Keeping Your SOCs Full

May 26, 2016

Strengthening Capacity in Cyber Talent

sans.org/cybertalent
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”

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)

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”

95% of security incidents involve human error.
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
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.
Graduate Profile to Date

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

Experience
- 16 years average in Information Technology
- 9 years average in Cybersecurity

Security Clearances
- SECRET
- TOP SECRET
- TS/SCI
- TS/SCI with CI Polygraph

Education
- Master’s Degrees
  - Systems Technology
  - Management Information Systems
  - Business Administration
- Bachelor’s Degrees
  - Information Technology Management
  - Network Security
  - Computer and Information Science
  - B.S. in Cybersecurity
  - Criminal Justice
  - Multimedia
  - Computer Information Systems
- Associate Degrees
  - Environmental Systems Technology
  - Electronic Systems Technology

50 Additional Candidates currently in the program
Immediate impact, Hands-on skills

“The relevance of the hands-on labs and exercises was clearly evident as we applied the skills we learned to real and recent scenarios from the security community... This instruction was as close to front line operations as one can get without being in a production work center.”

Edmond Russell
Academy graduate, recently hired by Solutionary

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

Talent Crisis
Severe shortage of skills
- 240,000 open positions in 12 months
- 91% increase in 5 years (2010-2014)
Joseph Robbins

“…without the Academy I’d have finished my degree and would still be looking for a job. Instead, everything worked out and I’m right where I want to be”

Military
US Air Force
24 years active duty, Master Sergeant, retired
Electronics Technology - radio systems repair, Air traffic control systems, etc.

Education
Bachelor’s in Computer Science, U MD, 3.9GPA
Master’s in Cyber, U of MD 4.0 GPA

Certifications
- GSEC Security Essentials
- GCIA Intrusion Analyst
- GCID Incident Handler
- EC council Hacking for Forensics

On Academy Training
“SANS gave me the practical hands-on experience. My master’s degree didn’t teach me what I had to do. It was theory - papers, research, policy. Employers want the certs and real-world experience”.

At Home
“I run my own servers, and have a Pen Testing Lab I built myself”

What’s Next
“I’m signing up for my next SANS course - “Web App Pen Testing.”

Currently
Web Security Engineer
at ISHPI

SANS VetSuccess Video: https://www.youtube.com/watch?v=A8PYwaoCxCE&rel=0
Women: Building a diverse industry

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: Building a diverse industry

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
• 19 candidates participating in the initial cohorts at three SANS conferences in May and June

Curriculum:
• SEC 401 & GSEC will be taken live as a cohort at three SANS events in May and June
• SEC 504 and & GCIH taken on demand after 401 is completed
• A third optional elective will be offered to successful candidates as well

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>APTITUDE</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
## Assessments: How they help

### Increase Hiring Success
- Identify candidates with high likelihood of success in cybersecurity
- *Performance on SANS CTE assessments shows strong positive correlation with performance on GIAC exams. (limited sample size)*

### Improve Training ROI
- Benchmark your team. Map strengths and areas of development to manage talent as a portfolio
- Develop personal training plans. Eliminate wasted and misaligned training costs
- Work from simple, easy to use web-based reporting

### Ensure Contractor Expertise
- Simple, reliable, cost-effective way to confirm contractors’ skills
Top talent, in one place, with one click

<table>
<thead>
<tr>
<th>Pre-Screened Applicants</th>
<th>Access to SANS CyberTalent Assessments provided to all job seekers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost-effective Recruiting &amp; Hiring</td>
<td>Innovative virtual format includes dynamic chat with viewable profiles and resumes, and next steps mechanisms to facilitate follow-up emails, interviews, etc.</td>
</tr>
</tbody>
</table>
Search, assess, find the talent you need

- A simple, easy to use database resource that helps employers search, assess, and find top talent faster and for less cost
- Connects individuals with cybersecurity experience to employers in the information security industry
- Initial emphasis on transitioning veterans with skills and experience in cybersecurity

SANS CTE = Better Data = Better Connection

- SANS CyberTalent Enhanced (CTE) offered to all members of the CyberTalent Connection database
- Provides employers with improved data and insights available only through CyberTalent Connection
- Working with new placement firm partner NinjaJobs on additional applications for the data base
Max Shuftan: mshuftan@sans.org
Jim Michaud: jmichaud@sans.org

Web: sans.org/cybertalent