Cisco’s Security Dojo: Raising the Application Security Awareness of 20,000+

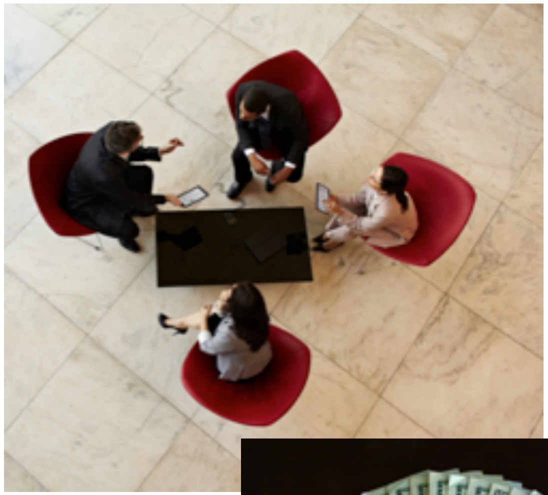
Chris Romeo, Security Journey; formerly of Cisco Systems

Chris Romeo @edgeroute

- Chris Romeo, CEO / Principal Consultant
- 20 years security experience
- 5 years leading the Cisco SDL & Cisco Security Ninja programs
- Speaker at RSA, AppSec USA, & ISC2 Security Congress

Security Journey

Would you believe we reached > 30K people with…



- A four person core team?
- A budget of less than 50K?
- A program created in 6.5 months?
- A non-mandatory program?

My Commitment

- Share the Cisco Security Dojo story
- Demonstrate our concept
  - Content, Metaphor, Recognition
- Show the systems
- Share the secrets of Cisco’s success

Once upon a time…

Security Development Conference
MAY 15–16, 2012 | WASHINGTON, DC

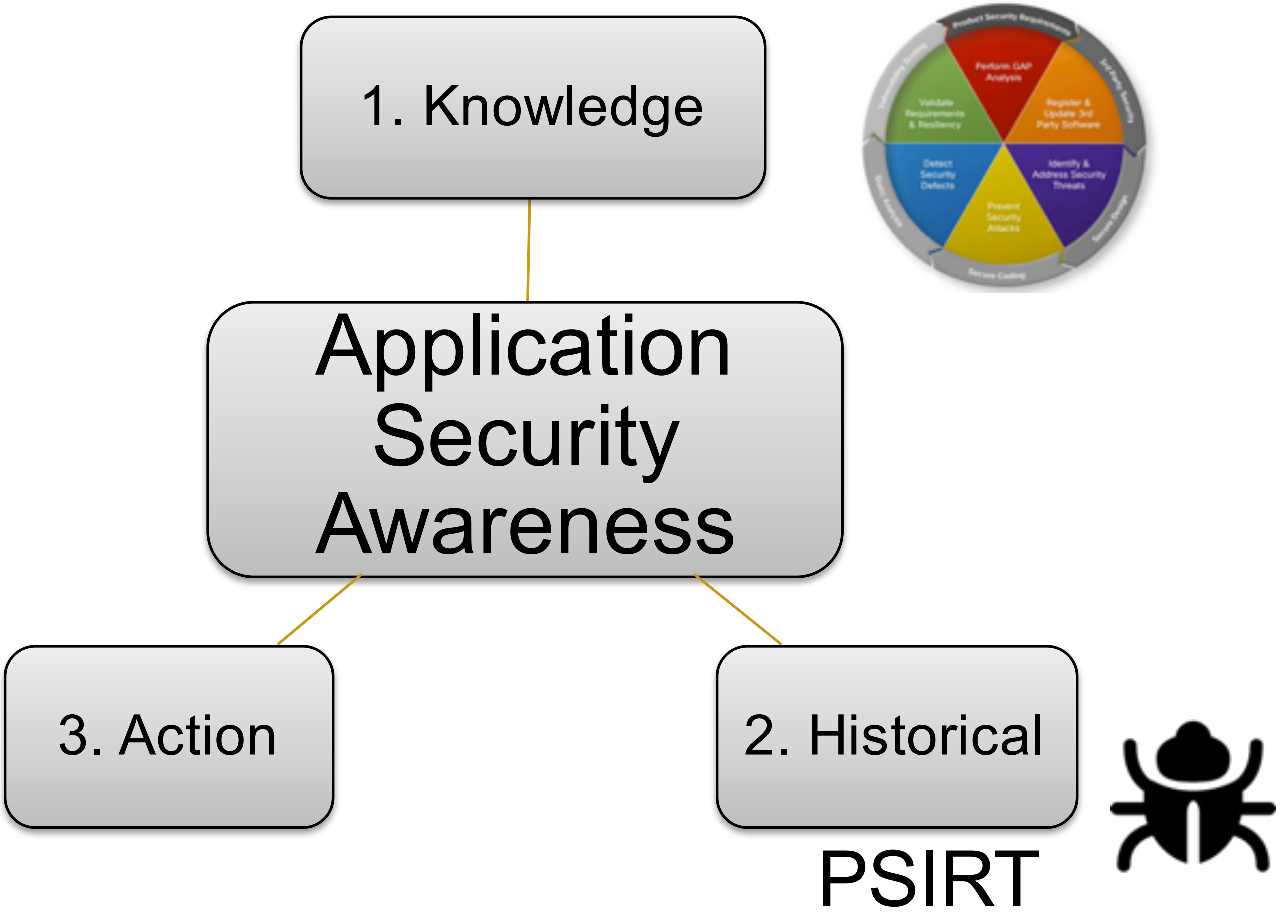
The Problem Space (2012)

- Cisco does not have a comprehensive, end-to-end security training program for Engineering
- Current security IQ is inconsistent with Cisco’s desire to be industry leaders in secure product development
- Many engineers do not know how to use CSDL to prevent product security flaws
- Engineers are not aware of how threats continue to increase, both in complexity and depth, and apply to their products

Most employees view training as medicine or worse, as punishment.

Denise D. Ryan

https://flic.kr/p/53Kyr8



1. Knowledge

Application Security Awareness

3. Action

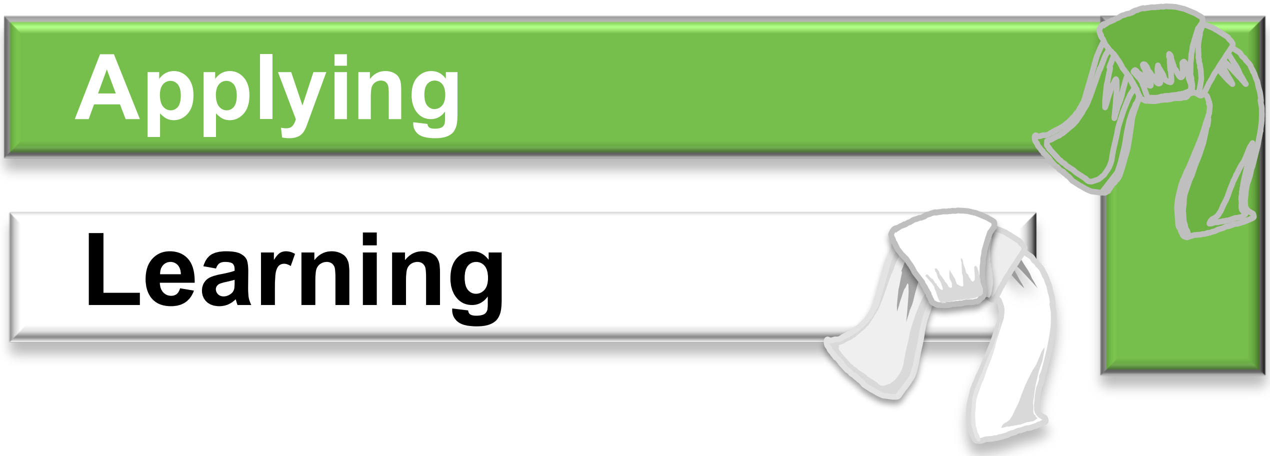
2. Historical

PSIRT

Cisco Security White Belt

Learning

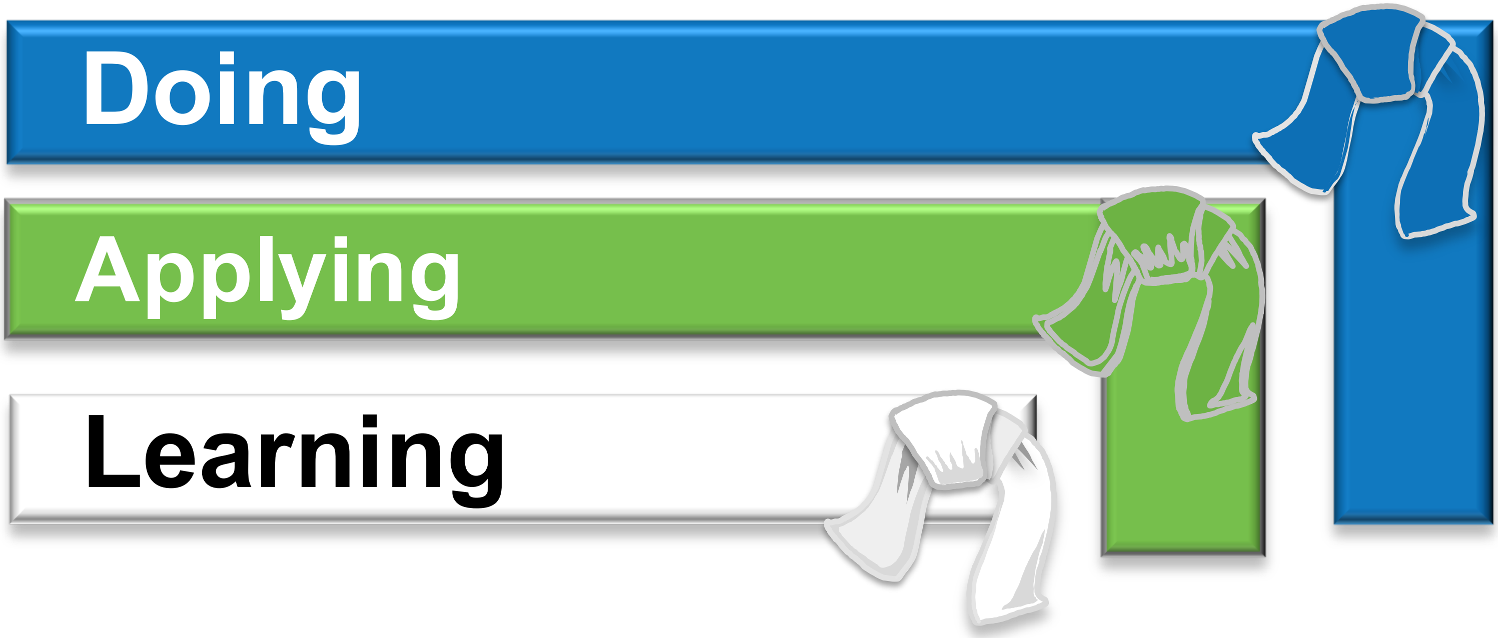
Cisco Security Green Belt



Applying

Learning

Cisco Security Blue Belt

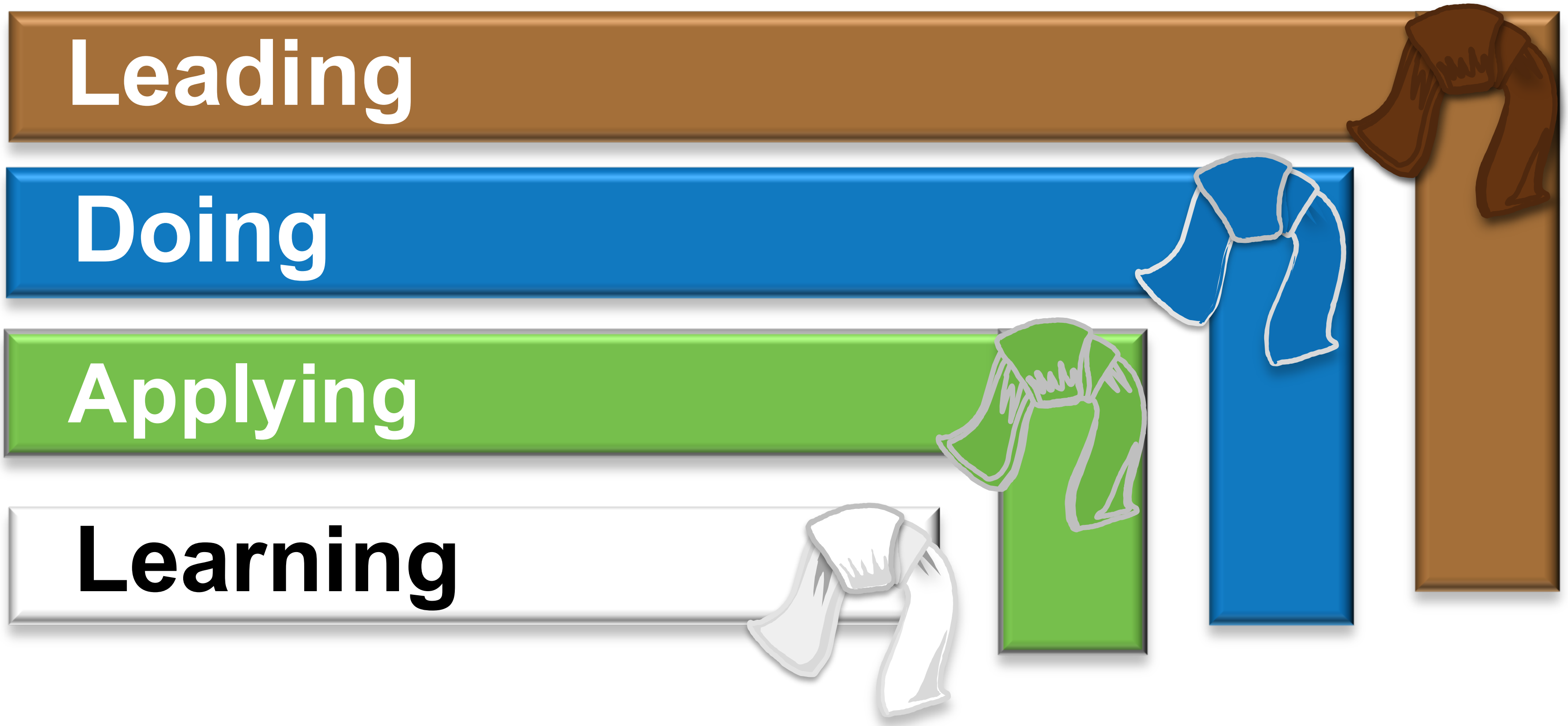


Doing

Applying

Learning

Cisco Security Brown Belt



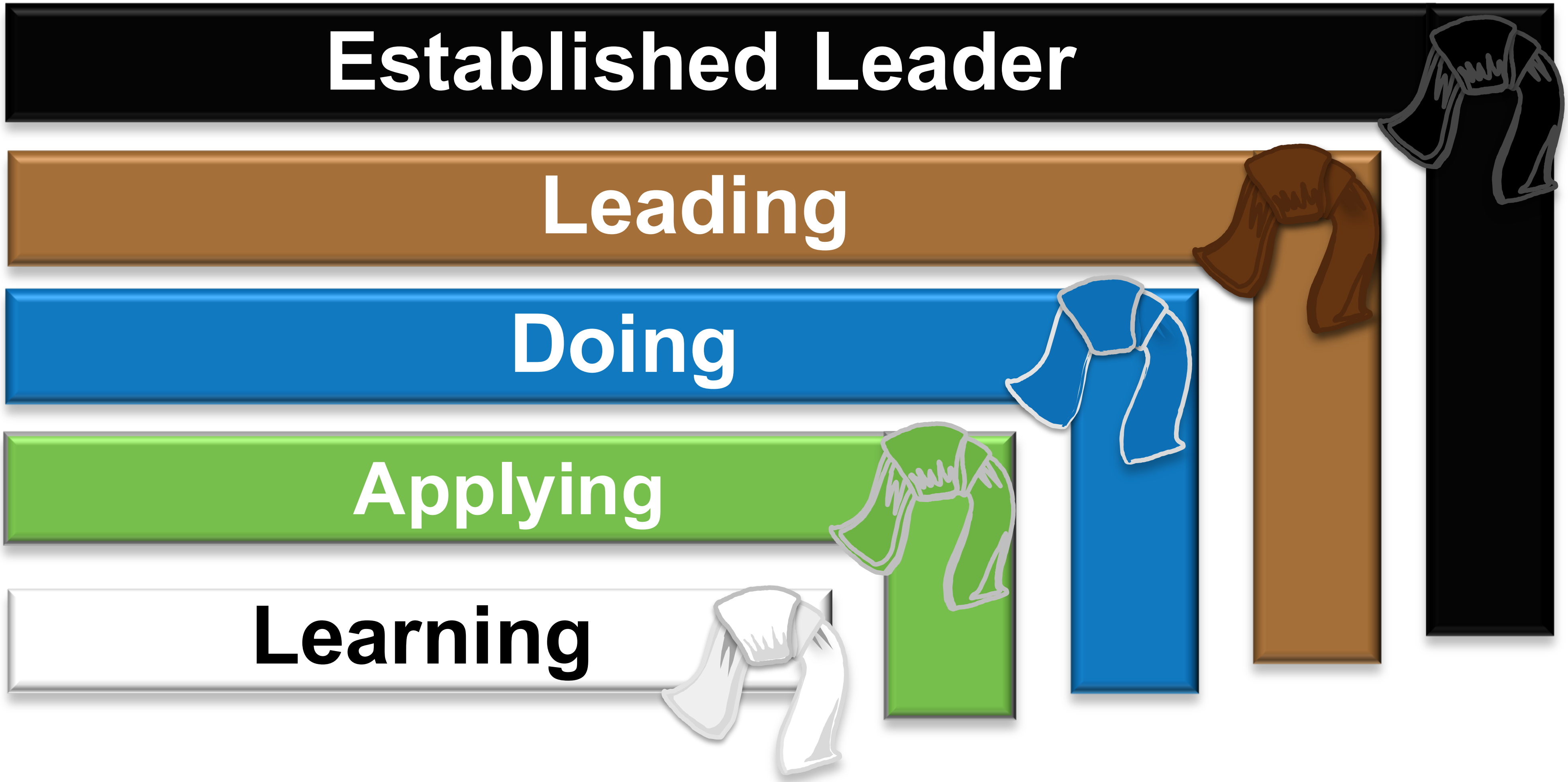
Leading

Doing

Applying

Learning

Cisco Security Black Belt



Established Leader

Leading

Doing

Applying

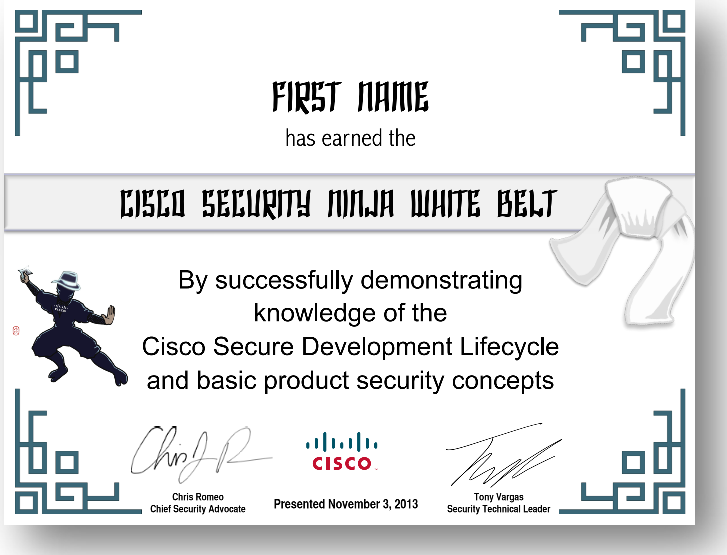
Learning

We are **all** security ninjas.

Content Delivery

Security Metaphors

Recognition



FIRST NAME

has earned the

CISCO SECURITY NINJA WHITE BELT

By successfully demonstrating knowledge of the Cisco Secure Development Lifecycle and basic product security concepts

Chris Romeo
Chief Security Advocate

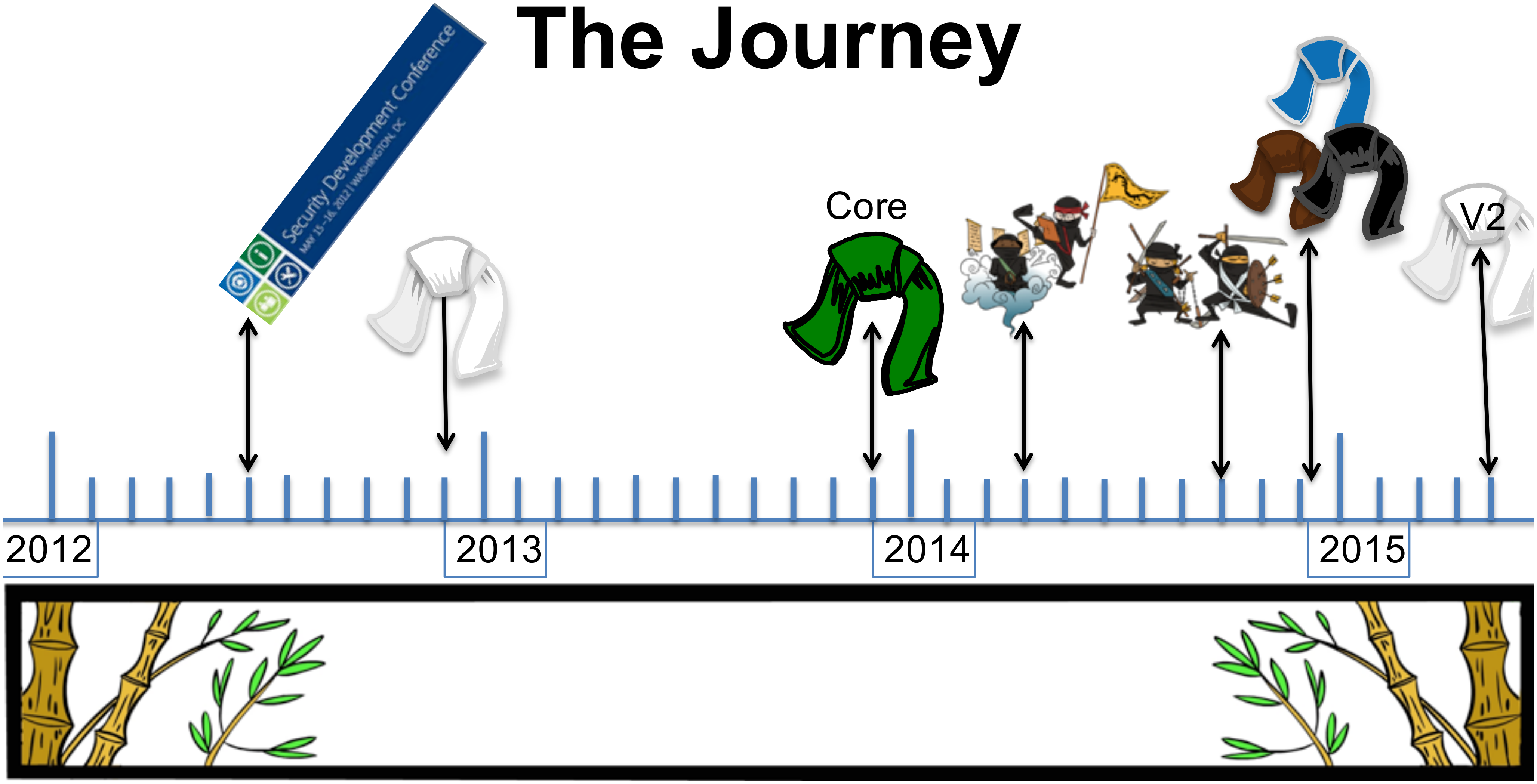
Presented November 3, 2013

Tony Vargas
Security Technical Leader

Cisco Security Black Belt
Cisco Security Brown Belt
Cisco Security Blue Belt
Cisco Security Green Belt
Cisco Security White Belt

FEDERAL RESERVE NOTE
HL 19268615 G
L12
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States
SERIES 2006
100
FRANKLIN

The Journey


Security Development Conference
MAY 15–16, 2012 | WASHINGTON, DC
Core
V2
2012
2013
2014
2015

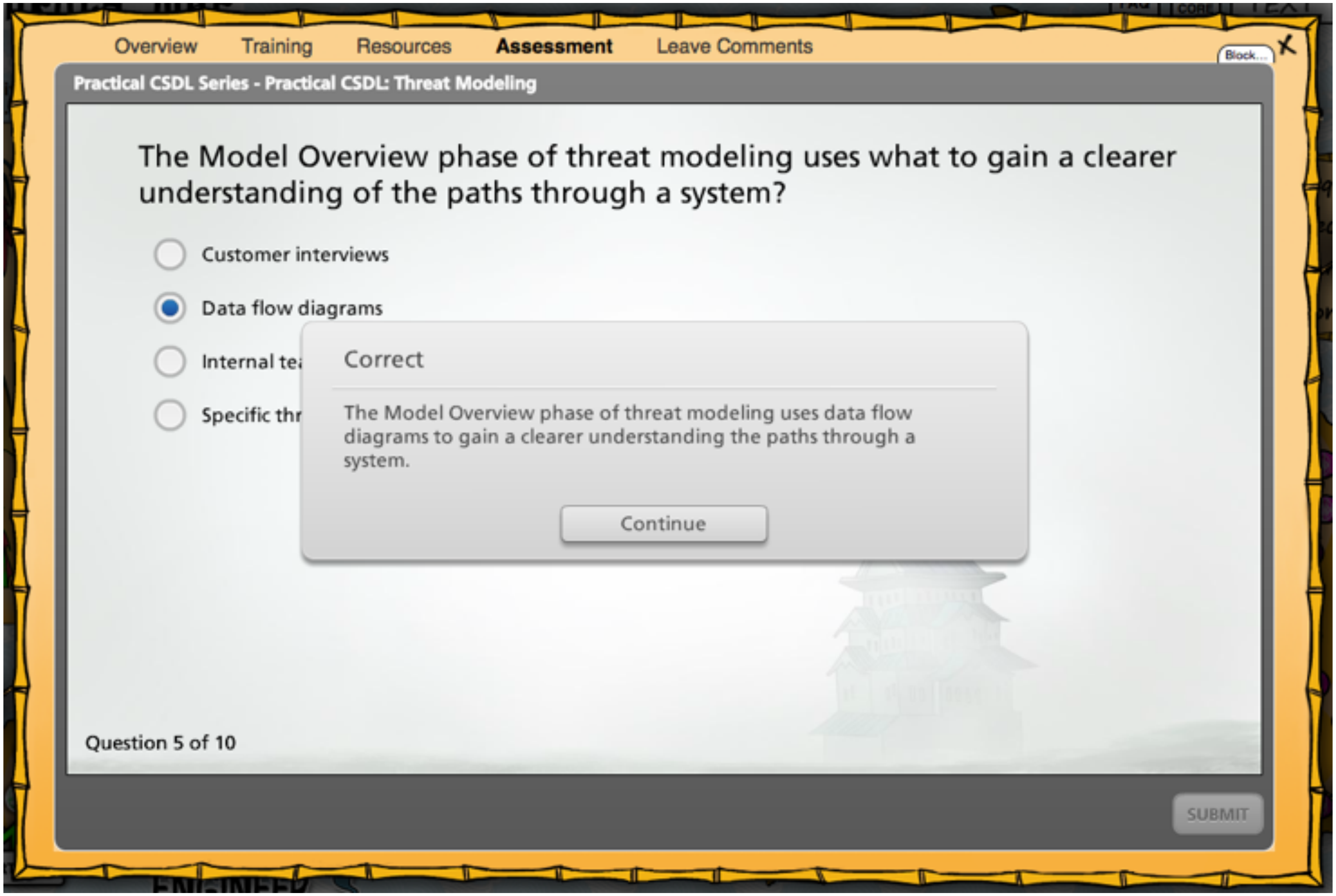
Cisco Security White Belt

Foundational

- Being a Trustworthy Company
- Security Vocabulary
- Security Business
- Public Sector
- Attacks & Attackers
- Security Myths
- Customer Data Protection
- Intro to CSDL
- PSIRT
- Intellectual Property
- Supply Chain
- Cisco Security Story

Advanced

- Input Validation
- Resource Exhaustion
- Authentication
- Authorization
- Configuration
- Information Leakage
- Hardware
- Cryptography



Practical CSDL Series - Practical CSDL: Threat Modeling

The Model Overview phase of threat modeling uses what to gain a clearer understanding of the paths through a system?

○ Customer interviews

● Data flow diagrams

○ Internal te

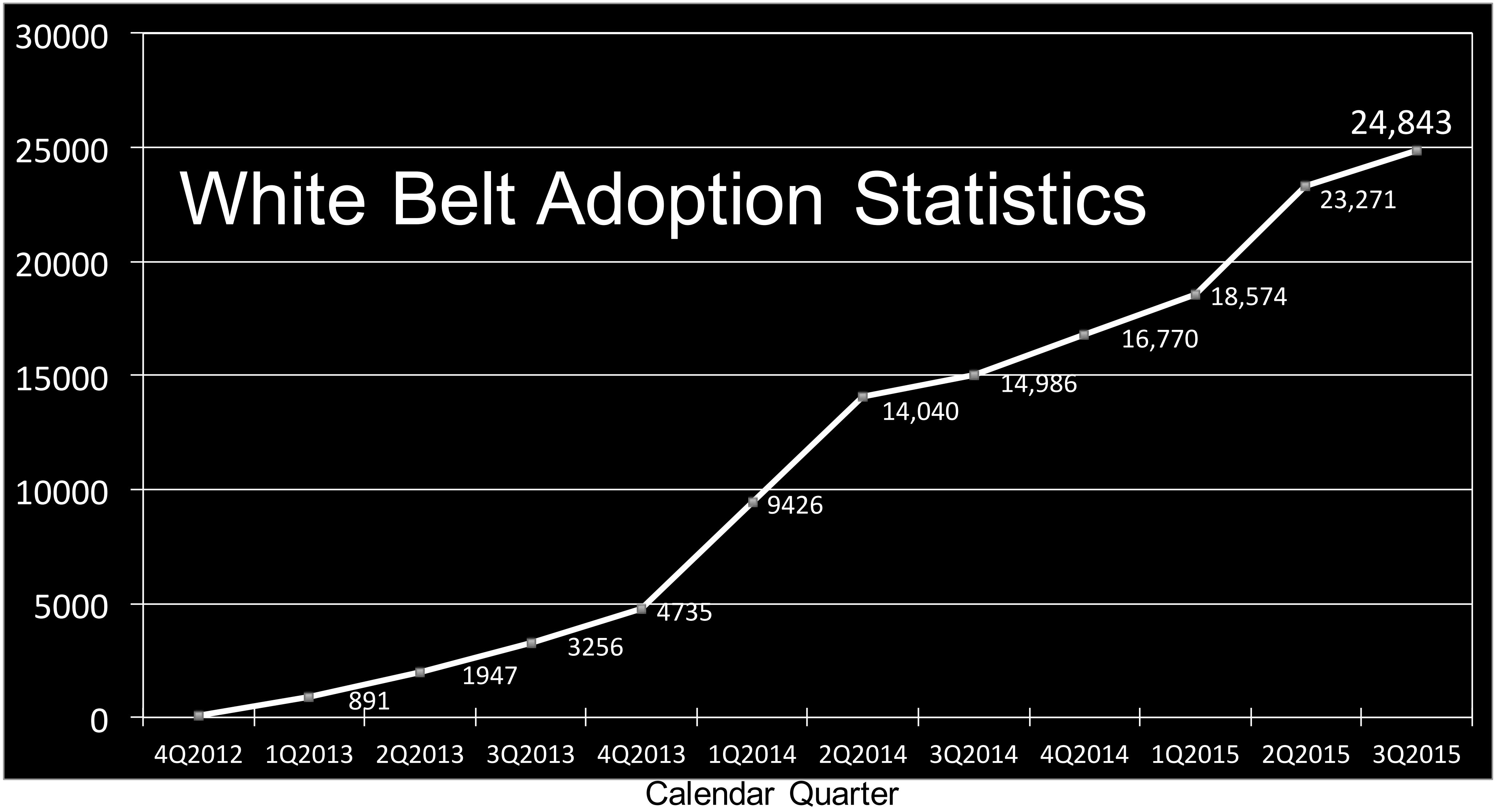
○ Specific thr

Correct

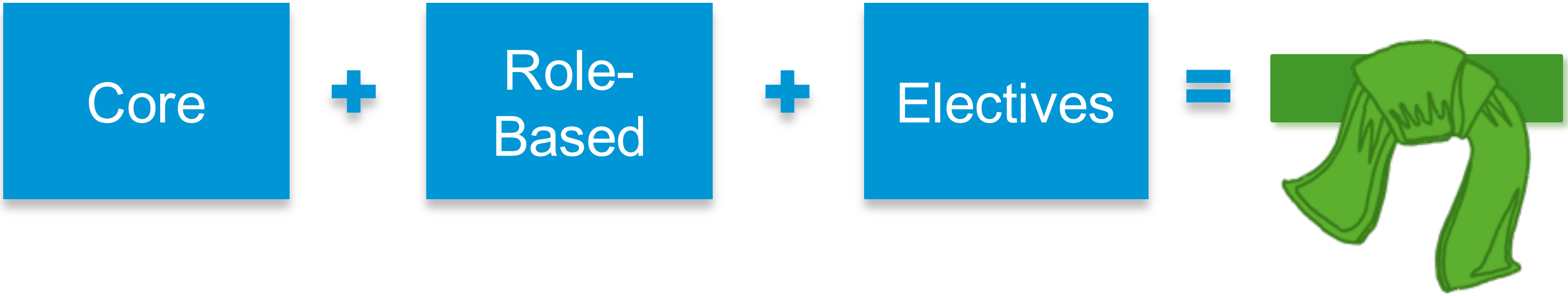
The Model Overview phase of threat modeling uses data flow diagrams to gain a clearer understanding the paths through a system.

Question 5 of 10

White Belt Adoption Statistics

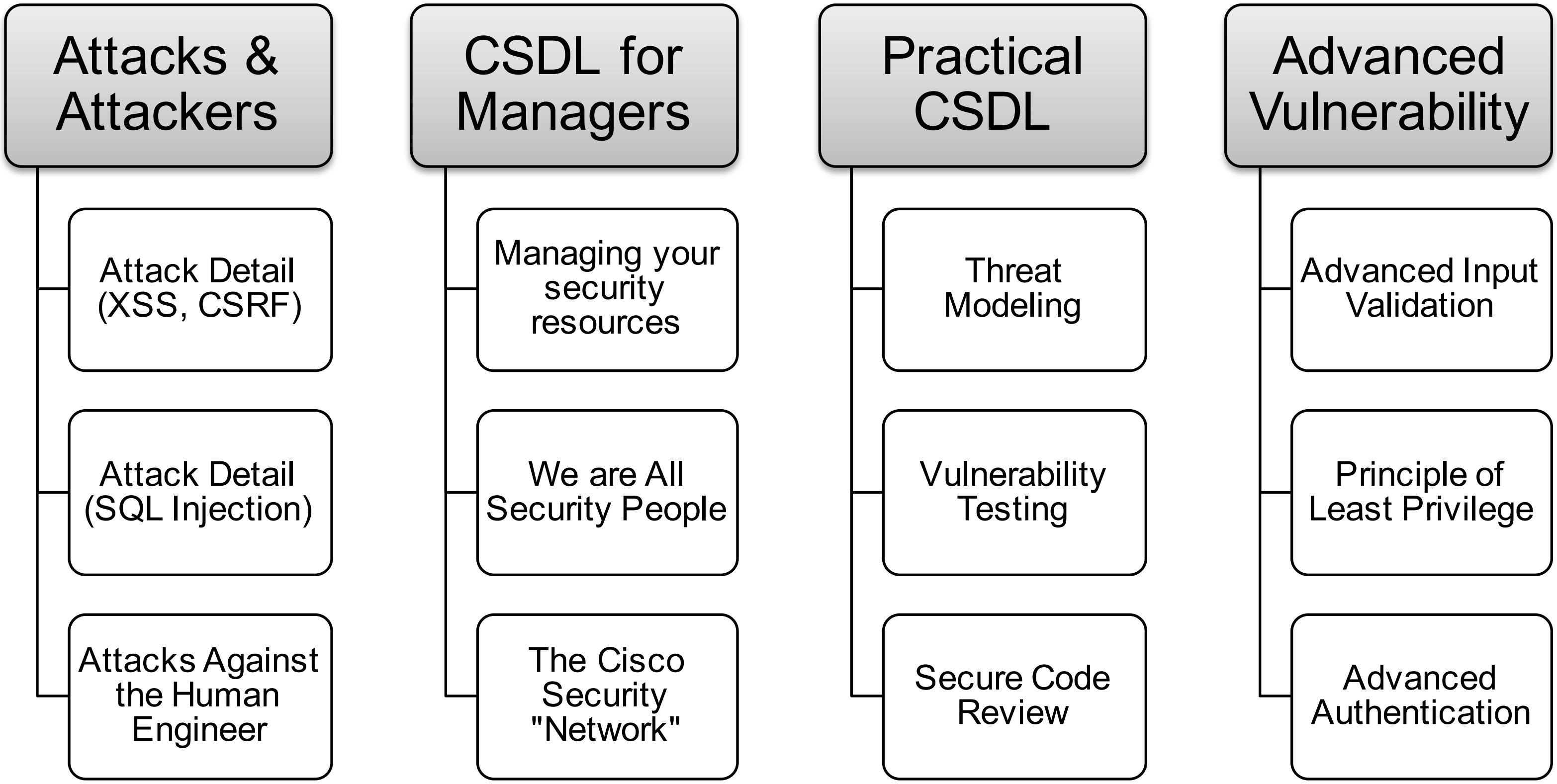


Cisco Security Green Belt



Core + Role-Based + Electives =

Green Belt Core Content



Attacks & Attackers

- Attack Detail (XSS, CSRF)
- Attack Detail (SQL Injection)
- Attacks Against the Human Engineer

CSDL for Managers

- Managing your security resources
- We are All Security People
- The Cisco Security "Network"

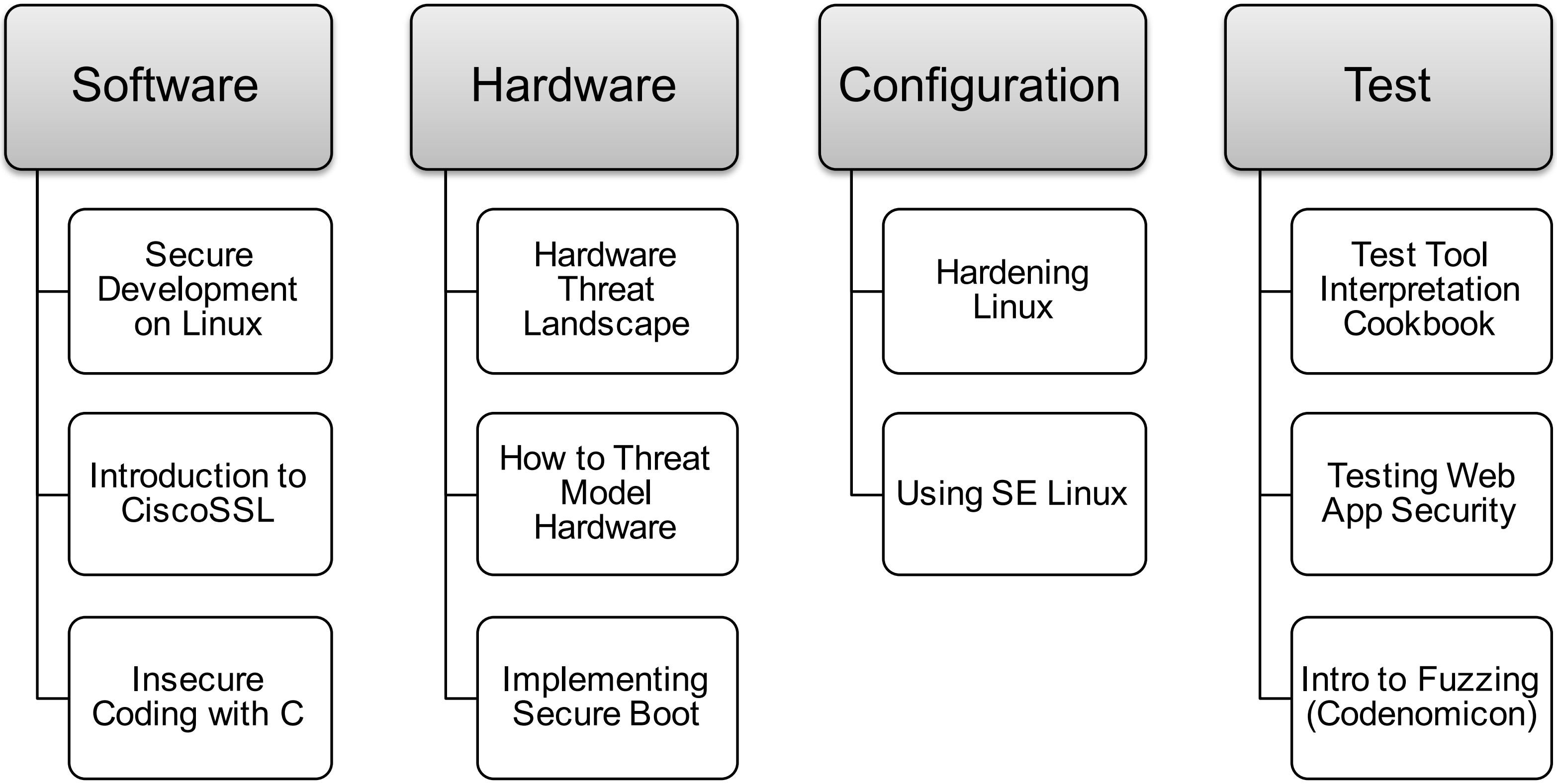
Practical CSDL

- Threat Modeling
- Vulnerability Testing
- Secure Code Review

Advanced Vulnerability

- Advanced Input Validation
- Principle of Least Privilege
- Advanced Authentication

Green Belt Content – Role Specific



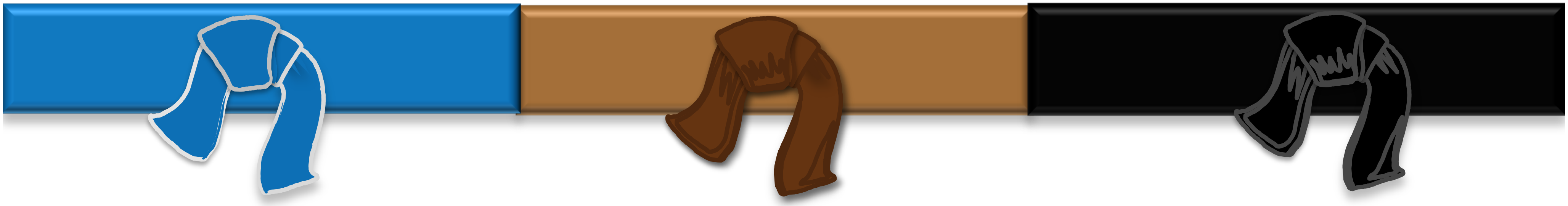
Level 3 Behavior Change: So What?

Behavior	Average Behavior Gap	Percentage of Behavior Increase	Average Confidence Level
Plan and allocate sufficient time for the required CSDL mandated activities	23	58%	78%
Instill a Hacker Mindset in your team's approach to development & testing.	25	51%	78%
Ensure team's knowledge of attack mechanisms in topics relevant work.	23	46%	77%
Execute the mandated CSDL elements in the CPDM Lifecycle in your projects?	21	46%	79%
Ensure that team has "Built security in from the start".	22	46%	75%
Team implements Attack Tools during the development, testing and/or deployment processes	13	36%	68%
Ensure that Threat Modeling takes place	15	33%	71%
Ensure that PSB Gap Analysis takes place?	17	33%	82%
Ensure that team acts in a way that protects Cisco from Social Engineering attacks?	15	27%	73%
Ensure registering Third Party components in IP Central	11	17%	80%
Average	**19**	**39%**	**76%**

L3 Behavior Change: So What (SW Eng)?

Behavior	Average Behavior Gap	Percentage of Behavior Increase	Average Confidence Level
In what percent of your development efforts does your team perform Threat Modeling as part of the product development?	21	53%	67%
How likely were/are you to respond quickly to CIAM alerts to determine if your product is vulnerable to a 3rd-party vulnerability?	25	52%	77%
In what percent of code reviews are security considerations included (for example overflows, cross-site scripting, vulnerabilities, etc)?	22	50%	76%
Rate your success in leveraging CiscoSSL for your product releases.	19	49%	78%
In what percent of your development does your team actively consider which data needs to be stored, the sensitivity of the data, and how data could be misused?	22	45%	79%
In what percent of your development does your team sanitize or encode inputted data before outputting to another component or function?	20	40%	78%
In what percent of your development does your team take advantage of available Run-time Protections to reduce occurrence and impact of buffer overflows?	16	35%	74%
How likely is your team to make sure that the web server of our released products do not run as admin/root user?	19	33%	76%
How likely is your team to make sure that you do NOT write your own security algorithms (i.e. uses Cisco or industry standards)?	17	27%	80%
In what percent of your development does your team consider memory/resource allocation during error conditions in your product?	15	27%	76%
In what percent of your development does your team use parameterized queries using bound, typed parameters in our application to avoid SQL injection?	13	25%	80%
Average	**19**	**39%**	**76%**

Advanced Belts



Complete activities, earn points, and achieve your next belt!

Activities for Blue, Brown, & Black

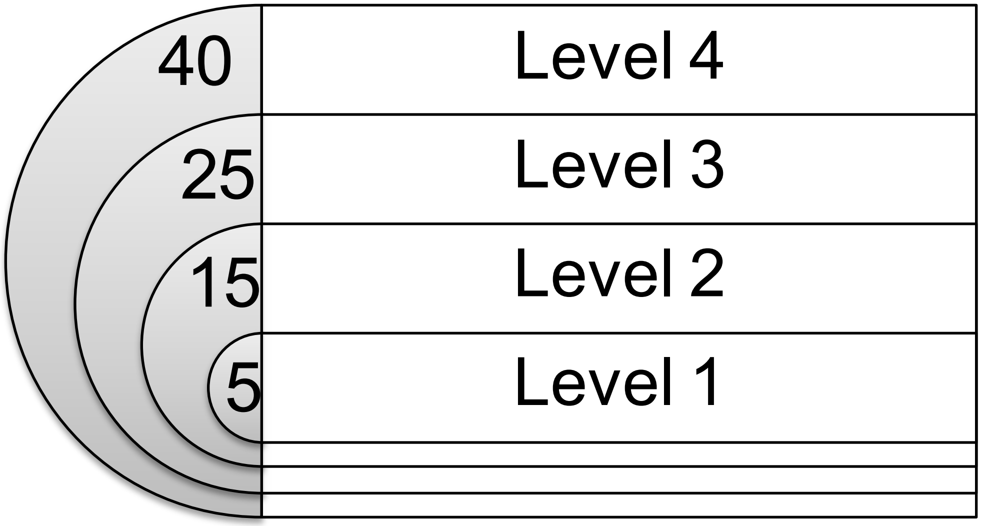
- A security tool or process
- Partnerships
- Security community

- Security issue analysis
- Participate in security committee
- Design / develop security feature

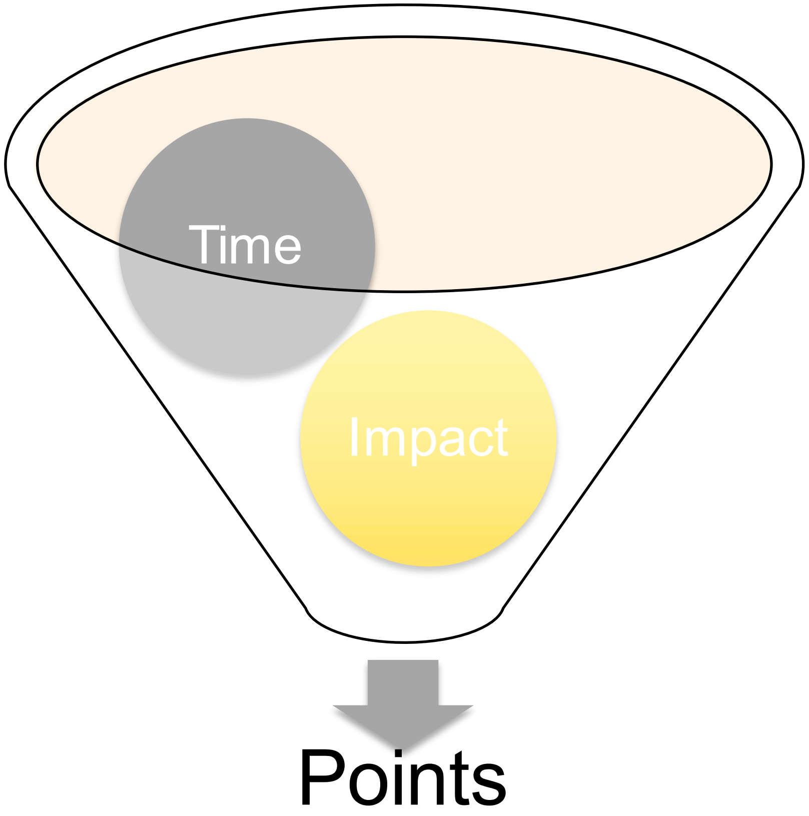
- Taking a security course
- Mentor
- Teach a course
- Deliver presentations

- A security feature
- A security test
- CSDL process
- Security strategy

Levels and Impacts



40	Level 4
25	Level 3
15	Level 2
5	Level 1

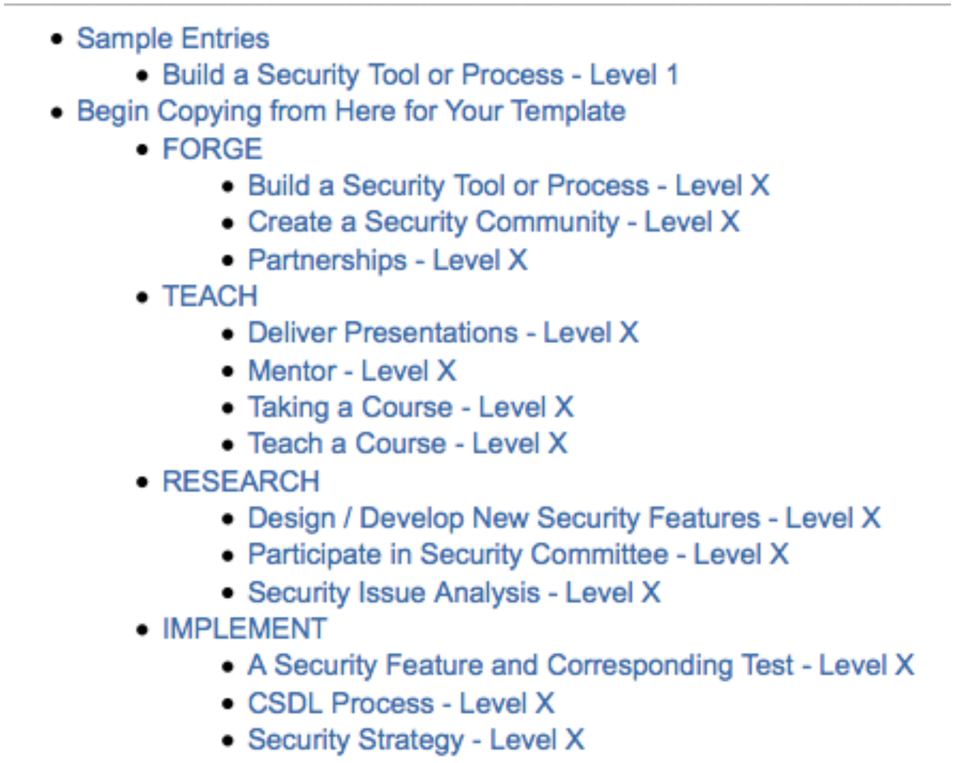


Time

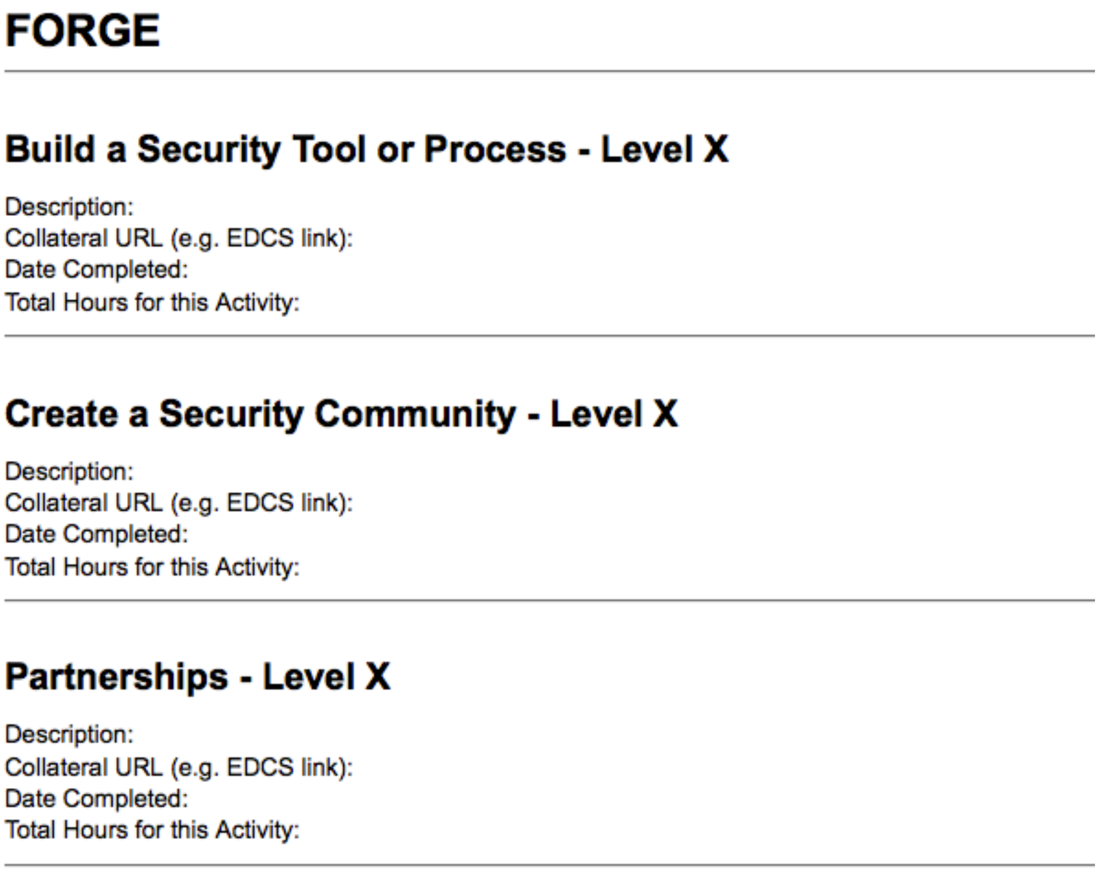
Impact

Points

Tracking Wiki



- Sample Entries
  - Build a Security Tool or Process - Level 1
- Begin Copying from Here for Your Template
  - FORGE
    - Build a Security Tool or Process - Level X
    - Create a Security Community - Level X
    - Partnerships - Level X
  - TEACH
    - Deliver Presentations - Level X
    - Mentor - Level X
    - Taking a Course - Level X
    - Teach a Course - Level X
  - RESEARCH
    - Design / Develop New Security Features - Level X
    - Participate in Security Committee - Level X
    - Security Issue Analysis - Level X
  - IMPLEMENT
    - A Security Feature and Corresponding Test - Level X
    - CSDL Process - Level X
    - Security Strategy - Level X



FORGE

Build a Security Tool or Process - Level X

Description:
Collateral URL (e.g. EDCS link):
Date Completed:
Total Hours for this Activity:

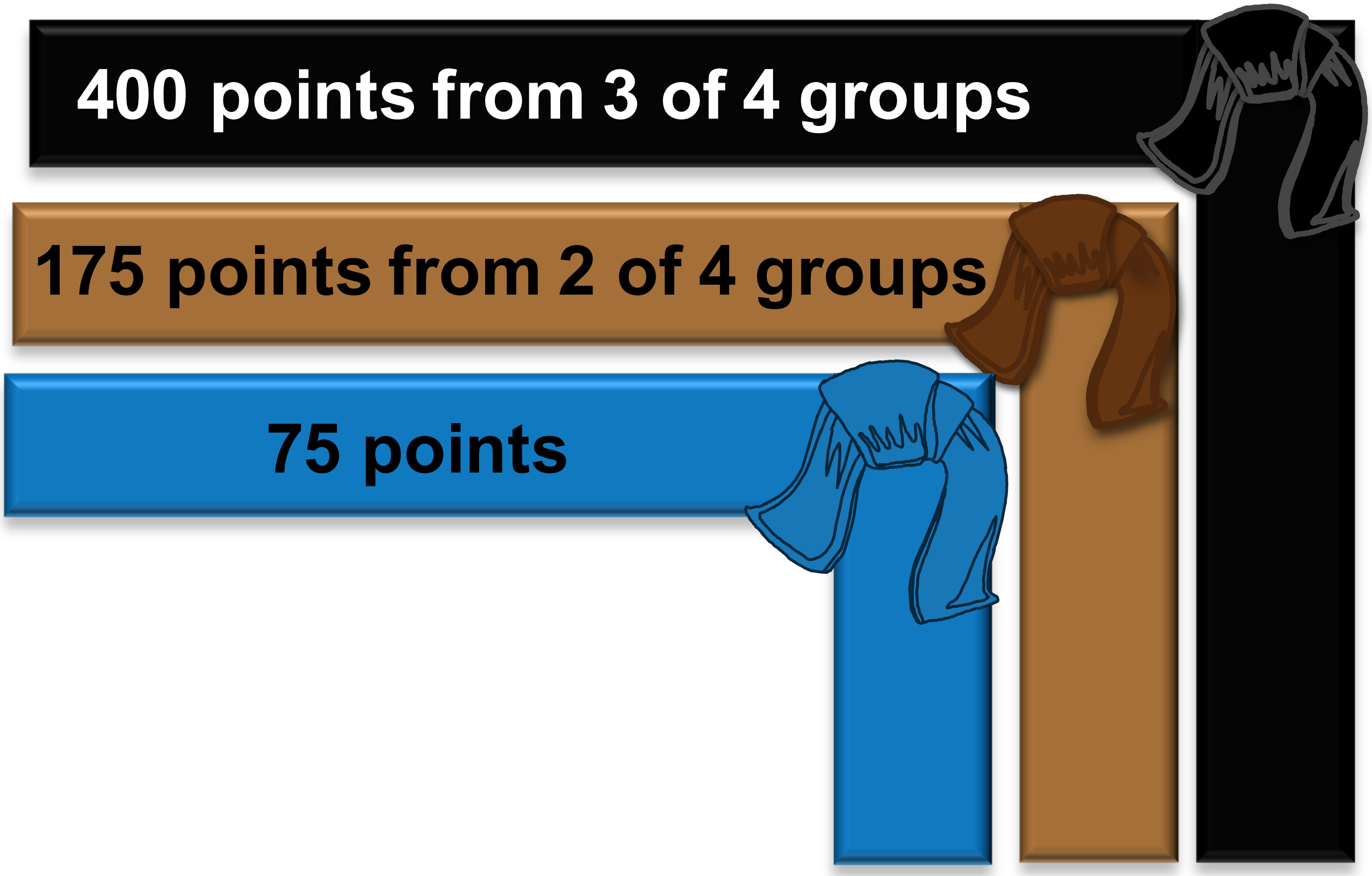
Create a Security Community - Level X

Description:
Collateral URL (e.g. EDCS link):
Date Completed:
Total Hours for this Activity:

Partnerships - Level X

Description:
Collateral URL (e.g. EDCS link):
Date Completed:
Total Hours for this Activity:

Cumulative Points by Belt



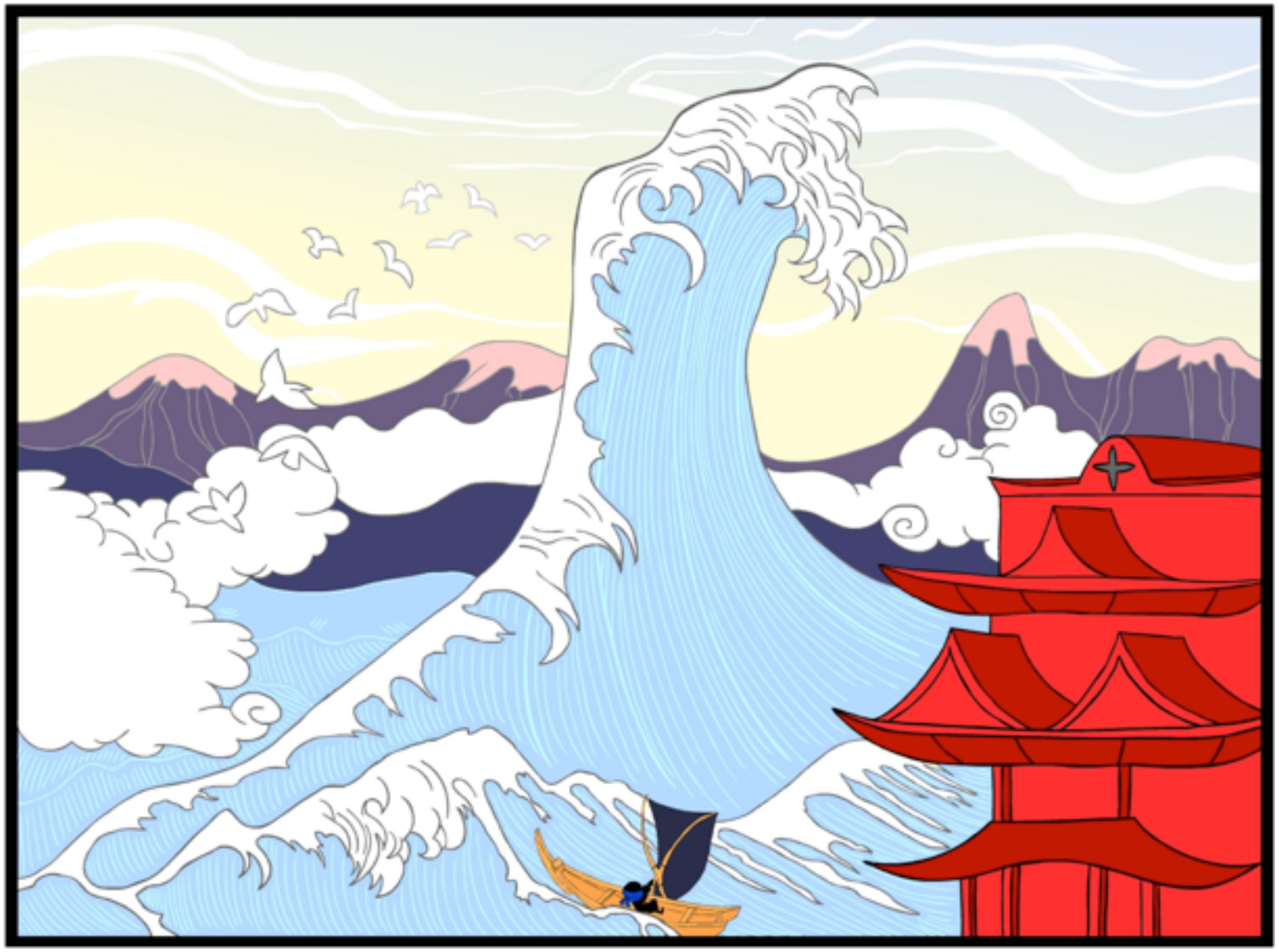
400 points from 3 of 4 groups

175 points from 2 of 4 groups

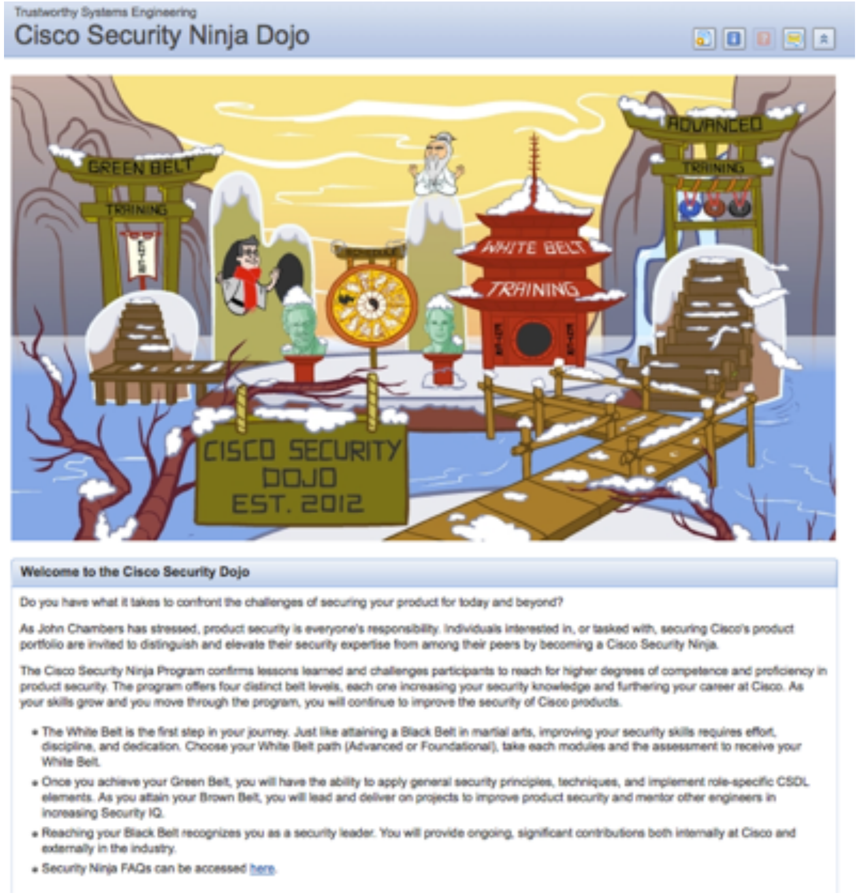
75 points

Activity	Total
Taking a Course	581
Deliver Presentations	338
Build a Security Tool or Process	265
A Security Feature and Corresponding Test	232
Security Issue Analysis	189
CSDL Process	181
Mentor	165
Participate in Security Committee	144
Partnerships	143
Create a Security Community	114
Security Strategy	102
Teach a Course	77
Design / Develop New Security Features	76
Total	2607

The Tidal Wave of Security Culture Change



The Cisco Security Dojo



Trustworthy Systems Engineering

Cisco Security Ninja Dojo

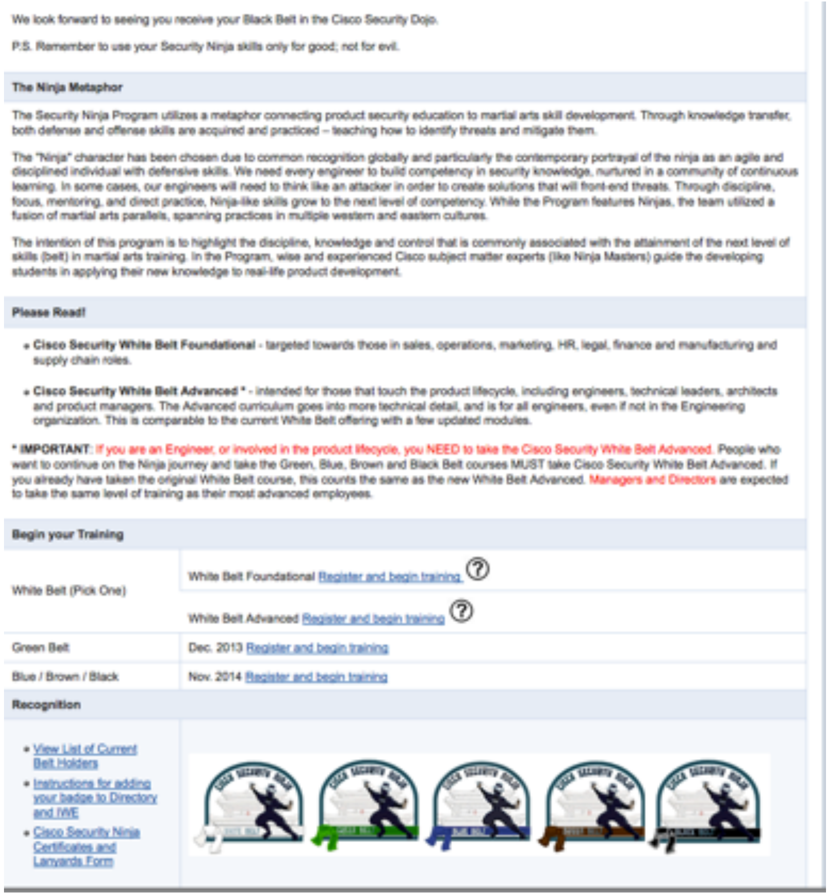
Welcome to the Cisco Security Dojo

Do you have what it takes to confront the challenges of securing your product for today and beyond?

As John Chambers has stressed, product security is everyone's responsibility. Individuals interested in, or tasked with, securing Cisco's product portfolio are invited to distinguish and elevate their security expertise from among their peers by becoming a Cisco Security Ninja.

The Cisco Security Ninja Program confirms lessons learned and challenges participants to reach for higher degrees of competence and proficiency in product security. The program offers four distinct belt levels, each one increasing your security knowledge and furthering your career at Cisco. As your skills grow and you move through the program, you will continue to improve the security of Cisco products.

- The White Belt is the first step in your journey. Just like attaining a Black Belt in martial arts, improving your security skills requires effort, discipline, and dedication. Choose your White Belt path (Advanced or Foundational), take each modules and the assessment to receive your White Belt.
- Once you achieve your Green Belt, you will have the ability to apply general security principles, techniques, and implement role-specific CSDL elements. As you attain your Brown Belt, you will lead and deliver on projects to improve product security and mentor other engineers in increasing Security IQ.
- Reaching your Black Belt recognizes you as a security leader. You will provide ongoing, significant contributions both internally at Cisco and externally in the industry.
- Security Ninja FAQs can be accessed here.



We look forward to seeing you receive your Black Belt in the Cisco Security Dojo.

P.S. Remember to use your Security Ninja skills only for good; not for evil.

The Ninja Metaphor

The Security Ninja Program utilizes a metaphor connecting product security education to martial arts skill development. Through knowledge transfer, both defense and offense skills are acquired and practiced – teaching how to identify threats and mitigate them.

The "Ninja" character has been chosen due to common recognition globally and particularly the contemporary portrayal of the ninja as an agile and disciplined individual with defensive skills. We need every engineer to build competency in security knowledge, nurtured in a community of continuous learning. In some cases, our engineers will need to think like an attacker in order to create solutions that will front-end threats. Through discipline, focus, mentoring, and direct practice, Ninja-like skills grow to the next level of competency. While the Program features Ninjas, the team utilized a fusion of martial arts parallels, spanning practices in multiple western and eastern cultures.

The intention of this program is to highlight the discipline, knowledge and control that is commonly associated with the attainment of the next level of skills (belt) in martial arts training. In the Program, wise and experienced Cisco subject matter experts (like Ninja Masters) guide the developing students in applying their new knowledge to real-life product development.

Please Read!

- **Cisco Security White Belt Foundational** - targeted towards those in sales, operations, marketing, HR, legal, finance and manufacturing and supply chain roles.
- **Cisco Security White Belt Advanced *** - intended for those that touch the product lifecycle, including engineers, technical leaders, architects and product managers. The Advanced curriculum goes into more technical detail, and is for all engineers, even if not in the Engineering organization. This is comparable to the current White Belt offering with a few updated modules.

* **IMPORTANT**: If you are an Engineer, or involved in the product lifecycle, you NEED to take the Cisco Security White Belt Advanced. People who want to continue on the Ninja journey and take the Green, Blue, Brown and Black Belt courses MUST take Cisco Security White Belt Advanced. If you already have taken the original White Belt course, this counts the same as the new White Belt Advanced. Managers and Directors are expected to take the same level of training as their most advanced employees.

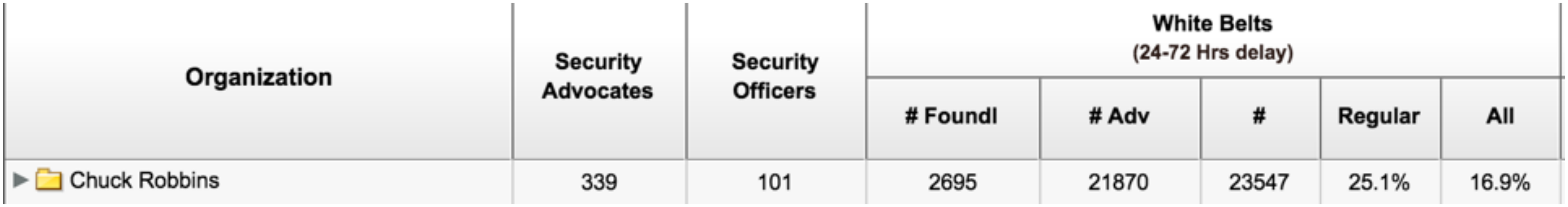
Begin your Training

White Belt (Pick One)	White Belt Foundational Register and begin training ⓘ
	White Belt Advanced Register and begin training ⓘ
Green Belt	Dec. 2013 Register and begin training
Blue / Brown / Black	Nov. 2014 Register and begin training

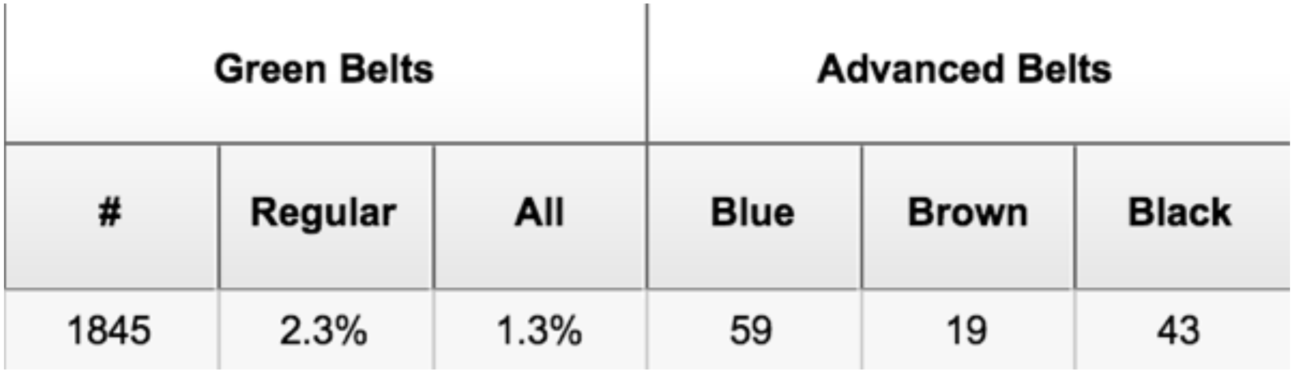
Recognition

- View List of Current Belt Holders
- Instructions for adding your badge to Directory and IWE
- Cisco Security Ninja Certificates and Lanyards Form

Security Insights Dashboard



Organization	Security Advocates	Security Officers	White Belts (24-72 Hrs delay)				
			# Foundl	# Adv	#	Regular	All
▶ Chuck Robbins	339	101	2695	21870	23547	25.1%	16.9%



Green Belts			Advanced Belts		
#	Regular	All	Blue	Brown	Black
1845	2.3%	1.3%	59	19	43

Secrets of Success

Secret of Success #1: 20 Minute Modules

- Keep each module to 20 minute maximum, but 10 is even better.

  - ◆ Application: Argue about the required content, then edit and reduce it, and ensure your production team understands the time constraints and keeps you honest!

Secret of Success #2: Subject Matter Expertise

- Collaborative pool of subject matter experts – include them in content creation & recording
  - Application: Start with a small pilot and invite well known security people from your organization to partner in creating a module
  - Application: If your org is smaller, find 1-5 key partners

~ 100 contributors

~ 500 contributors

Secret of Success #3: Recognition

- The 3 R’s: Recognition, Recognition, Recognition

◆ Application: Analyze your organization and create a recognition program using all your available corporate assets

Secret of Success #4: Gone Viral

- Viral nature of training

◆ Application: Build recognition processes to encourage your program to go viral; communicate with each manager when a team member earns a belt.

Secret of Success #5: Hire Instructional Design Help

- Test questions are HARD to write

  - Application: Use expert, Instructional Designers for creation of assessments

Secret of Success #6: Competition

- Built in competition amongst teams and Exec's

◆ Application: Exec's are competitive; build a dashboard that publicizes the statistics of each exec (number of belts, percentage).

Secret of Success #7: Break All the Rules

- Did not know the rules of classical learning & development, so we didn't follow them

  - ◆ Application: Avoid "we always do training this way", or "this is how the experts say to do it". Be creative and have fun. If you are having fun delivering, people will enjoy consuming.

Secret of Success #8: Creative People

- Creative video team (Cisco TV) that "gets" our concept and helps us to capture it

- ◆ Application: Partner with creative people that understand your vision and will help you to achieve it

Secret of Success #9: Executive Buy-In

- Senior Executive buy-in

  - ◆ Application: Pilot first, build momentum, and then ask for the world

Secret of Success #10: Gamification

- The interface is setup like a game, allowing learners to achieve and receive visual feedback.

- ◆ Application: Realize the importance to current generation of learners, be creative, make an interface that you would like to use

Secrets of Success: Summary

1. 20 Minute Modules
2. Subject Matter Expertise
3. Recognition
4. Gone Viral
5. Hire Instructional Design Help
6. Competition
7. Break All the Rules
8. Creative People
9. Executive Buy-In

10.Gamification

Security is a Journey

23,620
25.2 % of
regular
Cisco
employees
59.2 % of
Eng
employees

3916 Green Belts
3478 Unique
Learners
Software – 2024
Manager – 946
Test – 804
Hardware - 142

174 Blue
Belts

55 Brown
Belts

55 Black
Belts

Conclusions

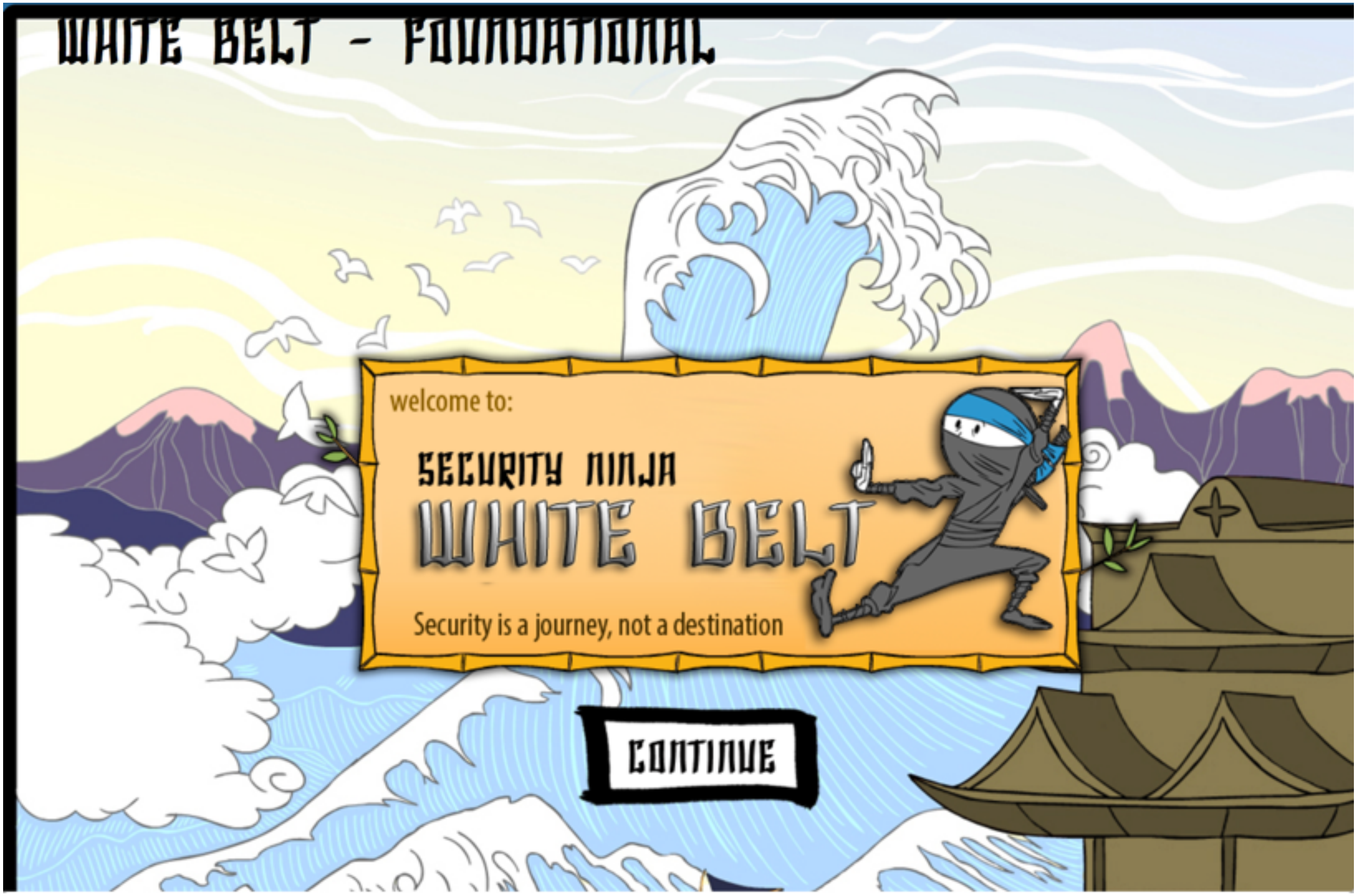
- Application Security Awareness
  - Knowledge, Historical, Action
- Not a blue print, but an example to learn from
  - Each culture is different, each company is different
  - Content, Metaphor, and Recognition
- Call to Action: You can build this for your company

Resources

- http://blogs.cisco.com/security/the-cisco-security-dojo
- Sample Module, highlighting our content approach
  - https://cisco.box.com/Cisco-Security-Ninja-Sample
- Single Module focused on Net / Sec Eng
  - https://cisco.box.com/Cisco-Ninja-Net-Eng
- Ninja Episode
  - http://www.cisco.com/go/tacsecuritypodcast

Questions & Answers

- Chris Romeo, CEO / Principal Consultant
- chris_romeo@securityjourney.com
- www.securityjourney.com
- (888) 637-5815
- @edgeroute



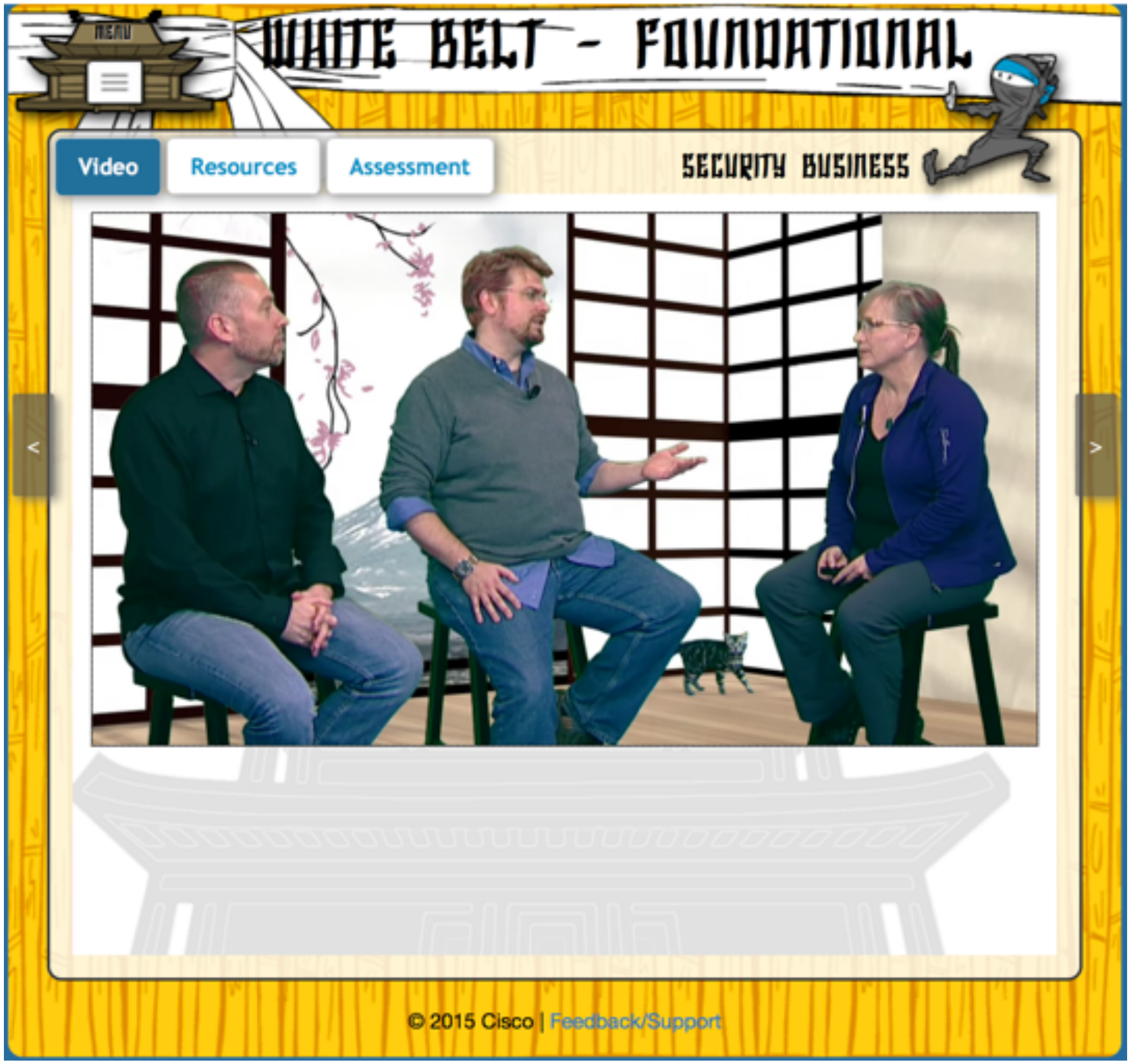
WHITE BELT - FOUNDATIONAL

welcome to:

SECURITY NINJA

WHITE BELT

Security is a journey, not a destination

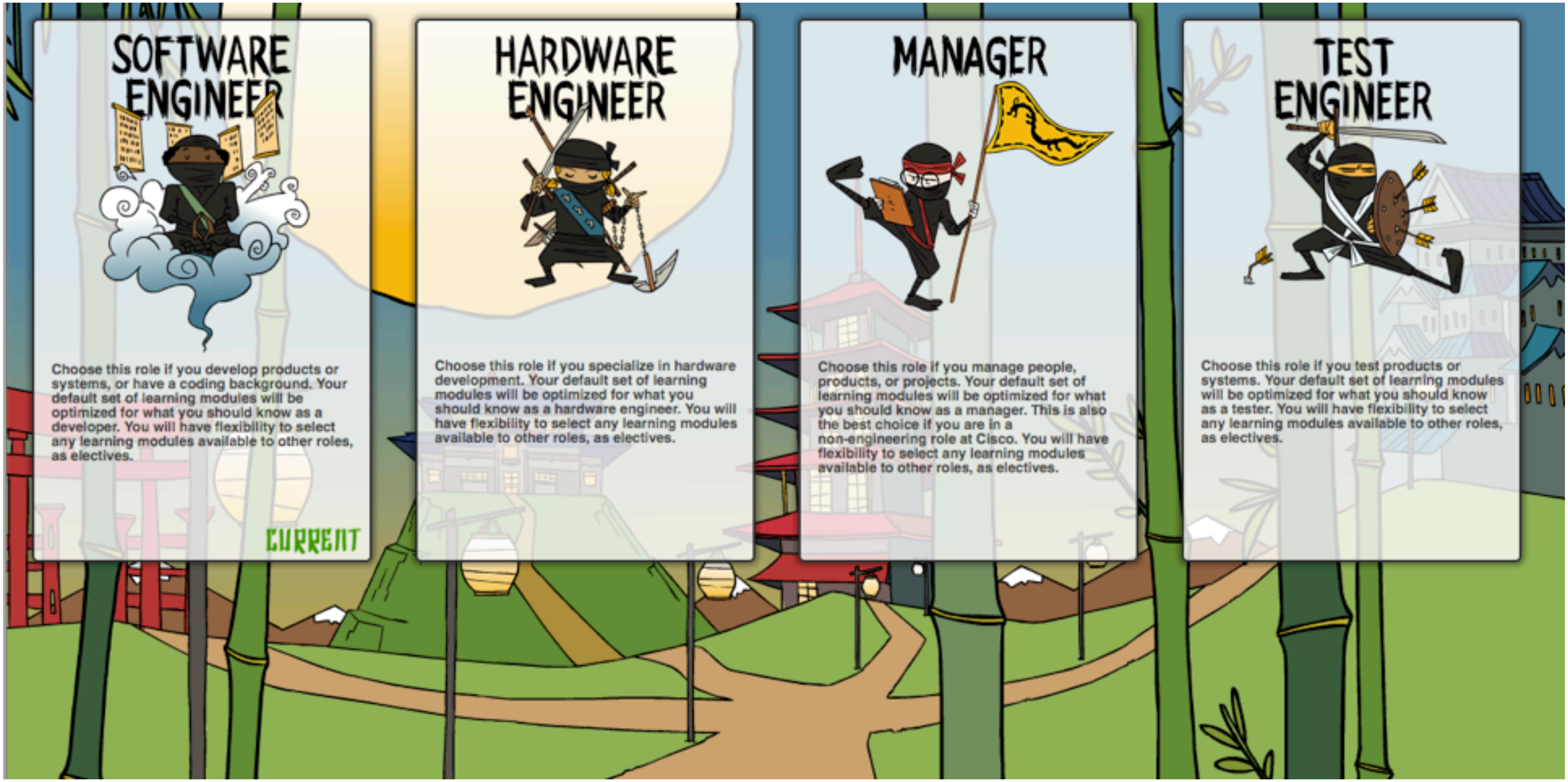

MENU
WHITE BELT - FOUNDATIONAL
Video
Resources
Assessment
SECURITY BUSINESS
<
>
© 2015 Cisco | Feedback/Support

welcome to:

SECURITY NINJA

GREEN BELT

Security is a journey, not a destination



SOFTWARE ENGINEER

Choose this role if you develop products or systems, or have a coding background. Your default set of learning modules will be optimized for what you should know as a developer. You will have flexibility to select any learning modules available to other roles, as electives.

HARDWARE ENGINEER

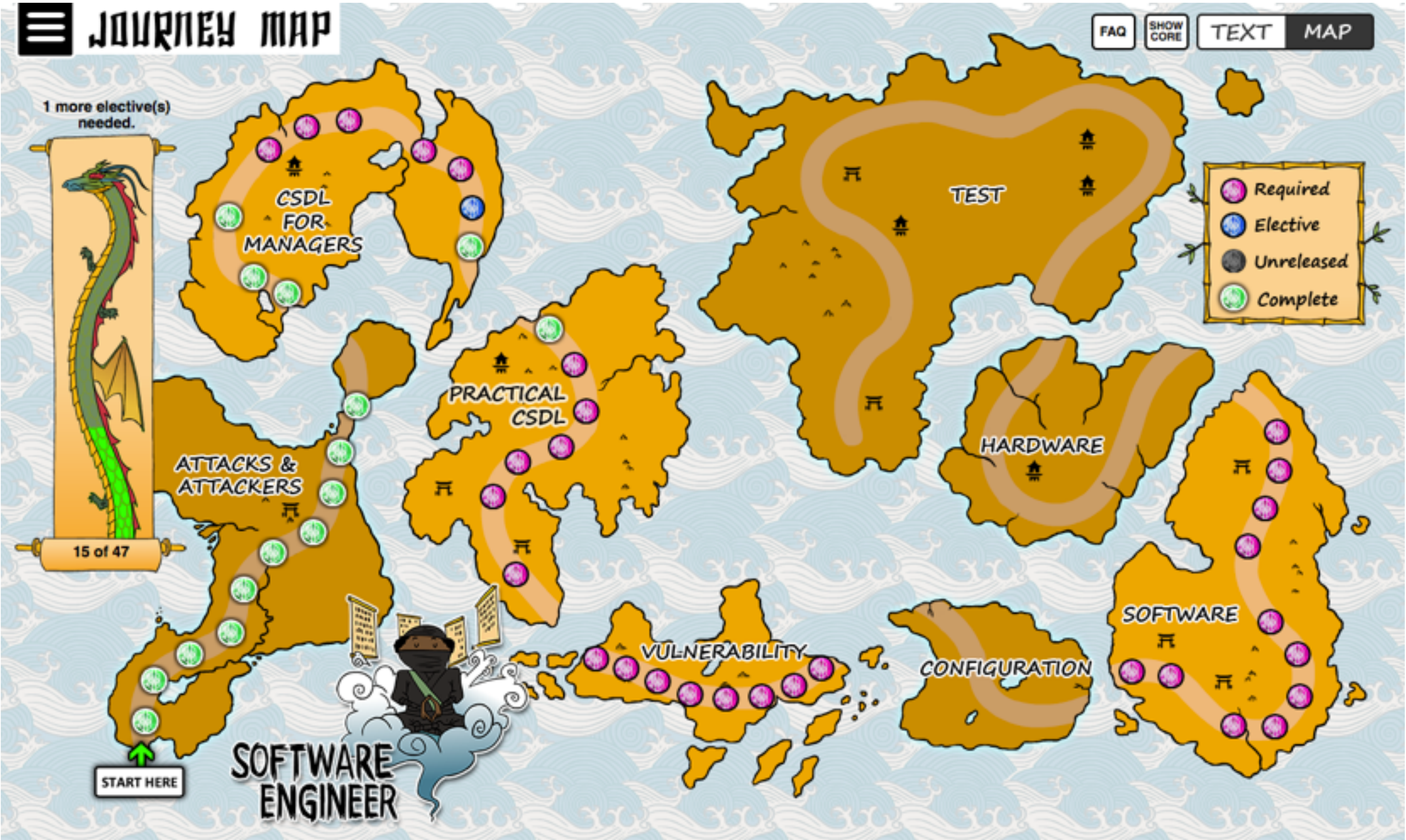
Choose this role if you specialize in hardware development. Your default set of learning modules will be optimized for what you should know as a hardware engineer. You will have flexibility to select any learning modules available to other roles, as electives.

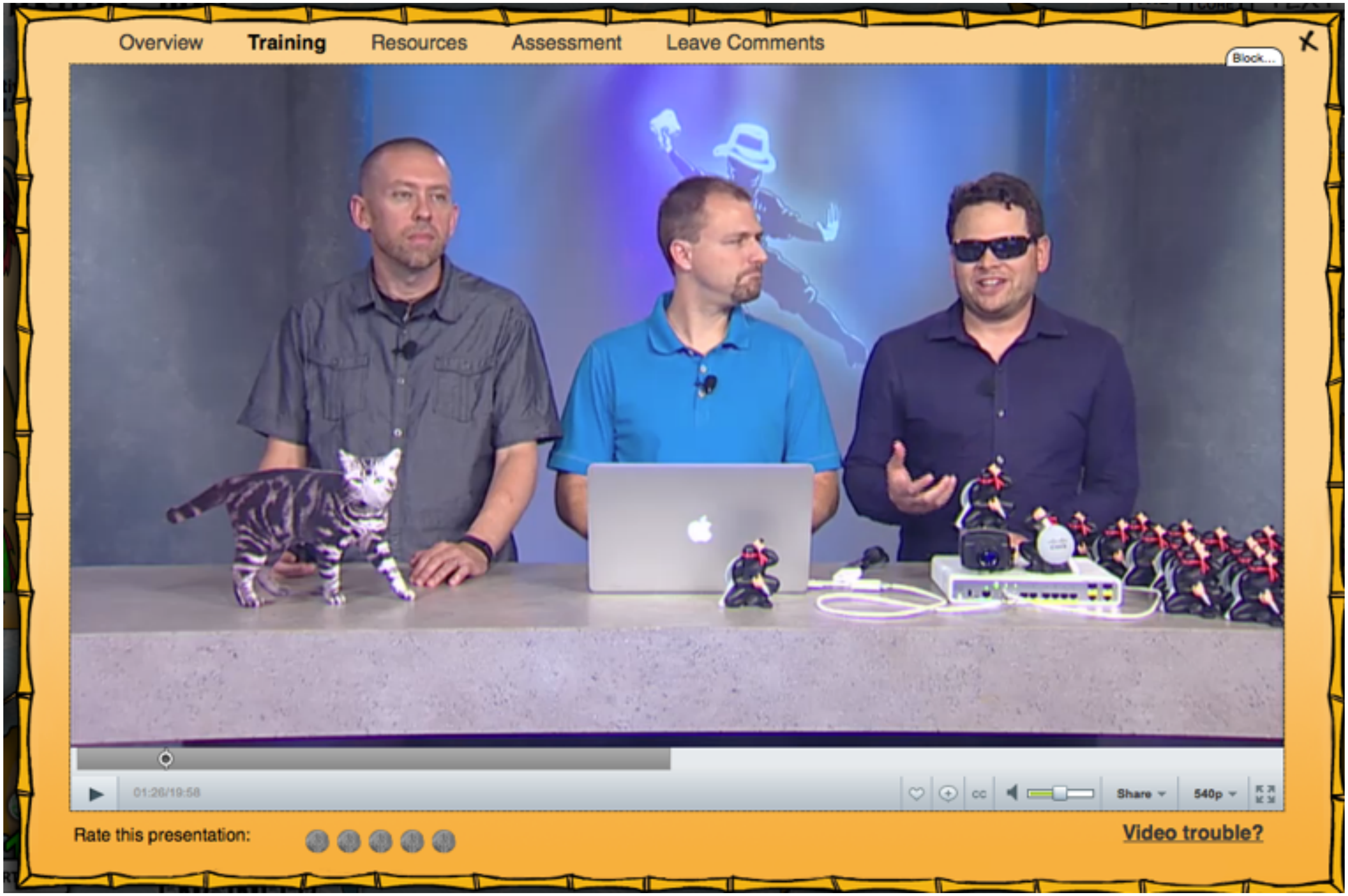
MANAGER

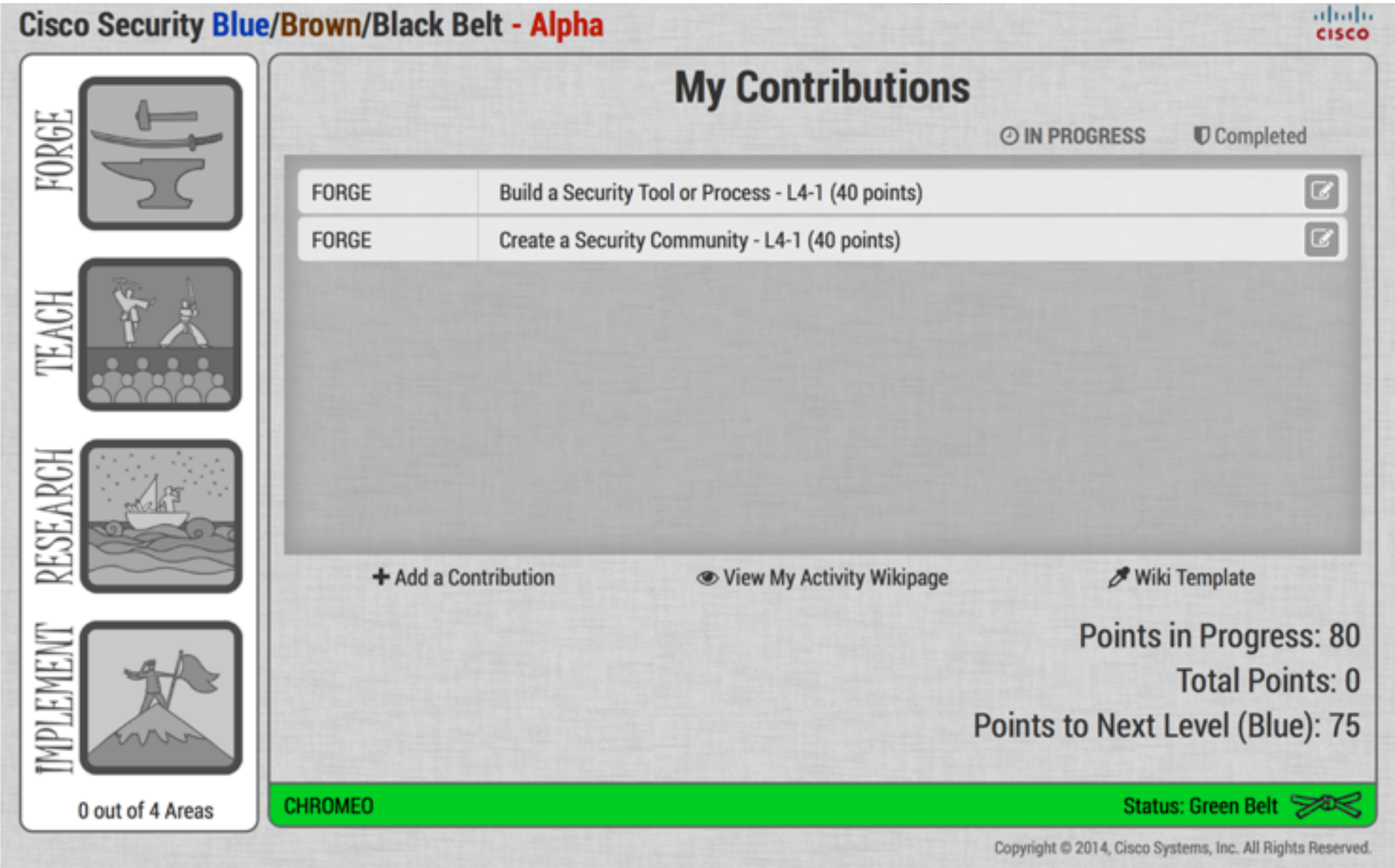
Choose this role if you manage people, products, or projects. Your default set of learning modules will be optimized for what you should know as a manager. This is also the best choice if you are in a non-engineering role at Cisco. You will have flexibility to select any learning modules available to other roles, as electives.

TEST ENGINEER

Choose this role if you test products or systems. Your default set of learning modules will be optimized for what you should know as a tester. You will have flexibility to select any learning modules available to other roles, as electives.


JOURNEY MAP
FAQ
SHOW CORE
TEXT
MAP
1 more elective(s) needed.
15 of 47
CSDL FOR MANAGERS
ATTACKS & ATTACKERS
PRACTICAL CSDL
TEST
HARDWARE
VULNERABILITY
CONFIGURATION
SOFTWARE
Required
Elective
Unreleased
Complete
START HERE
SOFTWARE ENGINEER


Overview
Training
Resources
Assessment
Leave Comments
Block...
01:26/19:58
CC
Share
540p
Rate this presentation:
Video trouble?



Cisco Security Blue/Brown/Black Belt - Alpha

0 out of 4 Areas

My Contributions

FORGE	Build a Security Tool or Process - L4-1 (40 points)
FORGE	Create a Security Community - L4-1 (40 points)

Points in Progress: 80

Total Points: 0

Points to Next Level (Blue): 75

CHROMEO

Status: Green Belt

Thank you.