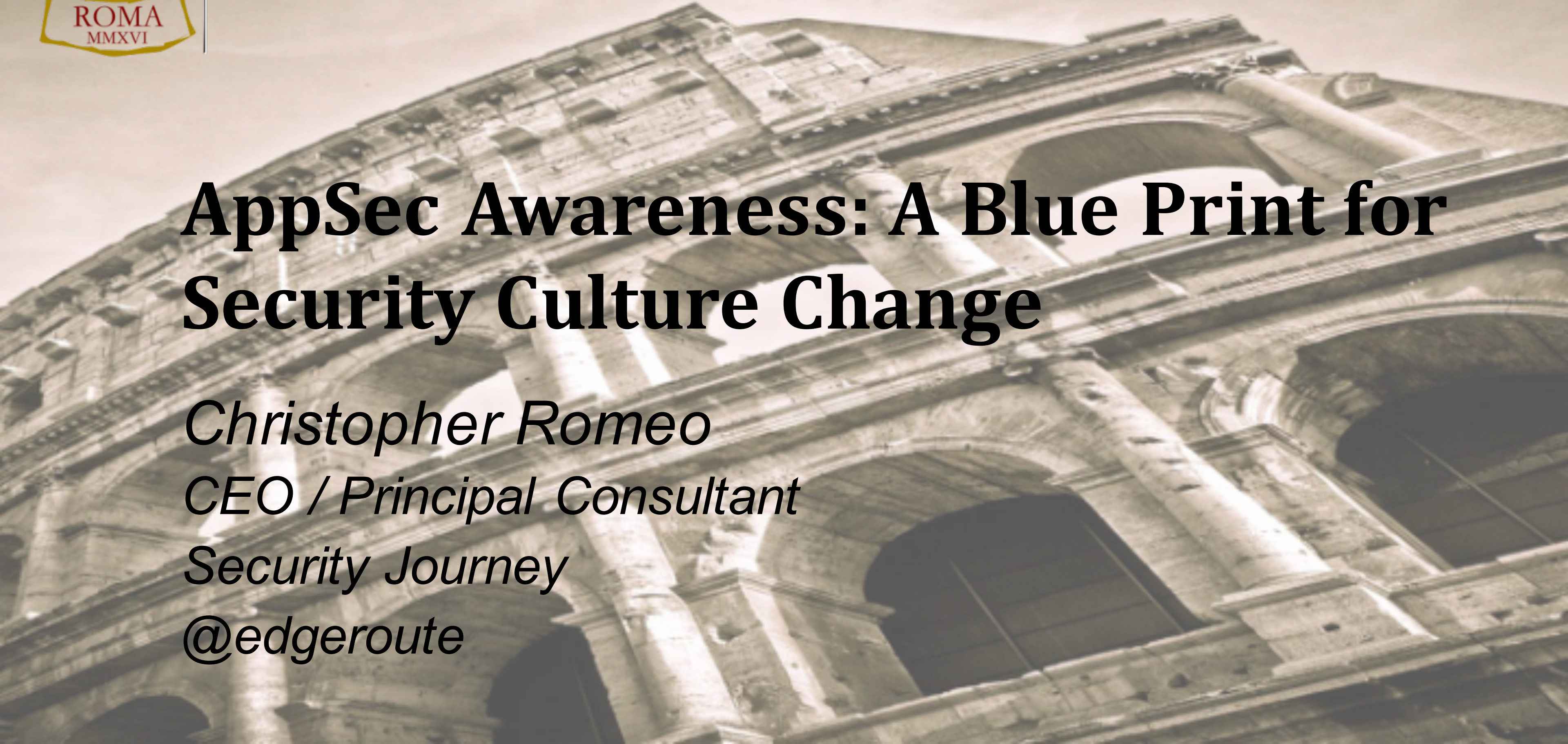
ROMA MMXVI | APPSEC EUROPE



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

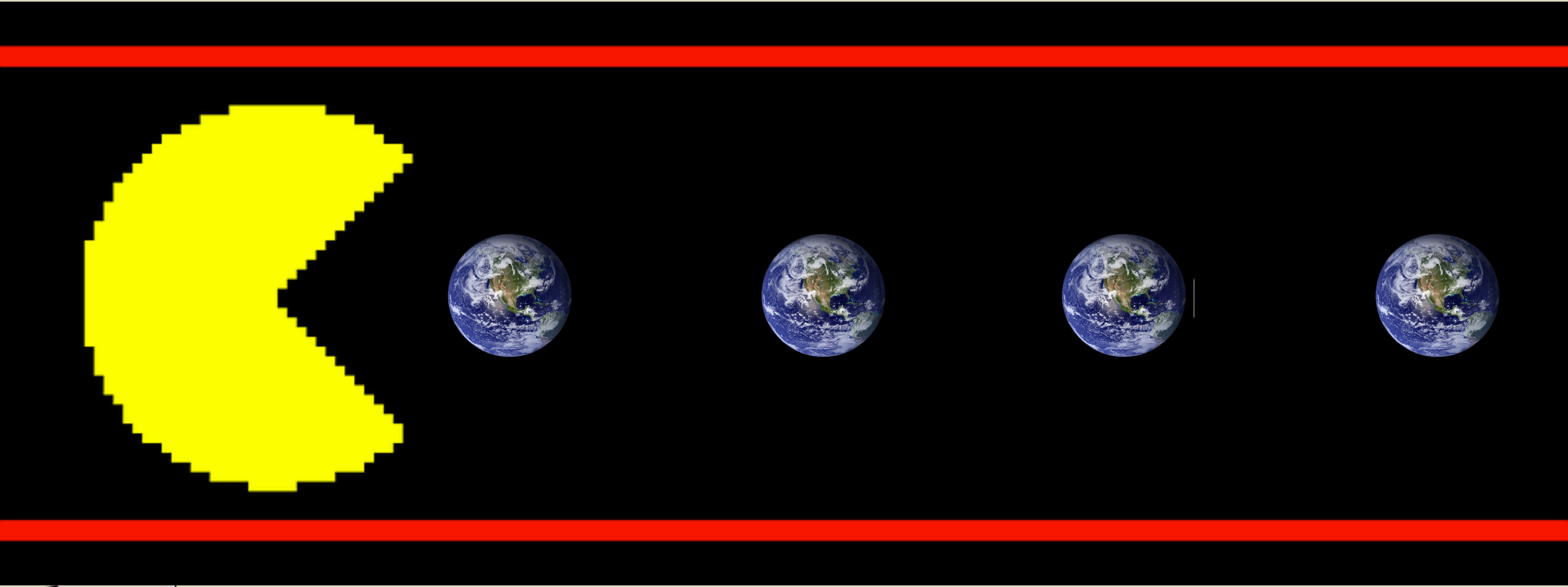
Security Journey

@edgeroute

Agenda

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

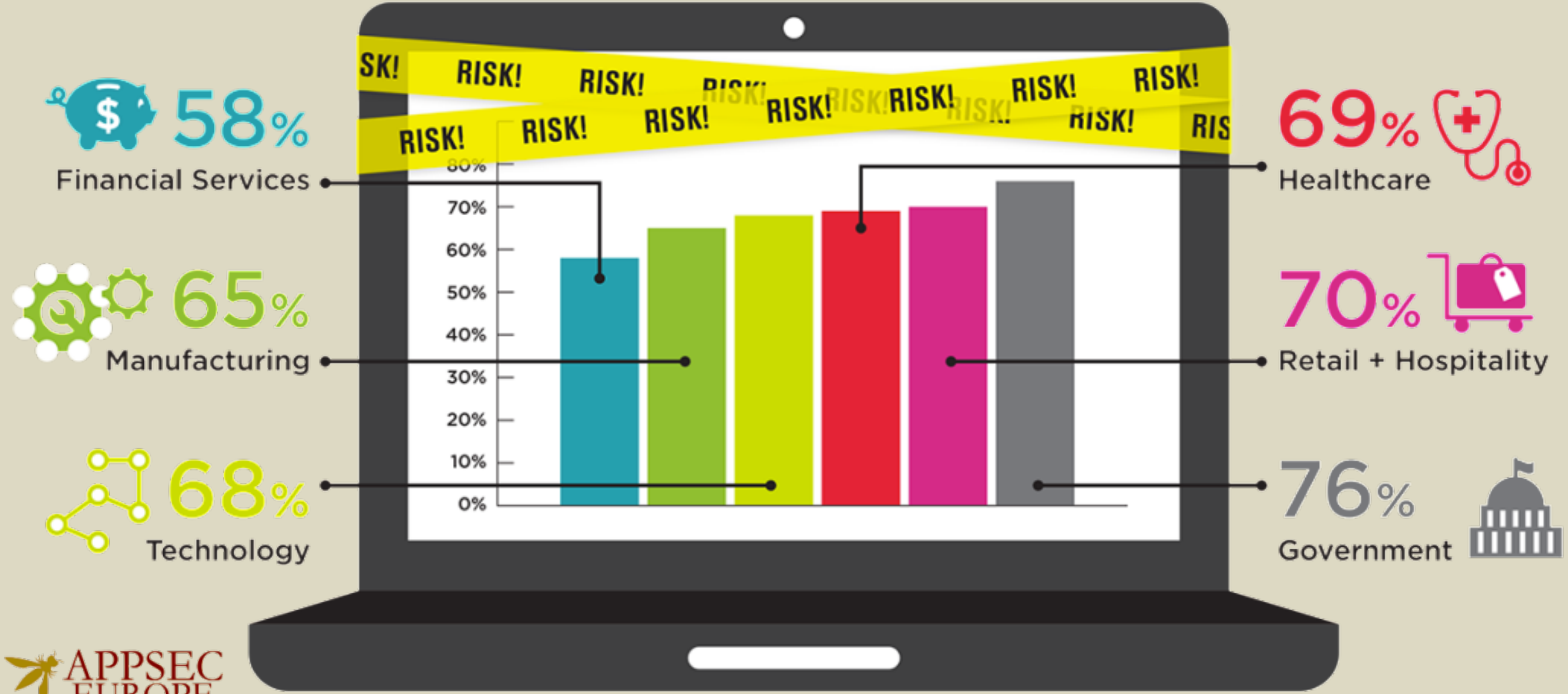
Software is eating the world



Customers demand security in everything

FAILED OWASP TOP 10

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

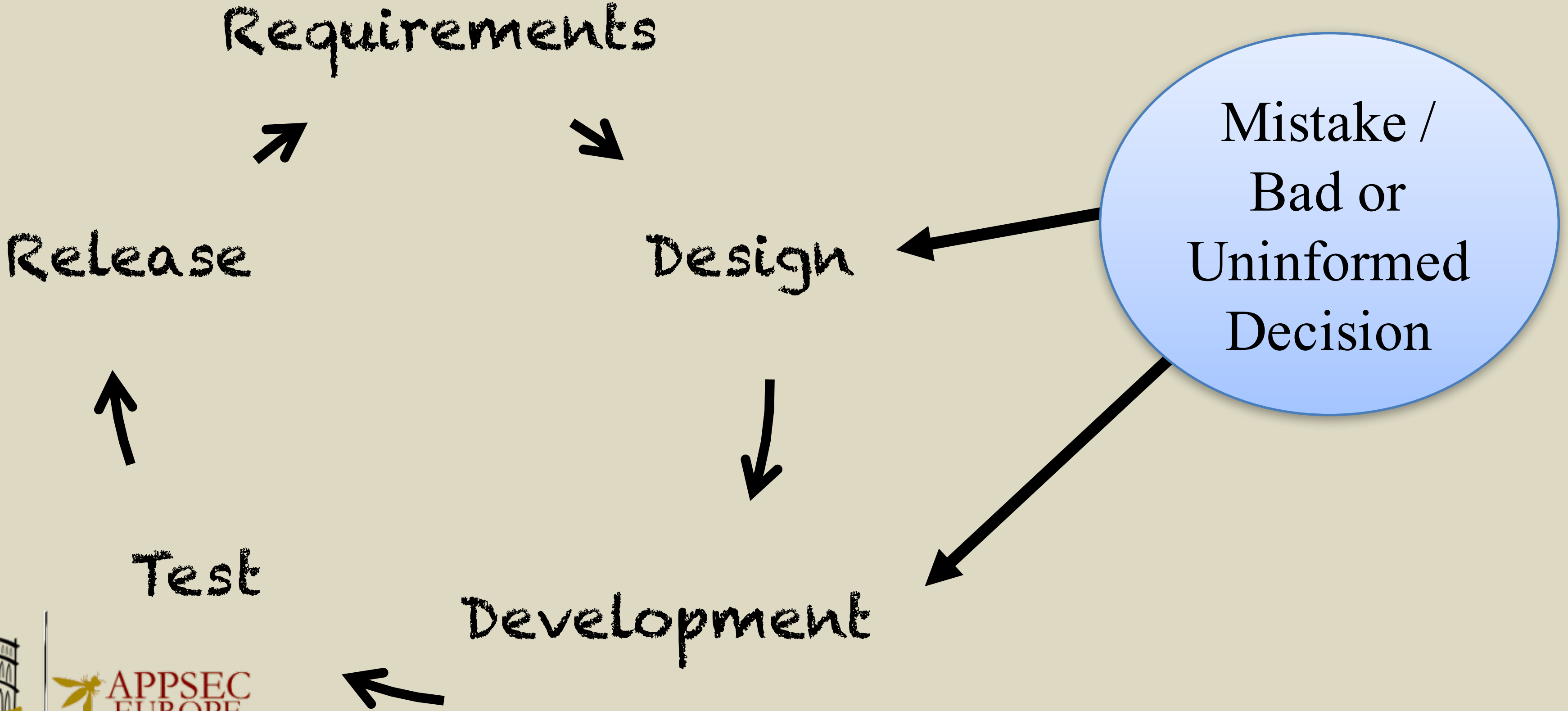


ROMA MMXVI | APPSEC EUROPE

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



Requirements

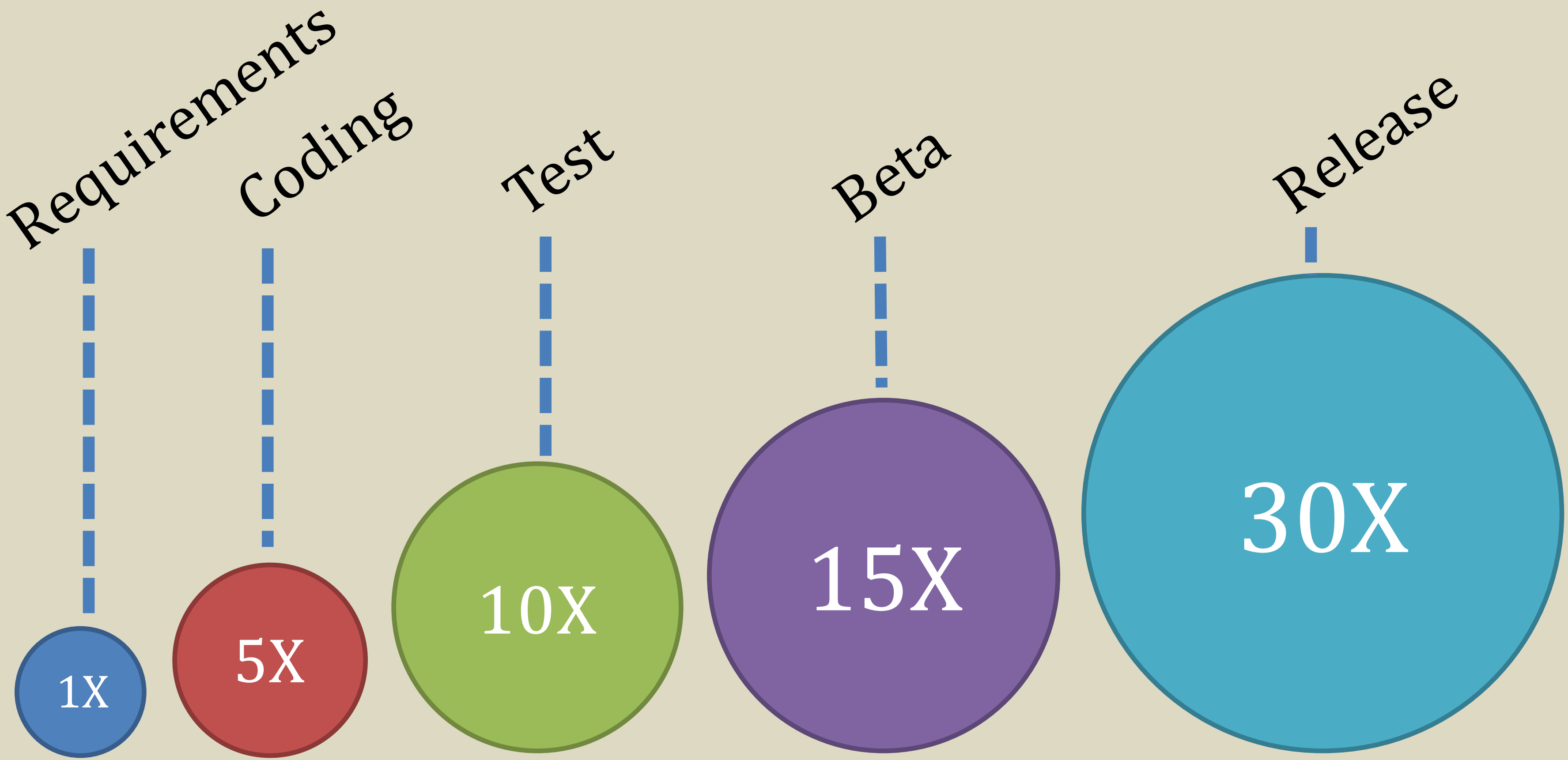
Design

Development

Test

Release

Mistake / Bad or Uninformed Decision



Requirements

Coding

Test

Beta

Release

1X

5X

10X

15X

30X

ROMA MMXVI

APPSEC EUROPE

Relative Cost to Fix

The Mindset of the "Average" Developer

The Goal

Developers that think like security people.

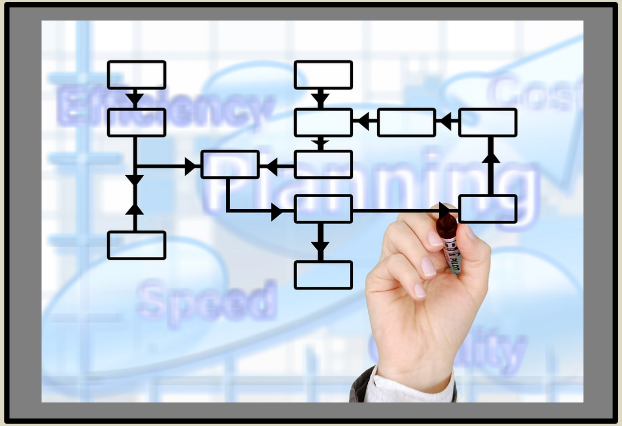
Security Culture

“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.

Why change a security culture?



Defining Features of a Sustainable Security Culture

Deliberate and disruptive

Engaging and fun

Rewarding

Return on investment

How do we change a security culture?

Open their eyes

Awareness

Fill their brains

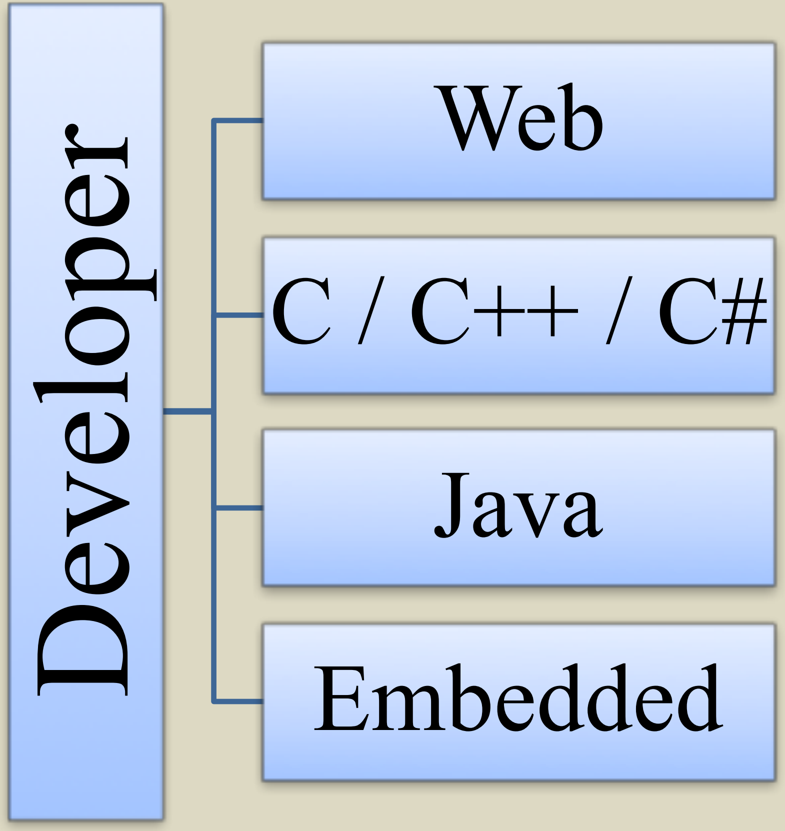
Knowledge

Fill their brains

History

Fill their brains

Role Specific



Developer

Web

C / C++ / C#

Java

Embedded

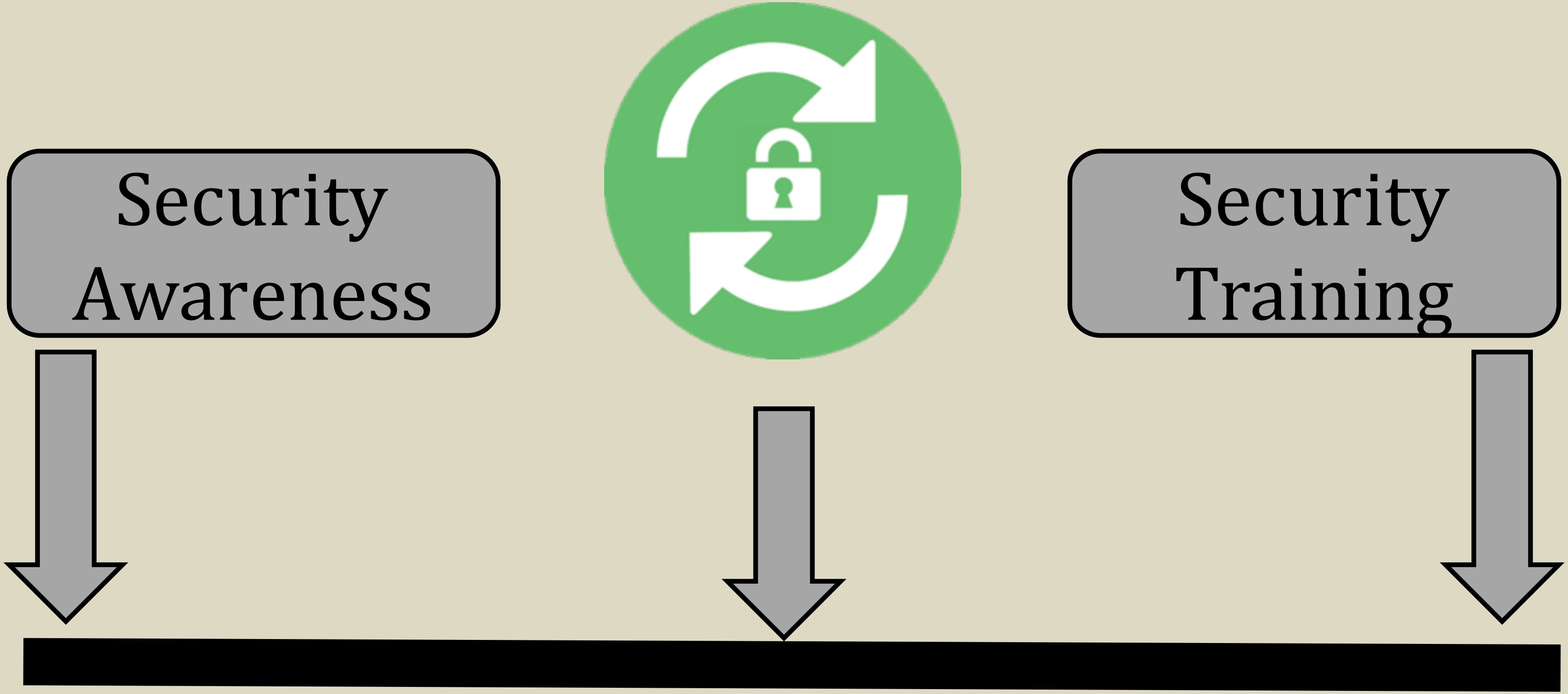
Task their hands

Activity

Embrace the gathering

Community

"Security Champions"



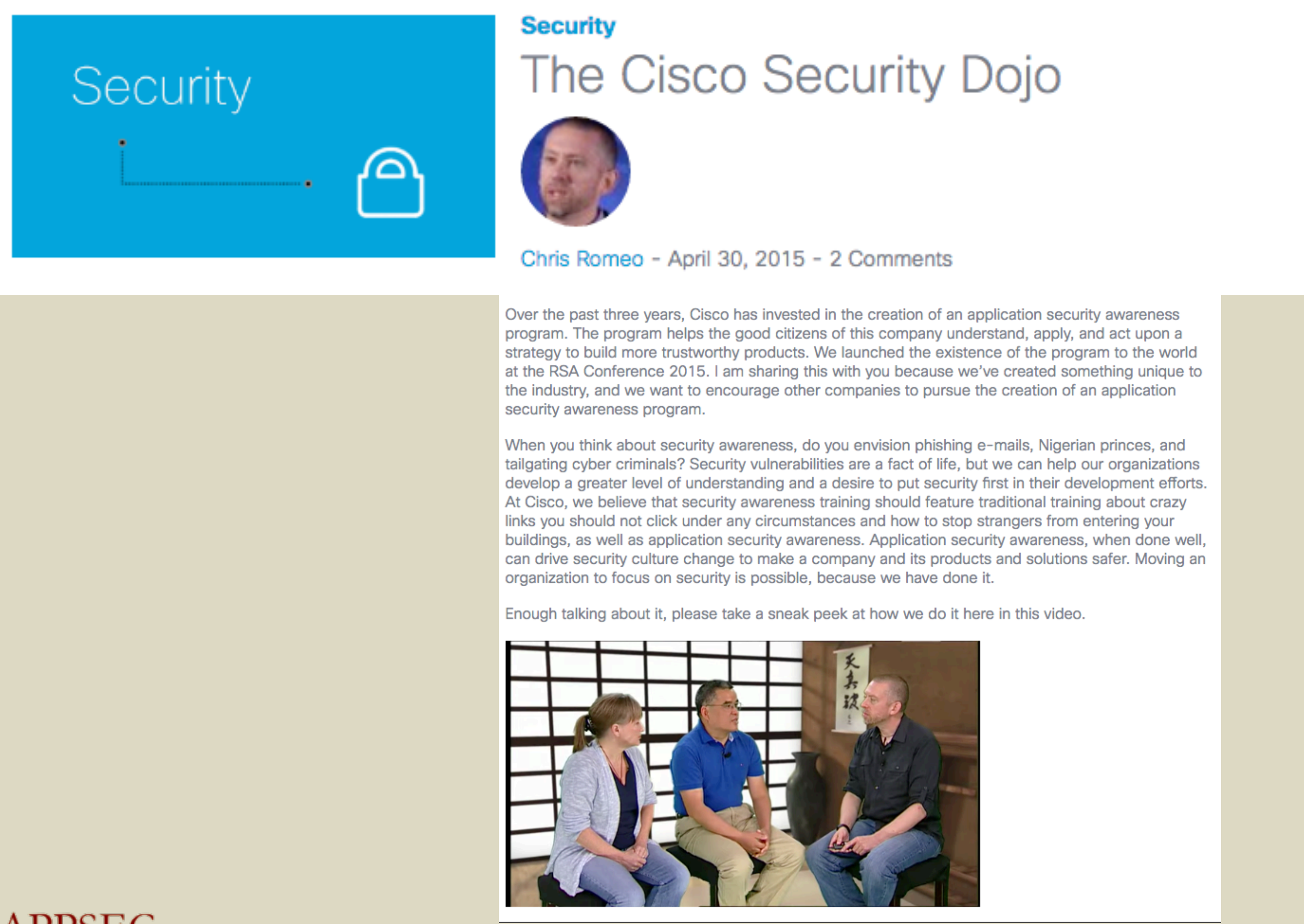
Security Awareness

Security Training

The Security Learning Spectrum

Benefits of an #appsec 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

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.

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

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

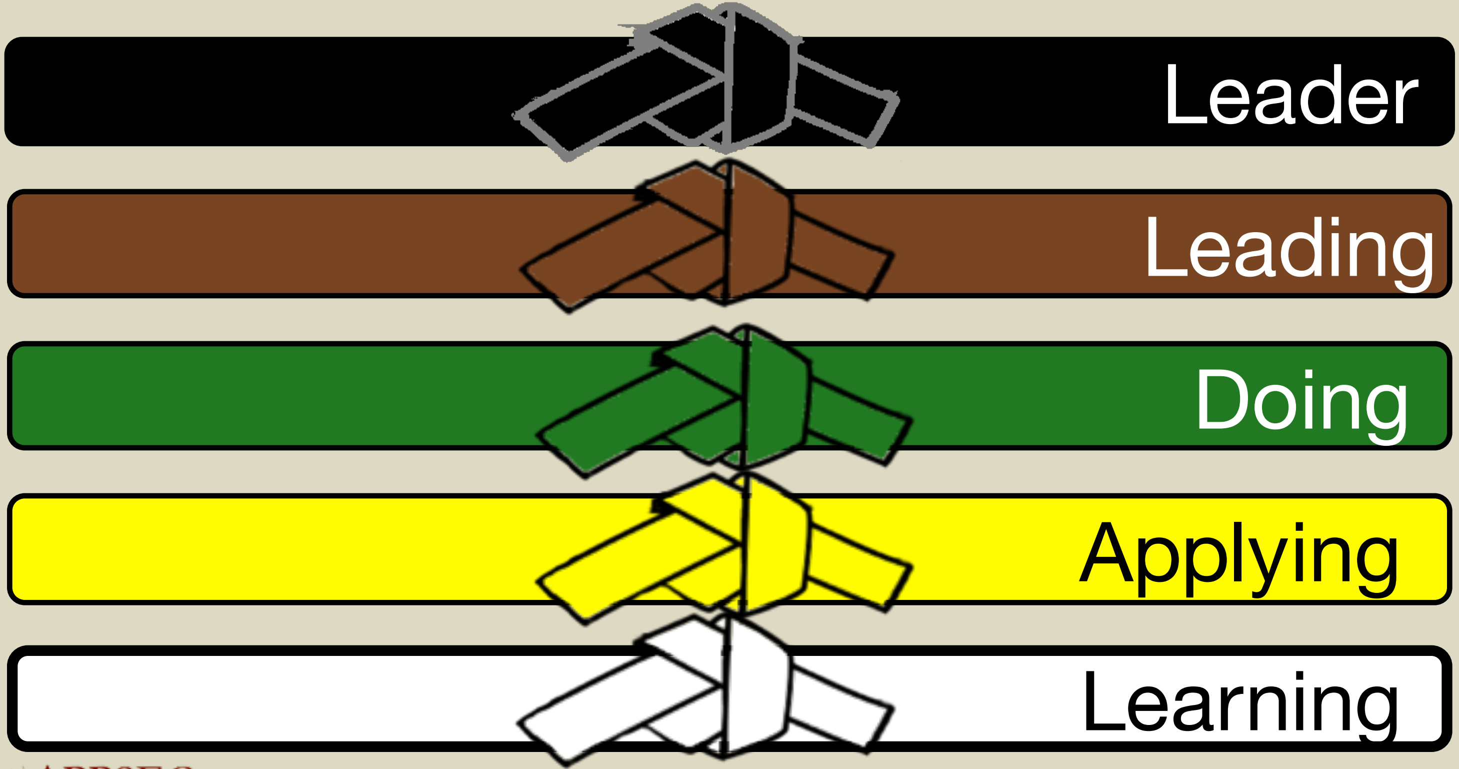
Define the problem

- 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



Leader

Leading

Doing

Applying

Learning

Design Decision #3: Roles

Development

- SW Engineer
- Tester
- Manager
- HW Engineer

Operations

- IT
- DevOps

Internal

- Sales
- Marketing
- Executives

Everyone

EVERYONE
E
CONTENT RATED BY
ESRB

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

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

Budget & Schedule

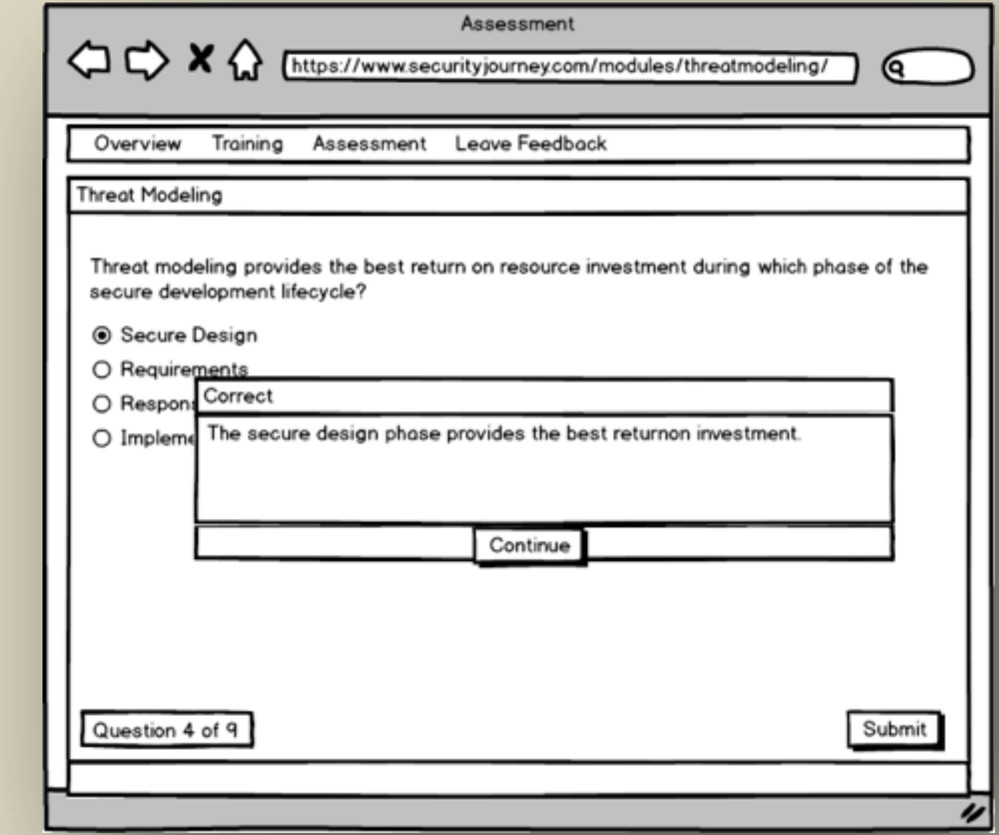
2016 → 2017, 18, 19?

Building an Application Security Awareness Program

Content

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

Assessment



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

● Secure Design

○ Requirements

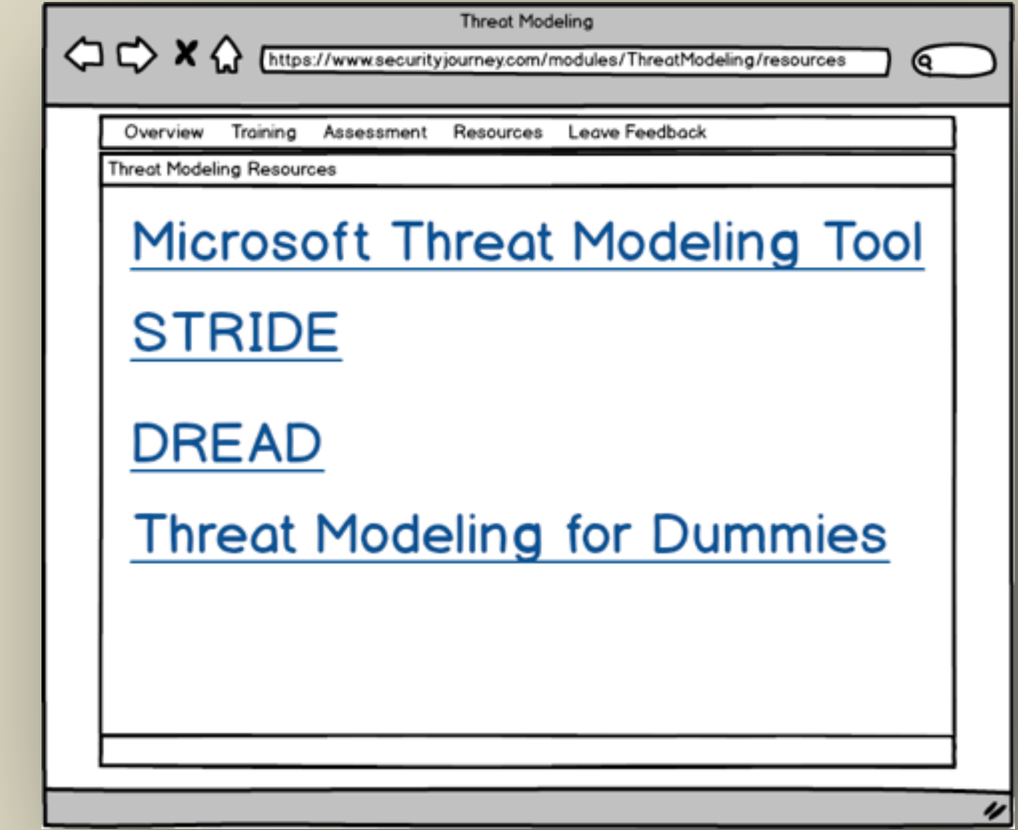
○ Respons

○ Impleme

Correct

The secure design phase provides the best returnon investment.

Resources


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

Threat Modeling Resources

Microsoft Threat Modeling Tool

STRIDE

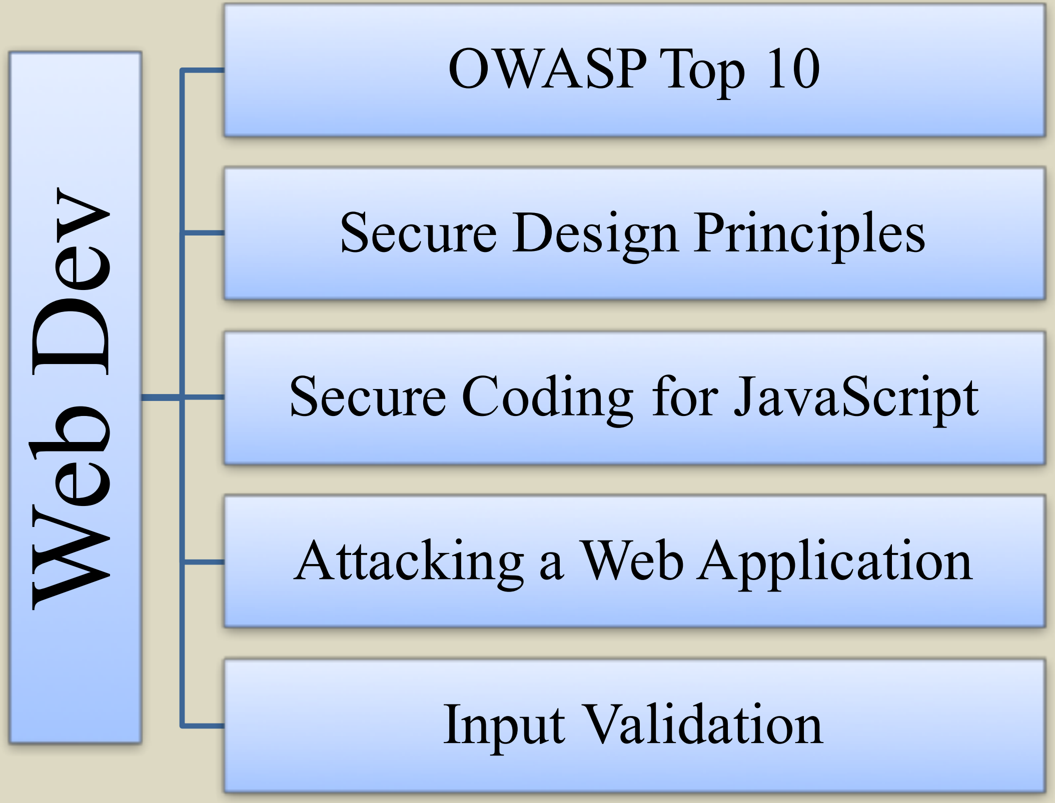
DREAD

Threat Modeling for Dummies

Level 1 Content Map

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

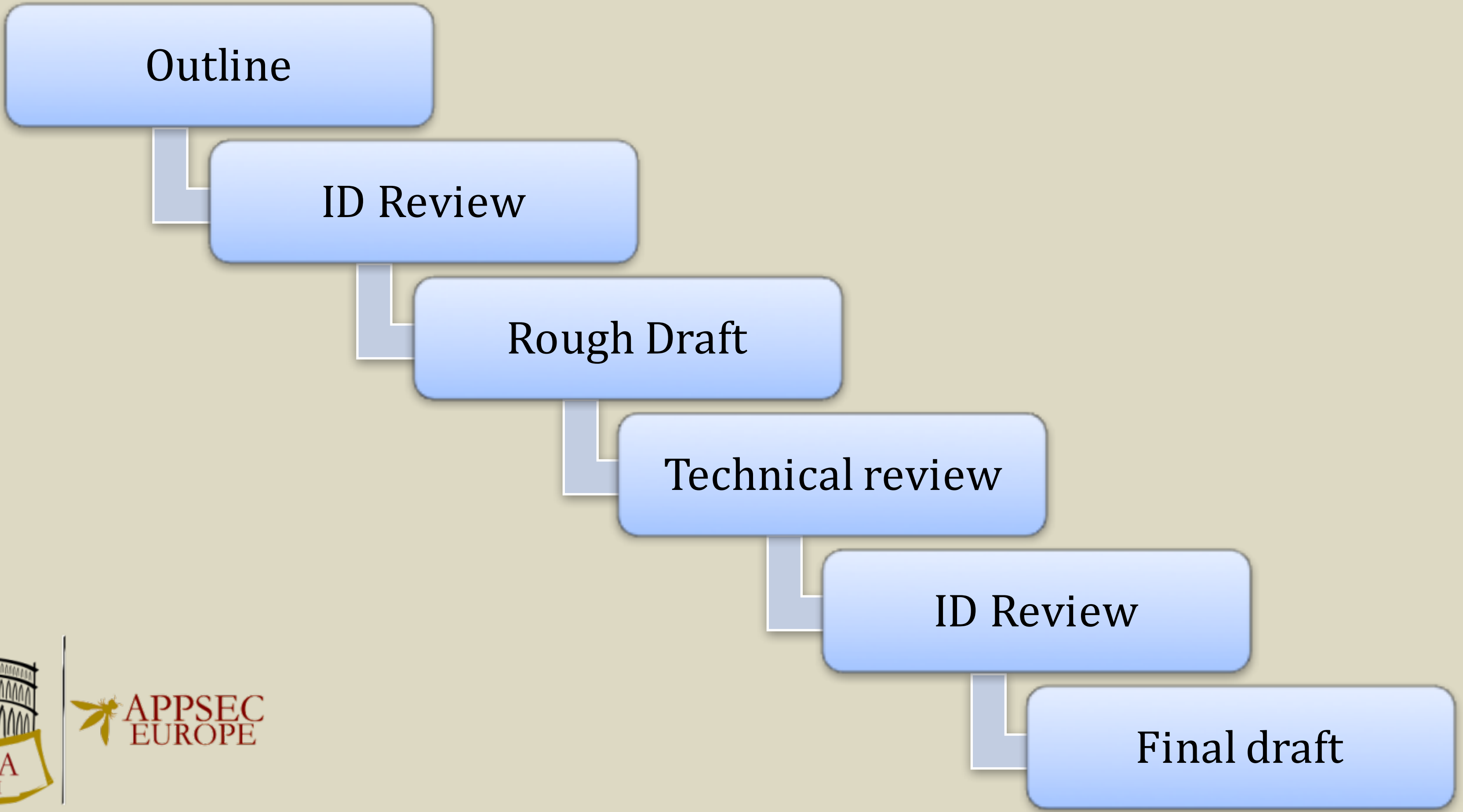
Level 2 Content Map



Web Dev

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

Content Creation Process



Outline

ID Review

Rough Draft

Technical review

ID Review

Final draft

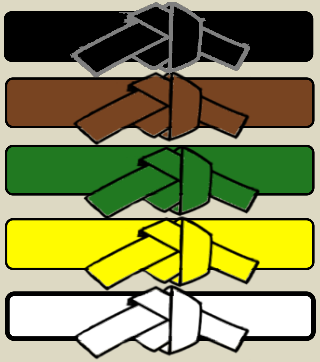
Humor / Story

Examples

- Still Cartoons
- Full motion cartoons
- Video

A word of caution…

Gamification



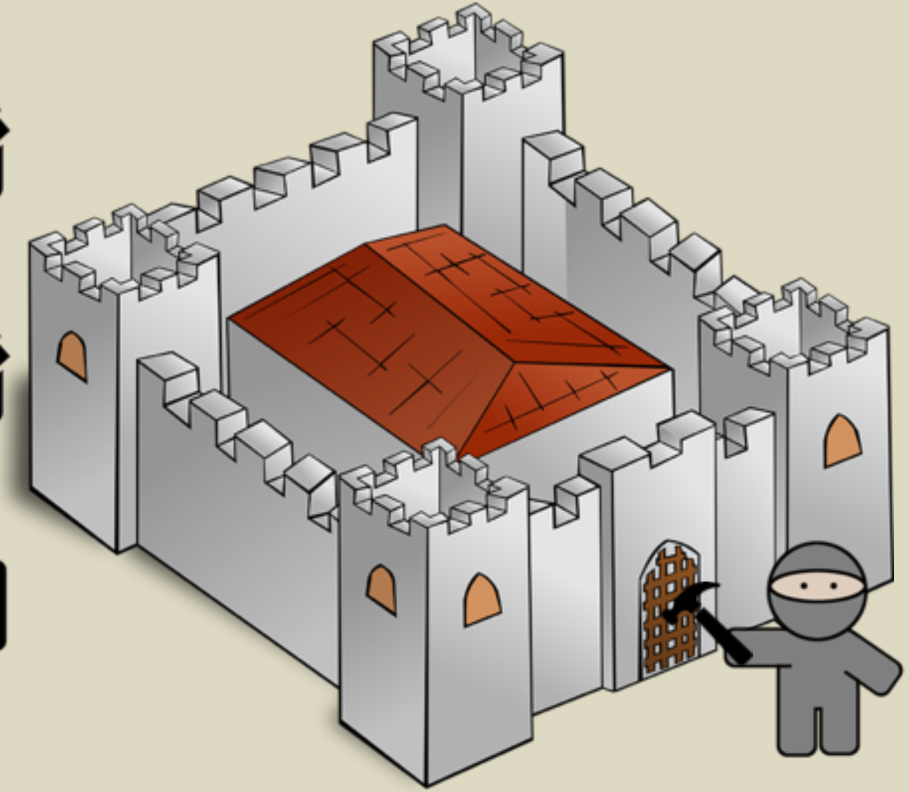
FEDERAL RESERVE NOTE
KB 46279860 I
B2
THE UNITED STATES OF AMERICA
100
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
ONE HUNDRED DOLLARS

User Interface

Security Fundamentals ☑

Attacks & Attackers ☑

Threat Landscape □

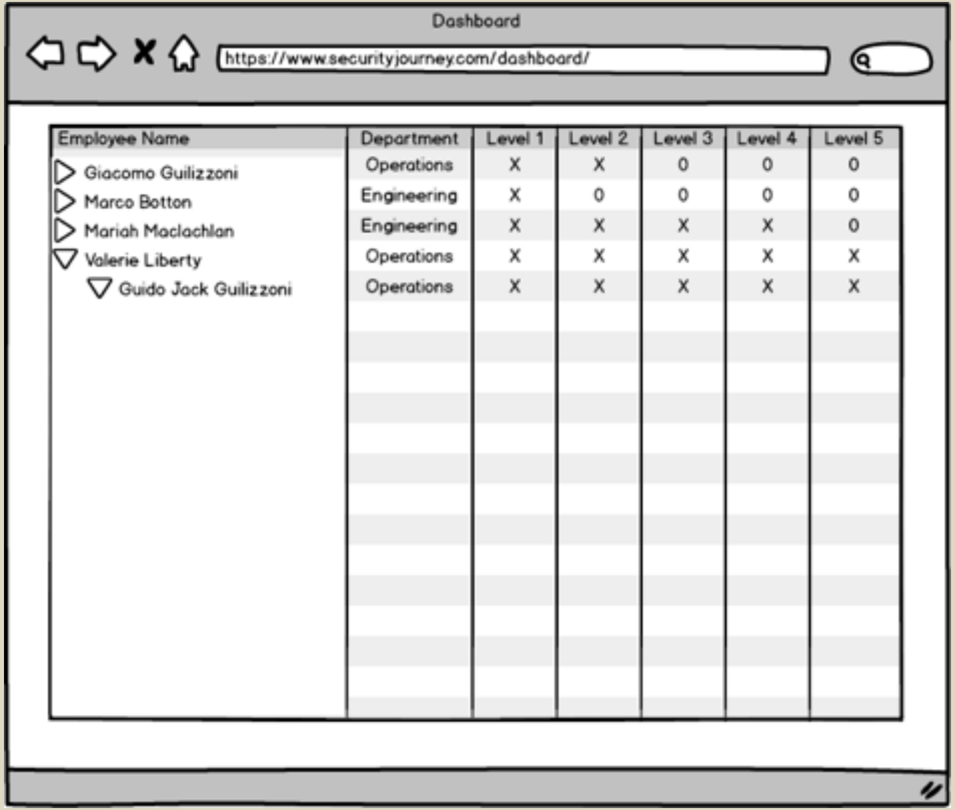


Security Myths □

Cryptography □

Privacy □

Competition



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

Build Your Own

Build one with OWASP

Q+A & Contact

Chris Romeo, CEO / Principal Consultant

chris_romeo@securityjourney.com

www.securityjourney.com

@edgeroute