Microsoft

Azure

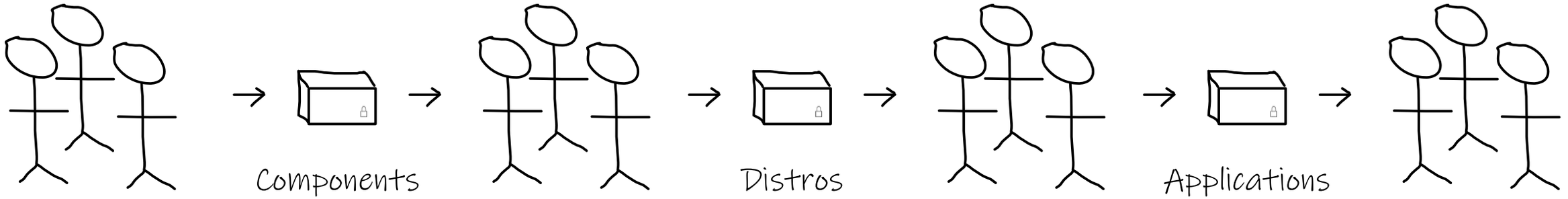
# Software Supply Chain Security

CD Summit - Lightening Talk

Kay Williams – Principal Program Manager, Azure Office of the CTO
kayw@microsoft .com

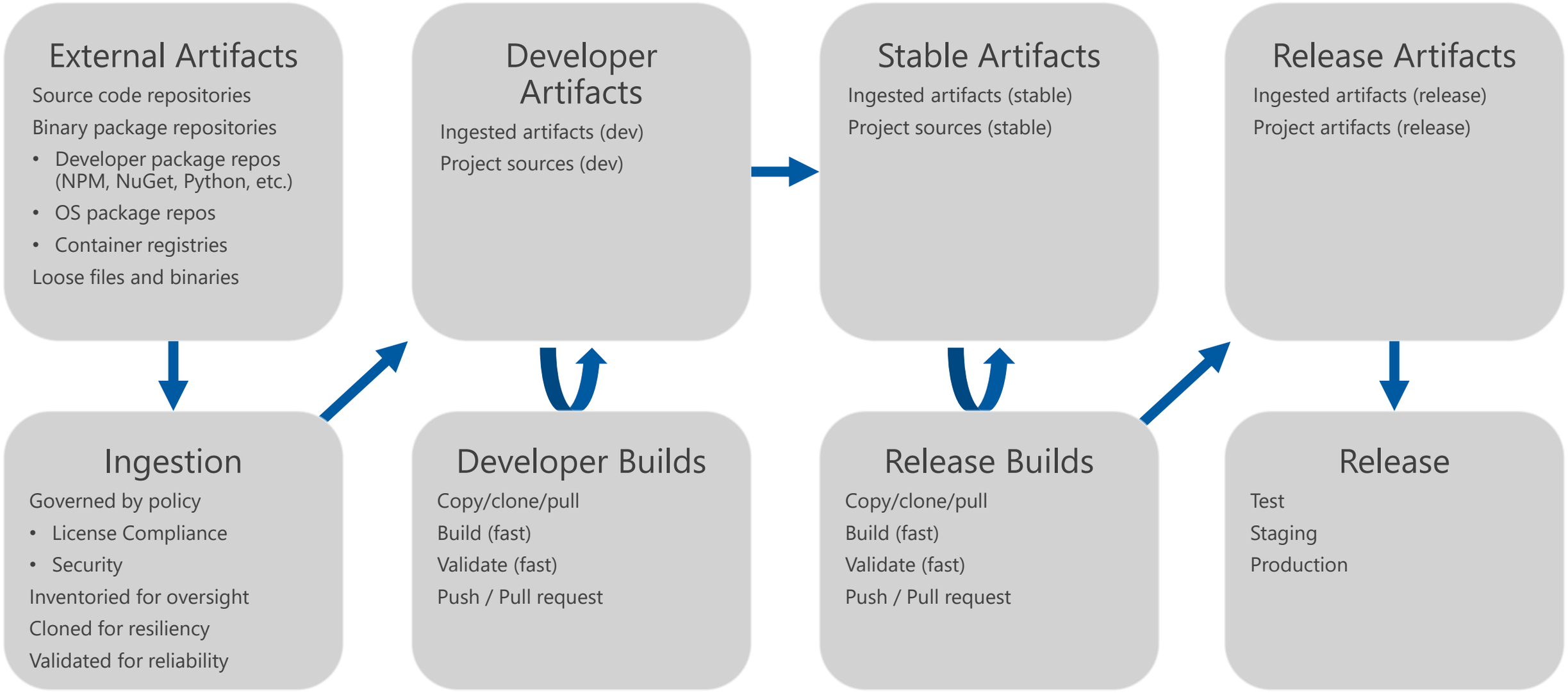
5/20/2019

# Software Supply Chain – Ecosystem

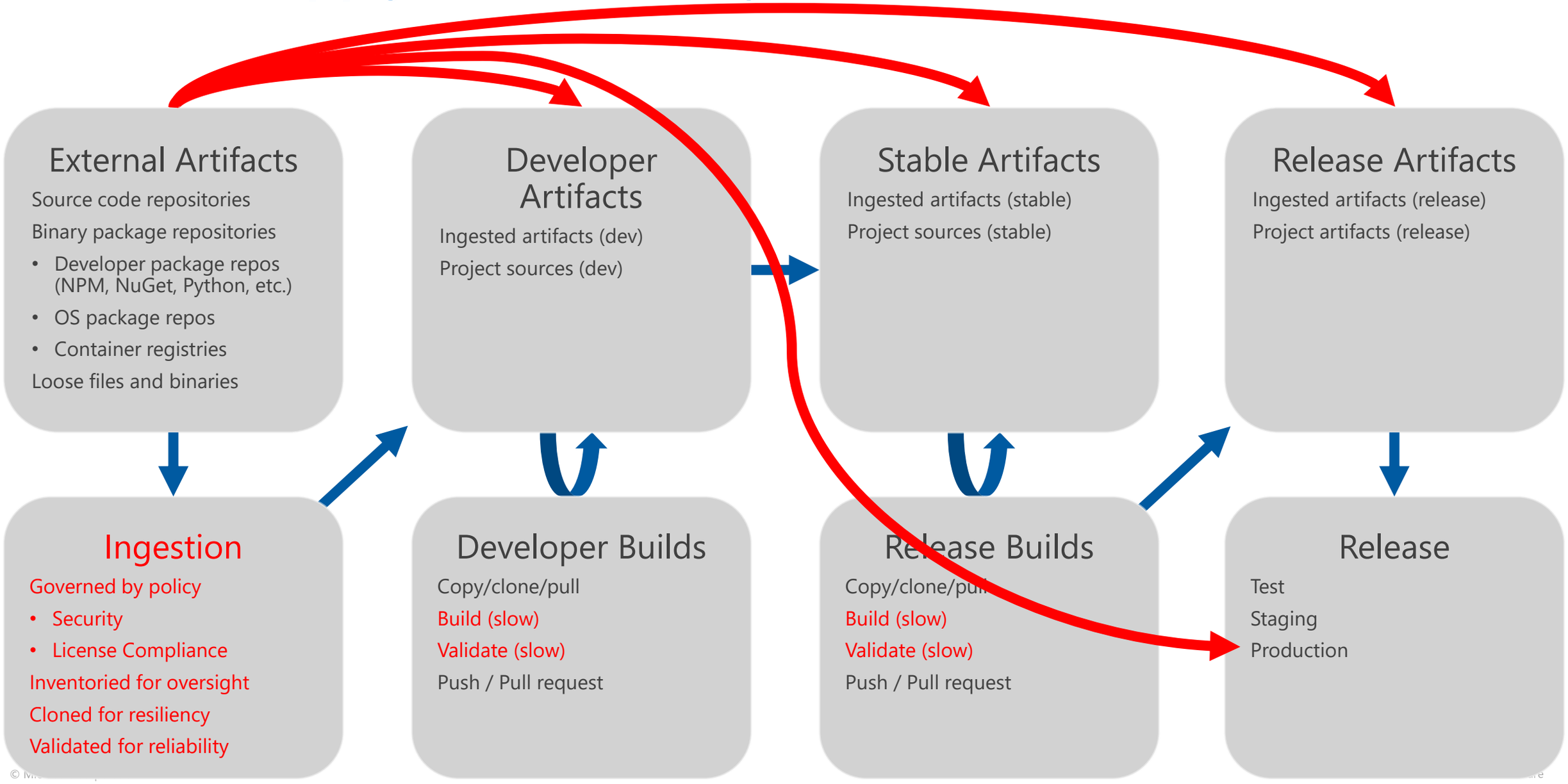



Job to be Done: As a developer, I can deliver trustworthy applications to my customers.

# Software Supply Chain - Desired



# Software Supply Chain - Today



# What do we need?

**Security Framework**

**Goal:** Software can move securely through the supply chain with signing, policy and validation at each step

e.g. https://in-toto.github.io/

Signed metadata describing artifacts (license, build steps)

Policy describing expected/allowed artifacts

Method for inspecting metadata to verify artifacts meet policy

**Reproducible Builds**

**Goal:** Verify the integrity of build environments

Software practices that allow building sources multiple times across diverse environments, comparing checksums of result

# Supply Chain Security is an Industry Issue

**Requires collaboration across tool providers**

Build/packaging tools – output signed manifests

Artifact ingestion (CI) tools – apply policy, inventory & inspect artifacts

Run-time validation tools – apply policy, inventory & inspect artifacts

# CDF & Software Supply Chain Security

- **SIG?**

# Contact

Kay Williams
kayw@microsoft.com