



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

Slide 2

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?

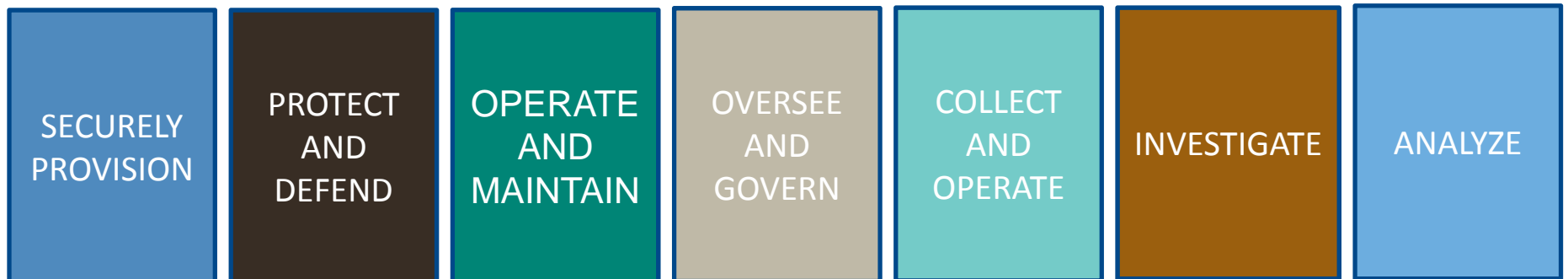
- **Higher Education = Limited Abilities**
- **Lack of Competent Talent Pool**
- **Poor Candidate Screening and Hiring**
- **Current Workforce Management**

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

Slide 6

AG2

There is update 800-181 i believe

Alan Gush, 30/05/2018

PS3

done

Phil Stoner, 30/05/2018

NCWF – Core to Capable & Ready Cybersecurity Workforce



Work Role Example

Work Role Name	Cyber Defense Analyst
Work Role ID	PR-CDA-001
Specialty Area	Cyber Defense Analysis (CDA)
Category	Protect and Defend (PR)
Work Role Description	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.
Tasks	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
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
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

Slide 8

AG3

Give example of a KSAT..

Alan Gush, 30/05/2018

PS2

done

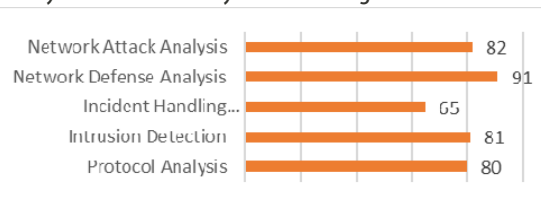
Phil Stoner, 30/05/2018



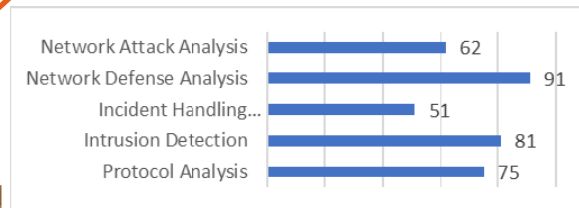
Individuals

Example: Cyber Defense Analyst

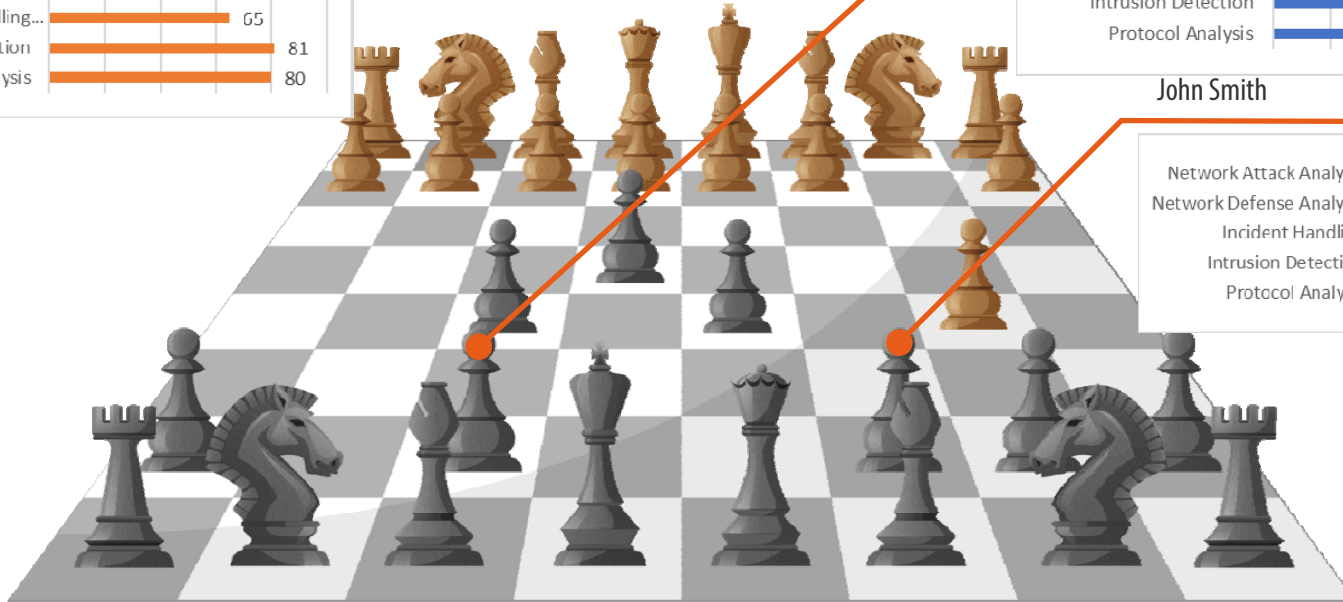
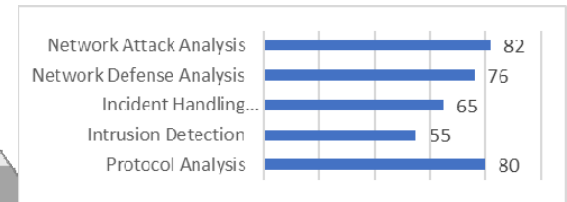
Cyber Defense Analyst – Team Avg



Jane Doe



John Smith



Methodology

The screenshot shows a Kali Linux desktop environment with several windows open. A Linux Terminal Window displays a list of connections to various services. A Visual Studio Code window shows a Python script named 'banner_grabber_mult.py' with the following code:

```
1 import socket
2 import sys
3
4 def bannergrab(ip, port):
5     try:
6         s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
7         s.connect((ip, port))
8         output = s.recv(1024)
9         outputBanner(output, ip, port)
10        print "Successfully added to Banner"
11        return True
12    except:
13        print "[ ] Failed"
14
15 def outputBanner(output, ip, port):
16     try:
17         f=open('BannerTargets.txt', 'a')
18         infoForFiles(ip) + " " + str(port)
19         f.write(infoForFile)
20         f.close()
21         print "[ ] Success. Banner added"
22     except:
23         sys.exit("Error writing file")
24
25 def main():
26     count=0
27     answer = "y"
28     while answer == "y":
29         ip = raw_input("What IP would you like to target? ")
30         port = int(raw_input("What port would you like to target? "))
31         bannergrab(ip, port)
32         answer = raw_input("Continue? y or n: ")
33
34     print "Goodbye..."
35
36 if __name__ == "__main__":
```

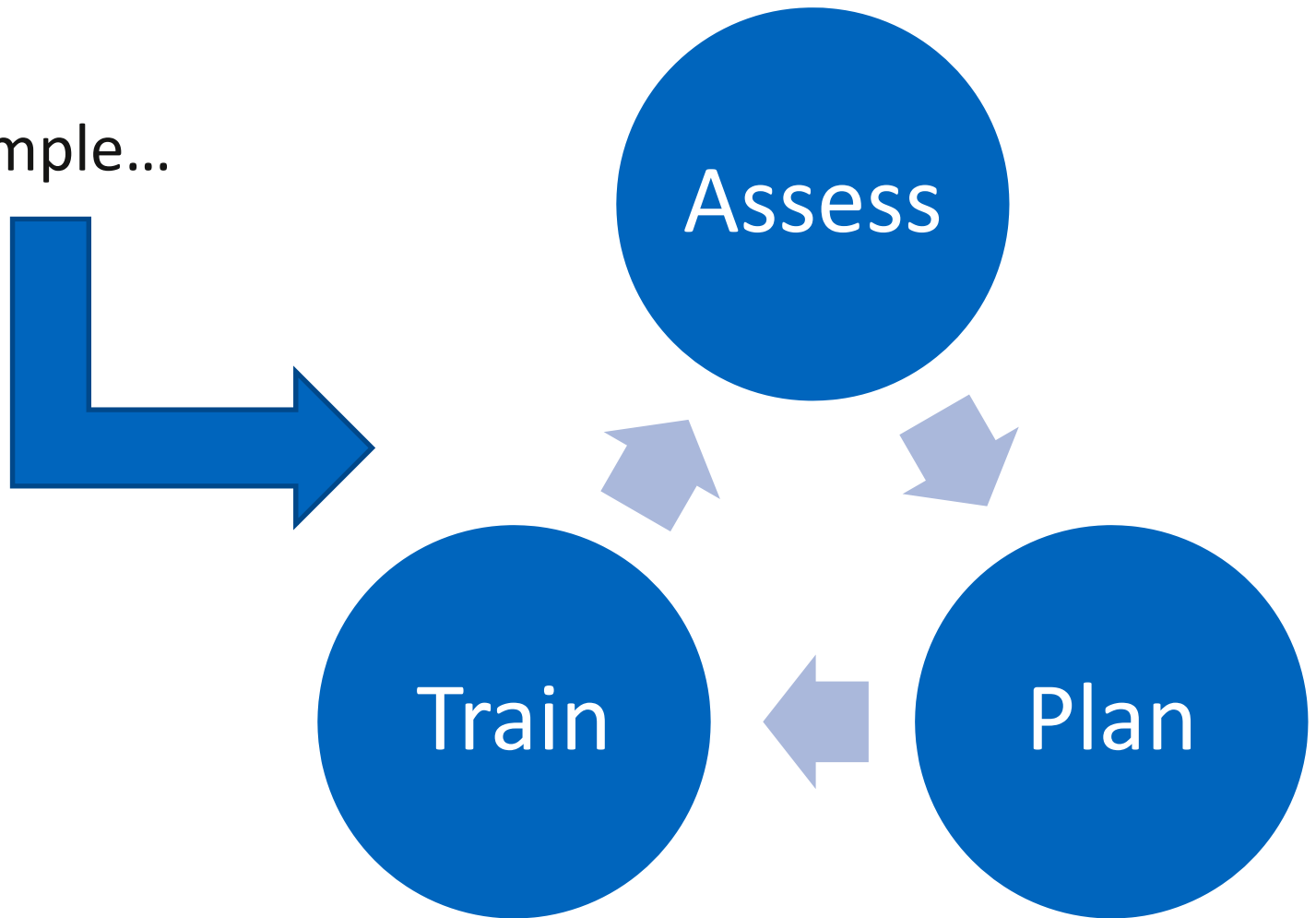
A Mozilla Firefox window is open to the 'Advanced' preferences page. A video player at the bottom of the screen shows a video titled 'Banner Grabber - Coding' with a description: 'Write a tool that scans an IP range [192.168.1.0-255] and tries to connect to the following ports [21, 22, 23, 25, 53, 80, 443, 445, 5900] on a remote target in order to conduct a banner grab and determine the services available. Print update information to the screen as the tool successfully finds a live service on a target IP port showing the IP, the port, and the banner information received from the open port.'

Callouts point to the following elements:

- 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...



Slide 12

AG4

Add arrow to show circular flow..

Alan Gush, 30/05/2018

PS4

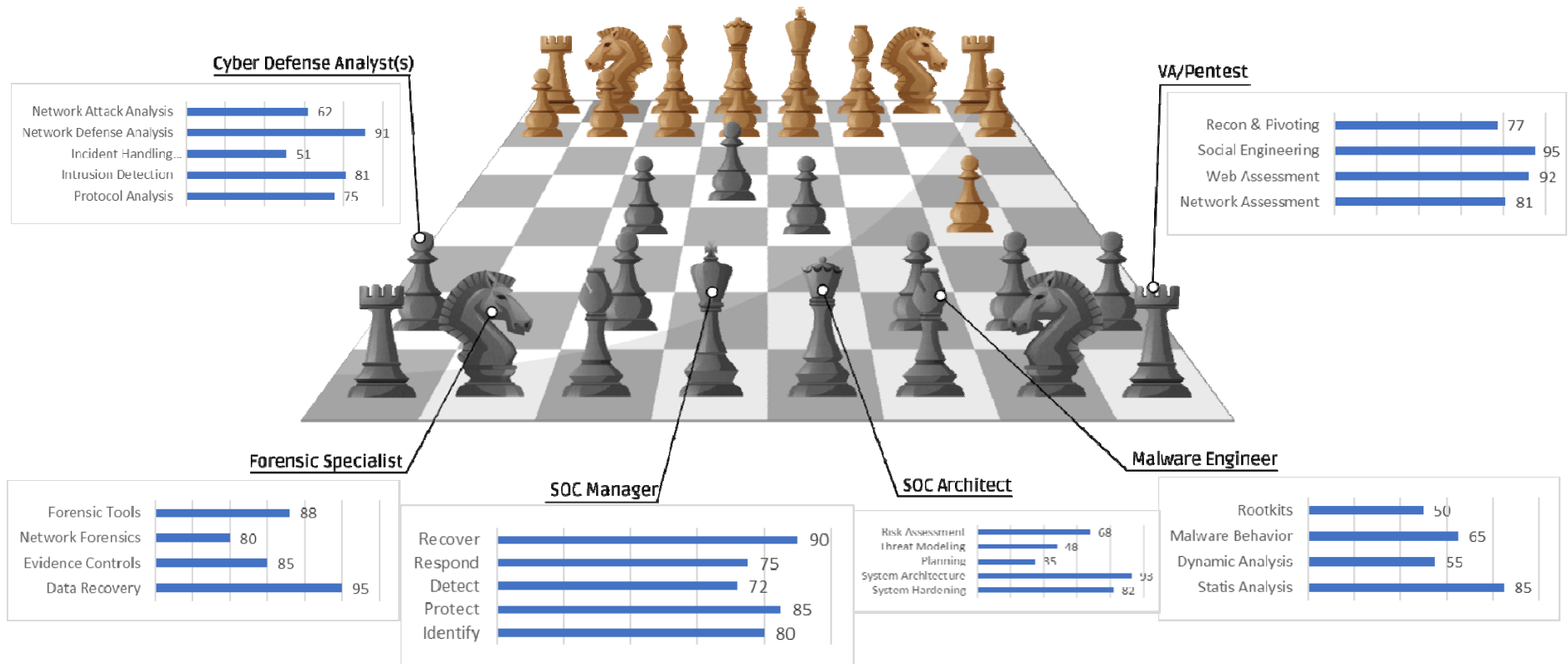
done

Phil Stoner, 30/05/2018



Team

Example: SOC Team



Slide 14

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

Contact Us

Phillip Stoner
Director, Cyber Solutions Group
(Whatsapp) +1 443 591 4135



275 West Street
Annapolis, MD 21401
United States



phillip.stoner@
comtechtel.com



@CYBRScore.io



CYBRScore.io