

# Composing the Ultimate SBOM

Ivana Atanasova, Velichka Atanasova  
VMware Open Source Program Office  
15 Oct 2022, OpenFest

 @VMWopensource

# Agenda

The Dependency Graph Nightmare

The SBOM and the Community Standards

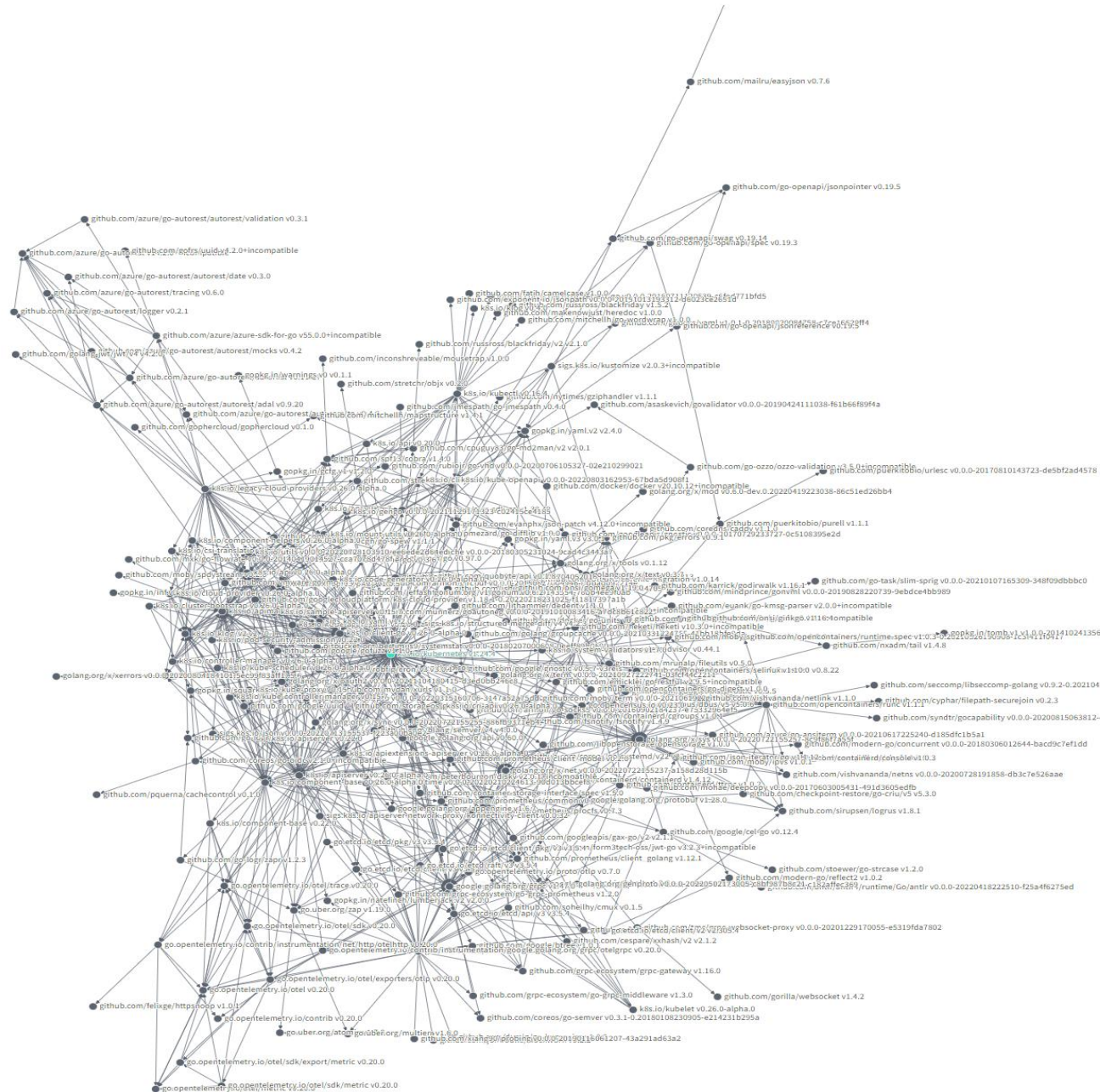
The Landscape of Tools

The Ultimate SBOM

Demo

Takeaways

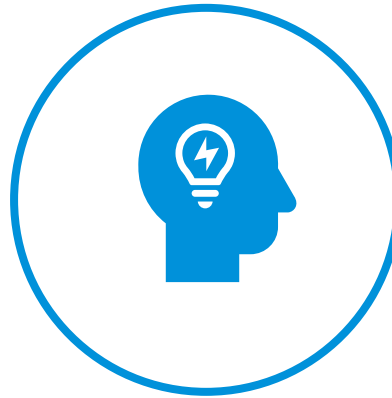
Q&A



# How We Build Software Today



Not reinventing  
the wheel



Focusing on  
unique  
innovations



Bringing  
solutions to life  
much faster

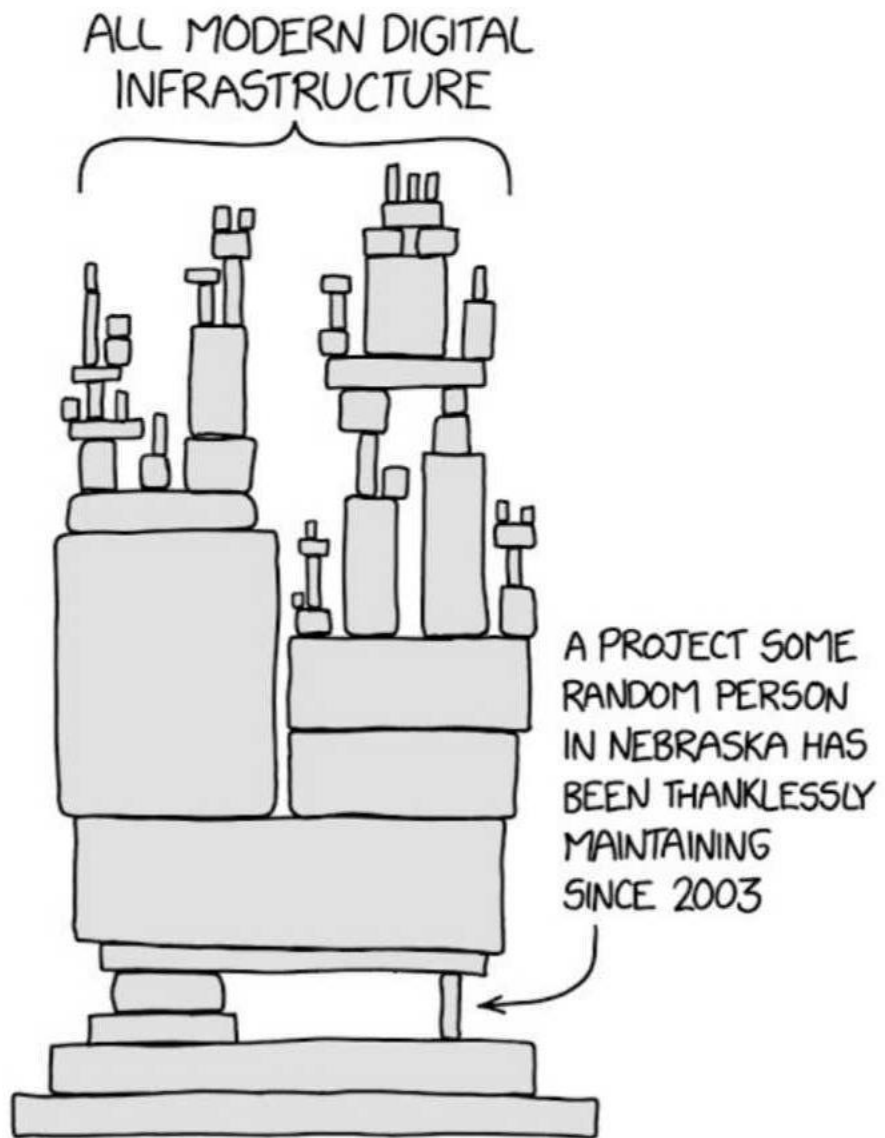


Image from xkcd.com

# Do we know our software?



Photo by [Towfiqu barbhuiya](#) on [Unsplash](#)

- > If we get hacked
- > When we get hacked
- > Hardened software supply chain
- > Explicitly declared software components





# Machine-readable Dependency Data

```
| photon
| 1 Relationships
| CONTAINS PACKAGE 37e73f039a18bf243eb5723af2f05ffadc4a0f442e7347df486106f943d83487
| 36 Relationships
| CONTAINS PACKAGE bash
| CONTAINS PACKAGE bzip2-libs
| CONTAINS PACKAGE ca-certificates
| CONTAINS PACKAGE ca-certificates-pki
| CONTAINS PACKAGE curl
| CONTAINS PACKAGE curl-libs
| CONTAINS PACKAGE e2fsprogs-libs
| CONTAINS PACKAGE elfutils-libelf
| CONTAINS PACKAGE expat
| CONTAINS PACKAGE expat-libs
| CONTAINS PACKAGE filesystem
| CONTAINS PACKAGE glibc
| CONTAINS PACKAGE krb5
| CONTAINS PACKAGE libcap
| CONTAINS PACKAGE libdb
| CONTAINS PACKAGE libgcc
| CONTAINS PACKAGE libmetalink
| CONTAINS PACKAGE libsolv
| CONTAINS PACKAGE libssh2
| CONTAINS PACKAGE lua
| CONTAINS PACKAGE ncurses-libs
| CONTAINS PACKAGE nspr
| CONTAINS PACKAGE nss-libs
| CONTAINS PACKAGE openssl
| CONTAINS PACKAGE photon-release
| CONTAINS PACKAGE photon-repos
| CONTAINS PACKAGE popt
| CONTAINS PACKAGE readline
| CONTAINS PACKAGE rpm-libs
| CONTAINS PACKAGE sqlite-libs
| CONTAINS PACKAGE tdnf
| CONTAINS PACKAGE tdnf-cli-libs
| CONTAINS PACKAGE toybox
| CONTAINS PACKAGE xz-libs
| CONTAINS PACKAGE zlib
| CONTAINS PACKAGE zstd-libs

Creator: Tool: tern-2.10.1
Created: 2022-05-03T17:34:13Z

PackageName: photon
SPDXID: SPDXRef-photon-3.0
PackageVersion: 3.0
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-photon-3.0
Relationship: SPDXRef-photon-3.0 CONTAINS SPDXRef-742bce9699

PackageName: 0a016225a33eefcb6357f20ef4f4f7b89a78c986fe87a8f7683e511a4b9443
SPDXID: SPDXRef-742bce9699
PackageFileName: 0a016225a33eefcb6357f20ef4f4f7b89a78c986fe87a8f7683e511a4b9443
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: false
PackageChecksum: SHA256: 742bce9699978f679680cb837df182097827617800d66afbe74cf271881749fd
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageComment: <text>
Layer 1:
  info: Layer created by commands: /bin/sh -c #(nop) ADD file:2c502d3d272ff0819f3d771e0be6be39eee46ca7a53d90160b12f2f62bc810a in /
  info: Found 'VMware Photon OS/Linux' in /etc/os-release.
  info: Retrieved package metadata using tdnf default method.

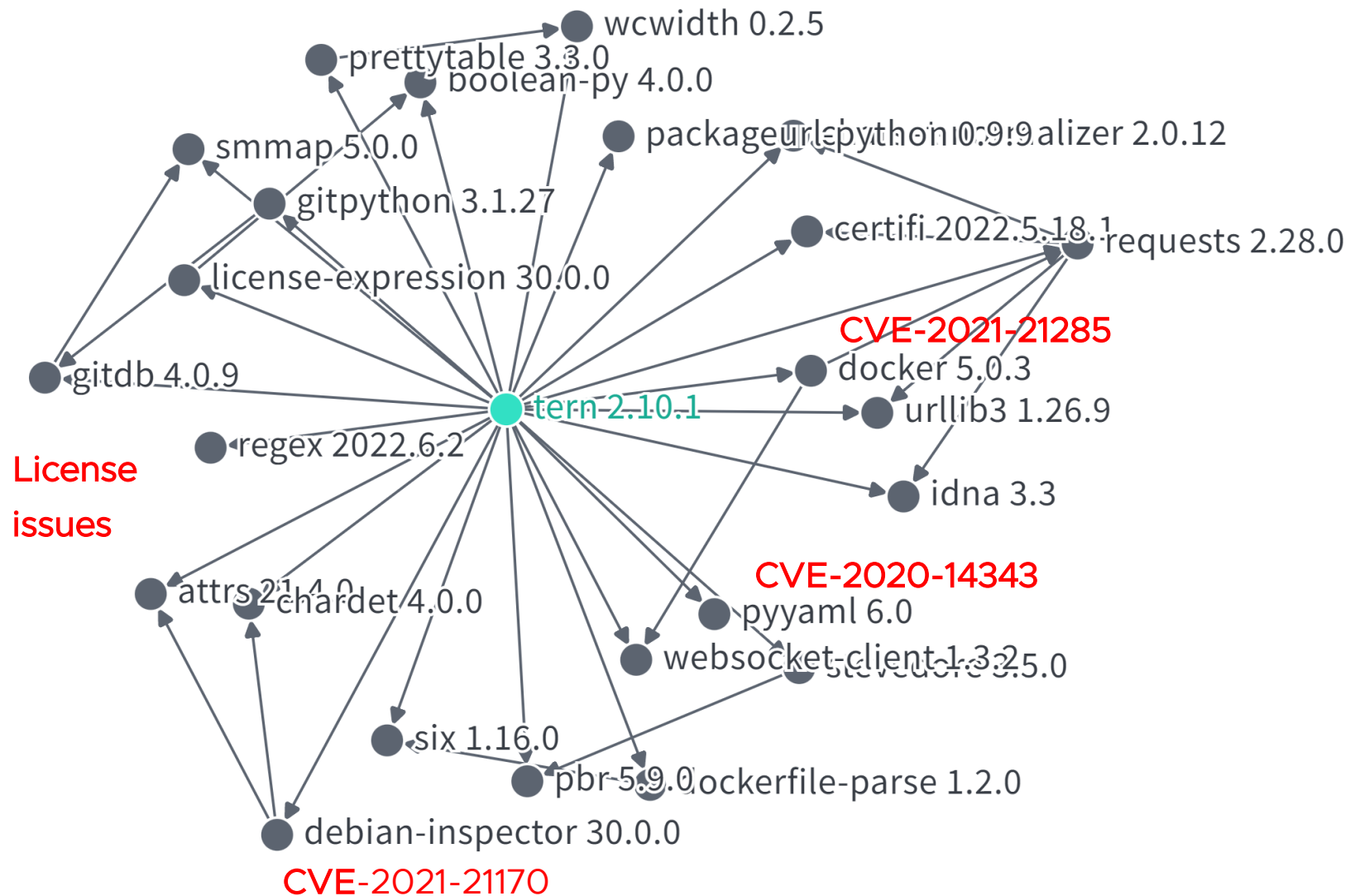
</text>

Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-bash-4.4.18-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-bzip2-libs-1.0.8-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-ca-certificates-20190521-3.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-ca-certificates-pki-20190521-3.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-curl-7.82.0-1.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-curl-libs-7.82.0-1.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-e2fsprogs-libs-1.45.5-3.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-elfutils-libelf-0.176-1.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-expat-2.2.9-9.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-expat-libs-2.2.9-9.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-filesystem-1.1-4.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-glibc-2.28-20.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-krb5-1.17-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-libcap-2.25-8.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-libdb-5.3.28-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-libgcc-7.3.0-5.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-libmetalink-0.1.3-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-lisolv-0.6.35-8.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-libssh2-1.9.0-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-lua-5.3.5-3.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-ncurses-libs-6.1-4.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-nspr-4.21-1.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-nss-libs-3.44-7.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-openssl-1.0.2zc-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-photon-release-3.0-6.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-photon-repos-3.0-8.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-popt-1.16-5.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-readline-7.0-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-rpm-libs-4.14.3-1.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-sqlite-libs-3.35.5-1.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-tdnf-3.1.8-2.ph3
Relationship: SPDXRef-742bce9699 CONTAINS SPDXRef-tdnf-cli-libs-3.1.8-2.ph3
.
```

Reduced cost,  
license  
compliance and  
security risks




# Machine-readable Dependency Data



# Machine-readable Dependency Data





*“90% of organizations across the sample have started their SBOM journey.”*

Linux Foundation Report on SBOM and Cybersecurity Readiness

# The SBOM Journey



Standards



Tooling



Best Practices

# The SBOM Community Standards

## Custom Format Documents Issues:

- ❑ Not comprehensive data
- ❑ Prevents interoperability
- ❑ Hard to use from existing automations
- ❑ Hard data exchange



# The SBOM Community Standards



## SPDX v2.2 Document contains:

Document Creation Information

Package Information

File Information

Snippet Information

Other Licensing Information

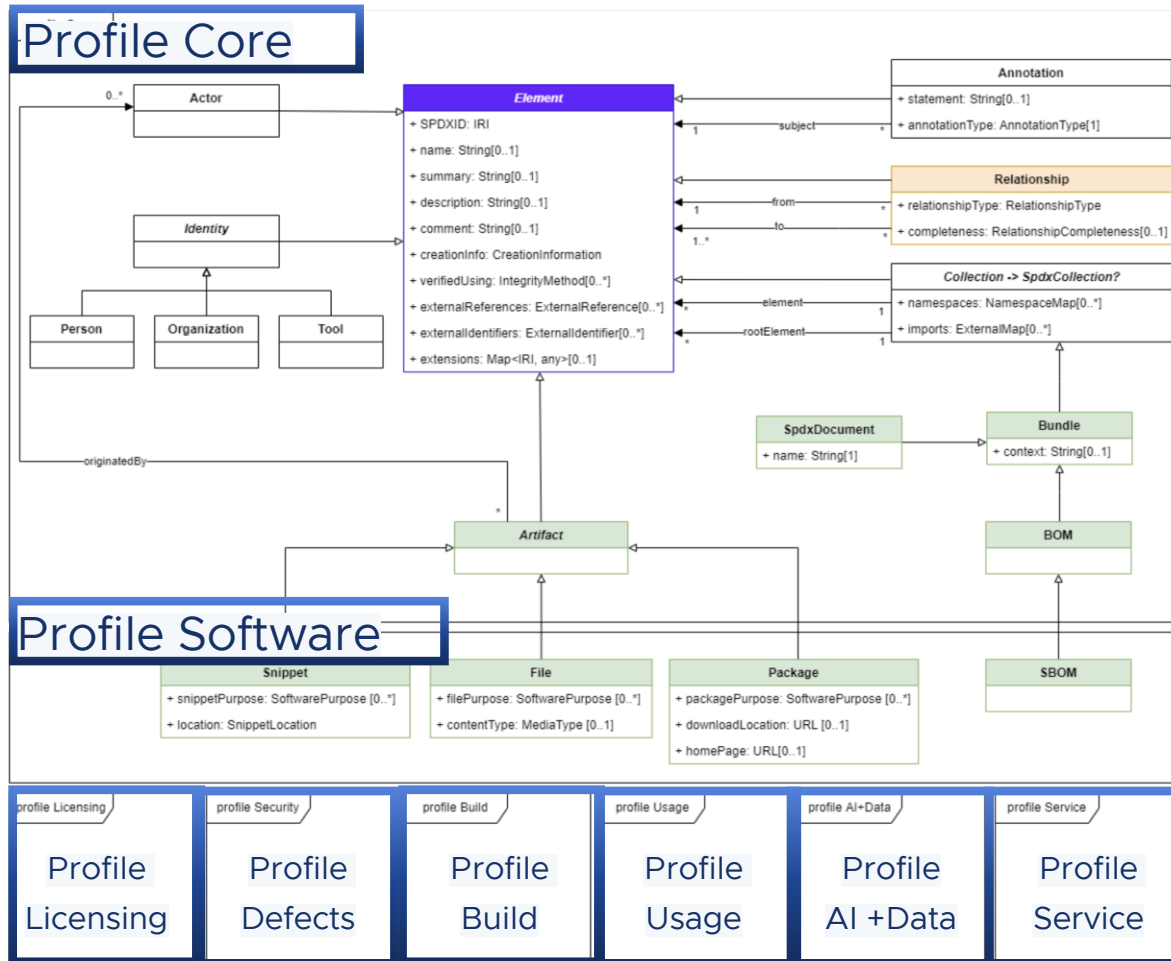
Relationships

Annotations



# The SBOM Community Standards

## The SPDX 3.0 Design

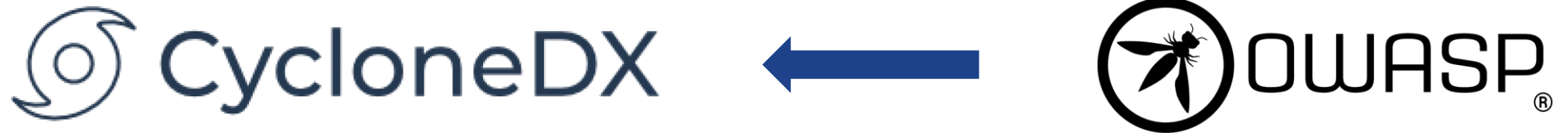


Redesigned into profiles

Profiles should be a valid SPDX SBOMs by themselves

# The SBOM Community Standards

CycloneDX



➤ CPE

➤ SWID

➤ PURL

# The SBOM Journey

SBOM Data

---



Standardized  
Formats

---



Tools

---



# The Landscape of Tools



SPDX Tools



OSS  
Review Toolkit



Salus

pkgconf bomtool

K8s BOM

# The Landscape of Tools



- Post-build
- Supports existing standards

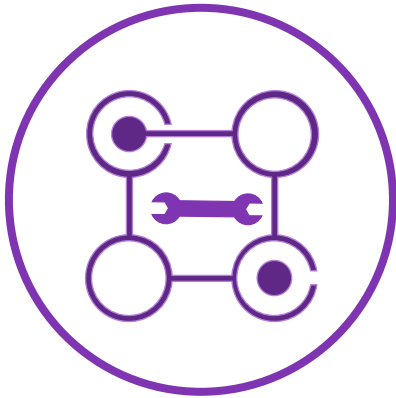


OSS  
**Review Toolkit**

SPDX Tools



# The Landscape of Tools



Salus



pkgconf  
bomtool



K8s BOM

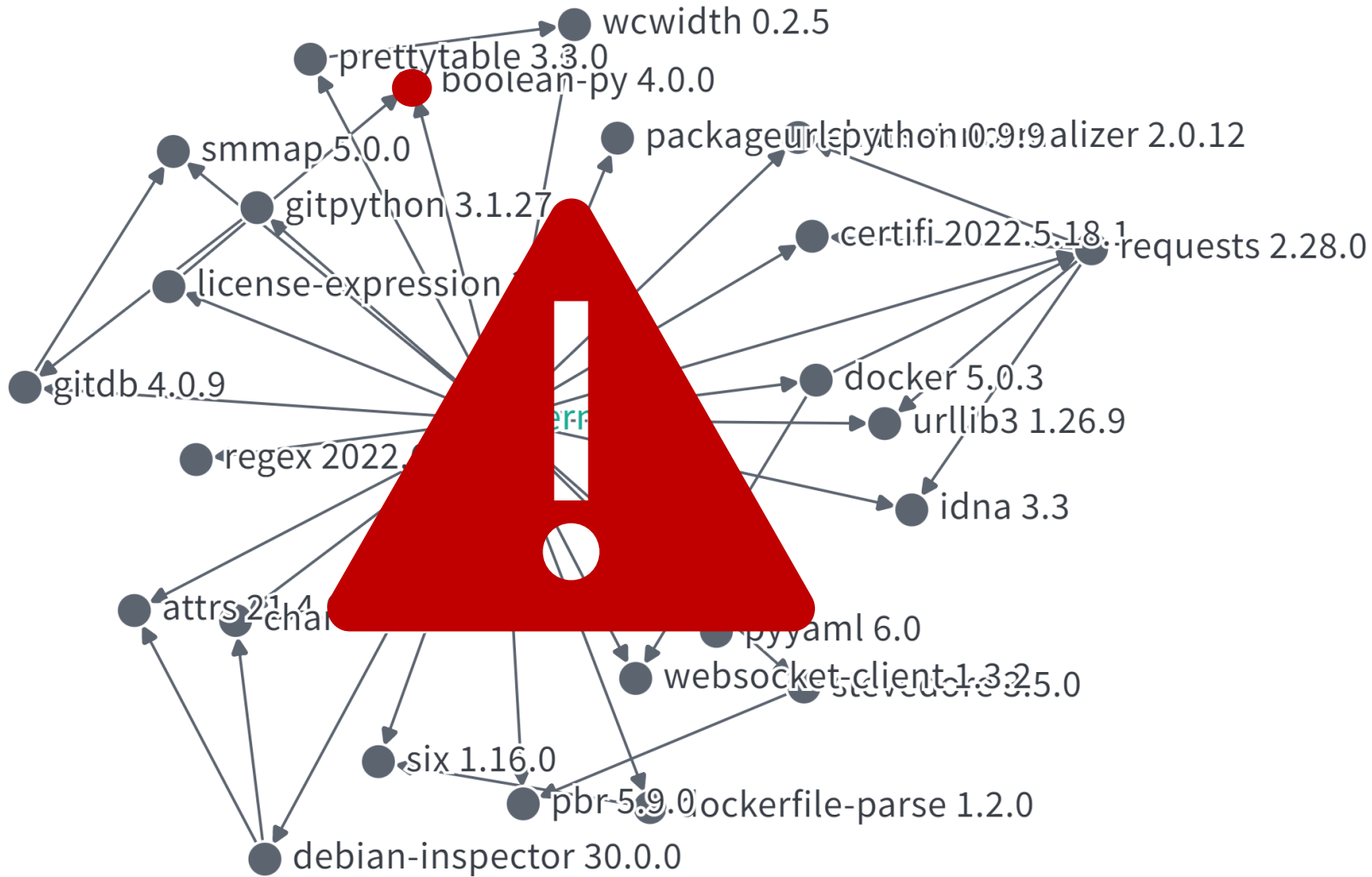


SPDX SBOM  
Generator

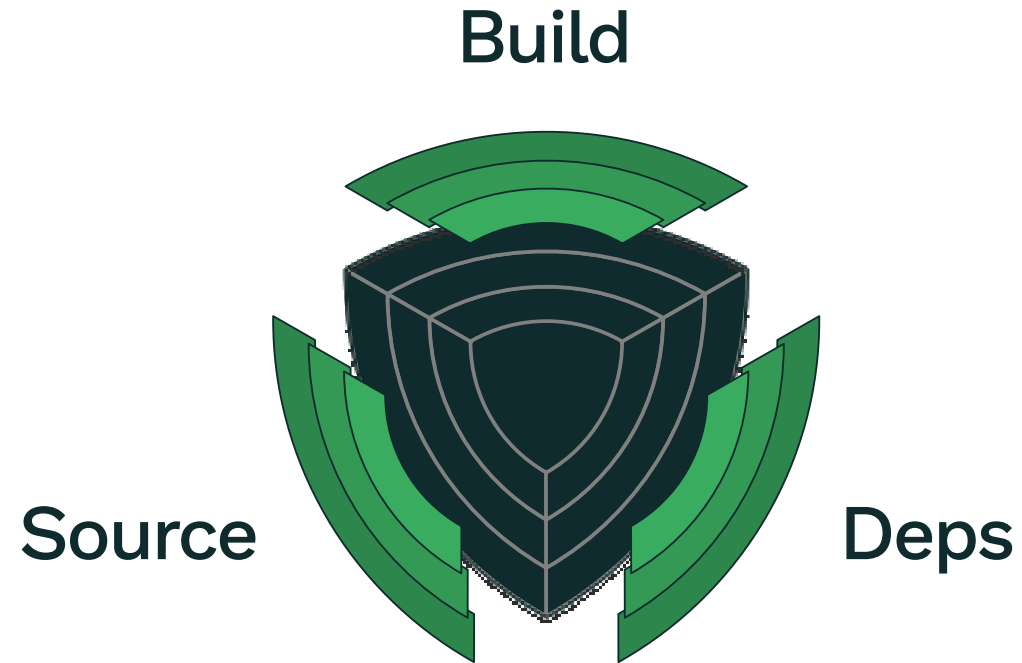


# The Landscape of Tools

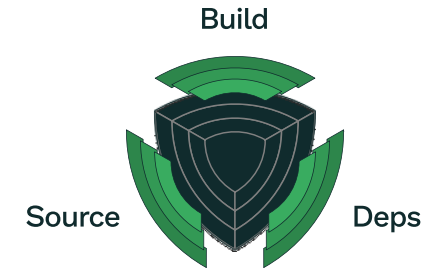




# Supply chain Levels for Software Artifacts (SLSA)



# Supply chain Levels for Software Artifacts (SLSA)



## Level 1

Easy to adopt, giving you supply chain visibility and being able to generate provenance



## Level 2

Starts to protect against software tampering and adds minimal build integrity guarantees



## Level 3

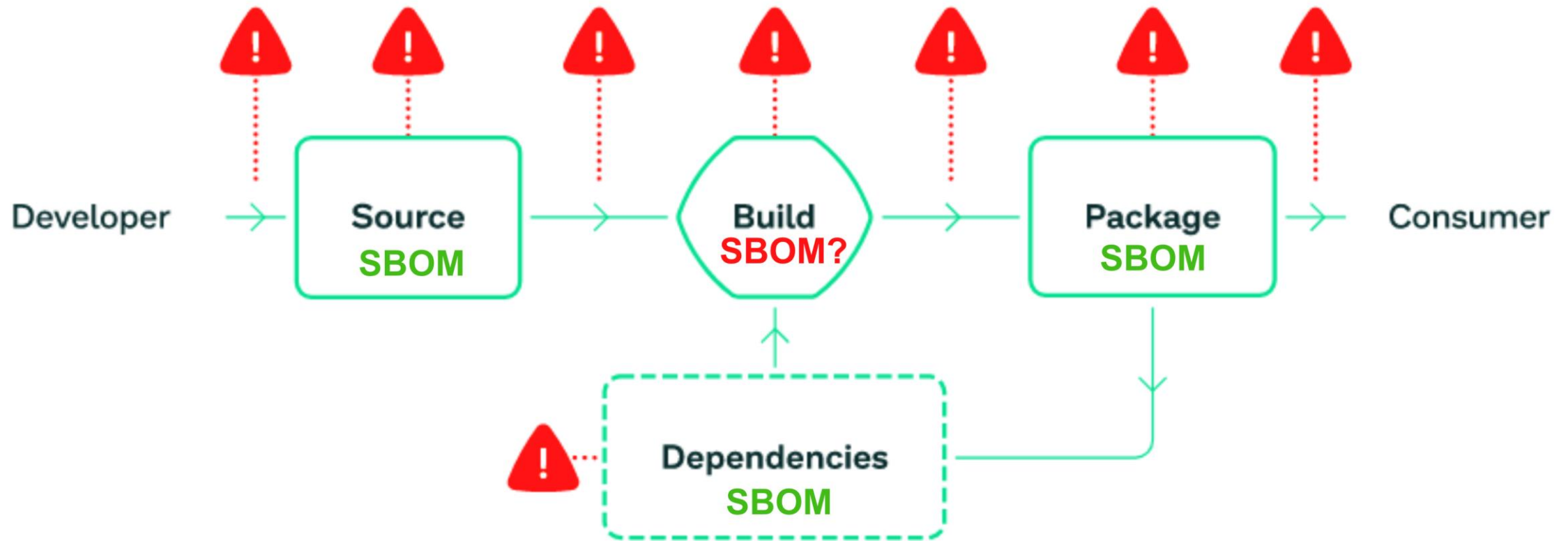
Hardens the infrastructure against attacks, more trust integrated into complex systems



## Level 4

The highest assurances of build integrity and measures for dependency management in place

# Supply chain Levels for Software Artifacts (SLSA)









# A composition of SBOMs



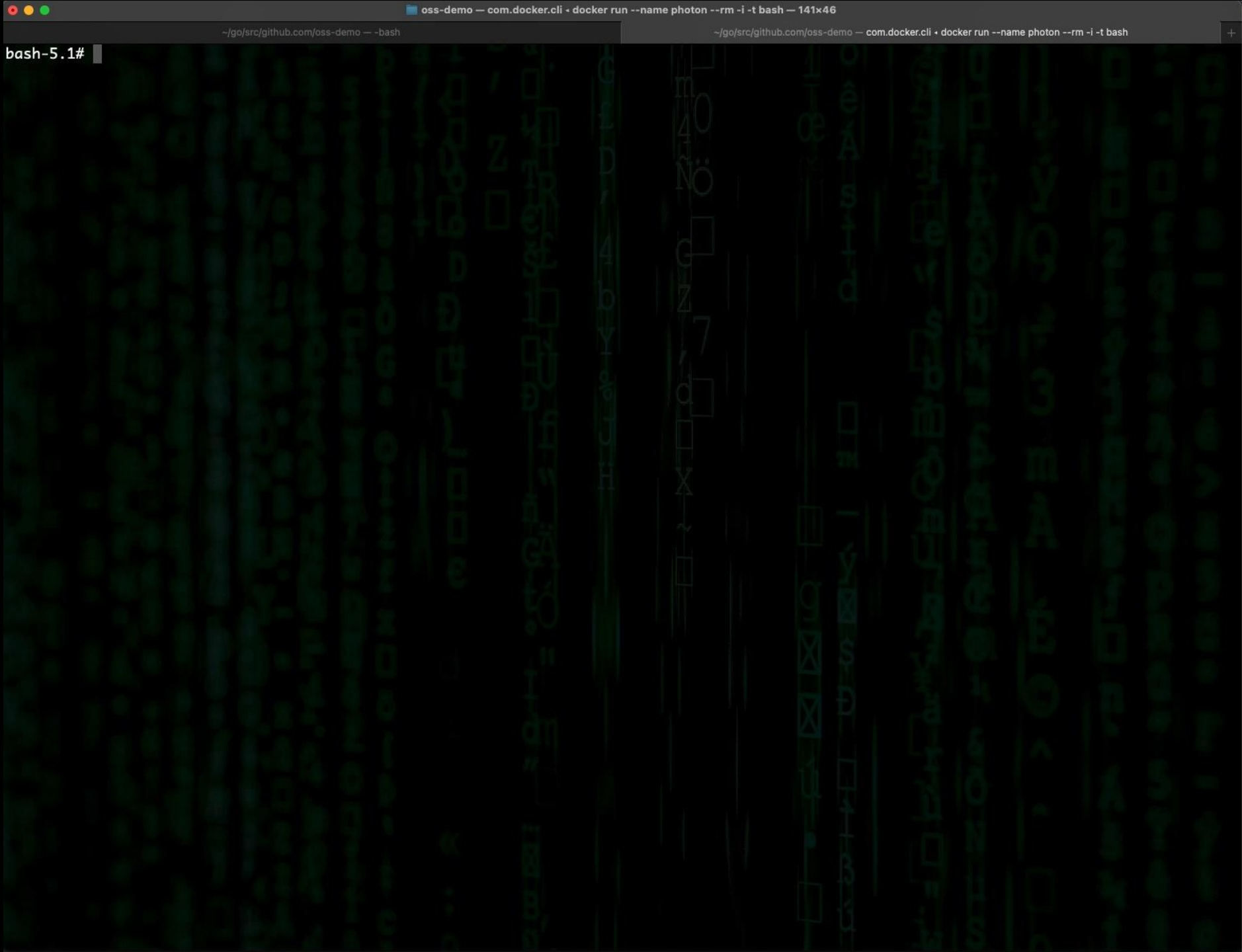
- ✓ Parsing the micro SBOMs
- ✓ Merging the parsed micro SBOMs
- ✓ Removing duplicates
- ✓ Updating relationships
- ✓ Constructing a fully functional SBOM



# DEMO



Photo by [Markus Spiske](#) on [Unsplash](#)



# Takeaways

## Technical challenges

---



## Get-together challenge

---





# Thank You



# Useful links

## ACT TAC

---

<https://automatecompliance.org>



<https://github.com/act-project/TAC>



## sbom-composer

---

<https://github.com/vmware-samples/sbom-composer>



## SPDX

---

<https://spdx.dev>



## Others

---

<https://slsa.dev>



<https://slsa.dev/blog/2022/05/slsa-sbom>



# Let's Keep in Touch

Ivana

---



Velichka

---

