Global ICT Capacity Building Symposium 2018
Developing Skills for the Digital Economy and Society

Mr. Phillip Stoner, Director, Cyber Solutions Group
Why Cybersecurity?

- 75% US households have PC, Laptop, Mobile device w/ broadband Internet – US Census (Sep 2017)
- Ransomware – 39% of malware-related breaches – Verizon DBIR, 2018
  – 68% of breaches took several months to discover
- The increasing theft of PII, Financial, Critical IP and illegal access of the world’s critical infrastructure
AG6  Top not Topple  
Alan Gush, 14/06/2018

PS6  fixed  
Phil Stoner, 14/06/2018

AG7  The third bullet doesn't answer why cybersecurity is becoming a core topic. Its a by product of why it's becoming important  
Alan Gush, 14/06/2018

PS7  agree, removed  
Phil Stoner, 14/06/2018
The Reality Is...

The Current Approach to Capacity Building in Cybersecurity is Broken
But Why?

• Higher Education = Limited Abilities
• Lack of Competent Talent Pool
• Poor Candidate Screening and Hiring
• Current Workforce Management
The Solution?

Implement Competency-Based Assessment and Training Solutions!
NICE Cybersecurity Workforce Framework (NCWF)

- 7 Categories, 30+ Specialty Areas, 50+ Work Roles
- Baselines Knowledge, Skills, Abilities, Tasks (KSAT’s)
- Reference Resource for Cybersecurity Workforce Development

- NCWF Version 1.0 posted in April 2013
- NCWF Version 2.0 posted in May 2014
- Special Pub. 800-181 released Aug 2017
<table>
<thead>
<tr>
<th>AG2</th>
<th>There is update 800-181 i believe</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alan Gush, 30/05/2018</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PS3</th>
<th>done</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Phil Stoner, 30/05/2018</td>
</tr>
</tbody>
</table>
NCWF – Core to Capable & Ready Cybersecurity Workforce

NCWF

Lexicon

Criticality Analysis

Proficiency Analysis

Workforce Identification, Tracking & Reporting

Human Capital Planning

Career Progression

Standardized Development of Position Descriptions

Qualification Requirements

Training Requirements and Standards

Capable and Ready Cybersecurity Workforce
## Work Role Example

<table>
<thead>
<tr>
<th>Work Role Name</th>
<th>Cyber Defense Analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Role ID</td>
<td>PR-CDA-001</td>
</tr>
<tr>
<td>Specialty Area</td>
<td>Cyber Defense Analysis (CDA)</td>
</tr>
<tr>
<td>Category</td>
<td>Protect and Defend (PR)</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>Uses 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.</td>
</tr>
<tr>
<td>Tasks</td>
<td>T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548</td>
</tr>
</tbody>
</table>

### Knowledge


### Skills

- S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370

### Abilities

- A0010, A0015, A0066, A0123, A0128, A0159

---

**K0167** | Knowledge of system administration, network and operating system hardening techniques

**S0057** | Skill in using protocol analyzers

**A0128** | Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies
AG3  Give example of a KSAT..
   Alan Gush, 30/05/2018

PS2  done
   Phil Stoner, 30/05/2018
Individuals
Example: Cyber Defense Analyst

Cyber Defense Analyst – Team Avg

<table>
<thead>
<tr>
<th>Capability</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Attack Analysis</td>
<td>82</td>
</tr>
<tr>
<td>Network Defense Analysis</td>
<td>91</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>65</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>81</td>
</tr>
<tr>
<td>Protocol Analysis</td>
<td>80</td>
</tr>
</tbody>
</table>

John Smith

Jane Doe

<table>
<thead>
<tr>
<th>Capability</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Attack Analysis</td>
<td>62</td>
</tr>
<tr>
<td>Network Defense Analysis</td>
<td>75</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>51</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>81</td>
</tr>
<tr>
<td>Protocol Analysis</td>
<td>70</td>
</tr>
</tbody>
</table>

Network Attack Analysis
Network Defense Analysis
Incident Handling
Intrusion Detection
Protocol Analysis
Methodology

- Linux Terminal Window
- Visual Studio “Python” Script for Website “Banner Grabber”
- Mozilla Firefox Window
- Video, Alerts and Supplemental Information
- Step by Step Instructions
Skills Assessment Goal

It’s really simple...

Assess → Train → Plan
AG4  Add arrow to show circular flow.
Alan Gush, 30/05/2018

PS4  done
Phil Stoner, 30/05/2018
Team
Example: SOC Team
AG5  Increase size of boxes so you can actually see the descriptions
    Alan Gush, 30/05/2018

PS5  best i can do the shit is all linked
    Phil Stoner, 30/05/2018
Conclusion

Cybersecurity is now at the forefront of concerns for Government and Commercial Enterprise across the globe.

Current Size of Competent Workforce is Woefully Inadequate.

Hands-on Competency-based Solutions can Quickly and Effectively Assist to Solve this.

Higher Education Needs to Adapt to Produce Job-Ready Cybersecurity Professionals.