CIS 283CA : CYBERSECURITY ANALYST

Transcript title
Cybersecurity Analyst

Credits
4

Grading mode
Standard letter grades

Total contact hours
50

Lecture hours
30

Other hours
20

Prerequisites
CIS 279SE.

Recommended preparation
CIS 183C.

Course Description
Focuses on how to prevent, detect, and combat cybersecurity threats through continuous security monitoring. Emphasizes skills in security operations, vulnerability management, incident response and management, and reporting and communications, as well as the latest in security analyst techniques, such as automated incident response, threat intelligence, cloud-based tools, and communication processes. Covers the skills to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventive measures, and effectively respond to and recover from security incidents.

Course learning outcomes
1. Detect and analyze indicators of malicious activity.
2. Describe threat hunting and threat intelligence concepts.
3. Use appropriate tools and methods to manage, prioritize, and respond to attacks and vulnerabilities.
4. Perform incident response processes.
5. Explain reporting and communication concepts related to vulnerability management and incident response activities.

Content outline
DOMAIN / PERCENTAGE OF EXAMINATION
1.Threat and Vulnerability Management / 22%
2.Software and Systems Security / 18%
3.Security Operations and Monitoring / 25%
4.Incident Response / 22%
5.Compliance and Assessment / 13%
Total 100%

Required materials
Reliable Internet access for web-based e-books and learning resources is required. As well as a modern computer, Windows OS is preferred, able to run multiple virtual machines.