AppSec in a World of Digital Transformation

John B. Dickson, CISSP #4649
@johnbdickson
March 14, 2019

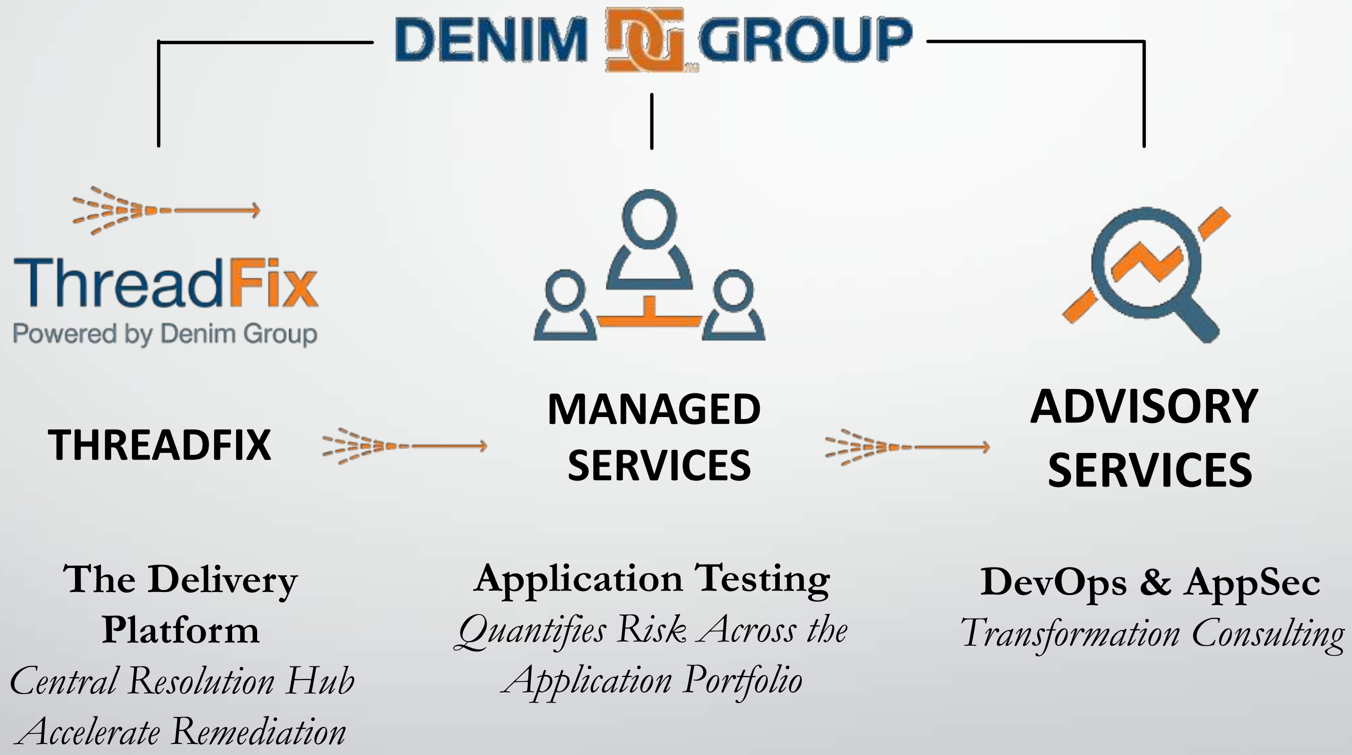
Overview

- Digital Transformation Defined (Ughhhh….)
- The Business Imperative to Move Faster
- What This Means for You
- AppSec in a New World

John’s Background

- Application Security Enthusiast
- Helps CSO’s and CISO’s with AppSec Programs
- ISSA Distinguished Fellow
- Security Author and Speaker
- DG Principal, MBA, & Entrepreneur

Denim Group Overview



DENIM GROUP

ThreadFix
Powered by Denim Group

THREADFIX

MANAGED SERVICES

ADVISORY SERVICES

The Delivery Platform
Central Resolution Hub
Accelerate Remediation

Application Testing
Quantifies Risk Across the Application Portfolio

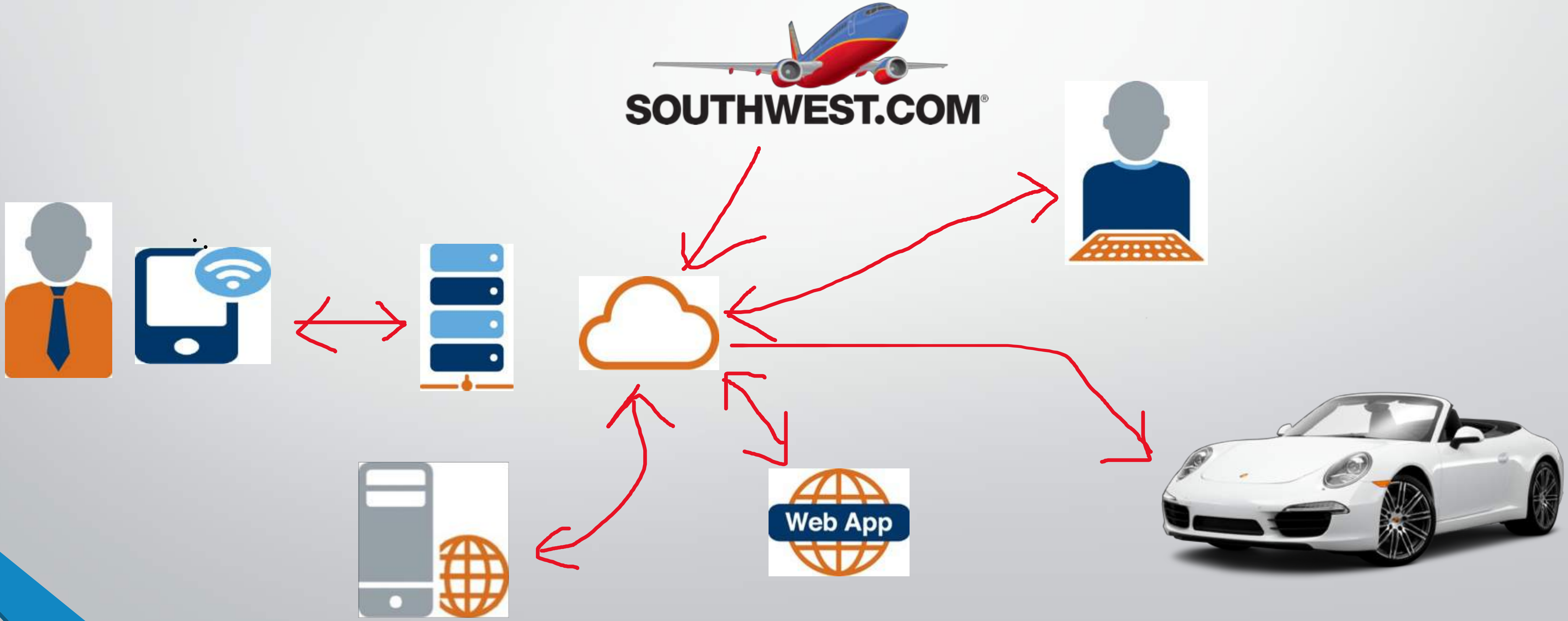
DevOps & AppSec
Transformation Consulting

Disclosure Statement

I hate the term “digital transformation”

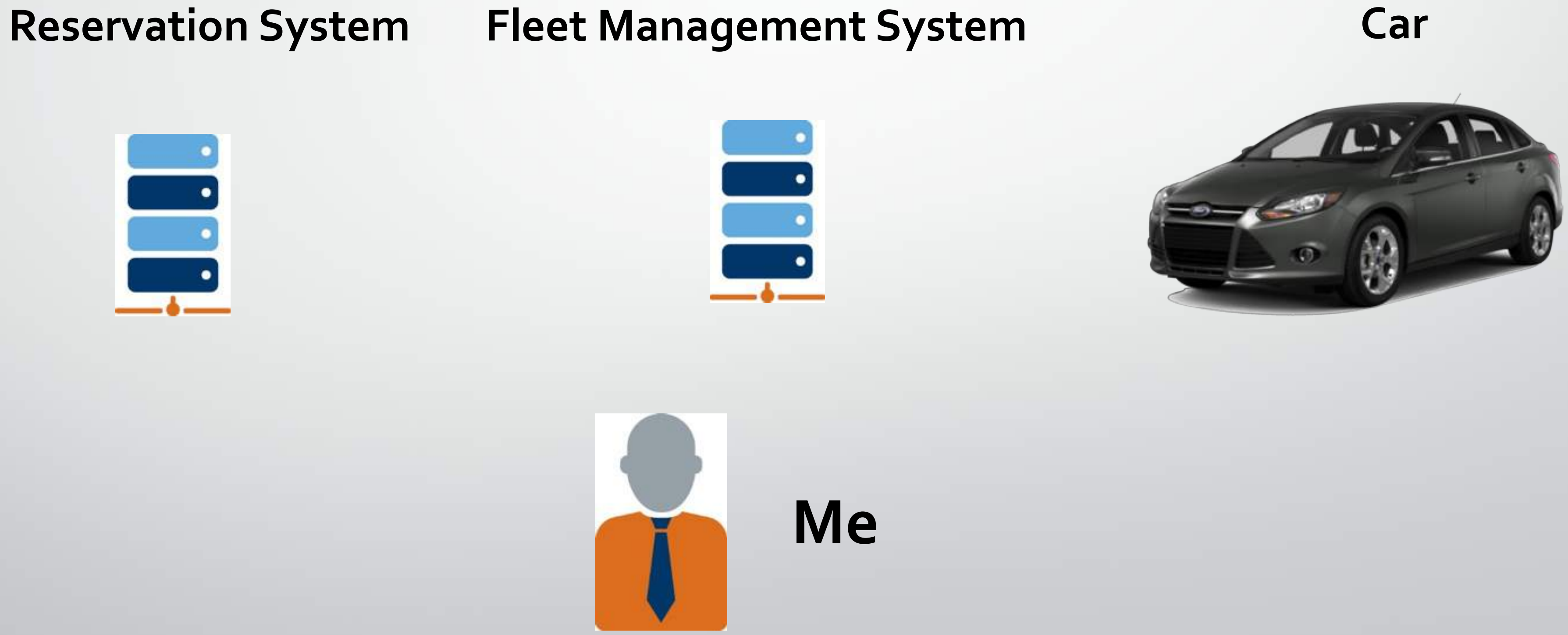
Tale of Two Rental Car Experiences

Story #1: Pleasant Customer Experience



Story #2: Customer Dumpster Fire

Story #2: Dumpster Fire Backend



Reservation System

Fleet Management System

Car

Me

Digital Initiatives

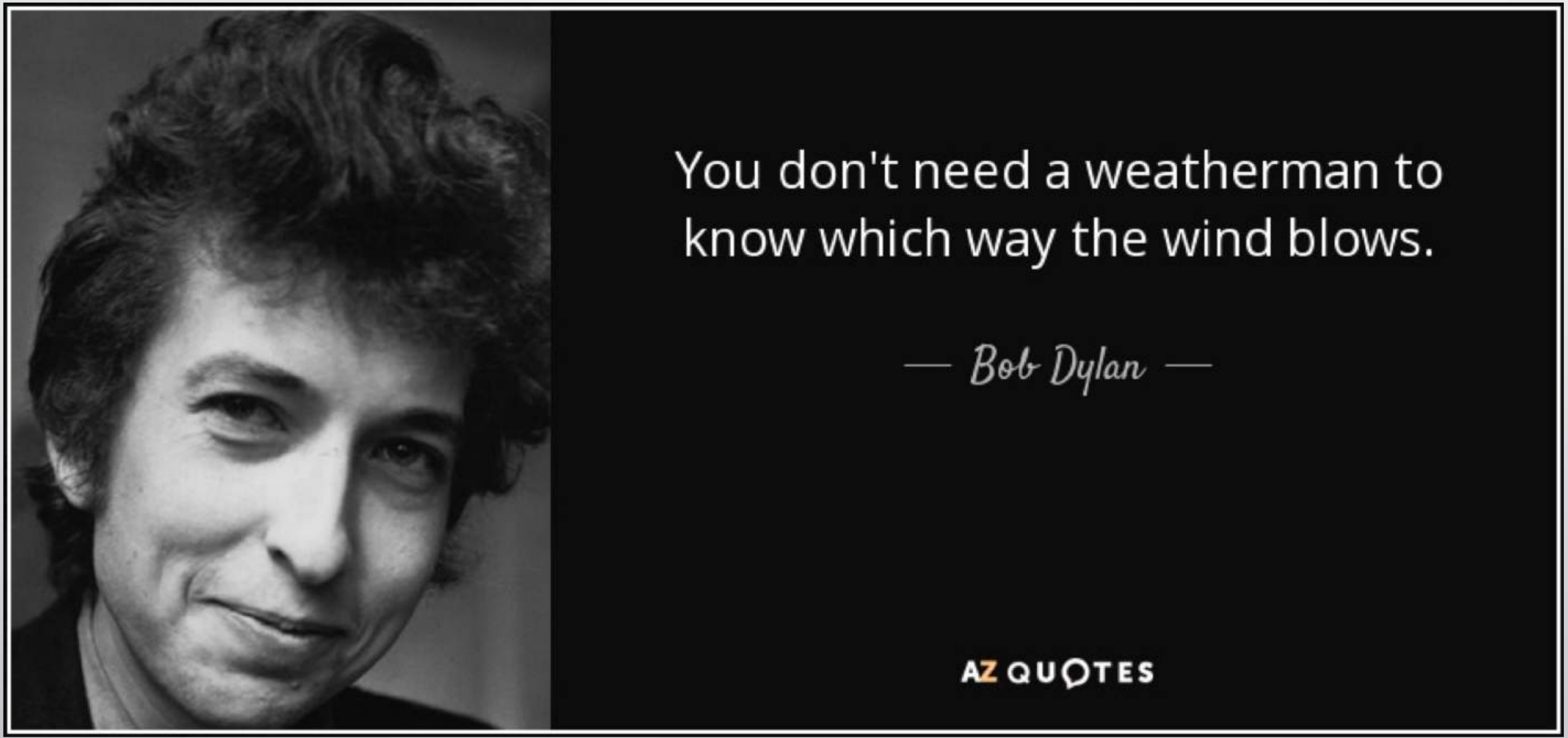
- Business survival instinct in play
- Pressure to push products to services to the market faster with a better customer experience
  - Time to market beats many other considerations
- Heavy use of user behavior analytics to customize buying experience

What This Means for You

- Rollout of new features measured in days & weeks, not months
- Connected systems throughout the organization
- Organizational changes are accelerating
- Security might be a consideration, but time-to-market considerations are paramount

Entire Tech Stack Changing

- Microservices
- Serverless Applications
- New(er) Languages & Frameworks
- All via CI/CD Pipelines

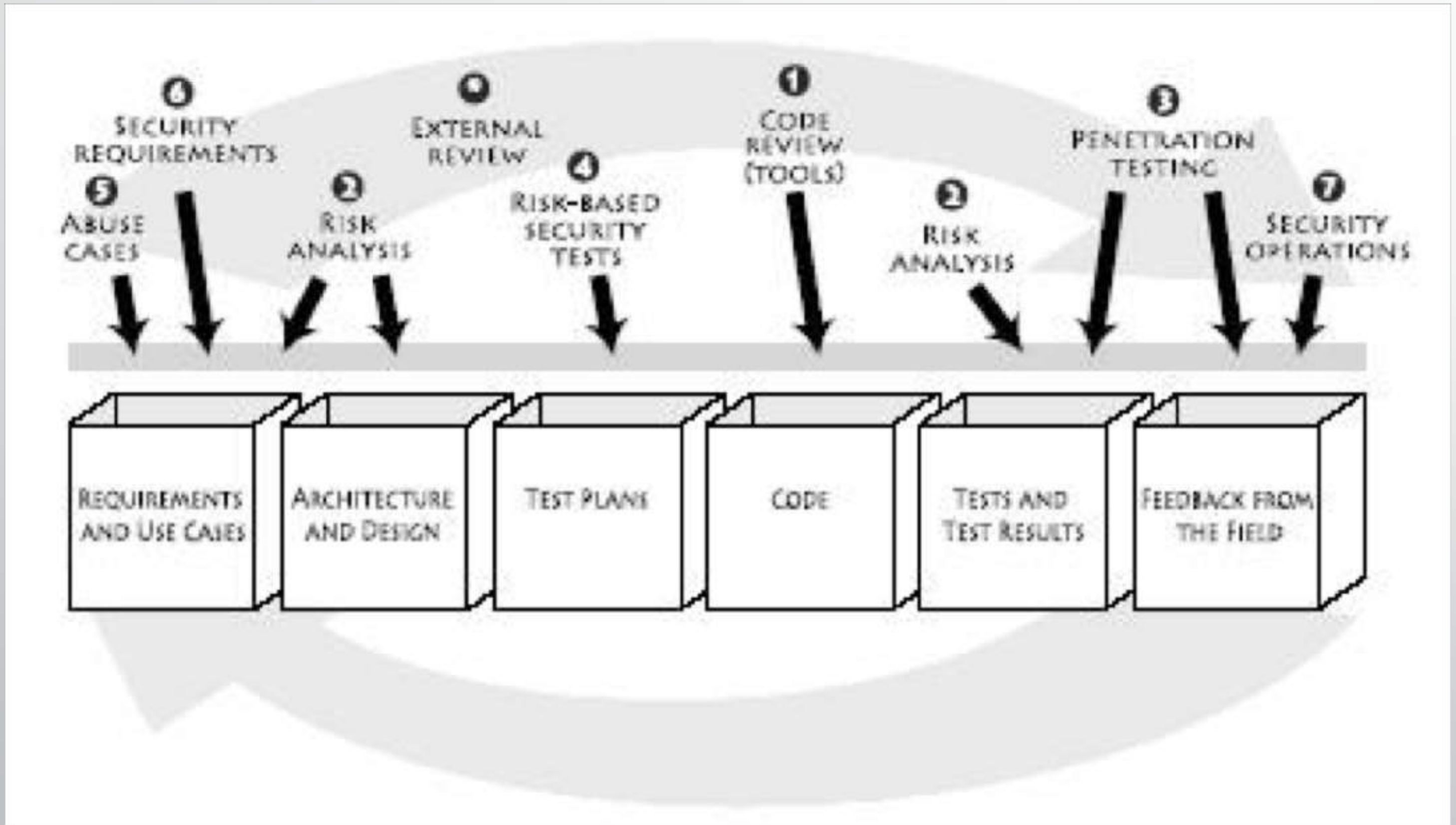


You don't need a weatherman to know which way the wind blows.

— Bob Dylan —

AZ QUOTES

Seven Touchpoints for Software Security



Gary McGraw, PhD.

One-Size-Fits-All Assembly Line AppSec

Dirty Truth of AppSec

- Most appsec automation was optimized for web applications written in compiled languages
- Many WAFs are still pure layer 7 logging devices
- Automated scanning coverage was never great
- Most organizations never got near 100% testing coverage

Don’t Forget Legacy Processes & Practices

Cool new Tech -> Stack

< - Legacy Apps & Infrastructure

Modernize Approach to Application Assessments

- Tune automation to technology stack you are implementing
- Beef up compensating approaches where automation comes up short
- Accelerate threat modeling
- Include as much testing in CI/CD pipeline as tolerated
- Worry more about trust
- Be mindful of where your app lands

Provide AppDev Team with Security-Annotated Cloud Reference Architecture

- On-prem security controls no longer exists
  - Not all developers have got this memo!
- So where it lands matters
  - Assume mixture of on prem/off prem clouds
- Absent of prescriptive guidance, expect devs to ”roll their own”

Streamline Threat Modeling Practices

- Threat modeling guides future dev far more than testing
- Threat modeling might be more important as automated test coverage is sketchier
- Knowing trust boundaries more important given where app lands

Help Dev Teams Build Pipelines with Securi Baked in

- Understand trade-offs of time/depth of testing
  - Understand what you’re getting and not getting
- Develop alternative dual-track testing models
- Iterative & tweak pipeline designs

Key Takeaways

- **Digital Transformation + Tech Stack Change = AppSec reset**
- **This change represents an opportunity to further security interests**
- **If not you, you risk recreating the legacy problems you inherited**

Q&A + Wrap up

@johnbdickson