SIEMENS Healthineers

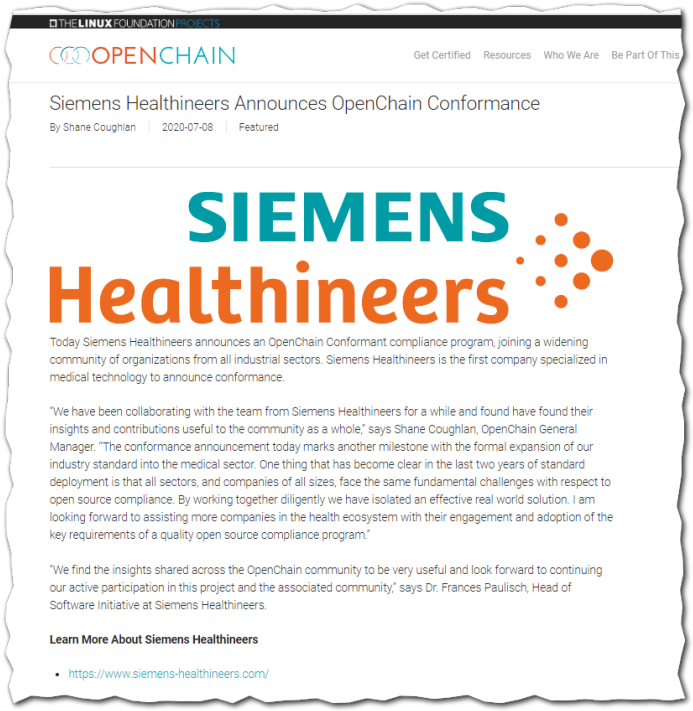
Open Source Approaches for Open Source License Compliance

Presentation at Open Source @ 西门子 2024

Frances Paulisch (with special thanks to Arun Azhakesan)
Siemens Healthineers AG

Nov. 28, 2024

OpenChain - ISO/IEC 5230 Conformant Program



THE LINUX FOUNDATION PROJECTS

OPENCHAIN

Get Certified Resources Who We Are Be Part Of This

Siemens Healthineers Announces OpenChain Conformance

By Shane Coughlan | 2020-07-08 | Featured

SIEMENS Healthineers

Today Siemens Healthineers announces an OpenChain Conformant compliance program, joining a widening community of organizations from all industrial sectors. Siemens Healthineers is the first company specialized in medical technology to announce conformance.

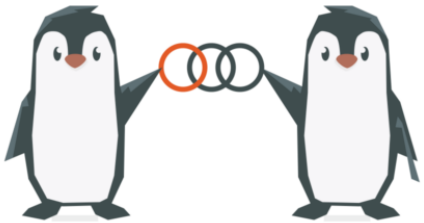
"We have been collaborating with the team from Siemens Healthineers for a while and found have found their insights and contributions useful to the community as a whole," says Shane Coughlan, OpenChain General Manager. "The conformance announcement today marks another milestone with the formal expansion of our industry standard into the medical sector. One thing that has become clear in the last two years of standard deployment is that all sectors, and companies of all sizes, face the same fundamental challenges with respect to open source compliance. By working together diligently we have isolated an effective real world solution. I am looking forward to assisting more companies in the health ecosystem with their engagement and adoption of the key requirements of a quality open source compliance program."

"We find the insights shared across the OpenChain community to be very useful and look forward to continuing our active participation in this project and the associated community," says Dr. Frances Paulisch, Head of Software Initiative at Siemens Healthineers.

Learn More About Siemens Healthineers

- https://www.siemens-healthineers.com/

https://www.openchainproject.org/community-of-conformance



COMMUNITY
OF
CONFORMANCE

Frances Paulisch

Open Source tools for License Compliance

SIEMENS Healthineers

Source Code Scanning Application:

Component Catalog Application:

See also interesting related link SCA the FOSS Way – Part 1: Software Composition Analysis - nexB

Frances Paulisch

The letter “F” in “Compliance” is for “Fun”

With special thanks to Philippe Ombredanne for re-use.

What is SW360?

SIEMENS Healthineers

SW360 is an open-source software project licensed under the EPL-2.0 that provides both a web application and a repository to collect, organize and make available information about software components. It establishes a central hub for software components in an organization.

SW360 allows for:

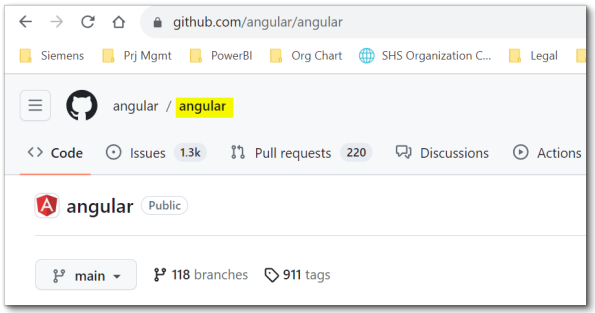
- Import & Export of SBOM-related information
- tracking components used by a project/product
- integrating security vulnerability tools
- maintaining license obligations
- enforcing policies and
- generating legal documents.

Frances Paulisch

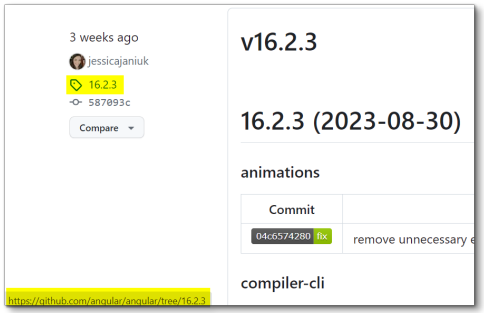
SW360 – Recent improvements

- Features support for SBOM (Software Bill of Materials) Management
  - Capabilities include import, export, and view functions for SPDX and Cyclone DX
- Supports installation via Docker-Compose
- (ongoing) Transitioning to a new GUI (Graphical User Interface) framework
- Package Portlet – a new option for modelling packages as “first class citizens” (in addition to components and releases). This establishes the connection between binary package and the corresponding source repository and enables more efficient clearing by clearing the source code one time.

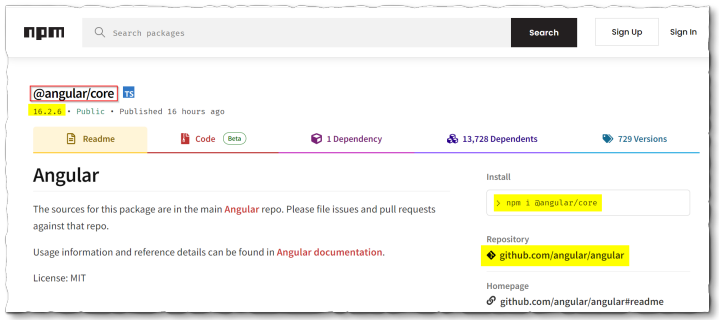
Component



Release

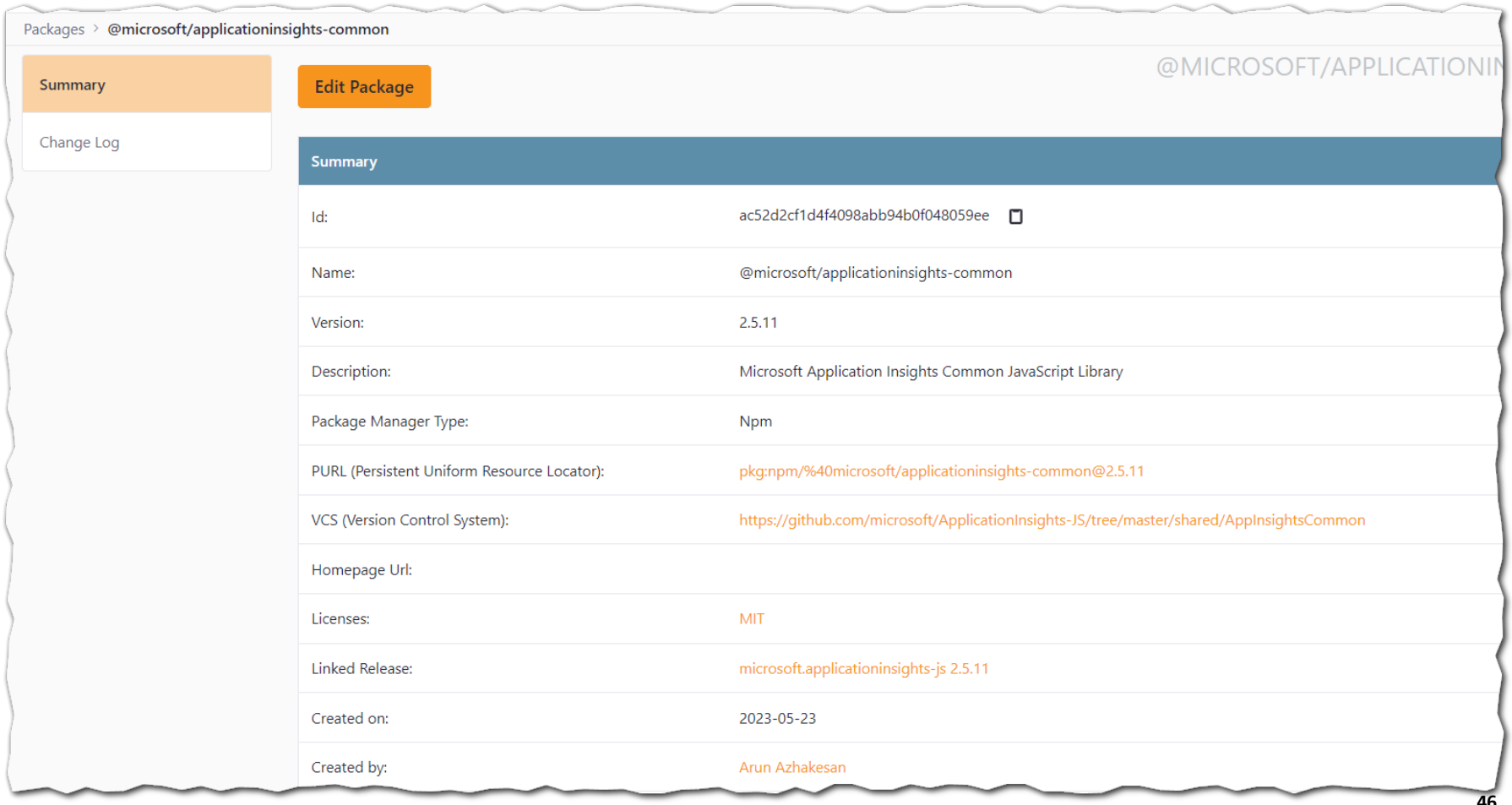


Package



Frances Paulisch

Package details page (example)



Frances Paulisch

What is a Software Bill of Material (SBOM) – Overview

SIEMENS Healthineers

Key Points

- Similar to “bill of material” in other areas
- An overview of all the software packages and components used in the product, with provenance information and (optionally) licensing
- Able to accompany distribution or deployment
- Various requirements to provide e.g. various government and regulatory authorities
- SBOM standards now more complex with rapid expansion of types and purposes

Formats for SBOMs

- SPDX
- CycloneDX
- SWID

Minimum elements of an SBOM

- Per component
  - Supplier Name
  - Component Name
  - Version of the Component
  - Other Unique Identifiers
  - Dependency Relationship
  - Author of SBOM Data
  - Timestamp
- Information about component completeness
- Information about frequency

Further characteristics

- Machine readable
- Association between components (e.g. “includes”)
- Handling of missing or non-applicable data
- Plus further information about the processes, tools, etc.

Frances Paulisch

“The 'SB' in SBOM does not stand for Silver Bullet”

– Allan Friedman, Cybersecurity and Infrastructure Security Agency (CISA, USA)

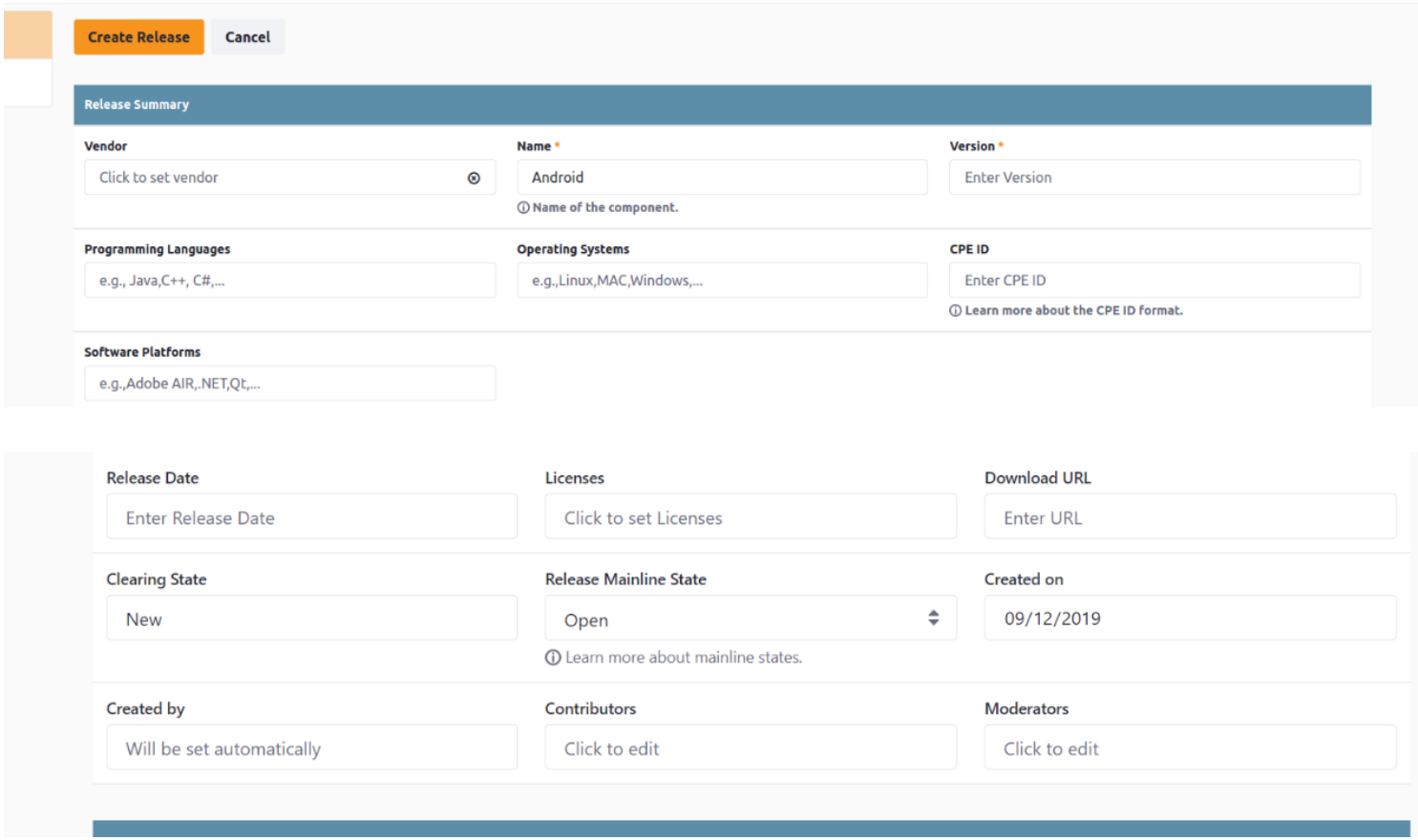
bullet image: http://pngimg.com/image/35567 license: CC-BY-NC-4.0 https://pngimg.com/license

(Again) with special thanks to Philippe Ombredanne for re-use.

Example of SW360's registration Items for software components

SIEMENS Healthineers

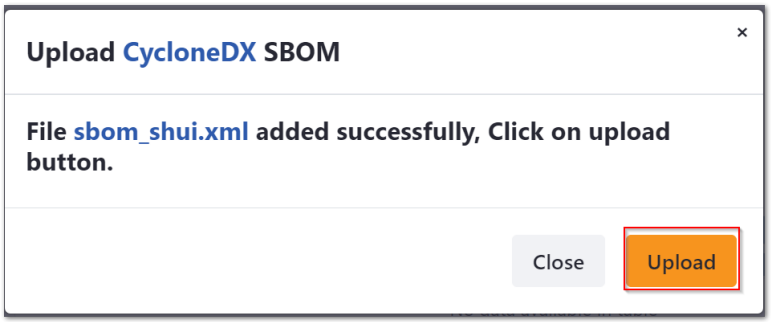
- Component Name
- Categories
- Component Type
- Languages
- Software Platforms
- Operating System
- Vendors
- Main Licenses
- Programming Languages
- Operating Systems
- CPE ID
- Software Platforms
- Release Date
- Download URL

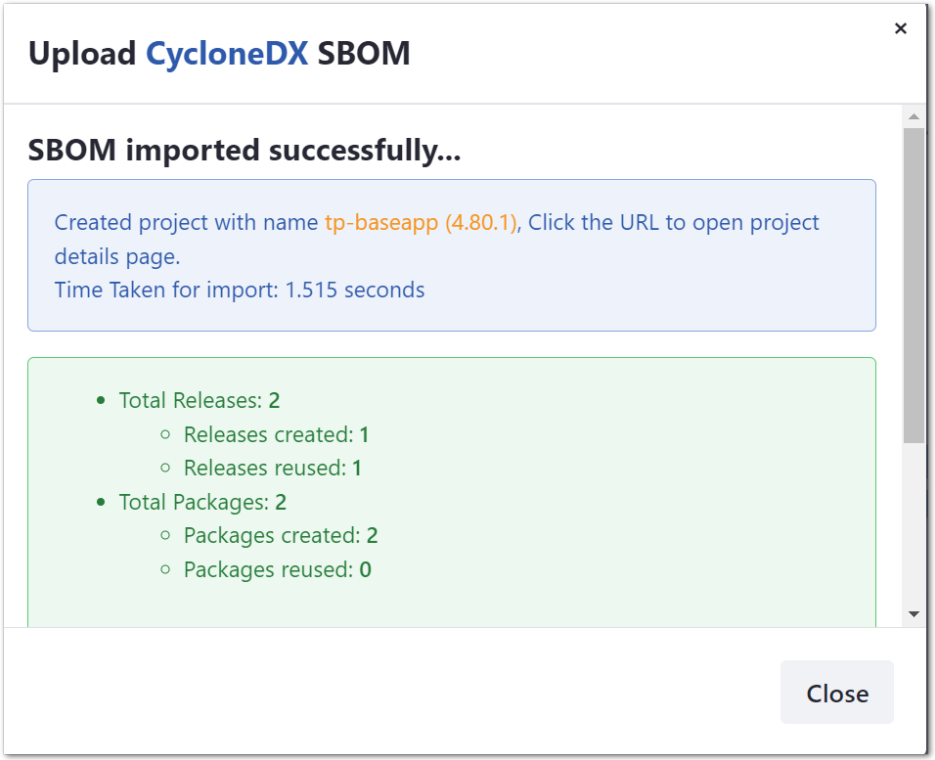


You can centralize and register SBOM-related data both through GUI and API

Importing a Cyclone DX SBOM

- Once the selected SBOM is added successfully, Click **Upload**.
- The status of successful SBOM import is displayed along with following details:
  - Time taken for import
  - Count of Releases and Packages created



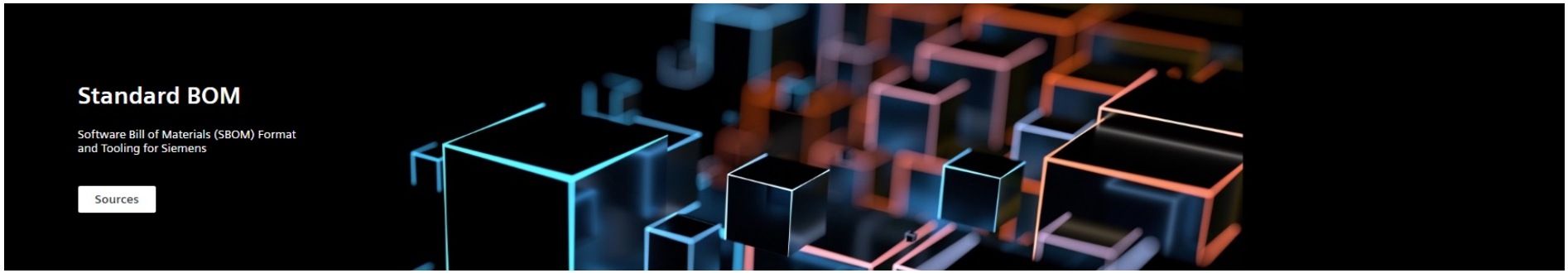


Frances Paulisch

Standard SBOM Format at Siemens and Siemens Healthineers

The Siemens Standard SBOM is a standardized SBOM format with tooling for Siemens and Siemens Healthineers.

You can read information on the format here: https://sbom.siemens.io



Standard BOM

Table of contents

- Use Cases
- Status

A standardized description of a Software Bill of Materials (SBOM), plus some tooling for generation and consumption of *standard-bom* SBOMs.

Standard BOM is:

- a subset of CycloneDX
- programming language agnostic
- independent of the source ecosystem (Java, .NET, Python, TypeScript, ...)
- independent of its consumers, although an SBOM can be tailored towards a specific use case

Frances Paulisch

Closing Thoughts

SIEMENS Healthineers

- The license clearing and cybersecurity communities are distinct, but they have increasingly common interests.
- Many tools e.g. Software Composition Analysis (SCA) tools, tend to focus on either vulnerabilities OR licensing
- Open Source tools and the Open Source community offer advantages and we expect this to lead to an improved common understanding across these two disciplines and across the global software community.

Frances Paulisch