CD Foundation
Security SIG Proposal

Kay Williams, Open Source Strategy and Partnerships, Azure Office of the CTO

Background

March 2019 - CD Foundation Announced

May 2019 - CD Summit Barcelona

- Lightning Talk - Software Supply Chain Security
- Propose Software Supply Chain Security SIG (informal)

June 2019

- Technical Oversight Committee (TOC) introduces proposal for Working Groups (WGs) and Special Interest Groups (SIGs) for discussion and vote

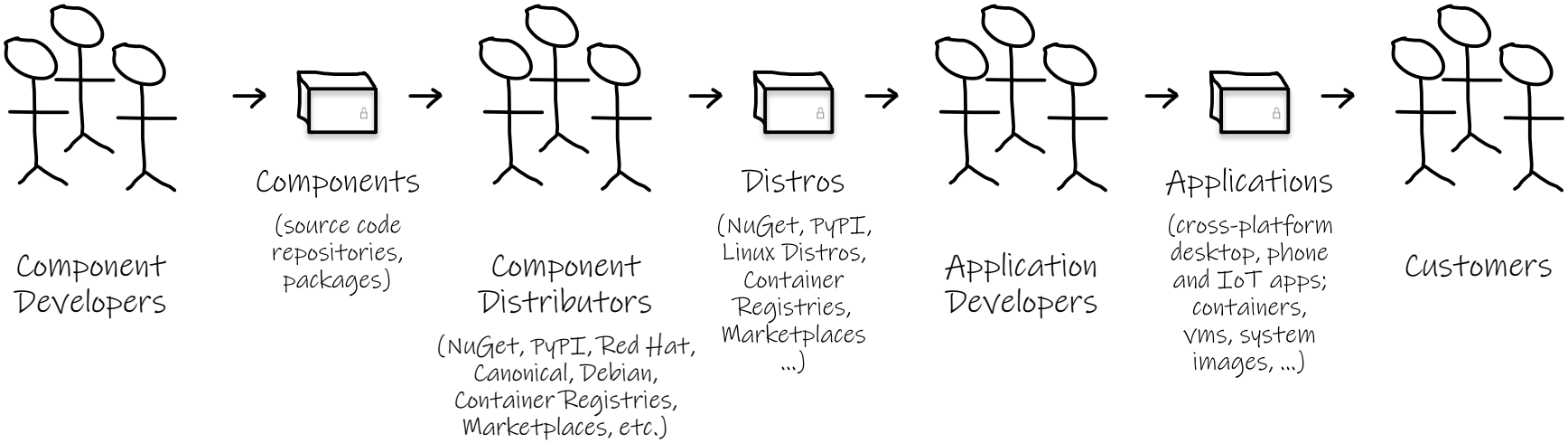
August 2019

- TOC adopts proposal for WGs and SIGs (8/12)
- Proposal for Security SIG presented to TOC

Next Steps

- Proposal for Security SIG - discussion and vote
- Creation of Software Supply Chain Security working group

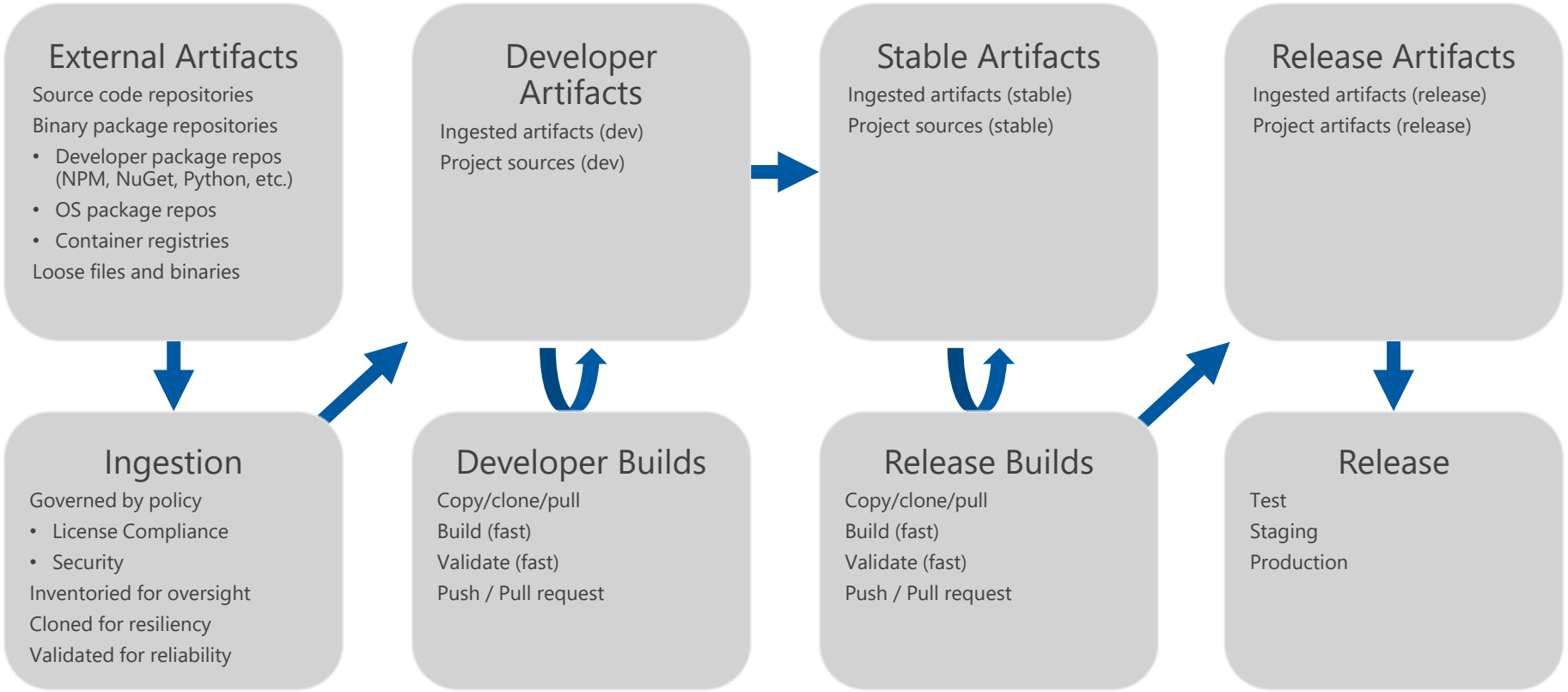
Software Supply Chain – Ecosystem



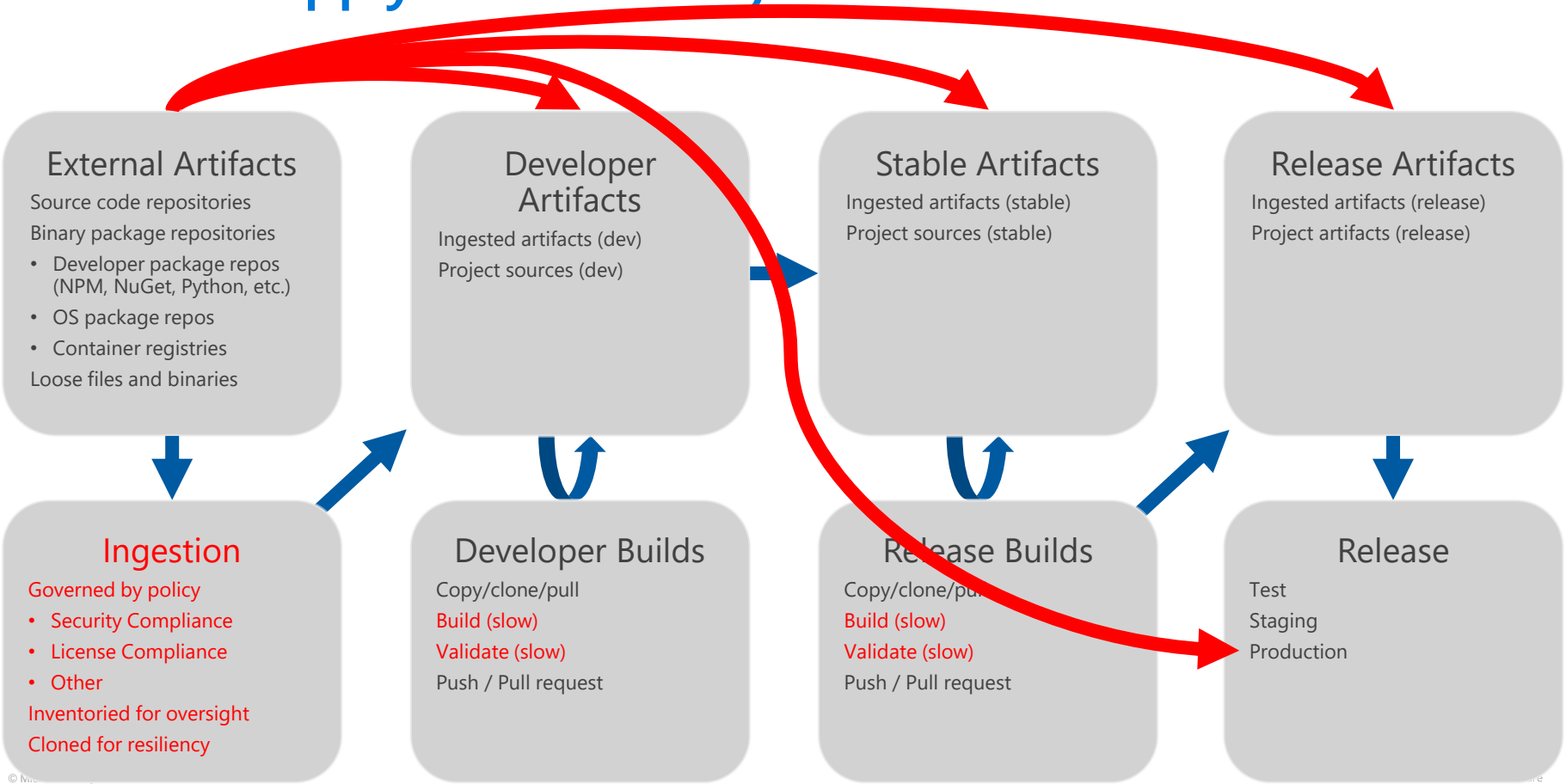
Job to be Done: As a developer, I can deliver trustworthy applications to my customers.

CD.FOUNDATION

Software Supply Chain - Desired



Software Supply Chain - Today



Software Supply Chain Security is an Industry Issue

Requires collaboration across tool providers

- Continuous integration tools – ingest, apply policy, inventory, cache external artifacts
- Build tools – output metadata describing built artifacts, including instructions to rebuild and validate
- Packaging tools – output metadata describing built packages, including instructions to rebuild and validate
- Install and update tools – apply policy, validate artifacts

What do we need?

Industry Wide…

Software Supply Chain Security Framework

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

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

Upcoming Talks and Events

DevOps World

- Wednesday 8/14 5:05 PM
- Software Supply Chain Security (Microsoft and in-toto)

CD Summit – San Diego

- Tuesday November 18th – San Diego
- Sessions/talks around Software Supply Chain Security (Under Planning)

Questions / Want to get involved?

Watch TOC Mailing List
Participate in CD Summit Planning

Contact:
Kay Williams
kayw@microsoft.com