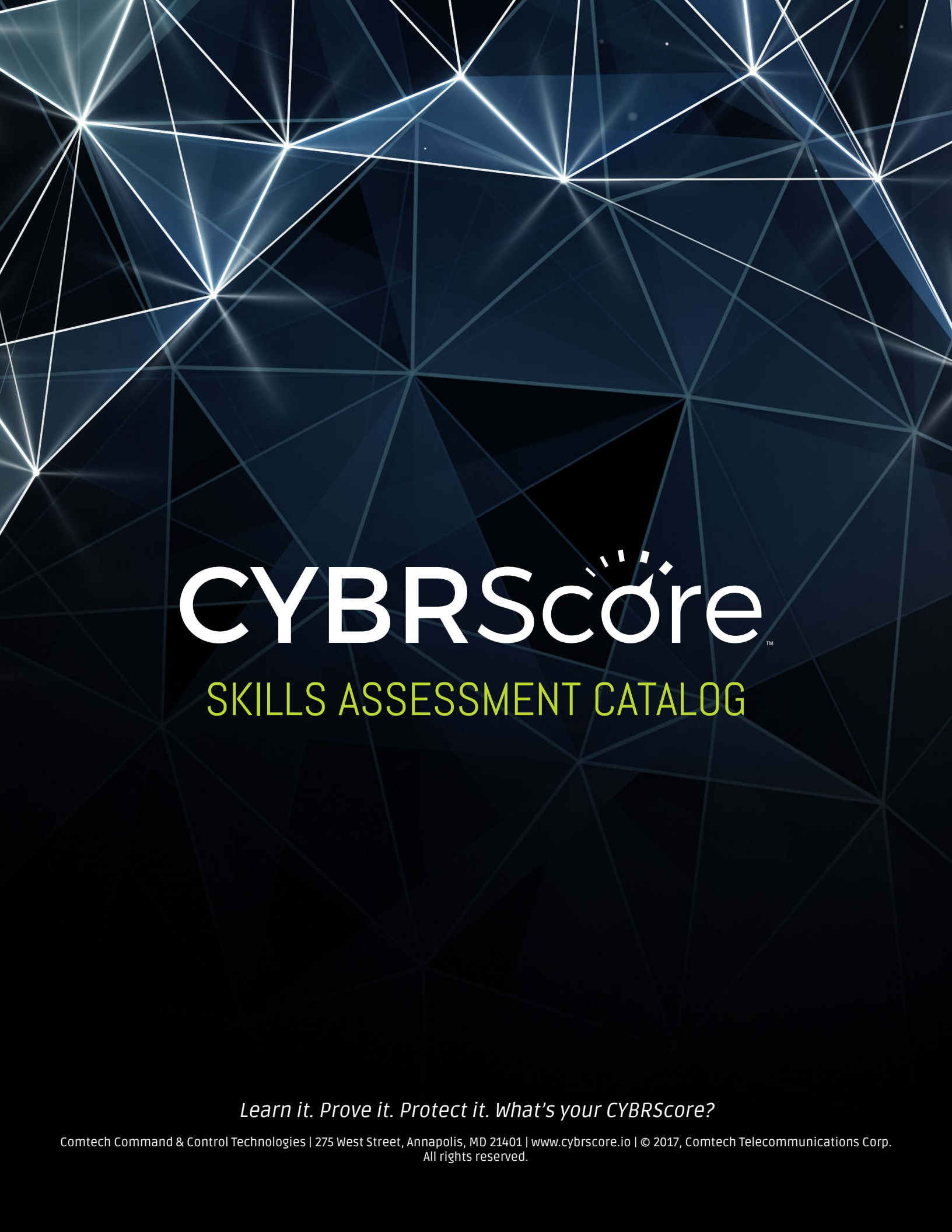

Learn it. Prove it. Protect it. What's your CYBRScore?

Comtech Command & Control Technologies | 275 West Street, Annapolis, MD 21401 | www.cybrscore.io |

TABLE OF CONTENTS

CYBRScore™

CYBRScore Skills Assessment

The CYBRScore Skills Assessment is carefully designed to meet the recommendations of the NICE Cybersecurity Workforce Framework (NCWF). NCWF is viewed as the "cybersecurity workforce dictionary," providing the nationally recognized information and standards necessary to educate, recruit, train, develop, and retain a highly-qualified cyber security workforce.

NCWF identifies seven high-level categories of common cyber security functions. These provide the overarching structure of the NCWF. These categories are further divided into work roles. The NCWF also identifies specific competencies and related knowledge, skills, and abilities (KSAs) expected of a professional working in one of the identified work roles.

CYBRScore Skills Assessments utilize the NCWF recommendations to provide a performance-based assessment solution for employers seeking to evaluate their current workforce and position candidates.

CATEGORIES	
Securely Provision (SP)	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development
Operate & Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Oversee & Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cyber security work
Protect & Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks
Analyze (AN)	Performs highly specialized review and evaluation of incoming cyber security information to determine its usefulness for intelligence
Collect & Operate (CO)	Provides specialized denial and deception operations and collection of cyber security information that may be used to develop intelligence
Investigate (IN)	Investigates cyber security events or crimes related to information technology (IT) systems, networks, and digital evidence

Source: U.S. Department of Commerce

CYBRScore™

OM500

SYSTEM ADMINISTRATION

OM500 - System Administration is designed to assess the knowledge, skills and abilities required by the System Administration specialty area as defined by the NICE Cybersecurity Workforce Framework.

Individuals in this role should have a comprehensive understanding of installing, configuring, troubleshooting and maintaining server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. They should also be able to manage accounts, firewalls, and patches, and be responsible for access control, passwords, and account creation and administration.

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 System Administration specialty area

RELEVANT JOB ROLES	
LAN Administrator	System Operations Personnel
Platform Specialist	Systems Administrator
Security Administrator	Website Administrator
Server Administrator	

CYBRScore™

ASSESSED COMPETENCIES

Computer Forensics	Information Systems/Network Security	Software Engineering
Computer Languages	Information Technology Architecture	Systems Integration
Configuration Management	Information Technology Performance Assessment	Systems Life Cycle
Encryption	Infrastructure Design	Technology Awareness
Identity Management	Network Management	Telecommunications
Incident Management	Operating Systems	

ASSESSED KNOWLEDGE

- Basic System Administration, Network & Operating System Hardening Techniques
- Enterprise IT Architecture
- File Extensions
- File System Implementations
- IT Security Principles & Methods
- Local Area & Wide Area Networking Principles & Concepts
- Measures/Indicators of System Performance & Availability
- Network Protocols
- New Technological Developments in Server Administration
- Organizational IT User Security Policies
- Performance Tuning Tools & Techniques
- Principles & Methods for Integrating Server Components
- Server Administration & Systems Engineering Theories, Concepts, & Methods
- Server & Client Operating Systems
- Server Diagnostic Tools & Fault Identification Techniques
- Systems Administration Concepts
- Transmission Methods & Jamming Techniques
- Type/Frequency of Routine Maintenance Needed for Proper Function
- Unix Command Line
- Virtual Private Network Security
- Virtualization Technologies & Virtual Machine Development & Maintenance

ASSESSED SKILLS

- Conducting Server Planning, Management & Maintenance
- Configuring & Optimizing Software
- Configuring & Utilizing Software-Based Computer Protection Tools
- Correcting Physical & Technical Problems that Impact Server Performance
- Diagnosing Connectivity Problems
- Diagnosing Failed Servers
- Identifying & Anticipating Server Performance, Availability, Capacity or Configuration Problems
- Installing Computer & Server Upgrades
- Maintaining Directory Services
- Monitoring & Optimizing Server Performance
- Recovering Failed Servers
- System Administration for Unix/Linux Operating Systems
- Using Virtual Machines

OM500
SYSTEM ADMINISTRATION

CYBRScore™

PR400

VULNERABILITY ASSESSMENT & MANAGEMENT

PR400 - Vulnerability Assessment & Management is designed to assess the knowledge, skills and abilities required by the Vulnerability Assessment & Management specialty area as defined by the NICE Cybersecurity Workforce Framework.

Individuals in this role should have a comprehensive understanding of the tools and techniques to detect and exploit security vulnerabilities in web-based applications, networks, and computer systems that use the Windows and Linux OS, as well as recommend mitigation countermeasures.

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 Vulnerability Assessment & Management specialty area

RELEVANT JOB ROLES		
Blue Team Technician	Ethical Hacker	Reverse Engineer
Certified TEMPEST Professionals	Governance Manager	Risk/Vulnerability Analyst
Certified TEMPEST Technical Authority	Information Security Engineer	Technical Surveillance Countermeasures Technician
Close Access Technician	Internal Enterprise Audit	Vulnerability Assessment Analyst
CND Auditor	Penetration Tester	Vulnerability Manager
Compliance Manager	Red Team Technician	

CYBRScore™

ASSESSED COMPETENCIES

Computer Forensics	Human Factors	Network Management
Computer Languages	Identity Management	Systems Testing & Evaluation
Computer Network Defense	Information Assurance	Vulnerability Assessment
Contracting/Procurement	Information Systems/Network Security	
Criminal Law	Infrastructure Design	

ASSESSED KNOWLEDGE	Application Vulnerabilities
	Classes of Attacks
	Content Development
	Constitution of Network Attacks & Relationship to Threats/Vulnerabilities
	Data Backup, Types of Backups, Recovery Concepts & Tools
	General Attack Stages
	Information Assurance Principles & Organizational Requirements for Data Protection
	Interpreted & Compiled Computer Languages
	Laws, Policies, Procedures & Governance Related to Critical Infrastructure Impact
	Network Access, Identity & Access Management
	Network Protocols & Directory Services
	Network Security Architecture Concepts
	Operational Threat Environments
	Pentesting Principles, Tools & Techniques
	Programming Language Structures & Logic
	System & Application Security Threats & Vulnerabilities
	Systems Diagnostic Tools & Fault Identification Techniques
	System Requirements for Safety, Performance & Reliability
	Traffic Flow Across a Network
ASSESSED SKILLS	Applying Host/Network Access Controls
	Assessing Robustness of Security Systems & Designs
	Detecting Host & Network-Based Intrusions Via Intrusion Detection Technologies
	Evaluating Trustworthiness of Supplier/Product
	Mimicking Threat Behaviors
	Performing Damage Assessments
	Performing Packet-Level Analysis
	Using Pentesting Tools & Techniques
	Using Social Engineering Techniques
	Using Network Analysis Tools to Identify Vulnerabilities
ASSESSED ABILITIES	Identification of Systemic Security Issues Based on Analysis of Vulnerability & Configuration Data

PR400

VULNERABILITY ASSESSMENT & MANAGEMENT

CYBRScore™