

SBOMs for isar: An Update

Christoph Steiger
Siemens

About me



Christoph Steiger

- Software Engineer @Siemens FT
- Maintainer of debsbom



@Urist-McGit



christoph.steiger@siemens.com

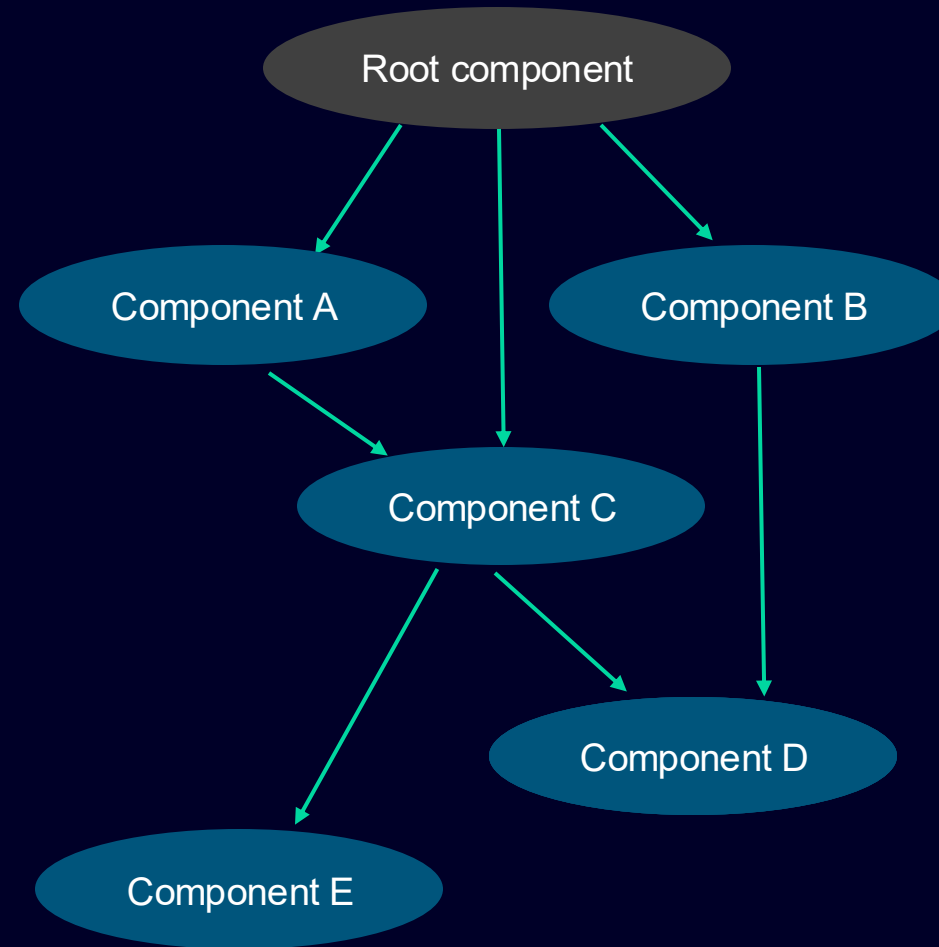
The Basics – What is an SBOM?

SBOMs (Software Bill of Material) is a **standardized file format** to exchange information about the components used in a software or system.

This information is needed for regulatory reasons, license clearing, and security (e.g., CVE tracking).

Commonly used formats are **SPDX** and **CycloneDX** (CDX).

Best represented as a **graph**.



```

{
  "SPDXID": "SPDXRef-DOCUMENT",
  "creationInfo": {
    "created": "2026-05-08T10:30:30Z",
    "creators": [
      "Tool: debsbom-0.7.2"
    ]
  },
  "dataLicense": "CC0-1.0",
  "name": "Debian",
  "spdxVersion": "SPDX-2.3",
  "documentNamespace": "https://spdx.org/spdxdocs/debsbom-0.7.2-06ac8894-1318-4744-9441-d392b5b64cc5",
  "packages": [
    {
      "SPDXID": "SPDXRef-dash-0.5.12-12-srcpkg",
      "copyrightText": "NOASSERTION",
      "downloadLocation": "NOASSERTION",
      "externalRefs": [
        {
          "referenceCategory": "PACKAGE_MANAGER",
          "referenceLocator": "pkg:deb/debian/dash@0.5.12-12?arch=source",
          "referenceType": "purl"
        }
      ],
      "filesAnalyzed": false,
      "licenseConcluded": "NOASSERTION",
      "licenseDeclared": "NOASSERTION",
      "name": "dash",
      "primaryPackagePurpose": "SOURCE",
      "summary": "Debian source code package 'dash'",
      "supplier": "Person: Andrej Shadura (andrewsh@debian.org)",
      "versionInfo": "0.5.12-12"
    }
  ]
}

```

debsbom – Design Principles

We do not guess

Package identification with PURLs

Checksums as identity proof

Focus on real world use-cases: license clearing and cybersecurity workflows

Implementation – Data Sources

Required:

- Installed packages and their relationships from dpkg status file

Optional:

- Apt repository metadata for packages (resides in */var/lib/apt/lists/*)
- Auto install information from *extended_states* file
- Apt binary package archive cache (in */var/cache/apt/archives*)
- Copyright information for licenses

All of the data sources are available in a standard isar build

Implementation – Modelling Package Metadata

```
Package: apt
Status: install ok installed
Priority: required
Section: admin
Maintainer: APT Development Team <deity@lists.debian.org>
Architecture: amd64
Version: 3.0.3
Replaces: apt-transport-https (< 1.5~alpha4~), apt-utils (< 1.3~exp2~)
Provides: apt-transport-https (= 3.0.3)
Depends: base-passwd (>= 3.6.1) | adduser, sqv (>= 1.3.0), libapt-pkg7.0 (>= 3.0.3),
        debian-archive-keyring, libc6 (>= 2.38), libgcc-s1 (>= 3.0),
        libseccomp2 (>= 2.4.2), libssl3t64 (>= 3.0.0), libstdc++6 (>= 13.1), libsystemd0
Recommends: ca-certificates
Suggests: apt-doc, aptitude | synaptic | wajig, dpkg-dev (>= 1.17.2),
        gnupg | gnupg2 | gnupg1, powermgmt-base
Description: commandline package manager
[...]
```

Exact mappings for both SBOM formats can be found in our documentation [1].

```
{
  "SPDXID": "SPDXRef-apt-amd64",
  "copyrightText": "NOASSERTION",
  "downloadLocation": "NOASSERTION",
  "externalRefs": [
    {
      "referenceCategory": "PACKAGE_MANAGER",
      "referenceLocator": "pkg:deb/debian/apt@3.0.3?arch=amd64",
      "referenceType": "purl"
    }
  ],
  "filesAnalyzed": false,
  "licenseConcluded": "NOASSERTION",
  "licenseDeclared": "NOASSERTION",
  "name": "apt",
  "primaryPackagePurpose": "LIBRARY",
  "summary": "commandline package manager",
  "supplier": "Organization: APT Development Team (deity@lists.debian.org)",
  "versionInfo": "3.0.3"
},
```

[1] <https://siemens.github.io/debsbom/design-decisions.html#mapping-of-debian-binary-packages-to-sbom-packages-components>

Implementation – Modelling Package Metadata

- Debian provides copyright files in `/usr/share/doc/*/copyright`
- For both SBOM formats SPDX license identifiers are expected [1]
- Problematic are obscure licenses and *public-domain* licensing
- Works for about 50% of packages.

```
Format: https://www.debian.org/doc/packaging-manuals/copyright-format/1.0/
Upstream-Name: apt
Upstream-Contact: APT Development Team <deity@lists.debian.org>
Source: https://salsa.debian.org/apt-team/apt
[...]
Files: *
Copyright: 1997-1999 Jason Gunthorpe and others
          2018, 2019 Canonical Ltd
          [...]
          2014 Anthony Towns
License: GPL-2+

Files: methods/connect.c
Copyright: Copyright (c) 1996 - 2023, Daniel Stenberg, <daniel@haxx.se>, and many
License: GPL-2+ and curl

Files: CMake/FindBerkeley.cmake
Copyright: 2006, Alexander Dymo, <adymo@kdevelop.org>
          2016, Julian Andres Klode <jak@debian.org>
License: BSD-3-clause
Redistribution and use in source and binary forms, with or without
[...]

Files: CMake/Documentation.cmake
       CMake/FindLFS.cmake
Copyright: 2016 Julian Andres Klode <jak@debian.org>
License: Expat
Permission is hereby granted, free of charge, to any person
[...]
```

```
{
  "SPDXID": "SPDXRef-apt-2.6.1-srcpkg",
  "copyrightText": "NOASSERTION",
  "downloadLocation": "NOASSERTION",
  "externalRefs": [
    {
      "referenceCategory": "PACKAGE_MANAGER",
      "referenceLocator": "pkg:deb/debian/apt@2.6.1?arch=source",
      "referenceType": "purl"
    }
  ],
  "filesAnalyzed": false,
  "licenseConcluded": "NOASSERTION",
  "licenseDeclared": "BSD-3-Clause AND GPL-2.0-or-later AND MIT",
  "name": "apt",
  "primaryPackagePurpose": "SOURCE",
  "summary": "Debian source code package 'apt'",
  "supplier": "Organization: APT Development Team (deity@lists.debian.org)",
  "versionInfo": "2.6.1"
}
```

[1] <https://spdx.org/licenses/>

Package Identification

- Debian packages can be identified by their (*name, version, architecture*) tuple. This can be encoded in a PackageURL (PURL):

pkg:deb/debian/apt@3.0.3?arch=amd64&distro=trixie

- The *arch* qualifier can also be *source* for a Source package.
- With this PURL it is possible to retrieve the correct package from s.d.o.
- For some packages the source distribution is also important (e.g. *trixie* vs *trixie-security*); encoded in the *distro* qualifier
- For isar we provide the *isar* distro e.g: *pkg:deb/debian/hello-isar@0.5-b48d156?arch=amd64&distro=isar*

But: it is never possible to know if you actually have the correct package. Checksums are the only way to guarantee that

Implementation – Modelling Package Relationships

Important Relationship Types:

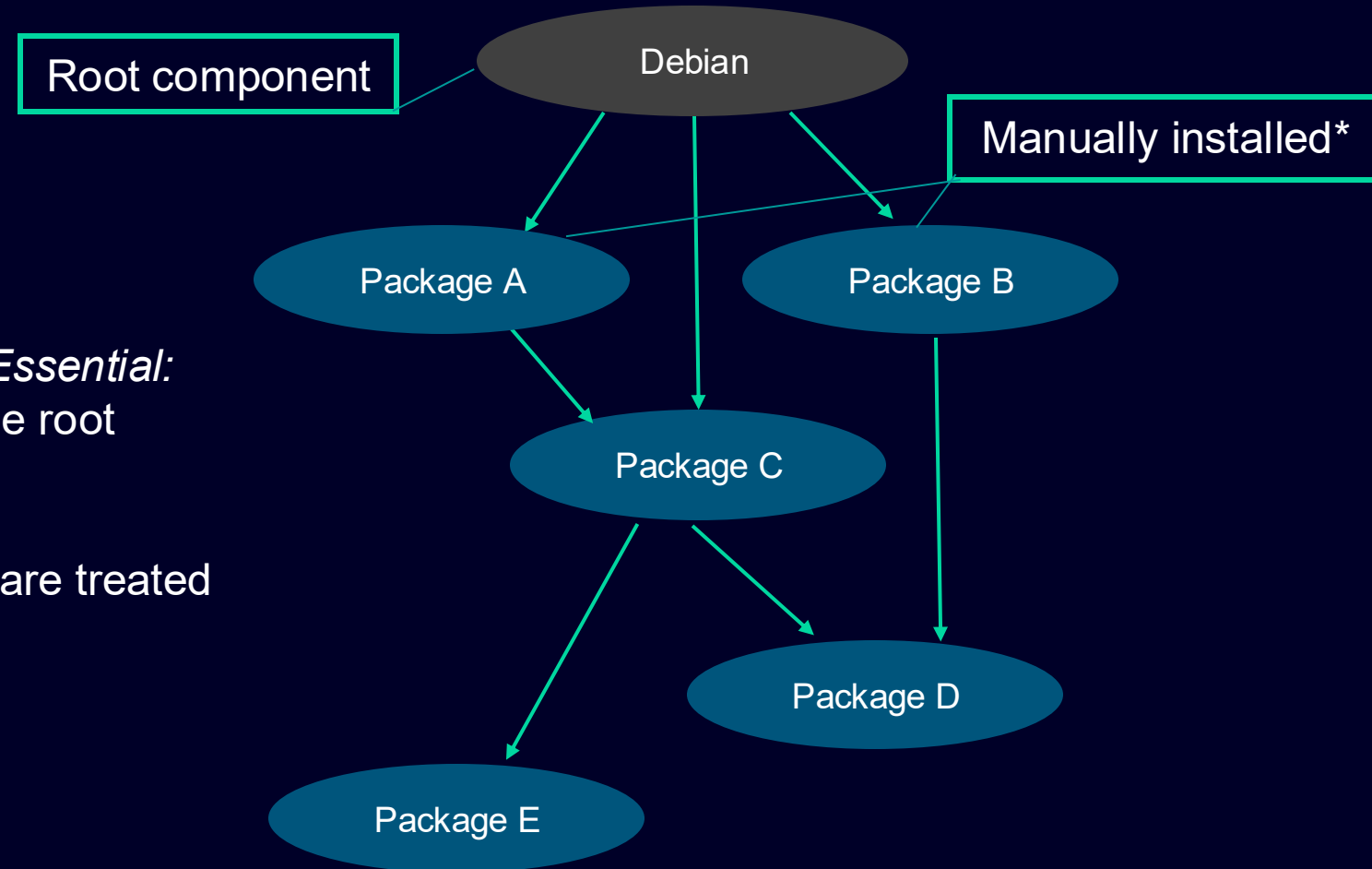
- Binary Dependencies (*Depends*)
- Source Dependencies (*Source*)
- Built-Using Dependencies (*Built-Using*, *Static-Built-Using*)
- Recommended Packages (*Recommends*)
- Suggested Packages (*Suggests*)

```
Package: apt
Status: install ok installed
Priority: required
Section: admin
Maintainer: APT Development Team <deity@lists.debian.org>
Architecture: amd64
Version: 3.0.3
Replaces: apt-transport-https (<< 1.5~alpha4~), apt-utils (<< 1.3~exp2~)
Provides: apt-transport-https (= 3.0.3)
Depends: base-passwd (>= 3.6.1) | adduser, sqv (>= 1.3.0), libapt-pkg7.0 (>= 3.0.3),
        debian-archive-keyring, libc6 (>= 2.38), libgcc-s1 (>= 3.0),
        libseccomp2 (>= 2.4.2), libssl3t64 (>= 3.0.0), libstdc++6 (>= 13.1), libsystemd0
Recommends: ca-certificates
Suggests: apt-doc, aptitude | synaptic | wajig, dpkg-dev (>= 1.17.2),
        gnupg | gnupg2 | gnupg1, powermgmt-base
Description: commandline package manager
[...]
```

The different package relationships cannot be completely expressed in current CycloneDX SBOMs, but SPDX allows us to differentiate all of them.

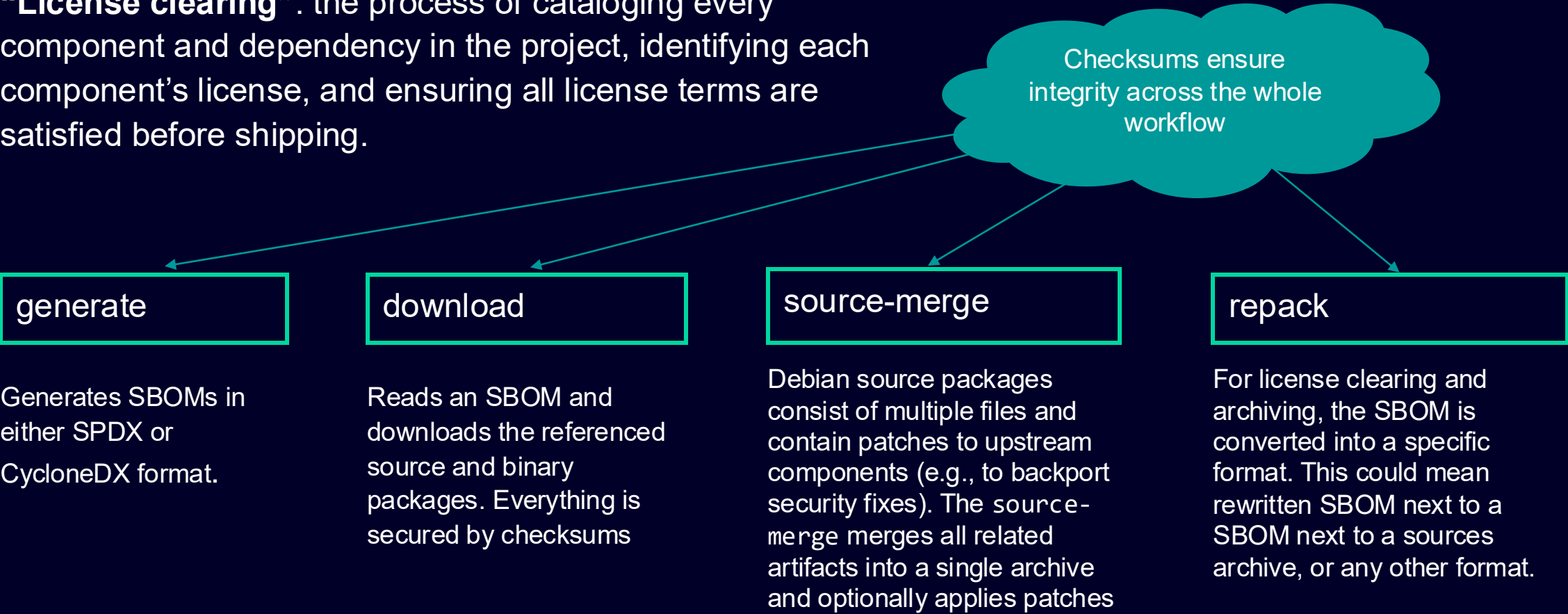
Implementation – Modelling Package Relationships

- Manually installed, *Priority: required* and *Essential: yes* packages are placed directly below the root component
- Recommended and suggested packages are treated as any other dependency.



Using debsbom for license clearing

“**License clearing**”: the process of cataloging every component and dependency in the project, identifying each component’s license, and ensuring all license terms are satisfied before shipping.



Examples

Recap: License Clearing

Generate SBOM (included in isar):

```
debsbom generate -r /path/to/the/rootfs -t cdx -o sbom.cdx.json
```

Download all source packages:

```
debsbom download --sources sbom.cdx.json
```

Merge all files of a source package into a single tarball:

```
debsbom source-merge --apply-patches sbom.cdx.json
```

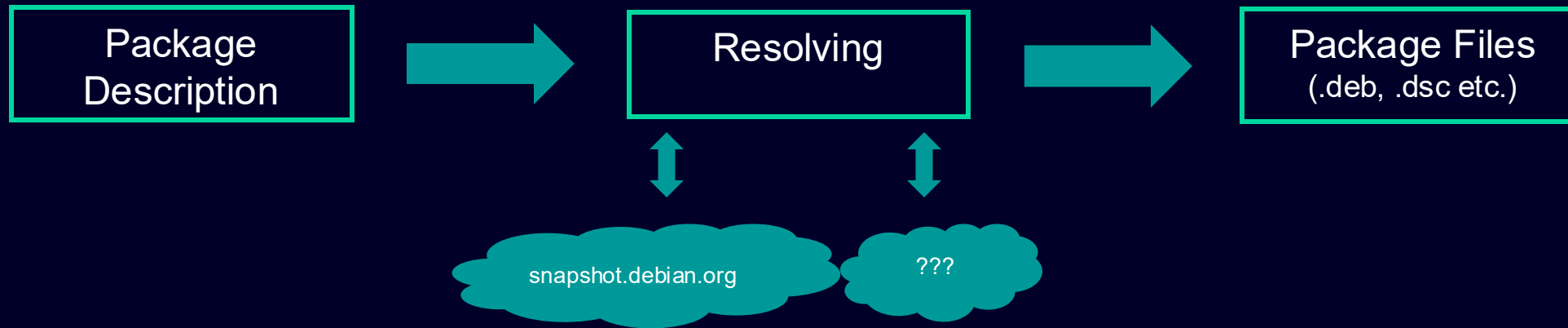
Repack it into the Siemens Standard BOM format:

```
debsbom repack --format siemens-standard-bom sbom.cdx.json sbom.packed.cdx.json
```

More examples: <https://siemes.github.io/debsbom/examples.html>

Pluggable Resolvers

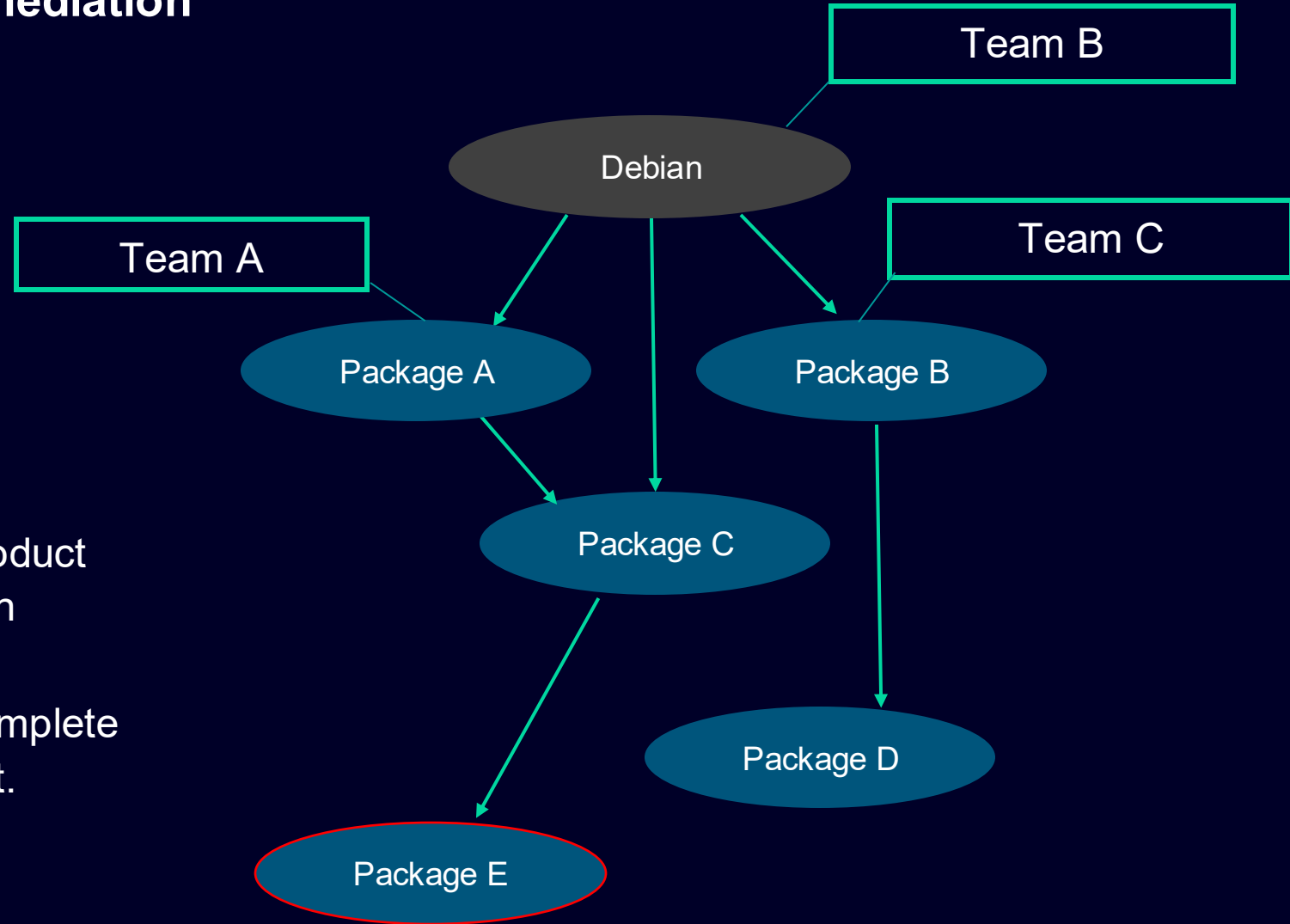
... or where to find Debian Packages



- debsbom supports resolving with the s.d.o out of the box
- Resolving is use-case specific: custom package repositories, Artifactory etc.
- debsbom provides plugin infrastructure to implement custom resolvers
- For isar: local apt repository and Debian snapshot mirror for everything else

Using debsbom for Vulnerability Remediation

- Common project structure: multiple teams working on various parts of a Debian-based distribution
- Assessment if a vulnerability affects a product needs to be done by the team that pulls in the vulnerable package
- Identification of that team requires the complete dependency graph as debsbom models it.



Using debsbom for Vulnerability Remediation

generate

Generates SBOMs in either SPDX or CycloneDX format.

sec-scan

Queries the DST for vulnerable packages in an SBOM. Outputs the results in standard formats like VEX or SARIF.

trace-path

Identify why vulnerable packages were pulled into the system and find the package maintainers.

Examples

Recap: Vulnerability Remediation

Generate SBOM (included in isar):

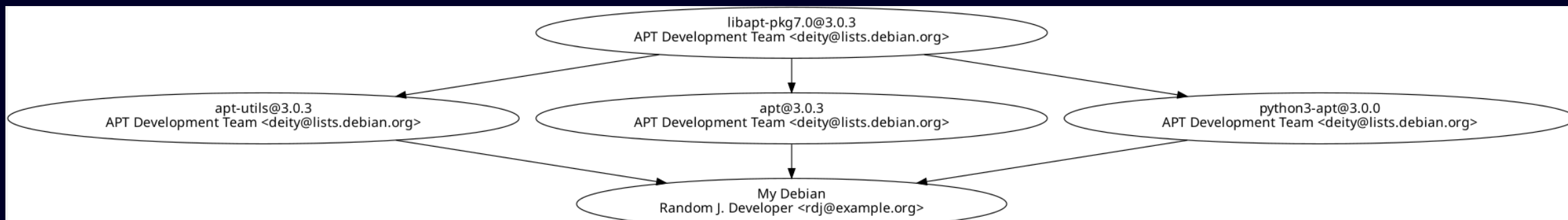
```
debsbom generate -r /path/to/the/rootfs -t cdx -o sbom.cdx.json
```

Query the DST for vulnerabilities:

```
debsbom sec-scan sbom.cdx.json
```

Identify who pulled in a vulnerable package:

```
debsbom trace-path --mode all-shortest --format dot sbom.spdx.json <PURL>
```



More examples: <https://siemens.github.io/debsbom/examples.html>

Future Topics

- Compliance with NIST/BSI guidelines
- Online Package Enrichment
- SPDX 3.x support

You have more topics? Let us know!

Siemens AG

Christoph Steiger
christoph.Steiger@siemens.com



[siemens / debsbom](#)