ISOM 4200 - Information and Cyber Security Management
Spring Semester, 2024

Thursday 09:00 ~ 11:50 am
Location: LSK 1001

Instructor:	Dr. Ricci IEONG. (ricci@ust.hk)
Tel:	3469 3028
Office:	LSK 4040
Office Hours:	By appointment
Teaching Assistant:	Chris TSE (imchris@ust.hk)
Tel:	2358-7638
Office:	LSK 4065
Office Hours:	By appointment
No. of Credits:	3 Credits
Prerequisite(s):	None
Course Website:	https://canvas.ust.hk

COURSE DESCRIPTION

Cybersecurity is an ever-expanding field that plays a critical role in safeguarding organizations and individuals from cyber attacks. In today's landscape, cyber attacks have emerged as a significant threat to companies and organizations across diverse industries. To effectively counter these attacks, security consultants have to possess a deep understanding of threat assessment and the ability to efficiently operate the blue team (Incident Response team) for robust defense against a wide range of attacks. This course aims to equip students with a comprehensive understanding of cybersecurity, with a specific emphasis on the investigative and responsive aspects of the field.

Throughout this course, students will have invaluable opportunities to engage with real-world scenarios and participate in hands-on exercises, enabling them to apply their knowledge and skills in incident response. They will also have access to the latest tools and technologies used in the cybersecurity industry, allowing them to gain practical experience and prepare for a career in this field.

Upon completing this course, students will have a solid grasp of cybersecurity incident response, including the blue team, threat intelligence, incident response, and threat hunting. They will also gain practical, in-demand skills for the cybersecurity job market, covering topics such as threat detection, tools, intelligence, hunting techniques, and security analysis. This knowledge and expertise will prepare them for rewarding career opportunities in the field, where there is a growing demand for professionals with incident response proficiency and specialized skills.

LEARNING OBJECTIVES

1. Understand the scope and nature of information and cyber security issues
2. Acquire knowledge on common threats and attacks
3. Understand the Cyberkill Chain, Mitre ATT&CK Framework and various incident response framework

4. Apply the incident detection and response skills to identify threats, and perform threat hunting based on real-life cases
5. Understand latest detective and preventive controls from the industry

MATERIALS

1. REFERENCE BOOKS

Adversarial Tradecraft in Cybersecurity. (2021). Packt Publishing, Limited.

Peiris, C., Pillai, B., & Kudrati, A. (2021). Threat Hunting in the Cloud : defending aws, azure, and other cloud platforms against cyberattacks. John Wiley and Sons.

Skulkin, O. (2022). Incident response techniques for ransomware attacks : understand modern ransomware attacks and build an incident response strategy to work through them. Packt Publishing, Limited.

Grimes, R. A. (2022). Ransomware protection playbook. Wiley.

Diogenes, Yuri., & Ozkaya, Erdal. (2022). Cybersecurity - Attack and Defense Strategies : Improve Your Security Posture to Mitigate Risks and Prevent Attackers from Infiltrating Your System. (3rd ed.). Packt Publishing, Limited.

Routin, D., Thoores, S., & Rossier, S. (2022). Purple team strategies : enhancing global security posture through uniting red and blue teams with adversary emulation (1st ed.). Packt Publishing, Limited.

Nicholas Dicola, & Benjamin Kovacevic. (2023). Security Orchestration, Automation, and Response for Security Analysts. Packt Publishing, Limited.

Marius Sandbu. (2023). Windows Ransomware Detection and Protection. Packt Publishing, Limited.

Sehgal, K., & Thymianis, N. (2023). Cybersecurity blue team strategies : uncover the secrets of blue teams to combat cyber threats in your organization (1st ed.). Packt Publishing, Limited.

2. CLASS WEBSITE

Updates of the course contents and other information will be posted on the course website - http://canvas.ust.hk/. You are advised to check this site regularly throughout this course.

3. SOFTWARE

Open source analysis software will be introduced during the lab sessions. Students are required to use the tools in the virtual lab environment to solve the questions posted in the lab session.

EVALUATION

Components	**Percentage of the grade**
A. In-class course work	40% (10 marks per lab, 10 marks for attendance)
B. Group project	40% (10 marks for proposal, 15% for presentation and 15% for report)
C. 1 Exam	20%
TOTAL:	**100%**

A. In-class course work (40%)

There will be about 3 to 4 graded in-class exercises throughout the semester. By the end of the class, student's answers will be collected and graded. The BEST THREE scores will be counted toward the final grade. **<u>There will be NO makeup in-class exercises for whatever reasons</u>**.

Besides, 10 marks will be counted towards the attendance score.

B. Assignment (40%)

There will be one group project assignment in a group of 3 – 4 students. The group will have to submit proposal, report and a group presentation. Details of the assignments will be provided later in the semester.

C. Exam (20%)

The exam covers all lecture, notes, together with other materials used in this course. It is an open book, open notes paper based examination. There will be no make-up exams except due to extraordinary circumstances beyond your control such as medical emergencies. In case of absence due to medical emergencies, students must submit appropriate documentation issued by a registered medical practitioner to be considered for a make-up exam.

Grade appeal

All scores will be uploaded to Canvas when ready. It is the student's responsibility to check their scores and make sure they are correct. Any appeal to score must be filed through email to Chris TSE at imchris@ust.hk within72 hours after its release.

OTHERS

Academic Integrity

Academic integrity is a critical value of the university community. Integrity violations destroy the fabric of a learning community and the spirit of inquiry that is vital to the effectiveness of the University. Anyone caught cheating, plagiarizing, and any other form of academic dishonesty will have their course grade lowered by at least one letter grade. Please remember the current university rule: "If a student is discovered cheating however minor the offence, the course grade will appear on the student's record with an X, to show that the grade resulted from cheating. This X grade stays on the record until graduation. If the student cheats again and 'earns' another X grade, the student will be dismissed from the University." Plagiarism is copying anything (text or ideas) from another source without citing that source. If you use another person's idea you must cite it, even if you rewrite the idea in your own words. Extreme care must be taken to avoid passing of other's work as one's own. You are required to provide appropriate citations when you use ideas and arguments or otherwise draw on others' work. If you use research from another source or from the Web you MUST cite the source. This is true even if you use only the general idea and not the exact words.

Learning environment

Ricci welcomes feedbacks on her teaching throughout the semester. You are encouraged to contact me at any time when you have any questions, suggestions, concerns, or would like to ask for advice. Please remember, I am here to help you learn. Therefore, please do NOT hesitate to contact me at any time, so I can do my job better!

TENTATIVE LECTURE SCHEDULE

WEEK (M.)	TOPICS/EXAMS	ASSIGNMENTS
1 (Feb 01)	Introduction to Syllabus Risk, Threats, Trends of attacks	
2 (Feb 08)	Incident Response and Handling Cycle	
3 (Feb 15)	Threat intelligence, Cyber Kill Chain, Mitre Att&ck framework, Intrusion detection - OSINT	
4 (Feb 22)	Network defense	
5 (Feb 29)	Network Detection Lab [Lab]	Lab exercise 1
6 (Mar 07)	Practical Log analysis, Unix, Windows log analysis, web server logs [Lecture with Lab]	Lab exercise 2
7 (Mar 14)	Log analysis lab of the incident [Lab]	Lab exercise 3
8 (Mar 21)	Threat Hunting	
9 (Mar 28)	No class	

10 (Apr 04)	No class	
11 (Apr 11)	Endpoint detect and response solutions and methodology	
12 (Apr 18)	Defense in Depth - Event logs consolidation and SIEM, SOC, XDR, SOAR, Playbook	
13 (Apr 25)	Log correlation and final lab [Lab]	Lab exercise 4
14 (May 02)	*Group Project Presentation*	
15 (May 09)	Post-Mortem Analysis & Digital Forensics Analysis	