ILLINOIS VALLEY COMMUNITY COLLEGE

COURSE OUTLINE

DIVISION: Workforce Development

COURSE: CSC 2206 CySA+

Date: Fall 2020

Credit Hours: 3

Prerequisite(s): CSC 2204

Delivery Method:		
	☒ **Lecture**	**2 Contact Hours (1 contact = 1 credit hour)**
	☐ **Seminar**	**0 Contact Hours (1 contact = 1 credit hour)**
	☒ **Lab**	**2 Contact Hours (2-3 contact = 1 credit hour)**
	☐ **Clinical**	**0 Contact Hours (3 contact = 1 credit hour)**
	☐ **Online**	
	☐ **Blended**	

Offered: ☐ **Fall** ☒ **Spring** ☐ **Summer**

IAI Equivalent –***Only for Transfer Courses***-go to *http://www.itransfer.org*:

CATALOG DESCRIPTION:
This course focuses on CompTIA's CySA+ Certification exam. This certification is the next level CompTIA certification to earn after the Security+. CompTIA's Cybersecurity Analyst course will teach you the fundamental principles of using threat and vulnerability analysis tools. CySA+ covers the most up-to-date core security analyst skills and upcoming job skills used by threat intelligence analysts, application security analysts, compliance analysts, incident responders/handlers, and threat hunters. This course is designed to provide you with the foundational knowledge necessary to prepare you to sit for the CySA+ certification exam.

GENERAL EDUCATION GOALS ADDRESSED

[See last page for Course Competency/Assessment Methods Matrix.]

Upon completion of the course, the student will be able:

[Choose up to three goals that will be formally assessed in this course.]

☒ To apply analytical and problem solving skills to personal, social, and professional issues and situations.
☒ To communicate successfully, both orally and in writing, to a variety of audiences.
☐ To construct a critical awareness of and appreciation for diversity.
☐ To understand and use technology effectively and to understand its impact on the individual and society.
☐ To develop interpersonal capacity.
☐ To recognize what it means to act ethically and responsibly as an individual and as a member of society.
☐ To recognize what it means to develop and maintain a healthy lifestyle in terms of mind, body, and spirit.
☐ To connect learning to life.

EXPECTED LEARNING OUTCOMES AND RELATED COMPETENCIES:

[Outcomes related to course specific goals. See last page for more information.]

Upon completion of the course, the student will be able to:

1. Leverage intelligence and threat detection techniques
    1.a. Investigate Threat Data and Intelligence Sources
    1.b. Explain Threat Modeling and Hunting Methodologies

2. Analyze and interpret data
    2.a. Analyze monitoring output
    2.b. Analyze log data

3. Identify and address vulnerabilities
    3.a. Discuss the Risk Management Process
    3.b. Analyze Monitoring output
    3.c. Configure Vulnerability Scanning and Analyze output

4. Suggest preventative measures
    4.a. Discuss Frameworks, Policies and Procedures
    4.b. Understand the Risk Identification, Calculation and Prioritization Process

5. Effectively respond to and recover from incidents
    5.a. Discuss Incident Response Process
    5.b. Apply Eradication, Recovery and Post-incident Processes

MAPPING LEARNING OUTCOMES TO GENERAL EDUCATION GOALS

[For each of the goals selected above, indicate which outcomes align with the goal.]

Goals	Outcomes
First Goal	
To apply analytical and problem solving skills to personal, social, and professional issues and situations.	1. Leverage intelligence and threat detection techniques 1.a. Investigate Threat Data and Intelligence Sources 1.b. Explain Threat Modeling and Hunting Methodologies 2. Analyze and interpret data 2.a. Analyze monitoring output 2.b. Analyze log data 3. Identify and address vulnerabilities 3.b. Analyze Monitoring output 3.c. Configure Vulnerability Scanning and Analyze output 4. Suggest preventative measures 4.b. Understand the Risk Identification, Calculation and Prioritization Process 5. Effectively respond to and recover from incidents 5.b. Apply Eradication, Recovery and Post-incident Processes
Second Goal	
To communicate successfully, both orally and in writing, to a variety of audiences.	3. Identify and address vulnerabilities 3.a. Discuss the Risk Management Process 4. Suggest preventative measures 4.a. Discuss Frameworks, Policies and Procedures 5. Effectively respond to and recover from incidents 5.a. Discuss Incident Response Process

COURSE TOPICS AND CONTENT REQUIREMENTS:

CySA+ Five Domains

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

INSTRUCTIONAL METHODS:

- Lecture
- Lab
- CompTIA Simulation software

INSTRUCTIONAL MATERIALS:
CompTIA CySA+ print or eBook
CompTIA eLab

STUDENT REQUIREMENTS AND METHODS OF EVALUATION:
A= 90-100
B= 80-89
C= 70-79
D= 60-69
F= 0-59

OTHER REFERENCES
NIST Publications

Course Competency/Assessment Methods Matrix

(Dept/# Course Name)	Assessment Options																																
For each competency/outcome place an "X" below the method of assessment to be used.	**Assessment of Student Learning**	Article Review	Case Studies	Group Projects	Lab Work	Oral Presentations	Pre-Post Tests	Quizzes	Written Exams	Artifact Self Reflection of Growth	Capstone Projects	Comprehensive Written Exit Exam	Course Embedded Questions	Multi-Media Projects	Observation	Writing Samples	Portfolio Evaluation	Real World Projects	Reflective Journals	Applied Application (skills) Test	Oral Exit Interviews	Accreditation Reviews/Reports	Advisory Council Feedback	Employer Surveys	Graduate Surveys	Internship/Practicum /Site Supervisor Evaluation	Licensing Exam	In Class Feedback	Simulation	Interview	Written Report	Assignment
Assessment Measures – Are direct or indirect as indicated. List competencies/outcomes below.	**Direct/ Indirect**	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	I	I	I	I	D	D							
Leverage intelligence and threat detection techniques					X			X	X				X															X				X
Analyze and interpret data					X			X	X				X					X											X				X
Identify and address vulnerabilities			X		X			X	X				X																X				X
Suggest preventative measures					X			X	X				X					X											X				X
Effectively respond to and recover from incidents			X		X	X		X	X				X					X											X				X