

AGIL ABER SICHER!

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



ANDREAS FALK

NOVATEC CONSULTING GMBH

andreas.falk@novatec-gmbh.de
@NT_AQE, @andifalk



UNSERE SOFTWARE IST DOCH SICHER!?



Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages



28 FEBRUARY 2017

Germany Issues Kill Order for a Domestic Spy—Cayla the Toy Doll

On a campaign to promote digital privacy, authorities warn that "My Friend Cayla" makes children vulnerable to malicious surveillance. They've ordered parents to d...

wsj.com

Quelle: troyhunt.com

MeltdownPrime & SpectrePrime: Neue Software automatisiert CPU-Angriffe

15.02.2018 16:14 Uhr – Fabian A. Scherschel

 vorlesen



(Bild: [Pixabay](#).)

Nach Meltdown und Spectre hatten Experten prognostiziert, dass das Zuschneiden auf spezifische Chips eine Weile dauern würde. Dieser Prozess lässt sich nun durch Automatisierung beschleunigen. Dabei wurden auch neue Variationen der Angriffe gefunden.

Quelle: [heise.de](#)

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

14.09.2017 13:29 Uhr – Dennis Schirrmacher

vorlesen



(Bild: [medithIT](#), CC BY 2.0)

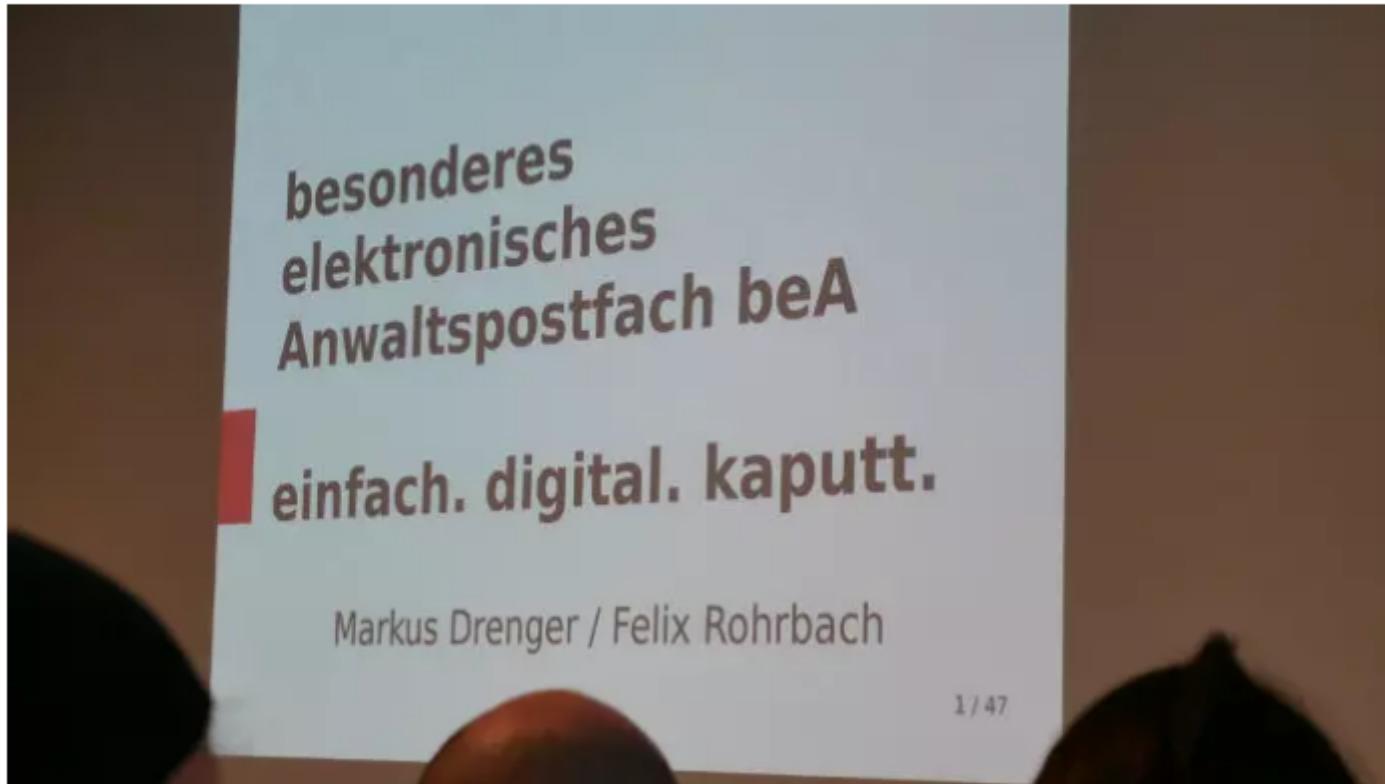
Untersuchungen zeigen, dass Equifax es offensichtlich versäumt hat, Sicherheitsupdates für eine kritische Lücke zu installieren. Darüber hinaus ist es zu einem weiteren Datenleck gekommen.

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](#)

Schwere Sicherheitslücke: root ohne Passwort mit macOS High Sierra UPDATE

29.11.2017 06:34 Uhr – Ben Schwan

vorlesen



macOS High Sierra ist seit September verfügbar. (Bild: Apple)

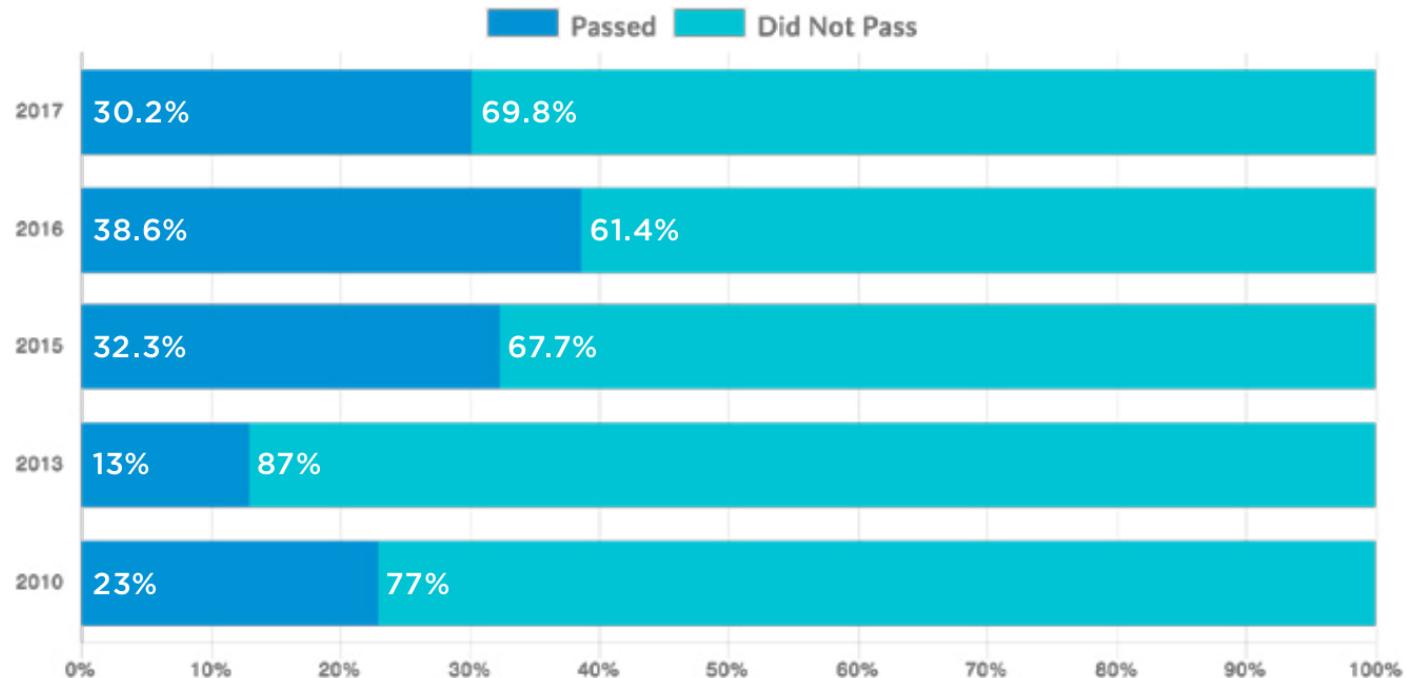
Mit ein paar Klicks können sich eingeloggte Nutzer in macOS 10.13 root-Rechte besorgen. Apple lässt eine extrem einfache Privilege Escalation zu.

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

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

269

pwned websites

4,868,606,237

pwned accounts

64,429

pastes

70,991,519

paste accounts

Top 10 breaches

✉ 711,477,622 Onliner Spambot
accounts ✉

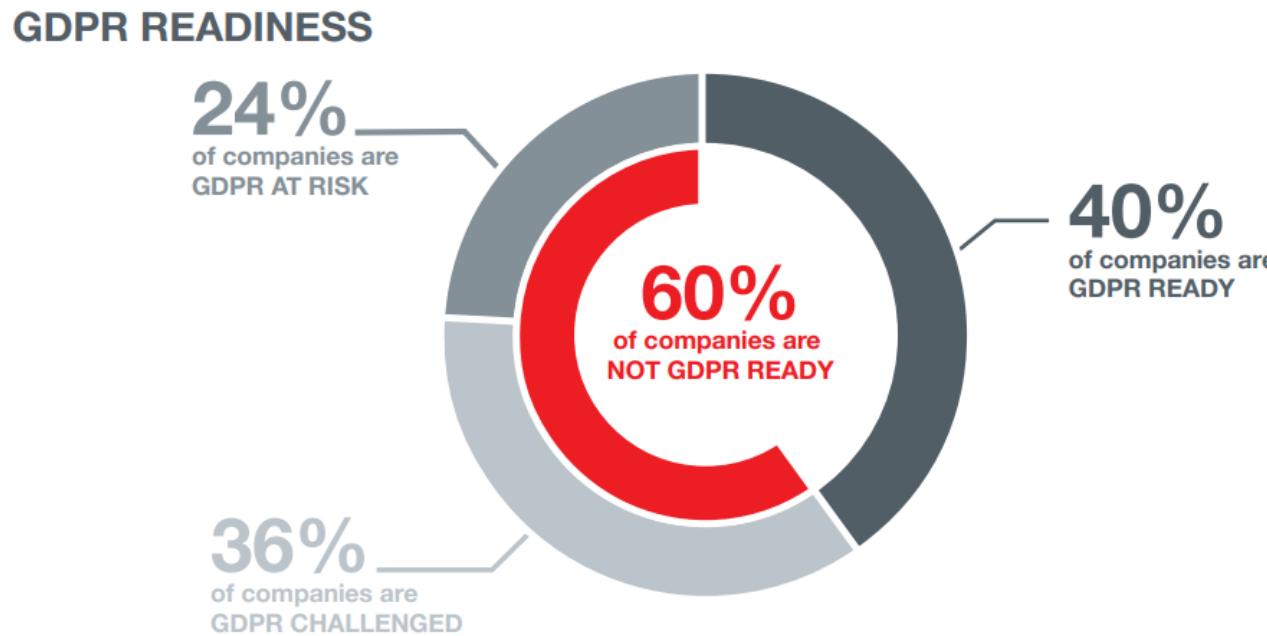
💻 593,427,119 Exploit.In accounts ⓘ

Quelle: haveibeenpwned.com

**SECURITY IST NICHT
MEIN JOB!?**

EU DATENSCHUTZ GRUNDVERORDNUNG (EU-DSGVO)

Ab Mai 2018 geltendes Recht!



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

ARTIKEL 32

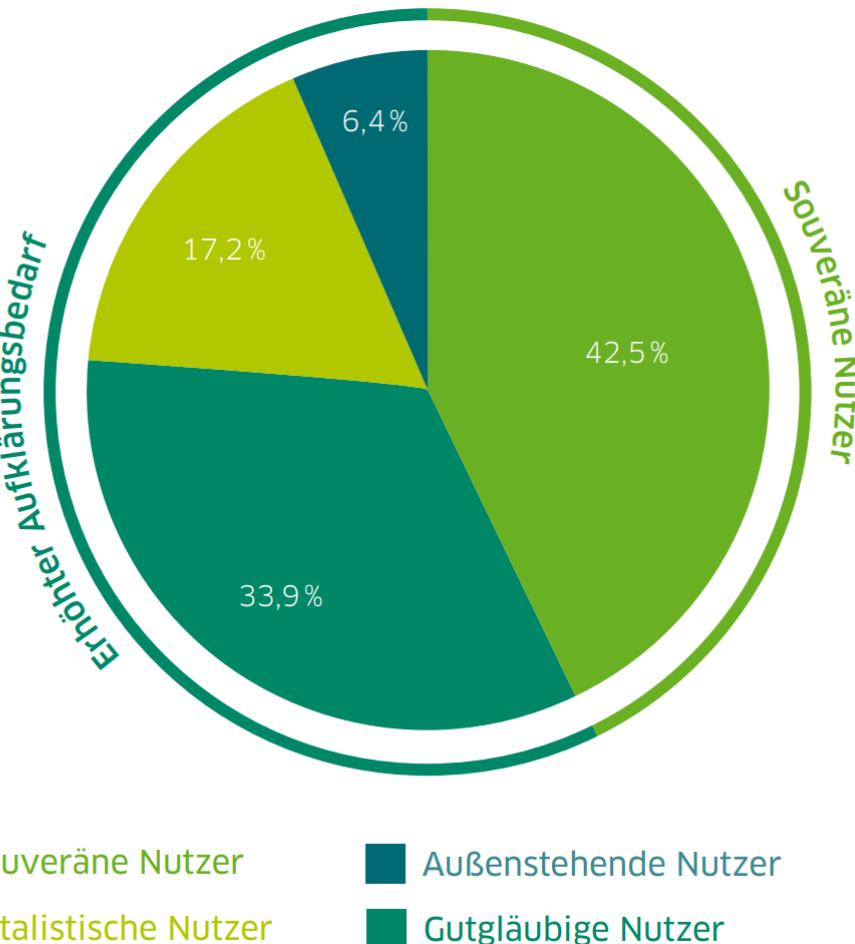
(SICHERHEIT DER VERARBEITUNG)

“ Unter Berücksichtigung des Stands der Technik, ... treffen der Verantwortliche ...geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten... ”

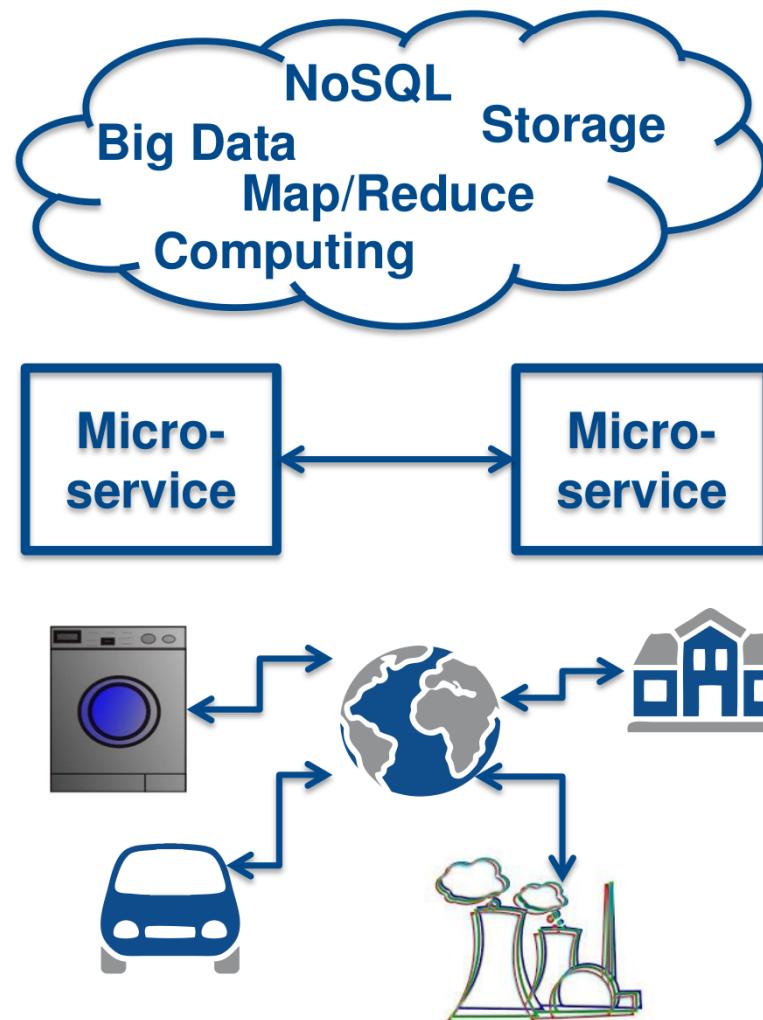
Quelle: eur-lex.europa.eu

NUTZERVERHALTEN

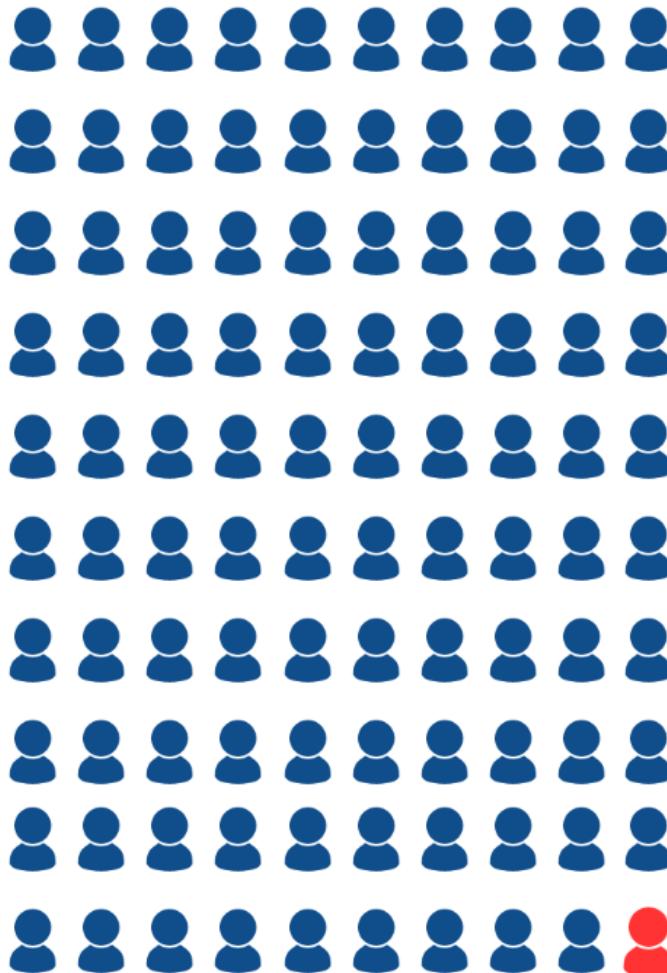


Quelle: Deutschland sicher im Netz (DsiN): Sicherheitsindex 2017

NEUE HERAUSFORDERUNGEN



1 SECURITY-PROFESSIONAL FÜR 100 ENTWICKLER

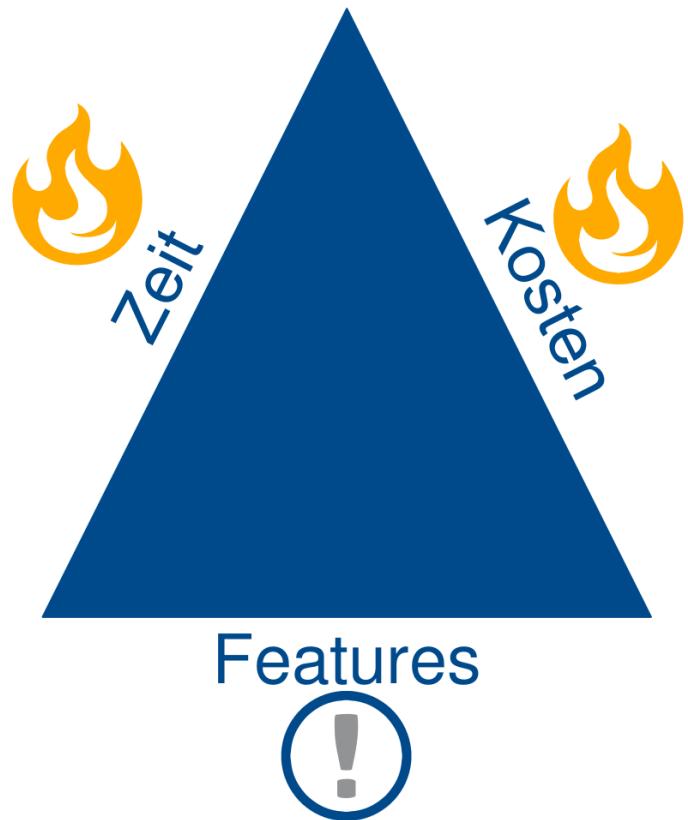


Quelle: sonatype.com/devops-survey-report

SICHERHEIT

IM PROJEKTALLTAG

WIR HABEN DOCH KEINE ZEIT



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

HACKER FINDEN UNS NICHT? (INTERESSANT)

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!

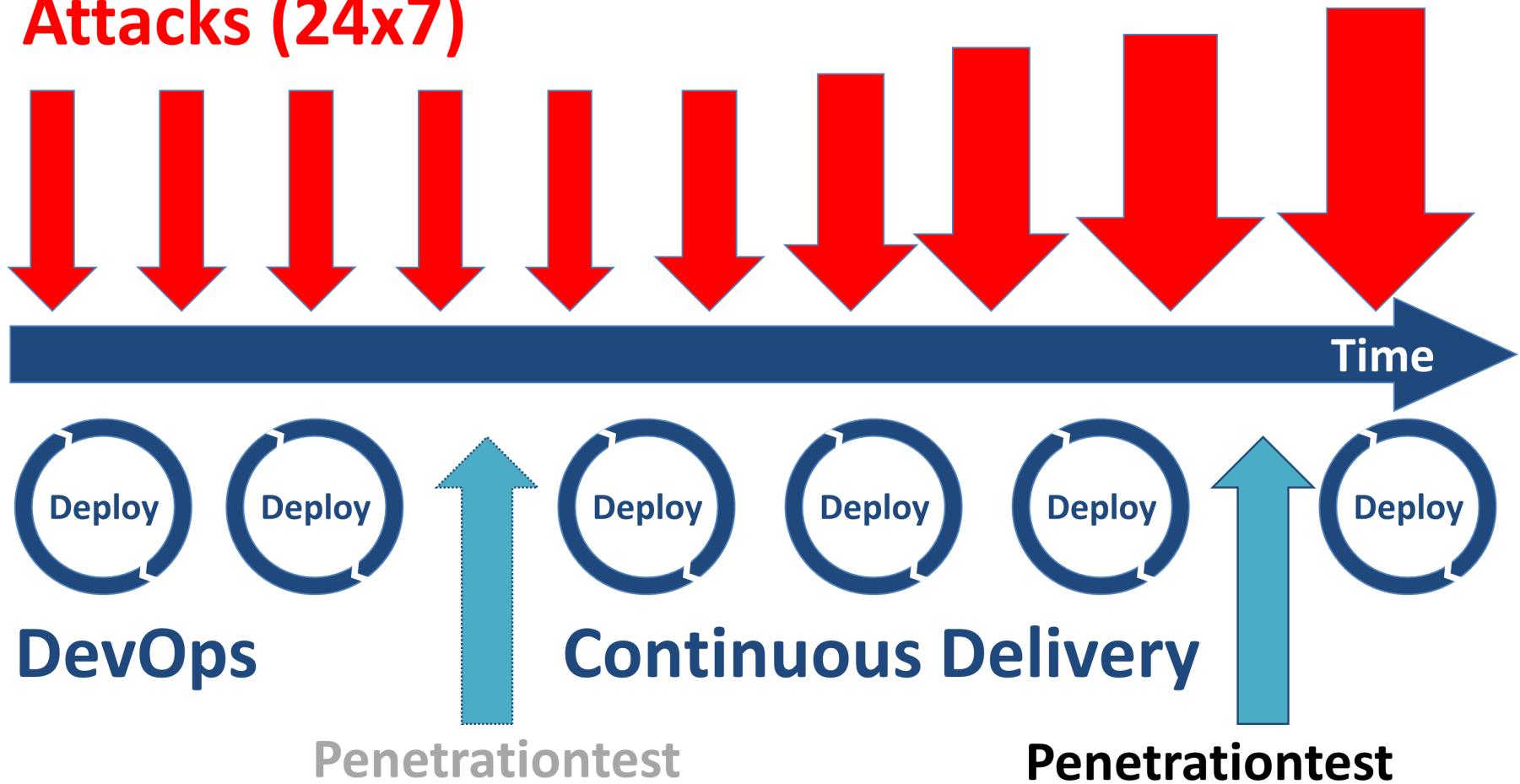


Get a Competitive Advantage

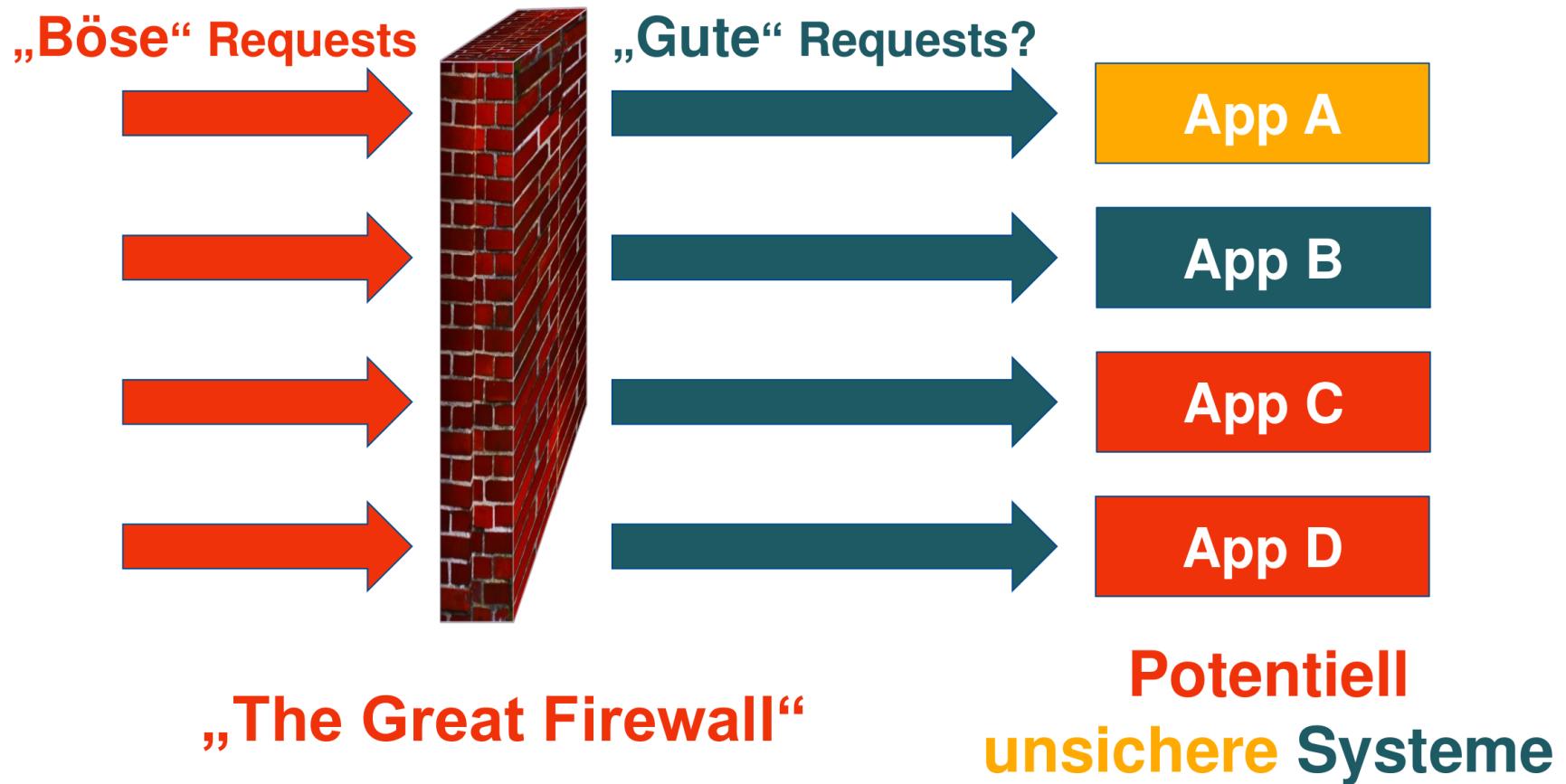
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Quelle: shodan.io

Attacks (24x7)



WIR HABEN DOCH EINE FIREWALL



AUSBILDUNG DER ENTWICKLER?

Entwicklung (Kopieren) aus stackoverflow.com

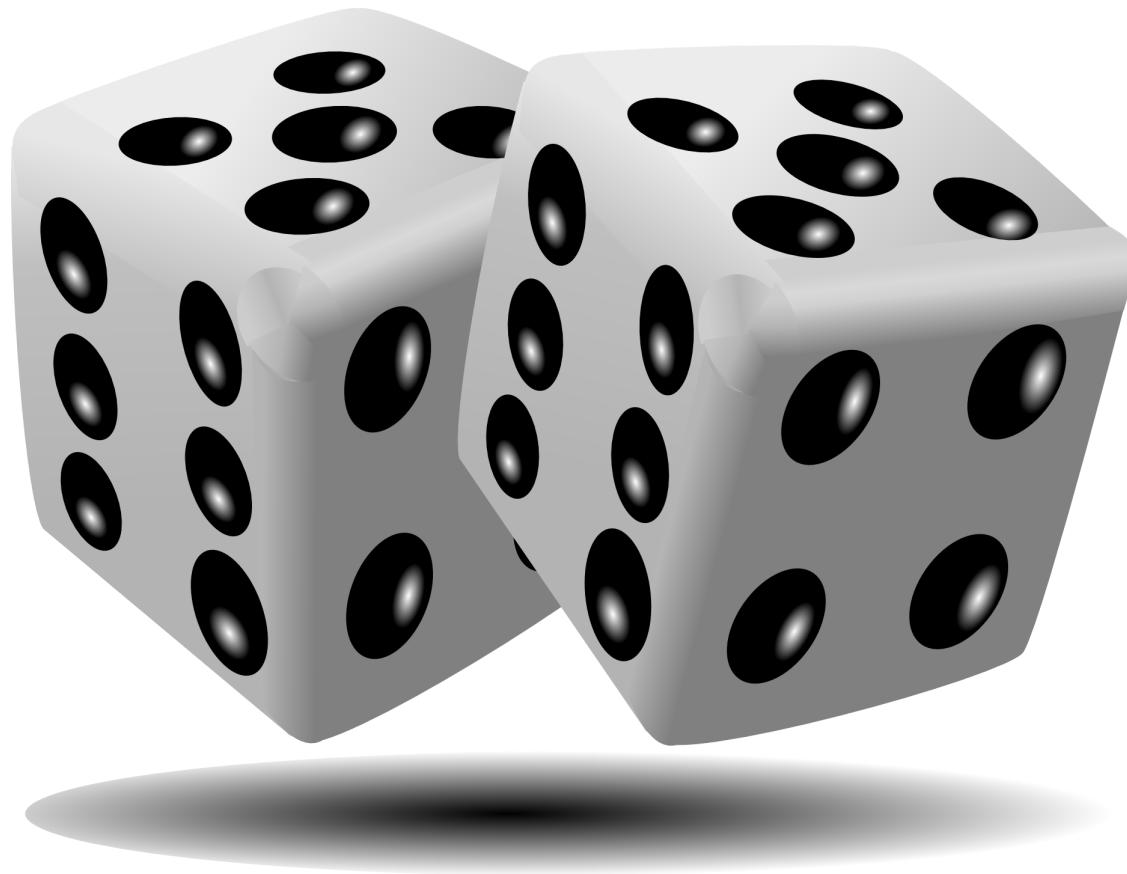
This is somewhat simple

```
string inp = "hai";
StringBuilder strb = new StringBuilder();
foreach (char s in inp)
{
    int sin = s + 5;
    char newch = (char)sin;
    strb.Append(newch);
}
string output = strb.ToString();
```

Now the output contains the encrypted string "mfn" (ie., 5 letters away from the original)in it....

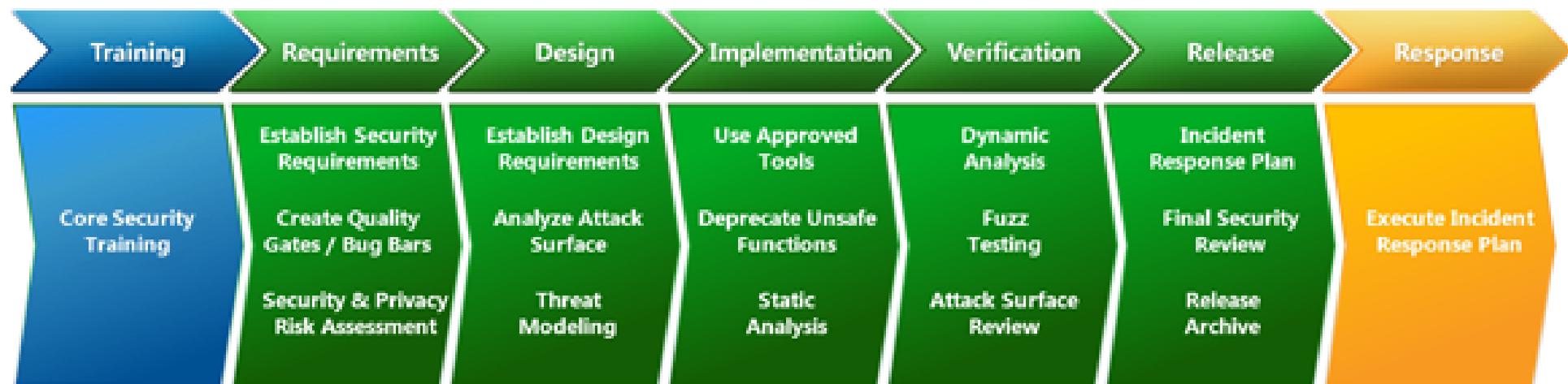
Quelle: stackoverflow.com

WEITER SO?



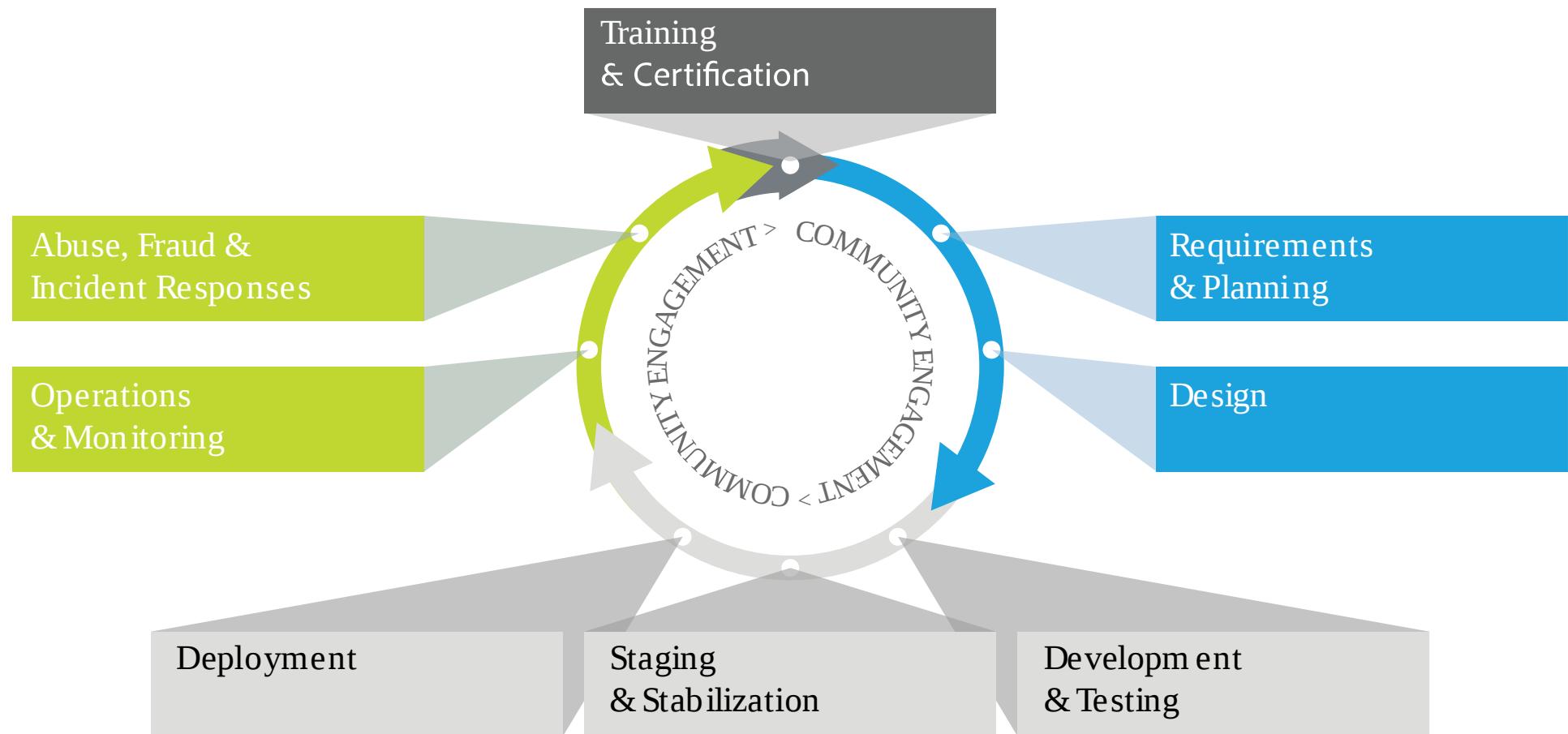
SICHERE ENTWICKLUNGS- PROZESSE ?

MICROSOFT SECURITY DEVELOPMENT LIFECYCLE



Quelle: microsoft.com/en-us/sdl

ADOBE SECURE PRODUCT LIFECYCLE



Quelle: adobe.com/security/engineering.html

Agile

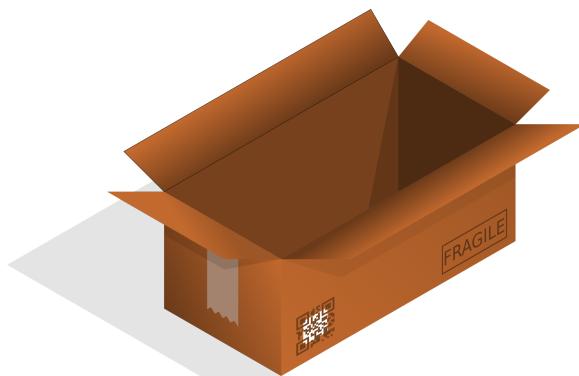


Waterfall

SCRUM GUIDE

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

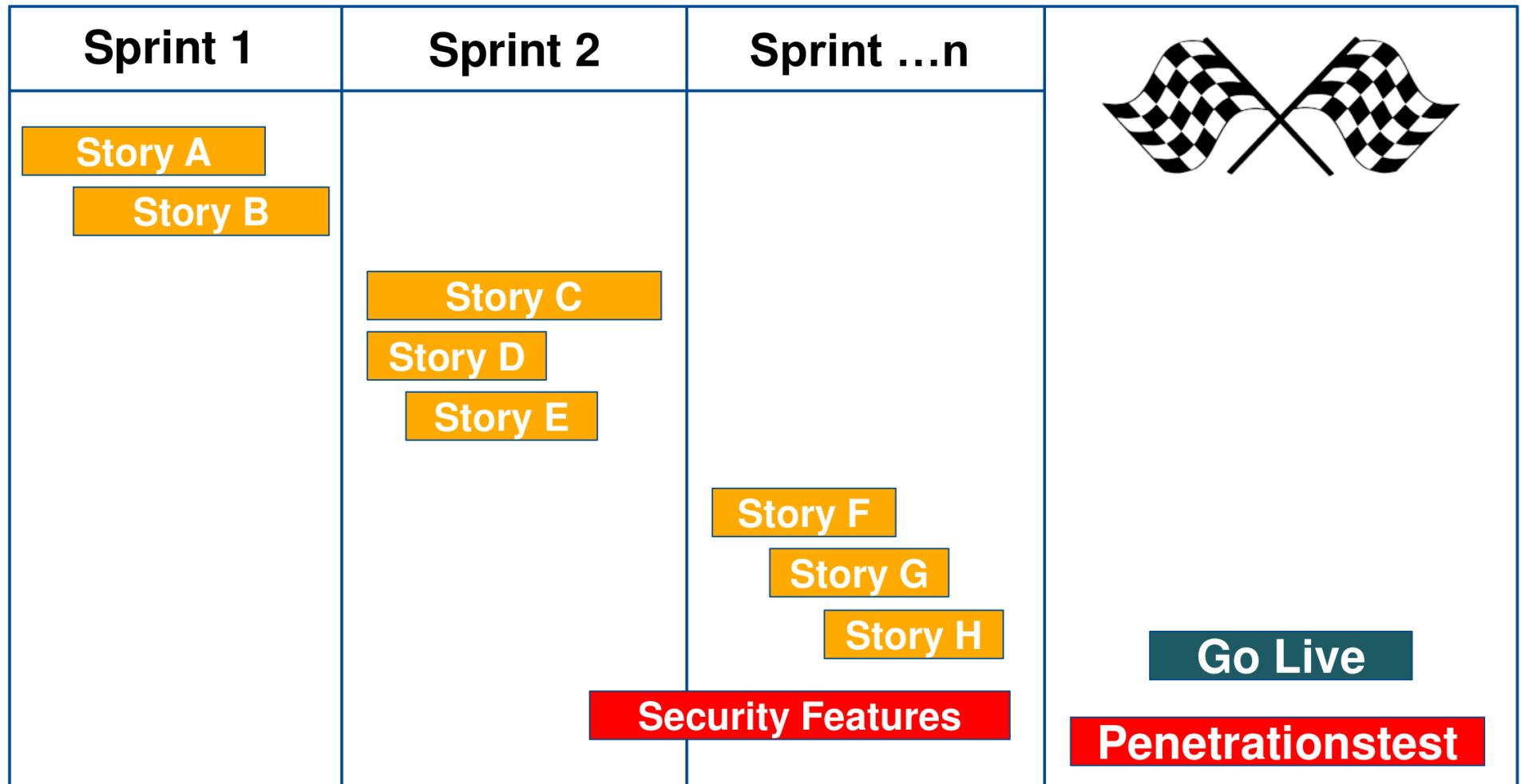
Quelle: www.scrumguides.org



POTENTIELL UNSICHER AUSLIEFERN ?



AUSGANGSLAGE: SECURITY != AGIL!



Agile Entwicklung

Inkrementell mit schnellem Feedback

Innerhalb von Sprints

“Working software over comprehensive documentation”

Business Value

Penetration-Testing

Punktuell und Aufwendig

Abseits von Sprints

Umfassende Reports

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 OS X 10.6.8, which reveals the inode number, can be triggered by sending an ETag header.

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:

Raw	Headers	Hex	JSON	JSON Beautifier
HTTP/1.1 200 OK				
	Content-Type: application/json			
	Date: Wed, 29 Nov 2017 10:43:01 GMT			
	Etag: W/"5a180090-acab"			
	Last-Modified: Fri, 24 Nov 2017 11:20:48 GMT			

Server: nginx

CVSS Base Score: 3.7

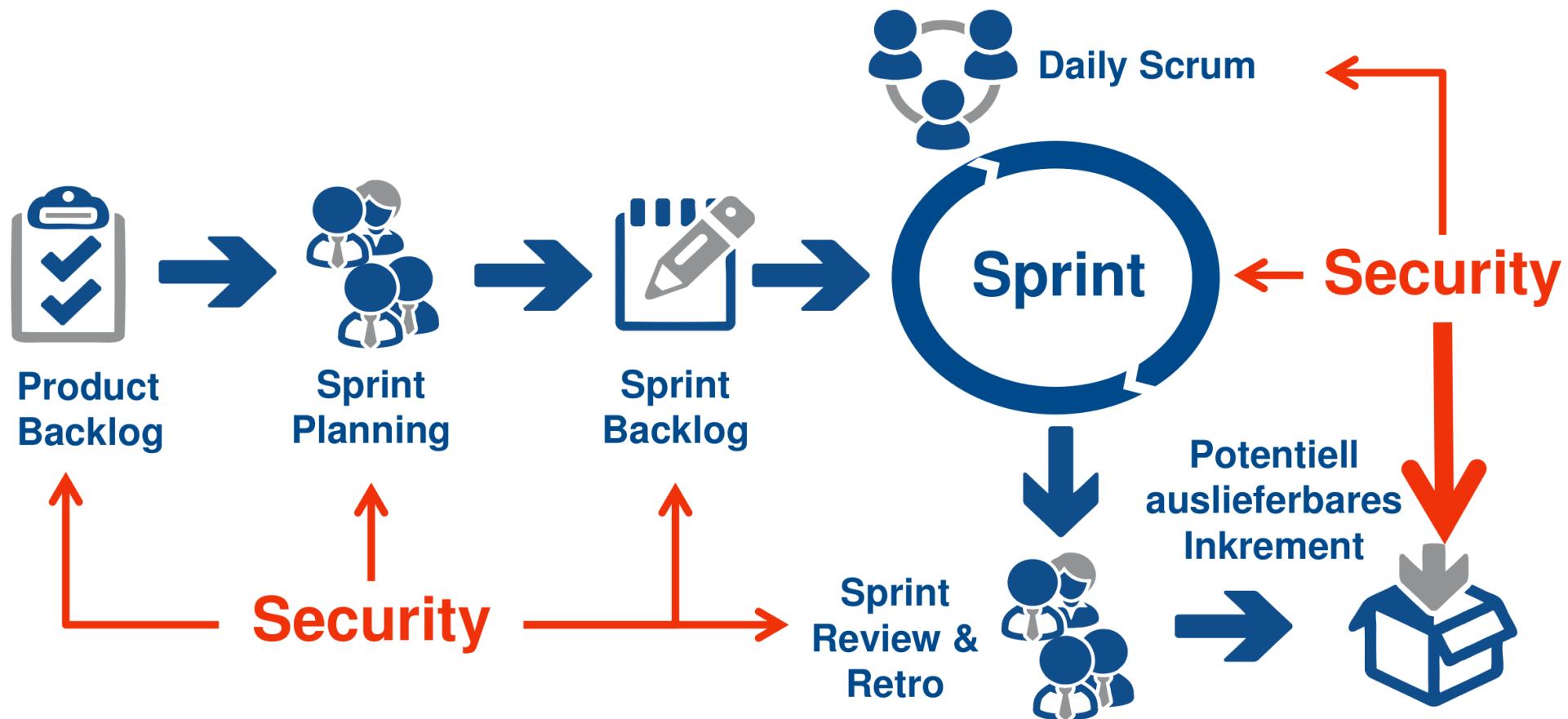
Possible Remediation:

B. 5

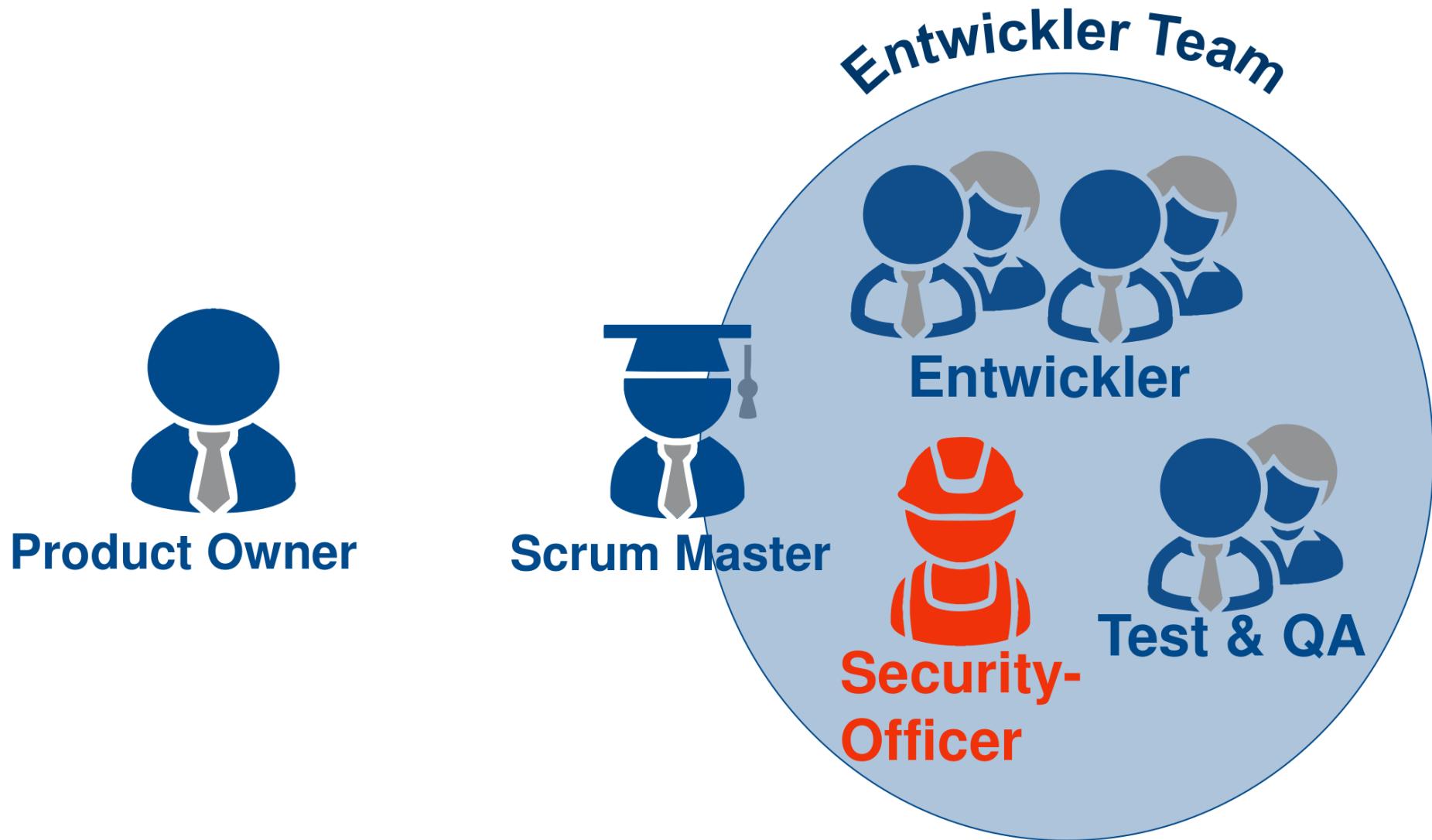
<https://nvd.nist.gov/vuln/detail/CVE-2003-1418>

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

SECURITY IN SCRUM



SECURITY OFFICER/CHAMPION



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 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]	↳	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]	↳	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

ANFORDERUNGEN UND TESTS



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

PRO ACTIVE CONTROLS

PATTERNS FÜR SICHERE ENTWICKLUNG



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

JUICE SHOP

OWASP Juice Shop v6.3.0

→ Login | English | Search... | Search | Contact Us | Score Board

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

Score Board

2%

Difficulty

★	★★	★★★	★★★★	★★★★★
✓ 1/9	✓ 0/8	✓ 0/21	✓ 0/9	✓ 0/6

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>



Product Backlog

- Threat Model Refinement
- **Ab**User 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

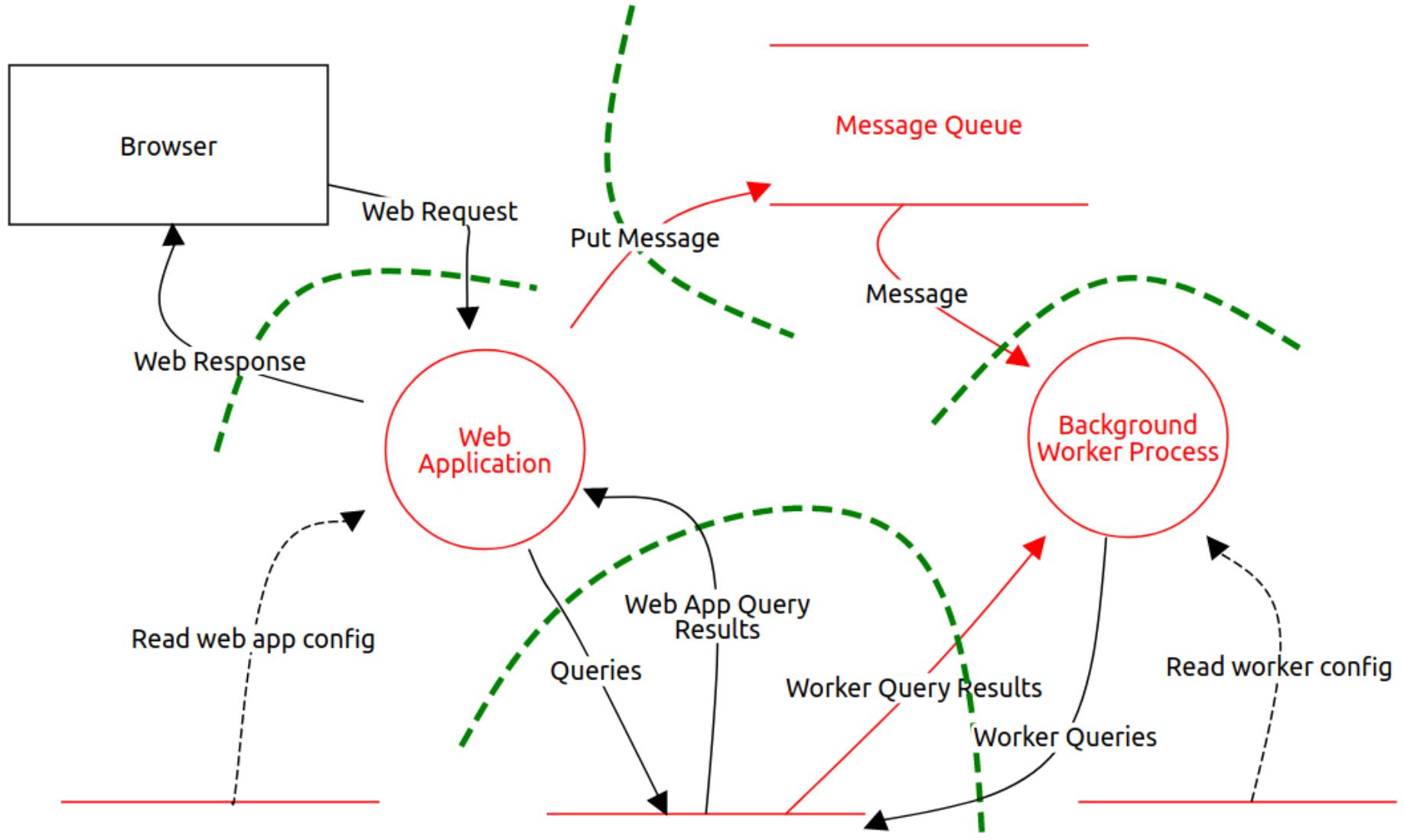
User Stories,
UML Diagramme

Threat Model
Als
Diskussions-Basis

Identifikation und
Vermeidung
von Bedrohungen

„Elevation of privilege“ Spiel





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

ABUSER STORY TASKS

To Do

In Progress

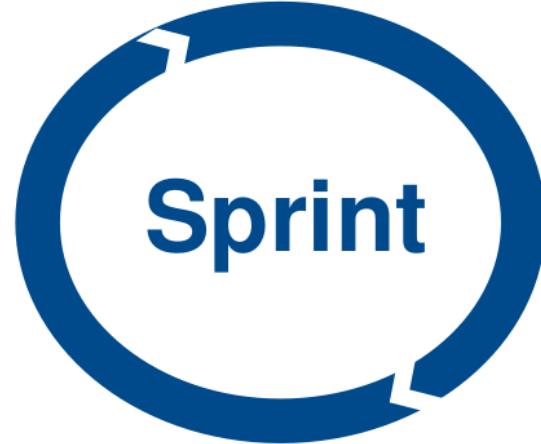
Done

>  TODO-11  6 sub-tasks Als Administrator möchte ich Benutzer verwalten um diese für die Anwendung zu autorisieren		
▼  TODO-10  4 sub-tasks Als Script-Kiddie möchte ich mich mit administrativen Rechten anmelden um Spam als ToDo's einzutragen		
 TODO-20 ↑ Test auf Session-Fixation (neue JSESSIONID nach Anmeldung)	 TODO-18 ↑ Verwundbarkeit der Eingabefelder für XSS-Injections testen	
 TODO-21 ↑ Prüfung, ob Passwort in Klartext ersichtlich ist (UI, Logs, DB, HTTP)		
 TODO-22 ↑ Alle Webseiten auf unauthorisierten Zugriff prüfen (Umgehung von Login möglich?)		



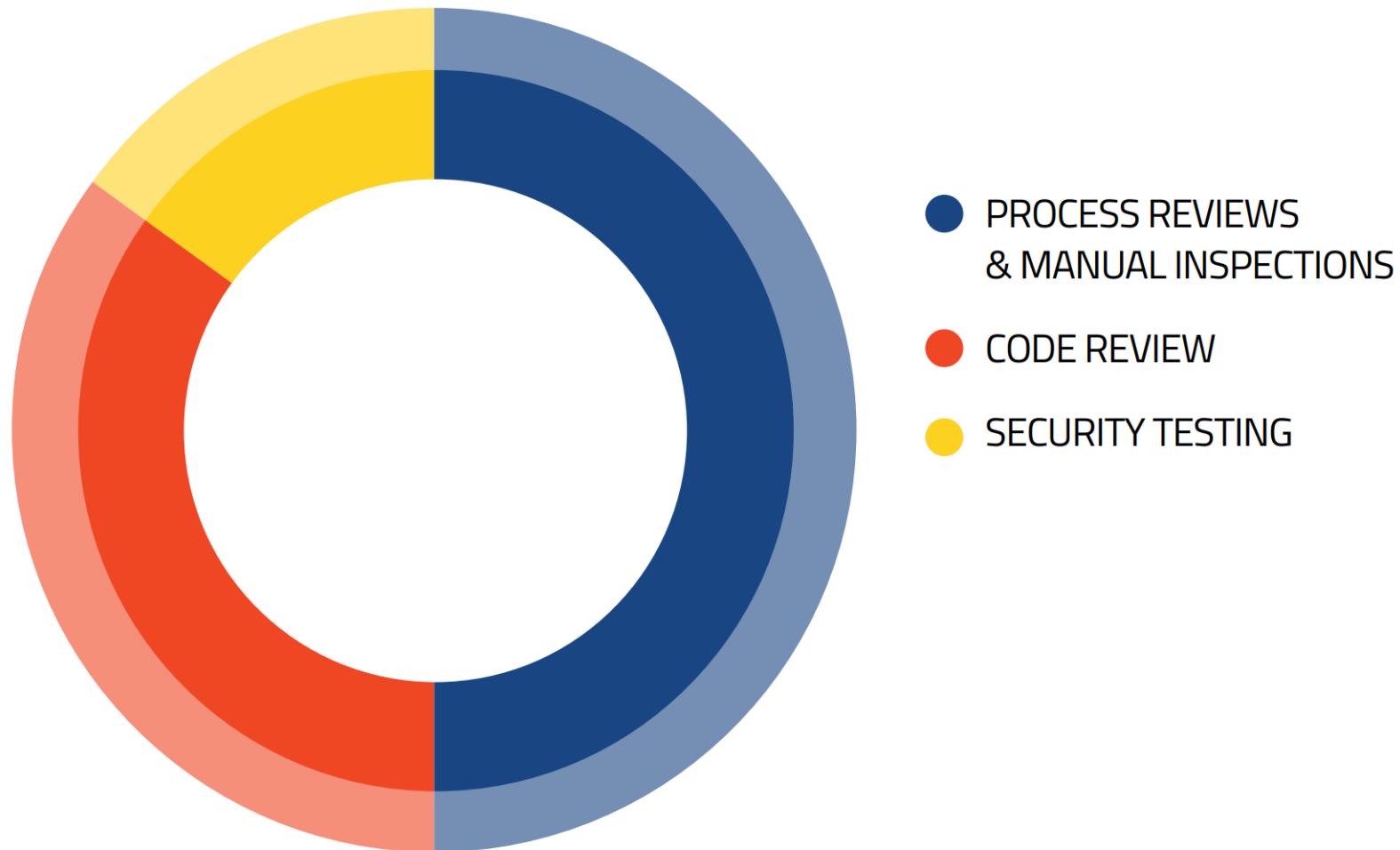
Daily Scrum

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



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

AGILE SECURITY TESTING



Quelle: www.owasp.org/index.php/OWASP_Testing_Project

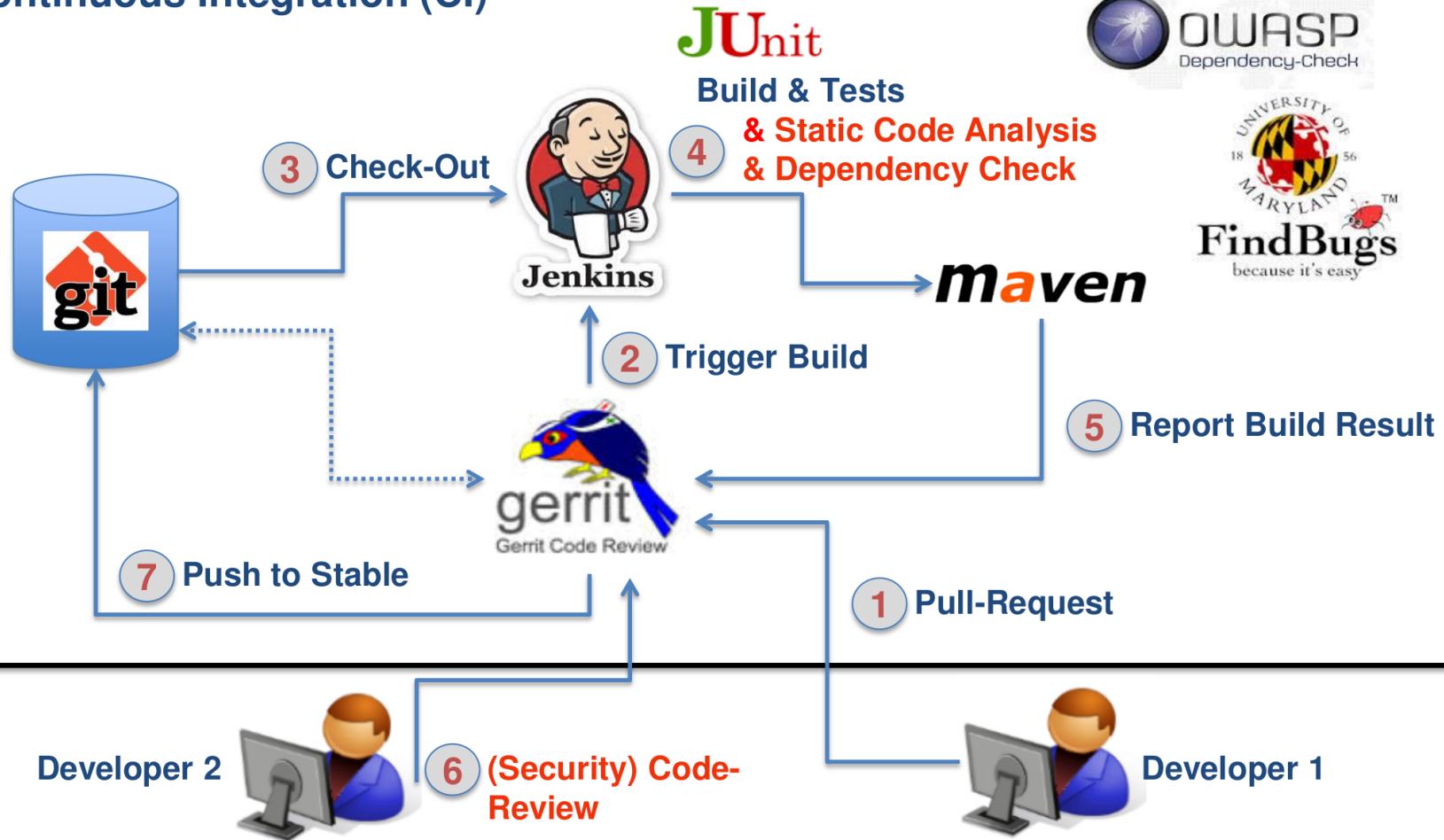
ENTWICKLER SECURITY TESTS

BEVOR EIN ANGREIFER “TESTET”

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

CI COMMIT-STAGE MIT STATISCHER ANALYSE (SAST)

Continuous Integration (CI)



OWASP DEPENDENCY CHECK

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

<https://github.com/jeremylong/DependencyCheck>

OWASP DEPENDENCY CHECK REPORT



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO WARRANTIES or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: google group](#) | [github issues](#)

Project: root project 'dependency-check-demo'

Scan Information ([show all](#)):

- dependency-check version: 3.0.2
- Report Generated On: Nov 24, 2017 at 10:48:37 +01:00
- Dependencies Scanned: 12 (12 unique)
- Vulnerable Dependencies: 4
- Vulnerabilities Found: 13
- Vulnerabilities Suppressed: 0
- ...

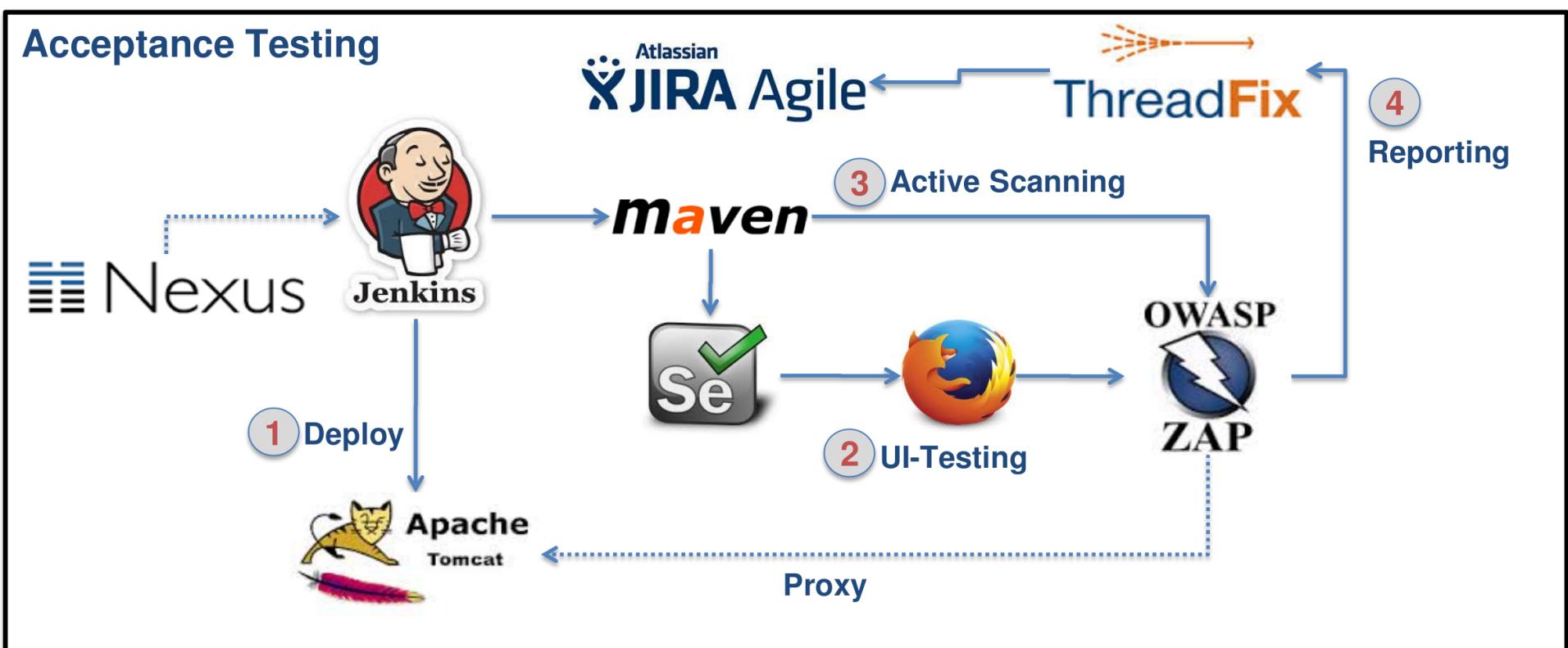
Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
struts2-core-2.5.jar	cpe:/a:apache:struts:2.5	org.apache.struts:struts2-core:2.5 ✓	High	9	Highest	32
commons-collections-3.2.jar	cpe:/a:apache:commons_collections:3.2.1	commons-collections:commons-collections:3.2 ✓	High	1	Low	36
log4j-api-2.5.jar	cpe:/a:apache:log4j:2.5	org.apache.logging.log4j:log4j-api:2.5 ✓	High	1	Highest	38
commons-fileupload-1.3.1.jar	cpe:/a:apache:commons_fileupload:1.3.1	commons-fileupload:commons-fileupload:1.3.1 ✓	High	2	Highest	38

Dependencies

[struts2-core-2.5.jar](#)

CI SECURITY-STAGE MIT DYNAMISCHER ANALYSE (DAST)

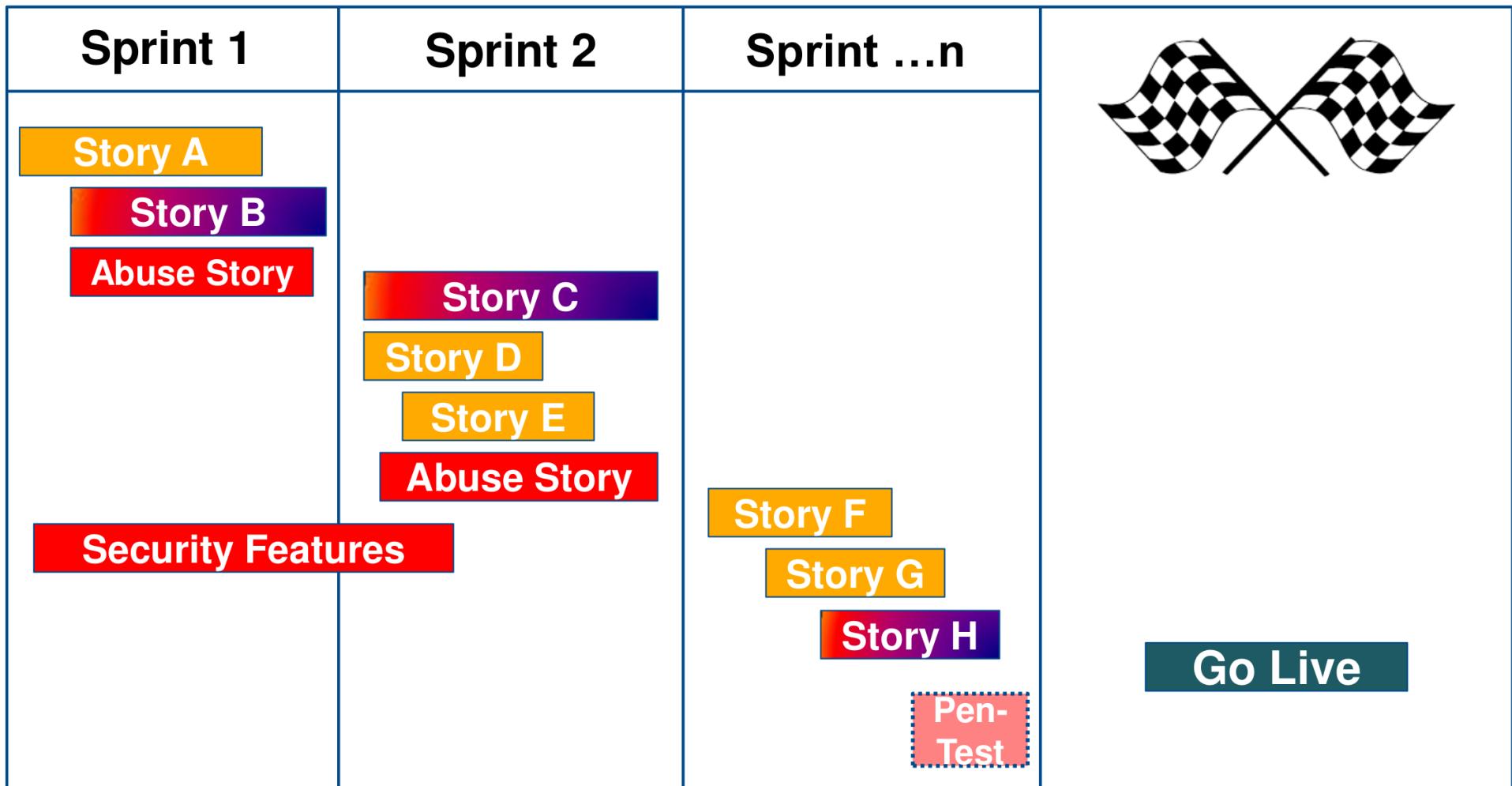




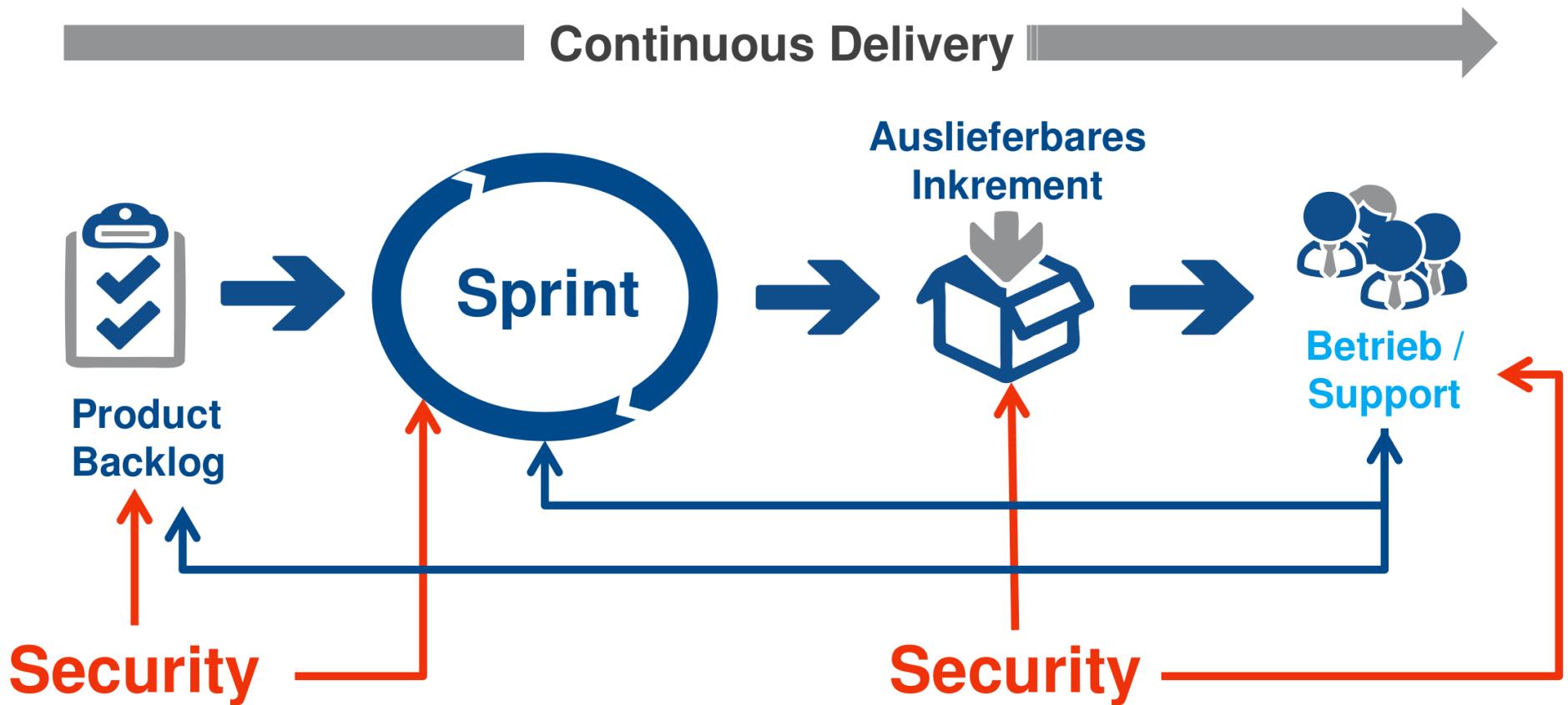
Sprint Review & Retro

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

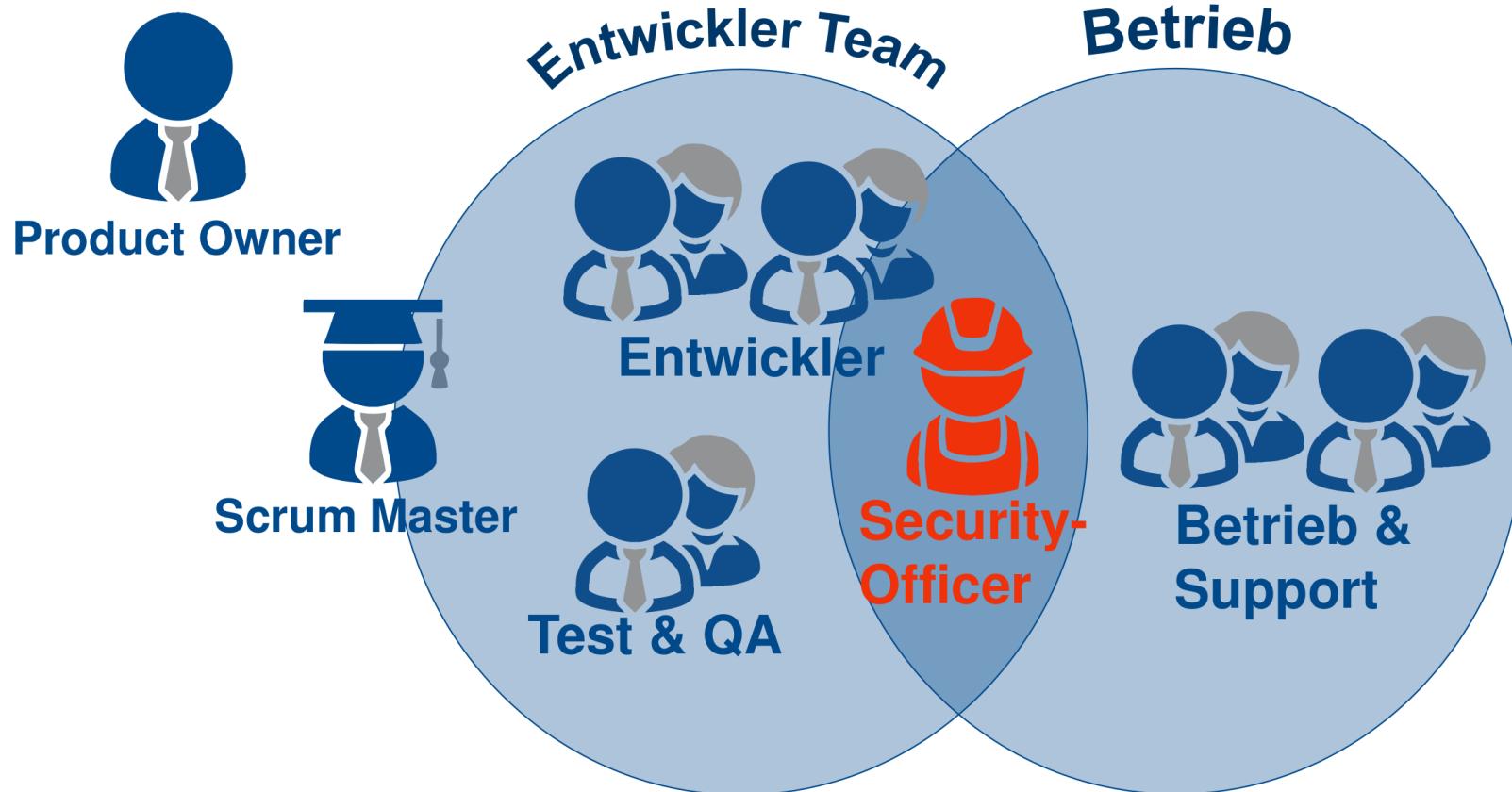
IDEALZUSTAND: SECURITY == AGIL!



SECDEVOPS

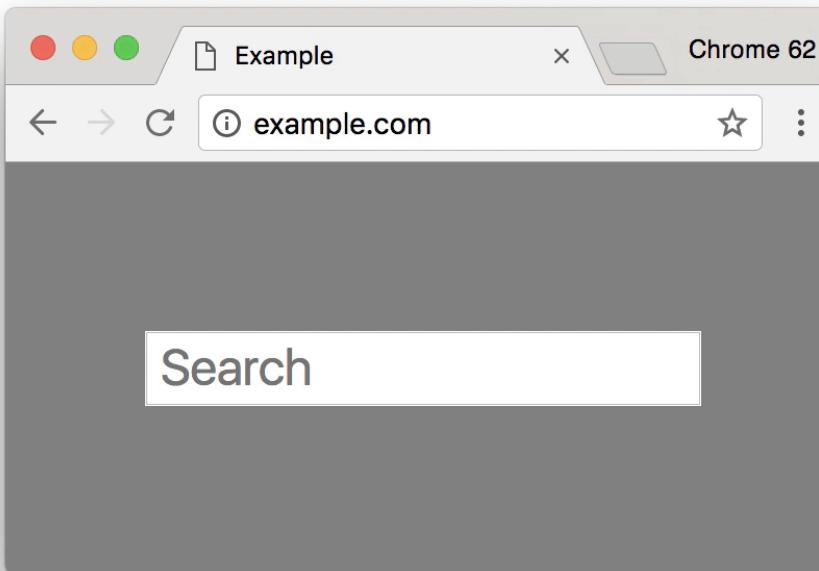


SECURITY OFFICER/CHAMPION IN SECDEVOPS



HTTPS IST PFLICHT !!

Let's Encrypt
CloudFlare
HTTP/2



HTTPS-KONFIGURATION ÜBERPRÜFEN

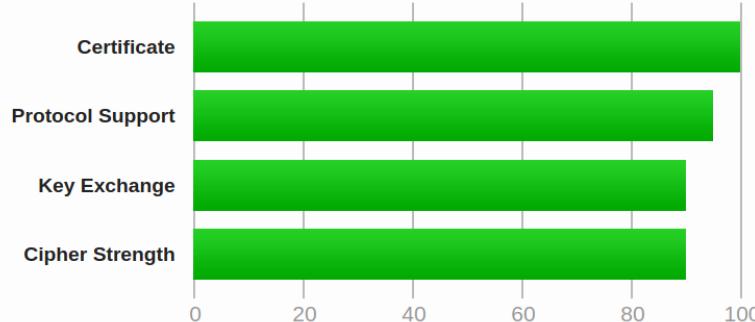
SSL Report: [andreas-falk.de](#) (104.28.12.71)

Assessed on: Fri, 23 Feb 2018 12:41:16 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

www.ssllabs.com/ssltest

SECURITY HEADER ÜBERPRÜFEN

Security Report Summary



Site:	https://andreas-falk.de/
IP Address:	2400:cb00:2048:1::681c:c47
Report Time:	23 Feb 2018 12:57:08 UTC
Report Short URL:	Feature disabled.
Headers:	✓ X-Frame-Options ✓ X-XSS-Protection ✓ X-Content-Type-Options ✓ Strict-Transport-Security ✗ Content-Security-Policy ✗ Referrer-Policy

Raw Headers

HTTP/1.1	200 OK
Date	Fri, 23 Feb 2018 12:57:08 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	keep-alive
Set-Cookie	_cfduid=d0e30045de3100883d49939d0349e6bdf1519390626; expires=Sat, 23-Feb-19 12:57:06 GMT; path=/; domain=.andreas-falk.de; HttpOnly; Secure
X-Powered-By	PHP/7.0.20
X-Frame-Options	DENY
X-XSS-Protection	1; mode=block
X-Content-Type-Options	nosniff
Link	< https://andreas-falk.de/wp-json/ >; rel="https://api.w.org/", < https://wp.me/P4NtFZ-3X >; rel=shortlink
Set-Cookie	wfvt_1740180939=5a900fa3c1772; expires=Fri, 23-Feb-2018 13:27:07 GMT; Max-Age=1800; path=/; secure; HttpOnly
Strict-Transport-Security	max-age=15552000
Expect-CT	max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server	cloudflare
CF-RAY	3f1a59548d279631-SJC

securityheaders.io

The background of the image is a clear blue sky with scattered white clouds of various sizes and shapes.

UND IN DER CLOUD?

ALTE BEKANNTE UND MEHR...

Alle OWASP Top 10 Web Probleme...

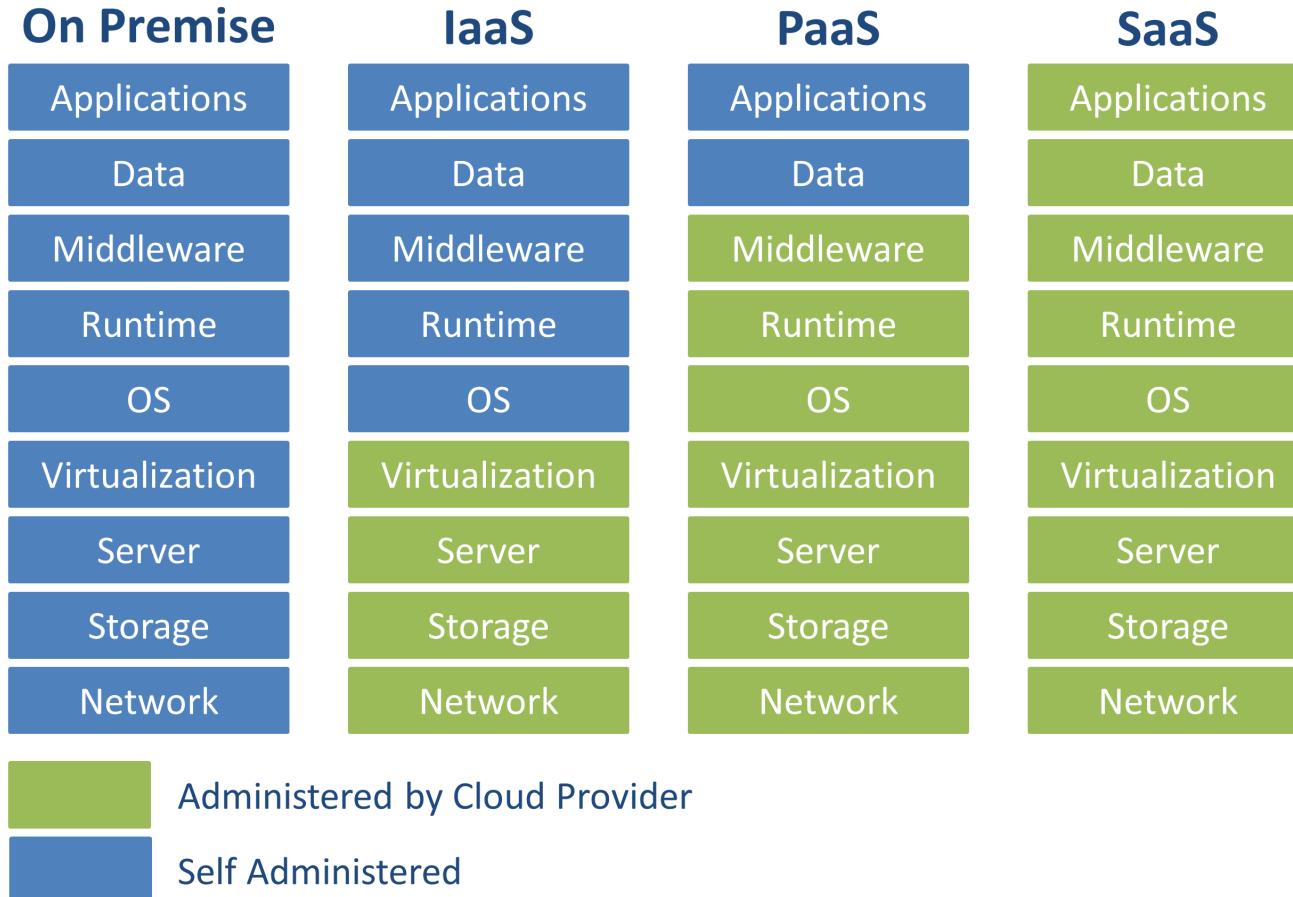
Distributed DoS

Economic DoS

The background of the image is a clear blue sky with scattered white clouds of various sizes and shapes.

**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)

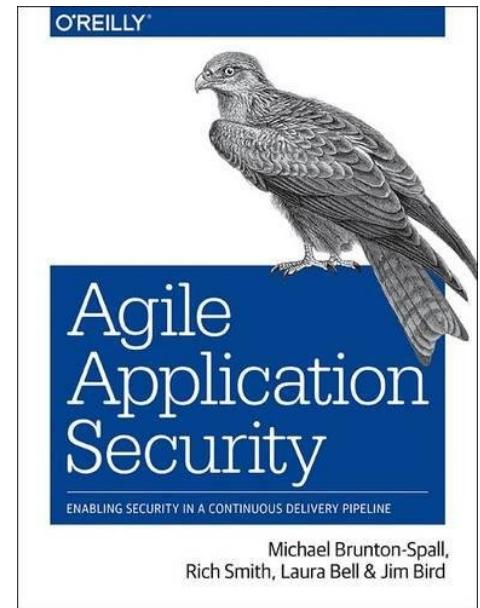
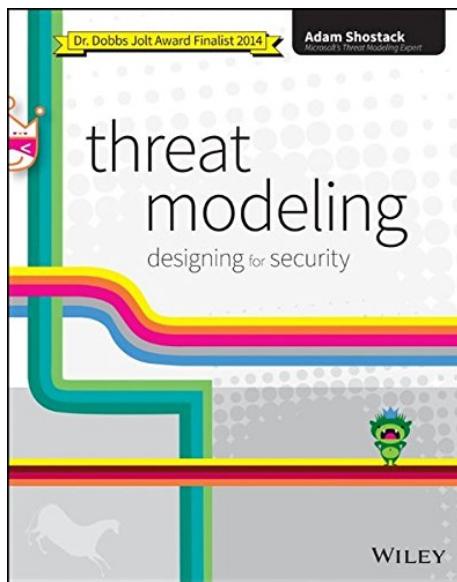
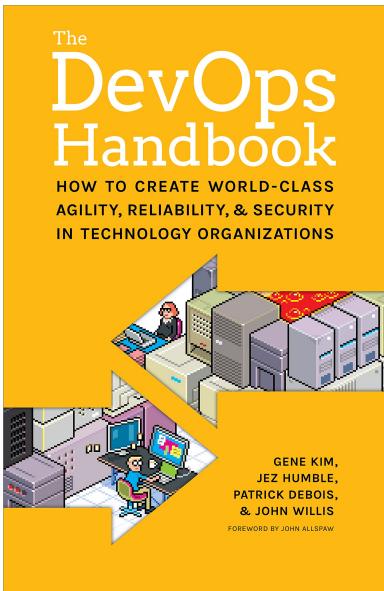
<https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave>

DAMIT DAS NICHT PASSIERT !!



Quelle: [youtube.com](https://www.youtube.com)

BOOK REFERENCES



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 \(\[https://www.owasp.org/index.php/OWASP_Proactive_Controls\]\(https://www.owasp.org/index.php/OWASP_Proactive_Controls\)\)](#)
- [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 \(<https://thenewstack.io/cloud-foundrys-approach-security-rotate-repair-repave>\)](#)

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

All used logos are trademarks of respective companies

Q&A

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

andreas.falk@novatec-gmbh.de

@NT_AQE, @andifalk



@JAX (Mainz)
25.4.2018

Datenschutz in der Cloud mit
Spring Cloud Vault



@Spring I/O (Barcelona)
24.5.-25.5.2018
[Spring Security Workshop](#)