AppSec in a DevOps World

Peter Chestna
Director of Developer Engagement
Who am I?

• 27 Years Software Development Experience
• 12 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
Goals

• Why is AppSec important?
• How is AppSec traditionally done?
• Goal of AppSec?
• What needs to change?
Applications Are as Risky as Ever

- 35% of all applications used some kind of hard-coded password
- 39% of all applications use broken or risky cryptographic algorithms
- 28% of all applications were vulnerable to open redirect attacks
- 16% of all applications mix trusted and untrusted data in the same data structure or message
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.

“Is poor software development the biggest cyber threat?” CSOonline.com, September 2, 2015.
High Profile Breaches Through the App Layer

**Retailer**
- **How:** Sophisticated kill chain including exploitation of vulnerable web application
- **Result:** Hackers stole names, mailing addresses, phone numbers and email addresses 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 businesses 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 personal data belonging to 4.5 million patients

**Financial Institution**
- **How:** Hackers exploited a known vulnerability in an open source component
- **Result:** Social Security Numbers and personal data for more than 143 million Americans stolen. Three executives lose their jobs.
California Breaches
Built mostly from components
Expanding Digital Footprint
Is this your current AppSec program?
Which outcome do you see?
AppSec at a glance

Training
(eLearning, instructor led, metadata driven)

Static Application Security Testing + 3rd Party Risk Analysis
Open Source Risk Monitoring

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
Technology

Waterfall

Agile

DevOps
The Goal?
When do we test?
Fitting into Agile and DevOps

1. Backlog

2. PI

5. Stand-up

6. Track Visibly

70%

10. Review & Reflect

Really finish work

Copyright 2005, Mountain Goat Software
The real cost of a bug?
The Goal?
“DevOps is a cultural and professional movement, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners.”

- Nathen Harvey (Chef)
What’s a DevOps Team?

DevOps Team

- Code
- Build
- Test
- Plan
- Release
- Deploy
- Operate
- Monitor
DevOps – Process: Where is security?
Strategy
The First Way: Systems Thinking
PULLING TOGETHER

Only works when you’re not jerking in opposite directions like idiots.
Mutual Accountability
The Second Way: Amplify Feedback Loops

DEV → SEC → OPS
Feedback is a Gift!
Measurement is Key
Training and Awareness
Train Security on the Process
DevOps – Security – Integrated into Pipeline

1. Backlog
2. Develop
3. Build & Test
4. Check in
5. Build
6. Static Analysis
7. Static Analysis
8. Unit Tests
9. Dynamic Analysis
10. Regression Testing
11. CI/CD Pipeline
12. Synchronize
13. Manual Testing*
14. Per Check-in
15. Yes
16. No
17. Deploy to QA/Stage
18. Stage then Prod
19. Pass?
20. Pass?
21. CD
22. Yes
23. No

* Manual Testing is an optional step in the pipeline.
Help them fix what they find
The Third Way: Experimentation and Learning
TRADITION
JUST BECAUSE YOU’VE ALWAYS DONE IT THAT WAY DOESN’T MEAN IT’S NOT INCREDIBLY STUPID.
MISTAKES
It could be that the purpose of your life is only to serve as a warning to others.
Security Champions