Syft Generate software SBOMs

CONCEPTS

> Syft only lists what it can find in the source: packages and files, not vulnerabilities. Feed the SBOM to Grype or Trivy to scan it.

Source image, dir, archive, file
↓ `catalogers`
Syft finds packages
↓ `-o format`
SBOM SPDX, CycloneDX, JSON
↓ `grype / attest`
Scan or sign Grype, Trivy, Cosign
From source to SBOM

> With no scheme, Syft tries the Docker daemon, then Podman, then containerd, then pulls from the registry. Pin it with --from or a scheme prefix.

SOURCES

`syft <image>`
Scan an image (daemon, else registry)

`syft dir:<path>`
Scan a directory

`syft <path>`
Directory, archive or SIF by path

`syft registry:<image>`
Pull from registry, skip the daemon

`syft docker:<image>`
Use the Docker daemon only

`syft --from <source> <target>`
Choose the source type explicitly

`syft docker-archive:<tar>`
Tarball from docker save

`syft <image> --platform <os/arch>`
Pick a platform of a multi-arch image

OUTPUT

`syft <src> -o json`
Syft JSON, all details

OUTPUT (cont.)

`syft <src> -o spdx-json`
SPDX as JSON

`syft <src> -o cyclonedx-json`
CycloneDX as JSON

`syft <src> -o <fmt>=<file>`
Write that format to a file

`syft <src> -o <fmt1>=<f1> -o <fmt2>=<f2>`
Several formats in one scan

SCOPE AND FILTERING

`syft <image> --scope squashed`
Final filesystem only (default)

`syft <image> --scope all-layers`
Packages from every layer

`syft <src> --exclude '<glob>'`
Skip paths matching a glob

`syft <src> --exclude '**/node_modules/**'`
Ignore dependency folders

`syft <src> --select-catalogers <expr>`
Add or drop catalogers by name or tag

CONVERT AND ATTEST

`syft convert <sbom> -o <fmt>`
Convert an SBOM to another format

`syft convert <sbom> -o <fmt>=<file>`
Convert into a file

`syft attest -o <fmt> <image>`
SBOM as in-toto attestation, keyless

`syft attest --key cosign.key -o <fmt> <image>`
Attest with a local key

CONFIG AND CLI

`syft --version`
Print the version