What's Your CYBRScore™ ?

QUESTION:

How Good is Your Cyber Athlete?

ANSWER:

Use Competency-based Assessment in Live Virtual Lab Environments to Measure Cyber Skills

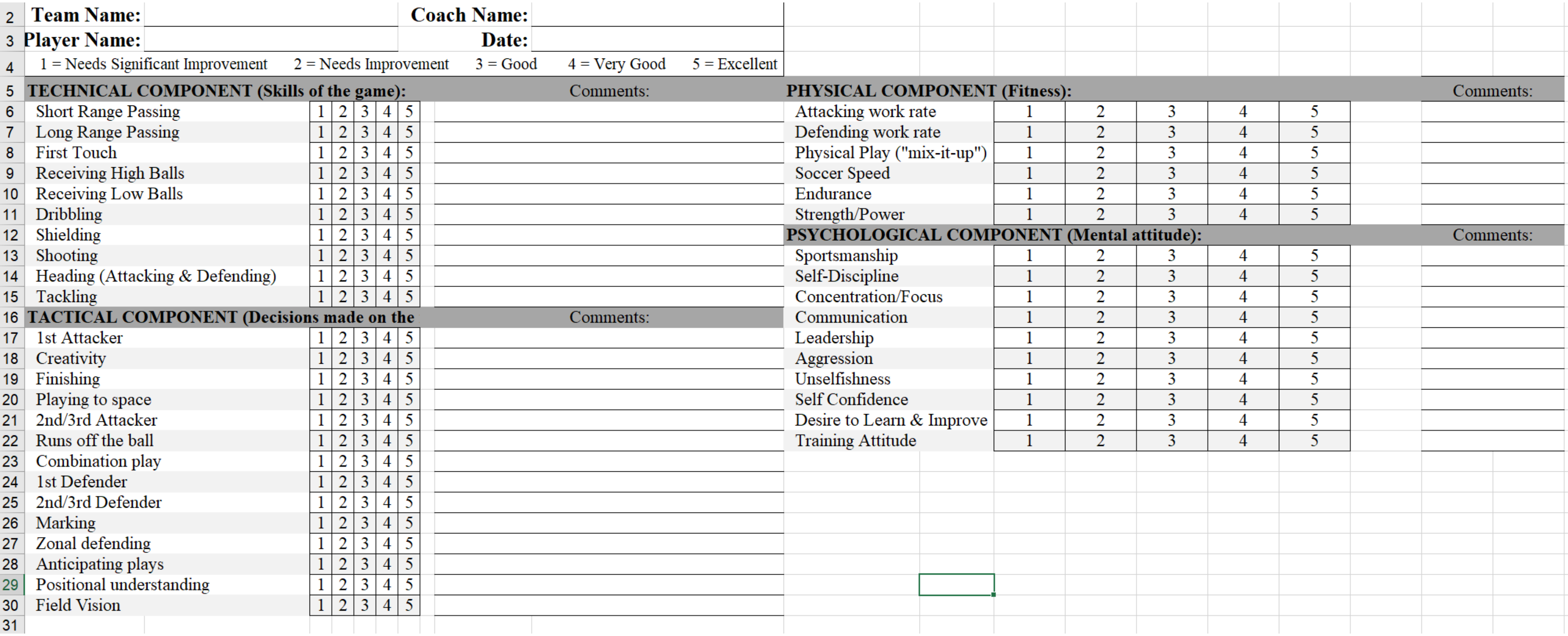
But, how do we do this?

With data, of course!

In football we measure an athlete in both practice and competition.

Why not do the same in Cyber?

Example: Football Player Skills Assessment



2 **Team Name:** **Coach Name:**

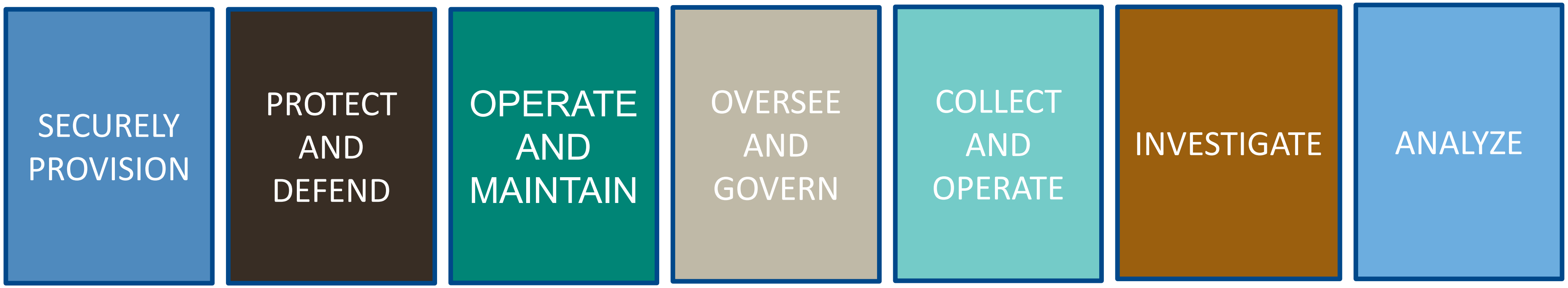
3 **Player Name:** **Date:**

4 1 = Needs Significant Improvement 2 = Needs Improvement 3 = Good 4 = Very Good 5 = Excellent

5	**TECHNICAL COMPONENT (Skills of the game):**						Comments:	**PHYSICAL COMPONENT (Fitness):**						Comments:
6	Short Range Passing	1	2	3	4	5		Attacking work rate	1	2	3	4	5	
7	Long Range Passing	1	2	3	4	5		Defending work rate	1	2	3	4	5	
8	First Touch	1	2	3	4	5		Physical Play ("mix-it-up")	1	2	3	4	5	
9	Receiving High Balls	1	2	3	4	5		Soccer Speed	1	2	3	4	5	
10	Receiving Low Balls	1	2	3	4	5		Endurance	1	2	3	4	5	
11	Dribbling	1	2	3	4	5		Strength/Power	1	2	3	4	5	
12	Shielding	1	2	3	4	5		**PSYCHOLOGICAL COMPONENT (Mental attitude):**						Comments:
13	Shooting	1	2	3	4	5		Sportsmanship	1	2	3	4	5	
14	Heading (Attacking & Defending)	1	2	3	4	5		Self-Discipline	1	2	3	4	5	
15	Tackling	1	2	3	4	5		Concentration/Focus	1	2	3	4	5	
16	**TACTICAL COMPONENT (Decisions made on the**						Comments:	Communication	1	2	3	4	5	
17	1st Attacker	1	2	3	4	5		Leadership	1	2	3	4	5	
18	Creativity	1	2	3	4	5		Aggression	1	2	3	4	5	
19	Finishing	1	2	3	4	5		Unselfishness	1	2	3	4	5	
20	Playing to space	1	2	3	4	5		Self Confidence	1	2	3	4	5	
21	2nd/3rd Attacker	1	2	3	4	5		Desire to Learn & Improve	1	2	3	4	5	
22	Runs off the ball	1	2	3	4	5		Training Attitude	1	2	3	4	5	
23	Combination play	1	2	3	4	5								
24	1st Defender	1	2	3	4	5								
25	2nd/3rd Defender	1	2	3	4	5								
26	Marking	1	2	3	4	5								
27	Zonal defending	1	2	3	4	5								
28	Anticipating plays	1	2	3	4	5								
29	Positional understanding	1	2	3	4	5								
30	Field Vision	1	2	3	4	5								
31														

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



SECURELY PROVISION

PROTECT AND DEFEND

OPERATE AND MAINTAIN

OVERSEE AND GOVERN

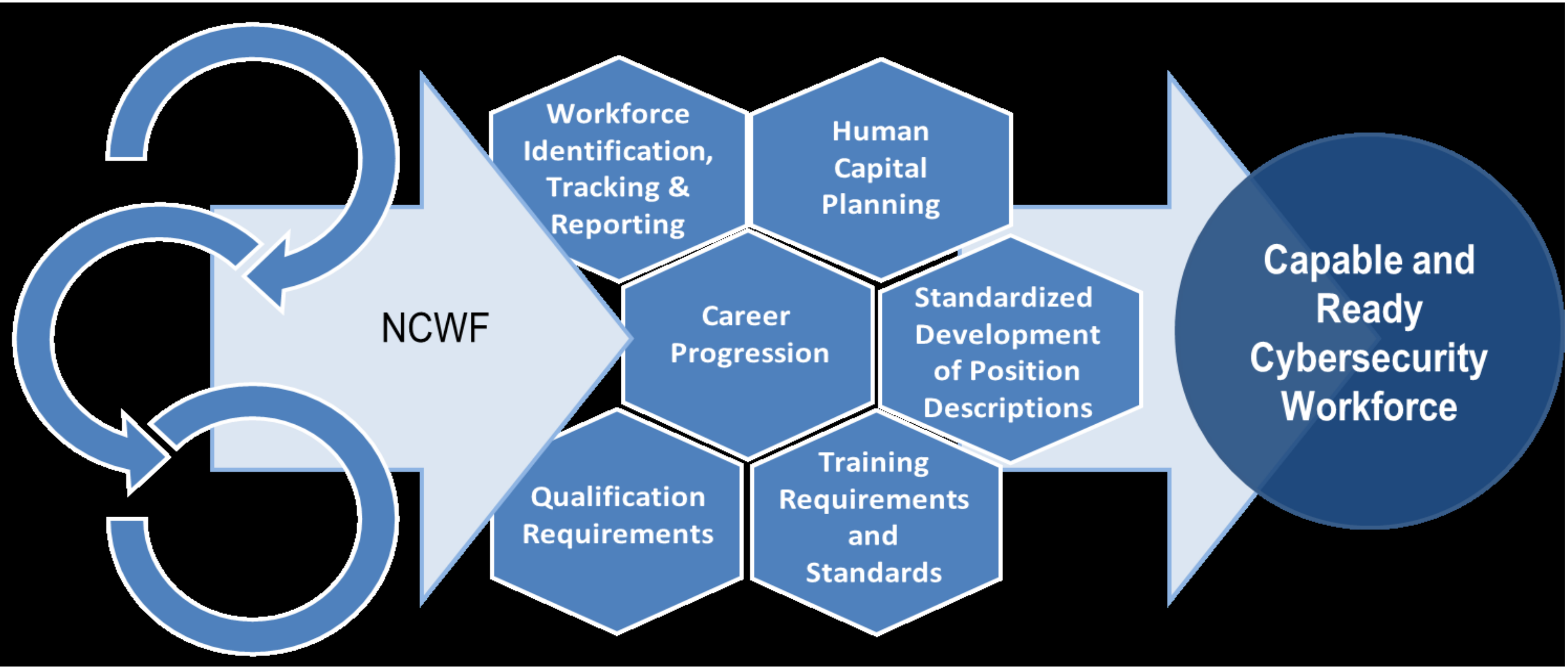
COLLECT AND OPERATE

INVESTIGATE

ANALYZE

- NCWF Version 1.0 posted in April 2013
- NCWF Version 2.0 posted in May 2014
- Special Pub. 800-181 released Aug 2017

NCWF – Core to Capable & Ready Cybersecurity Workforce



NCWF

Workforce Identification, Tracking & Reporting

Human Capital Planning

Career Progression

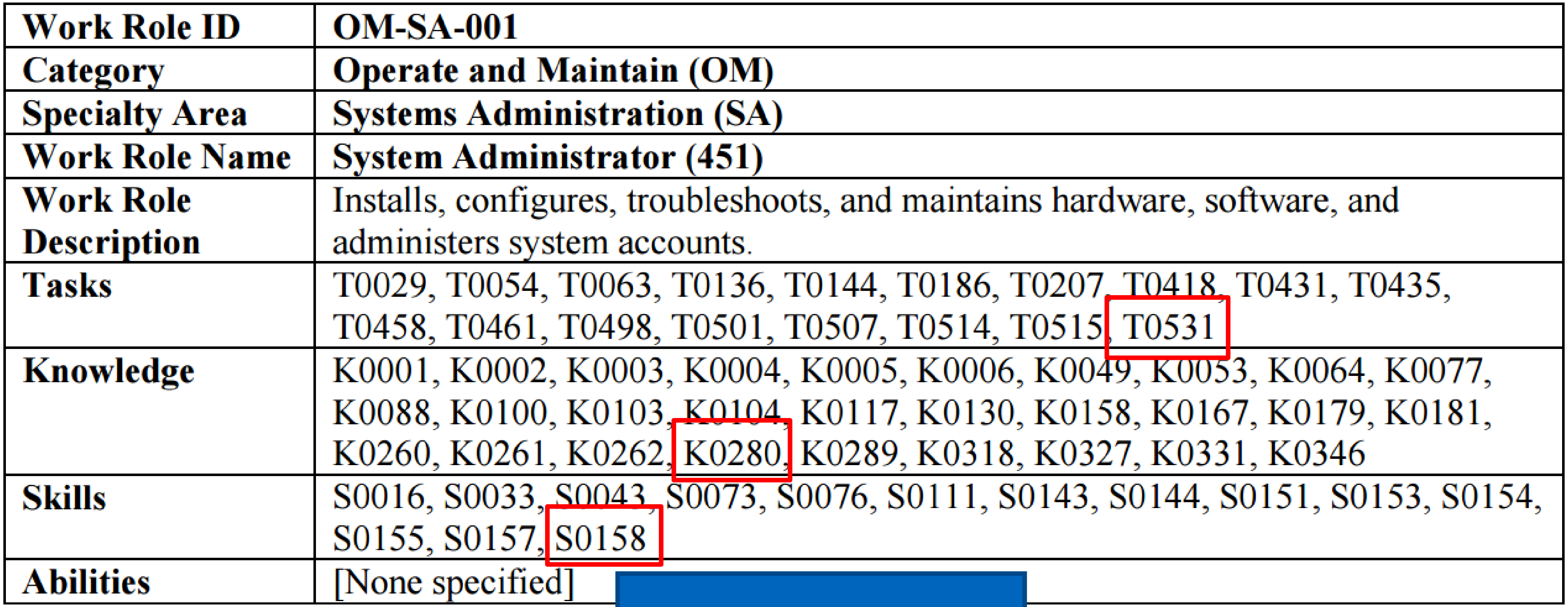
Standardized Development of Position Descriptions

Qualification Requirements

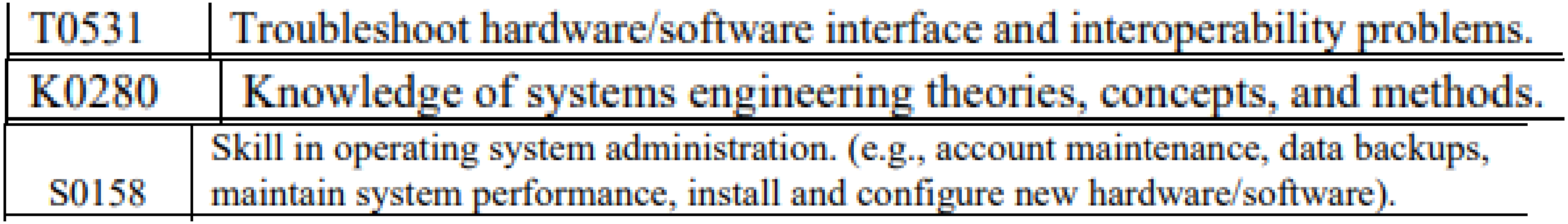
Training Requirements and Standards

Capable and Ready Cybersecurity Workforce

Work Role Example



Work Role ID	**OM-SA-001**
Category	**Operate and Maintain (OM)**
Specialty Area	**Systems Administration (SA)**
Work Role Name	**System Administrator (451)**
Work Role Description	Installs, configures, troubleshoots, and maintains hardware, software, and administers system accounts.
Tasks	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0181, K0260, K0261, K0262, K0280, K0289, K0318, K0327, K0331, K0346
Skills	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
Abilities	[None specified]



T0531	Troubleshoot hardware/software interface and interoperability problems.
K0280	Knowledge of systems engineering theories, concepts, and methods.
S0158	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).

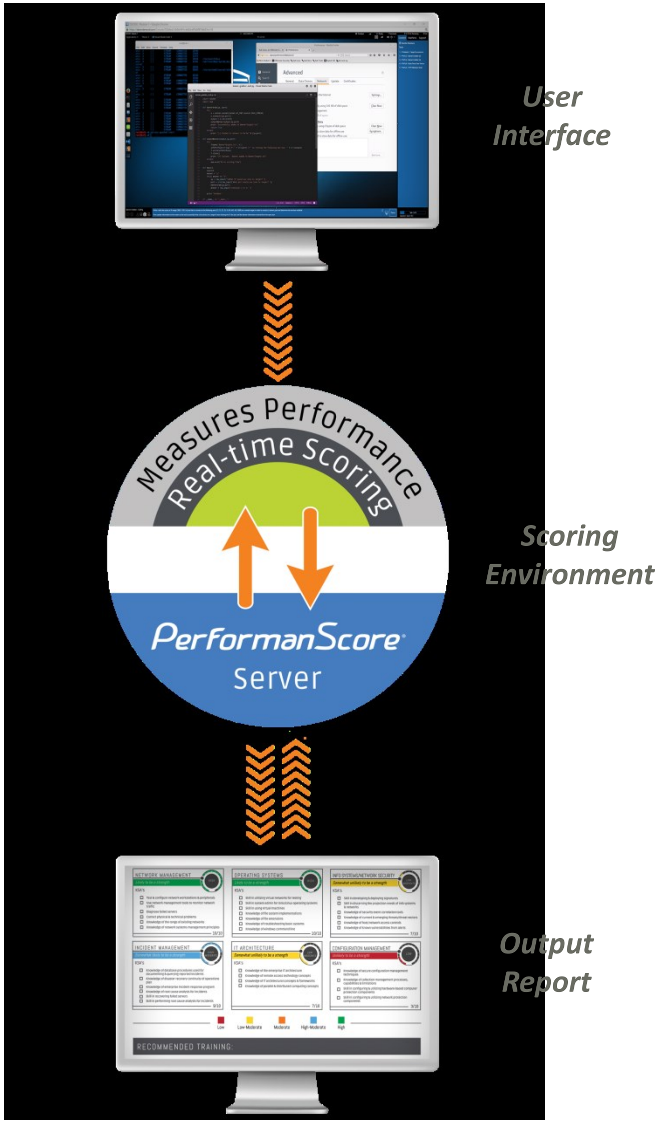
Data is the Driver…

In cyber, we can track an athlete in a cyber range, via certifications, and with live skills assessments.

Skills Assessment

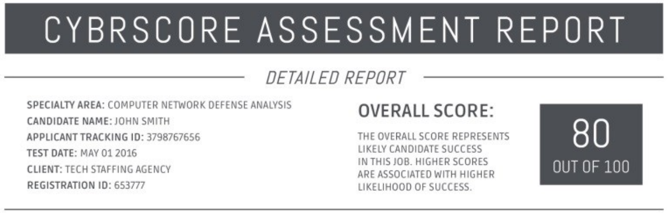
Virtual Cyber Skill Assessment Scenarios with Automated Scoring & Reporting

PROCESS:



OUTPUT REPORT:

Overall Score



CYBRSCORE ASSESSMENT REPORT

DETAILED REPORT

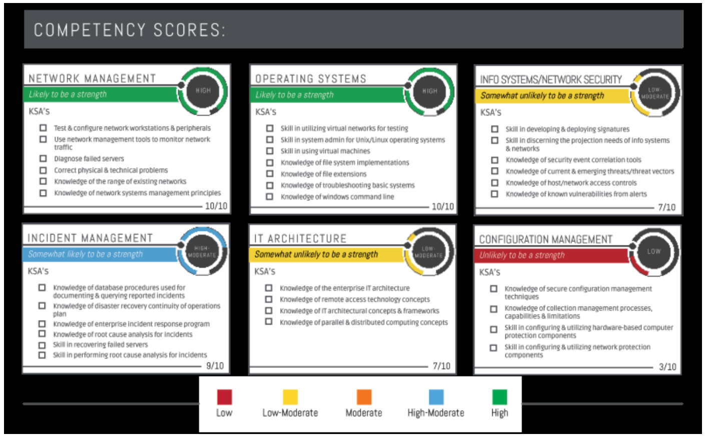
SPECIALTY AREA: COMPUTER NETWORK DEFENSE ANALYSIS
CANDIDATE NAME: JOHN SMITH
APPLICANT TRACKING ID: 3798767656
TEST DATE: MAY 01 2016
CLIENT: TECH STAFFING AGENCY
REGISTRATION ID: 653777

OVERALL SCORE:

THE OVERALL SCORE REPRESENTS LIKELY CANDIDATE SUCCESS IN THIS JOB. HIGHER SCORES ARE ASSOCIATED WITH HIGHER LIKELIHOOD OF SUCCESS.

80
OUT OF 100

Competency Scores



COMPETENCY SCORES:

NETWORK MANAGEMENT — HIGH
Likely to be a strength
KSA's
- □ Test & configure network workstations & peripherals
- □ Use network management tools to monitor network traffic
- □ Diagnose failed servers
- □ Correct physical & technical problems
- □ Knowledge of the range of existing networks
- □ Knowledge of network systems management principles

10/10

OPERATING SYSTEMS — HIGH
Likely to be a strength
KSA's
- □ Skill in utilizing virtual networks for testing
- □ Skill in system admin for Unix/Linux operating systems
- □ Skill in using virtual machines
- □ Knowledge of file system implementations
- □ Knowledge of file extensions
- □ Knowledge of troubleshooting basic systems
- □ Knowledge of windows command line

10/10

INFO SYSTEMS/NETWORK SECURITY — LOW-MODERATE
Somewhat unlikely to be a strength
KSA's
- □ Skill in developing & deploying signatures
- □ Skill in discerning the projection needs of info systems & networks
- □ Knowledge of security event correlation tools
- □ Knowledge of current & emerging threats/threat vectors
- □ Knowledge of host/network access controls
- □ Knowledge of known vulnerabilities from alerts

7/10

INCIDENT MANAGEMENT — HIGH-MODERATE
Somewhat likely to be a strength
KSA's
- □ Knowledge of database procedures used for documenting & querying reported incidents
- □ Knowledge of disaster recovery continuity of operations plan
- □ Knowledge of enterprise incident response program
- □ Knowledge of root cause analysis for incidents
- □ Skill in recovering failed servers
- □ Skill in performing root cause analysis for incidents

9/10

IT ARCHITECTURE — LOW-MODERATE
Somewhat unlikely to be a strength
KSA's
- □ Knowledge of the enterprise IT architecture
- □ Knowledge of remote access technology concepts
- □ Knowledge of IT architectural concepts & frameworks
- □ Knowledge of parallel & distributed computing concepts

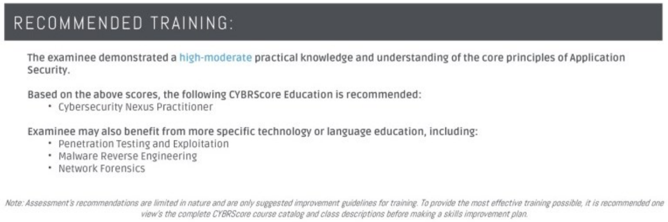
7/10

CONFIGURATION MANAGEMENT — LOW
Unlikely to be a strength
KSA's
- □ Knowledge of secure configuration management techniques
- □ Knowledge of collection management processes, capabilities & limitations
- □ Skill in configuring & utilizing hardware-based computer protection components
- □ Skill in configuring & utilizing network protection components

3/10

🟥 Low 🟨 Low-Moderate 🟧 Moderate 🟦 High-Moderate 🟩 High

Recommended Training



RECOMMENDED TRAINING:

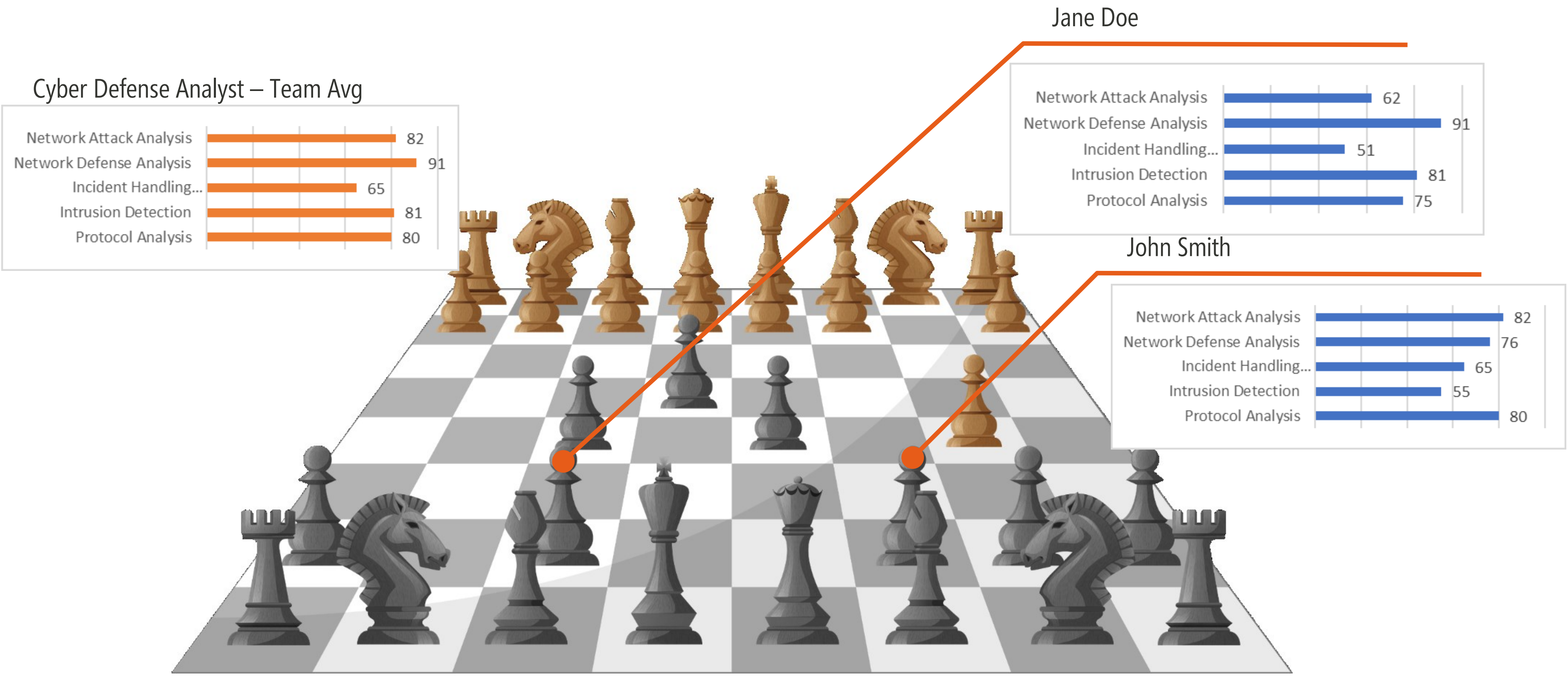
The examinee demonstrated a high-moderate practical knowledge and understanding of the core principles of Application Security.

Based on the above scores, the following CYBRScore Education is recommended:
- Cybersecurity Nexus Practitioner

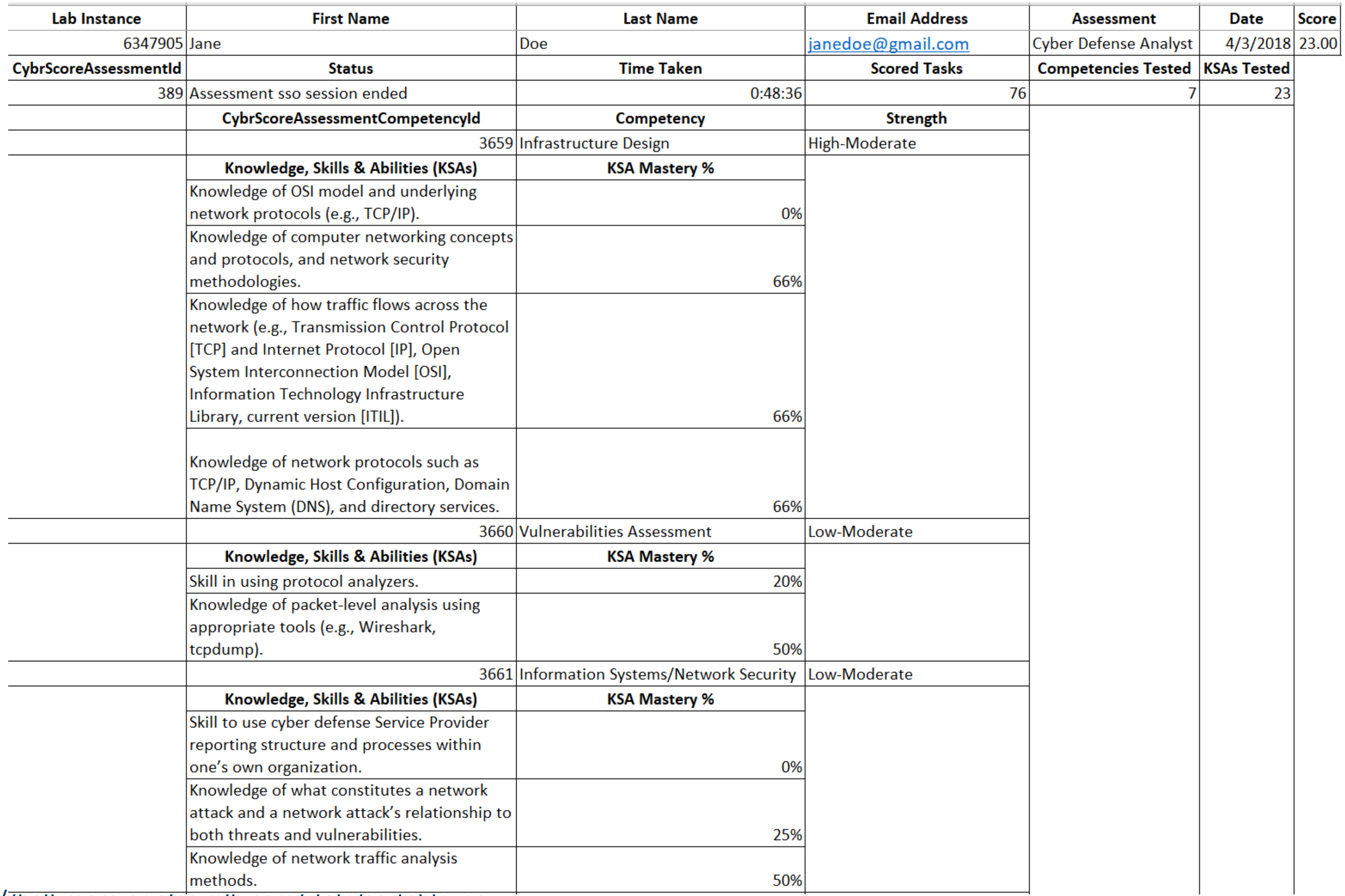
Examinee may also benefit from more specific technology or language education, including:
- Penetration Testing and Exploitation
- Malware Reverse Engineering
- Network Forensics

Note: Assessment's recommendations are limited in nature and are only suggested improvement guidelines for training. To provide the most effective training possible, it is recommended one view's the complete CYBRScore course catalog and class descriptions before making a skills improvement plan.

Example: Cyber Defense Analyst



Skills Data Example (Cyber “stats”)

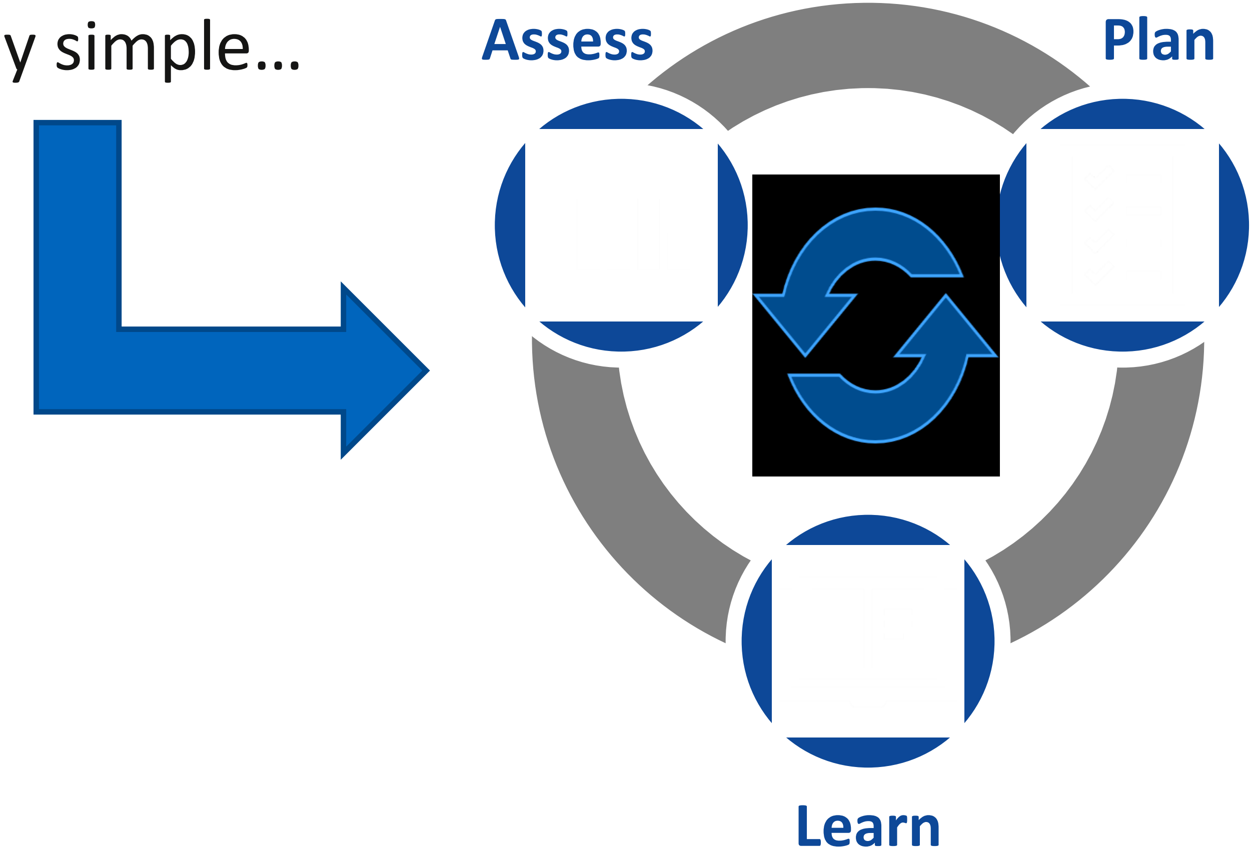


Lab Instance	First Name	Last Name	Email Address	Assessment	Date	Score
6347905	Jane	Doe	janedoe@gmail.com	Cyber Defense Analyst	4/3/2018	23.00
CybrScoreAssessmentId	Status	Time Taken	Scored Tasks	Competencies Tested	KSAs Tested	
389	Assessment sso session ended	0:48:36	76	7	23	
	CybrScoreAssessmentCompetencyId	Competency	Strength			
	3659	Infrastructure Design	High-Moderate			
	Knowledge, Skills & Abilities (KSAs)	KSA Mastery %				
	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	0%				
	Knowledge of computer networking concepts and protocols, and network security methodologies.	66%				
	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	66%				
	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	66%				
	3660	Vulnerabilities Assessment	Low-Moderate			
	Knowledge, Skills & Abilities (KSAs)	KSA Mastery %				
	Skill in using protocol analyzers.	20%				
	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	50%				
	3661	Information Systems/Network Security	Low-Moderate			
	Knowledge, Skills & Abilities (KSAs)	KSA Mastery %				
	Skill to use cyber defense Service Provider reporting structure and processes within one’s own organization.	0%				
	Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.	25%				
	Knowledge of network traffic analysis methods.	50%				

http://baltimore.orioles.mlb.com/stats/sortable.jsp

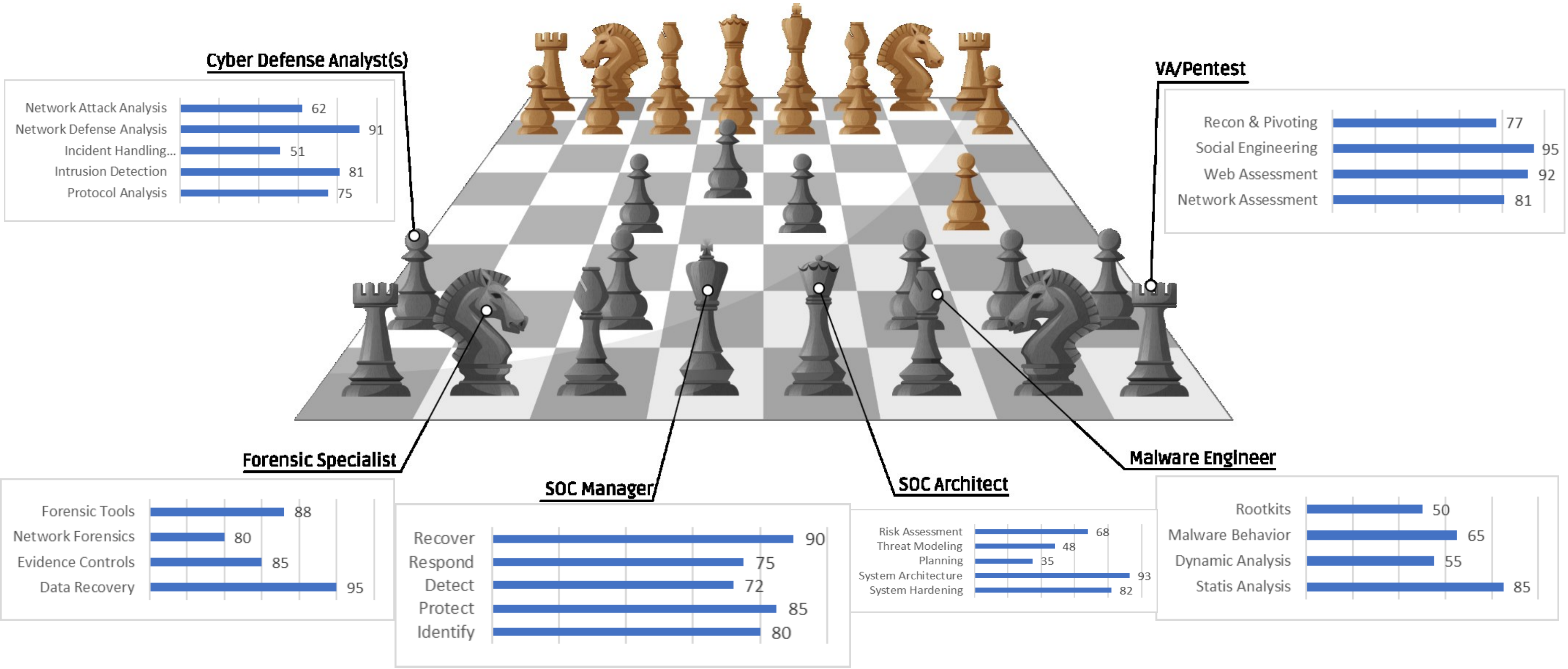
Skills Assessment Goal

- It’s really simple…



But, what about my entire team?

Example: SOC Team



CYBRScore™

Building the Team

- Accurately measure employee competencies
  - Targeted training and up-skilling
  - Effectively identify gaps; close them
- Prevent potentially costly hiring errors
- Demonstrate compliance
- Increases confidence in employee performance, and confidence in the team

What's Your CYBRScore™?

Contact Us

Phillip Stoner
Director, Cyber Solutions Group
(m) +14435914135

275 West Street
Annapolis, MD 21401
United States

phillip.stoner@
comtechtel.com

@CYBRScore.io

CYBRScore.io

Now What?

- Choose an assessment from the list below:
  - Cyber Defense Analyst
    - Protocol Analysis
    - Intrusion Detection
    - Incident Handling Methodology
    - Network Defense Analysis
    - Network Attack Analysis
  - Vulnerability Assessment Analyst
    - Intelligence Gathering
    - Red Team
    - Blue Team

Next Steps

- Complete Assessment
- Review Assessment Report
  - Identify Areas of Strength
  - Identify Areas for Improvement
    - Review Training Lab Recommendations
- Create Account on Training Platform
- Get Trained!