From Compliance to Code

the Cyber Resilience Act (CRA), SBOMs, DevTeams and YOU

Version: 1.4.1

Marcus Ross, Peter Dickten

Agenda

- CRA - why it matters
- SBOMs and your team
- Checklist & Learnings

This presentation is not a substitute for professional legal advice

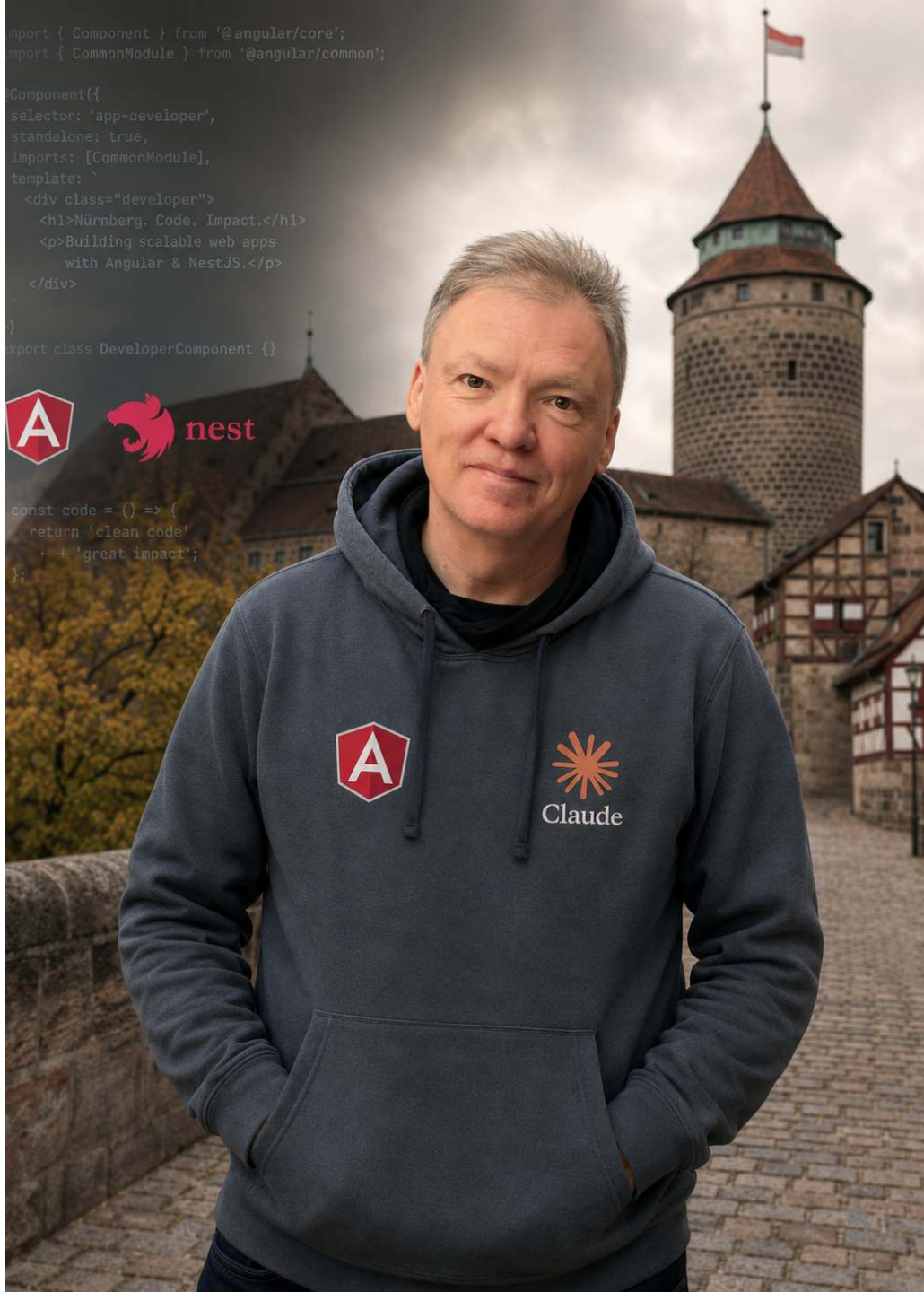
About me

```yaml
apiVersion: v1
kind: Human
metadata:
  name: "Marcus Ross"
  namespace: "Hamburg"
spec:
  hobbies: ['triathlon','movies','3dprint']
  job: "CCoE Lead"
  employer: "Hamburg Port Authority"
  certifications:
  - Kubestronaut / Cert. Ethical Hacker
  - ISO-27001 cert. / ITIL-Expert
  - AWS-Champion / Cert. STACKIT Engineer
  social:
    linkedIn: linkedin.com/in/zahlenhelfer
    github: zahlenhelfer.github.com
```

About me

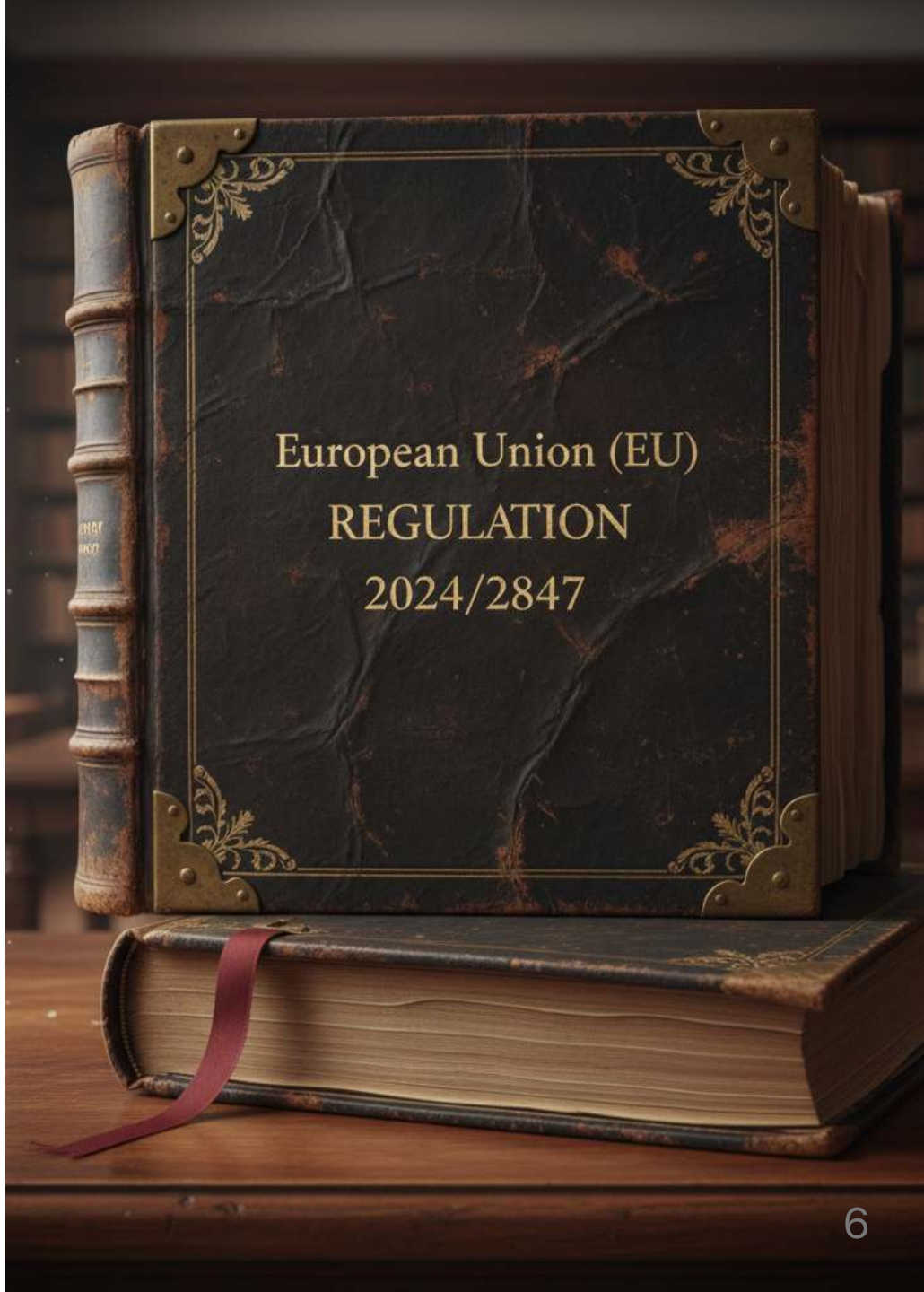
Peter Dickten

```yaml
apiVersion: v1
kind: Human
metadata:
  name: "Peter Dickten"
  namespace: "Nuremberg"
spec:
  hobbies: ['coding','cycling']
  job: "founder and CTO"
  employer: "dcs-fuerth (germany)"
  certifications:
  - Scrum / Prince2
  - Java / Anthropic (AI)
  social:
    linkedIn: linkedin.com/in/peter-dickten/
    github: github.com/dcsfuerth/
```



The Cyber Resilience Act

- a fancy term for "EU regulation 2024/2847"
- a document with
  - 130 recitals (justifications)
  - 71 articles
  - 8 annexes
  - with over 52,000 words



CRA Scope

Source: Art. 1-3

general requirements:

- Applies to "product with digital elements" (PDE)
- If made available on the EU market
- Risk management, design, development, and production of PDEs for cybersecurity

CRA-Timeline

Source: Art. 1, 71

- Into force: 10th Dec. 2024
- Key provisions: June 2026
- Vul. Reporting: 11th Sept 2026
- Full Compliance: **11th Dec 2027**

What is a PDE?

Source: Art. 3(1)

> “Any software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.”"

CRA - Which Digital Products are Excluded?

Source: Art. 2

- Non-commercial
- websites or services without a product
- specialty cases with their own regulations
  - medical products / in-vitro diagnostica
  - vehicles
  - civil aviation & marine equipment

CRA & OpenSource Software

Sources: Recital 10 & OSSF-Talk:CRA-Ready

Checklist if CRA Applies

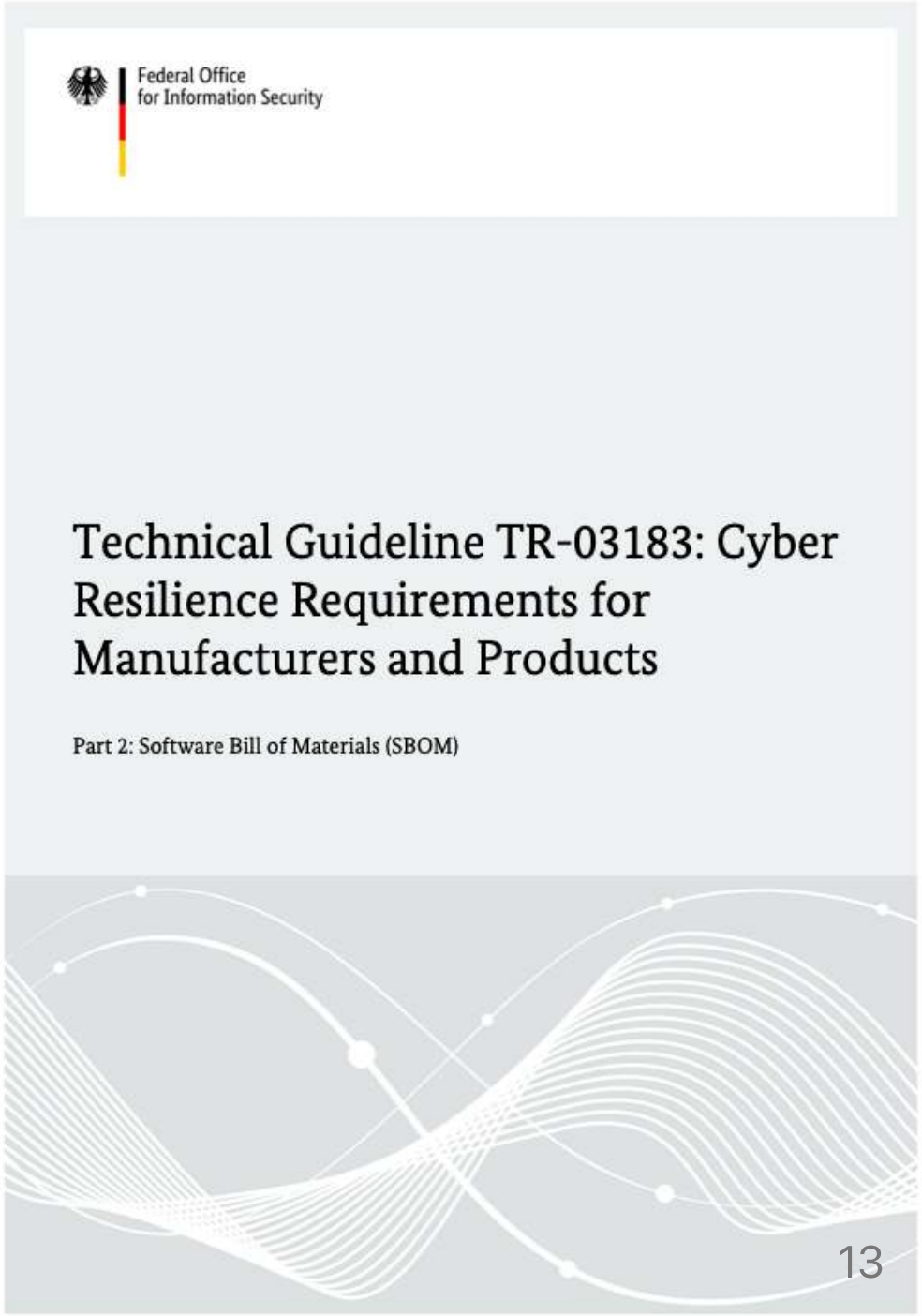
Source: BSI

- entered EU market at the end of 2027
- not part of excluded sector of CRA
- is not a free of charge open source software (making profit)
- uses digital elements
- has a data connection (common!)
- or is software

CRA, (SBOMs) and your team

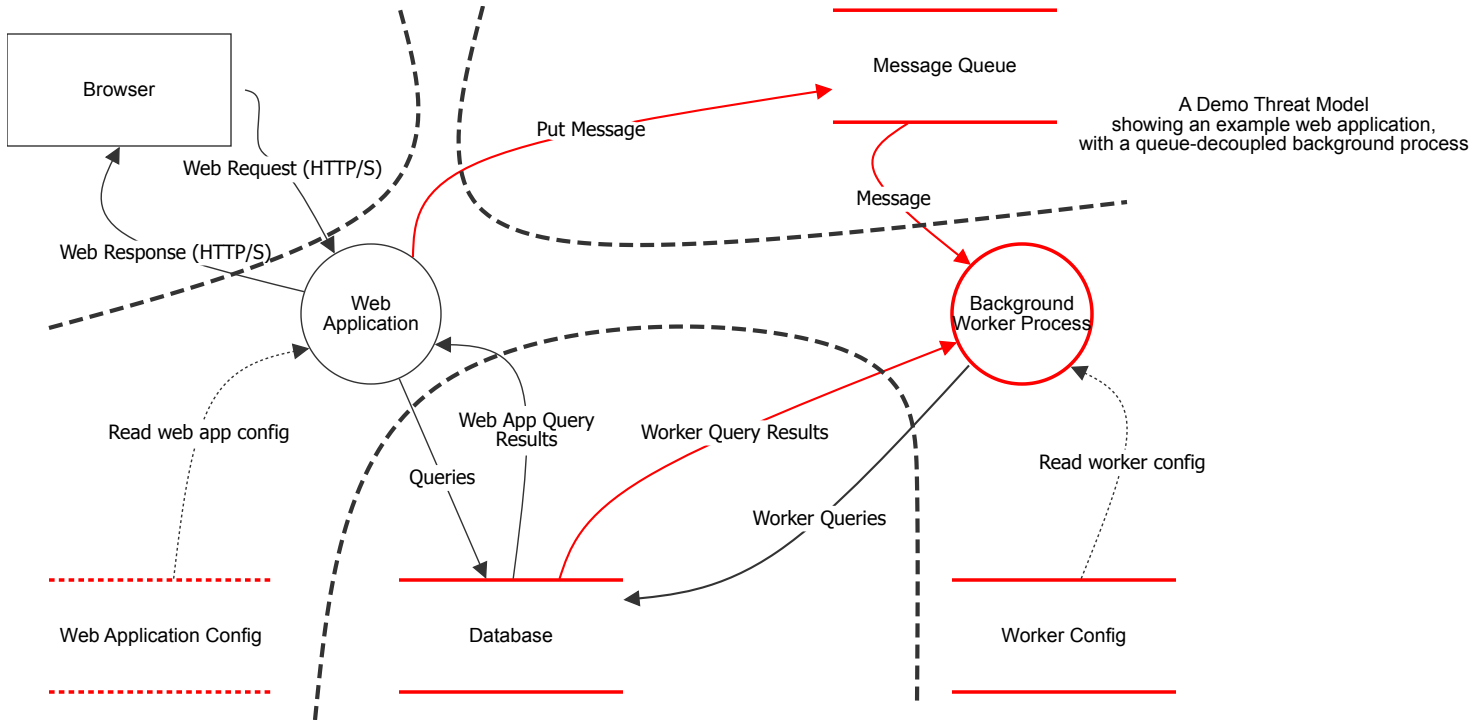
Source: TR-03183 - Chapter 3.11

- Honest cybersecurity risk assessment
- Use appropriate security controls
- Transparent and open communication
- Don't reinvent the wheel - use best practices
- Up-to date PDEs are mandatory for their whole lifecycle
- Mitigate identified risks to a tolerable level



Threat Modelling

- identify & document potential threats
- use frameworks like STRIDE
- use software like Threat Dragon



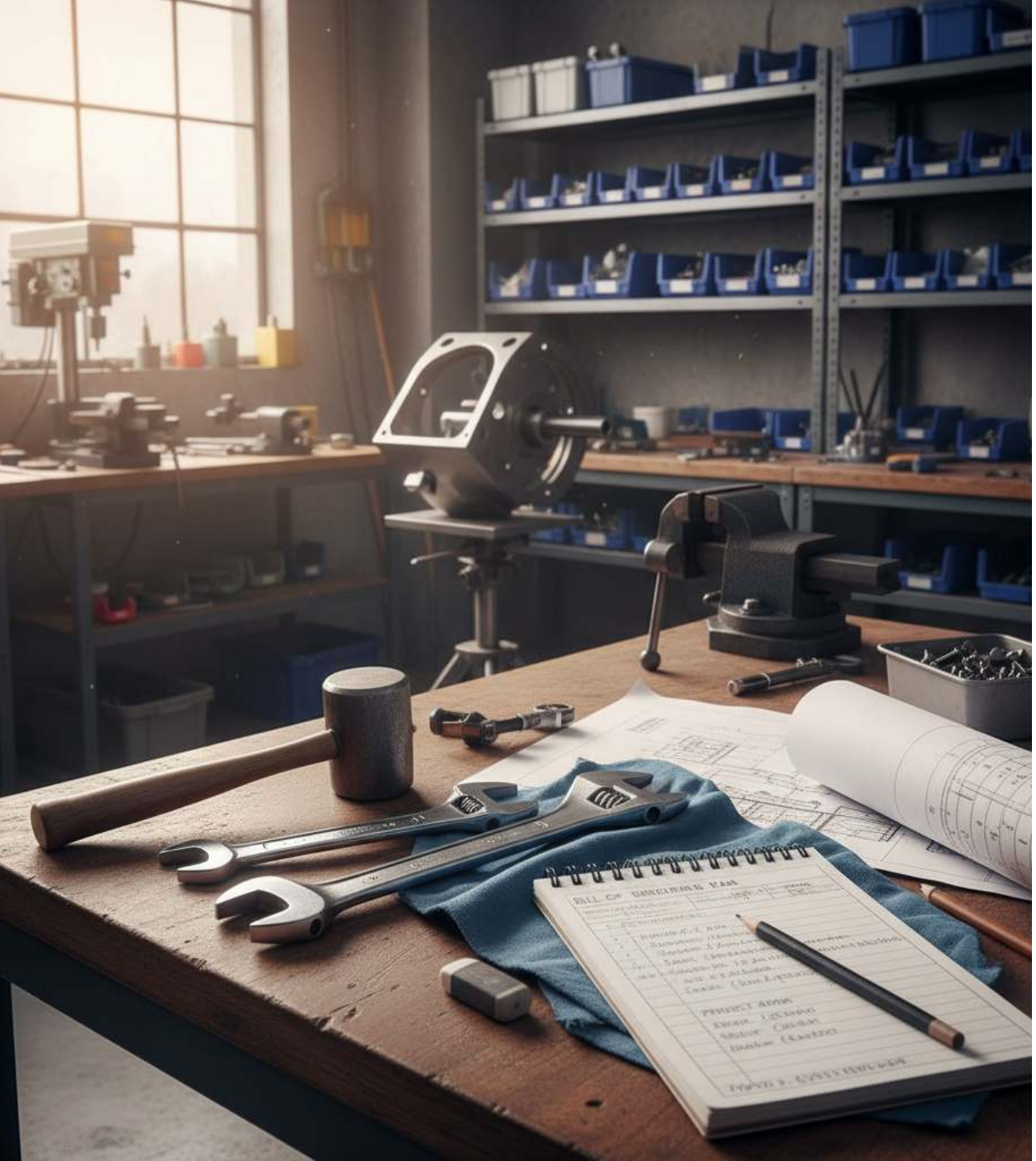
SBOMs - The Ingridient List of your Software

List of all **components** including their **version and license**, enabling:

- **Transparency & Security** – Like the ingridient list for food
- **Vulnerability & Licensemanagement** – Identitfy risks early
- **Compliance** – Provenance about source, licence and version information

There are two *allowed* formats

Format	Origin	Focus
SPDX	Linux Foundation	**License-Compliance & Open Source**
CycloneDX	OWASP	**Security & Riskmanagement**



Automatically generate SBOM on Release

- CycloneDX Maven Plugin
- GoReleaser
- Kubernetes bom
- Microsoft's SBOM Tool
- SPDX SBOM Generator
- Syft

Example: Marvin-App

- simple Angular 21 - Application
- runs on GH-Pages
- create SBOM via `cdxgen`

```
npx @cyclonedx/cdxgen \
  -o sbom.cdx.json
```

Excerpt from sbom.cdx.json - (30.469 Lines)


```
{
  "name": "vite",
  "version": "7.3.0",
  "properties": [
    {
      "name": "SrcFile",
      "value": "package-lock.json"
    },
    {
      "name": "ResolvedUrl",
      "value": "https://registry.npmjs.org/vite/-/vite-7.3.0.tgz"
    }
  ]
}
```

Use `trivy` to scan SBOM

```
$ trivy sbom sbom.cdx.json
2026-05-17T13:10:38-05:00 INFO [vulndb] Need to update DB
2026-05-17T13:10:38-05:00 INFO [vulndb] Downloading vulnerability DB...
2026-05-17T13:10:38-05:00 INFO [vulndb] Downloading artifact... repo="mirror.gcr.io/aquasec/trivy-db:2"
93.01 MiB / 93.01 MiB [-------------------------------------------------------------------------------------------] 100.00% 1.24 MiB p/s 1m15s
2026-05-17T13:11:55-05:00 INFO [vulndb] Artifact successfully downloaded repo="mirror.gcr.io/aquasec/trivy-db:2"
2026-05-17T13:11:55-05:00 INFO [vuln] Vulnerability scanning is enabled
2026-05-17T13:11:55-05:00 INFO Detected SBOM format format="cyclonedx-json"
2026-05-17T13:11:55-05:00 WARN Third-party SBOM may lead to inaccurate vulnerability detection
2026-05-17T13:11:55-05:00 WARN Recommend using Trivy to generate SBOMs
2026-05-17T13:11:55-05:00 INFO Number of language-specific files num=1
2026-05-17T13:11:55-05:00 INFO [node-pkg] Detecting vulnerabilities...

Report Summary
```

Target	Type	Vulnerabilities
Node.js	node-pkg	49

```
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


Node.js (node-pkg)

Total: 49 (UNKNOWN: 0, LOW: 3, MEDIUM: 23, HIGH: 23, CRITICAL: 0)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
vite	CVE-2026-39363	HIGH		7.3.0	8.0.5, 7.3.2, 6.4.2	Vite: Vite: Information disclosure via WebSocket connection bypasses access control https://avd.aquasec.com/nvd/cve-2026-39363
	CVE-2026-39364				8.0.5, 7.3.2	vite: Vite: Information disclosure via query parameter manipulation on the development server... https://avd.aquasec.com/nvd/cve-2026-39364
	CVE-2026-39365	MEDIUM			8.0.5, 7.3.2, 6.4.2	vite: Vite: Information disclosure via path traversal in dev server's .map request... https://avd.aquasec.com/nvd/cve-2026-39365

Lookup vulnerability at nvd.nist.gov

CVE-2026-39363 Detail

Description

Vite is a frontend tooling framework for JavaScript. From 6.0.0 to before 6.4.2, 7.3.2, and 8.0.5, if it is possible to connect to the Vite dev server's WebSocket without an Origin header, an attacker can invoke fetchModule via the custom WebSocket event vite:invoke and combine file://... with ?raw (or ?inline) to retrieve the contents of arbitrary files on the server as a JavaScript string (e.g., export default "..."). The access control enforced in the HTTP request path (such as server.fs.allow) is not applied to this WebSocket-based execution path. This vulnerability is fixed in 6.4.2, 7.3.2, and 8.0.5.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

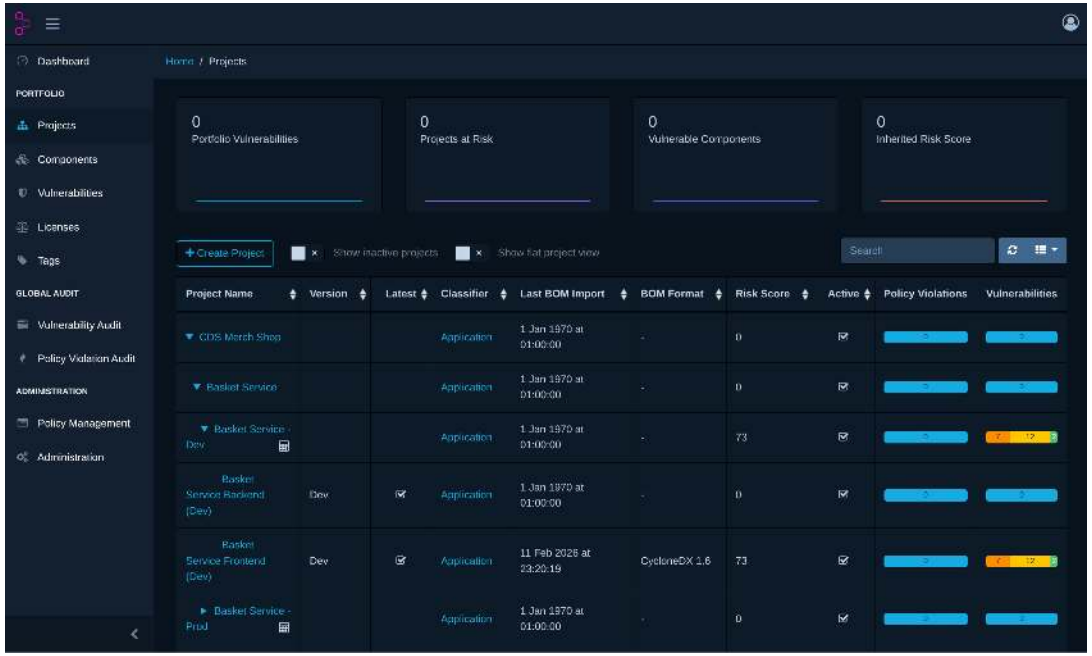
CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

QUICK INFO

CVE Dictionary Entry:
CVE-2026-39363
NVD Published Date:
04/07/2026
NVD Last Modified:
04/30/2026
Source:
GitHub, Inc.

DependencyTrack



- Use *Collection Projects* to organize your apps and services
- Enable Google OSV Advisories, as GHSA malwares are not included
- Use Terraform to manage DependencyTrack (Module for project creation)

Don't Forget your Team

You are happy, SBOMs are created automatically created for every envrionment. Everything looks fine.

- Who handles incidients?
- How are they handled?
- What is your RISK-Appetite?
- Don´t forget you team,
- and the process around it!

Finally, what about our `vite`-example?

- don´t worry, it´s a `devDependency`
- `vitest` purpose is to execute tests
- therefore it´s not part of the final product
- ask your team - they know

CRA Checklist

- ✓ Use Open Source solutions, like DependencyTrack, Kubernetes bom, etc.
- ✓ Use Guidance like TR-03183 - from the BSI
- ✓ Tight communication with your teams, users and peers
- ✓ Keep your Software up-to date
- ✓ Create KPIs for Management
- ✓ Document your efforts

Learnings

- CRA is not an end in itself
- The holistic Security Posture of your product becomes visible & measurable
- Start and evolve continuously
- Find your journey through the ocean and use the provided help (like TGs)

Thank you - let´s stay connected

Peter Dickten @ LinkedIn

Marcus Ross @ LinkedIn