



Federal Cyber Reskilling Academy (FCRA)

Assessment, Selection, Training and Evaluation at Scale

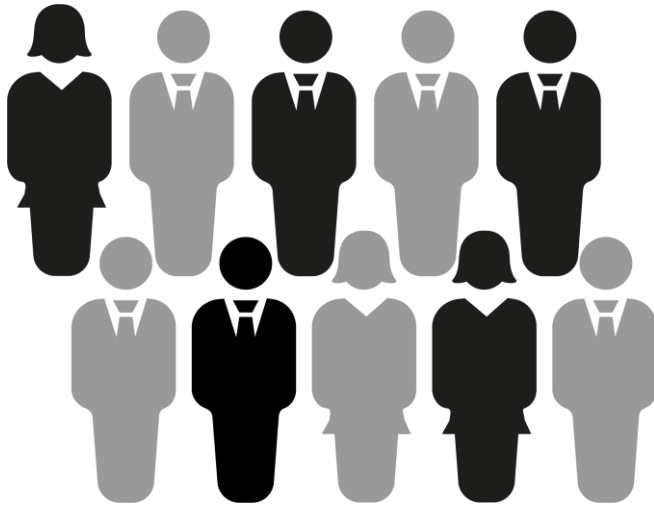
CYBRScore®

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

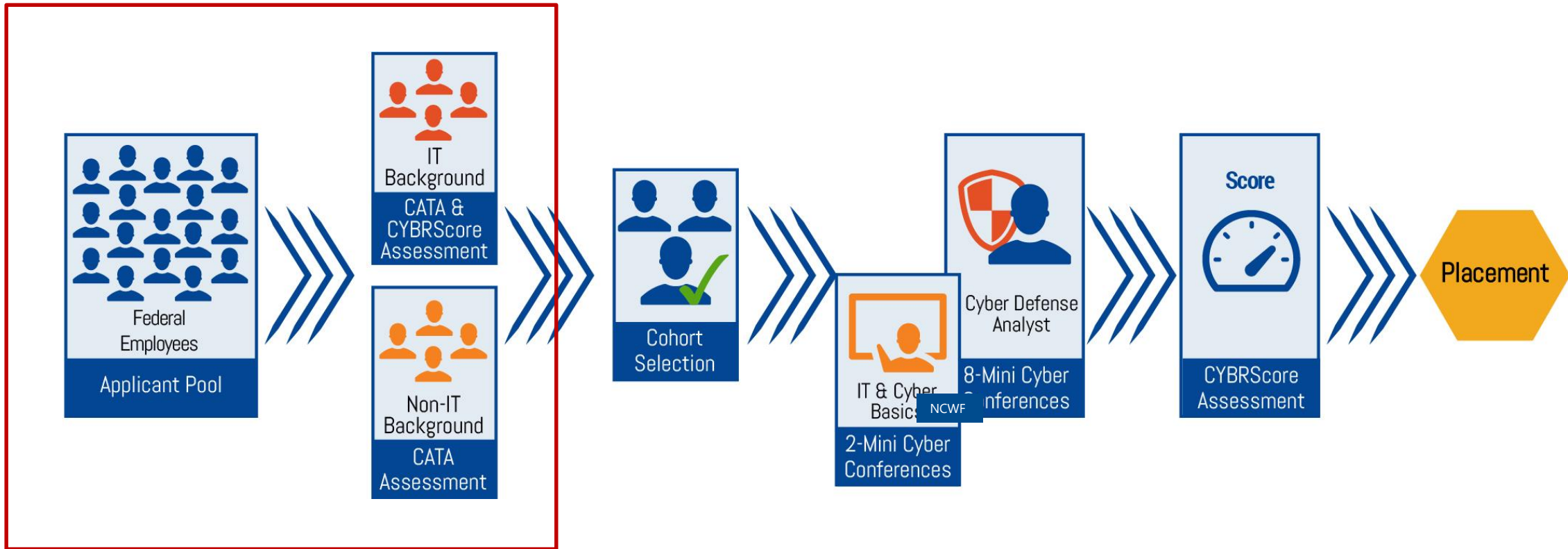


Federal Cyber Reskilling Academy

- 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



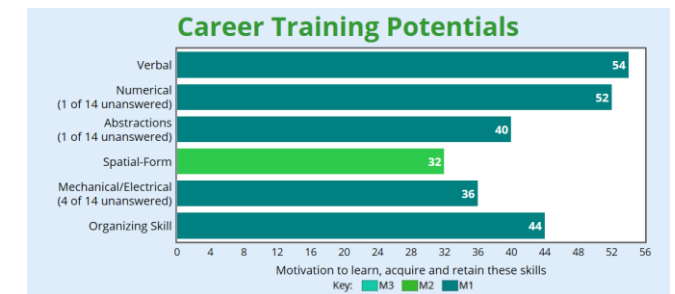
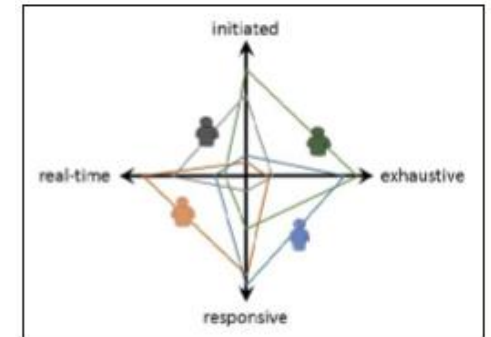
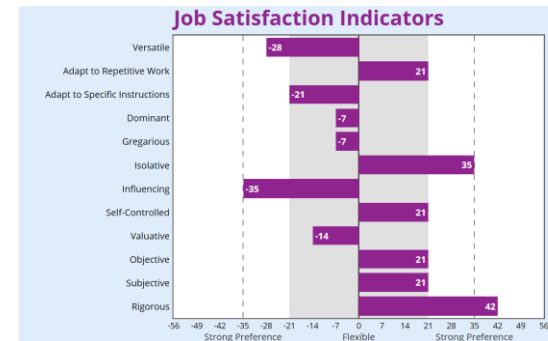
Cohort Selection – Federal Cyber Reskilling Academy

- 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

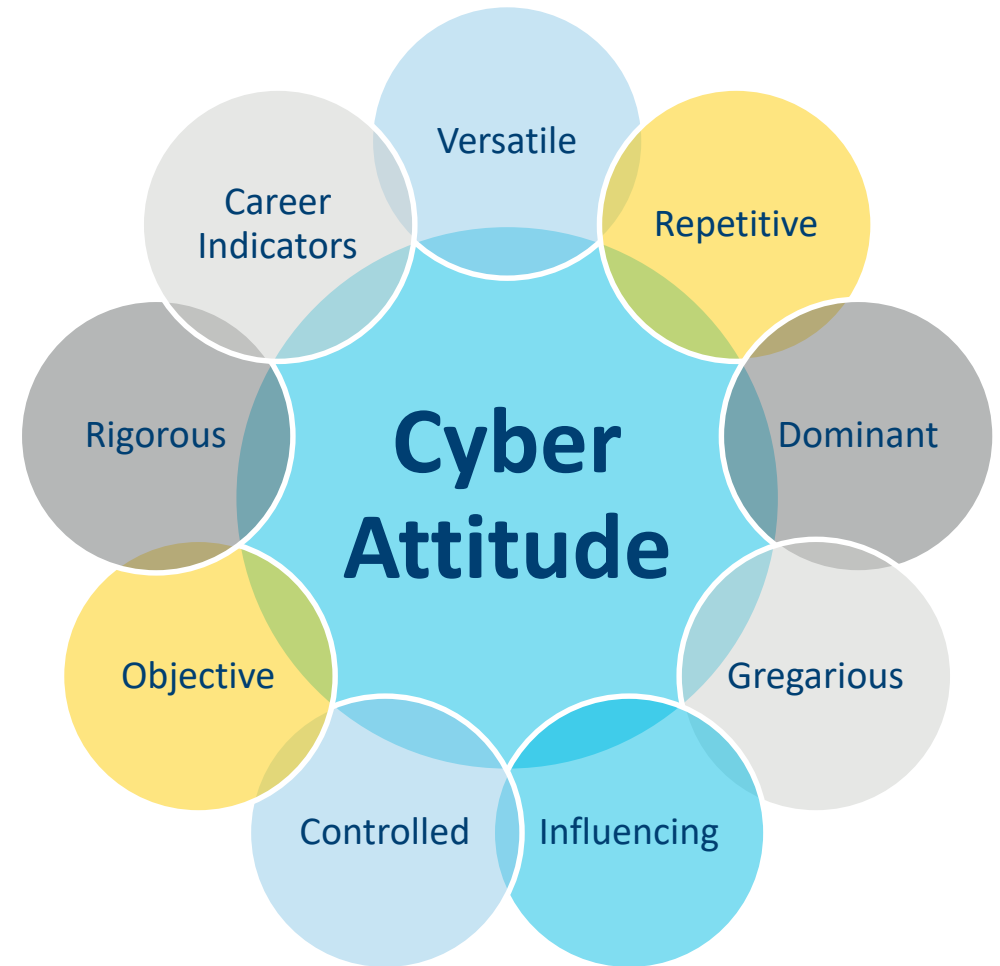
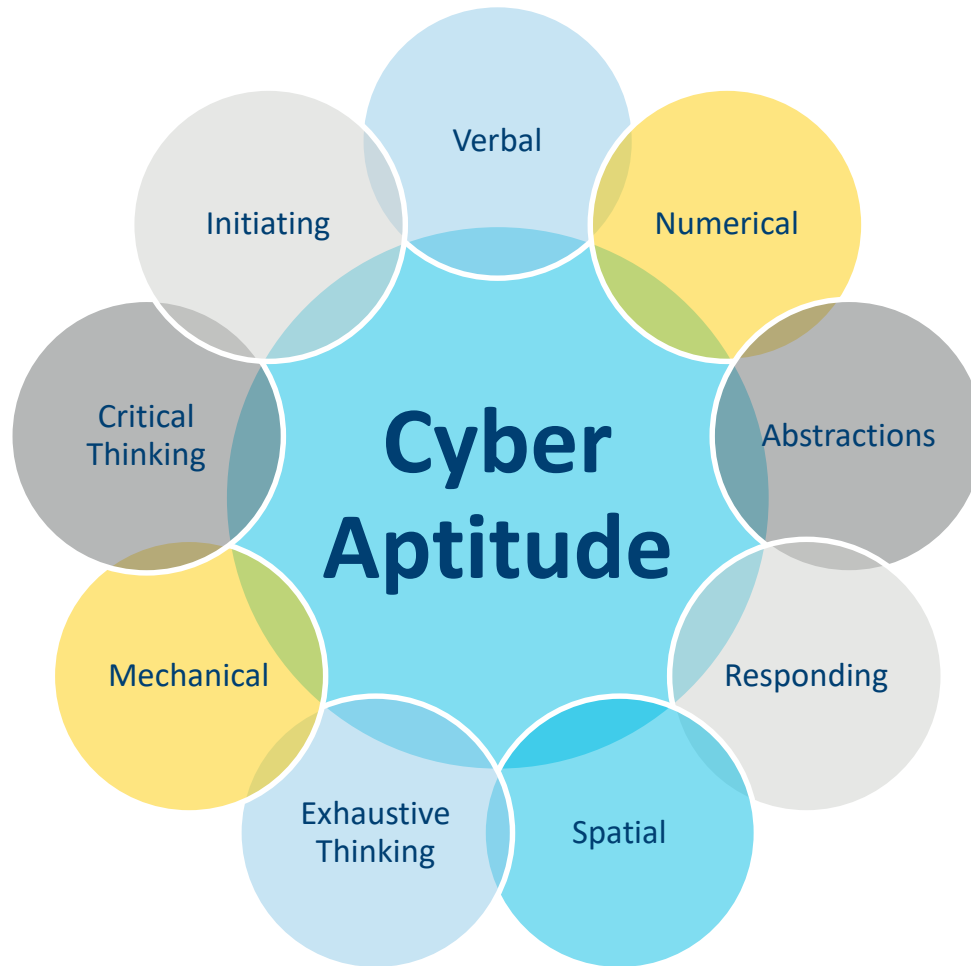


Selection: Aptitude and Attitude – Who should we select?

- 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

Wireshark 1.10.6 (v1.10.6 from master-1.10)

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
122	22.87645600	10.10.1.5	10.10.1.20	DNS	84	Standard query response 0x1142 Server failure
123	22.87645700	10.10.1.5	10.10.1.20	DNS	84	Standard query response 0x08c0 Server failure
124	22.87645800	10.10.1.5	10.10.1.10	DNS	79	Standard query response 0x2894 Server failure
125	22.87645800	10.10.1.5	10.10.1.10	DNS	79	Standard query response 0xbd51 Server failure
126	22.87649800	10.10.1.10	10.10.1.5	ICMP	107	Destination unreachable (Port unreachable)
127	22.87657100	10.10.1.10	10.10.1.5	DNS	97	Standard query 0xd8aa A clients2.google.com.prospectboost.c
128	22.88017600	10.10.1.5	10.10.1.10	DNS	164	Standard query response 0xd8aa No such name
129	22.88324200	10.10.1.20	10.10.1.5	DNS	84	Standard query 0x9895 A sls.update.microsoft.com
130	22.88402000	10.10.1.5	198.41.0.4	DNS	84	Standard query 0xd159 A sls.update.microsoft.com
131	22.98892800	10.10.1.20	10.10.1.255	BROWSER	248	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Dom.
132	23.88210700	10.10.1.20	10.10.1.5	DNS	84	Standard query 0x9895 A sls.update.microsoft.com
133	24.69356500	10.10.1.5	202.12.27.33	DNS	79	Standard query 0x09d6 A clients2.google.com
134	24.89710700	10.10.1.20	10.10.1.5	DNS	84	Standard query 0x9895 A sls.update.microsoft.com
135	26.51338900	10.10.1.5	202.12.27.33	DNS	84	Standard query 0xd159 A sls.update.microsoft.com

Frame 64: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 1

- Ethernet II, Src: Microsof_01:80:22 (00:15:5d:01:80:22), Dst: Microsof_01:80:14 (00:15:5d:01:80:14)
- Internet Protocol Version 4, Src: 10.10.1.5 (10.10.1.5), Dst: 202.12.27.33 (202.12.27.33)
- User Datagram Protocol, Src Port: 56266 (56266), Dst Port: domain (53)
 - Source port: 56266 (56266)
 - Destination port: domain (53)
 - Length: 45
 - Checksum: 0xd671 [validation disabled]
- Domain Name System (query)
 - Transaction ID: 0x2424
 - Flags: 0x0000 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0

0000 00 15 5d 01 80 14 00 15 5d 01 80 22 08 00 45 00 ..].....]..".E.

0010 00 41 36 e0 00 00 11 13 90 0a 0a 01 05 ca 0c .A6.....

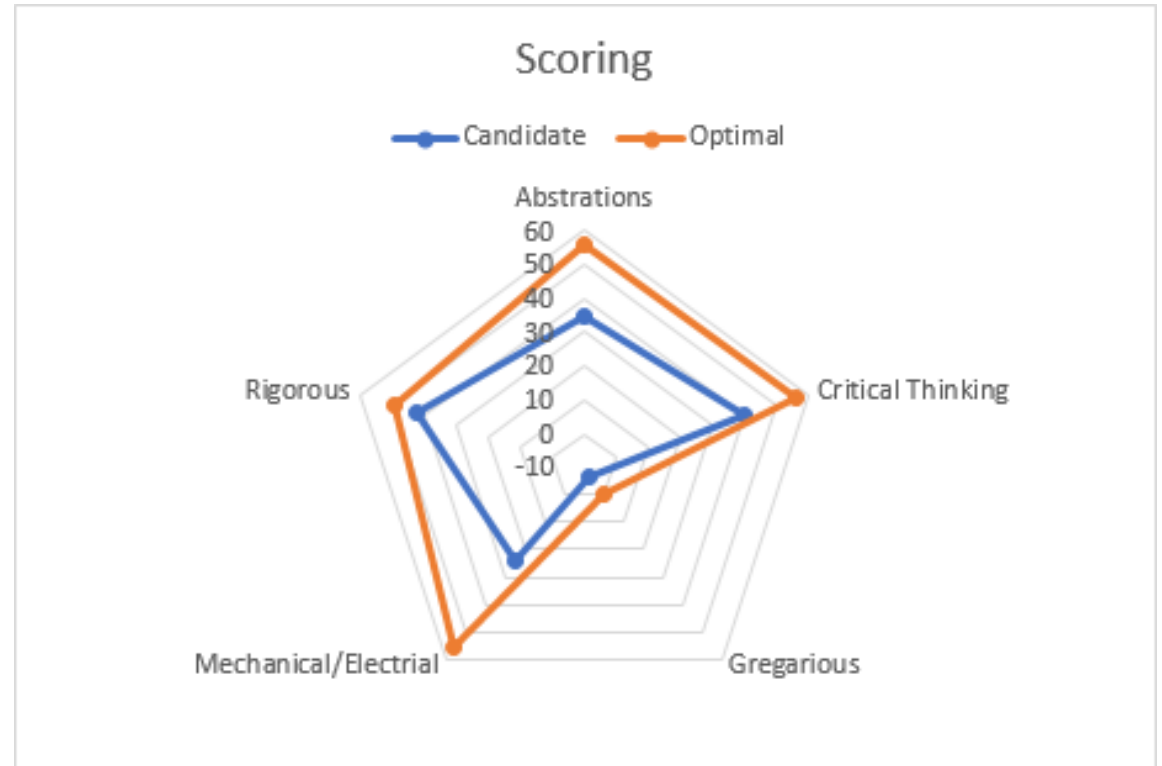
0020 1b 21 db ca 00 35 0d d6 71 24 24 00 00 00 01 .!...5.-.q\$\$...

0030 00 00 00 00 00 00 08 63 6c 69 65 6e 74 73 32 06c lients2.

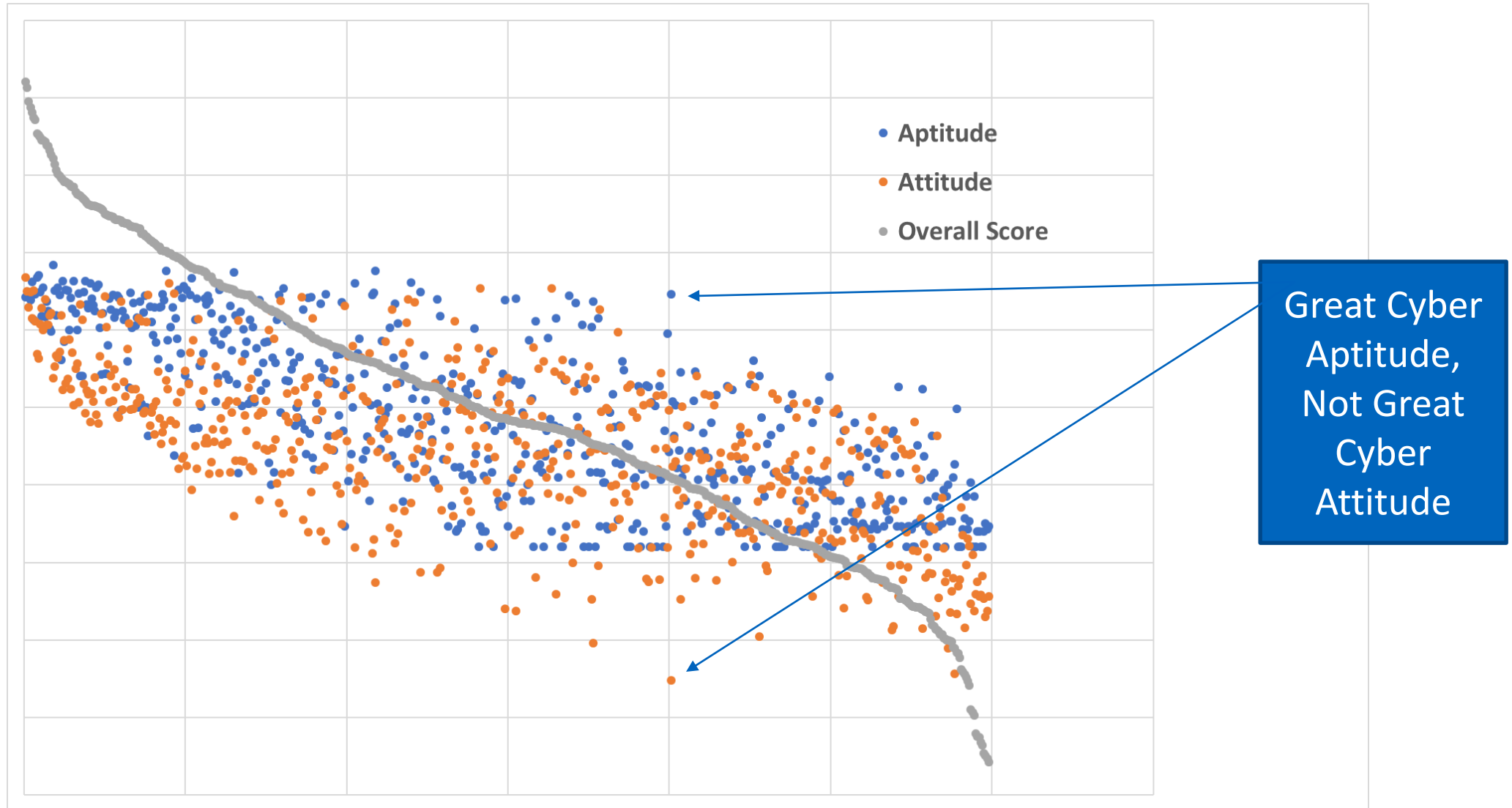
Frame (frame), 79 bytes Packets: 135 · Displayed: 135 (100.0%) · Dropped: 0 (0.0%) Profile: Default

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!!!

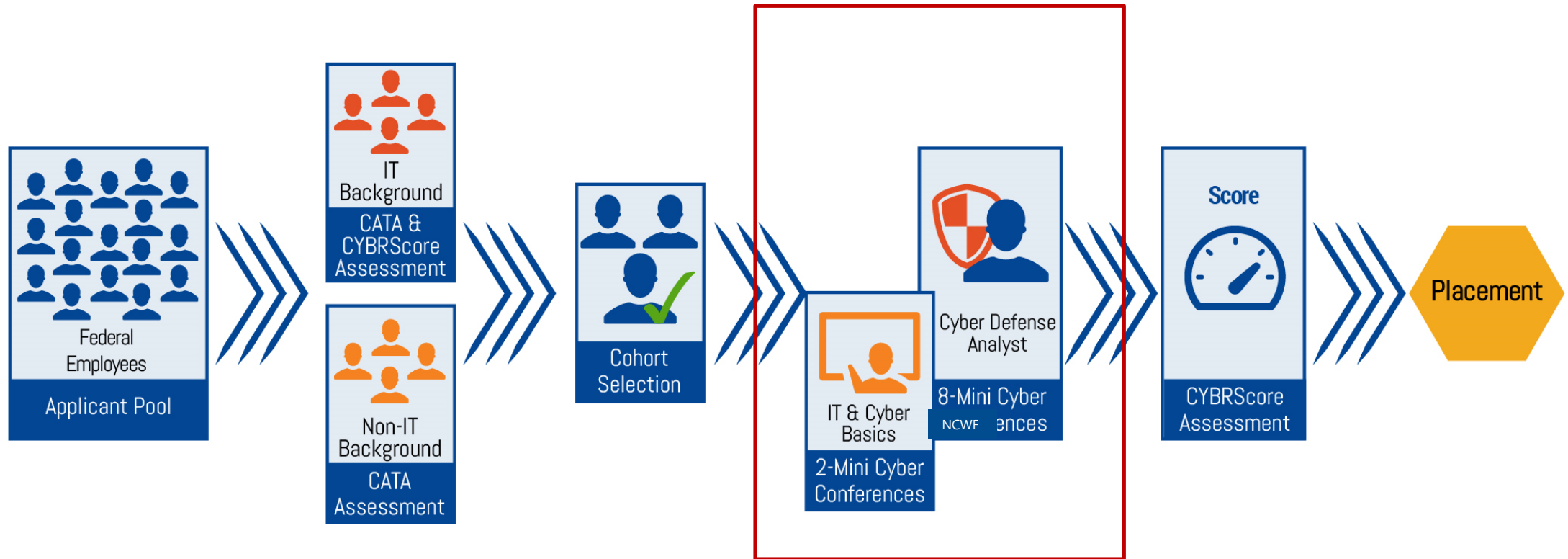


FCRA Candidate Selection Scoring



Workforce Development Challenges

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

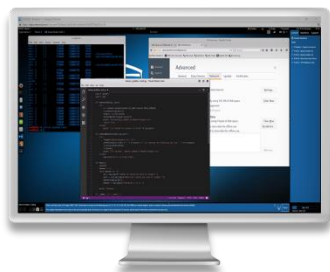


FCRA Training

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:

<div>NETWORK MANAGEMENT</div> <div>Likely to be a strength</div> <div>High</div> <div>KSA's</div> <ul style="list-style-type: none">Test & configure network workstations & peripheralsUse network management tools to monitor network trafficDiagnose failed serversCorrect physical & technical problemsKnowledge of the range of existing networksKnowledge of network systems management principles <div>10/10</div>	<div>OPERATING SYSTEMS</div> <div>Likely to be a strength</div> <div>High</div> <div>KSA's</div> <ul style="list-style-type: none">Skill in utilizing virtual networks for testingSkill in system admin for Linux/Unix operating systemsSkill in using virtual machinesKnowledge of file system implementationsKnowledge of the extensionsKnowledge of troubleshooting basic systemsKnowledge of windows command line <div>10/10</div>	<div>INFO SYSTEMS/NETWORK SECURITY</div> <div>Somewhat unlikely to be a strength</div> <div>Low-Moderate</div> <div>KSA's</div> <ul style="list-style-type: none">Skill in developing & deploying signaturesSkill in discerning the protection needs of info systems & networksKnowledge of security event correlation toolsKnowledge of current & emerging threat/threat vectorsKnowledge of host/network access controlsKnowledge of known vulnerabilities from alerts <div>7/10</div>
<div>INCIDENT MANAGEMENT</div> <div>Somewhat likely to be a strength</div> <div>High-Moderate</div> <div>KSA's</div> <ul style="list-style-type: none">Knowledge of database procedures used for documenting & querying reported incidentsKnowledge of disaster recovery continuity of operations planKnowledge of enterprise incident response programKnowledge of root cause analysis for incidentsSkill in recovering failed serversSkill in performing root cause analysis for incidents <div>8/10</div>	<div>IT ARCHITECTURE</div> <div>Somewhat unlikely to be a strength</div> <div>Low-Moderate</div> <div>KSA's</div> <ul style="list-style-type: none">Knowledge of the enterprise IT architectureKnowledge of remote access technology conceptsKnowledge of IT architectural concepts & frameworksKnowledge of parallel & distributed computing concepts <div>7/10</div>	<div>CONFIGURATION MANAGEMENT</div> <div>Unlikely to be a strength</div> <div>Low</div> <div>KSA's</div> <ul style="list-style-type: none">Knowledge of secure configuration management techniquesKnowledge of collection management processes, capabilities & limitationsSkill in configuring & utilizing hardware-based computer protection componentsSkill in configuring & utilizing network protection components <div>3/10</div>

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® Assessments: Baseline Your Team

CYBRScore™: CYBER DEFENSE ANALYST

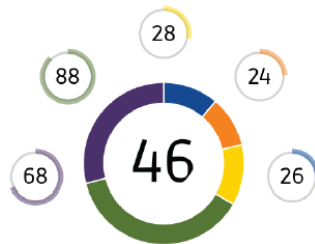
WORK ROLE DETAILS

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	28%	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%	00:59:04	6111769

HIGHER COMPETENCY SCORES:

Cryptography	Database Management Systems	Enterprise Architecture
<div><div></div><div>Likely to be a strength</div><div>High</div></div>	<div><div></div><div>Likely to be a strength</div><div>High</div></div>	<div><div></div><div>Likely to be a strength</div><div>High</div></div>
KSAa [200] Knowledge of encryption methodologies. [200] Knowledge of cryptography and cryptographic key management concepts [200] Knowledge of encryption algorithms 3/3	KSAa [200] Knowledge of database systems. 2/2	KSAa [200] Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). 1/1

LOWER COMPETENCY SCORES:

Criminal Law	Embedded Computers	Encryption
<div><div></div><div>Unlikely to be a strength</div><div>Low</div></div>	<div><div></div><div>Unlikely to be a strength</div><div>Low</div></div>	<div><div></div><div>Unlikely to be a strength</div><div>Low</div></div>
KSAa [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	KSAa [0] Knowledge of embedded systems. 0/1	KSAa [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:

- PR100-24: 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:

Computer Languages	Computer Network Defense
Configuration Management	Criminal Law
Cryptography	Database Management Systems
Embedded Computers	Encryption
Enterprise Architecture	Enterprise Network Defense Analysis
Identity Management	Incident Management
Information Assurance	Information Systems/Network Security
Infrastructure Design	Legal, Government, and Jurisprudence
Mathematical Reasoning	Network Management
Operating Systems	Risk Management
Security	Systems Testing and Evaluation
Tasks	Technology Awareness
Telecommunications	Vulnerabilities Assessment

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	PR100-1-1: Identify Whether High-Risk Systems Were Affected PR100-4-1: Threat Designation 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

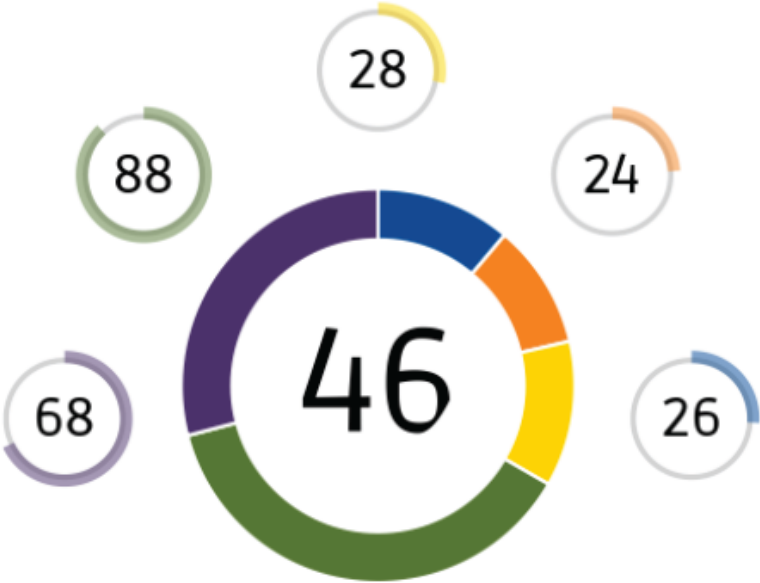
Infrastructure Design	Low-Moderate
• K0332 - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	66
• K0061 - Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	66
• K0001 - Knowledge of computer networking concepts and protocols, and network security methodologies.	66
• K0221 - Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	100
• K0303 - Knowledge of the use of sub-netting tools.	0
• K0300 - Knowledge of network mapping and recreating network topologies.	0
• K0111 - Knowledge of network tools (e.g., ping, traceroute, nslookup)	0
• A0159 - Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).	0
Information Assurance	Low-Moderate
• S0078 - Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	100
• S0367 - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	20
• S0147 - Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	25
• 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
• K0074 - Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	25
• K0044 - Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	20
• A0123 - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	20
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
• S0063 - Skill in collecting data from a variety of cyber defense resources.	28
• K0324 - Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	33
• K0177 - Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	100
• 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
• K0160 - Knowledge of the common attack vectors on the network layer.	16
• K0112 - Knowledge of defense-in-depth principles and network security architecture.	33
• K0046 - Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	25
• S0026 - Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	0
• K0161 - Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).	0
• K0157 - Knowledge of cyber defense and information security policies, procedures, and regulations.	0
• 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
• A0010 - Ability to analyze malware.	0

Skills Assessments: Score Your Team

CYBRScore™ : CYBER DEFENSE ANALYST

WORK ROLE DETAILS

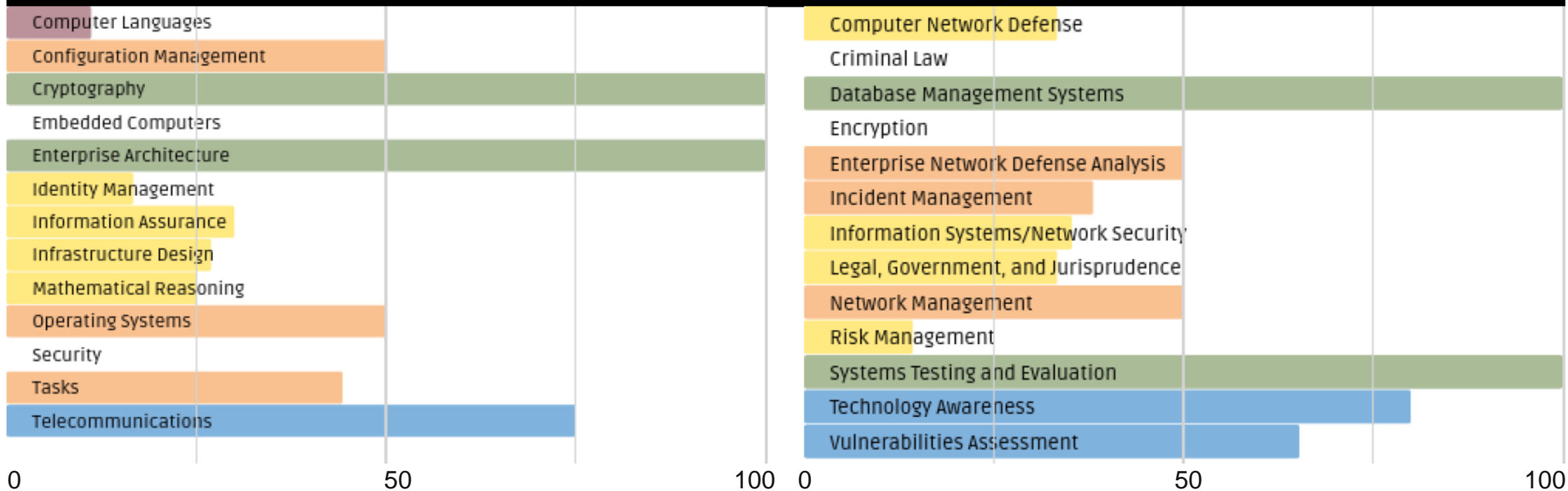
Work Role: Cyber Defense Analyst
Candidate Name: Not Provided
Customer: Not Provided
Overall Score: 46%



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

CYBER DEFENSE ANALYST WORK ROLE COMPETENCY ROLLUP:



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 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 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

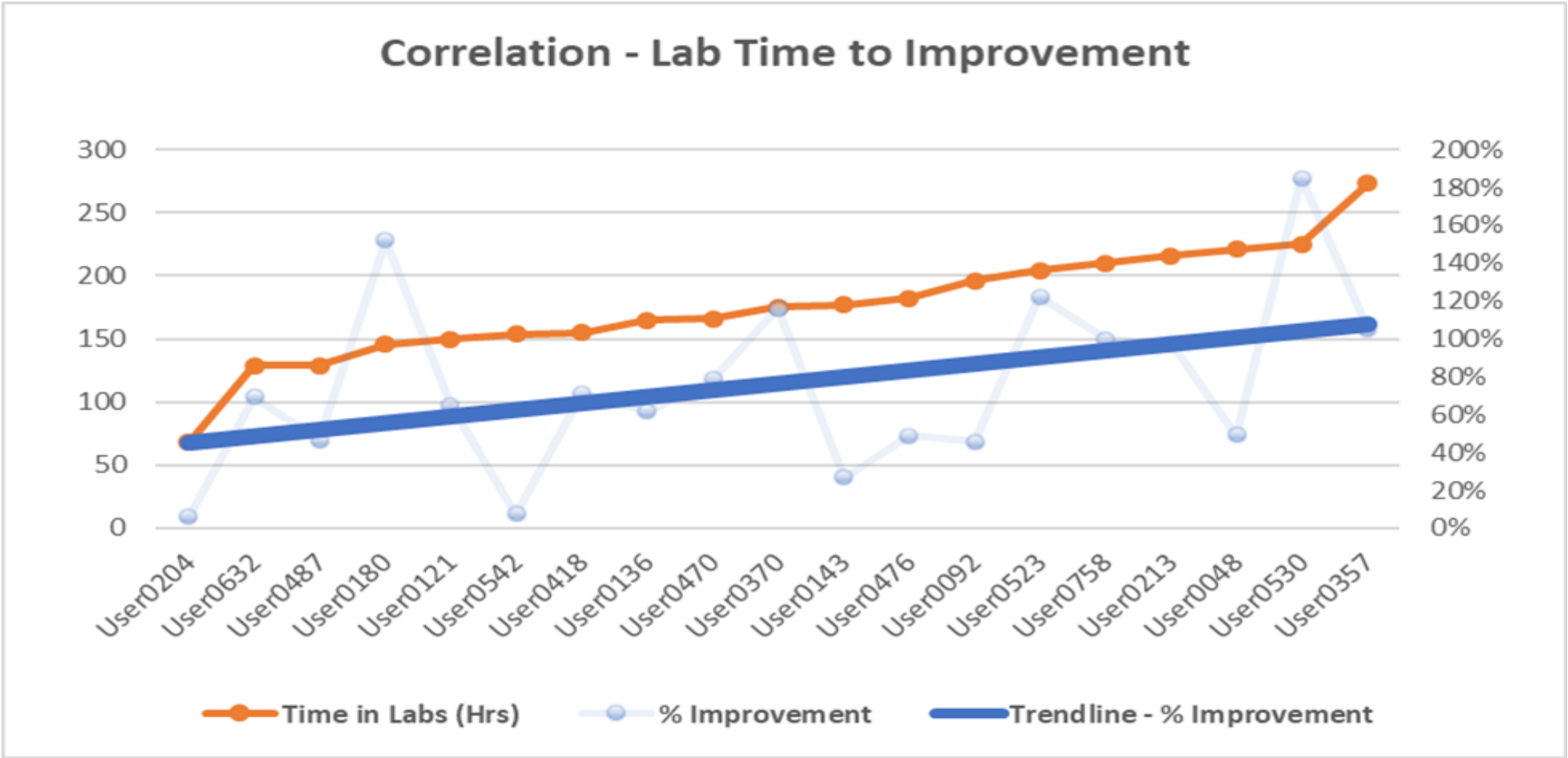
FCRA Cohort 2 – Successes / Highlights

- 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?