

CSEC 342 – 801 and 810: Cybersecurity Operations, 2023–2024 Winter

In-Person (801): Course meets Wednesday at 5:45 PM to 9:00 PM in Lewis Center Room 1108 on the Loop Campus

Async (810): Recordings of class and lecture will be published in D2L

Instructor Info



Instructor: Samuel Jevitz

Email: sjevitz@depaul.edu

Office: Lewis 1108

Office Hours: Wednesdays 5:00 PM – 5:45 PM | Thursdays
(Online/Zoom) 5:00 PM – 5:45 PM

Communication: I can be readily contacted at my University email address (sjevitz@depaul.edu) regarding any questions, comments, or concerns related to the class. I will typically respond to emails within 24 hours. I can also be contacted via walk-ins during office hours.

If you need to see me outside of office hours, and for something more complex than easily discussed over email, I will try to work with you to schedule a Zoom call during additional timeslots.

Course Description



The Cybersecurity Operations course presents the knowledge and skills needed for a Security Analyst in a typical Security Operations Center environment.

The course covers the core security skills needed for monitoring, detecting, investigating, analyzing and responding to security events. Extensive laboratory exercises are included to apply knowledge learned in the lectures and allow the students to implement typical SOC tools.

In addition to technologies, the course will also cover cybersecurity operations network principles, roles and responsibilities as well as the related technologies, tools, regulations and security frameworks.

This course does not have any pre-requisites.



Required Materials

This course does not have any required textbooks. Any supplemental reading material will be supplied and available directly through the course site on D2L.

Students will perform a variety of security labs throughout the quarter, and will need to have a personal computer capable of running a virtual guest environment (specifically a supported version of Oracle VirtualBox).

Please see Oracle's documentation if you are not sure if your device can run Oracle Virtual Box. Generally, a modern system running a modern version of Windows, MacOS, or Linux, and containing at least 8 GB of RAM and at least 40 GB of free disk space should be capable of running the labs, with some exceptions.

Students that do not have access to adequate computer technology and have limited financial resources may review the CDM Tech Loan Program here:

<https://www.cdm.depaul.edu/Student-Resources/Pages/Tech-Loans.aspx>

Students will also make use of Microsoft Azure's free Data Cluster to utilize Azure Data Explorer for SOC simulations. Students will have access to this free tool via their Microsoft accounts.

Learning Outcomes

This course is intended to help students become familiar with the work performed by, and the concepts understood by, cybersecurity operations professionals.

By the end of this course, you will be able to:

- Understand core operating system and network principles
- Understand core cybersecurity principles, including attacks, vulnerabilities, and defenses, with an emphasis on incident management
- Perform investigations of basic information security incidents

Class Policies

Attendance & Participation

Attendance and participation are key elements of a successful learning environment. Missing lectures and/or participation could create difficulties in terms of knowledge building, and can impact your ability to excel in the class.



Students in the in-class section are expected to attend all classes for the entirety of the lecture. Attendance will be taken at the start of each class. Students are expected to participate during in-class discussions. These students may miss one class without penalty. Each additional absence will result in an additional 5% overall grade reduction, unless special arrangements are discussed with the instructor.

Students in the asynchronous section may satisfy attendance and participation requires in one of the following ways:

- Watch the recorded lecture and participate in the weekly discussion forums in D2L

- Synchronously join the lecture (to be counted during attendance taking) and participate during in-class discussions over Zoom
- Asynchronous students may fail to complete their participation requirement once, without penalty. Each additional failure will result in an additional 5% overall grade reduction, unless special arrangements are discussed with the instructor.
-

Late Work



Timely completion of work is a core tenant of professional work, and is critical to cybersecurity operations. It also allows me to work as quickly as possible to provide you with important feedback. However, I understand there may be other responsibilities or concerns that get in the way.

Late work will be accepted after the due date, for a maximum of seven days (except for the final project and extra credit), unless special arrangements are discussed with the instructor. Late work penalties will be applied as follows:

- Less than 24 hours late: 2.5% assignment grade penalty
 - Between 24 and 48 hours late: 5% assignment grade penalty
 - Between 48 and 72 hours late: 10% assignment grade penalty
 - Over 72 hours late: 50% assignment grade penalty
-



COVID-19 Updates

For the latest news and resources, please visit [DePaul's response to COVID-19 page](#).



Changes to Syllabus

The course syllabus is subject to change, where necessary, throughout the quarter. Any changes to the syllabus will be explicitly communicated to students via email, an announcement in D2L, and during lecturing.

Assignments

The focus of course assignments is on hands-on lab work, providing students with practical experience with core course concepts.

- Lab #1: Installing the Lab Environment
- Lab #2: Exploring Windows' Functionality and Linux Basics
- Lab #3: Introduction to Wireshark
- Lab #4: Snort and Firewall Rules
- Lab #5: Vulnerability Research
- Lab #6: Assessing Security Products
- Lab #7: Log Normalization and Review
- Lab #8: SIEM Usage and SOC Investigation
- Final Project: Incident Management Procedure Creation and Tabletops
- Extra Credit Opportunity: Phishing PSA

Grading

The student's final grade in the course will be determined by the following grading scheme:

- Lab #1 - 1%
- Lab #2 - 10%
- Lab #3 - 10%
- Lab #4 - 10%
- Lab #5 - 10%
- Lab #6 - 10%
- Lab #7 - 10%
- Lab #8 - 14%
- Final Project - 25%
- Attendance and Participation Penalties - See Attendance & Participation Class Policy
- Extra Credit Opportunity - 2%

Grading Scale

Upon completion of the course, dependent on your academic performance you will receive a grade on the following scale:

A	93-100	C+	77-79
A-	90-92	C	73-76
B+	87-89	C-	70-72
B	83-86	D	66-69
B-	80-82	F	0-65

Course Schedule

Week	Topic	Assignments
Week 1 <i>Jan 10th</i>	Cybersecurity and Incident Management Basics	<ul style="list-style-type: none">• Lab #1 Available <i>Due Wednesday, January 17th at 5:00 PM Central</i>• Extra Credit Opportunity Available <i>Due Wednesday, March 20th at 9:00 PM Central</i>
Week 2 <i>Jan 17th</i>	Operating System Basics	<ul style="list-style-type: none">• Lab #2 Available <i>Due Wednesday, January 24th at 5:00 PM Central</i>
Week 3 <i>Jan 24th</i>	Network Basics I	<ul style="list-style-type: none">• Lab #3 Available <i>Due Wednesday, January 31st at 5:00 PM Central</i>
Week 4 <i>Jan 31st</i>	Network Basics II	<ul style="list-style-type: none">• Lab #4 Available <i>Due Wednesday, February 7th at 5:00 PM</i>

		<i>Central</i>
Week 5 <i>Feb 7th</i>	Vulnerabilities	<ul style="list-style-type: none"> • Lab #5 Available <i>Due Wednesday, February 14th at 5:00 PM Central</i>
Week 6 <i>Feb 14th</i>	Security Hardening and Defenses	<ul style="list-style-type: none"> • Lab #6 Available <i>Due Wednesday, February 21st at 5:00 PM Central</i>
Week 7 <i>Feb 21st</i>	Proactive Monitoring	<ul style="list-style-type: none"> • Lab #7 Available <i>Due Wednesday, February 28th at 5:00 PM Central</i>
Week 8 <i>Feb 28th</i>	Incident Response I	<ul style="list-style-type: none"> • Lab #8 Available <i>Due Wednesday, March 13th at 5:00 PM Central</i> • Final Project Available <i>Due Wednesday, March 20th at 9:00 PM Central</i>
Week 9 <i>March 6th</i>	Incident Response II	<i>Continue working on Lab 8 and Final Project</i>
Week 10 <i>March 13th</i>	Industry Certifications, Roles, and Responsibilities + Quarter Review	<i>Continue working on Final Project</i>
Finals Week	No Class	<i>Reminder: Final Project Due Wednesday, March 20th at 9:00 PM Central</i> <i>Reminder: Extra Credit Opportunity Due Wednesday, March 20th at 9:00 PM Central</i>

University Policies & Resources

Academic Integrity

DePaul University is a learning community that fosters the pursuit of knowledge and the transmission of ideas within a context that emphasizes a sense of responsibility for oneself, for others and for society at large. Violations of academic integrity, in any of their forms, are, therefore, detrimental to the values of DePaul, to the students' own development as responsible members of society, and to the pursuit of knowledge and the transmission of ideas. Violations include but are not limited to the following categories: cheating; plagiarism; fabrication; falsification or sabotage of research data; destruction or misuse of the university's academic resources; alteration or falsification of academic records; and academic misconduct. Conduct that is punishable under the Academic Integrity Policy could result in additional disciplinary actions by other university officials and possible civil or criminal prosecution. Please refer to your Student Handbook or visit Academic Integrity at DePaul University (<http://academicintegrity.depaul.edu>) for further details.

Library Resources

The DePaul University Library (<https://library.depaul.edu>) provides access to authoritative information sources, such as scholarly articles, journals, and books, primary sources, and research databases. Research help is available daily in-person and via chat, email, phone, or text. You may also make an appointment (in-person, phone, or Zoom) with a librarian to discuss your research projects.

Center for Students with Disabilities

Students seeking disability-related accommodations are required to register with DePaul's Center for Students with Disabilities (CSD) enabling you to access accommodations and support services to assist your success. There are two office locations:

Loop Campus - Lewis Center #1420 - (312) 362-8002
Lincoln Park Campus - Student Center #370 - (773) 325-1677

Students can also email the office at csd@depaul.edu

Students who are registered with the Center for Students with Disabilities are also invited to contact me privately to discuss how I may assist in facilitating the accommodations you will use in this course. This is best done early in the term. Our conversation will remain confidential to the extent possible.

University Counseling & Psychological Services

[University Counseling & Psychological Services](#) (UCAPS) helps remove barriers to learning and support academic success by providing free, goal-focused, collaborative, short-term, confidential, individual, and group counseling services for DePaul's students. UCAPS has a diverse multi-disciplinary staff that includes licensed mental health professionals in psychology, counseling, and social work.

Students* can talk to a therapist or schedule a brief screening and consultation appointment in the following ways:

- To speak directly to a therapist 24 hours a day, 7 days a week, students should call 773-325-CARE (2273) and Press "1" when prompted.
- To schedule a brief screening and consultation (BSC) appointment, students should call 773-325-CARE (2273) during regular business hours and Press "2" when prompted.
- Students can visit go.depaul.edu/ucaps and click the '[Schedule a Consultation](#)' button to use online scheduling for a Brief Screening & Consultation (BSC) appointment. Online scheduling is available Monday through Friday from 8:00 am to 4:30 pm. *All BSCs scheduled online are for phone appointments. To schedule an in-person or telehealth BSC, please call 773-325-CARE (2273) and Press "2" when prompted.*

*Services are provided based on student eligibility. For full eligibility details please visit go.depaul.edu/ucaps.

The Writing Center

It is strongly recommended that you make use of the Writing Center throughout your time at DePaul. The Writing Center provides free peer writing tutoring for DePaul students, faculty,

staff, and alumni. Writing Center tutors work with writers at all stages of the writing process, from invention to revision, and they are trained to identify recurring issues in your writing as well as address any specific questions or areas that you want to talk about. Visit www.depaul.edu/writing for more information.

Name & Pronouns

I will gladly address you by the name and pronouns that you indicate. Please advise me of your name and/or your pronouns early in the quarter so that I may make appropriate notes in my records. Please also note that students may choose to identify within the University community with a first name that differs from their legal name, and they may also update their gender and gender pronouns. If a new name is identified, it will display as a “preferred name” in University-related systems and documents except where the use of the legal name is necessitated or required by University business or legal necessity. For more information and instructions on how to make these updates, please see the LGBTQIA Resource Center’s [Personal Information Change](#) resources and the Student Preferred Name and Gender Policy at policies.depaul.edu.

Dean of Students

The [Dean of Students Office \(DOS\)](#) promotes student learning and ethical decision making in an inclusive and validating environment. Utilizing a comprehensive approach to student advocacy that is informed by DePaul’s Catholic, Vincentian, and urban mission, the office collaborates with students, staff, faculty, parents and community partners to support students in reaching their academic and personal success.

The Dean of Students Office is primarily responsible for administering and adjudicating violations of the Code of Student Responsibility at DePaul University. Additionally, the office provides the administrative withdrawal and absence notification process, and can help students identify campus and community resources in times of personal and/or family crises and medical emergencies.

You can contact the Dean of Students Office by calling (773) 325-7290 or emailing deanofstudents@depaul.edu. In cases of emergency, please call the Department of Public Safety at (773) 325-7777.

Sexual & Relationship Violence

As a DePaul community, we share a commitment to take care of one another. Classroom relationships are based on trust and communication. Sometimes, material raised in class may bring up issues for students related to sexual and relationship violence. In other instances, students may reach out to faculty as a source of help and support. It is important for students to know that faculty are required to report information reported to them about experiences with sexual or relationship violence to DePaul’s [Title IX](#) Coordinator. Students should also know that disclosing experiences with sexual or relationship violence in course assignments or discussion does not constitute a formal report to the University and may not begin the process of DePaul providing a response. Students seeking to report an incident of sexual or relationship violence to DePaul should contact Public Safety (Lincoln Park: 773-325-7777; Loop: 312-362-8400) and/or the Title IX Coordinator (Lincoln Park: 312-362-8970 or titleixcoordinator@depaul.edu).

Students seeking to speak confidentially about issues related to sexual and relationship violence should contact a Survivor Support Advocate in the Office of Health Promotion & Wellness for information and resources (773-325-7129 or hpw@depaul.edu). More information is available at <http://studentaffairs.depaul.edu/hpw/shvp.html>. Students are

encouraged to take advantage of these services and to seek help around sexual and relationship violence for themselves as well as their peers who may be in need of support.

Basic Needs

Access to nutritious food and reliable housing are factors that influence many students' ability to succeed in the classroom and beyond. However, students facing food or housing insecurities may be hesitant to call attention to their ongoing struggles. DePaul University is committed to and cares about all students. To help you manage personal challenges and basic needs security, the university offers several resources. Any student who has difficulty affording groceries or accessing sufficient food to eat every day, or who lacks a safe and stable place to live, is urged to contact the Dean of Students Office for support: by calling (773) 325-7290 or emailing deanofstudents@depaul.edu. You can also contact [Elizabeth Ann Seton Food Pantry and Sandwich Kitchen](#) and the [Dax Program](#) (Chicago - Depaul; email: emily.edwards@depaulusa.org; phone: (312) 362-7931 for support. The Center for Access and Attainment has also created [a guide for Food and Housing Resources](#) that you can review.