Software Supply Chain

Understanding and Addressing Risk in OSS

Michael Winser - Google


Why Now?

Three Kinds of Security Attacks

Front door

Back door

Underground

A very long time ago

Monolithic Application

SDK

Big Thick Operating System

Microservices Application

A Mountain of Open Source Dependencies

Wafer Thin Container

Michael doesn't code anymore


Software Supply Chain Risk

Correctness

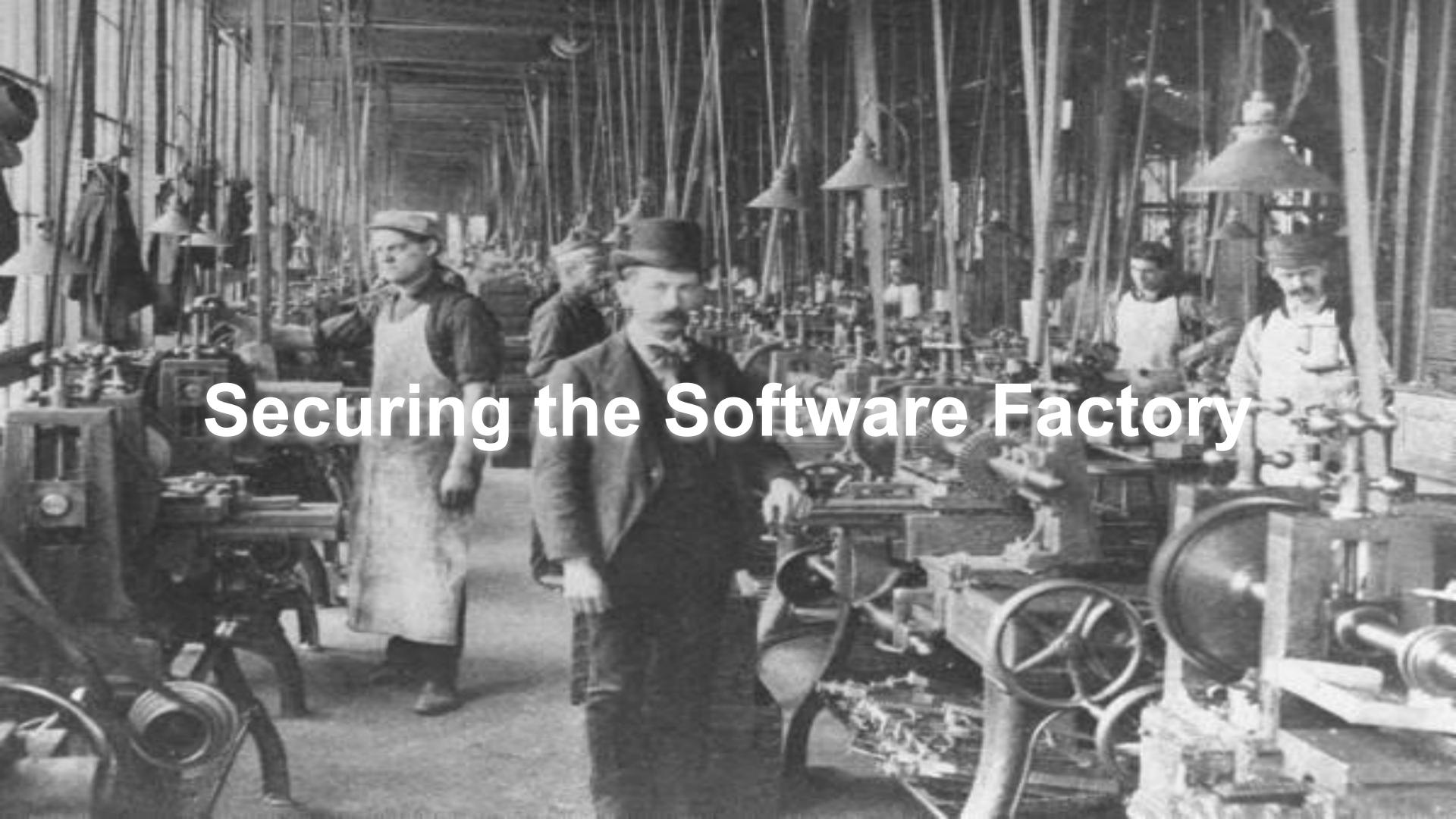
Does the code have vulnerabilities that increase risk

Integrity

Has the code been modified from source to production

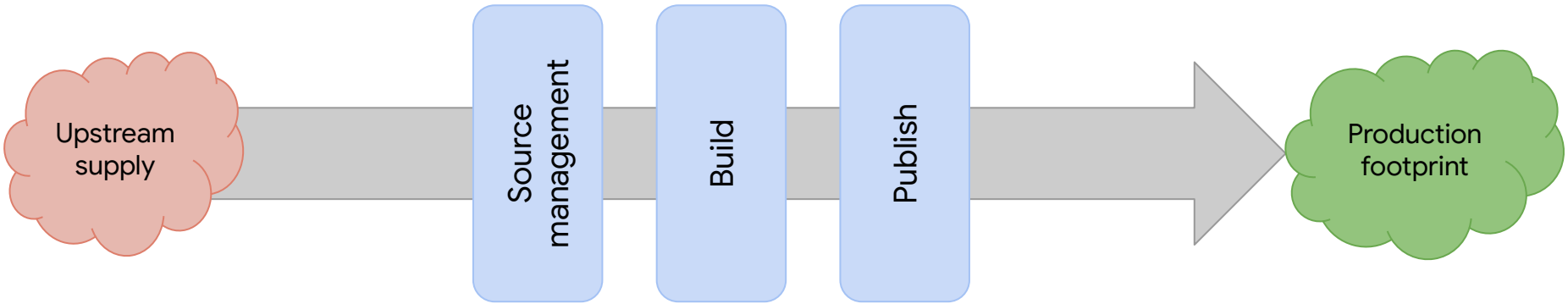
Availability

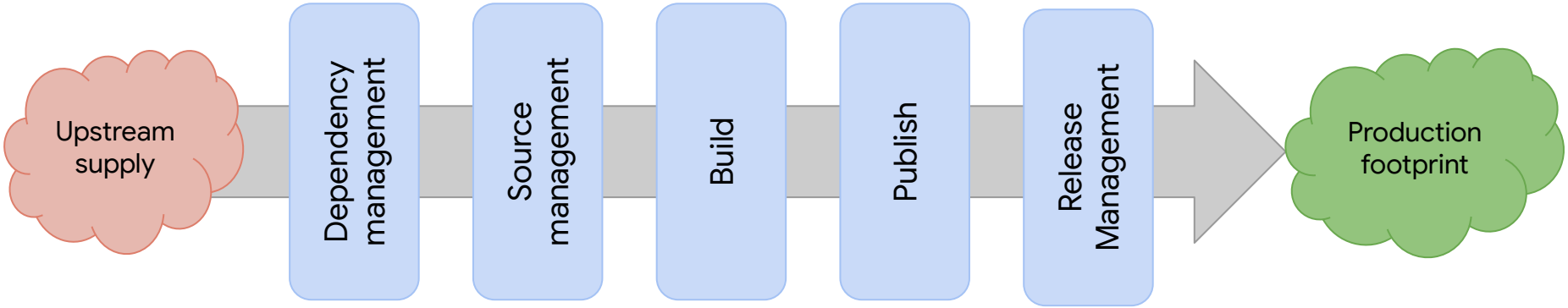
Is the code available to keep building software

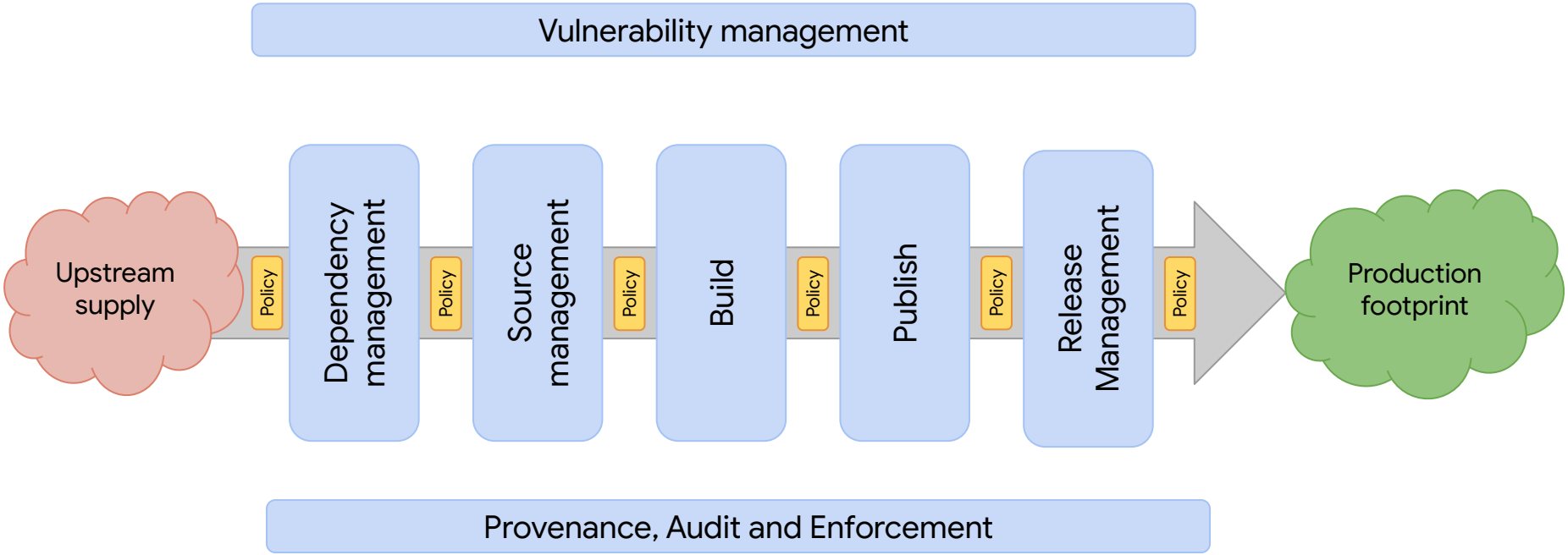

Securing the Software Factory

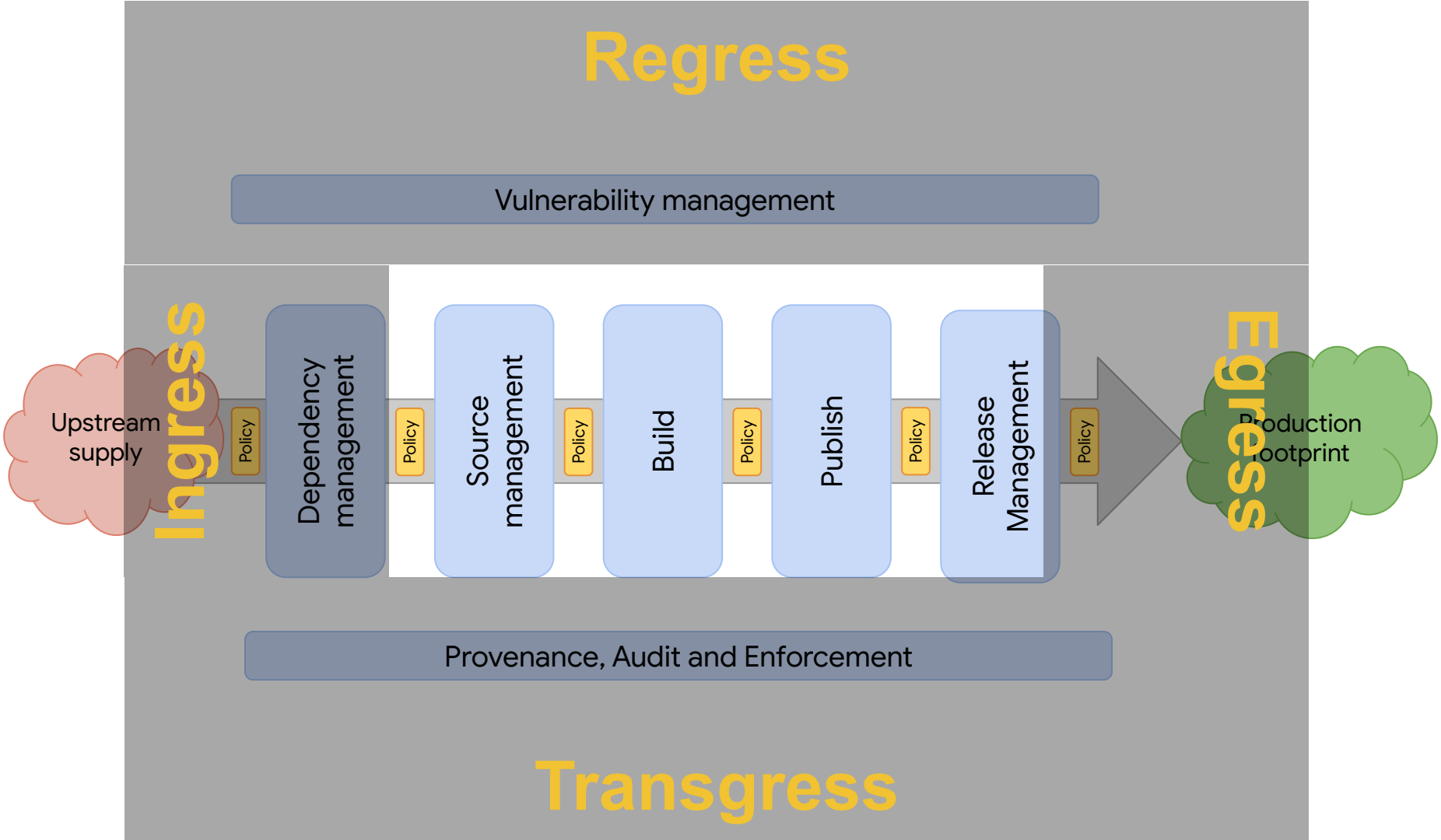
What Could Possibly Go Wrong?

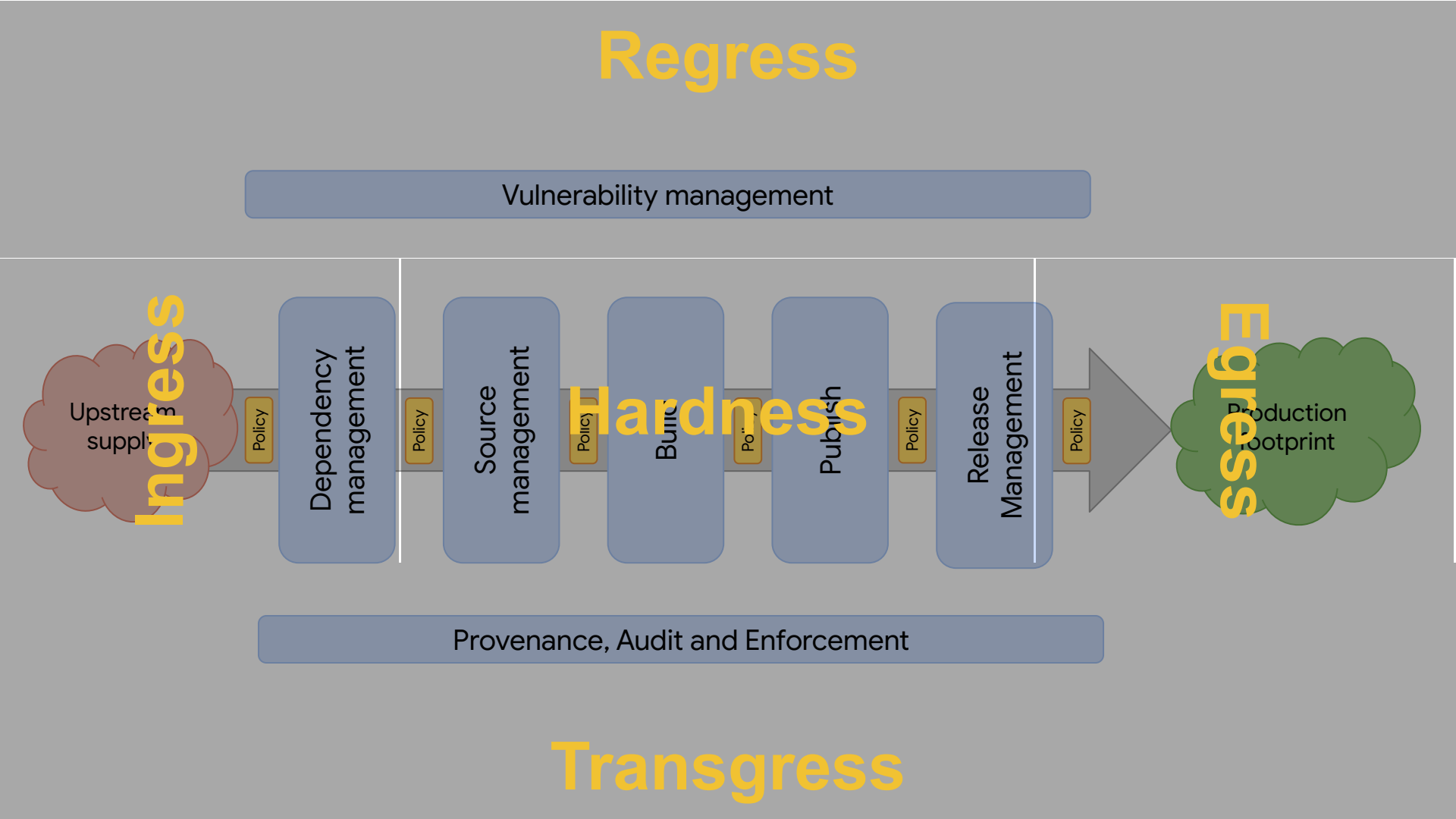
```
npm install foo
```


Upstream supply
Source management
Build
Publish
Production footprint


Upstream supply
Dependency management
Source management
Build
Publish
Release Management
Production footprint

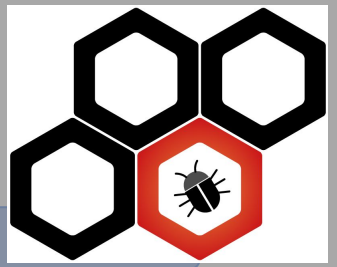

Vulnerability management
Upstream supply
Policy
Dependency management
Policy
Source management
Policy
Build
Policy
Publish
Policy
Release Management
Policy
Production footprint
Provenance, Audit and Enforcement


Regress
Vulnerability management
Ingress
Upstream supply
Policy
Dependency management
Policy
Source management
Policy
Build
Policy
Publish
Policy
Release Management
Policy
Egress
Production Footprint
Provenance, Audit and Enforcement
Transgress


Regress
Vulnerability management
Ingress
Upstream supply
Policy
Dependency management
Policy
Source management
Policy
Build
Policy
Publish
Policy
Release Management
Policy
Hardness
Egress
Production footprint
Provenance, Audit and Enforcement
Transgress

Open Source Vulnerabilities

OSV



OSS Fuzz

Scorecards

Policy

Dependency management

Policy

Source management

Policy

Build

Policy

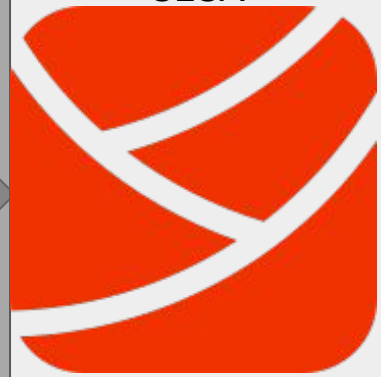
Publish

Policy

Release Management

Policy

SLSA



Provenance, Audit and Enforcement

sigstore

What About Right Now?

Alpha-Omega

Joint $5M investment by Microsoft and Google

Alpha: Direct research and engagement on top OSS projects

Omega: Scaled approach to the next 10,000 projects

Over $1.3M invested in Node, Python, Rust, Eclipse

10 Vulnerabilities reported, 50% fixed

~100 fully automated security reviews done against npm modules

Open source vulnerability detection toolkit

Resources

Scorecards: https://securityscorecards.dev/

Open Source Vulnerabilities: https://osv.dev/

Sigstore: https://www.sigstore.dev/

Open Source Insights: https://deps.dev/

OSS Fuzz: https://google.github.io/oss-fuzz/

Alpha Omega: https://openssf.org/community/alpha-omega/

Alpha Omega Toolkit https://github.com/ossf/alpha-omega

DORA: https://cloud.google.com/devops/state-of-devops