Building the Next Generation of Cyber Defenders
Tapping into the League of Wounded Warriors to help Protect and Defend the Nation’s Information Systems

Sam Maroon
Jim Wiggins
Speaker Introduction

- **Mr. Sam Maroon**
  - Technical Instructor at the Foreign Service Institute (FSI) for the U.S. Department of State
  - Former Electronics Warfare Officer
  - Former Tactics Officer – Desert Storm
  - Graduate of Virginia Military Institute – BS Engineering
  - Graduate of George Washington University – Master’s Certificate

- **Mr. Jim Wiggins**
  - Executive Director of the Federal IT Security Institute and the FITSI Foundation
  - Cybersecurity Trainer and Information Security Practitioner
  - 16 of experience in IT
  - 12 of experience in IT security
  - 2010 FISSEA “Educator of the Year Award”
Overview

- The Idea…
- Why?
- What?
- How?
The Idea…

- The Three Wise Men…
  - David
    - November 2009
  - Sam
    - Fall of 2011
  - Manny
    - February of 2012

- All of them posed the same question:
  - Can’t we train Wounded Warriors in cybersecurity?
The Cybersecurity Problem Space

Historic Background

18th Century

19th Century

20th Century

Always a Target, But Always Defendable
Have We Lost The Advantage of Our Geography?
The Cybersecurity Problem Space

Basis for Change

Information ∨ Property & Commodity
Network Connectivity ∨ New Benefits/New Risks
Globalization ∨ World-wide Competition
Cyber Dimension ∨ No Protecting Borders
Deregulation/Restructuring ∨ Potential Vulnerabilities
Military Superiority ∨ Asymmetric Warfare
Pace of Change ∨ Assimilation Problems
The Cybersecurity Problem Space

Cost and Availability

- Invasion
- Bomber w/Nuke
- Missiles ICBM & SLBM
- Cruise Missile
- Precision Guided Munitions
- Computer

Availability of Capability

Cost of Capability
The Cybersecurity Problem Space

- Attack Recognition and Attribution
The Cybersecurity Problem Space

- Consider the Traditional National Security Model

- Federal Gov’t: Most Data
- Private Experts: More Data
- State/Local Gov’t: Some Data
- Owner/Operator/Business: Minimal Data
Today’s Cyber Security Model Stands the Traditional Model on Its Head!
The Need for Technical Cyber Defenders

- Cyber attacks continue to escalate
  - RSA
  - Oak Ridge National Laboratory
  - Many government contracting firms

- Attacks are highly sophisticated
  - Not just Denial of Service
  - Data theft and intellectual property being lost
    - i.e. - Advanced Persistent Threat
The Need for Technical Cyber Defenders

In 2010, James Gosler, a veteran cyber security specialist who has worked at the CIA, the National Security Agency and the Energy Department made the following comment:

"We don't have sufficiently bright people moving into this field to support those national security objectives as we move forward in time."

- Estimated that there were only 1,000 people in the entire United States with the necessary skills
- A force of 20,000 to 30,000 skilled specialists is needed.¹

Lots of skills are required

- Hardware Skills
- Operating System Skills
- Server Skills
- Linux Skills
- Networking Skills
- Foundational Security Skills
- Generalist Security Skills
- Specialty Skills
  - Penetration Testing
  - Network Defense
  - Incident Handling
  - Forensic Analysis
  - Security Control Assessors
Building Technical Cyber Capabilities

- Penetration Testing Skills
- Incident Handling Skills
- Forensics Skills
- Network Defense Skills

- Generalist Security Skills
- Foundational Security Skills
- Networking Skills
- Linux Operating System Skills
- Windows Server Skills
- Basic Operating System Skills
- Hardware Skills
The League of Wounded Warriors

Who is a Wounded Warrior?
- Military service members who have suffered a serious life altering injury
  - In combat or non-combat situations
  - Injury typically ends their ability to continue to serve
  - Mostly served in Iraq or Afghanistan
**The League of Wounded Warriors**

- What makes a wounded warrior an ideal candidate as a cyber defender?
  - Ability to be trained
  - Highly patriotic
  - Availability of time
  - Desire to repatriate
  - Aptitude for tactics and strategy
  - The Nation needs them

- They are dedicated, highly motivated, disciplined, and trustworthy team players who both industry and government seek as workers.
Wounded Warrior Training Model

- High Level Overview
- Use of Industry Certifications
- Use of Online Training Platform
- Use of a Cyber Range
- Use of Performance Based Assessments
- How the Pieces Fit Together
Wounded Warrior Training Model

- High Level Overview

- Expert Level Role Based Skills
- Core Cyber Security Skills
- Foundational Cyber Security Skills
- Foundational IT Skills
Use of Industry Certifications

- CompTIA
  - A+, Network+, Security+, Linux+, Server+, CASP
- EC-Council
  - Certified Ethical Hacker, Licensed Penetration Tester
- FITSI
  - FITSP-Operator
- ISC2
  - Systems Security Certified Practitioner
- Security Certified
  - Security Certified Network Specialist
  - Security Certified Network Professional
  - Security Certified Network Architect
Use of Industry Certifications

- A+
- Linux+
- Network+
- Server+
- Security+
- SCNS
- SCNP
- SCNA
- FITSP-Operator
- CEH
- LPT
- FCSP-PT
- Core Cyber Security Skills
- Level 3
- Expert Cyber Technical Skills
- Level 4
- Foundational IT Skills
- Level 1
- Foundational Cyber Security Skills
- Level 2
Wounded Warrior Training Model

- Hybrid Training Platform

Traditional Classroom  Online Classroom
## Wounded Warrior Training Model

- Use Cyber Range Technologies

### Figure 1

<table>
<thead>
<tr>
<th>AVAILABLE IA/CND TOOLS</th>
<th>ENVIRONMENT FEATURES</th>
<th>ENVIRONMENT FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight</td>
<td>Multi-protocol Label Switching (MPLS) Cloud</td>
<td>Virtual Internet</td>
</tr>
<tr>
<td>Sourcefire</td>
<td>Defense Enterprise Computing Centers (DECC) and Community Data Center (CDC), Internet Access Point, Multi-WAN Transport</td>
<td>Hundreds of sites</td>
</tr>
<tr>
<td>HBSS</td>
<td>Base boundary defense</td>
<td>Full Domain Name System (DNS) replication</td>
</tr>
<tr>
<td>Splunk</td>
<td>Base network infrastructure</td>
<td>Network- and host-based traffic generation</td>
</tr>
<tr>
<td>Wireshark</td>
<td>Virtual actors</td>
<td>Malicious content</td>
</tr>
<tr>
<td>Palo Alto</td>
<td>Full Microsoft Office suite</td>
<td>Boundary defense</td>
</tr>
<tr>
<td>Security</td>
<td>Numerous operating systems</td>
<td>Real Hardware</td>
</tr>
</tbody>
</table>
Wounded Warrior Training Model

- Curriculum and Exercises on the Cyber Range

<table>
<thead>
<tr>
<th>Role on the Cyber Range</th>
<th>Certification program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help desk technician</td>
<td>A+</td>
</tr>
<tr>
<td>Network administrator</td>
<td>Network+</td>
</tr>
<tr>
<td>Network engineer</td>
<td>Server+</td>
</tr>
<tr>
<td>Network engineer</td>
<td>Linux+</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>Security+</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>SCNS</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>SCNP/SCNA</td>
</tr>
<tr>
<td>Information Assurance Manager</td>
<td>CISSP</td>
</tr>
<tr>
<td>Information Systems Security Officer</td>
<td>FITSP-Operator</td>
</tr>
<tr>
<td>Blue Team Member</td>
<td>CEH</td>
</tr>
<tr>
<td>Red Team Member</td>
<td>ECSA/FCSP-Penetration Tester</td>
</tr>
</tbody>
</table>
Wounded Warrior Training Model

- Use of Performance Based Assessments
  - Capstone for all graduates of the program
  - Exercises as part of the cyber range will train towards preparation of the capstone project
  - Can help demonstrate that the students can actually “do the work”
  - Will earn a final certification
    - Federal Cyber Security Professional - Penetration Tester
Wounded Warrior Training Model

How the Pieces Fit Together

- **Stage 1**: Instructor Led Training
- **Stage 2**: Certification Exam Preparation
- **Stage 3**: Cyber Range Activities
Program Details

- Overview
- Training Stages
- End Game
- Schedule
- Funding Sources
Overview

- Started with a small group of 20 in a pilot program
- Use a dozen certifications
- Use the Cyber Range
- Use Performance Based Assessments
Training Stages
- 4 stages
- 4 quarters – 1 year
Program Details

- End Game

**Industry Certifications**
- Outcome
  - Cyber Knowledge
  - Cyber Skills
  - Cyber Abilities

**FITSI Cyber Range**
- Outcome
  - Hand’s On Practice
  - Performance-Based Simulations
## Program Details

### Schedule – Timing Breakdown

<table>
<thead>
<tr>
<th>Program</th>
<th>Time Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>6 Weeks</td>
</tr>
<tr>
<td>Network+</td>
<td>5 Weeks</td>
</tr>
<tr>
<td>Server+</td>
<td>5 Weeks</td>
</tr>
<tr>
<td>Linux+</td>
<td>5 Weeks</td>
</tr>
<tr>
<td>Security+</td>
<td>5 Weeks</td>
</tr>
<tr>
<td>SCNS</td>
<td>5 Weeks</td>
</tr>
<tr>
<td>SCNP</td>
<td>5 Weeks</td>
</tr>
</tbody>
</table>
## Program Details

### Schedule – Typical Month

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Team Cohort (6:00-10:00pm)</td>
<td></td>
<td>Cyber Team Cohort (6:00-10:00pm)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Team Cohort (6:00-10:00pm)</td>
<td></td>
<td>Cyber Team Cohort (6:00-10:00pm)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Team Cohort (6:00-10:00pm)</td>
<td></td>
<td>Cyber Team Cohort (6:00-10:00pm)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Program Details

Funding Sources

- Initial pilot program handled with corporate/personal sponsor donations
- Future funding to be handled by charitable donations
  - Setup the FITSI Foundation
  - Received 501c3 status as of August 4th, 2013
    - Only took IRS application 90 days!
The Players

■ Online Providers
  ○ Avaya Government Solutions
    ■ Provides the Online “Avatar-based” learning platform
  ○ Department of Defense
    ■ Provides the online cyber range
The Players

- Certification Bodies
  - CompTIA
    - Provides the entry-level certifications
  - EC-Council
    - Provides some of the highly technical certifications
  - FITSI
    - Provides the federally focused certification programs
  - ISC2
    - Provides the “core” cyber security certification programs
  - Security Certified
    - Provides the foundational cyber security certification programs
The Players

- Textbook Providers
  - Axzo Press
  - Logical Operations
Registration Process

- What traits are ideal for Wounded Warriors
- Criteria for W2CCA Registration
- How to Apply
Registration Process

What traits are ideal for Wounded Warriors

- Ideal candidates will possess
  - Desire to enter a market with a “zero” percent unemployment rate
  - Ability to think abstractly
  - Aptitude to work well with others
  - Geek traits as it relates to technology
  - Ability to commit to a long term program
  - Acceptance of a career requiring continuous learning
Criteria for W2CCA Registration

1. Be transitioning or have transitioned from military service;
2. Suffer from injuries or illnesses incurred while deployed in overseas contingency operations supporting Operation Iraqi Freedom (OIF) and/or Operation Enduring Freedom (OEF) since September 11, 2001; and
3. Receive, or expect to receive, a physical disability rating of 30% or greater in at least one of the specific categories listed below that substantially affect a major life function, or receive, or expect to receive, a combined rating equal to or greater than 50% for any other combat or combat related condition:
   - Blindness/loss of vision
   - Deafness/hearing loss
   - Fatal/ incurable disease
   - Loss of limb
   - Permanent disfigurement
   - Post traumatic stress
   - Severe burns
   - Spinal cord injury/paralysis
   - Traumatic brain injury
   - Any other condition requiring extensive hospitalizations or multiple surgeries
Criteria for W2CCA Registration

- Should a service member be unable to participate due to the severity of his/her injuries, the same support will be extended to a member of his/her immediate family who may be seeking training. Widows and widowers of service members who have paid the ultimate sacrifice during OIF or OEF are also eligible for support under the W2CCA program. If support is provided to a family member and the service member becomes able to participate, support will then be extended to him/her.
Registration Process

How to Apply

Active Duty
- Meet the Registration Criteria
- Occupational Therapist Referral
- IT Aptitude Exam

Veteran
- Meet the Registration Criteria
- Three Professional Referrals
- IT Aptitude Exam
The Results

- Program will benefit
  - The Nation
  - The League of Wounded Warriors
  - The Cybersecurity Industry
The Results

Benefits to the Nation

- Highly trained cyber defenders
- Graduates will have real job performance
- Every candidate will be fully DoD 8570 compliant in multiple levels of the Information Assurance Management (IAM) and Information Assurance Technical (IAT) certification framework
The Results

- Benefits to the League of Wounded Warriors
  - Ability to continue serving their country
  - Using their military aptitude to defend the Nation in a new theatre of battle
  - Enter a job market where there is a virtual zero percent unemployment rate*
The Results

- Benefits to the Cybersecurity Industry
  - Begin to build the necessary technical cyber capability
  - Helps address workforce shortage of personnel
  - Establishes comprehensive training framework using existing industry players
How Can You Help?

Three ways to help

- Recruit a wounded warrior you may know
  - Point them to [http://www.w2cca.org](http://www.w2cca.org)

- Ask your organization to become a corporate sponsor
  - Corporate sponsorship form
    - [http://www.fitsi.org/w2cca-cs.pdf](http://www.fitsi.org/w2cca-cs.pdf)
  - Three levels of sponsorship
    - Gold
    - Silver
    - Bronze

- Consider a personal donation
  - Any level of giving is greatly appreciated
  - Make a tax deductible donation to the FITSI Foundation at [http://www.w2cca.org](http://www.w2cca.org)
Contact Information

- Sam Maroon
  - 703-302-3155 – maroonsa@state.gov
- Jim Wiggins
  - 703-828-1196 x701 – jim.wiggins@fitsi.org

- Wounded Warrior Cyber Combat Academy Website
  - http://www.w2cca.org
- FITSI
  - http://www.fitsi.org
Questions and Answers

- Comments?
- Questions?
- Thoughts?
Recap

- The Idea...
- Why?
- What?
- How?