Cybersecurity: Prevention and Intervention – LEA.D8
AEC Program

COURSE OUTLINE

Course Title:	Incident Management	**Course Number:**	420-4C1-DW
Course Hours:	75	**Ponderation:**	2 – 3 – 1
Credits:	2 2/3		
Prerequisite:	None	**Corequisite:**	None
Group:	1	**Term:**	4
Teacher Name:	*Asen Grozdanov*	**Contact Details:**	*agrozdanov@dawsoncollege.qc.ca*

COURSE COMPETENCY STATEMENT:

EZ07 - Perform penetration (hacking) tests.
This course will address competency EZ07 in its entirety.
(*See page 7 for full course competency).*

COURSE DESCRIPTION:

This course provides a comprehensive overview of the incident management lifecycle, equipping students with the skills to detect, validate, contain, and eradicate information security threats. Based on industry-standard frameworks, the curriculum covers the core incident handling process—from preparation and first response to forensic analysis and system recovery. Students will explore specific incident categories, including malware, email security, network attacks, web application vulnerabilities, cloud security, and insider threats. Through a combination of theoretical instruction and practical labs, participants will learn to apply incident response automation, utilize forensic tools for evidence gathering, and implement best practices to secure organizational assets against future attacks.

COURSE ASSESSMENT:

Students will be evaluated though both formative and summative assessments through a variety of means including:

- Lab exercises
- Case study analysis
- Group discussions
- Hands-on projects
- Simulations and incident response drills

Appropriate mastery of the course objectives is essential to Succeed both in the program and in practice. Assessment of student performance will involve the ability to understand and apply key Cybersecurity concepts.
The passing grade for all assessments is 60%.

COURSE LEARNING OUTCOMES:

By the end of the course, students will be able to :

- Develop cybersecurity incident response plans.
- Identify incidents within systems.
- Analyze incidents within systems.
- Effectively contain incidents within systems.
- Eradicate the cause of incidents and ensure a return to normal.
- Write incident reports.

INTEGRATION:

The course *Incident Management* prepares students for future terms in the program. Specifically, the course is a prerequisite for the following courses in the program

Term 4: Implementation and Management of Corporate Cybersecurity Measures – 420-4C2-DW

WEEKLY SCHEDULE OF LEARNING ACTIVITIES *:

Week	Dates	Class 1	Topic	Class 2	Topic
1	April 20, April 22	4.5 hrs	Introduction to Incident Handling & Security Concepts, **Research Topic.**	4.5 hrs	The Incident Handling & Response (IH&R) Process, **Rsearch Topic.**
2	April 25	3.0 hrs	First Response & Evidence Handling	4.0 hrs	**Lab :** Securing Crime Scenes & Collecting Digital Evidence
3	April 27, April 29	4.5 hrs	Handling Malware Incidents	4.5 hrs	**Lab :** Malware Detection, Analysis & Containment
4	May 2	3.0 hrs	Email Security Incidents (Phishing & Spam)	4.0 hrs	**Lab :** Analyzing Email Headers & Tracing Attacks
5	May 4, May 8	4.5 hrs	Web Application Security Incidents, **Research Topic.**	4.5 hrs	**Midterm Review**
6	May 9	0.0 hrs	**No Class**	4.0 hrs	**Midterm Assessment**: *Theoretical exam based on Weeks 1-5 Weeks' Lessons*

7	May 15, May 16	5.0 hrs	Network Security Incidents (DoS, Unauthorized Access)	4.0 hrs	**Lab :** Network Traffic Analysis & Incident Validation
8	May 21, May 22	4.0 hrs	Insider Threats	4.0 hrs	**Lab :** Detecting & Eradicating Insider Activity
9	May 23, May 25	4.0 hrs	Endpoint Security (Mobile, IoT, OT)	3.0 hrs	**Lab :** Endpoint Forensics and Analysis
10	May 28, May 29	3.0 hrs	**Final Exam's Review**	3.0 hrs	**Final Theory /Final Lab Assessment**

**Learning activities are subject to change.*

Evaluation:

Component	Tentative Date	Value of element
Research Topics	April 20, 22, May 4	12%
Labs	April 25, 29, May 2, 16, 22, 25	18%
Midterm Exam	May 9 – 1:30 PM **(in-person)**	30%
Final Exam **Summative Assessment**	May 29 – 6:00 PM **(in-person)**	40%
		100%

IMPORTANT INFORMATION REGARDING EVALUATION:

Summative Assessment:

Students must successfully pass the summative assessment element in the course. Students who are unsuccessful on the Summative Assessment will fail the course.

Late Submission Policy:
Penalties for late submissions will be as follows: 10% for each day late with no submission accepted 7 days after due date.

Missed Tests / Quizzes: *[Adjust as needed for your course]*
Students with a valid reason for missing assessments can be provided with make-up exams. For absences and illnesses of 5 days or less, a medical certificate is not required. Absences of more than 5 days require the submission of a valid medical certificate to attest that the student was not able to attend the test component on the given date and time.

Note: A minimum grade total of 60% must be achieved to successfully complete this course with a passing grade.

Literacy policy:
In graded activities, teachers may deduct up to 10% for grammar, spelling, punctuation and/or syntax errors.

The Computer Science Department recognizes that literacy in all its forms (read, written, spoken) is essential to students in their careers.

Teachers may choose to incorporate a literacy component into the marking scheme for any piece of work. Teachers may use their discretion to insist that any piece of work submitted for credit is revised by the student if it is unsatisfactory with regard to literacy.

Teachers will inform all students in their courses of this policy at the beginning of each semester either by including it in the course description or otherwise.

Required/Recommended Reading
Students must create a free, online account through the *Bibliothèque et Archives Nationale du Québec (BANQ)*: https://cap.banq.qc.ca/inscription?locale=en

Students can access resources through the *BANQ* such as:

- O'Reilly Publishing
- LinkedIn Learning

The Institutional Student Evaluation Policy (ISEP) is designed to promote equitable and effective evaluation of student learning and is therefore an essential policy to read and understand. The policy describes the rights and obligations of students, faculty, departments, programs, and the College administration regarding evaluation in all your courses, including grade reviews and resolution of academic grievance. ISEP is available on the Dawson website (see link above). This course outline has been

prepared in conformity with the Institutional Student Evaluation Policy (ISEP). The full policy is available on the Dawson College webpage.

Below are excerpts of important policies and procedures outlined in ISEP:

Literacy Standards

In graded activities, teachers may deduct up to 10% for grammar, spelling, punctuation, and/or syntax errors.
The Computer Science Department recognizes that literacy in all its forms (read, written, spoken) is essential to students in their careers.
Teachers may choose to incorporate a literacy component into the marking scheme for any piece of work.
Teachers may use their discretion to insist that any piece of work submitted for credit is revised by the student if it is unsatisfactory regarding literacy.
Teachers will inform all students in their courses of this policy at the beginning of each semester either by including it in the course description or otherwise.

Academic Integrity Policy

Cheating and Plagiarism are serious offences and will result in failure in the assignment, test or exam, or **entire evaluation component** and **may also result in failure of the course.** Further disciplinary action might be taken which may result in suspension or expulsion from the program and the College.
Every instance of cheating or plagiarism leading to a resolution that impacts a student's grade must be reported, with explanation, in writing, to the appropriate Dean. (ISEP Section V-A)

Students are asked to familiarize themselves with ISEP p. 21 to 24. In addition, the Business Administration Department enforces the following rules: Electronic dictionaries and cell phones are prohibited during tests.

Code of Conduct

"*Everyone has the right to a safe and non-violent environment. Students are obliged to conduct themselves as stated in the Student Code of Conduct and in the ISEP section on the roles and responsibilities of students.*" (ISEP section II-D).

The full text of the Code of Conduct Policy is available on the Dawson College webpage.

Your attention is directed to the ISEP provision requiring respectful behaviour and general decorum. Violation of these provisions may lead to the exclusion from the classroom and the case referred to the Director of Student Services or the Dean of Continuing Education.

Professional Conduct

Faculty members in the program are responsible for assessing student behaviour in terms of suitability to the profession, advising students that exhibit inappropriate behaviour, and reporting said behaviour to the Program Coordinator when necessary. (ISEP section IV-O.2)

Attendance Policy:
"*Students should refer to the Institutional Student Evaluation Policy* (ISEP section IV-C) *regarding attendance."*

Policy on Religious Observances Statements:
"Students observing religious holidays must inform their teachers, in writing, as prescribed in the ISEP Policy on Religious Observances, no later than the end of the second week of the impacted semester or term. This applies both to the semester or term, as well as to any final examination period." (ISEP section IV-D).

If applicable, a statement indicating any modifications to planned course activities resulting from the teacher's own religious observances must be included as per ISEP Policy on Religious Observances (ISEP section IV-D).

	Code:	EZ07

Objective ***Standard***

Statement of the Competency	**Achievement Context**
Manage security incidents.	• For various types of incidents affecting the security of systems and data. • From a service request. • On a variety of systems and platforms. • Under supervision. • In collaboration with analysts and other technicians. • With the help of: • Event reports; • Protocols; • Supplier documentation or scientific articles; • Application frameworks; • Software or applications.

Performance Criteria for the Competency as a Whole
• Compliance with policies and standards. • Compliance with operational constraints. • Compliance with best practices in cybersecurity. • Respect for professional ethics. • Effective priority management. • Speed of execution. • Effective communication with stakeholders in incident management. • Detailed documentation of operation performed. • Taking account of the various sources of information. • Accurate interpretation of results. • Appropriate use of equipment and software.

- Respect for confidentiality.

Elements of the Competency	Performance Criteria
1. Carry out a risk analysis.	1.1Identification of relevant sources of information. 1.2Methodical collection and analysis of information. 1.3Prioritization of information assets. 1.4Identification of the main threats and vulnerabilities. 1.5Clear, concise presentation of results.
2. Secure information.	2.1 Correct application of norms, policies and standards. 2.2Effective correction of high-risk security vulnerabilities. 2.3Application of the relevant access control measures. 2.4Methodical validation of the effectiveness of the measures put in place.
3. Manage incidents.	3.1Implementation of effective incident detection measures. 3.2Rapid detection of incidents. 3.3Complete resolution of the incident. 3.4 Drawing up a detailed incident report.
4. Raise user awareness.	4.1 Identification of relevant threats. 4.2 Demonstration of the impact of different vulnerabilities. 4.3 Presentation of relevant case studies. 4.4 Appropriate use of visual aids. 4.5 Recommendations for safe behaviour.