RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HUM-T11

AppSec Awareness: A Blue Print for Security Culture Change

Christopher Romeo
CEO / Principal Consultant
Security Journey
@edgeroute

#RSAC

My Commitment

- Explain security culture and application security awareness
- Provide the process for how to build your own application security awareness program
- Share knowledge, experience, and best practices building application security awareness programs

Security Journey

What is Security Culture?

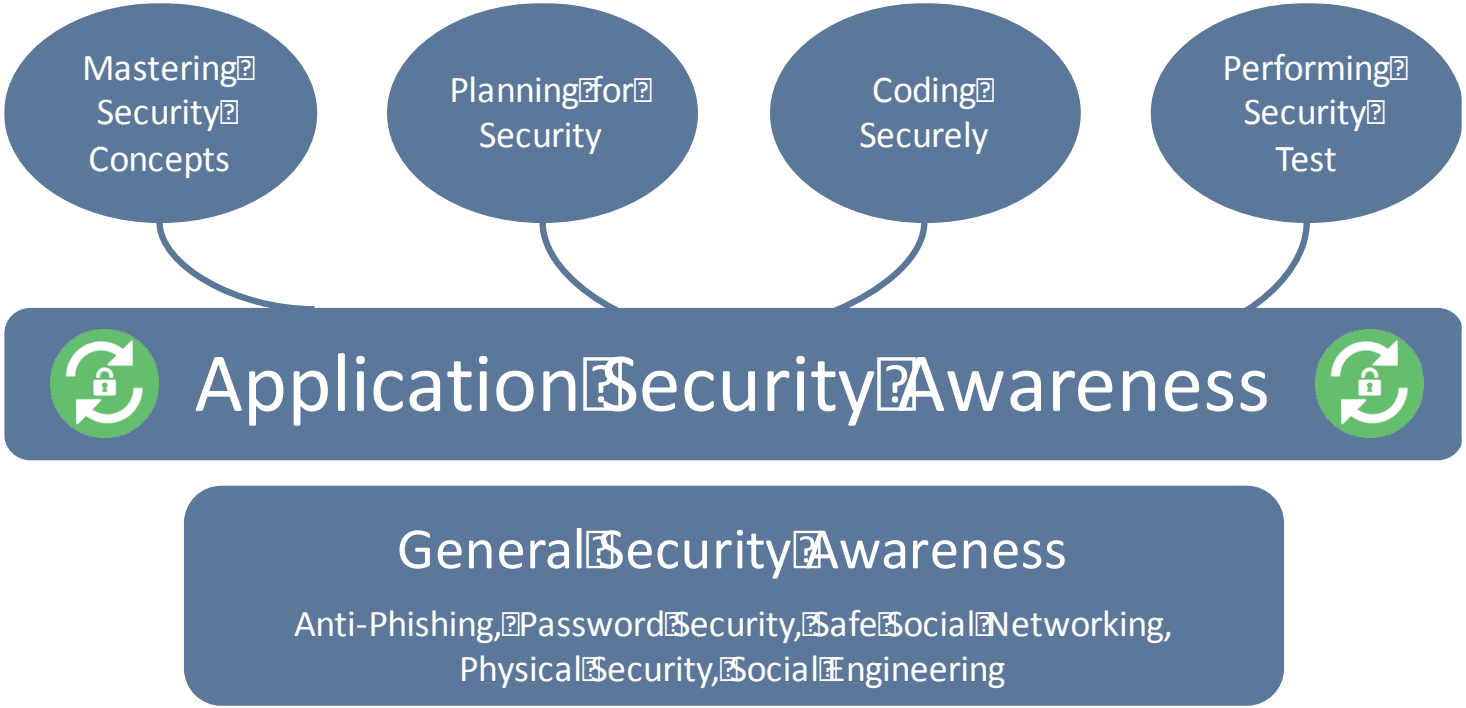
"What happens {**with security**} when people are left to their own devices."

--Tim Ferriss

Security Journey

Security is non-negotiable

What is Appsec Awareness?



Knowledge & History

Security Journey

Role Based

Developer

Tester

Manager

IT

Security Journey

Activity

Application Security Awareness is…

A program that instills a security foundation, changing security culture from the inside out

Goals of AppSec Awareness

Disrupt

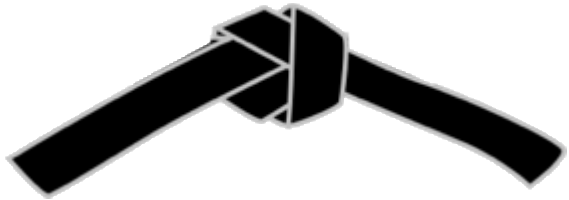
Goals of AppSec Awareness

Sustainable

Goals of AppSec Awareness

Secure

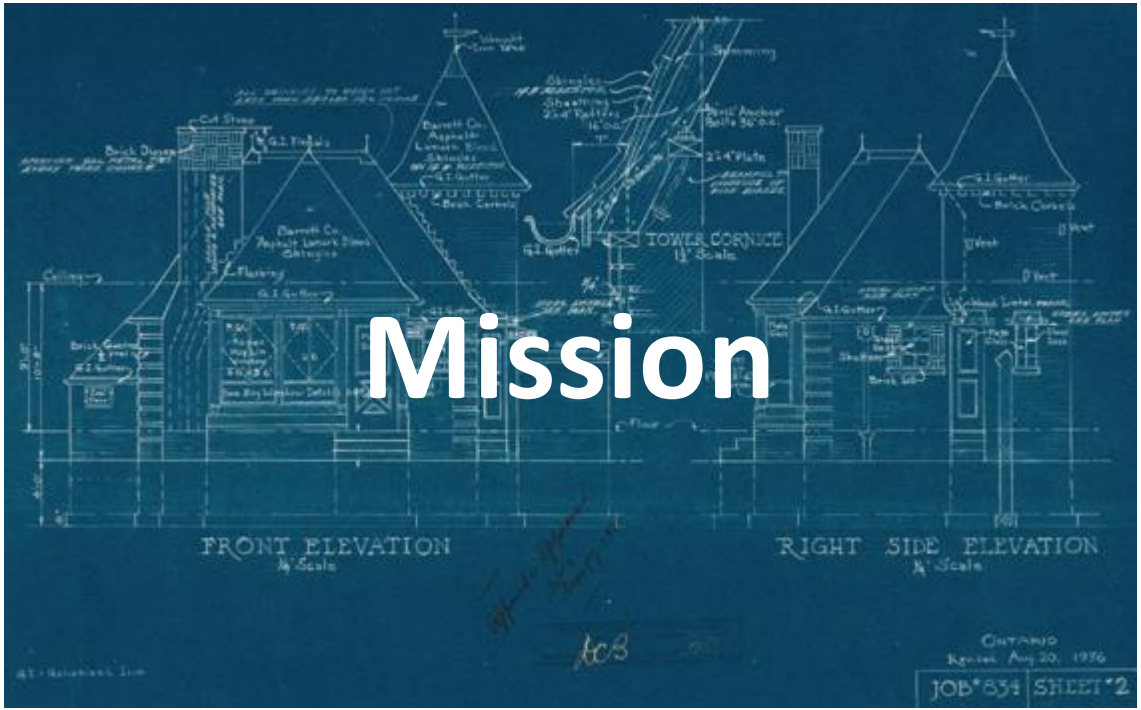
My Experience



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

Security Journey

Security Journey


TOWER CORNICE
FRONT ELEVATION
RIGHT SIDE ELEVATION
JOB*834
SHEET*2

Mission

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 step up and improve security

Assess Security Culture

Program Objectives

- ❑Create a thriving program
- ❑Teach everyone the importance of security
- ❑Generate activity towards improving security
- ❑Build security community

Security Journey

Build a Team

SME

Security Journey

Apply: Mission

- **Define** the problem as it exists in YOUR organization
- **Assess** YOUR security culture, to determine how far you have to go
- **Define** what you are trying to accomplish (program objectives)
- **Build** a team of internal and external experts

Security Journey

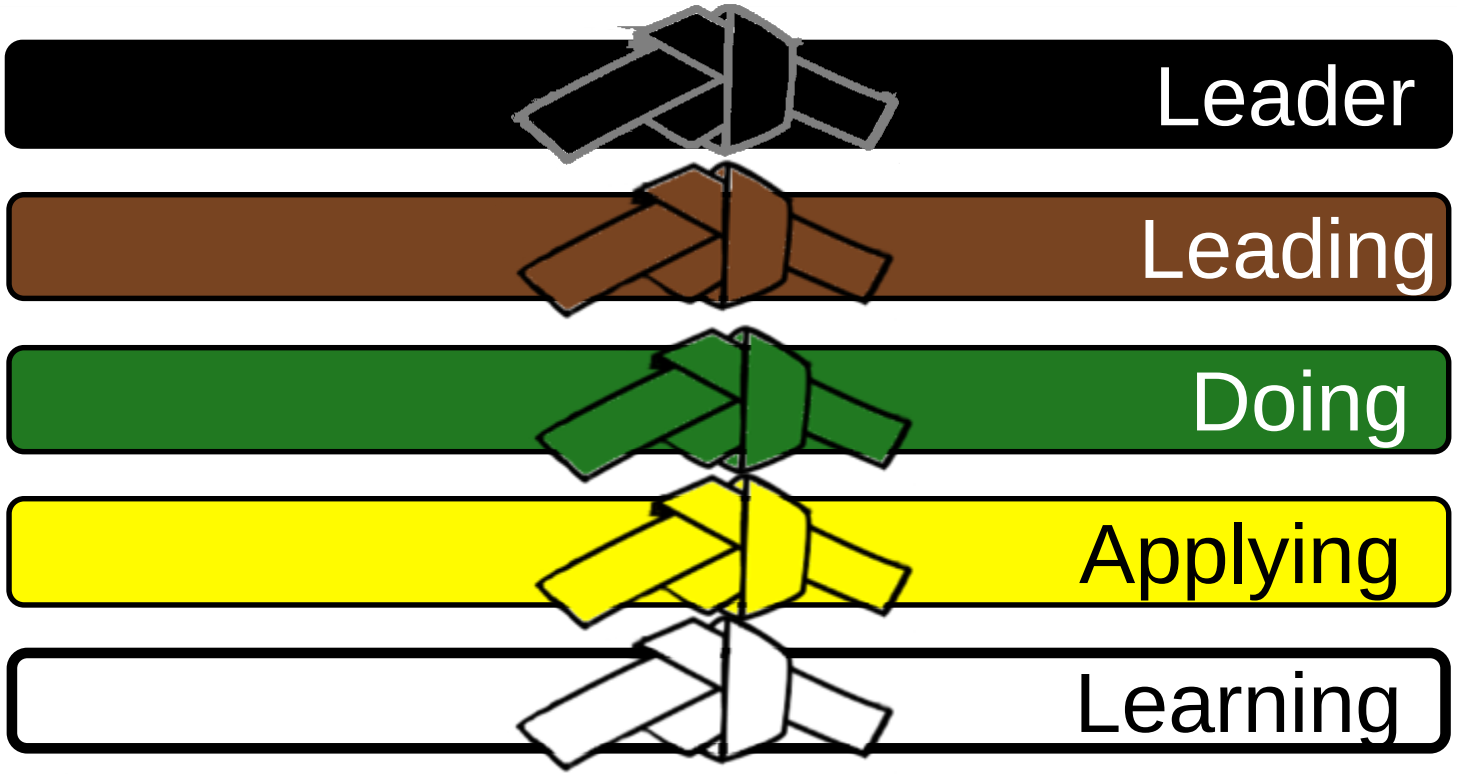
A foundation…

Security Journey

Program Architecture

Theme

Levels



Roles

Development	Operations	Internal	Everyone
• SW Engineer • Tester • Manager • HW Engineer	• IT • DevOps	• Sales • Marketing • Executives	

Activities

Build

- A security tool or process
- Partnerships
- Security community

Enrich

- Mentor
- Teach a course
- Deliver presentations

Explore

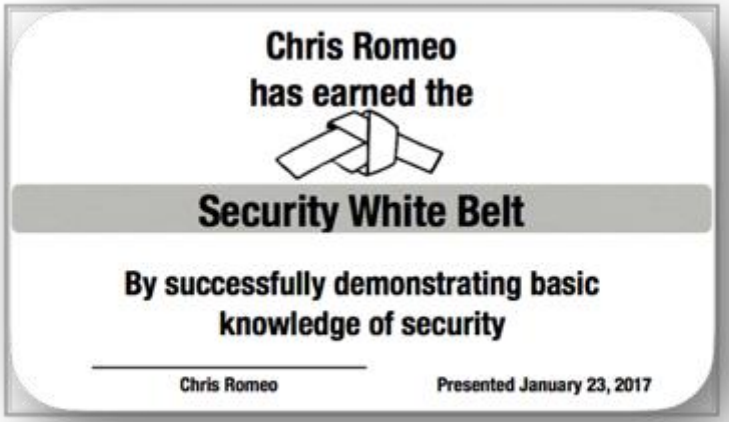
- Security issue analysis
- Security committee
- A vulnerable web app

Implement

- A security feature
- A security test
- Security strategy

Security Journey

Recognition

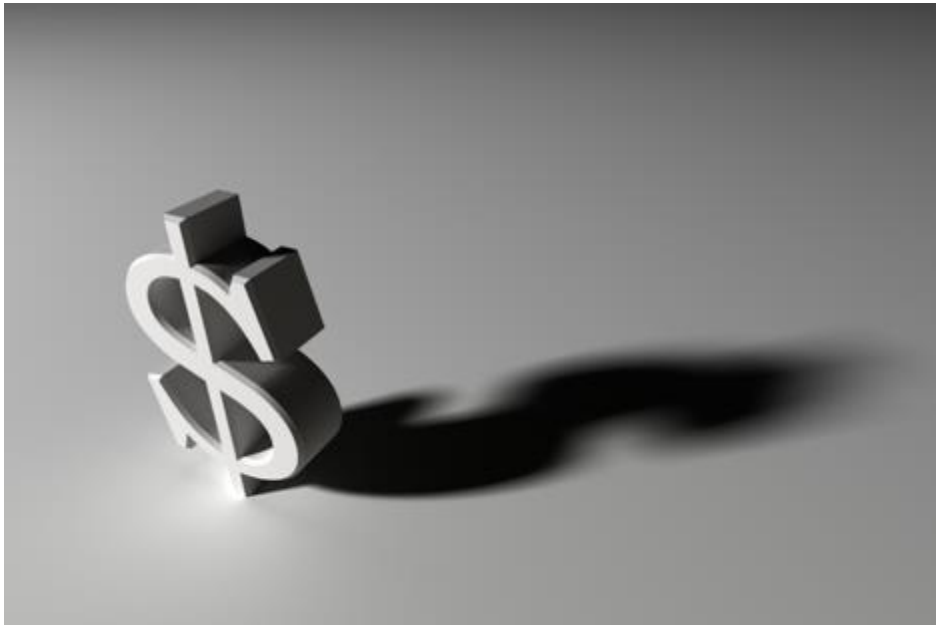


Security Journey

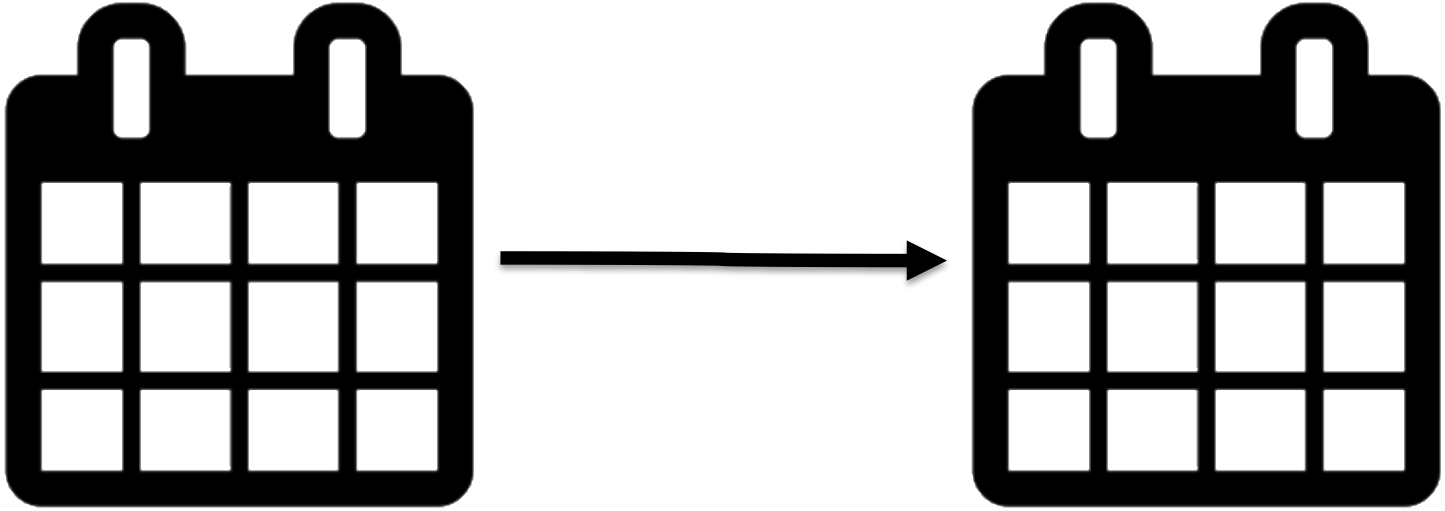
Recognition

Budget

- Time
- External production partners
- Could be shoestring, could be millions



Schedule



2016

2017, 18, 19?

Security Journey

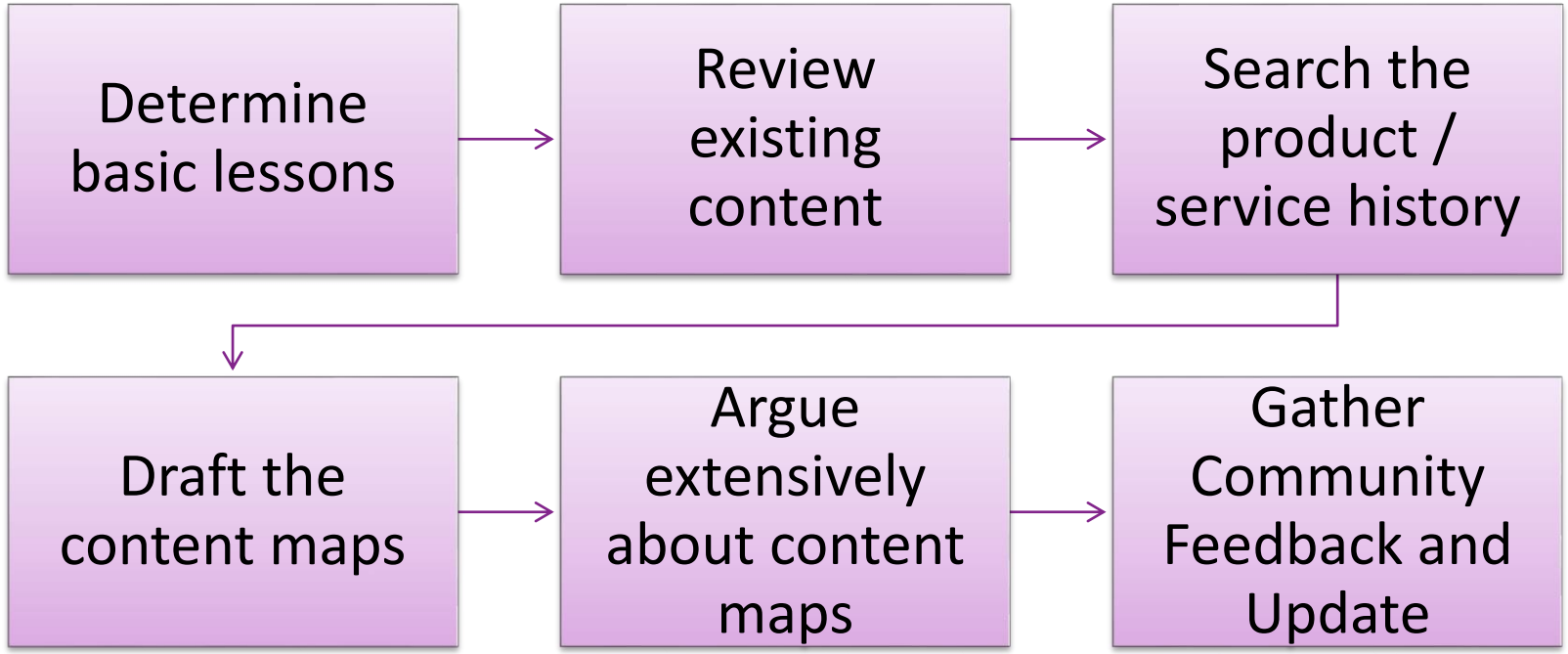
Apply: Program Architecture

- **Choose** a theme that fits within the boundaries of YOUR organization
- **Define** your roles
- **Determine:**
  - the number of levels
  - what activities will you promote (if any)
  - your recognition philosophy and implementation

Security Journey

Curriculum

Curriculum Development Process



Level 1 Content Map

Security Fundamentals	Threat Landscape	Attacks & Attackers	OWASP Top 10
Secure Development Life Cycle	Security Myths	Cryptography	Secure Design Principles
	Security Standards	Privacy	

Security Journey

Level 2 Content Map -- Developer

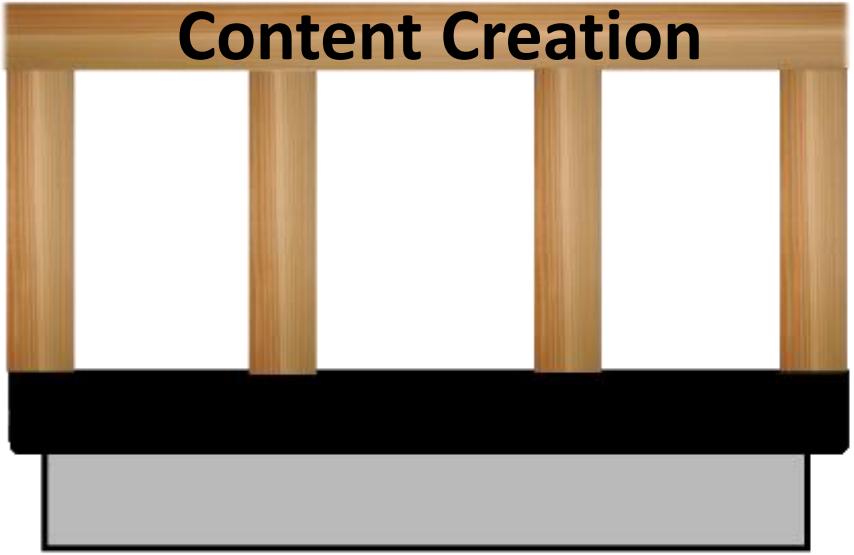
Secure Coding with Java	XSS	Threat Modeling	Input Validation
SQL Injection	CSRF	Secure Code Review	Using OpenSSL
	Attacks Against Human Engineers	Testing Web App Security	

Security Journey

Apply: Curriculum

- **Develop:**
  - a curriculum development process for your program
  - a content map for each level of your program

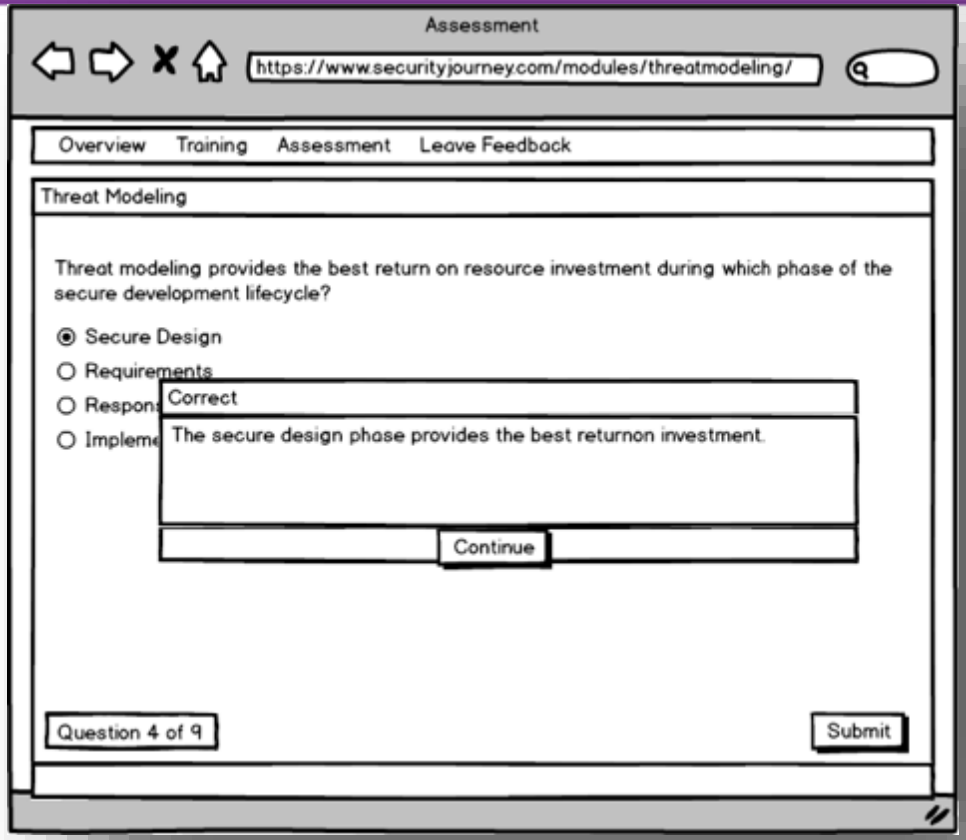
Content Creation



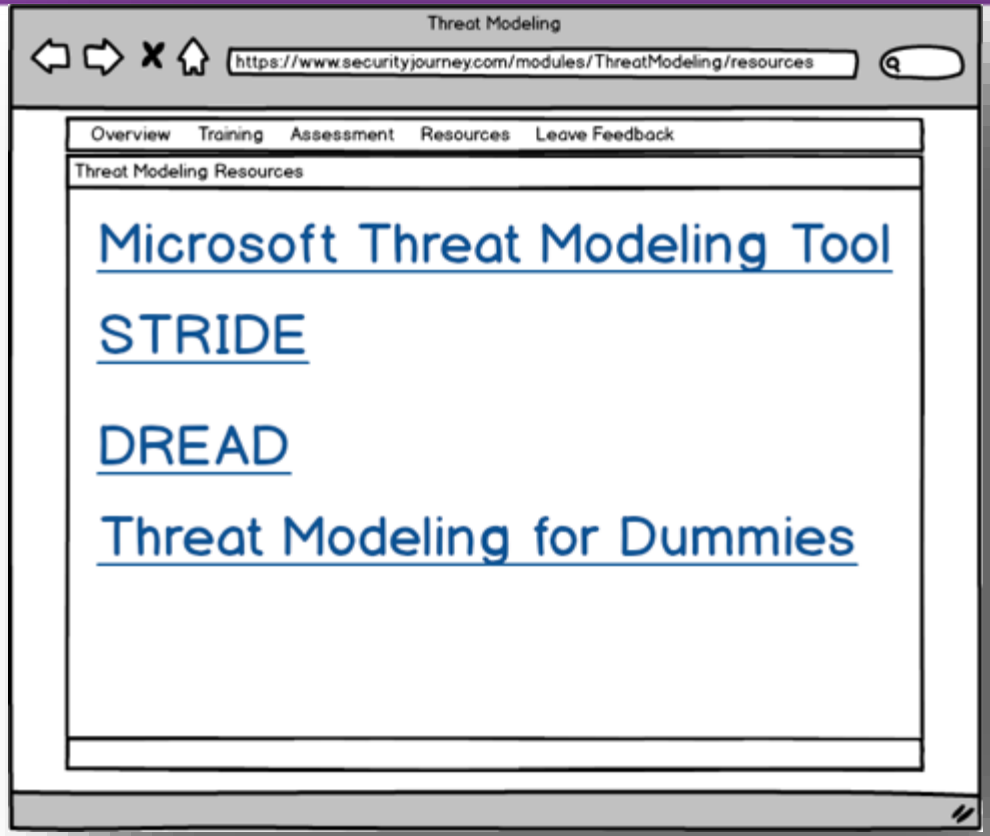
Content

Security Journey

Assessment

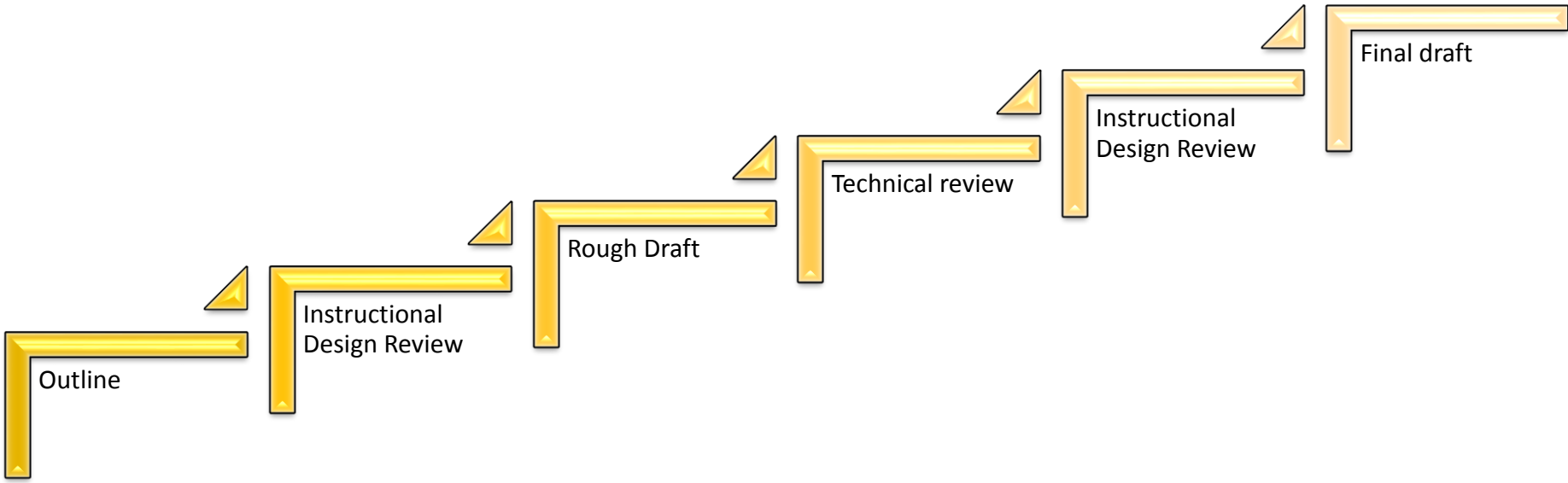

Assessment
https://www.securityjourney.com/modules/threatmodeling/
Overview
Training
Assessment
Leave Feedback
Threat Modeling
Threat modeling provides the best return on resource investment during which phase of the secure development lifecycle?
Secure Design
Requirements
Correct
The secure design phase provides the best returnon investment.
Continue
Question 4 of 9
Submit

Resources



Security Journey

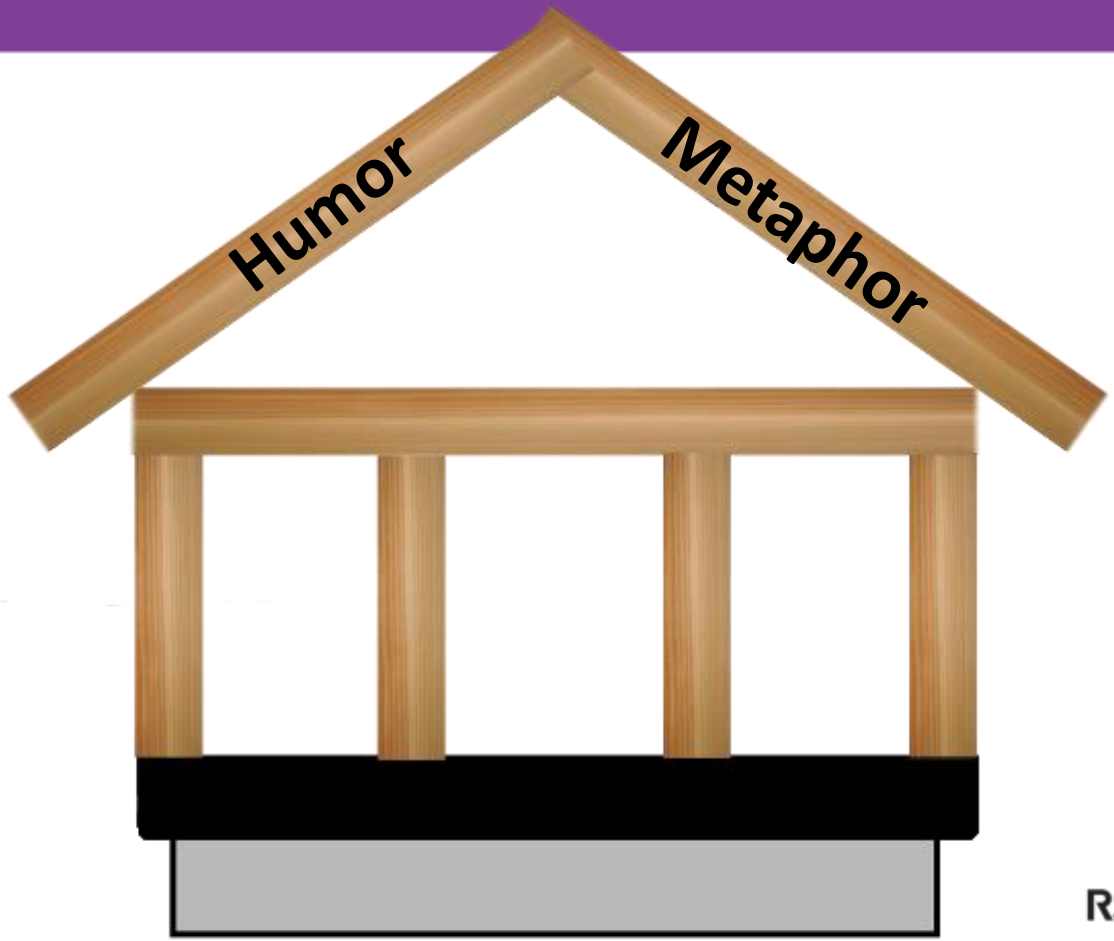
Content Creation Process



Security Journey

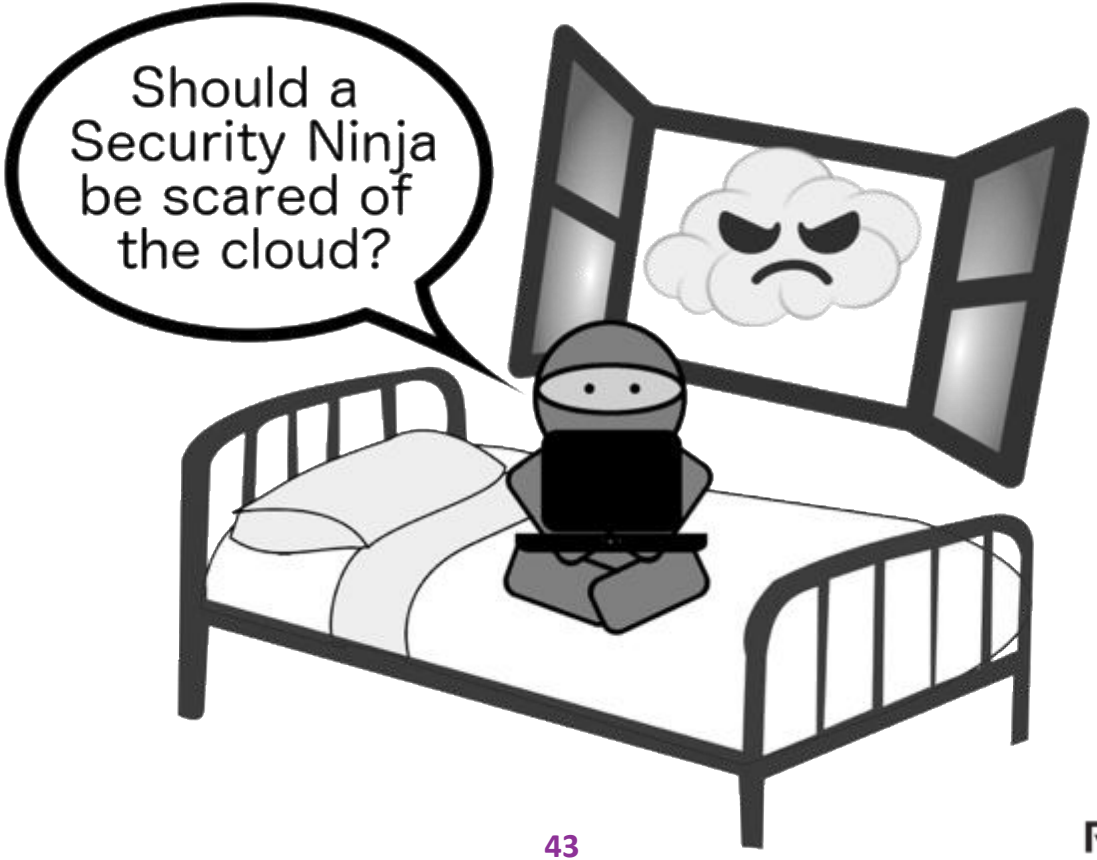
Apply: Content Creation

- **Determine**:
  - Content style
  - Assessment structure
- **Build** your content development process



Security Journey

What is a security metaphor?



Security Journey

Examples

- Still Cartoons
- Full motion cartoons
- Video

A word of caution…

TYPG

Apply: Humor & Metaphor

- **Decide** on your organization's tolerance for humor
  - Edgy to tame: where do you sit?
- **Brainstorm** ideas for security metaphors
  - bring your production team into the loop

Security Journey

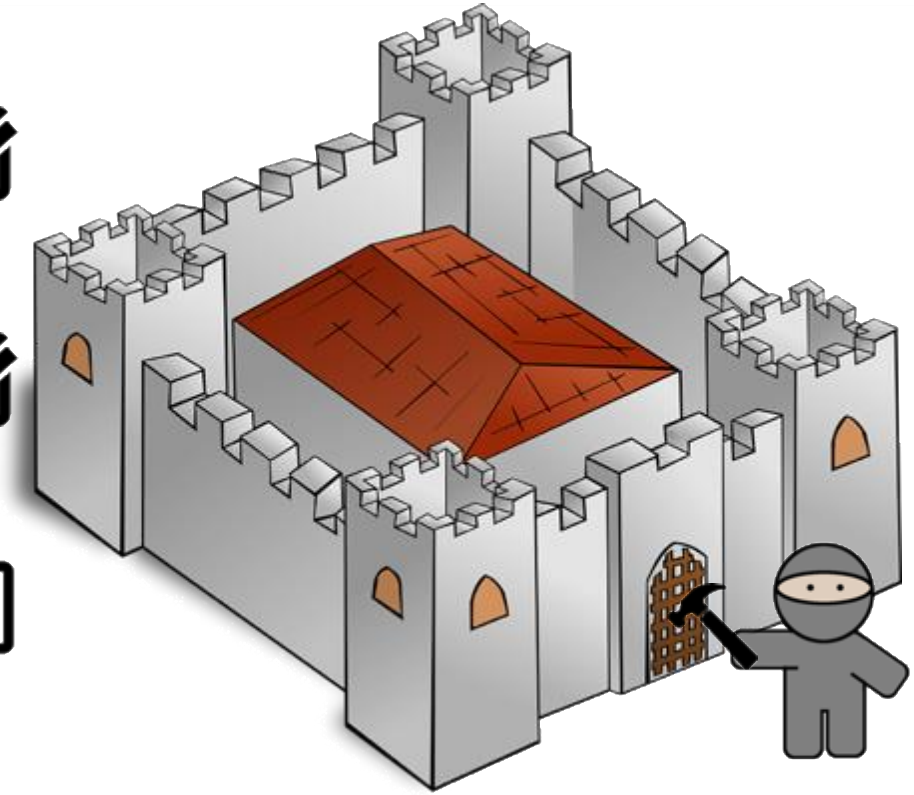
Security Journey

Gamification

Security Journey

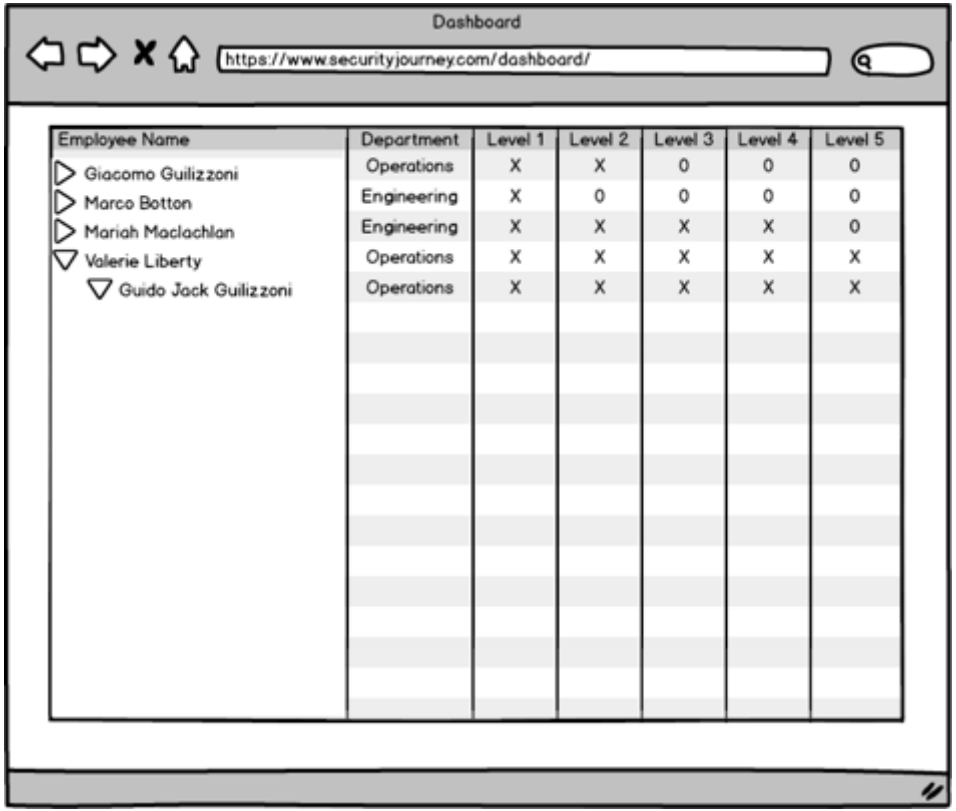
Interface

- Security Fundamentals ☑
- Attacks & Attackers ☑
- Threat Landscape ☐
- Security Myths ☐
- Cryptography ☐
- Privacy ☐



Security Journey

Dashboard

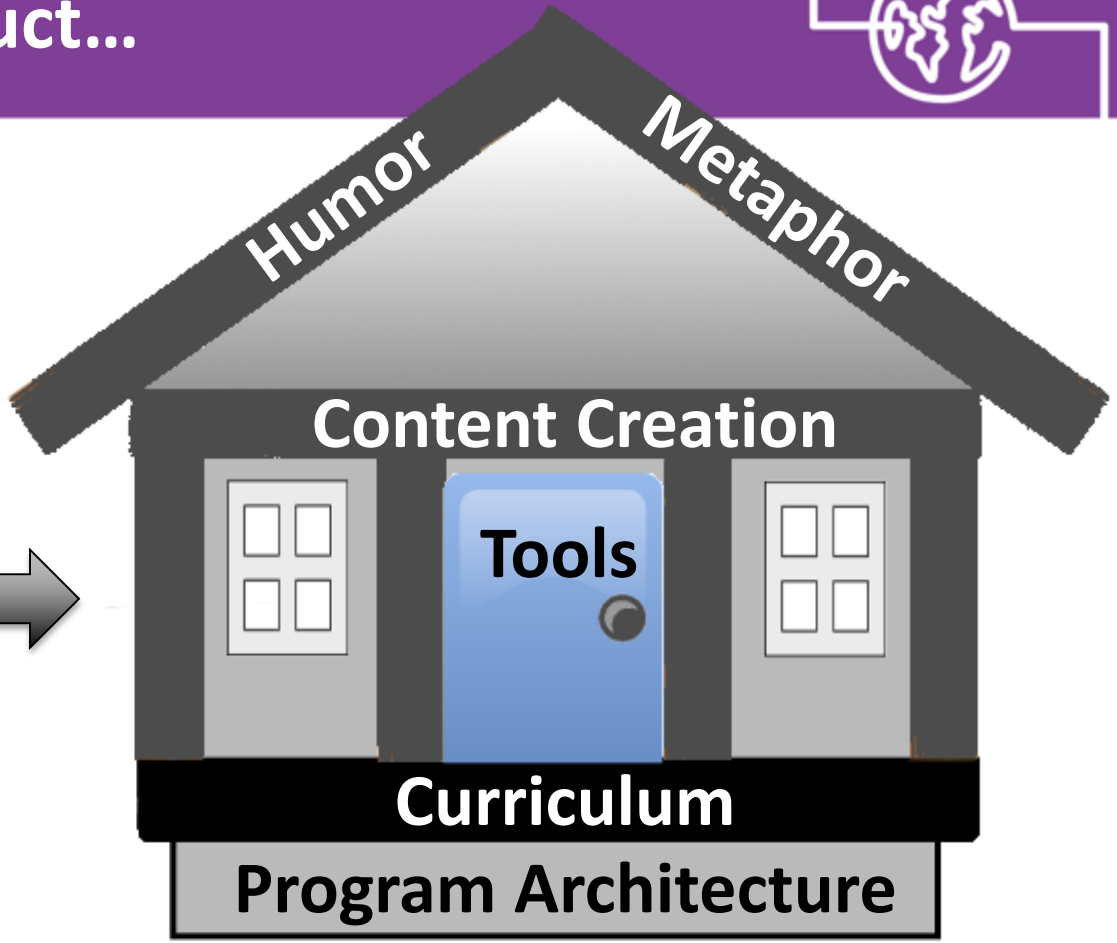

Dashboard
https://www.securityjourney.com/dashboard/
Employee Name
Department
Level 1
Level 2
Level 3
Level 4
Level 5
Giacomo Guilizzoni
Operations
X
X
0
0
0
Marco Botton
Engineering
X
0
0
0
0
Mariah Maclachlan
Engineering
X
X
X
X
0
Valerie Liberty
Operations
X
X
X
X
X
Guido Jack Guilizzoni
Operations
X
X
X
X
X

Apply: Tools

- **Decide** how to model your theme and content in a catchy interface that engages your learners
- **Study** gamification principles and incorporate
  - HINT: Ask your kids!
- **Plan** your dashboard; what is the hard hitting information that will bring visibility to your program?

Security Journey

The finished product…



Security Journey

Build Your Own

Q+A & Contact

Chris Romeo, CEO / Principal Consultant

chris_romeo@securityjourney.com

www.securityjourney.com

@edgeroute

Security Journey