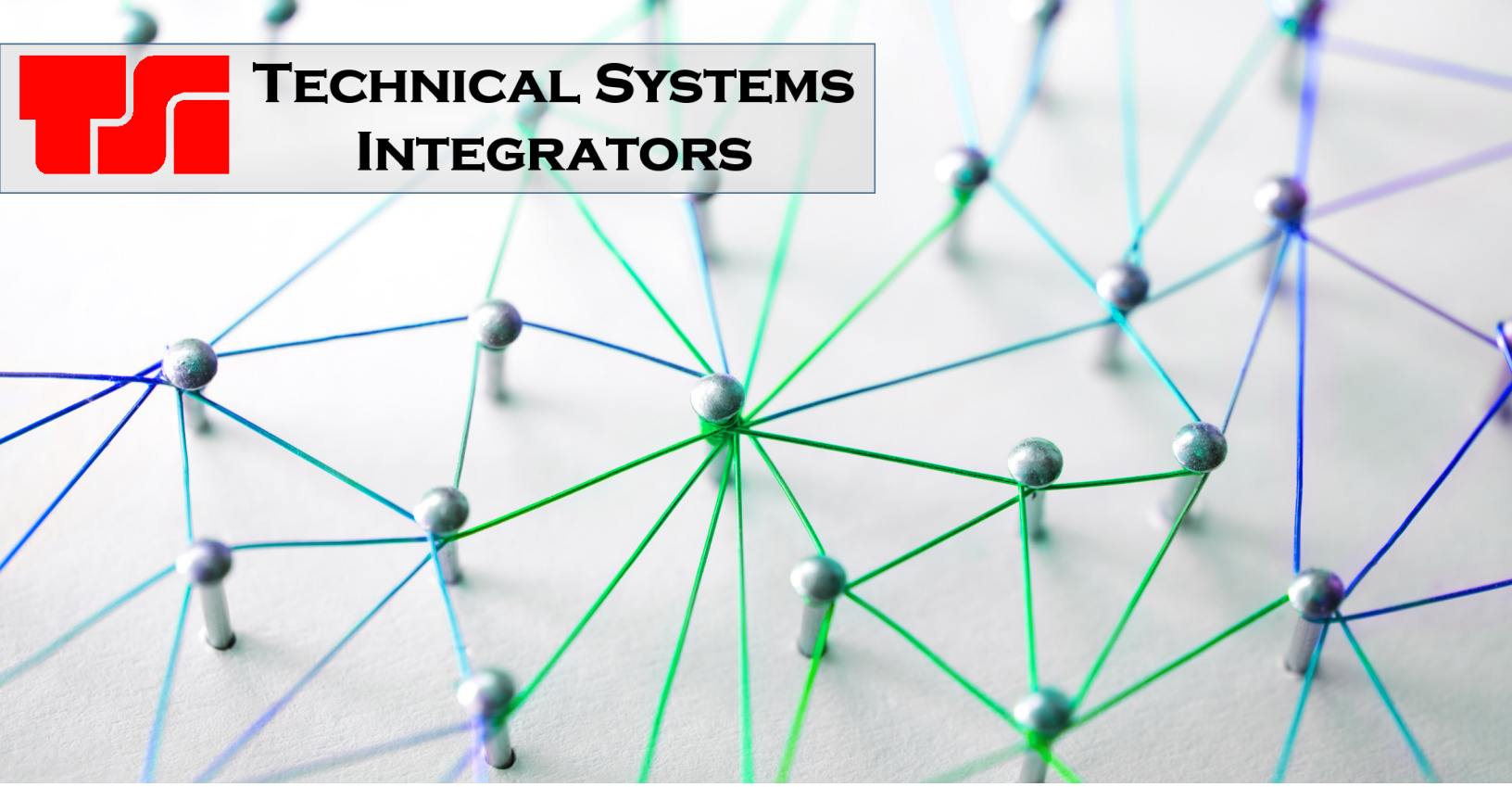
TECHNICAL SYSTEMS INTEGRATORS



CYBRSCORE® ACADEMY

LEARN BY DOING!

CYBRScore® educates cybersecurity professionals in "hands-on" lab environments on topics that include incident response, malware analysis, computer, media and mobile device exploitation, penetration testing and vulnerability assessment, reverse engineering, information assurance and cyber forensics.

Our students train on the latest cybersecurity practices and methodologies, whether in a classroom, workplace or at home. Our courses are mapped directly to specific learning objectives from governing institutions and cybersecurity communities of practice, including the NICE National Cybersecurity Workforce Framework and DoD Directive 8140.

OUR MISSION

With over 20+ courses and 400+ hands-on labs, we provide entry-level through seasoned cyber professionals with world-class education to build knowledge, skills and abilities in the latest cyber security techniques, skills, and best practices.

Why CYBRScore?

- Hands-on, Performance-Based Education Tied to Clearly-Defined and Accurate Performance Outcomes
- Education Developed from the Job Outward
- Practice and Immediate Feedback Provided
- Tasks Replicated through Real-World Scenarios
- Focus on Essentials
- Required Student Demonstration of Competencies and Tasks

CYBRScore®

SAMPLE COURSE LISTING

Cybersecurity

CYB300 – Cybersecurity Awareness: Provide detailed-discussion & hands-on practical application in the identification/classification of vulnerabilities & malware; explanation of the hacker threat & methodology & explore best-practice procedures & processes associated with security appliances & applications.

LNX101-OD – Fundamentals of Linux Security for System Administrators - Teaches students basic Linux command line usage and filesystem structure, how to configure, evaluate and troubleshoot common management services used on today's Linux systems, and well as how to configure and test a Linux-based firewall.

Development

DEV400– Introduction To Programming C: Provide an introduction to writing language for operating systems, embedded processors, micro-controllers, assemblers, exploits and network drivers.

DEV550 – Python For Pentesters: Provide students with the knowledge necessary to analyze technical situations, solving them through the development of Python tools.

Forensics

FOR300 – Basic Digital Media Forensics: Provide a solid understanding of what is considered valuable digital media used as forensic evidence for an investigation, including how data is stored, retrieved and analyzed.

FOR400 – Fundamentals Of Network Forensics: Provide an understanding of devices used to set up computer networks, where useful data may reside within the network, and how the data is stored and retrieved to acquire analysis

FOR410 – Mobile Device Forensics: Provide students with an understanding of how mobile devices actually work and store data, and what data can be of forensic value, as well as how certain types of damage can determine what data can be acquired from the device.

AWE500-OD– Advanced Web Application Exploitation - Explores how to search for, find, and exploit web application security vulnerabilities.

Incident Response

IR500 – Incident Response: Provide in-depth exposure to network and systems intrusion protection methods, what to do before, during and after an event, and how to recover from events and strengthen organizational security.

Malware

MAL400 – Fundamentals Of Malware Analysis: To obtain the basic skills needed for the identification and analysis of software that causes harm to users, computers and networks.

MAL500 – Reverse Engineering Malware: Provide students with a working knowledge of analyzing malicious Windows programs, debugging user-mode & kernel-mode malware, identifying common malware functionality, & other related topics.

MAL600 – Advanced Malware Analysis: Provide an in-depth understanding of identifying & analyzing the presence of advanced packers, polymorphic malware, encrypted malware & malicious code.

Networking

NET400 – TCP/IP Fundamentals: Provide an understanding of TCP/IP fundamentals including where/how to capture and analyze network traffic for summary reporting based on findings and observations.

Pentesting

PEN500 – Pentesting & Network Exploitation: Provide in-depth exposure and hands-on practice with all facets of 802.3 hacking, vulnerability research, pivoting, exploitation, password/hash cracking, post-exploitation pillaging and methods of setting up persistence on a victim's network.

PEN540 – Wireless Pentesting & Network Exploitation: Provide in-depth exposure to all facets of 802.11 penetration testing, encryption cracking, post-exploitation pillaging and report writing.

WEB101-OD – Web Application Exploitation - Instructs students on the most common web vulnerabilities (OWASP Top 10) in modern web applications, why they often exist, and several methods to test for their existence.

WEB241-OD – Hardening PHP Web Applications - Walks students through the list of the OWASP Top Ten vulnerabilities common in web application code and demonstrates various methods of secure coding to harden web applications.

About CYBRScore®

Comtech Mission Critical Technologies (Comtech MCT) provides cybersecurity solutions and services tailored to training and workforce development. The CYBRScore® product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech MCT CYBRScore® offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.