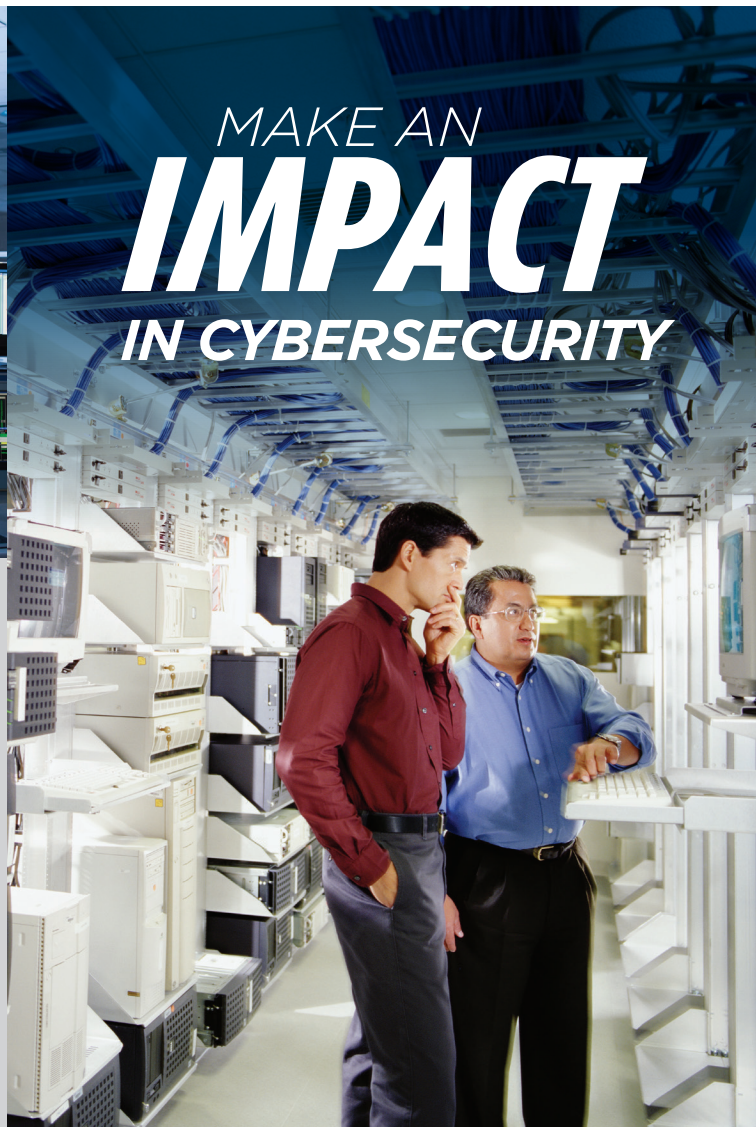# IMPACT

Radford University is delivering IMPACT: a competency-based education (CBE) workforce development program focused on cybersecurity. This program is the first and only one of its kind among public universities in Virginia.

Radford University is designated as a 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).
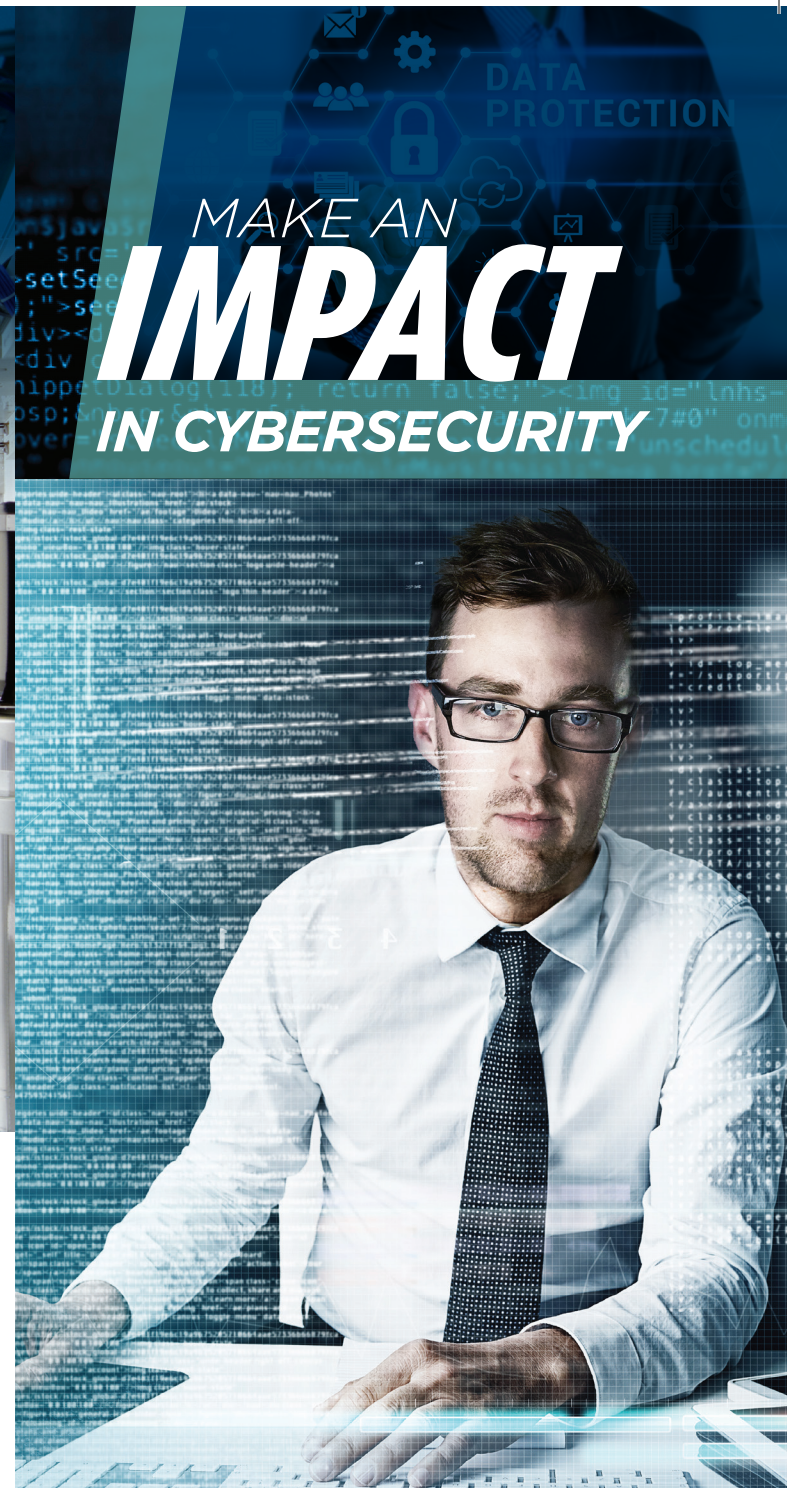
MAKE AN
IMPACT
IN CYBERSECURITY

RADFORD
UNIVERSITY

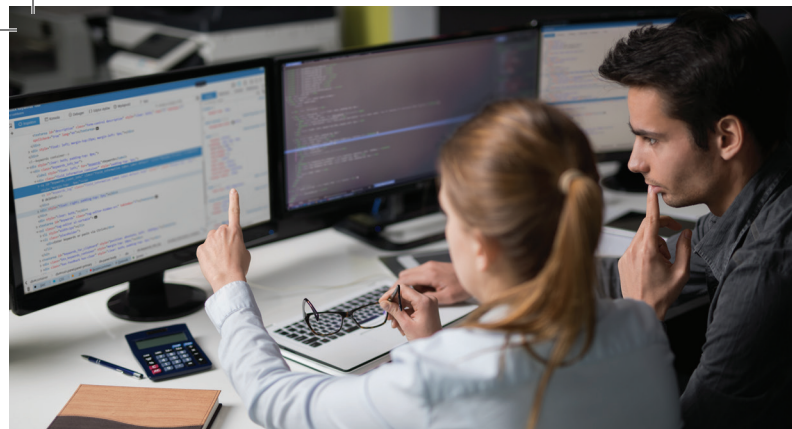**Innovative Mobile
Personalized Accelerated
Competency Training**

Contact: IMPACT Program Office
540-831-7168
www.radford.edu/impact

MAKE AN
IMPACT
IN CYBERSECURITY

RADFORD UNIVERSITY

**Innovative Mobile Personalized
Accelerated Competency Training**

PROGRAM FEATURES

- Builds a foundation for a career in cybersecurity
- Curriculum designed for professionals by professionals
- Improves employee effectiveness and retention
- Designed for busy professionals
- Structured, self-paced learning activities
- Delivered asynchronously online
- Designed to improve skills acquisition and retention
- Embeds learning sciences, analytics, scenario-based learning and gamification principles
- Virtual testing lab for each learner
- Collaborative environment encourages networking with experts and other learners
- Covers five of the seven domains of the NIST Cybersecurity Workforce Framework
- Compliant with DoD 8140 directive

IMPACT CYBERSECURITY CERTIFICATION

- Directly aligned with national standards:
  - National Institute for Science and Technology (NIST)
  - NIST's National Initiative for Cybersecurity Education (NICE)
- Focused on preparing learners for professional certification exams:*
  - CISSP
  - SANS GCIH
  - SANS GPEN
  - CompTIA Security+
  - CompTIA Network+
  - CISCO CCENT

COURSES - 18 TOTAL CREDITS

CBIT 101 (3 credits)
Foundations of Cybersecurity

- Goals of security
- Fundamentals of cryptography and networking
- Basic digital forensics
- Linux command line and scripting (with Python and Perl)

Prerequisites: None

🛡 **Content aligned with CompTIA Security+**

CBIT 240 (3 credits)
Data and Web Security

- Database management systems
- Database and web security
- Data security and privacy
- OWASP web security standards

Prerequisite: CBIT 101

🛡 **Content aligned with CISSP Domain 2 (Asset Security) and parts of Security Engineering**

CBIT 250 (3 credits)
Network Security Fundamentals

- Fundamentals of computer networking
- Network architectures
- Network standards
- Common protocols
- Basics of network security
- Network security and administration tools

Prerequisite: CBIT 101

🛡 **Content aligned with CISCO CCENT, CompTIA Network+, CISSP Domain 4 (Communications and Network Security)**

CBIT 475 (4 credits)
Penetration Testing and Incident Handling

- Planning and reporting
- Common exploits
- OSSTMM methodology
- Penetration testing tools
- Incident handling
- Hardening of operating systems and networks
- Introduction to hacking

Prerequisite: CBIT 240, 250

🛡 **Content aligned with SANS GCIH (Certified Incident Handler), SANS GPEN (Pen Tester)**

CBIT 476 (4 credits)
Cyber Defense

- Principles of secure design
- Network defenses
- Secure protocols
- Host and perimeter security mechanisms
- Compliance, policies, plans, procedures
- Trust and assurance

Prerequisite: CBIT 240, 250

🛡 **Content aligned with CISSP**

CBIT 100 (1 credit) (Capstone)
Ethics and Laws in Cybersecurity

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

Prerequisite: None

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