

SCHOOL OF COMPUTING

Faculty of Engineering

Project Proposal Form MCST1043 Sem: 2 Session: 2024/25

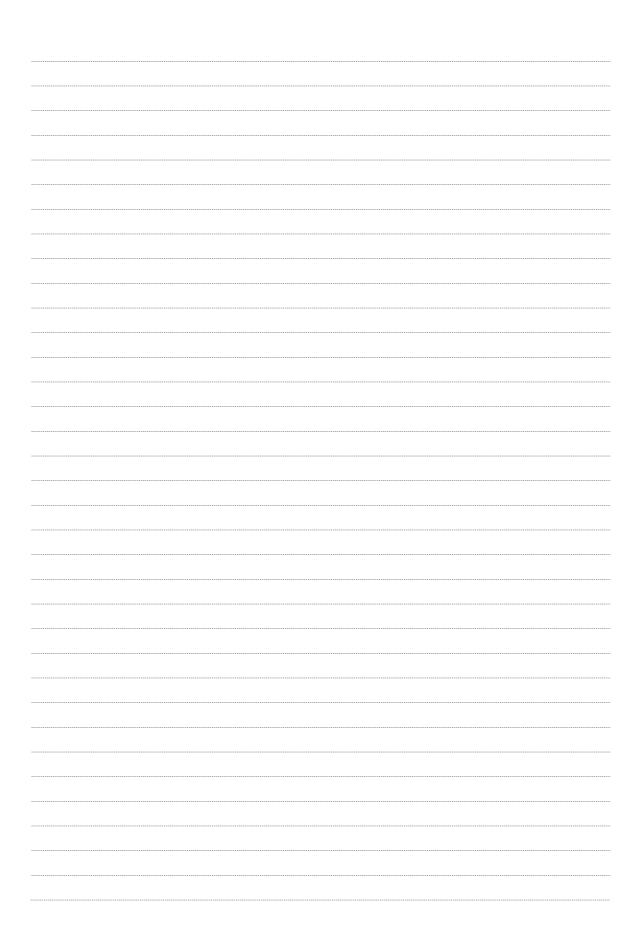
SECTION A: Project Information.

Program Name:	Masters of Science (Data Science)
Subject Name:	Project 1 (MCST1043)
Student Name:	Cui ZhiWen
Metric Number:	MCS241040
Student Email & Phone:	cuizhiwen@graduate.utm.my
Project Title:	Discover common methods of corporate network attacks through data analysis
Supervisor 1: Supervisor 2 / Industry Advisor(if any):	
SECTION B: Project	et Proposal
Introduction: The cybersecurity threats fa	acing enterprises are becoming increasingly complex.
fight,	n attack infrastructure for a long time,Design Trojan virus, and continuously improve and
	ncidents,Plan carefully before attack, conduct multiple tests .
As the means of cyber attac	cks gradually increase, data analysis can help companies that have not been attacked to take
adequate measures to prote	æt themselves.
Problem Background: With the rapid development	nt of big data, the Internet of Things, and cloud computing, increasingly fierce cyber attacks
have become a new challer	nge to enterprise security. Enterprises may be threatened by cyber attacks at any time.
In this context, we use data	a analysis to find out the most vulnerable ways for enterprises to be attacked.
Problem Statement: Discover common method	ls of corporate network attacks through data analysis

Aim of the Project:

The project aims to discover common methods of corporate network attacks through data analysis.					
In order to :					
1. Helping businesses that ha	ve not been attacked by cyber attacks to protect themselves				
2. Reduce the number of companies that are successfully attacked by cyber attacks					
3. Combine internal enterpris detection accuracy	e logs with external threat intelligence data to build a hybrid data model to improve				
Objectives of the Project: Analyze common network att	tack methods and network defense methods				
Identify which businesses are	most vulnerable				
Explore blockchain technolog	gy for attack tracing or federated learning analysis methods to protect data privacy				
2025 Log data: firewall logs, intrusi	n Malaysia Or China that were attacked by cyber attacks within one year April 2024 to April ion detection system (IDS) logs, terminal device logs, etc.;Network traffic data: Capture				
Integrate	as MITRE ATT&CK) to assist in attack pattern identification.				
Expected Contribution of th Visualize the network attacks	ne Project: that enterprises are vulnerable to, and optimize defense measures through modeling.				
Design a real-time attack dete	ection framework based on streaming data processing (such as Apache Kafka)				
Project Requirements:	Phyton, Power BI and Excel				
Hardware:	Thyon, Tower of and Elect				
	Exploratory Data Analysis, Visualisation				
Type of Project (Focusing o	on Data Science): ta Preparation and Modeling				

[√] Data Ar	nalysis and Visualization		
[√] Business	s Intelligence and Analytic	S	
[] Machine	e Learning and Prediction		
[] Data Sci	ience Application in Busin	less Domain	
Status of Project:			
[/] New			
[] Continu			
If continued, what is the previous title?			
SECTION C: Declaration	n		
I declare that this project is prop	posed by:		
[/] Myself	1 · A1: /		
[] Supervisor/II	ndustry Advisor ()	
Student Name:			
Signature		Date	
SECTION D: Supervisor	Acknowledgement		
The Supervisor(s) shall complete this se	ection.		_
I/We agree to become the super	rvisor(s) for this student	under aforesaid proposed title.	
N			
Name of Supervisor 1:			
	Signature	Date	
Name of Supervisor 2 (if any):			
	Signature	Date	
SECTION E: Evaluation	Panel Approval		
The Evaluator(s) shall complete this sec			_
Result:			
[] FULL APPROVAL [] CONDITIONAL APPROV * Student has to submit new proposal f		[] CONDITIONAL APPROVAL (Major)* [] FAIL* ors' comments	
Comments:			



Name of Evaluator 1:			
	Signature	Date	
Name of Evaluator 2:	Signature	Date	