# GLOBAL SUMMER PROGRAMME 2024

## CS445S CYBER THREAT INTELLIGENCE


- Instructor Name: Yihao Lim
- Title: Adjunct Faculty, School of Computing and Information Systems
- Email: yihaolim@smu.edu.sg


### A. COURSE DESCRIPTION

This course aims to introduce Cyber Threat Intelligence as a concept and teach students the approach and different techniques for managing and processing Cyber Threat Intelligence – from collections to prioritization of assets and to better leverage tactical, operational, and strategic-level threat intelligence as well as to better comprehend, synthesize, and leverage cyber threat intelligence to respond to different cyber situations.

### B. LEARNING OBJECTIVES

By the end of the semester, the students should be able to

1. Discuss and explain the concept of cyber threat intelligence, the need for cyber threat intelligence, the cyber threat intelligence cycle and how it can be applied at tactical, operational and strategic levels to augment existing security measures in the organization.
2. Discuss and explain various cyber threat actors' profiles, sorted according to espionage, cyber-criminals and hacktivists, their different motivations and modus operandi; and explain how these characteristics can help to determine potential targets, which data or assets are valuable to them, and how they will carry out their attacks.
3. Design and develop cyber threat intelligence requirements, to prioritize assets to protect and sort assets by various classification such as personal information, intellectual property, confidential business information, credentials and systems information.
4. Discuss and explain concepts of threat models and how it can be used, and demonstrate ways to counter analytic bias and convert raw threat data or information into actionable intelligence.

### C. PRE-REQUISITES / REQUIREMENTS

No perquisites needed.

### D. ASSESSMENT METHODS / GRADING DETAILS

| | |
|---|---|
| Class Participation | 10% |
| Closed Book Quiz | 15% |
| Group Assignment | 25% |
| Group Presentation | 20% |
| Closed Book Quiz | 15% |

| | |
|---|---|
| Closed Book Quiz | 15% |
| **Total** | **100%** |

## E. ACADEMIC INTEGRITY

All acts of academic dishonesty (including, but not limited to, plagiarism, cheating, fabrication, facilitation of acts of academic dishonesty by others, unauthorized possession of exam questions, or tampering with the academic work of other students) are serious offenses.

All work (whether oral or written) submitted for purposes of assessment must be the student's own work. Penalties for violation of the policy range from zero marks for the component assessment to expulsion, depending on the nature of the offense.

When in doubt, students should consult the instructors of the course. Details on the SMU Code of Academic Integrity may be accessed at https://oasis.smu.edu.sg/Pages/DOS-WKLSWC/UCSC.aspx

## F. ACCESSIBILITY

SMU strives to make learning experiences accessible for all. If students anticipate or experience physical or academic barriers due to disability, please let the instructor know immediately. Students are also welcome to contact the university's disability services team if they have questions or concerns about academic provisions: dss@smu.edu.sg. Please be aware that the accessible tables in the seminar room should remain available for students who require them.

## G. INSTRUCTIONAL METHODS AND EXPECTATIONS

This course focuses on more hands on and investigative based topics, it encompasses a lot of topics leveraging open source techniques and it will encompass a series of lectures, company visits and guest lectures.

## H. IMPORTANT ASSIGNMENT DATES

To be determined

## I. CONSULTATIONS

To be advised

## J. RECOMMENDED TEXT / READING LIST / CASE STUDIES LIST

To be advised

| LESSON PLAN | |
|---|---|
| **LESSONS** | **TOPICS** |
| LESSON 1<br>Tuesday<br>25 June | Introduction to Cyber Threat Intelligence<br>- What is cyber threat intelligence<br>- Why use cyber threat intelligence<br>- Types of cyber threat intelligence |
| LESSON 2<br>Wednesday<br>26 June | Cyber Threat Intelligence Operations<br>- Introduction to the cyber-attack lifecycle<br>- Analyst Tradecraft<br>- Cognitive Bias |
| LESSON 3<br>Thursday<br>27 June | Analytic Skills<br>- Applying Bias to Cyber Threat Intelligence<br>- Structural Analysis Techniques<br>- Quantitative Analysis<br>- Determining Confidence |
| LESSON 4<br>Tuesday<br>2 July | Cyber Artifacts<br>- Introduction to Indicators of Compromise<br>- Host-based indicators<br>- Network-based indicators<br>- Threat hunting |
| LESSON 5<br>Wednesday<br>3 July | Develop OSINT Intel Collection Techniques<br>- Introduction to VirusTotal<br>- OSINT collection techniques<br>- Introduction to Criminal Cyber Underground |
| LESSON 6<br>Thursday<br>4 July | Develop OSINT Intel Collection Techniques<br>- OSINT collection techniques<br>- Guest Lecture<br>- Class activity |
| LESSON 7<br>Tuesday<br>9 July | Develop Raw Data into Cyber Threat Intelligence<br>- Introduction to threat intelligence requirements<br>- Understand how to classify and identify stakeholders<br>- Understand the need for and how to evaluate sources |
| LESSON 8<br>Wednesday<br>10 July | Company visit |

| | |
|---|---|
| LESSON 9<br>Thursday<br>11 July | Develop Raw Data into Cyber Threat Intelligence<br>- Case study – Strategic Intelligence<br>- Case study – Operational Intelligence<br>- Case study – Tactical Intelligence |
| LESSON 10<br>Tuesday<br>16 July | Group presentations |
| LESSON 11<br>Wednesday<br>17 July | Group presentations |
| LESSON 12<br>Thursday<br>18 July | Group presentations |