TRANSFORMING DEVELOPERS INTO SECURITY PEOPLE
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

@edgeroute

Copyright © Security Journey, 2017
Agenda

- Security Matters, Developer
- Security is a Stretch for Developers
- Four Developer Responses to Security
- Security Behaviors
Software is Eating the World
The Mindset of the “Average” Developer
When software is eating the world, it becomes your *social* responsibility to write correct, maintainable and understandable code.
Objections to Application Security

- Speed
- Methodology
- No
We Already Have a "Security Department"

Source: BSIMM-7
State of Developer Security

- Security is a stretch.
- Security IQ is low.
- Dev is first line of defense.
Developers Are Not Monsters
The Goal

Developers that think like security people.
The Security Person Mindset

- Foundational knowledge
- Understand attacks
- Acknowledge attacks
- Utilize tools and processes
Start with Why

Source: Simon Sinek, “Start with Why”
The Security Culture Bell Curve

- Security people
- Security interested
- Early Majority
- Forced compliance
- Probably never going to do it
1. Application security is about the people.
2. The developers are the key.
Developer Responses

Unfamiliar  Overworked  Apathetic  Gung Ho
Developer Response #1: Unfamiliar / Ignorance

1. “Why? like legit why do we need to do security?”
2. “Don’t understand security and don’t know what to do.”
3. “We’re little. No one would go after us.”
4. “Security causes change, and change is too risky for our apps.”
Action: Foundational Lessons

- Security Fundamentals
- Attacks & Attackers
- Simple SDL
- Security Myths
- Privacy & Customer Data Protection
- Security Business Case
Action: Everyone is a Security Person
Developer Response #2: Overworked

1. “Too much other work to do”
2. “Management does not provide time for security”
3. “Security is an unfunded mandate.”
4. “We don't have time to build in security.”
Action: Automation and Simplify
Action: Management / Executive Education
Developer Response #3: Apathetic / Complacent / “Know it All”

2. “It's someone else's responsibility, not mine.”
3. “We have nothing worth protecting.”
4. “We’ve always done things THIS way.”
5. “I already know all this stuff.”
Action: Shock Value

11.5 million documents
214,488 offshore entities
2.6 terabytes of data
Action: Compliance
1. “Where can we learn more about security?”
2. “Is there someone that can mentor me to help me grow as a security person?”
3. “I could see security as a job I could transition into full time.”
Action: Build Security Community

Build a security [advocate, guild, champion] program

- Monthly Training
- Security Days
- Internal Capture the Flag
- Conferences
Who do you encounter the most?

- Unfamiliar
- Overworked
- Apathetic
- Gung Ho
Security behavior

- Light weight
- Well defined
- Easily repeatable
- Why and ROI
- Clear start and finish point

**Security Behavior**
- a manner of behaving that decreases danger, risk, or threat
What is a security behavior NOT?

Step 1 → Step 2 → Step 3
Security Habits

Reminder → Routine → Reward → Reminder
Learning
Experience

> codebashing.
Community
Manager: Plan Resources

To Do
Security
Security

Doing
Security

Done
Resource Security
Threat Modeling
Code Review
Red Teaming
Responses

Unfamiliar
Overworked
Apathetic
Gung Ho

Transforms

Knowledge
Automation / Education
Shock Value / Compliance
Community

Behaviors

Learning
Experience
Community
Plan Resources
Threat Modeling
Code Review
Red Teaming
Response
Apply What You Have Learned Today

■ Next week:
  - *Assess your organizational security culture*
  - *Survey developer 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. Application security is a stretch for the average developer
2. Everyone has an excuse; break on through
3. True security culture change comes through behavior and not process
Q+A and Thank you!

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