ASPECT SECURITY
Application Security Experts

Achieving Visible Security at Scale with the NIST Cybersecurity Framework

SRCE Workshop
Atlanta, GA
Nov 17, 2015

Aspect Security | 9175 Guilford Road, Suite 300 | Columbia, MD 21046 | www.aspectsecurity.com

ASPECT SECURITY
Application Security Experts

ABOUT US

KEVIN FEALEY

- Principal Consultant & Practice Lead
  Automation & Integration Services
- 7 years Cybersec experience, @secfealz

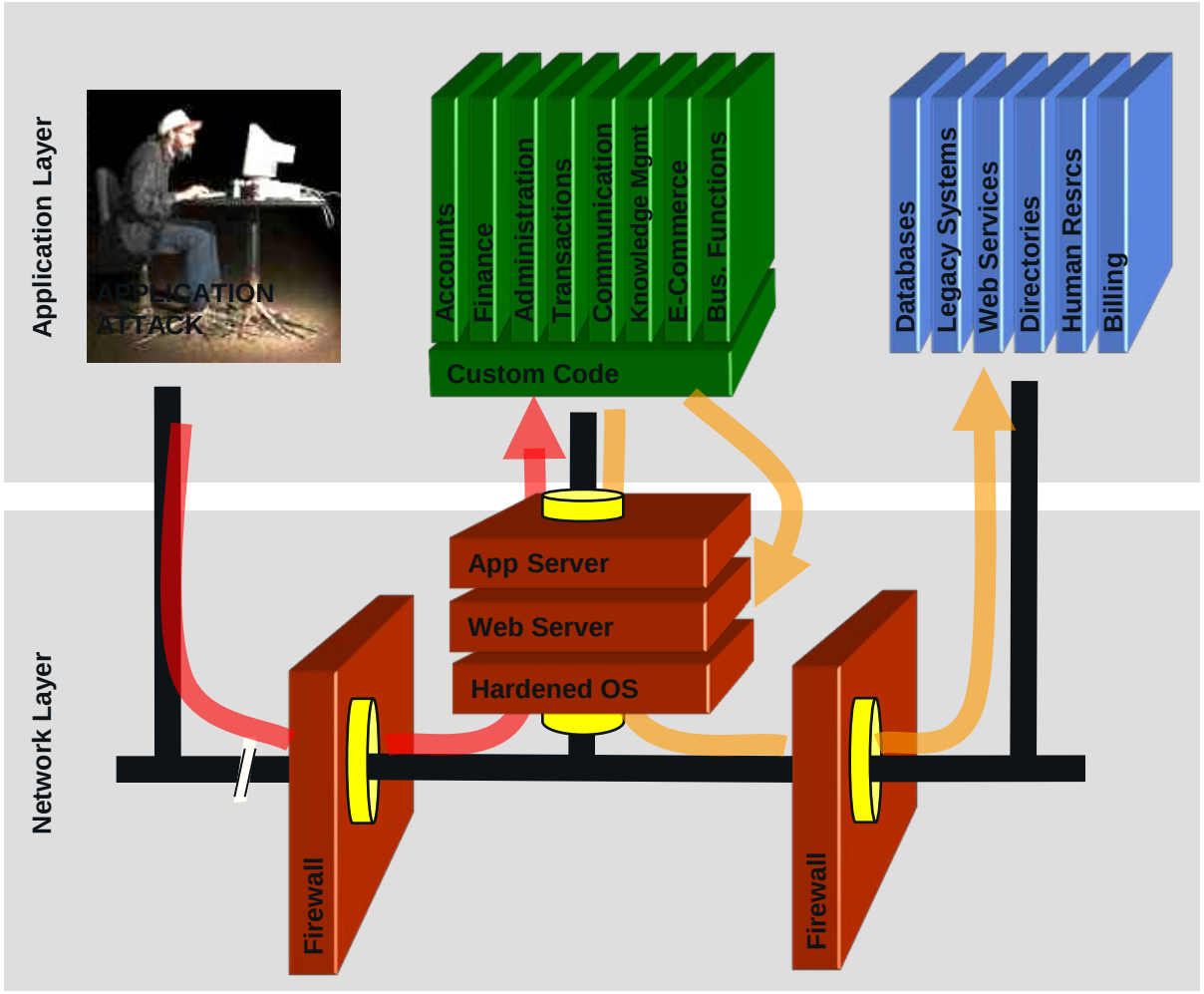
TONY MILLER

- Principal Consultant & Practice Lead
  Application Program Services
- 10 years Cybersec experience, @tjmmgd

ABOUT YOU

- Government, Private Sector?
- AppSec Team, Risk Managers?
- Used Cybersecurity Framework?

APPLICATION SECURITY VS. NETWORK SECURITY



Application Layer

- Attacker sends attacks inside valid HTTP requests.
- Custom code is tricked into doing something it should not.
- Security requires software development expertise, not signatures.

Network Layer

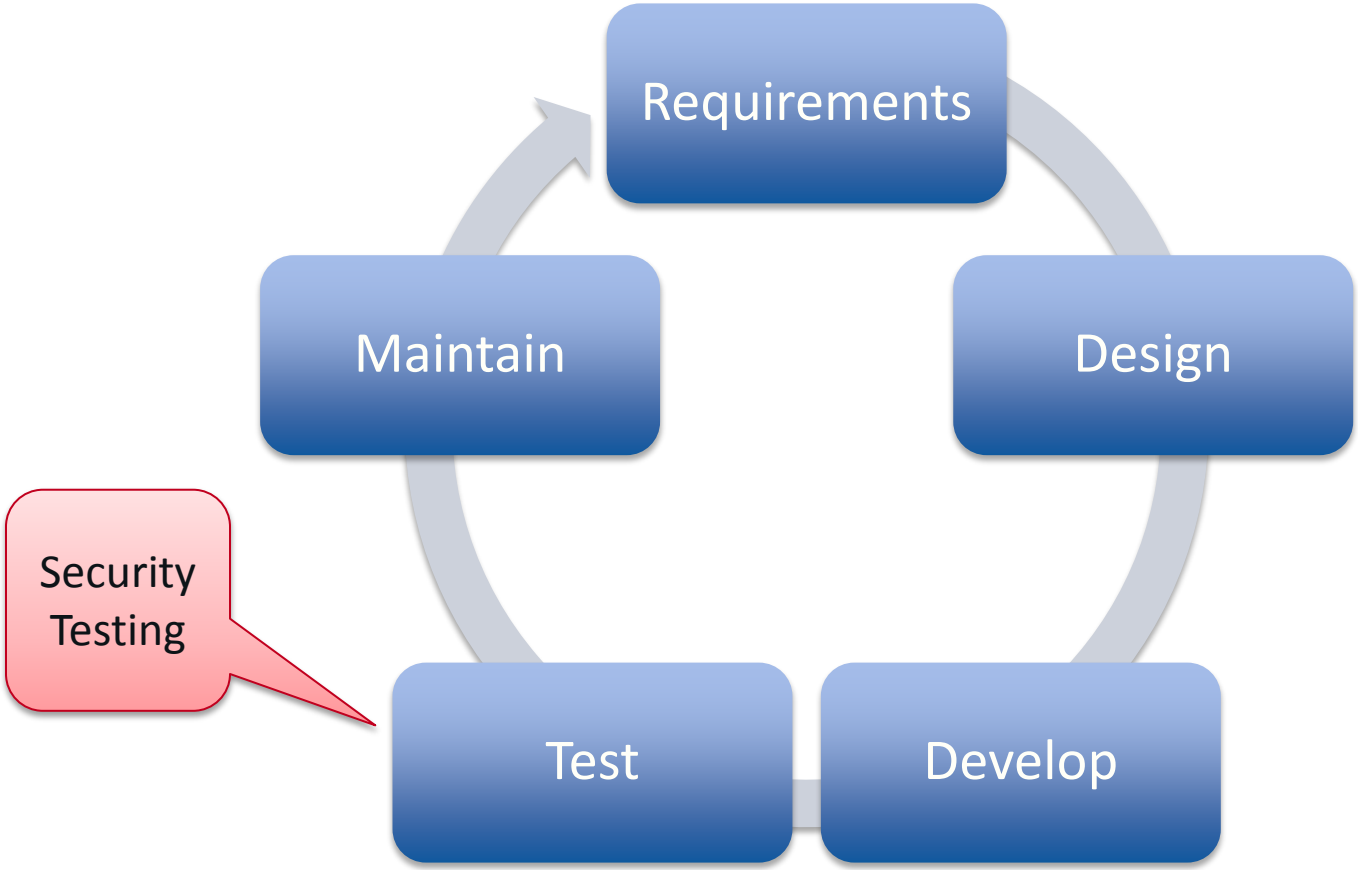
- Firewall, hardening, patching, IDS, and SSL/TLS cannot detect or stop attacks inside HTTP requests.
- Security relies on signature databases.

OWASP TOP TEN: COMMON VULNERABILITIES

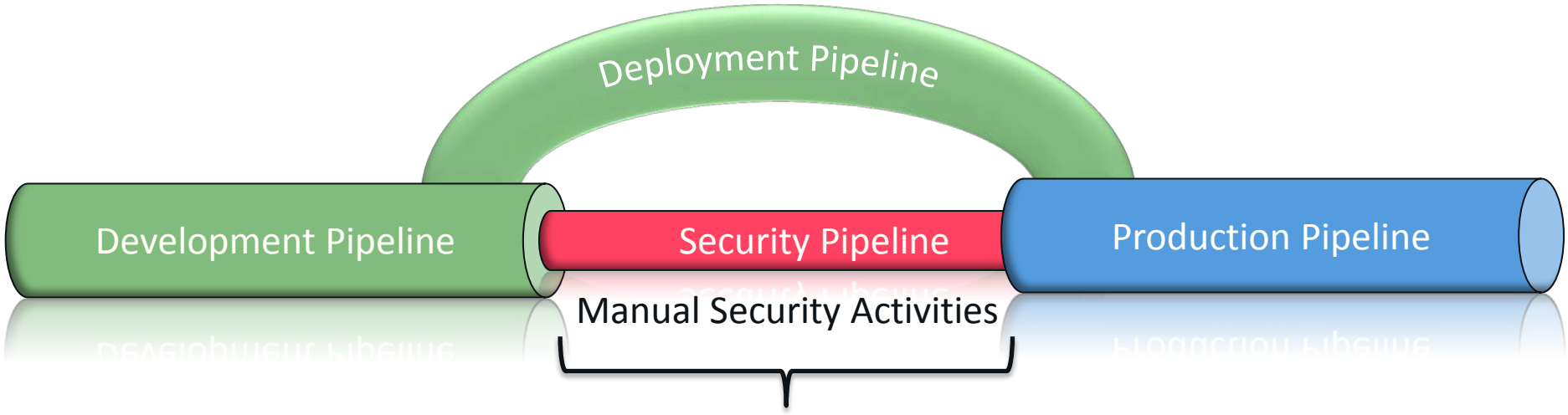
1. Injection Flaws
2. Broken Account and Session Management
3. Cross-Site Scripting Flaws
4. Direct Object References
5. Web/Application Server Misconfigurations
6. Sensitive Data Exposure
7. Broken Access Control
8. Cross-Site Request Forgery
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

OWASP
The Open Web Application Security Project
http://www.owasp.org

STANDARD SDLC

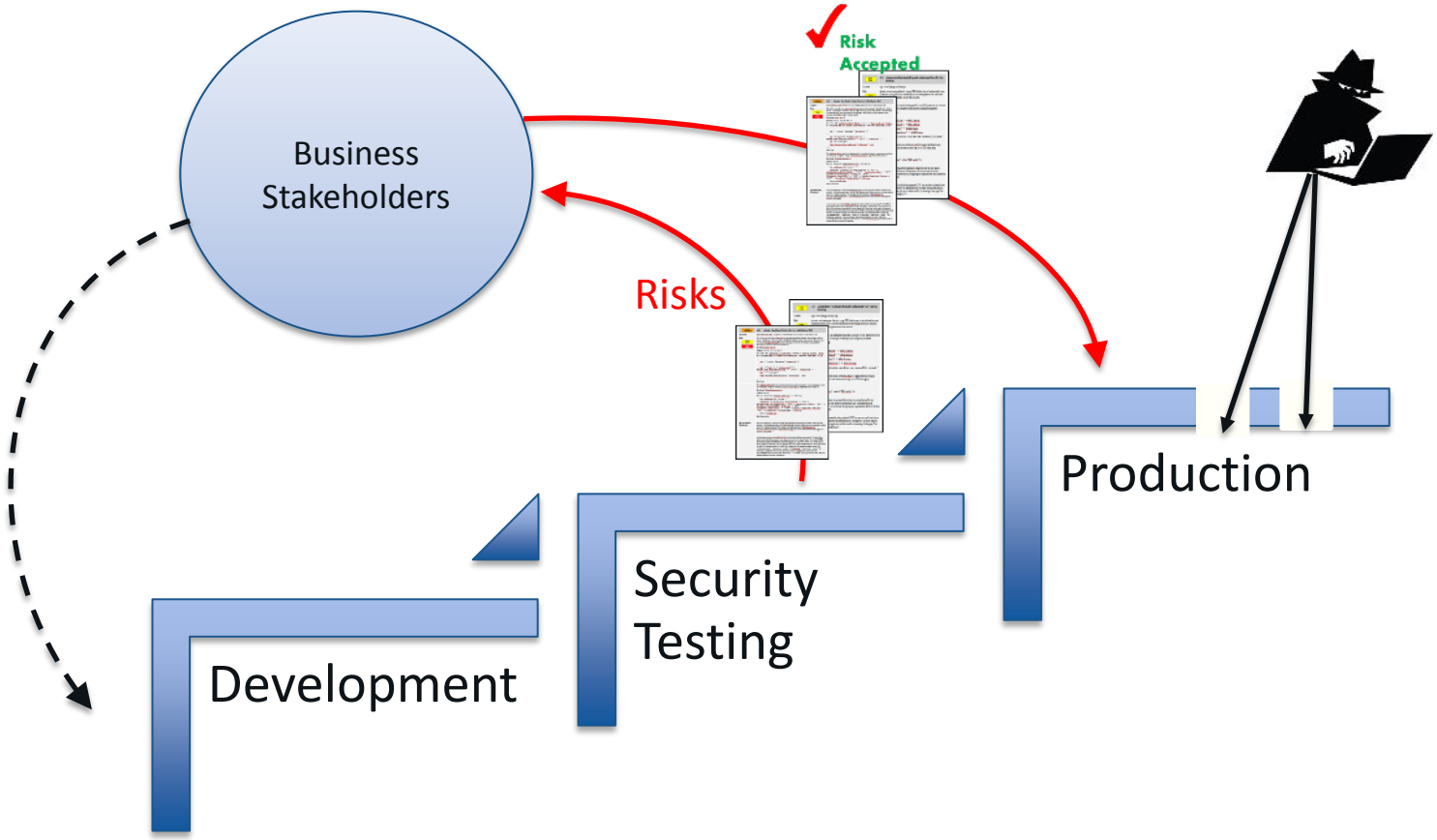


CURRENT PIPELINE



- 1-2 week duration
- Late in the SDLC
- Prone to human error

MANUAL SECURITY REVIEWS



FUTURE PIPELINE (IE. WHAT IS APPSEC AUTOMATION?)

Automate:

- Tasks that do not require security intelligence
- Verification of security policies/requirements
- Vulnerability testing
- Correlation and reporting

- Development, Security, and Operations collaborate early and often

ASPECT SECURITY
Application Security Experts

APPSEC AUTOMATION PROGRAM DEPENDENCIES

IDENTIFY	Application Inventory	• What are our assets?
IDENTIFY	Identify Risk Thresholds	• When is automated detection insufficient?
PROTECT	Standard Security Requirements	• What do we expect from our assets?
PROTECT	Common Security Controls	• How can we maximize our automation capabilities and mitigate risk?
PROTECT	Developer Training and Support	• How will we support our developers?
RESPOND RECOVER	Vulnerability Management Program	• How will we prioritize and fix issues we identify?
RECOVER	Continuous Improvement Process	• How will feedback be generated and integrated back?

ASPECT SECURITY
Application Security Experts

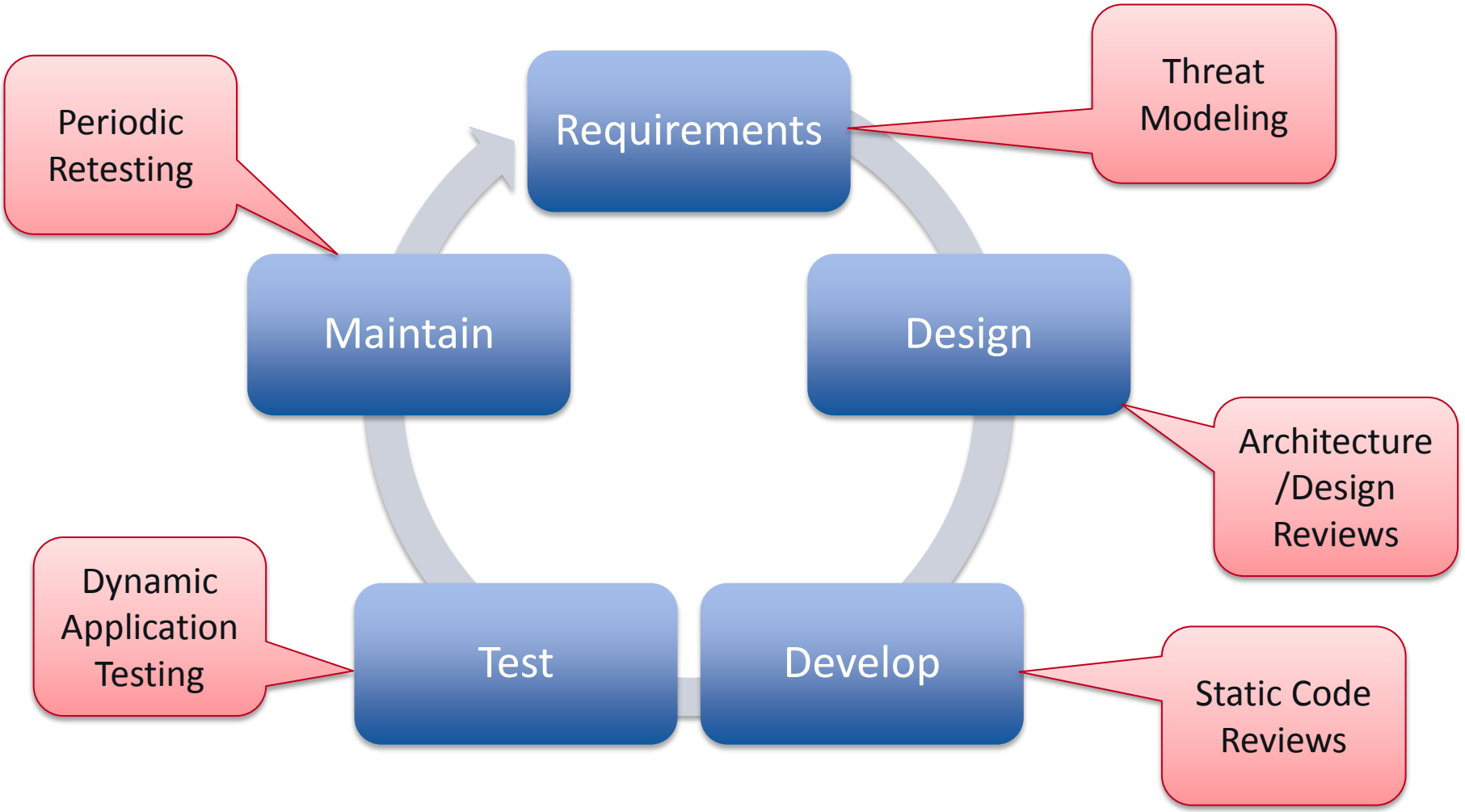
APPSEC AUTOMATION PROGRAM DEPENDENCIES

IDENTIFY	Application Inventory	• What are our assets?
IDENTIFY	Identify Risk Thresholds	• When is automated detection insufficient?
DETECT	AppSec Automation Program	• How can we effectively scale our security program to achieve business goals at a more rapid pace?
RESPOND / RECOVER	Vulnerability Management Program	• How will we prioritize and fix issues we identify?
RECOVER	Continuous Improvement Process	• How will feedback be generated and integrated back?

CYBERSECURITY FRAMEWORK 3.2

Software Security Program Review

TRADITIONAL SDLC



CHALLENGES OF DEV-OPS/AGILE

Requirements & Design Phases

- Hardly accommodated

Development to Deployment

- Highly compressed timeframes

Traditional Testing Cycles

- Can’t accommodate stunning speed

So, how do we integrate security?

ASPECT SECURITY
Application Security Experts

SECURE DEV-OPS/AGILE MODEL

Proactive	Lifecycle	Continuous Monitoring
Developer Training	Local Security SME Program	Operational Security Team
Secure Code & Architecture Standards	Targeted Security Activities (small scope)	Risk-Based Security Assurance Model
Standardized Security Controls Components	Self-Service Model Utilizing Automation	Feedback Loop Via Stories/Features

Thank you!

ASPECT SECURITY
Application Security Experts

Kevin Fealey & Tony Miller
Kevin.Fealey@aspectsecurity.com
Tony.Miller@aspectsecurity.com