YOUR CHANCE TO GET IT RIGHT: KEYS TO BUILDING APPSEC INTO DEVOPS

Chris Wysopal
CTO & Co-founder Veracode
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?
Release Timelines & Team Sizes

**Waterfall**
- 1-4 Releases Per Year
- 50+ people

**Agile**
- 12-24 Releases Per Year
- 6-12 people

**DevOps**
- 100+ Releases Per Year
- 6-12 people
Plan | Dev | QA | Sec | Ops
---|---|---|---|---
Waterfall | ![Lightbulb](image1) | ![Arrow](image2) | ![Checkmark](image3) | ![Shield](image4) | ![Factory](image5)

Business Intent
App Knowledge
Ops Knowledge

Agile | ![Lightbulb](image1) | ![Arrow](image2) | ![Checkmark](image3) | ![Shield](image4) | ![Factory](image5)

Business Intent
App Knowledge
Ops Knowledge

DevOps | ![Lightbulb](image1) | ![Arrow](image2) | ![Checkmark](image3) | ![Shield](image4) | ![Factory](image5)

Continuity
Technology

Waterfall

Agile

DevOps
What is 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.

- NATHEN HARVEY (CHEF)
What’s a DevOps team?
What is DevSecOps?
How can you implement DevSecOps?

- Security Champions
- Relationship & Accountability
- Training & Remediation Coaching
- 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 – 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
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.
Strategy - Training
Strategy - Remediation Coaching

<table>
<thead>
<tr>
<th>Flaw Density - First Scan</th>
<th>Flaw Density - Last Scan</th>
<th>Reduction</th>
<th>Fix Rate</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation Coaching</td>
<td>41.04</td>
<td>12.4</td>
<td>30.2%</td>
<td>87.6%</td>
</tr>
<tr>
<td>No Remediation Coaching</td>
<td>33.81</td>
<td>6.5</td>
<td>16.1%</td>
<td></td>
</tr>
</tbody>
</table>
Strategy – Right-sized 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
Conclusions

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

Chris Wysopal
cwysopal@veracode.com
@WeldPond