Rezilion

The SBOM of the Future

A Software Bill of Materials (SBOM) is a machine-readable list of the items and dependencies contained in a piece of software. Heightened concerns over the security of the software supply chain, and a recent directive (EO 14028) from the federal government for software vendors to provide one if they want to contract with agencies, means the SBOM is becoming a cornerstone for secure software development.

But today's SBOM is just the beginning of better visibility into the software components and supply chain. Here we examine the nature of SBOMs today and the potential enhancements that will make SBOMs of the future an essential part of software security.

SBOMs Today

While SBOMs today are important to increasing visibility into software components, they have limitations.

NOT DYNAMIC — SBOMs are static documents and do not incorporate updates automatically.

MINIMAL INFORMATION — SBOMs provide a list of different components present in the software. They do not provide any context for which a companion document Vulnerability Exploitability eXchange (VEX) has been recommended by US National Telecommunications and Information Administration (NTIA).

NOT ALWAYS RELIABLE — SBOMs are produced by software and product vendors, including their supply chain, without any third party or regulatory agency validation. So, you need to trust its source in order to trust its contents.

MANUALLY PRODUCED — SBOMs are manually produced at the end of the development cycle when the software goes to production. They are not interoperable, meaning they are format specific.

SBOMs in the Future

As SBOMs come into common use, technology will enhance how they are created and updated.

DYNAMIC — Dynamic SBOMs will become a requirement especially within organizations that create and update products regularly. Additionally, dynamic SBOMs will incorporate automatic updates.

COMPREHENSIVE — SBOMs of the future will have multiple inputs from threat intel assessment sources to provide the contextual information necessary to identify issues and make updates.

VERIFIED AND RELIABLE — SBOMs will be independently verified via third party testing agencies, national SBOM databases or security products that provide validation features.

PROACTIVE — In the future SBOMs will be integrated into the product security lifecycle and will be produced automatically at predefined stages. SBOMs will also be interoperable allowing for greater adoption and flexibility of use.

Rezilion can help you get to the future of SBOMs today. **REZILION** creates a dynamic SBOM automatically and updates it every time code is pushed. Learn more at Rezilion.com.