Supply-Chain Capture

Go up to Terms and Definitions

Discussion

Supply-Chain Capture is the controlled process of identifying, collecting, recording, and preserving the inputs, dependencies, artifacts, relationships, and evidence associated with the production and delivery of a system or software artifact.

The process may capture source revisions, installation media, packages, libraries, machine images, container images, infrastructure providers, build tools, compliance content, manifests, integrity values, licenses, and Provenance.

Supply-Chain Capture extends beyond Dependency Capture when it records the broader relationships among suppliers, sources, transformations, tools, processes, artifacts, and delivery mechanisms.

Within Crucible, Supply-Chain Capture supports reproducible builds, disconnected operations, transfer-bundle creation, verification, Auditability, and Supply-Chain Integrity.

Definition

controlled process of identifying, collecting, recording, and preserving the inputs, dependencies, artifacts, relationships, and evidence associated with the production and delivery of a system or software artifact

Source

Generalized from software supply-chain management, dependency management, provenance, configuration management, and reproducible-build practice and specialized for the Crucible architecture and operational model.

Note

Supply-Chain Capture does not require every external service or organizational relationship to be copied into a local store. The capture may preserve a controlled record or evidence reference when the original entity cannot be transferred.

The defined capture scope should identify which lifecycle stages, dependency classes, artifacts, and relationships the process covers.

Example

Crucible captures the source revisions, Red Hat Enterprise Linux (RHEL) 9 installation media, downloaded packages, Ansible collections, Packer plugins, compliance content, scan results, image digests, and provider registration information associated with a Hardened Image.
