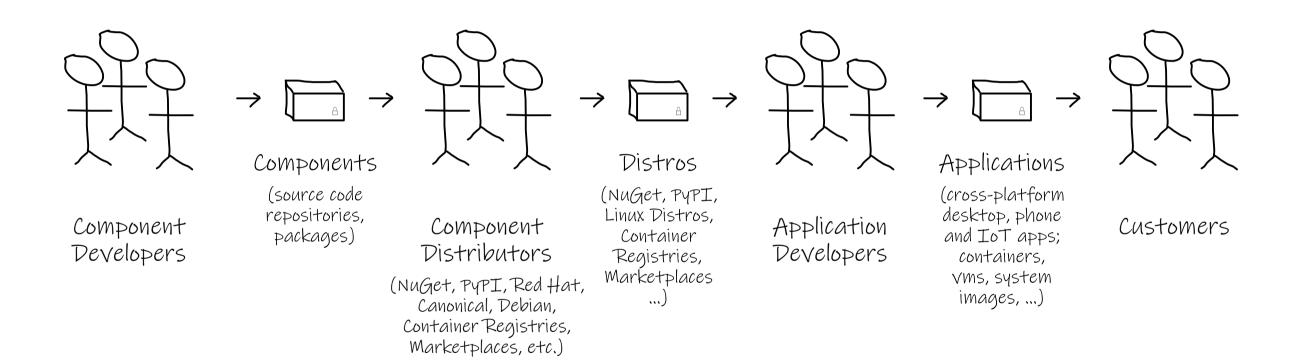
# **Software Supply Chain Security**

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**

#### **External Artifacts**

Source code repositories

Binary package repositories

- Developer package repos (NPM, NuGet, Python, etc.)
- OS package repos
- Container registries

Loose files and binaries

#### Developer Artifacts

Ingested artifacts (dev)
Project sources (dev)

#### Stable Artifacts

Ingested artifacts (stable)
Project sources (stable)

#### Release Artifacts

Ingested artifacts (release)
Project artifacts (release)



## U



#### Release Builds

Copy/clone/pull

Build (fast)

Validate (fast)

Push / Pull request



#### Release

Test

Staging

Production

### Ingestion

Governed by policy

- License Compliance
- Security

Inventoried for oversight

Cloned for resiliency

Validated for reliability

#### Developer Builds

Copy/clone/pull

Build (fast)

Validate (fast)

Push / Pull request

© Microsoft Corporation

### **Software Supply Chain - Today**

#### **External Artifacts**

Source code repositories

Binary package repositories

- Developer package repos (NPM, NuGet, Python, etc.)
- OS package repos
- Container registries

Loose files and binaries

#### Developer Artifacts

Ingested artifacts (dev)
Project sources (dev)

#### Stable Artifacts

Ingested artifacts (stable)
Project sources (stable)

#### Release Artifacts

Ingested artifacts (release)
Project artifacts (release)



### Ingestion

Governed by policy

- Security
- License Compliance
   Inventoried for oversight
   Cloned for resiliency
   Validated for reliability



#### Developer Builds

Copy/clone/pull

Build (slow)

Validate (slow)

Push / Pull request



#### Release Builds

Copy/clone/pun

Build (slow)

Validate (slow)

Push / Pull request



#### Release

Test

Staging

Production

### 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. <a href="https://in-toto.github.io/">https://in-toto.github.io/</a>

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

© Microsoft Corporation Azure

### 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

© Microsoft Corporation Azure

## **CDF & Software Supply Chain Security**

• SIG?

© Microsoft Corporation

## Contact

Kay Williams kayw@microsoft.com

© Microsoft Corporation Azure