SYNOPSYS®

GUIDE

Cheat Sheet: Your Recipe for an Actionable SBOM

Software Bill of Materials (SBOM): Everyone's heard of it, everyone's talking about it, but what does it mean for you and what should you be doing about it?

It's been a year since President Biden's executive order (EO 14028), which ignited an examination of supply chain security and highlighted the lackluster approach most organizations take when tackling cybersecurity.

On May 5, 2022, the National Institute of Standards and Technology (NIST) released a finalized version of Special Publication 800-161, Revision 1, which details best practices for cybersecurity supply chain risk management for systems and organizations. A key tenet of the revision—and what we're focused on here—is recommended minimum standards for vendors and developer verification of software. The publication specifically focuses on SBOMs.

What does EO adoption look like a year later?

In short, it's *okay*. Even a year after the fact, many are still scrambling to adequately address their supply chain weaknesses and figure out how best to satisfy the specific SBOM requirements laid out in the order.

On May 12 of this year, the Advanced Technology Academic Research Center (ATARC) hosted a webinar to discuss progress and challenges with implementation of the EO[1] featuring a panel of guests from various U.S. government agencies. The consensus of the discussion was that there has been an across-the-board improvement and progress in addressing cybersecurity—with still-gaping areas begging for improvement.

The panel agreed that organizations are facing challenges in implementing security practices in a landscape of rapidly changing technology. The lag in action compared to the speed of technological advancements is resulting in an unideal *reactive* approach to security, where organizations are failing to get ahead of security pressures and scrambling just to keep up. Panelists emphasized that they are pressuring software companies to help out. They want these organizations to perform their own due diligence and security practices before government agencies purchase the software. Put simply, they want transparency from vendors on the composition and DNA of their software.

Sounds familiar, right? They're asking for an SBOM.

Meeting the requirements for SBOM reporting to satisfy both the EO and customer demands is very much at the forefront of priorities for the government, and it should be for you, too. While the EO only directly addresses organizations that do business with the government, this new approach to cybersecurity has already shown itself to be a de facto model that everyone should—and will—follow in the future.

In an effort to demystify the SBOM, we've compiled the concerns and confusion we're seeing from our customers and boiled them down to several key recommendations you should consider when finetuning your SBOM efforts.

Recommendation 1

Think of an SBOM as more than a document: It's a document AND a process

Traditionally, we think of SBOMs as an inventory of the software components that a software application is composed of (open source, third-party, custom code). Today, however, an SBOM extends beyond this; it's meant to also encapsulate the processes an organization uses to inventory its software.

The purpose of an SBOM is to help manage open source usage, provide insight into software "ingredients," and standardize how that information is communicated. We encourage looking at SBOMs in the broader sense as a management system. Your SBOM system should focus on identifying open source components with origin awareness, and it should map those components to vulnerability data. It should also include workflow and notification capabilities.

SBOMs encourage a conversation around strategy for software supply chain management. Being able to create an SBOM entails having a process in place that automates and fortifies your SBOM accuracy. Think about how you can improve and standardize the practices, processes, and activities involved in creating and maintaining your SBOM.

Recommendation 2

Adopt a standardized SBOM format such as SPDX

In November 2021, the National Telecommunications and Information Administration (NTIA), as part of its obligations under EO 14028, defined a minimum set of fields for a compliant SBOM. Although compliance targets have yet to be defined by the U.S. government, it's expected that compliance will require more than just an SBOM.

Adopting a standardized SBOM format will help streamline efforts now and in the event of changing standards. Two of the most common SBOM formats are SPDX (also known as ISO/IEC 5962:2021) and CycloneDx. While there is currently no format standard, SPDX looks like the frontrunner. SPDX helps reduce redundant work by providing "common formats for organizations and communities to share important data, thereby streamlining and improving compliance, security, and dependability."[2]

We highly recommend adopting a standardized SBOM format that will support you now and as specifics continue to emerge in the months to come.

Recommendation 3

Use both first-party and third-party SBOMs

There are two options when it comes to generating an SBOM: first-party and third-party. In most instances, organizations will need both.

A first-party SBOM is one that a software builder produces. It can be used internally to track dependencies and risk, and it can be easily provided to customers who want or need one.

A third-party SBOM is procured by a consumer or purchaser of software. It enables consumers to understand what components are powering their business and any related risk they are inheriting.

Software builders, who often use third-party code, should seek a related SBOM for it. The software they create using this inherited software requires its own first-party SBOM.

Recommendation 4

Use third-party SBOMs to chart a security map

An SBOM is a key component of a software supply chain risk management approach, but if you don't take any action on it, it's only a document. SBOMs received from suppliers and third parties should prompt efforts to define a process centered around creating a detailed and actionable path toward achieving specific and tangible security goals.

The overarching goal should be to automate security workflows and address any existing security gaps. An SBOM is only as helpful as you make it. Use it to inform your security activities and it can be a critical asset to reducing business risk and building trust in your software.

Recommendation 5

Make sure your SBOM covers your industry's specific requirements

Although EO 14028 and NTIA set a standard for SBOM usage, there are other requirements in different industries. Most notably, the FDA recommends additional data be collected with the SBOM for medical devices. In the automotive industry, ISO 5230/ OpenChain requirements direct SBOMs to include software licensing information.

It is therefore crucial to understand the driving requirements for SBOMs in your industry, and which sectors of your business are in scope. Select an SBOM solution that covers all these requirements.

Recommendation 6
Implement automated SBOM tooling

When considering SBOM solutions, automation is your best friend. NTIA-compliant SBOMs need to be all-encompassing and machine-readable, and it is nearly impossible to gather this level of detail manually. Further, software builders need a solution that can scale with them, so an automated solution is key.

A powerful software composition analysis (SCA) tool can easily generate a complete open source SBOM and also offers the ability to include third-party custom components. Most importantly, SCA tools provide SBOM information on a continuous basis, meaning you have the most complete picture of open source risks in real time. The right SCA tool can even build SBOM generation directly into your SDLC, making the process even easier.

Recommendation 7
Think beyond open source

Of course, open source is critically important to consider when building your SBOM. But it's vital to look beyond it. Commercial, third-party, and proprietary components are equally important in an SBOM. The code you write and the code you inherit have the same potential to introduce risk to your software development ecosystem.

Developers are not security experts, so it's likely they will, at some point, inadvertently introduce security weaknesses into the code they write. Tackling security weaknesses in your proprietary code is therefore your responsibility.

You should assume the same for third-party or commercial code; their developers are likely not security experts either. Taking a "trust but verify" perspective is key. Your takeaway: ALL code should be analyzed and included in your SBOM.

Recommendation 8
Embrace VEX

VEX[3] (vulnerability exploitability eXchange) is a new concept; the NTIA describes it as a "companion artifact" to an SBOM.

In very simple terms, VEX is a sort of vulnerability "exception" classification—a way for an organization to report that a vulnerability discovered in its application is not of any concern and does not need any remediation.

Let's say you found a vulnerability that exists in one of your components, but it's inaccessible to attackers. How do you communicate in your SBOM and to your customers that it's there but that it's not a problem? With a VEX document.

In the near future, a VEX disclosure or document will likely be part of the SBOM as a basic communication that a discovered vulnerability requires no remediation activities. You don't need to wait though. You can add VEX documents as a part of your SBOM process today.

---

1 Robert K. Huffman, Susan B. Cassidy, Michael Wagner, May 2022 Developments Under President Biden's Cybersecurity Executive Order: One Year Anniversary Update, Lexology.com, 6/1/2022.

2 The Linux Foundation, SPDX about page, accessed 6/22/2022.

3 Derek Kruszewski, What is VEX and What Does it Have to Do with SBOMs?, adolus.com, 8/12/2021.

SYNOPSYS®

The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com