SBOM

Inhaltsverzeichnis

Eine SBOM (Software Bill of Materials) listet Komponenten und Abhängigkeiten einer Software. So lassen sich Schwachstellen und Lizenzrisiken schneller den betroffenen Systemen zuordnen.

1 Funktionsweise

Build- oder Scanner-Prozesse erzeugen eine Stückliste (z. B. SPDX/CycloneDX) mit Libraries, Versionen und Lieferkettenbezug. Bei neuen CVEs kann gezielt geprüft werden, ob man betroffen ist.

- **Inventar:** was steckt in Image/App
- **Formate:** maschinenlesbare Standards
- **Abgleich:** CVE-/Policy-Matching

2 Typische Einsatzbereiche

- Container- und Application Security
- Lieferkettenanforderungen und Audits
- Reaktion auf kritische Library-Schwachstellen

3 Wichtige Hinweise

- SBOM ohne Prozesse zur Auswertung nutzt wenig.
- Transitive Dependencies nicht vergessen.
- Erzeugung in CI automatisieren.

4 Fazit

SBOMs machen Software-Lieferketten sichtbar – Grundlage für schnelle, evidenzbasierte Reaktion auf Abhängigkeitsrisiken.