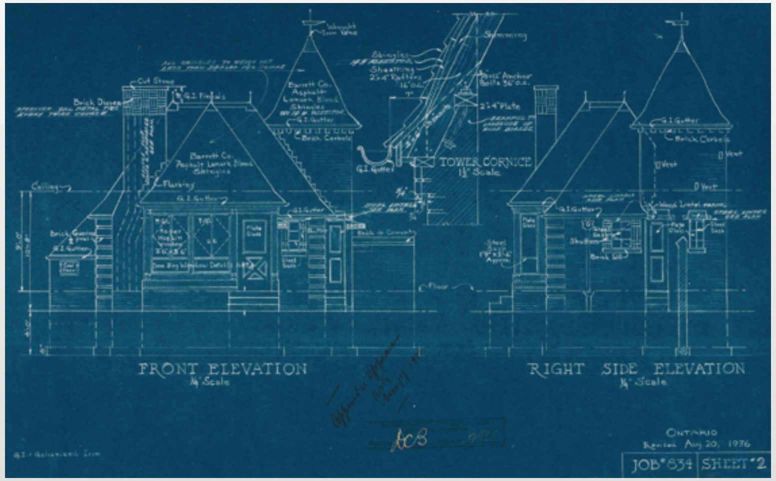


Security Journey

APPSEC AWARENESS: A BLUE PRINT FOR SECURITY CULTURE CHANGE

CHRISTOPHER ROMEO
CEO / PRINCIPAL CONSULTANT
SECURITY JOURNEY
@EDGEROUTE

About Chris Romeo

- CEO / Principal Consultant @ Security Journey
- 20 years security experience, CISSP, CSSLP
- 10 years at Cisco, leading the Cisco Security Ninja program & CSDL
- Speaker at RSA, AppSec USA, AppSec EU, & ISC2 Security Congress

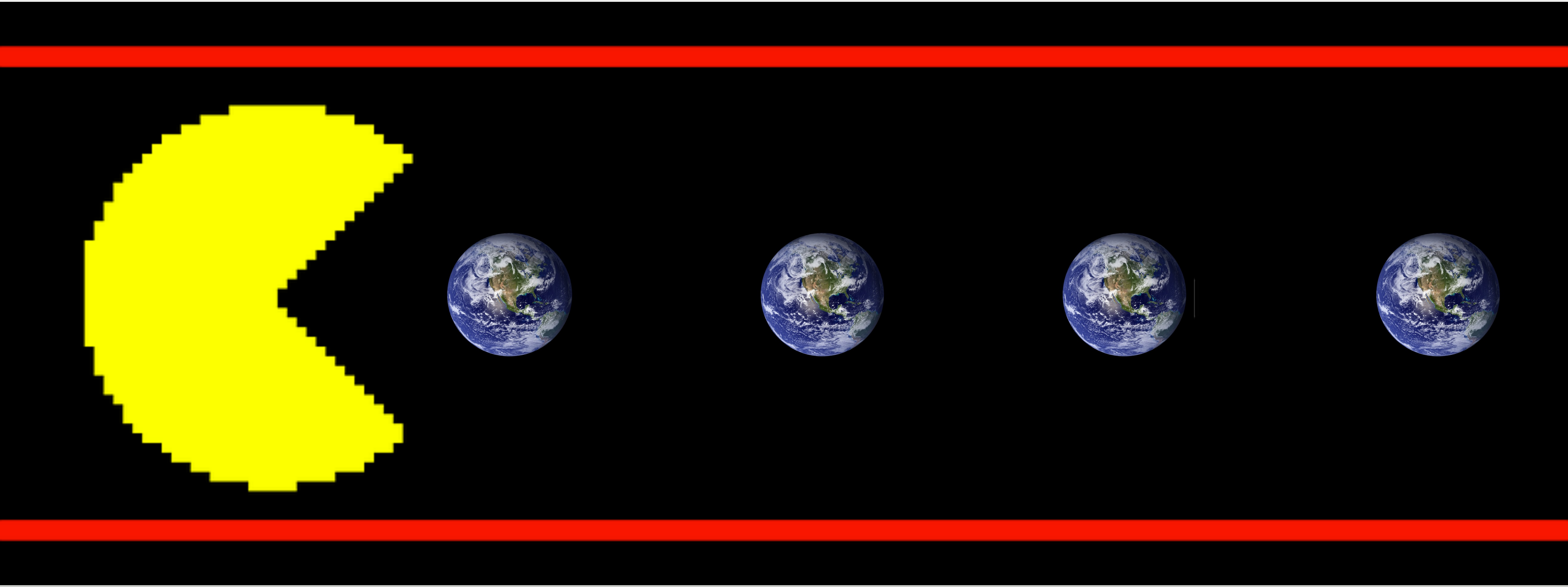
Security Journey

Agenda

- The Problem Space or why do we need an application security awareness?
- Creating sustainable security culture
- Application Security Awareness
  - *Designing your own program*

Security Journey

Software is eating the world



Security Journey

Customers demand security in everything

Security vulnerabilities and bug counts continue to rise

00fc 1819 0019 0098 d9d8
0057 7b7a 007a bab9 00b9 3a3c
8888 8888 8888 288e be88
88 8888 8888 7667 778e
d61f 7abd 8818 8888 467c 585f 8814
8b06 e8f7 88aa 8388 8b3b 88f3 88bd e988
3a18 880c e841 c988 b328 6871 688e 958b
5862 5884 7e81 3788 1ab4 5a84
3d86 dcb8 5cbb 8888 8888 8888 8888
8888 8888 8888 8888 8888 8888 8888

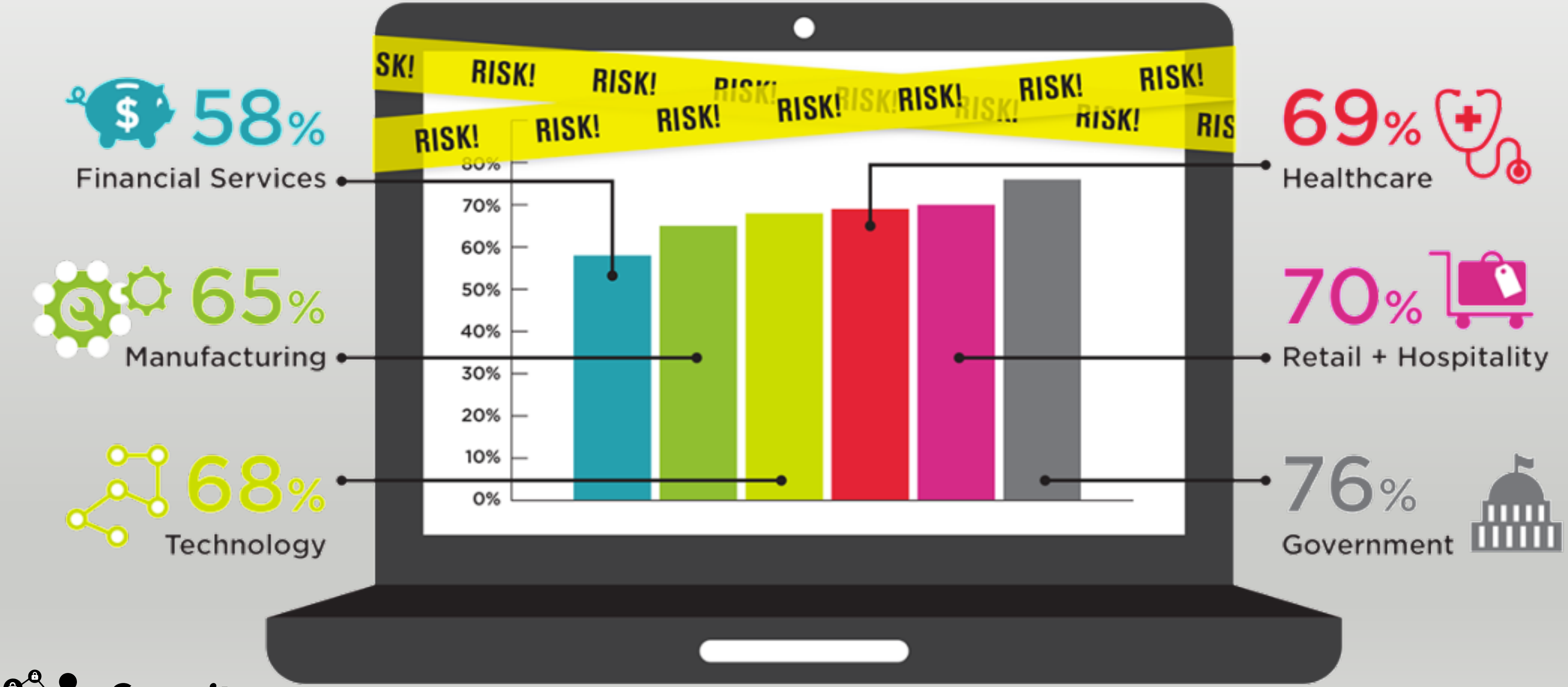
OWASP TOP 10

- *A1: Injection*
- *A2: Broken Authentication and Session Management*
- A3: Cross-Site Scripting (XSS)
- A4: Insecure Direct Object References
- *A5: Security Misconfiguration*
- *A6: Sensitive Data Exposure*
- A7: Missing Function Level Access Control
- A8: Cross Site Request Forgery (CSRF)
- *A9: Using Known Vulnerable Components*
- A10: Unvalidated Redirects and Forwards

https://owasp.org/index.php/TopTen

FAILED OWASP TOP 10

How many apps fail the OWASP Top 10
upon initial risk assessment?

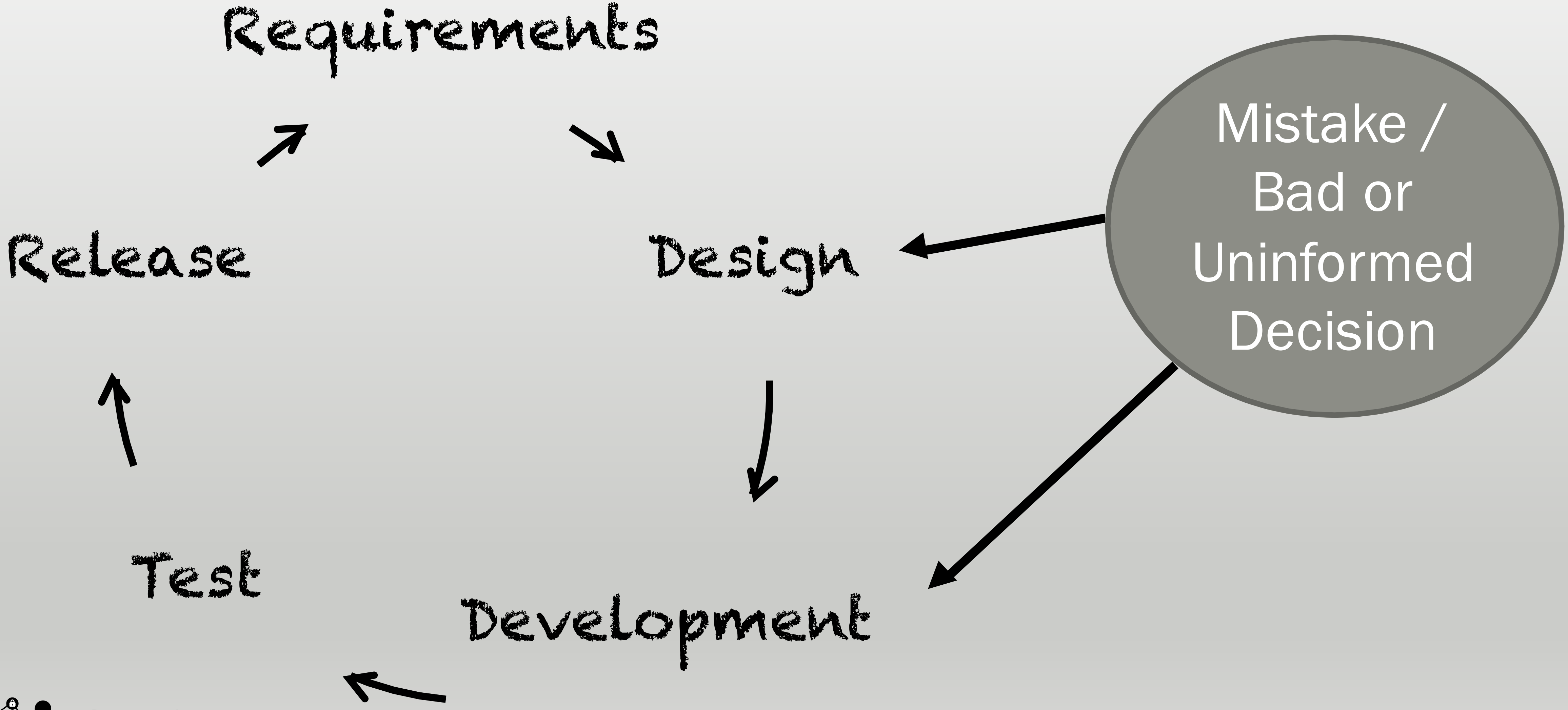


Security Journey

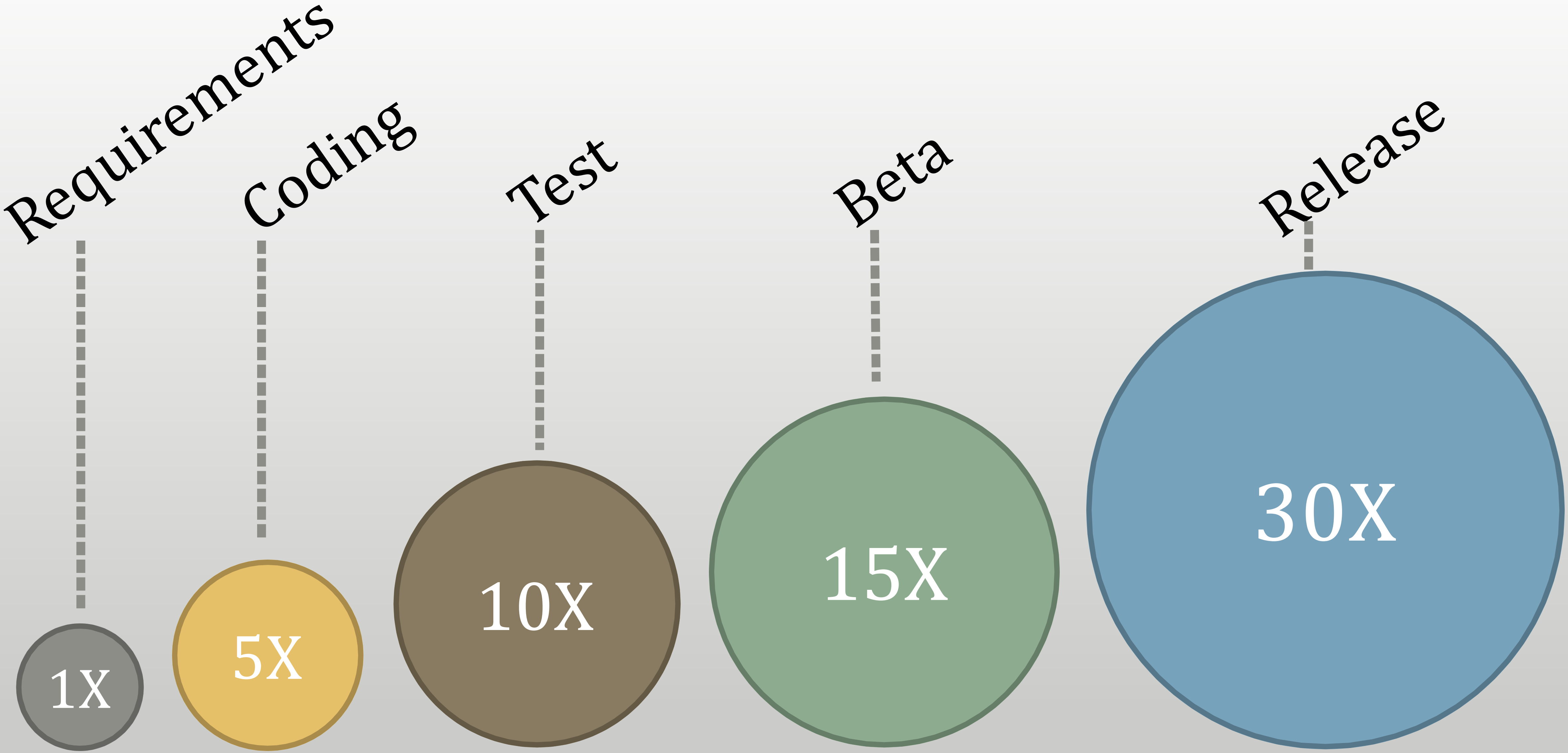
The data represents 208,670 application assessments submitted for analysis during the 18-month period from October 1, 2013 through March 31, 2015 by large and small companies, commercial software suppliers, open source projects and software outsourcers.

VERACODE

The Source of Vulnerabilities



Security Journey



Relative Cost to Fix

Security Journey

The Mindset of the "Average" Developer

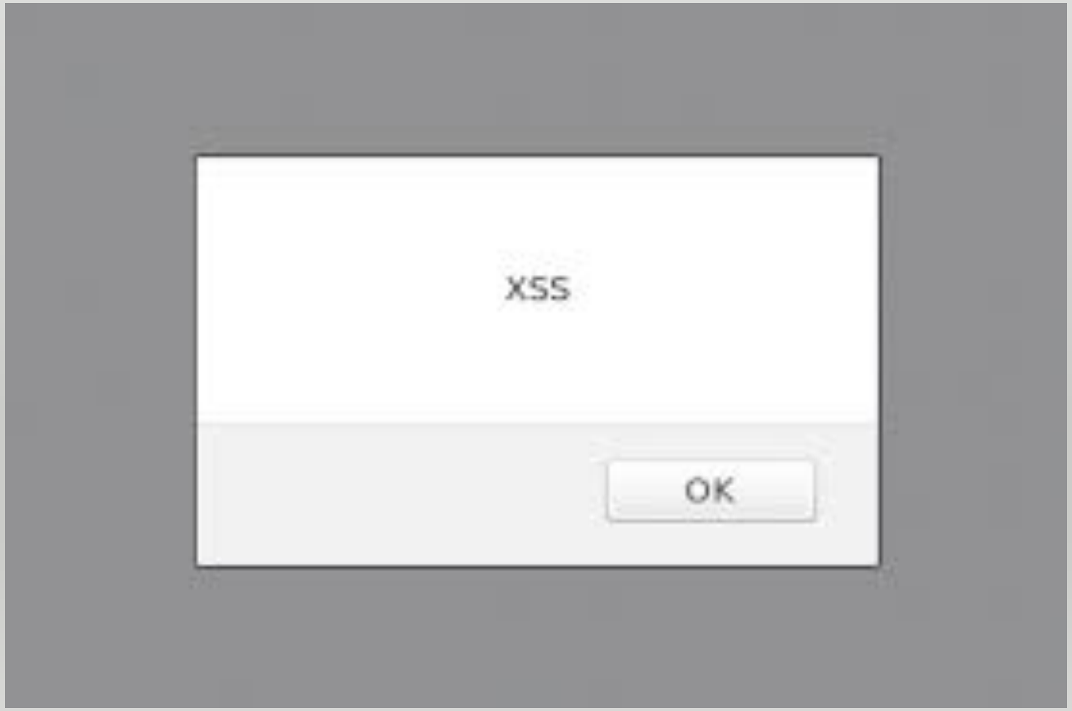
Security Journey

Security is a stretch for everyone.

Lack of understanding of the real problem.

Security is a stretch for everyone.

They do not understand the ramifications of inaction or the why.



Developers are not monsters.

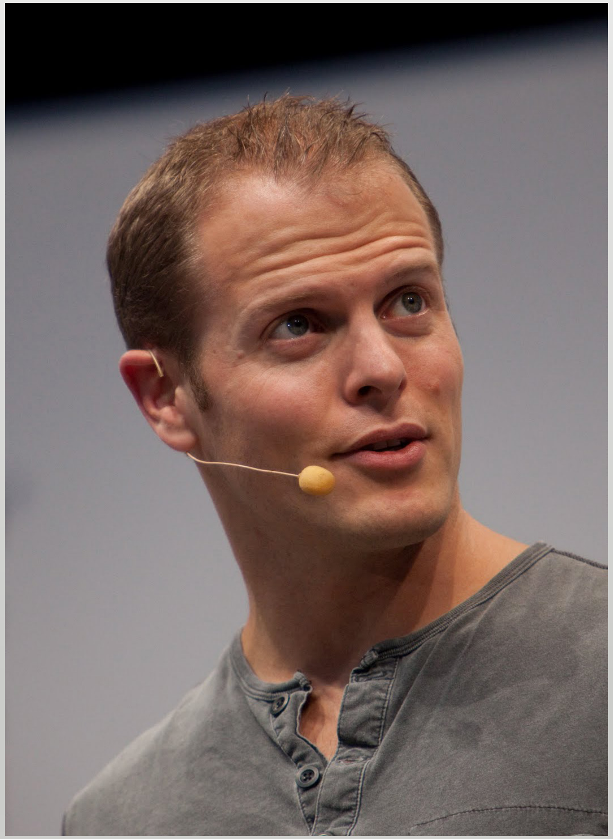
They want to do the right thing.

The Goal

Developers that think like security people.

RVASec

Security Culture



"What happens {**with security**} when people are left to their own devices."

--Tim Ferriss

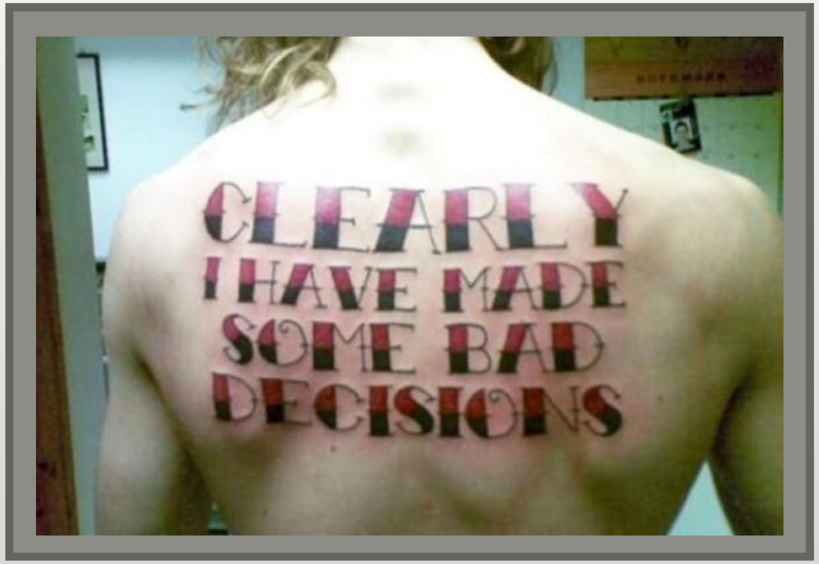
Security Journey

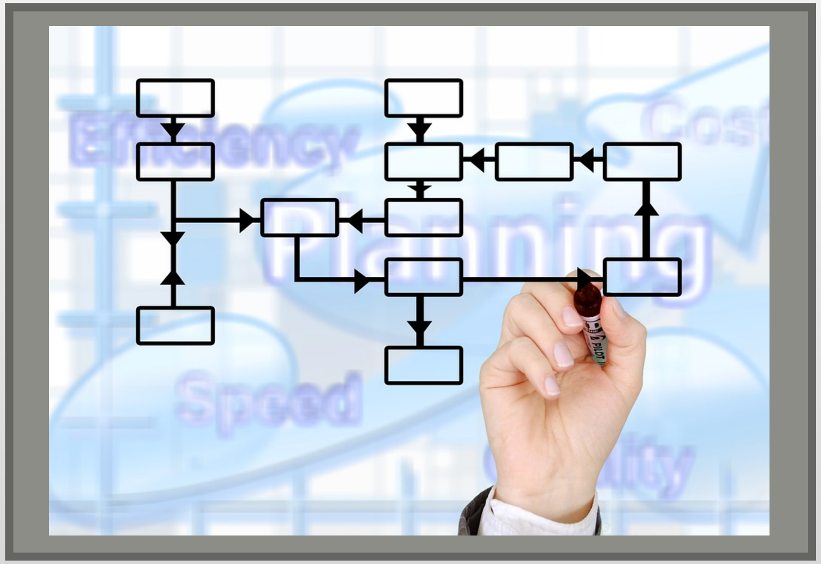
Application security is about the people.

Security Journey

The people introduce the vulnerabilities.

Why change a security culture?





Security Journey

Defining Features of a Sustainable Security Culture

Deliberate and disruptive

Engaging and fun

Rewarding

Return on investment

Security Journey

How do we change a security culture?

Open their eyes

Awareness

Fill their brains

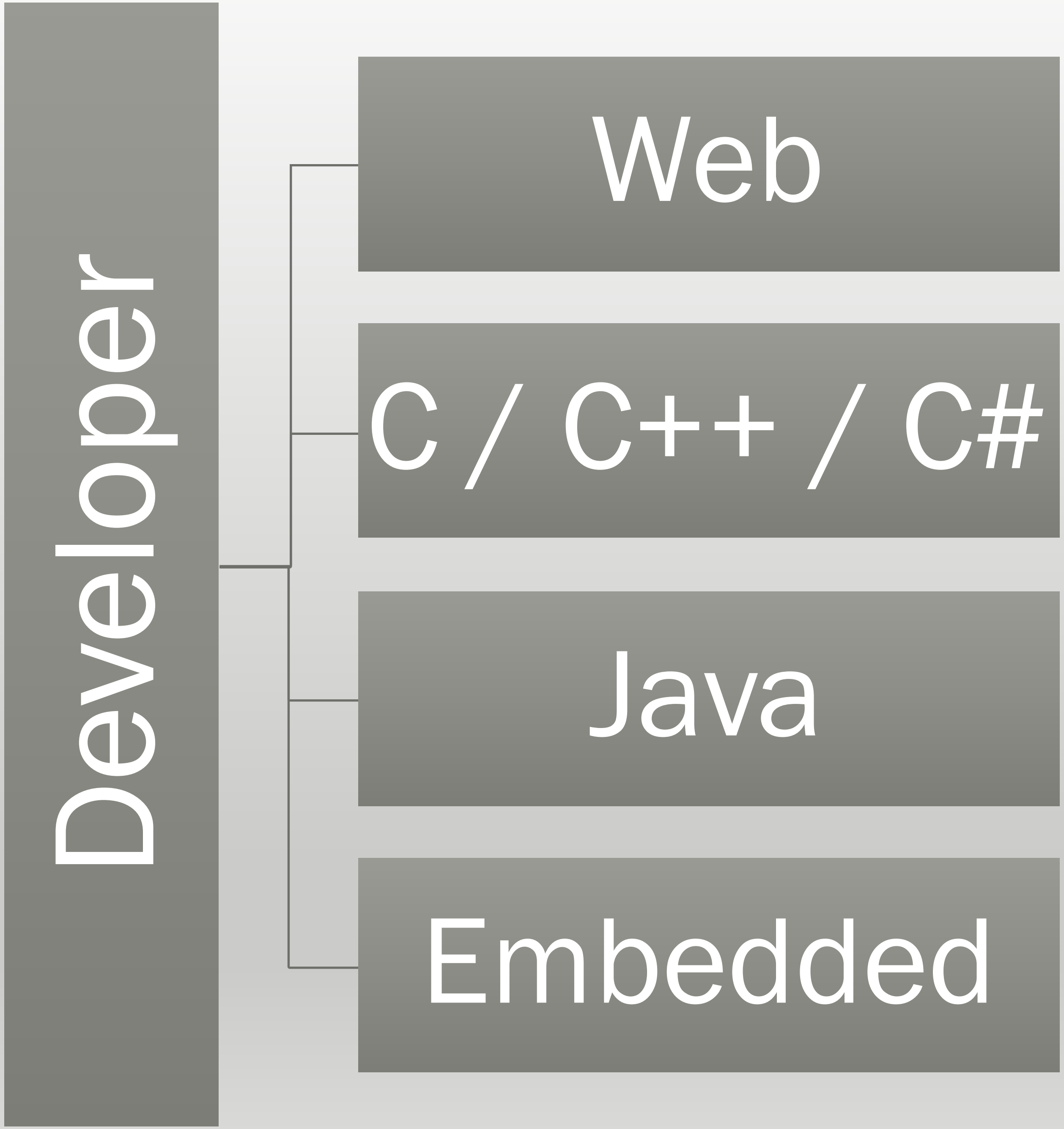
Knowledge

Fill their brains

History

Fill their brains

Role Specific



Task their hands

Activity

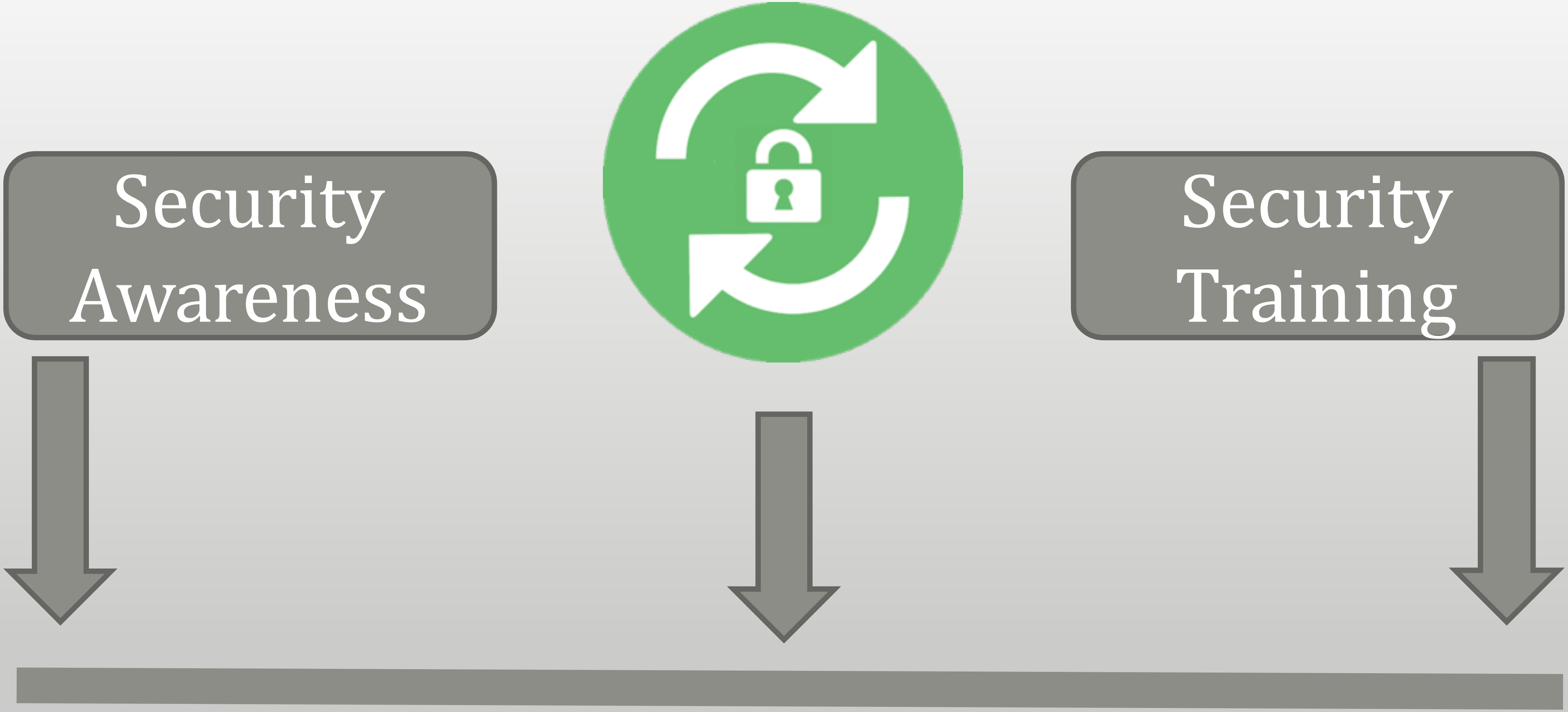
Embrace the gathering

Community

Solution?

Security Journey

Security Journey



Security Awareness

Security Training

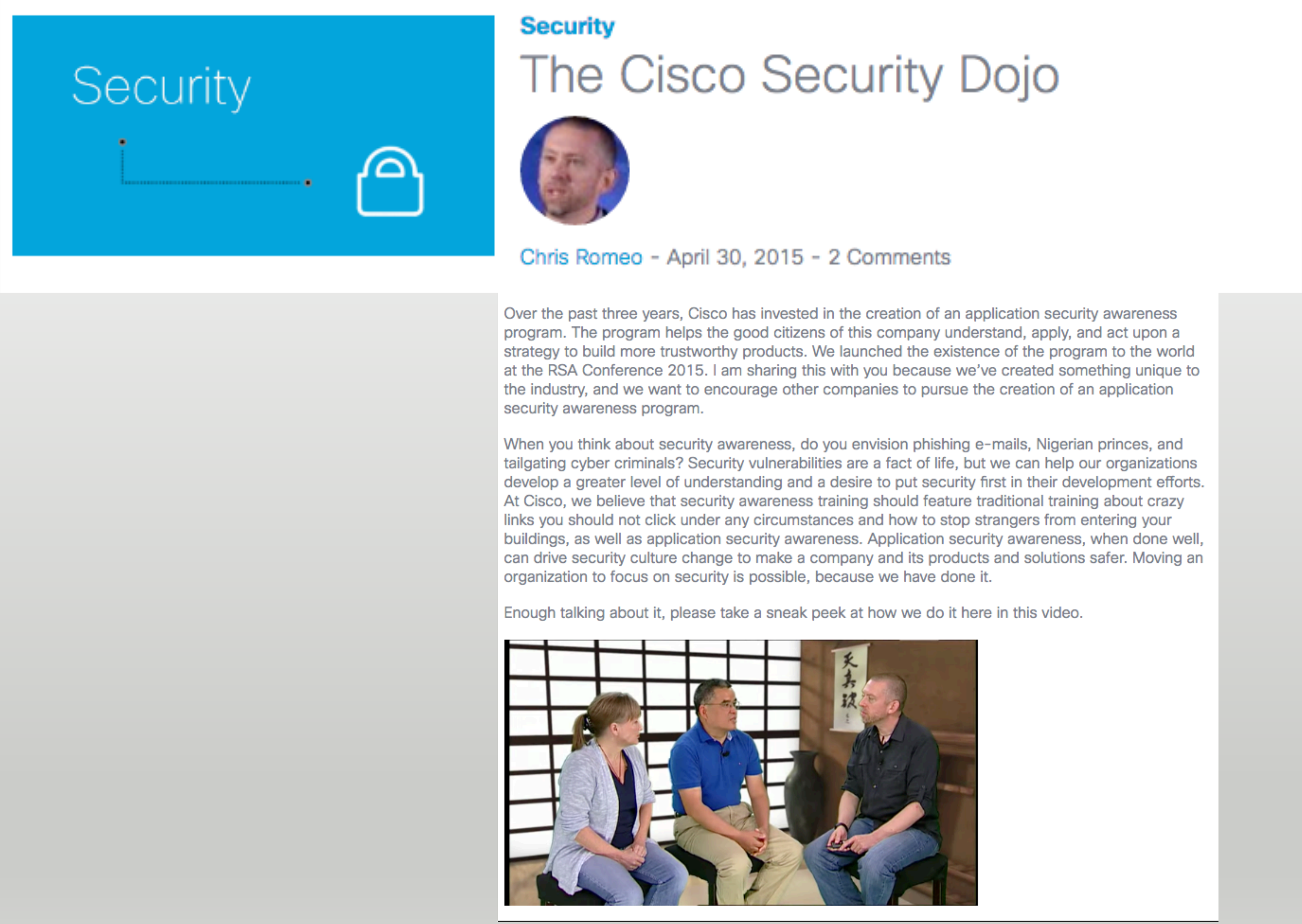
The Security Learning Spectrum

Security Journey

Benefits of an application security awareness program

1. Everyone gains a foundational knowledge of #appsec and with minimal investment
2. Dev's learn the detailed lessons of #appsec and avoid repeating history
3. Provides a defined mission through security activity
4. Central connection point for your new crop of security conscious

Security Journey



Security

The Cisco Security Dojo

Chris Romeo - April 30, 2015 - 2 Comments

Over the past three years, Cisco has invested in the creation of an application security awareness program. The program helps the good citizens of this company understand, apply, and act upon a strategy to build more trustworthy products. We launched the existence of the program to the world at the RSA Conference 2015. I am sharing this with you because we've created something unique to the industry, and we want to encourage other companies to pursue the creation of an application security awareness program.

When you think about security awareness, do you envision phishing e-mails, Nigerian princes, and tailgating cyber criminals? Security vulnerabilities are a fact of life, but we can help our organizations develop a greater level of understanding and a desire to put security first in their development efforts. At Cisco, we believe that security awareness training should feature traditional training about crazy links you should not click under any circumstances and how to stop strangers from entering your buildings, as well as application security awareness. Application security awareness, when done well, can drive security culture change to make a company and its products and solutions safer. Moving an organization to focus on security is possible, because we have done it.

Enough talking about it, please take a sneak peek at how we do it here in this video.

Security Journey

https://blogs.cisco.com/security/the-cisco-security-dojo

Building an Application Security Awareness Program

1. Program Architecture

2. Content

3. Humor / Story

4. Gamification

Security Journey

Program Architecture

- Design your program and record decisions in a planning document
- Impact: Everyone involved in the project understands the vision and execution

Assess Security Culture

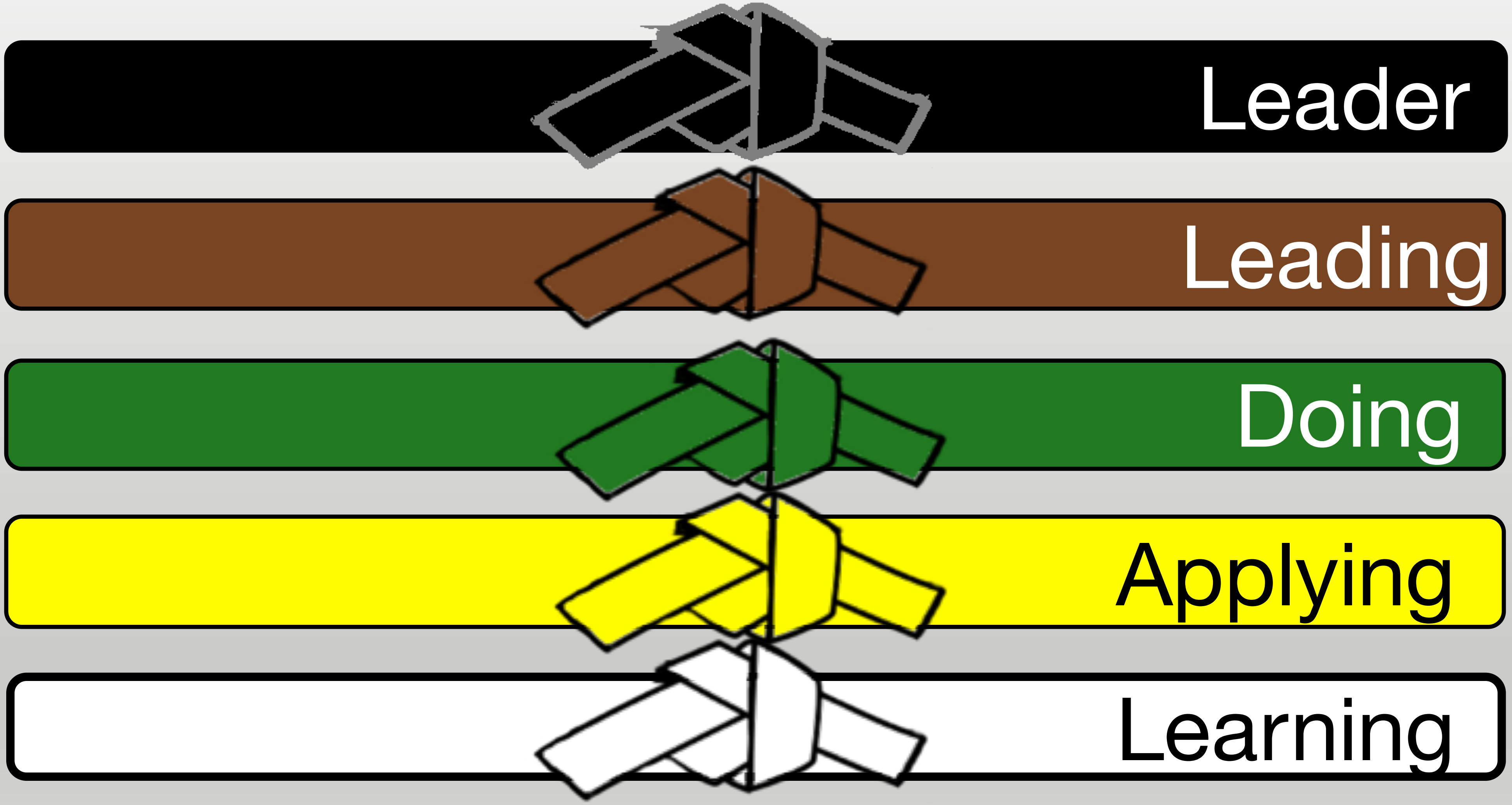
Define the problem

- Our organization lacks:
  - general application security knowledge
  - appreciation for the evolving threat landscape
  - experience with secure development practices and tools
  - motivation to improve security

Build a Team

Design Decision #1: Theme

Design Decision #2: Levels



Security Journey

Design Decision #3: Roles

Development

- SW Engineer
- Tester
- Manager
- HW Engineer

Operations

- IT
- DevOps

Internal

- Sales
- Marketing
- Executives

Everyone

Design Decision #4: Activities & Behaviors

Build

- A security tool or process
- Partnerships
- Security community

Enrich

- Mentor
- Teach a course
- Deliver presentations

Explore

- Security issue analysis
- Security committee
- A vulnerable web app

Implement

- A security feature
- A security test
- Security strategy

Recognition

100
100
FEDERAL RESERVE NOTE
KB 46279860 I
B2
UNITED STATES FEDERAL RESERVE SYSTEM
THE UNITED STATES OF AMERICA
100
KB 46279860 I
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES 2006 A
G2
G 205
Secretary of the Treasury.
100
100
FRANKLIN
ONE HUNDRED DOLLARS

Security Journey

Budget & Schedule

2016

2017, 18, 19?

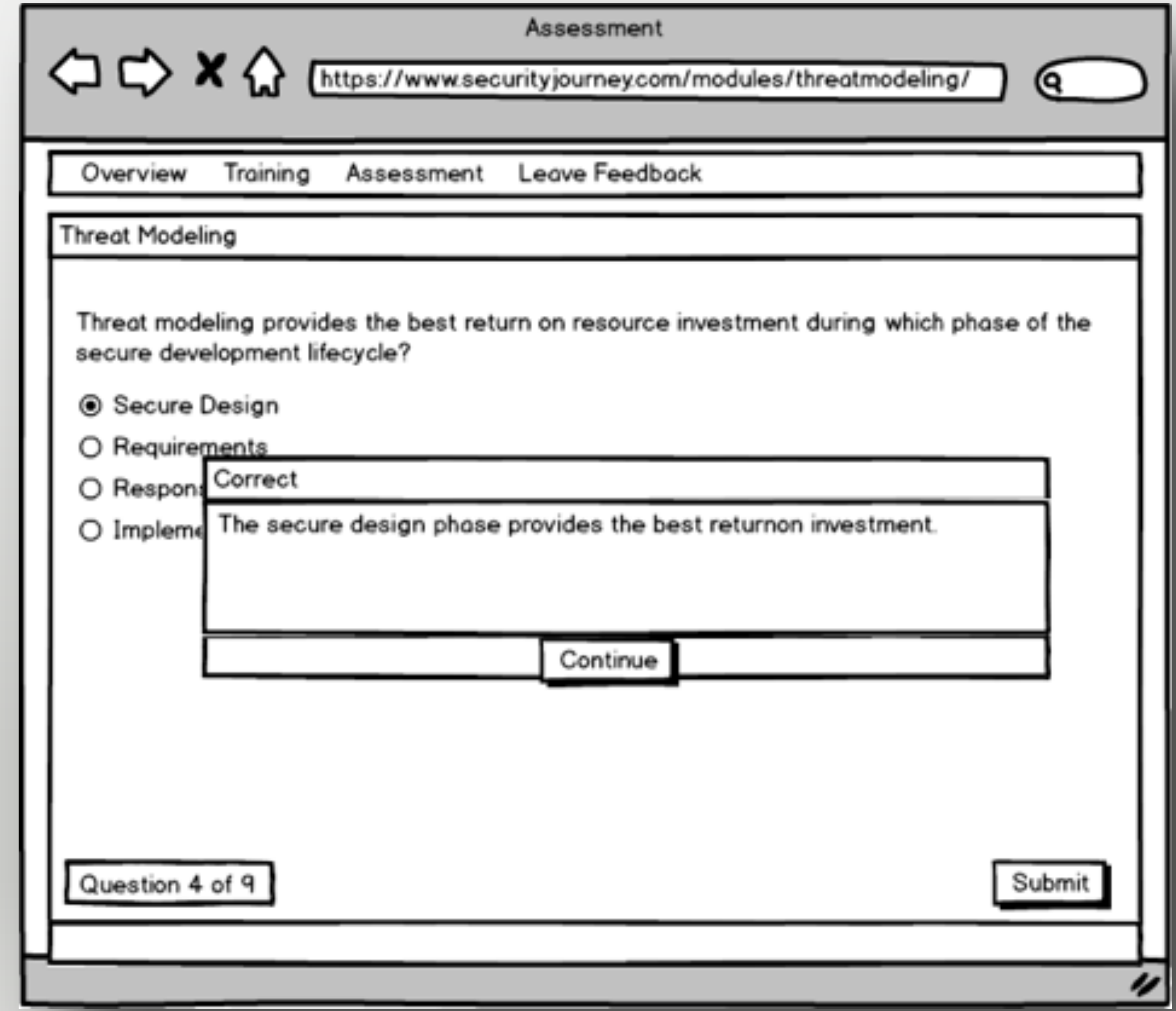
Content

- Foundational and role specific video modules, answering:
  - *"Why care about appsec?"*
  - *"How do we do #appsec?"*
- Impact: Video scales to the size of your organization

Content

Application Security Awareness
https://www.securityjourney.com/modules/ThreatModeling
Overview
Training
Assessment
Leave Feedback

Assessment



Threat Modeling

Threat modeling provides the best return on resource investment during which phase of the secure development lifecycle?

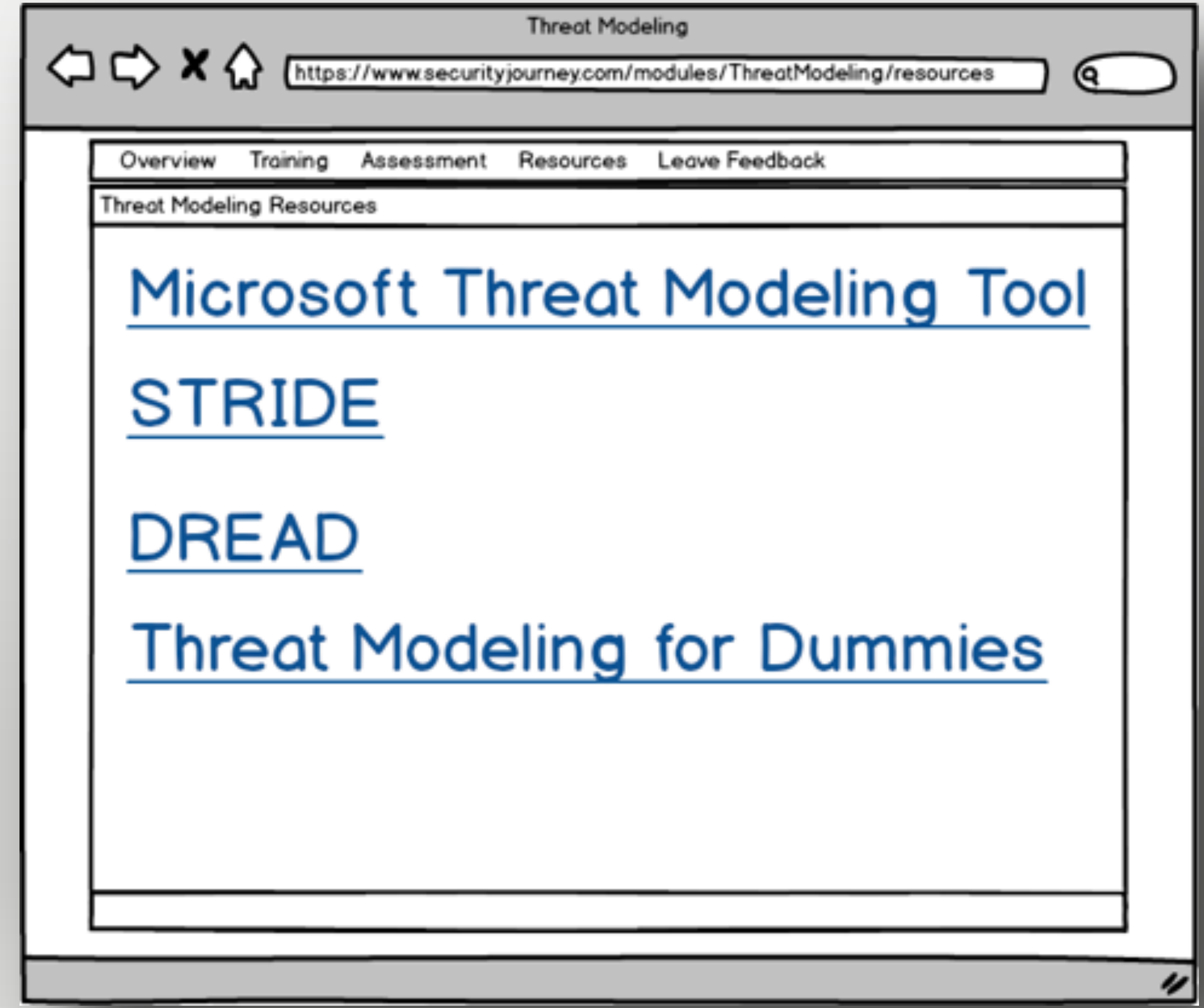
● Secure Design
○ Requirements
○ Respons
○ Impleme

Correct

The secure design phase provides the best returnon investment.

Security Journey

Resources



Threat Modeling
https://www.securityjourney.com/modules/ThreatModeling/resources
Overview
Training
Assessment
Resources
Leave Feedback

Threat Modeling Resources

Microsoft Threat Modeling Tool

STRIDE

DREAD

Threat Modeling for Dummies

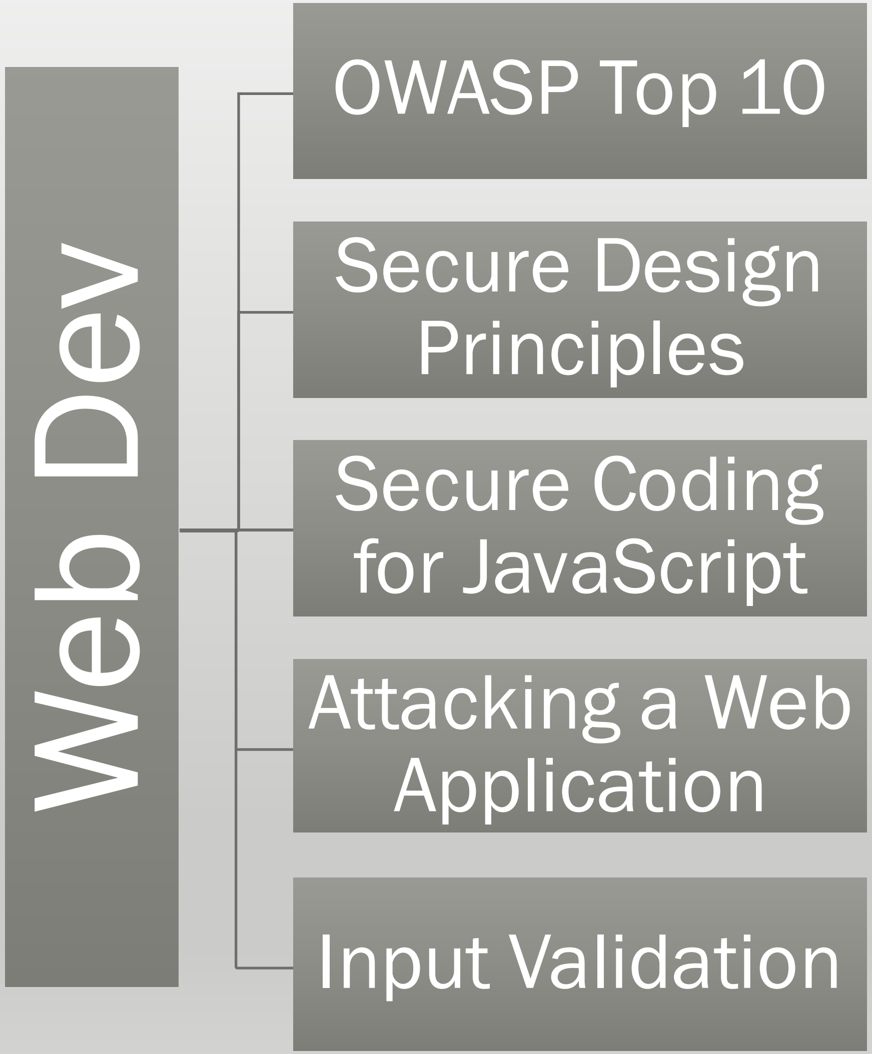
Security Journey

Level 1 Content Map

- Security Fundamentals
- Attacks & Attackers
- Simple SDL
- Security Myths
- Privacy & Customer Data Protection
- Security Business Case

Security Journey

Level 2 Content Map

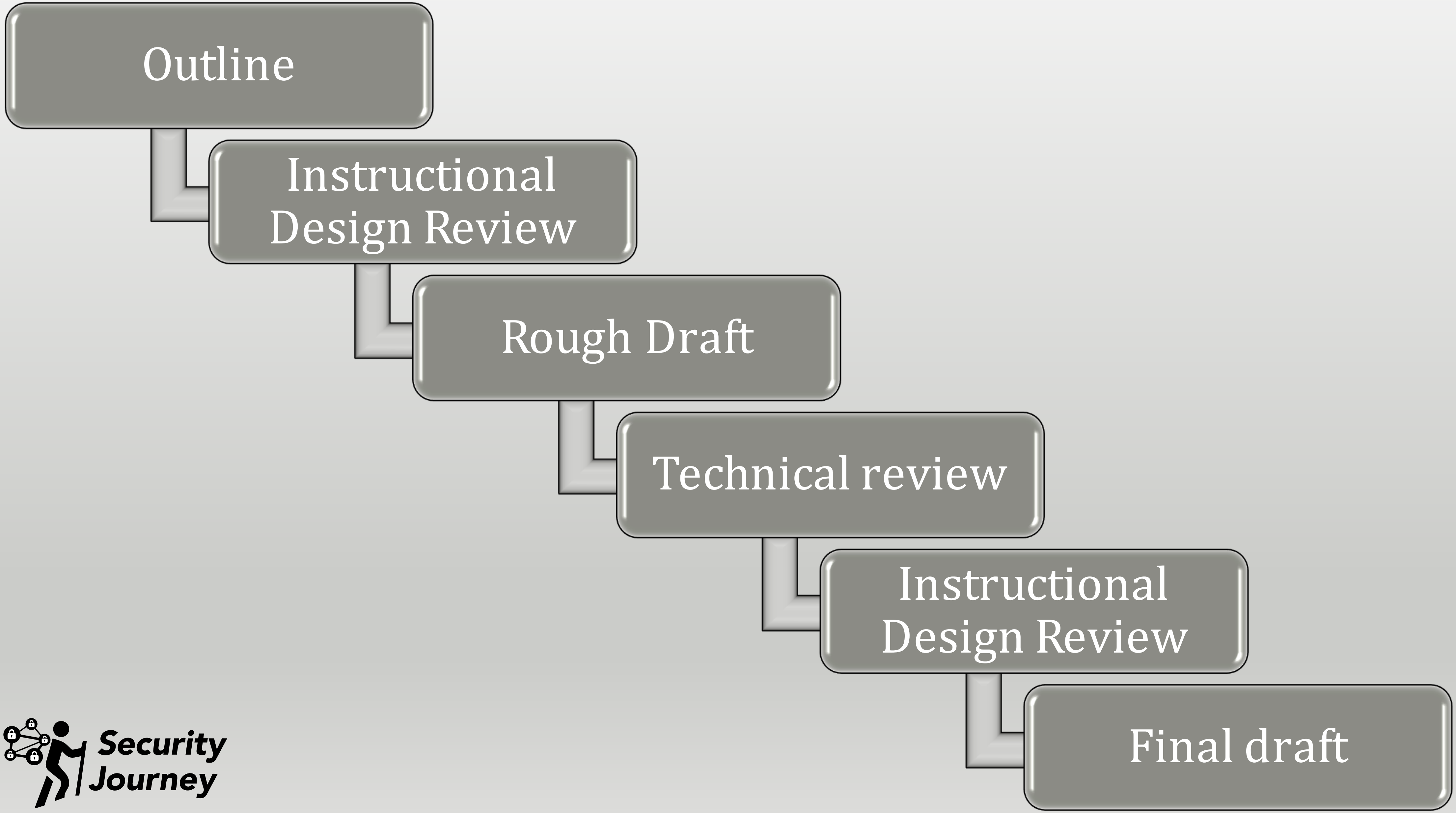


Web Dev

- OWASP Top 10
- Secure Design Principles
- Secure Coding for JavaScript
- Attacking a Web Application
- Input Validation

Security Journey

Content Creation Process


Outline

Instructional Design Review

Rough Draft

Technical review

Instructional Design Review

Final draft

Security Journey

Humor / Story

- Inject some humor into your security learning
- Use a story to illustrate security principles
- Impact: Content is not so serious and learners begin to have FUN

What is a security metaphor?

Should a Security Ninja be scared of the cloud?

Security Journey

Examples

- Still Cartoons
- Full motion cartoons
- Video

Security Journey

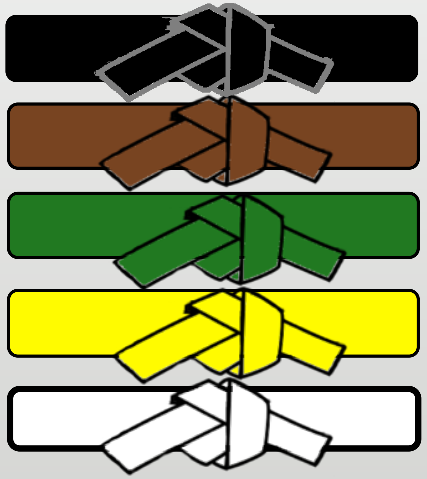
A word of caution…

Gamification

- Utilizing what makes games fun and apply it to #appsec
- Impact: An engaged learner is a learner that sticks around

Security Journey

Gamification



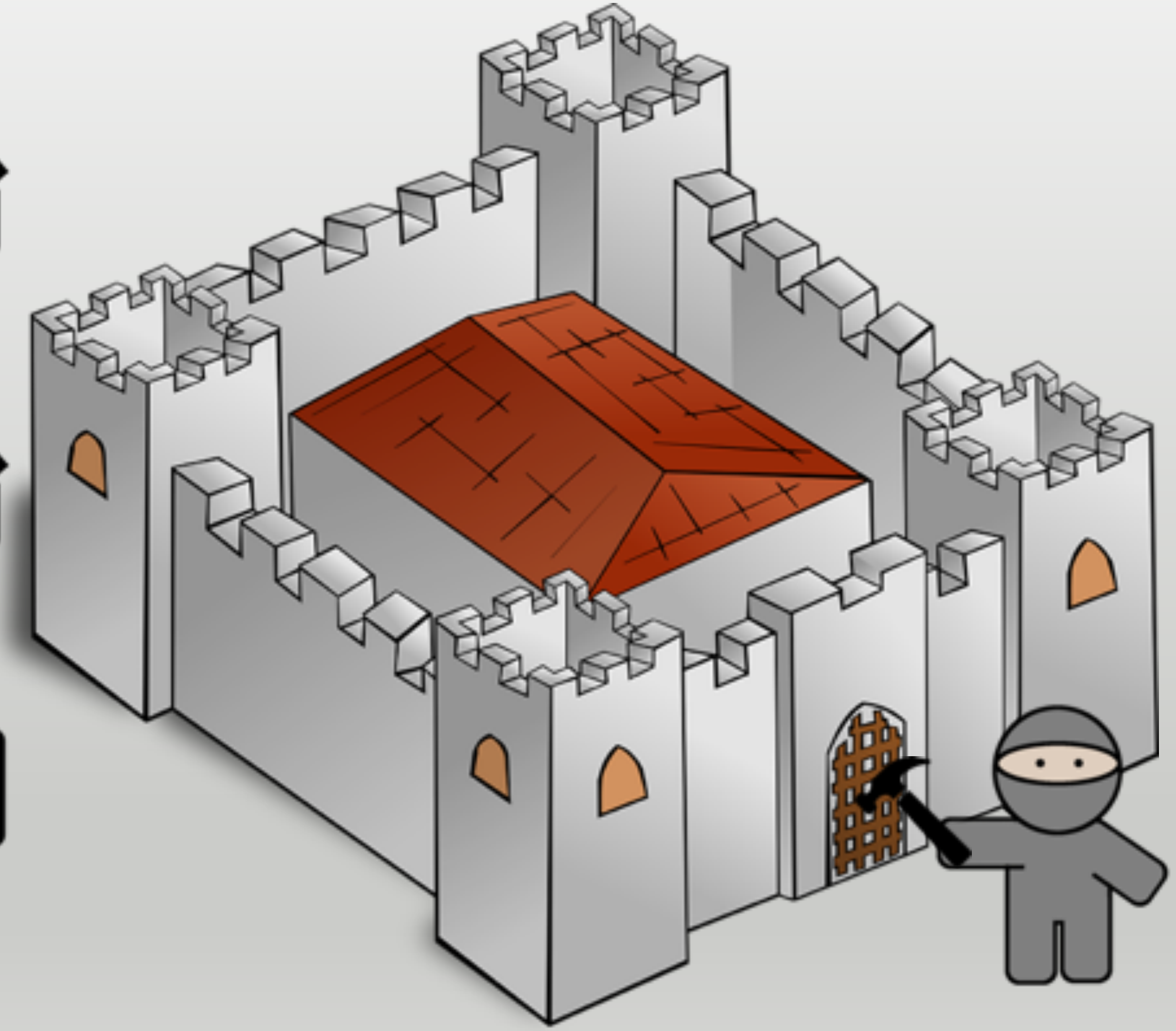
100
FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
KB 46279860 I
B2
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES 2006 A
Secretary of the Treasury.
FRANKLIN
ONE HUNDRED DOLLARS

User Interface

Security Fundamentals ☑

Attacks & Attackers ☑

Threat Landscape □



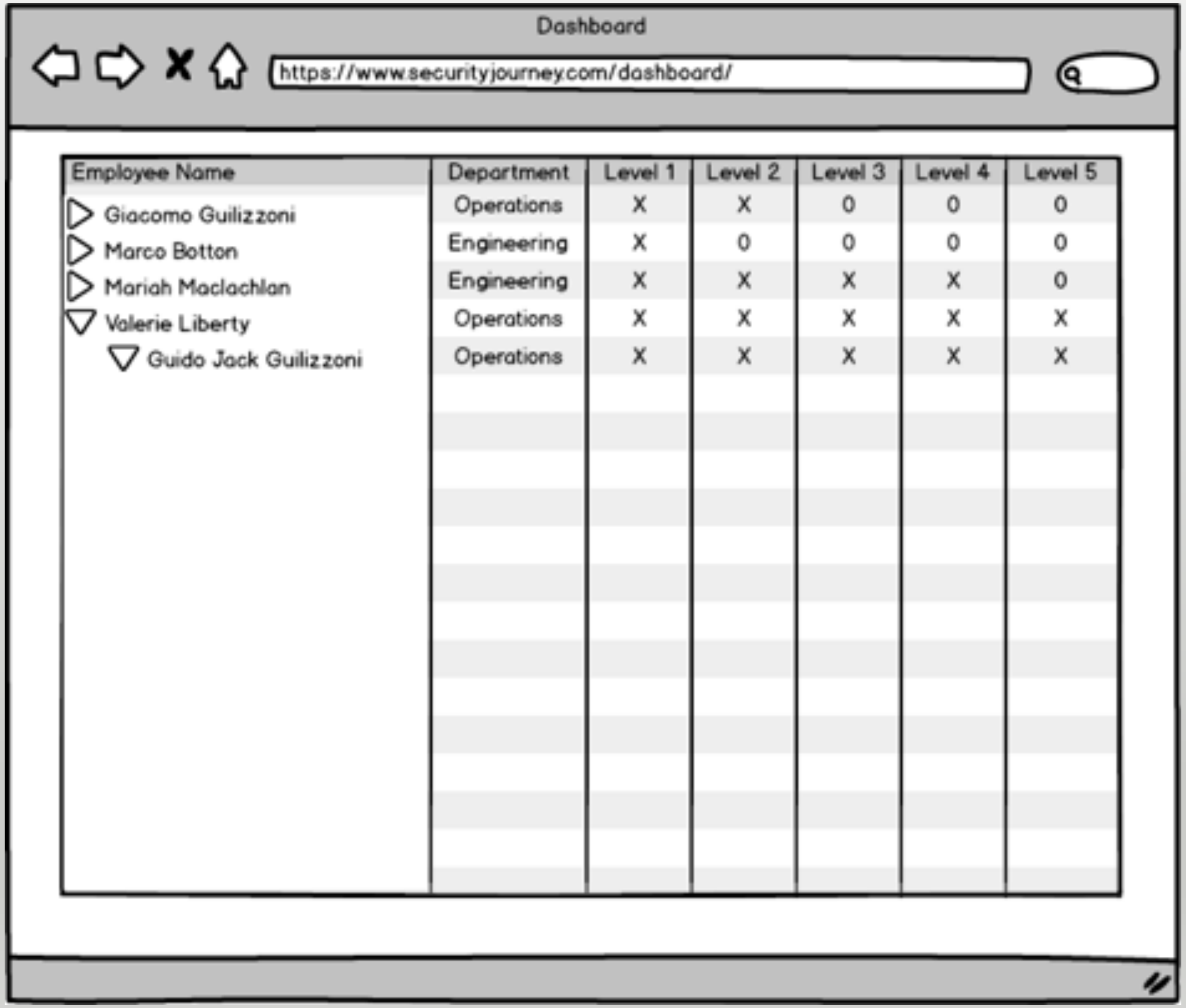
Security Myths □

Cryptography □

Privacy □

Security Journey

Competition



Dashboard

https://www.securityjourney.com/dashboard/

Employee Name	Department	Level 1	Level 2	Level 3	Level 4	Level 5
▷ Giacomo Guilizzoni	Operations	X	X	0	0	0
▷ Marco Botton	Engineering	X	0	0	0	0
▷ Mariah Maclachlan	Engineering	X	X	X	X	0
▽ Valerie Liberty	Operations	X	X	X	X	X
▽ Guido Jack Guilizzoni	Operations	X	X	X	X	X

Key Takeaways

- Vulnerabilities are real and everywhere
- Changing security culture
  - *Open their eyes (awareness)*
  - *Fill their brains (knowledge / history)*
  - *Task their hands (activity)*
- Building an application security awareness program
  - *Program Architecture*
  - *Content*
  - *Humor / Story*
  - *Gamification*

Security Journey

Build Your Own

Security Journey

Q+A & Contact

Chris Romeo, CEO / Principal Consultant

chris_romeo@securityjourney.com

www.securityjourney.com

@edgeroute

Security Journey