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 specialists to follow best practices to protect computer networks, devices, and data. The training also prepares students to take the appropriate steps to deal with cybersecurity incidents that inevitably occur.

Cybersecurity is one of the fastest-growing fields in the labor market according to the U.S. Bureau of Labor Statistics and there is a huge shortage of qualified cybersecurity specialists for all the job openings that need to be filled. The goal of the Cybersecurity COA is to train students to be qualified to take advantage of these employment opportunities in as little as one academic year. A student who completes the Cybersecurity COA will be prepared for the CompTIA Network+, CompTIA Security+, EC-Council Certified Ethical Hacker, and Red Hat Linux System Administration I certification exams. Depending on the electives that are chosen, students will also be prepared for 2 additional industry certification exams.

A student that is pursuing the Cybersecurity COA should take the required foundation-level networking course in their first semester (CNIT R120 or CNIT R144) so that the student is prepared to excel in the standalone cybersecurity courses.

Course ID	Title	Units/ Hours
Required Core Courses		
CNIT R120 or CNIT R144	Cisco CCNA Computer Networking I CompTIA Network+ Fundamentals and Certification Preparation	4
CNIT R143	Linux Fundamentals	3
CNIT R145	CompTIA Security+ IT Security and Certification Preparation	3
CNIT R146	Cybersecurity: Fundamentals of Ethical Hacking	3
Complete two elective courses:		
CNIT R127	Wireless Networking Fundamentals	3
CNIT R131	Administer Microsoft Windows Server	3
CNIT R151	Cloud Computing and Virtualization	4
CNIT R161	Programming Essentials in Python	3
Total Required Units for Certificate		**19-20**

Year 1		
Fall Semester		**Units/Hours**
CNIT R120 or CNIT R144	Cisco CCNA Computer Networking I or CompTIA Network+ Fundamentals and Certification Preparation	4
CNIT R143	Linux Fundamentals	3
	Units/Hours	**7**
Spring Semester		
CNIT R145	CompTIA Security+ IT Security and Certification Preparation	3
CNIT R151	Cloud Computing and Virtualization	4
CNIT R146	Cybersecurity: Fundamentals of Ethical Hacking	3
	Units/Hours	**10**
Summer Semester		
CNIT R127	Wireless Networking Fundamentals	3
	Units/Hours	**3**
	Total Units/Hours	**20**

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.
- Describe the elements of an effective security policy for a company.