SKILLS ASSESSMENT: PR100 CYBER DEFENSE ANALYST

WHAT'S YOUR CYBRSCORE?

CYBRScore™ Skills Assessments are designed to accurately evaluate an organization's cyber security workforce using practical hands-on tasks in a virtual computer and network environment to evaluate one's knowledge, skills and abilities related to specific work roles. CYBRScore Skills Assessments align to the requirements of the NICE Cybersecurity Workforce Framework (NCWF) as defined by NIST SP 800-181.

PR100 Cyber Defense Analyst is designed to assess an individual's knowledge, skills and abilities related to using data collected from cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purpose of mitigating threats.

TARGET AUDIENCE

Employers seeking to verify the performance-based skills of their current workforce, or to assess a candidate employee prior to making a critical hiring decision

OBJECTIVE

Test one's competency-level in the Cyber Defense Analyst work role

RELATED JOB TITLES

Persons in the Cyber Defense Analysts work role may have job titles similar to:

- CND Analyst (Cryptologic)
- Cyber Security Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Network Security Engineer
- Security Analyst
- Security Operator
- Sensor Analyst

CYBRScore

AVAILABLE ASSESSMENTS

PR100 CYBER DEFENSE ANALYST

PR100 Cyber Defense Analyst is comprised of the following assessments.

PR100-1 PROTOCOL ANALYSIS

Evaluates an individual's ability to use a network protocol analyzer to examine network traffic, discover malicious activity, and report their findings.
OS/Tools used: Security Onion / Wireshark, tcpdump.

PR100-2 INTRUSION DETECTION

Evaluates an individual's ability to monitor events that occurred on a computer network and to review and interpret captured traffic for signs of incidents that could be considered an imminent threat or violation of security policies, standard security practices, or acceptable use policies.
OS/Tools used: Security Onion / Wireshark, Snort.

PR100-3 INCIDENT HANDLING METHODOLOGY

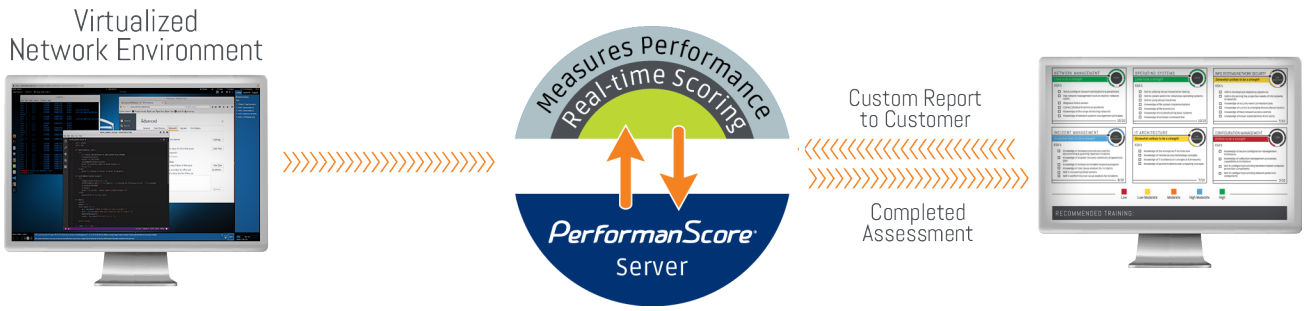
Evaluates an individual's ability to gather information on an incident, to understand the importance of following industry standard reporting techniques, to comprehend commonly utilized attack types, and to perform analysis and response tasks for a sample incident.
OS/Tools used: Security Onion, Windows / Wireshark, Microsoft Baseline Security Analyzer.

PR100-4 NETWORK DEFENSE ANALYSIS

Evaluates an individual's ability to define, identify, and classify weaknesses or vulnerabilities that exist in a system or networked environment.
OS/Tools used: Kali Linux / network scanners.

PR100-5 NETWORK ATTACK ANALYSIS

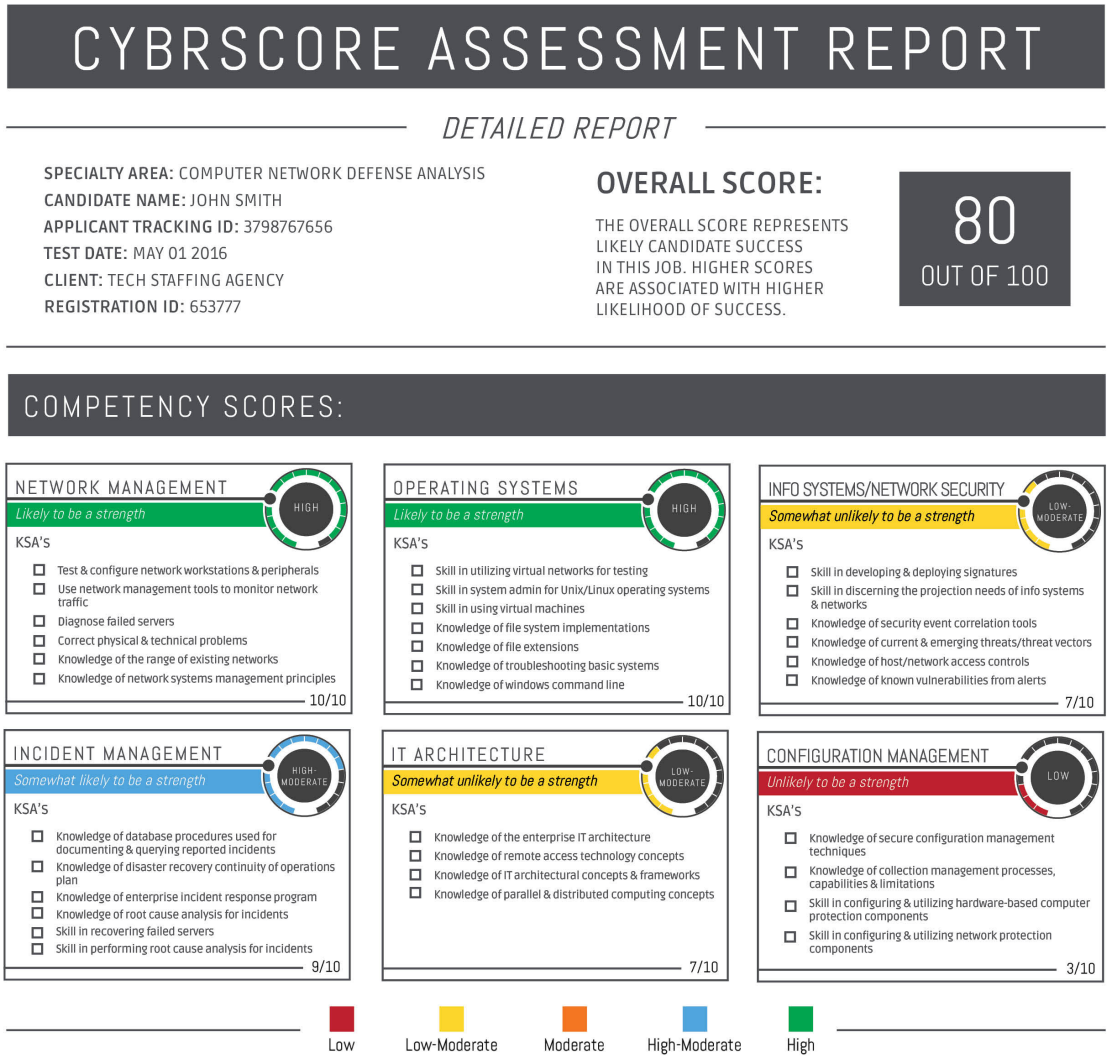
Evaluates an individual's ability to exploit previously identified weaknesses or vulnerabilities on a system or network environment.
OS/Tools used: Kali Linux / Metasploit, network scanners.



CYBRScore

CYBRSCORE SKILLS ASSESSMENT DETAILED REPORT

CYBRScore Skills Assessment delivers a detailed report that provides an individual's strengths and weaknesses in assessed competencies, KSAs, and tasks.



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.

ABOUT THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK (NCWF)

The NCWF provides a blueprint to categorize, organize, and describe cybersecurity work into Work Roles, tasks, and knowledge, skills, and abilities (KSAs). The Workforce Framework provides a common language to speak about cyber roles and jobs and helps define personnel requirements in cybersecurity.

More information about the NCWF, including the specific KSAs, Tasks and Competencies included in Cyber Defense Analyst work role can be found online at the National Initiative for Cybersecurity Education (NICE) https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework and at the National Initiative for Cybersecurity Careers and Studies (NICCS) https://niccs.us-cert.gov/.

ABOUT CYBRSCORE

CYBRScore is a premium, performance-based cyber skills training and assessment provider that quantifies a user's ability. Leveraging the NICE National Cybersecurity Workforce Framework, CYBRScore creates the complete end-to-end experience, delivering targeted, outcome-oriented cyber security training experiences that provide users with confidence to get the job done.

In a world of recognized certifications and written knowledge-based exams, our solutions stand out by providing real insight into actual on-ground cyber security skills, and the capability to support your knowledge base with demonstrated network defense skills. Headquartered in Annapolis, Maryland, CYBRScore's offerings include turnkey and custom training, hands-on labs, and performance assessment for individual skill set and defined job-role competencies.

CYBRScore

