Microsoft

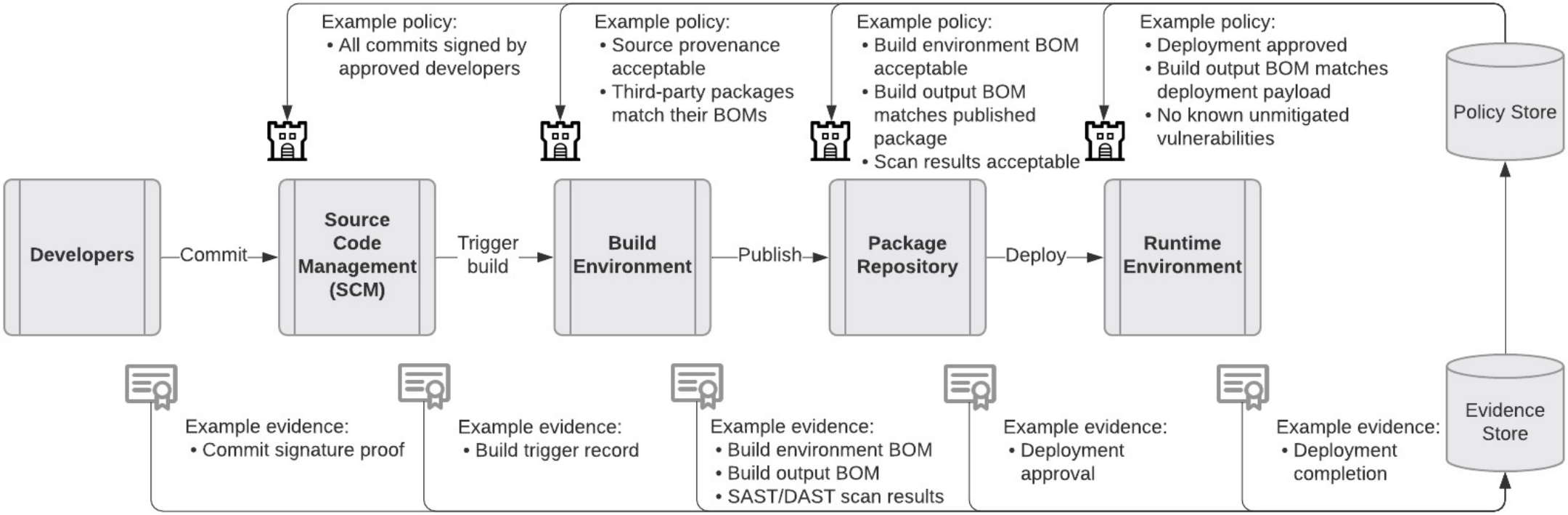
Criteria and attestation for maintaining provenance of code and components including open-source software

NIST Executive Order on Cyber Security Workshop
November 8, 2021

Relevant Executive Order Sections

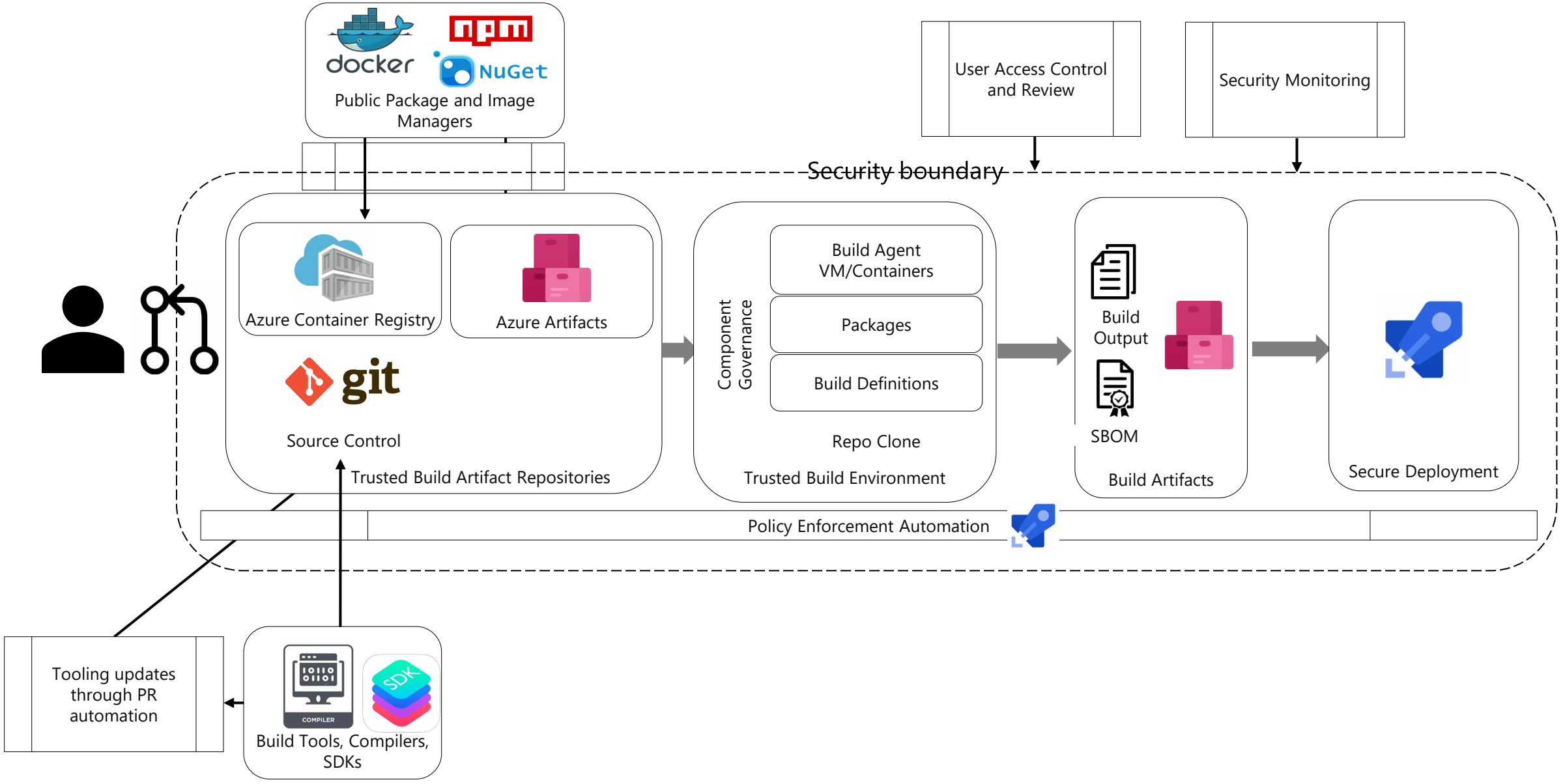
- 4 (e) (vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;
- 4 (e) (vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;
- 4 (e) (x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

Supply Chain Integrity Model

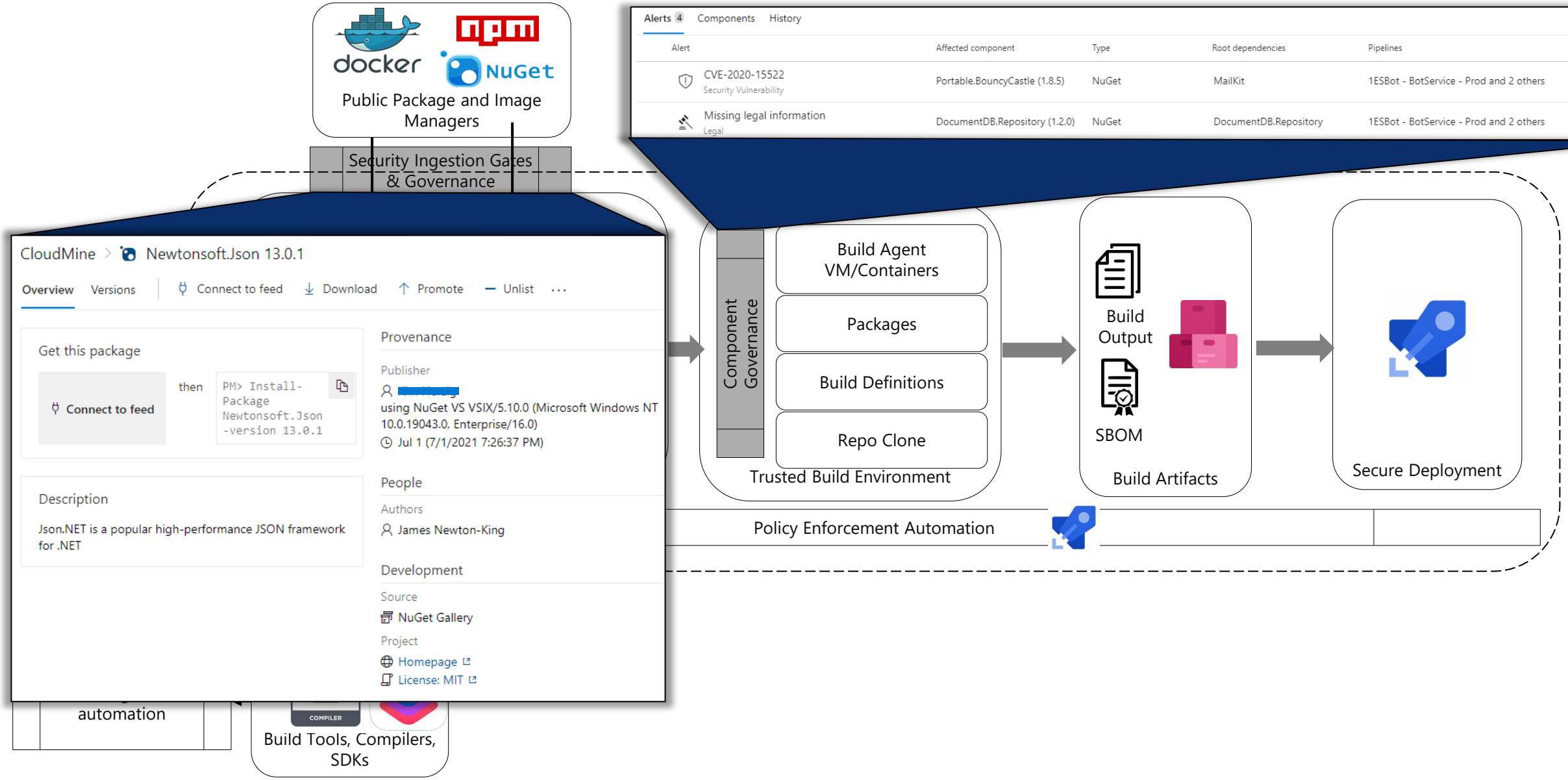


[GitHub - microsoft/scim: Supply Chain Integrity Model]

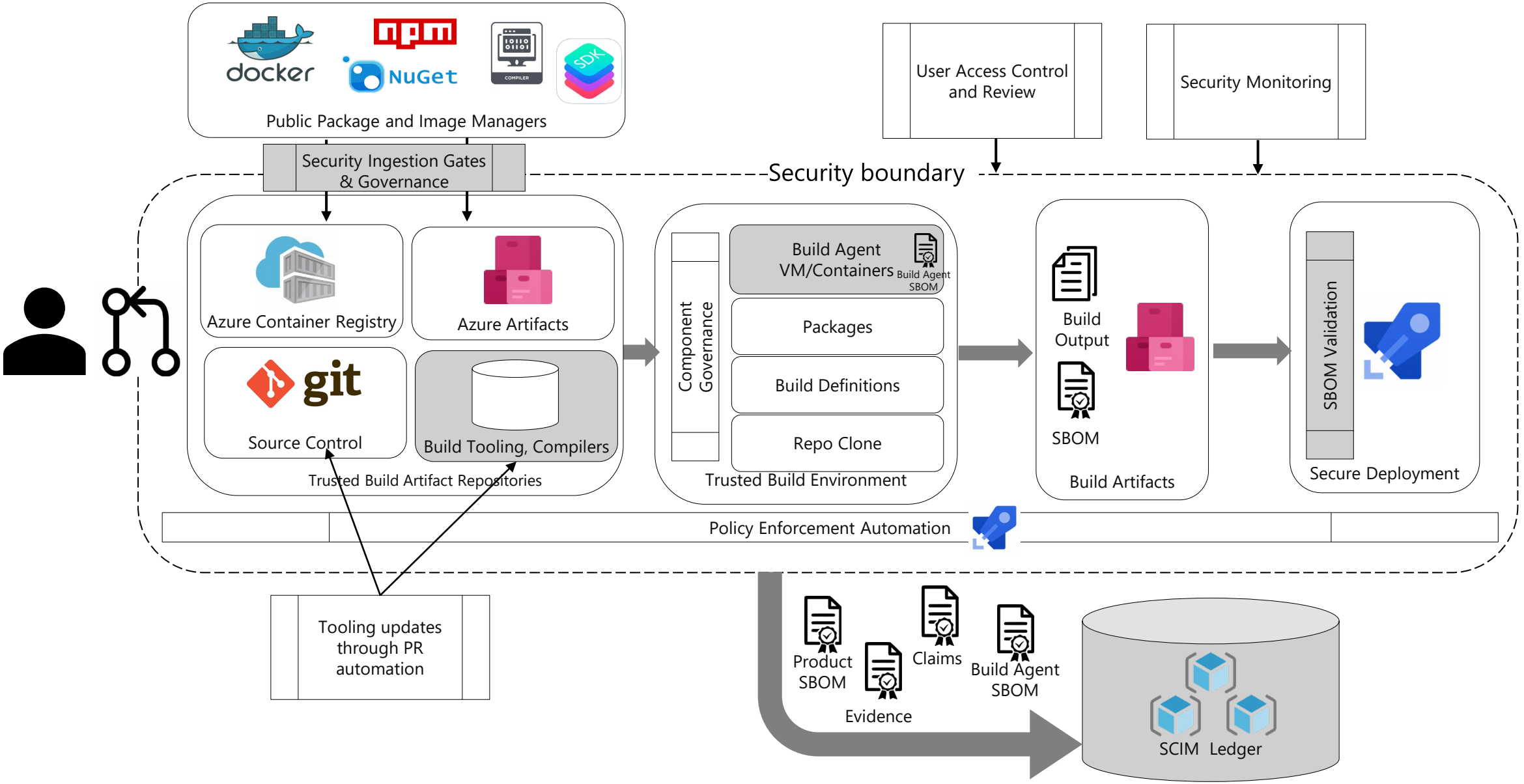
Build tool and OSS provenance management today



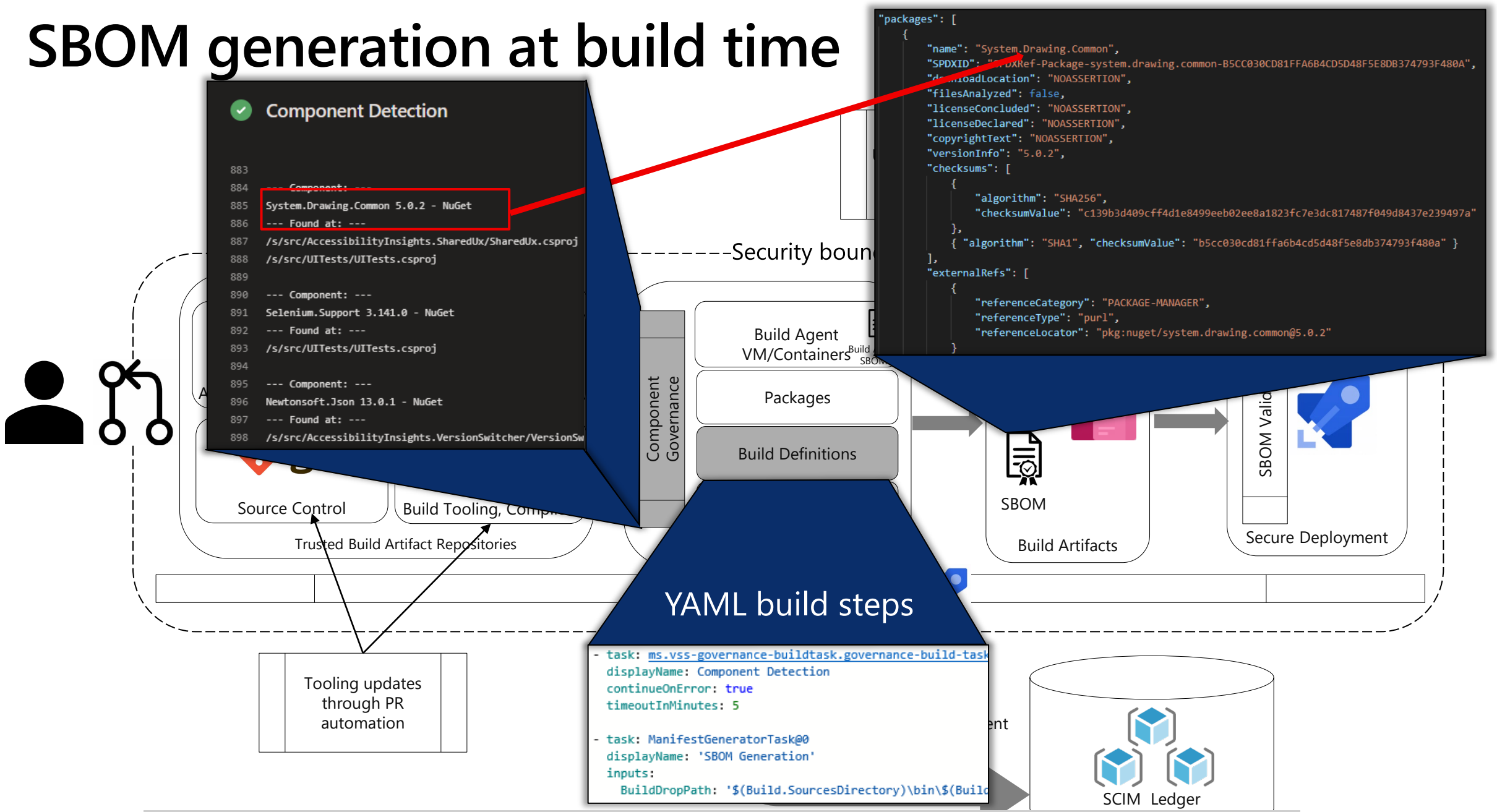
OSS ingestion & provenance



Future tool and OSS provenance management

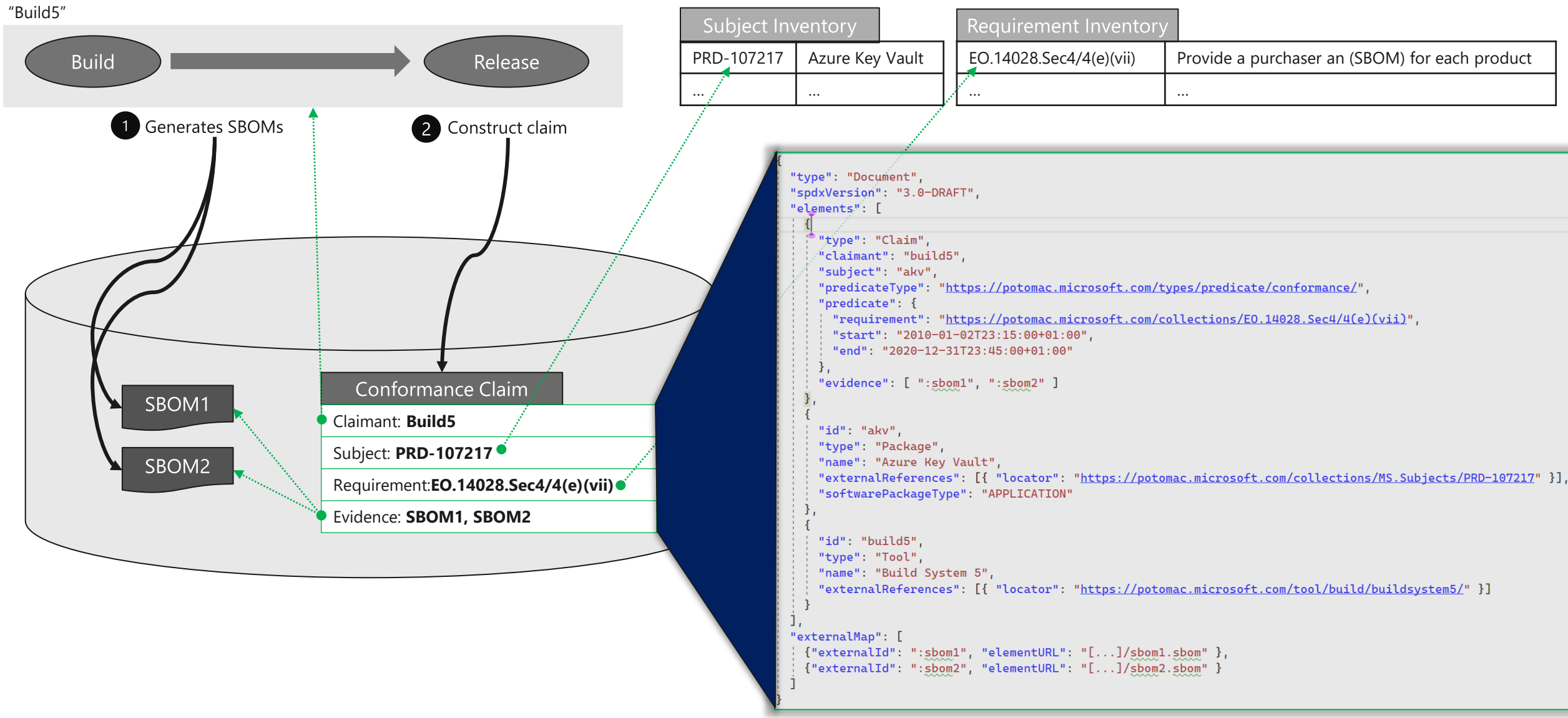


SBOM generation at build time



For more info: [Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft - Engineering@Microsoft]

Tracking conformance



Microsoft

Thank you

NIST Executive Order on Cyber Security Workshop
November 8, 2021