

國立政治大學資訊管理學系

2024 年專題發表會

第 4A 組 專題報告書

專題名稱：資安樂解析 Loglytics

專題成員：

110306071 資管四甲 徐婉蓁

110306011 資管四甲 盧柏瑜

110306018 資管四乙 陳彥融

110306044 資管四乙 樊秉逸

110306053 資管四甲 黃婷筠

110306061 資管四甲 林廷奕

日期：2024 年 12 月

資安樂解析 Loglytics

摘要

身處於眾多數據、知識等重要信息都以資訊形式存在的資訊爆炸時代，人人都擁有著許多價值極高的資訊，因此如何保護這些資訊免於侵害、竊取甚至盜用，以及防禦層出不窮的資安攻擊就顯得無比重要。此時，資安樂解析 Loglytics 這個系統就能夠幫上忙，資安樂解析旨在支援使用者進行資安事件的快速分析與防禦，提升攻擊事件應對效率，降低企業或個人所面臨的風險，這不僅讓熟悉資安的專業人員受益，也能幫助初學者快速掌握網路安全知識，進而提升全體使用者的資安知識水平與攻擊防禦能力。

1、專題簡介

1、 專題動機

近年來隨著網路的普及和資訊量爆炸式的增長，企業和個人面臨的資安攻擊數量不斷增加，攻擊方式更加多變，複雜程度與嚴重性也不停上升，再加上新型攻擊方式不斷問世與快速演變，這些棘手的特性都讓資安攻擊的應對與防禦成為無法忽視的議題。

除此之外，如今數位資訊有著極高的價值，若不慎受到攻擊，可能導致資訊的洩漏、損壞或惡意利用，造成財損、聲譽損失、侵害隱私，甚至影響企業營運，可以看出保障資訊的安全不論是對個人、企業或組織而言都是至關重要的。

然而，儘管資安非常重要，大多數的民眾卻對於資安攻擊、如何防範這方面的知識往往不夠深入，因此，本專題希望做出一個實用且高效能的系統，能夠有效率的分析大量的資安攻擊，提供合適的應對、防禦方式，讓使用者能夠保護重要的資訊免於侵害，同時也能協助使用者快速的獲取資安方面的知識，增進這方面的認知與提升應對能力。

2、 專題目的

資訊安全方面的資料以文字型為主，即使細至攻擊指令，也能夠用文字表示之，再加上本系統提供的服務會以易於理解的自然語言呈現，因此善於文字資料處理的語言模型極為適合用於本系統。然而，現今的語言模型大多是在各個領域都具備一定程度的知識量的「通才」，卻難以專精於某個特定領域，尤其是資訊安全領域存在大量專業術語和行業特有的知識，故使用專精於資訊安全領域的模型更能夠提供能滿足專業需求的深度和精確度。

綜上所述，本專題旨在透過 T5 這個強大的語言模型，打造一個專門針對資訊安全領域的語言模型，並以此模型為核心提供多樣化的功能，系統將側重於強化威脅的識別與應對能力，協助使用者快速識別既有或新型態的攻擊並做出適當防禦。不僅如此，為了讓使用者更有效率的得到資訊安全方面的專業知識，模型將支援問答的互動模式，為使用者的疑問提供即時、準確的解答，或協助彙整常見威脅與防禦對策，還能夠幫助使用者從長篇的安全報告或事件描述中提取關鍵資訊，生成簡明扼要的摘要，幫助用戶快速瞭解重要細節。

3、專題特色

- (1) 專屬於資訊安全的語言模型：系統利用 T5 模型結合 LoRA 技術進行微調，針對資訊安全領域量身打造，能夠深入理解並生成與攻擊指令相關的內容。
- (2) 預測新型攻擊：模型能從未見過的攻擊指令中識別潛在威脅，有助於提前預防未來可能出現的攻擊模式，增強系統防護能力。
- (3) 資訊安全分析：語言模型可生成專業的分析報告，提升安全事件的應對效率，減少人工處理的時間與精力，增強整體應急反應速度。
- (4) 客群多樣：本系統含有豐富的功能，無論是熟悉資安領域、尋求資訊安全診斷，或是剛接觸資安領域的客群皆可使用。

4、專題內容

(1) 資安攻擊分類功能(Classification)

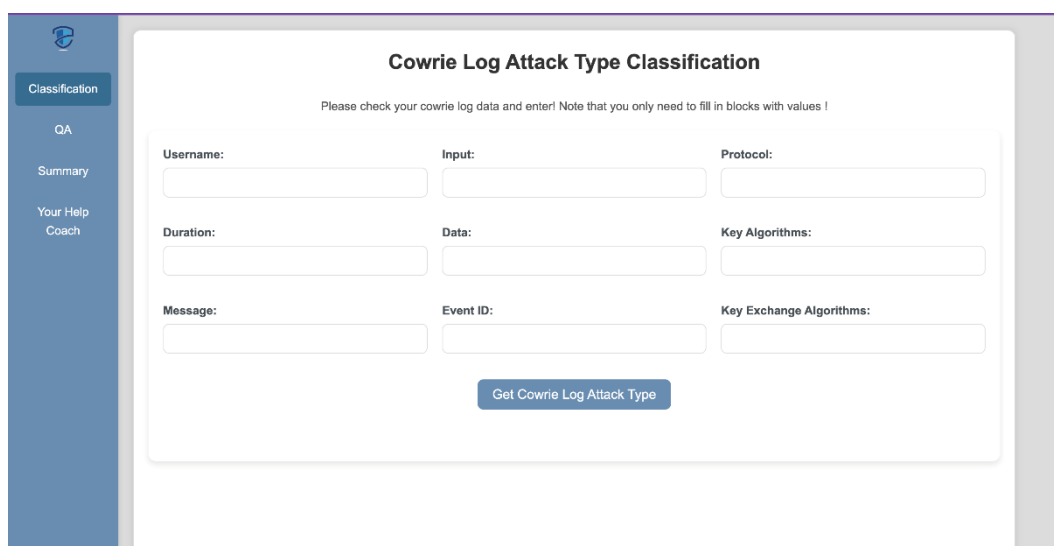


圖 1、分類功能圖

(2) 資安疑問問答功能(QA)

Question and Answer

Enter Question:

Type or paste your question here...

Get Answer

圖 2、問答功能圖

(3) 資安文章總結功能(Summarization)

Summarization

Please input cyber security related paragraph or sentences:

Type or paste your paragraph here...

Generate Summary

圖 3、總結功能圖

(4) 資安診斷分析功能(Your Help Coach)

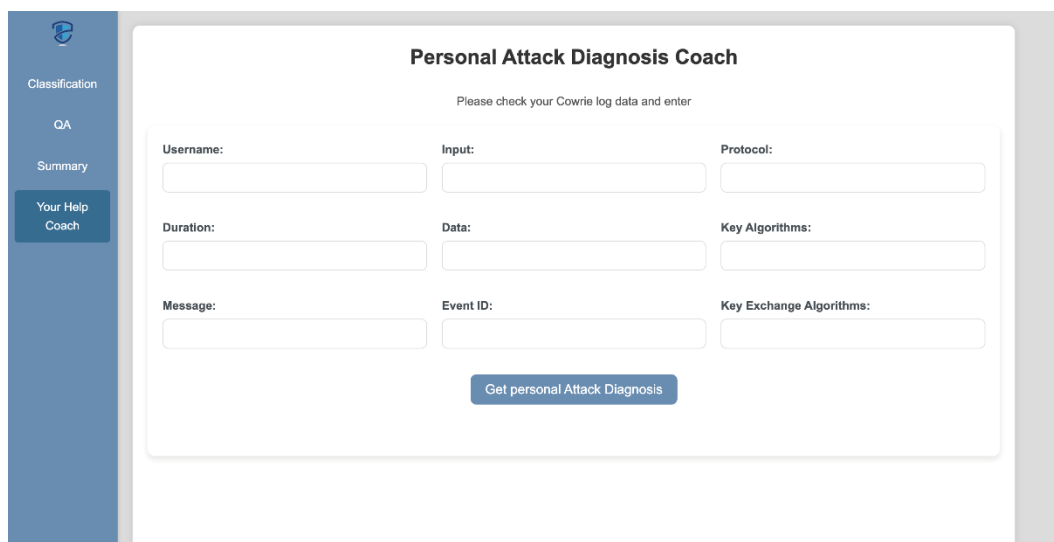


圖 4、診斷功能圖

2、需求分析

1、需求分析

根據 Fortinet 公布的《2023 上半年全球資安威脅報告》，台灣 2023 年上半年的惡意威脅數量急遽成長，共偵測到 2,248 億次惡意威脅，與 2022 年同期相比增加超過 8 成，平均每秒就有將近 1.5 萬次攻擊發生，高居亞太地區之冠。若以全球性的角度而言，每年的資訊安全攻擊數量同樣不斷攀升，如 2022 年全球的資安攻擊就較 2021 年增加高達 38% 的數量，專門收集資安弱點與漏洞的通用漏洞披露 (CVE) 記錄到的個數也從 2015 年的約莫 6500 個，在 10 年間竄升到如今的超過 30000 個，由此可知，現如今資安在世界各地都已成為不容忽視的議題，且其嚴重性仍隨著數量上漲而不停上升中。此外，也正是因為資安攻擊日漸嚴峻，每年全球因資安攻擊而蒙受的損失也以驚人的幅度提升，2023 年資安損失約為 8 兆美金，2024 年預計會上升到 9.5 兆美金，而為了因應攻擊，資訊安全相關的支出也持續的以每年超過 10% 的比例成長，以 2023 年為例，全球的資安支出約為 1881 億美金，較 2022 年成長 14.2%，顯示出資安方面的惡意攻擊帶來的成本極為沉重。

另一方面，目前全球已發現超過萬種漏洞入侵手段，與 5 年前情況相比，如今的威脅種類數增加近七成，近乎所有惡意軟體家族的變種數量皆在過去 5 年內翻倍，整體呈現爆炸性增長。不僅如此，人工智能、生成式 AI 和 5G 基礎設施等新興科技的發展，讓攻擊者得以演化出新的攻擊技術，越來越多相互鏈接的基礎設施也容易被瞄準為攻擊目標，使得威脅形態不斷演變。尤有甚者，資安攻擊愈趨規模化，成熟度、複雜度與破壞力皆有所提升，種種跡象都顯示出企業、組織或一般使

用者面對的駭侵行為日益增加，攻擊手法也變得越來越多樣化。

總而言之，網路犯罪正在呈現前所未有的複雜性，不斷提升的攻擊頻率與新技術的利用，使攻擊變得更加複雜、難以被檢測。因此，本專題希望能打造一個專門針對資訊安全領域的語言模型，並以此模型為核心提供多樣化的功能，包括但不限於解讀並歸納攻擊指令、以自然語言方式提供容易理解的警報說明、專業且詳盡的諮詢服務等，以求提高企業或組織之資安團隊的工作效率和生產力，同時也讓較不熟悉資訊安全的一般民眾也能執行精確、有效的查詢或同享上述服務。

2、分工說明

專題的主題發想與訂定、需求分析、目標設定與系統功能設計為全員皆有參與，實作部分的分工則如表 1 所示。

表 1、分工說明表

團隊成員	負責內容
盧柏瑜	後端程式撰寫、前端介面開發
陳彥融	後端程式撰寫、文件撰寫
樊秉逸	資料處理、前後端串接
黃婷筠	前端介面開發、影片製作
林廷奕	後端程式撰寫、文件撰寫
徐婉蓁	前端介面開發、簡報製作

3、系統架構與說明

1、系統架構

下圖為本專題的系統架構圖：

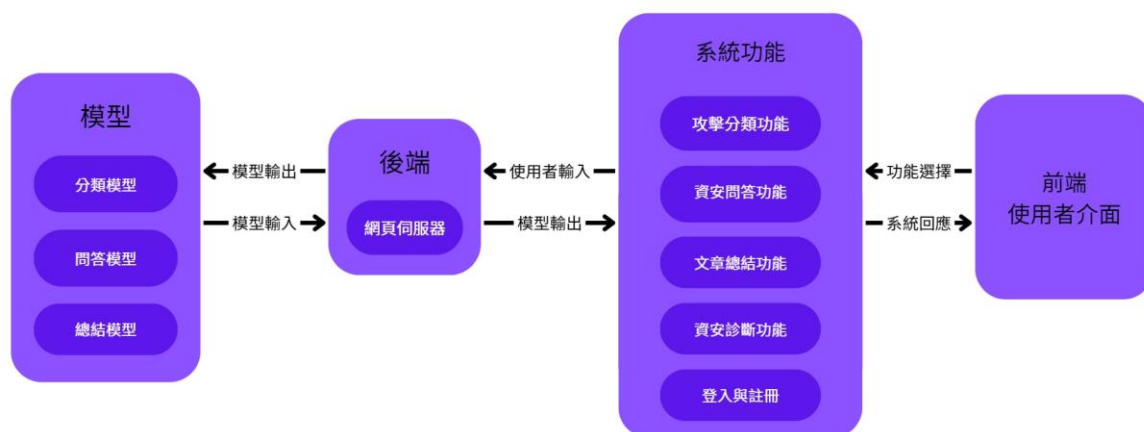


圖 5、系統架構圖

圖 5 展示了系統的整體架構，從模型、後端到前端的運作流程。主要的流程從使用者的輸入開始，透過前端的使用者介面將需求傳遞到後端伺服器。伺服器在接收到使用者的指令後，將資料傳送給不同的模型進行處理。

整體流程從使用者介面開始，使用者在前端進行操作，選擇所需的功能。這些請求經由伺服器傳遞給模型進行分析和計算，最後將模型的輸出結果返回給使用者介面，提供所需的回應和資訊。這種架構確保了系統能以高效且模組化的方式運作，同時滿足不同的資安應用場景。

系統包含三種模型：分類模型負責將輸入資料進行攻擊類型或事件的分類；問答模型能針對特定問題提供其對應之回應，特別適用於資安領域的問答場景；而總結模型則用來生成文件或文章的摘要，以便快速掌握重點內容。

伺服器作為中介，負責在使用者和模型之間傳遞資料，確保每個請求都能準確地由對應的模型處理。處理完成後，系統根據模型的輸出提供對應的功能，例如攻擊分類、資安問答、文章摘要和資安診斷。此外，系統還包含基本的登入與註冊功能，確保只有經授權的使用者能夠使用。

2、系統功能

(1) 分類 (Classification)

1. 功能描述：系統自動識別和分類各類網路攻擊事件或指令，共分成 15 類。
2. 輸入：Cowrie log
3. 輸出：各類攻擊的分類標籤及相應描述

(2) 總結(Summarization)

1. 功能描述：系統從長篇的安全報告或事件描述中提取關鍵資訊，生成簡明扼要的摘要，幫助用戶快速瞭解重要細節。
2. 輸入：長文本資訊安全報告或事件描述
3. 輸出：經過總結的短文本

(3) 問答(Causal language modeling)

1. 功能描述：系統回答使用者提出的問題，提供有關特定攻擊技術、預防措施或最佳實踐的建議，從而一步步幫助用戶作出適當決策。
2. 輸入：使用者提出的任何資訊安全相關問題
3. 輸出：針對問題的精確回答，包含解釋、說明或建議作為等

3、系統開發工具與技術

圖 6 為從專題動機到系統功能實作的開發流程圖：

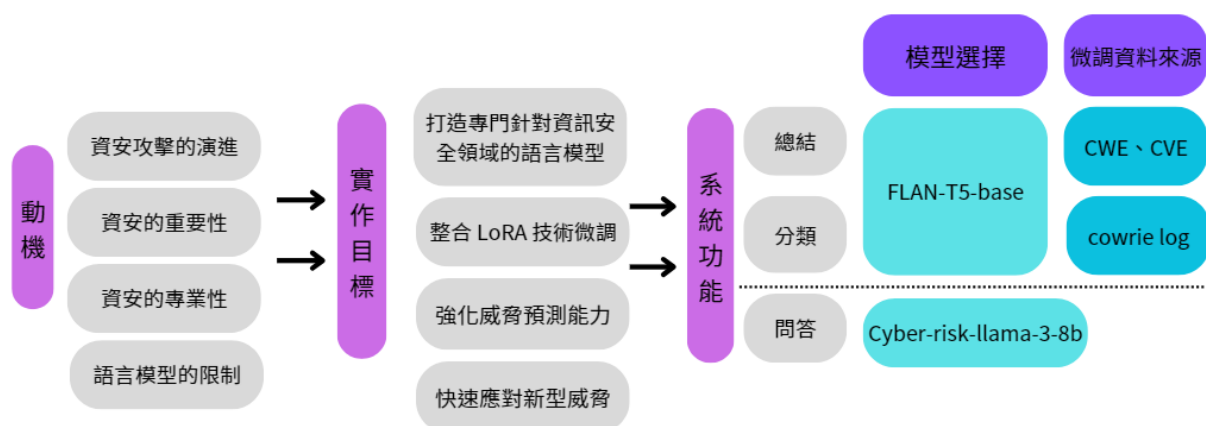


圖 6、開發流程圖

(1) 模型運行平台與程式語言：

大型語言模型參數量巨大，使用上會對硬體設備有一定的要求，因此為求有效率的運行，本專題使用 Google Colaboratory (以下簡稱 Colab) 平台進行模型相關的作業，這是一個由 Google 運營的 Jupyter notebook 雲端開發環境，讓使用者可以在瀏覽器上編寫程式碼，並使用 Google 提供的運算資源來執行，如此便能利用 Google 強大的處理器來高效使用模型。

程式語言方面，由於 Python 在 AI、語言模型方面有著最為豐富的函式庫與完整的生態系，因此本專題選用 Python 作為主要程式語言。

(2) 模型選擇

1. FLAN-T5-base

T5 (Text-To-Text Transfer Transformer) 是一個統一的架構，將所有自然語言處理 (NLP) 任務轉換為「文本到文本」的格式。無論是文本分類、摘要、翻譯，T5 都能以相同的方式處理，讓一個模型能夠有效應對多種下游任務。此外，T5 採用了編碼器-解碼器的設計，這種架構不僅能處理語言理解任務，還能進行語言生成，展現出語言理解與生成之間的平衡能力。表現方面，T5 在多項任務中展現了卓越的性能，憑藉其完整的架構設計、創新的任務處理模式與充足的參數配置，在各項下游任務上取得亮眼成果。這樣的表現將有助於我們系統的優化與完善，進一步提升整體效能與應用價值。最後，實際應用上本系統的 Summarization 和 Classification 兩項功能使用到 T5 模型。

2. Cyber-risk-llama-3-8b

這個模型是基於微調 Meta 的 Llama-3-8b 模型而得來，該模型採用了僅具備解碼器的架構，使其特別適合於問答等需要文字生成的任務。透過使用包含大量資訊安全資料的專屬資料集進行微調，模型能深入學習資安領域的專業知識，從而提升回應的準確性與專業度。此外，選用開源的大型語言模型也展現了環保意識，讓團隊無需耗費大量運算資源自行訓練或微調，達到減少碳排放和其他環境成本的效果。實際應用上本系統的 Causal language modeling 功能使用到此模型。

(3) 微調模型方式

1. 依不同功能微調

由於本系統具備多種功能，我們認為每個功能都由一個模型負責能較為精準，故微調預訓練模型時是以特定任務為導向，製作微調資料集，使用封裝完善的套件實現微調。

首先需要劃分任務，依照本系統的功能，可列出任務為分類、摘要，以及較為特殊的掩碼填充(fill-mask)。其次為載入模型，根據任務載入合適的預訓練模型檢查點。再者，依照任務的微調方式製作微調用的資料集，資料來源為組員自行上網抓取。最後實做微調，使用 Hugging Face 提供的 Transformer 套件來實作微調，並檢驗微調成效。

2. 掩碼任務

鑑於掩碼填充能讓模型高效率學習資料中的知識，我們便以此任務微

調 T5 模型，但由於掩碼填充在應用面的實用性不高，我們便沒有設計相關功能。最終訓練成果可見圖 7 與圖 8：

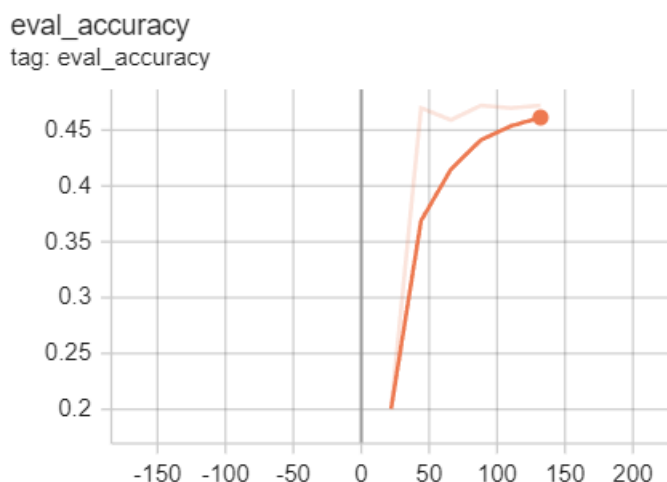


圖 7、掩碼填充之驗證準確率走勢圖

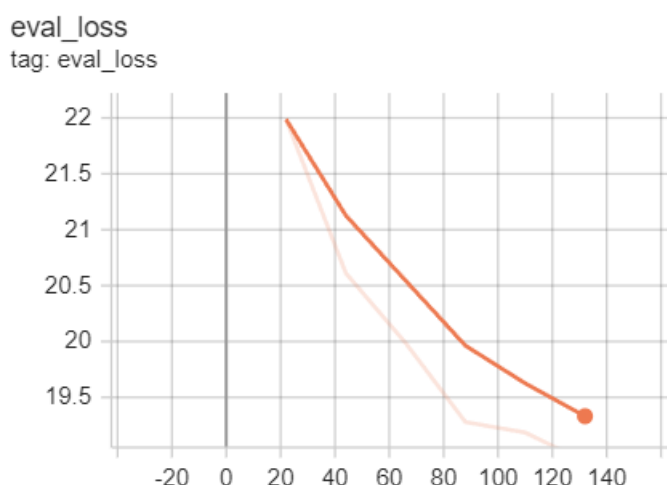


圖 8、掩碼填充之驗證損失走勢圖

可以看到準確率提升了 27% 左右，表示模型確實有學到知識，而若用 eval_loss 來計算困惑度(perplexity)，也可以見得困惑度明顯降低許多。

3. LoRA(Low-Rank Adaptation)

LoRA 的概念是凍結預訓練模型的參數，並外加一個小的可訓練參數矩陣於模型旁，最終輸出來自兩參數矩陣的輸出相結合，如此便可稍微改變原先的輸出，且由於外加的矩陣源自兩個低秩矩陣的乘積，故能夠大幅壓縮可訓練參數量，以較少資源就可以達到很好的 Fine-tuning 效果。

之所以會使用 LoRA，是因為 T5-base 模型擁有超過兩億個參數，直接進行微調需要大量運算與記憶體資源，透過使用 LoRA (Low-Rank

Adaptation)，資源需求能大幅降低。其次，LoRA 的微調方法不會更新原模型的參數，而是僅調整附加的低秩矩陣參數，這不僅有效減少了過擬合的風險，也保留了 T5 預訓練模型所累積的大量知識，提升其在新任務上的泛化能力。最後，LoRA 技術與 Transformer 模型的兼容性良好，一般將低秩矩陣置於注意力層來進行微調，故屬於 Transformer 架構的 T5 可得益於 LoRA。實際應用上 Summarization 模型使用到此技術。

(4) 資料預處理

1. 實作方式：在微調分類模型時，會先將每一筆 Cowrie Log 資料的 8 個重要屬性 (attribute) 合併成一個長字串，再以此資料及進行微調，屬性分別為 username, input, protocol, duration, keyAlgs, data, message, keyAlgs。同理，使用分類模型進行分類時也會採取此操作，以字串格式作為 T5 模型的輸入，再行分類。其中，如果值為空值，程式會直接將該屬性代入“nan”到字串中。
2. 優點：首先，合併多個特徵成單一字串，統一了數據的表示方式，符合 T5 模型「文本到文本」的設計，使模型能夠輕鬆處理複雜輸入。其次，將所有特徵合併在一起有助於模型理解各個特徵之間的關聯，從而提升分類性能，特別是在多個特徵共同影響結果時。最後，對於不同型態的數據 (如數字、文本、列表等)，轉化為統一的文本格式，可以簡化特徵處理和模型適應的步驟，使模型更專注於特徵之間的關係。
3. 使用到此技術的模型：Classification 模型

(5) Beam search 演算法

1. 概述：一種常用的序列生成算法，通過保留多個候選句子路徑來提高生成結果的質量。在每一步中，它選擇概率最高的 num_beams 條路徑，並繼續擴展這些路徑，最終選擇最優的生成序列。
2. 優點：同時探索多條候選路徑，避免選擇單一高概率路徑導致的局部最優解，從而提高生成結果的準確性，也能產生更具多樣性和合理性的分類結果。平衡品質與效率，還能減少選擇不佳序列的風險，使模型更穩定。
3. 使用到此技術模型：Classification 模型

(6) 前端與模型之串接

本專案在 Colab 上運行模型，再以 Flask 作為框架建立 API 及網頁伺

服务器，最後用 Ngrok 套件提供連結伺服器 IP 的公開連結，供前端訪問使用與傳輸資料。

(7) 前端技術

本專題使用 Django 作為主要的網頁框架，並透過串接 Flask 提供的 T5 下游模型 API 來實現問答與分類等功能。

前端所使用到技術與工具主要有三項，分別如下：

1. Django 模板系統：使用 Django 的模板系統來動態生成網頁，並確保前後端數據的交互順暢。模板檔案依功能區分，模組化設計提升了代碼的重用性與維護效率。
2. 靜態資源管理，靜態資源管理涵蓋了專題中的 CSS 文件、通用模板、以及其他靜態文件（如圖片等）。
3. 前後端數據交互，Django 的視圖負責處理用戶請求，將用戶的輸入資料提交至 Flask 後端的 API。後端將資料送進預先訓練好的模型並處理，最後將模型返回的結果顯示在相應的前端頁面中。

4、系統開發環境

本系統後端運行於 Colab 平台，開發環境由平台所提供，因此僅有需要一個 Google 帳號這一項要求，而前端的 Django 框架則運行於本機端，因此開發會需要安裝版本 3.8 以上的 Python、版本 4.0 以上的 Django 套件與虛擬環境工具，以及能正常執行 Python 的環境設置。

5、系統使用對象

- (1) Ask Me：此功能專為資安領域的初學者，或正在學習資安知識的使用者設計。通過資安分類、總結及問答功能，使用者可以深入了解各種網路安全攻擊的分類，並獲得相關知識與解答，進一步提升其在資安領域的理解與應用能力。
- (2) Help Coach：此功能適用於面臨資安危機的使用者，特別是在緊急情況下需要診斷出問題的人。透過 Help Coach 的診斷功能，使用者能迅速分析出 Cowrie log 攻擊的類型，並根據網站提供的緩解方法，及時處理安全威脅，減少風險影響。

6、系統使用環境

本系統以網頁形式提供服務，為求完整的體驗與使用功能，建議透過電腦訪問

為佳，並可運行於任何作業系統，如主流的 Windows、MacOS 等皆可，使用時需經由瀏覽器連接到系統網頁，故使用者需處於有接到網際網路的狀態，而瀏覽器的種類則不限，同時也不要求強大的圖形處理器(GPU)。總而言之，只要能夠進到系統網站，都可以順利使用本系統。

7、系統使用方式

本系統旨在提供資安相關的多項服務，各功能間的運作相互獨立，力求進到頁面就能方便的上手使用。本系統的功能主要可分為 5 種，圖 9 是其中較為重要的 4 項功能之說明圖。

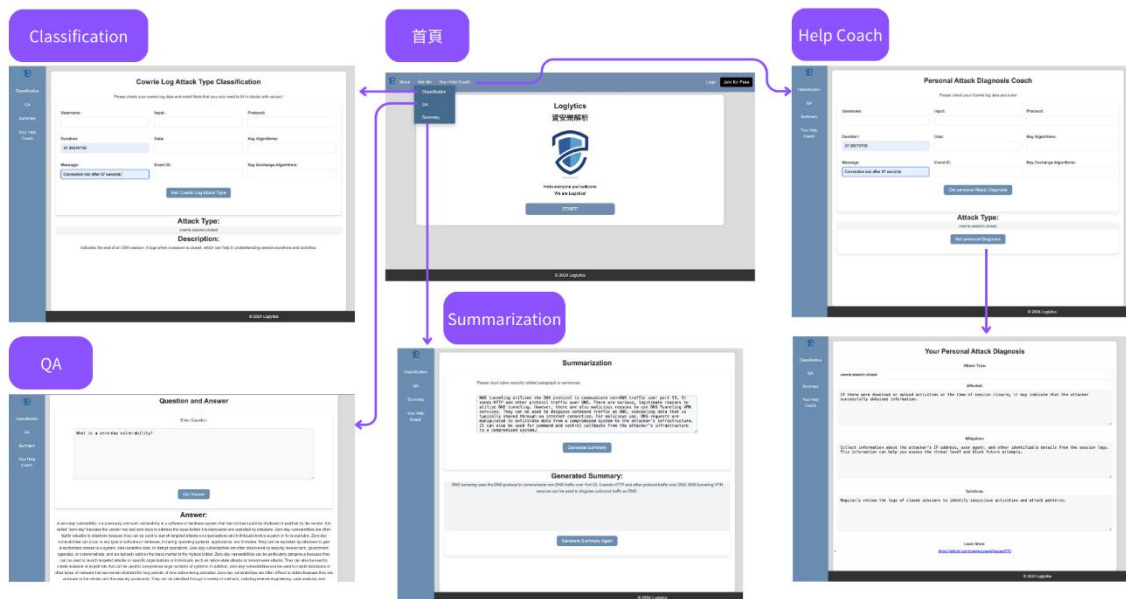


圖 9、功能說明圖

以下將分別說明其使用方法與展現實際使用的結果：

(1) 資安攻擊分類(Classification)：

使用者在每個欄位填上對應的 Cowrie log 內容後，按下「Get Cowrie Log Attack Type」按鈕，即可得到輸入資料的攻擊分類，以及該分類的簡潔描述。此功能的展示圖如圖 10，在 Duration 與 Message 兩個欄位輸入值後，即可判斷此紀錄屬於 cowrie.session.closed 類別。

Cowrie Log Attack Type Classification

Please check your cowrie log data and enter! Note that you only need to fill in blocks with values !

Username: Input: Protocol:

Duration: Data: Key Algorithms:

Message: Event ID: Key Exchange Algorithms:

Get Cowrie Log Attack Type

Attack Type:
cowrie.session.closed

Description:
Indicates the end of an SSH session. It logs when a session is closed, which can help in understanding session durations and activities.

© 2024 Loglytics

圖 10、分類功能展示圖

(2) 問答對話(QA)：

如同聊天機器人的操作一般，使用者可以輸入任意想問的資安相關疑問，按下「Get Answer」按鈕後，靜待一段時間讓即可得到系統生成之專業且適切的回答。例如詢問 "What is a zero-day vulnerability?"，系統便會詳細說明 zero-day vulnerability，如下圖所示。

Question and Answer

Enter Question:

What is a zero-day vulnerability?

Get Answer

Answer:

A zero-day vulnerability is a previously unknown vulnerability in a software or hardware system that has not been publicly disclosed or patched by the vendor. It is called "zero-day" because the vendor has had zero days to address the issue before it is discovered and exploited by attackers. Zero-day vulnerabilities are often highly valuable to attackers because they can be used to launch targeted attacks on organizations and individuals before a patch or fix is available. Zero-day vulnerabilities can occur in any type of software or hardware, including operating systems, applications, and firmware. They can be exploited by attackers to gain unauthorized access to a system, steal sensitive data, or disrupt operations. Zero-day vulnerabilities are often discovered by security researchers, government agencies, or cybercriminals, and are typically sold on the black market to the highest bidder. Zero-day vulnerabilities can be particularly dangerous because they can be used to launch targeted attacks on specific organizations or individuals, such as nation-state attacks or ransomware attacks. They can also be used to create malware or exploit kits that can be used to compromise large numbers of systems. In addition, zero-day vulnerabilities can be used to create backdoors or other types of malware that can remain dormant for long periods of time before being activated. Zero-day vulnerabilities are often difficult to detect because they are unknown to the vendor and the security community. They can be identified through a variety of methods, including reverse engineering, code analysis, and

圖 11、問答功能展示圖

(3) 文章總結(Summarization)：

若遇到篇幅較長的資安文章，使用者可以將其輸入進文字框內，按下「Generate Summary」按鈕後，系統就會迅速的生成言簡意賅的摘要，方便快速獲取重點。舉例來說，輸入與 DNS tunneling 相關的長文本，系統便會告訴使用者文章的摘要，如圖 12。

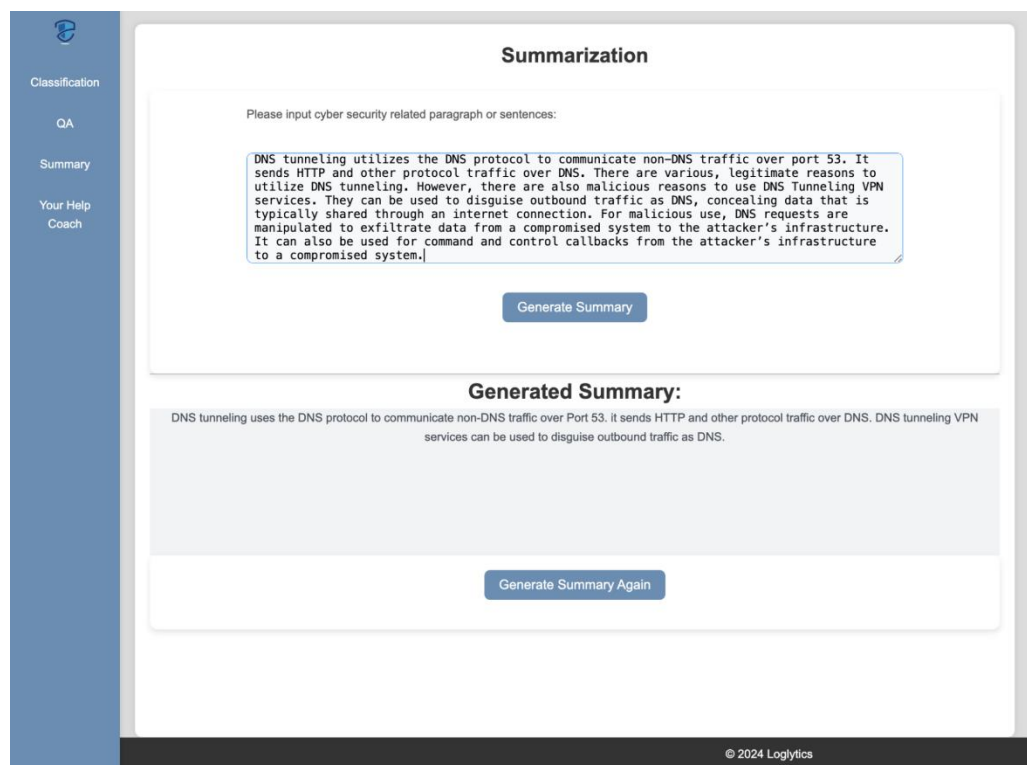


圖 12、總結功能展示圖

(4) 診斷分析(Your Help Coach)：

和上述的分類功能相似，系統會先根據使用者輸入的 Cowrie Log 來進行攻擊分類，如圖 13 所示，之後可以按下寫著「Get personal Attack Diagnosis」字樣的按鈕，就能夠得到該類別的影響範圍、緩解或根絕方式等應對手法，以及更多相關資訊，如圖 14 所示。

Personal Attack Diagnosis Coach

Please check your Cowrie log data and enter

Username: Input: Protocol:

Duration: Data: Key Algorithms:

Message: Event ID: Key Exchange Algorithms:

[Get personal Attack Diagnosis](#)

Attack Type:
cowrie.session.closed

[Get personal Diagnosis](#)

© 2024 Loglytics

圖 13、診斷分析功能展示圖其一

Your Personal Attack Diagnosis

Attack Type:
cowrie.session.closed

Affected:
If there were download or upload activities at the time of session closure, it may indicate that the attacker successfully obtained information.

Mitigation:
Collect information about the attacker's IP address, user agent, and other identifiable details from the session logs. This information can help you assess the threat level and block future attempts.

Solutions:
Regularly review the logs of closed sessions to identify suspicious activities and attack patterns.

Learn More:
<https://github.com/cowrie/cowrie/issues/770>

© 2024 Loglytics

圖 14、診斷分析功能展示圖其二

(5) 登入與註冊(Login / Join For Free)

使用者可以在登入頁面輸入帳密來登入自己的帳戶，如圖 15 所示，若尚

未註冊過的話也可以前往註冊頁面，輸入必要的資訊後即可註冊一個帳戶，如圖 16 所示。

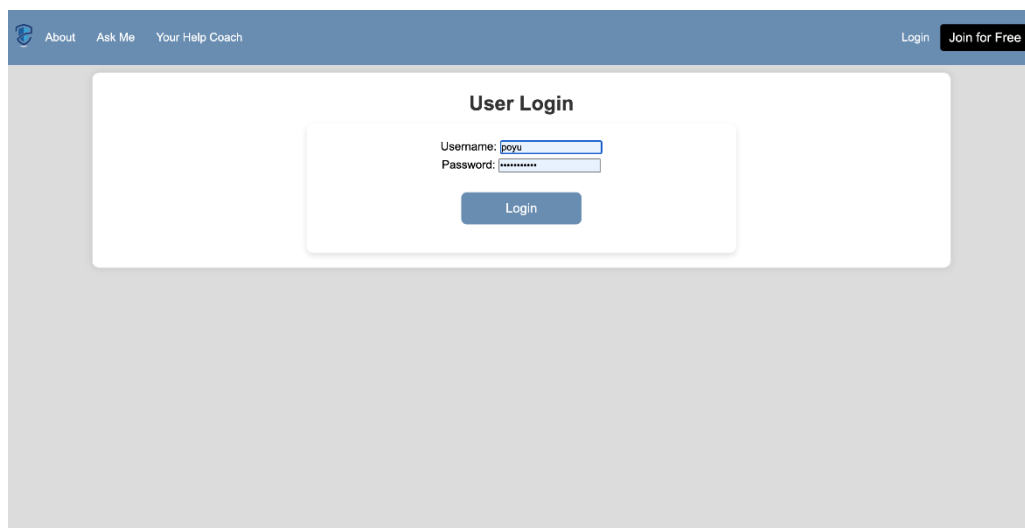
A screenshot of a web application's login page. The page has a blue header with navigation links: 'About', 'Ask Me', and 'Your Help Coach'. On the right side of the header are links for 'Login' and 'Join for Free'. The main content area is white and centered, featuring a 'User Login' form. The form has two input fields: 'Username' with the text 'poyu' and 'Password' with masked characters. Below the fields is a blue 'Login' button.

圖 15、登入功能展示圖

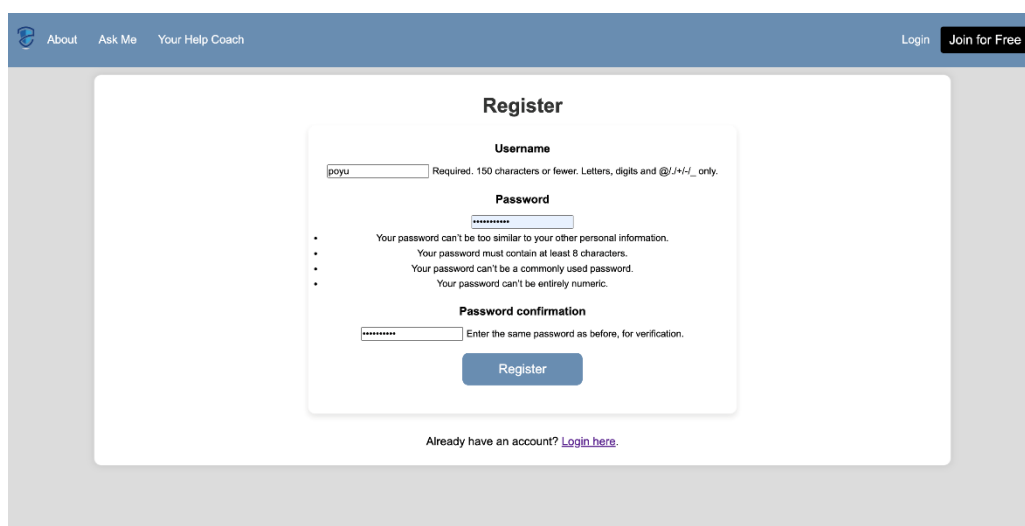
A screenshot of a web application's registration page. The page has a blue header with navigation links: 'About', 'Ask Me', and 'Your Help Coach'. On the right side of the header are links for 'Login' and 'Join for Free'. The main content area is white and centered, featuring a 'Register' form. The form has three sections: 'Username' with a text input field containing 'poyu' and a requirement note 'Required: 150 characters or fewer. Letters, digits and @/!+/_ only.'; 'Password' with a masked input field and a list of four password requirements; and 'Password confirmation' with a masked input field and a note 'Enter the same password as before, for verification.' Below the form is a blue 'Register' button. At the bottom of the form, there is a link: 'Already have an account? [Login here.](#)'

圖 16、註冊功能展示圖

4、結論與未來發展方向

1、 結論

在開發「資安樂解析 Loglytics」的過程中，我們團隊學習到如何把機器學習技術和語言模型結合於資訊安全領域，透過模型的微調和專業資料集的使用，系統展現了高度的專業性與準確性，成功地將一個通才型的語言模型轉變為專精於資安的高效能工具，增強了模型在面對複雜資安威脅時的應對能力，並針對資訊安全領

域提供了一系列實用功能，包括資安攻擊分類、文章摘要、以及問答互動模式。系統能有效支援使用者進行資安事件的快速分析與防禦，提升事件應對效率，降低企業或個人所面臨的風險，這不僅讓熟悉資安的專業人員受益，也能幫助初學者快速掌握網路安全知識，進而提升全體使用者的資安知識水平與攻擊防禦能力。

2、未來發展

為了進一步提升資安樂解析的功能和使用者的體驗，我們團隊預計會在未來針對此專題進行優化，優化內容包括：

(1) 商業化：

1. 市場定位

我們的資安語言模型專為資安專業人士、企業安全團隊及資安愛好者打造，適合不同技術水平的使用者。產品不僅能預測新型攻擊，還能自動生成專業資安分析建議，減少人工分析時間，提升應急反應速度。無論是初學者還是尋求專業協助的企業，皆可從中受益。

2. 盈利模式

可分為訂閱制、按需付費與教育機構合作三種，訂閱制會細分為不同計劃，具有不同的月費與診斷請求數量上限，按需付費則是對每次的診斷收費，適合不需要長期訂閱的客戶，而教育機構合作針對教育機構和企業提供團體購買優惠，並附加免費培訓和資源包，推廣資安學習和應用。

(2) 模型效能優化與擴展：持續追蹤新型態攻擊與威脅的變化，更新模型所使用的資料集，以保持模型與功能的最新性和有效性。

(3) 提升系統的可擴展性：將系統部署至更多環境，如雲端平台或企業內部網路，讓系統能夠因應更多的應用場景。除此之外，我們預計會開發 API，讓第三方系統也能利用本系統的功能。

(4) 推出多語言支持：鑒於資安實為世界各地都須重視之要務，故期望能為系統增加支援的語言種類，為不同語系的使用者提供本系統之服務與相關協助，還能拓展客群的範圍、邁向國際化。

此專案的未來發展將著眼於提升模型與系統的準確度和可擴展性，並與產業發展趨勢同步。透過不斷優化與創新，Loglytics 系統期望能成為資安領域的重要工具，為企業與個人在資訊安全的防護提供更全面且高效的支持。

5、參考資料

- 1、Check point research team. (2023, January 5). *Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks*. Check Point.
<https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>
- 2、MITRE CVE. (n.d.). *CVEdetails.Com Documentation*. CVEdetails.Com.
<https://www.cvedetails.com/browse-by-date.php>
- 3、Cybersecurity ventures. (2022, December 15). *Cybercrime Damages To Cost The World \$8 Trillion USD in 2023*. Newswires.
https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023
- 4、Goasduff, L. (2023, September 28). *Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024*. Gartner.
<https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024>
- 5、林芷圓. (2023, August 17). *每秒 1.5 萬次網路攻擊，台灣慘居亞太之冠！駭客從亂槍打鳥變「企業化」，5 大資安威脅一次看*. 今周刊.
<https://www.businesstoday.com.tw/article/category/183015/post/202308170006/>
- 6、Fortinet 台北訊. (2023, November 14). *Fortinet 公布《2024 全球資安威脅預測》：經典攻擊靠 AI 進化、漏洞掇客現身、從內部滲透，攻擊者將更輕鬆扣下板機*. Fortinet.
<https://www.fortinet.com/tw/corporate/about-us/newsroom/press-releases/2023/2024-threat-predictions-chained-ai-and-caas-operations>