

# DevOps – Security's Big Opportunity

Peter Chestna, Director of Developer Engagement  
Veracode/CA

# Who am I?



- 25+ Years Software Development Experience
- 11+ 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!
  - Tell me where to drink local whiskey



@PeteChestna

# Lack of App Security is Damaging Companies



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



# High Profile Breaches through the app layer



## Retailer

**How:** Sophisticated kill chain including exploitation of vulnerable web application

**Result:** Hackers stole PII for more than 70 million shoppers



## Financial Institution

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

**Result:** Usernames and passwords for 76 million households and 7 million business were stolen



## Healthcare Provider

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

**Result:** The theft of Social Security Numbers and other PII of 4.5 million patients



## Financial Institution

**How:** Hackers exploited a known vulnerability in an open source component

**Result:** Social Security Numbers and PII for more than 143 million Americans stolen. Three executives lose their jobs.



# Is this your current AppSec program?





# Which outcome do you see?

01



 @PeteChestna

The background features a large, abstract blue geometric design on the right side, composed of various overlapping shapes like triangles and polygons in different shades of blue. The rest of the background is white.

# Times have changed





# Release Timelines & Team Sizes

## Waterfall

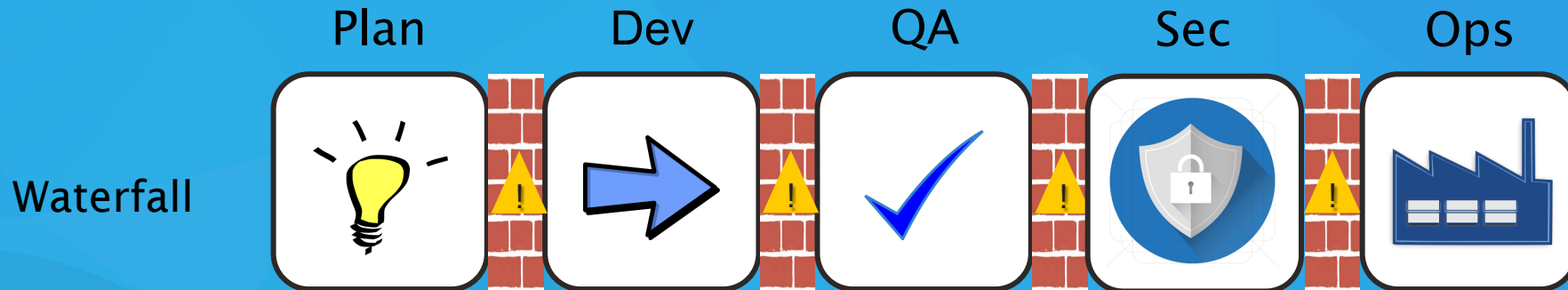


## Agile



## DevOps





Waterfall

VERACODE

 = Handoff

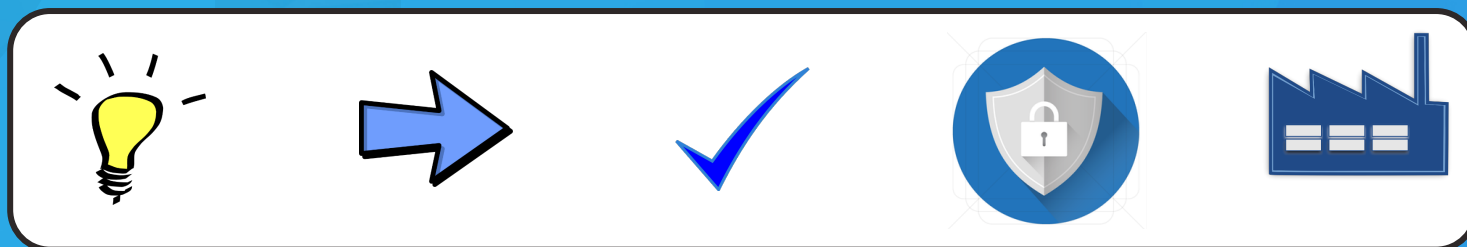
Business Intent  
App Knowledge  
Ops Knowledge

Agile



Business Intent  
App Knowledge  
Ops Knowledge

DevOps



Continuity

# Technology

01

Waterfall



Agile



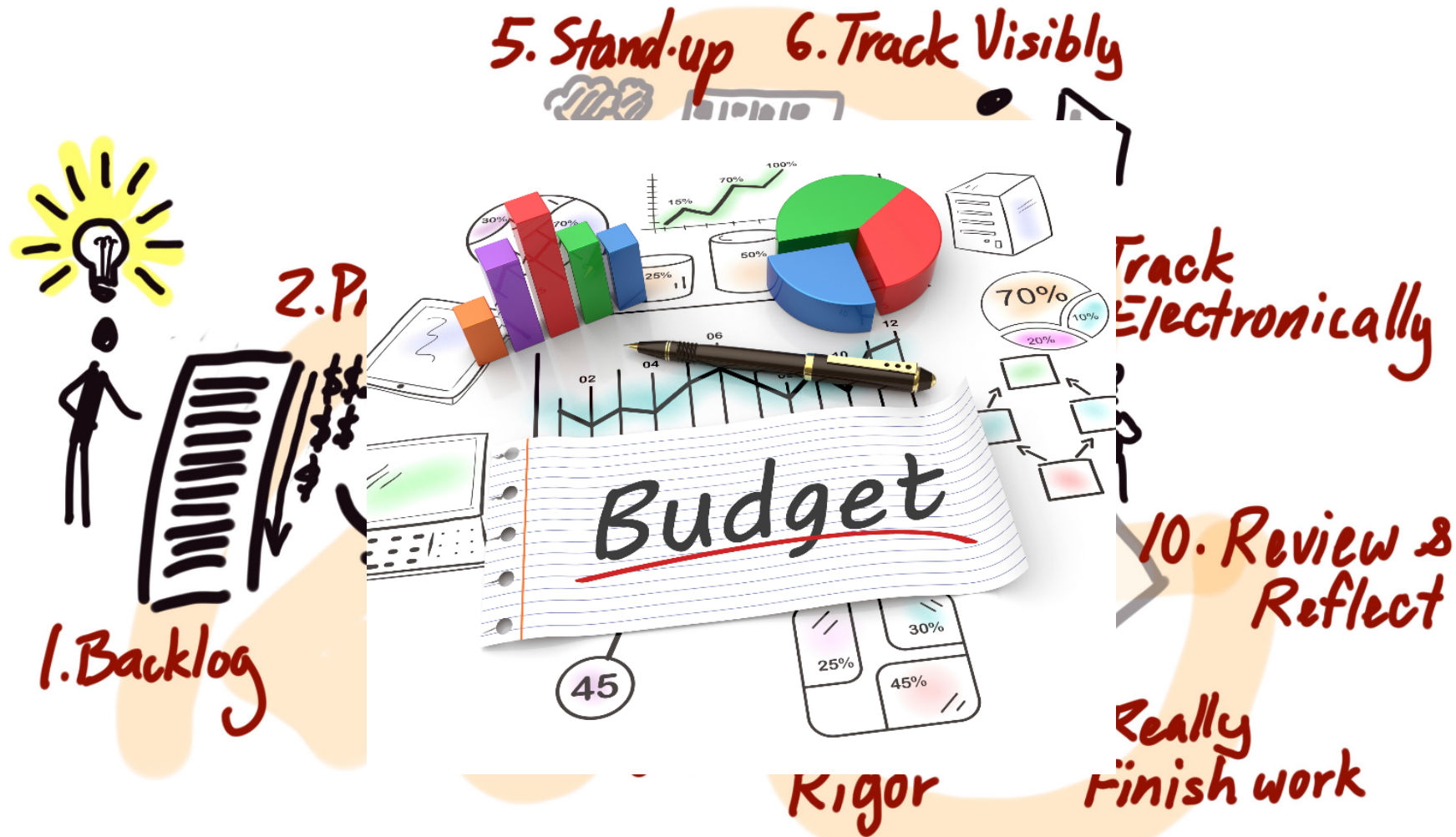
DevOps





# Agile - Process

01





# What is DevOps?

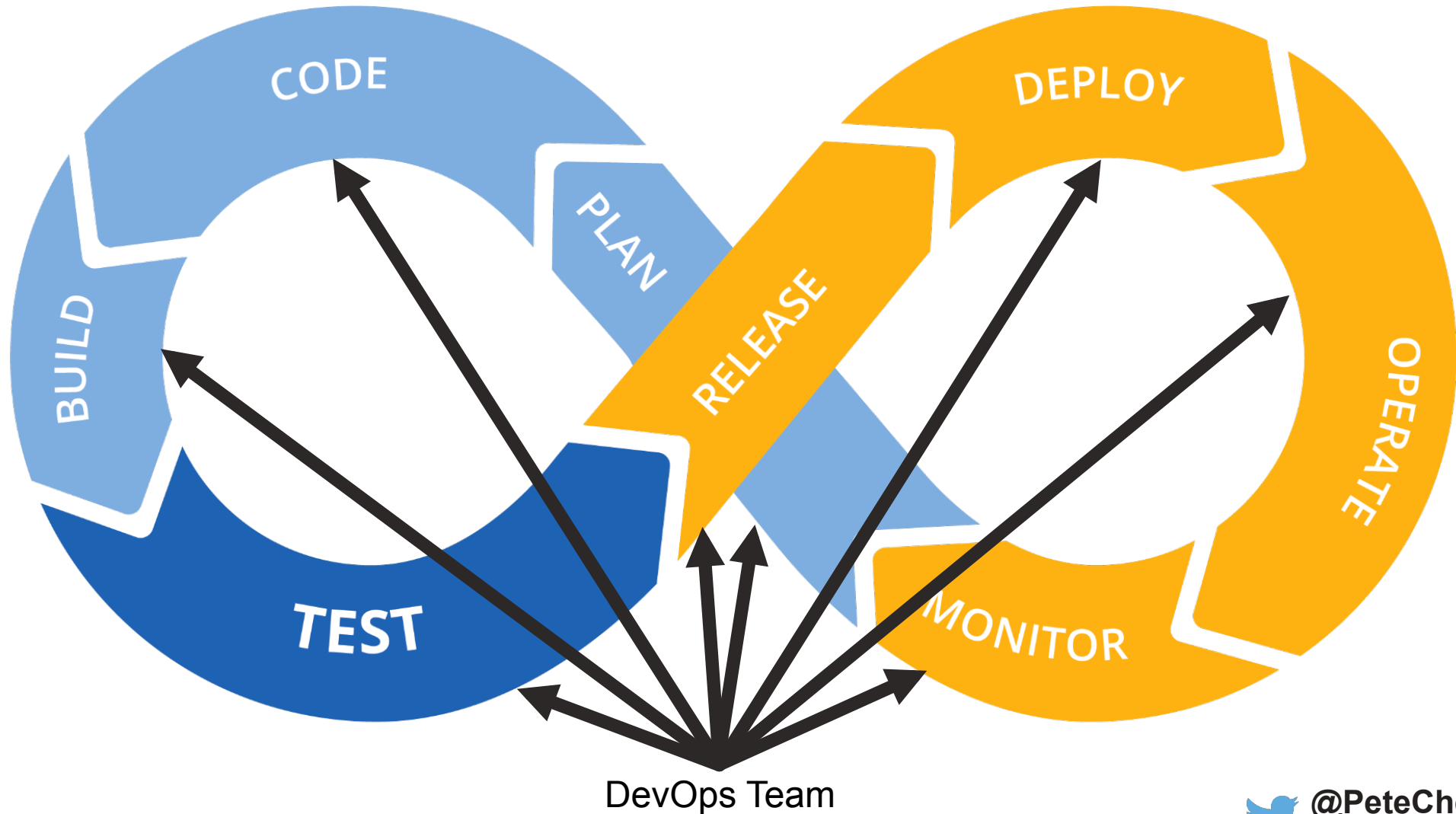
# Definition of DevOps



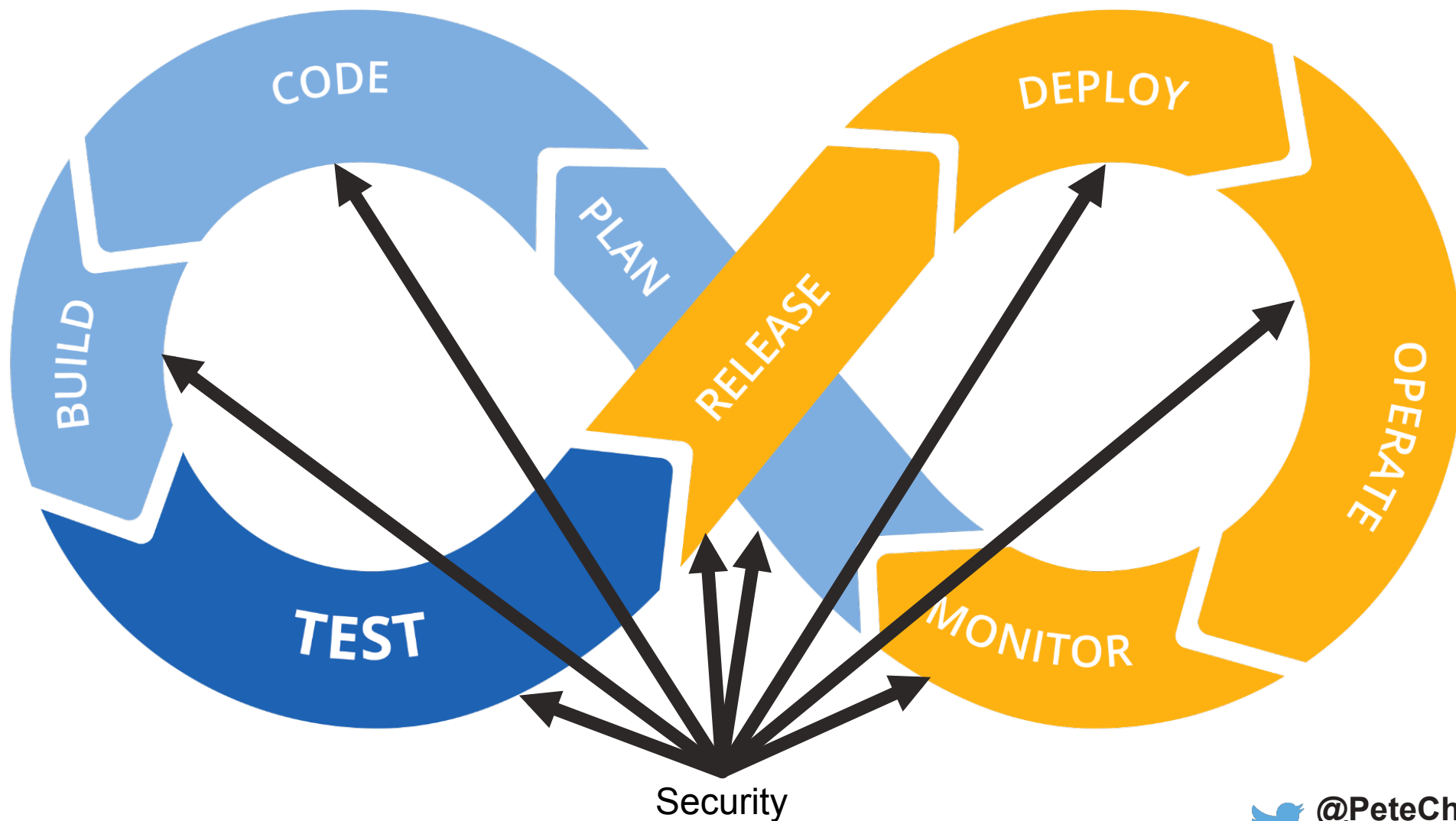
“DevOps is a cultural and professional movement, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners.”

- Nathan Harvey (Chef)

# What's a DevOps Team?



# DevOps – Process: Where is security?



# Strategy



- Relationship & Accountability
- Training & Remediation Coaching
- Security Champions & Right-sized testing



# Strategy - Relationships



- Who is your peer in development?
- Do you understand how they are goaled?
- What are their struggles?
- How often do you meet with them?
- Are they sympathetic to your goals and struggles?





# Strategy - Accountability



- Shared between development and security
- Part of annual goals for both teams
- Measured and reported regularly



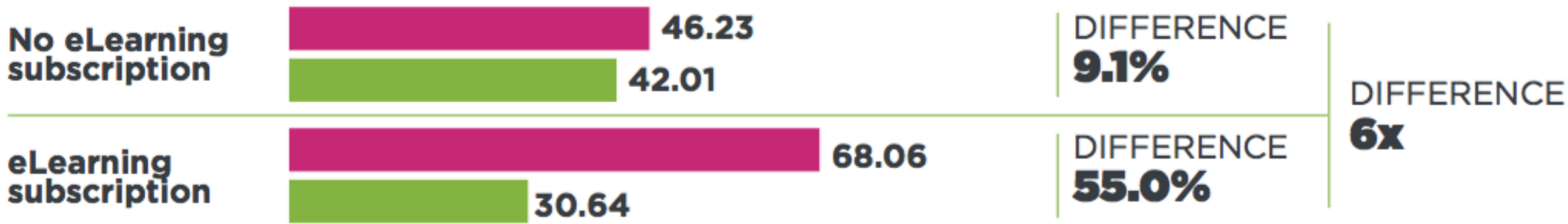


# Strategy - Training

## Reduction in flaw density via eLearning

● FIRST SCAN

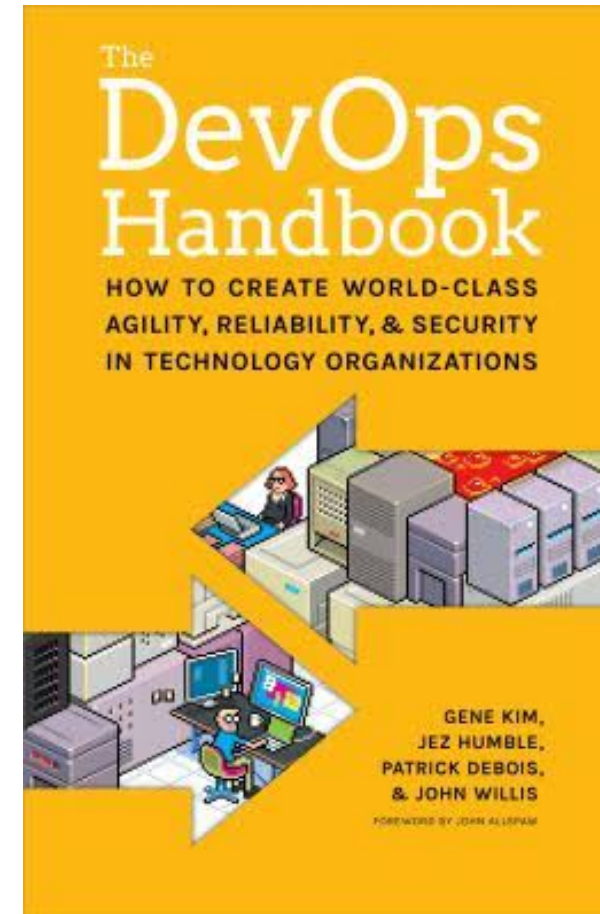
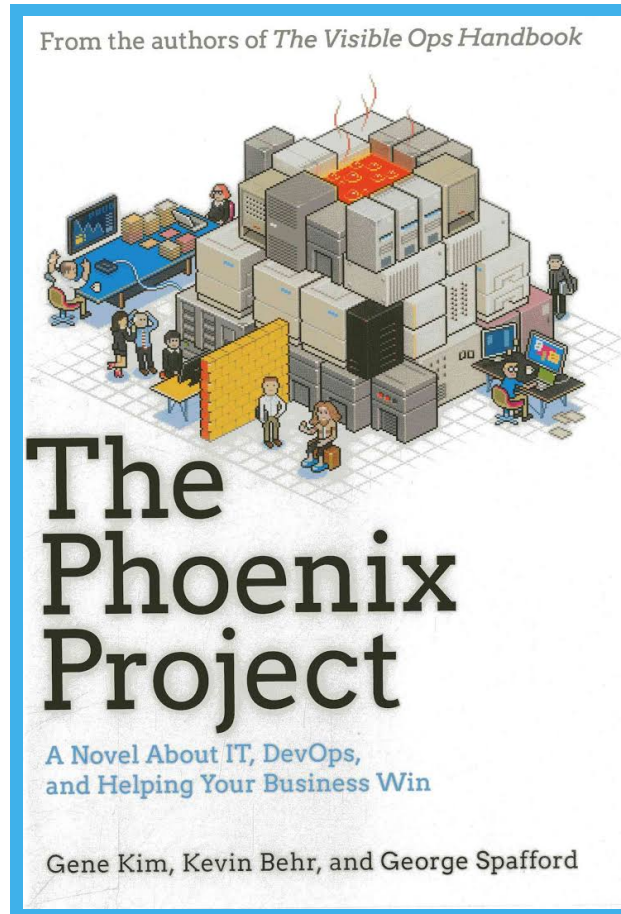
● LATEST SCAN



- 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*

# Strategy - Training



# Strategy - Remediation Coaching

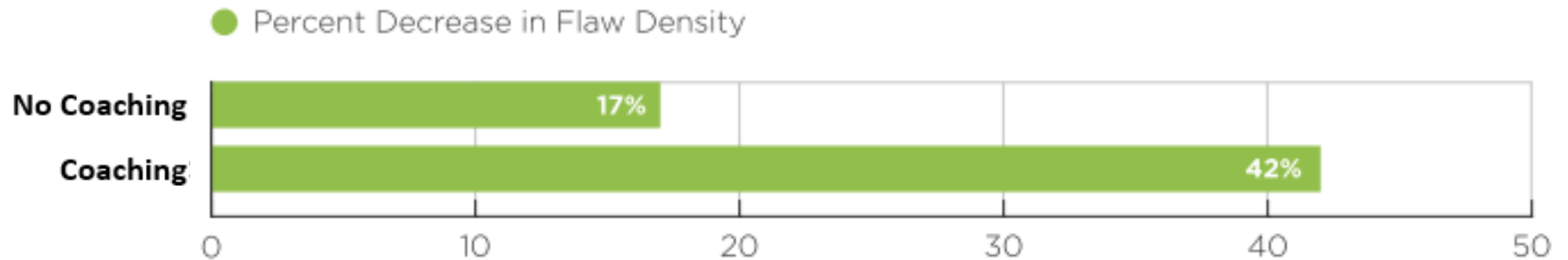


Figure 10: Relative Improvement in Flaw Density via Remediation Coaching (Readout)

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

# Strategy – Security Champions



- Eyes and ears of security
- Specialized training
  - Basic security concepts
  - Threat modeling
  - Grooming guidelines
  - Secure code review training
  - Security controls
  - CTF Exercises
- Escalate when necessary



# Strategy – Right-sized Security

Plan

Code

Build

Test

Stage

Deploy

Monitor



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



**Static Application Security Testing + 3<sup>rd</sup> Party Risk Analysis**

**Dynamic Application Security Testing**

**Runtime Application  
Self Protection**



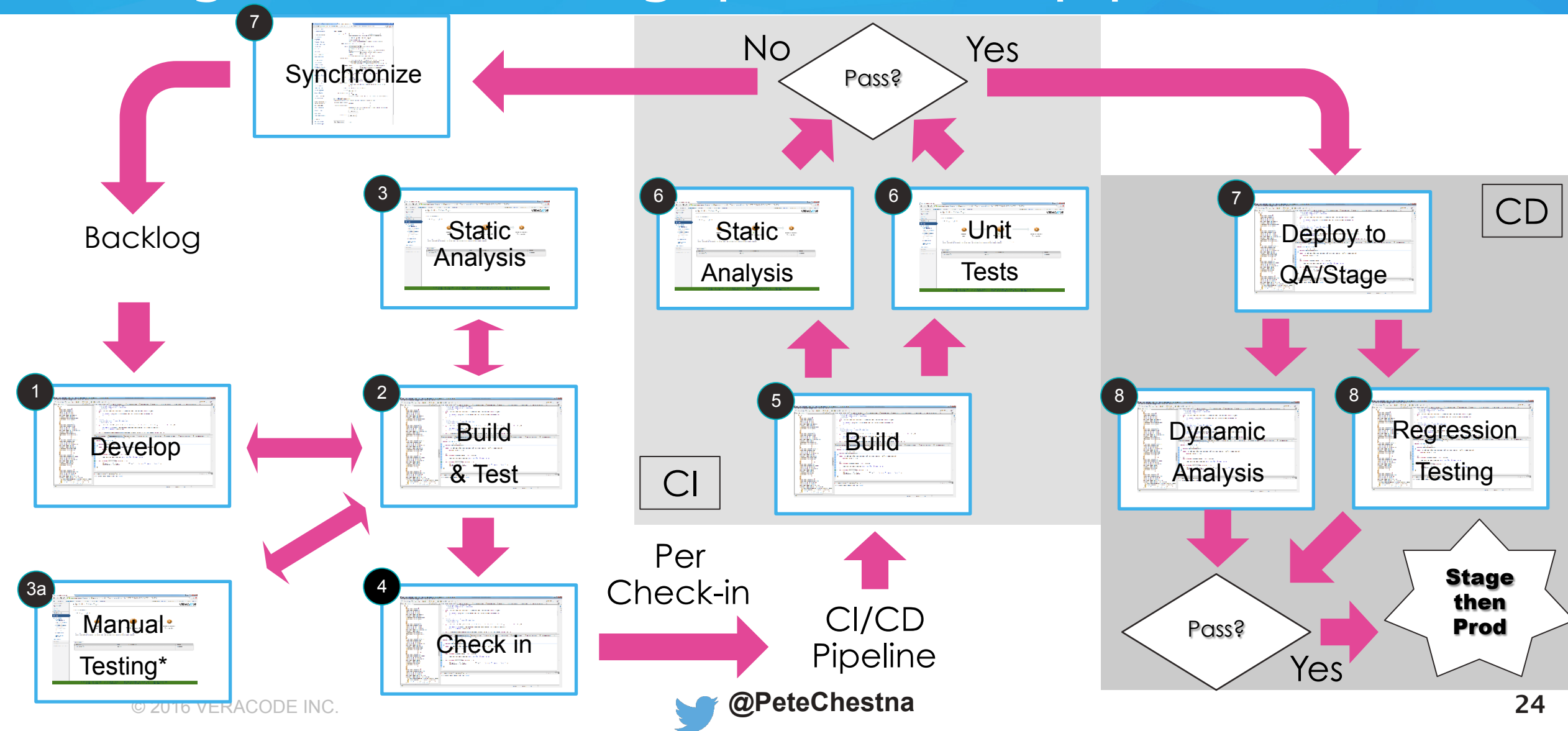
**Threat Modeling  
Security Grooming  
Secure Design**

**Remediation and Mitigation Guidance  
Secure Code Reviews**

**Manual Penetration Testing  
Red Team Activities**



# Strategy – Right-sized testing: protect the pipeline

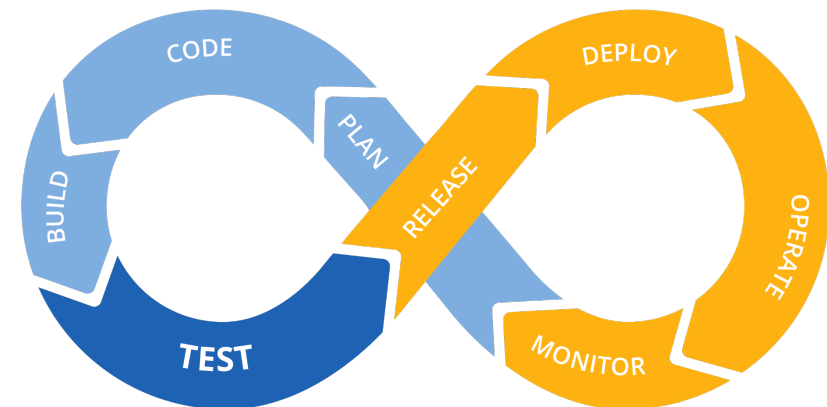




# Conclusions



- DevOps is inevitable – learn it
- Relationships and shared accountability is key to securing apps
- Train developers and help them fix what they find
- Adjust to the speed of DevOps and right-size your security requirements





# Questions?

