GUIDE

Your Recipe for an Actionable SBOM

Key considerations for building, maintaining, and using a Software Bill of Materials

Less is not better in the case of SBOMs. It's easier to remove elements for certain customers than it is to add elements from different sources. For example, the FDA requires many fields in an SBOM, whereas a specific hospital may require only a subset. We recommend you focus on producing comprehensive, up-to-date SBOMs that you can modify by removing unnecessary elements for special cases.

Recommendation 7

Know what you'll do with your SBOM

Now that you have generated an SBOM, what are you going to do with it? How are you going to map it to areas of risk? How are you going to use it as a tool to control and manage your software supply chain? Answering these questions will ensure that you derive full benefit from your SBOM to reduce supply chain risks, increase customer confidence, and support regulatory compliance.

An SBOM can help identify risks and threats before bad actors can exploit them. But to be effective, it can't be created once and then forgotten about. Software is constantly changing; new dependencies are added, old ones are updated or removed, and vulnerabilities are discovered and patched. Without continuous updates, an SBOM can quickly become outdated and inaccurate, rendering it useless. By following these seven recommendations, your organization can generate, manage, and use SBOMs to build secure and compliant software applications.

Learn more about generating, managing, and using SBOMs

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information about the Synopsys Software Integrity Group, visit usccelerso appliancee41 91.279)5120vsverovvdemarkynok. With SynInc