RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: HUM-T08

Cisco's Security Dojo: Raising the Technical Security Awareness of 20,000+

Chris Romeo

Chief Security Advocate
Cisco Systems
@edgeroute

Would you believe we reached 20K 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

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Content, Metaphor, and Recognition

#RSAC

Once upon a time…

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

Application Security Awareness

1. Knowledge

Application Security Awareness

3. Action

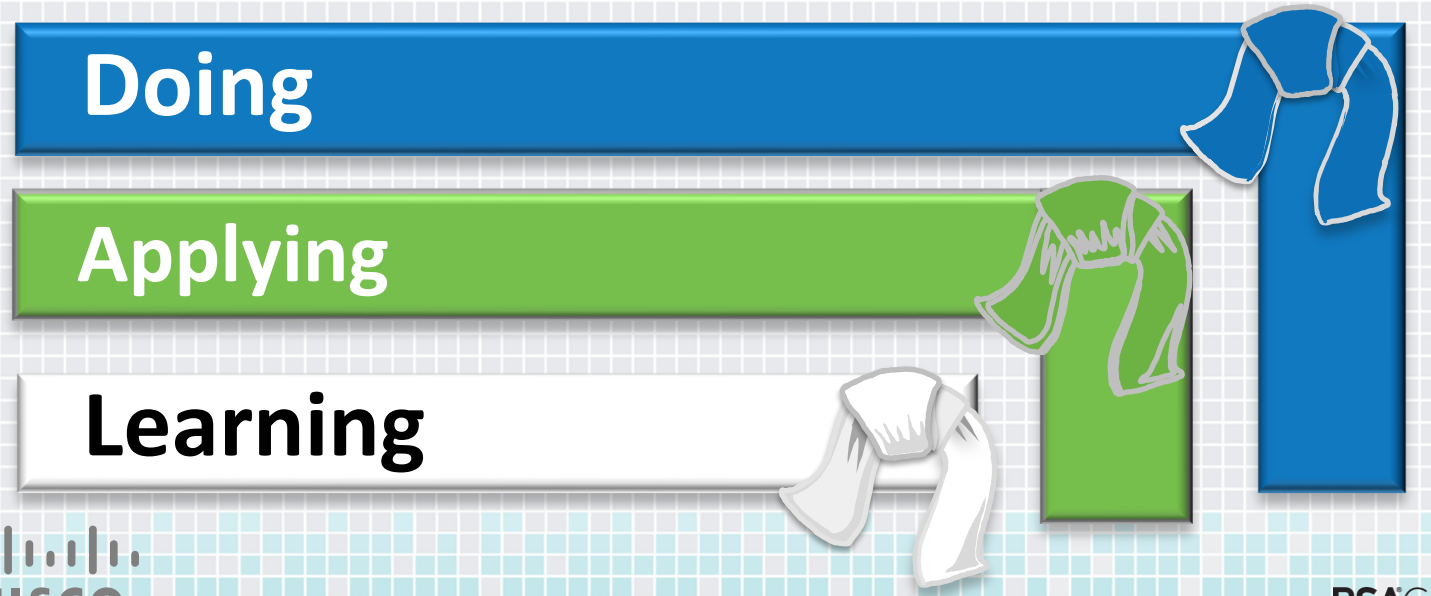
2. Historical

PSIRT

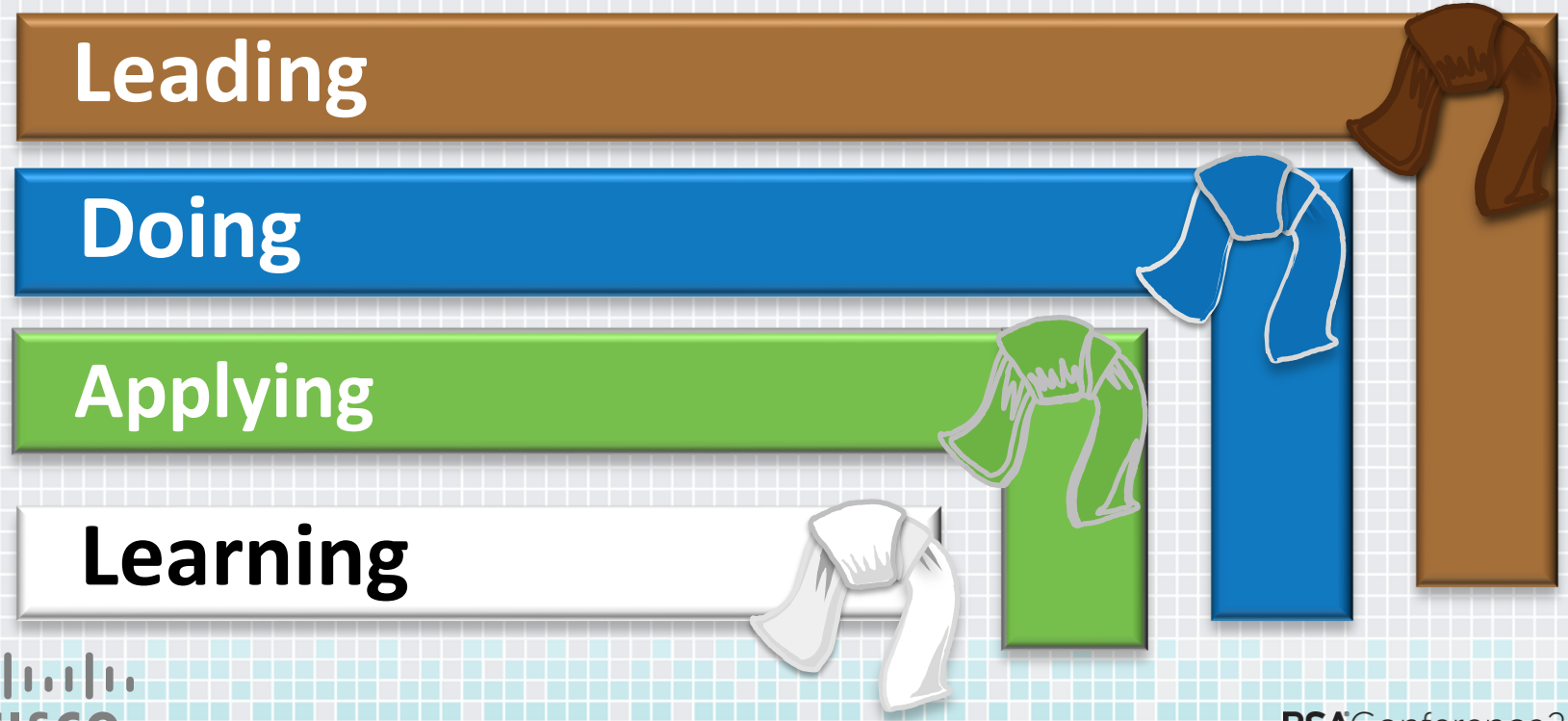
Cisco Security White Belt

Cisco Security Green Belt

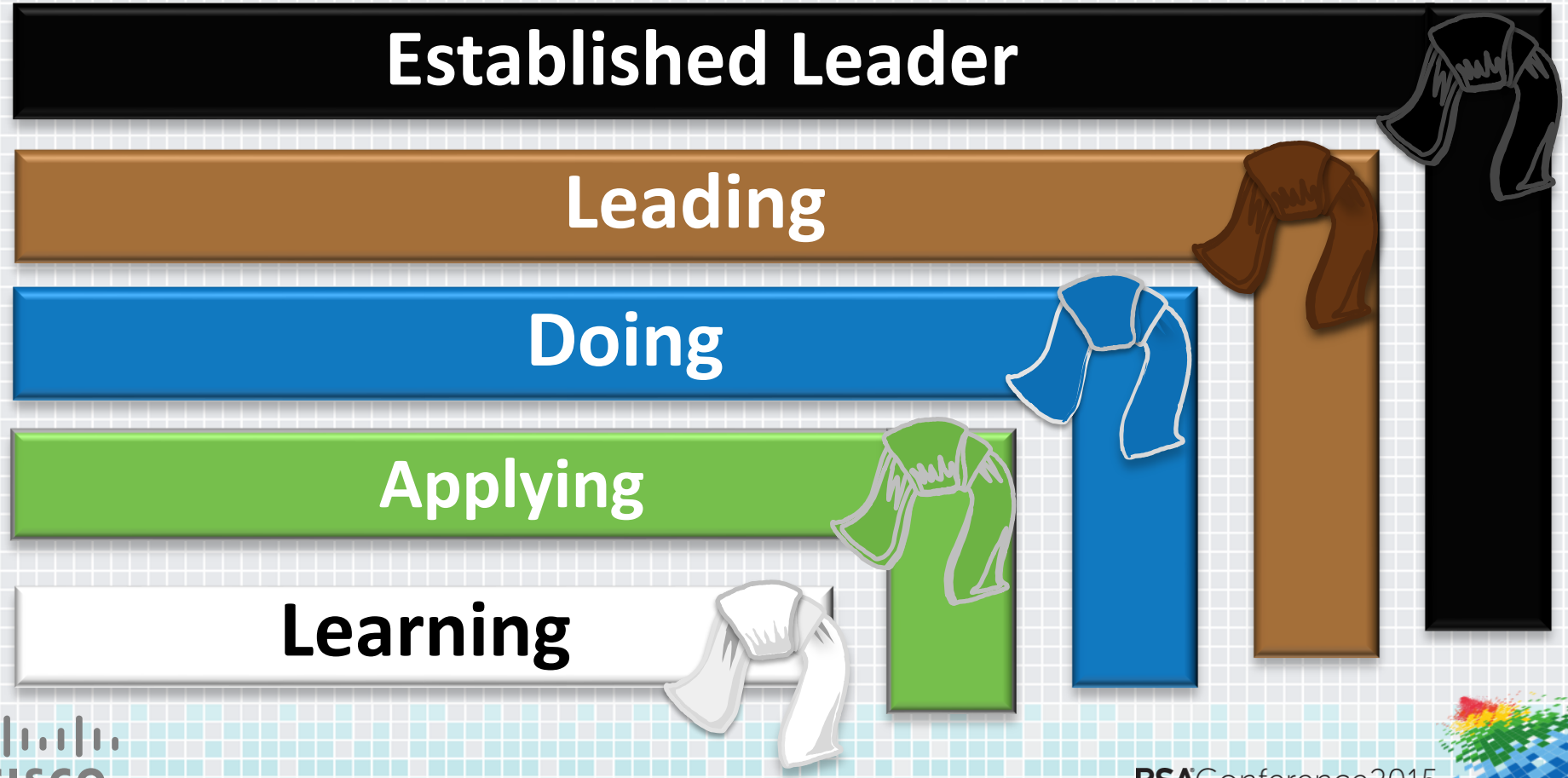
Cisco Security Blue Belt



Cisco Security Brown Belt



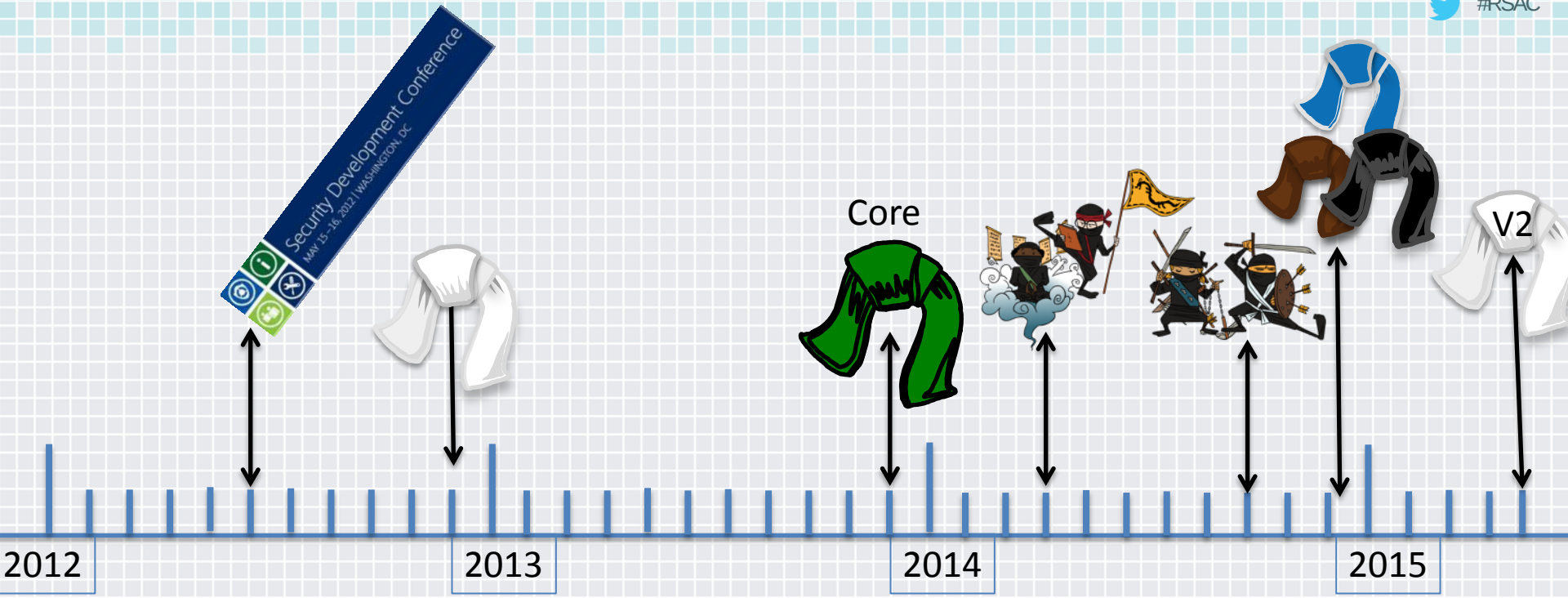
Cisco Security Black Belt



Content Delivery

Security Metaphors

Recognition

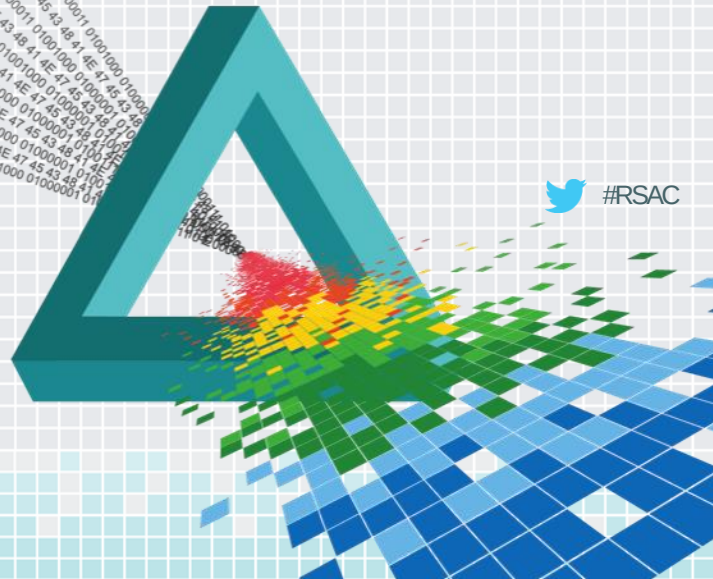


Program Timeline

RSAConference2015

San Francisco | April 20-24 | Moscone Center

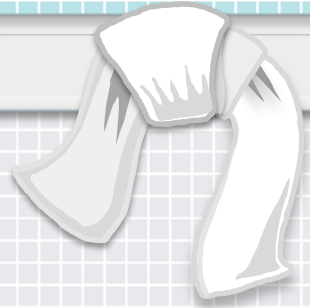
Video



Cisco Security White Belt

Foundational Modules

- 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



Basic Vulnerability Series

Input Validation

Resource Exhaustion

Authentication

Authorization

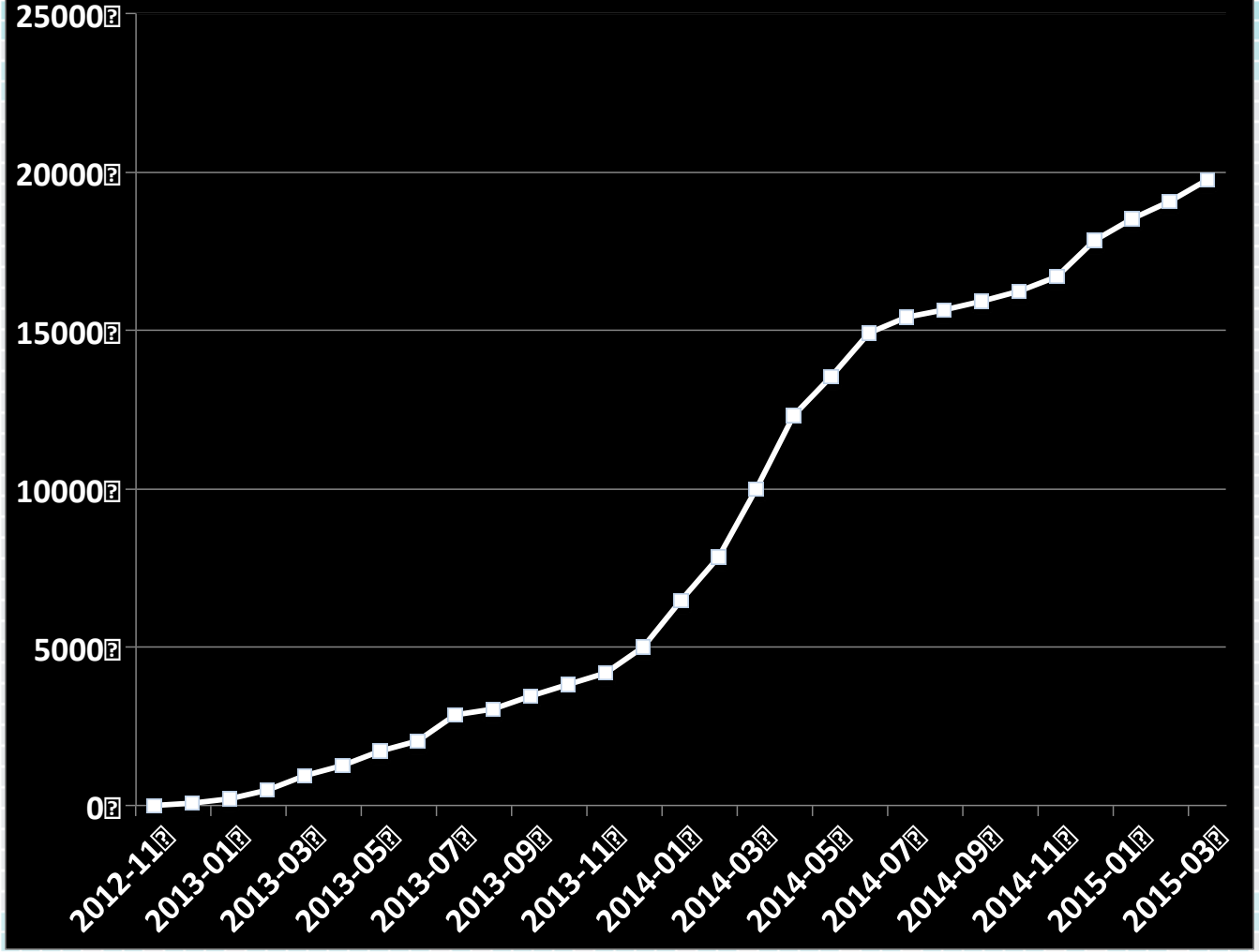
Configuration

Information Leakage

Hardware

Cryptography

White Belt Adoption



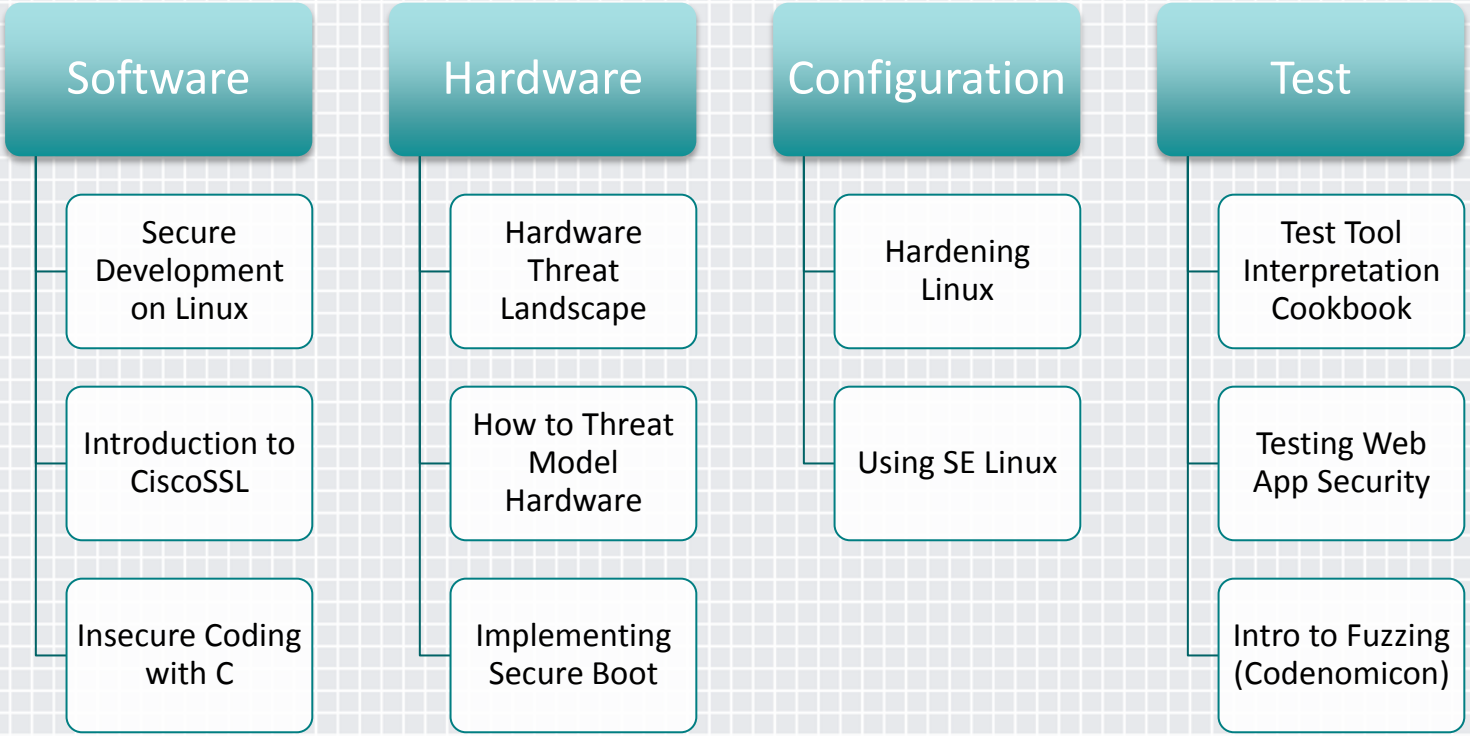
Cisco Security Green Belt

Core + Role-Based + Electives =

Green Belt Core Content

Attacks & Attackers	CSDL for Managers	Practical CSDL	Advanced Vulnerability
Attack Detail (XSS, CSRF)	Managing your security resources	Threat Modeling	Advanced Input Validation
Attack Detail (SQL Injection)	We are All Security People	Vulnerability Testing	Principle of Least Privilege
Attacks Against the Human Engineer	The Cisco Security "Network"	Secure Code Review	Advanced Authentication

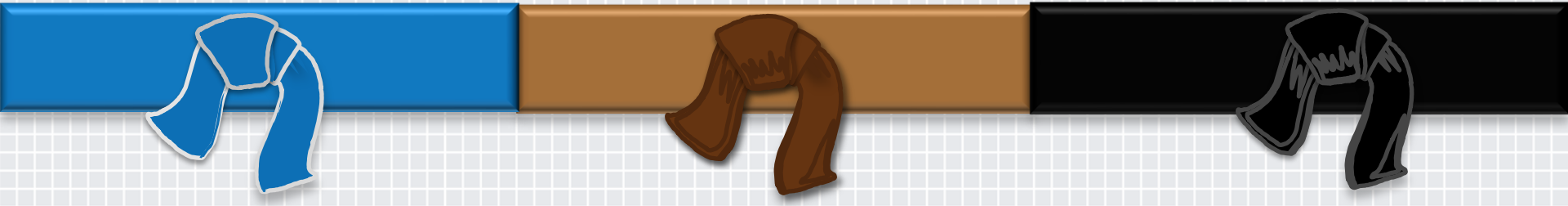
Green Belt Content – Role Specific



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%**

Advanced Belts



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

Activities for Blue, Brown, & Black

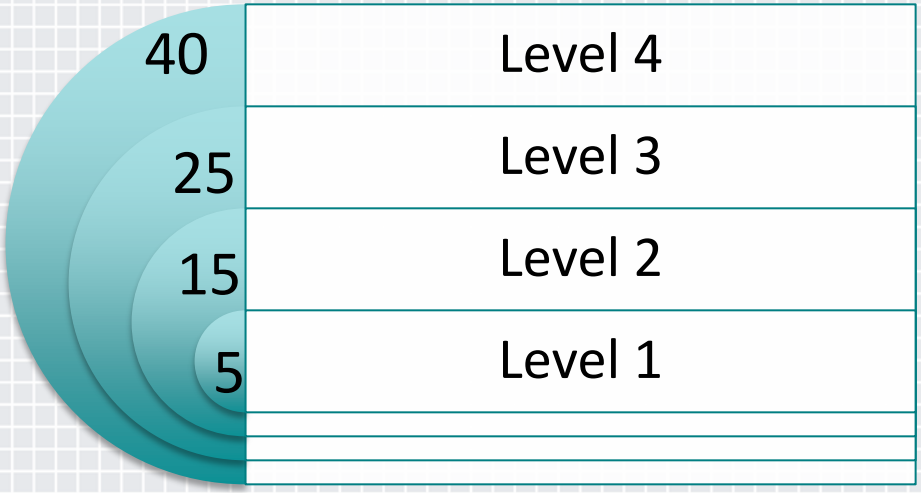
- A security tool or process
- Partnerships
- Security community

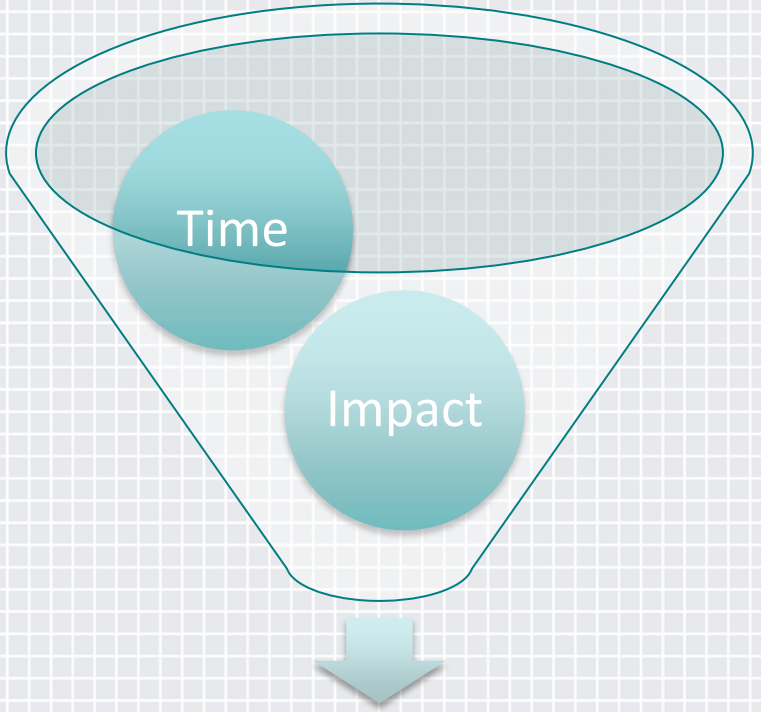
- Security issue analysis
- Participate in security committee
- Design / develop security feature

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

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

Levels and Impacts





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

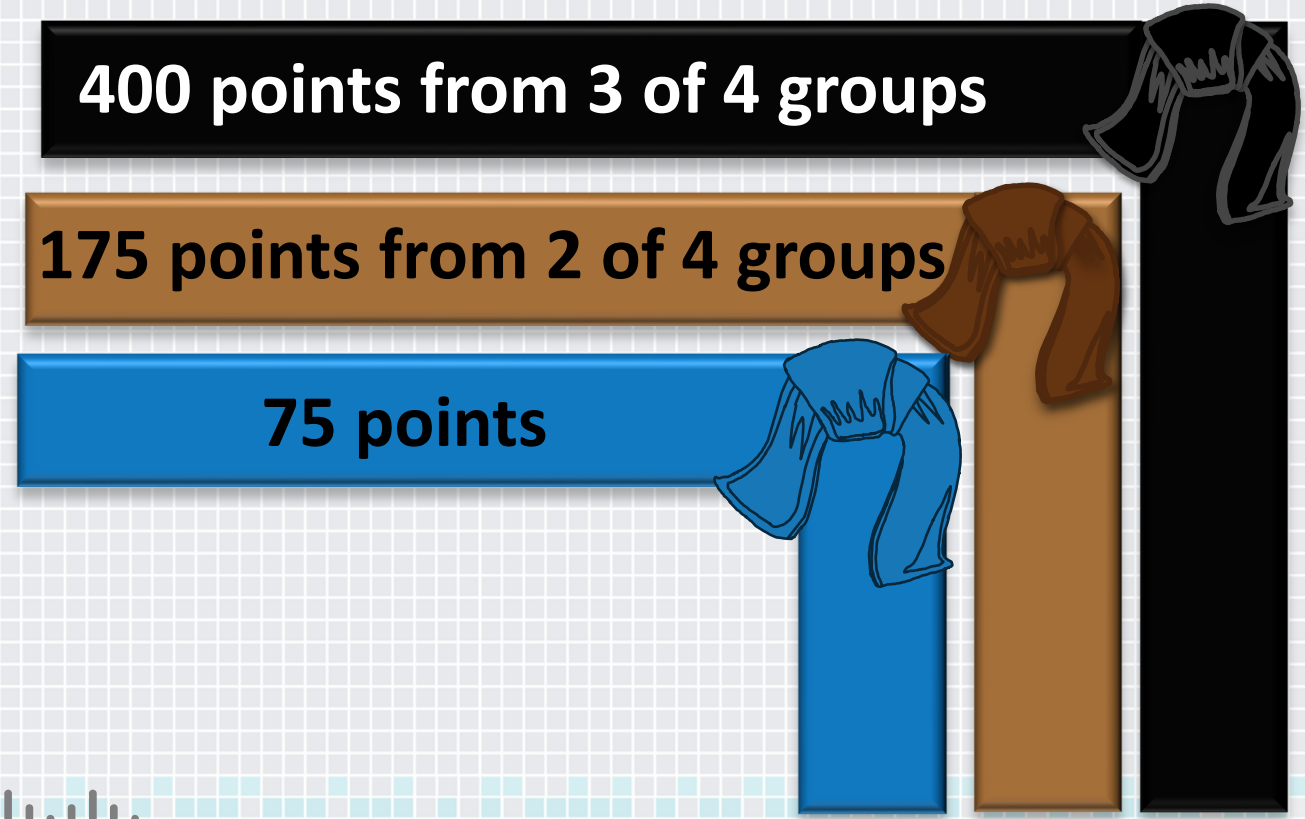
Description:
Collateral URL (e.g. EDCS link):
Date Completed:
Total Hours for this Activity:

Cumulative Points by Belt

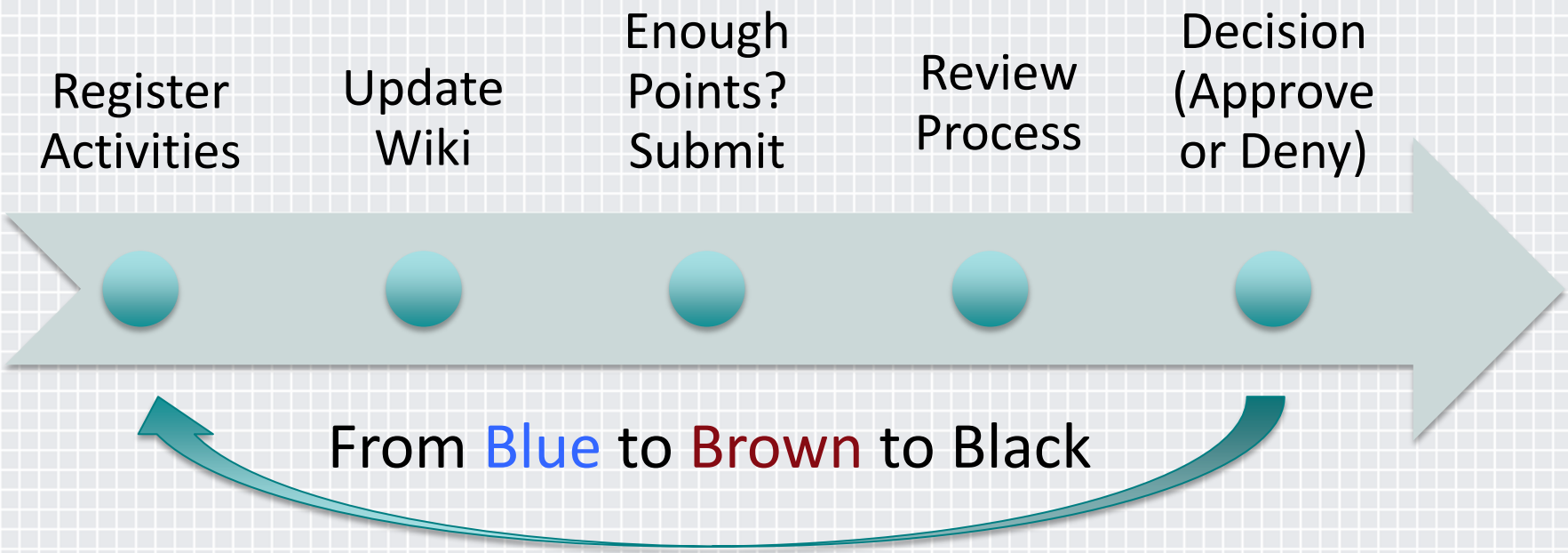
400 points from 3 of 4 groups

175 points from 2 of 4 groups

75 points



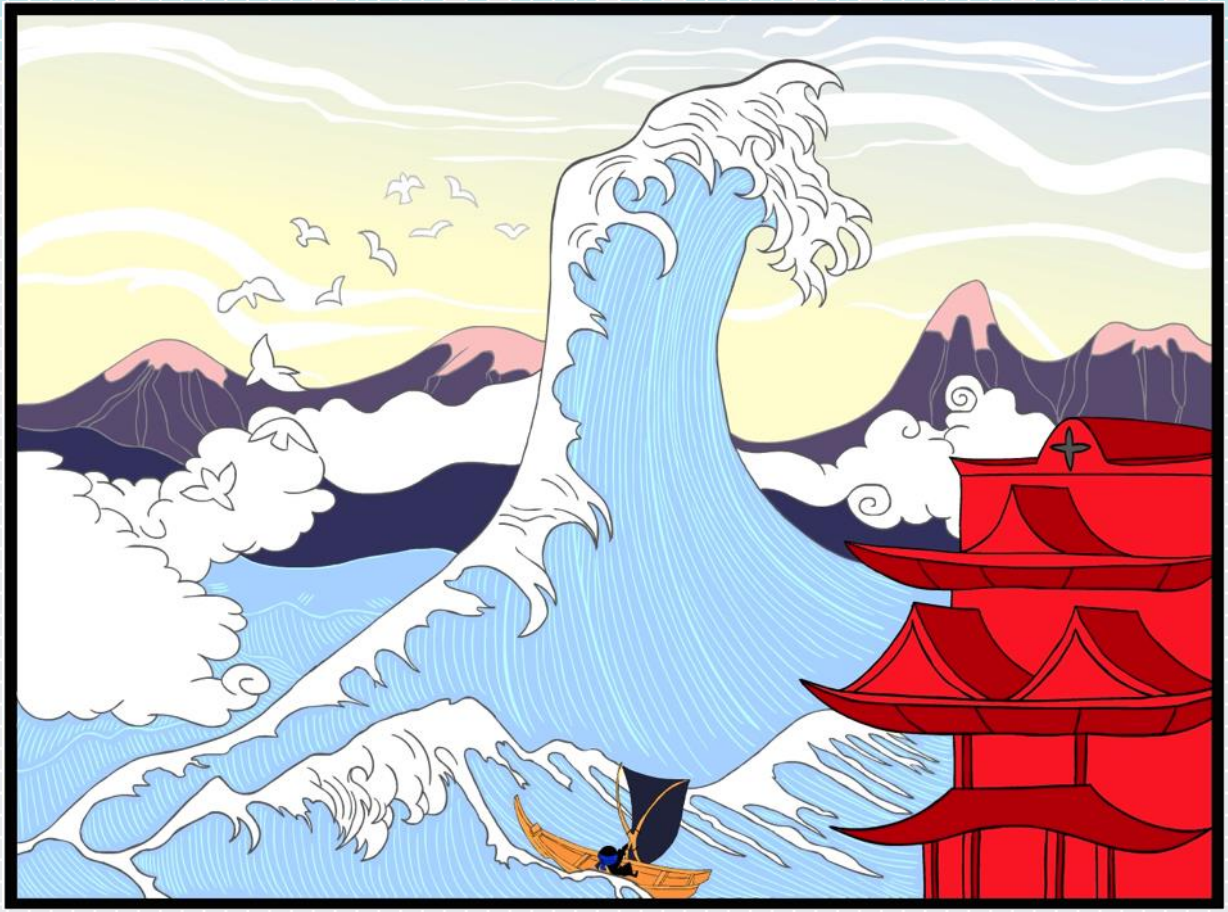
Advanced Belt Process Flow



Stats and Highlights from Wiki

- Taking a Course
  - CISSP, CEH, CCIE Security, Masters in Information Assurance
- CSDL Process
  - XSS Mitigations Architectural Document
- Partnerships
  - Engaged Director to add security faults to backlog
- Teach a Course
  - Web App Security Testing
- Security Community
  - BXB Security Research Group

Activity	Total
Taking a Course	265
Deliver Presentations	203
Build a Security Tool or Process	130
A Security Feature and Corresponding Test	83
CSDL Process	83
Participate in Security Committee	77
Security Issue Analysis	74
Mentor	73
Partnerships	69
Teach a Course	55
Create a Security Community	51
Security Strategy	49
Design / Develop New Security Features	47



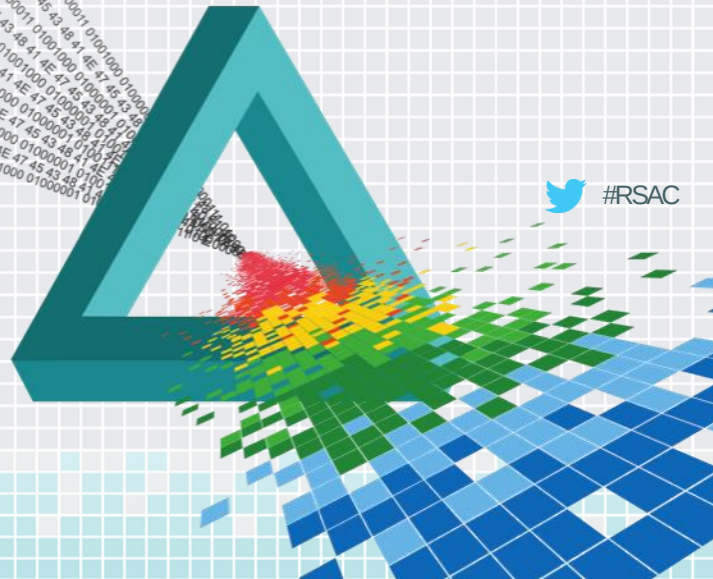
The Tidal Wave of Security Culture Change

We are **all** security ninjas.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Systems



The Cisco Security Dojo

#RSAC

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

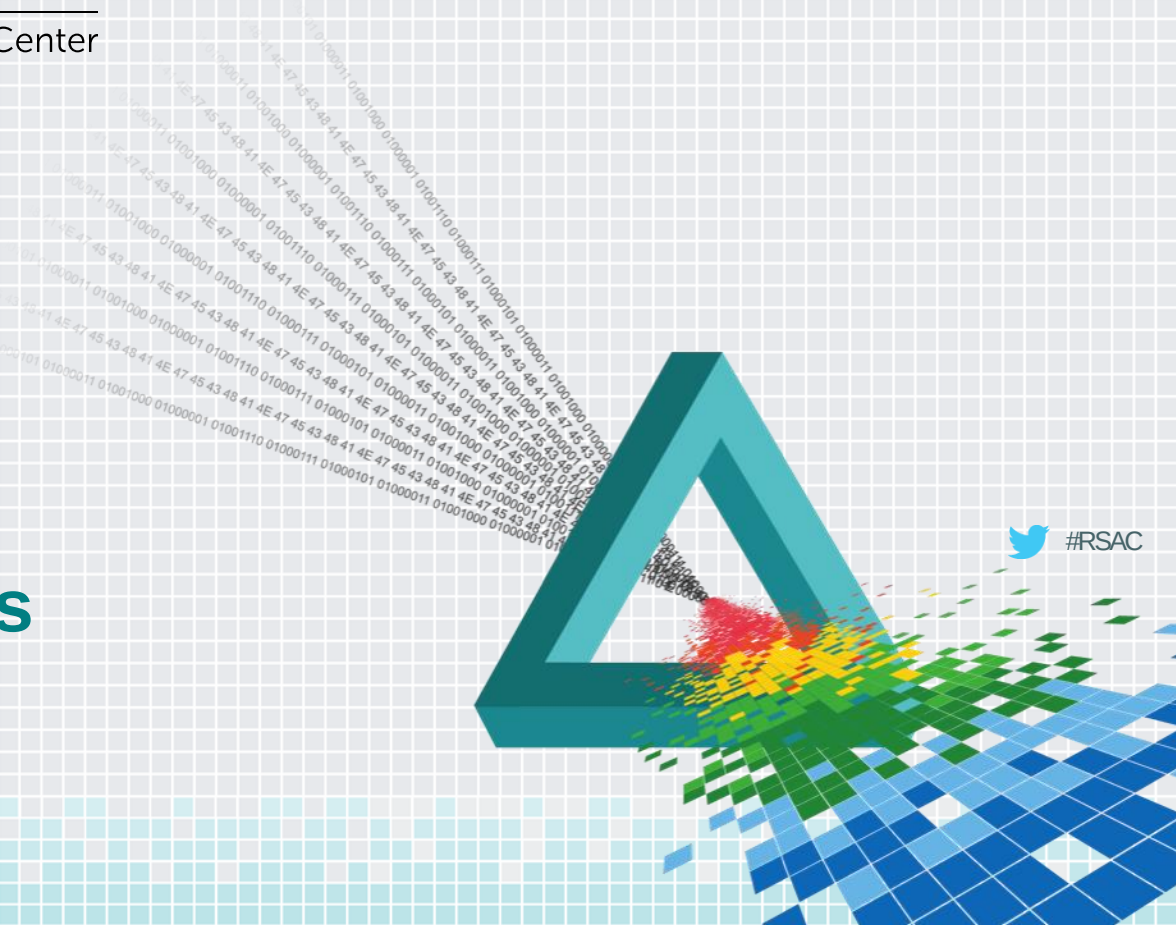
Executive View | Detail View | Certifications | Security Awareness | Revenue View | Top 50 Revenue

Organization	Security Advocates	Security Officers	White Belts (24-72 Hrs delay)		
			#	Regular	All
▶ John Chambers	240	80	19440	21.5%	14.1%

Green Belts			Advanced Belts		
#	Regular	All	Blue	Brown	Black
2085	2.7%	1.5%	72	22	47

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Secrets of Success

Secret of Success #1: 20 Minute Modules

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

- Application: Edit and reduce the required content, 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

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 reach 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

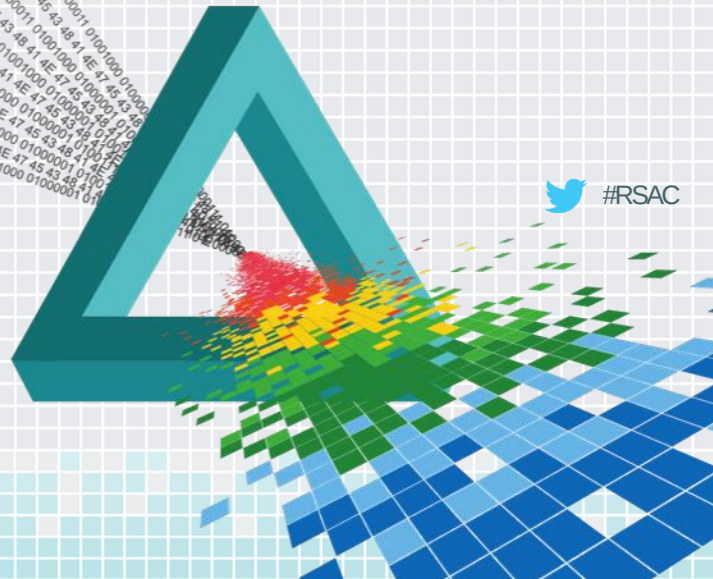
- The interface is setup like a game, allowing learners to achieve and receive visual feedback.

- 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

Conclusion



Security is a Journey

19,440 White Belts

2640 Green Belts
2290 Unique Learners
Software – 1415
Manager – 709
Test – 419
Hardware - 97

72 Blue Belts

22 Brown Belts

47 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

Questions & Answers

Chris Romeo
chromeo@cisco.com
@edgeroute

Cisco Security Ninja

ADVANCED

- Course Overview
- #1 IT and Security Company
- Security Vocabulary
- Security Business
- Security Standards
- Attacks & Attackers
- Security Myths
- Intro to CSDL
- Input Validation
- Resource Exhaustion
- Authentication
- Authorization
- Configuration
- Information Leakage
- Crypto
- Hardware
- PSIRT
- Intellectual Property
- Supply Chain
- Assessment
- Take the Survey

Watch Video | Resources | Leave Comments

What is C-I-A ?

Confidentiality
Information can only be viewed by authorized parties

Integrity
Information is not unexpectedly modified

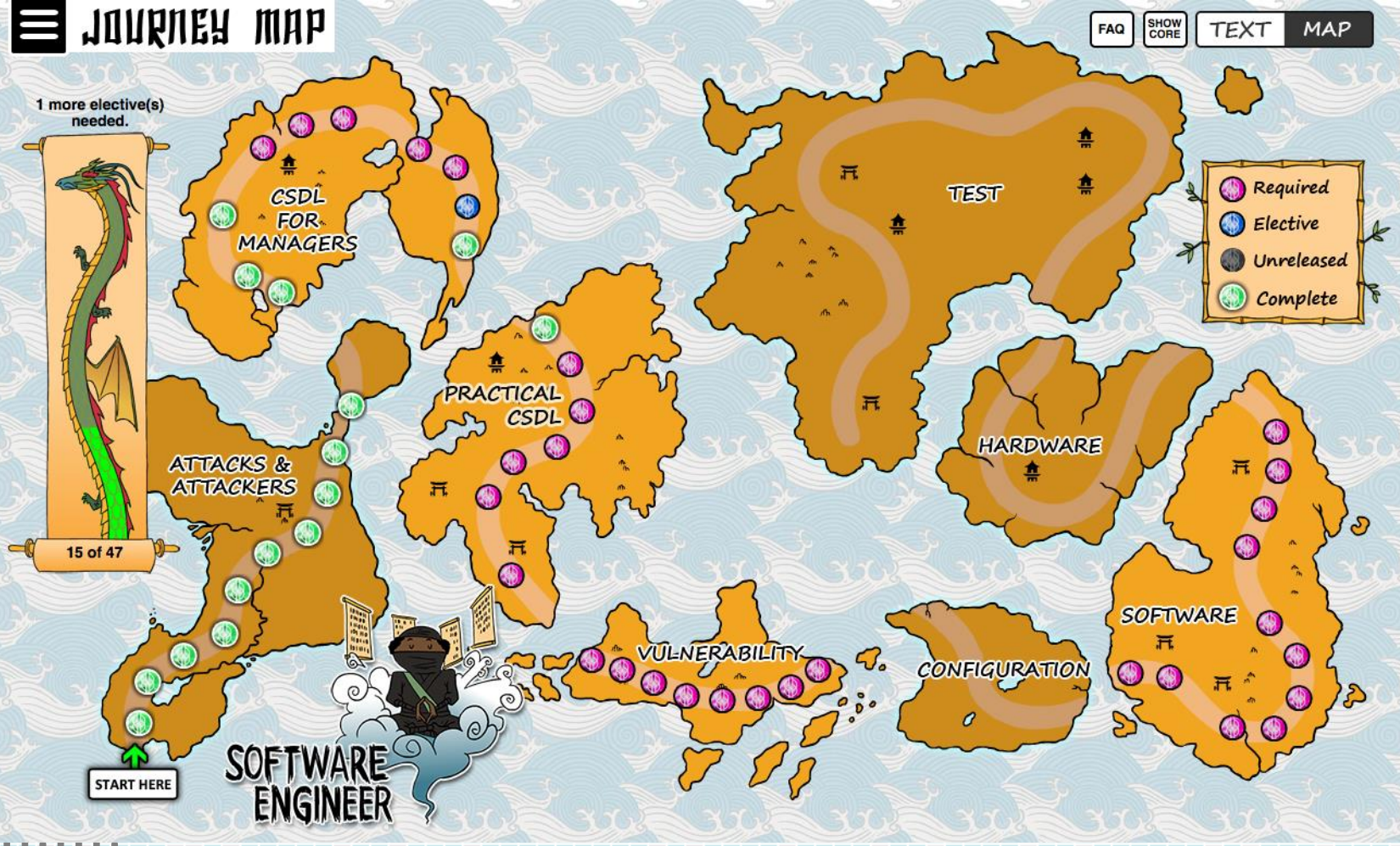
Availability
Information or resource are available when needed

02:22/15:17

Rate this presentation:


chromeo
welcome to:
SECURITY NINJA
GREEN BELT
Security is a journey, not a destination
CONTINUE

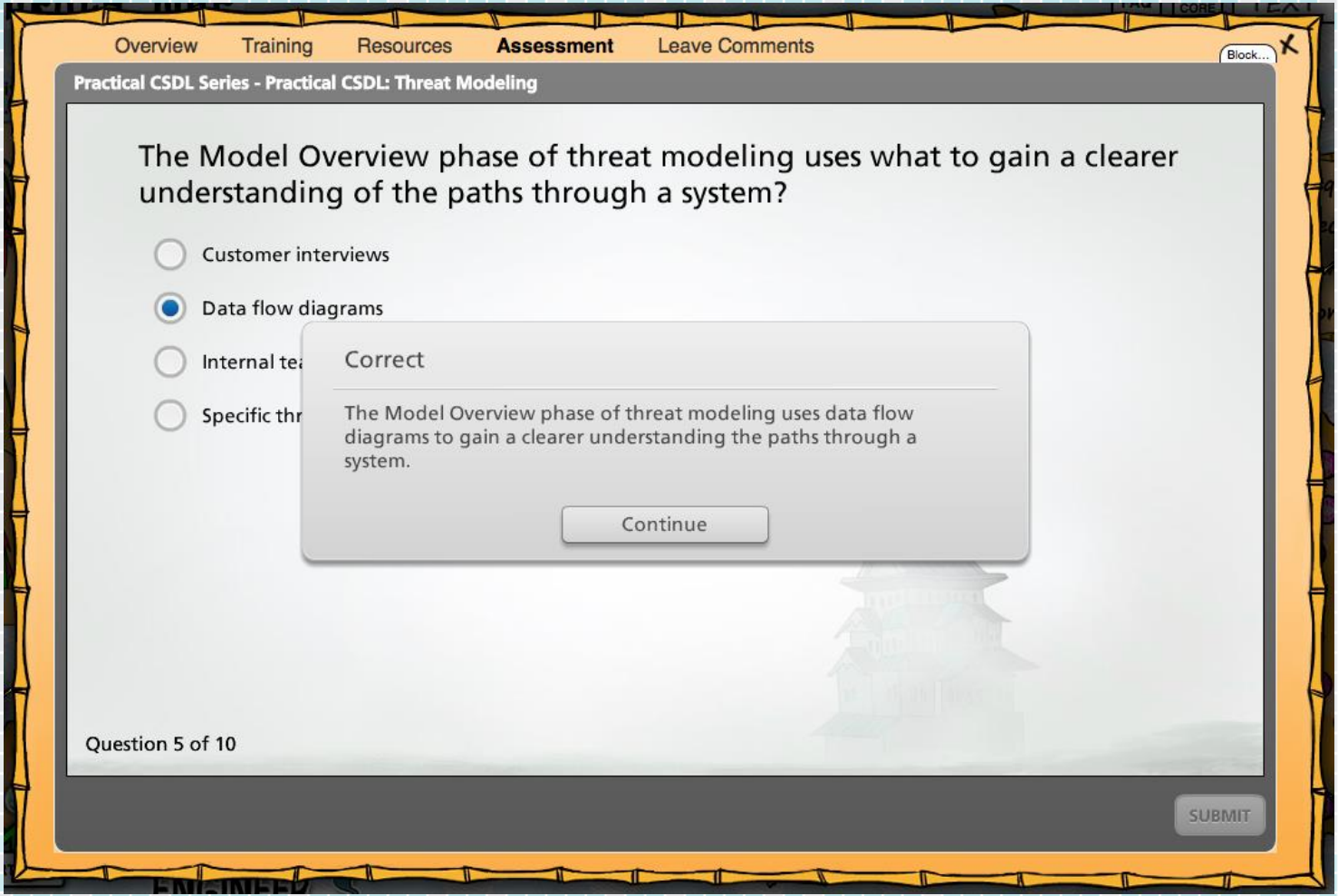

SOFTWARE ENGINEER
Choose this role if you develop products or systems, or have a coding background. Your default set of learning modules will be optimized for what you should know as a developer. You will have flexibility to select any learning modules available to other roles, as electives.
CURRENT
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
#RSAC
1 more elective(s) needed.
15 of 47
CSDL FOR MANAGERS
PRACTICAL CSDL
ATTACKS & ATTACKERS
TEST
HARDWARE
SOFTWARE
VULNERABILITY
CONFIGURATION
Required
Elective
Unreleased
Complete
START HERE
SOFTWARE ENGINEER

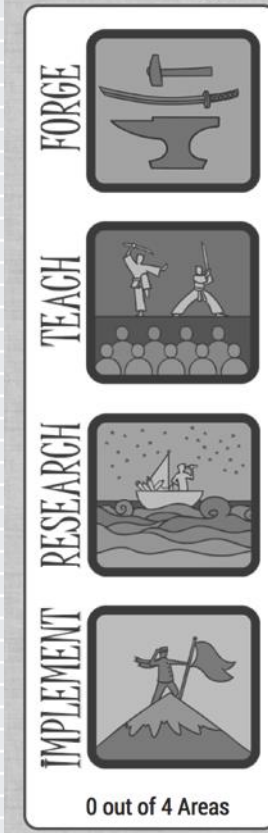
Overview **Training** Resources Assessment Leave Comments

Rate this presentation:

Video trouble?


Overview
Training
Resources
Assessment
Leave Comments
Block...
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 tea
Specific thr
Correct
The Model Overview phase of threat modeling uses data flow diagrams to gain a clearer understanding the paths through a system.
Continue
Question 5 of 10
SUBMIT

Cisco Security Blue/Brown/Black Belt - Alpha



My Contributions

IN PROGRESS Completed

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

+ Add a Contribution View My Activity Wikipage Wiki Template

Points in Progress: 80
Total Points: 0
Points to Next Level (Blue): 75

CHROMEO Status: Green Belt