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

NOVATEC

UNSERE SOFTWARE IST DOCH SICHER!?

Equifax-Hack: Angreifer über Apache-Struts-Lücke eingestiegen

14.09.2017 13:29 Uhr – Dennis Schirrmacher

vorlesen

(Bild: medithIT, CC BY 2.0)

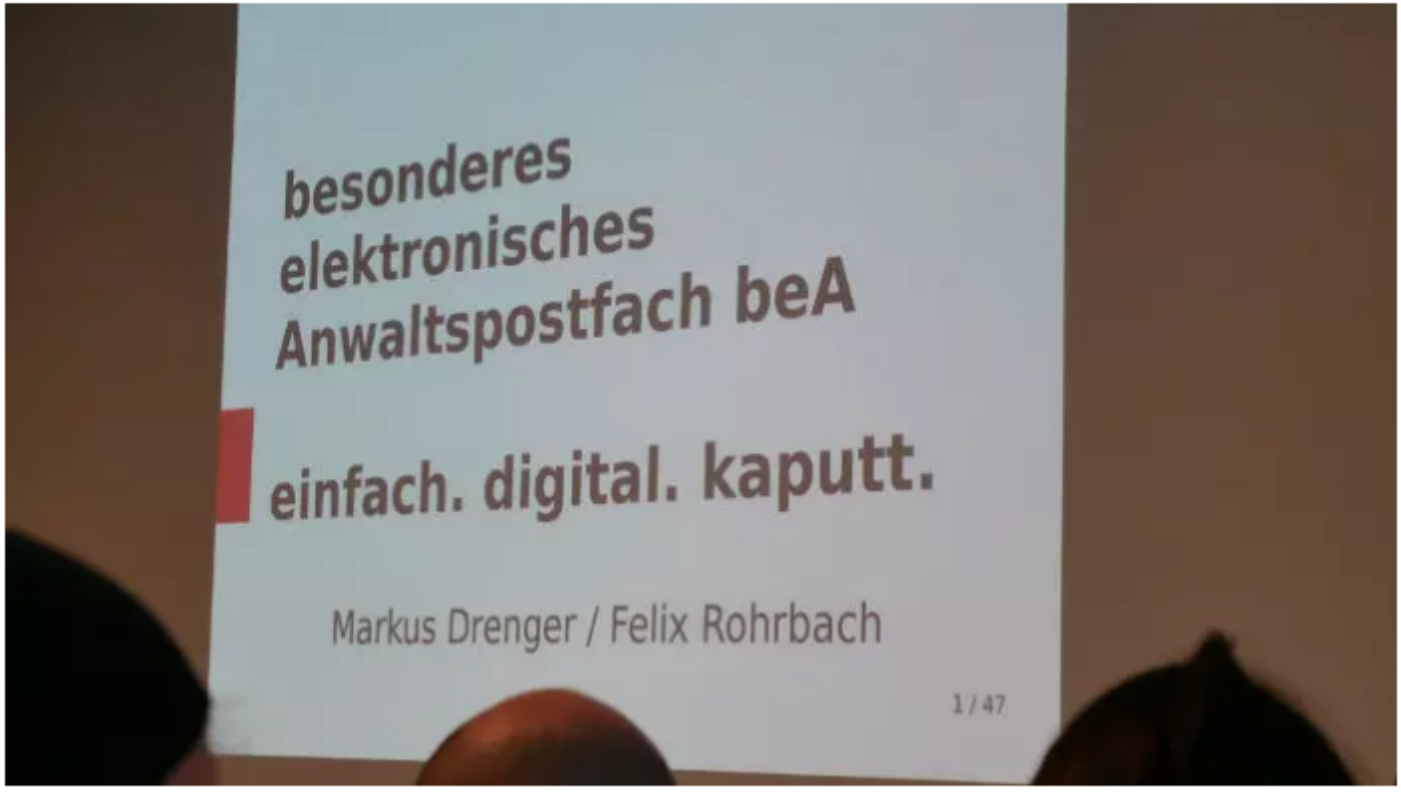
Untersuchungen zeigen, dass Equifax es offensichtlich versäumt hat, Sicherheitsupdates für eine kritische Lücke zu installieren. Darüber hinaus ist es zu einem weiteren Datenleck gekommen.

Quelle: heise.de

34C3: Das besondere Anwaltspostfach beA als besondere Stümperei

28.12.2017 16:09 Uhr – Detlef Borchers

vorlesen



Darmstädter Hacker zeigen, dass das besondere elektronische Anwaltspostfach, kurz beA, mit veralteter Software und einem veralteten Anwendungskonzept entwickelt wurde.

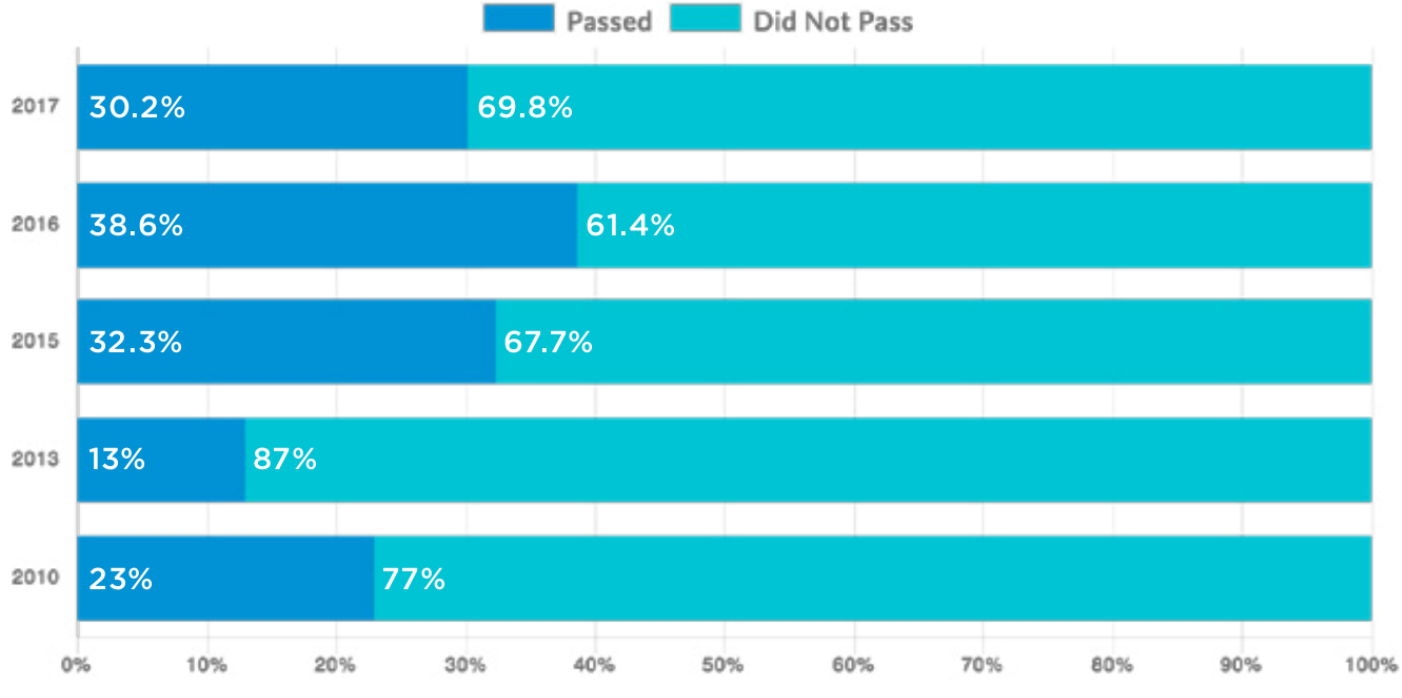
Quelle: heise.de

STATE OF SOFTWARE SECURITY REPORT 2017

(VERACODE)

OWASP TOP 10 POLICY PASS RATE

Percentage of Applications Passing on First Scan

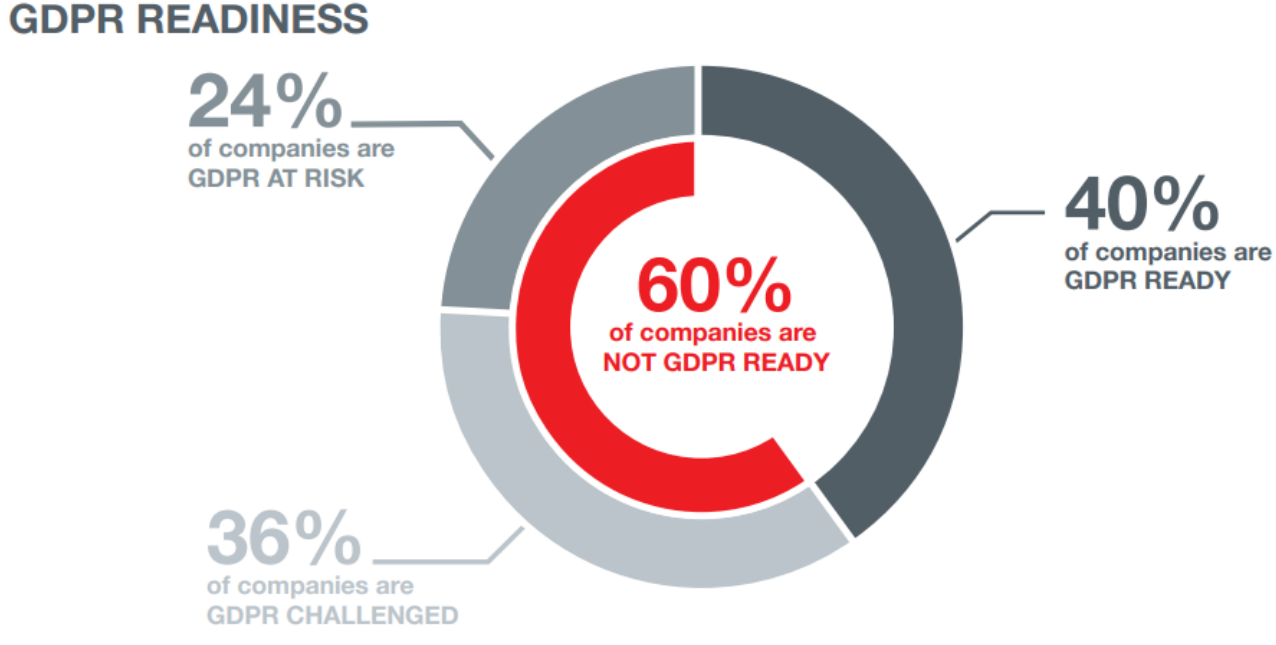


Quelle: veracode.com

SECURITY IST NICHT MEIN JOB!?

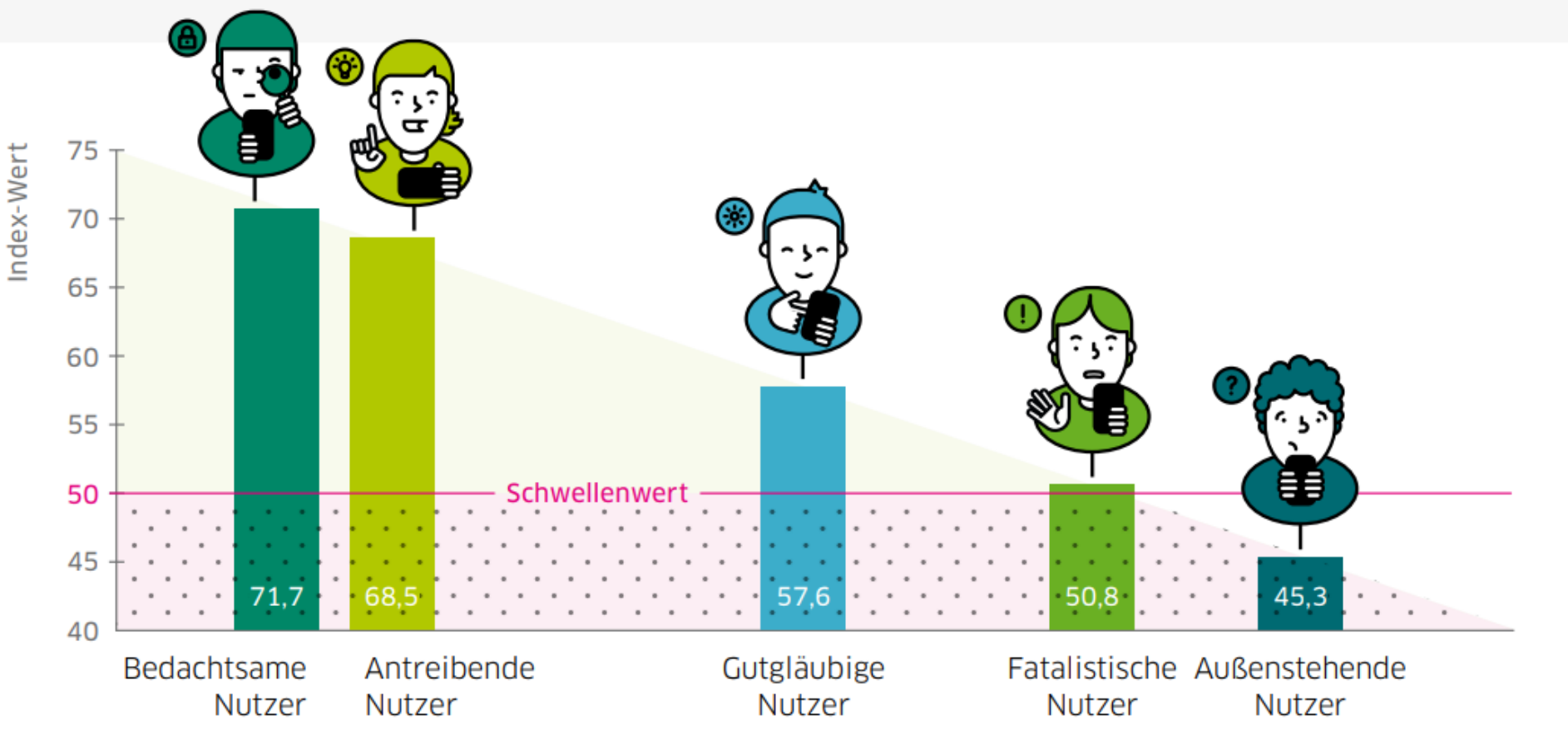
EU DATENSCHUTZ GRUNDVERORDNUNG

Seit Mai 2018 geltendes Recht!



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

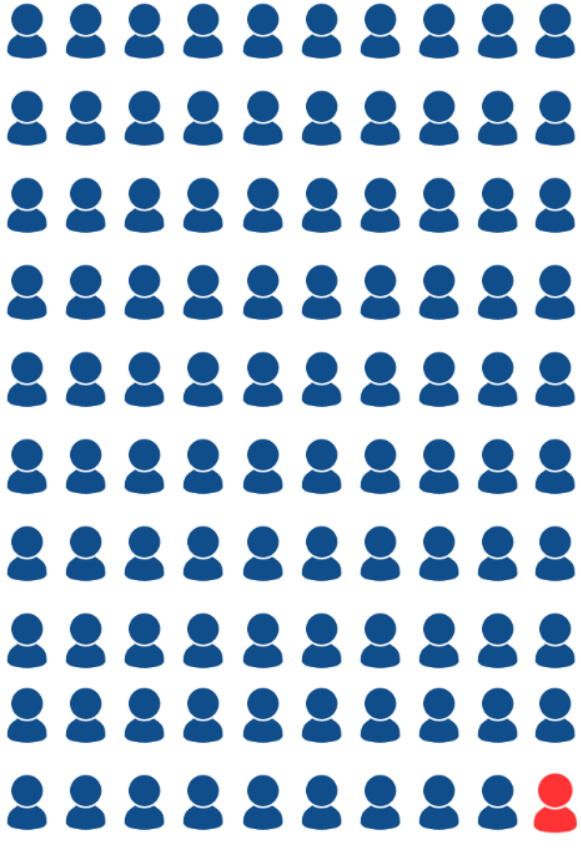
NUTZERVERHALTEN



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

NEUE HERAUSFORDERUNGEN

1 SECURITY-PROFESSIONAL FÜR 100 ENTWICKLER

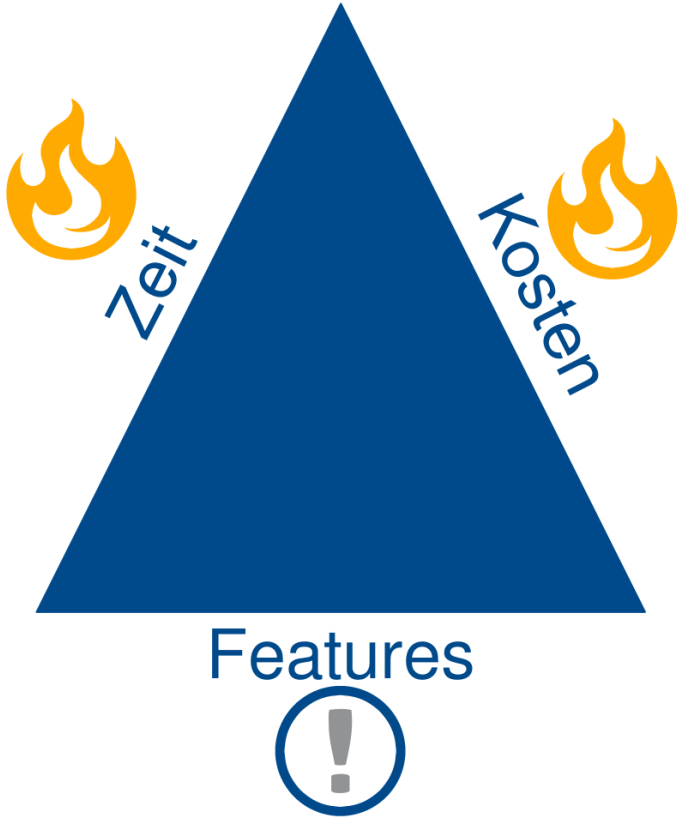


Quelle: sonatype.com/devops-survey-report

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!

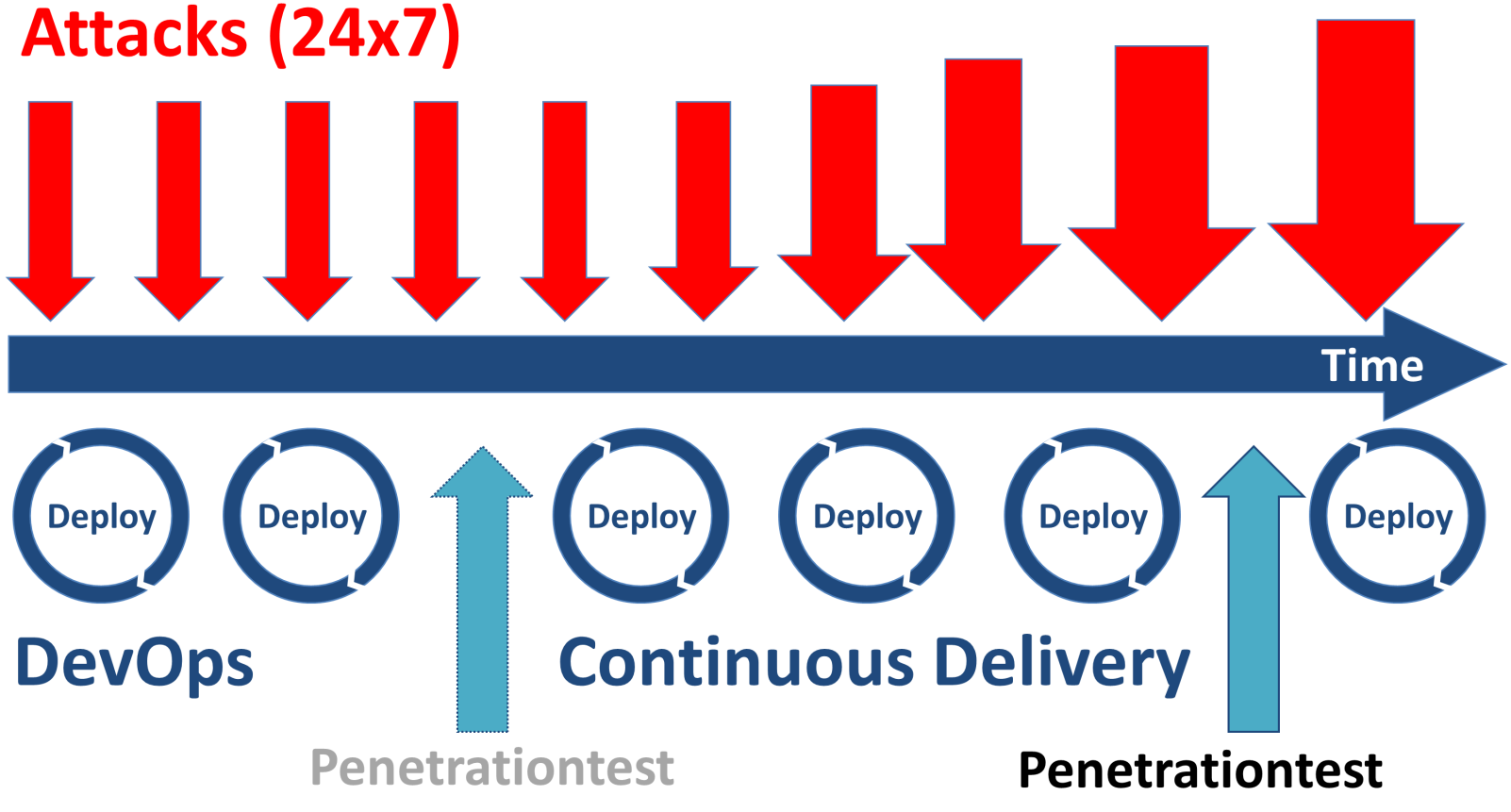
Monitor Network Security

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

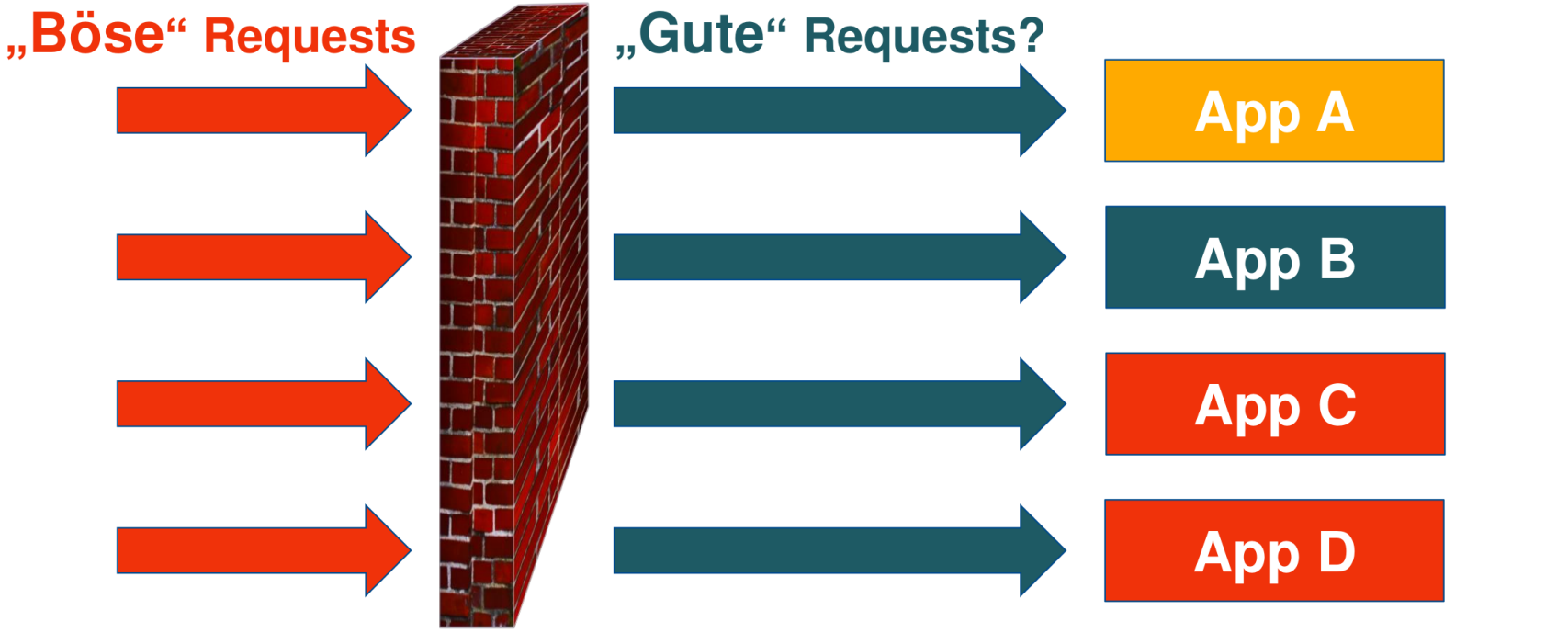
Get a Competitive Advantage

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

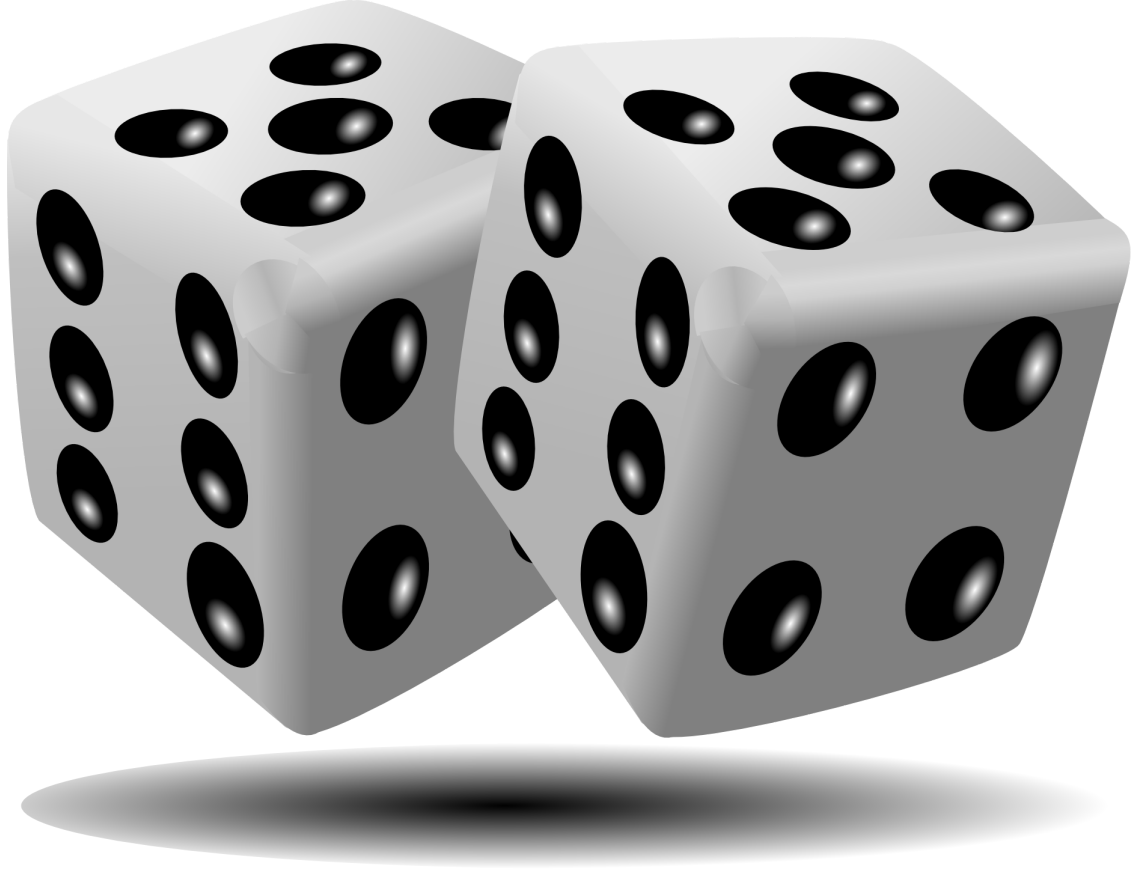
Quelle: shodan.io


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

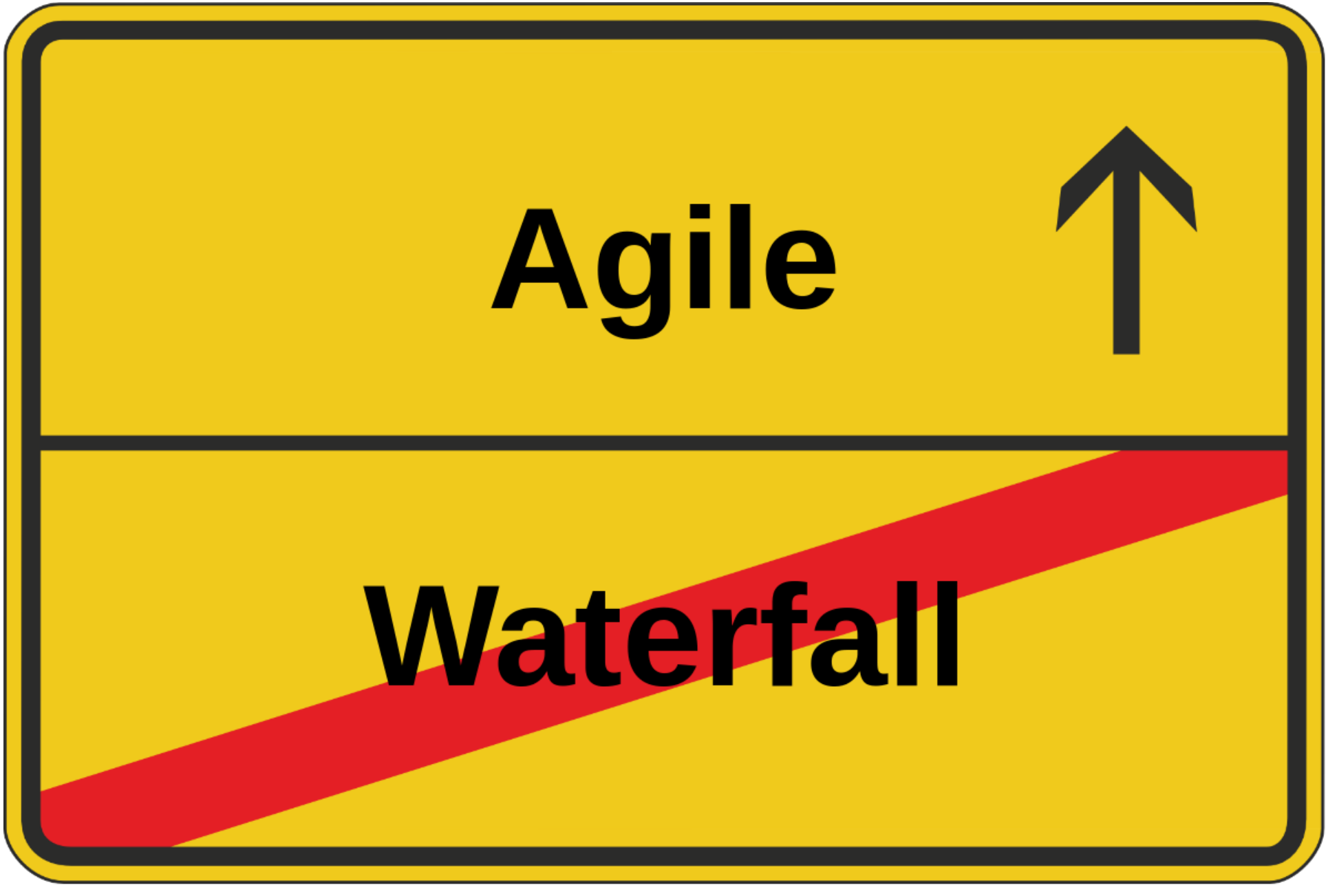
WIR HABEN DOCH EINE FIREWALL



WEITER SO?



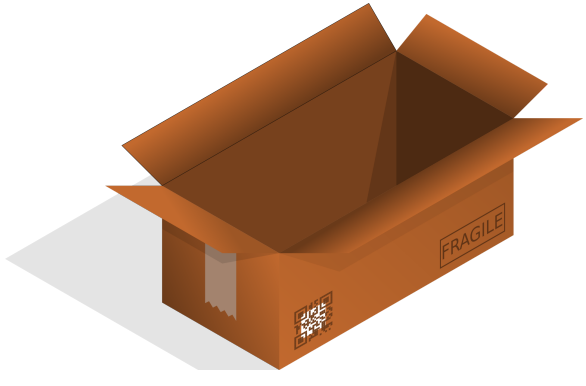
SICHERE ENTWICKLUNGS-PROZESSE ?


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

Agile Entwicklung	Penetration-Testing
Inkrementell mit schnellem Feedback	Punktuell und Aufwendig
Innerhalb von Sprints	Abseits von Sprints
“Working software over comprehensive documentation”	Umfassende Reports
Business Value	Nicht-Funktional

UNVERSTÄNDLICHE PEN-TEST REPORTS

CVE-2003-1418 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

Apache HTTP Server 1.3.22 through 1.3.27 on O
ETag header, which reveals the inode number, c

Etag header is presented in application response.

Threat:

Etag header allows remote attackers to obtain sensitive information, which include the inode number or may reveal child process IDs (PID).

Screenshot:

CVSS Base Score: 3.7 (Low) (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

Possible remediation:

Disable Etag header in webserver configuration.

Reference:

https://nvd.nist.gov/vuln/detail/CVE-2003-1418

But we use NGINX and **NOT** Apache??

SECDEVOPS

DEVSECOPS

DEVOPSSEC

SECDEVOPS

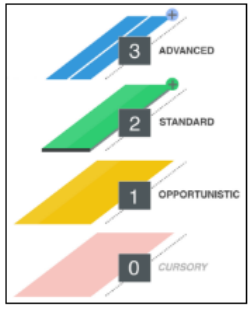
DEVOPSSEC

SECDEVOPS

SECDEVOPS

<<< “SHIFT LEFT” <<<

THE BIG PICTURE



OWASP ASVS

OWASP Pro Active CONTROLS

OWASP ZAP

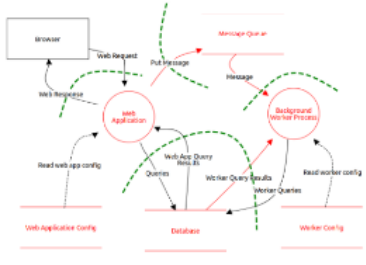
DEPENDENCY-CHECK

OWASP Testing Guide 4.0

Requirements

Development

Test



Threat Modeling
+
AbUser Stories

Applications

JAKARTA EE

PaaS

kubernetes

Istio

Cloud Foundry

Cloud Security + Infrastructure Security Patching

aws

CI/CD

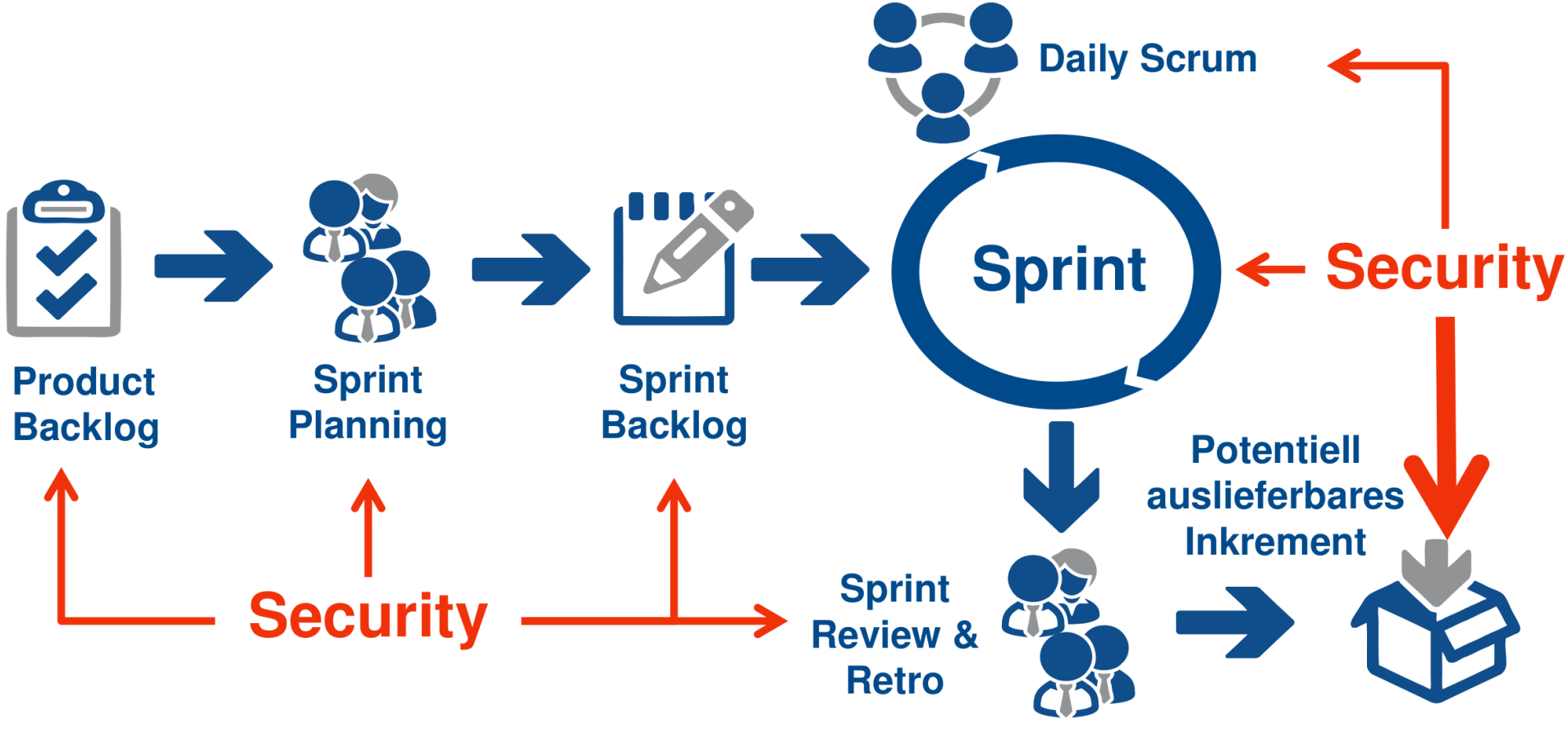
Jenkins

JFrog ARTIFACTORY

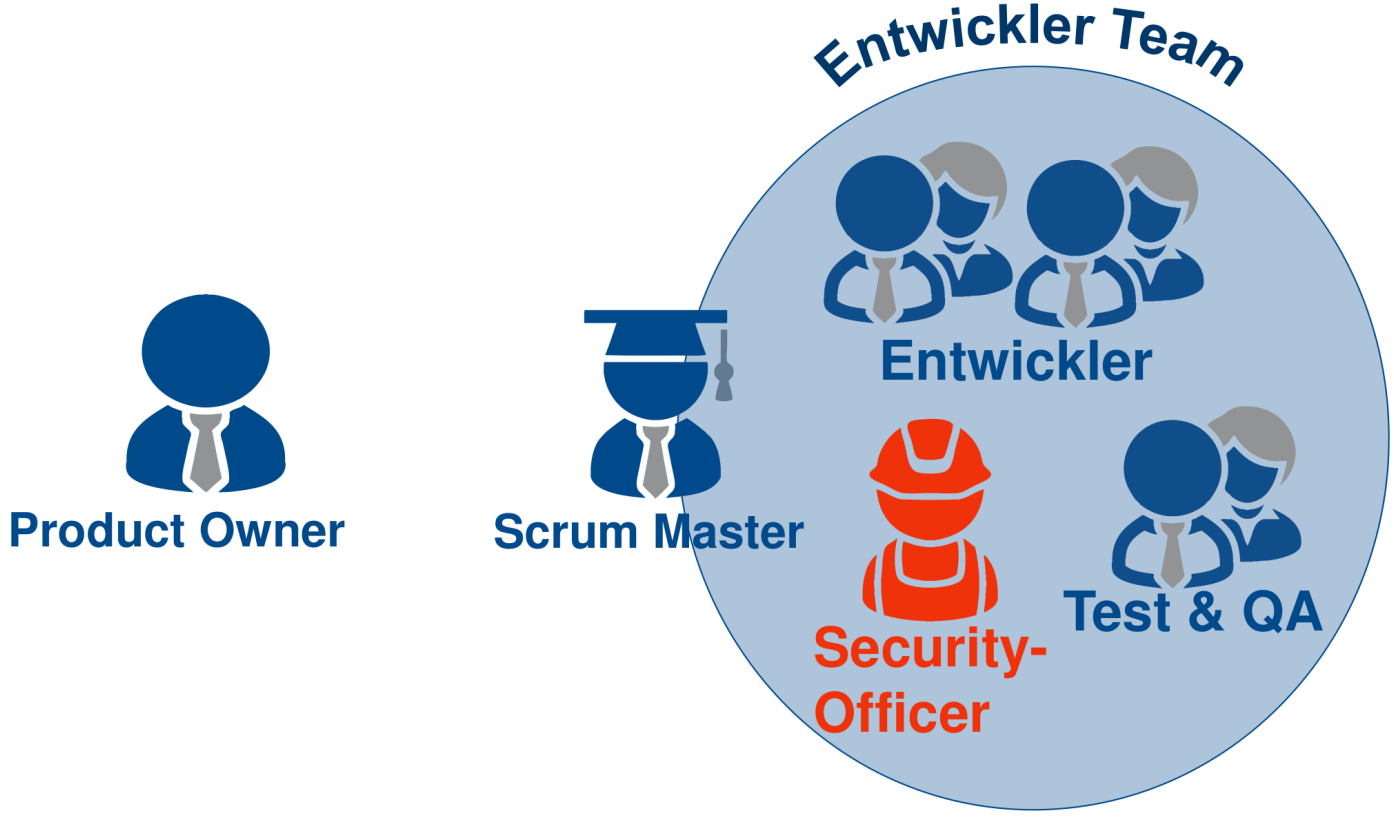
Sonatype

SecDevOps

SECURITY IN SCRUM



SECURITY OFFICER



SECURITY TRAININGS

SECURITY TRAININGS

Product Owner

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

SECURITY TRAININGS

Development Team

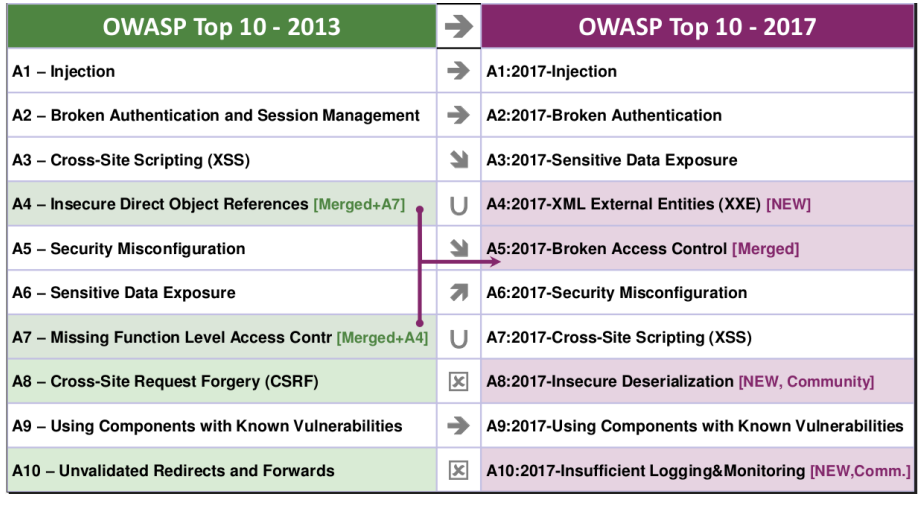
- Threat Modeling
- Secure Design Patterns
- Security Code Reviews
- Security Testing
- Security Dojos

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

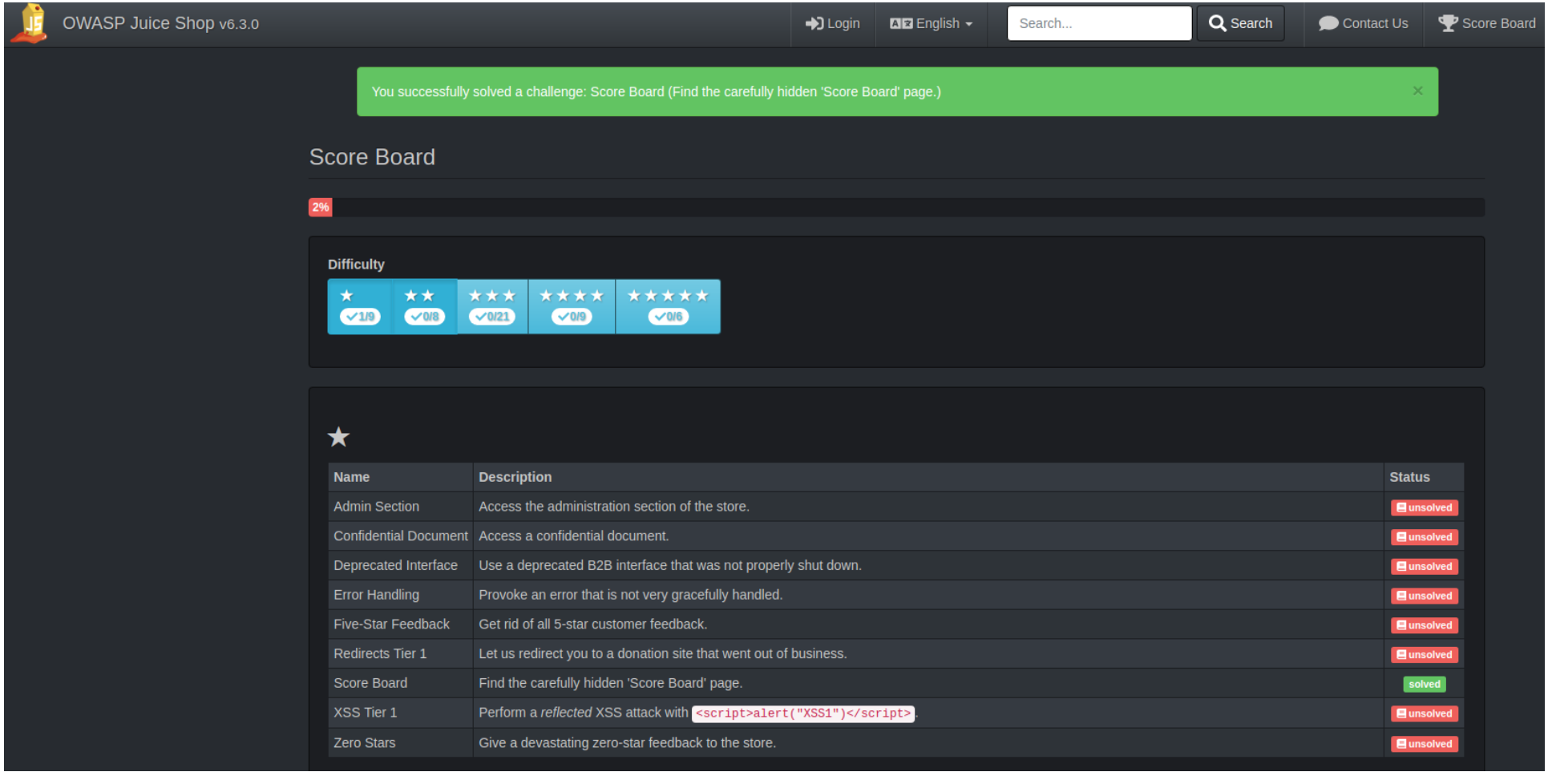
Application Security Verification Standard

https://github.com/OWASP/ASVS

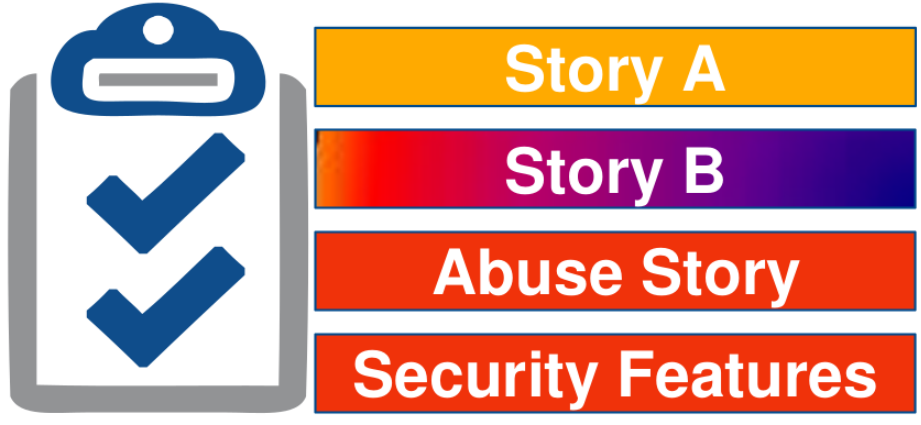
Pro Active Controls

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

JUICE SHOP



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



Product Backlog

- Threat Model Refinement
- AbUser Stories erstellen
- Security Features mit hoher Prio
- Akzeptanzkriterien für Sicherheit

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

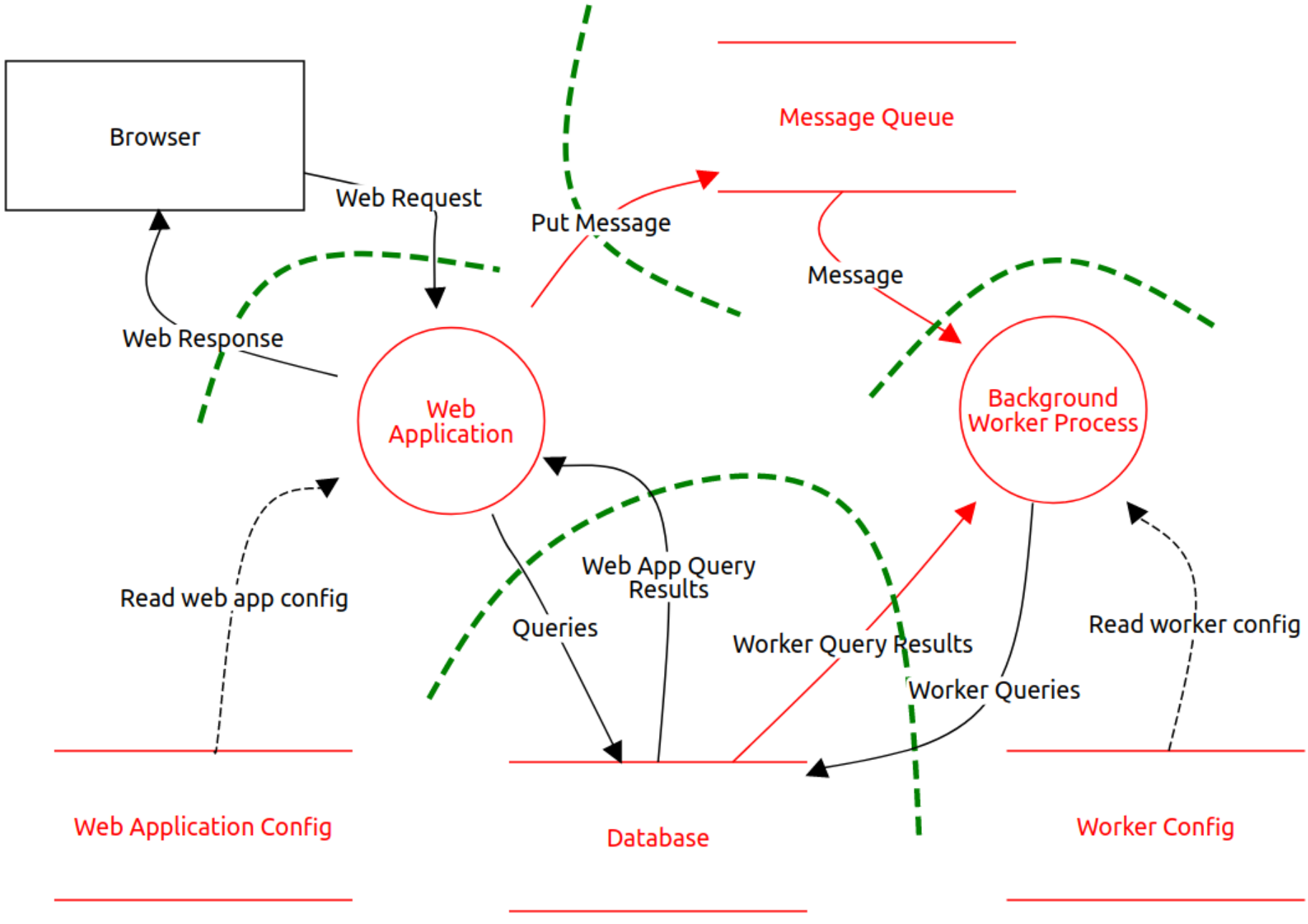
User Stories, UML Diagramme

Threat Model

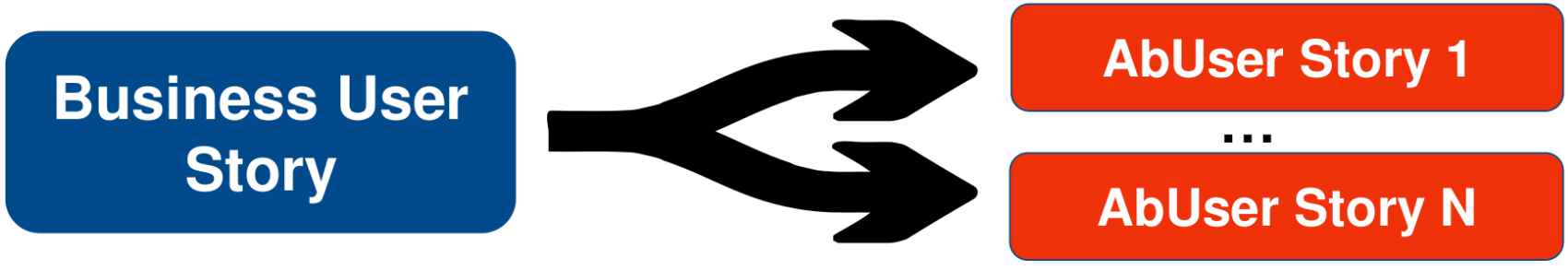
Als Diskussions-Basis

Identifikation und Vermeidung von Bedrohungen

„Elevation of privilege“ Spiel


Browser
Web Request
Web Response
Message Queue
Put Message
Message
Web Application
Background Worker Process
Read web app config
Web App Query Results
Queries
Worker Query Results
Worker Queries
Read worker config
Web Application Config
Database
Worker Config

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.

ABUSER UND SECURITY STORIES

TODO-5

Als Benutzer möchte ich mich an der ToDo Anwendung anmelden um neue ToDo's anzuzeigen/anzulegen

Security Feature 5

TODO-6

Als Administrator möchte ich mich an der ToDo Anwendung anmelden um Kategorien und Benutzer zu verwalten

Security Feature 5

TODO-10

Als Script-Kiddie möchte ich mich mit administrativen Rechten anmelden um Spam als ToDo's einzutragen

Abuse Story 2

TODO-8

Als Benutzer möchte ich eine Liste meiner aktuellen ToDo's anzeigen

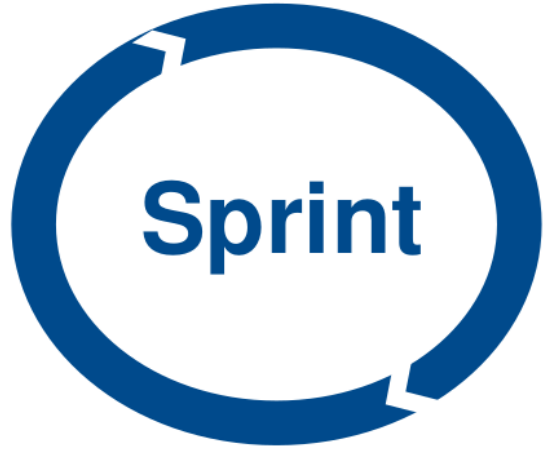
Business Feature 3

Sprint Planning

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

Daily Scrum

- Neue Security-Risiken diskutieren
- Security Tasks ggf. neu planen



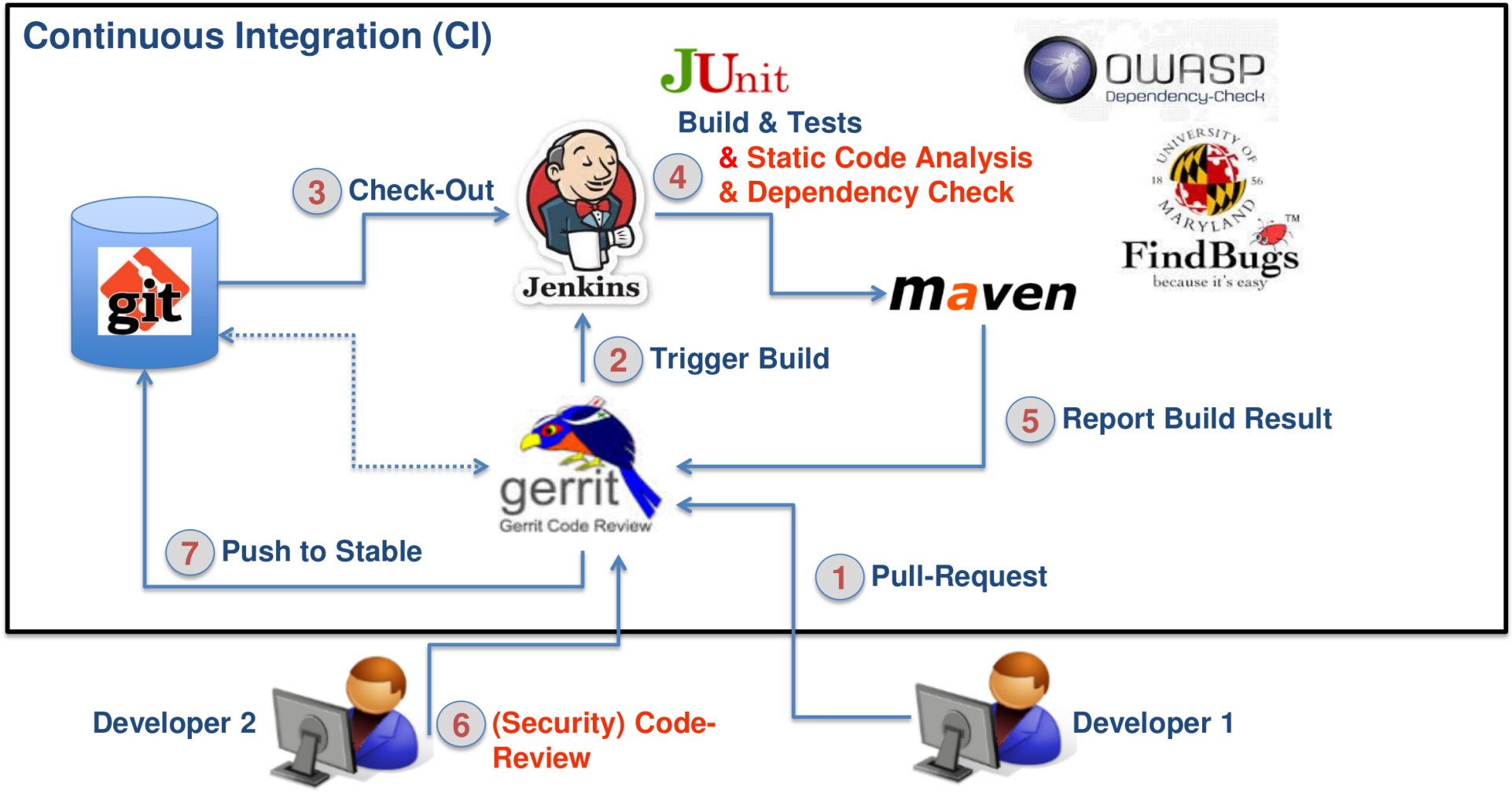
- Secure Design / Coding
- Pairing mit Security-Officer/Champion
- Security-Aware DoD
- Security Code Reviews
- Security Testing
- CI Pipeline mit Security

ENTWICKLER SECURITY TESTS

BEVOR EIN ANGREIFER “TESTET”

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

CI COMMIT-STAGE MIT STATISCHER ANALYSE (SAST)

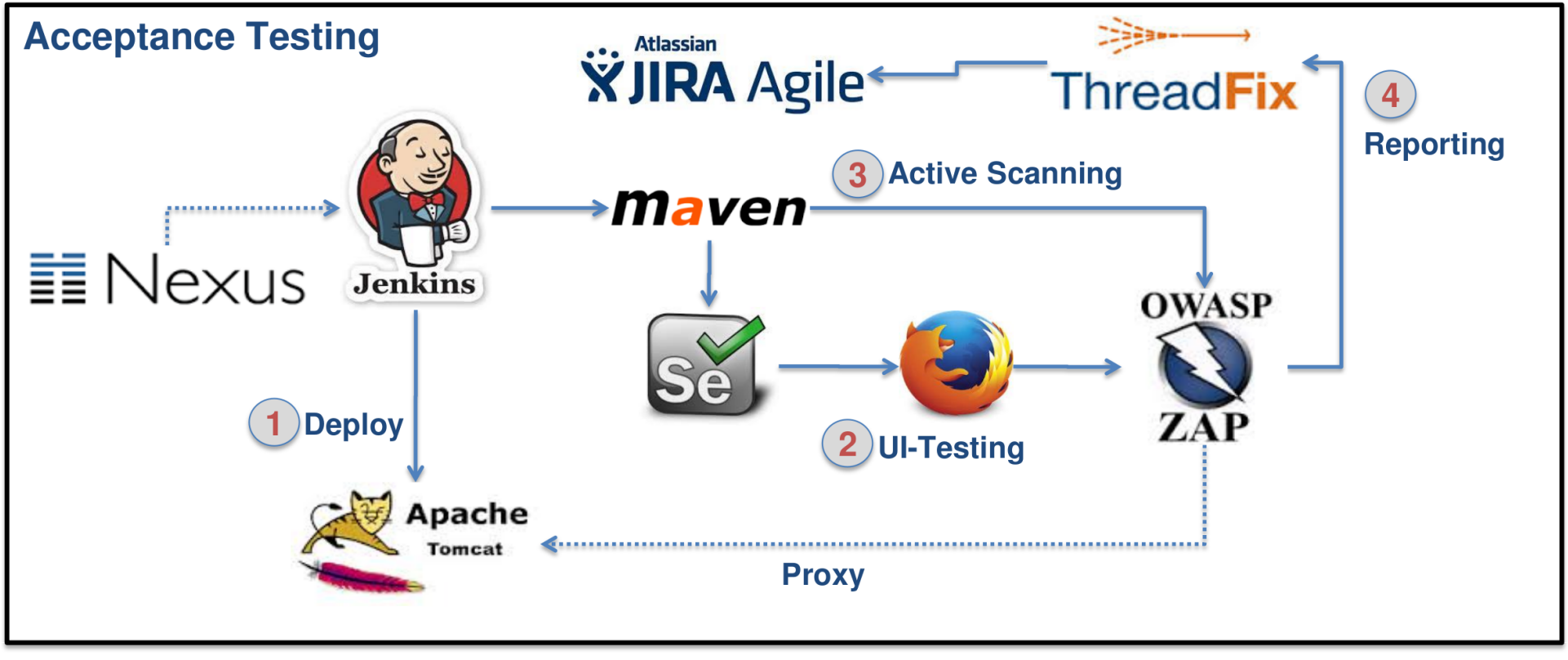


OWASP DEPENDENCY CHECK

- Prüft Projektabhängigkeiten auf Sicherheitsprobleme
- Unterstützt Java und .NET Anwendungen
- Command line, Ant, Maven, Gradle, Jenkins, SBT

https://github.com/jeremylong/DependencyCheck

CI SECURITY-STAGE MIT DYNAMISCHER ANALYSE (DAST)



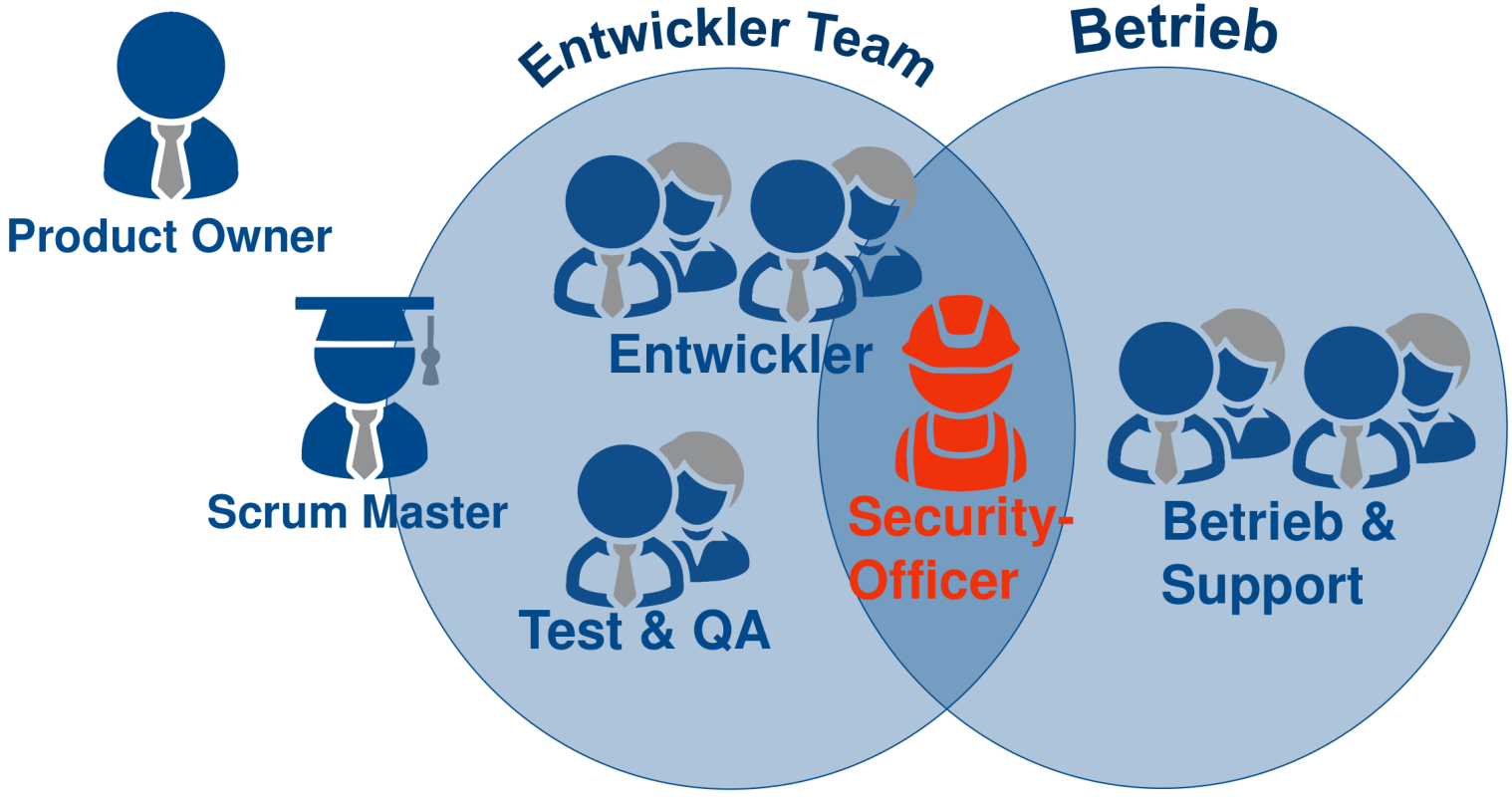
Sprint Review & Retro

- 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	

SECURITY OFFICER IN SECDEVOPS



HTTPS IST PFLICHT !!

Let's Encrypt

CloudFlare

HTTP/2

Aktuelle Chrome Versionen:


UND IN DER
CLOUD?

ALTE BEKANNTE UND MEHR...

Alle OWASP Top 10 Web Probleme...

Distributed DoS

Economic DoS

ALTE BEKANNTE UND MEHR...

Alle OWASP Top 10 Web Probleme...

Distributed DoS

Economic DoS

ALTE BEKANNTE UND MEHR...

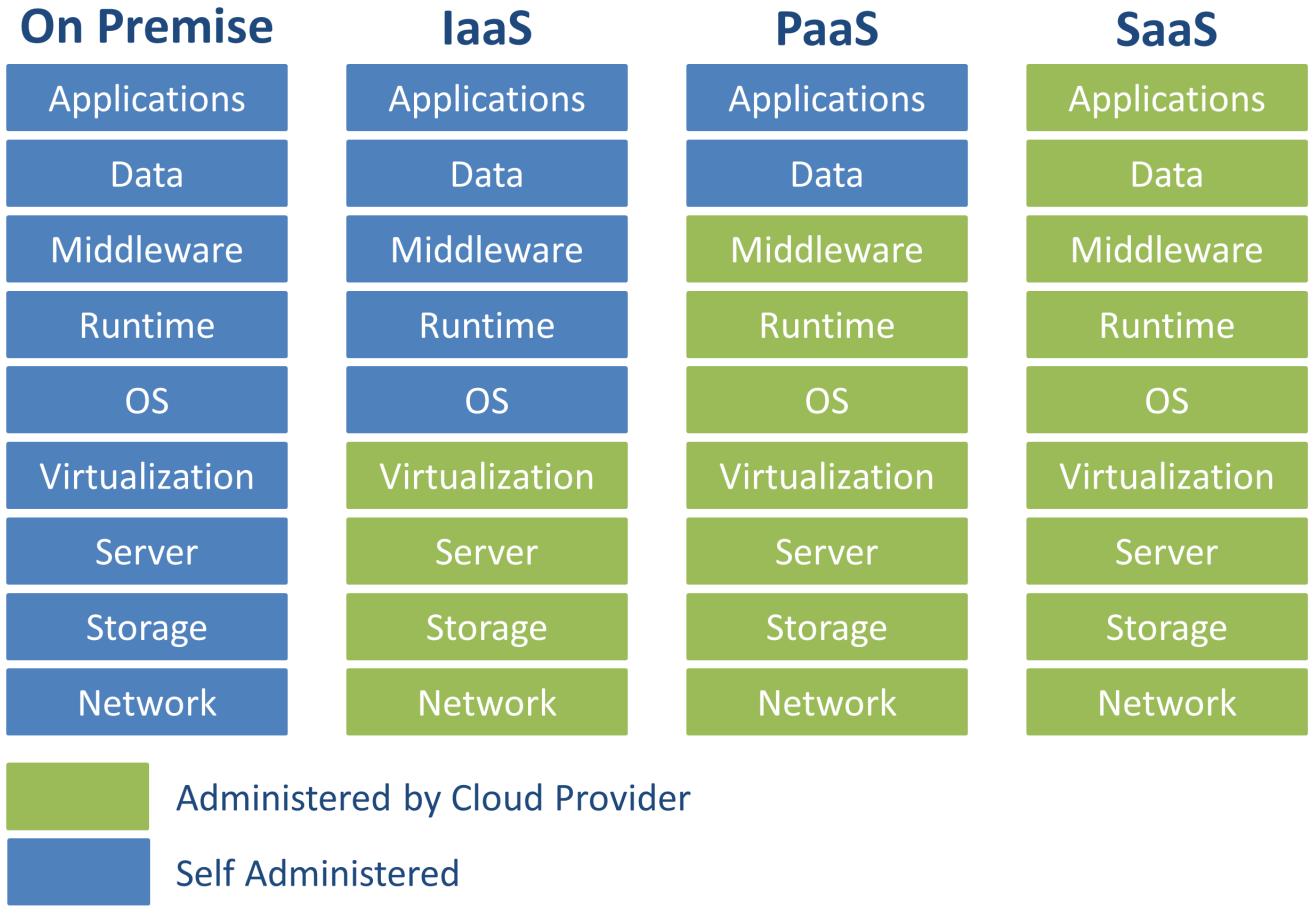
Alle OWASP Top 10 Web Probleme...

Distributed DoS

Economic DoS


UND WAS ÄNDERT SICH DANN
IN DER CLOUD?

Cloud Service Models



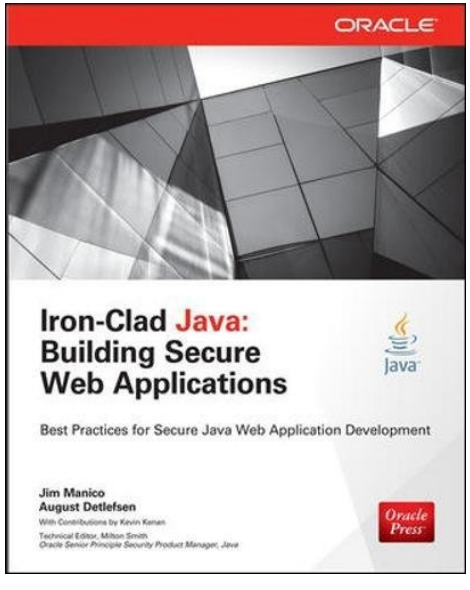
ROTATE, REPAIR, REPAVE

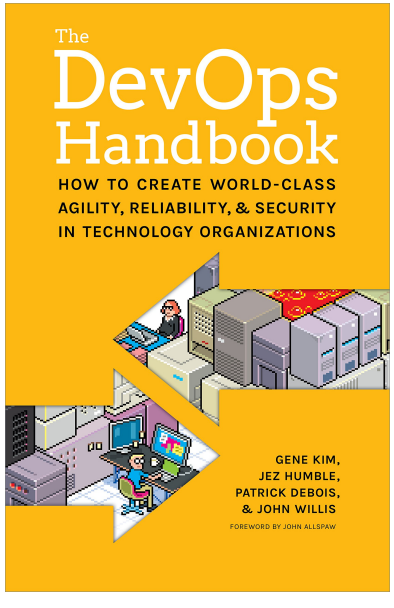
“What if every server inside my data center had a maximum lifetime of two hours? This approach would frustrate malware writers...”

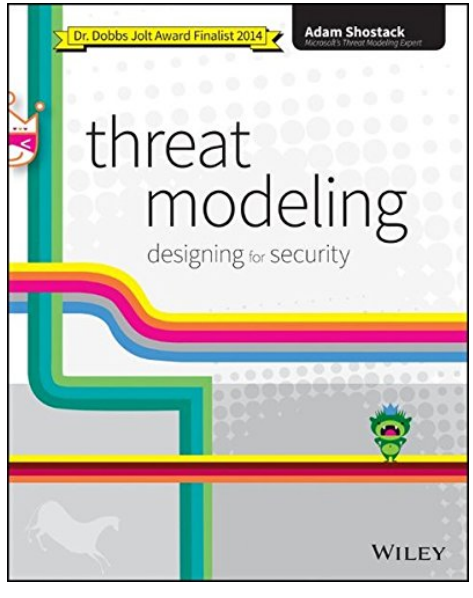
Justin Smith (Chief Security Officer at Pivotal)

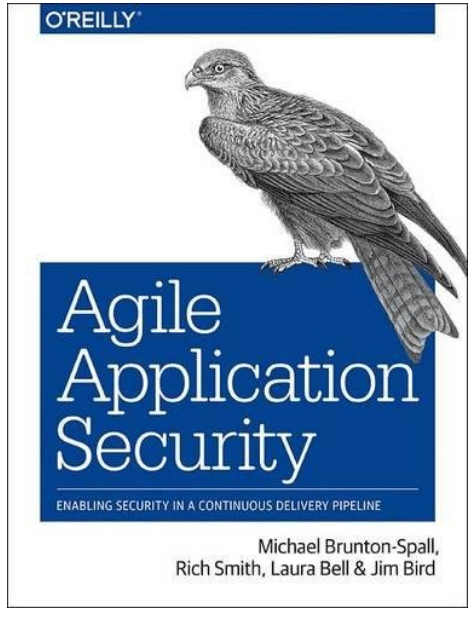
https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave

BOOK REFERENCES









Q&A

https://www.novatec-gmbh.de
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

- Have I been pwned?
- Shodan.io
- Deutschland sicher im Netz (DsiN): Sicherheitsindex 2017
- 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/mike-goodwin/owasp-threat-dragon
- https://github.com/bkimminich/juice-shop
- Rotate, Repair, Repave (https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave)