OpenChain Tooling Work Group - Overview

Introduction

Open Source Tooling Group

- Reducing resource costs and improving the quality of results
- Uses open source principles to accomplish the objective
- A meritocracy producing real world solutions for real world challenges and it shares results to all interested parties.

THE LINUX FOUNDATION PROJECTS

OPENCHAIN

About Get Started Translations Resources Partners

OpenChain Launches Tooling Work Group

By Shane Coughlan | July 25, 2019 | News

Today the OpenChain Project announces the launch of our global Tooling Work Group. This work group, chaired by Oliver Fendt of Siemens, will see contributors from Siemens, Bosch, Toshiba, Fujitsu, Hitachi and many other companies accelerate collaboration around open source tooling for open source compliance.

Oliver Fendt, Siemens

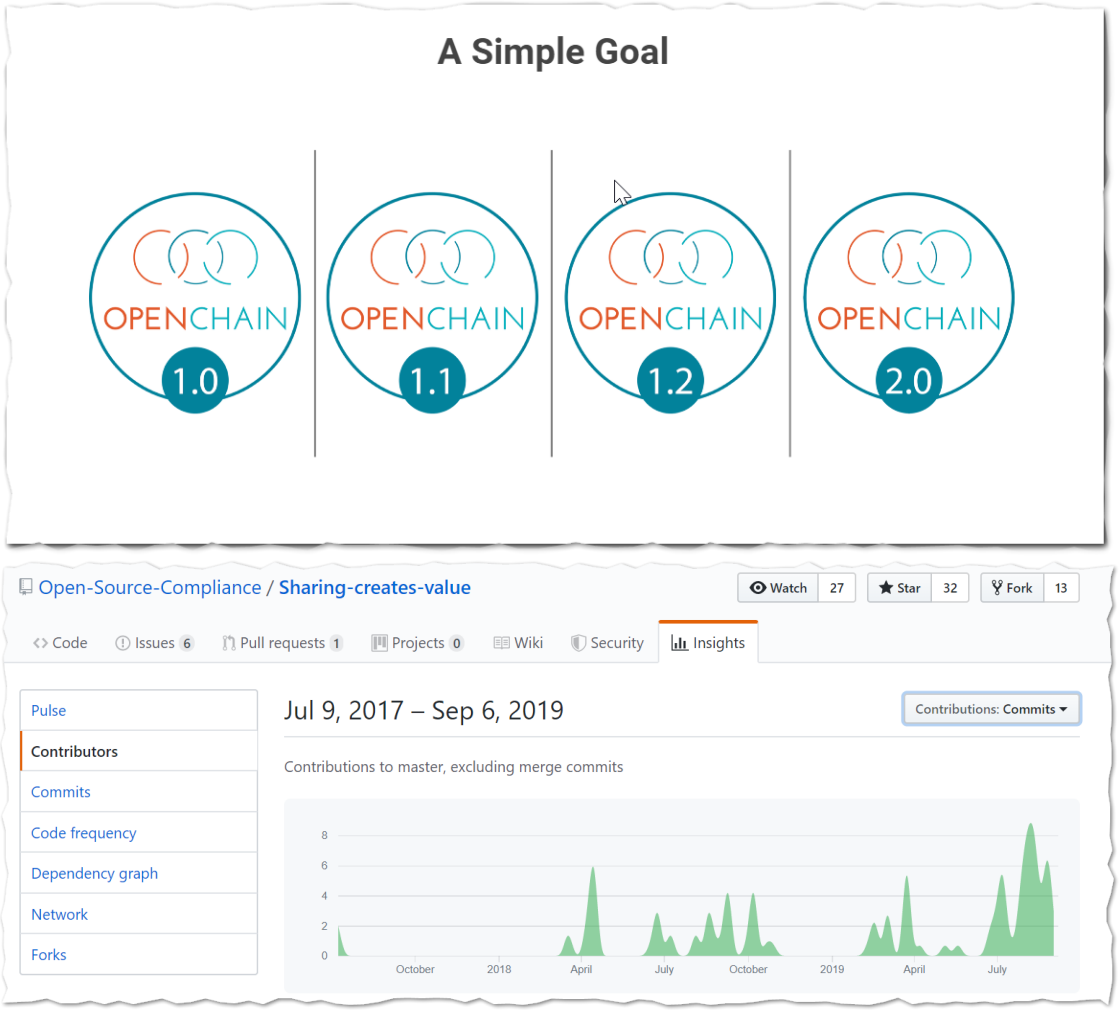
This work group is focused on reducing resource costs and improving the quality of results around open source compliance activities. We use open source principles to accomplish this, creating a meritocracy producing real world solutions for real world challenges, and sharing these results with all interested parties.

1. We are making turn-key Open Source tooling for Open Source Compliance
2. We are considering what open data database(s) can support this
3. We plan to work with existing projects to make this happen (FOSSology, Software Heritage, SPDX, sw360

Hierarchy

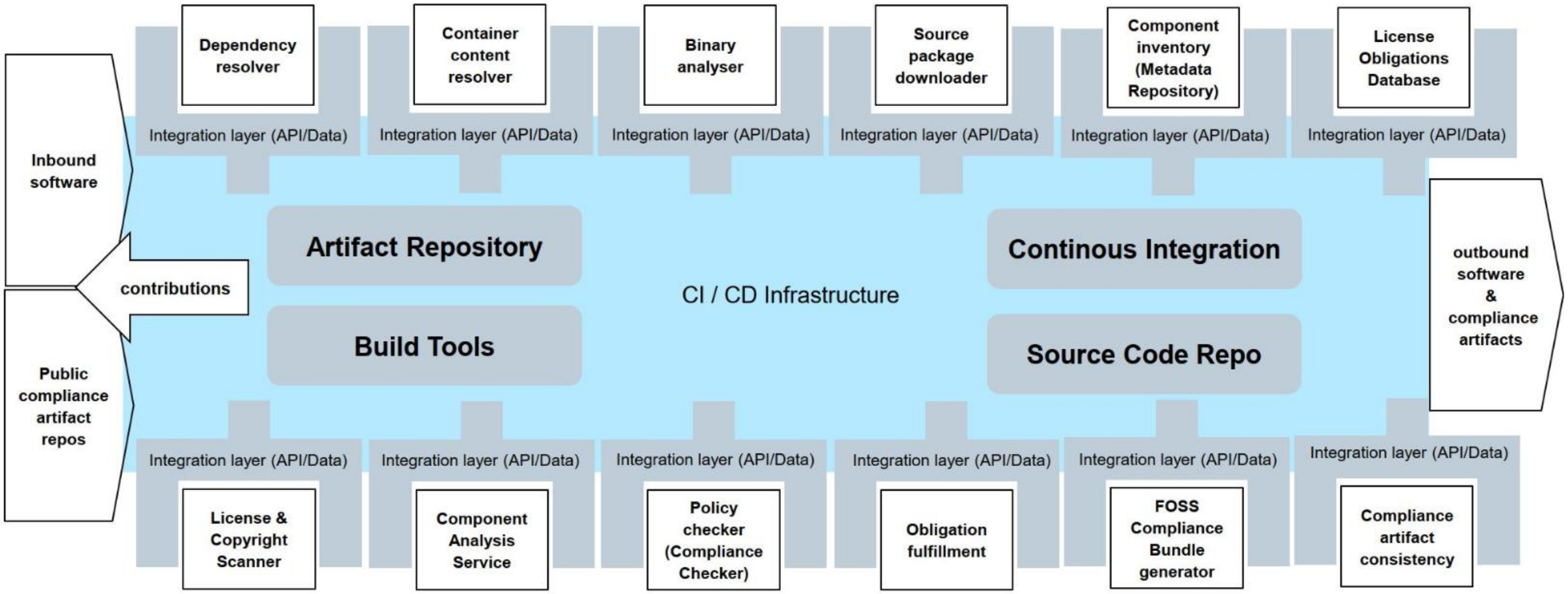
Open Source Tooling Group

- The OpenChain Project maintains the standard for open source compliance in the supply chain.
- The OpenChain Project has various Work Groups where volunteers work on specific compliance challenges.
- We use the Sharing Creates Value GitHub Repository and OSS Compliance Tooling mailing list.



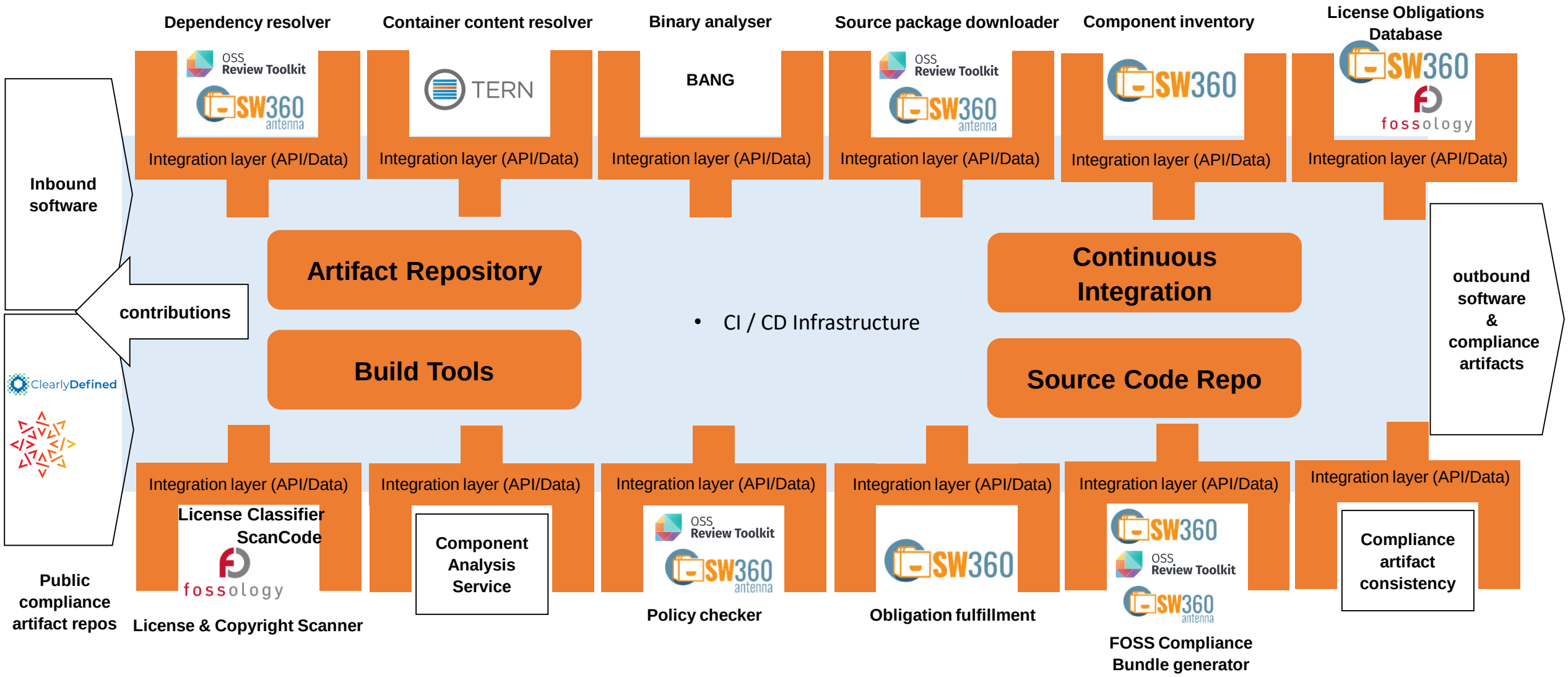
Big Picture – Integrated Compliance Toolchain Instance

Open Source Tooling Group



License: CC-BY-SA-4.0

Big Picture – Integrated Compliance Toolchain Instance

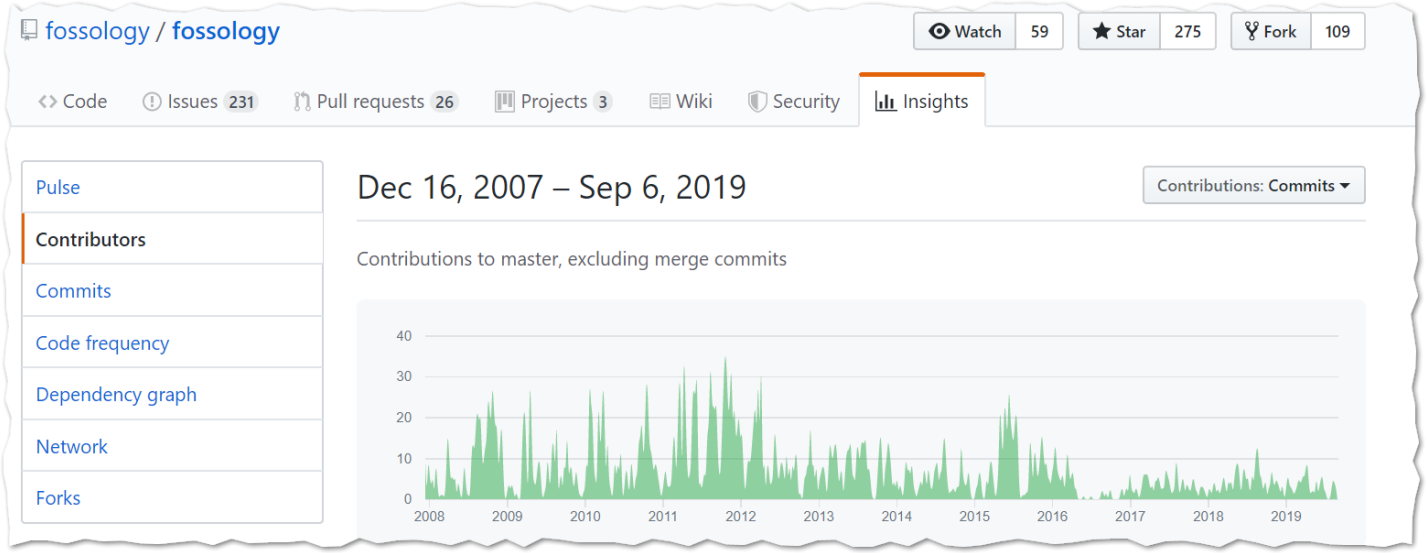


Fossology

Open Source
Tooling Group

- Scanning tool for license, copyright and export control scans.
- Can generate an SPDX file, or a ReadMe with all the copyrights notices .
- Web UI and a database for a compliance workflow.
- Scanners provided are Monk, Nomos and Ninka.
- Licensed under GPL-2.0 or 2.1

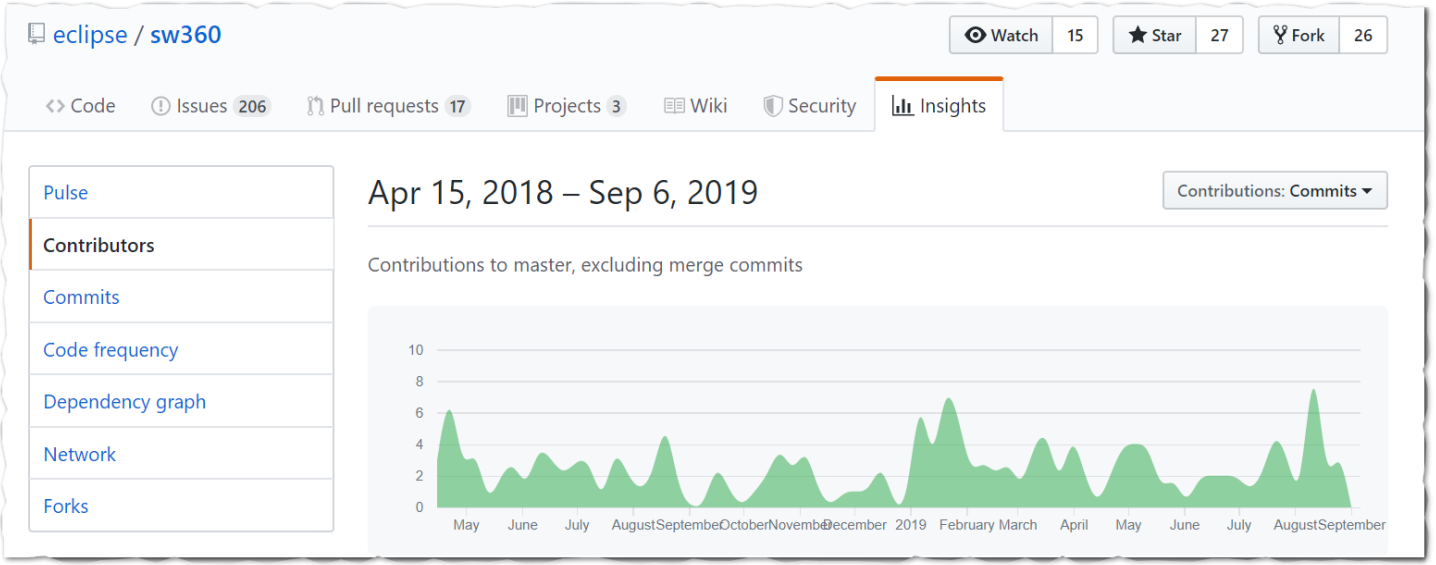
fossology



Eclipse SW360

Open Source Tooling Group

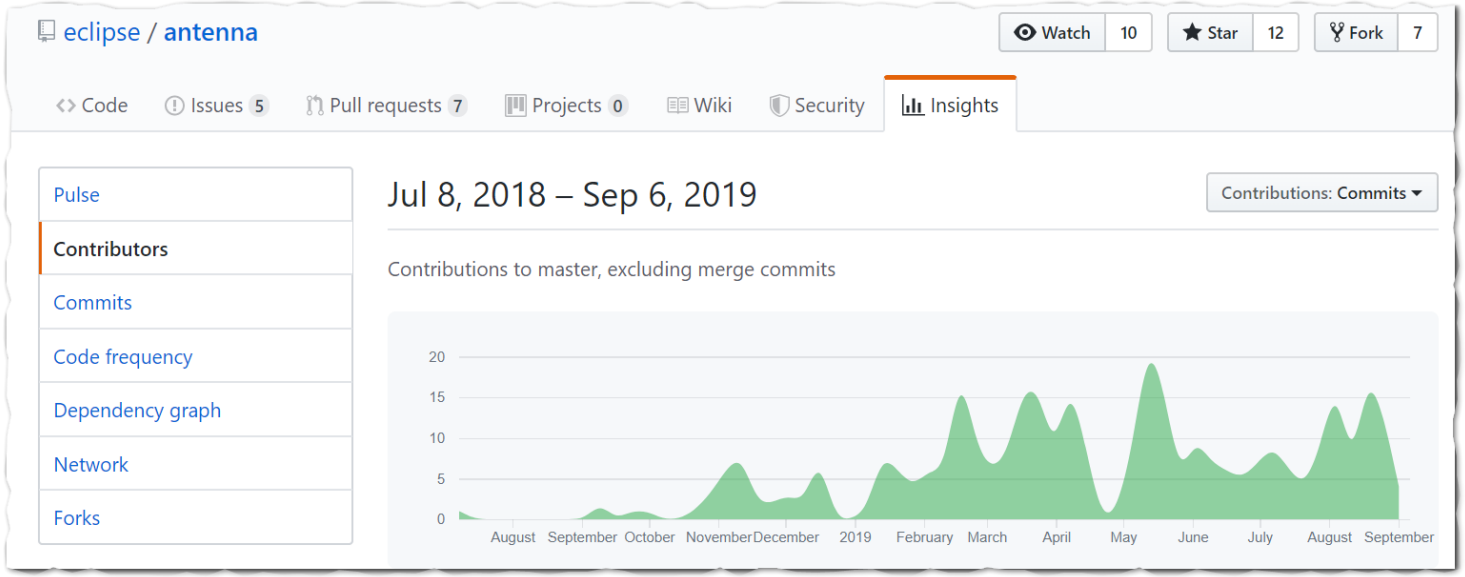
- A software component catalogue application - designed to work with FOSSology.
- SW360 is a server with a REST interface and a Liferay portal application to maintain your projects / products and the software components within.
- Licensed under EPL-2.0



Eclipse SW360 Antenna

Open Source Tooling Group

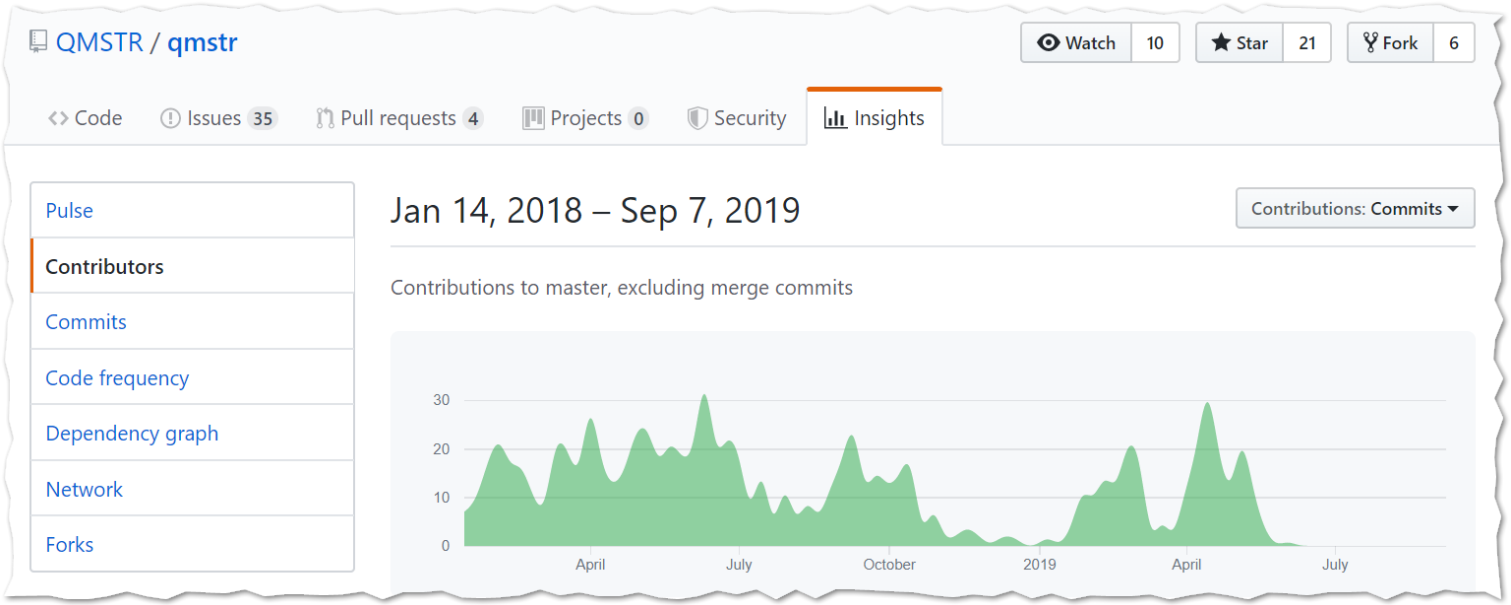
- A tool to automate your open source license compliance process.
- Collect all compliance relevant data
- Process that data and warn if there might be any license compliance related issues.
- Generate a set of compliance artifacts (source code bundle, disclosure document, report)
- Licensed under EPL-2.0



The Quartermaster Project QMSTR

Open Source Tooling Group

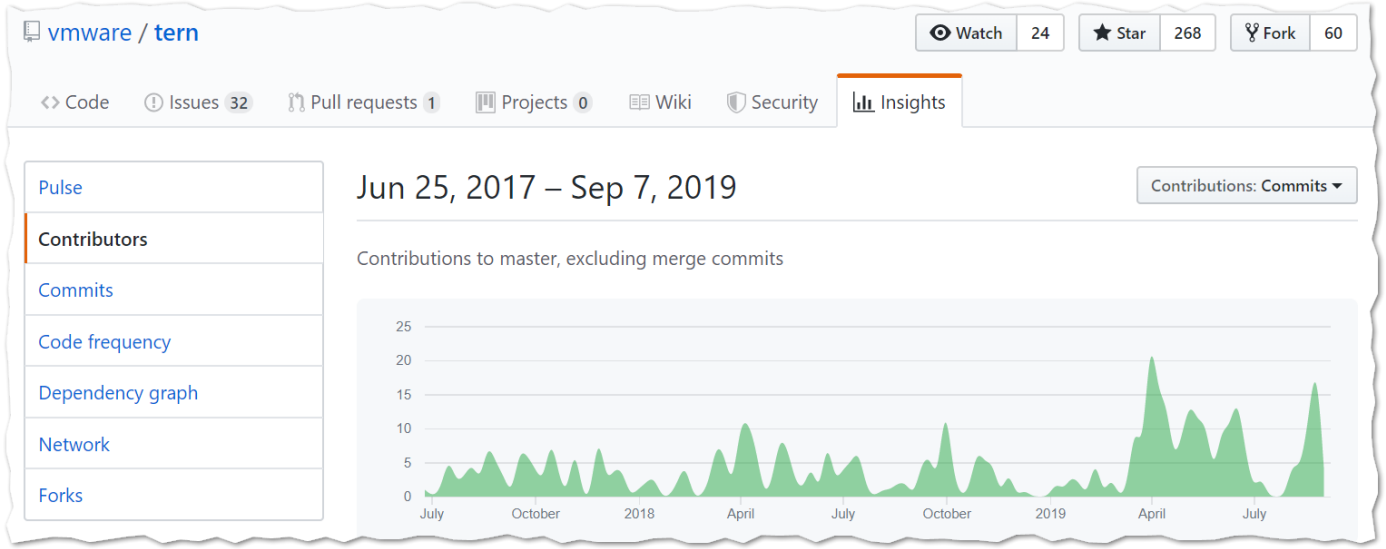
- Suite of command line tools and build system extensions.
- Executes as part of a software build process to generate reports about the analyzed product.
- Part of LF's Automated Compliance Tooling (ACT) project.
- Licensed under GPL-3.0



TERN

Open Source Tooling Group

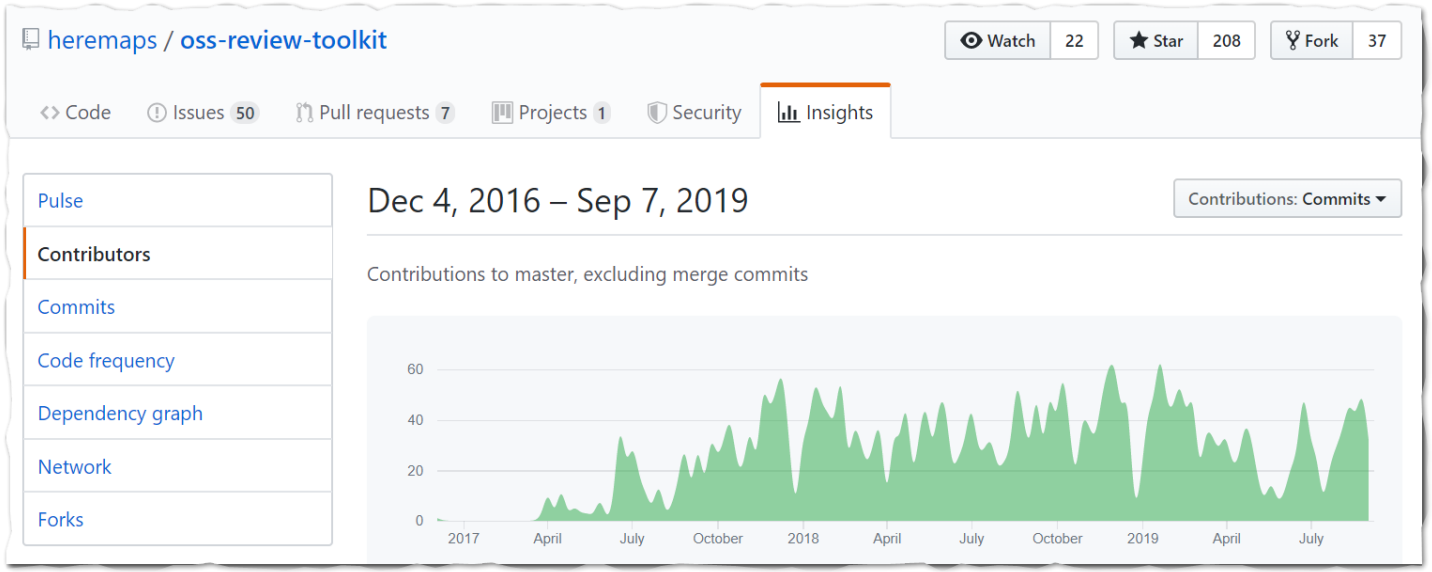
- Inspection tool to find the metadata of the packages installed in a container image.
- Default report is a verbose explanation of what layers brought in what software components.
- Licensed under BSD-2-Clause.



OSS Review Toolkit

Open Source Tooling Group

- Analyses the project's build system for dependencies.
- Download and scan the source code of the dependencies for license information and summarize the results.
- Available Toolkits: Analyzer, Downloader, Scanner, Evaluator, Reporter.
- Planned Toolkits: Advisor, Documenter.
- Licensed under Apache-2.0



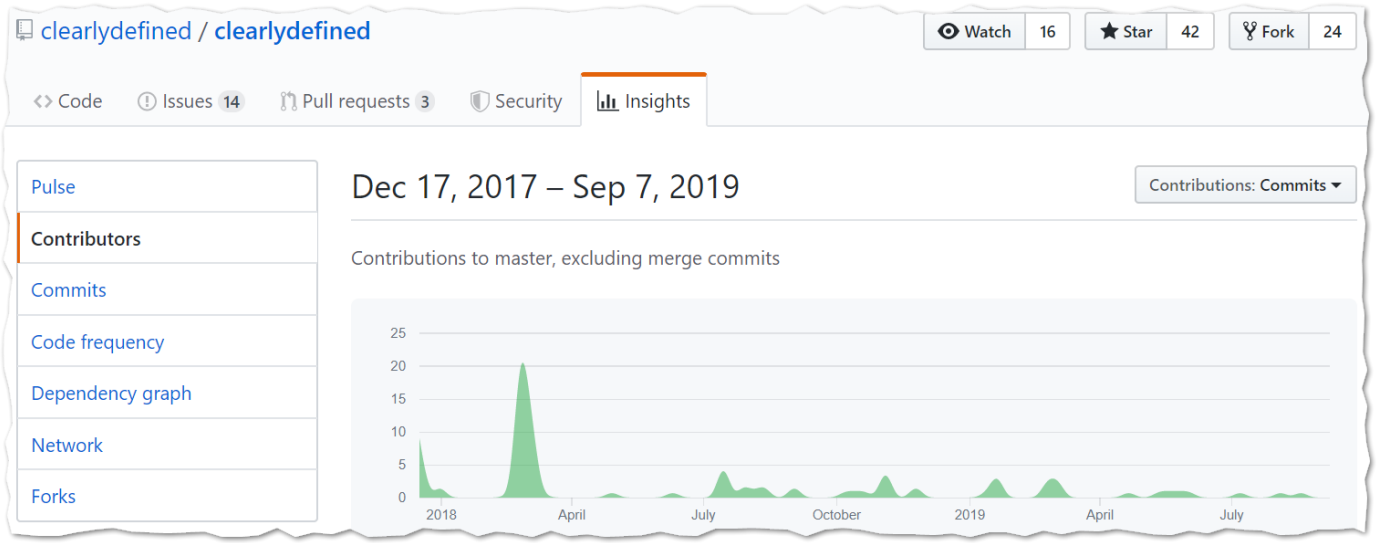
OSS Review Toolkit

Clearly Defined

Open Source Tooling Group

- **Mission:** To help FOSS projects thrive by being, well, clearly defined.
- Clearly Described
- Clearly Licensed
- Clearly Secure
- Licensed under Creative Commons CC0 1.0 Universal

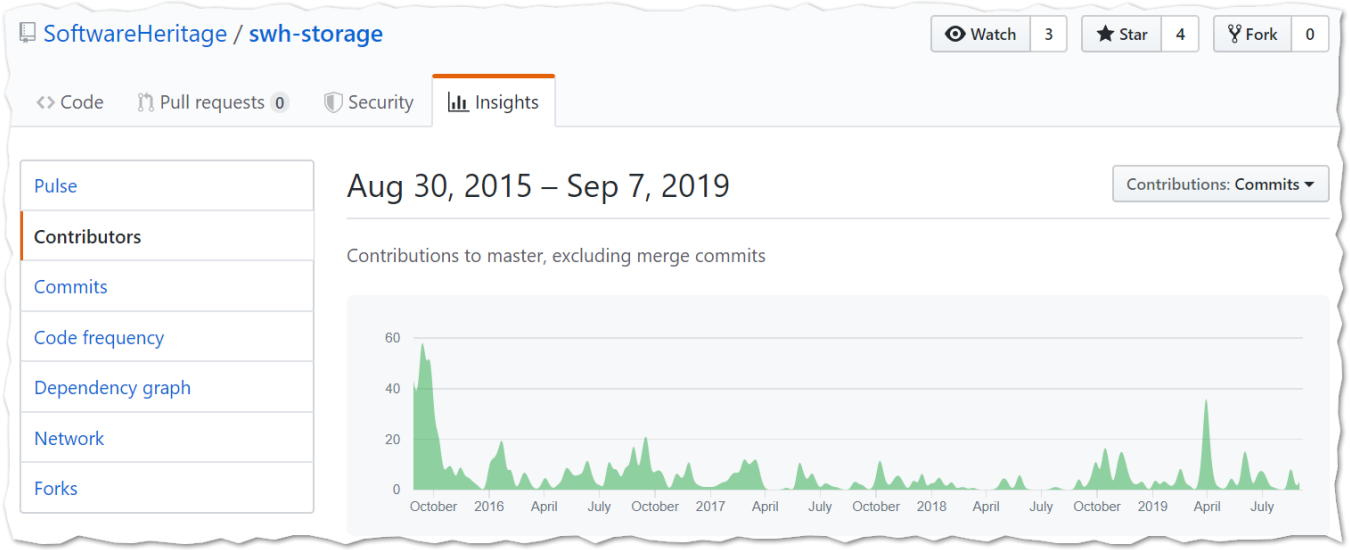
ClearlyDefined



Software Heritage

Open Source
Tooling Group

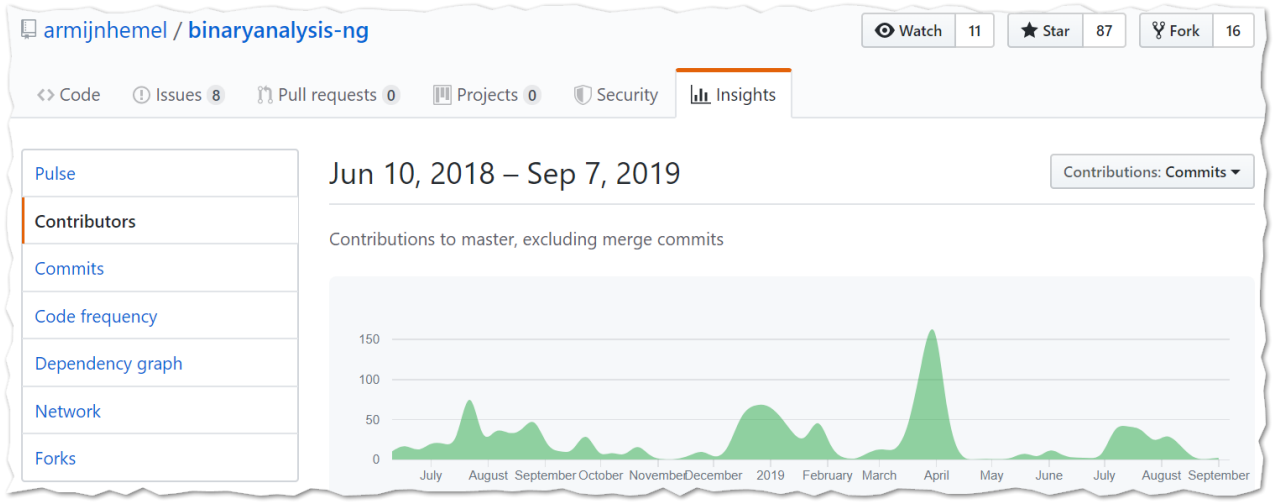
- To **collect**, **preserve**, and **share** all software that is publicly available in source code form.
- Ensures: Availability, Traceability and Uniformity of the collected source code.
- Licensed under GPL-3.0



BANG – Binary Analysis- NG

Open Source Tooling Group

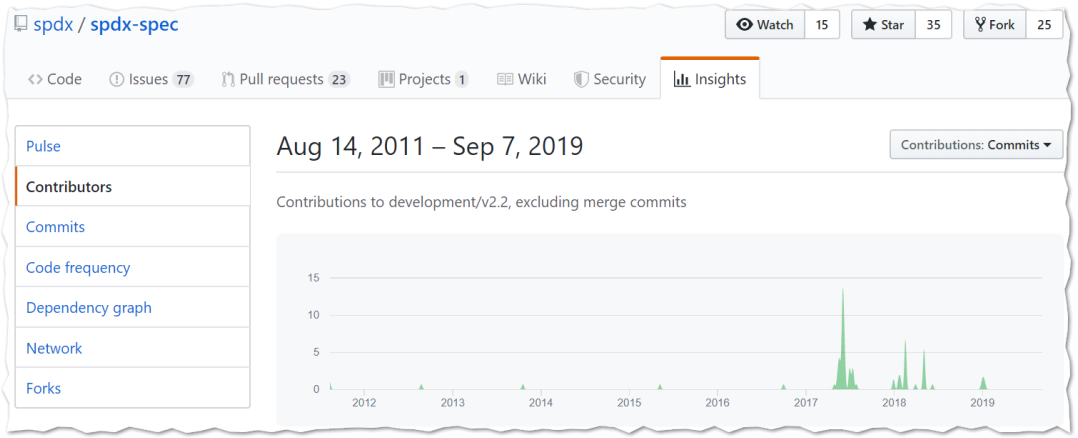
- Framework for unpacking files (like firmware) recursively and running checks on the unpacked files.
- To find out the provenance of the unpacked files and classify/label files, making them available for further analysis.
- Supports around 130 different file formats.
- Licensed under AGPL-3.0

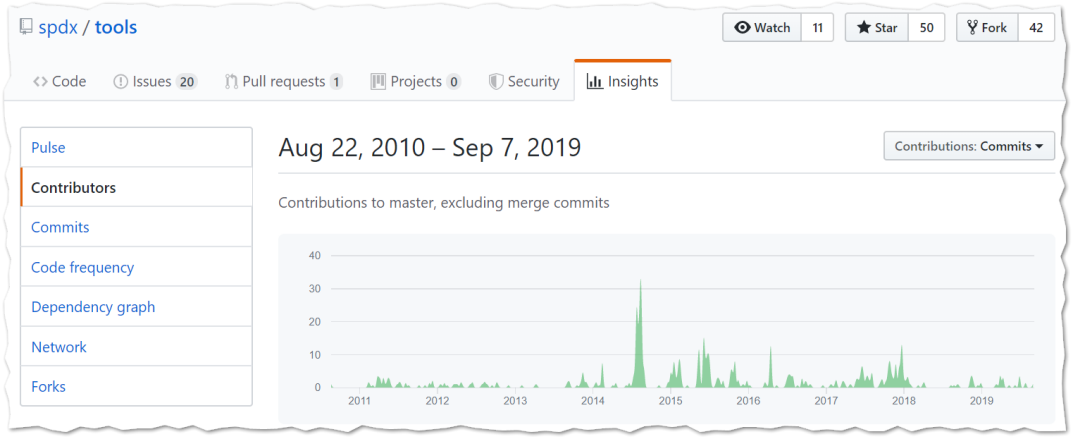


SPDX

Open Source Tooling Group

- Open standard for communicating software bill of material information.
- For communicating the components, licenses and copyrights associated with a software package.
- Spec Licensed under Creative Commons Attribution 3.0 Unported
- Tools Licensed under Apache-2.0



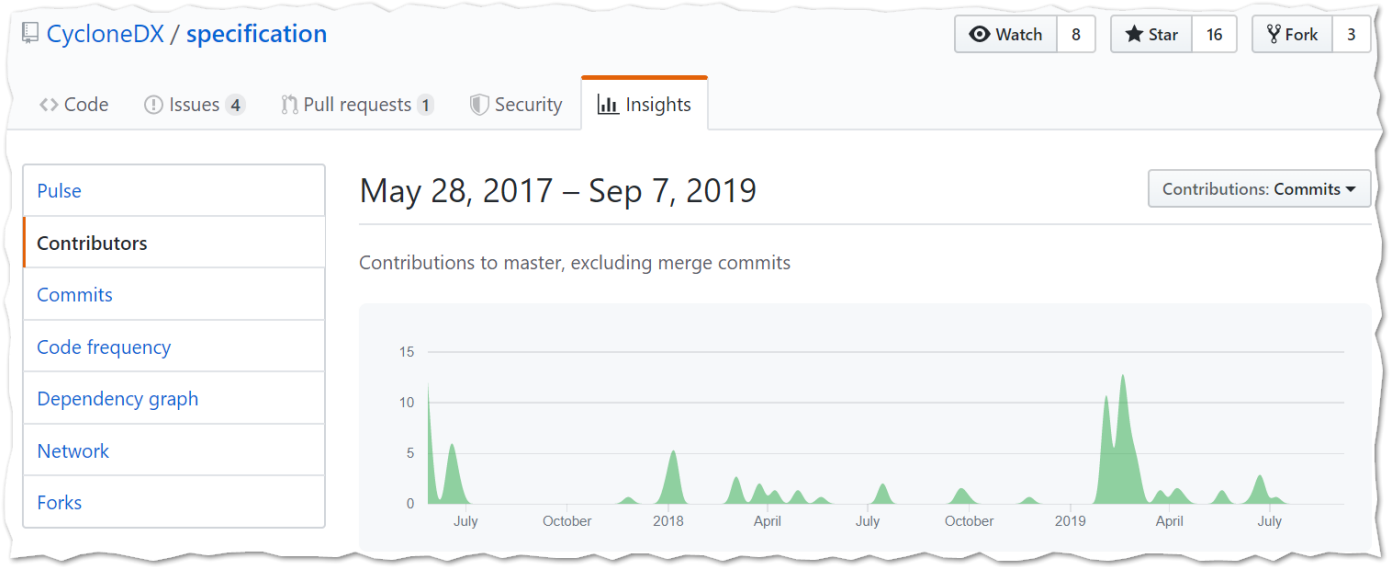


SPDX

CycloneDX

Open Source
Tooling Group

- Software Bill-of-Material (SBOM) specification designed for use in application security contexts and supply chain component analysis.
- Licensed under Apache-2.0



Open Source Automation Development Lab (OSADL)

- Intended to promote and coordinate the development of open source software for the machine, machine tool, and automation industry.

Open Source License Checklists - Checklists and license texts

License name	Project checklists
Academic Free License v2.0	AFL-2.0
Academic Free License v2.1	AFL-2.1
GNU Affero General Public License v3.0 only	AGPL-3.0-only
GNU Affero General Public License v3.0 or later	AGPL-3.0-or-later
Apache License 1.0	Apache-1.0
Apache License 1.1	Apache-1.1
Apache License 2.0	Apache-2.0
Artistic License 1.0 (Perl)	Artistic-1.0-Perl

Open Source License Checklists - Checklists and license texts

Academic Free License v2.0 (AFL-2.0)

Show reference license text in a new window Next

Checklist (Unreferenced raw data, Referenced raw data)

USE CASE Source code delivery
IF Software modification Hide ref.

6) Attribution Rights. You must re-in, in the Source Code of any Derivative Works that You cr
the Original Work, as well as any notices of licensing and any descriptive text identified there
Derivative Works that You create to carry a prominent Attribution Notice reasonably calculate

YOU MUST *Forward* Copyright notices Ref.
YOU MUST *Forward* Patent notice Ref.
YOU MUST *Forward* Trademark notice Ref.
YOU MUST *Forward* License notice Ref.
YOU MUST *Provide* Copyright notices Ref.
YOU MUST *Provide* Modification notice Ref.
YOU MUST *Forward* Warranty disclaimer Ref.
YOU MUST NOT *Promote* Ref.

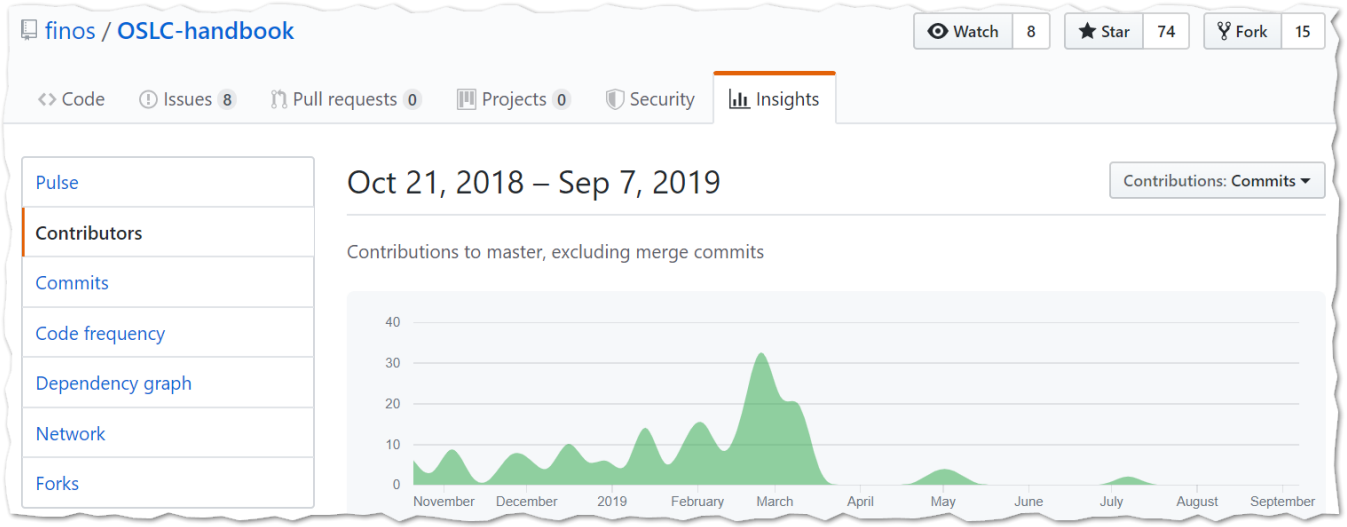
USE CASE Binary delivery
EITHER
YOU MUST *Include* Original source code Ref.
ATTRIBUTE Machine-readable Ref.
IF Software modification Ref.
YOU MUST *Forward* Copyright notices Ref.
YOU MUST *Forward* Patent notice Ref.

FINOS – OSLC Handbook

Open Source Tooling Group

- Data store and handbook of practical information about complying with the most common open source licenses.
- Based on uses cases (modified/unmodified, binary/source)
- Licensed under Creative Commons Attribution-ShareAlike 4.0 International

FINOS

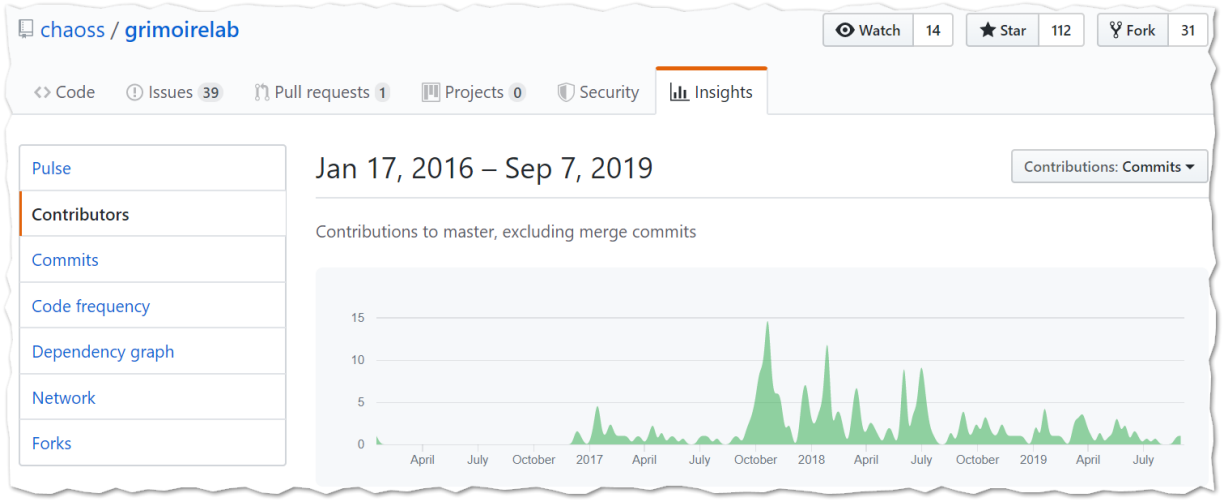


CHAOSS

Open Source Tooling Group

- Linux Foundation project focused on creating analytics and metrics to help define community health.
- Working groups to refine the metrics and to work with software implementations.
- GrimoireLab: toolset for software development analytics
- Augur: Python library and web service for Open Source Software Health and Sustainability metrics.

CHAOSS



Open Source
Tooling Group

Thank You!

Arun Azhakesan

Lead – Open Source License Compliance

Siemens Healthineers, Bangalore, India

@arunazhakesan