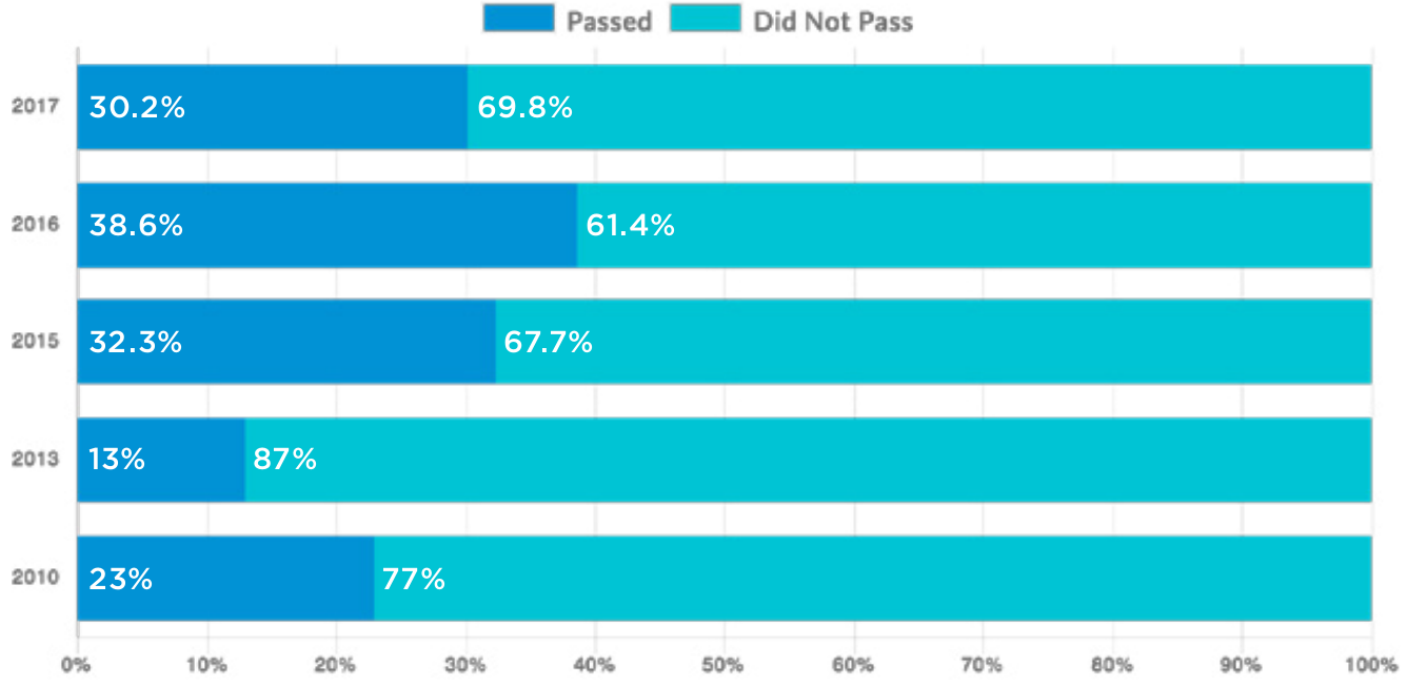
Quelle: heise.de

STATE OF SOFTWARE SECURITY REPORT 2017

(VERACODE)

OWASP TOP 10 POLICY PASS RATE

Percentage of Applications Passing on First Scan

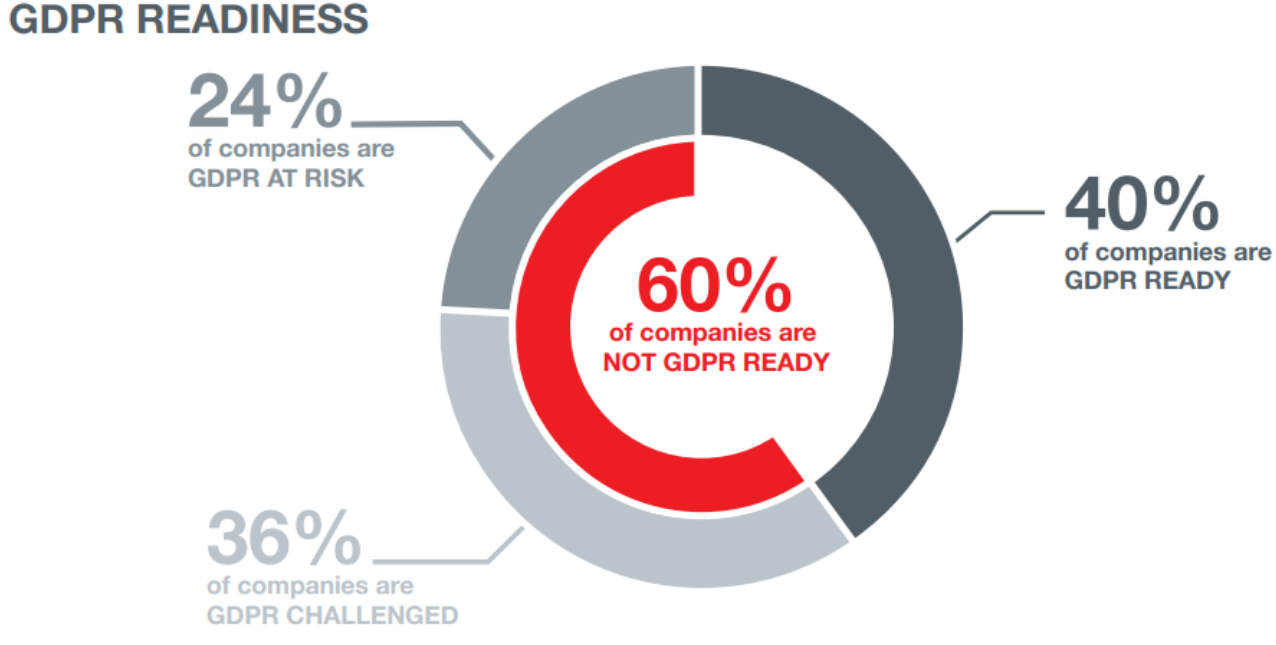


Quelle: veracode.com

SECURITY IST NICHT MEIN JOB !?

EU DATENSCHUTZ GRUNDVERORDNUNG

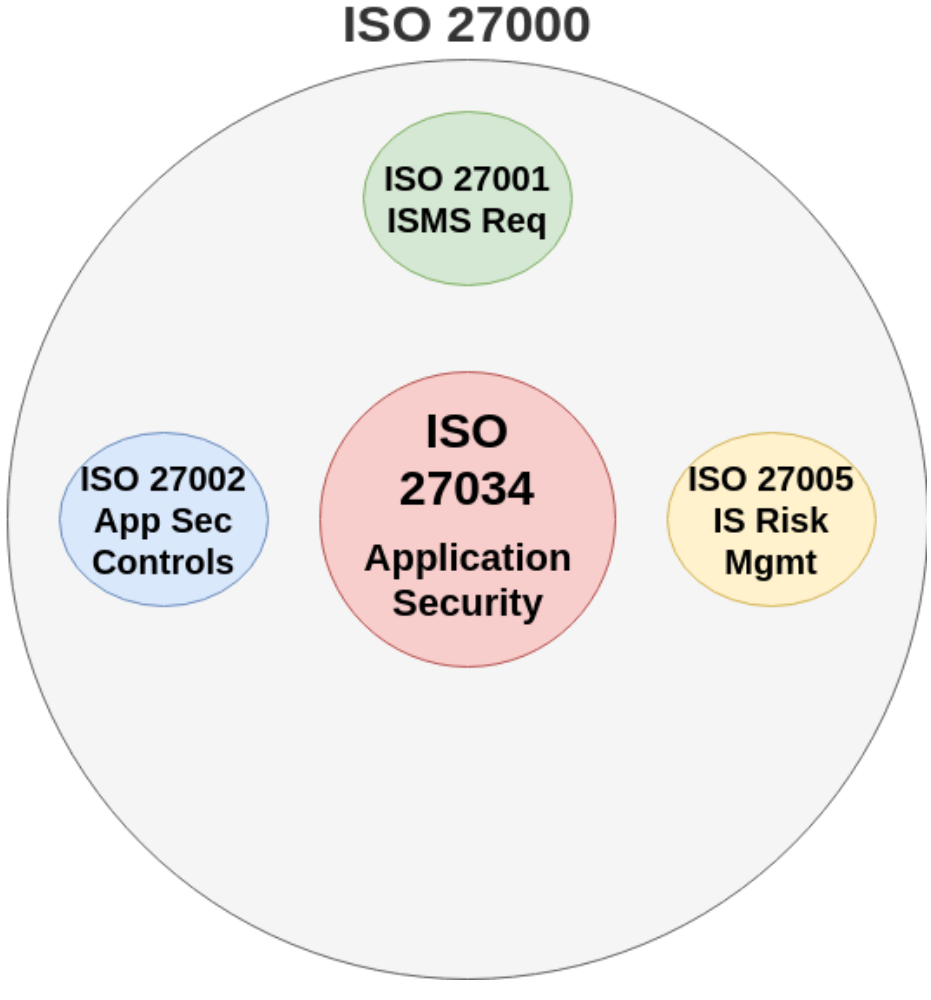
Seit Mai 2018 geltendes Recht!



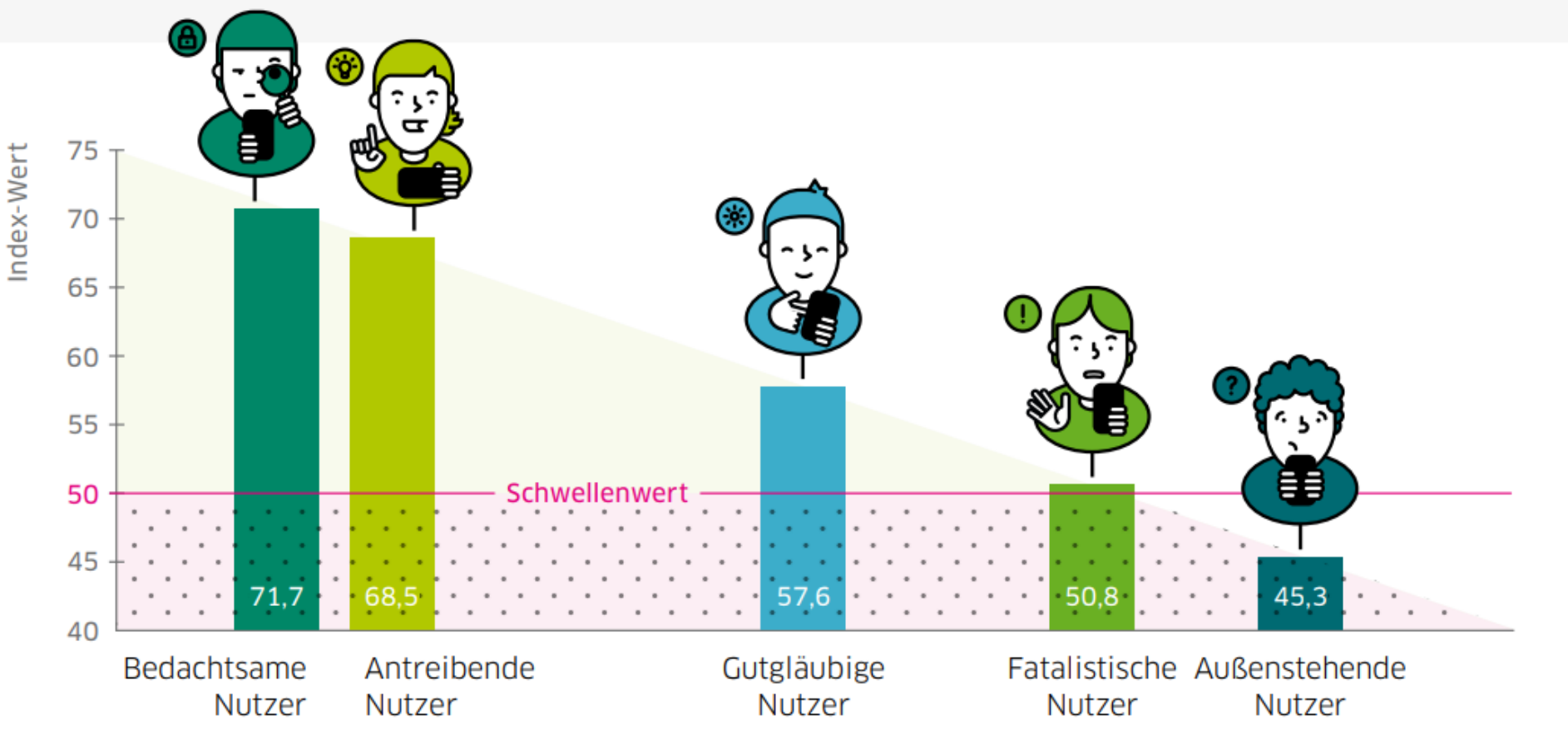
Quelle: GDPR's Missing Link Report (senzing.com/gdpr)

ISO 27034

Neuer Standard für Anwendungssicherheit

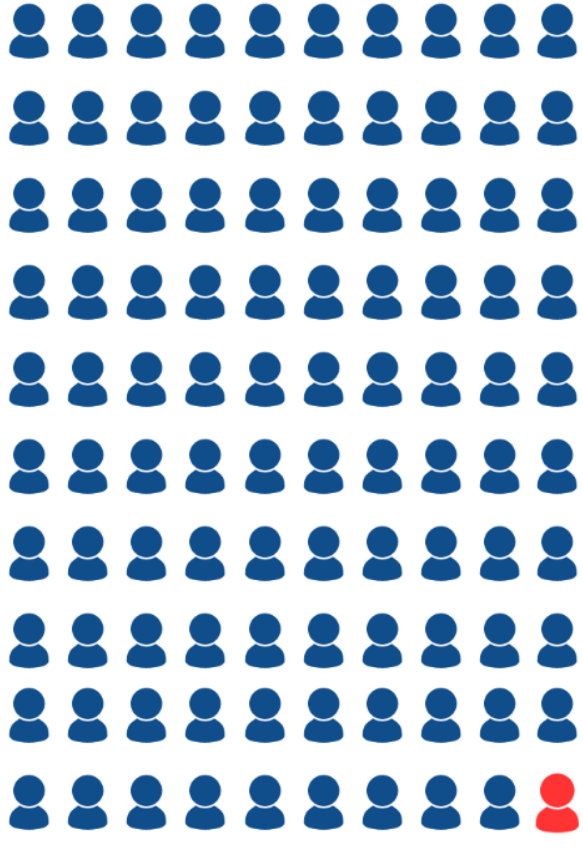


NUTZERVERHALTEN



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

1 SECURITY-PROFESSIONAL FÜR 100 ENTWICKLER

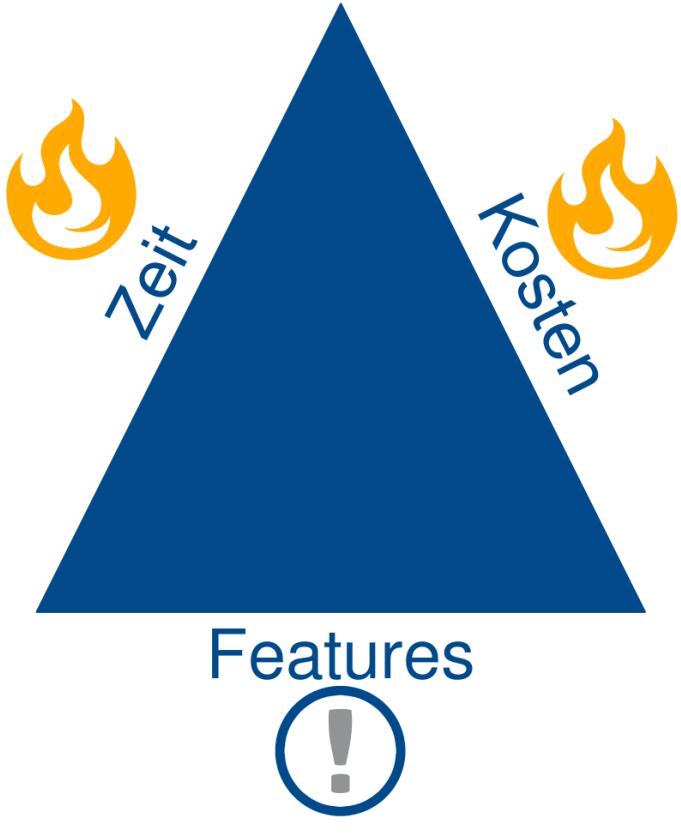


Quelle: sonatype.com/devops-survey-report

SICHERHEIT

IM PROJEKTALLTAG

WIR HABEN DOCH KEINE ZEIT



~~Dokumentation~~

~~Security / Tests~~

Features!

HACKER FINDEN UNS NICHT !

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.

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!

Monitor Network Security

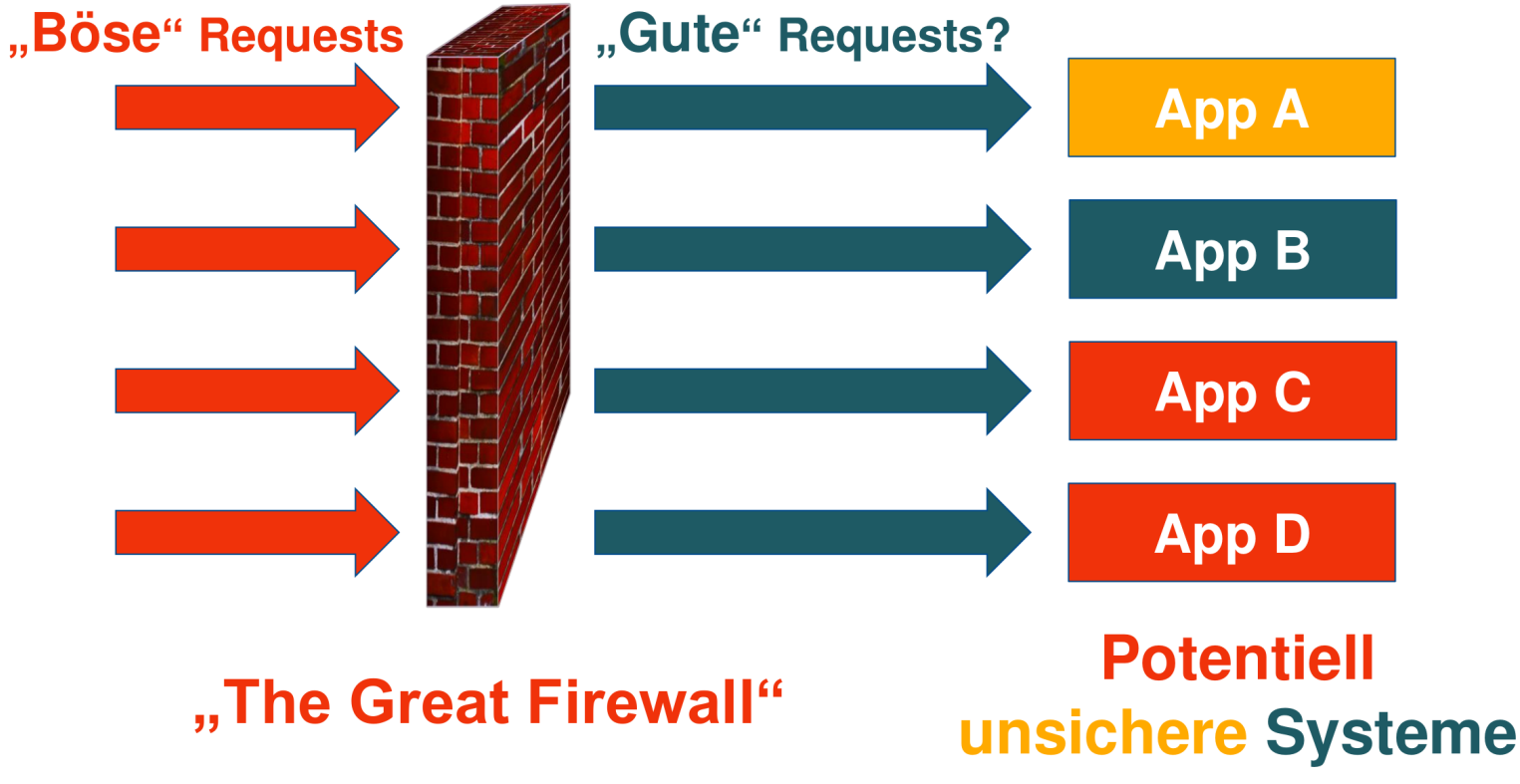
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

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

Quelle: shodan.io

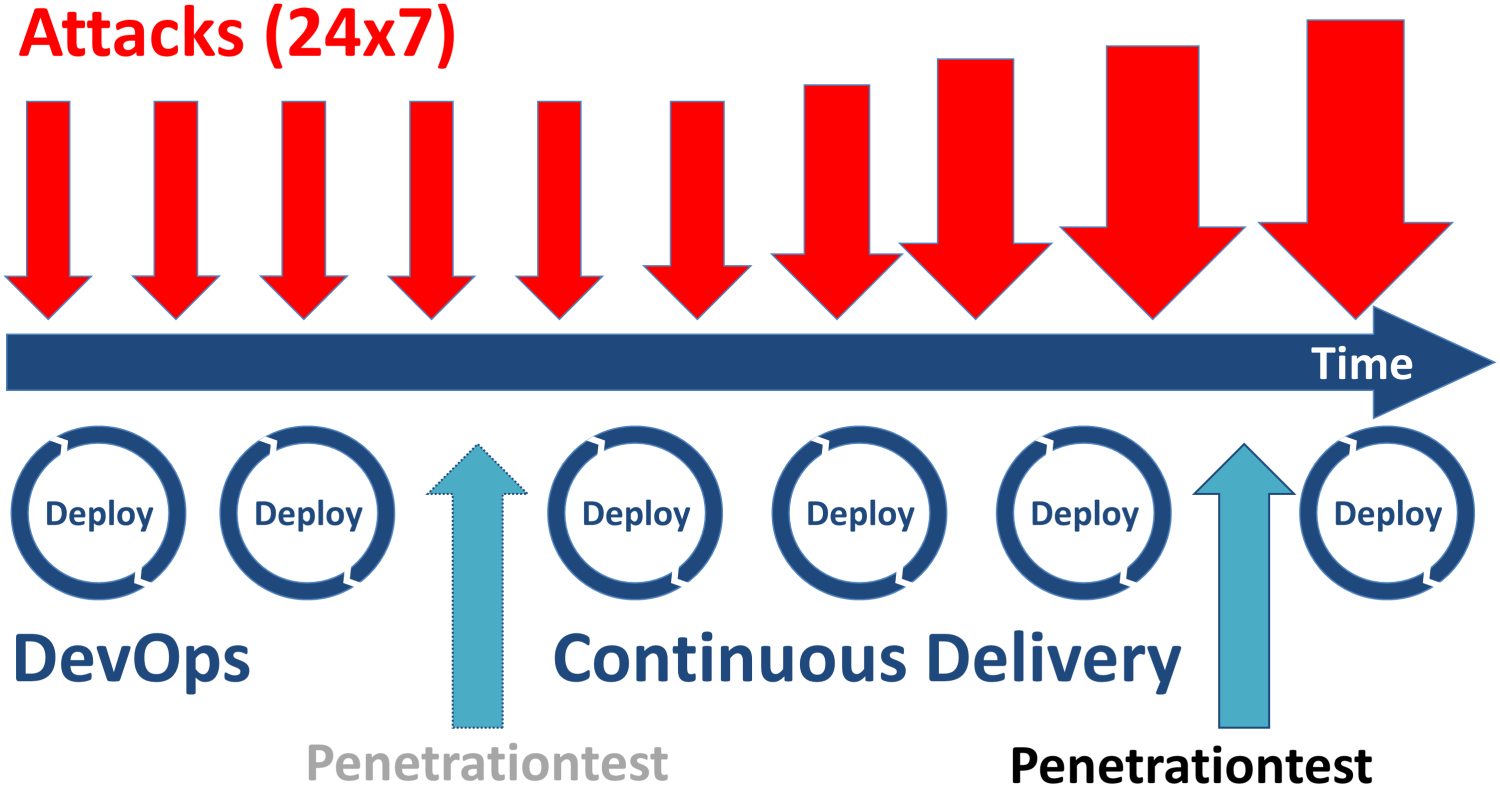
WIR HABEN DOCH EINE FIREWALL!



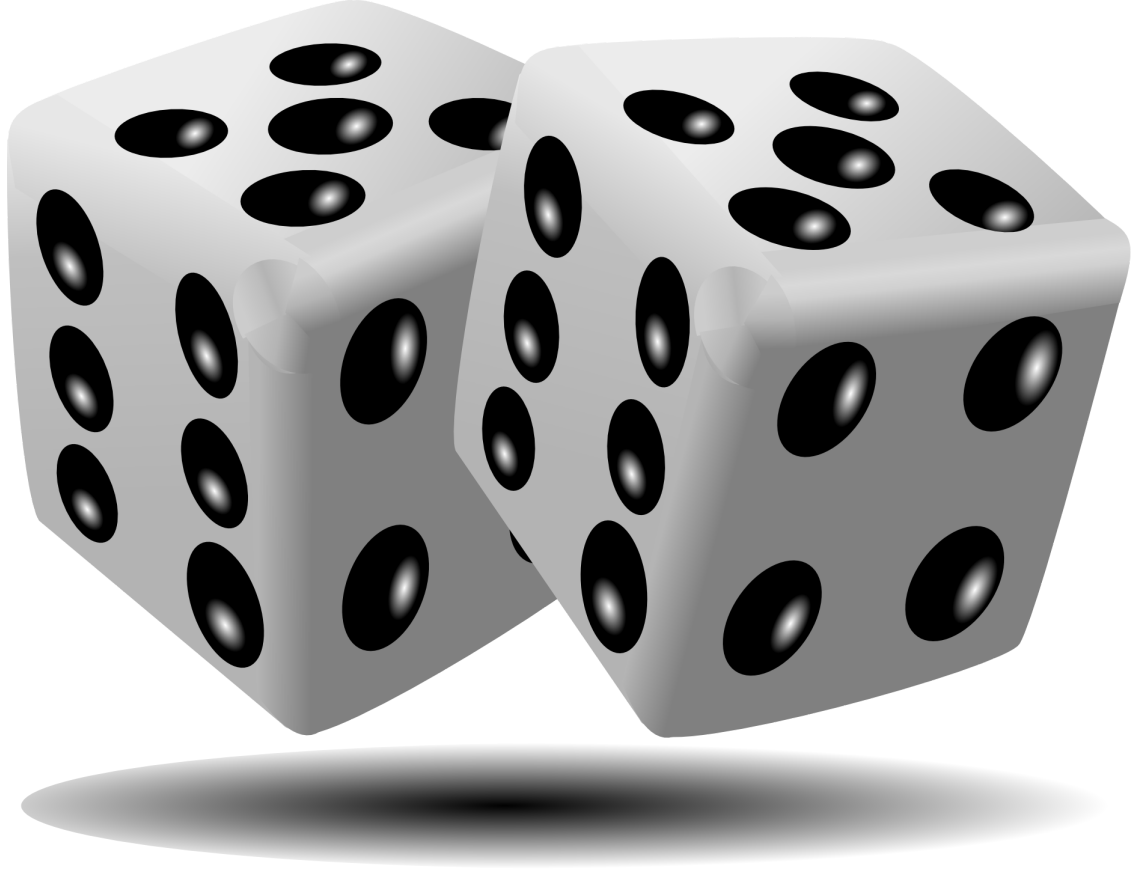
Niemals dem internen Netzwerk blind vertrauen!

PEN-TEST KURZ VOR “GOING LIVE”

“Wir testen die Sicherheit in die Software hinein”

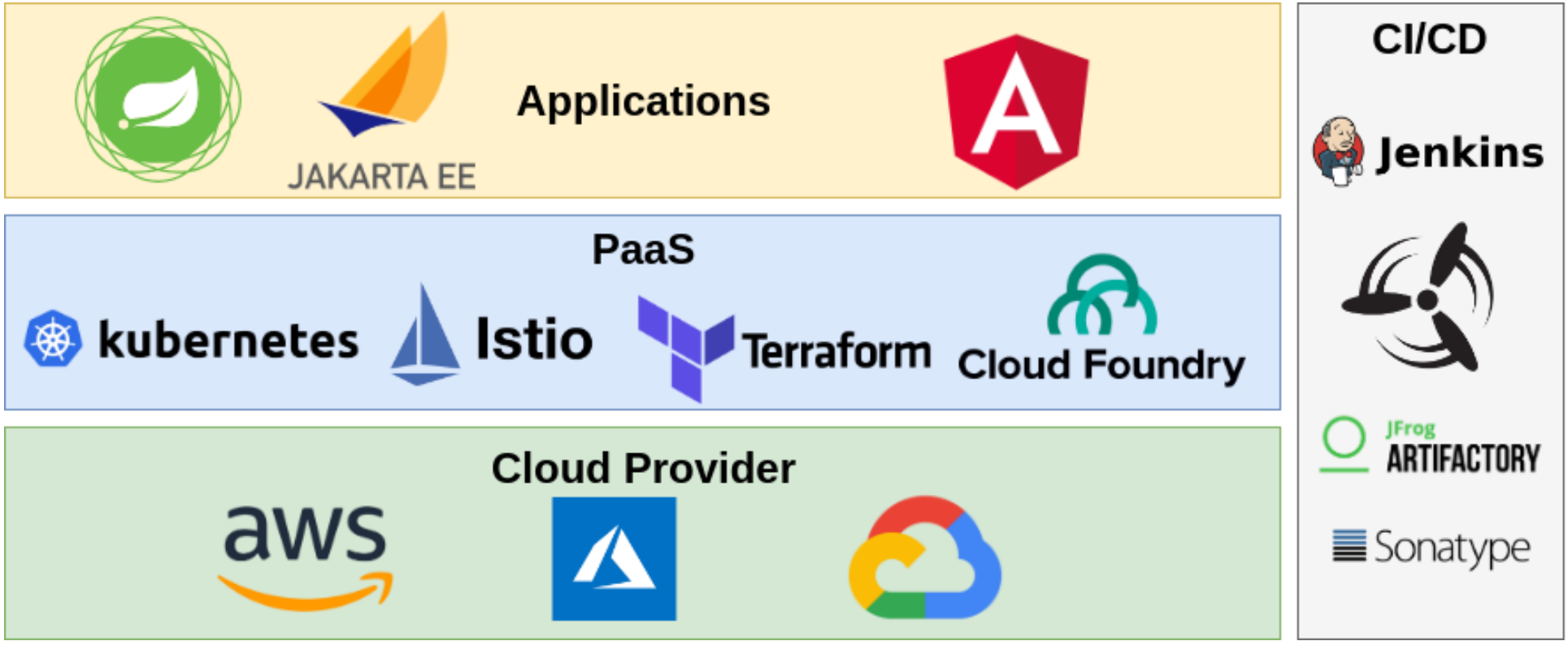

Attacks (24x7)
Time
Deploy
Deploy
Deploy
Deploy
Deploy
Deploy
DevOps
Continuous Delivery
Penetrationtest
Penetrationtest

WEITER SO ?

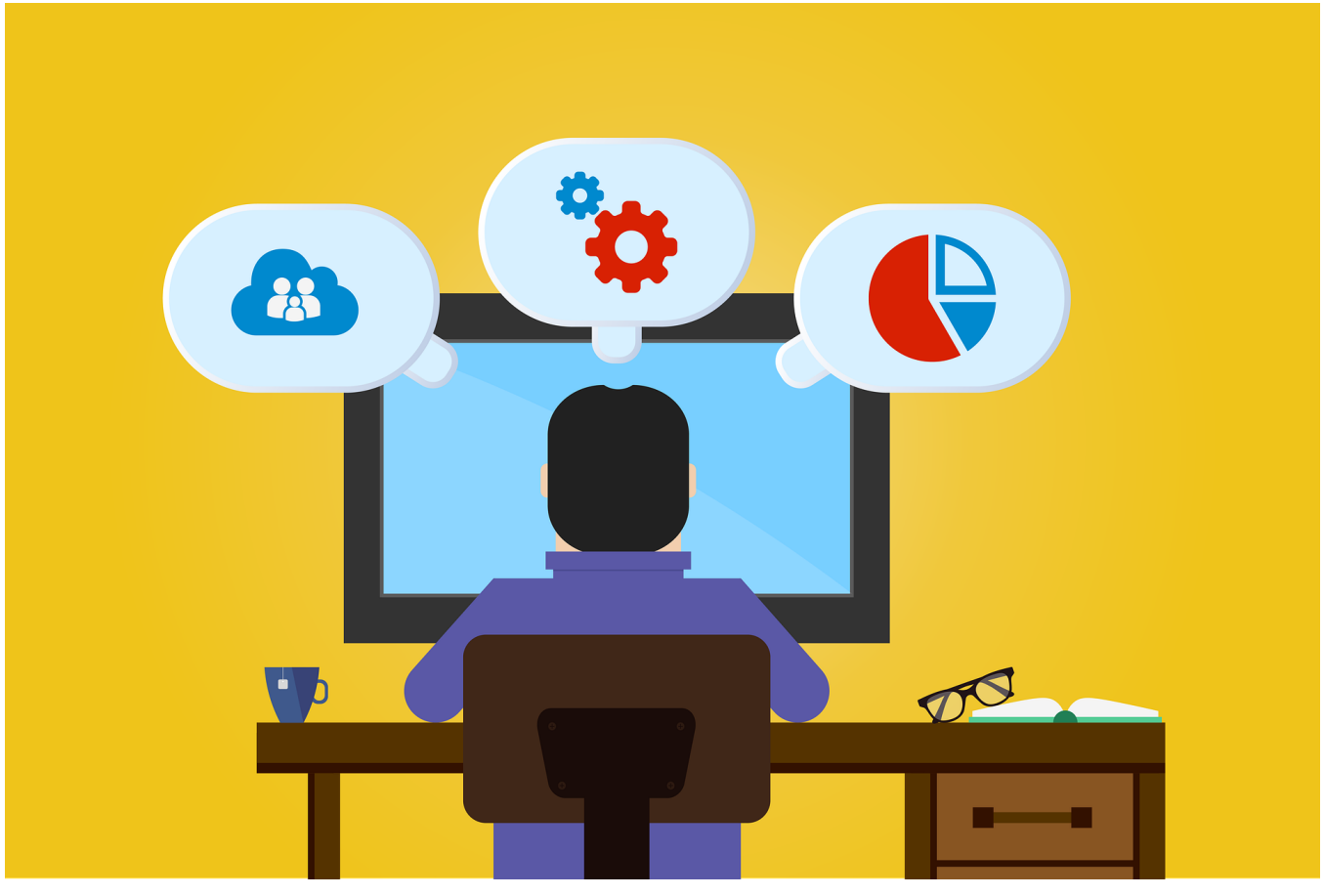


WAS NUN ?

TECHNOLOGY STACKS



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.

Secure

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

Password Encoding Upgrades

User's can implement UserDetailsPasswordService 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 `UserDetailsPasswordService` so it can be saved with the upgraded password encoding.

MEHR TRANSPARENZ

Spring Project Vulnerability Reports Published

ENGINEERING  ROSSEN STOYANCHEV OCTOBER 16, 2018 0 COMMENTS

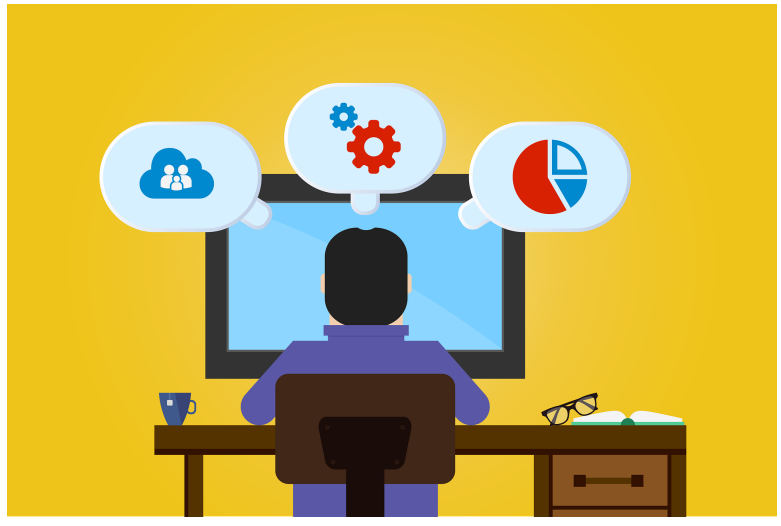
The following CVEs have been published today:

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

SECDEVOPS

DEVSECOPS

DEVOPSSEC

SECDEVOPS

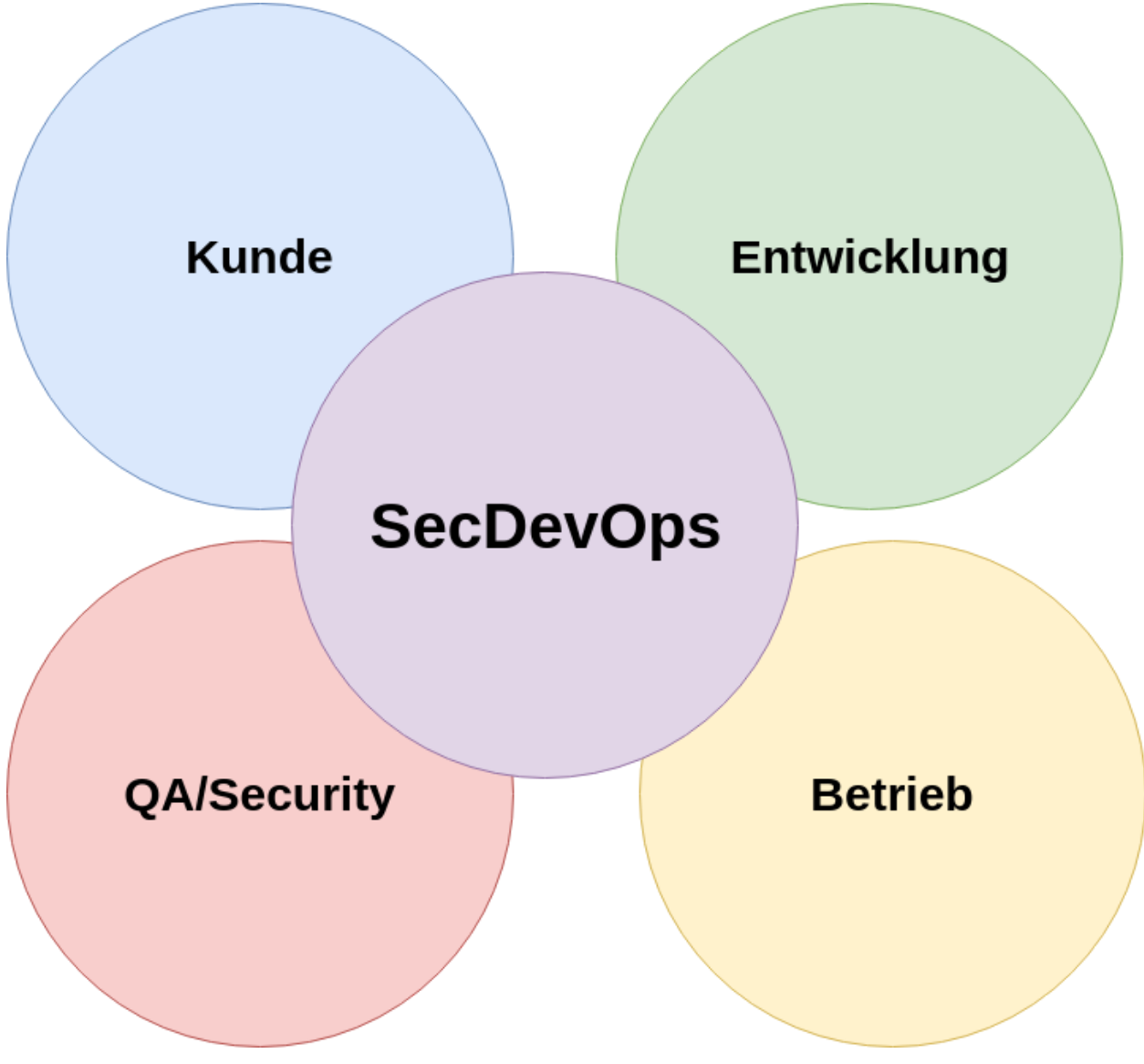
DEVOPSSEC

SECDEVOPS

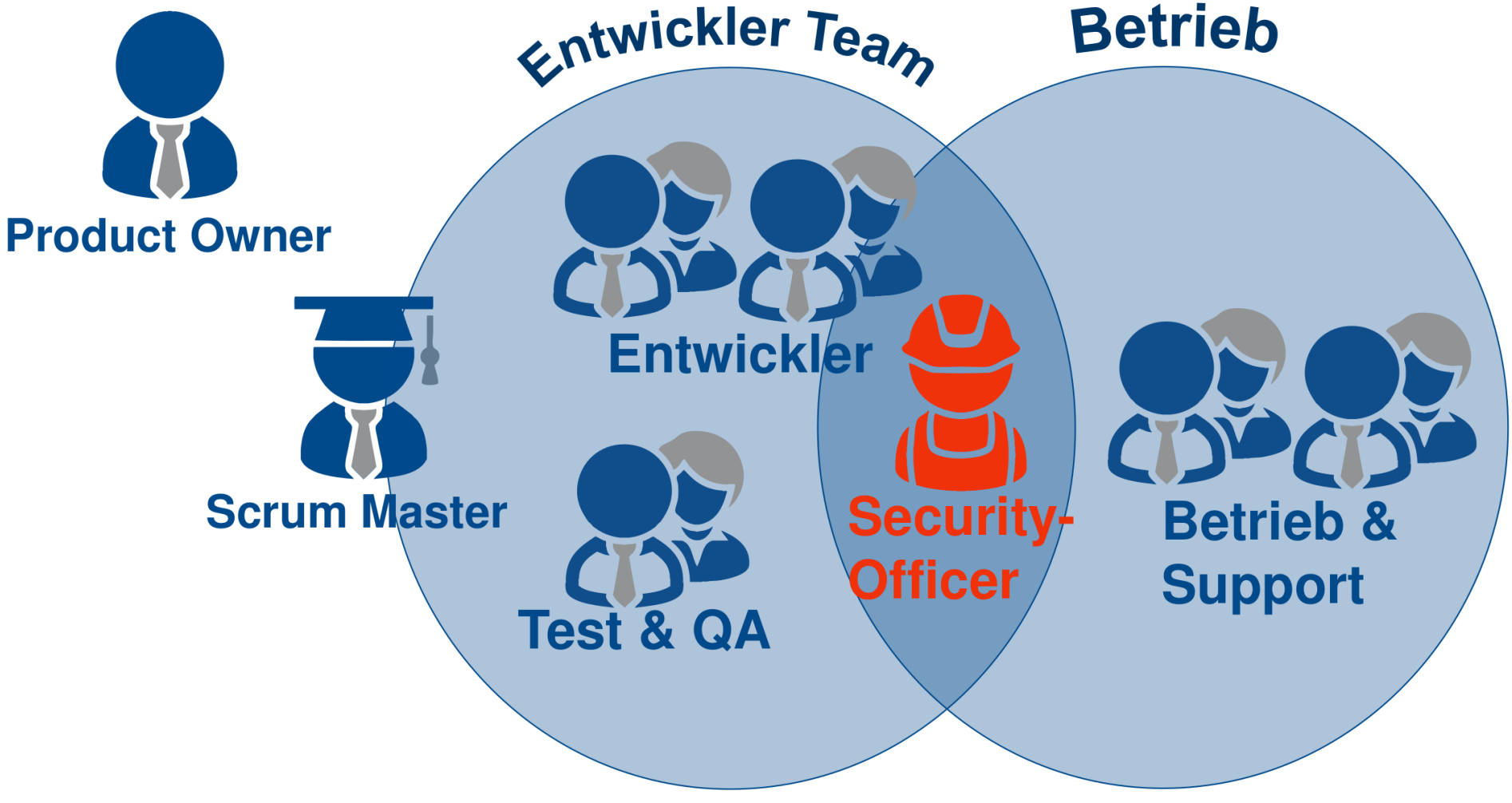
SECDEVOPS

“SHIFT LEFT”

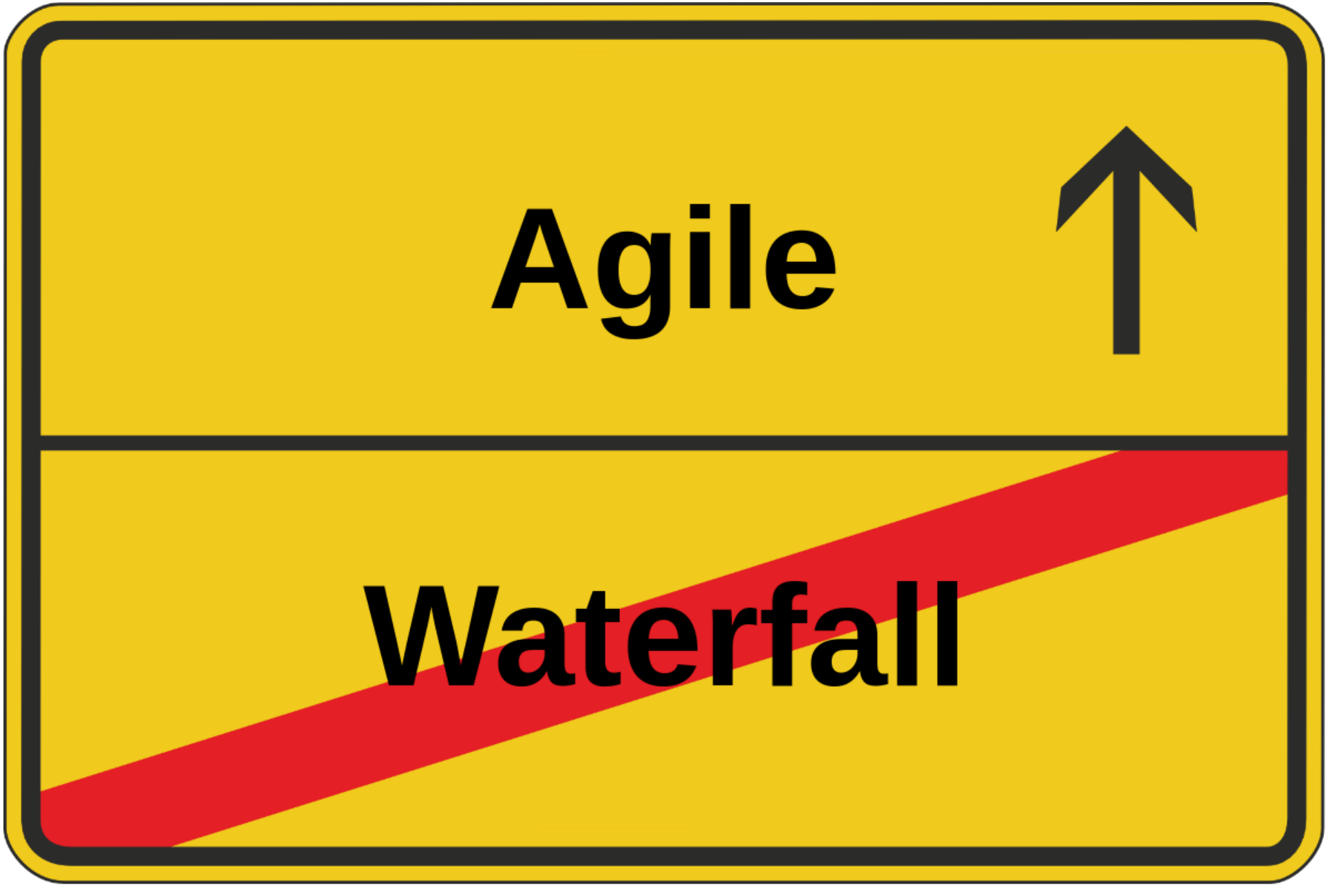
ES GEHT NUR GEMEINSAM



SECURITY OFFICER/CHAMPION



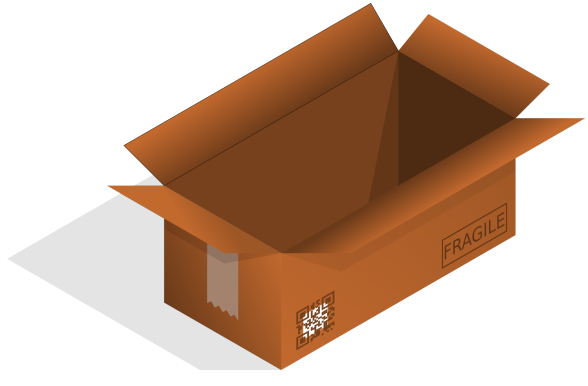
SICHERE ENTWICKLUNGS-PROZESSE ?


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

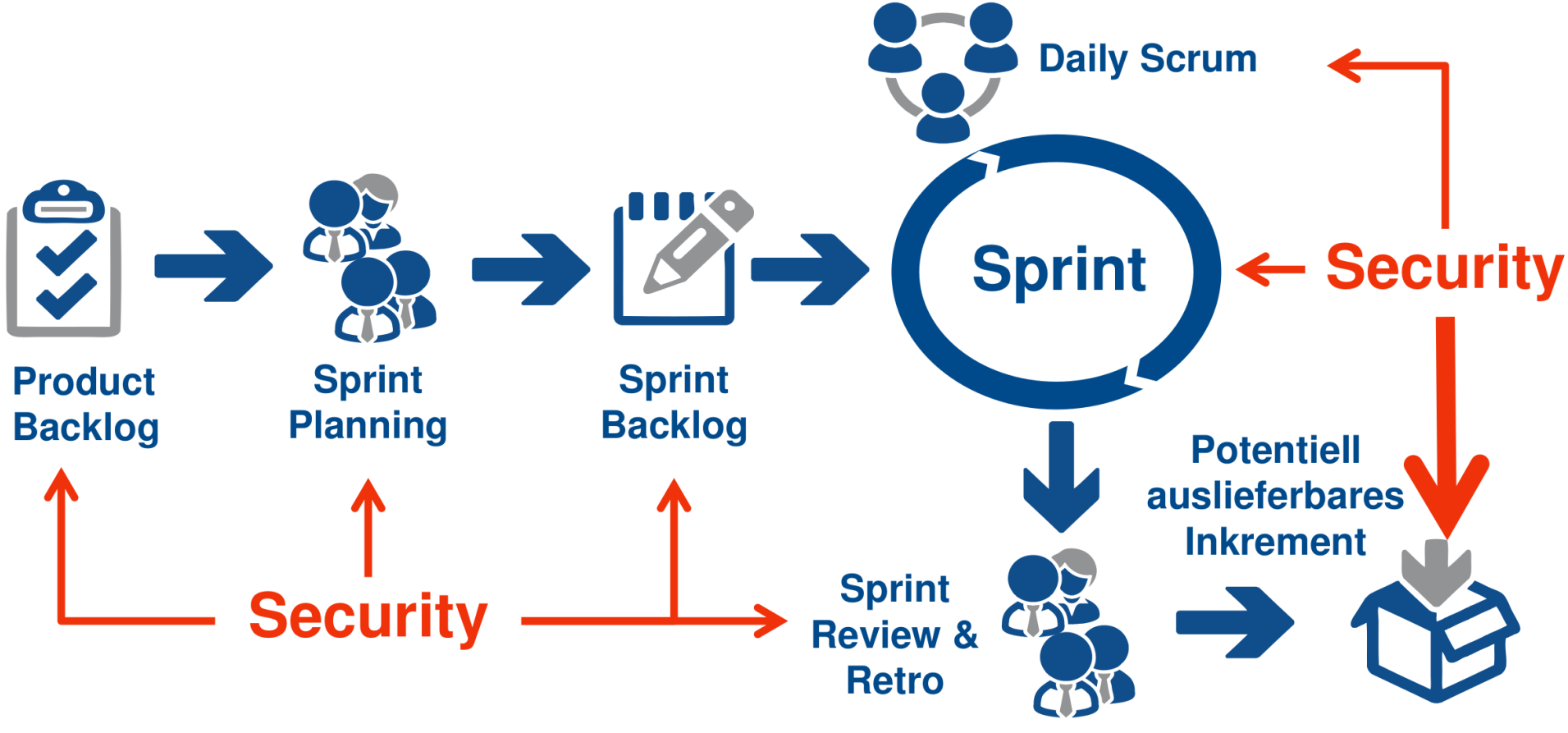


POTENTIELL UNSICHER AUSLIEFERN ?

AUSGANGSLAGE: SECURITY != AGIL!

Sprint 1	Sprint 2	Sprint …n	
Story A			
Story B			
	Story C		
	Story D		
	Story E		
		Story F	
		Story G	
		Story H	Go Live
		Security Features	Penetrationstest

SECURITY IN SCRUM



SECURITY TRAININGS

Product Owner

- Identifikation von Assets
- 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

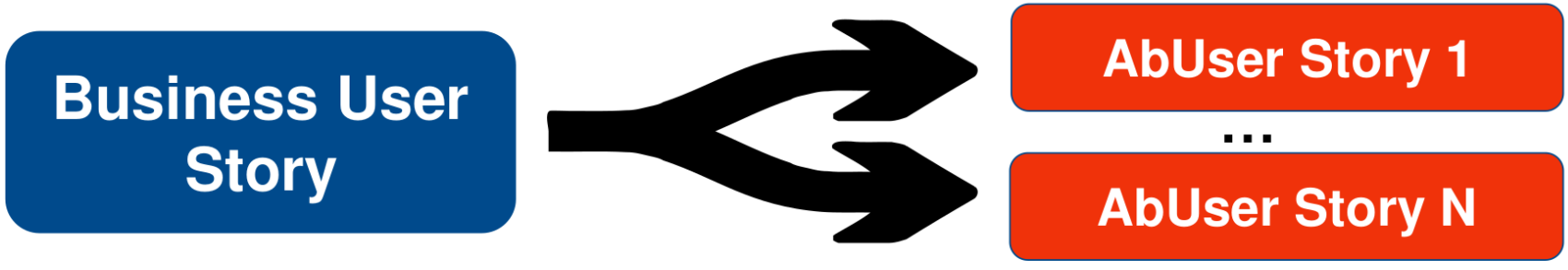
Threat Model

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

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

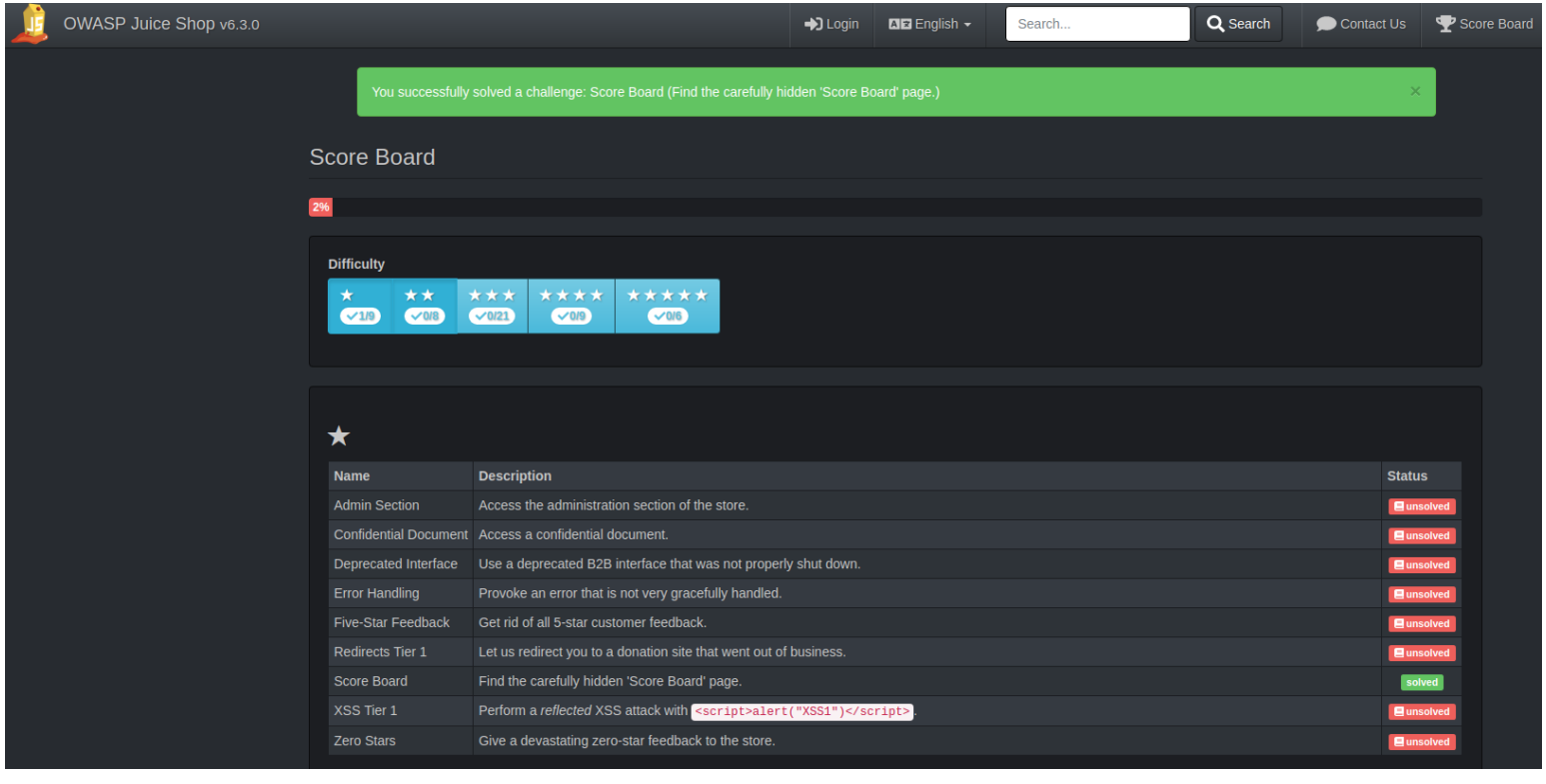
Application Security Verification Standard

https://github.com/OWASP/ASVS

Pro Active Controls

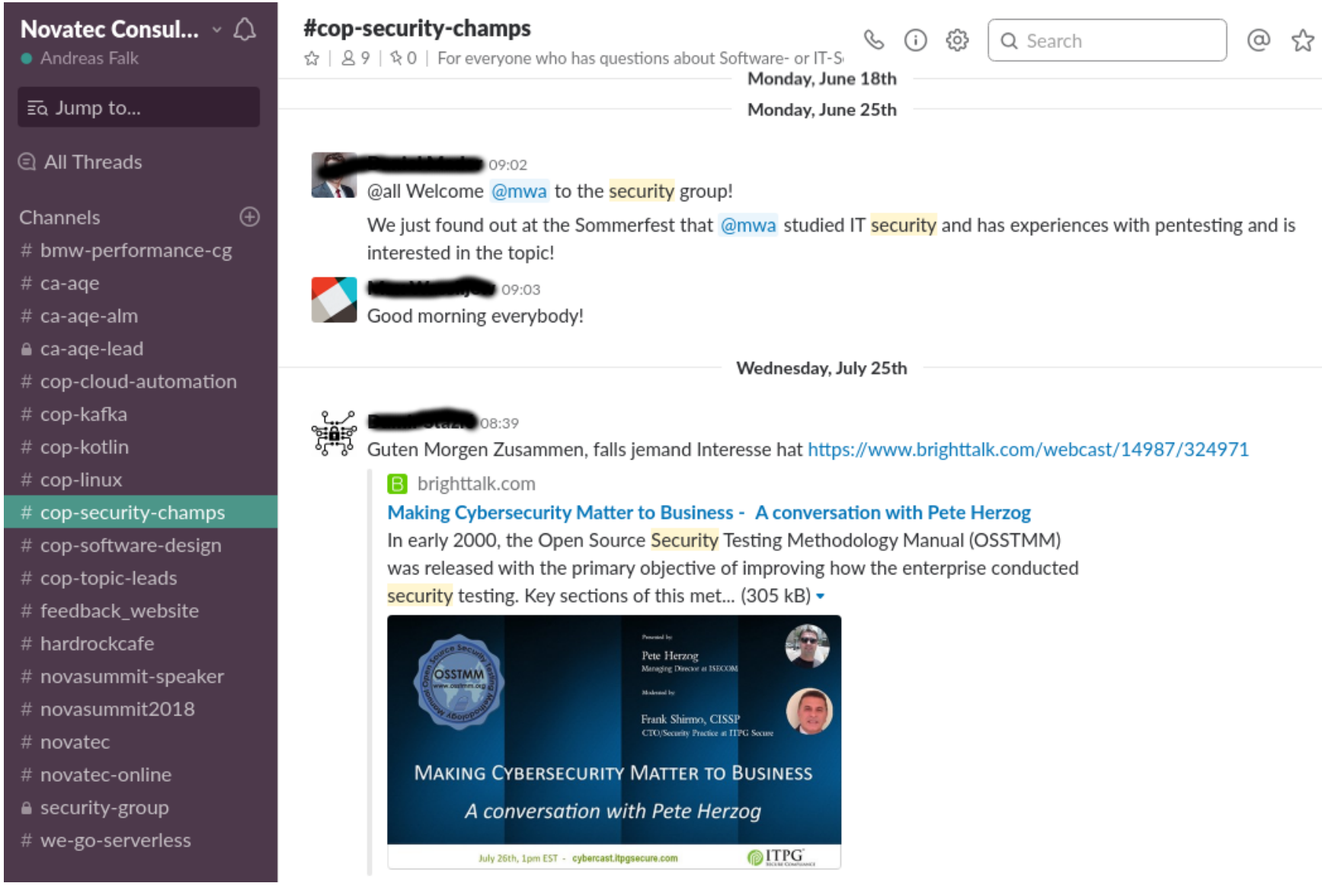
https://www.owasp.org/index.php/OWASP_Proactive_Controls

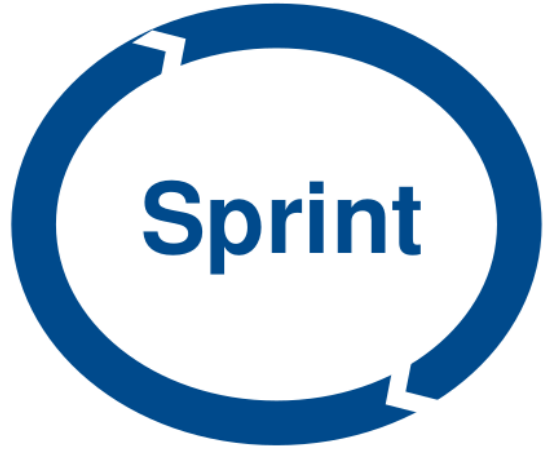
SECURITY DOJO'S JUICE SHOP



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

SLACK SECURITY CHAMPIONS





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

ENTWICKLER SECURITY TESTS

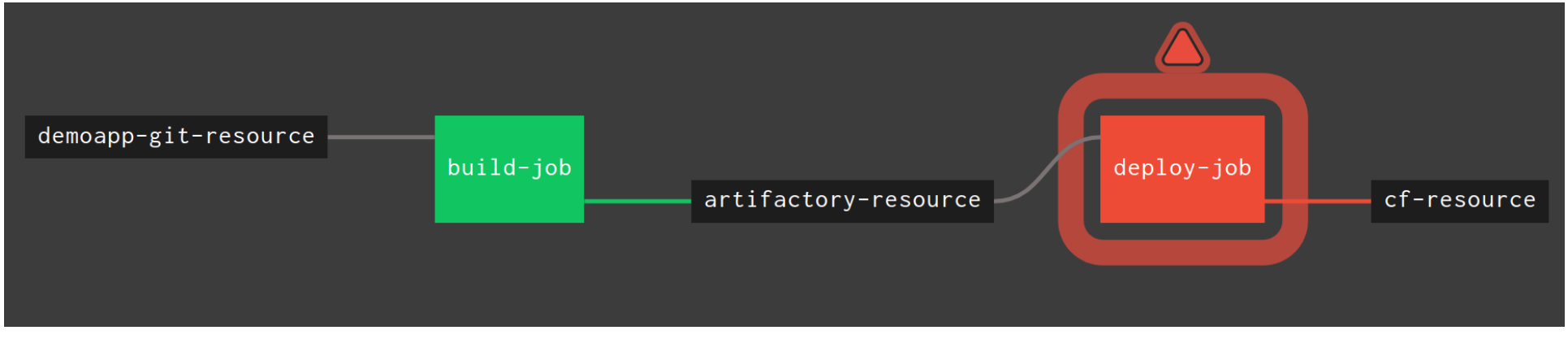
BEVOR EIN ANGREIFER “TESTET”

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

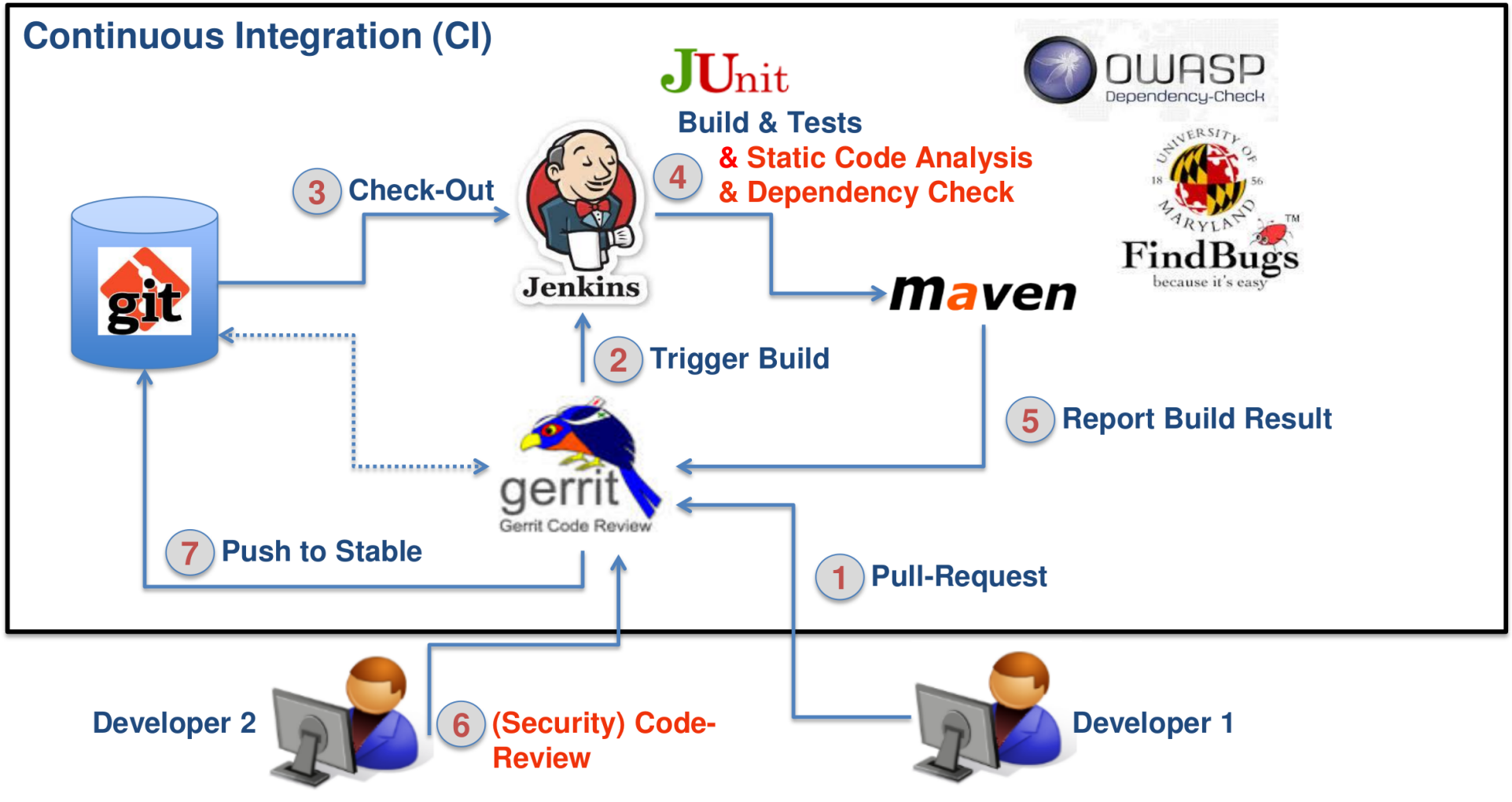
CI/CD PIPELINES

Continuous Delivery/Deployment ermöglicht

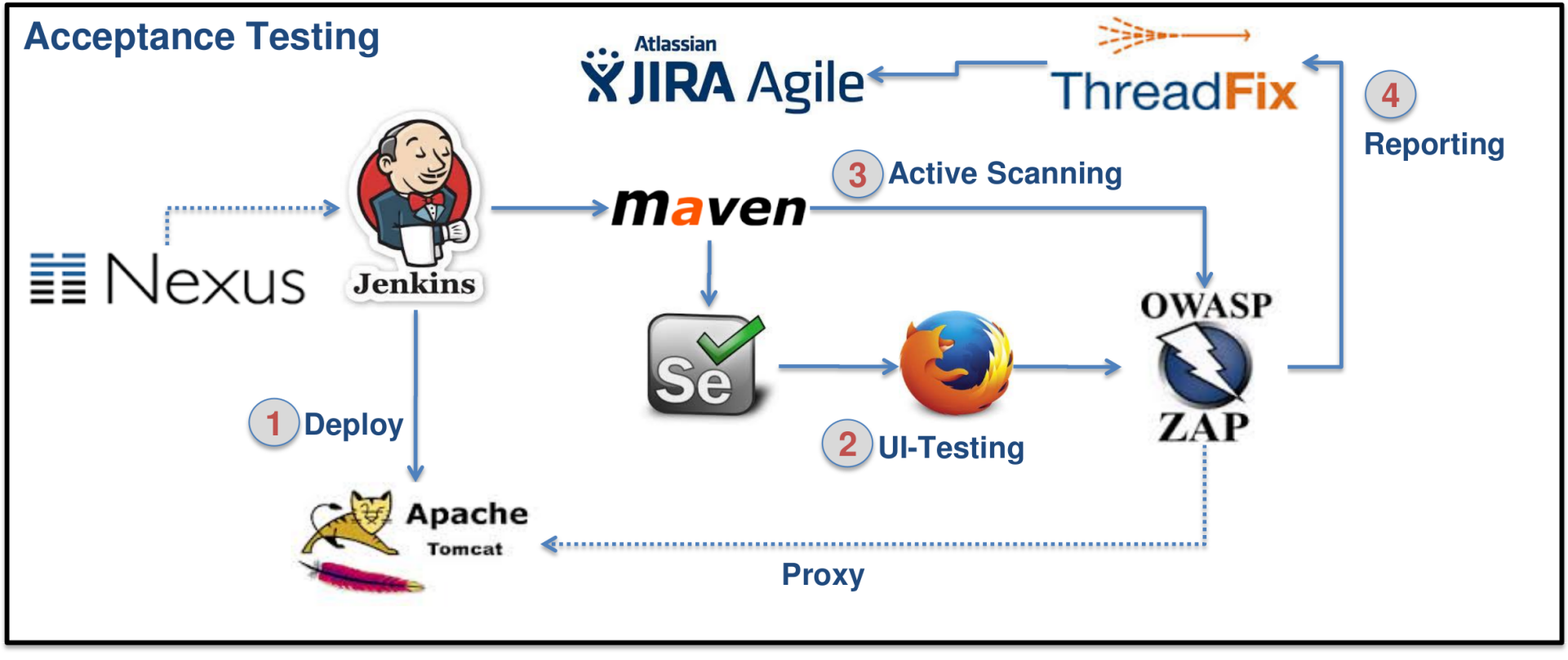
schnelle Reaktion mit Security-Fixes



CI COMMIT-STAGE MIT STATISCHER ANALYSE (SAST)



CI SECURITY-STAGE MIT DYNAMISCHER ANALYSE (DAST)



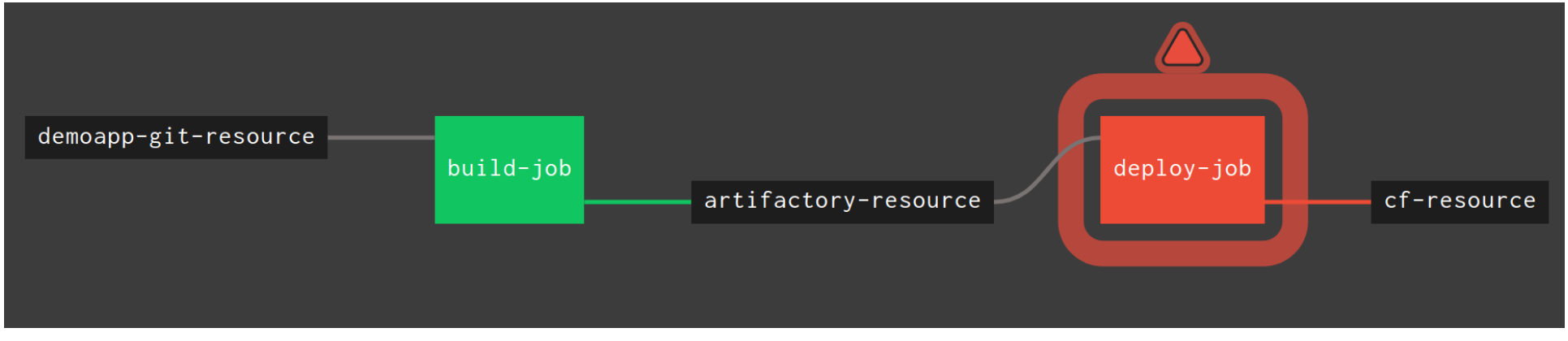
ABSICHERUNG DER CI/CD-PIPELINE

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

Credentials in Jenkins, Concourse,... sicher ablegen

Jenkins & Co regelmäßig aktualisieren

Test Code ist kein 2.Klasse Code



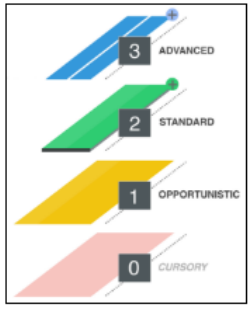
Sprint Review & Retro

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

IDEALZUSTAND: SECURITY == AGIL!

Sprint 1	Sprint 2	Sprint …n	
Story A			
Story B			
Abuse Story	Story C		
	Story D		
	Story E		
	Abuse Story	Story F	
Security Features		Story G	
		Story H	Go Live
		Pen-Test	

THE BIG PICTURE



OWASP ASVS

OWASP Pro Active CONTROLS

OWASP ZAP

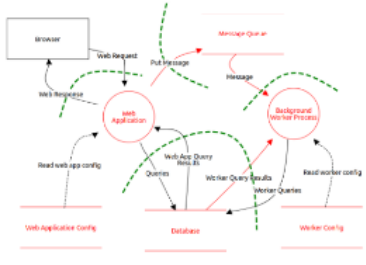
DEPENDENCY-CHECK

OWASP Testing Guide 4.0

Requirements

Development

Test



Threat Modeling
+
AbUser Stories

Applications

JAKARTA EE

PaaS

kubernetes Istio Terraform Cloud Foundry

Cloud Security + Infrastructure Security Patching

aws

CI/CD

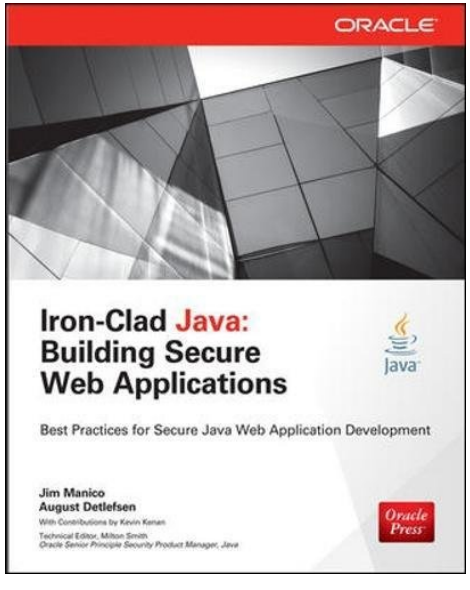
Jenkins

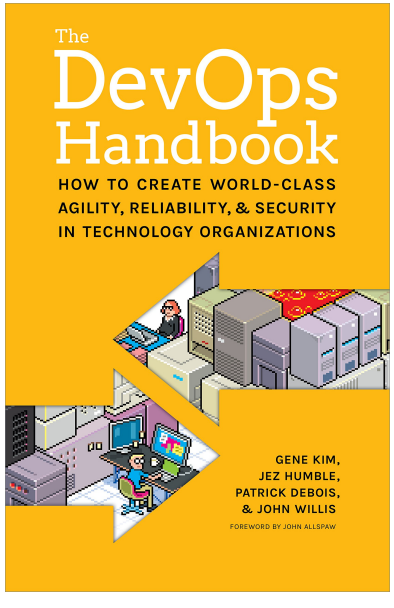
JFrog ARTIFACTORY

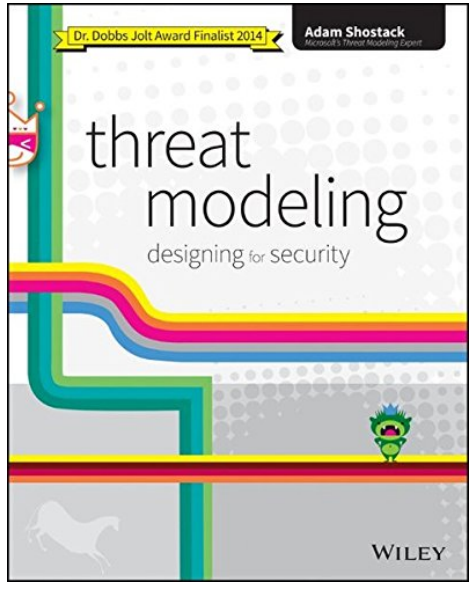
Sonatype

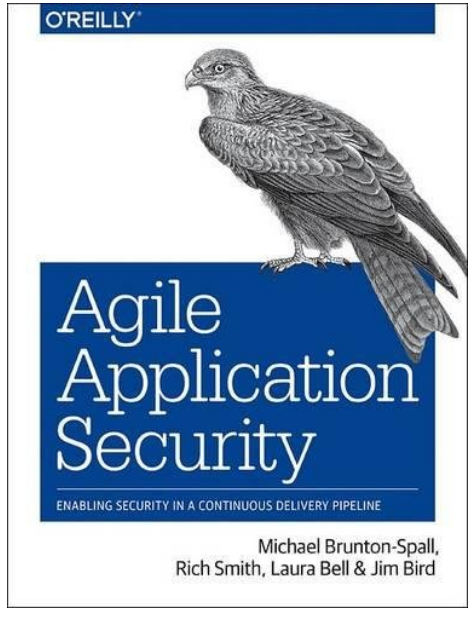
SecDevOps

BOOK REFERENCES









Q&A

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

https://blog.novatec-gmbh.de

andreas.falk@novatec-gmbh.de

@andifalk

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://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)