"SBOM 101"

SOFTWARE BILL OF MATERIALS

SBOM 101

Agenda

What is an SBOM?

What is the purpose?

How many formats are there?

How to create SBOM?

How to consume SBOM?

Where to learn more

WHAT IS AN SBOM?

- SBOM stands for Software Bill Of Materials: a nested description of software artifact components and metadata.
- Simple: think of this is as an ingredients list for a recipe that builds software
- Abstracting from package management systems we get “environments” so an SBOM would traverse all environments (example: npm + pip + rpm for a python web app)

GOVERNMENT LIKES SBOM

- https://www.cisa.gov/sbom
- SBOM@cisa.dhs.gov
- CISA SBOM-a-RAMA happening annually?
- ntia.gov/sbom
- https://www.cisa.gov/sites/default/files/publications/VEX_Status_Justification_Jun22.pdf
- https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

SBOM PURPOSE

- visibility and tracking the software supply chain
- foundation for SCA tooling (software component analytics)
- license inventory and enforcement
- tool that enables compliance to requirements (all source code origin tracked)

SBOM HISTORY

Palamida and BlackDuck manage software license inventory projects with “bill of materials” for licensing and legal analysis

In **2014**, the Cyber Supply Chain Management and Transparency Act of 2014 (H.R.5793) was introduced in The House of Representatives of the US Congress. The legislation did not pass - but it drew attention to SBOM and the importance of transparency in the supply chain of software products.October 2015 – SWID Tags standard, from NIST, published as ISO/IEC 19770-2:2015.

May 2017 – Initial drafts of CycloneDX, an OWASP SBOM standard.

December 2020 – The ISO International Standard for open source license compliance (ISO/IEC 5230:2020 – Information technology — OpenChain Specification) is published, requiring a process for managing a bill of materials for supplied software.

2020 – 2021 – NTIAs publishes latest work as part of the ongoing Software Component Transparency effort around Software Bill of Materials (SBOM).

February 2021 – Executive Order 14017 on America’s Supply Chain.

May 2021 – Executive Order 14028 on Improving the Nation’s Cybersecurity.

July 2021 – NIST releases the Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028.

August 2021 – SPDX published as ISO/IEC 5962:2021 standard.

September 2021 – First draft of SLSA (Supply-Chain Levels for Software Artifacts) framework.

February 2022 – DoD plan on Securing Defense-Critical Supply Chains which includes Software Supply Chain.

SBOM ANATOMY

Although there is not a single definitive standard for SBOM, NTIA did define the minimal requirements.

An SBOM must describe the **supplier of the software** and the **author of the SBOM**:

The organization/person that created the artifact.

The tool used to generate the SBOM.

The timestamp when the SBOM was generated.

In addition, the SBOM must contain a complete **description of the artifact components**, including:

Component name.

Component version.

A unique identifier (e.g. CPE / PURL / SWID).

Relationship with other components.

FOUR PRIMARY SBOM FORMATS

- **Software package data exchange (SPDX)—**an open source machine-readable format with origins in Linux.
- **Software identification tags (SWID)—**an industry standard used by different commercial software publishers
- **CycloneDX (CDX)—**an open source machine-readable format with origins in the Open Web Application Security Project (OWASP) community
- **json** formatted SBOM and software inventories (.json)
- other formats can include freeform plaintext and xml not mentioned here

SPDX

- SPDX was developed by the open source software development community for “ease of ingestion within a developer workflow and within corporations to support compliance and software transparency for open source and proprietary code,” according to the NTIA working group. Given its **open source roots**, the format is supported by a wide and distributed population of commercial international organizations, as well as developers who may not be associated with vendors, the NTIA said.
- Importantly, the accessibility of SPDX means that a developer of an experimental library can generate an SBOM without much effort, free of charge. The availability of open source tools and cost-saving makes it attractive to organizations, along with the ability to link artifacts to global reference systems via Common Platform Enumeration (CPE), Package URL (purl), Software Heritage persistent ID (SWHID), as well as other package build coordinates. This enables flexibility to handle security use cases.
- SPDX became an internationally recognized standard for SBOM published as **ISO/IEC 5962:2021** in September 2021.
- its supporters include Cisco, Google, Intel, Microsoft, SAP, Siemens, Sony, VMware and MITRE
- see SPDX.org or SPDX.dev, the SPDX specification is recognized as the international open standard for security, license compliance, and other software supply chain artifacts as ISO/IEC 5962:2021.

CYCLONEDX

- CycloneDX is an open source standard developed by the **OWASP foundation**. It supports a wide range of development ecosystems, a comprehensive set of use cases, and focuses on automation, ease of adoption, and progressive enhancement of SBOMs throughout build pipelines. The specification is widely used among organizations with security use cases and is equally capable of describing both open source and proprietary software.

- A large and growing collection of community and officially supported open source tools are available, and the project's website includes many examples for achieving various use cases. CycloneDX natively supports multiple standards for component identity including coordinates, Package URL, CPE, and SWID for both binary and source software artifacts.

- OWASP CycloneDX has launched a **BOM Exchange API** that aims to operationalize an SBOM. It also standardizes how BOMs are published and retrieved and aims to be software agnostic. Smells like a standard!

- supporters include Google, Intel, IBM, Red Hat, Oracle, Cisco and SAP.

SOFTWARE ID TAGS

- SWID tags were designed to provide a transparent way for organizations to track their software inventory on managed devices. SWID tags contain descriptive information about a specific software release such as the product and version. It also identifies the organizations and individuals that played a role in producing and distributing the product. Tags are removed when associated software is uninstalled, enabling tags to be used for software asset inventory.
- NIST recommends adoption of the SWID Tag standard by software producers, and multiple standards bodies, including the Trusted Computing Group (TCG) and the Internet Engineering Task Force (IETF) utilize SWID Tags in their standards.
- A developer can use readily available guidance on how to develop SWID tags to configure their build pipeline to produce SWID tags automatically during the software build and packaging process. Geared at deployed software, SWID tags follow the binary artifact and are updated as changes are made to the compiled codebase. This lends itself to integration with automated scanning, and a variety of risk management use cases and tooling, NIST said.
- NIST is working with the IETF to develop multiple specifications that use SWID Tags. It is also working to incorporate SWID Tag data into the National Vulnerability Database's (NVD) vulnerability dataset and has incorporated the use of SWID Tag data into Security Content Automation Protocol (SCAP) version 1.3.

SYFT FROM ANCHORE

- open source - command line and a library written in Go
- Converts between SBOM formats: CycloneDX, SPDX, and Syft's own format
- Focused on containers more than on built software
- 

PACKAGE MANAGEMENT VERSUS SBOM ON THE PLATFORM LEVEL

- https://thenewstack.io/create-a-software-bill-of-materials-for-your-operating-system/
- dpkg --list
- rpm -qa --qf
- wmic \ output:C:\list.txt product get name, version
- pkgutil --pkgs

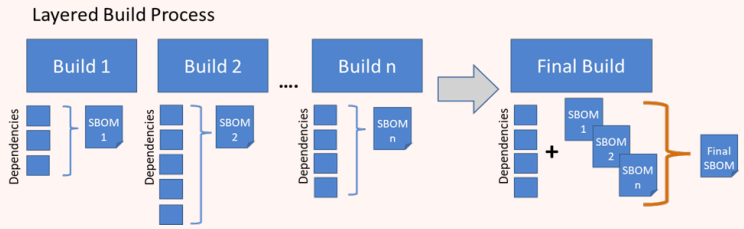
INTELLECTUAL PROPERTY REVIEW FOR CODE DUPLICATION AND OPEN SOURCE LICENSES

- https://spdx.org/licenses/

- Synopsys/BlackDuck/Flexera and other consulting firms use SBOM for license review

MICROSOFT'S SBOM TOOL

- https://devblogs.microsoft.com/engineering-at-microsoft/microsoft-open-sources-software-bill-of-materials-sbom-generation-tool/

- 

- https://github.com/microsoft/sbom-tool#installation

SOME NOTABLE VENDORS AND PROJECTS

- Anchore https://www.anchore.com
- Rezilion https://www.rezilion.com/platform/dynamic-sbom/
- RapidFort https://rapidfort.com
- Finite State
- SCANOSS project
- Dependency Track
- mend.io (formerly whitesource)
- ChainGuard
- Veracode
- CodeGrip.net

WHAT'S NEXT?

- incorporation into anti-malware and code whitelisting infrastructure
- tracking origin of source by nation-state
- cloud services for SBOM generation, analysis, compliance, package management
- incorporation into fuzzing and AI code testing techniques
- performance at scale and code removal for security

- will SBOM's hold software firms accountable or just create more red tape?
  - both, but definitely more work than the workforce can handle

QUESTIONS / ANSWERS

- **Mat Caughron CISSP CSSLP NSA-I[AE]M**
- **caughron@gmail.com**
- **(408) 910-1266**