

# Leveraging **SBOMS** to Automate Packaging, Transfer, and Reporting of Dependencies Between Secure Environments

---

CloudNativeSecurityCon

## **PRESENTER**

Ian Dunbar-Hall  
Jerod Heck

## **DATE**

Feb 2nd 2023



# Introductions



**Ian Dunbar-Hall**

Lockheed Martin Software Factory Chief Engineer



**Jerod Heck**

Lockheed Martin Software Factory Product Architect

# Premise

## Common Practice

- SBOMS are often a build artifact and used for compliance or tracking

## Consider SBOMs as a packaging definition or interface

- What if it were used to package dependencies instead of just an artifact?
- It becomes a package type independent method for defining dependencies

# Problem

**It sucks being a developer in disconnected strict environments!**

- Slow to get packages approved
- Slow to get package updates
- Way too much paperwork
- Lots of “rinse and repeat”

**Is there a way to ...**

- Automate the patching, compliance, and delivery of build dependencies to “strict environments”?
- Can this be done using existing tooling?
- Can this be automated for multiple teams in a single dataflow?
- Can many artifacts be collected from many different sources at once?



A yellow and orange hopper-style airplane with a white banner attached to its tail.

Hoppr™

The Lockheed Martin logo, featuring the company name and a stylized star symbol.

LOCKHEED MARTIN

- **Hoppr™** is a framework for defining, validating, and transferring dependencies between environments using **Software Bill of Materials (SBOM) Open Source Standards.**
- **Hoppr™** is a solution for delivering a well-defined, repeatable bundle to secure environments combating customer problems with digital asset delivery.



# Leveraging Other Excellent Projects

## Automate Dependency Updates

➤ **Renovate** detects updates to packages, container images, and other projects in gitlab.

## Semantic version generate

➤ **Semantic Release** used to create semantic versioned releases based on conventional commit messages

When pair together, you have the ability to create semantic versioned SBOMs which are updated automatically with dependency updates.

**Hoppr™** consumes these semantic versioned **SBOMs** to collect, validate, and delivery of “stuff” to a strict environment. Since these updates are triggered by renovate, this results in a continuous delivery pipeline.



# Multiple teams, Single Process

## Renovate Maintains:

- Upstream “patching” of build dependencies
- Hoppr included project changes

## Semantic Release

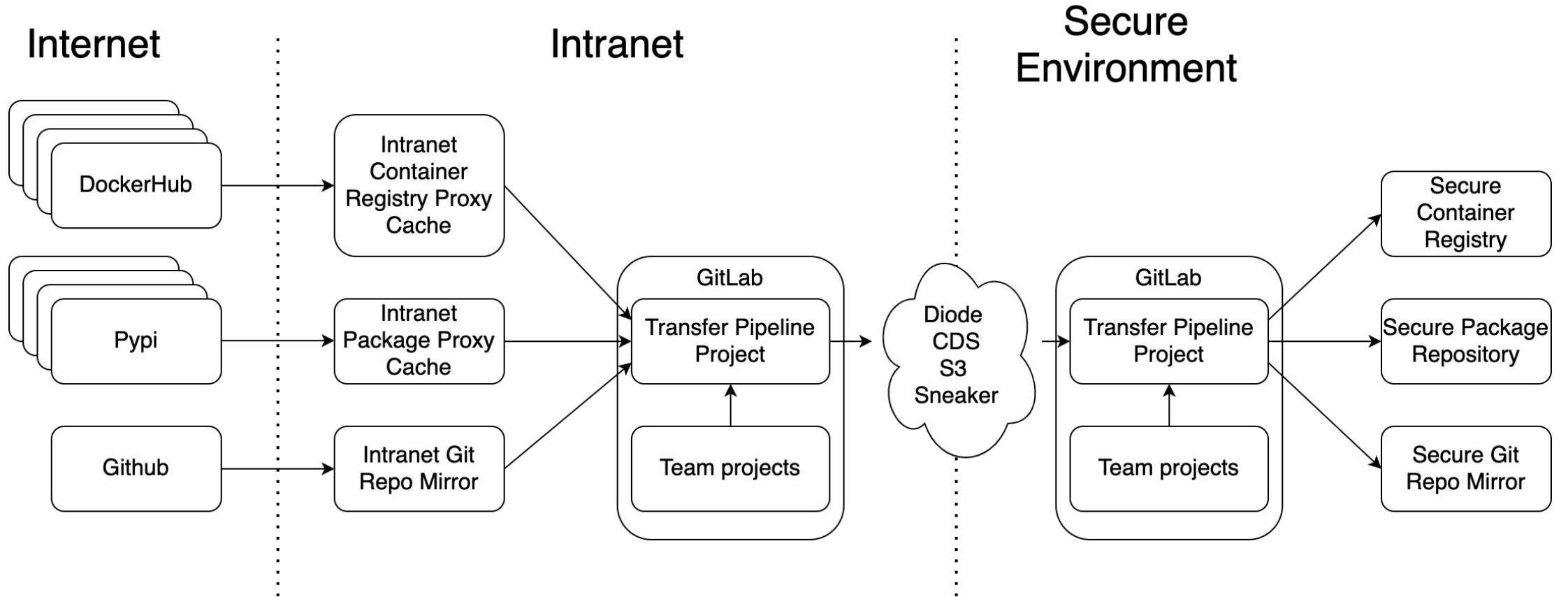
provides semver of internal products



# Hoppr Machine

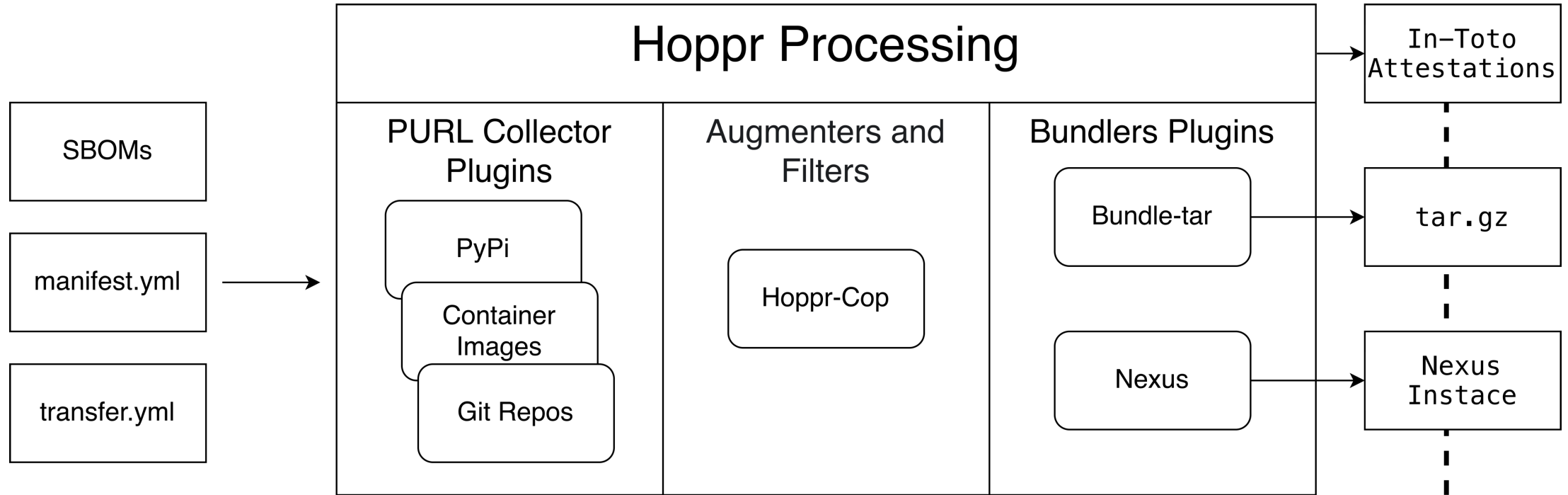


# Dataflow

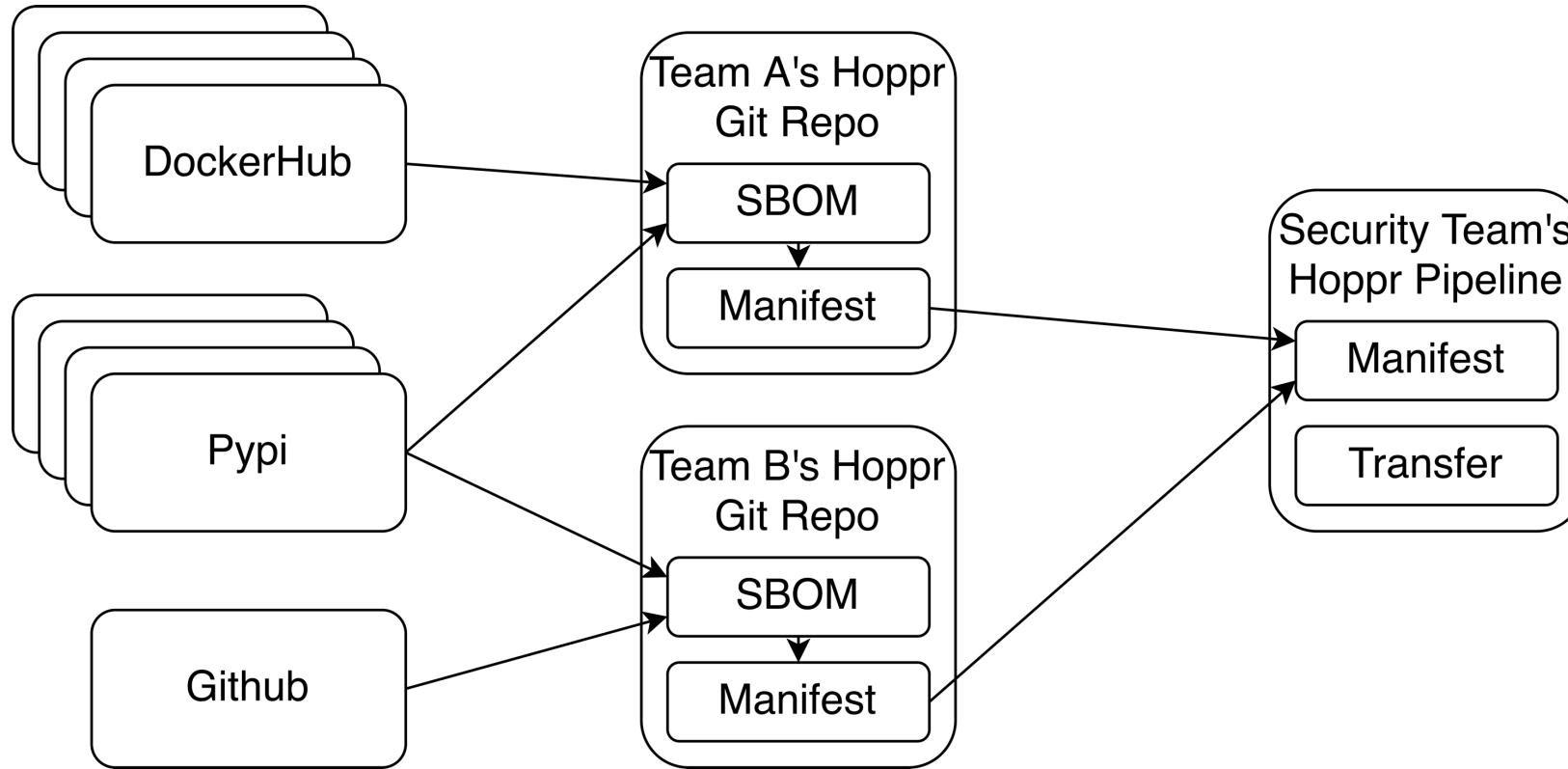




# Appflow



# Project Dependency Updates



# Hurdles

- **Incomplete SBOM metadata for security approvals**
  - Lack of tooling or incomplete BOMs
- **Generate** compliance documentation in custom formats
- **Legacy** approval processes
- **Ability to restrict** source repositories
- **Ability to detect** new packages in partially connected networks to address security patching
- **Ability to automate** collection of build dependencies in a consistent manner across teams
- **Delivery** into environments with one way connectivity



# Advantages

- Reproducible Releases
- Continuous detection of patched dependencies push to an disconnected environment
- All components entering disconnected environment are tracked using **CycloneDX SBOMs** which can be leveraged by other opensource tooling (**like DepdencyTrack!**)
- **Hoppr™** provides process for augmenting **SBOMs** with additional data
  - Vex CVE
  - Attestation creating from collection and reports
- No manual interaction



# Demo Features

- Show dependencies between teams and projects
- Show CVE report with Hoppr-cop
- Attestation creation
- Show tar bundle

# Demo

Located in  
[gitlab.com/hoppr/examples](https://gitlab.com/hoppr/examples)

[Gitpod Demo](#)



# Future

- **Unified Report Generation**
- **Expand component validation**
  - Signature validation with rekor
  - Attestation validation with in-toto
- **OpenSSF ScoreCard SBOM augmentation**
- **Unbundling and installation on disconnected networks**
- **In-Toto Secured Digitally Attested SBOM (its-da-(s)bom)**
  - An in-toto attestation implementation for SBOMs



# Shout Outs

## Inspiration

- > Sigstore

## Communities we engage in

- > CycloneDX
- > In-toto

## Other interesting projects in this space

- > Zarf – DefenseUnicorns
- > Witness – TestifySec



# Questions?



[Hoppr.dev](https://hoppr.dev)