



Making Software Bill of Materials (SBOMs) Actionable



Who am I?




Ciara Carey
Developer Relations
Cloudsmith

 [@Ciara_Carey_](https://twitter.com/Ciara_Carey_)



Agenda

- Software supply chain
 - Threats to your software supply chain
 - SBOM as one the responses to secure your supply chain
 - When to generate, host and analyze an SBOM
 - Making SBOMs actionable
- 
- A decorative graphic at the bottom of the slide consisting of numerous thin, light blue lines that flow and curve across the width of the slide, creating a sense of motion and depth.

Software Supply Chain

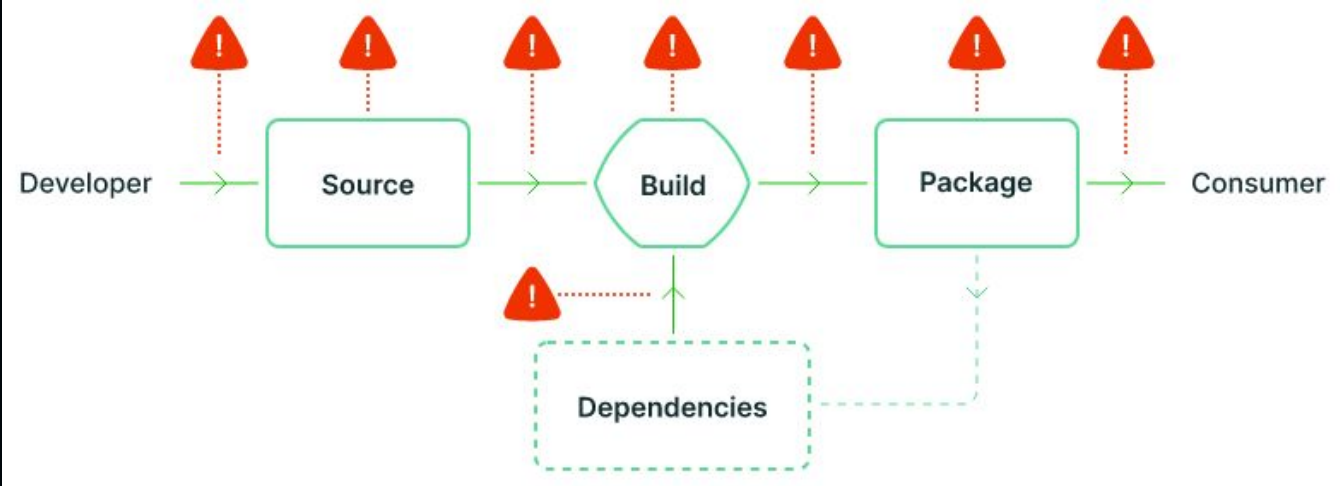


Image from SLSA's website

Open Source Software

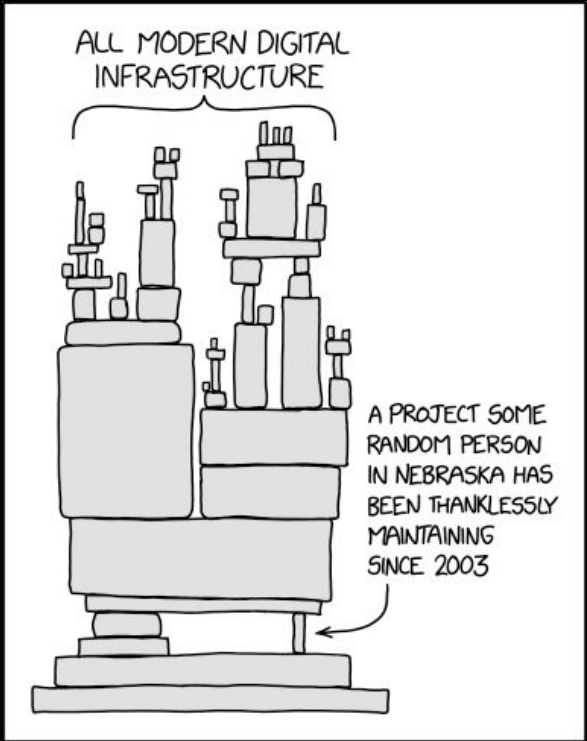


Image: xkcd



Threats in Open Source Software



Critical Vulnerabilities in OSS are a major threat



Solarwinds supply chain attack





Response!



Software Bill Of Materials



How to Generate, Host and Analyze SBOMs for Vulnerabilities



When to generate an SBOM



syft



CycloneDX



Merge.dev

FOSSA



dependency track


Source

FOSSA

Build

 CycloneDX



 dependency track

Built Binary

Package in a Container Image





Runtime


by Contrast Security - <https://contrastsecurity.com>
jbm generates SBOMs for all JVMs running on a host
<https://github.com/Contrast-Security-GSS/jbm>

How to Host SBOMs



Hosting SBOMs

- Host your Container SBOM using Sigstore tooling
- The best way to host SBOMs for non-OCI artifacts, e.g. Maven, RubyGem, NPM packages, is not fully understood.



SBOMs and Vulnerability Management



What's A Vulnerability Again?



Vulnerability Exploitability eXchange (VEX)



How Can SBOMs help with Vulnerability Management?



Workflows to make SBOMs actionable



syft



grype

 Quarantined

Future work





ciara-carey-7540173/



@Ciara_Carey_