Exploring Policy as Code

May 2021 | OWASP DevSlop

Rosemary’s first security incident...

- Insecure development environments
- Infrastructure as code probably would have helped
- We forgot about 0.0.0.0/0
- We didn’t know what we should have known

Rosemary Wang

Developer Advocate
HashiCorp
she/her
@joatmon08

Tracy Holmes

Open Source Engineer
VMware
she/her
@tracypholmes

1. Introduction to Policy as Code
2. Using static analysis for configuration
3. Using dynamic analysis for runtime configuration
4. Adding policy as code to delivery pipelines

Introduction to Policy as Code

Policy

What is it?

Ensures systems comply with security, audit, and organizational requirements.

Depends on industry, organization size, country, and more.

Which is not considered a policy?

A. Development should not communicate with production.

B. Write an application in Java.

C. Password should not be older than 30 days.

D. Two different people must approve for production.

E. All cloud resources must be tagged.

Which is not considered a policy?

A. Development should not communicate with production.

B. Write an application in Java.

C. Password should not be older than 30 days.

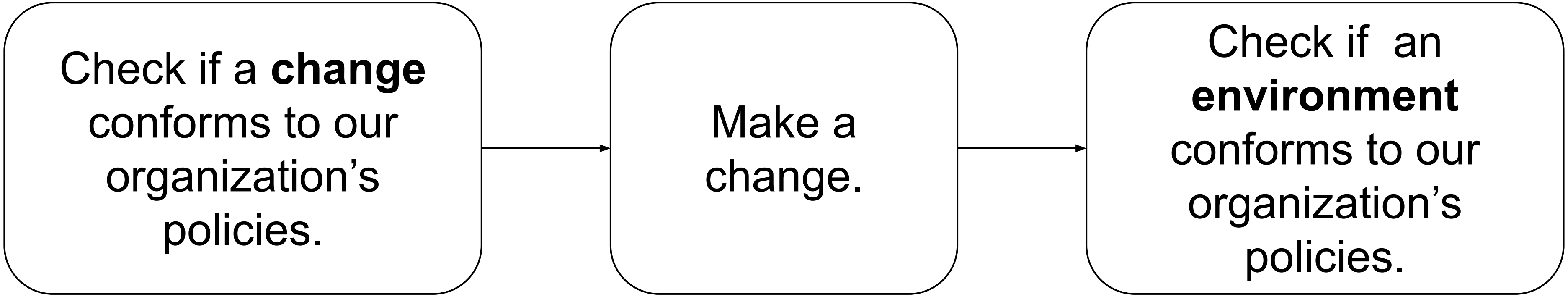
D. Two different people must approve for production.

E. All cloud resources must be tagged.

Policy as Code

What is it?

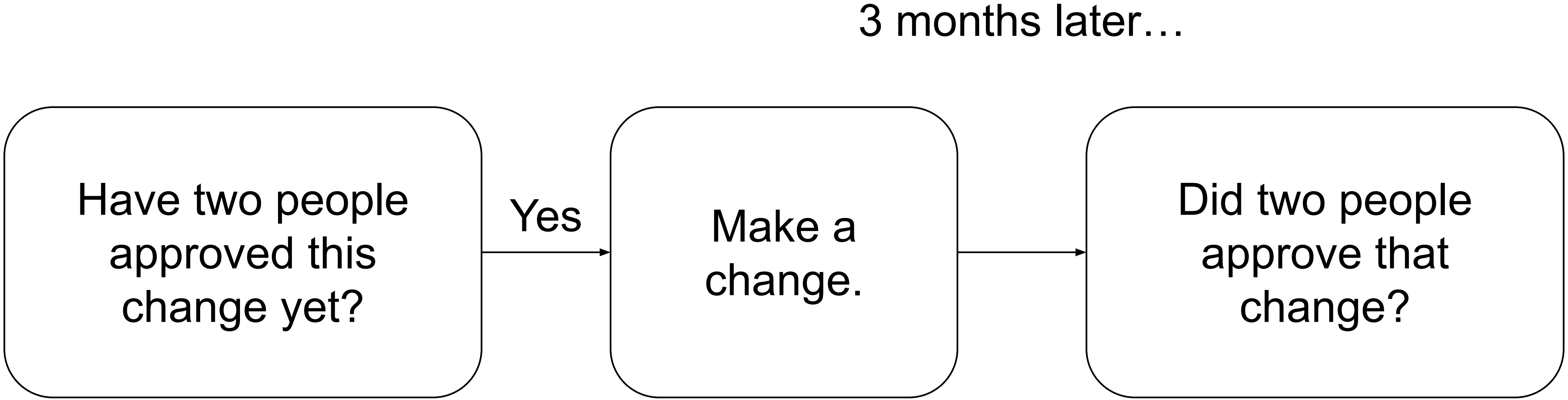
The **management** of an organization’s policies **with code** to ensure the conformance of changes.



Check if a **change** conforms to our organization’s policies.

Make a change.

Check if an **environment** conforms to our organization’s policies.



3 months later…

Have two people approved this change yet?

Yes

Make a change.

Did two people approve that change?

Policy as Code

Why do it?

Communicate policy requirements across teams.

Make unknown knowns into knowns.

Prevent policy violations from going into production.

Policy as Code

Codify all the policy!

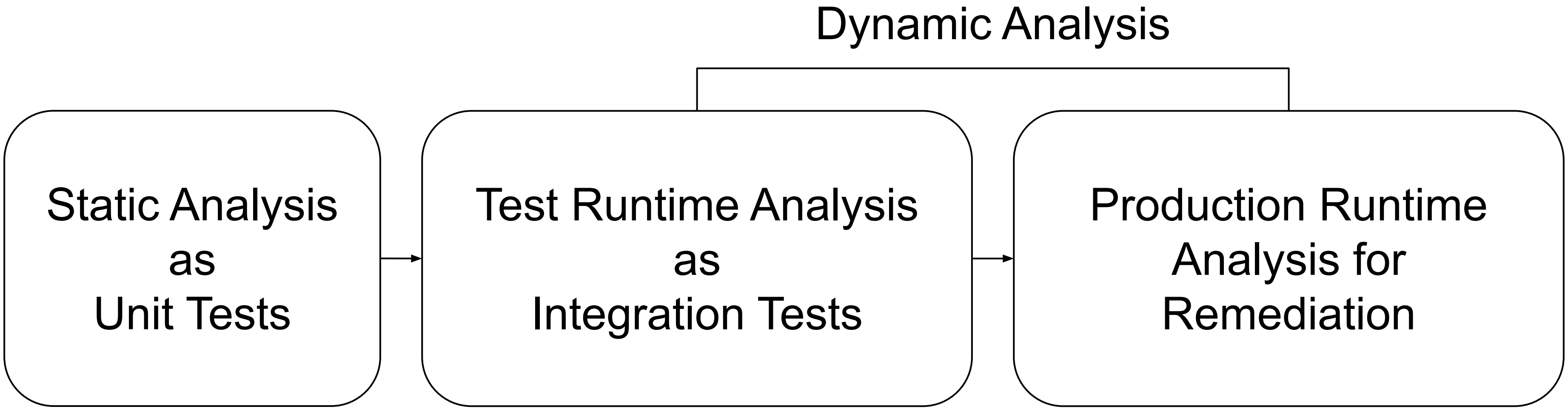
API Authorization

Network Policy

Infrastructure Configuration

Access Control Configuration

Runtime Security (e.g., Vulnerability Management)



Dynamic Analysis

Static Analysis as Unit Tests

Test Runtime Analysis as Integration Tests

Production Runtime Analysis for Remediation

Which of the following does not express policy as code?

A. Shift-left security testing of infrastructure

B. Static code analysis and scanning

C. Code quality scanning

D. Vulnerability scanning for servers

E. Root access alerting

Which of the following does not express policy as code?

A. Shift-left security testing of infrastructure

B. Static code analysis and scanning

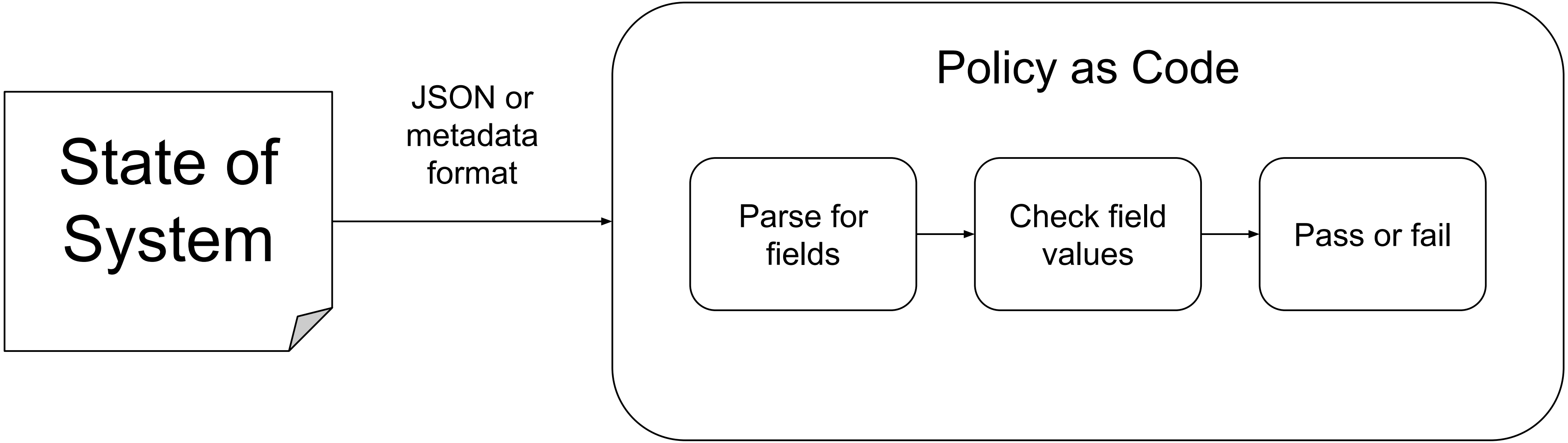
C. Code quality scanning

D. Vulnerability scanning for servers

E. Root access alerting

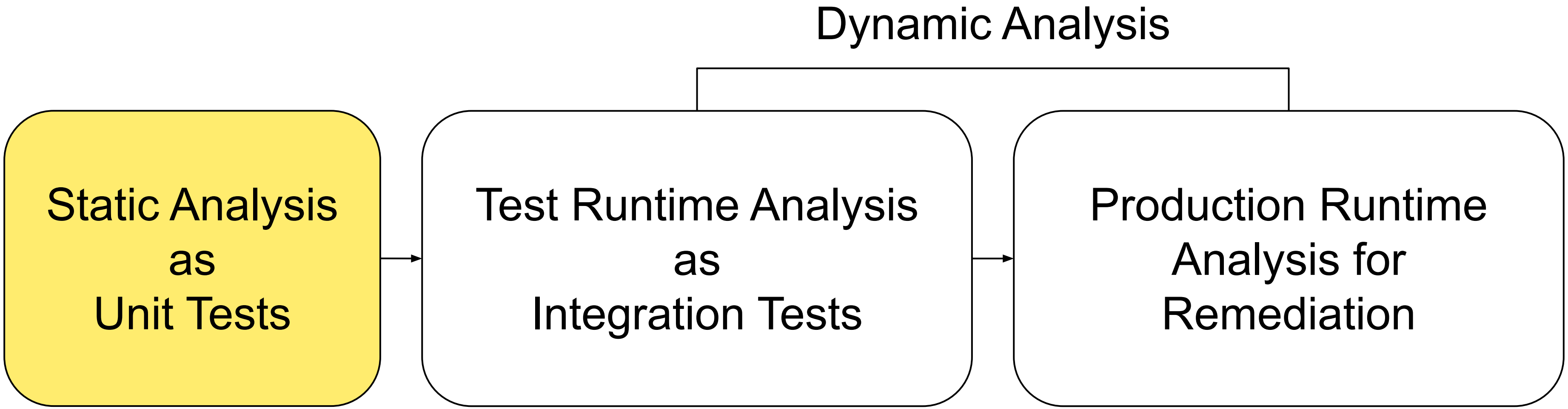
F. None of the above

Policy as Code Tools



02 **OWASP DevSlop** / Policy as Code

Using static analysis



Dynamic Analysis

Static Analysis as Unit Tests

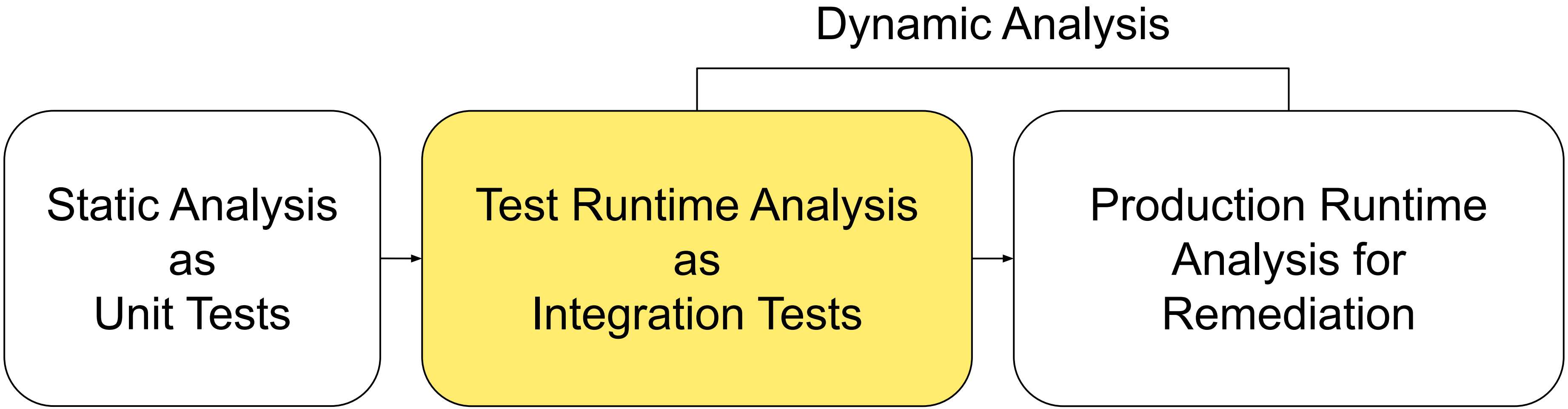
Test Runtime Analysis as Integration Tests

Production Runtime Analysis for Remediation

github.com/tracypholmes/policy-as-code-workshop

03 **OWASP DevSlop** / Policy as Code

Using dynamic analysis



Dynamic Analysis

Static Analysis
as
Unit Tests

Test Runtime Analysis
as
Integration Tests

Production Runtime
Analysis for
Remediation

github.com/tracypholmes/policy-as-code-workshop

04 **OWASP DevSlop** / Policy as Code

Adding to delivery pipelines

Policy Gates for Production

Choose a level.

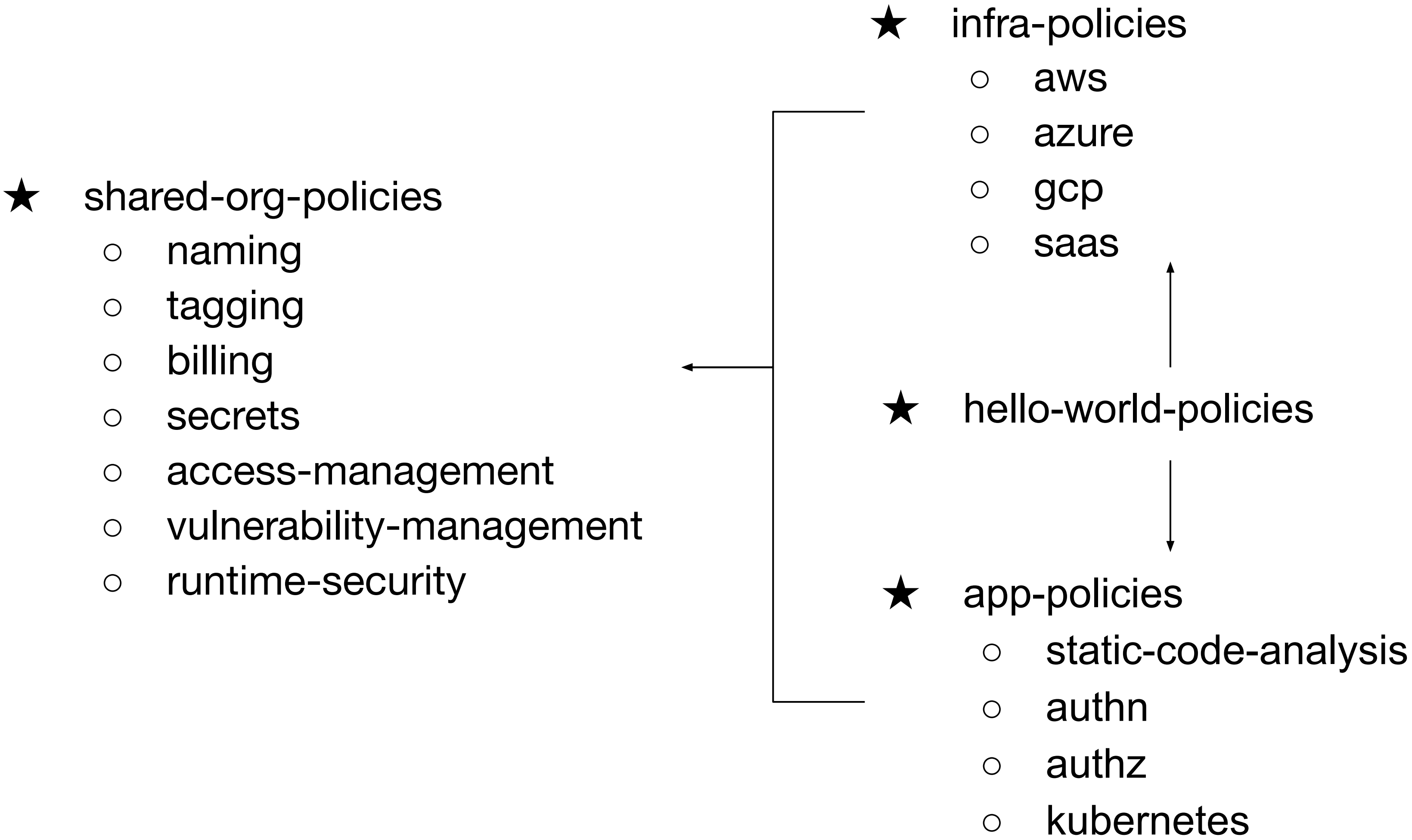
- Hard mandatory - policy must pass
- Soft mandatory - someone can manually override
- Advisory - informational / warning

(Terminology borrowed from HashiCorp Sentinel)

Sharing Policy as Code

Communicate context

- Modularize by business unit or application
- Version policies
- Offer shared libraries
- Consider setting enforcement level

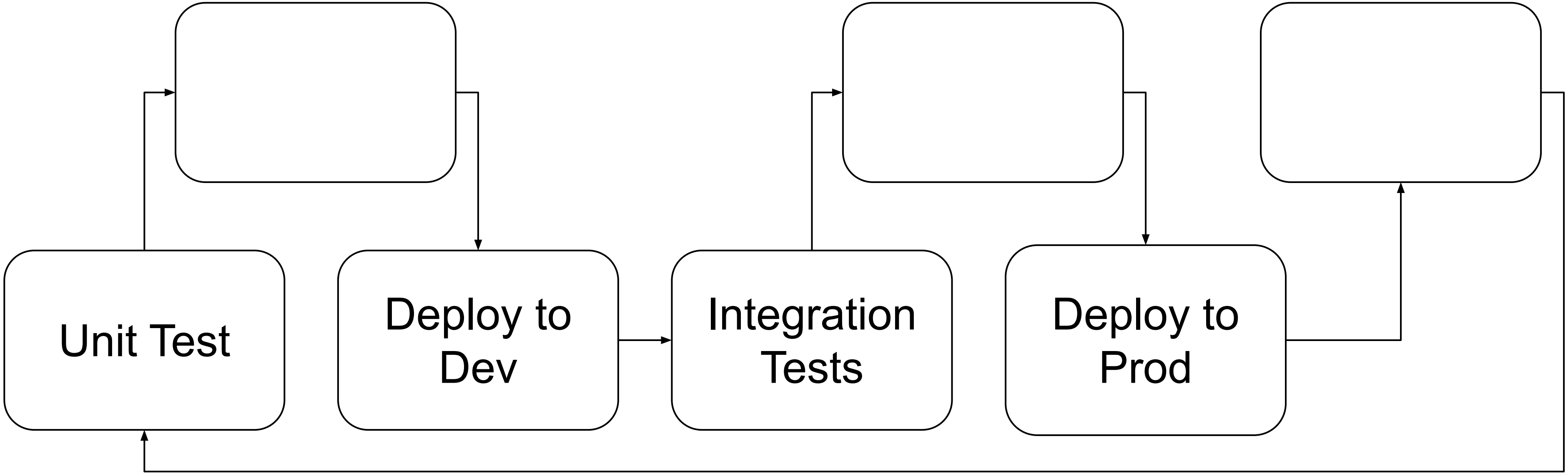


- shared-org-policies
  - naming
  - tagging
  - billing
  - secrets
  - access-management
  - vulnerability-management
  - runtime-security

- infra-policies
  - aws
  - azure
  - gcp
  - saas

- hello-world-policies

- app-policies
  - static-code-analysis
  - authn
  - authz
  - kubernetes



Unit Test

Deploy to Dev

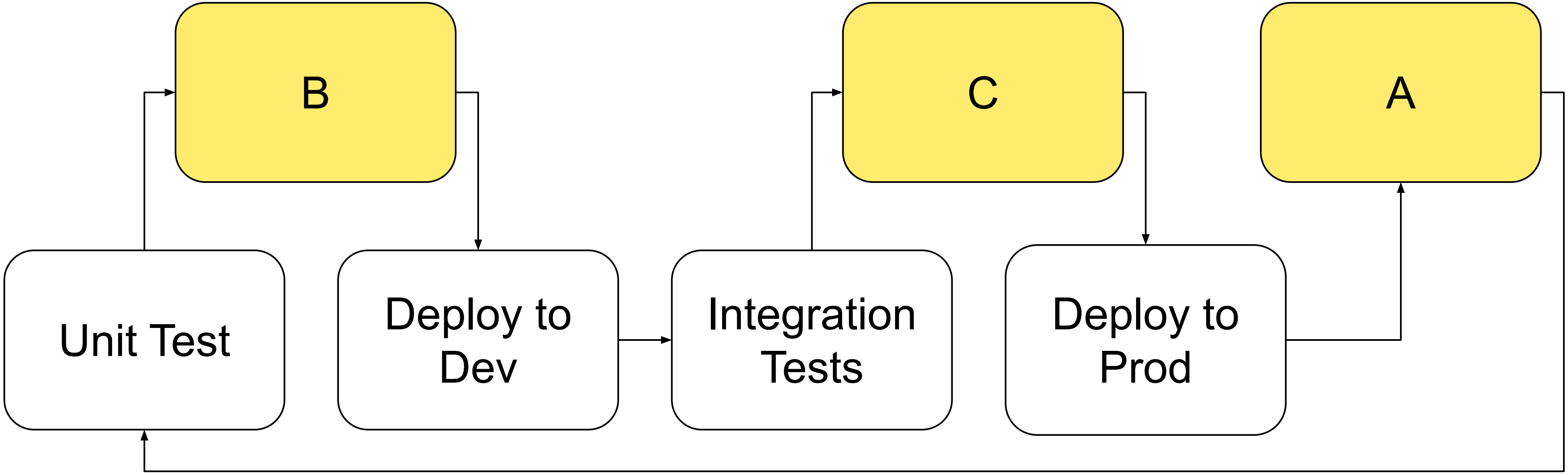
Integration Tests

Deploy to Prod

(A)
Production Runtime Analysis

(B)
Static Analysis

(C)
Test Runtime Analysis



B

C

A

Unit Test

Deploy to Dev

Integration Tests

Deploy to Prod

(A) Production Runtime Analysis

(B) Static Analysis

(C) Test Runtime Analysis

github.com/tracypholmes/policy-as-code-workshop

Rosemary Wang

Developer Advocate
HashiCorp
she/her
@joatmon08

Tracy Holmes

Open Source Engineer
VMware
she/her
@tracypholmes