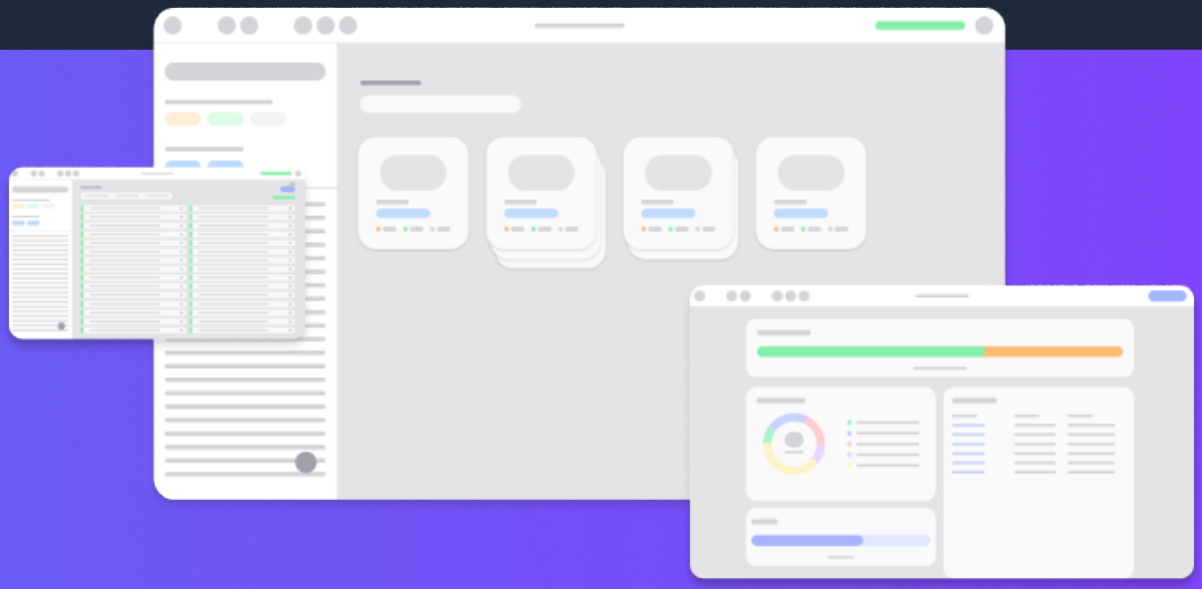
Whitepaper

The Future of Software Supply Chain Transparency

Open source solution enabling massive SBOM adoption.



SCANOSS

Background

The Software Supply Chain suffers from a noxious condition that leads to an absolute lack of transparency. While the hardware world would have never developed without standardized product composition information exchange across suppliers, somehow the Software industry made it to this point without such standards. Needless to say, we are paying the consequences of this shortcoming. The worst part of the recent LOG4J vulnerability was not the exploit itself, but the absolute lack of visibility on which products and services it affected.

Despite numerous efforts and standards in place around Software Bills of Materials (SBOM), still today large enterprises assume a tremendous expense of auditing most incoming software components from their suppliers. The reason? It is nearly impossible to find a software component that does not contain Open Source. Without proper handling, incoming software carries license compliance, security and technical risks.

The lack of transparency is the Achilles´ heel of the software supply chain, and this is the reason why President Biden signed the “Executive Order on Improving the Nation’s Cybersecurity”. This order has rapidly propagated way beyond U.S. borders, and is becoming the catalyst of software supply chain improvements around the globe.

The Need for SBOM Tooling

Open Source management processes instruct development teams on how to properly account for Open Source software components in a product. However, it is very easy for a developer to inadvertently introduce external Open Source component dependencies in a product which, without proper management, could have detrimental consequences. All

processes require adequate tools to enforce them. Software Composition Analysis tools cover this specific need.

During the past two decades, due to their costly price tags, Software Composition Analysis tools have only been within the reach of Large Enterprises. This forced these enterprises to adopt expensive auditing processes for every piece of software arriving from suppliers that could not afford such tooling themselves.

There are two categories of Software Composition Analysis tools, depending on the software analyzed:

Declared Open Source:

These tools analyze source code and metadata searching for dependency declarations, license headers, copyright statements, etc. A generous amount of tools like these exist in the Open Source world and are good at detecting declared Open Source software.

Undeclared Open Source:

These types of tools compare source code files against large databases of known Open Source code. In some cases, detection can be made not only on complete files, but also on code fragments. This enables code plagiarism detection, and also the ability to detect files even after having been modified. These curated databases usually also provide rich additional metadata associated with detected software components.

In both cases, the output of the tool is a software inventory, or SBOM. However, unless the source code is checked against an Open Source Knowledge Base, source code files whose headers have been stripped, or source code fragments conveniently borrowed from webpages, will simply be passed along undetected. These pieces of Open Source code, turn into a liability for the company integrating such code into a final product.

The Future of SBOM Tooling

Seeking massive SBOM adoption, SCANOSS has released the first Open Source Software Composition Analysis tool with a snippet-level Open Source Knowledge Base. It is capable of detecting both declared and undeclared open source.

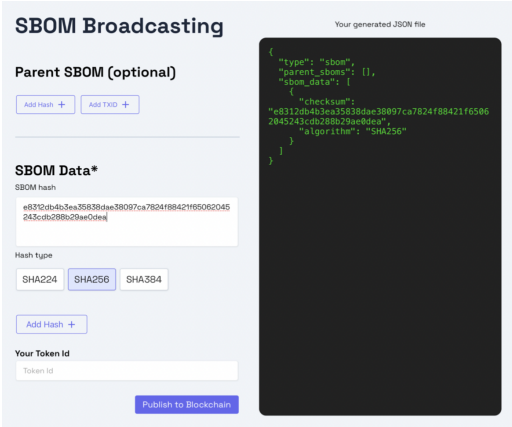
It is now possible to demand complete, accurate and traceable SBOMs from suppliers, which not only reduces risk and cost for Large Enterprises, but also improves efficiency and provides traceability in the Software Supply Chain.

The SCANOSS Platform offers a broad range of tools that covers Auditing User Experience (UX), Command Line Interfaces, APIs and even ready to consume integrations for Web Hooks & CI/CD pipelines.

In addition to SBOM generation, the lack of integrity validation and traceability of SBOMs across the supply chain has also raised concerns. The NTIA (National Telecommunications and Information Administration, U.S Dept. of Commerce) explained this issue in detail in 2019:

https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

With the purpose of addressing this concern, SCANOSS has developed the SBOM Ledger. Using blockchain technology, the decentralized SBOM Ledger provides a solid foundation for solving SBOM linking and integrity validation.



The SCANOSS Audit Workbench can be configured to automatically record SBOM integrity validation and linking information in the SBOM Ledger. Leveraging blockchain technology, the SBOM Ledger is a decentralized, immutable registry of SBOM integrity validators and SBOM to SBOM relationships..

The answer is broad SBOM adoption

Having SBOM standards in place, like SPDX and CycloneDX, and even an International Standard for Open Source License Compliance (ISO/IEC 5230) by the OpenChain, what remains is to stimulate broad SBOM adoption.

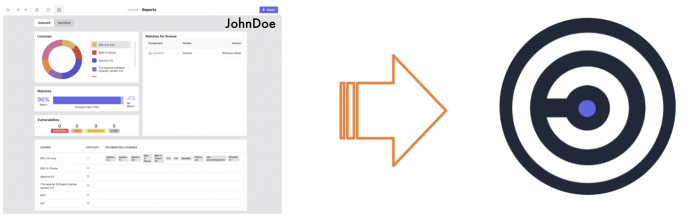
SCANOSS brings an end to decades of costly SCA tools which imposed vendor lock-in mechanisms to software composition data exchange. SMEs and independent developers, a key part of the Software Supply Chain, now have access to leading edge tooling which facilitates software composition, data analysis and exchange. This lowers risks and expenses and finally brings absolute transparency to the Software Supply Chain.

The first white-label SBOM tool

The SCANOSS Audit Workbench is a modern and feature rich multi-platform auditing tool that allows easy generation of SBOMs from any desktop or laptop computer.

As an Open Source tool, it allows enterprises to distribute a conveniently preconfigured tool that will all but eliminate supplier software auditing costs.

Example of a customized Audit Workbench making use of a dedicated (SaaS or on-prem) Knowledgebase and API



John Doe's SBOM Tool

https://sbom.johndoe.com

Consistent SBOMs with plagiarism check

The SCANOSS Audit Workbench offers an easy solution for standardized SBOM deliveries. The tool can be preconfigured, rebranded and redistributed to suppliers freely. With a seamless integration with existing procurement processes, SCANOSS standardizes consistent, plagiarism-checked SBOMs in standard SPDX or CycloneDX formats.

Get involved

The SCANOSS Platform is made entirely available as Open Source. The collaboration guidelines are available in the source code tree. Questions and suggestions are welcome at https://www.scanoss.com

Get in touch

SCANOSS offers commercial agreements and custom Service Level Agreements.
Please contact info@scanoss.com for further information.

Published on 2022-03-08 by SCANOSS.com