CYBERSECURITY, CERTIFICATE OF ACHIEVEMENT

The Cybersecurity Certificate of Achievement prepares students for a variety of careers in the broad and lucrative field of cybersecurity. Every industry is counting on cybersecurity and information assurance professionals to detect system vulnerabilities and protect sensitive data.

Course ID	Title	Units/ Hours
Required Core Courses		
CNIT R120	Cisco CCNA Computer Networking I	4
or CNIT R144	CompTIA Network+ Fundamentals and Certification Preparation	
CNIT R145	CompTIA Security+ IT Security and Certification Preparation	3
CNIT R146	Cybersecurity: CompTIA PenTest+	3
Complete two elective courses:		
CNIT R127	Wireless Networking Fundamentals	3
CNIT R131	Administer Microsoft Windows Server	3
CNIT R143	CompTIA Linux+ Fundamentals and Certification Preparation	3
CNIT R151	Cloud Computing and Virtualization	4
Total Required Units for Certificate		**16-17**

Year 1		
Fall Semester		**Units/Hours**
CNIT R120 or CNIT R144	Cisco CCNA Computer Networking I or CompTIA Network+ Fundamentals and Certification Preparation	4
	Units/Hours	**4**
Spring Semester		
CNIT R144 or CNIT R120	CompTIA Network+ Fundamentals and Certification Preparation or Cisco CCNA Computer Networking I	4
CNIT R145	CompTIA Security+ IT Security and Certification Preparation	3
CNIT R143	CompTIA Linux+ Fundamentals and Certification Preparation	3
	Units/Hours	**10**
Summer Semester		
CNIT R127	Wireless Networking Fundamentals	3
	Units/Hours	**3**
Year 2		
Fall Semester		
CNIT R146	Cybersecurity: CompTIA PenTest+	3
CNIT R151	Cloud Computing and Virtualization	4
	Units/Hours	**7**
Spring Semester		
CNIT R131	Administer Microsoft Windows Server	3
	Units/Hours	**3**
	Total Units/Hours	**27**

Upon successful completion of this program, students will be able to:

- Secure network operating systems including the desktop, the server, and intermediary devices such as a network switch and router.
- Construct and apply group policies to secure end devices and the network.
- Perform a vulnerability assessment and penetration test.
- Create a report up to industry standards after completing a vulnerability assessment and penetration test.
- Analyze and interpret the results of vulnerability scan and penetration test.
- Mitigate identified vulnerabilities on devices and the network.
- Follow a structured methodology as it relates cybersecurity incident handling.
- Configure firewalls to increase security from internal and external threats.
- Implement and configure an intrusion detection system (IDS) and intrusion protection system (IPS).
- Implement a secure wireless network using enterprise level wireless security.
- Analyze organizational needs and implement a security policy.