COURSE OUTLINE: CYB306 - CAPSTONE PROJECT

Prepared: IT Studies

Approved: Corey Meunier, Dean, Technology, Trades, and Apprenticeship

Course Code: Title	CYB306: CAPSTONE PROJECT
Program Number: Name	2198: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2023-2024
Course Description:	The primary focus of the Capstone Project course is experiential learning through an applied project. This course integrates the knowledge and skills students have obtained throughout the Program. Students implement a security analysis, research, and plan, design and deploy cyber defenses, focusing on security policy, incident response, business continuity, information systems security and threat management. Students will apply their cyber security knowledge and skills to explore solutions and to identify current industry-related problems and make recommendations that create practical solutions.
Total Credits:	4
Hours/Week:	4
Total Hours:	56
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**2198 - CYBERSECURITY** VLO 1 Develop and implement cyber security solutions to protect network systems and data VLO 2 Plan and implement security assessment methodologies, vulnerability management strategies and incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization VLO 3 Recommend processes and procedures for maintenance and deployment of cyber security VLO 4 Select and deploy optimal security appliances and technologies to safeguard an organization's network VLO 5 Comply with existing industry policies, regulations, and ethics for information systems and information technology security solutions to ensure industry expectations and standards are met or exceeded VLO 6 Analyze security risks to organizations and business processes to mitigate risk in compliance with industry standards VLO 7 Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability VLO 9 Perform various types of cyber analysis to detect actual security incidents and suggest solutions

SAULT COLLEGE | 443 NORTHERN AVENUE | SAULT STE. MARIE, ON P6B 4J3, CANADA | 705-759-2554

	VLO 10 Maintain ongoing personal and professional development to improve work performance in the field of information technology
	VLO 11 Present and summarize cybersecurity solutions to business stakeholders in a professional manner to inform decision making
Essential Employability Skills (EES) addressed in this course:	EES 1 Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience.
	EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication.
	EES 4 Apply a systematic approach to solve problems.
	EES 5 Use a variety of thinking skills to anticipate and solve problems.
	EES 6 Locate, select, organize, and document information using appropriate technology and information systems.
	EES 7 Analyze, evaluate, and apply relevant information from a variety of sources.
	EES 8 Show respect for the diverse opinions, values, belief systems, and contributions of others.
	EES 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals.
	EES 10 Manage the use of time and other resources to complete projects.
	EES 11 Take responsibility for ones own actions, decisions, and consequences.
Course Evaluation:	Passing Grade: 50%, A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Other Course Evaluation & Assessment Requirements:	A+ = 90-100% A = 80-89% B = 70-79% C = 60-69% D = 50-59% F < 50% Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test. If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test. Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information. In order to qualify to write a missed test, the student shall have: a.) attended at least 75% of the classes to-date. b.) provide the professor an acceptable explanation for his/her absence. c.) be granted permission by the professor. NOTE: The missed test that has met the above criteria will be an end-of-semester test. Labs / assignments are due on the due-date indicated by the professor. Notice by the professor

will be written on the labs / assignments and verbally announced in the class. Labs and assignments that are deemed late will have the following penalty: 1 day late - 10% reduction, 2 days late, 20% reduction, 3 days late, 30% reduction. After 3 days, no late assignments and labs will be accepted. It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which is 50 minutes into the class or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
Course Outcome 1: Conduct a comprehensive security analysis.	1.1 Apply knowledge of cybersecurity principles, techniques, and tools to identify vulnerability and risks. 1.2 Apply several methodologies to assess the security posture of the systems, networks, and applications. 1.3 Analyze security assessment findings and develop recommendations for improving the overall security posture.
Course Outcome 2	Learning Objectives for Course Outcome 2
Course Outcome 2: Develop effective security policies and strategies.	2.1 Understand the importance of security policies in defining procedures, guidelines, and best practices for safeguarding critical information. 2.2 Define and propose new security policies that address emerging threats and technologies.
Course Outcome 3	Learning Objectives for Course Outcome 3
Course Outcome 3: Implement Incident Response Plan.	3.1 Develop Incident Response Plans. 3.2 Understand various tools to effectively manage security breaches. 3.3 Practice incident response scenarios.
Course Outcome 4	Learning Objectives for Course Outcome 4
Course Outcome 4: Evaluate and manage threats effectively.	4.1 Understand strategies for continuous monitoring, threat hunting and security detection and response. 4.2 Monitor and analyze threat indicators.

Evaluation Process and

Evaluation Type	Evaluation Weight

Grading System:		
	1.) Project Status: Phase I Checklist - Week 5	25%
	2.) Project Status: Phase II Checklist - Week 9	25%
	3.) Project Documentation	10%
	4.) Project Final Evaluation	40%

Date:	July 5, 2023
Addendum:	Please refer to the course outline addendum on the Learning Management System for further information.