

# CYBERSECURITY ADMINISTRATOR CERTIFICATE

The Cybersecurity Administrator Certificate is designed to equip students with the essential skills to manage and protect information systems and infrastructures. This program covers various aspects of information security policy, processes and technical skills required to prevent, detect and respond to cyber attacks. Students will gain hands-on experience and develop a thorough understanding of network security, ethical hacking, digital forensics and security management.

25 Semester Credit Hours; Curriculum: 0152

Code	Title	Hours
<b>Courses for a Certificate</b>		
CNS 105	Networking Essentials	3
CNS 121	IT Certification Preparation	1
CNS 172	Network Defense and Countermeasures	3
CNS 173	Cybersecurity Operations Analysis	3
CNS 174	Introduction to Computer Forensics	3
CNS 176	Network Security	3
CNS 178	Ethical Hacking	3
CNS/CIS 218	Linux Essentials	3
CSC 157	Python Computer Science I	3
<b>Total Hours</b>		<b>25</b>

Due to rapid changes in information technology, we are frequently updating our certificate and degree programs to better prepare you for the job market. Please consult the CNS department chair for help with your pathway.

**Note:** Students can obtain Credit for Prior Learning through evaluation by Oakton faculty for any of the third-party IT certifications.

## Program Learning Outcomes

1. Develop a network security policy to protect a network.
2. Identify the basic techniques and methodologies for security threats.
3. Explain why basic security measures are necessary on network devices.
4. Explain the importance of physical security controls.
5. Summarize security best practices in a Linux environment.