
white
duck

Container Security Made Easy – Tools and Techniques for Developers

ContainerDays, September 24

white duck

Who we are

Philip Welz
Senior Platform & Kubernetes Engineer,
Azure MVP

+49 8031 230159-0
philip.welz@whiteduck.de
@philip_welz
www.linkedin.com/in/philip-welz

Nico Meisenzahl
Head of Platform Engineering,
Cloud Solution Architect

+49 8031 230159-0
nico.meisenzahl@whiteduck.de
@nmeisenzahl
www.linkedin.com/in/nicomeisenzahl

The idea & the goal

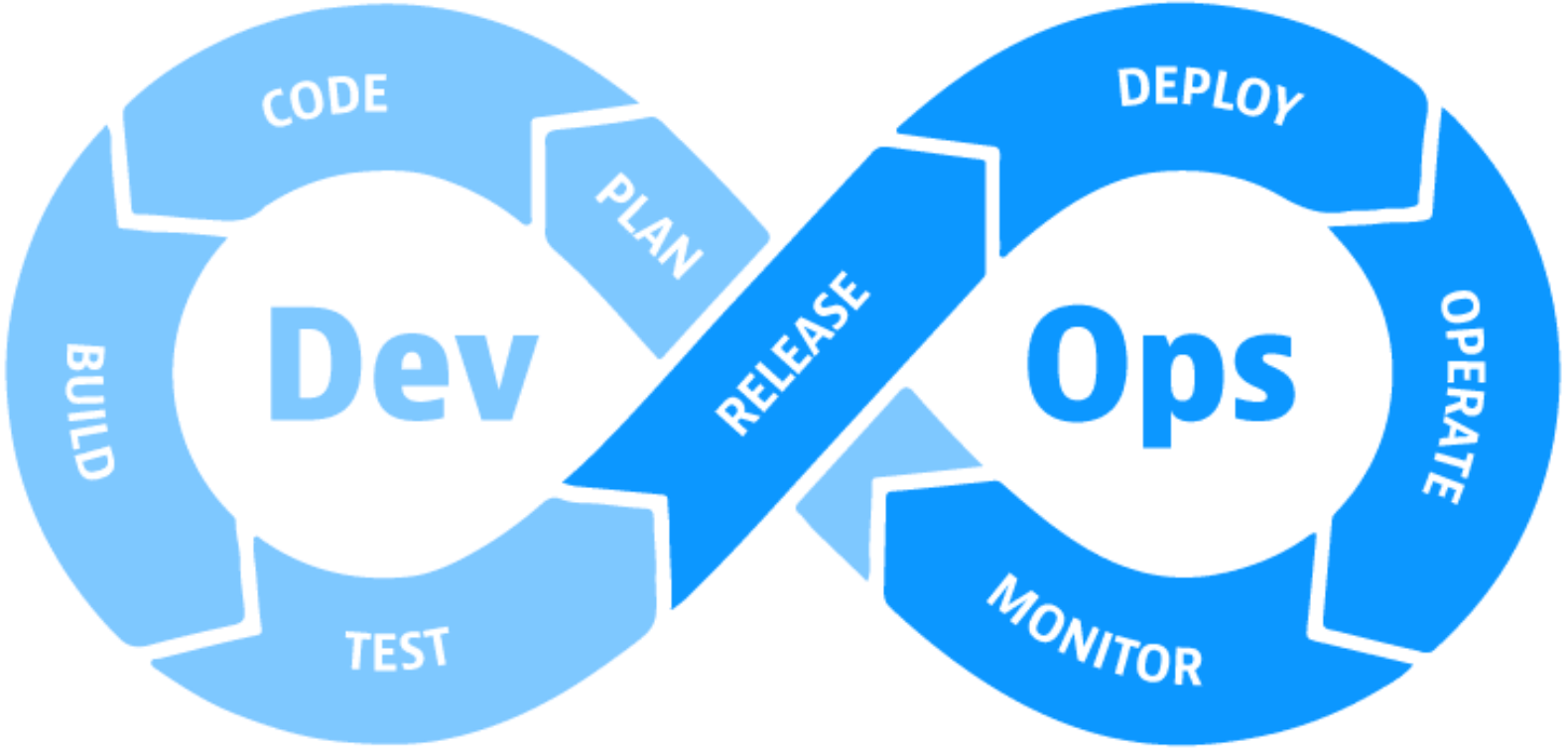
- Raising security awareness – yep, still required
- Make security easy and accessible for developers
- Prove that security can be integrated without bothering people
- Showcase real-world examples
- (There might be alternatives for those who have the money and time to invest in security)

Who is a developer?

- Who feels confident when it comes to security? 😉

DevSecOps

... is the **integration of security** within the whole DevOps process.

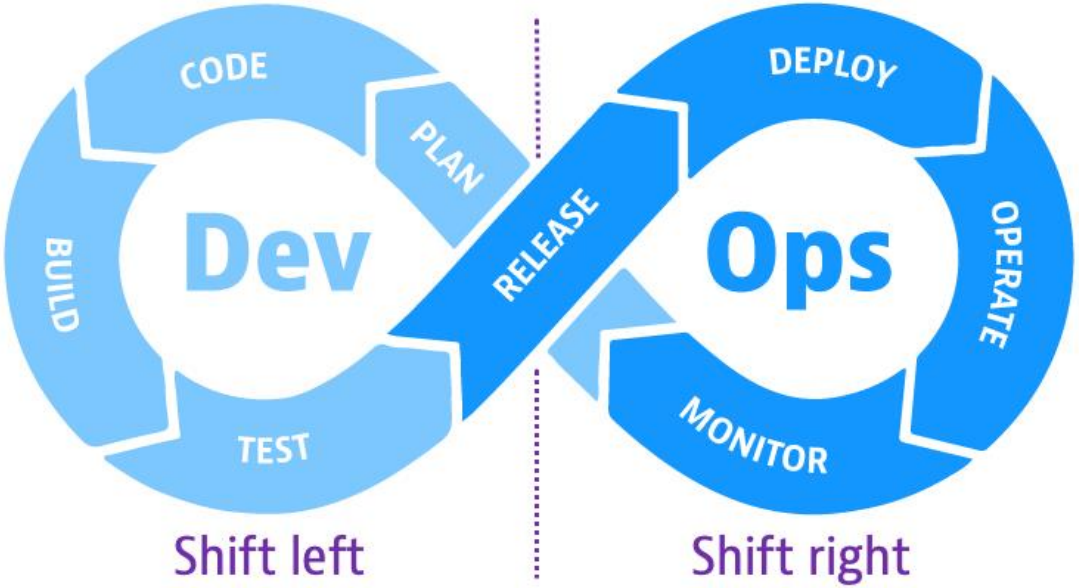


Picture source: https://www.dynatrace.com

Shift left

... is the practice of integrating testing **into the earliest stages** of the software development process

- Faster feedback loops
- Improved overall quality
- Fewer production issues



Picture source: https://www.dynatrace.com

Abstract security into a platform to scale

- An Internal Developer Platform can help scaling
- You can integrate security into all phases to make it easy to consume
- But: It‘s like with Kubernetes – only build complexity when you need it

Demo – What we will show you

1. Getting awareness of dependency updates and vulnerabilities
   - Automated dependency updates with integrated validation
   - Software Bill of Material (SBOM) for awareness of vulnerabilities
2. Automatically fixing vulnerabilities in container images
   - Remedying vulnerabilities by automatically fixing container images
   - Fully integrated testing to ensure software quality

Demo, demo, demo 🚀

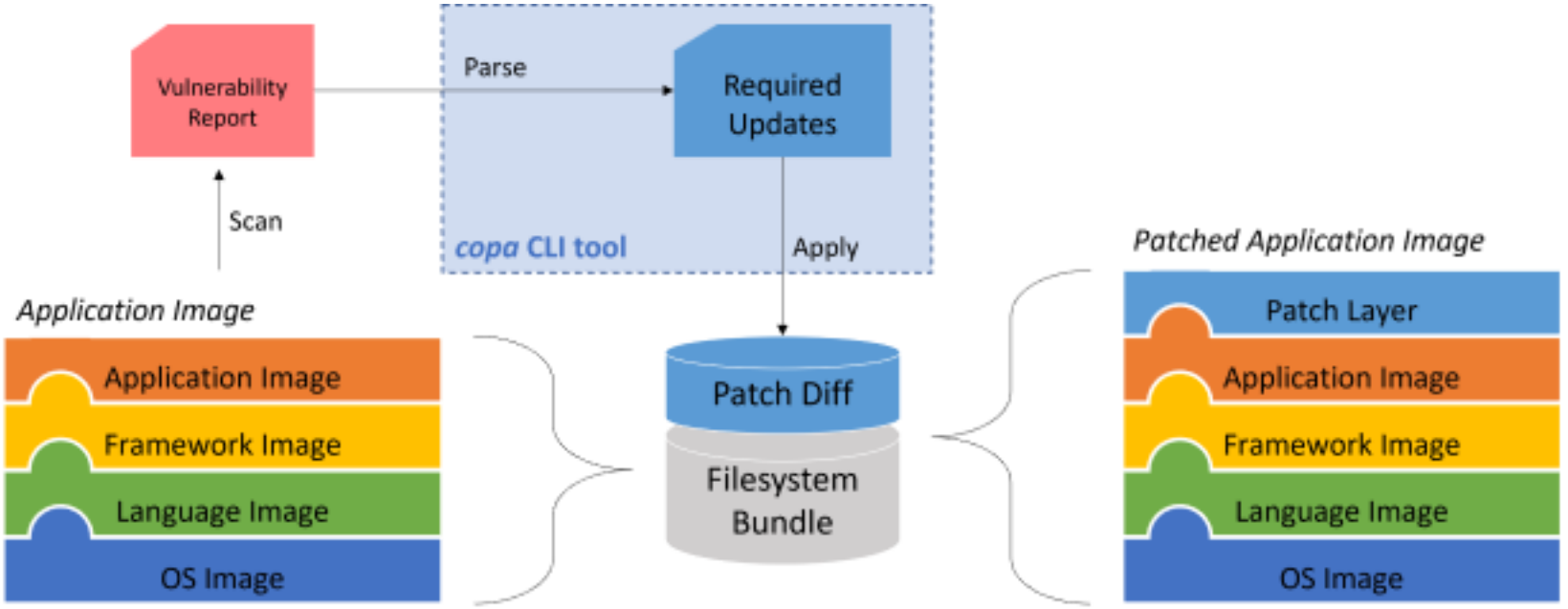
- The showcased tools are an example
  - There are many
  - Check the CNCF/Open-Source ecosystem and choose the ones that best suit your needs
- Slides are also available within the repo
- https://github.com/whiteducksoftware/cd-security-dev-demo

Software Bill of Materials (SBOM)

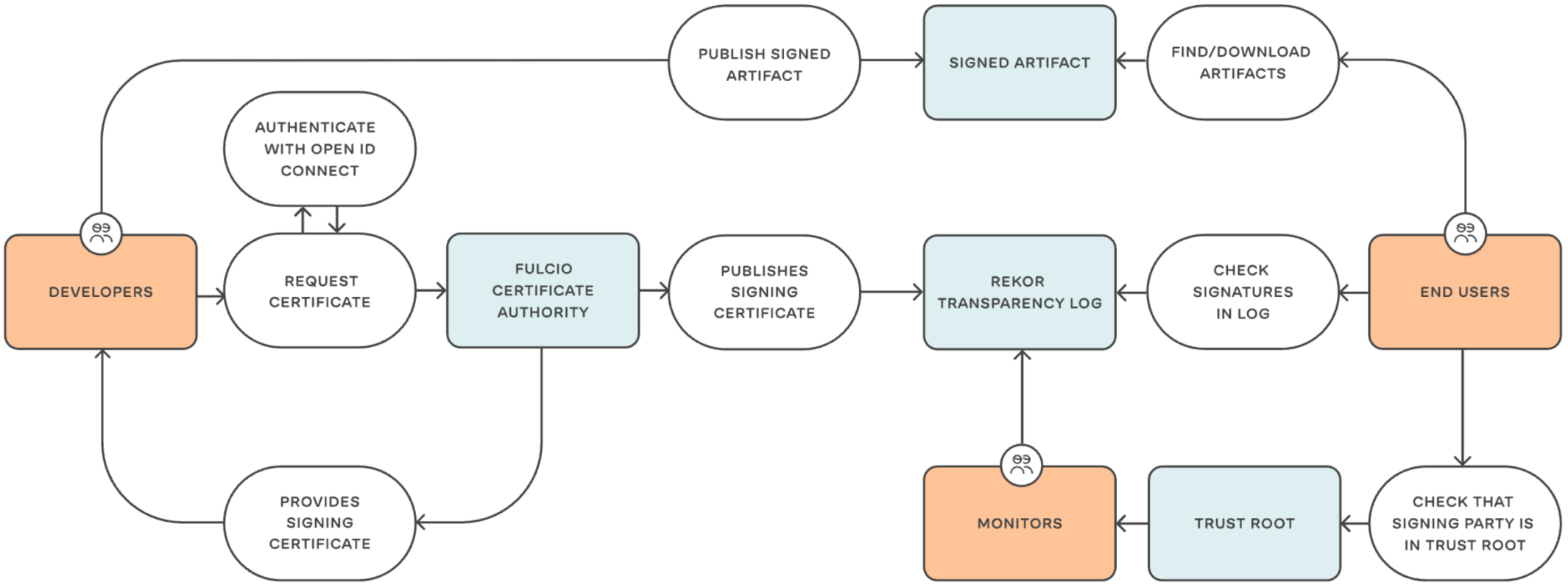
- “List of ingredients” for all your software and dependencies
  - Supports hierarchy and therefore multi-level dependencies
- Without you don’t have the full visibility
  - In an ideal world you would only need to care about your own stuff
- SBOMs can be the baseline for your vulnerability and license scanning
- Currently, there are multiple standards (SPDX, CycloneDX, SWID, …)

Copacetic

- “Directly patch container image vulnerabilities”
- https://project-copacetic.github.io
- Note: You will have to invest into testing!



Keyless Signing with Sigstore



Questions?

Philip Welz
Senior Platform & Kubernetes Engineer,
Azure MVP

+49 8031 230159-0
philip.welz@whiteduck.de
@philip_welz
www.linkedin.com/in/philip-welz

Nico Meisenzahl
Head of Platform Engineering,
Cloud Solution Architect

+49 8031 230159-0
nico.meisenzahl@whiteduck.de
@nmeisenzahl
www.linkedin.com/in/nicomeisenzahl

Thank you!