SecuraPoint INFORMATIONSSICHERHEIT

From Pain to Process

Automating Open Source Compliance and Security

SecuraPoint INFORMATIONSSICHERHEIT

Who are we?

Marco Berger

DevOps Engineer & Product Owner

Sarah Berger

Security Consultant & ISO 27001 Auditor

SecuraPoint
INFORMATIONSSICHERHEIT

What can you expect?

Practical, Hands-On Approach

The focus is on demonstrating real, practical examples rather than relying on PowerPoint theory.

Only Open-Source Tools

All tools shown today are based entirely on open-source technology.

SBOM, Notice File, and Vulnerability Report

These three outputs will form the core of today's session.

Slides & Breaks

The slides will be shared afterwards, and a short 10-minute coffee break will take place roughly halfway through the webinar.

SecuraPoint INFORMATIONSSICHERHEIT

Would you buy and eat this chocolate?

We don’t trust food when we don’t know the ingredients but we trust software without knowing what is actually inside.

You will learn today how to address and solve this problem.

SecuraPoint INFORMATIONSSICHERHEIT

Why Do We Use Open-Source Packages?

Faster Development

Open-source packages accelerate development because teams can rely on proven, ready-to-use components instead of building everything from scratch.

Higher Quality and Security

Open-source code is continuously reviewed and improved by a broad community, resulting in more reliable software and faster security fixes.

"There is no such thing as a free lunch"

— Milton Friedman

SecuraPoint INFORMATIONSSICHERHEIT

Where Open-Source Packages Can Become a Problem

Licenses and Copyrights

Open-source packages can come with complex licensing and attribution requirements that must be understood and fulfilled to avoid legal or compliance issues.

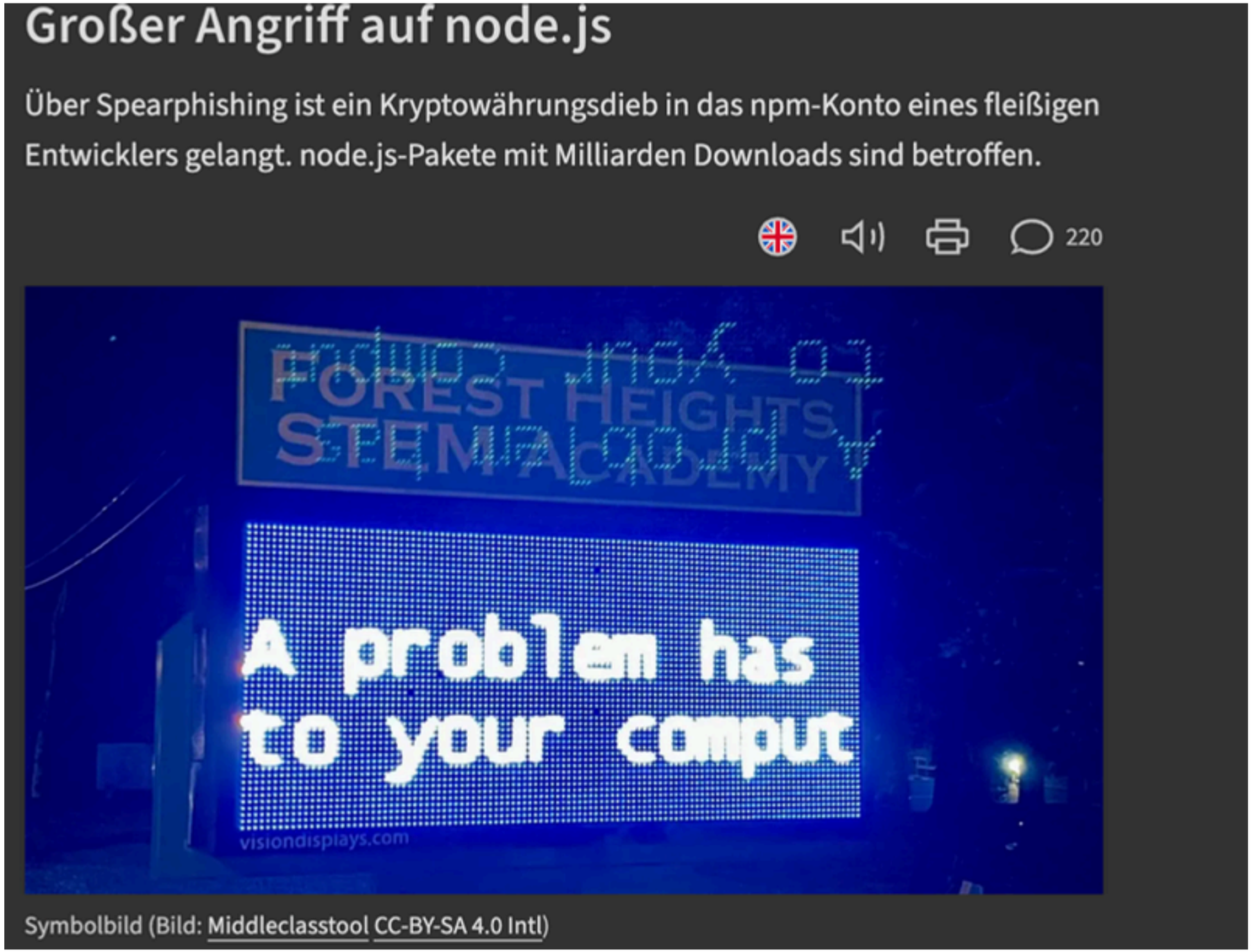
We need to know under which license conditions we are allowed to use the package.

Attacks and Vulnerabilities

Security risks arise when open-source components contain known vulnerabilities that attackers can exploit if they remain unnoticed or unpatched.

We need to be aware of any vulnerabilities both before and after the software release.

You’d better know which NPM packages you are using…

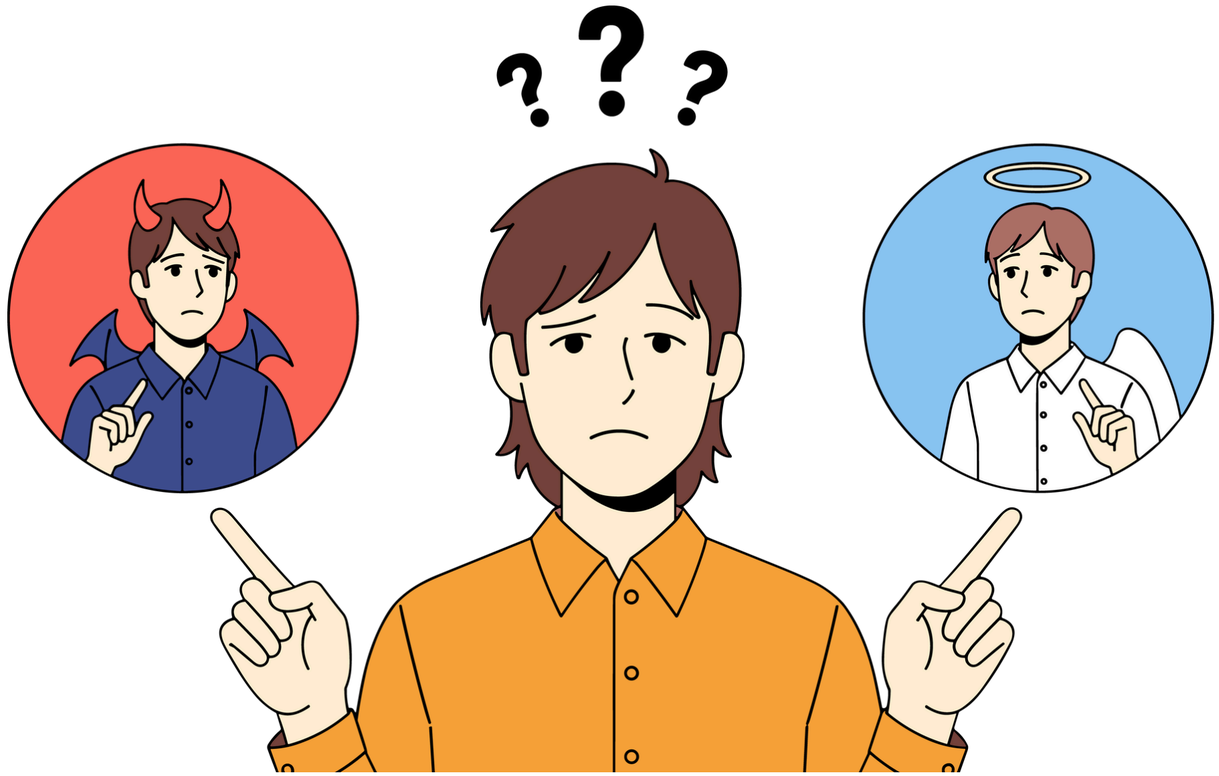


SecuraPoint INFORMATIONSSICHERHEIT

Why the license condition matters

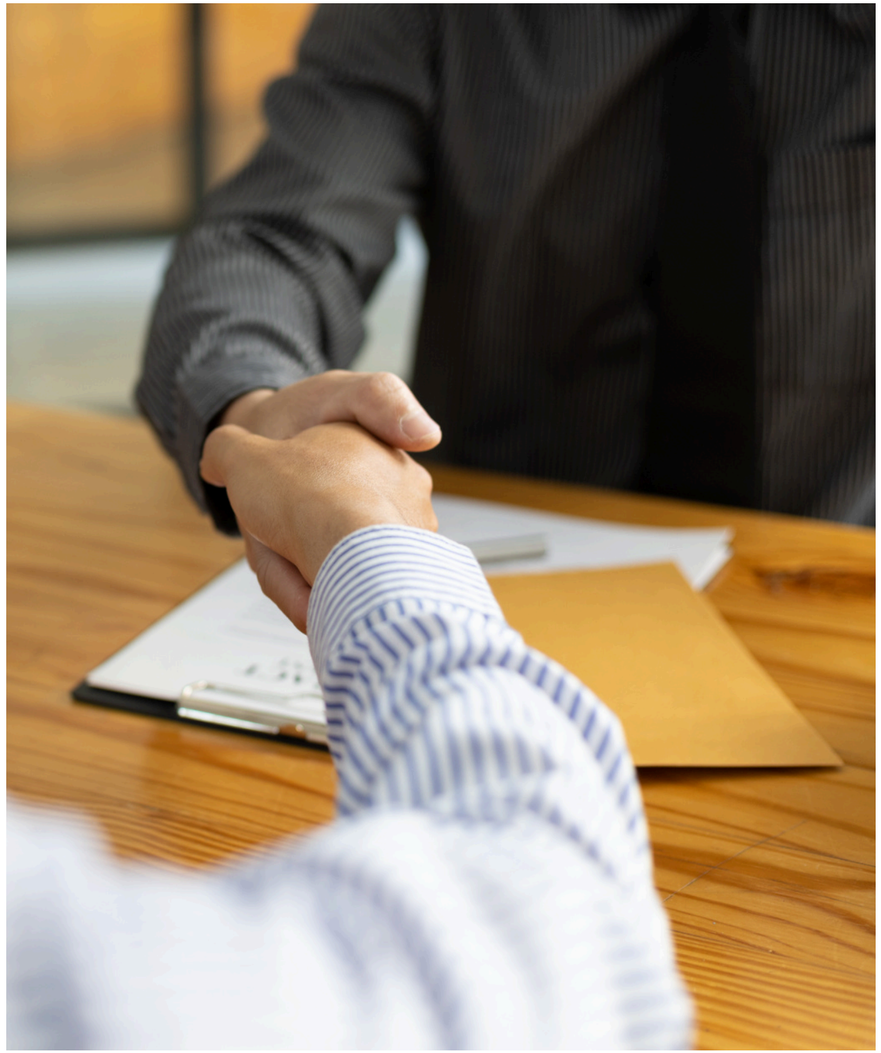
Evil licenses?

Copyleft effect
(e.g. GPLv3, AGPLv3, LGPL, etc.)



Good licenses?

Permissive licenses
(e.g. MIT, Apache 2.0, BSD 2-Clause, etc.)



Why do you need to create a notice file?

The obligation to provide license and copyright information comes directly from the open-source licenses, which act as contractual agreements when you use a package.

SecuraPoint INFORMATIONSSICHERHEIT

Notice File Example

3rd Party Software License Information

No changes have been made to the source code of the open source software components used in this application. All open source software components used are in their original, unmodified state.

Software	Version	License	License Text
@angular/animations	17.3.12	MIT	Read
@angular/cdk	17.3.10	MIT	Read
@angular/common	17.3.12	MIT	Read
@angular/core	17.3.12	MIT	Read
@angular/forms	17.3.12	MIT	Read
@angular/localize	17.3.12	MIT	Read
@angular/material	17.3.10	MIT	Read
@angular/platform-browser	17.3.12	MIT	Read
@angular/router	17.3.12	MIT	Read
@angular/service-worker	17.3.12	MIT	Read
@iplab/ngx-color-picker	17.2.2	MIT	Read
@kurkle/color	0.3.4	MIT	Read

@iplab/ngx-color-picker@17.2.2

MIT License

Copyright (c) 2018 Ivan Pintar

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

https://www.miele-move.com/pages/legal/thirdPartyLicenses

If intrinsic motivation to understand which software packages you are using, including their license conditions and potential vulnerabilities, is not enough, then there is always one final driver:

Compliance.

"Der CRA ist ein Gamechanger für die Sicherheit digitaler Produkte"

— BSI Präsidentin Claudia Plattner

https://www.heise.de/news/Cyber-Resilience-Act-BSI-wird-Marktaufsichtsbehoerde-10733564.html

SecuraPoint INFORMATIONSSICHERHEIT

Cyber Resilience Act (CRA)

The Cyber Resilience Act is laid down in Regulation (EU) 2024/2847 — it entered into force on 10 December 2024 and will apply in full from 11 December 2027, affecting all manufacturers, importers and distributors of products with digital elements on the EU market.

During Development

- Conduct continuous risk assessments and apply security-by-design principles.
- Ensure the software is free from known vulnerabilities before release.
- Create and maintain an **SBOM** for every software version.
- Implement secure development and testing practices.

&

After Release

- Monitor vulnerabilities and respond without delay.
- Report exploited vulnerabilities or severe incidents within set timeframe.
- Provide timely security updates and communicate risks to users.
- Maintain a vulnerability handling process throughout the product lifecycle.

SecuraPoint INFORMATIONSSICHERHEIT

Long story short: What you need to do

Create a SBOM

List all third-party and first-party components used in your software. The CRA requires this, and the SBOM forms the baseline for effective vulnerability management.

Create a Notice File

Document all third-party components along with their obligations (e.g., license texts, modifications, copyrights). This ensures transparency and legal compliance.

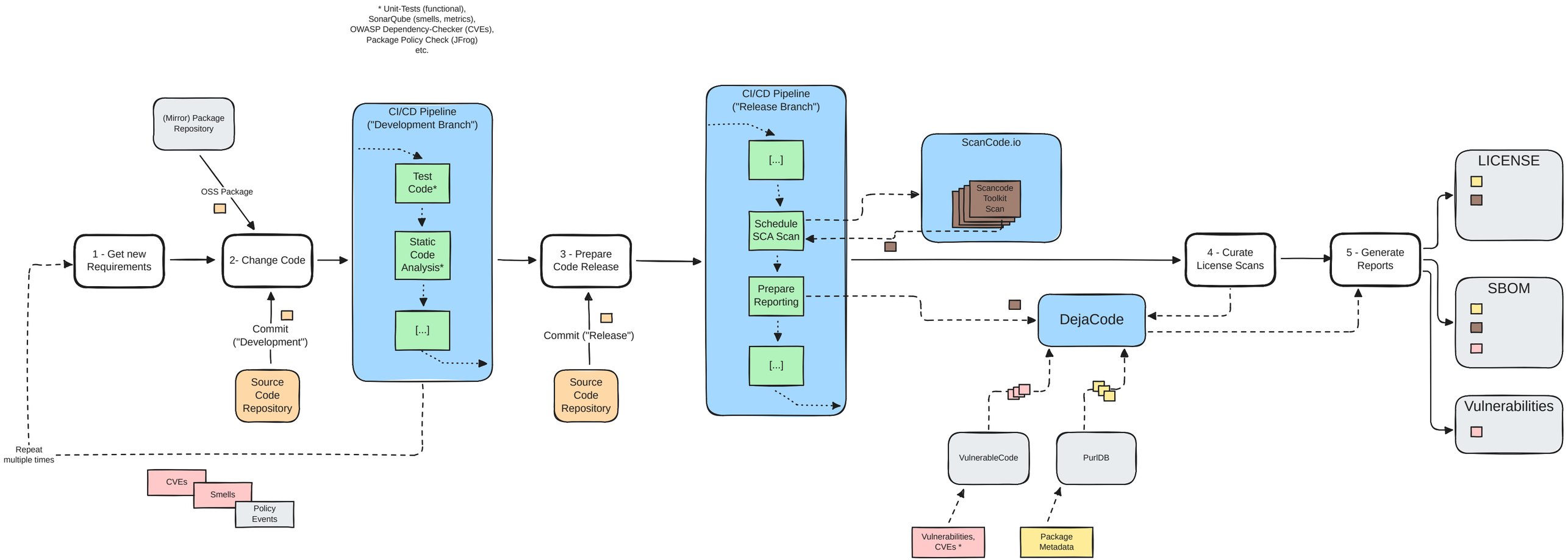
Check for Vulnerabilities

Scan third-party components for known vulnerabilities before release and continuously after release to maintain product security over time.

SecuraPoint INFORMATIONSSICHERHEIT

Sichere Softwareentwicklung

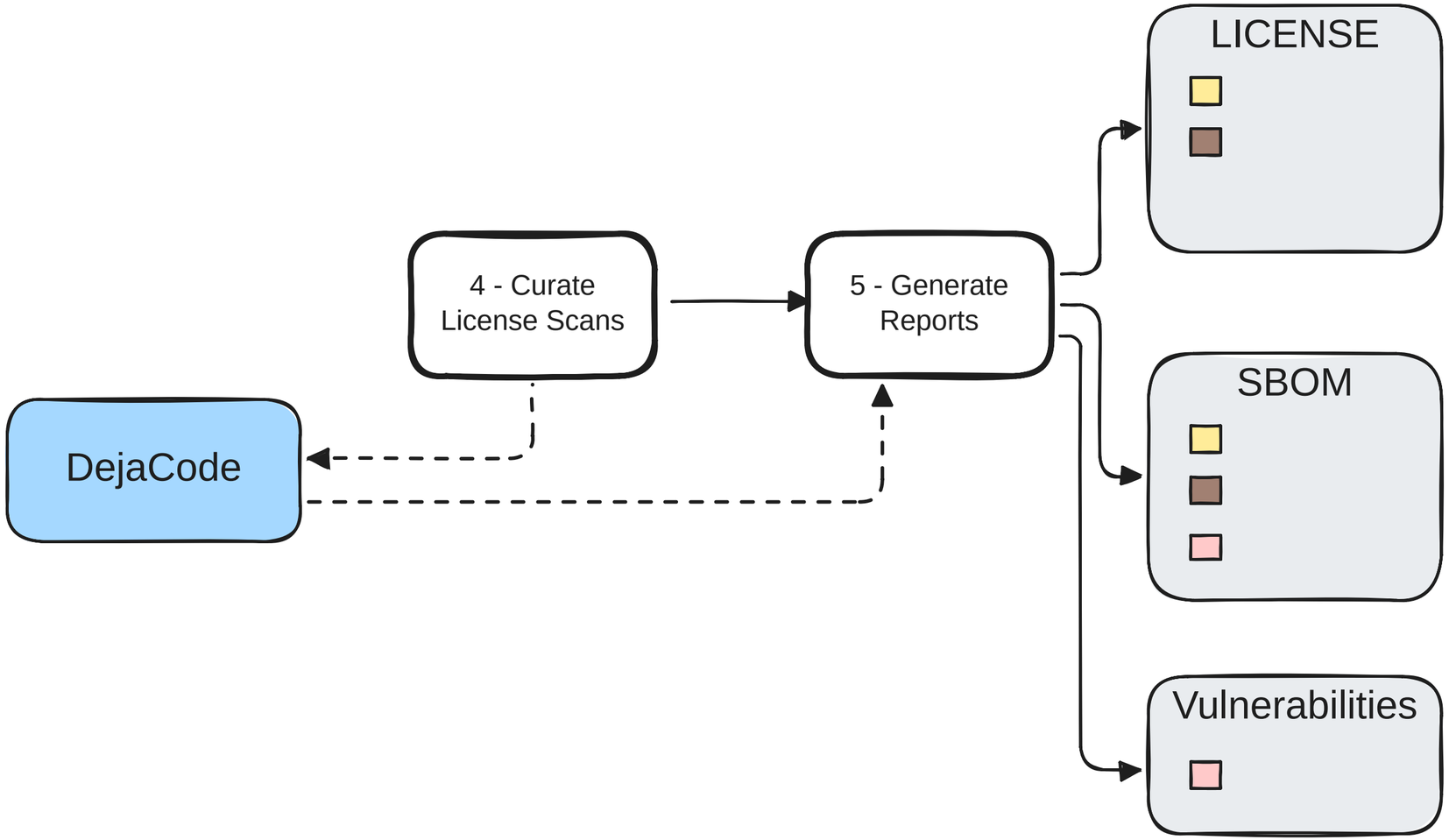
Ein beispielhafter Prozess mit passender Tool-Unterstützung



SecuraPoint INFORMATIONSSICHERHEIT

Wichtige Artefakte

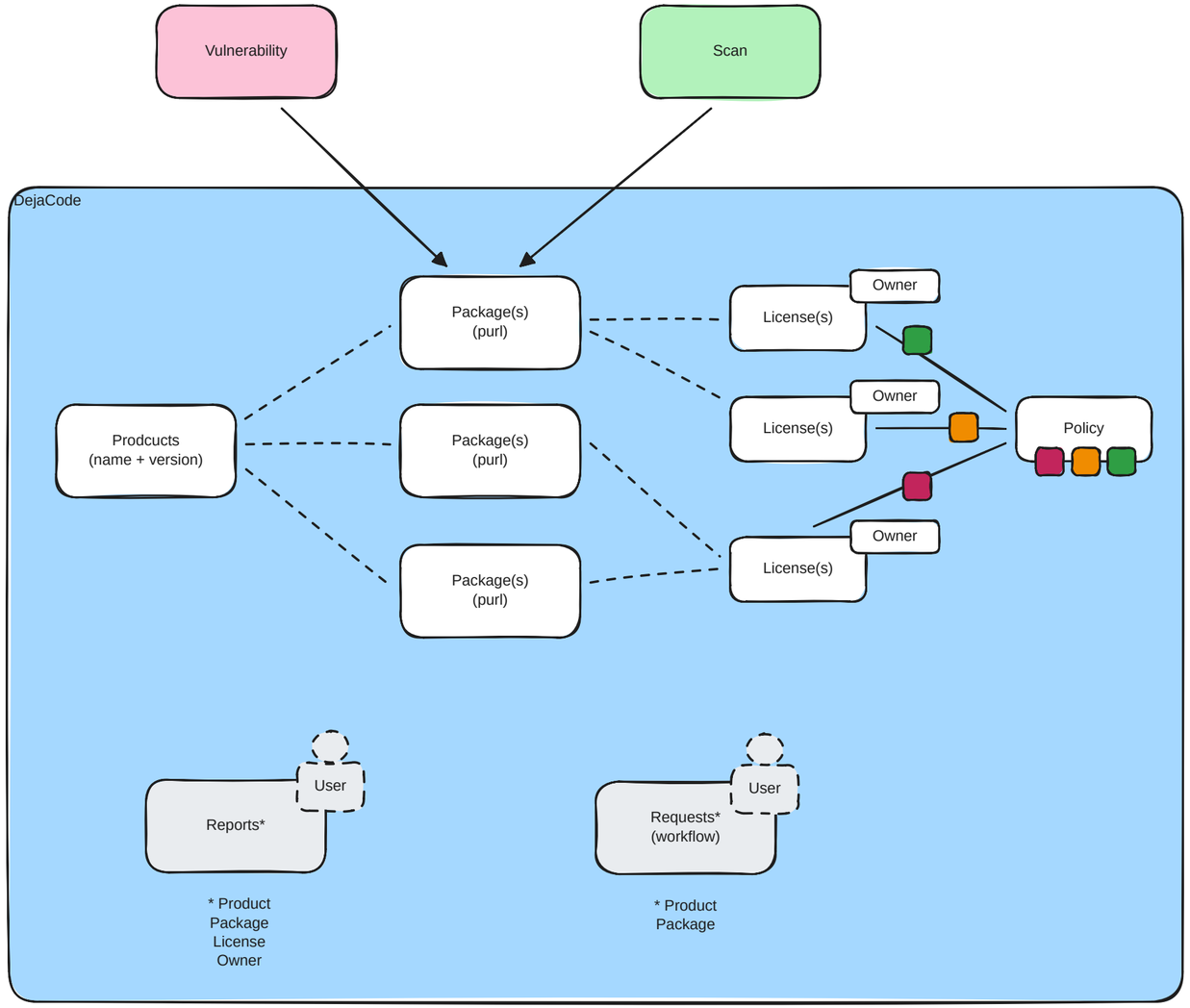
LICENSE / NOTICE File, SBOM und Vulnerability-Report



SecuraPoint INFORMATIONSSICHERHEIT

Package in DejaCode

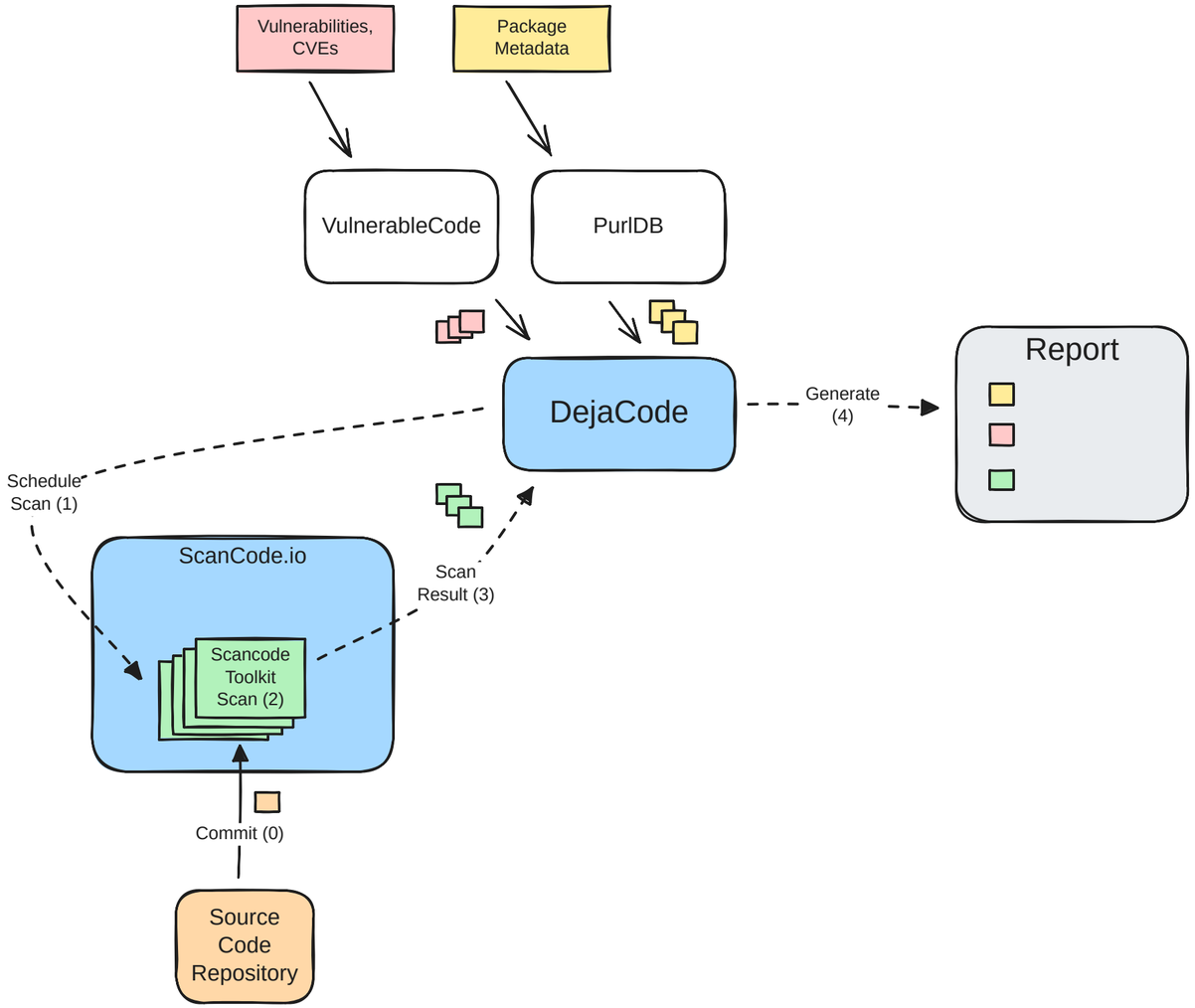
Beziehungen zwischen Objekten in DejaCode



SecuraPoint INFORMATIONSSICHERHEIT

DejaCode & Scancode.io

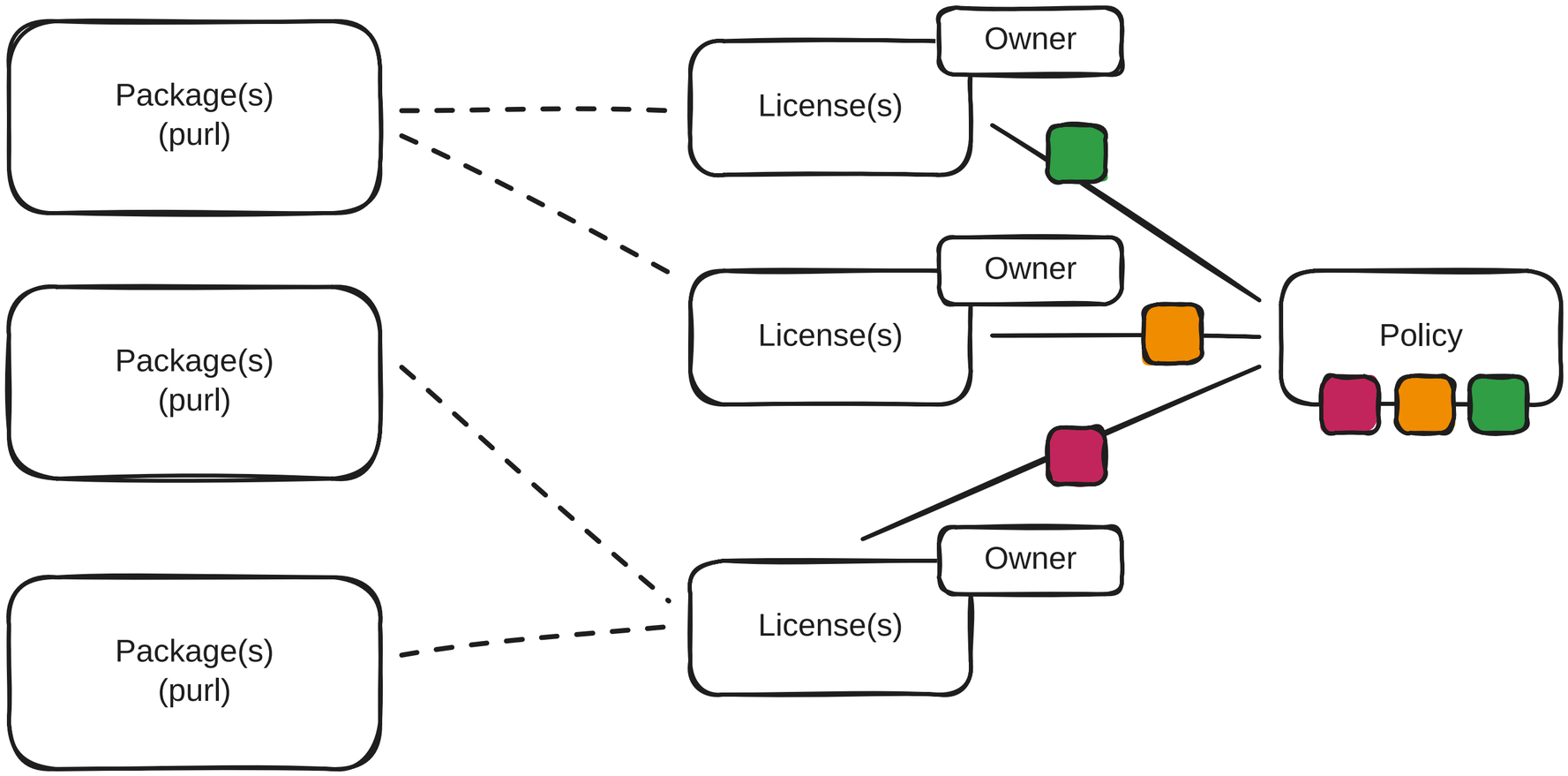
Integration der beiden Tools und Arbeitsabläufe



SecuraPoint
INFORMATIONSSICHERHEIT

Policies in DejaCode

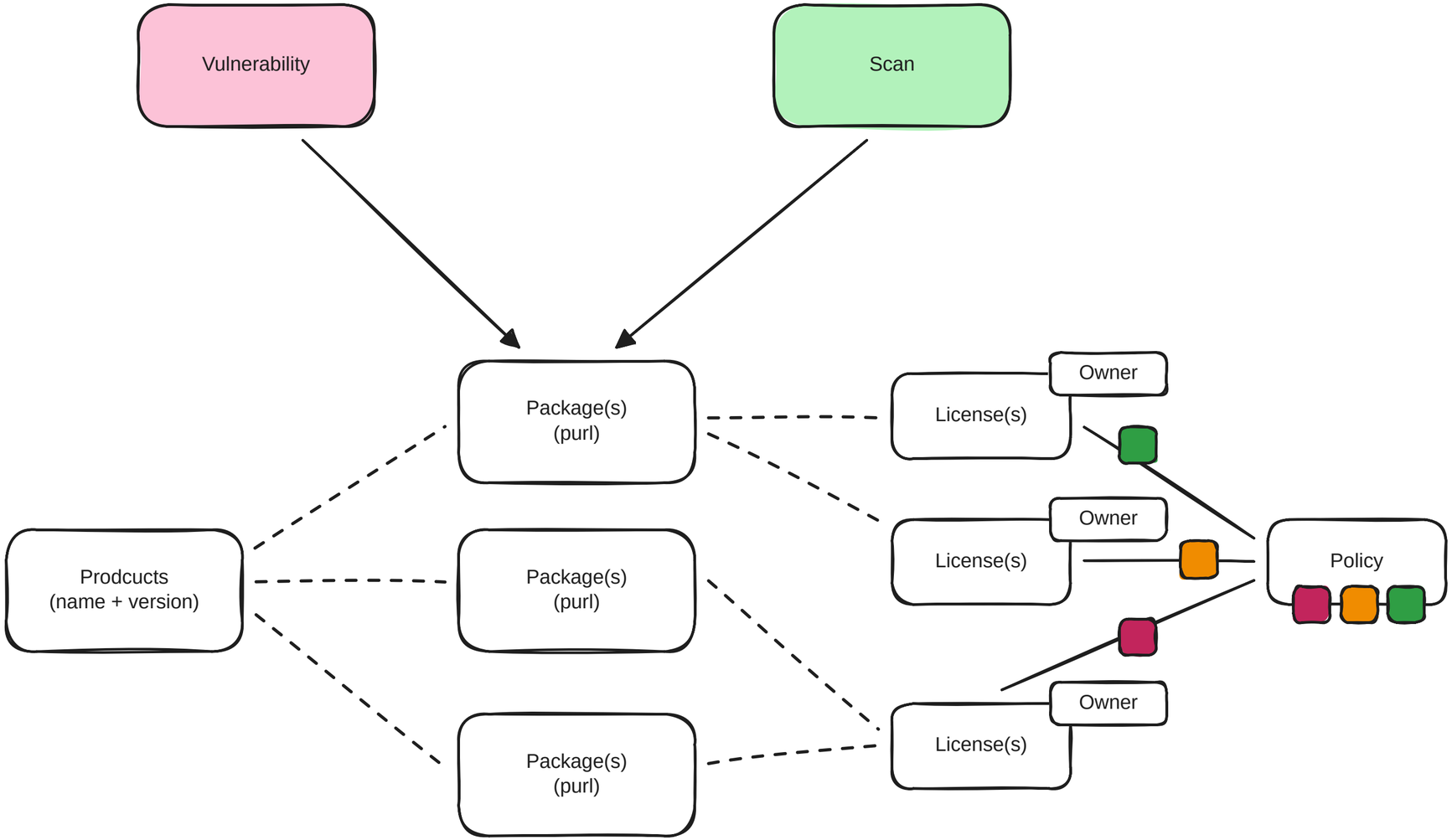
Die Wirkung von Policy auf Packages und Products



SecuraPoint INFORMATIONSSICHERHEIT

Product in DejaCode

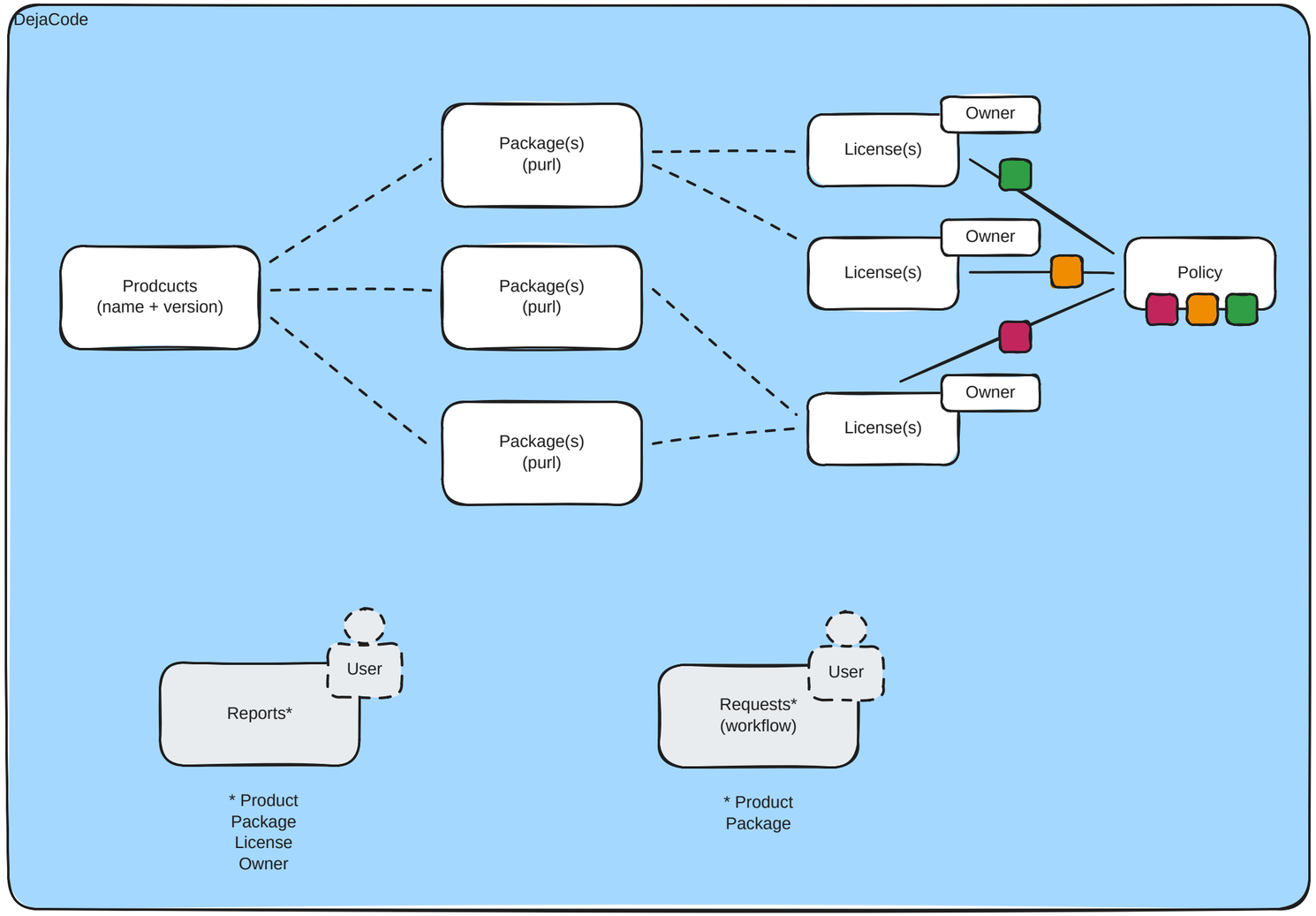
Der Container für alle weiteren Objekte



SecuraPoint INFORMATIONSSICHERHEIT

Custom Reports

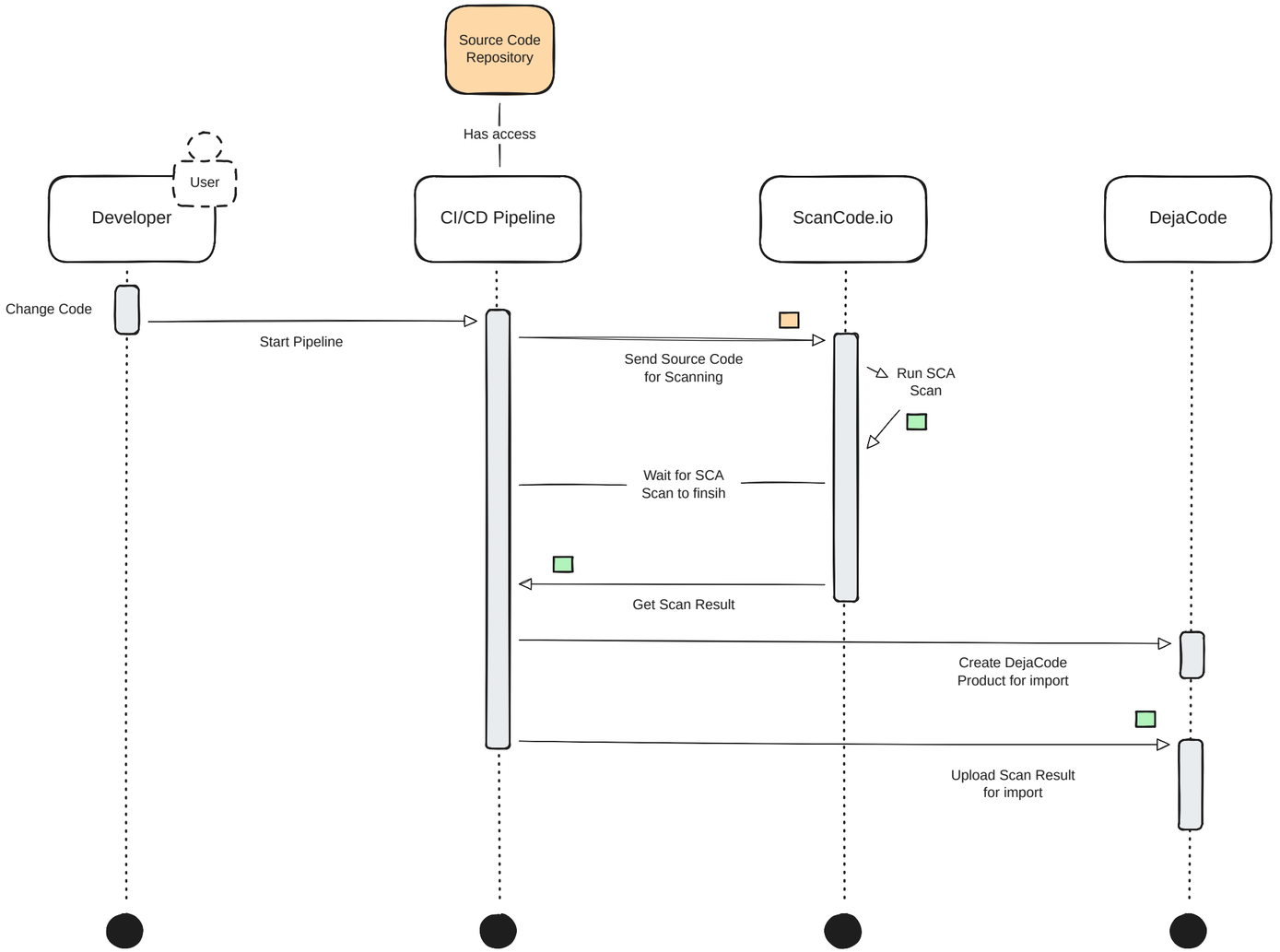
Werkzeug für weiterführende Prozesse



SecuraPoint INFORMATIONSSICHERHEIT

Integration in CI/CD

APIs für Automatisierungen in Pipelines



SecuraPoint
INFORMATIONSSICHERHEIT

Vielen Dank

Bei Fragen können Sie sich gerne melden via
info@securapoint.de