Cybervets

Leveraging Veterans to build the Cybersecurity Workforce

P. Shane Gallagher, PhD
SG Systems Consulting, LLC
Subcontractor to MITRE For Cyberoperations Training
shane@sg-systems.com

Aaron Burnett
Federal Lead, Centers For Medicare And Medicaid Services (CMS)
Cybersecurity Integration Ctr (CCIC)
aaron.burnett@cms.hhs.gov

NIST Cybersecurity Risk Management Conference November 7-9, 2018
About the CMS Alliance to Modernize Healthcare

The CMS Alliance to Modernize Healthcare is the first federally-funded research and development center (FFRDC) dedicated to strengthening the nation’s healthcare system. CAMH is sponsored by the Centers for Medicare & Medicaid Services (CMS) and all divisions of the Department of Health and Human Services (HHS). MITRE, an objective not-for-profit organization, operates CAMH in partnership with CMS and all HHS agencies to implement innovative ideas to solve our nation’s toughest health problems.
CAMH Contributors

SG Systems Consulting, LLC
Cyber Veterans Apprenticeship Program

Partnership between CMS, VA, and OPM
Partnership to develop a 1 year immersive pilot program that:

- Provides Knowledge Skills and Abilities (KSAs) as defined in the National Institute for Cyber Education (NICE) framework
- Provides work experience
- Facilitates Veteran transition into the civilian workforce in cybersecurity

Currently in 6th month
Sī-bƏr/vȅts

Cyber…
- Serious existential threats – cyberwarfare, cyberterrorism, cybercrime
- Driving demand signal for expert operators

Vets…
- More than just a training program
- Supporting Veteran transition with a goal of ensuring maximum employability
Organizations recognize that investment in security is a necessity

_Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades_

_Cybercrime damages is predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015_

But….
Current estimated 350,000 open cyber security positions in the U.S.

And….
Predicted global shortfall of 3.5 million cyber security jobs by 2021

Two of the ten biggest investment mistakes by organizations:
Not investing in training
Not providing the right training

**CyberVets provides both**

1. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
2. https://cybersecurityventures.com/jobs

"...the industry clearly has a massive problem regarding supply and demand." (cybersecurityventures.com)

"FBI's flagship cybersecurity program had not filled 52 of the 134 computer scientist jobs authorized under the Justice Department's Next Generation Cyber Initiative..." (Washington Post)
How?

Goal: Ensuring maximum employability by:

- Aligning to work roles, supporting job tasks, and KSAs within the Federal NICE competency framework
- Using a proven cyber talent development model ensuring graduates can actually do the job that includes:
  - Cognitive Apprenticeship
  - Problem-based Learning
Cognitive Apprenticeship

Methods of Instruction
• Modeling, Coaching, Scaffolding, Reflection, Exploration

Sequencing of Learning Content
• Global before Local, Increasing Complexity, Increasing Diversity

Social Characteristics
• Context, Community of Practice, Intrinsic Motivation, Cooperation, Collaboration

Learning Content
• Domain Knowledge, Heuristics Strategies, Control Strategies, Learning Strategies
Cognitive Apprenticeship in Action

Daily Meetups
- Scaffolding
- Reflection
- Modeling

“Fireteam” Lead
- Facilitator/Coach
- “Connect the dots”
- Reflection:
  - Journaling
  - AARs

Research/Challenge Work
- Coaching
- Scaffolding
- Exploration

“Shoulder Surfing”
- SOC
- Modeling

1 to 1 Mentoring
- Coaching

SOC™

CMS Alliance to Modernize Healthcare
Program Status

- Year long
- Immersive
- Design is guided by formative evaluation
  - Currently guided by initial six-month design and content outline
  - Second six months under development
Who are our CyberVets?

- Recently separated to retired military
- Little if any direct hands-on experience with cybersecurity
- All seeking experience
- All motivated
- All willing to spend 5 days/week 8 hours/day immersed in cybersecurity
- All active seeking employment opportunities ideally within the federal sector
CyberVet Orientation

June 11, 2018

- Introduction of key personnel and mentors
- Briefed on CMS Office of Information Technology’s (OIT) roles and functions
- CMS Tour - Cybersecurity resources and locations
- Received badges and government furnished equipment
Learning Content

Goals:
- The learner can use data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
  - **NICE Work Role: Cyber Defense Analyst (PR-DCA-001)**
    - General knowledge and skill set in cybersecurity and privacy principles.
    - Understand status and project briefing attributes at multiple levels (i.e. technical, peer, executive).
    - Prepare candidates to enter cyber workforce positions in civilian government services.

Knowledge Skills and Abilities (KSAs) and Tasks
- KSAs and Tasks are mapped to those associated with the work role of Cyber Defense Analyst
  - Each module address specific KSA
Learning Content

KSAs: K0001, K0004, K0044, K0060, K0192

- **Module 1 - Networking Essentials**
  - Gain basic understanding of networking fundamentals through research and problem solving
    - Deploy a Windows and a Linux virtual machine on a Windows 10 operating system
    - Develop and present a brief describing the characteristics (or other attributes…) of well-known ports and IPv4 classfull addressing, classless addressing, and subnetting
  - MITRE training on cybersecurity fundamentals
    - Hands-on introduction from cyber instructors at MITRE on:
      - Linux/Unix Security
      - Windows Enterprise Security
      - Applied Network Security
      - Network Security (Advanced)
Learning Content

KSAs: K0013, K0058, K0191, K0192

- **Module 2 – Security Operations Center Analyst Apprentice**
  - Understand Roles of the Cyber Defense Analyst (CDA)
  - Introduction to Cyber defense tools
  - Shadow CDA to analyze events for the purpose of mitigating threats
  - Achieve baseline knowledge of SOC analysts tools, techniques, and procedures
Learning Content

- **Module 3 – Advanced Networking/Engineering**
  - Understand adequate access controls based on principles of least privilege and need-to-know.
  - Identify security gaps in security architecture.
  - Provide recommendations for addressing security gaps for inclusion in the risk mitigation strategy.
  - Using existing tools within the CMS SOC environment, identify sources of cyber defense data and interpret signatures from the source identified
    - Deploy Security Onion suite in VM
    - Deploy Apache server in VM and setup accounts
    - Automate network traffic
    - Compare tools visibility
    - Provide leadership briefing
Learning Content

Module 4 – Cybersecurity Concepts/CDM
- Understand the basic principles required to use tools for continual monitoring and analysis
- Create and review CDM capability reports and identify defects in security status of assets and recognize trends
- Analyze the security architecture for the CDM and ISCM program to understand capability usage, limitations, tuning, and optimization techniques

KSAs: K0005, K0006, K0013, K0070, K0074, K0624, S0078, S0167, S0169, S0367, A0015, A0123
Learning Content

- Problem-based learning using challenges
- Gamified
- Online and available 24/7
External Activities

- **HHS Summer Tech Exchange 2018**
  - June 14, 2018
  - National Institute of Health (NIH), Bethesda, MD

- **CMS CyberWorks**
  - June 21, 2018
  - CMS Auditorium, Baltimore, MD

- **National Cryptologic Museum**
  - July 18, 2018
  - Fort Meade, MD
Netwars – September 7, 2018

- Facilitated by SANS at CMS CCIC and HHS HQ
- Defensive Jeopardy-style CTF-like event
- 54 multiagency participants
- 5 CyberVets participated in different teams
Mentoring

- All assigned to a mentor
- Most have met at least once
- Areas mentors are helping:
  - HR/federal hiring process
  - Policy
  - Job expectations
- Areas of improvement:
  - More mentor availability
  - More proactive stance from Vets
  - Matching areas of interest
Evaluation

Ongoing Formative and Summative Evaluation
Ensure all Program Goals are Met

**GOALS**

- **Informal**
  - Employment for graduates within the cybersecurity sector
  - Expanded qualified applicant pool for HHS
  - Cybersecurity qualifications for graduates’ resumes
  - Students are capable of performing cybersecurity roles

- **Formal**
  - Provide a successful one-year apprenticeship program for veterans to gain hands-on experience within the CMS Cybersecurity Integration Center (CCIC)
  - Integrate a balanced curriculum focused on getting the veterans engaged on real work problems while challenging them to develop their skills as part of cohort
  - Develop candidates for cybersecurity vacancies in critical positions from a diversity of backgrounds
Method

Program Goals

Alignment

Curriculum Improvement

- Level 4: Impact
  - Organizational impact due to training

- Level 3: Performance
  - Workplace changes in performance due to training

- Level 2: Learning
  - Learning occurring as a result of training

- Level 1: Reaction
  - Learner/stakeholder reactions to the training program

- Provides levels of evaluation
  - Levels have differing goals
  - Levels have differing methods
  - Levels should be aligned in an overall strategy

- Focusing on Levels 1 & 2 with insight into Level 3

- Data collected:
  - Background and motivation
  - Self-efficacy
  - Goal commitment
  - Knowledge and performance
Findings

Self-Efficacy & Goal Commitment

5 Week Reaction ScoreCard
Findings

Reaction #2 - 5 Months

- **SOC Tour rating:**
  - Passive
  - Placement in curriculum
  - Wanting something different

- **Motivation:**
  - Still high but dropped some
  - Personal and financial concerns
  - Length of program
  - Mismatched expectations
Findings

Pre-Test Scores

Networking Essentials Pre-Test

Module Pre-Test Scores
## Design Recommendations Moving Ahead

<table>
<thead>
<tr>
<th>Recommendation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure all learning activities incorporate authentic real-world challenges or problem-solving or be in preparation for solving progressively more difficult challenges or problems</td>
<td>✔</td>
</tr>
<tr>
<td>Ensure all challenges integrate knowledge and skills with other program components</td>
<td>✔</td>
</tr>
<tr>
<td>Full-time dedicated facilitator and coach integrating activities, self-reflection, &amp; scaffolding</td>
<td>✔</td>
</tr>
<tr>
<td>Consider deleting or restructuring SOC Tours</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>Incorporate daily individual and group self-reflection activities</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>Use direct instruction deliberately to prepare for challenges or events where it can be readily applied</td>
<td>✔</td>
</tr>
<tr>
<td>Use outside experts for special topics seminars as another form of direct instruction</td>
<td>✔</td>
</tr>
<tr>
<td>Ensure that the facilitator integrates any direct instruction back within the problem-solving environment handily</td>
<td>✔</td>
</tr>
</tbody>
</table>
Next Steps
# Roadmap CY 2018

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue with Advanced Networking Module</td>
<td>35 days</td>
<td>Mon 9/10/18</td>
<td>Fri 10/26/18</td>
</tr>
<tr>
<td>Escalate Foundations into Reverse Engineering (overlapping with CDM for 1 wk)</td>
<td>20 days</td>
<td>Wed 10/10/18</td>
<td>Tue 11/6/18</td>
</tr>
<tr>
<td>Special Topic White Board sessions (2 day/mo)</td>
<td>45 days</td>
<td>Mon 10/22/18</td>
<td>Fri 12/21/18</td>
</tr>
<tr>
<td>Begin SANS SEC 401 1 Day/Wk</td>
<td>26 days</td>
<td>Mon 10/29/18</td>
<td>Mon 12/3/18</td>
</tr>
<tr>
<td>CDM (as originally scheduled overlapping with Escalate)</td>
<td>40 days</td>
<td>Mon 10/29/18</td>
<td>Fri 12/21/18</td>
</tr>
<tr>
<td>Escalate Network Linux and Windows Exploitation (overlapping CDM)</td>
<td>25 days</td>
<td>Wed 11/7/18</td>
<td>Tue 12/11/18</td>
</tr>
<tr>
<td>SANS Review and Practice Testing</td>
<td>15 days</td>
<td>Mon 11/12/18</td>
<td>Fri 11/30/18</td>
</tr>
<tr>
<td>SANS SEC 401 Cert Testing</td>
<td>14 days</td>
<td>Tue 12/4/18</td>
<td>Fri 12/21/18</td>
</tr>
</tbody>
</table>

Topics in 2019 may include:
- Forensics/Malware Analysis
- Incident Management
- Advanced Web/Linux/Windows exploitations
- Advanced Reverse Engineering
- Compliance
- Policy
Data Rights Notice

NOTICE

This software/technical data was produced for the U. S. Government under Contract Number 75FCMC18D0047, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data-General.

No other use other than that granted to the U. S. Government, or to those acting on behalf of the U. S. Government under that Clause is authorized without the express written permission of The MITRE Corporation.