CYBRScore® SKILLS ASSESSMENT

CYBRScore is a premium, performance-based cyber skills training and assessment provider that quantifies a user's ability to defend a network. Leveraging the NICE framework, CYBRScore creates the complete end-to-end experience, delivering targeted, outcome-oriented cyber security training experiences.

CYBRScore Skills Assessments employ practical hands-on exercises hosted in our virtual network environment which walk users through various simulated scenarios. Using our patented PerformanScore technology, each assessment collects hundreds of data points in real-time as the user completes the tasks within the exercises. Once completed, the user's manager or instructor will receive a score and report that outlines strengths and weaknesses and provides recommendations for skills development.

Skills Assessments can be implemented within a workforce development or individual learning program or used as an evaluation for job placement.

The assessment scenarios and scoring rubric are based on the National Cybersecurity Workforce Framework per NIST SP 800-181 that defines KSAs and tasks for a variety of cybersecurity work roles.

CYBRScore®

Facts about the Cybersecurity Talent Gap and Skills Shortage

Cyberattacks are growing, but the talent pool of incoming cyber defenders is not keeping pace. To further compound the problem, those present in the existing talent pool are often not fully qualified.

3.5 M cybersecurity job openings by 2021[1]

2M global shortage of cybersecurity professionals by 2019 [2]

3 in 10 cybersecurity professionals came to the field from a background outside of IT [3]

Two-thirds of its nearly 20,000 respondents indicated that their organizations lack the number of cybersecurity professionals needed for today's threat climate [4]

Estimates say women only make up 14% of the U.S. cybersecurity workforce -- huge opportunity space [5]

More than half (52%) of those surveyed report that it's difficult to find people with industry-specific experience [6]

Key Benefits

➤ On Demand based on your schedule - Available 24x7.

➤ Simple HTML5 web browser use; no special software required, VPN, or plug-ins required.

➤ Turn-key, we host everything, no hardware/software or licenses to manage.

➤ Easily Scales to support growing workforce or student base (tens, hundreds, thousands).

➤ Evaluates candidate performance in real-time - Scored results returned immediately.

➤ Real-world scenarios – using real operating systems and complex networks.

➤ Individual Learning Plans reduce training time and costs.

➤ Quickly identify talent with best in class measurements and reporting.

---

[1]Cybersecurity Jobs Report 2018-2021, Cybersecurity Ventures, 2018

[2]UK House of Lords Digital Skills Committee

[3]1) 2017 GISW Study - https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#745dca65a6b3

[4]2017 GISW Study - https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#745dca65a6b3

[5]2017 GISW Study - https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#745dca65a6b3

[6]Dark Reading, Surviving the IT Security Skills Shortage, May 31, 2015

DEMONSTRATE COMPETENCE + DOLLARS IN YOUR POCKET.

Overall Score provides numerical value as to where the user falls on determined grading criteria, between 0-100. Competency Scores detail user's strengths and weaknesses in specific job-role competencies.

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:

NETWORK MANAGEMENT
Likely to be a strength — HIGH

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
Likely to be a strength — HIGH

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
Somewhat unlikely to be a strength — LOW-MODERATE

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
Somewhat likely to be a strength — HIGH-MODERATE

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
Somewhat unlikely to be a strength — LOW-MODERATE

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
Unlikely to be a strength — LOW

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:

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.

Recommend Training offers supplemental training suggestions for job-role competencies where user can improve.

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.

Assessments Available Today

OM500 – System Administration Full Assessment

PR100 – Cyber Defense Analyst Full Assessment

PR100-1 – Protocol Analysis

PR100-2 – Intrusion Detection

PR100-3 – Incident Handling Methodology

PR100-4 – Network Defense Analysis

PR100-5 – Network Attack Analysis

PR400 – Vulnerability Assessment Analyst Full Assessment

PR400-1 – Intelligence Gathering

PR400-2 – Attack (Red Team)

PR400-3 – Defend (Blue Team)

Assessments – Coming Soon

PR300 – Cyber Defense Incident Responder Full Assessment

PR300-1 – Collection and Analysis

PR300-2– Reporting and Remediation

IN300 – Cyber Defense Forensics Analyst Full Assessment

IN300-1 – Network Collection and Handling

IN300-2 – File Collection and Analysis

IN300-3 – Malware Analysis

About CYBRScore

CYBRScore® is a premium, performance-based cyber skills training and assessment provider that qualifies a user's capacity to perform cybersecurity operations. Leveraging the NICE framework, CYBRScore creates the complete end-to-end experience, delivering targeted, outcome-oriented cybersecurity training experiences to 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-net cybersecurity skills, and the capability to support your knowledge base with demonstrated practical skills.

CYBRScore® Skills Lab Library

TRAINING FOR THE CYBER PROFESSIONALS OF TOMORROW

CYBRScore's immersive hands-on labs allow professionals to develop and enhance their skills in an independent fashion. Our library includes over 300 labs in a variety of topic areas including system hardening, vulnerability analysis, incident response, digital media forensics, malware analysis, and penetration testing as well as general IT skills. Labs are available in a hosted environment that can be accessed in an **on-demand anywhere, anytime** fashion.

CYBRScore labs are delivered in 3 formats. **Step-by-step labs** provide sufficient instructions such that they can be used as standalone learning environments. They walk the student thru the lab for structured but independent learning. **Scored labs** provide scoring results back to the instructor providing information on lab completion and amount of time spend in the lab. **Capstone labs** remove the scaffolding and test student's knowledge, skills and abilities (KSAs). Capstone labs evaluate the student in a scored scenario-based environment providing real time results.

Key benefits

➤ On Demand based on your schedule - Available 24x7.

➤ Browser Based – HTML5 – No special software, VPN, or plug-ins required.

➤ Turn-key, we host everything, no hardware/software or licenses to manage.

➤ Easily Scales to support growing workforce or student base (tens, hundreds, thousands).

➤ Evaluates candidate performance in real-time - Scored results returned immediately.

➤ Real-world scenarios – using actual operating systems and complex networks.

➤ Individual Learning Plans reduce training time and costs.

www.cybrscore.io

CYBRScore
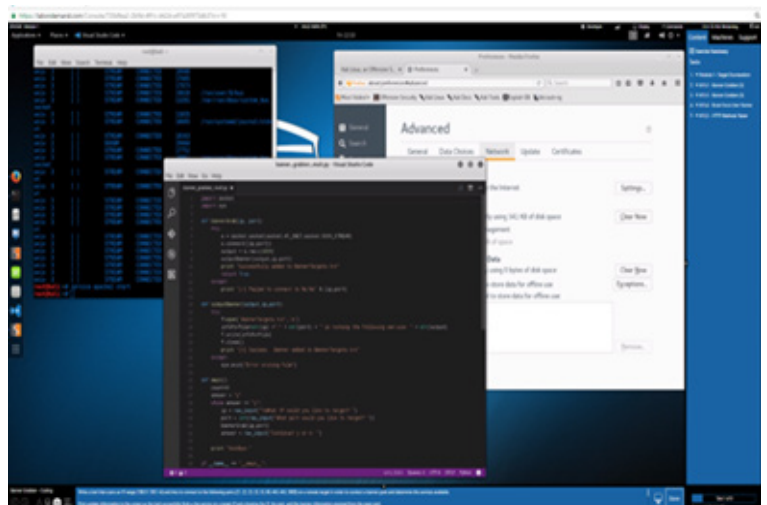
Lab Library (Example)

Beginner
- » Personal Security Products (Expected Duration 45 minutes)
- Report Writing for Presentation to Management (Expected Duration 1 hour)
- Sensitive Information Identification (Expected Duration 1 hour)
- Wireshark (Expected Duration 1 hour)
- Implement Single System Changes in Firewall (Expected Duration 45 minutes)
- Incident Detection and Identification (Expected Duration 2 hours, 30 minutes)
- Installing Patches and Testing Software (Expected Duration 1 hour, 30 minutes)
- Interoffice Communications Correction (Expected Duration 30 minutes)
- Linux Users and Groups (Expected Duration 1 hour)

Intermediate
- Analyze SQL Injection Attack (Expected Duration 42 minutes)
- Analyze Various Data Sources to Confirm Suspected BlackHole Infection (Expected Duration 1 hour)
- Baseline Systems in Accordance with Policy Documentation (Expected Duration 1 hour)
- Core Impact Web Application Penetration Testing (Expected Duration 1 hour)
- Create Custom Snort Rules (Expected Duration 1 hour)
- Log Analysis (Expected Duration 45 minutes)
- Log Correlation and Analysis (Expected Duration 49 minutes)
- Recover from Illegal Bitcoin Mining Incident (Expected Duration 45 minutes)
- Recover from Incident (Expected Duration 48 minutes)

Advanced
- Advanced Techniques for Malware Recovery (Expected Duration 1 hour, 5 minutes)
- Analyze Browser-based Heap Spray Attack (Expected Duration 43 minutes)
- Analyze Structured Exception Handler Buffer Overflow Exploit (Expected Duration 32 minutes)
- Detect Embedded Shellcode in a Microsoft Office Document (Expected Duration 1 hour)
- Pentesting & Network Exploitation - LAN Exploitation Labs (Expected Duration 3 hours)
- Pentesting & Network Exploitation - WAN/DMZ Exploitation & Pivoting Labs (Expected Duration 3 hours)
- Penetration Tester Challenge (Expected Duration 3 hours) Mini-Assessment Available

Available Lab Bundles

Custom Lab Bundles Built On-Request

- Network Essentials
- Security Essentials
- Ethical Hacker Essentials
- Security Professional Essentials
- Pentesting & Network Exploitation
- Pentest Module 1 Windows Target Analysis

- Pentest Module 2 LINUX Target Analysis
- Pentest Module 3 LAN Exploitation
- Pentest Module 4 DMZ Exploitation
- Digital Media Forensics Basic Digital Media Forensics Advanced
- Digital Media Forensics Network
- Protocol Analysis

- Intrusion Detection
- Incident Handing Methodology
- Network Defense
- Network Attack
- Information Gathering
- Attack (Red Team)
- Defend (Blue Team)

Tools Utilized Throughout CYBRScore® Labs

- Apache
- Armitage
- bro
- Core Impact
- CU Spider
- DarkComet RAT
- ELSA
- Foxit PDF reader
- Hping3
- Kali
- md5deep
- Metasploit

- Microsoft Baseline Security Analyzer
- mmc (Microsoft Management Console)
- MS Baseline Analyzer
- MS Security Essentials
- MySQL
- Network Miner   Nmap
- OpenVAS
- pfsense firewall
- PHP
- Python 2.7
- Scanline
- Security Essentials

- Server Backup
- Snorby
- Snort
- Splunk
- Suricata
- tcpdump
- Win 7 SP1 installer
- Windows Firewall
- Windows offline updater
- Wireshark
- Zenmap

About CYBRScore

CYBRScore® is a premium, performance-based cyber skills training and assessment provider that quantifies a user's ability to defend a network. Leveraging the NICE 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.