APPSEC BEHAVIORS FOR DEVOPS
BREED SECURITY CULTURE CHANGE
About Chris Romeo

• CEO / Co-Founder / Security Culture Hacker @ Security Journey

• Experience

  • 20 years in the security world, CISSP, CSSLP
  • 10 years at Cisco, leading the Cisco Security Ninja program & CSDL

• Speaker at RSA, AppSec USA, AppSec EU, & ISC2 Security Congress

• Co-host of the #AppSec PodCast

• Owner of a DevOps build pipeline; consulting with companies trying to figure out AppSec + DevOps
Behaviors $\rightarrow$ mindset, skills $\rightarrow$ skill sets
Agenda

• The State of DevOps and Security
• DevOps Culture
• Security Components for DevOps
• Creating a DevOps + Security Culture
• Security Behaviors and Habits
• Conclusion and Key Takeaways
DevOps delivers agility and growth, but 80 percent still struggle with it

Everyone is doing DevOps, but how many are really doing DevOps? Survey shows there's work to be done.

By Joe McKendrick for Service Oriented | January 12, 2016 -- 16:52 GMT (08:52 PST) | Topic: Enterprise Software

DevOps largely failing to improve security, study shows

Despite the promise of improved application security, DevOps is failing to deliver due to some key barriers, an HPE study shows

Warwick Ashford Security Editor
25 Oct 2016 12:45
A DevOps
DevOps according to DevOps Borat

To make error is human. To propagate error to all server in automatic way is #devops.

Rockstar programmer are just as you and me but they can also able write insecure Ruby code.
WORKED FINE IN DEV

OPS PROBLEM NOW

I DON'T ALWAYS TEST MY CODE

BUT WHEN I DO I DO IT IN PRODUCTION
All things continuous

Continuous

Integration
Delivery
Deployment
Security?
Security Test?
So What?

Why does PSIRT care?
5 things people HATE about DevOps

1. Everyone thinks it's all about Automation.

2. "True" DevOps apparently have no processes - because DevOps takes care of that.

3. The Emergence of the "DevOps' DevOp", a pseudo intellectual loudly spewing theories about distantly unrelated fields that are entirely irrelevant and speaking at conferences.

4. People constantly pointing to Etsy, Facebook & Netflix as DevOps. Let's promote the stories of companies that better represent the market at large.

5. Lack of fit for anyone who is not in a Dev or Ops role.
A DevOps culture

1. Things move fast
2. Small pieces of work checked in often
3. Autonomous teams with transparency; No silos
4. Building quality into the development process
5. Feedback / eliminate blame / embrace failure
6. Automation
Can we stop the \{Sec\}Dev\{Sec\}Ops\{Sec\} naming foolishness? Just call it DevOps and focus on making security a natural part of building stuff.
Security components to go fast

- Security best practices
- Threat modeling
- Static analysis
- Security code review
- Dynamic analysis
- Vulnerability scanning
- 3rd Party SW / Dependency checker
- Red Teaming
- PSIRT
A DevOps + Security

- Threat modeling
- Static analysis
- Security code review
- Dynamic analysis
- Vulnerability scanning
- Red Teaming
- 3rd Party SW / Dependency checker
- PSIRT

Security best practices
“What happens \{with security\} when people are left to their own devices.”

--Tim Ferriss
1. Application security is about the people.
2. The people introduce the vulnerabilities.
3. Security in DevOps must change the people.
Defining features of a **sustainable** DevOps security culture

- **Deliberate and disruptive**
- **Eliminate Security Blame**
- **Building Quality AND Security In**
- **Security Transparency**
- **No security silo**
How do we embed a culture of security?

Culture Hacking

Community

Automation
Security Behavior

- a manner of behaving that decreases danger, risk, or threat

Light weight

Well defined

Easily repeatable

Why and ROI

Clear start and finish point
Security behavior vs. security process

Step 1  Step 2  Step 3
Security habits

Reminder → Routine → Reward
Build security in

Security best practices

Desired Outcome
- A wide spread attitude / culture change
- Consideration of security best practices early

Habit Generation
- Explain WHY they should care
- Demonstrate how best practices are done
- Understand the negative case, or not doing them
Uncover design security problems

Desired Outcome
- Choose the design decision that protects the confidentiality and integrity of customer data

Threat modeling

Habit Generation
- Show developers how to create a threat model
- Quickly move to threat modeling an active design on which they are working
- Enable the security light bulb
React to automated security bugs

Desired Outcome

- Interpret automated security notifications as a gift and not a curse

Habit Generation

- Position the interruption as close to the dev as possible (IDE based SA)
- Aggressively limit false positives – do not scan for everything in the beginning
Detect security flaws in other’s code

Security code review

**Desired Outcome**

- Find the errors in the code that could be exploited if they reach production (those missed by automated scans)

**Habit Generation**

- Force a security code review in the code commit process
- Require a security +1 for each check-in
- Teach your developers the fundamental security lessons of their languages, and how to find those issues in code
Eradicate 3rd party software vuln’s

3rd Party SW / Dependency Checking

Desired Outcome
• Eliminate known vulnerable components at deploy time

Habit Generation
• Break the build on a dependency checker failure
Be mean to your code

Desired Outcome

- Uncover flaws using active testing, fix those flaws, and push the fixes to production as fast as possible.

Habit Generation

- Instill the idea that your code will be attacked
- Provide the time and tools for everyone to spend time attacking
Respond in a timely and organized fashion

Desired Outcome
• Partnership between dev and PSIRT to alleviate any security bugs in the shortest amount of time possible

Habit Generation
• Talk to and educate developers about the PSIRT mission
<table>
<thead>
<tr>
<th>Security Behaviors for DevOps</th>
<th>Build Security In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncover design security problems</td>
<td></td>
</tr>
<tr>
<td>React to automated security bugs</td>
<td></td>
</tr>
<tr>
<td>Detect security flaws in other’s code</td>
<td></td>
</tr>
<tr>
<td>Eradicate 3rd party software vuln’s</td>
<td></td>
</tr>
<tr>
<td>Be mean to your code</td>
<td></td>
</tr>
<tr>
<td>Respond in a timely and organized fashion</td>
<td></td>
</tr>
</tbody>
</table>
Security behaviors through security community

- People
- Monthly Training
- Security Days
- Internal Capture the Flag
- Conferences

Build a security [advocate, guild, champion] program
Apply What You Have Learned Today

■ Next week:
  – *Assess your organizational DevOps and security culture*
  – *Survey DevOps population to gauge response to security*

■ In the first three months:
  – *Prioritize security behaviors and form a plan*
  – *Focus on the security behavior that is your top priority and invest in making it successful*

■ Within six months:
  – *Branch out to your top three security behaviors and focus in*

■ Within one year:
  – *Roll out all the security behaviors*
Key takeaways

1. Just call it DevOps and focus on making security a natural part of building stuff.
2. Security behaviors embed security without all the overhead.
Resources to learn more

https://techbeamcom/contributors/chris-romeo
Q&A and Thank you!

Chris Romeo, CEO / Co-Founder
chris_romeo@securityjourney.com
www.securityjourney.com
@edgeroute, @SecurityJourney