Graduate Course Syllabus

ISE 620: Incident Detection and Response

Center: Online

Course Prerequisites

IT 549

Course Description

This course provides students with the background and skills to manage information security incidents to minimize impact on business operations. Topics include detection, investigation, and response to different types of security incidents. Students explore these topics by developing incidence response plans; utilizing industry-standard processes and tools for investigating information security incidents; and recommending processes for incidence response that adhere to legal, regulatory, and organizational compliance. Students who have completed the course have a comprehensive view of cyber security incident detection and response.

Course Outcomes

- Assess how legislation, policies, and regulations shape incident detection and response practices
- Employ incident detection and response tools and techniques necessary for successfully detecting, managing, and resolving incidents
- Develop security countermeasures that reduce the negative impacts of incidents on organizational systems, operations, and personnel
- Communicate the results of incident response activities to technical and non-technical audiences for enhancing the security posture of an organization

Required Materials

Using your learning resources is critical to your success in this course. The textbooks for this course are available for free through the Shapiro Library.

InfoSec

Your course uses virtual labs from InfoSec Learning. We encourage you to register before your course begins, as students are most successful when they obtain their digital resources prior to the first week of class. See the course announcements for details.

Diversity, Equity, and Inclusion

As indicated in our core values, SNHU is committed to "embrace diversity where we encourage and respect diverse identities, ideas, and perspectives by honoring difference, amplifying belonging, engaging civilly, and breaking down barriers to bring our mission to life."

This may or will be reflected in SNHU's curriculum as we embrace and practice diversity, equity, and inclusion (DEI) to provide the most transformative experience for our students, faculty, and staff. Because topics pertaining to DEI can be sensitive, please remember that embodying and practicing diversity, equity, and inclusion is one of our core values that you will encounter throughout the academic experience. In higher education, we are expected to think and engage critically. Use a growth mindset to embrace the diverse readings, course assignments, and experiences of your peers and faculty.

For more information about DEI at SNHU, please visit our website at the Office of Diversity and Inclusion.

Instructor Availability and Response Time

Your class interaction with the instructor and your classmates will take place on a regular, ongoing basis. Your instructor will be actively engaged within the course throughout the week. You will normally communicate with your instructor in the weekly discussions or the General Questions discussion topic so that your questions and the instructor's answers benefit the entire class. You should feel free, however, to communicate with your instructor via SNHU email at any time, particularly when you want to discuss something of a personal or sensitive nature. Your instructor will generally provide a response within 24 hours. Instructors will post grades and feedback (as applicable) within seven days of an assignment's due date, or within seven days of a late submission.

Grade Distribution

Assignment Category	Number of Graded Items	Point Value per Item	Total Points
Discussions	6	30	180
Module Five Discussion	1	40	40
Final Project Review Quiz	1	10	10
Quizzes	3	20	60
Lab Activities	4	40	160
Final Project			
Milestones	3	50	150
Final Project Submission	1	400	400
			Total Course Points: 1,000

This course may also contain practice activities. The purpose of these non-graded activities is to assist you in mastering the learning outcomes in the graded activity items listed above.

University Grading System: Graduate

Grade	Numerical Equivalent	Points
A	93–100	4.00
A-	90–92	3.67
B+	87–89	3.33
B	83–86	3.00
B-	80–82	2.67
C+	77–79	2.33

Grade	Numerical Equivalent	Points
C	73–76	2.00
F	0–72	0.00
I	Incomplete	
IF	Incomplete/Failure *	
W	Withdrawn	

* Please refer to the policy page for information on the incomplete grade process.

Grading Guides

Specific activity directions, grading guides, posting requirements, and additional deadlines can be found in the Assignment Guidelines and Rubrics section of the course.

Weekly Assignment Schedule

All reading and assignment information can be found within each module of the course. Assignments and discussion posts during the first week of each term are due by 11:59 p.m. Eastern Time. Assignments and discussion posts for the remainder of the term are due by 11:59 p.m. of the student's local time zone.

In addition to the textbook readings that are listed, there may be additional required resources within each module.

Module	Topics and Assignments
1	Why It All Matters: The Concept of Due Care 1-1 Discussion: Due Care 1-2 Quiz: Due Care 1-3 Getting Started With Infosec (Non-graded) 1-4 Final Project Review and Quiz
2	From 30,000 Feet: The Incident Response Process 2-1 Quiz: Incident Response Basics 2-2 Discussion: Roles and Responsibilities Matrix
3	On the Ground: Operationalizing Incident Response 3-1 Final Project Milestone One: Incident Response Process Diagram With Key Roles and Responsibilities Annotations 3-2 Lab Activity: Using Public Encryption Keys to Secure Messages
4	Cyberattacks: Thinking Like a Hacker 4-1 Discussion: Thinking Like a Hacker 4-2 Lab Activity: Social Engineering Using SET
5	Incident Detection Methods and Tactics: Part I 5-1 Lab Activity: Incident Response Procedures, Forensics, and Forensic Analysis (Non-graded) 5-2 Discussion: Mindset: Incident Response Procedures, Forensics, and Forensic Analysis 5-3 Lab Activity: Common Locations of Windows Artifacts
6	Incident Detection Methods and Tactics: Part II 6-1 Lab Activity: Closing Security Holes 6-2 Final Project Milestone Two: Courses of Action Table

Module	Topics and Assignments
7	Defensive Countermeasures 7-1 Discussion: Layering for Security 7-2 Final Project Milestone Three: Countermeasures Analysis
8	Communicating the Impacts 8-1 Discussion: Reaching the Nontechnical Audience 8-2 Quiz: Effective Communication
9	Final Ascent: Completing the Project 9-1 Final Project Submission: Executive Summary and Plan
10	Advanced Topics in Incident Detection 10-1 Discussion: Honeypots and Ransomware

Course Participation

Course participation is required within the first week of the term for all online courses. *Participation* in this context is defined as completing one graded assignment during the first week of the course. Otherwise, students will be administratively removed for nonparticipation. Students who do not participate during the first week may forfeit their rights to be reinstated into the course. Students who stop attending a course after the first week and who do not officially withdraw will receive a grade calculated based on all submitted and missed graded assignments for the course. Missed assignments will earn a grade of zero. See the course withdrawal policy and the full attendance policy for further information.

Late Assignments

Students who need extra time may submit assignments (excluding discussion board postings) up to one week after the assignment due date. Discussion board submissions will not be accepted for credit after the deadline except in extenuating circumstances.

- A penalty of 10 percent of the total value of the assignment will be applied to the grade achieved on the late assignment regardless of the day of the week on which the work is submitted.
- Students who submit assignments more than one week late will receive a grade of zero on the assignment unless they have made prior arrangements with the instructor.

Students must submit all assignments no later than 11:59 p.m. (in their own time zone) on the last day of the term. No assignments are accepted after the last day of the term unless an incomplete has been submitted. See the incomplete grades policy.

There may be times an instructor makes an exception to the late assignment policy. Instructors may accept late work, including discussion board posts, with or without prior arrangement.

- Exceptions to the late policy on these grounds are left to the instructor's discretion, including whether the late penalty is applied or waived. Students should not assume that they will be allowed to submit assignments after the due dates.
- If an instructor finds that they are unable to determine whether an exception to the late policy would be appropriate without documentation, the collection and review of student documentation should be

handled through the Dispute Resolution team in order to protect the student's privacy. In these cases, students should file a Student Concern Dispute form to have the circumstances reviewed.

If a student is experiencing (or knows they will experience) a circumstance, including pregnancy, that is protected under the Americans with Disabilities Act or Title IX, they are encouraged to contact the Online Accessibility Center (OAC) as soon as possible to explore what academic accommodations might be offered. Instructors must honor all deadlines established through the OAC.

Student Handbook

Review the student handbook.

ADA/504 Compliance Statement

Southern New Hampshire University (SNHU) is dedicated to providing equal access to individuals with disabilities in accordance with Section 504 of the Rehabilitation Act of 1973 and with Title III of the Americans with Disabilities Act (ADA) of 1990, as amended by the Americans with Disabilities Act Amendments Act (ADAAA) of 2008.

SNHU prohibits unlawful discrimination on the basis of disability and takes action to prevent such discrimination by providing reasonable accommodations to eligible individuals with disabilities. The university has adopted the ADA/504 Grievances Policy (version 1.2 effective October 16, 2017), providing for prompt and equitable resolution of complaints regarding any action prohibited by Section 504 or the ADA.

For further information on accessibility support and services, visit the Disability and Accessibility Services webpage.

Academic Integrity Policy

Southern New Hampshire University requires all students to adhere to high standards of integrity in their academic work. Activities such as plagiarism and cheating are not condoned by the university. Review the full academic integrity policy.

Copyright Policy

Southern New Hampshire University abides by the provisions of United States Copyright Act (Title 17 of the United States Code). Any person who infringes the copyright law is liable. Review the full copyright policy.

Withdrawal Policy

Review the full withdrawal policy.

Southern New Hampshire University Policies

More information about SNHU policies can be found on the policy page.