VERACODE

# AppSec in a DevOps World

Peter Chestna, Director of Developer Engagement

# Who am I?

- 25 Years Software Development Experience
- 10+ Years Application Security Experience
- Certified Agile Product Owner and Scrum Master
- At Veracode since 2006
  - From Waterfall to Agile to DevOps
  - From Monolith to MicroService
  - Consultant on DevSecOps best practices
- Fun Fact: I love whiskey!

@PeteChestna

# Goals

- Why is AppSec important?
- How is DevOps changing application development?
- How is AppSec traditionally done?
- What needs to change?
  - What to build
  - What to measure
  - How to help

# Applications are as risky as ever

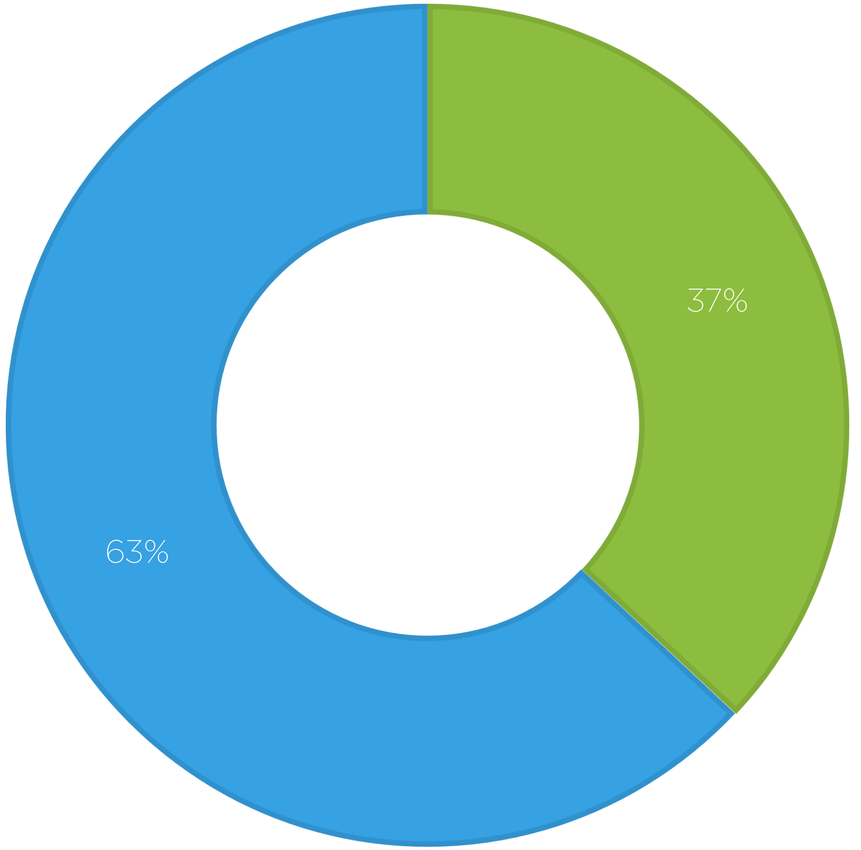

**of all applications used some kind of hard-coded password**


**of all applications use broken or risky cryptographic algorithms**


**of all applications were vulnerable to open redirect attacks**


**of all applications mix trusted and untrusted data in the same data structure or message**

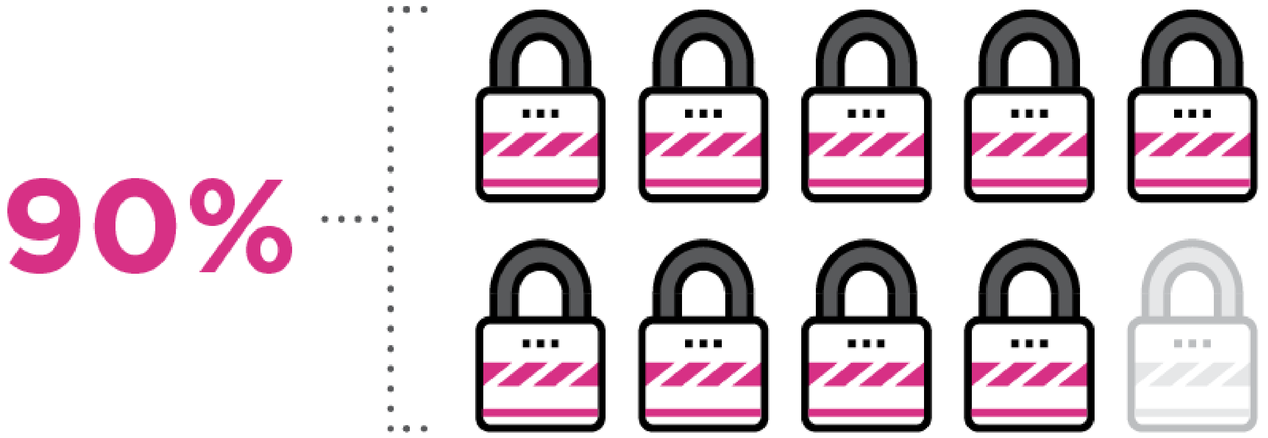
# Majority of internally developed applications fail OWASP



# Lack of App Security is Damaging Companies

01

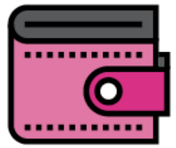
U.S. Department of Homeland Security (DHS) research found that **90 percent** of security incidents result from exploits against defects in software.




"Is poor software development the biggest cyber threat?" CSOonline.com, September 2, 2015.

# High Profile Breaches
# All attacked through the app layer

01



## TARGET

**HOW:** Sophisticated kill chain including exploitation of a vulnerable web application

**RESULT:** Hackers stole names, mailing addresses, phone numbers and email addresses from over 70 million shoppers

## JPMORGAN CHASE

**HOW:** Vulnerability on website built and maintained by a third-party vendor in support of a charity

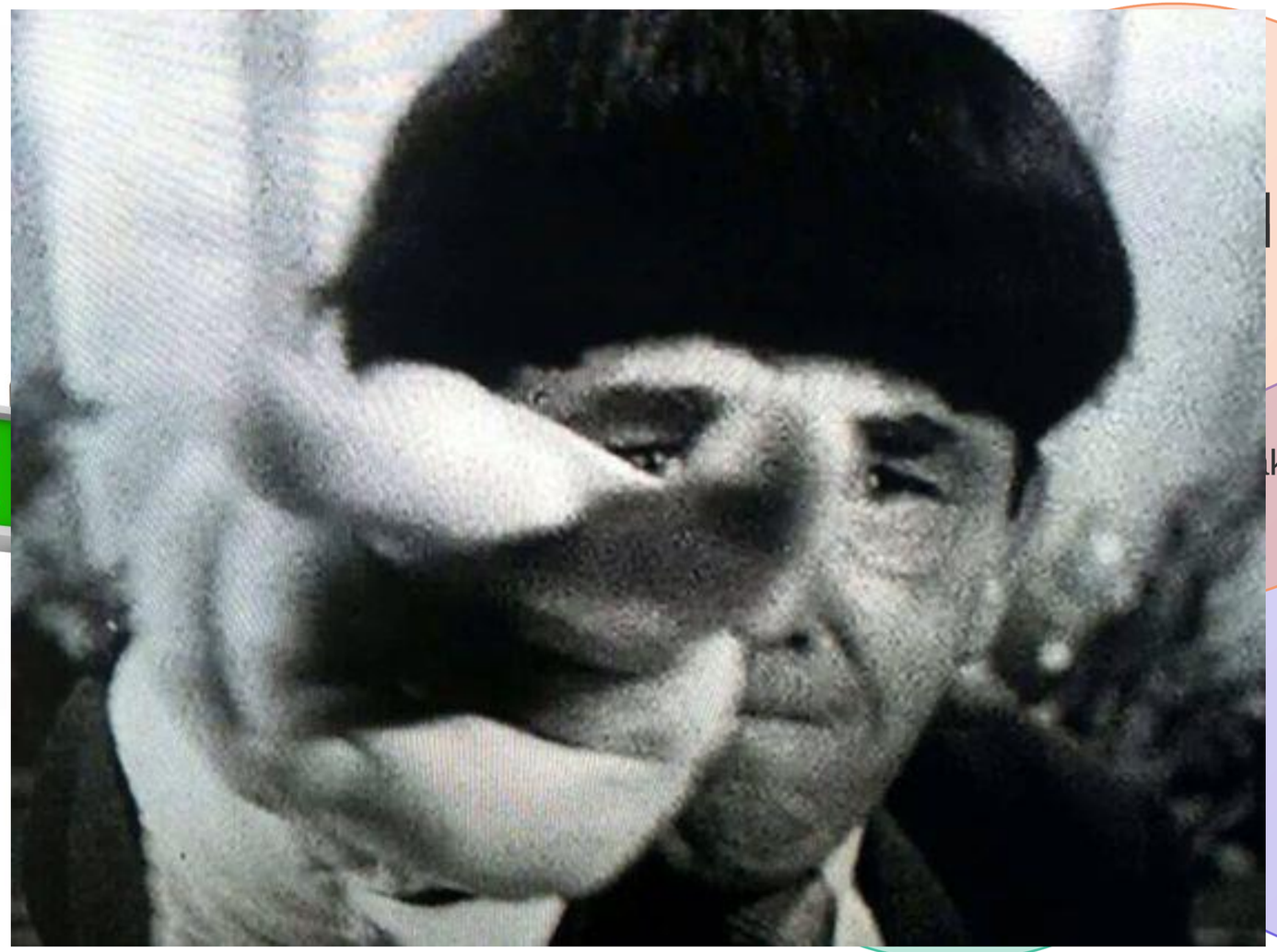
**RESULT:** Usernames and passwords for 76 million households and 7 million businesses accounts were stolen

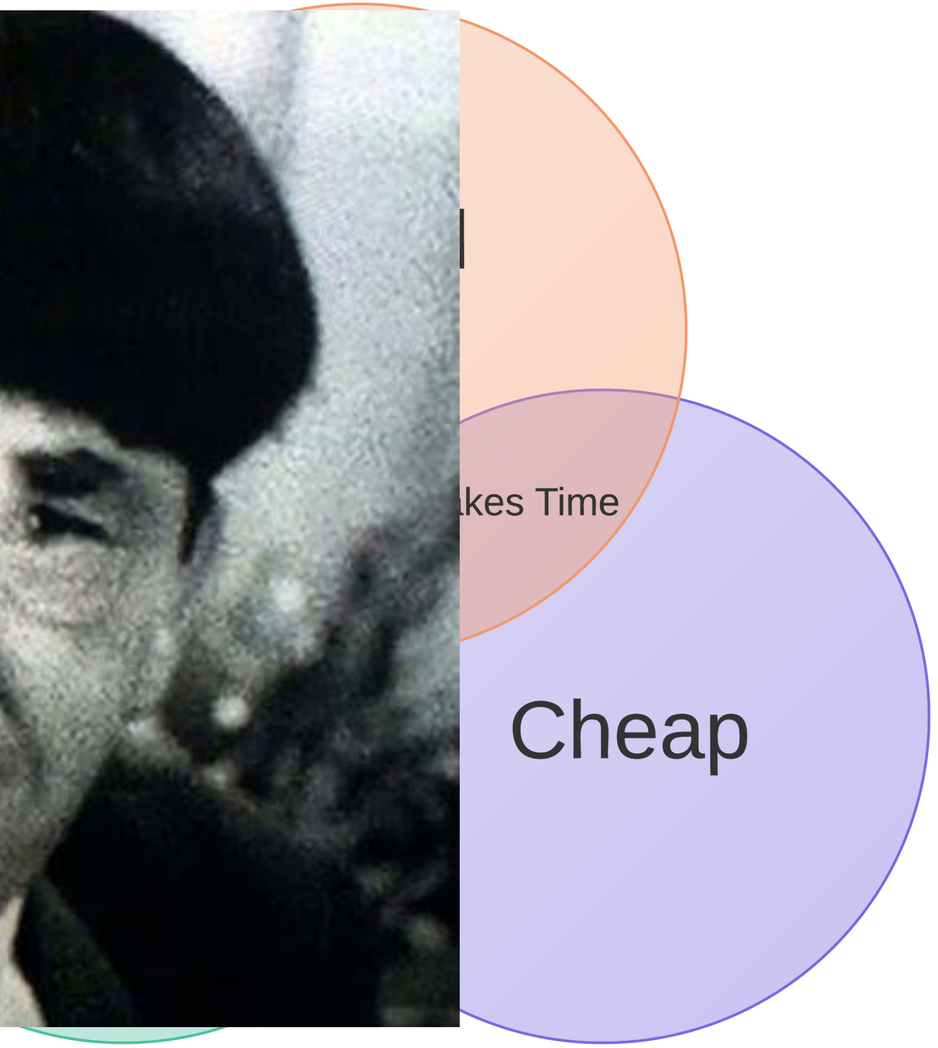
## COMMUNITY HEALTH

**HOW:** Targeted a flaw in OpenSSL, CVE-2014-0160, better known as Heartbleed

**RESULT:** The theft of Social Security numbers and other personal data belonging to 4.5 million patients

# Business Mandate



# Compressed Timelines

| Waterfall | Agile | DevOps |
| --- | --- | --- |
| 1-4 Releases Per Year | 12-24 Releases Per Year | 100+ Releases Per Year |

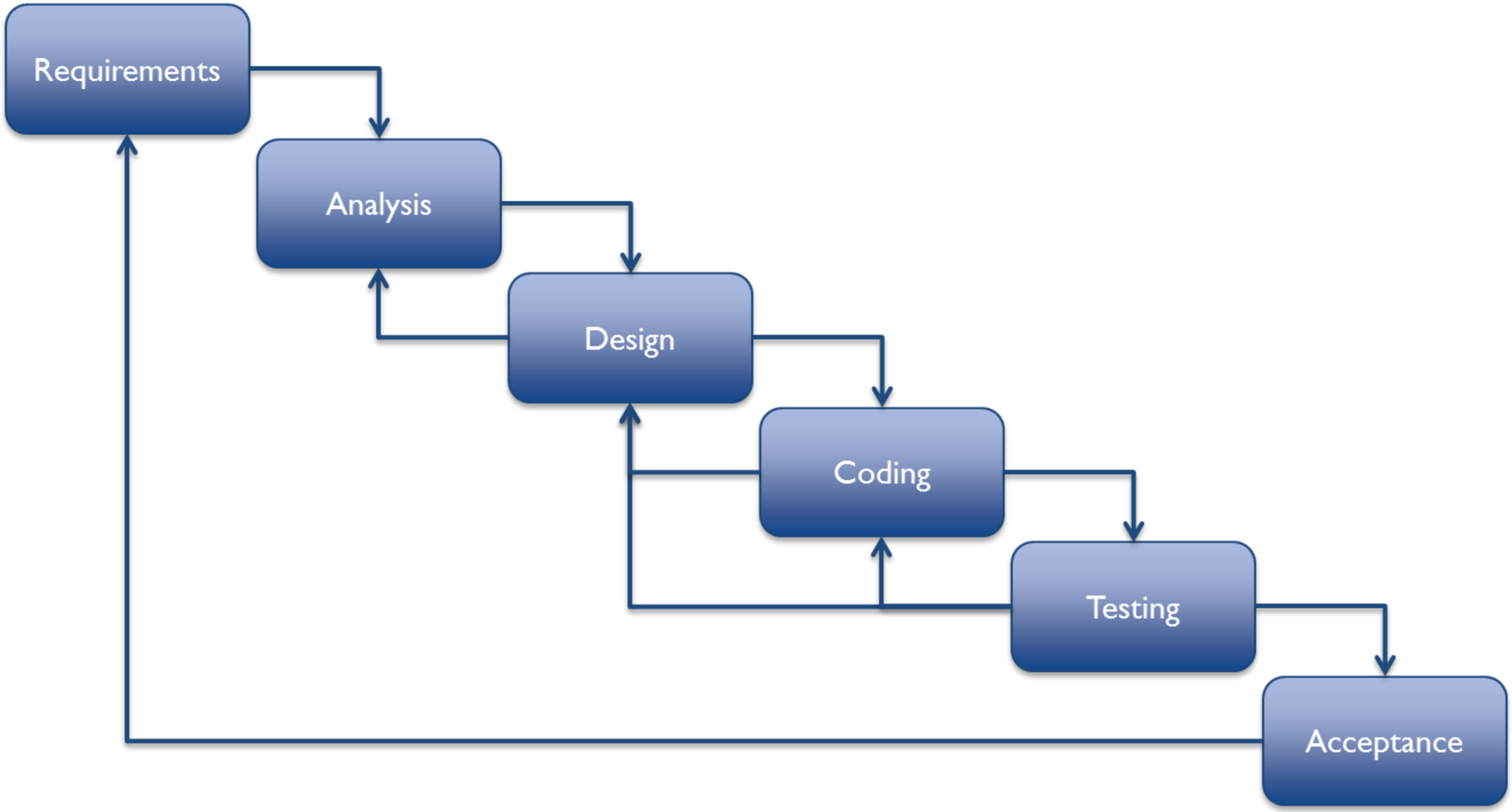


# Definition of DevOps

"DevOps is a cultural and professional movement, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners."

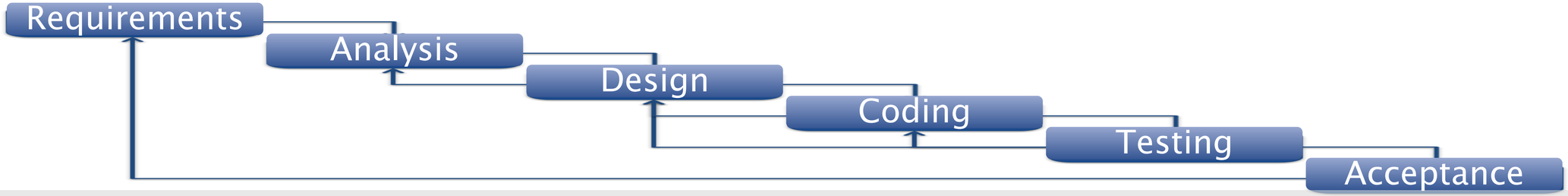
- Nathan Harvey (Chef)

# Basic development cycle

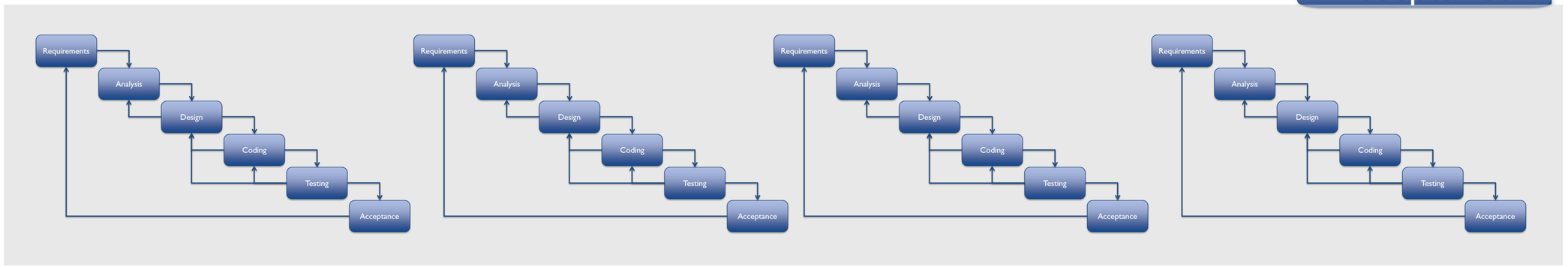


# Not so different after all

Waterfall

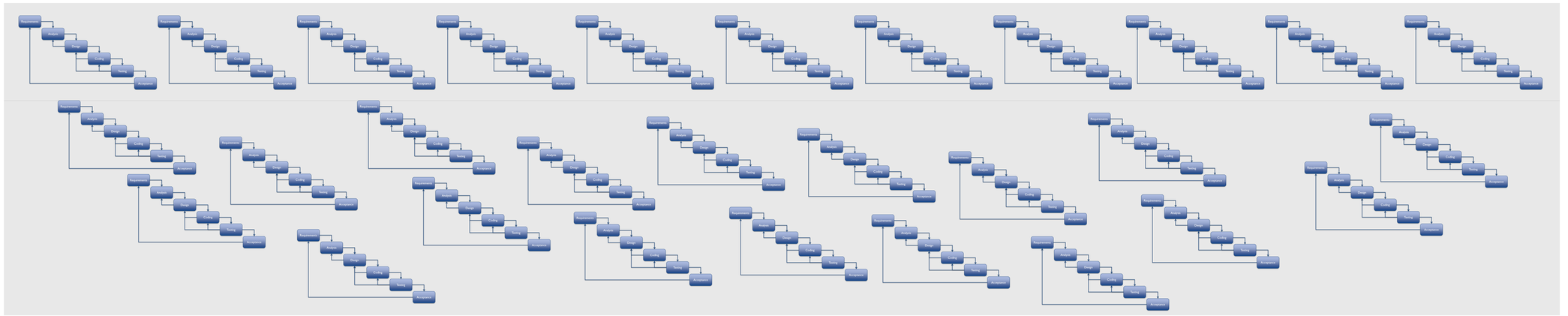



Agile

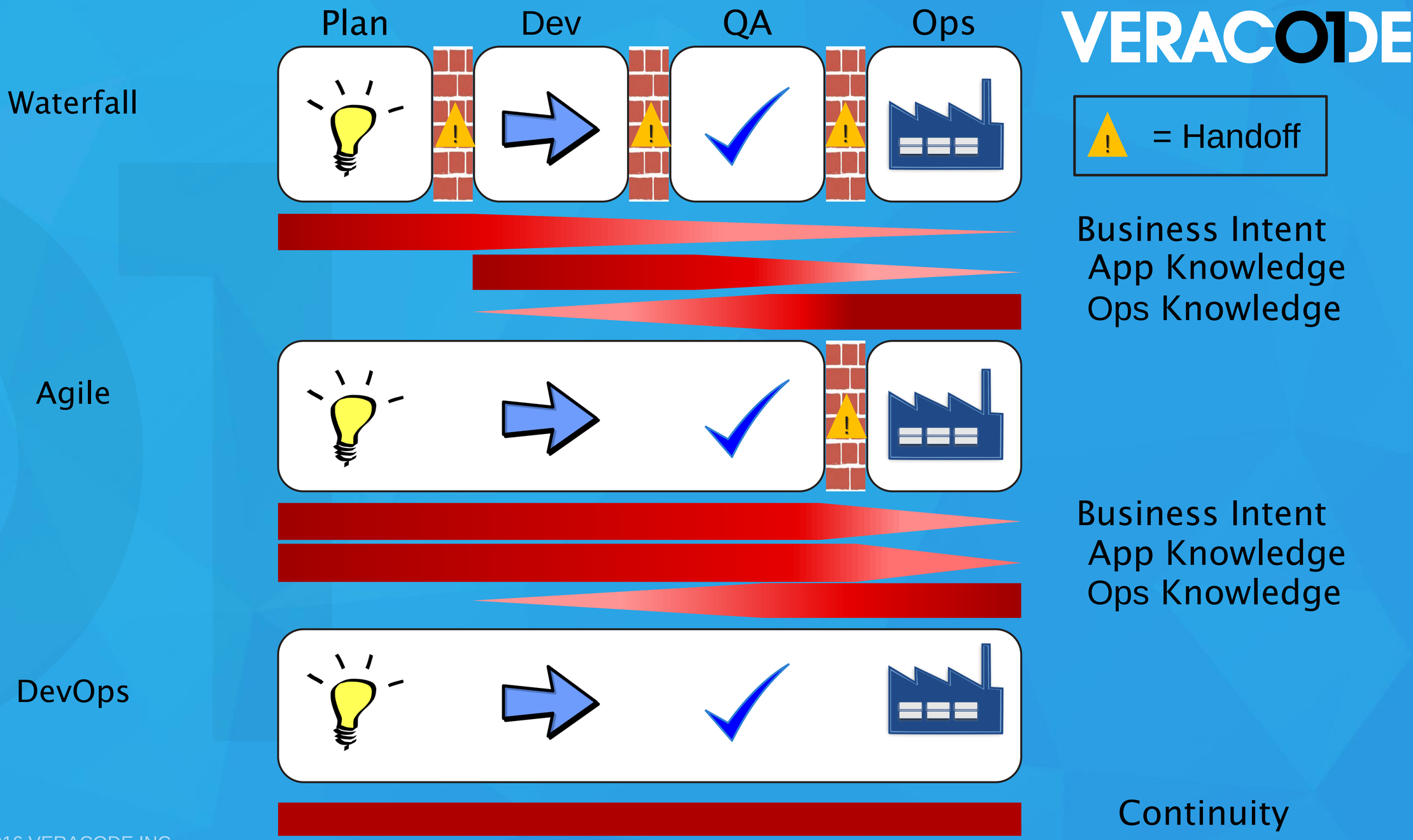



DevOps

At Scale



Time



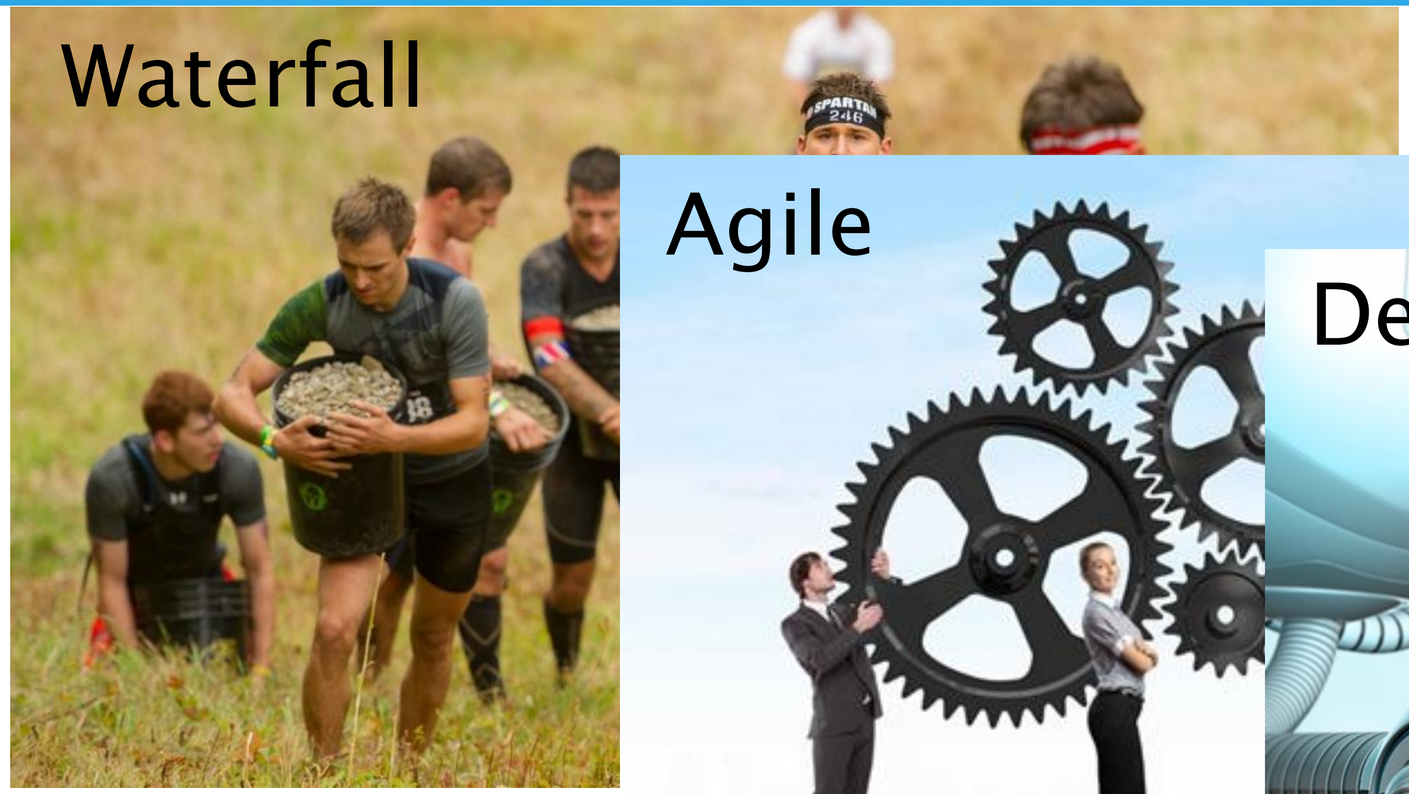
# Agile - Process





Copyright 2005, Mountain Goat Software

# Transformation - Technology



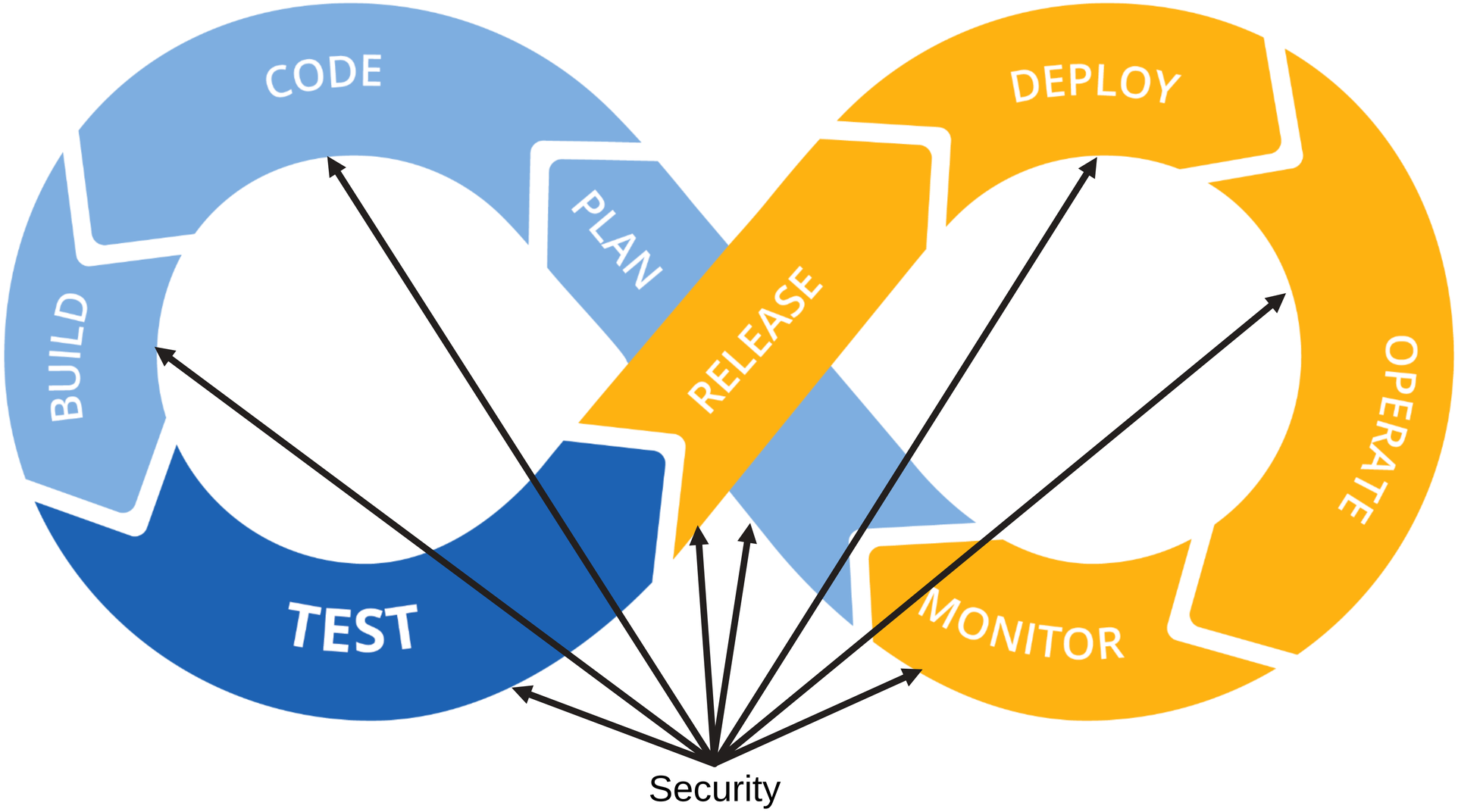

# Is this your current AppSec program?

# They/We know it's coming…

# Which outcome do you see?



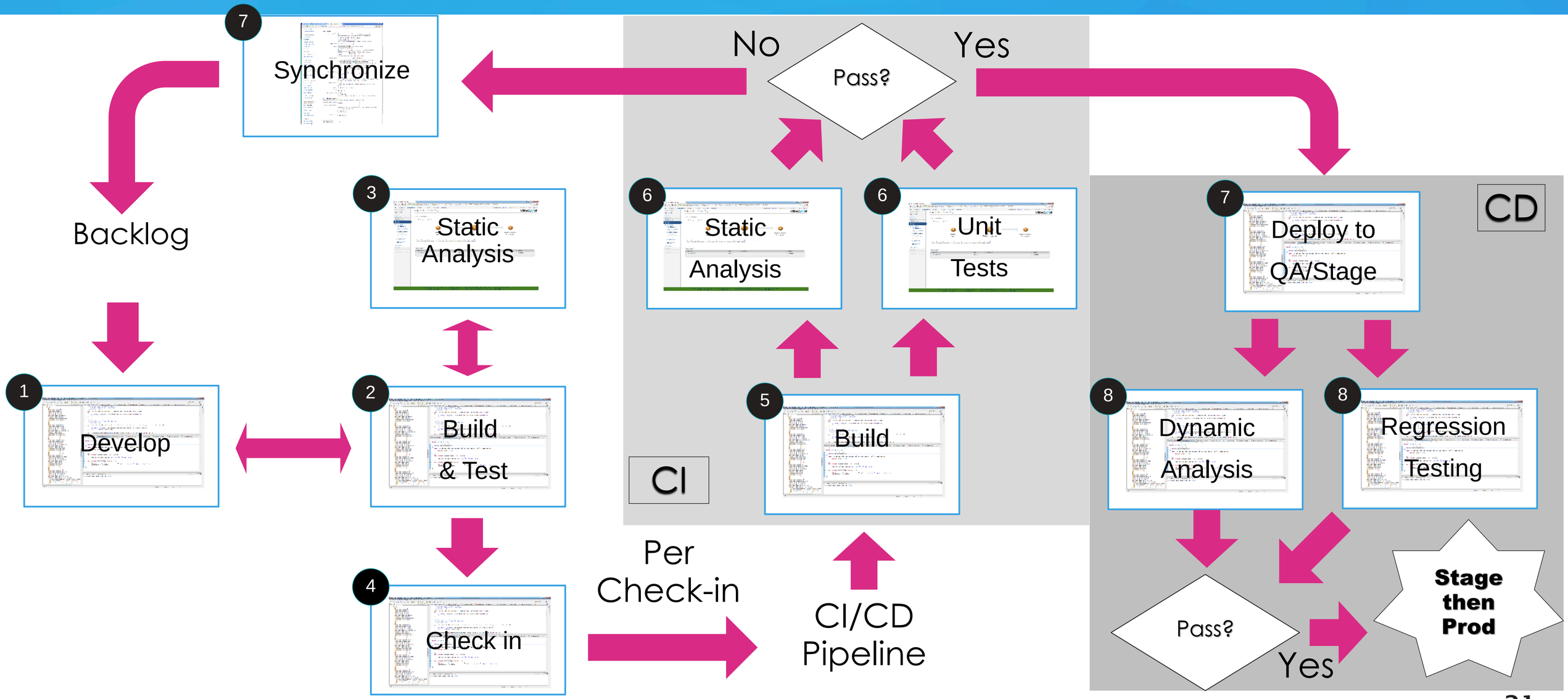
# DevOps – Process: Where is security?



# Strategy

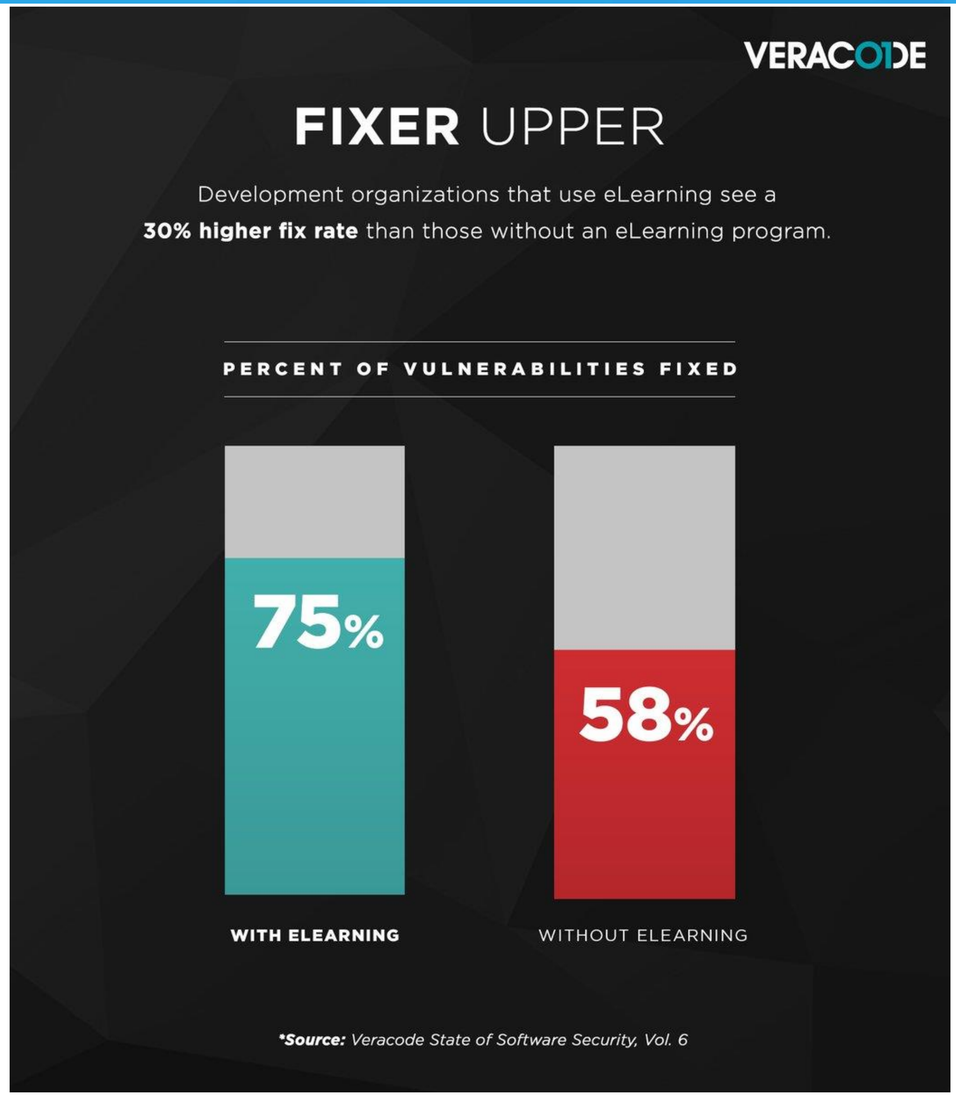
- Integration & Automation
- 3-legged barstool:
  - Training
  - Remediation Coaching
  - Scan early & often

# Strategy – Integration & Automation



# Strategy - Training

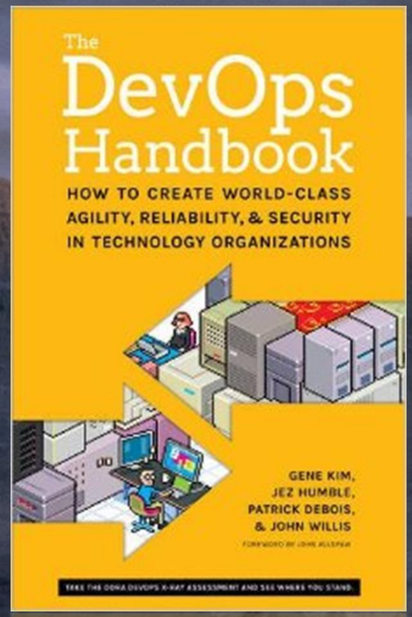
- Security teams can help developers by providing training,  either through eLearning or in-person Instructor Led Training
- Think about targeted training based on policy violations




*State of Software Security Report: Focus on Industry Verticals*, Volume 6, Veracode

# Get smart on DevOps

## Train beyond your walls



# Strategy - Remediation Coaching

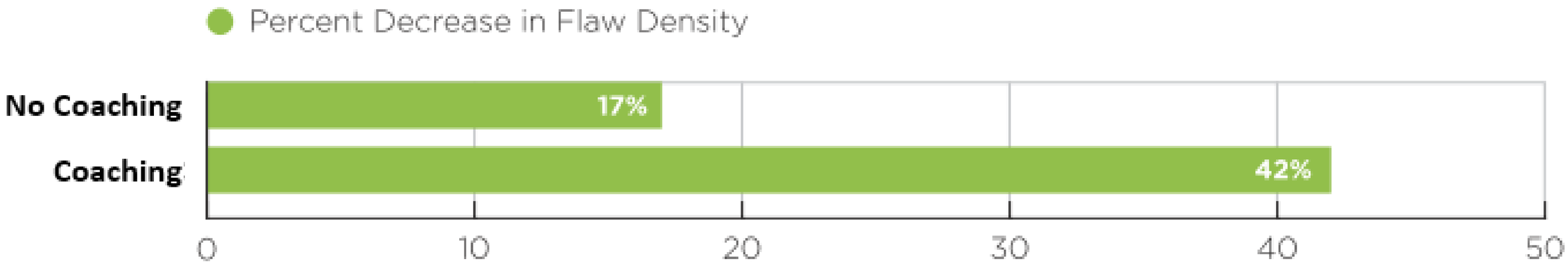
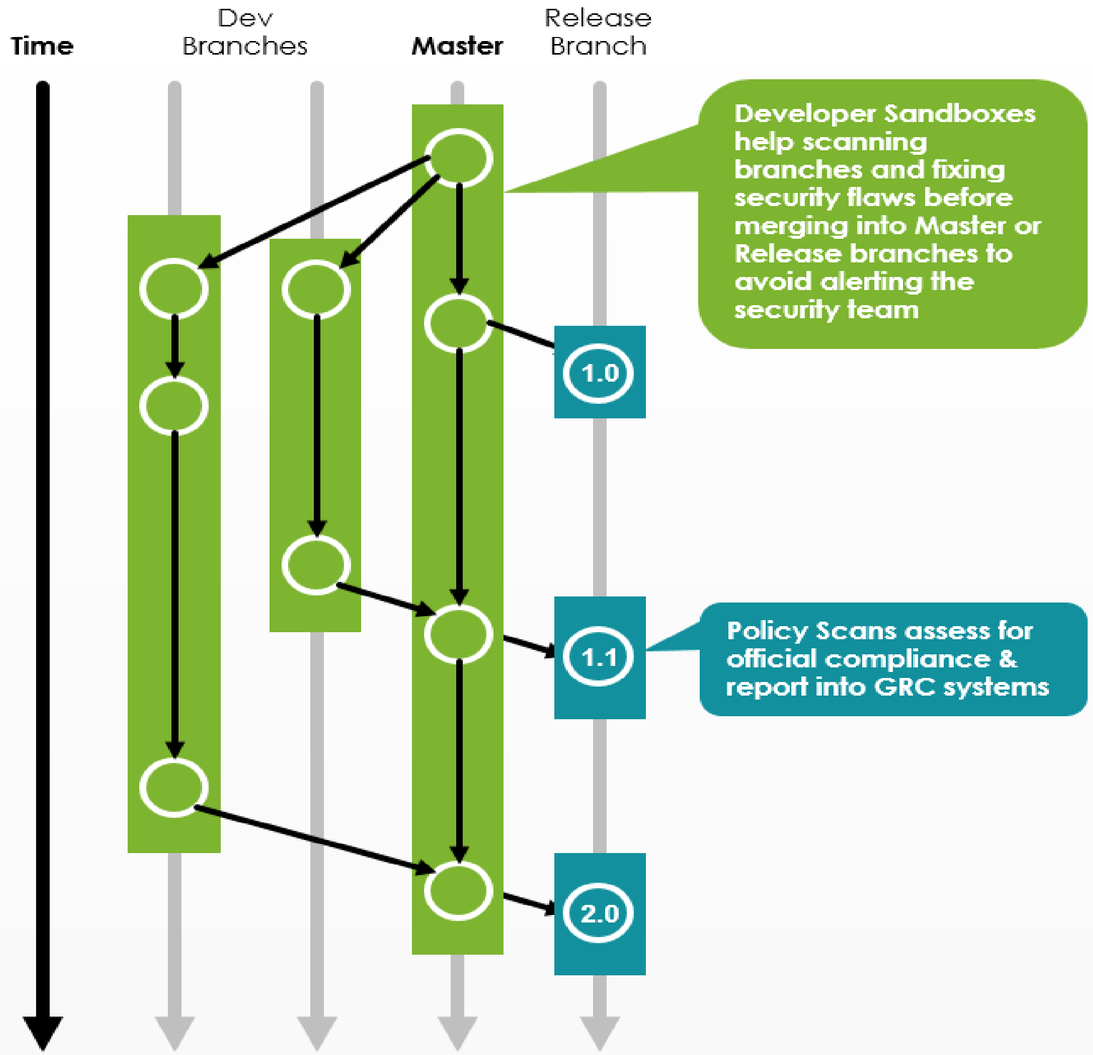



Figure 10: Relative Improvement in Flaw Density via Remediation Coaching (Readout)

**For applications that used remediation coaching, development teams fixed more than 2.5x the average # of flaws per megabyte**

# Strategy – Measurement (Scan early, scan often)




Applications that used sandbox had an average fix rate of 59%, or a 2x improvement in fix rate

# DevOps – Pervasive Security

Plan | Code | Build | Test | Stage | Deploy | Monitor

**Training**
**(eLearning, instructor led, metadata driven)**

**Static Application Security Testing + 3rd Party Risk Analysis**

**Dynamic Application Security Testing**

**Runtime Application Self Protection**

**Threat Modeling**
**Security Grooming**
**Secure Design**

**Remediation and Mitigation Guidance**
**Secure Code Reviews**

**Manual Penetration Testing**
**Red Team Activities**

VERACODE

# Thank You!