*Austin Peay State University*

# Cybersecurity Bootcamp

## Launch Your Career in Cybersecurity

The Cybersecurity Bootcamp at Austin Peay State University powered by ThriveDX is an accelerated training program designed to successfully prepare people with little or no background in IT for entry-level jobs in cybersecurity – one of the most in-demand technology fields.

Developed around military training methodologies and hands-on learning, the program focuses on the key skills sought by employers. The Bootcamp prepares students not only with technical knowledge, but also with the best practical cybersecurity skills to help them excel in the tech job market.

**Accelerated training program**

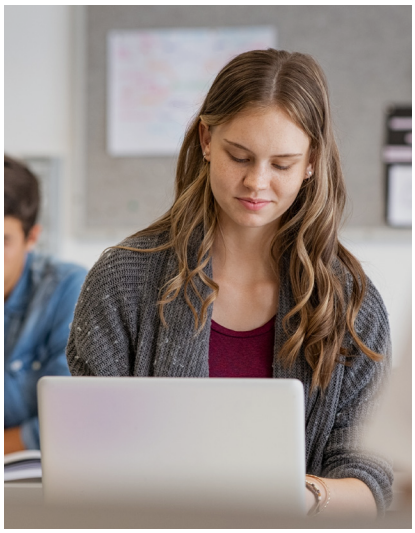
**Industry Leading Certifications**

**+100 hands-on real-world labs**

**www.apsu.edu/continuing-education**

Austin Peay State University
CLARKSVILLE TENNESSEE

impact ThriveDX



**Future-proof job sector**

**Competitive entry-level salary**

**Over 4M unfilled cybersecurity positions**

## Why Cybersecurity?

According to NIST, there are approximately 600,000 job openings in cybersecurity in the US alone, and demand in this field is only expected to increase.* With plentiful opportunities and competitive compensation, an accelerated Cybersecurity Bootcamp is the best way to gain the necessary skills to fill these positions.

## What cybersecurity roles can I pursue after the Bootcamp?

This Bootcamp will prepare you to start your career in cybersecurity with entry-level jobs such as:

- Cyber Defense Analyst
- Cyber Incident Responder
- Cyber Forensics Analyst
- Network Operations Specialist
- Cyber Infrastructure Support Specialist

# Our Bootcamp Includes

### *ACCELERATED PROGRAM*

The Bootcamp was developed under the principle of “everything you need to know, and only what you need to know.” Our accelerated learning methodology and streamlined curriculum focus on teaching you the specific skills to hit the ground running in the cyber industry.

PLUS - Ongoing access to ThriveDX’s online learning platform after graduation, including continuous learning and content updates covering emerging cyber threats and tools.

### *HANDS-ON SKILLS TRAINING*

To ensure you get to practice what you learn, we have developed over 100 unique real-world labs. Technical skills, frameworks, and tools are taught through hands-on exercises in a safe virtual environment.

### *INDUSTRY LEADING CERTIFICATIONS*

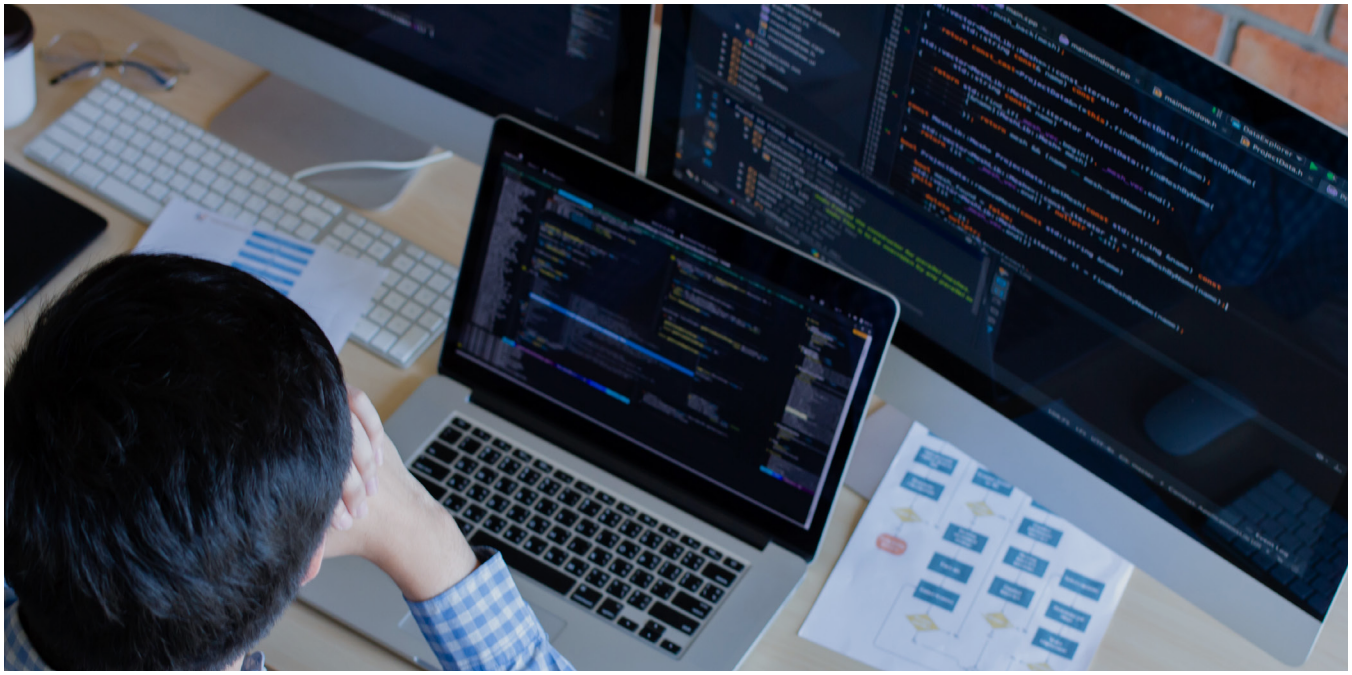
ThriveDX is an official partner of CertNexus and is aligned with NIST-NICE, providing graduates with the opportunity to pursue industry-standard cybersecurity certifications to further their professional development.

### *FLEXIBLE LEARNING*

Our Bootcamp is delivered through our online platform, and our flexible schedule allows students to learn concepts at their own pace. Our program leverages the latest modern learning technologies including microlearning, gamification, on-demand videos and hands-on exercises ensuring an effective learning experience.

### *CAREER SERVICES AND SUPPORT*

Essential soft-skills training, from teamwork to interview prep, is embedded throughout the program. Upon graduation, you will also connect to a global alumni network and community.



# Bootcamp Format

**Self-directed, 6 months:** Our Bootcamp is delivered on a digital platform, allowing students to learn at their own pace, according to their own schedule. We incorporate cutting-edge learning strategies such as microlearning, gamification, on-demand videos, and hands-on exercises to deliver a compelling learning experience. Moreover, our students are continually supported by asynchronous facilitator guidance, further tailoring the educational process to individual needs. $11,995

# Bootcamp Syllabus

### *PREWORK*

- The cybersecurity field, the main challenges in the industry the cybersecurity mindset and "learning how to learn."
- Computer fundamentals, operating systems (Windows,Linux, macOS), and command line utilities.
- Computer networks, OSI model, and network protocols
- MITRE ATT&CK Framework tactics and techniques

### *I. BOOTCAMP INTRODUCTION*

- Introduction to the Bootcamp and Cybersecurity Landscape
- Cybersecurity Career Paths
- Prework Content Review

### *II. NETWORK ADMINISTRATION*

- Network Configuration – LAN, WAN
- Segmentations, VLANs and Subnetting
- Network Mapping Tools
- Troubleshooting and Monitoring Networks
- Network Devices – Switches, Routers
- Telecommunication
- System Administration

### *III. CYBERSECURITY FUNDAMENTALS*

- Most common vurnerabilities, Risks, And Threats
- The Main Concepts In Cybersecurity
- Types Of Malaware And Attackers
- NIST & International Cybersecurity Framework
- Most common Cyber-Attacks
- Famous Cyber-Attacks

### *IV. NETWORK APPLICATION SECURITY*

- Cryptography – Symmetric vs Asymmetric Keys
- Encryption/Decryption, Hash functions
- Security Architecture
- Security Tools – Firewalls, Antivirus, IDS/IPS, SIEM
- Access Control Methods, Multi-factor Authentication, Authentication Protocols
- Honeypots and Cyber Traps

### *V. INCIDENT HANDLING*

- Types Of Attacks in The Web Area (DDOS, SQLInjection, XSS, LFI, Command Injection)
- Types Of Attacks in The Domain Area (Typo Squatting,Domain Hijacking, Pass The Hash, Pass The Ticket,LDAP Reconnaissance, Brute Force)
- Types Of Attacks in The Malware Area (Ransomware,Virus, Worm, Trojan Horse, Adware)
- Practicing The Role of SOC Analysts by Detecting And
- Analyzing Alerts And Incidents In Splunk, SIEM, And EDR
- Analyzing Malicious Indicators Using VirusTotal
- Group and Individual Incident Report Writing

## VI. FORENSICS

- Computer Memory Forensics, Memory Dump Analysis
- FTK Imager, Autopsy, Redline and RAM capturing
- Digital Evidence Acquisition Methodologies
- Registry Forensics
- Windows Timeline Analysis and Data Recovery
- Network Forensics, Anti-Forensics and Steganography

## VII. MALWARE ANALYSIS

- Dynamic Malware Analysis, Reverse Engineering and Malware Obfuscation
- Fileless Malware Analysis
- Containment, Eradication and Recovery Malware Stages
- Analysis using Sysinternals

## VIII. ETHICAL HACKING AND INCIDENT RESPONSE

- Hacking, Ethical Hacking and the Penetration Testing Frameworks
- Ethical Hacking Phases: Reconnaissance, Scanning, Obtaining Access, Maintaining Access,Covering tracks, and The Cyber Kill Chain.
- Network Hacking - Metasploit Framework
- Web Application Hacking - OWASP Top 10 – XSS, SQL Injection, Manual and Automated Attacks
- Post-Incident Activities
- Capture the Flag Challenge

## IX. SECURE DESIGN PRINCIPLES

- Trend Analysis
- Artificial Intelligence in Cybersecurity
- Zero-Trust Policy
- Best Detection Methodologies
- Incident Impact Mitigation

## X. RISK MANAGEMENT

- Risk Management Processes
- Analyzing, Prioritizing, Evaluating and Monitoring Severity of Internal and External Risks
- Risk Management Policies, Procedures, Standards, and Guidelines
- Security Models

## XI. THREAT INTELLIGENCE

- Threat Intelligence Cycle Methodology and Industry Implementation
- Google Hacking – Operators, Finding Sensitive Data, Directory Listing, Devices and Hardware
- Dark Web and Dark Market Investigation
- Online Anonymity using Metadata, Google Cache, VPN and Tor
- Trend Analysis, Basic Excel Data Analysis
- Industrial Tool Practice in Real Environments

## XII. FINAL SCENARIOS AND INTERVIEW PREP

- Final Hands-on Scenarios and Final Exam
- Course Summary and Bootcamper Presentations
- Technical and Soft-Skill Preparation for Job Interviews

As advocates of lifelong learning, **ThriveDX** is committed to closing the digital divide by providing people with the cyber education and digital skills they need.

**By partnering with community colleges and universities, we contribute further to cybersecurity workforce development,** helping to bridge the lingering skills gap and talent shortage and empowering individuals to thrive in the age of digital disruption.

**For additional information, please email us at pro-work-center@apsu.edu or call 931-221-6487.**

**www.apsu.edu/continuing-education**

Austin Peay State University
CLARKSVILLE TENNESSEE

impact ThriveDX