Agile + DevOps EAST

A TECHWELL EVENT

DT5

Continuous Delivery

Thursday, November 8th, 2018 11:30 AM

Integrating Infrastructure as Code into a Continuous Delivery Pipeline

Presented by:

Adarsh Shah

Contino

‘

Adarsh Shah

Adarsh Shah is a principal consultant at Contino, a global leader in DevOps and cloud enablement. Prior to Contino, he was at ThoughtWorks, where he led various engineering teams. With thirteen years of engineering and DevOps experience, Adarsh has a keen interest in building systems that add business value, and he is passionate about helping clients achieve continuous delivery by improving all three aspects of DevOps: people, process, and technology. These days, Adarsh is excited about working with distributed systems architecture and cloud technologies.

Agile + DevOps EAST

A TECHWELL EVENT

Integrating Infrastructure as Code into a Continuous Delivery Pipeline

Considerations, Best Practices & Patterns

Adarsh Shah

Technical Principal & Cloud Native Practice Lead

Contino

@ShahAdarsh

Deck: *http://bit.ly/IaC-CD*

Who am I?

CONTINO

Adarsh Shah

Technical Principal & Cloud Native Practice Lead

ShahAdarsh

Infrastructure as Code

Infrastructure as Code (IaC) is the approach that takes proven coding techniques used by software systems and extends them to infrastructure.

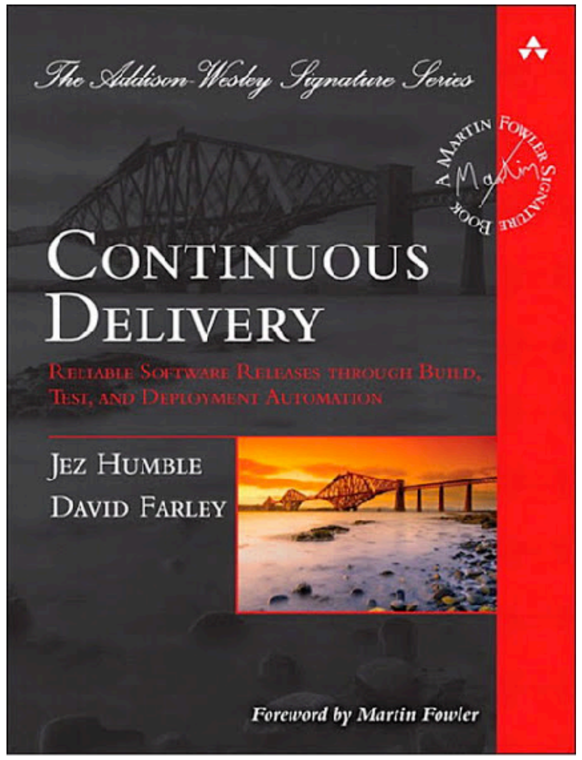
Challenges without IaC

- Configuration Issues
- Repeatability
- Human Error
- Time to Complete

Continuous Delivery

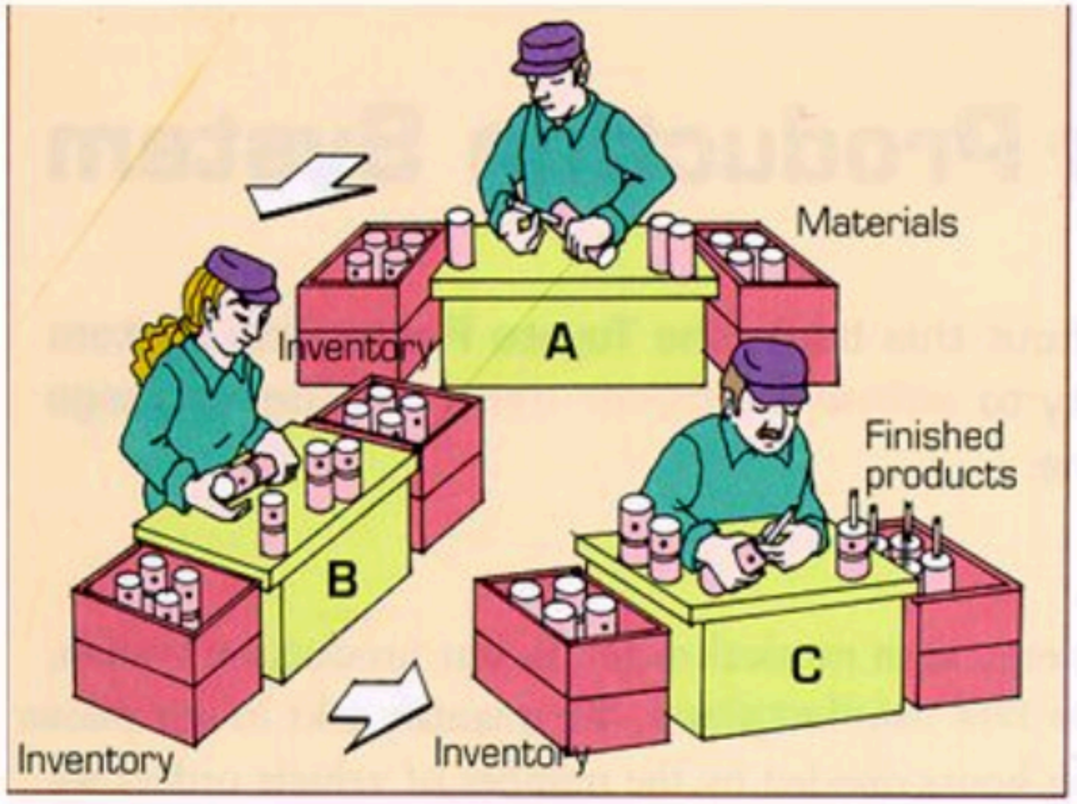
Continuous Delivery is the ability to get changes of all types—including new features, configuration changes, bug fixes and experiments—into production, or into the hands of users, safely and quickly in a sustainable way.

- Jez Humble


The Addison-Wesley Signature Series
A Martin Fowler Signature Book
Continuous Delivery
Reliable Software Releases through Build, Test, and Deployment Automation
Jez Humble
David Farley
Foreword by Martin Fowler

Continuous Delivery

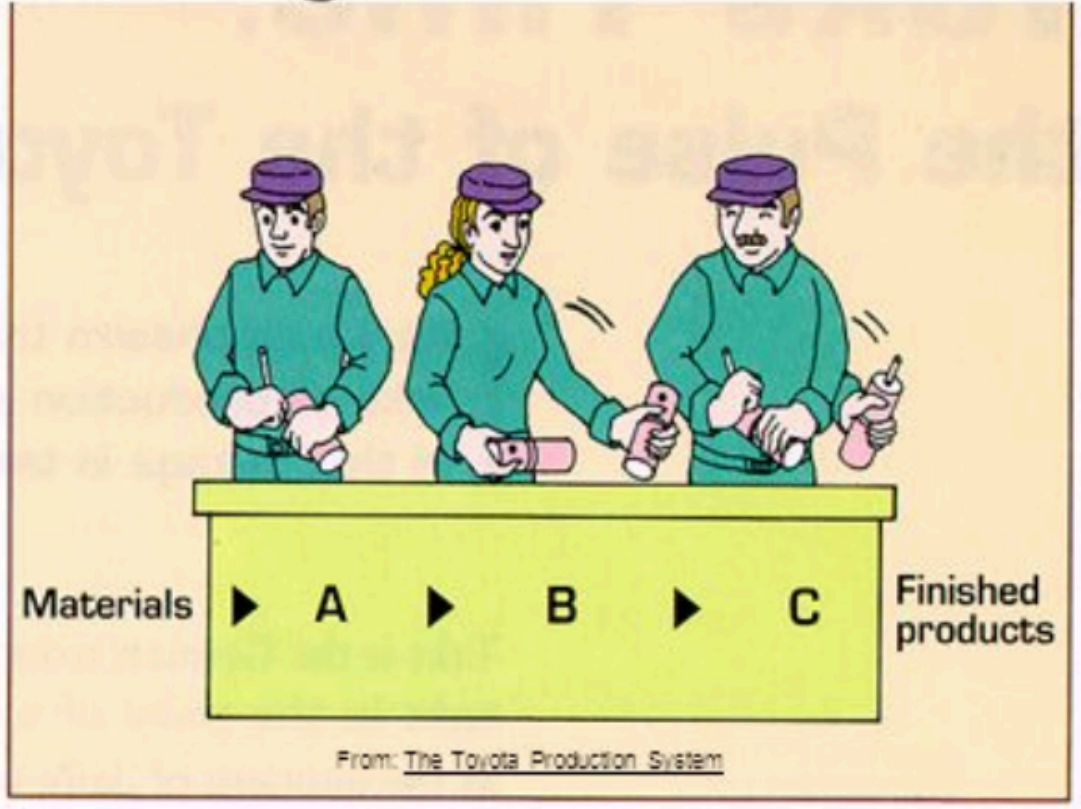
Batch



Catches Defects too Late

- How many more do you have?
- Where are they in the process?
- What is the root cause?

Single Piece Flow



Catches Defects Immediately

- You only have one
- You know where it occurred
- Resolve the root cause immediately

Considerations & best practices

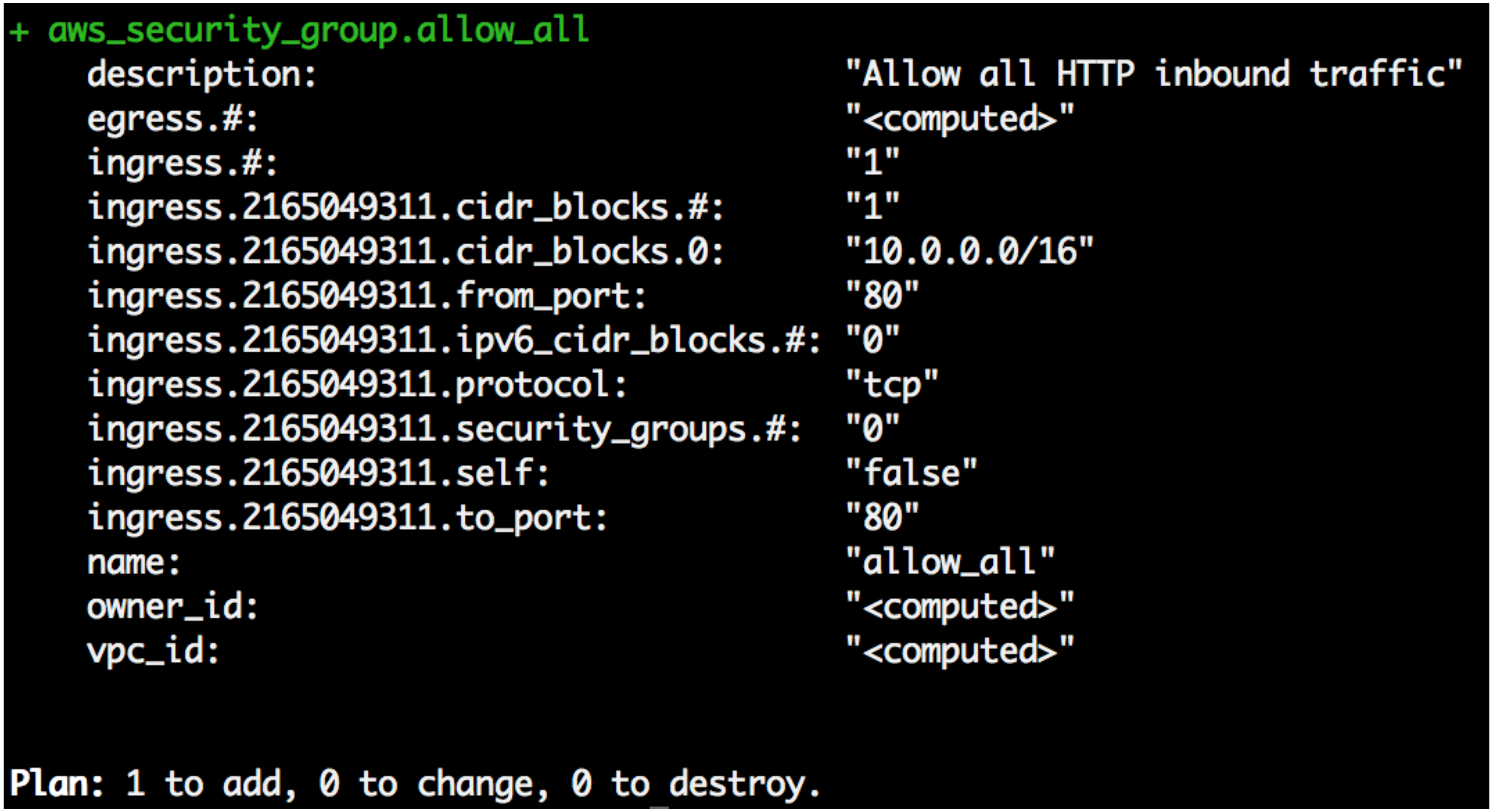
Source Control

Everyone knows where to look
http://www.flickr.com/photos/thunderchild5/1330744559/

Source Control

- Everything in source control
- Code accessibility
- Modularize
- Collaboration!!
- Code/test as documentation

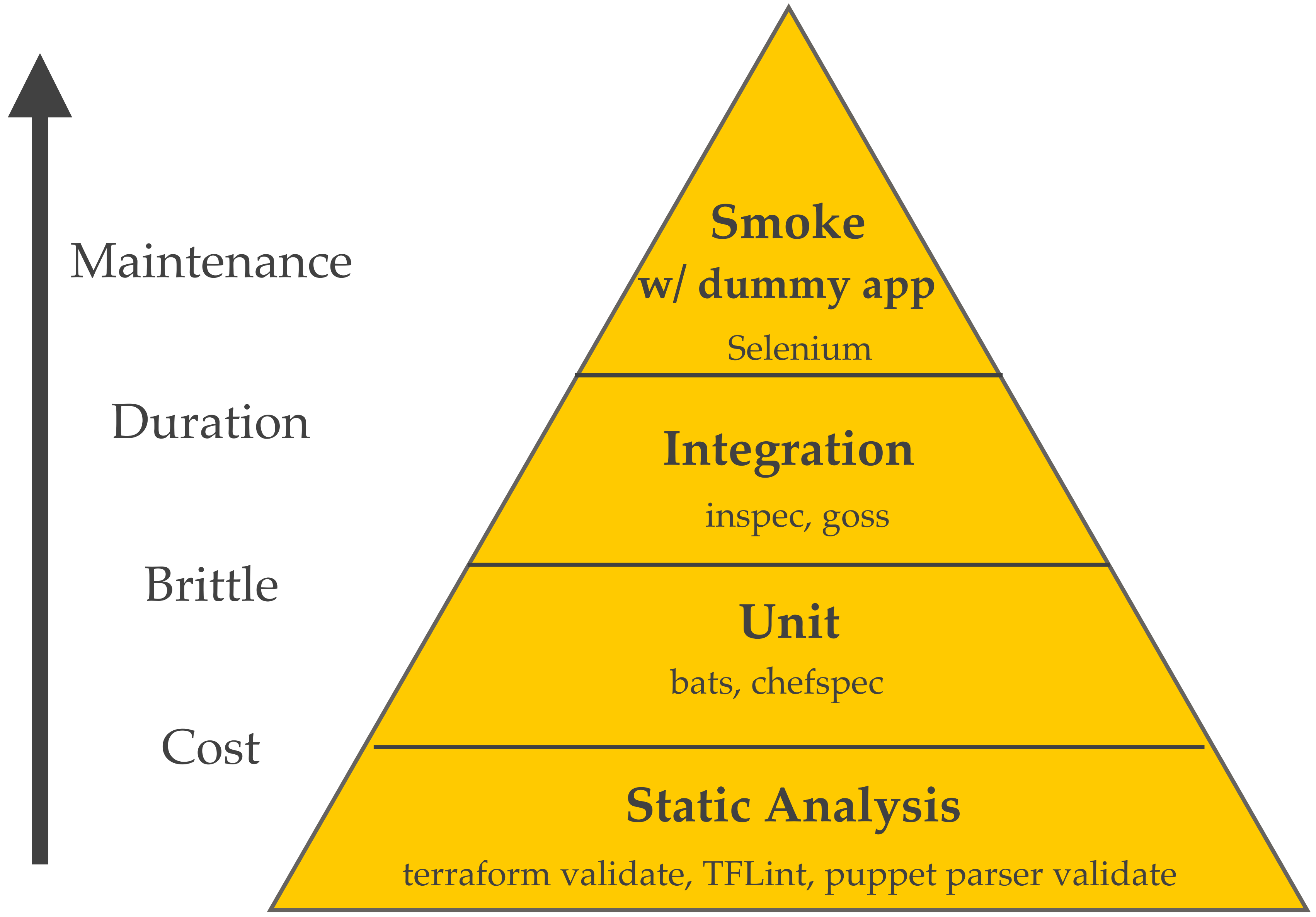
Source Control



```
+ aws_security_group.allow_all
    description:                              "Allow all HTTP inbound traffic"
    egress.#:                                 "<computed>"
    ingress.#:                                "1"
    ingress.2165049311.cidr_blocks.#:         "1"
    ingress.2165049311.cidr_blocks.0:         "10.0.0.0/16"
    ingress.2165049311.from_port:             "80"
    ingress.2165049311.ipv6_cidr_blocks.#:    "0"
    ingress.2165049311.protocol:              "tcp"
    ingress.2165049311.security_groups.#:     "0"
    ingress.2165049311.self:                  "false"
    ingress.2165049311.to_port:               "80"
    name:                                     "allow_all"
    owner_id:                                 "<computed>"
    vpc_id:                                   "<computed>"


Plan: 1 to add, 0 to change, 0 to destroy.
```

Infra as Code testing



Infra as Code Test Pyramid

Security Patterns

- CIS benchmark automation
- Building hardening policies
- Static scanning

Security Considerations

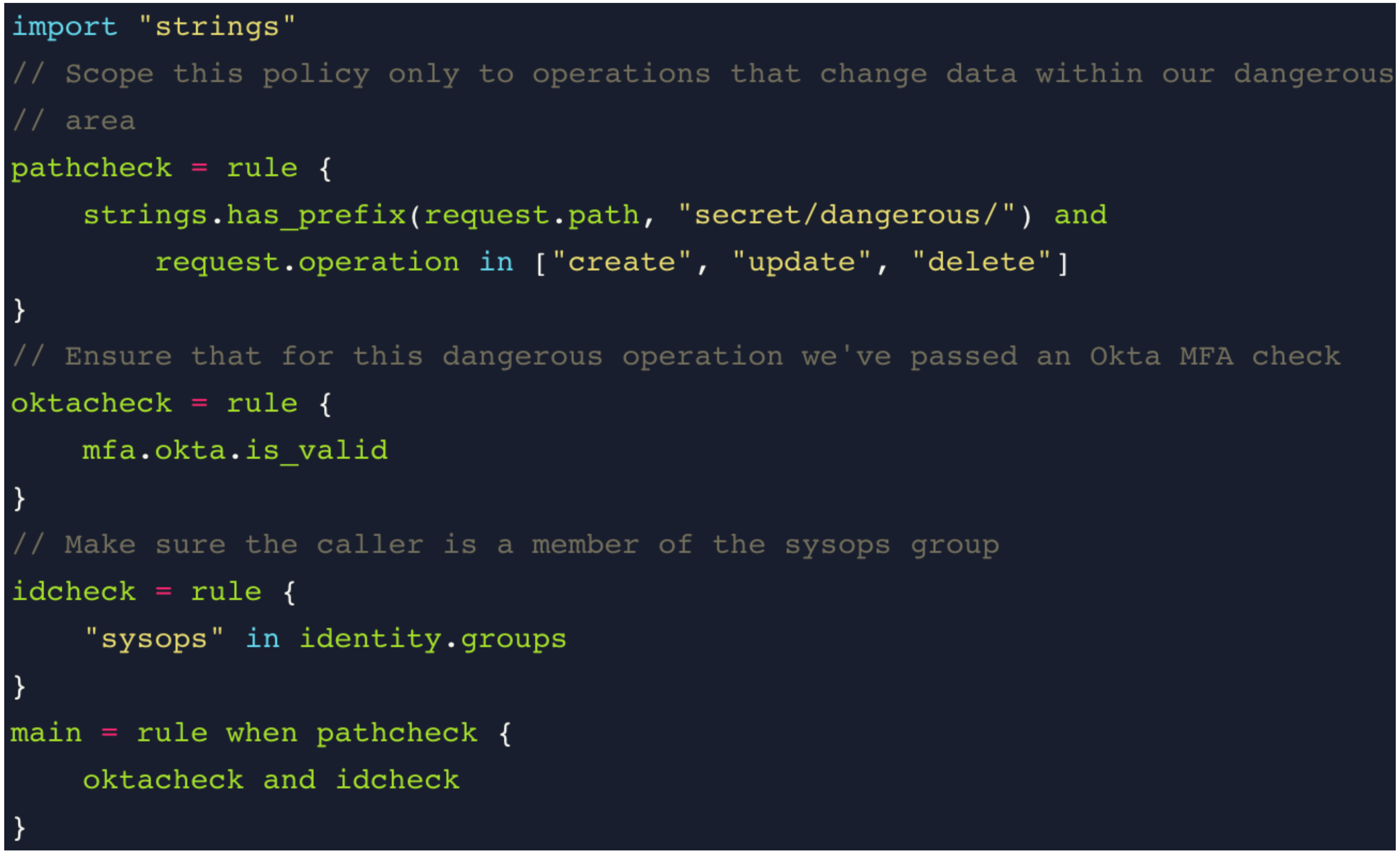
- Dynamic scanning
- Secrets management
- Artifact signing & verification

Compliance

- Finance, Healthcare & other industries
  - SOX, PII, HIPPA, PCI
- Compliance as Code - Code instead of Paperwork
- Chef InSpec, HashiCorp Sentinel (Policy as Code)

Compliance as Code using HashiCorp Sentinel

Ensure that modification of critical data can only be performed
by authorized sysops with valid MFA



```
import "strings"
// Scope this policy only to operations that change data within our dangerous
// area
pathcheck = rule {
    strings.has_prefix(request.path, "secret/dangerous/") and
        request.operation in ["create", "update", "delete"]
}
// Ensure that for this dangerous operation we've passed an Okta MFA check
oktacheck = rule {
    mfa.okta.is_valid
}
// Make sure the caller is a member of the sysops group
idcheck = rule {
    "sysops" in identity.groups
}
main = rule when pathcheck {
    oktacheck and idcheck
}
```

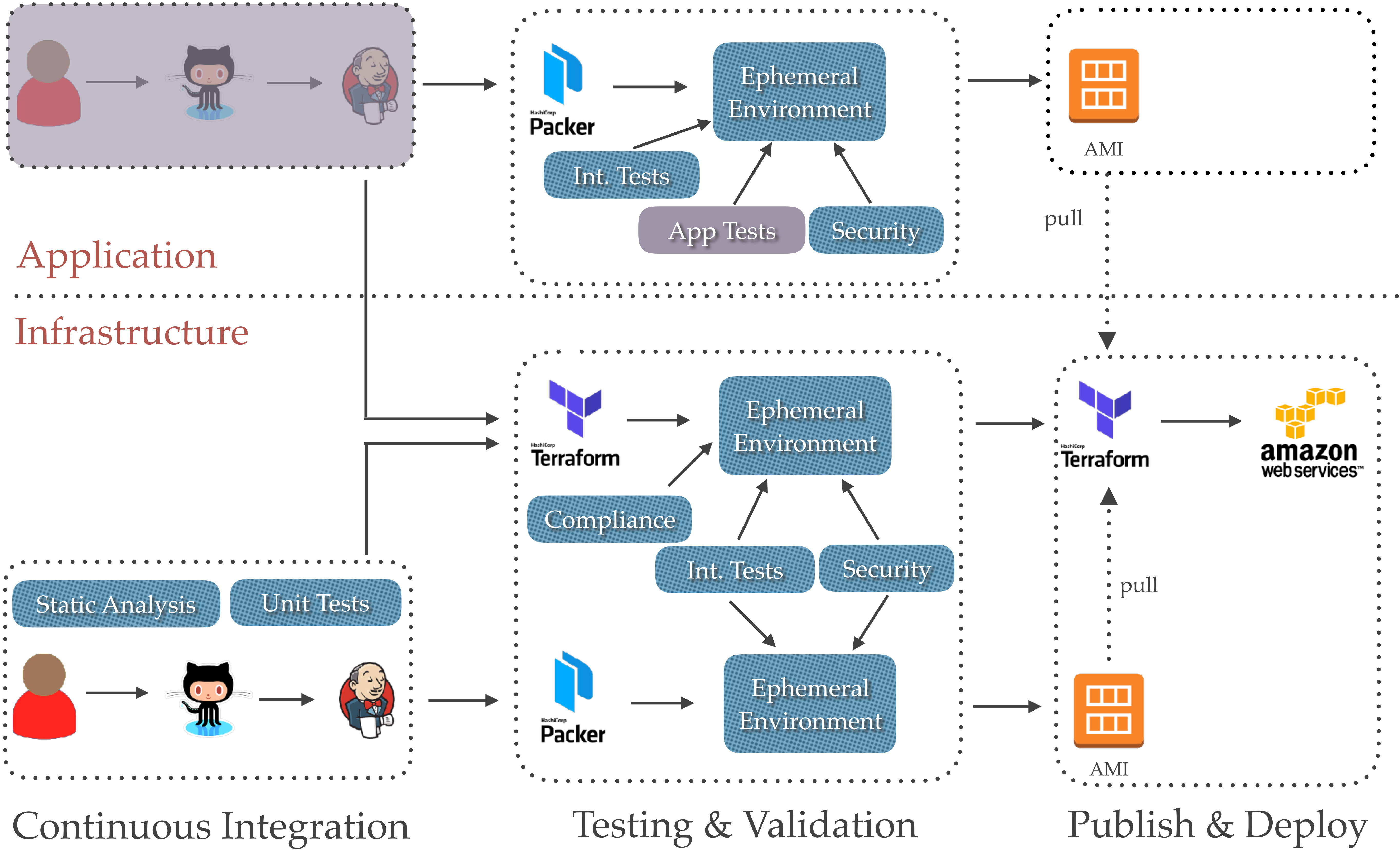
Patterns for Provisioning

- Immutable VMs
- Containerized Services
- Base Image & App Pull

Immutable VMs

- Infra Module - Multitier App w/ Cache Cluster
- Loosely Coupled
- App Image consumed by Infrastructure Module

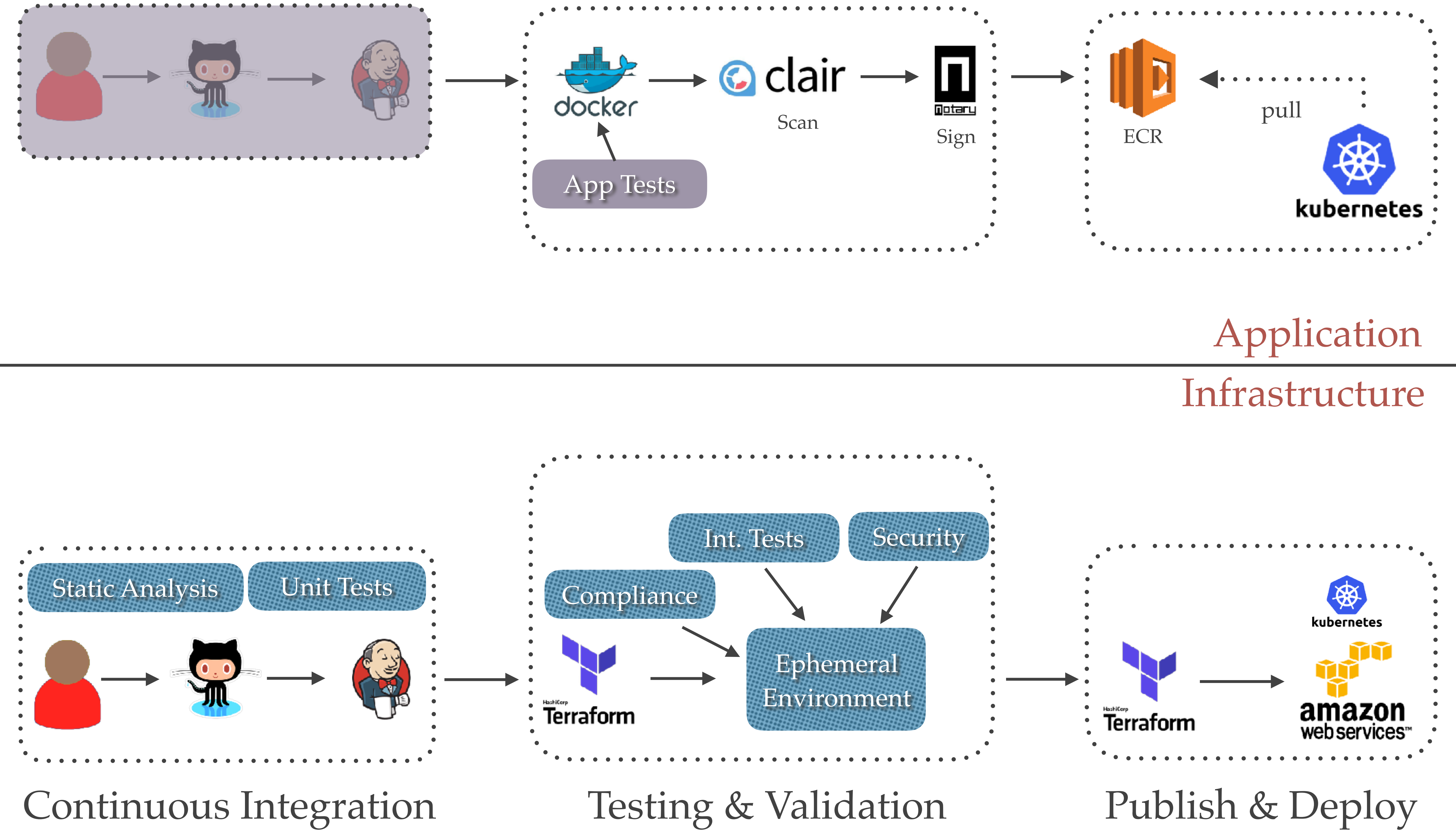
Immutable VMs



Containerized Services

- Infra Module - Container Management System
- Fully Decoupled from Apps
- Apps are deployed with Container Management System specific tools

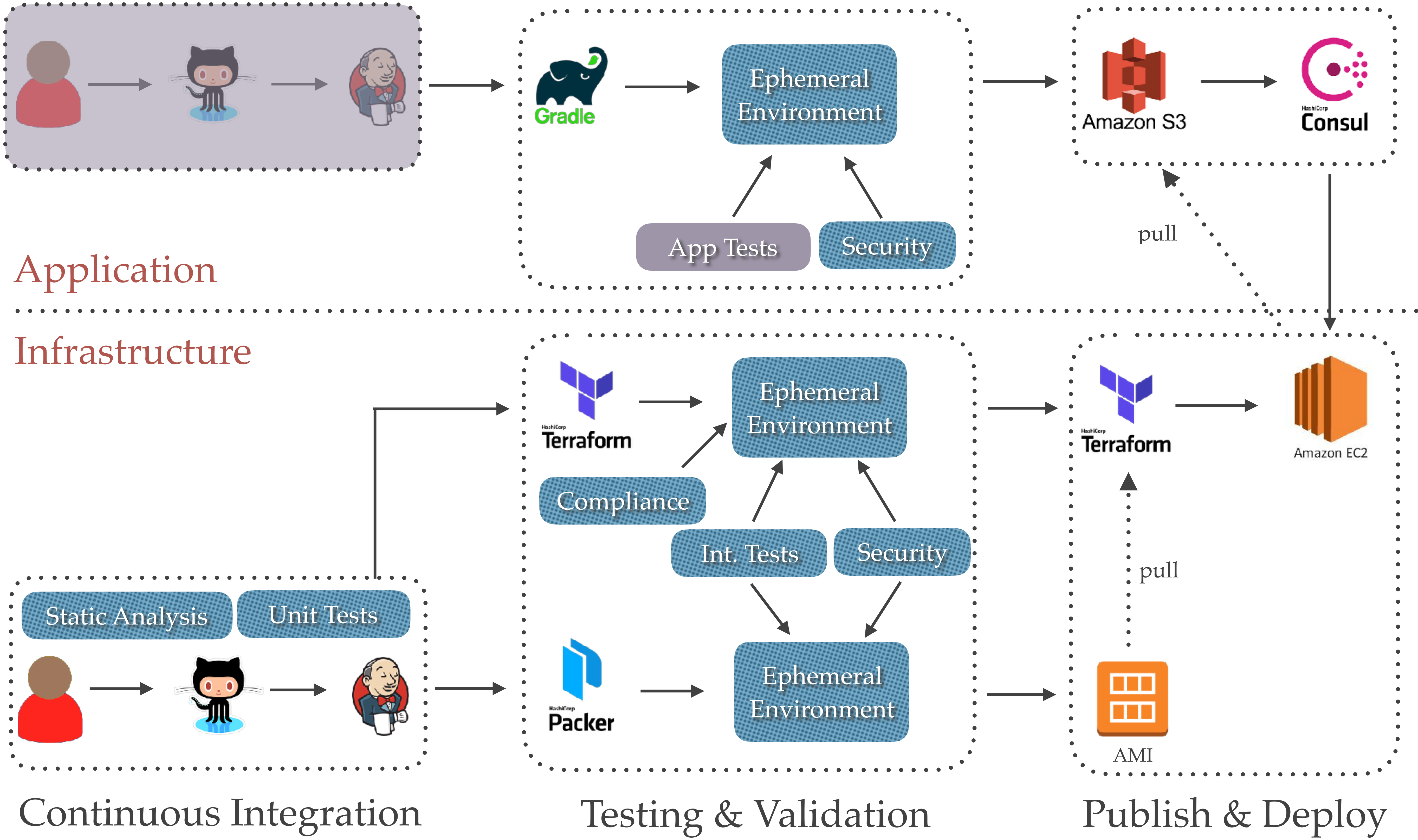
Containerized Services



Base Image & App Pull

- Infra Module - App Servers
- VMs pull app on deploy, or app update
- **Anti-Pattern**: Allowing Long-Lived VMs

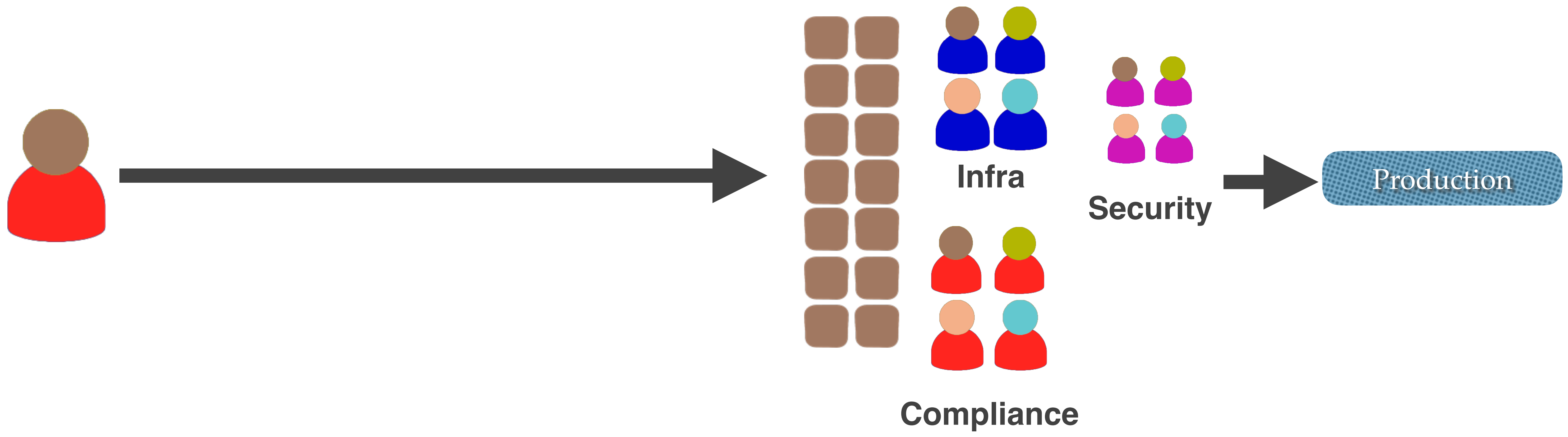
Base Image & App Pull



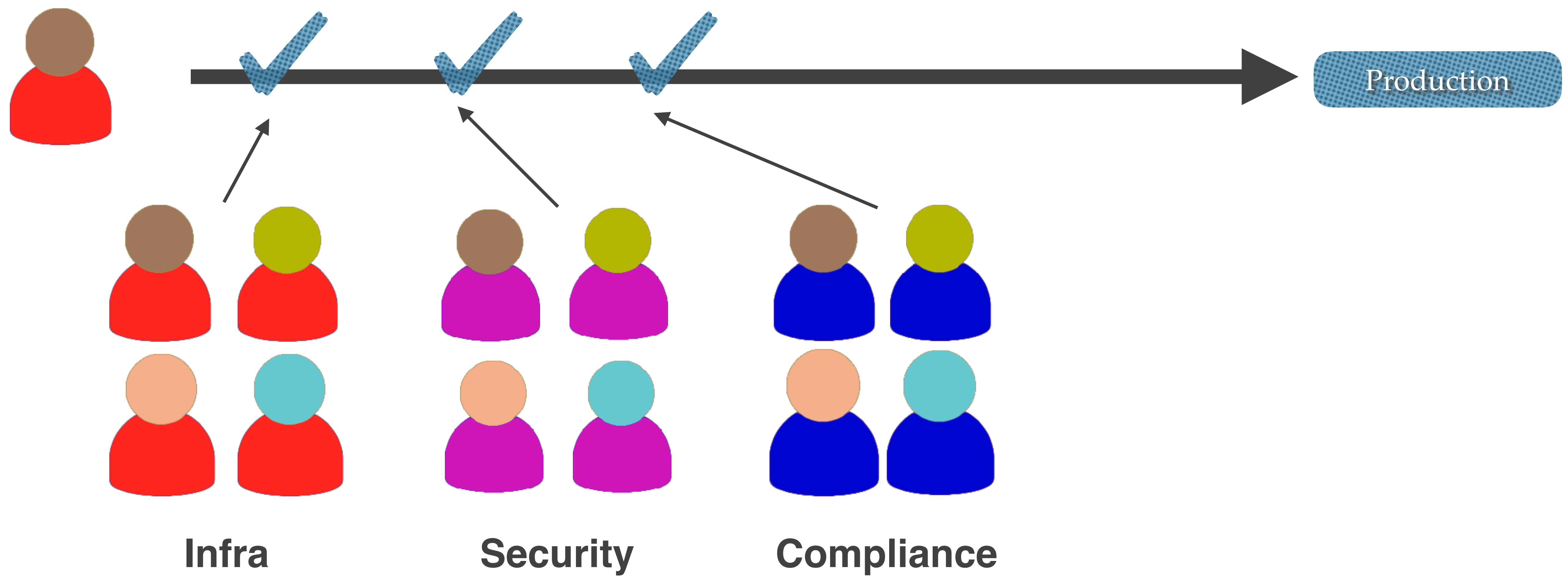
People & Process

- Enables teams to interact
- Infra, Security, Compliance, QA etc teams work together
- Improvement in processes
- Faster feedback

Inspection



Building Quality In



CONTINO

Summary

- Infrastructure as Code
- Continuous Delivery
- Considerations & best practices when integrating IaC to CD
  - Source Control
  - Testing
  - Security
  - Compliance
  - Patterns for Provisioning
  - Build and Deploy pipelines
- People & Process

Agile + DevOps EAST

A TECHWELL EVENT

Questions

Adarsh Shah

Technical Principal & Cloud Native Practice Lead

Contino

@ShahAdarsh

Deck: *http://bit.ly/IaC-CD*