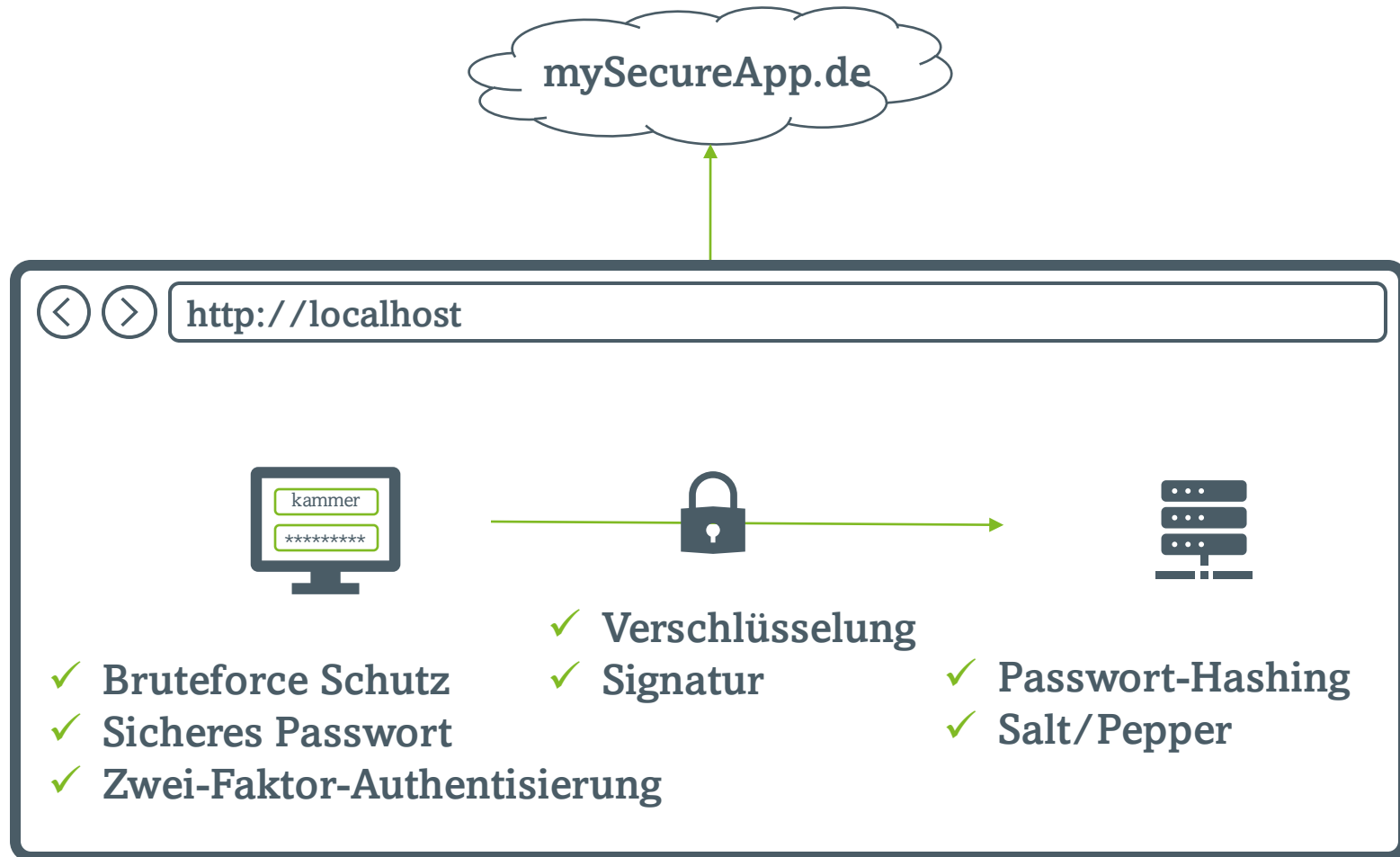


Secure Deployment

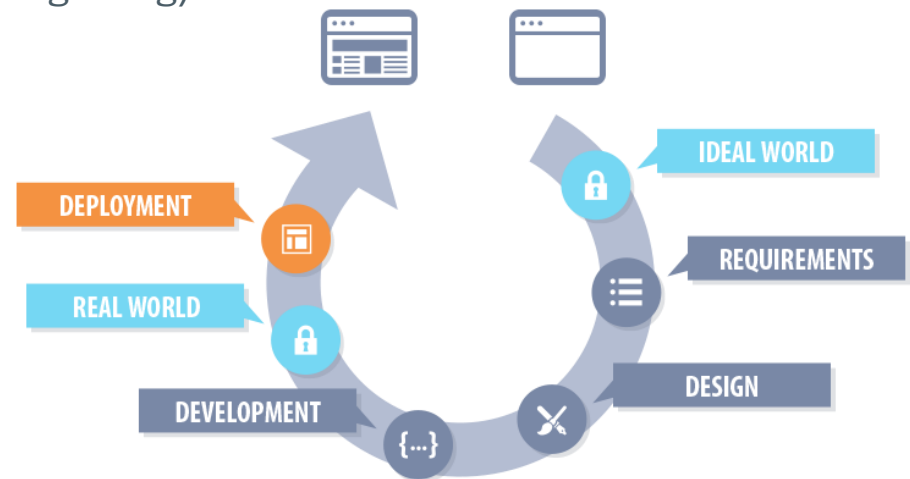


Rückblick



Was ist Deployment?

- Alle Maßnahmen, die dafür sorgen, dass die Software für die Nutzung bereitgestellt wird.
 - Installation (auf einer bestimmten Umgebung)
 - Konfiguration
 - Aktualisierung
 - Wartung
 - Updates und Patches



Die Umgebung in Kombination mit der neu entwickelten Software ist oft eine Quelle von Sicherheitsproblemen.

Was ist Secure Deployment?

Ziele

- Sicherheitsanforderungen sind auf die Umgebungen anzupassen
- Möglicherweise muss auch die Umgebung gewisse Sicherheiten zur Verfügung stellen (etwa: Einsatz von SSL zur Kommunikation)
- Zudem darf der Installationsprozess selbst keine Sicherheitslücken hinterlassen, etwa durch Einrichten von Test-Accounts
- Das Abstellen von erweiterter Fehler-Information und deaktivieren von Zugriffsmöglichkeiten dürfen nicht vergessen werden

Was ist Secure Deployment?

Incident Response

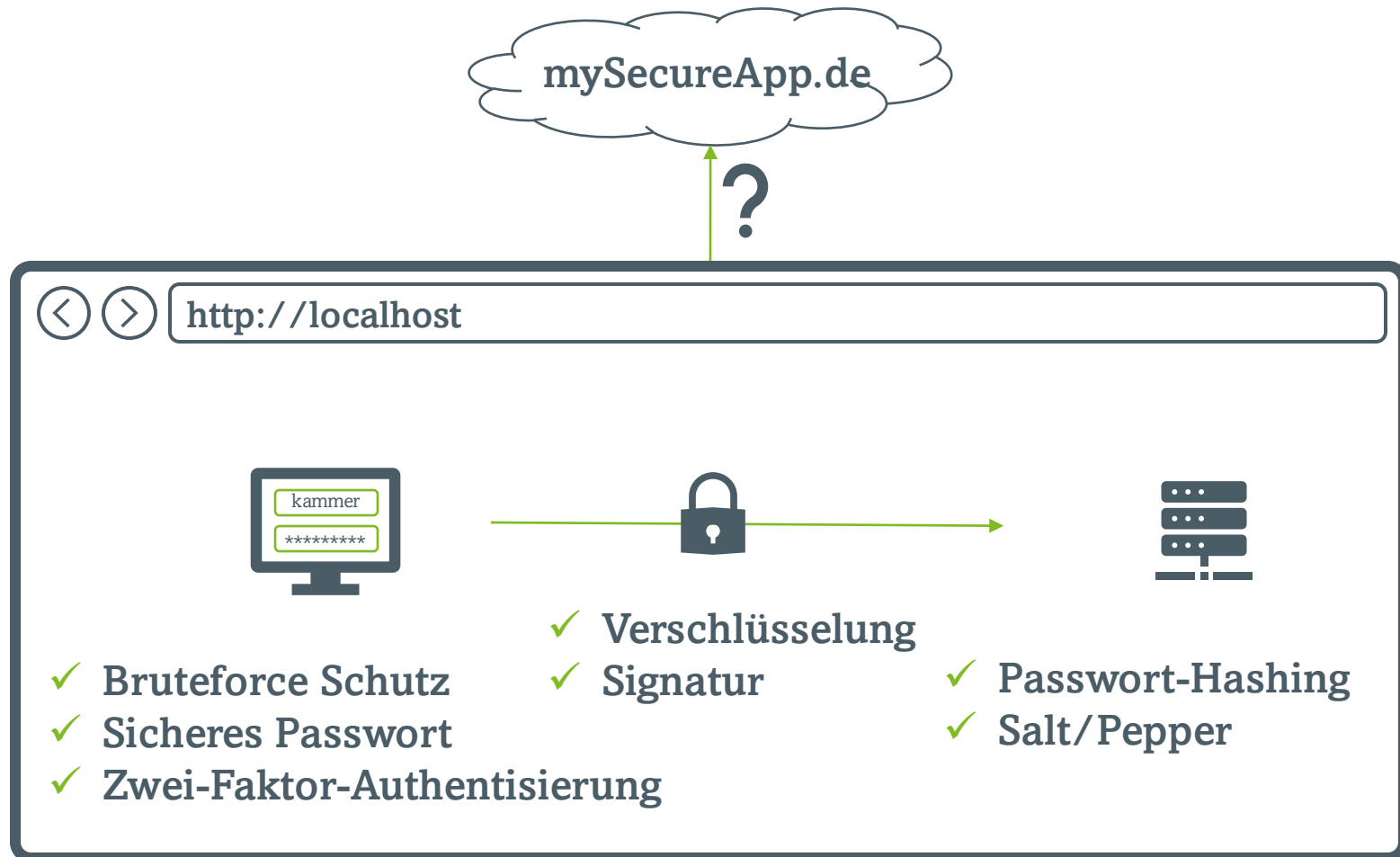
- **Keine Software ist fehlerfrei, erfolgreiche Angriffe gibt es immer!**
- Um auf entdeckte Sicherheitslücken angemessen zu reagieren, ist eine Vorbereitung innerhalb der Entwicklung erforderlich
- Im Gegensatz zu vielen Standard-Software-Fehlern ist bei Sicherheitsproblemen zu entscheiden:
 - Wann wird das Problem dem Kunden kommuniziert
 - Evtl. macht es Sinn, den Kunden schon zu informieren, auch wenn noch kein Patch vorhanden ist

Was ist Secure Deployment?

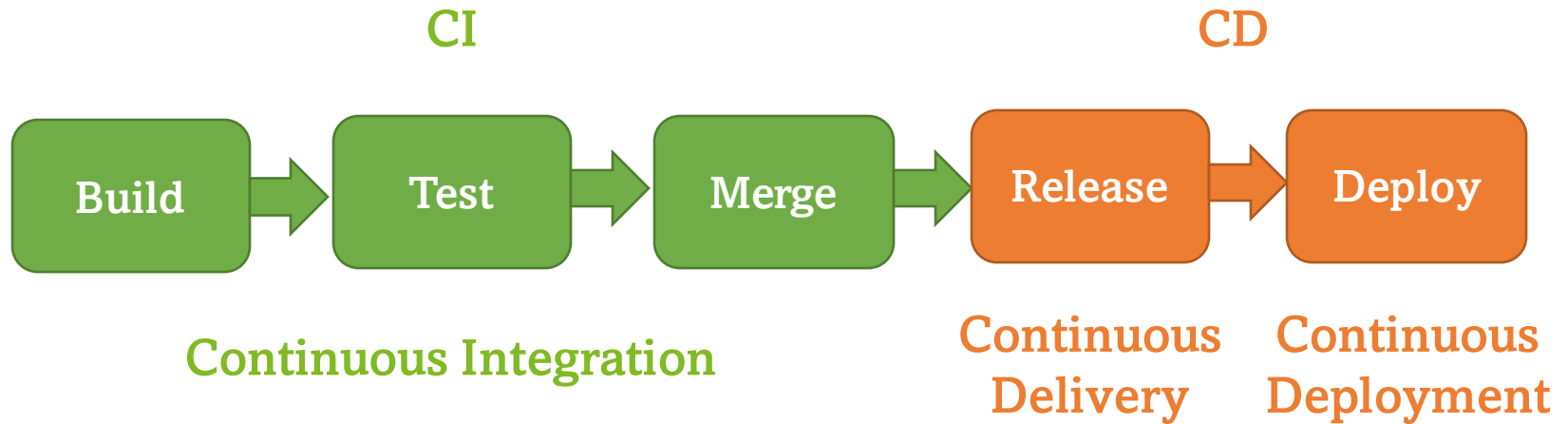
Security Metrics

- Investitionen in die Sicherheit sind oft schwer zu rechtfertigen
- Insbesondere gibt es kein unmittelbar sichtbares Ergebnis
- Im Gegenteil: Oft ist die Software weniger flexibel und es dauert länger
- Um einer grundsätzlichen Ablehnung von Sicherheitsmaßnahmen im Entwicklungsprozess entgegenwirken, sollte man die Auswirkung von Sicherheitsmaßnahmen messbar machen
 - Angriffsfläche (Schnittstellen, Zeilen Code, etc.)
 - Aufwand durch nachträgliches Lösen von Sicherheitsproblemen
 - Anzahl gefundener Coding-Schwachstellen bei Black-Box-Tests
 - Misst man derartige Werte regelmäßig, dann wird der Effekt von Aktivitäten zur Verbesserung der Software-Sicherheit transparent

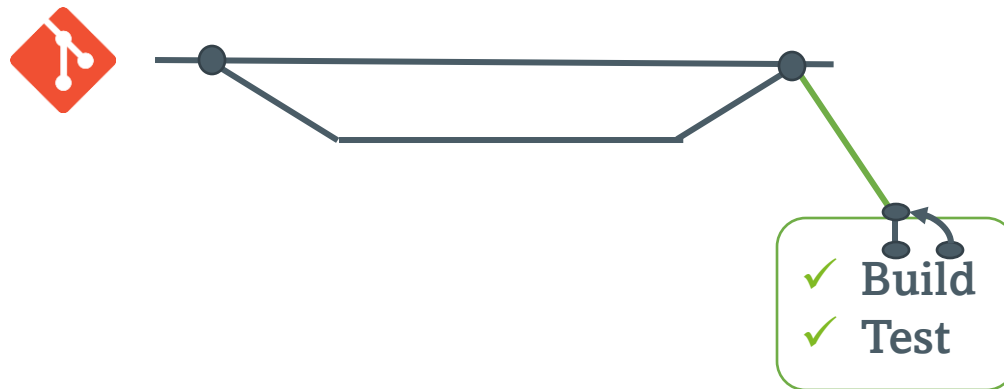
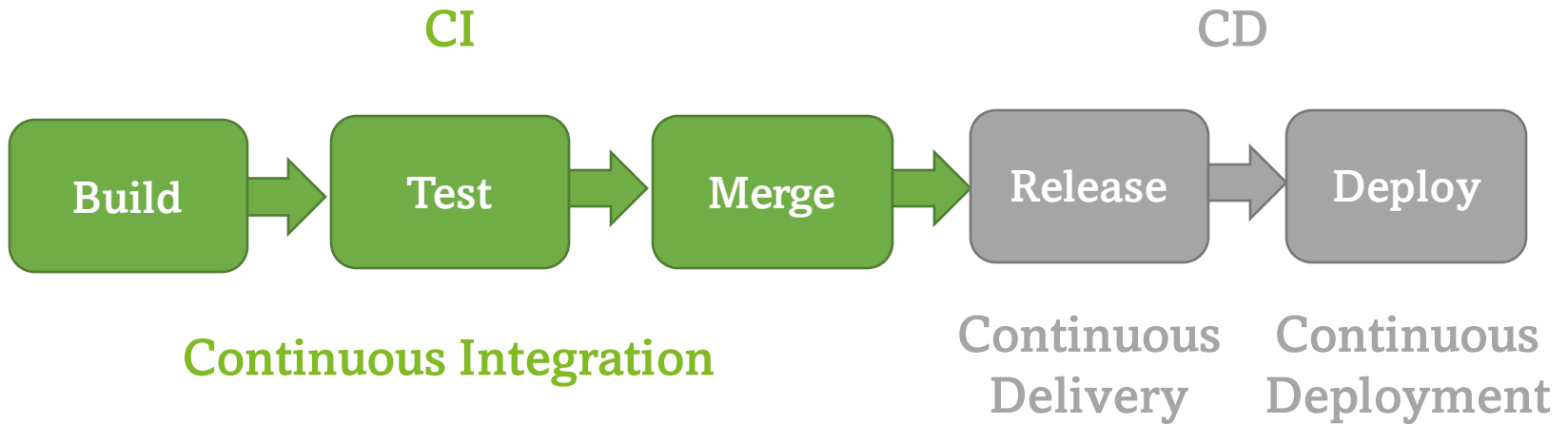
Rückblick



CI/CD



CI/CD



CI/CD

Beispiel: Github Actions

```
1   name: CI/CD
2
3   on: [push, pull_request]
4
5   jobs:
6     frontend-tests:
7       name: Frontend tests
8       runs-on: ubuntu-latest
9
10      steps:
11        - uses: actions/checkout@v2
```


CI/CD


Beispiel: Github Actions

```
12       - uses: actions/setup-node@v1
13         with:
14           node-version: '14'
15       - name: Install dependencies
16         run: (cd frontend && npm ci)
17       - name: Run tests
18         run: (cd frontend && npm run test:cov)
```





CI/CD


Beispiel: Github Actions



**All checks have passed**
2 successful checks

[Hide all checks](#)

	 CI/CD / Frontend tests (pull_request) Successful in 4m	Details
	 CI/CD / Frontend tests (push) Successful in 7m	Details

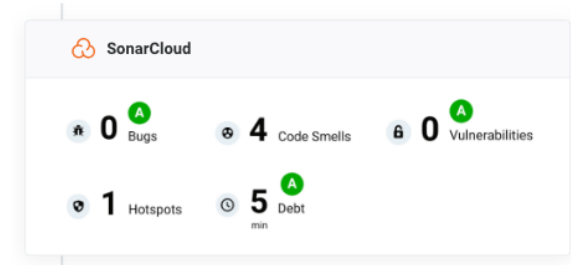
Merge pull request 

You can also [open this in GitHub Desktop](#) or view [command line instructions](#).

CI/CD

■ sonarcloud

- Fehler-, Schwachstellen- und Code-Smell-Erkennung
- <https://sonarcloud.io>



■ Codacy

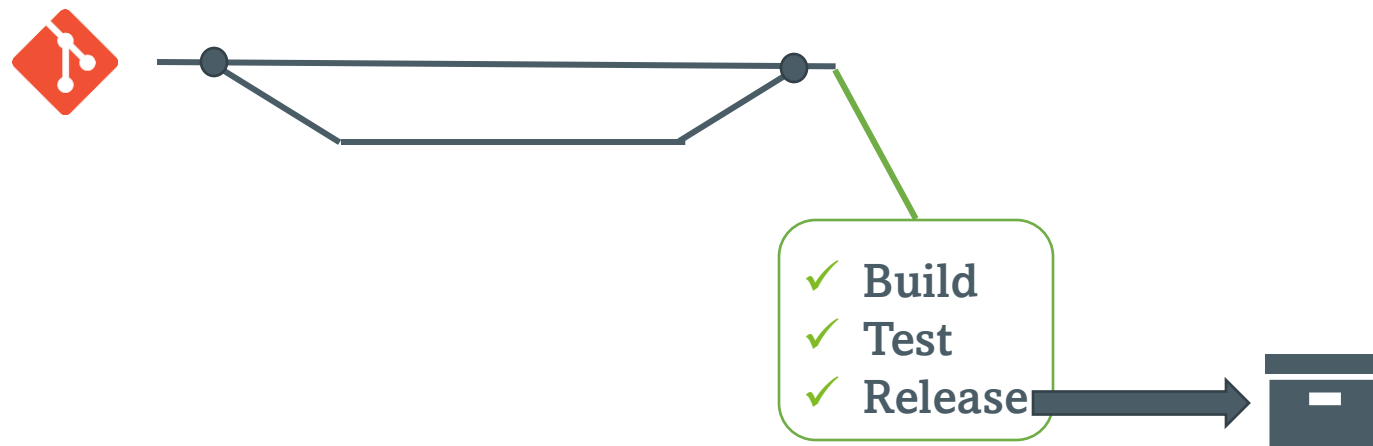
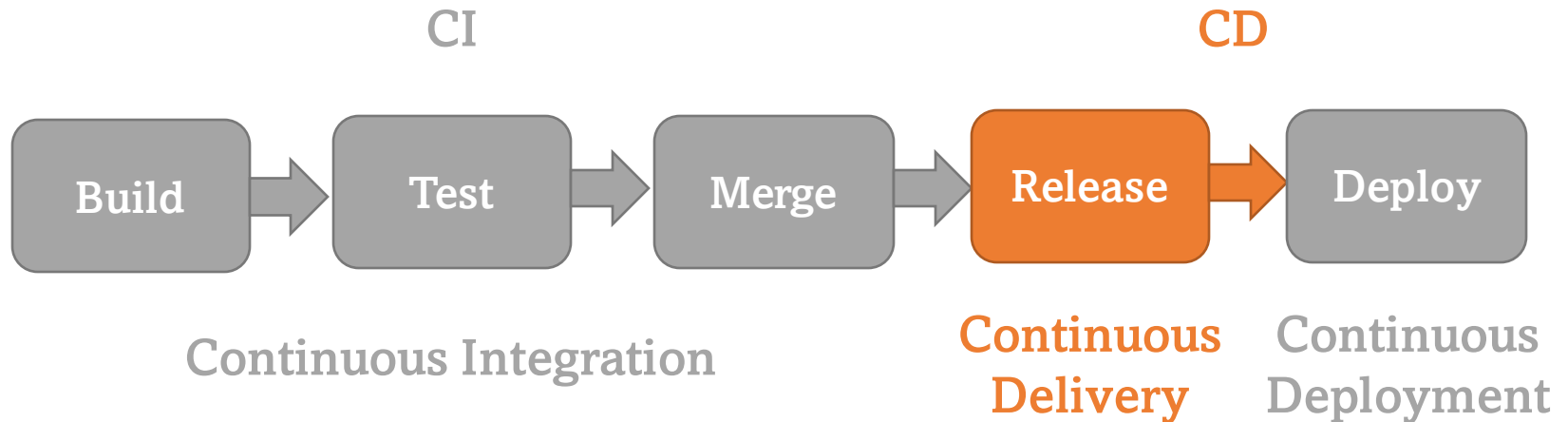
- High-security Standards, Code-Standardisierung
- <https://docs.codacy.com/>



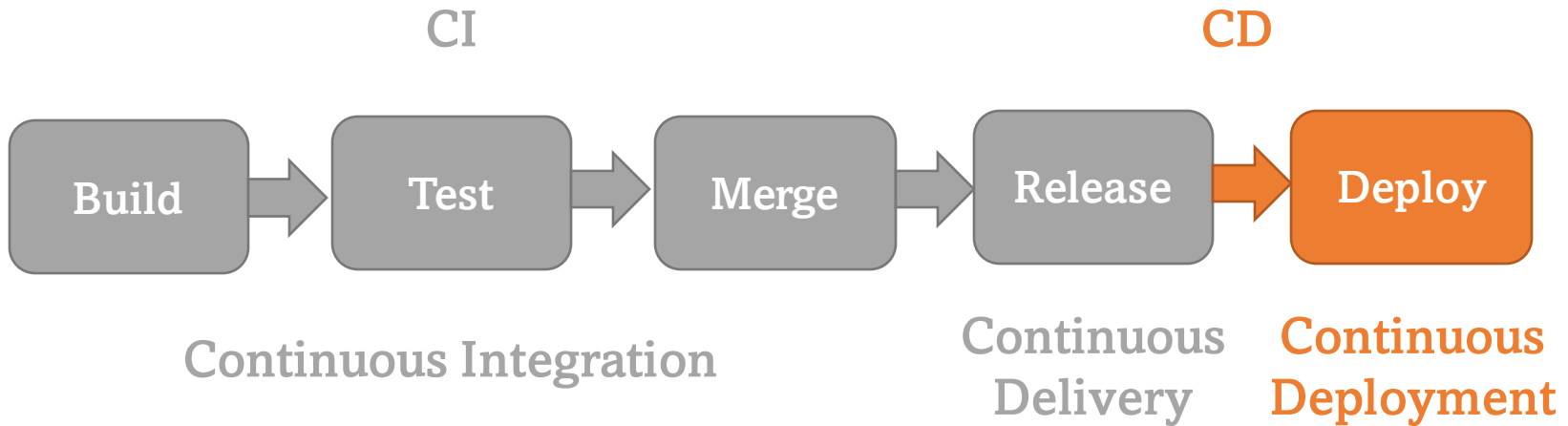
■ Static Application Security Testing (SAST)

- Quellcode auf bekannte Schwachstellen prüfen
- https://git.thm.de/help/user/application_security/sast/index

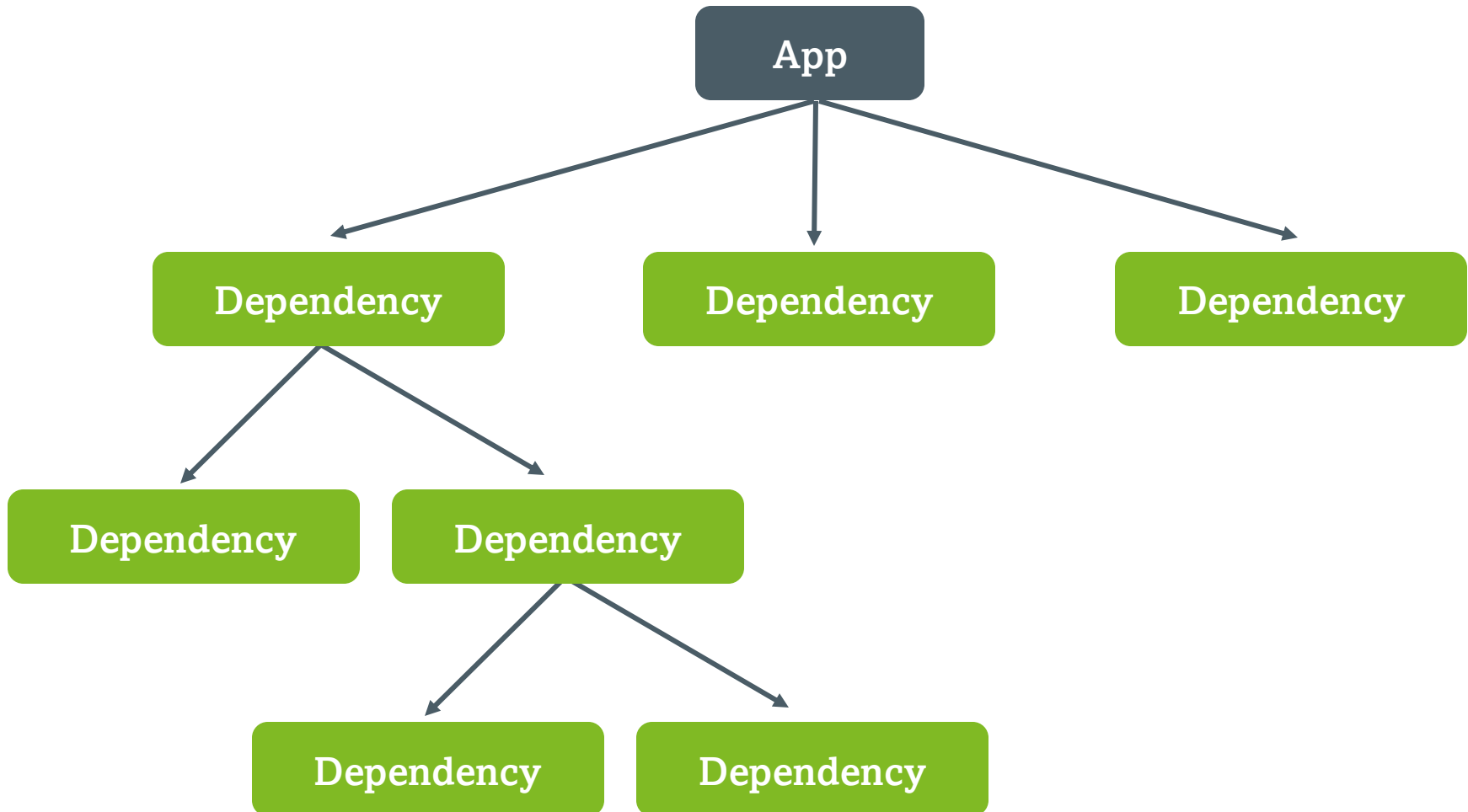
CI/CD



CI/CD



Dependencies



Dependencies - Auswahl

 Dependency überhaupt notwendig?

Dependency überhaupt notwendig?

- Funktion möglicherweise trivial?

Beispiel:

www.google.de → www.google.de



Autolinker.js



ngx-linky

Dependency überhaupt notwendig?

- Funktion möglicherweise trivial?

Beispiel:

```
1  import { Pipe, PipeTransform } from '@angular/core';
2  import Autolinker, { AutolinkerConfig } from 'autolinker';
3
4  @Pipe({ name: 'linky' })
5  export class LinkyPipe implements PipeTransform {
6      transform(value: string, options?: AutolinkerConfig): string {
7          return Autolinker.link(value, options);
8      }
9  }
```

Dependency überhaupt notwendig?

- Funktion möglicherweise trivial?

Beispiel:

www.google.de → www.google.de

 Angular



Dependency überhaupt notwendig?

- Funktion möglicherweise trivial?
- Funktion möglicherweise auch mit Standardfunktionen einfach möglich?
- Andere Dependency enthält diese Funktion bereits
- ...

Dependencies - Auswahl

 Dependency überhaupt notwendig? 

 Lizenz geeignet?

Lizenz passend?

■ Ist die Lizenz der Dependency mit der des Projektes kompatibel?



remcplasmeyer/flowy-vue is licensed under the
MIT License

A short and simple permissive license with conditions only requiring preservation of copyright and license notices. Licensed works, modifications, and larger works may be distributed under different terms and without source code.

Permissions

- ✓ Commercial use
- ✓ Modification
- ✓ Distribution
- ✓ Private use

Limitations

- ✗ Liability
- ✗ Warranty

Conditions

- ① License and copyright notice



matrix-org/matrix-js-sdk is licensed under the
Apache License 2.0

A permissive license whose main conditions require preservation of copyright and license notices. Contributors provide an express grant of patent rights. Licensed works, modifications, and larger works may be distributed under different terms and without source code.

Permissions

- ✓ Commercial use
- ✓ Modification
- ✓ Distribution
- ✓ Patent use
- ✓ Private use

Limitations

- ✗ Trademark use
- ✗ Liability
- ✗ Warranty

Conditions

- ① License and copyright notice
- ① State changes



nextcloud/server is licensed under the
GNU Affero General Public License v3.0

Permissions of this strongest copyleft license are conditioned on making available complete source code of licensed works and modifications, which include larger works using a licensed work, under the same license. Copyright and license notices must be preserved. Contributors provide an express grant of patent rights. When a modified version is used to provide a service over a network, the complete source code of the modified version must be made available.

Permissions

- ✓ Commercial use
- ✓ Modification
- ✓ Distribution
- ✓ Patent use
- ✓ Private use

Limitations

- ✗ Liability
- ✗ Warranty

Conditions

- ① License and copyright notice
- ① State changes
- ① Disclose source
- ① Network use is distribution
- ① Same license

Lizenz passend?

- Github Action zur Überprüfung der Lizenzen bei PRs:
- <https://github.com/actions/dependency-review-action>

```
# only allow MIT-licensed dependents
- name: Dependency Review
  uses: actions/dependency-review-action@v2
  with:
    allow-licenses: MIT
```

```
# Block Apache 1.1 and 2.0 licensed dependents
- name: Dependency Review
  uses: actions/dependency-review-action@v2
  with:
    deny-licenses: Apache-1.1, Apache-2.0
```


Dependencies - Auswahl

 Dependencie überhaupt notwendig? ✓

 Lizenz geeignet? ✓

 Verbreitung / Weiterentwicklung / Dokumentation

Verbreitung / Weiterentwicklung

■ Letzte Änderung (Letzter Commit)

main

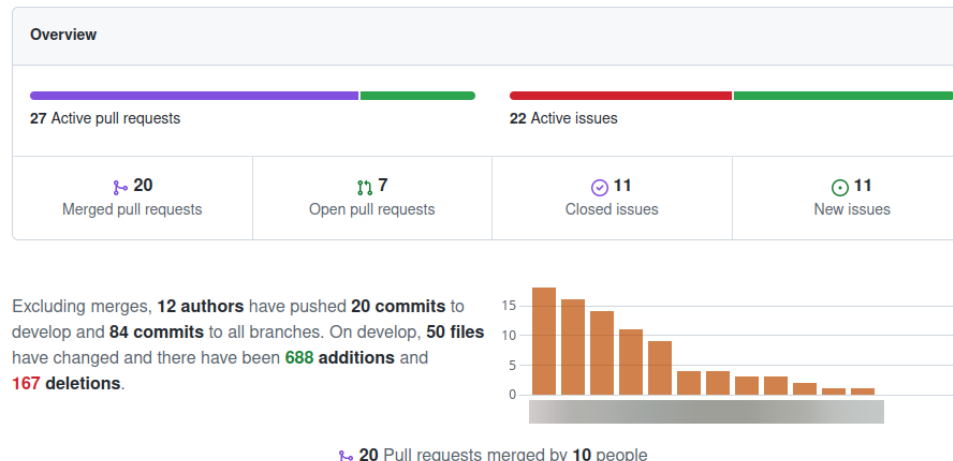
Go to file

Add file

Code

mxsph 42c2c81 3 days ago

■ Aktivitäten (Insights)



Verbreitung / Weiterentwicklung

■ Community Größe

Contributors 389



+ 378 contributors

 Issues 1.3k
  Pull requests 68

■ Downloads

↓ Weekly Downloads

649.373







Dokumentation

- Wie umfangreich ist die Dokumentation?
- Wie aktuell ist die Dokumentation?
- Enthält die Dokumentation Beispiele?
- Enthält die Dokumentation nicht nur Beispiele?

➤ **Beispiel für eine gute Dokumentation:** <https://mui.com/material-ui/getting-started/overview/>

Dependencies - Auswahl


-  Dependencie überhaupt notwendig? ✓
-  Lizenz geeignet? ✓
-  Verbreitung / Weiterentwicklung / Dokumentation ✓
-  Funktionsumfang passend?

Funktionsumfang passend?

- Enthält die Dependency möglicherweise viel mehr Funktionalität als benötigt?
- Hat die Dependency möglicherweise erwartete/unerwünschte Nebenwirkungen?
- Deckt die Dependency alle benötigten (in Zukunft benötigten) Funktionalitäten ab?

Funktionsumfang passend?

Bundlesize

- Größe der Anwendung möglicherweise wichtig (Wie z.B. bei Web-Anwendungen)
- Größere Anwendung  Längere Ladezeiten

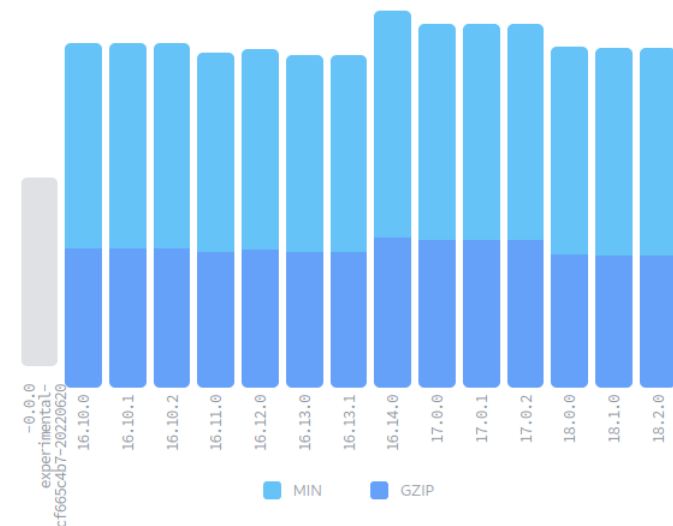
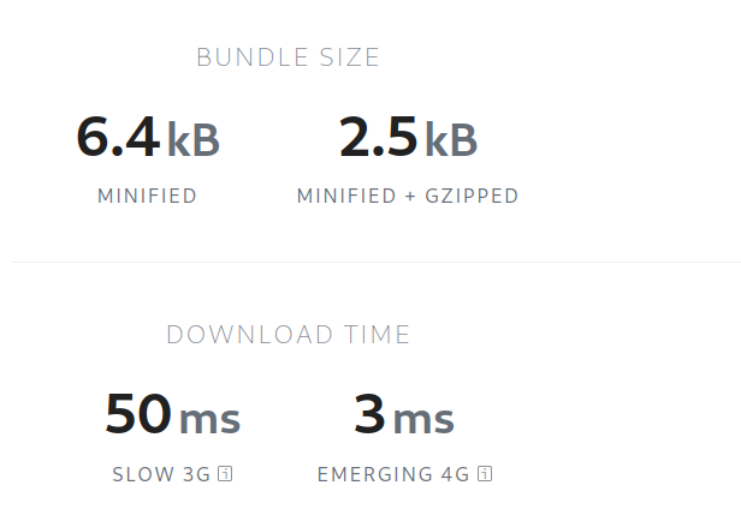
“Every 100ms delay cost [Amazon] 1% of sales”

[<https://glinden.blogspot.com/2006/12/slides-from-my-talk-at-stanford.html>, 2006]

Funktionsumfang passend?

Bundlesize Beispiele:

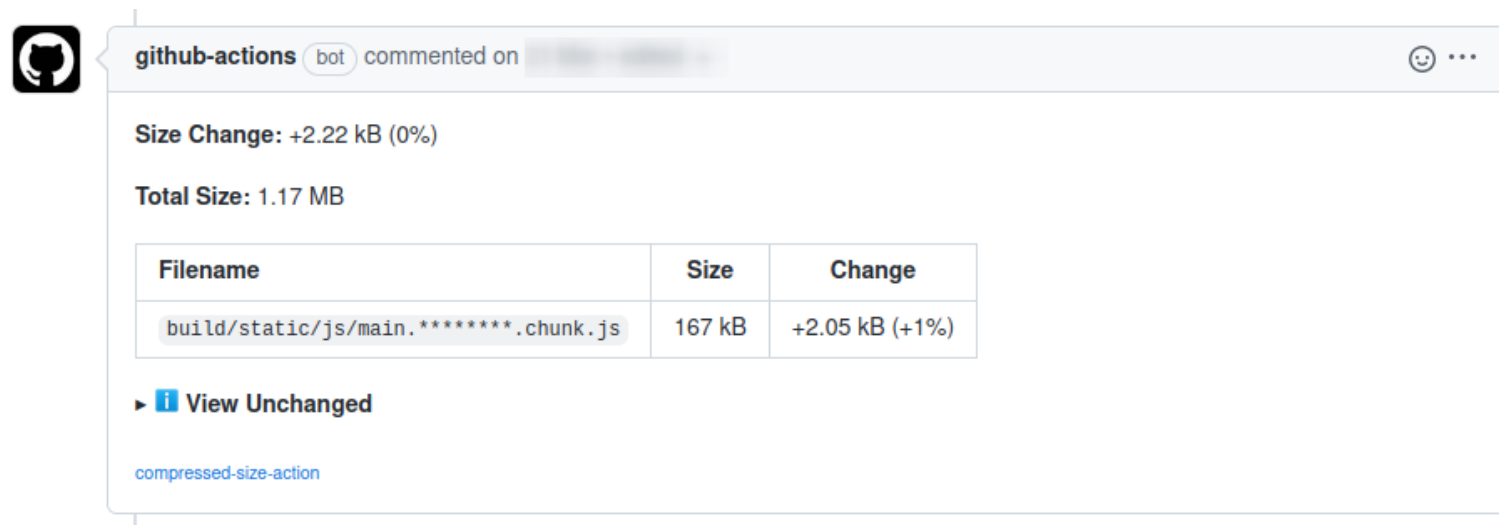
- Tool zum Überprüfen der Größe von **NPM** Dependencies: <https://bundlephobia.com/>



Funktionsumfang passend?

Bundlesize Beispiele:

- Github Action zur Überprüfung der Bundelsize bei PRs: <https://github.com/preactjs/compressed-size-action>




github-actions bot commented on [REDACTED]

Size Change: +2.22 kB (0%)






Total Size: 1.17 MB

Filename	Size	Change
build/static/js/main.*****.chunk.js	167 kB	+2.05 kB (+1%)

►  View Unchanged

[compressed-size-action](#)

Dependencies - Auswahl

-  Dependencie überhaupt notwendig? ✓
-  Lizenz geeignet? ✓
-  Verbreitung / Weiterentwicklung ✓
-  Funktionsumfang passend? ✓
-  Bekannte Fehler?

Bekannte Fehler?

- Gibt es (offene) Vulnerabilities/**CVE`s** für diese Dependency?
- Gibt es Anmerkungen in der **README** über bekannte Fehler / notwendige Sicherheitsschritte?
- Anschauen von Code abschnitten, welche Sicherheitsrelevanten Code enthalten






Bekannte Fehler?

- Github Action zur Überprüfung der Dependency bei PRs: <https://github.com/actions/dependency-review-action>

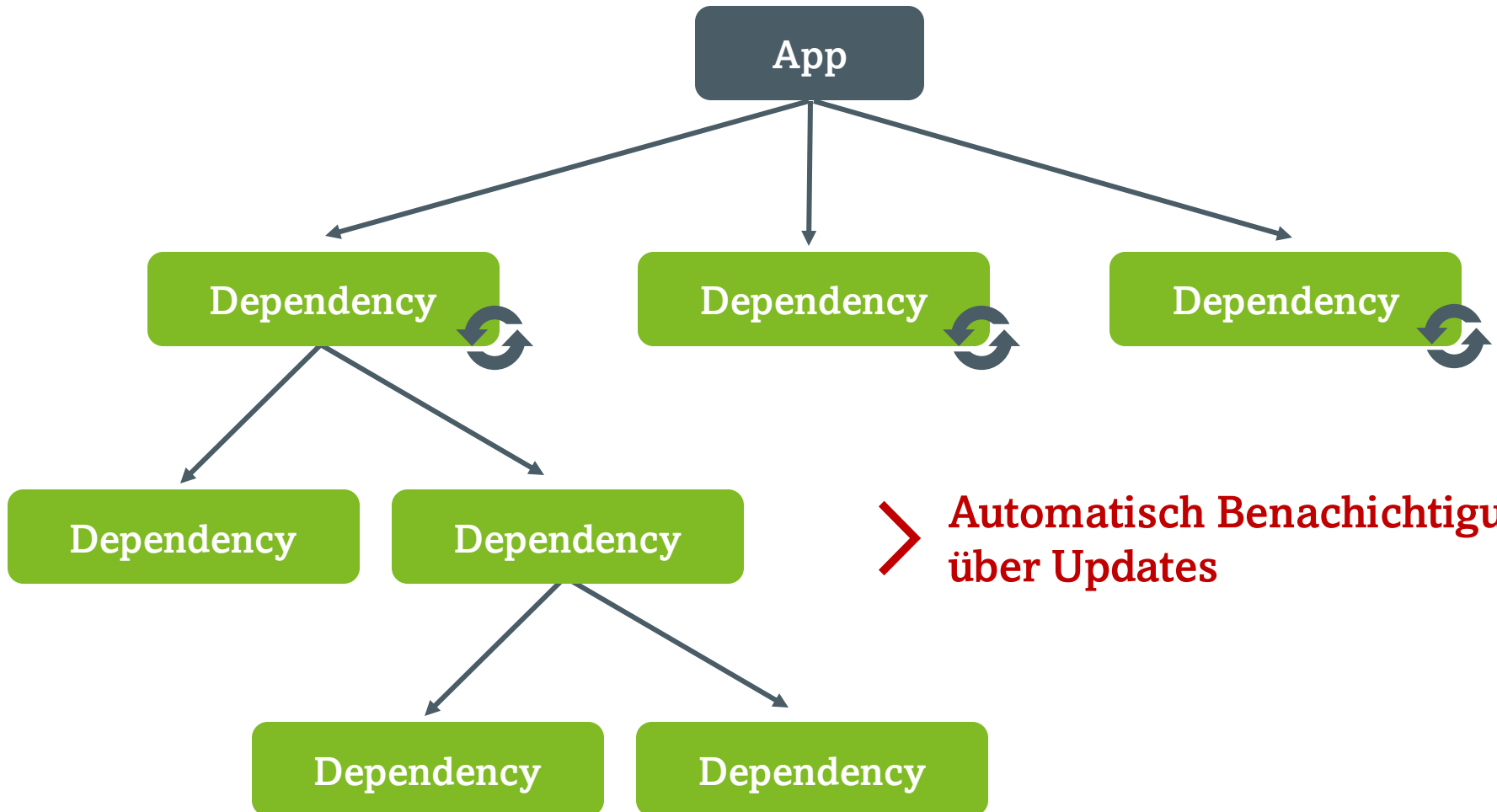
```
▼ ⓧ Dependency Review

1 ▶ Run actions/dependency-review-action@v1
4 Gemfile » activerecord@6.0.0.1 – Unintended unmarshalling in ActiveSupport (high severity)
5   ↳ https://github.com/advisories/GHSA-2p68-f74v-9wc6
6 package.json » json-schema@0.3 – json-schema is vulnerable to Prototype Pollution (moderate severity)
7   ↳ https://github.com/advisories/GHSA-896r-f27r-55mw
8 Error: Dependency review detected vulnerable packages.
```

Dependencies - Auswahl

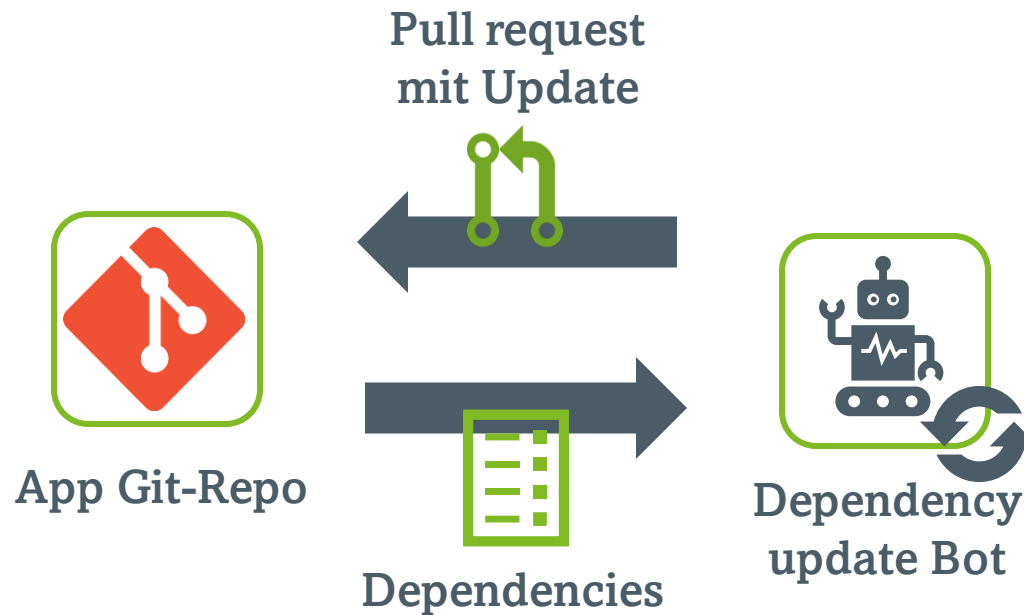
-  Dependencie überhaupt notwendig? ✓
-  Lizenz geeignet? ✓
-  Verbreitung / Weiterentwicklung ✓
-  Funktionsumfang passend? ✓
-  Bekannte Fehler? ✓

Dependencies - Updates



> **Automatisch Benachrichtigung
über Updates**



Dependencies - Updates



Dependencies - Updates


Dependabot

<https://docs.github.com/en/code-security/dependabot/working-with-dependabot>

dependabot bot commented 3 days ago Contributor  

Bumps [typescript](#) from 4.2.3 to 4.7.4.

- Release notes
- Commits

 compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.


- Dependabot commands and options

Dependencies - Updates

Renovate

<https://github.com/marketplace/renovate>


renovate
bot
commented on 6 Apr • edited





This PR contains the following updates:


Package	Update	Change
redis	minor	16.8.2 -> 16.12.3

Configuration

 **Schedule:** Branch creation - At any time (no schedule defined), Automerge - At any time (no schedule defined).

 **Automerge:** Disabled by config. Please merge this manually once you are satisfied.

 **Rebasing:** Whenever PR becomes conflicted, or you tick the rebase/retry checkbox.

 **Ignore:** Close this PR and you won't be reminded about this update again.

☐ If you want to rebase/retry this PR, click this checkbox.

This PR has been generated by [Mend Renovate](#). View repository job log [here](#).

Dependencies – Bösertige Updates

- Update enthält möglicherweise Schadcodes / Unterwünschte Funktionen
- Ursachen für solche Probleme:
 - Account des Erstellers gehackt
 - Ersteller ist unzufrieden über Stand des Projekts
- Auftretende Probleme:
 - Malware wird bei der Installation mit installiert
 - Funktionen der Dependency funktionieren nicht mehr
 - Schade Code wird bei Anwender ausgeführt

CWEs

- **Common Weakness Enumeration** ist eine von der Gemeinschaft entwickelte Liste von Software- und Hardware-Schwachstellen
 - Katalogisieren von Schwachstellen
 - mehr als 600 Kategorien
 - <https://cwe.mitre.org/data/>

Beispiel: CWE-804: Guessable CAPTCHA

CVE

- **Common Vulnerabilities and Exposures**
 - Liste der derzeit bekannten Probleme in Bezug auf bestimmte Systeme und Produkte
 - <https://www.cve.org/>
 - Einträge in der Liste wird als **CVE Record** bezeichnet

CVE



CVE Program participant

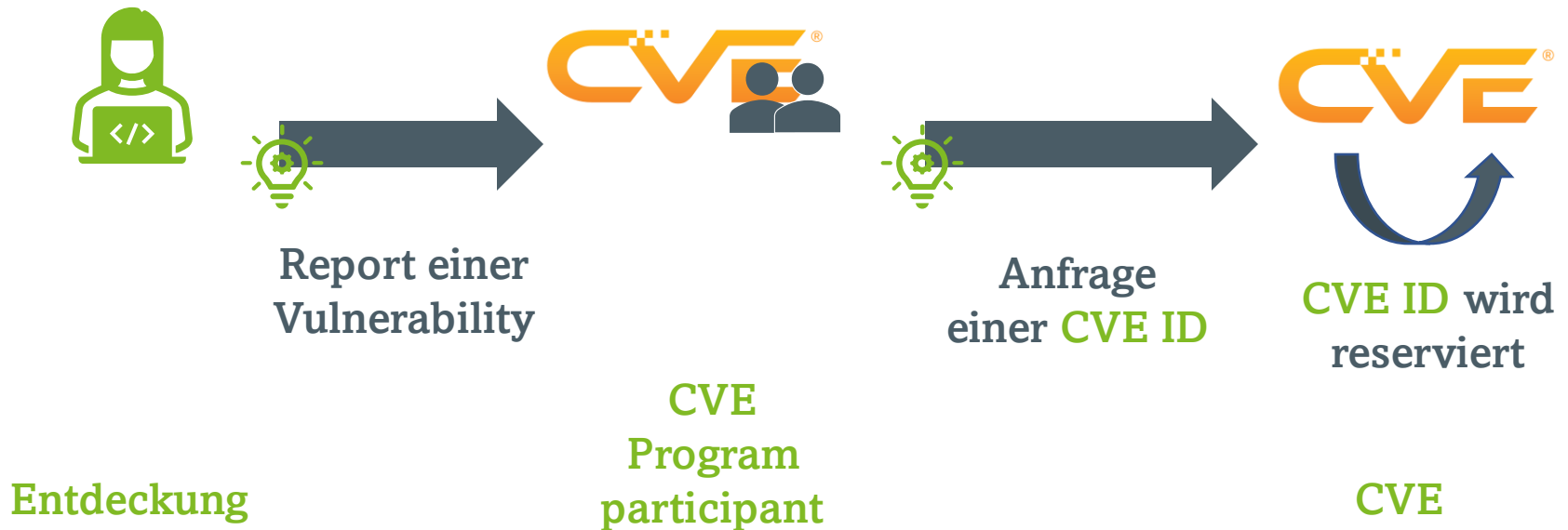
Program Roles

- CVE Numbering Authority (CNA)
- CVE Numbering Authority of Last Resort (CNA-LR)
- Root
- Top-Level Root (TL-Root)

Organization Types

- Bug Bounty Programs
- Hosted Services
- National and Industry CERTs
- Vendors and Projects
- Vulnerability Researcher(s)

CVE



CVE ID

- Eindeutige ID welche von CVE Programm zugewiesen wird
- Jede ID referenziert eine Vulnerability

CVE-2017-7474

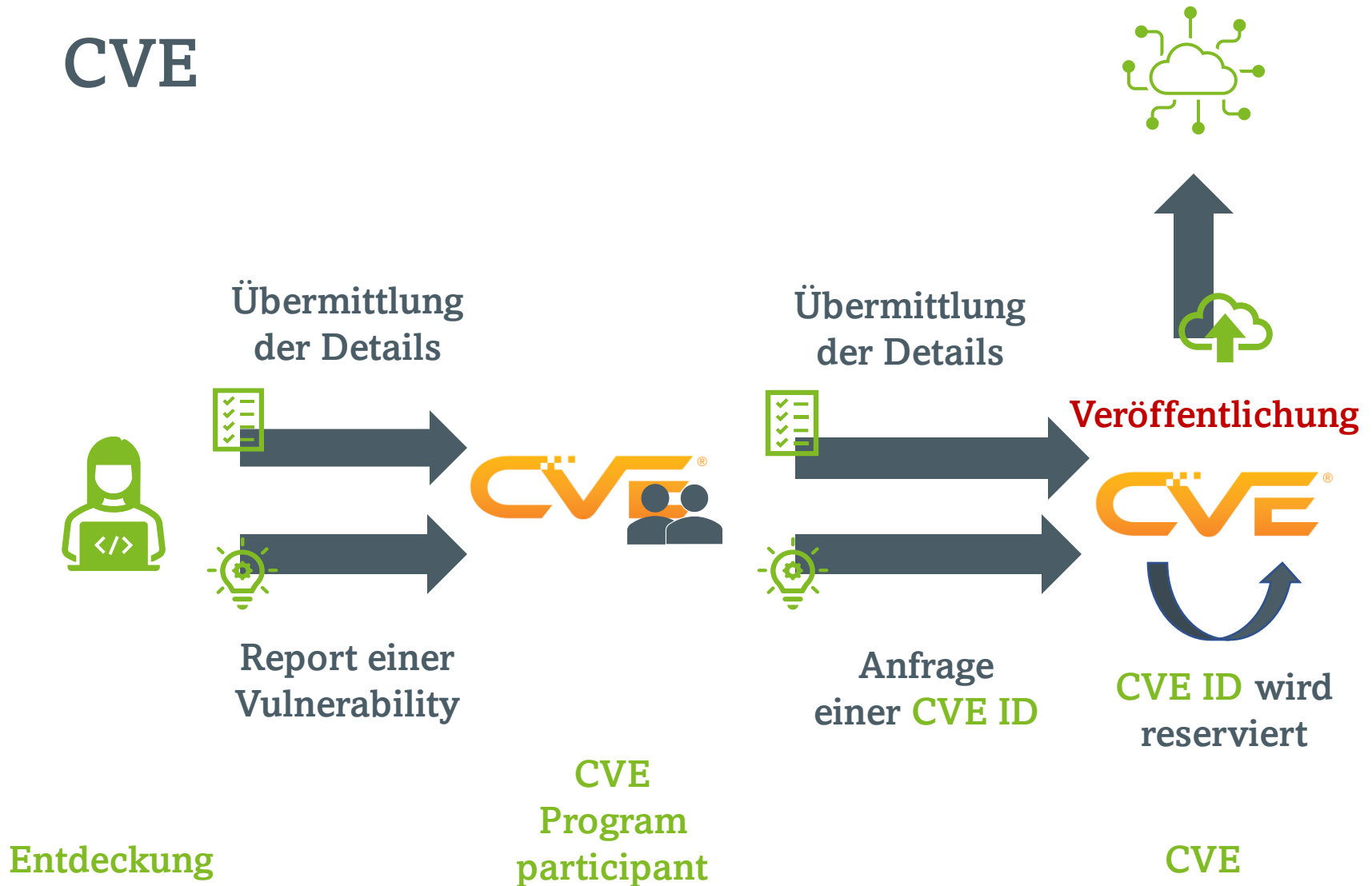
CVE Prefix

Arbitrary Digits

vier oder mehr Ziffern

Jahr der Reservierung /
Veröffentlichung

CVE



CVE Record

- Beschreibung einer Schwachstelle mit einer CVE-ID
- Wird von einer CNA bereitgestellt
- Wird in verschiedenen für Menschen und Maschinen lesbaren Formaten bereitgestellt.

CVE Record - Inhalt

- Name des betroffenen Produkts
- betroffene oder korrigierte Version(en)
- CVE ID
- Mindestens eine der folgenden Punkte:
 - Vulnerability Type
 - Ursache
 - Auswirkung
- Öffentliche Referenz
- Beschreibung
- (Angabe ob das betroffene Produkt noch unterstützt wird)

CVE Record


[GitHub Advisory Database](#) / [GitHub Reviewed](#) / CVE-2013-7452

Moderate severity vulnerability that affects validator

Moderate severity [GitHub Reviewed](#) Published on 24 Oct 2017 • Updated on 17 Sep 2021

Vulnerability details Dependabot alerts **0**

Package

 **validator** (npm)

Affected versions

< 1.1.0

Patched versions

1.1.0

Severity

Moderate6.1 / 10

Description

The validator module before 1.1.0 for Node.js allows remote attackers to bypass the cross-site scripting (XSS) filter via a crafted javascript URI.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2013-7452>
- [GHSA-rh6c-q938-3r9q](#)

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Changed
Confidentiality	Low
Integrity	Low
Availability	None

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

GitHub Advisory Database

- <https://github.com/advisories>

GitHub Advisory Database

Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.

GitHub reviewed advisories

All reviewed 7,756

Composer	940
Go	530
Maven	1,472
npm	2,517
NuGet	193
pip	1,171
RubyGems	493
Rust	486

Unreviewed advisories

All unreviewed 171,106

 CC-BY-4.0 License

Q Search by CVE/GHSA ID, package, severity, ecosystem, credit...

7,756 advisories

Severity ▾ CWE ▾ Sort ▾

Improper handling of CSS at-rules in lettersanitizer High

CVE-2022-31103 was published for lettersanitizer (npm) 14 hours ago

Weave GitOps leaked cluster credentials into logs on connection errors Critical

CVE-2022-31098 was published for github.com/weaveworks/weave-gitops (Go) 14 hours ago

Denial of Service (DoS) vulnerability in RSSHub High

GHSA-jvxx-v45p-v5vf was published for rsshub (npm) yesterday

Cross-site Scripting in Microweber Moderate

CVE-2022-2174 was published for microweber/microweber (Composer) yesterday

Log Injection in Apache Sling Commons Log and Apache Sling API High

CVE-2022-32549 was published for org.apache.sling:org.apache.sling.api (Maven) yesterday

Server-Side Request Forgery in Directus Moderate

CVE-2022-23080 was published for directus (npm) yesterday

Unsafe yaml deserialization in NVFlare Critical

CVE-2022-31605 was published for nvflare (pip) yesterday

CVE Benachrichtigung



Gitlab:

[https://gitlab.com/dependabot-
gitlab/dependabot#vulnerability-alerts](https://gitlab.com/dependabot-gitlab/dependabot#vulnerability-alerts)



Github:

[https://docs.github.com/en/code-
security/dependabot/dependabot-alerts/about-
dependabot-alerts](https://docs.github.com/en/code-security/dependabot/dependabot-alerts/about-dependabot-alerts)

CVE Benachrichtigung

Github

Actions Projects Security Insights Settings

Overview Reporting Policy Advisories 1 Vulnerability alerts Dependabot Code scanning Secret scanning

Dependabot alerts

is:open

Open 4 Closed Closed as Package Ecosystem Manifest Severity Sort

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Prototype Pollution in async High	closed as fixed 16 days ago • Detected in async (npm) •
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Exposure of Sensitive Information in eventsource Critical	closed as fixed 16 days ago • Detected in eventsource (npm) •
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inefficient Regular Expression Complexity in chalk/ansi-regex High	closed as fixed 16 days ago • Detected in ansi-regex (npm) •
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorization Bypass Through User-Controlled Key in url-parse Critical	closed as fixed 4 months ago • Detected in url-parse (npm) •

CVE Benachrichtigung

Github

Code security and analysis

Security and analysis features help keep your repository secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your repository.

Dependency graph

Understand your dependencies.

Disable

Dependabot

Keep your dependencies secure and up-to-date. [Learn more about Dependabot.](#)

Dependabot alerts

Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications.](#)

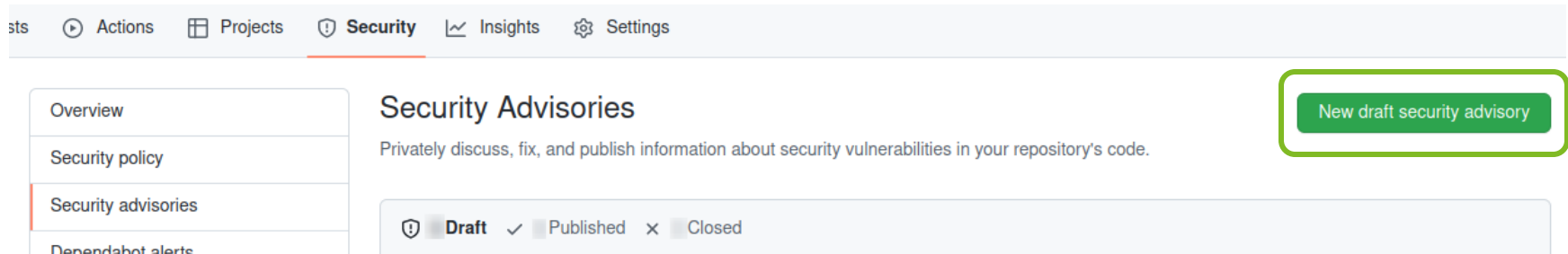
Disable

Dependabot security updates

Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.

Disable

CVE Erstellen - Github



The screenshot shows the GitHub interface for creating a security advisory. At the top, a navigation bar includes links for 'Issues', 'Actions', 'Projects', 'Security' (which is highlighted with a red underline), 'Insights', and 'Settings'. On the left side, a sidebar menu lists 'Overview', 'Security policy', 'Security advisories' (which is highlighted with a red border), and 'Dependabot alerts'. The main content area is titled 'Security Advisories' and includes a subtitle: 'Privately discuss, fix, and publish information about security vulnerabilities in your repository's code.' In the top right corner of this section, there is a green button labeled 'New draft security advisory' which is highlighted with a green rounded rectangle. Below the title, there is a filter bar with three options: 'Draft' (selected with a radio button), 'Published' (with a radio button), and 'Closed' (with a radio button).

CVE Erstellen - Github

Affected product

Ecosystem

Select an ecosystem

Package name

e.g. example.js

Affected versions

e.g. < 1.2.3

Patched versions

e.g. 1.2.3

+ Add another affected product

Severity

Assess severity using CVSS

Vector string

CVSS:3.1/AV:_/AC:_/PR:_/UI:_/S:_/C:_/I:_/A:_

Score

Pending selection

Calculator
[Learn more about CVSS scoring](#)

Attack vector

Network
Adjacent
Local
Physical

Attack complexity

Low
High

Privileges required

None
Low
High

User interaction

None
Required

Scope

Unchanged
Changed

Confidentiality

None
Low
High

Integrity

None
Low
High

Availability

None
Low
High

CVE Erstellen - Github

Affected product

Ecosystem
 Select an ecosystem

Package name
 e.g. example.js

Affected versions
 e.g. < 1.2.3

Patched versions
 e.g. 1.2.3

[+ Add another affected product](#)

Severity
 Assess severity using CVSS

Vector string
 CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/L:I/H:A:H

Score
high 8.2

Calculator
[Learn more about CVSS scoring](#)

Attack vector
 Network Adjacent Local Physical

Attack complexity
 Low High

Privileges required
 None Low High

User interaction
 None Required

Scope
 Unchanged Changed

Confidentiality
 None Low High

Integrity
 None Low High

Availability
 None Low High

CVE Erstellen - Github

Affected product

Ecosystem

Select an ecosystem

Package name

e.g. example.js

Affected versions

e.g. < 1.2.3

Patched versions

e.g. 1.2.3

+ Add another affected product

Severity

Assess severity using CVSS

CVSS: <https://www.first.org/cvss/v3.1/user-guide>

Calculator

Learn more about CVSS scoring

Attack vector

Network Adjacent Local Physical

Attack complexity

Low High

Privileges required

None Low High

User interaction

None Required

Scope

Unchanged Changed

Confidentiality

None Low High

Integrity

None Low High

Availability

None Low High

CVE Erstellen - Github

Common weakness enumerator (CWE)

Search by CWE

CVE identifier

Request CVE ID later

Title

Description

Write
 Preview
 H B I ≡ <> 🔗 ≡ ≡ ☑ ↶

Impact
 What kind of vulnerability is it? Who is impacted?

Patches
 Has the problem been patched? What versions should users upgrade to?

Workarounds
 Is there a way for users to fix or remediate the vulnerability without upgrading?

Attach files by dragging & dropping, selecting or pasting them.

Create draft security advisory

CVE Erstellen - Github

Common weakness enumerator (CWE)

Q Search by CWE








CVE identifier

Request CVE ID later

Anleitung: <https://docs.github.com/en/code-security/repository-security-advisories/publishing-a-repository-security-advisory>

Description

Write Preview

H B I       

Impact
What kind of vulnerability is it? Who is impacted?

Patches
Has the problem been patched? What versions should users upgrade to?

Workarounds
Is there a way for users to fix or remediate the vulnerability without upgrading?

Attach files by dragging & dropping, selecting or pasting them.

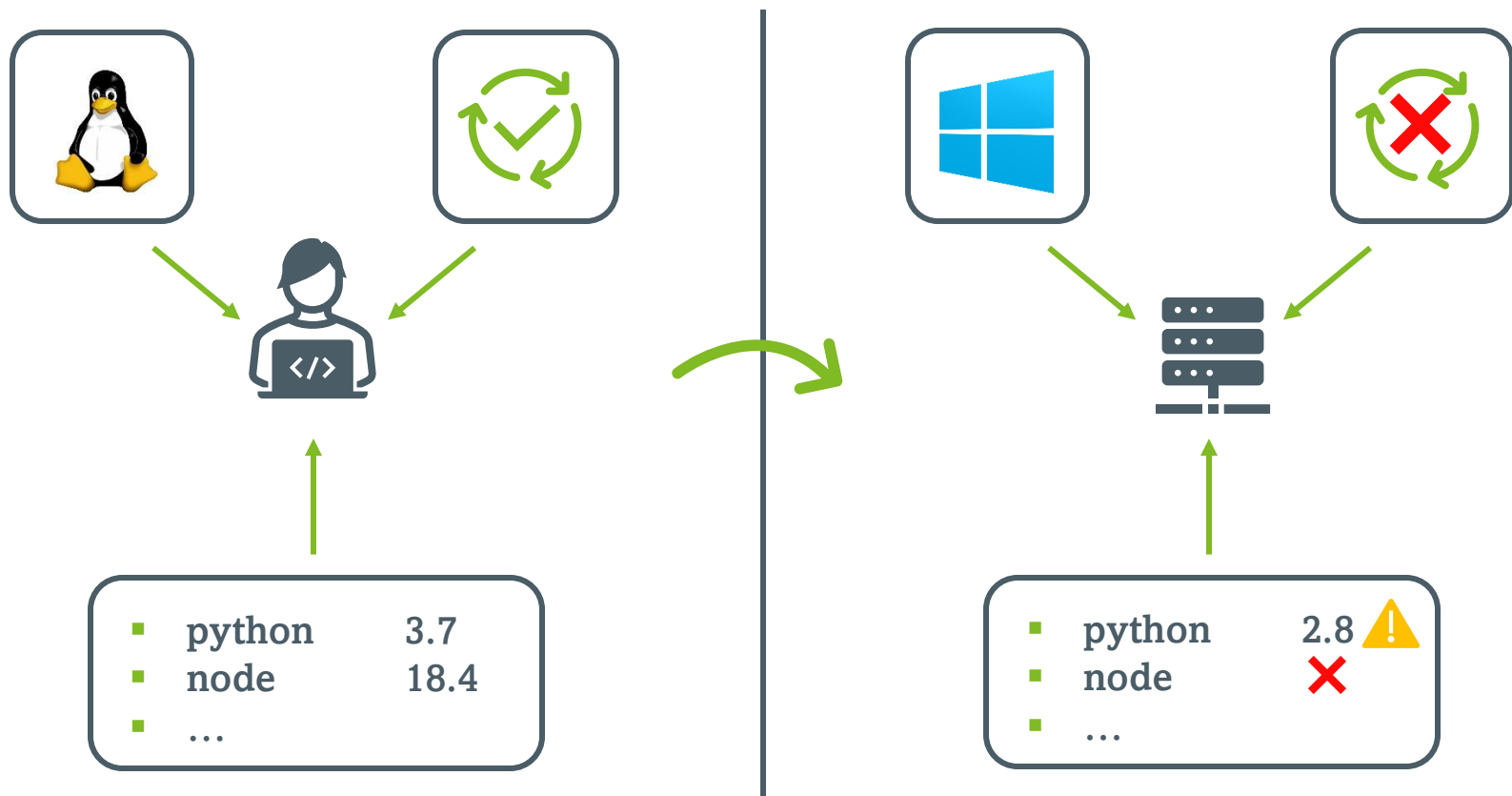
Create draft security advisory

Virtualisierung

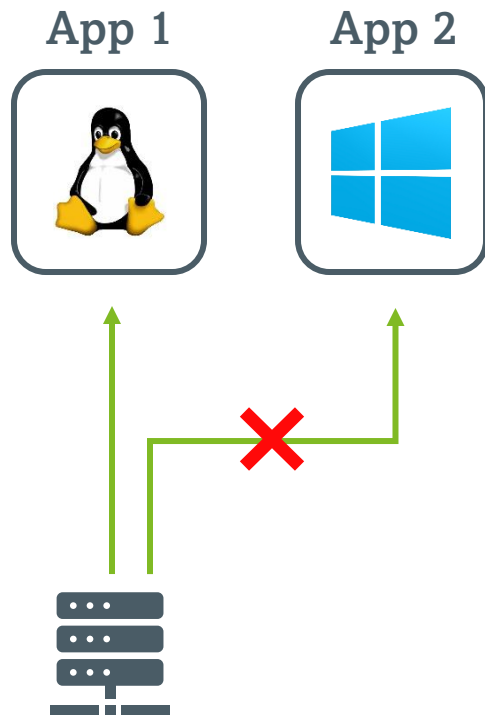


Warum Virtualisierung?

🕒 Früher

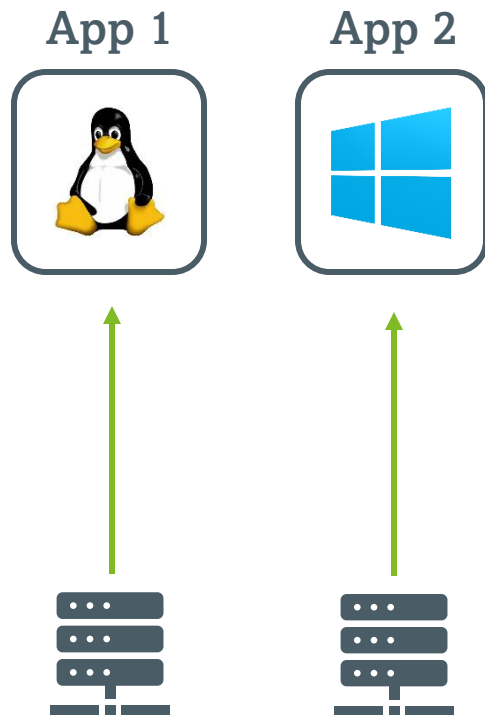


Warum Virtualisierung?



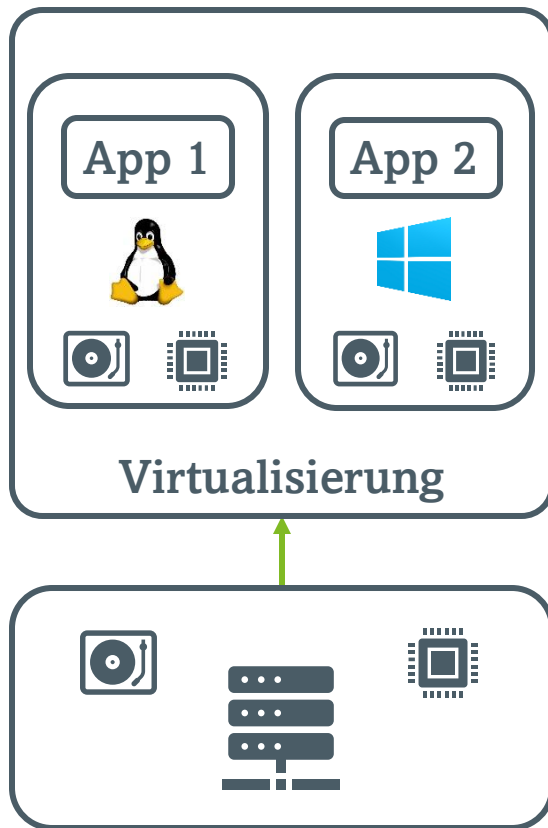
- Mehrere Anwendungen mit verschiedenen Voraussetzungen
- **Auf einem Server kann nur ein Betriebssystem laufen**

Warum Virtualisierung?



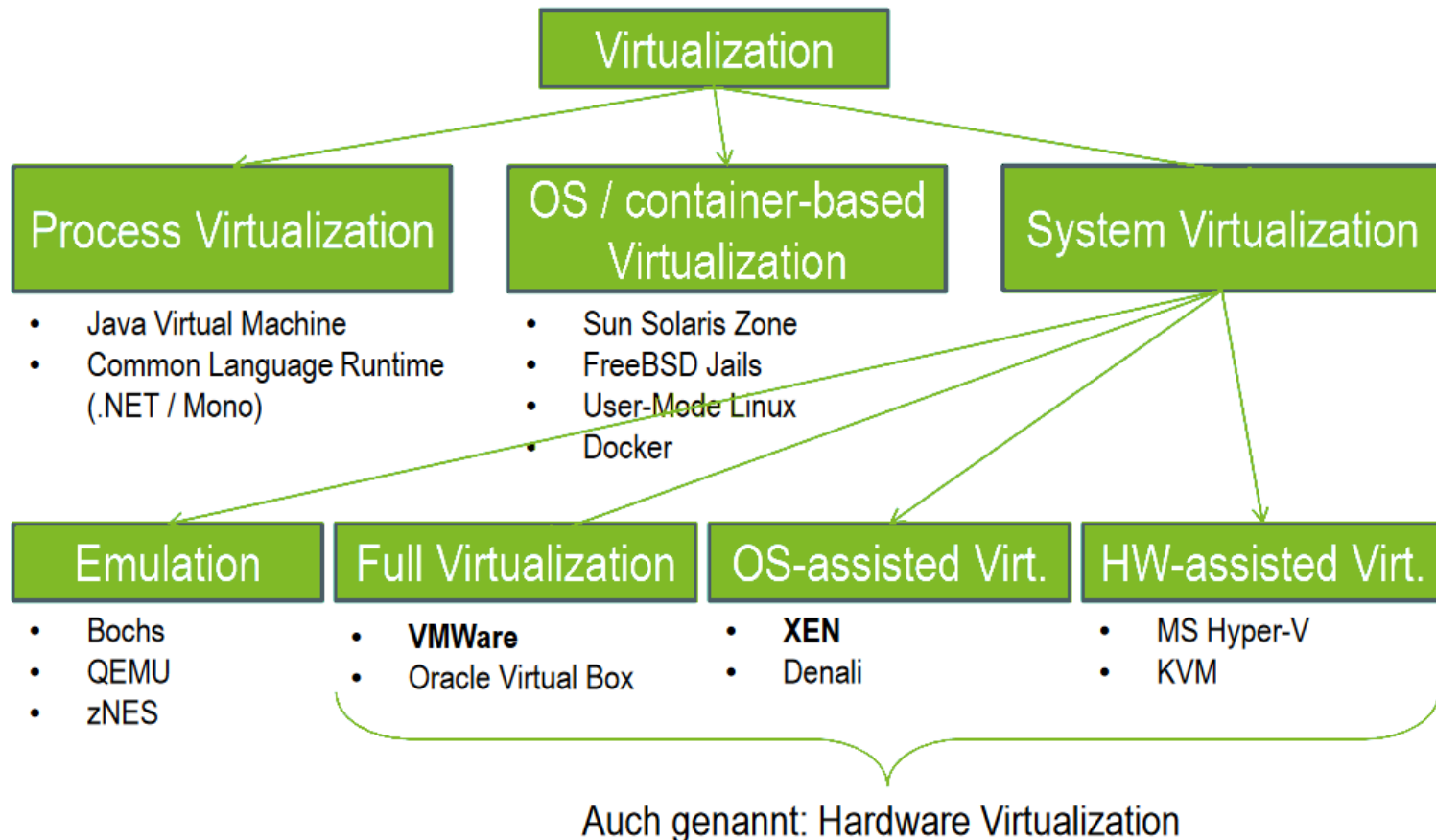
- Mehrere Anwendungen mit verschiedenen Voraussetzungen
- **Auf einem Server kann nur ein Betriebssystem laufen**
- **Es benötigt mehrere Server, die nur wenig ausgelastet sind**

Virtualisierung

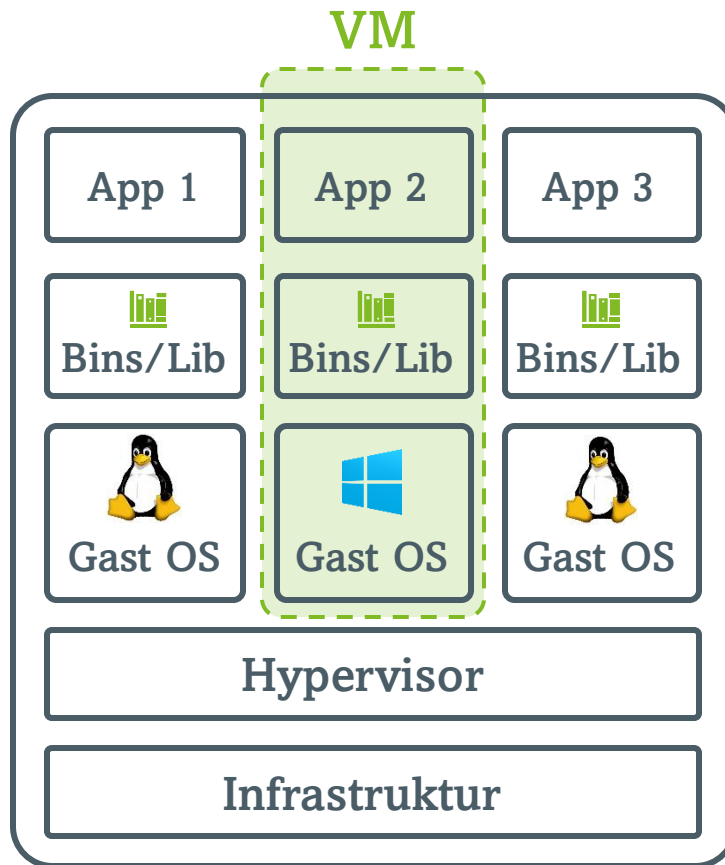


- Z.B. Linux und Windows auf einem Rechner
- bessere Auslastung der Hardware
- Isolation des Gast-Betriebssystems und damit mehr Sicherheit
- Gast-Betriebssysteme lassen sich leicht klonen
- Test neuer, modifizierter oder fremder Software
- Bei Inkompatibilität älterer Software mit neuer Hardware, kann die Software auf einem entsprechenden virtuellen PC betrieben werden

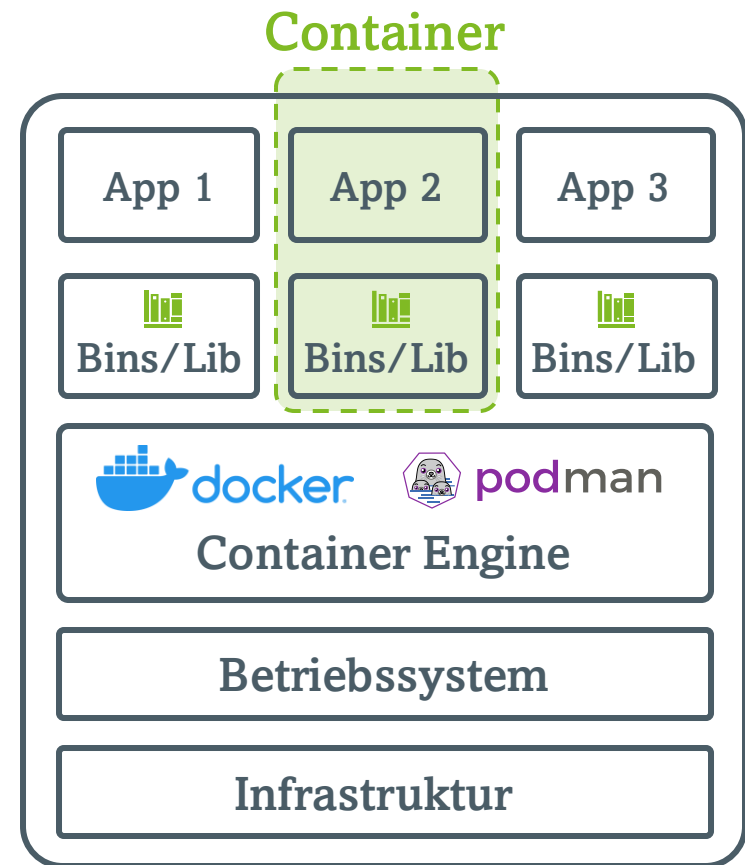
Arten der Virtualisierung



Container



VMs



Containers

Container

- Relativ kleines, eigenständiges, ausführbares Softwarepaket, das alles enthält, was zum Ausführen benötigt wird:
 - Code, Systemtools, Systembibliotheken und Einstellungen
- Nutzen Betriebssystem des Hosts sowie ein Abbild von dessen Dateien (z.B. durch Nutzung von UnionFS)
 - Benötigen weniger Rechen- und Arbeitsspeicher
 - minimiert Plattenauslastung, Zugriff ist schneller
- Für Linux- und Windows-basierte Apps verfügbar
- Unabhängig von der Umgebung immer gleich ausgeführt

Container

- Container **isolieren Software von ihrer Umgebung**
 - Isolation und Limitierung von Ressourcennutzung (CPU, RAM, I/O, ...)
- Container **Reduzieren Konflikte**
 - Unterschiede zwischen Entwicklungs- und Staging-Umgebung Software auf unterschiedlichen Infrastrukturen ausführen
- Bekannteste Container-Software





Docker

- Freie Containervisualisierungs-Software
- Im März 2013 von dotCloud veröffentlicht
- Ausgerichtet auf die Virtualisierung mit Linux
 - mittels Hyper-V oder VirtualBox auf Windows
- Docker in Zahlen

318 Mrd.

Total Pulls on Hub

8.3 Mio.

Hub Repositories

7.3 Mio.

Docker Accounts

3.3 Mio.

Desktop Installations

(Docker) Container - Definition

Image

- Blaupause für das Starten eines Containers
- Dateisystem-Abbild eines Betriebssystems inklusive Anwendungen und Konfigurationsdateien

(Docker) Container - Dockerfile

- Docker erstellt ein Image aus einer Dockerfile
 - `docker build`
- Beispiel:

```
FROM ubuntu:20.04
```

Spezifiziert das Parent-Image

```
COPY ./app
```

Kopiert die Dateien in den Container

```
WORKDIR /app
```

Setzt den das working-directory für RUN, CMD etc.

```
ENV EXAMPLE_ENV=true
```

Setzt eine Enviroment Variable

```
RUN npm install
```

```
RUN apt-get update && ... python3.8
```

Führt das Kommando in der shell aus

(Docker) Container - Dockerfile

- Docker erstellt ein Image aus einer Dockerfile
 - `docker build`
- Beispiel:

...

CMD python3 main.py

ENTRYPOINT python3 main.py

Befehl, welcher beim Starten ausgeführt wird

(Docker) Container - Definition

Volume

- Im Container geänderte Dateien werden in einem Dateisystem-Layer über dem Image gespeichert.
 - Gehen verloren, wenn der Container gelöscht wird!
- Volumes werden benötigt, um persistent Daten zu halten.
- Volumes können für Ordner innerhalb eines Containers eingerichtet werden.

Container

- Wie erfolgt die Trennung ?
- **Namespaces**: Virtuelle Namen für
 - Prozess Ids, User Ids, Mount Points, Netzwerk, Hostname, ...
- **CGroups**: Isolation und Limitierung von
 - CPU, RAM/Hugepages, Festplatten I/O, Netzwerk, ...
- **UnionFS**:
 - Gespiegeltes Dateisystem

Docker Compose

- Container-Orchestrierungs-System
- Erstellen und Verwalten von Containern automatisieren
- Verwalten von verwendeten Ressourcen wie Volumes und Netzwerke
- Definiert in einer YAML-Datei

Docker Compose YAML-Datei

```
version: "3"

services:
  db:
    image: postgres:13-alpine
    restart: always
    environment:
      POSTGRES_PASSWORD: root

  app:
    build: ./src
    restart: always
    ports:
      - 8080:8080
    volumes:
      - ./src/local/folder:/home/container/folder
```

Container Sicherheit

- **Sind Container sicher?**
- Es gibt Personen, die glauben: Container sind von Natur aus sicherer als VMs
 - Zugriffe und Schnittstellen eng begrenzt → Angriffsfläche insgesamt reduziert
 - VM mit eigenem Betriebssystem muss gewartet werden und bietet jede Menge Angriffsfläche.

Container Sicherheit

- **Sind Container sicher?**
 - **Aber!** Container haben gegenüber VMs Risiken bzgl. des offenen Netzwerkverkehrs und einen gemeinsam genutzten Linux-Kernel. Deshalb ist es wichtig:
 - Mikrosegmentierung des internen Netzwerkes vorzunehmen
 - Host- und Container-Versionen aktuell zu halten
 - <https://docs.docker.com/engine/security/security>
 - https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html#docker-security-cheat-sheet
- **Alternative:** Container von gleicher Sicherheitsrelevanz und zur Segmentierung ggf. auf virtuelle Maschinen aufteilen.

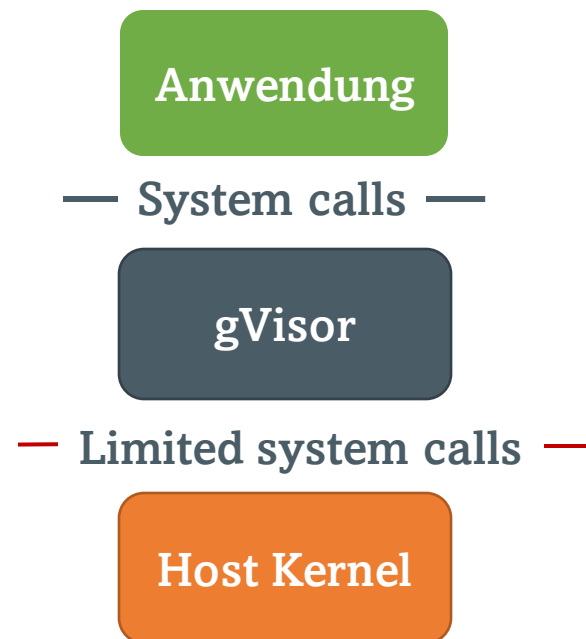
Sandbox (spezieller Container)

- Isolierter Container von der Systemumgebung abgeschottet.
- Software lässt sich innerhalb geschützt ausführen
- Beispiele:
 - Browser: Ausführen von JavaScript-Code
 - Testen von Software

Sandbox (spezieller Container)

- gVisor um Docker Container als Sandbox auszuführen

```
docker run --rm --runtime=runsc hello-world
```



 <https://gvisor.dev>

Sandbox (spezieller Container)

- HTML5 erlaubt Sandboxes:

```
<iframe src="untrusted.html" sandbox>...</iframe>
```

Nicht mehr möglich:

- Plugins instanziiieren
- Skripte ausführen
- Popup-Fenster öffnen
- Formulare absenden
- XMLHttpRequests verschicken
- Plattenzugriff (HTML5 LocalStorage, SessionStorage, Cookies, ...)
- Zugriff auf die DOM des Parent Fensters
- Benutzung von HTML Components (HTCs)

