ISSC298

Course Summary

Course : ISSC298 **Title :** Cybersecurity Capstone Portfolio
Length of Course : 8 **Faculty :**
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description:

This Capstone course provides a comprehensive overview of major components of Information Systems Security. The course explores various security-related plans and policies that demonstrate mastery of the program of study and results in a meaningful culmination of the student's learning; these plans and policies will be used to assess one's level of mastery of the stated outcomes of the degree requirements. This is a capstone course to be taken after all other Information Systems Security courses have been satisfactorily completed. (Prerequisite: Completion of a minimum of 57 hours towards the degree program)

Course Scope:

This Capstone course is a Associates Level course designed to allow the student to review, analyze, and integrate the work the student has completed toward the Associates of Science in Cybersecurity degree. Students will examine a number of real-world scenario cases related to various aspects of Cybersecurity to complete various cybersecurity related plans and policies that demonstrate mastery of their program of study in a meaningful culmination of their learning and to assess their level of mastery of the stated outcomes of their degree requirements. (Prerequisite: Completion of a minimum of 60 hours towards your program including ENGL101 or ENGL110)

Course Scope: This course presents students with an opportunity to investigate the various aspects of Cybersecurity including the relationship between cyber defense, cyber operations, cyber exploitations, cyber intelligence, cybercrime, Cyberlaw within Federal and State Laws. Students will be able to demonstrate an in-depth understanding of Cybersecurity as a discipline with many associations and complexities and to develop an understanding of how legal, ethical and criminal justice theories are applied. This course blends together the vast issues and challenges associated with the discipline of Cybersecurity while emphasizing the need to conduct research associated with securing the United States cyberspace and safeguarding it from a myriad of threats both national and international. The overall goal is that each student will apply the knowledge and skills that have been obtained over the course of their undergraduate Cybersecurity studies to real-world challenges. The capstone course is designed to polish students' writing, analytical, and research skills from the variety of discipline areas studied so that he or she may confidently confront the challenges and demands of specialized research and written communication. This course provides students with the opportunity to complete an approved academic research exercise or other creative scholarly activity resulting in a tangible product that demonstrates synthesis of a student's coursework and substantial knowledge of the Cybersecurity field of study. The course also addresses the notion of capstone by considering overall academic accomplishments in light of specific personal and career goals. This course is to be taken as the LAST course in the Cybersecurity program.

Objectives

The successful student will fulfill the following learning objectives:

CO-1: Examine the various aspects of cybersecurity including the relationship between cyber defense, cyber operations, cyber exploitations, cyber intelligence, cybercrime, Cyberlaw within Federal and State Laws

CO-2: Deconstruct the processes and goals of cyber forensics investigations including the importance of search warrants and chain of custody in a forensic investigation of computer related crimes

CO-3: Prepare a plan to manage functions that encompass overseeing a program or technical aspect of a security program at a high level ensuring currency with changing risk and threat environments.

CO-4: Prepare a plan to design functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.

CO-5: Develop strategies and plans for security architecture consisting of tools, techniques, and technologies to detect and prevent network penetration, and to design effective cybersecurity countermeasures.

CO-6: Develop a policy to analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management for wired, wireless, and satellite networks that affect the security of the cyberspace.

CO-7: Develop a policy to implement functions that encompass putting programs, processes, or policies into action within an organization.

CO-8: Prepare a plan to evaluate functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives.

Outline

Week 1:

Learning Outcomes

CO-1: Examine the various aspects of cybersecurity including the relationship between cyber defense, cyber operations, cyber exploitations, cyber intelligence, cybercrime, Cyberlaw within Federal and State Laws.

Required Readings
Assignments

- Reading: Chapters 1
- Assignment #1
- Week 1 Introduction
- Discussion Assignment #1

Recommended Optional Reading
Recommended Media

Week 2:

Learning Outcomes

CO-2: Deconstruct the processes and goals of cyber forensics investigations including the importance of search warrants and chain of custody in a forensic investigation of computer related crimes

Required Readings
Assignments

- Reading: Chapter 2
- Reading: Supplemental Resources
- Week 2 Discussion
- Assignment #2
- Capstone Project Topic selection (4 - 6 page idea paper)

Recommended Optional Reading
Recommended Media

Week 3:

Learning Outcomes

CO-3: Prepare a plan to manage functions that encompass overseeing a program or technical aspect of a security program at a high level ensuring currency with changing risk and threat environments.

Required Readings
Assignments

- Reading: Chapter 3
- Reading: Supplemental Resources
- Week 3 Discussion
- Assignment #3

Recommended Optional Reading
Recommended Media

Week 4:

Learning Outcomes

CO-4: Prepare a plan to design functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.

Required Readings
Assignments

- Reading: Chapter 4
- Reading: Supplemental Resources
- Week 4 Discussion
- Assignment #4

Recommended Optional Reading
Recommended Media

Week 5:

Learning Outcomes

CO-5: Develop strategies and plans for security architecture consisting of tools, techniques, and

technologies to detect and prevent network penetration, and to design effective cybersecurity countermeasures.

Required Readings
Assignments

- Reading: Supplemental Resources
- Week 5 Discussion
- Assignment #5

Recommended Optional Reading
Recommended Media

Week 6:

Learning Outcomes

CO-6: Develop a policy to analyze network designs, topologies, architectures, protocols, communications, administration, operations, and resource management for wired, wireless, and satellite networks that affect the security of the cyberspace.

Required Readings
Assignments

- Reading: Chapters 5
- Reading: Supplemental Resources
- Week 6 Discussion
- Assignment #6

Recommended Optional Reading
Recommended Media

Week 7:

Learning Outcomes

CO-7: Develop a policy to implement functions that encompass putting programs, processes, or policies into action within an organization.

Required Readings
Assignments

- Reading: Chapters 6
- Reading: Supplemental Resources
- Week 7 Discussion
- Assignment #7

Recommended Optional Reading
Recommended Media

Week 8:

Learning Outcomes

CO-8: Prepare a plan to evaluate functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives.

Required Readings
Assignments

- Reading: Supplemental Resources
- Week 8 Discussion
- Assignment #8 Project paper
-

Recommended Optional Reading
Recommended Media

Evaluation

Grading:

Name	Grade %
Discussions	**16**
Weekly Progress Assignments	**40**
Final Project	**44**

Materials

Required Text:

Book Title: NIST Cybersecurity Framework – A pocket guide
Author: Calder, Alan
Publication Info: IT Governance Publishing (ITGP)
ISBN: 9781787780408

Additional Supplemental Resources for Cybersecurity at the End of This Syllabus. The books below are additional resources if you want to learn more.

- **Book Title:** The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and
  Practice - e-book available in the APUS Online Library
  Author: Winterfeld, Steve
  Publication Info: Syngress
  ISBN: 9780124047372

- **Book Title:** The 7 Qualities of Highly Secure Software - e-book available in the APUS Online Library
  Author: Paul, Mano
  Publication Info:
  ISBN: 9781439814468

- **Book Title:** Cybersecurity: Public Sector Threats and Responses - e-book available in the APUS Online
  Library
  Author: Andreasson, Kim
  Publication Info:
  ISBN: 9781439846636

Book Title: Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives - e-book
available in the APUS Online Library
Author: Raghu, Santanam
Publication Info: IGI Global
ISBN: 9781609601232

Software Requirements

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint)
2. IE, Firefox, Google Chrome

Course Guidelines

Citation and Reference Style

- Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrativeessay or composition format must follow the citation style cited in the APA Format.

Tutoring

- Tutor.com offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

- Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under each Assignment.
- Generally speaking, late work may result in a deduction up to 15% of the grade for each day late, not to exceed 5 days.
- As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

- Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

- Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is

academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

- Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Disclaimer Statement

Course content may vary from the outline to meet the needs of this particular group.

Communicating on the Discussion

- Discussions are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the discussion. The purpose of the discussions is to actively participate in an on-going discussion about the assigned content.
- “Substantive” means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says “I agree” is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.
- As a class, if we run into conflicting refer points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Identity Verification & Live Proctoring

- Faculty may require students to provide proof of identity when submitting assignments or completing assessments in this course. Verification may be in the form of a photograph and/or video of the student’s face together with a valid photo ID, depending on the assignment format.
- Faculty may require live proctoring when completing assessments in this course. Proctoring may include identity verification and continuous monitoring of the student by webcam and microphone during testing.

Communications

Student Communication

To reach the instructor, please communicate through the MyClassroom email function accessible from the Classlist of the Course Tools menu, where the instructor and students email addresses are listed, or via the Office 365 tool on the Course homepage.

- In emails to instructors, it’s important to note the specific course in which you are enrolled. The name of the course is at the top center of all pages.
- Students and instructors communicate in Discussion posts and other learning activities.
- All interactions should follow APUS guidelines, as noted in the Student Handbook, and maintain a professional, courteous tone.

- Students should review writing for spelling and grammar.
- Tips on Using the Office 365 Email Tool

Instructor Communication

The instructor will post announcements on communications preferences involving email and Instant Messaging and any changes in the class schedule or activities.

- Instructors will periodically post information on the expectations of students and will provide feedback on assignments, Discussion posts, quizzes, and exams.
- Instructors will generally acknowledge student communications within 24 hours and respond within 48 hours, except in unusual circumstances (e.g., illness).
- The APUS standard for grading of all assessments (assignments, Discussions, quizzes, exams) is five days or fewer from the due date.
- Final course grades are submitted by faculty no later than seven days after the end date of the course or the end of the extension period.

University Policies

Consult the Student Handbook for processes and policies at APUS. Notable policies:

- Drop/Withdrawal Policy
- Extension Requests
- Academic Probation
- Appeals
- Academic Dishonesty / Plagiarism
- Disability Accommodations
- Student Deadlines
- Video Conference Policy

Mission

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.

Minimum Technology Requirements

- Please consult the catalog for the minimum hardware and software required for undergraduate and graduate courses.
- Although students are encouraged to use the Pulse mobile app with any course, please note that not all course work can be completed via a mobile device.

Disclaimers

- Please note that course content – and, thus, the syllabus – may change between when a student

registers for a course and when the course starts.

- Course content may vary from the syllabus' schedule to meet the needs of a particular group.