Course Number and Title: ITN 271 Advanced Security Operations

Campus Location:
Georgetown, Dover, Stanton, Wilmington

Effective Date:
2020-51

Prerequisite:
ITN 150, ITN 170

Co-Requisites:
None

Course Credits and Hours:
3.00 credits
2.00 lecture hours/week
2.00 lab hours/week

Course Description:
This course prepares students to maintain and analyze system and network security of on-premise and cloud-based systems. Topics include identity and access management, automation tools for provisioning, deployment, and management of resources, and challenges in securing networked architectures.

Required Text(s):
Obtain current textbook information by viewing the campus bookstore - https://www.dtcc.edu/bookstores online or visit a campus bookstore. Check your course schedule for the course number and section.

Additional Materials:
Access to high-speed Internet.

Schedule Type:
Classroom Course
Video Conferencing
Web Conferencing
Hybrid Course
Online Course

Disclaimer:
None

Core Course Performance Objectives (CCPOs):

1. Design a Security Operations Center (SOC). (CCC 1, 2, 3, 4; PGC 1, 2, 3, 4)
2. Evaluate and implement technologies that enable fault tolerant architectures. (CCC 1, 2, 3; PGC 1, 3)
3. Analyze and respond appropriately to security incidents. (CCC 1, 2, 4; PGC 1, 3)
4. Implement threat hunting procedures to detect malicious activity. (CCC 1, 2, 4; PGC 1, 3)

See Core Curriculum Competencies and Program Graduate Competencies at the end of the syllabus. CCPOs are linked to every competency they develop.

Measurable Performance Objectives (MPOs):
Upon completion of this course, the student will:

1. Design a Security Operations Center (SOC).
    1. Explain SOC fundamentals.
    2. Select the appropriate metrics that can be used for a basis of action.
    3. Develop response capability plans aligned with business requirements.
    4. Select Security Incident and Event Management (SIEM) to meet business requirements.
    5. Configure SIEM to collect appropriate metrics.
    6. Develop a report to communicate meaningful metrics to a business.
    7. Use industry standard procedures for privileged access to networked resources.
2. Evaluate and implement technologies that enable fault tolerant architectures.
    1. Use and manage container resources.
    2. Automate provisioning of container resources to support business operations.
    3. Implement and monitor resources for availability and responsiveness.
    4. Design architectures to support system resilience and availability.
3. Analyze and respond appropriately to security incidents.
    1. Define industry standard incident handling procedures.
    2. Compare and contrast incidents versus events.
    3. Discuss tools used to estimate and track costs associated with incidents.
    4. Determine appropriate communication and actions given a scenario.
    5. Analyze output from Intrusion Detection System/Intrusion Prevention System (IDS/IPS) to recognize an incident.
    6. Describe the purpose of wireless IDS/IPS.
    7. Describe the steps of a kill chain.
4. Implement threat hunting procedures to detect malicious activity.
    1. Explain the concept of passive intrusion monitoring.
    2. Explain the concept of active intrusion deterrents.
    3. Explain the purpose and function of threat hunting.
    4. Configure passive intrusion monitoring tools to detect malicious activity.
    5. Configure active intrusion deterrents to thwart malicious activity.

Evaluation Criteria/Policies:
Students must demonstrate proficiency on all CCPOs at a minimal 75 percent level to successfully complete the course. The grade will be determined using the Delaware Tech grading system:

92	–	100	=	A
83	–	91	=	B
75	–	82	=	C
0	–	74	=	F

Students should refer to the Student Handbook - https://www.dtcc.edu/handbook for information on the Academic Standing Policy, the Academic Integrity Policy, Student Rights and Responsibilities, and other policies relevant to their academic progress.

Core Curriculum Competencies (CCCs are the competencies every graduate will develop):

1. Apply clear and effective communication skills.
2. Use critical thinking to solve problems.
3. Collaborate to achieve a common goal.
4. Demonstrate professional and ethical conduct.
5. Use information literacy for effective vocational and/or academic research.
6. Apply quantitative reasoning and/or scientific inquiry to solve practical problems.

Program Graduate Competencies (PGCs are the competencies every graduate will develop specific to his or her major):

1. Solve technology-related problems using critical thinking and troubleshooting skills.
2. Articulate the role of the technology professional in organizations to support the ethical use of information technology.
3. Apply fundamental security concepts and strategies for maintaining and securing information technology.
4. Read and interpret technical information and effectively communicate to a wide range of audiences using oral, print, and multimedia strategies.
5. Demonstrate the importance of lifelong learning that empowers personal and professional growth.

Disabilities Support Statement:
The College is committed to providing reasonable accommodations for students with disabilities. Students are encouraged to schedule an appointment with the campus Disabilities Support Counselor to request an accommodation needed due to a disability. A listing of campus Disabilities Support Counselors and contact information can be found at the disabilities services - https://www.dtcc.edu/disabilitysupport web page or visit the campus Advising Center.