Cybersecurity: The Current State

**Skills Mismatch**
- Emphasis on theory over practice
  - Education focus on theoretical over applied knowledge
  - Lack of real-world skills
  - 95% of security incidents involve human error

**Threat Proliferation**
- Outpacing ability to respond
  - “97% of Fortune 500 companies have been hacked. The other 3% have too, they just don’t know it”
  - Average annualized cost of cyber incidents for U.S. companies is $15.4 million

**Increasing Risk**
- Increasing data breaches
- Increasing vulnerabilities

**Talent Crisis**
- Severe shortage of skills
  - 240,000 open positions in 12 months
  - 91% increase in 5 years (2010-2014)
  - Fast growth across industry verticals (e.g. Finance, HC, Retail Trade)

**Undervalued**
- in the organization
  - C-suite understanding remains weak
  - “Rarely has something been so important and so talked about with less clarity and less understanding”

“97% of Fortune 500 companies have been hacked. The other 3% have too, they just don’t know it”
A Systems Approach is Needed

Cyber Human Capital Management Strategy

Talent Lifecycle

Training & Development

Community Resources & Thought Leadership

CT SOLUTIONS
Strategy Consulting
Organization Design
CT Career Mapping

CT SOLUTIONS
VetSuccess Academies
Women’s Academies
Skills and Aptitude Assessments

CT SOLUTIONS
Technical Training
Management Training
Onboarding & Retention Strategy

CT INITIATIVES
Collaboratives
Summits
White Papers
Community Investment
VetSuccess

The VetSuccess program provides transitioning US military veterans with advanced technical training, certifications, and connections to high-paying jobs in cybersecurity.
Fast Track: Three steps to a cybersecurity career

1. Qualify
   Take the qualifying exam, complete the application process, and interview with the admissions committee.

2. Train & Certify
   Develop practical, hands-on skills by completing world-class SANS training courses. Two and three course programs available. Earn GIAC certifications, recognized by employers around the world.

3. Employ
   Earn a guaranteed employment opportunity at Sponsored Academies (agreed to an anticipated minimum two-year term), or seek multiple non-guaranteed opportunities at Open Academies.
“We’ve been thrilled with the opportunity to participate in the VetSuccess Academy. I can’t say enough about the cooperation and tireless efforts by SANS to make this program successful for both veterans and employers.”

-Arlin Halstead, VP, Human Resources

Participant Profile (2015 Pilot Cohorts)

18 United States Veterans
13 US Air Force
3 US Army
1 US Marines
1 US Navy

Experience
16 years average in Information Technology

<table>
<thead>
<tr>
<th>STARTING SALARY</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>$70-90K</td>
<td>8</td>
</tr>
<tr>
<td>$90-120K</td>
<td>8</td>
</tr>
<tr>
<td>$120K+</td>
<td>2</td>
</tr>
</tbody>
</table>

37 additional candidates currently completing the program. Six Academies in the planning phase.

Contact: mshuftan@sans.org
Women: Bringing Diversity to Cyber Security

Academy Goals

• Provide educational opportunities to women interested in cybersecurity fields

• Increase gender diversity in the information security work force

• Meet needs of critical national infrastructure firms, industry, law enforcement, and intelligence agencies

• Match talented, employment-ready women with top cybersecurity employers
Women: Bringing Diversity to Cyber Security

Recruiting:
• Partnership with the National Center For Women in Information Technology (NCWIT)
• 300 inquiries with 200 qualified candidates taking the Aptitude Exam
• 90 high scoring candidates identified and invited to submit resumes and transcripts for interviews
• 19 top candidates selected for the initial cohort

Curriculum:
• SEC 401 was taken live as cohorts at three SANS conferences in May and June
• SEC 504 will be taken on demand after passaged of GSEC; third elective will be offered to successful candidates as well
• Expected graduation in September 2016

Employment:
• Graduates will be matched with prospective employers.
• We are currently looking for additional employers to participate as well as to be named sponsors of the program
### Essential tools to assess and develop talent

<table>
<thead>
<tr>
<th>CYBERTALENT ENHANCED (CTE)</th>
<th>CYBER DEFENSE</th>
<th>PENETRATION TESTING</th>
<th>APPLICATION SECURITY</th>
<th>DIGITAL FORENSICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides predictability for likelihood for success in cybersecurity</td>
<td>Cornerstone Information Security</td>
<td>Cornerstone Penetration Testing</td>
<td>Web technologies &amp; service</td>
<td>Cornerstone Digital Forensics</td>
</tr>
<tr>
<td></td>
<td>Advanced Information Security Principles</td>
<td>Advanced Penetration Testing Principles</td>
<td></td>
<td>Advanced Digital Forensics Principles</td>
</tr>
</tbody>
</table>

**Free Demo:** [sans.org/cybertalent/free-demo](https://sans.org/cybertalent/free-demo)
How to use CyberTalent Enhanced

CyberTalent Enhanced (CTE) was developed to determine if an individual has the aptitude and basic skills to succeed in information security, as demonstrated on various GIAC exams such as GSEC (SANS SEC401 training) and GCIH (SANS SEC504 training). The exam was developed using common measurement and testing standards to support a validity claim for the CTE test. The 50 item exam was developed by qualified information security subject matter experts, and predicts potential success on GIAC exams. With hundreds of test takers to date, the assessment shows a strong correlation with success in passing GIAC certifications.
Aptitude (25 questions)

**Information Security Aptitude:** The aptitude of the candidate toward general information security principles will be observed

Basic InfoSec Skills (25 questions)

**Networking Concepts Domain:** The candidate will demonstrate a thorough understanding of networking design, hardware, and common protocols such as IPv4, IPv6, TCP, UDP, and ICMP, and will be able to read network packets.

**Defense in Depth Domain:** The candidate will demonstrate a thorough understanding of defense-in-depth such as anti-malware, access control, authentication, and application security.

**Internet Security Technologies Domain:** The candidate will demonstrate a thorough understanding of communications security including cryptography, VPNs, PKI, and data encryption.

**Communications Security Domain:** The candidate will demonstrate a thorough understanding of common Internet security technologies such as firewalls, and processes such as vulnerability management, intrusion detection and prevention, and risk management.

**Operating Systems Security Domain:** The candidate will demonstrate a thorough understanding of common operating system security for Windows and Linux, auditing, permissions, and security configuration.
How CyberTalent Assessments Help

Improve your training ROI

Benchmark your Team

• Establish a baseline to more effectively manage and measure progress.

• Take a portfolio management approach to overall IS performance.

Personnel Development Plans

• Receive clear views of where individual team members are strong and where skills need development.

• Eliminate wasted and ineffective training costs.

Simple Web-based Reports

• Generate an easy to use report summarizing the individual and team performance.
Top talent, in one place, with one click

**Pre-Screened Applicants**
- Access to SANS CyberTalent Assessments provided to all job seekers

**Cost-effective Recruiting & Hiring**
- Innovative virtual format includes dynamic chat with viewable profiles and resumes, and next steps mechanisms to facilitate follow-up emails, interviews, etc.
Max Shuftan: mshuftan@sans.org
Jim Michaud:  jmichaud@sans.org

Web: sans.org/cybertalent