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

Wounded Warrior Cyber Combat Academy

FITSI
FEDERAL IT SECURITY INSTITUTE
HELPING SECURE THE NATION'S FEDERAL INFORMATION SYSTEMS

Speaker Introduction

- Mr. Sam Maroon
  - IT Operations Instructor for the US Department of State
  - was an Electronic Warfare Officer and Tactics Officer while serving in the US Air Force

- Mr. Jim Wiggins
  - Cyber Security Trainer and Information Assurance Practitioner
  - 12 years of experience in IT security
  - FISSEA “Educator of the Year” for 2010
  - **Executive Director of the Federal IT Security Institute (FITSI)**

Overview

- The Cyber Security Problem Space
- The Need for Technical Cyber Defenders
- How to Build Technical Cyber Capabilities
- The League of Wounded Warriors
- Wounded Warrior Training Model
- Program Details
- The Players
- The Results
- Registration Process
- How Can You Help
- Contact Information
- Questions and Answers
- CEU/CPE Information

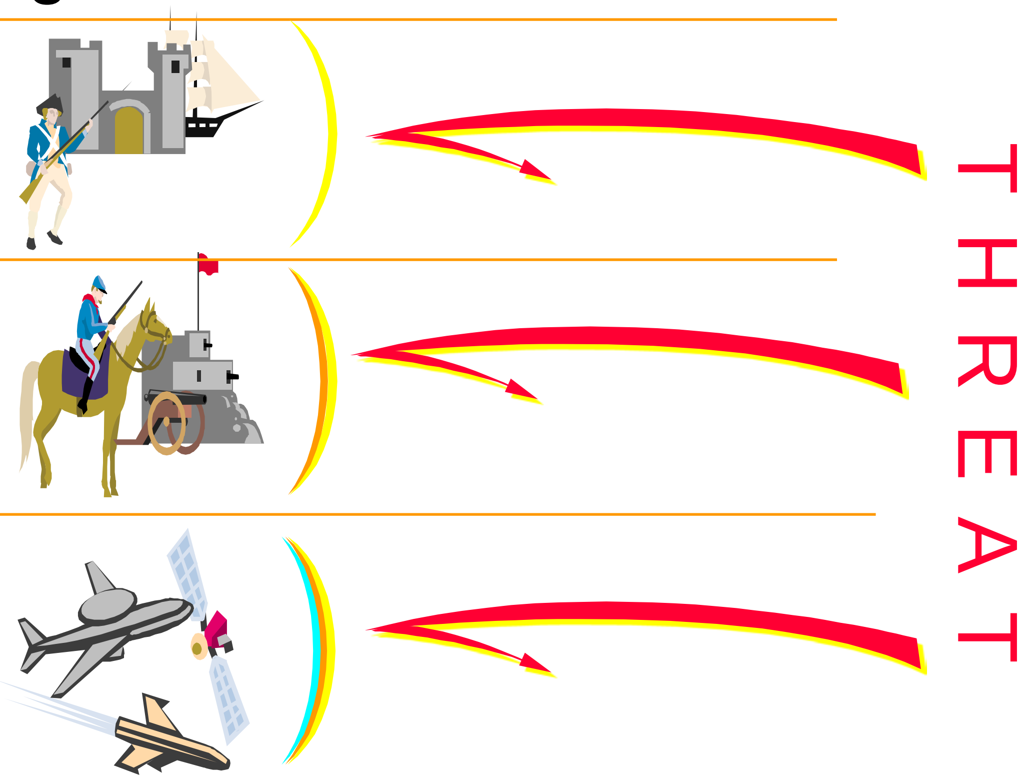
The Cyber Security Problem Space

- Historic Background

18th Century

19th Century

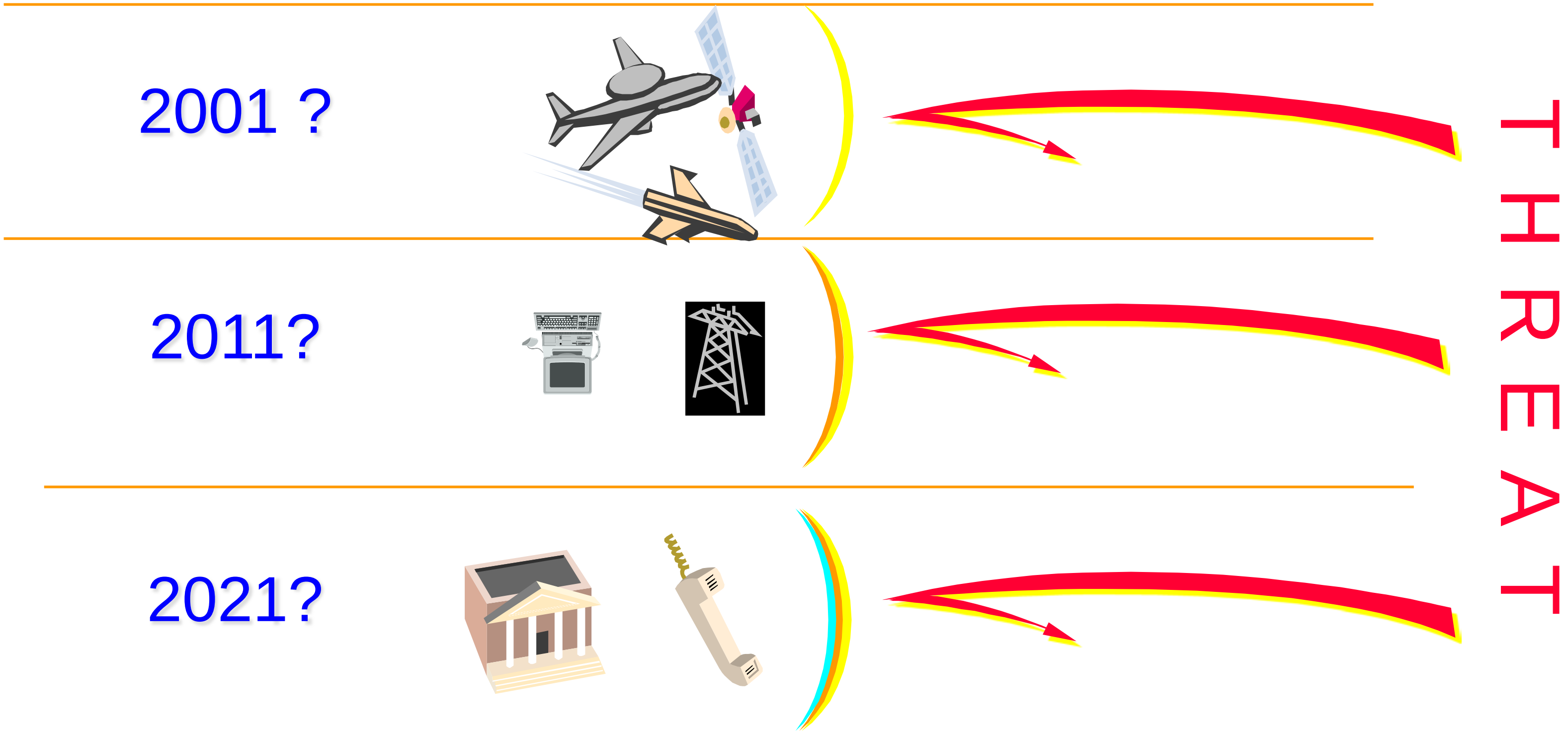
20th Century



Always a Target, But Always Defendable

The Cyber Security Problem Space

- Where are we headed?



2001 ?

2011?

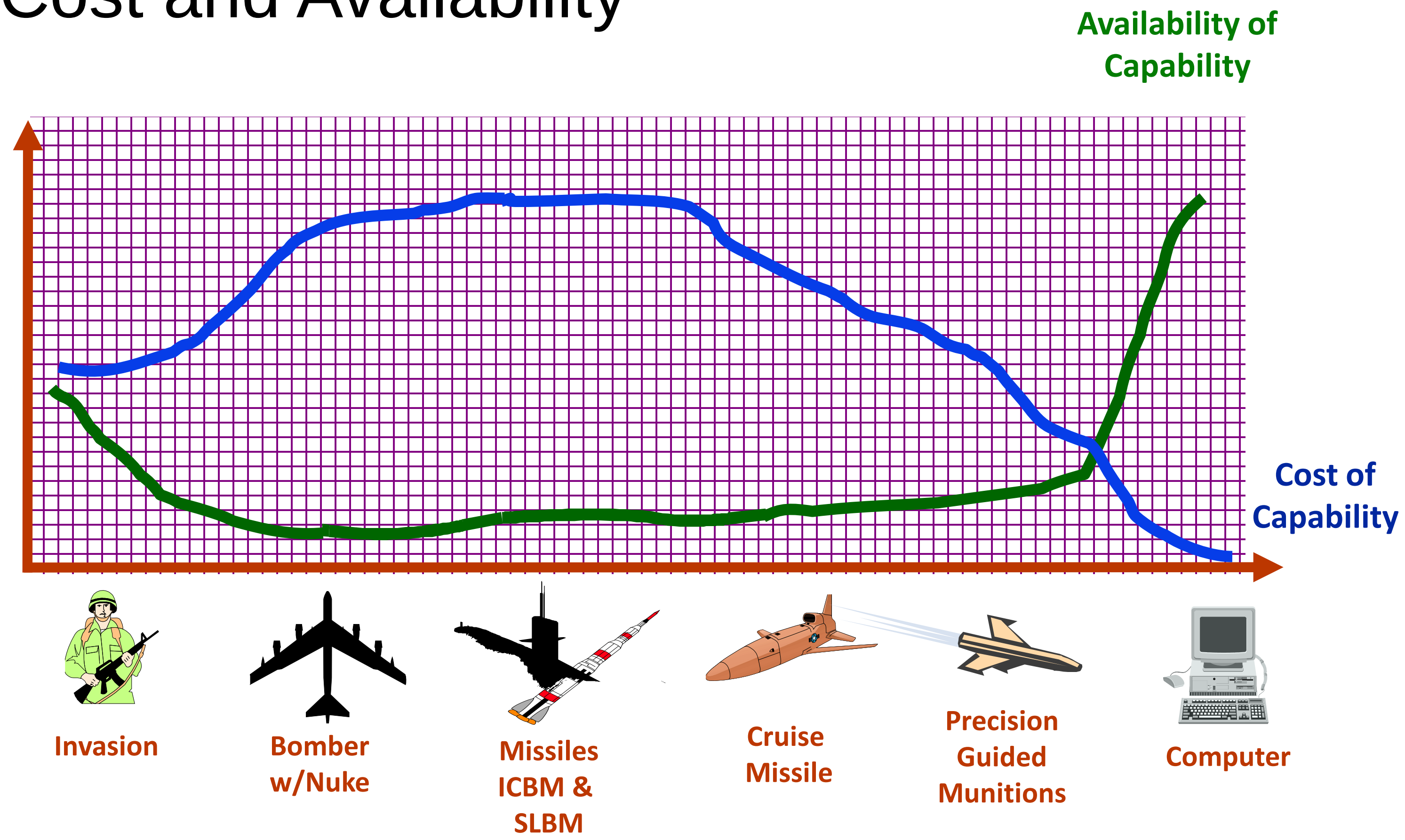
2021?

THREAT

Have We Lost The Advantage of Our Geography?

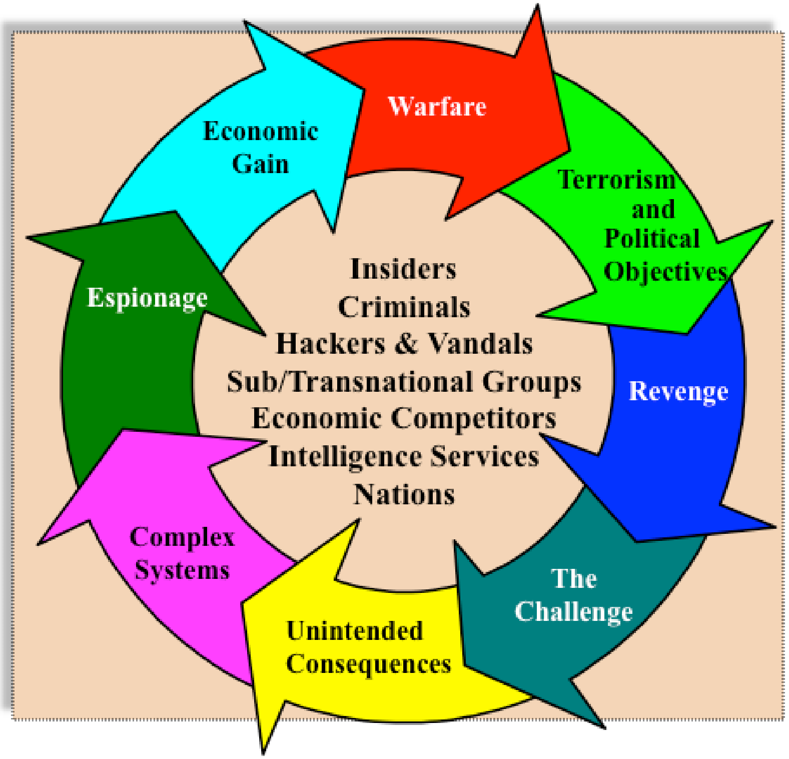
The Cyber Security Problem Space

- Cost and Availability



The Cyber Security Problem Space

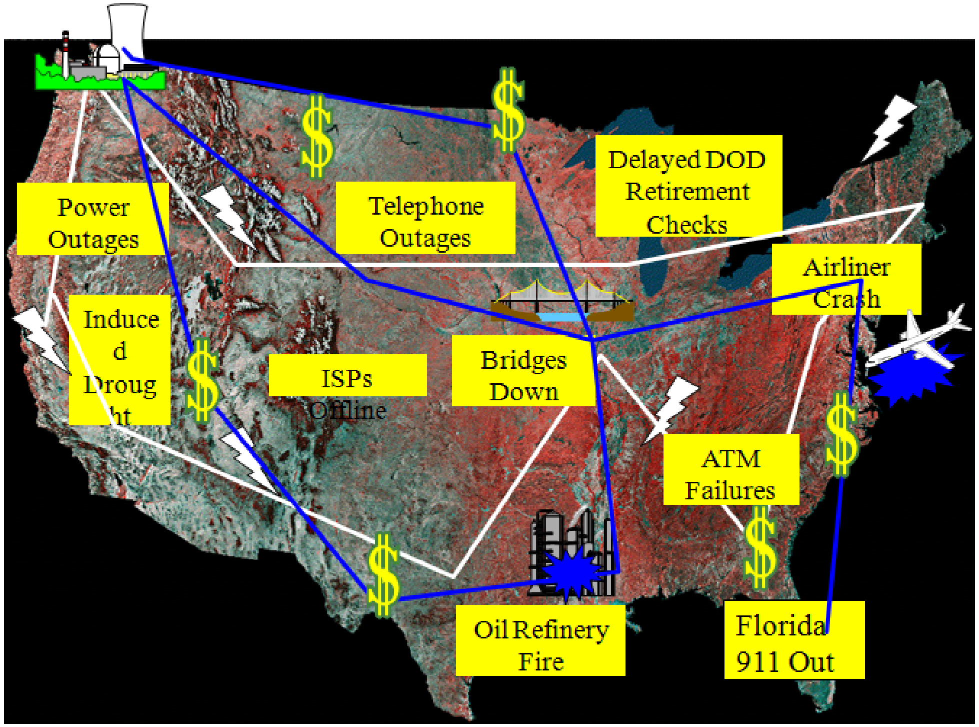
- Attack Motivation



- Detection capabilities are too limited to reliably know what is going on
- Automated attack tools make it very difficult to evaluate who the attacker is or the motivation.
- **In fact, our first reaction to unusual circumstances on our computers is defined by three keys: Control, Alt, Delete - -**

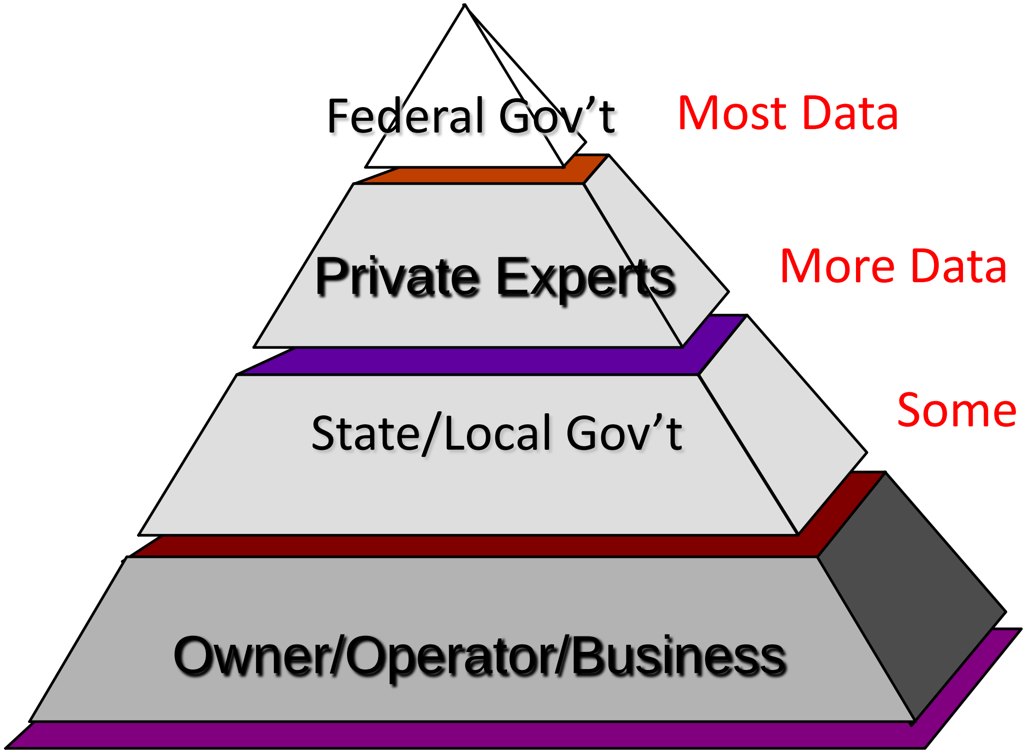
The Cyber Security Problem Space

- Attack Recognition and Attribution



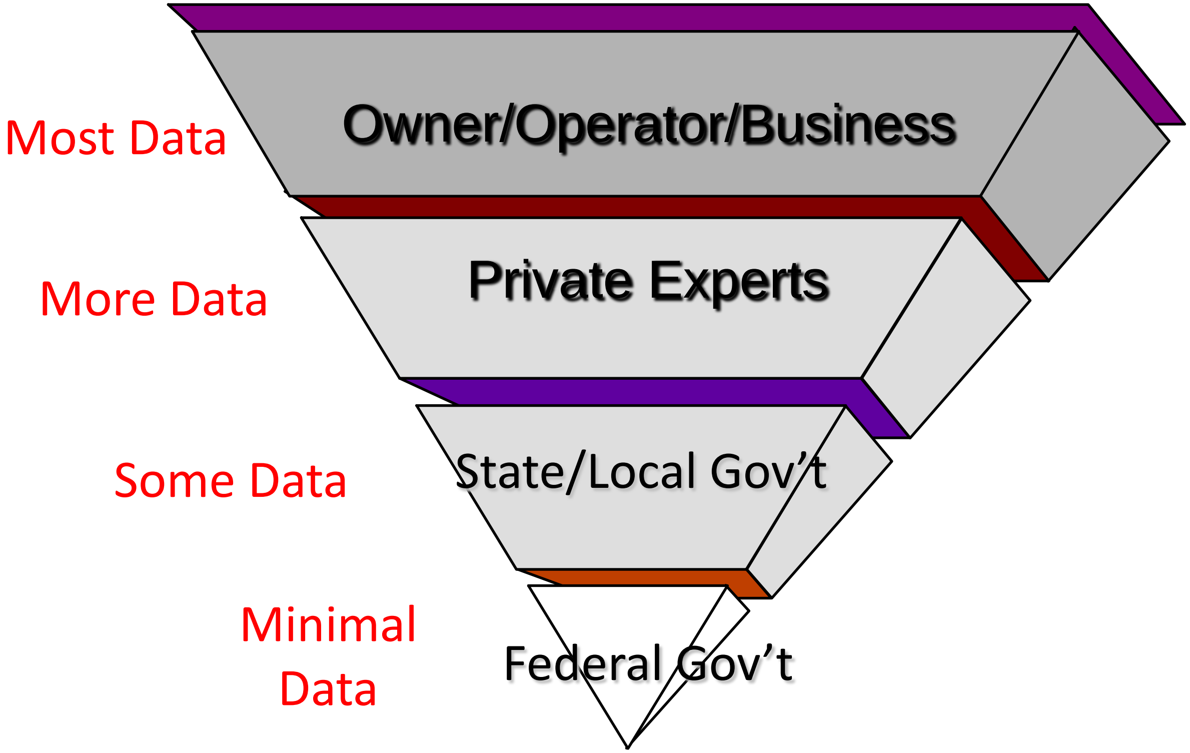
The Cyber Security Problem Space

- Consider the Traditional National Security Model



The Cyber Security Problem Space

- 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

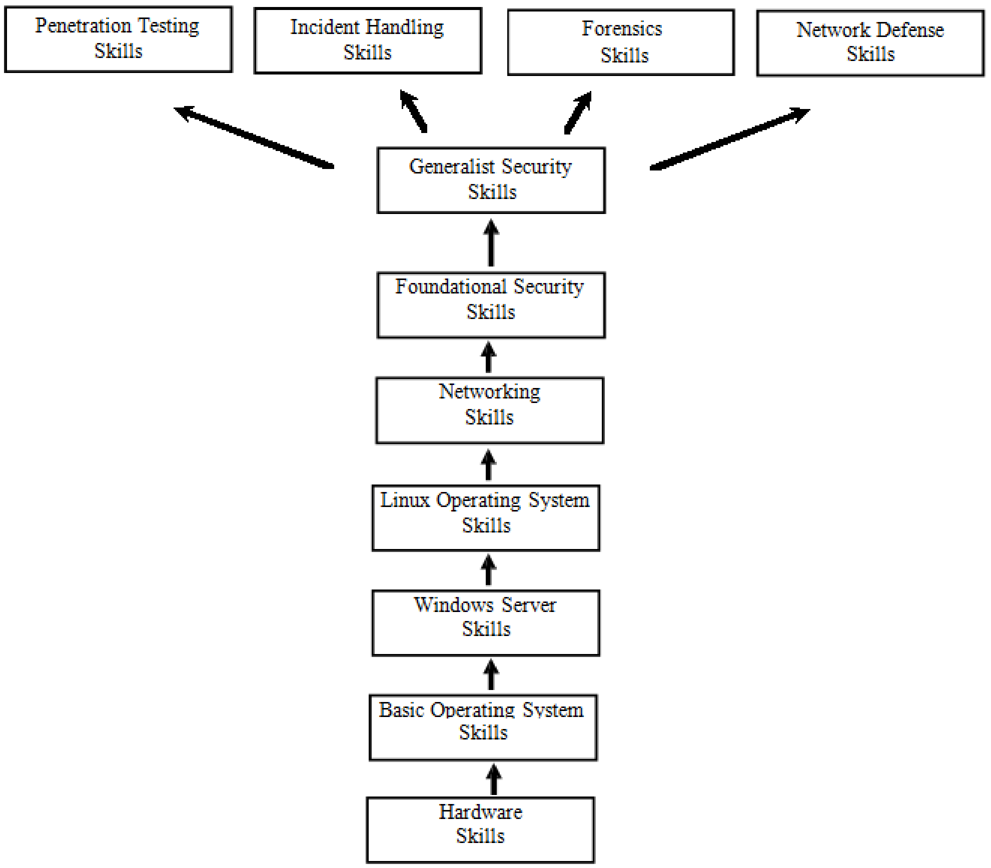
- In 2010, James Gosler, a veteran cyber security specialist who has worked at the CIA, the National Security Agency and the Energy Department made the following comment, “"*We don't have sufficiently bright people moving into this field to support those national security objectives as we move forward in time.”*
  - Gosler estimated in 2010 that there were only 1,000 people in the entire United States with the sophisticated skills needed for the most demanding cyber defense tasks.
  - To meet the computer security needs of U.S. government agencies and large corporations, he says, a force of 20,000 to 30,000 similarly skilled specialists is needed.[1]

[1] http://www.npr.org/templates/story/story.php?storyId=128574055

How to Build Technical Cyber Capabilities

- 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

How to Build 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 on active duty as determined through normal Medical Evaluation Board/Physical Evaluation Board processes
    - Most are returning service men and women who have served in combat environments such as 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

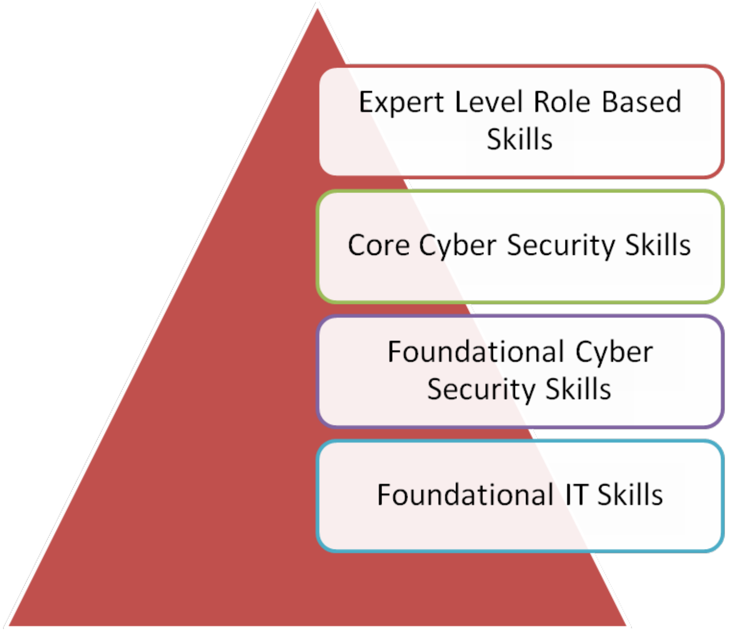
- They are dedicated, highly motivated, disciplined, and trustworthy team players who both industry and government seek as workers.

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

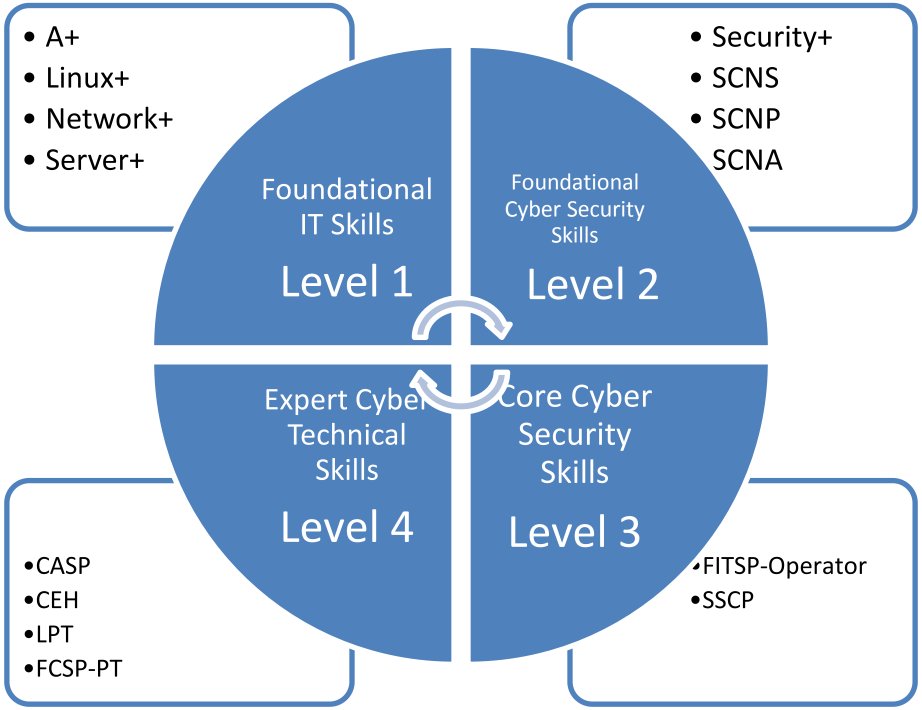
Foundational IT Skills

Wounded Warrior Training Model

- 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

Wounded Warrior Training Model

- Use of Industry Certifications



- A+
- Linux+
- Network+
- Server+

Foundational IT Skills

Level 1

Foundational Cyber Security Skills

Level 2

- Security+
- SCNS
- SCNP

SCNA

Core Cyber Security Skills

Level 3

- FITSP-Operator
- SSCP

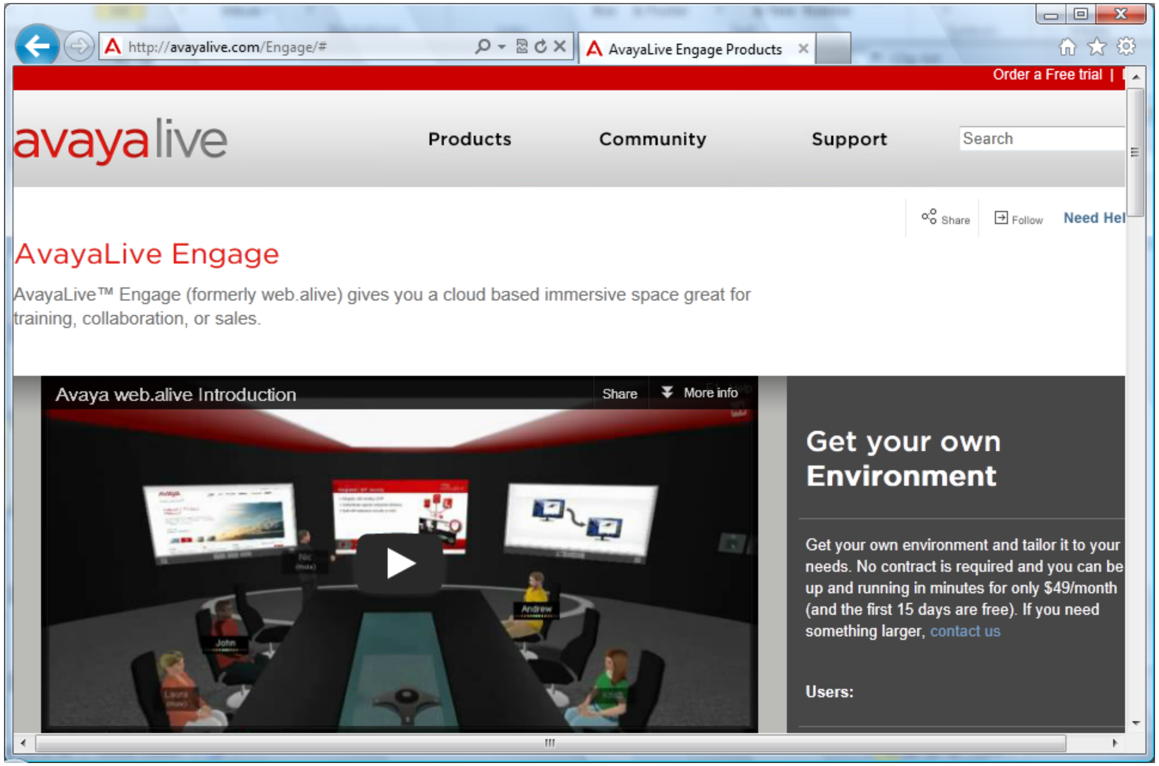
Expert Cyber Technical Skills

Level 4

- CASP
- CEH
- LPT
- FCSP-PT

Wounded Warrior Training Model

- Online Training Platform – Avaya Live



AvayaLive Engage

AvayaLive™ Engage (formerly web.alive) gives you a cloud based immersive space great for training, collaboration, or sales.

Get your own Environment

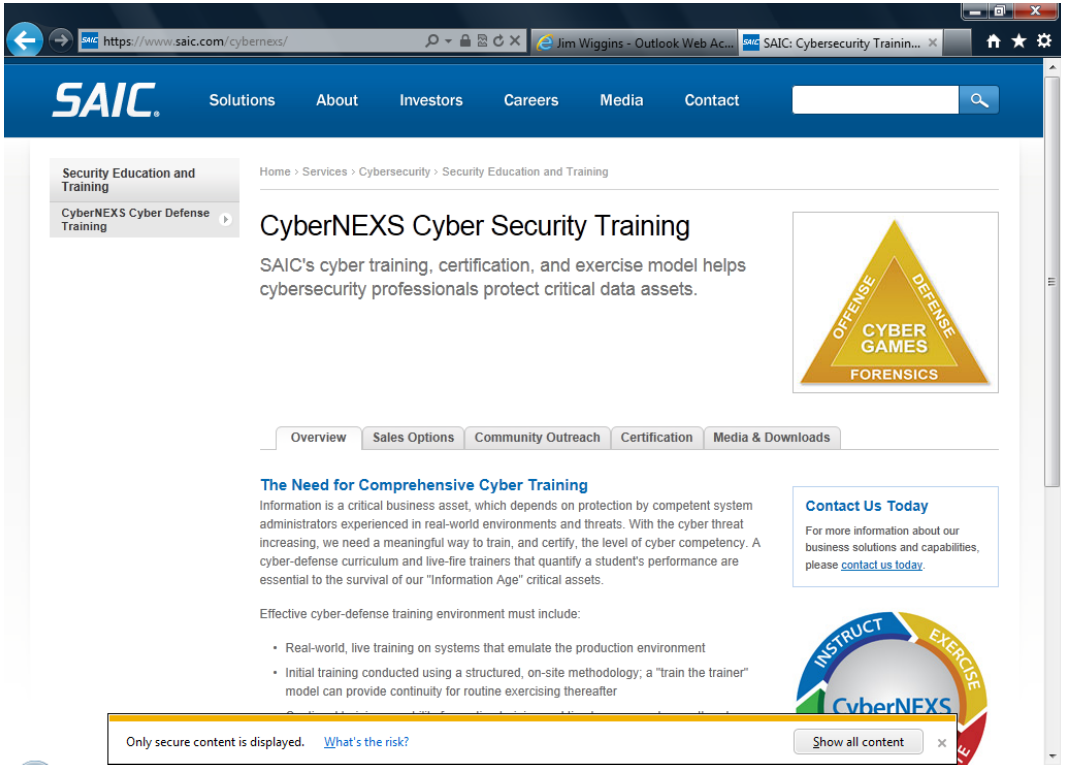
Get your own environment and tailor it to your needs. No contract is required and you can be up and running in minutes for only $49/month (and the first 15 days are free). If you need something larger, contact us

Users:

Each student has an Avatar!

Wounded Warrior Training Model

- Use Cyber Range Technologies - SAIC


https://www.saic.com/cybernexs/
Jim Wiggins - Outlook Web Ac...
SAIC: Cybersecurity Trainin...
SAIC
Solutions
About
Investors
Careers
Media
Contact
Security Education and Training
CyberNEXS Cyber Defense Training

Home › Services › Cybersecurity › Security Education and Training

CyberNEXS Cyber Security Training

SAIC's cyber training, certification, and exercise model helps cybersecurity professionals protect critical data assets.

OFFENSE
DEFENSE
CYBER GAMES
FORENSICS
Overview
Sales Options
Community Outreach
Certification
Media & Downloads

The Need for Comprehensive Cyber Training

Information is a critical business asset, which depends on protection by competent system administrators experienced in real-world environments and threats. With the cyber threat increasing, we need a meaningful way to train, and certify, the level of cyber competency. A cyber-defense curriculum and live-fire trainers that quantify a student's performance are essential to the survival of our "Information Age" critical assets.

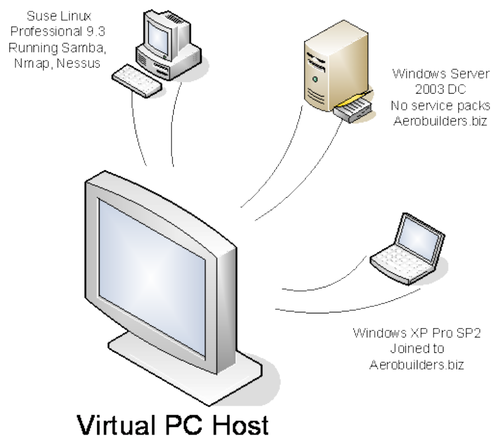
Effective cyber-defense training environment must include:

- Real-world, live training on systems that emulate the production environment
- Initial training conducted using a structured, on-site methodology; a "train the trainer" model can provide continuity for routine exercising thereafter

Contact Us Today

For more information about our business solutions and capabilities, please contact us today.

Only secure content is displayed. What's the risk?



Wounded Warrior Training Model

- Curriculum and Exercises on the Cyber Range

Role on the Cyber Range	Certification program
Help desk technician	A+
Network administrator	Network+
Network engineer	Server+
Network engineer	Linux+
Security Analyst	Security+
Security Administrator	SCNS
Security Engineer	SCNP/SCNA
Information Assurance Manager	CISSP
Information Systems Security Officer	FITSP-Operator
Blue Team Member	CEH
Red Team Member	ECSA/FCSP-Penetration Tester

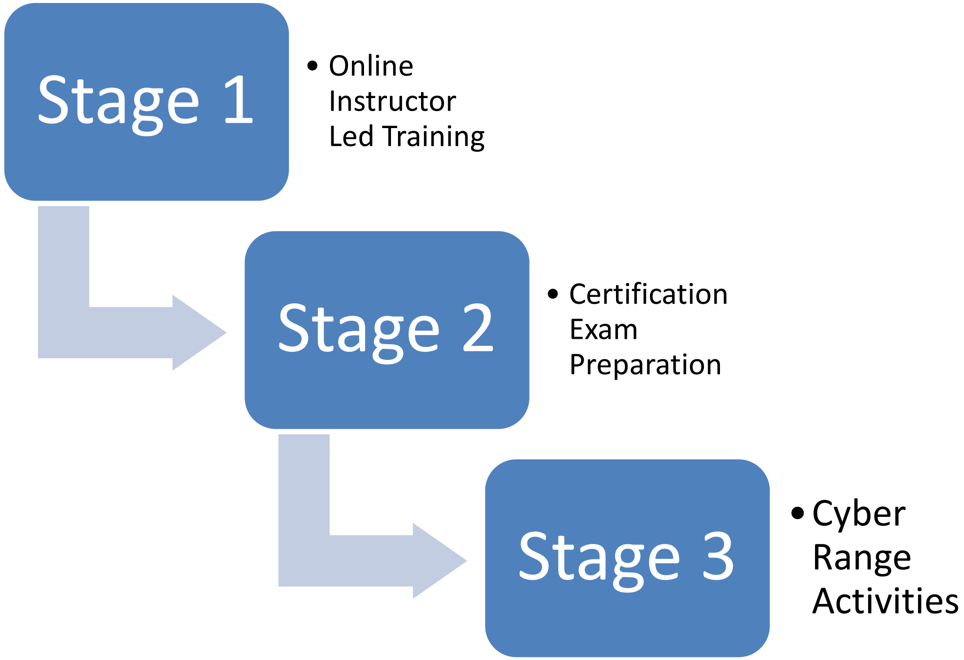
Wounded Warrior Training Model

- 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

FCSP
Federal Cyber Security Professional
Penetration Tester

Wounded Warrior Training Model

- How the Pieces Fit Together



Stage 1

- Online Instructor Led Training

Stage 2

- Certification Exam Preparation

Stage 3

- Cyber Range Activities

Program Details

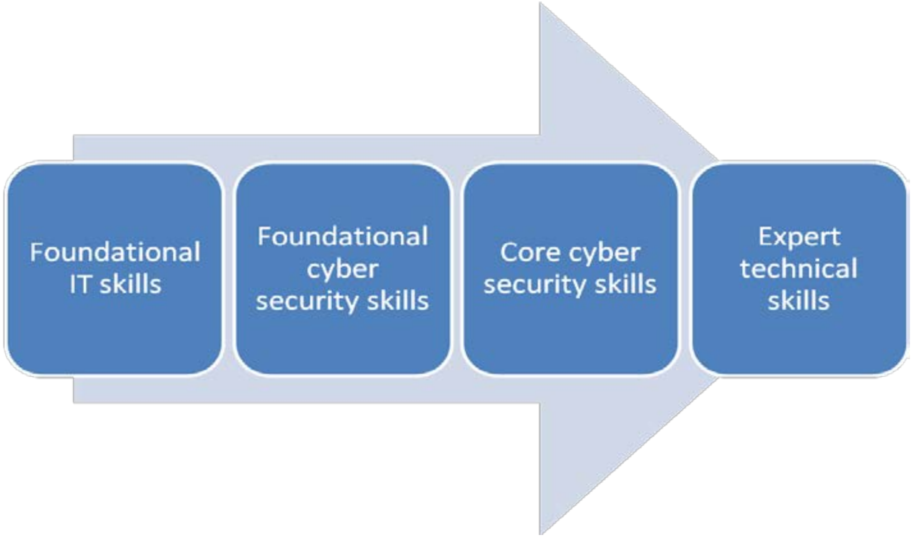
- Overview
- Training Stages
- End Game
- Schedule
- Funding Sources

Program Details

- Overview
  - Start with a small group of 20 in a pilot program
  - Use a dozen certifications
  - Use the Cyber Range
  - Use Performance Based Assessments

Program Details

- Training Stages
  - 4 stages
  - 4 quarters – 1 year



Foundational IT skills

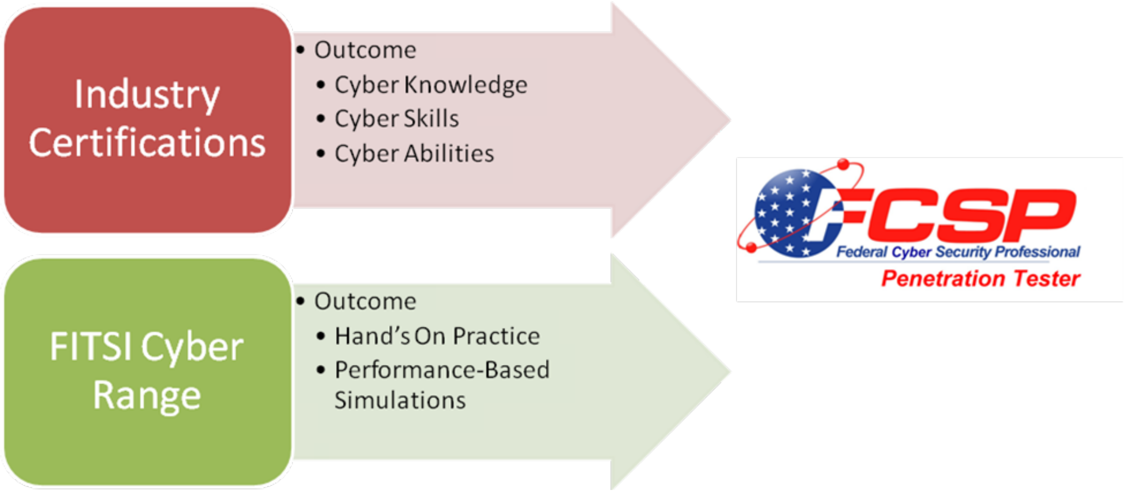
Foundational cyber security skills

Core cyber security skills

Expert technical skills

Program Details

- End Game



Industry Certifications

- Outcome
  - Cyber Knowledge
  - Cyber Skills
  - Cyber Abilities

FITSI Cyber Range

- Outcome
  - Hand's On Practice
  - Performance-Based Simulations

FCSP
Federal Cyber Security Professional
Penetration Tester

Program Details

- Schedule – Monthly Breakdown

Program	Month
A+	March 2013
Server+	April 2013
Linux+	May 2013
Network+	June 2013
Security+	July 2013
SCNS	August 2013
SCNP	September 2013

Program Details

- Schedule – Typical Month

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

Program Details

- Funding Sources
  - Initial pilot program handled with corporate/personal sponsor donations
  - Future funding to be explored as program grows

The Players

- Online Providers
  - Avaya Government Solutions
    - Provides the Online “Avatar-based” learning platform
  - SAIC
    - Provides the online cyber range

AVAYA
GOVERNMENT
SOLUTIONS

SAIC®
From Science to Solutions

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

axzo

Logical Operations

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

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

Registration Process

- 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

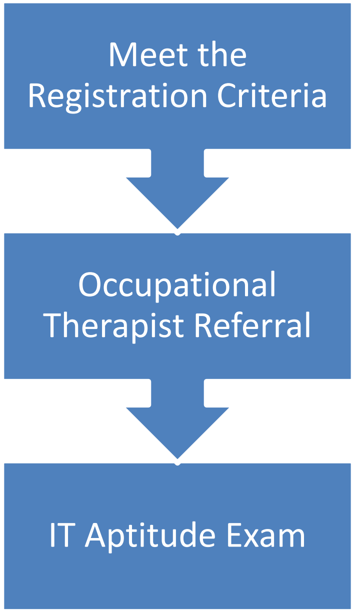
Registration Process

- 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

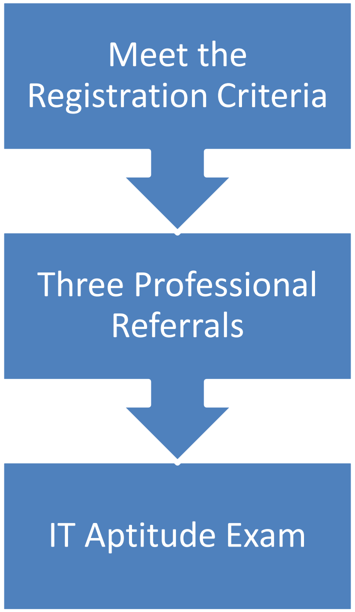


Meet the Registration Criteria

Occupational Therapist Referral

IT Aptitude Exam

Veteran



Meet the Registration Criteria

Three Professional Referrals

IT Aptitude Exam

How Can You Help?

- Three ways to help
  - Recruit a wounded warrior you may know
    - Point them to http://www.w2cca.org
  - Ask your organization to become a corporate sponsor
    - Corporate sponsorship form
      - 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
    - Personal sponsorship form
      - http://www.fitsi.org/w2cca-ps.pdf

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?

CEU/CPE Information

- Thanks for attending today's session!

- A generic webinar completion certificate can be downloaded from the following site
  - http://www.fitsi.org/w2cca-ceu-cert.pdf

- Hold onto the following:
  - Completion certificate after filling in your name
  - A copy of the email confirmation showing you registered for the webinar

Recap

- The Cyber Security Problem Space
- The Need for Technical Cyber Defenders
- How to Build Technical Cyber Capabilities
- The League of Wounded Warriors
- Wounded Warrior Training Model
- Program Details
- The Players
- The Results
- Registration Process
- How Can You Help?
- Contact Information
- Questions and Answers
- CEU/CPE Information