# STEP
Student Training Engagement Program

# Creating the Cyber Workforce

## TRAINING PROGRAM FEATURES

- Training aligned with NICE Cybersecurity Workforce Framework KSA's
- Targets high-demand skills
- Designed by professionals for professionals
- Structured, self-paced learning activities
- Delivered asynchronously online enabling self-paced training
- Designed to improve skills acquisition, retention, and performance
- Embeds learning sciences, analytics, scenario-based learning and gamification principles
- Learners utilize advanced cyber environments scalable to today's critical industry needs
- Collaborative environment encourages knowledge sharing and networking
- Compliant with DoD 8140 directive
- Learner progress tracking with personalized coaching provided upon learner request

## CYBERSECURITY CERTIFICATION

- Accredited Professional Certification
- Maps to national standards:
  - NICE Cybersecurity Workforce KSA's (Knowledge, Skills, and Abilities)
  - CIS Security Controls
- Aligns with syllabus for professional certification exams:*
  - CompTIA Security+
  - SANS GCIH
  - SANS GPEN
  - CISSP

For more information visit...

**www.civiliancyber.com/programs**

## COURSES

### CBIT 100
### Ethics and Laws in Cybersecurity

- Compliance, policies, plans, and procedures
- Types of cybercrimes
- Ethics in cybersecurity
- Laws to fight cybercrime
- Other forms of computer crime

Prerequisites: None

### CBIT 101
### Foundations of Cybersecurity

- Legal and ethical obligations of a cyber warrior/employee
- Explore threats, attacks and vulnerabilities
- Planning an IT architecture in a digital economy
- Risk mitigation and access management concepts/techniques
- Basic concepts of PKI Management and cryptography

Prerequisites: None

### CBIT 240
### Data and Access Controls

- Introduction to SQL
- Database management systems
- Database security controls
- Database threats and access control method
- Database management best practices

Prerequisite: CBIT 101

*Although training will help prepare for professional certification exams, additional preparation will be necessary due to the complexity and proprietary nature of the respective exam content.

### CBIT 250
### Network Security Fundamentals

- Networking fundamentals
- Network architectures
- Network standards
- Common protocols
- Network security fundamentals
- Administrative tools

Prerequisite: CBIT 101

### CBIT 475
### Penetration Testing and Incident Handling

- Penetration testing methodologies
- Penetration testing steps (ethical hacking)
- Intrusion handling

Prerequisites: CBIT 240, 250

### CBIT 476
### Cyber Defense

- CIS controls
- People, policies, and technology security controls

Prerequisites: CBIT 240, 250

**Content aligned with NICE Cybersecurity Workforce Framework KSA's (Knowledge, Skills, and Abilities) to fully apply learning to necessary skills in today's high-tech job market. Content addresses majority of subject matters within CompTIA Security+, and GSEC Security Essentials.**

**Delivered by... The Radford IMPACT Lab**

**Radford University is a designated National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) by both the National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS).**