How to Generate and Consume SBOMs

Tooling, CI integration, and vulnerability correlation

Step 1: Choose Format and Tooling

Two dominant formats — pick one and standardize:

- CycloneDX (recommended): JSON/XML, rich vulnerability data, OWASP-backed
- SPDX: ISO standard (ISO/IEC 5962:2021), better for license compliance
- Generation tools: Syft (containers), cdxgen (applications), Trivy (both)

Step 2: Integrate into CI Pipeline

Generate SBOMs automatically on every release build:

- Add SBOM generation step after build, before artifact publishing
- Store SBOM alongside release artifact in registry
- Sign SBOM with same key used for artifact signing
- Validate SBOM schema before storage (cyclonedx-cli validate)

Step 3: Consume and Monitor

SBOMs are only valuable if you use them:

- Feed SBOMs into vulnerability database (OSV, NVD) for continuous monitoring
- Set up alerts when new CVEs affect components in your SBOMs
- Use SBOMs for incident response: 'which systems use Log4j 2.14?'
- Share SBOMs with customers/partners per contractual or regulatory requirements