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
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...
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

2. Historical

3. Action

PSIRT
Cisco Security White Belt
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 Ninja White Belt
The Journey
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
The Model Overview phase of threat modeling uses what to gain a clearer understanding of the paths through a system?

- [ ] Customer interviews
- [x] Data flow diagrams
- [ ] Internal testing
- [ ] Specific threat analysis

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

Calendar Quarter

- 4Q2012: 891
- 1Q2013: 1947
- 2Q2013: 3256
- 3Q2013: 4735
- 4Q2013: 9426
- 1Q2014: 14,040
- 2Q2014: 14,986
- 3Q2014: 16,770
- 4Q2014: 18,574
- 1Q2015: 23,271
- 2Q2015: 24,843
- 3Q2015: 24,843

Values in thousands.
Cisco Security Green Belt

Core + Role-Based + Electives = Green Belt
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

We are All Security People
## Level 3 Behavior Change: So What?

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Average Behavior Gap</th>
<th>Percentage of Behavior Increase</th>
<th>Average Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan and allocate sufficient time for the required CSDL mandated activities</td>
<td>23</td>
<td>58%</td>
<td>78%</td>
</tr>
<tr>
<td>Instill a Hacker Mindset in your team's approach to development &amp; testing.</td>
<td>25</td>
<td>51%</td>
<td>78%</td>
</tr>
<tr>
<td>Ensure team's knowledge of attack mechanisms in topics relevant work.</td>
<td>23</td>
<td>46%</td>
<td>77%</td>
</tr>
<tr>
<td>Execute the mandated CSDL elements in the CPDM Lifecycle in your projects?</td>
<td>21</td>
<td>46%</td>
<td>79%</td>
</tr>
<tr>
<td>Ensure that team has &quot;Built security in from the start&quot;.</td>
<td>22</td>
<td>46%</td>
<td>75%</td>
</tr>
<tr>
<td>Team implements Attack Tools during the development, testing and/or deployment processes</td>
<td>13</td>
<td>36%</td>
<td>68%</td>
</tr>
<tr>
<td>Ensure that Threat Modeling takes place</td>
<td>15</td>
<td>33%</td>
<td>71%</td>
</tr>
<tr>
<td>Ensure that PSB Gap Analysis takes place?</td>
<td>17</td>
<td>33%</td>
<td>82%</td>
</tr>
<tr>
<td>Ensure that team acts in a way that protects Cisco from Social Engineering attacks?</td>
<td>15</td>
<td>27%</td>
<td>73%</td>
</tr>
<tr>
<td>Ensure registering Third Party components in IP Central</td>
<td>11</td>
<td>17%</td>
<td>80%</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>19</strong></td>
<td><strong>39%</strong></td>
<td><strong>76%</strong></td>
</tr>
</tbody>
</table>
### L3 Behavior Change: So What (SW Eng)?

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

Complete activities, earn points, and achieve your next belt!
Activities for Blue, Brown, & Black

**Forge**
- A security tool or process
- Partnerships
- Security community

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

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

**Implement**
- A security feature
- A security test
- CSDL process
- Security strategy
Levels and Impacts

<table>
<thead>
<tr>
<th>Points</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>Level 1</td>
<td></td>
<td></td>
<td>Level 4</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>Level 3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>Level 4</td>
</tr>
</tbody>
</table>

Points

Time

Impact

- Levels: Level 1, Level 2, Level 3, Level 4
- Impacts: Time, Impact
Tracking Wiki

- Sample Entries
  - Build a Security Tool or Process - Level X
- 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
<table>
<thead>
<tr>
<th>Activity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taking a Course</td>
<td>581</td>
</tr>
<tr>
<td>Deliver Presentations</td>
<td>338</td>
</tr>
<tr>
<td>Build a Security Tool or Process</td>
<td>265</td>
</tr>
<tr>
<td>A Security Feature and Corresponding Test</td>
<td>232</td>
</tr>
<tr>
<td>Security Issue Analysis</td>
<td>189</td>
</tr>
<tr>
<td>CSDL Process</td>
<td>181</td>
</tr>
<tr>
<td>Mentor</td>
<td>165</td>
</tr>
<tr>
<td>Participate in Security Committee</td>
<td>144</td>
</tr>
<tr>
<td>Partnerships</td>
<td>143</td>
</tr>
<tr>
<td>Create a Security Community</td>
<td>114</td>
</tr>
<tr>
<td>Security Strategy</td>
<td>102</td>
</tr>
<tr>
<td>Teach a Course</td>
<td>77</td>
</tr>
<tr>
<td>Design / Develop New Security Features</td>
<td>76</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2607</strong></td>
</tr>
</tbody>
</table>
The Tidal Wave of Security Culture Change
The Cisco Security 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 knowledge 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.

- White Belt (Pick One)
- Green Belt
- Blue / Brown / Black Belt

Recognition

- View List of Current Belts
- Instructions for adding your badge to a Directory and MIE

Cisco Security Ninja Certification and Graduation Form
Security Insights Dashboard

<table>
<thead>
<tr>
<th>Organization</th>
<th>Security Advocates</th>
<th>Security Officers</th>
<th>White Belts (24-72 Hrs delay)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chuck Robbins</td>
<td>339</td>
<td>101</td>
<td># Foundl</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2695</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Green Belts</th>
<th>Advanced Belts</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Regular</td>
</tr>
<tr>
<td>1845</td>
<td>2.3%</td>
</tr>
</tbody>
</table>
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 regular Cisco employees (25.2%)
- 3916 Green Belts
- 3478 Unique Learners
- Software – 2024
- Manager – 946
- Test – 804
- Hardware - 142

- 59.2% of Eng employees

- 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


• Sample Module, highlighting our content approach

• Single Module focused on Net / Sec Eng

• Ninja Episode
Questions & Answers

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

SECURITY NINJA
WHITE BELT

Security is a journey, not a destination
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

1 more elective(s) needed.

START HERE

SOFTWARE ENGINEER

CSDL FOR MANAGERS

ATTACKS & ATTACKERS

PRACTICAL CSDL

TEST

HARDWARE

SOFTWARE

VULNERABILITY

CONFIGURATION

Required
Elective
Unreleased
Complete
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