SBOM Generation & Verification Checklist

CycloneDX/SPDX compliance and SLSA levels

SBOM Generation

- ■ Select format: CycloneDX (recommended) or SPDX
- ■ Integrate SBOM generation into CI build pipeline
- ■ Include all direct and transitive dependencies
- ■ Include license information for all components
- ■ Generate SBOM for container images (Syft, Trivy)

SBOM Verification

- ■ Validate SBOM against schema (CycloneDX/SPDX validator)
- ■ Cross-reference SBOM components against vulnerability databases
- ■ Verify completeness (compare package manager lock files)
- ■ Store SBOMs alongside release artifacts in registry

SLSA Compliance

- ■ SLSA Level 1: Documented build process
- ■ SLSA Level 2: Version-controlled build definition, hosted build service
- ■ SLSA Level 3: Hardened build platform, non-falsifiable provenance
- ■ Provenance attestation generated and signed for each build