COURSE OUTLINE: CYB301 - SECURITY/DEFENSE/RES

Prepared: IT Studies
Approved: Corey Meunier, Dean, Technology, Trades, and Apprenticeship

Course Code: Title	CYB301: SECURITY, DEFENSE AND RESPONSE
Program Number: Name	2198: CYBERSECURITY 5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2023-2024
Course Description:	This course covers IT security defense and response in the Canadian and Ontario regulatory environments. This course covers the procedures used to implement and configure security within an enterprise environment, as well as respond to security incidents. Focus will be placed on tools that can be used to secure access to data and mitigate security breaches.
Total Credits:	5
Hours/Week:	5
Total Hours:	70
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 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 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 **5911 - CYBERSECURITY** 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 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.
Essential Employability Skills (EES) addressed in this course:	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 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.
Course Evaluation:	Passing Grade: 50%, D 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.

Books and Required Resources:

CompTIA CySA+ Study Guide by Mike Chapple, David Seidl
Publisher: Sybex (Wiley) - Print Edition: 8th
ISBN: 978-1-119-73625-7

CompTIA CySA+ Study Guide by Mike Chapple, David Seidl
Publisher: Sybex (Wiley) - eBook Edition: 8th
ISBN: 978-1-119-73626-4

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Analyze indicators and various threats, attacks, and vulnerabilities and explain the impact associated with each.	THREATS, ATTACKS, AND VULNERABILITIES 1.1 Compare and contrast different types of social engineering techniques. 1.2 Analyze potential indicators to determine the type of attack. 1.3 Analyze potential indicators associated with application attacks. 1.4 Analyze potential indicators associated with network attacks.1.5 Explain different threat actors, vectors, and intelligence sources. 1.6 Explain the security concerns associated with various types of vulnerabilities. 1.7 Summarize the techniques used in security assessments. 1.8 Explain the techniques used in penetration testing.
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Implement secure protocol, security solutions, secure network designs, and install and configure wireless security settings.	IMPLEMENTATION 2.1 Implement secure protocols. 2.2 Implement host or application security solutions. 2.3 Implement secure network designs. 2.4 Install and configure wireless security settings. 2.5 Implement secure mobile solutions. 2.6 Apply cybersecurity solutions to the cloud. 2.7 Implement identity and account management controls. 2.8 Implement authentication and authorization solutions. 2.9 Implement public key infrastructure.
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Evaluate the importance of physical controls and various frameworks for risk mitigation and secure systems design.	ARCHITECTURE AND DESIGN 3.1 Explain the importance of security concepts in an enterprise environment. 3.2 Summarize virtualization & cloud computing concepts. 3.3 Summarize secure application development, deployment, and automation concepts. 3.4 Summarize authentication and authorization design concepts. 3.5 implement cybersecurity resilience. 3.6 Explain the security implications of embedded and specialized systems. 3.7 Explain the importance of physical security controls.

	3.8 Summarize the basics of cryptographic concepts.
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Investigate and utilize proper data sources, proper tools to assess organizational security and explain the importance of policies, processes, and procedures of incident response.	OPERATIONS AND INCIDENT RESPONSE 4.1 Utilize the appropriate tool to assess organizational security. 4.2 Summarize the importance of policies, processes, and procedures for incident response. 4.3 Utilize appropriate data sources to support an investigation. 4.4 Apply mitigation techniques or controls to secure an environment. 4.5 Explain the key aspects of digital forensics. 4.6 Explain the importance of the incident response 4.7 Apply the appropriate incident response procedure. 4.8 Analyze potential indicators of compromise. 4.9 Utilize basic digital forensics techniques.
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Explain the importance of regulations, standards, security policies.	GOVERNANCE, RISK AND COMPLIANCE 5.1 Compare and contrast various types of controls. 5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture. 5.3 Explain the importance of policies to organizational security. 5.4 Summarize risk management processes and concepts. 5.5 Explain privacy and sensitive data concepts in relation to security.
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Understand and explain the importance of data privacy, protection, framework policies and procedures	COMPLIANCE AND ASSESSMENT 6.1 Understand the importance of data privacy and protection. 6.2 Apply security concepts in support of organizational risk mitigation. 6.3 Explain the importance of frameworks, policies, procedures, and controls.
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Recommend appropriate responses to threats after implementing various reconnaissance technique and analyzing the output from vulnerability assessment tools.	THREAT AND VULNERABILITY MANAGEMENT 7.1 Explain the importance of threat data and intelligence. 7.2 Utilize threat intelligence to support organizational security. 7.3 Perform vulnerability management activities. 7.4 Analyze the output from Common vulnerability assessment tools. 7.5 Explain the threats and vulnerabilities associated with specialized technology. 7.6 Explain the threats and vulnerabilities associated with operating in the cloud. 7.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.
Course Outcome 8	**Learning Objectives for Course Outcome 8**
Apply security solution and software/hardware	SOFTWARE AND SYSTEMS SECURITY 8.1 Apply security solutions for infrastructure management.

assurance best practices.	8.2 Explain software assurance best practices. 8.3 Explain hardware assurance best practices.

Course Outcome 9	**Learning Objectives for Course Outcome 9**
Analyze data and implement configuration changes for the improvement of security.	SECURITY OPERATIONS AND MONITORING 9.1 Analyze data as part of security monitoring activities. 9.2 Implement configuration changes to existing controls to improve security. 9.3 Explain the importance of proactive threat hunting. 9.4 Compare and contrast automation concepts and technologies.

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Labs, Assignments and Quizzes	40%
Test #1	30%
Test #2	30%

Date: July 27, 2023

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.