# Federal Cyber Reskilling Academy (FCRA)

## Assessment, Selection, Training and Evaluation at Scale

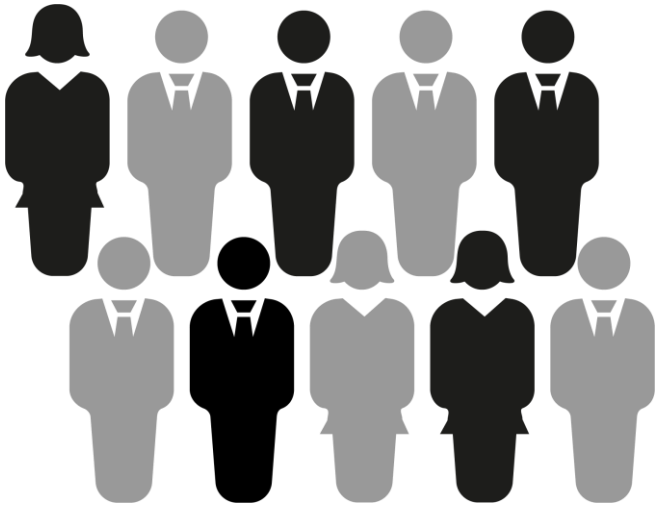
CYBRScore®

# Agenda

- Introduction to Federal Cyber Reskilling Academy Program
- Cohort Selection Process – Cyber Aptitude and Attitude
- Selection Results
- Training Plan
- Student Performance Evaluation
- Key Take Aways
- Lessons Learned

# Cybersecurity Gap Not Shrinking

69% say their cybersecurity teams are understaffed



58% have unfilled (open) cybersecurity positions

32% say it takes six months or more to fill cybersecurity jobs at their organization

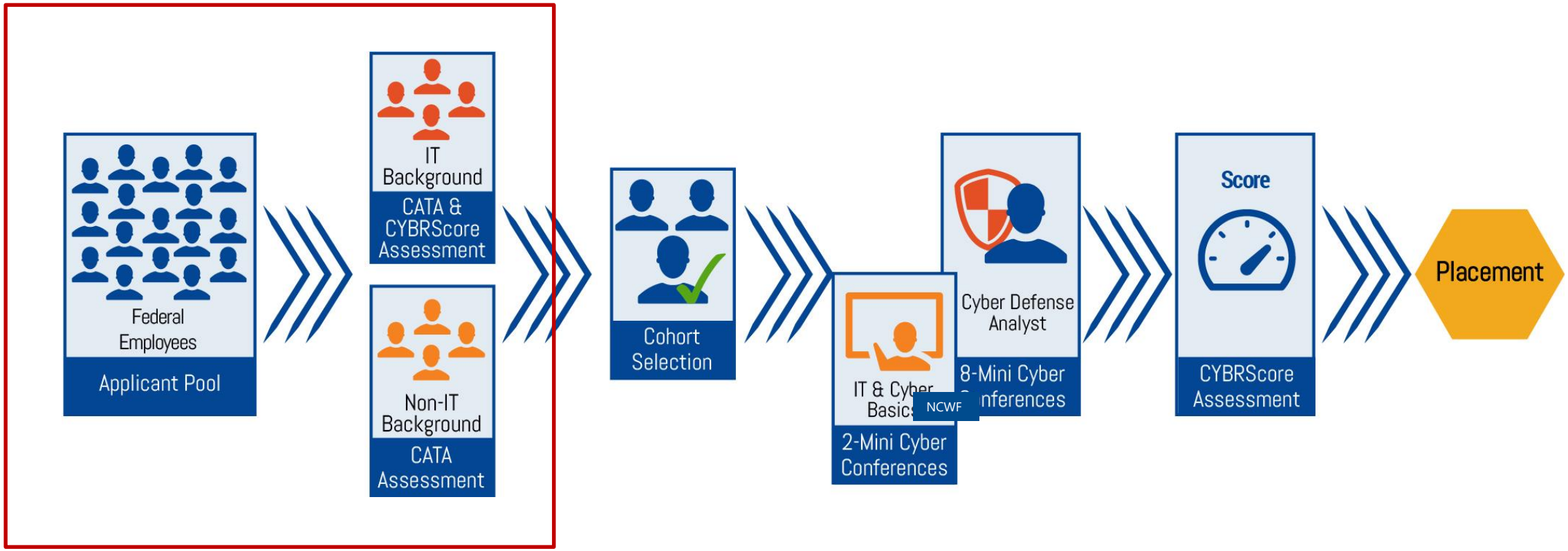
Source: ISACA State of Cybersecurity 2019

# Federal Cyber Reskilling Academy

- Innovative Training Program - Develop New Cyber Professionals
- FCRA is a USG Initiative to Reskill / Upskill  Current Workforce
- Collaboration Between the OMB, and the CIO Council
- Cohort 2 Led by Comtech CYBRScore and Marcom Group
- The Cohort Goal - Find Cybersecurity Talent and Upskill or Reskill

# Workforce Development Challenges

- Initial Candidate Screening  - Cognitive and Behavioral Evaluation
- Tracking Candidate Performance Within the Program

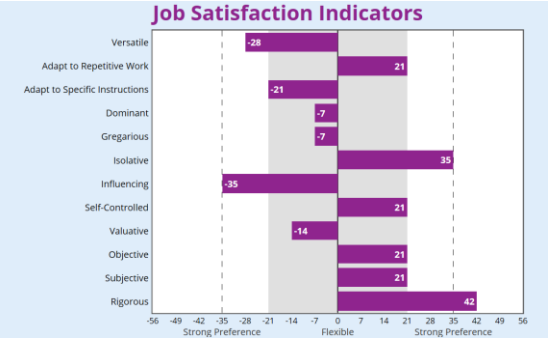


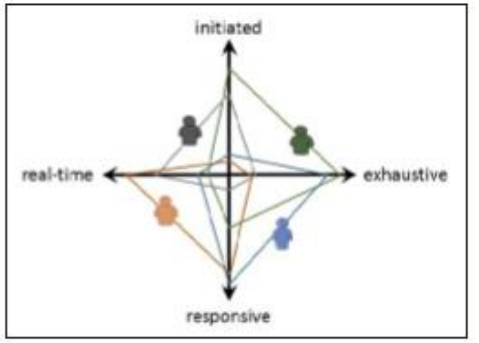
# Cohort Selection – Federal Cyber Reskilling Academy

- 750 Applicants
- 20 Positions in the Cohort
- Provided Selection Guidance Based on Cyber Aptitude and Attitude Assessments
- Government Evaluated Assessment Data, Resume, Personal Statement, Interview of the Top ~50 Candidates

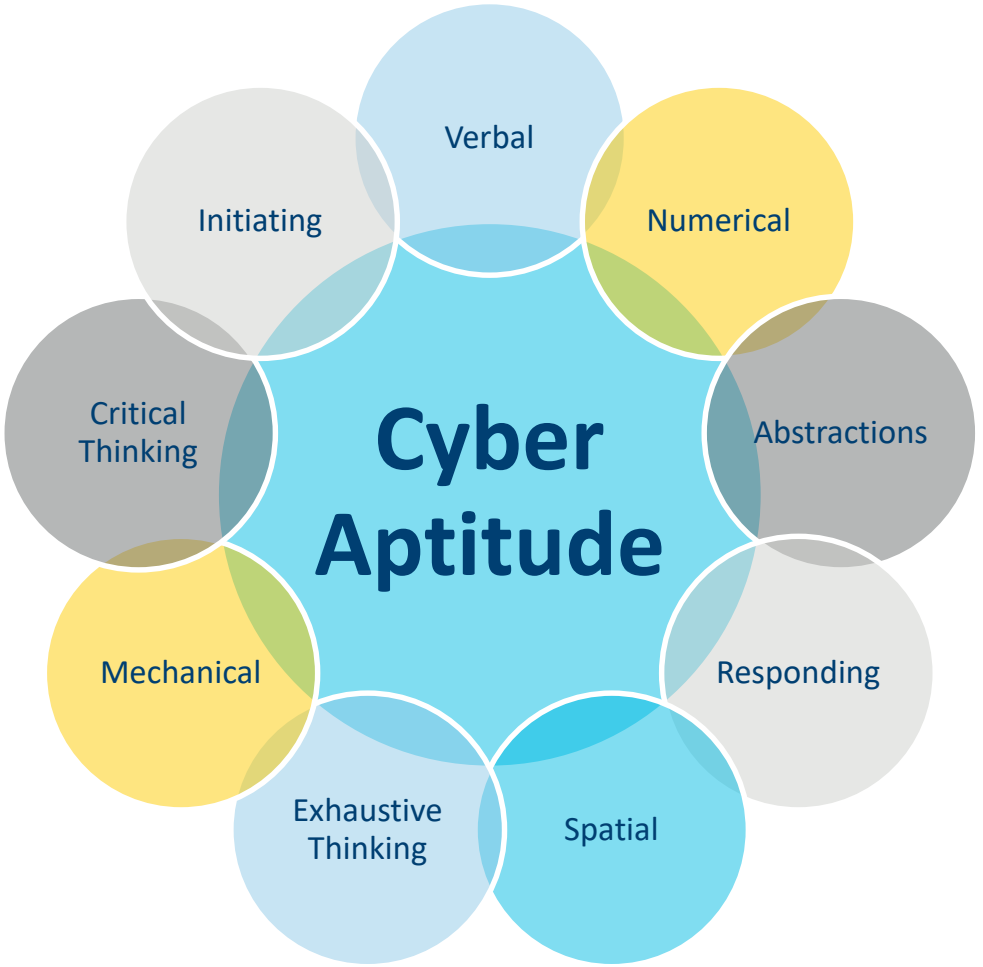
# Selection: Aptitude and Attitude – Who should we select?

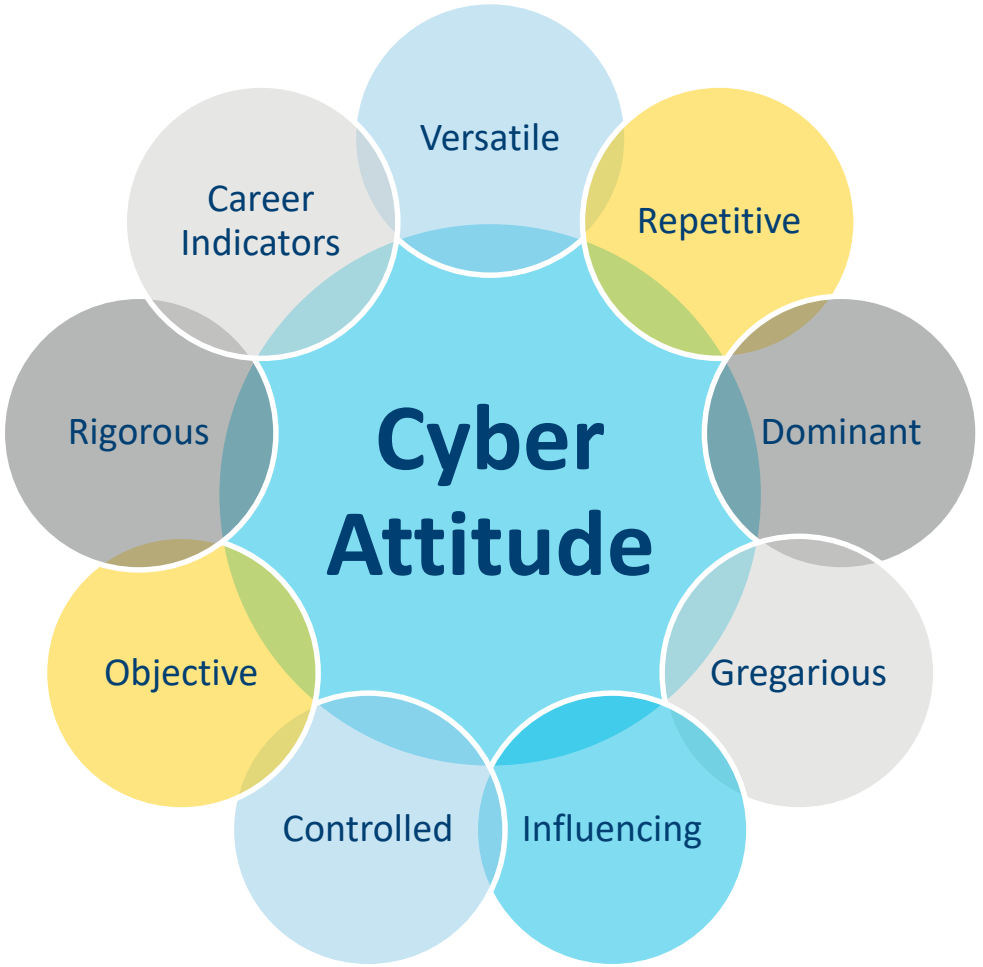
- Cyber Aptitude
  - Puzzles
  - Critical Thinking
  - STEM Components
- Cyber Attitude
  - Are They a Good Fit?
  - Does Their Personality Align?
  - Will They be a Good Long-Term Candidate?
  - Do They Have Passion & Tenacity for the Role?
- Automated Evaluation Tools – Critical for Selection



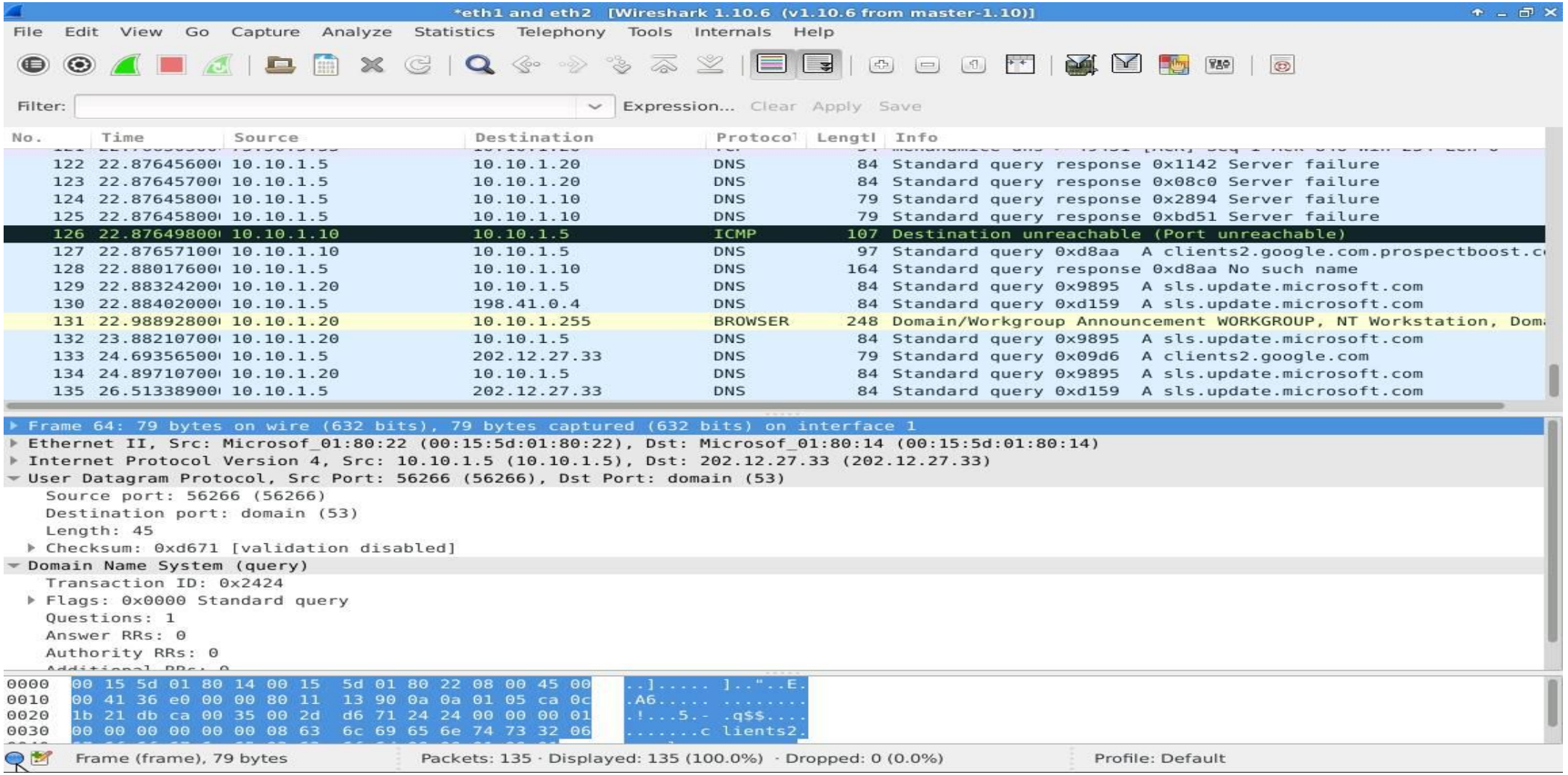




# Measuring Cyber Potential



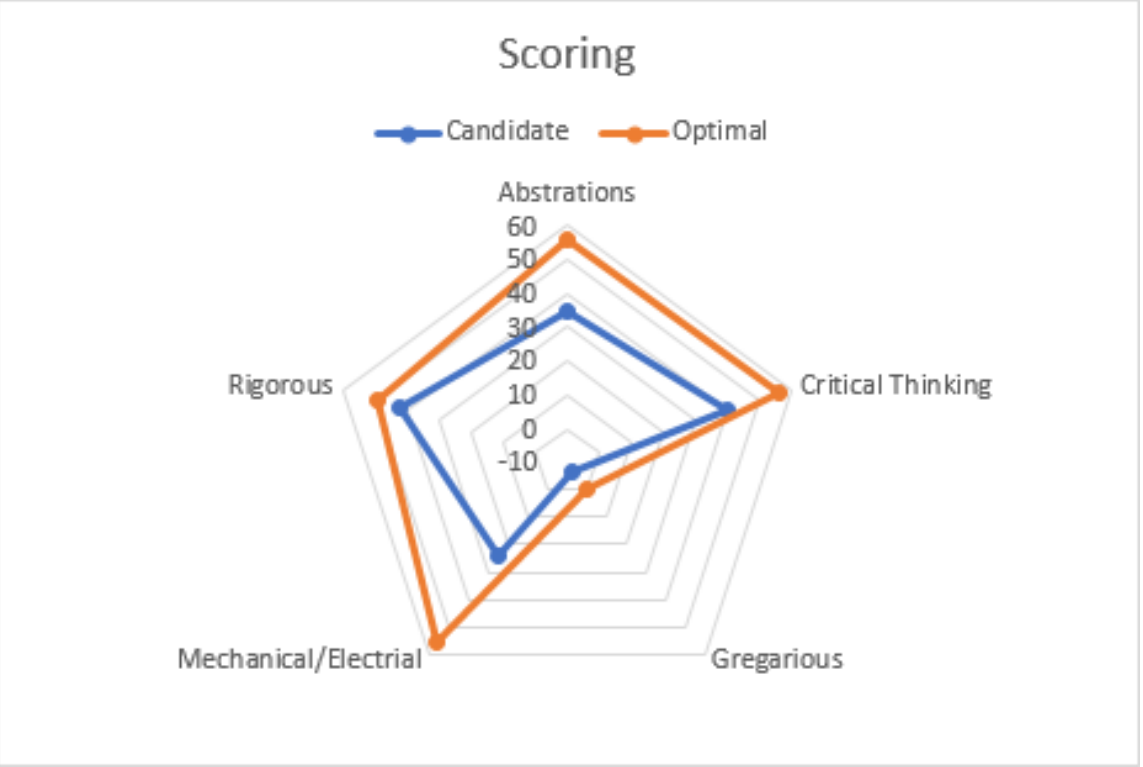



# Example Repetitive Work

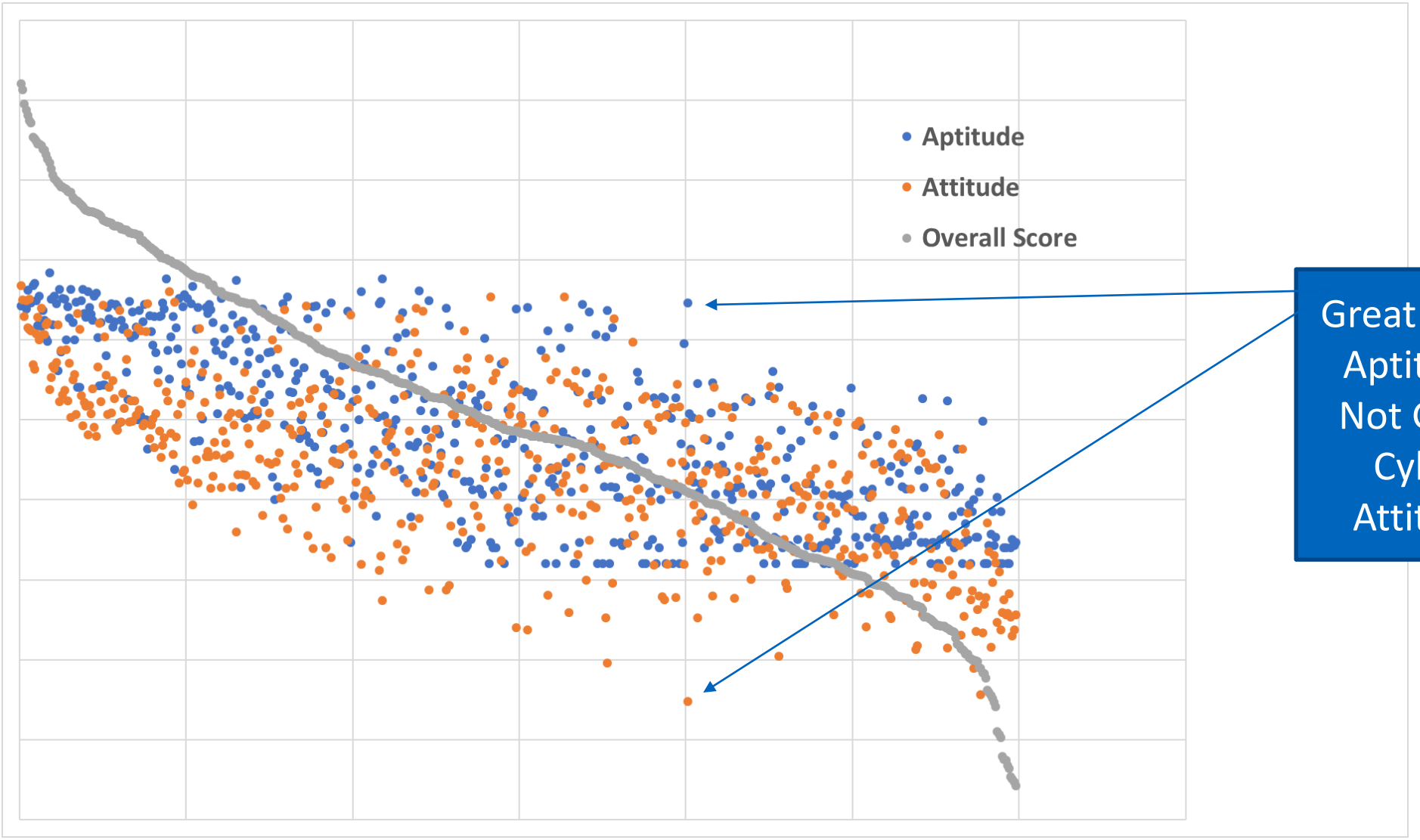


# Aligning the Data to the Work Role

- Measured Data – Applicable to Work Role?
- What is Optimal
  - (SMEs & Psychometricians)
  - Weighting
- Optimal vs Measured
- A Guide to Selection
- Automated!!!

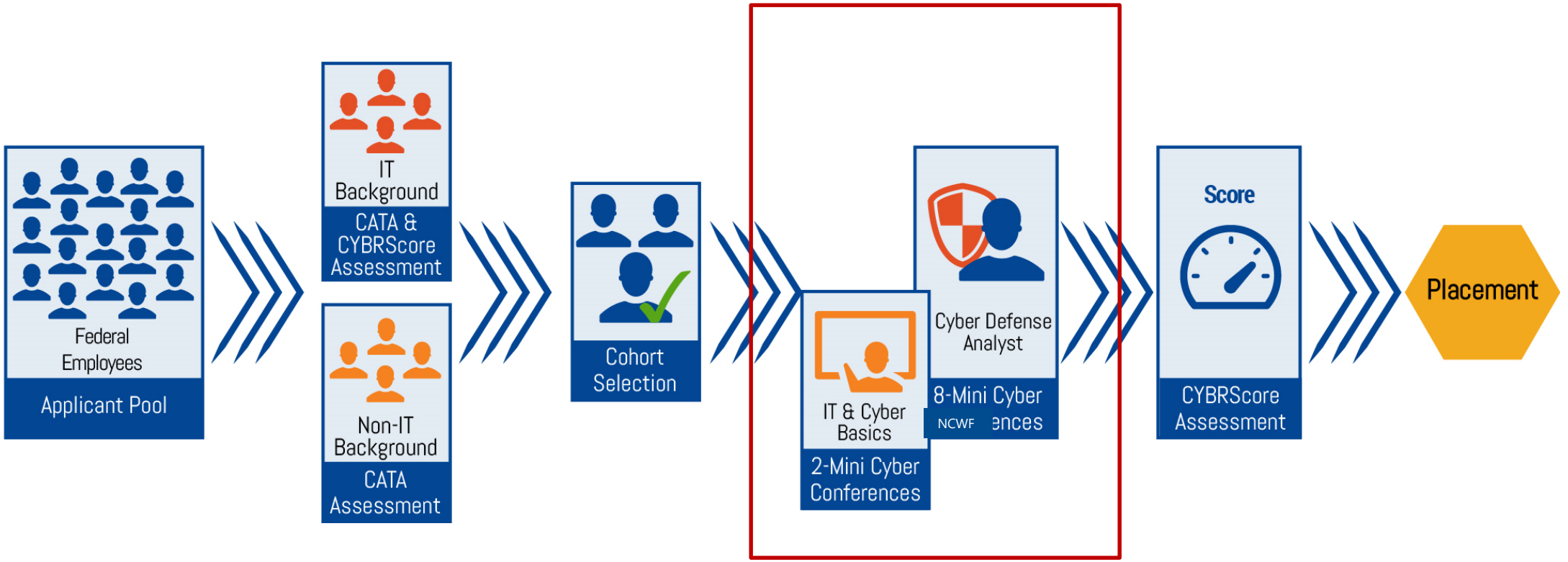


# FCRA Candidate Selection Scoring



# Workforce Development Challenges

- Initial Candidate Screening  - Cognitive and Behavior Evaluation
- Tracking Candidate Performance Within the Program

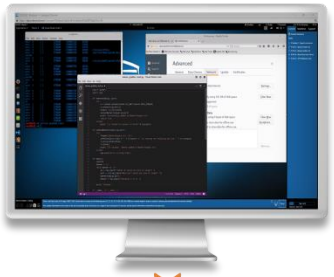


# FCRA Training

| WEEK | TRAINING |
|---|---|
| 1 | Linux Familiarization |
| 2 | Sec Fund / Win Familiarization |
| 3 | Self Study |
| 4 | Protocol Analysis / Intrusion Detection |
| 5 | Incident Handling |
| 6 | Self Study |
| 7 | Network Defense / Network Attack |
| 8 | Network Attack / Practical Exercises |
| 9 | Self Study |
| 10 | Capture The Flag / Refresher / CYBRScore Assessments |
| 11 | King of the Hill / Refresher / CYBRScore Assessments |
| 12 | Graduation |

# CYBRScore® Assessment

## PROCESS:



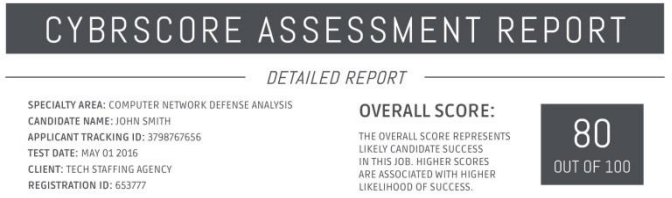
*User Interface*


*Scoring Environment*

*Output Report*

## OUTPUT REPORT:

### *Overall Score*



CYBRSCORE ASSESSMENT REPORT

DETAILED REPORT

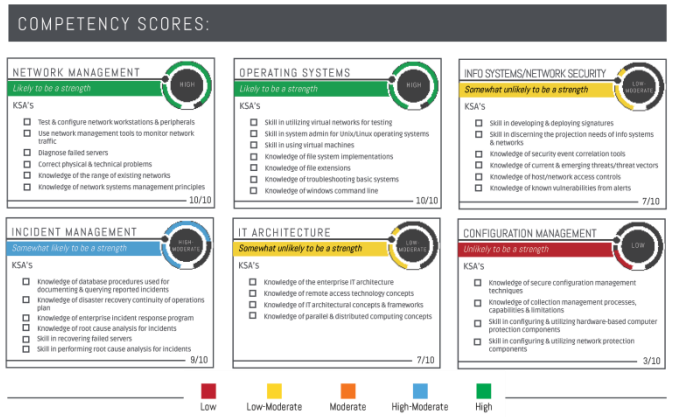
**SPECIALTY AREA:** COMPUTER NETWORK DEFENSE ANALYSIS
**CANDIDATE NAME:** JOHN SMITH
**APPLICANT TRACKING ID:** 3798767656
**TEST DATE:** MAY 01 2016
**CLIENT:** TECH STAFFING AGENCY
**REGISTRATION ID:** 653777

**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*

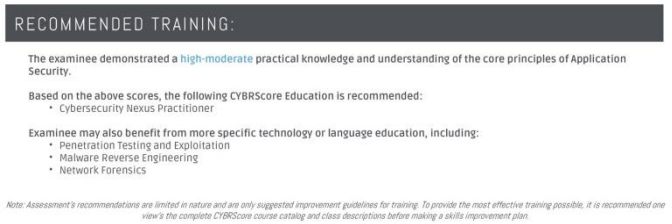


COMPETENCY SCORES:

NETWORK MANAGEMENT — Likely to be a strength — HIGH — KSA's — 10/10
OPERATING SYSTEMS — Likely to be a strength — HIGH — KSA's — 10/10
INFO SYSTEMS/NETWORK SECURITY — Somewhat unlikely to be a strength — LOW-MODERATE — KSA's — 7/10
INCIDENT MANAGEMENT — Somewhat likely to be a strength — HIGH-MODERATE — KSA's — 9/10
IT ARCHITECTURE — Somewhat unlikely to be a strength — LOW-MODERATE — KSA's — 7/10
CONFIGURATION MANAGEMENT — Unlikely to be a strength — LOW — KSA's — 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.*

**Measures** abilities, NOT a Q&A exam
**Recommends** training
**Aligns to NICE** National Cybersecurity Workforce Framework (NCWF) (NIST SP 800-181)

## FEATURES:

- **Cloud Based**
- **E-Commerce Enabled**
- **Fully Automated**
- **Multiple Work Roles**

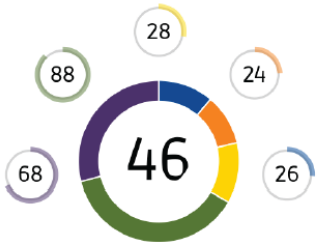
CYBRScore®

# CYBRScore® Assessments: Baseline Your Team

## CYBRScore™ : CYBER DEFENSE ANALYST

*WORK ROLE DETAILS*

**Work Role:** Cyber Defense Analyst
**Candidate Name:** Not Provided
**Customer:** Not Provided
**Overall Score:** 46%




| Assessment | Date | Score | Time | Instance |
|---|---|---|---|---|
| Incident Handling Methodology | 02/27/18 | 26% | 00:59:14 | 6127775 |
| Intrusion Detection | 02/26/18 | 24% | 00:59:51 | 6118620 |
| Network Attack Analysis | 03/05/18 | 28% | 00:59:51 | 6171995 |
| Network Defense Analysis | 02/27/18 | 88% | 00:32:04 | 6128399 |
| Protocol Analysis | 02/25/18 | 68% | 00:58:04 | 6111769 |

### HIGHER COMPETENCY SCORES:

**Cryptography** — *Likely to be a strength* — High
KSAs
[100] Knowledge of encryption methodologies.
[100] Knowledge of cryptography and cryptographic key management concepts
[100] Knowledge of encryption algorithms
3/3

**Database Management Systems** — *Likely to be a strength* — High
KSAs
[100] Knowledge of database systems.
2/2

**Enterprise Architecture** — *Likely to be a strength* — High
KSAs
[100] Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
1/1

### LOWER COMPETENCY SCORES:

**Criminal Law** — *Unlikely to be a strength* — Low
KSAs
[0] Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
0/1

**Embedded Computers** — *Unlikely to be a strength* — Low
KSAs
[0] Knowledge of embedded systems.
0/1

**Encryption** — *Unlikely to be a strength* — Low
KSAs
[0] Knowledge of Virtual Private Network (VPN) security.
0/4

Low or N/A | Low-Moderate | Moderate | High-Moderate | High

## RECOMMENDED TRAINING:

**The examinee demonstrated a moderate understanding of the core principals of Cyber Defense Analyst.**

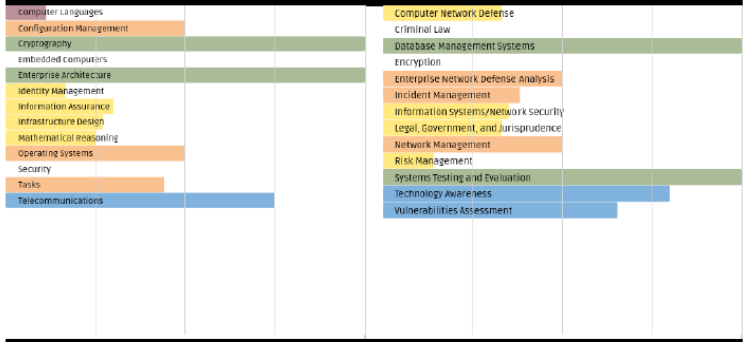
**Based on the above scores, the following CYBRScore training is recommended:**

- PEN-500: Analyze and Classify Malware - In this lab you will attempt to conduct basic analysis on some malware samples that were found on the internal network.

**Examinee may also benefit from more specific technology or language education, including:**

- PR100-2-L: Create Custom Snort Rules - You will configure snort as an IDS. Additionally, you have received the following indicators during an active intrusion investigation. You are going to eliminate the existing snort rules and run a packet capture against this snort rule which will be later deployed to detect network activity using these indicators.
- PEN-500: Network Discovery - The Network Discovery lab is designed to help students facilitate open source collection by teaching them how to use more intimate network discovery techniques.

## CYBER DEFENSE ANALYST WORK ROLE COMPETENCY ROLLUP:




## CYBER DEFENSE ANALYST KSA DETAILS:

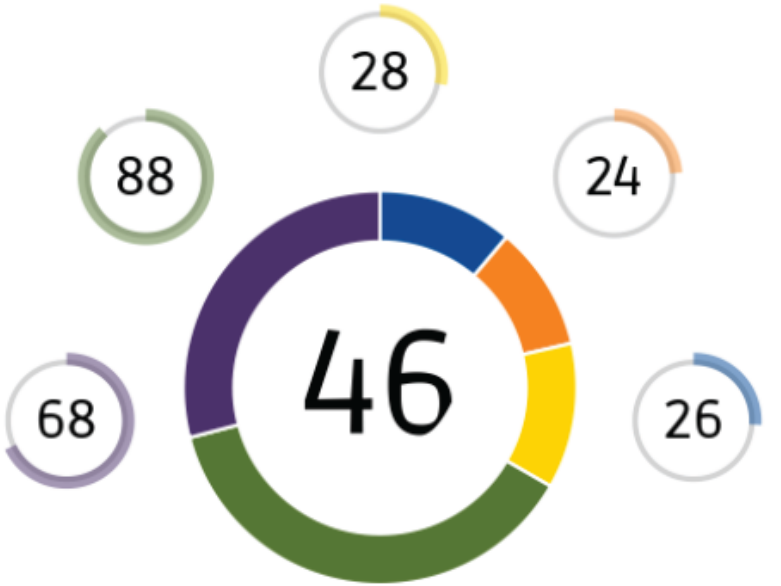
| Competency/KSA | Score | Available Training |
|---|---|---|
| **Security** | **Low** | |
| • K0262 - Knowledge of Personal Health Information (PHI) data security standards. | 0 | |
| • K0261 - Knowledge of Payment Card Industry (PCI) data security standards. | 0 | |
| • K0260 - Knowledge of Personally Identifiable Information (PII) data security standards. | 0 | |
| **Encryption** | **Low** | |
| • K0104 - Knowledge of Virtual Private Network (VPN) security. | 0 | |
| **Embedded Computers** | **Low** | |
| • K0322 - Knowledge of embedded systems. | 0 | |
| **Criminal Law** | **Low** | |
| • K0168 - Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. | 0 | |
| **Computer Languages** | **Low** | |
| • K0318 - Knowledge of operating system command-line tools. | 14 | NET-400: Linux Users and Groups |
| • K0139 - Knowledge of interpreted and compiled computer languages. | 0 | |
| **Risk Management** | **Low** | |
| • K0002 - Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). | 14 | PR100-1-L: Identify Whether High-Risk Systems Were Affected<br>PR100-4-L: Threat Designation<br>NET-400: System Administration |
| **Identity Management** | **Low** | |
| • K0007 - Knowledge of authentication, authorization, and access control methods. | 33 | PEN-500: System Hardening |
| • K0065 - Knowledge of policy-based and risk adaptive access controls. | 0 | PEN-500: Block Incoming Traffic on Known Port |
| **Infrastructure Design** | **Low-Moderate** | |
| • K0332 - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. | 66 | PR100-1-L: Network Segmentation<br>PEN-500: Network Discovery |
| • K0061 - 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 | PEN-500: Network Discovery<br>PR100-1-L: Network Segmentation |
| • K0001 - Knowledge of computer networking concepts and protocols, and network security methodologies. | 66 | PEN-500: Network Discovery |
| • K0221 - Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). | 100 | PR100-1-L: Using Snort and Wireshark to Analyze Traffic |
| • K0303 - Knowledge of the use of sub-netting tools. | 0 | |
| • K0300 - Knowledge of network mapping and recreating network topologies. | 0 | PR100-5-L: Network Topology Generation |
| • K0111 - Knowledge of network tools (e.g., ping, traceroute, nslookup) | 0 | PEN-500: Network Discovery |
| • A0159 - Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute). | 0 | PEN-500: Network Discovery |
| **Information Assurance** | **Low-Moderate** | |
| • S0078 - Skill in recognizing and categorizing types of vulnerabilities and associated attacks. | 100 | PR100-4-L: Threat Designation |
| • S0367 - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | 20 | PR400-3-L: Implementing Least-Privilege on Windows |
| • S0147 - Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). | 25 | PR100-2-L: Assessing Vulnerabilities Post Addressal |
| • S0027 - Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. | 25 | PR100-2-L: Open and Close Ports on Windows 7 |
| • K0074 - Knowledge of key concepts in security management (e.g., Release Management, Patch Management). | 25 | PEN-500: Microsoft Baseline Security Analyzer |
| • K0044 - Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | 20 | PR400-3-L: Implementing Least-Privilege on Windows |
| • A0123 - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | 20 | PR400-3-L: Implementing Least-Privilege on Windows |
| **Legal, Government, and Jurisprudence** | **Low-Moderate** | |
| • K0003 - Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. | 50 | |
| • K0222 - Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities. | 0 | |
| **Computer Network Defense** | **Low-Moderate** | |
| • K0013 - Knowledge of cyber defense and vulnerability assessment tools and their capabilities. | 100 | PEN-500: Identifying System Vulnerabilities with OpenVAS |
| • S0063 - Skill in collecting data from a variety of cyber defense resources. | 28 | PR100-1-L: Using Snort and Wireshark to Analyze Traffic |
| • K0324 - Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. | 33 | PR100-2-L: IDS Setup |
| • K0177 - Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). | 100 | PR100-1-L: Comprehensive Threat Response<br>PR100-1-L: Vulnerability Analysis/Protection |
| • K0110 - Knowledge of adversarial tactics, techniques, and procedures. | 66 | |
| • K0162 - Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored). | 100 | PR100-4-L: Threat Designation |
| • K0160 - Knowledge of the common attack vectors on the network layer. | 16 | PR100-1-L: Vulnerability Analysis/Protection |
| • K0112 - Knowledge of defense-in-depth principles and network security architecture. | 33 | PR100-2-L: Assessing Vulnerabilities Post Addressal |
| • K0046 - Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions. | 25 | PR100-1-L: Using Snort and Wireshark to Analyze Traffic |
| • S0025 - Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). | 0 | PR400-3-L: SNORT Configuration and Operation Lab<br>PR100-1-L: Using Snort and Wireshark to Analyze Traffic |
| • K0161 - Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks). | 0 | PR100-1-L: Using Snort and Wireshark to Analyze Traffic |
| • K0157 - Knowledge of cyber defense and information security policies, procedures, and regulations. | 0 | PR100-1-L: Comprehensive Threat Response |
| • K0107 - Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. | 0 | |
| • A0128 - Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies. | 0 | PR100-2-L: Create Custom Snort Rules |
| • A0010 - Ability to analyze malware. | 0 | PEN-500: Analyze and Classify Malware |

# Skills Assessments: Score Your Team

## CYBRScore™ : CYBER DEFENSE ANALYST

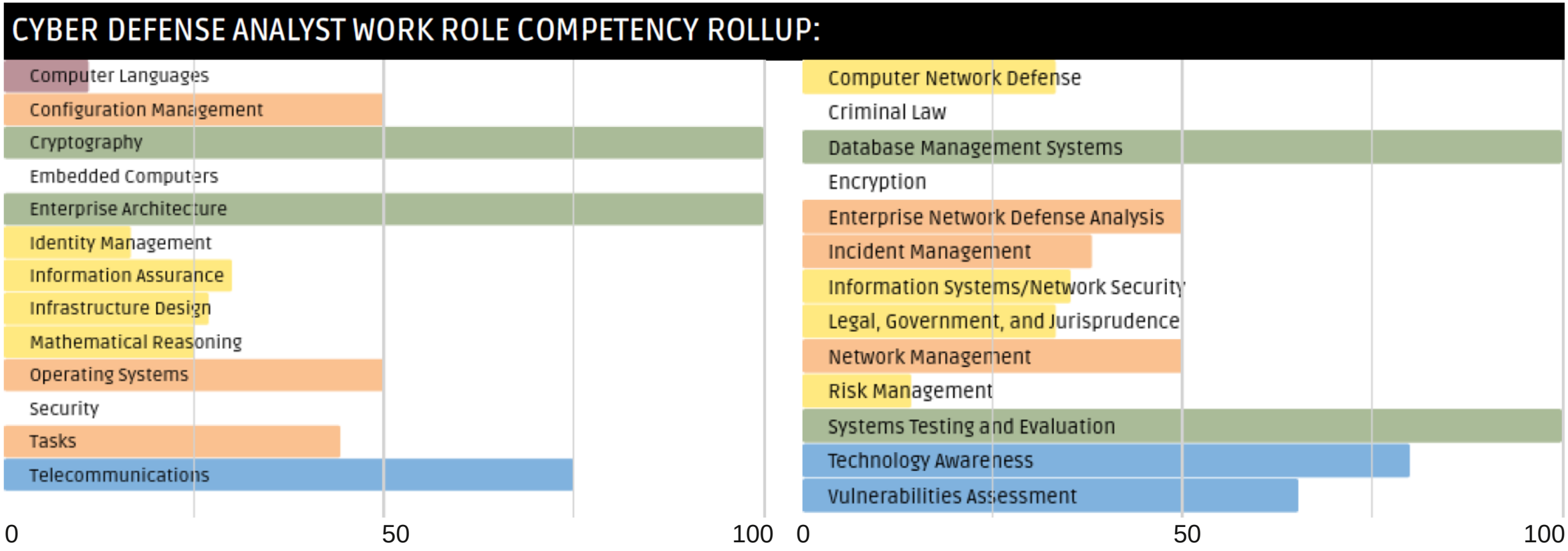
*WORK ROLE DETAILS*

**Work Role:** Cyber Defense Analyst
**Candidate Name:** Not Provided
**Customer:** Not Provided
**Overall Score:** 46%




| Assessment | Date | Score | Time | Instance |
|---|---|---|---|---|
| Incident Handling Methodology | 02/27/18 | 26% | 00:59:14 | 6127775 |
| Intrusion Detection | 02/26/18 | 24% | 00:59:51 | 6118620 |
| Network Attack Analysis | 03/05/18 | 28% | 00:59:51 | 6171995 |
| Network Defense Analysis | 02/27/18 | 88% | 00:32:04 | 6128399 |
| Protocol Analysis | 02/25/18 | 68% | 00:58:04 | 6111769 |

# Skills Assessment:  Identify Strengths and Weaknesses



# Skills Assessment: Individual Learning Plan

| Infrastructure Design | Low-Moderate | |
|---|---|---|
| • K0332 - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. | 66 | PR100-1-L: Network Segmentation<br>PEN-500: Network Discovery |
| • K0061 - 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 | PEN-500: Network Discovery<br>PR100-1-L: Network Segmentation |
| • K0001 - Knowledge of computer networking concepts and protocols, and network security methodologies. | 66 | PEN-500: Network Discovery |
| • K0221 - Knowledge of OSI model and underlying network protocols (e.g., TCP/IP). | 100 | PR100-1-L: Using Snort and Wireshark to Analyze Traffic |
| • K0303 - Knowledge of the use of sub-netting tools. | 0 | |
| • K0300 - Knowledge of network mapping and recreating network topologies. | 0 | PR100-5-L: Network Topology Generation |
| • K0111 - Knowledge of network tools (e.g., ping, traceroute, nslookup) | 0 | PEN-500: Network Discovery |
| • A0159 - Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute). | 0 | PEN-500: Network Discovery |
| **Information Assurance** | **Low-Moderate** | |
| • S0078 - Skill in recognizing and categorizing types of vulnerabilities and associated attacks. | 100 | PR100-4-L: Threat Designation |
| • S0367 - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | 20 | PR400-3-L: Implementing Least-Privilege on Windows |
| • S0147 - Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). | 25 | PR100-2-L: Assessing Vulnerabilities Post Addressal |
| • S0027 - Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. | 25 | PR100-2-L: Open and Close Ports on Windows 7 |
| • K0074 - Knowledge of key concepts in security management (e.g., Release Management, Patch Management). | 25 | PEN-500: Microsoft Baseline Security Analyzer |
| • K0044 - Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | 20 | PR400-3-L: Implementing Least-Privilege on Windows |
| • A0123 - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). | 20 | PR400-3-L: Implementing Least-Privilege on Windows |

# CYBRScore Assessments (Key To )

- Benchmark the Cohort
  - Baseline Progress of the Cohort
  - Looking at Larger Picture Aspects (NICE Framework)
- Develop Individual Learning Plans
  - Drill Down into Each KSAT and Determine Strengths and Training Gaps
  - Automatically Recommend Training
  - Eliminate Wasted Candidate Training Time
- Provide Web-Based Reporting
  - Easy to Use Reporting Allowing for Tracking of Individual and Overall Cohort Performance

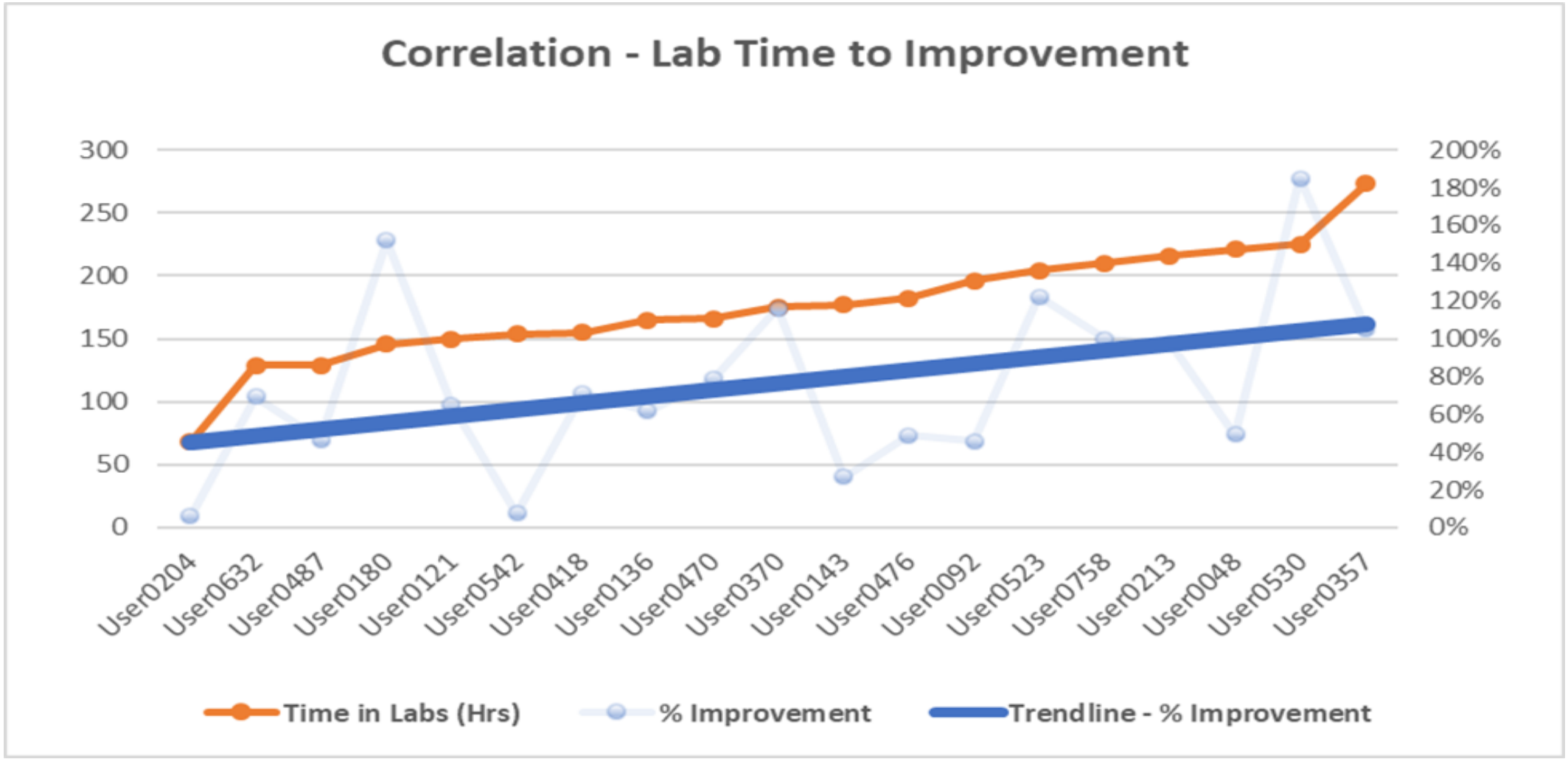
# FCRA Cohort 2 – Successes / Highlights

- 20 Completed Training; 19 Completed CYBRScore Assessments
- 18 Achieved Apprentice(+) Level on CYBRScore Assessments
- Cohort Average Assessment Score 62%
- Cohort Average Improvement was 73% From Baseline
- Successful Measurement of Hands-On Skills vs NICE Framework
- Specific Guidance for Continued Individual Improvement

# Key Take Aways

- Automated Measurement of Aptitude and Attitude Key for Cohort Selection
- Candidate Evaluation and Training Can be Accomplished at Scale
- Assessments Should be Job Role Specific
- Performance Metrics Should be Used to Track Individual and Cohort Development
- More Hands-on Time >> Better Job Role Performance

# More Hands On – Better Skills Improvement



# Lessons Learned

- Cyber Job-Placement
- Better Use of Non-Classroom Time
- Difficult to Keep Work @ Work
- Some Participants Experienced Varying Levels of “Test Anxiety”


**Erik Wallace, Director, Business Development**

**erik.wallace@comtechtel.com**

**(410) 280-1184(o)**

# Questions?