A NICE WAY TO FIND AND KEEP CYBERSECURITY WORKERS

Greg Witte  
Sr. Cybersecurity Engineer  
G2, Inc.  
@TheNetworkGuy

Tom Conkle  
Cybersecurity Engineer  
G2, Inc.  
@TomConkle
In this digital world, it is critical that we train, hire, and retain top quality cyber workforce.
The National Initiative for Cybersecurity Education (NICE)

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.
The NICE Strategic Plan goals for improving awareness and education
NICE supports the cyber workforce lifecycle

- Educate with effective curricula
- Describe needs (e.g., job postings)
- Hire to Fit based on complete descriptions
- Consistently and effectively evaluate staff / vendors
- Retain effective workers and improve skills & abilities
Failure to hire, train, and develop qualified staff has negative effects

Has a shortage of cybersecurity skills had a negative effect on your organization?

- We can’t maintain an adequate staff of cybersecurity professionals: 35%
- We are a target for hackers as they know our cybersecurity is not strong enough: 22%
- We’ve lost proprietary data through cyberattacks: 17%
- We’ve suffered reputational damage: 33%
- We’ve had a reduced ability to create new IP for products and services

Certs are critical, but yesterday’s ways of training & hiring must improve

Certification is one great way to demonstrate acquired abilities and for employers to help quickly identify potential hires with needed qualifications

Source: http://becomeacybersecurity.expert
Cybersecurity activities are supported by many roles.
The Struggle is Real, but the Glass is ½ Full

State of Cyber Security 2017
Part 1: Current Trends In Workforce Development

Abstract

State of Cyber Security 2017 reports the results of the annual global cyber security survey, conducted in October 2016. The survey results bolster the belief that the field of cyber security remains dynamic and relevant during its formative years. Weekly news headlines confirm that cyberattacks are not a seasonal threat or dependent on specific industries or certain attributes, but are constant and could occur at any time in any environment. Similarly, thought pieces, reports, and studies emphasize understanding of the cyber security industry through the lens of those who operate in the industry and practitioners. iSACA is preparing the survey results in a series of reports that focus on individual facets. This report is the first in the iSACA State of Cyber Security 2017 series and presents findings related to cyber security workforce development and the current trends.

© 2017 ISACA. All Rights Reserved.
There are significant benefits to a more diverse cybersecurity workforce
NIST released the NICE Framework in 2017

- NIST Special Publication 800-181
  - NICE Cybersecurity Workforce Framework
NIST 800-181 categorizes cybersecurity roles

NICE Framework Categories

- Securely Provision
- Operate and Maintain
- Oversee and Govern
- Protect and Defend
- Analyze
- Collect and Operate
- Investigate
The NICE Framework builds a cybersecurity capable and ready workforce
A sample of a recent cyber defense incident responder requisition

Required Knowledge, Skills and Abilities
• 3+ years of experience with network security
• Knowledge of TCP/IP communications and how common protocols and applications work at the network level
• Knowledge of network monitoring, analysis, troubleshooting, and configuration control technologies
• Ability to learn and operate in a dynamic environment
• Ability to demonstrate analytical expertise, close attention to detail, critical thinking, logic, and solution orientation and to learn and adapt quickly
• TS/SCI clearance
• Security+ CE, and CEH or GCIH Certification

Additional Qualifications:
• Experience with working in a 24/7 SOC environment
• Experience in managing cases with enterprise SIEM and logging systems
• Possession of excellent oral and written communication skills
• BA or BS degree in Engineering, CS, Information Security, or Information Systems
Let’s walk through the NICE Workforce Framework tool

<table>
<thead>
<tr>
<th>NICE Framework Specialty Areas and Work Role Table of Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NICE Specialty Area</td>
<td>Work Role</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Cybersecurity Defense Analysis (CDA)</td>
<td>Cyber Defense Analyst</td>
</tr>
<tr>
<td>Cybersecurity Defense Infrastructure Support (INF)</td>
<td>Cyber Defense Infrastructure Support Specialist</td>
</tr>
<tr>
<td>Incident Response (CIR)</td>
<td>Cyber Defense Incident Responder</td>
</tr>
<tr>
<td>NICE Specialty Area Definition</td>
<td>IT Investment/Portfolio Manager</td>
</tr>
<tr>
<td></td>
<td>IT Program Auditor</td>
</tr>
</tbody>
</table>
There are a broad range of work roles supporting incident response and recovery.

Figure 3-1. Incident Response Life Cycle
Online tools help track our progress in closing the cybersecurity workforce gaps

Cybersecurity Career Pathway

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skill sets associated with each role.
NICE is about Partnership and Collaboration

- **NICE Staff**
  - Rodney Petersen, Director
  - Bill Newhouse, Deputy Director
  - Danielle Santos, Program Manager
  - Marian Merritt, Lead - Industry Engagement
  - Davina Pruitt-Mentle, Lead – Academic Engagement
  - Clarence Williams, Lead - Government Engagement

- **NICE Interagency Coordinating Council (ICC)**

- **Cybersecurity Credentials Collaborative (C3)**

- **NICE Working Group and Sub-Groups**
  - K-12
  - Collegiate
  - Competitions
  - Training and Certifications
  - Workforce Management

niceframework@nist.gov
Working together we can help achieve the NICE strategic goals

- Using the tools and collaboration described, NICE helps organizations to create, connect, retain, and improve cybersecurity professionals that are qualified, effective, and satisfied.
Time to go hire train and prepare your staff for the exciting challenges in cybersecurity

- Next week you should:
  - Review NIST 800-181 and familiarize yourself with the roles, tasks and KSAs

- In the first three months following this presentation you should:
  - Align training programs with the roles and tasks within NIST 800-181
  - Revise existing requisitions to properly identify the type of staff needed for the position

- Within six months you should:
  - Share your knowledge required the KSAs and how your organization uses them to standardize hiring and performance reporting reviews
We are happy to answer your questions

Greg Witte
Senior Security Engineer
greg.witte@g2-inc.com
(301) 346-2385

Tom Conkle
Cybersecurity Engineer
tom.conkle@g2-inc.com
(301) 575-5139