團隊資料報名表(此為封面頁)

提案主題：SBOM 資安智慧整合與建議平台

團隊名稱：護豐智者

	姓名	學校/系級	電話	Email	簽名處
1.					
2.					
3.					
4.					
5.					

一、 團隊資料 - 隊名、團隊成員、參賽動機

隊名：護豐智者

（一）團隊資料

指導教授：

鐘建屏教授：現任國立台北科技大學資訊與財金管理學系副教授、國科會文字與聲音情緒辨識國際產學技術聯盟計畫主持人兼執行長，研究領域：金融創新、金融科技、人工智慧應用、國際金融、行為財務。

林敬皇教授:現任國立台北科技大學資訊與財金管理學系助理教授,研究領域:資訊安全、網路資安攻防、雲端與物聯網、數位鑑識。

成員介紹：

余守恩：

就讀北科資財，擅長程式開發，包括後端規劃、UI/UX 設計、人工智慧應用。

廖梓鈞：

就讀北科資財，擅長投資分析，包括總經分析、個股研究、債券與 ETF 研究。

黃定弘：

就讀北科資財，擅長數據分析、美術設計，包括資料庫、封面與海報設計。

劉世宥：

就讀北科資財，擅長數據分析、金融商品操作，包括 AI 建模、後端開發。

（二）參賽動機

永豐金控近期於 DAWHO 數位帳戶中推出許多金融服務整合，主要功能包含：數位帳戶管理、投資理財、信用卡、外匯。金控在所有軟體服務中必須保護客戶資產與隱私，勢必得於資訊安全深耕，同時我們也注意到近年在軟體供應鏈上的攻擊崛起，因此我們希望提出 SBOM[註 1]智慧資安整合與建議平台，透過人工智慧跨域金融解決痛點，協助金控完善資訊安全，因此取名為"護豐智者"。

[註一]SBOM：Software Bill of Materials 軟體物料清單，以 json、xml 等格式呈現軟體內部元件、授權、函式庫、相依關係，NTIA 於 2021 年發佈其基本元素規範。

（三）人工智慧跨域賦能重要性

1. 加速開發

因應市場需求的快速變化，企業需要能馬上應對並提出對策，人工智慧可以在各領域協助決策，並且深化多角化開發，產品與服務整合效率將大幅提升，幫助企業活化市場定位與提升價值。

2. 人機協作效率提升

生成式 AI 崛起的年代，導致各式技術的推出增快，資訊維度的提升導致工作量上升，常導致企業需要大量人力資源解決單一問題，人工智慧能夠提供我們良好的人機協作環境，不僅簡化工作複雜度，也減少企業對人事成本的負擔。

3. 滿足跨領域需求

人工智慧能夠蒐集大量的各領域資料，並且透過這些資料整理與擬合，提出客觀價值的建議，成為企業在不同領域起步時的專業顧問，使跨域開發負擔減少。

（四）SBOM 智慧資安整合與建議平台之優點

1. 專屬金融業之資安服務平台

市面上大多 SBOM 工具雖多元且成熟，但較不具針對性，無法針對行業特性做出深化結合，我們的平台不只做到漏洞分析與管理，更加注重融入金融特性，生成自家企業與金融業整體的資安競品分析報告，在開發面與維運面達成極佳平衡。

2. 提供漏洞細節追蹤與重要性分析

服務提供所有漏洞對應細節資訊，提供漏洞發生方式、可能攻擊手法及修補方式，藉此強化漏洞認知，透過這個功能可以具體了解系統存在的問題，而市面中常見資安漏洞資訊分析大多數只提供 CVSS、EPSS 分數[註 2]，然而並非分數越高，就代表對該服務、元件有越大威脅，我們對此做相關性分析、機器學習預測，獨創”絕對威脅程度評分”，使企業修補漏洞順序性更加透明。

[註 2]CVSS、EPSS：CVSS 為通用漏洞評分系統，評估整體威脅性，EPSS 為漏洞利用預測計分系統，計算未來 30 天內再次被利用機率，皆由美國組織 FIRST 管理。

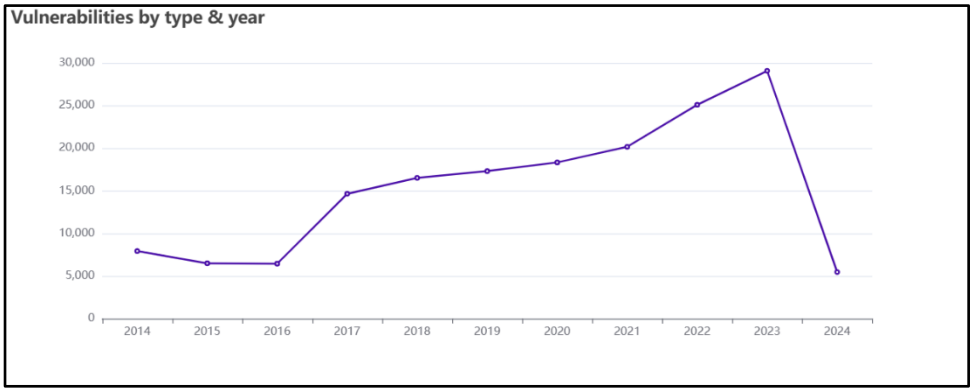
3. 導入生成式 AI 打造資安 Gen-AI

在漏洞分析過後，使用我們透過 RAG 技術開發之資安 Gen-AI，消除過往對於一般 LLM 資訊不精確之疑慮，資安 Gen-AI 不僅能完美解答您的任何問題，更能夠提供準確率極高的資安回覆與建議。

二、 數位創新方案、社群使用習慣及金融交易行為喜好及痛點

（一）數位創新方案

我們提出 SBOM 智慧資安整合與建議平台，使用人工智慧結合美國聯邦政府大力推動之軟體物料清單(Software Bill Of Materials，簡稱 SBOM)，幫助企業守護已成為駭客攻擊目標的軟體供應鏈。圖(一)為 CVEdetail.com 所整理之歷屆各年公布漏洞數量，可以發現有逐年攀升的趨勢，資安防護已然成為首要任務。



圖(一) 歷屆各年 CVE 公布數量

（二）社群使用習慣

現代人傾向使用一站式整合服務，近年來發展較穩定之社群、軟體皆有此特質，單一平台可以滿足使用者的多樣需求，便能鎖住更多來源顧客，達成分眾行銷。

（三）金融業與軟體供應鏈之痛點

1. 資安需求提高、風險增加

在投資理財觀念逐漸提升的時代，人們對於資產保護要求相當高，金融業必須做好相當完善的資安防護，這將大幅提高企業付出的人力、物力及時間成本。

2. 漏洞管理與風控工程龐大

金融業為滿足不同消費者需求，需要佈署非常大量的軟體與服務，因此需要管理的漏洞相當可觀，且資安威脅動態隨時隨地都有可能改變，造成管理困難，風險控制與效益評估作業也非常龐大。

3. 金融業高度依賴軟體供應商

金融業為維持其高度彈性之業務，大量委外尋求軟體供應商的服務，導致資安風險大幅提高，當軟體供應商自身擁有嚴重漏洞遭到駭客攻擊，位於其下游的大部分企業將會遭殃，這將使得金融業處在風險難以自控的處境。

4. 法遵時間成本高、資安政策難以落實

面對不同機構的法規和政策，常因標準不一需耗費大量人力與時間成本解讀，而進行法遵作業時，企業自身所公布的資安政策，卻又難以在各部門落實，導致法遵效率低落。

5. 供應鏈公開透明度低

金融業的軟體服務雖時常委外負責，但依然會需要各樣的客製化配套，導致軟體內部資源難以管理，也缺乏對應方式去紀錄，導致透明度低、跨部門溝通效率差。

三、 永豐金控數位金融產品與服務

（一）數位理專服務

永豐提供 ibrAin 理專平台，強調只需 3000 元即可投資、0 手續費以及客製化投資組合，不只建構自我投資，也為退休提前準備。服務可以在網頁中進行 ibrAin 投資試算，使用者輸入對應條件與期望，即可快速列出建議投資標的、績效表現，甚至針對歷年重大經濟事件都可以做出市場模擬，使用者可以透過圖表輕鬆了解投資績效。

（二）線上投資平台

在永豐銀行、DAWHO、大戶投、大戶豐等軟體提供完善的線上投資整合服務，內容包括：

1. 存貸：

多幣活存、定存、換匯優利定存、轉帳、無卡提款、雲端信貸、豐雲房貸、大優貸。

2. 證券投資：

台股下單、定期存股、複委託、期權、基金、股票抽籤、AI 選股、股市資訊。

3. 保險：

網路投保、保單查詢、保險試算。

4. 信用卡：

電子帳單、卡費自動扣繳、線上辦卡、預借現金、永豐日刷卡回饋、T Point 回饋計畫、消費碳足跡查詢。

5. 外匯：

匯率查詢、走勢分析、定期定額換匯、約匯日特惠。

（三）帳單繳費管理

稅費&帳單統一管理、信用卡管理、交易紀錄整合。

（四）官方 LINEBot 服務

整合軟體服務、智慧客服、e 指服務、帳務管家、金融友善專區、分行預約、客製化訂閱通知。

四、 同業的數位金融產品與服務分析

（一）各式金融議題下細項服務　　O：擁有該服務/ Δ：服務不完全/ X：未擁有該服務

服務 \ 金控		永豐	國泰	中信	玉山
綠色金融	綠債	O	O	O	O
	綠色存款	O	O	O	O
金融科技	生物辨識	O	O	O	O
	客戶端 Open API	O	X	O	O
	行動支付	Δ	X	O(中信錢包)	Δ
智慧金融	智能投資	O	O	O	O
	智能理賠	X	O	X	X
	區塊鏈金融平台	O	O	O	X
客戶體驗	智能客服	O	O	O	O
	生活繳費	O	O	O	O

表(一) 金融業數位產品與服務分析表

我們針對目前消費者、社會關注之四大議題進行分析，並且在金控中挑選信用卡發卡量最龐大之三大金融業者與永豐做比較。

在綠色金融方面各金控皆有所佈署，足見綠色議題對金融業者來說意義重大；金融科技的生物辨識佈署較為完善，但我們注意到永豐搶先開發出掌靜脈辨識 ATM，在此方面較其他金控優勢。整體觀察下來國泰於金融科技應用較不足，中信更能使用自身開發錢包功能為客戶打造完善生態系；智慧金融則以國泰較為突出，

首創”核保理賠智能工作臺”，節省核保時間，創造業者與消費者雙贏；客戶體驗各家金控皆有服務，畢竟是金控最重視的部分，貼近客戶的日常才能穩定客源。

五、 團隊所規劃的產品、服務、商業模式，或行銷推廣方案

（一）SBOM 智慧資安整合與建議平台

為了使永豐與金融業者能在提供多元金融整合服務的同時，建構優良的資安工程，守住客戶的隱私與資產。我們使用人工智慧結合 SBOM 進行漏洞分析管理，並且打造獨特的資安 Gen-AI，強調金融特性結合，以 B2B 的商業模式，創造專屬金融業的資安管理平台整合服務。

（二）服務內容介紹

1. 分析檔案創建 SBOM

軟體內部系統資源透明化是首要任務，我們將協助企業建立 SBOM，便於服務後續漏洞分析管理，廠商合作時也可以透過 SBOM 快速分享軟體資訊，在軟體維護時能更輕鬆追蹤版本資訊與相依關係，集中式的安全管理效率將全面提升，大幅減少時間成本。

2. 分析漏洞與絕對威脅程度評分

透過分析 SBOM，我們可以幫助企業快速了解軟體的漏洞、具體的資安事件細節，並且透過絕對威脅程度評分析統，可以具體了解漏洞修補順序，CVSS 與 EPSS 難以對單一軟體、系統造成威脅作出有效評估，因此我們使用機器學習技術增強判斷，漏洞修補的必要性與威脅程度，使企業可以完全掌握漏洞資訊並對症下藥。

3. 同業競品 LS3C 分析

透過 SBOM 表我們可協助企業進行我們自創的資安五力分析，稱”LS3C Analysis”，分別為授權可信度、來源分布、元件更新程度、架構複雜度、核心風險，這五力可以完整體現 SBOM 能帶來的效益，視覺化呈現與同業平均比分數據，並且提供具體建議與自我改善方案，知己知彼才能百戰百勝。

4. 自動回報漏洞系統

企業可以選擇是否將 SBOM 交由我們集中管理，當有新型資安事件被公布時，系統將會自動比對所有已託管的 SBOM，若掃描出對應漏洞，將立即通報企業，並提出最佳解決方案，企業也可以省下許多自行關注漏洞的時間，減輕資安威脅追蹤壓力，輕鬆避免不可挽回的傷害。

5. 資安 Gen-AI

我們透過近期 Google 新推出之 Gemini 模型，導入 RAG 技術，使 Gemini 可以從漏洞資料庫參考答案，不僅解決日常問答，還可以尋找更適合開發人員的資安深入回覆，消除過往對於一般 LLM 準確率的疑惑，甚至能選擇機器人回覆特性，提供金融、安全、科技三面向選擇，強化金融業使用特性。

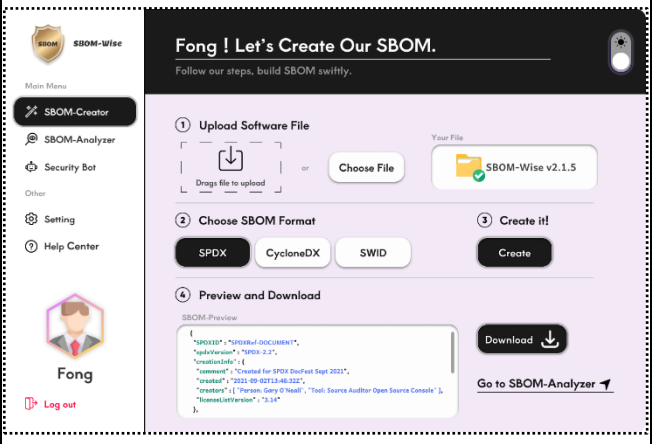
（三）介面展示與說明

UI 介面展示

1.掃描檔案建立 SBOM

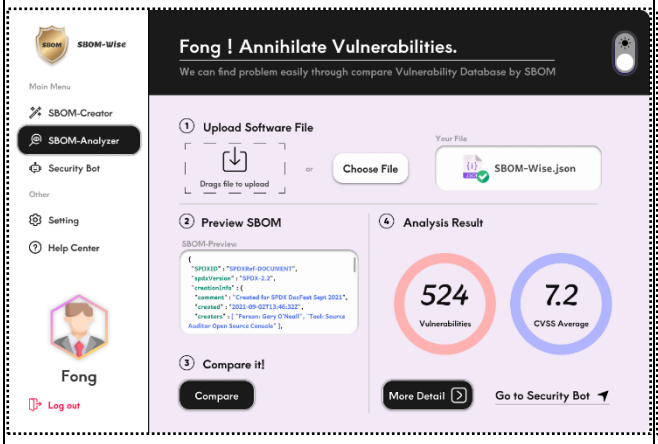
根據軟體類型、掃描深度、路徑過濾掃描符合條件軟體檔案，並且生成選取檔案之 SBOM。

2.上傳檔案建立 SBOM



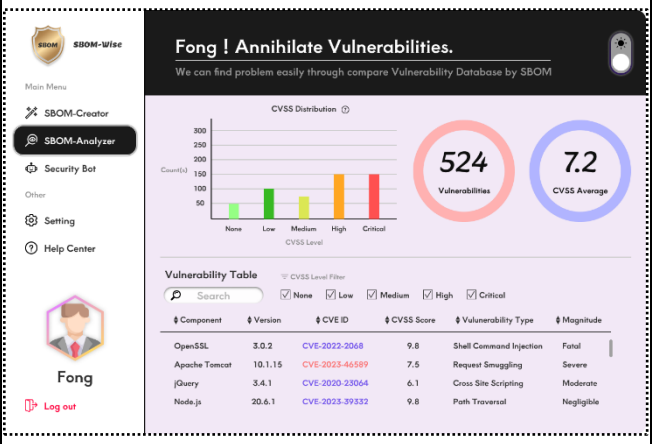
自主選擇檔案上傳，生成選取檔案之 SBOM。

3.漏洞分析系統



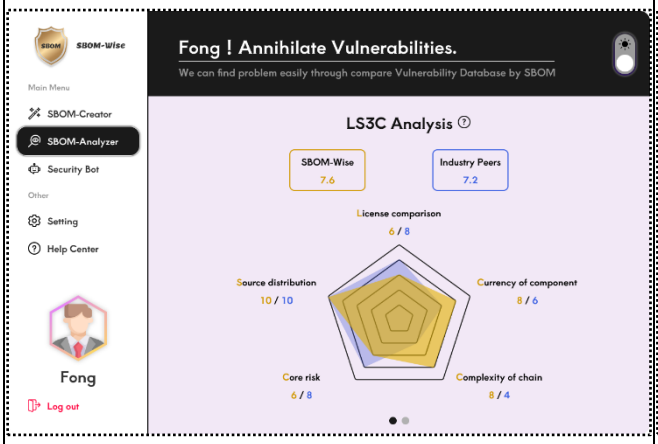
將準備好之 SBOM 匯入，系統將會自動分析存在漏洞以及平均 CVSS 分數。

4.漏洞分析細節



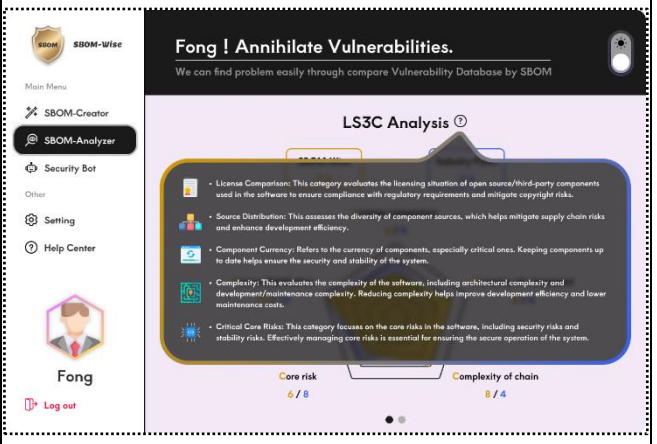
存在漏洞元件列舉，提供事件概況，也能連結至細節頁面，並呈現絕對威脅程度評分。

5.同業競品 LS3C 分析

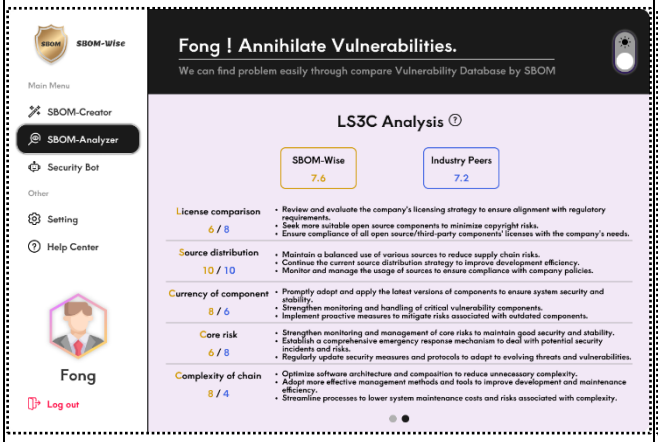
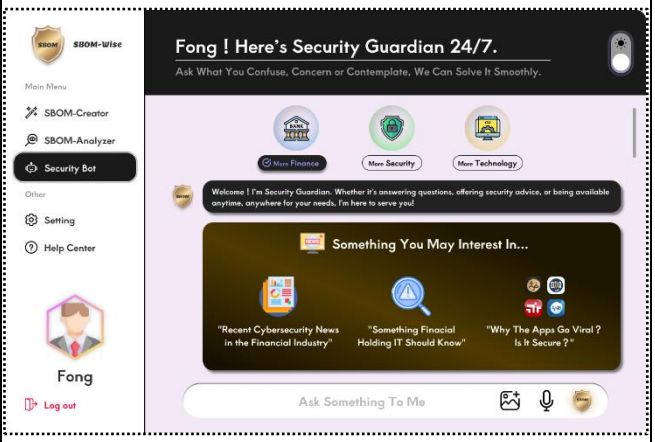
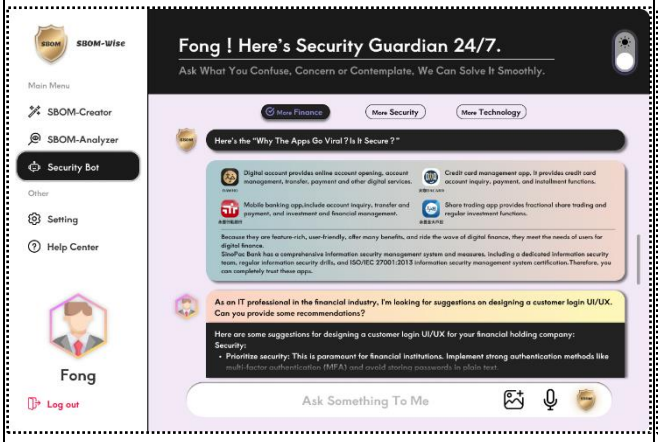
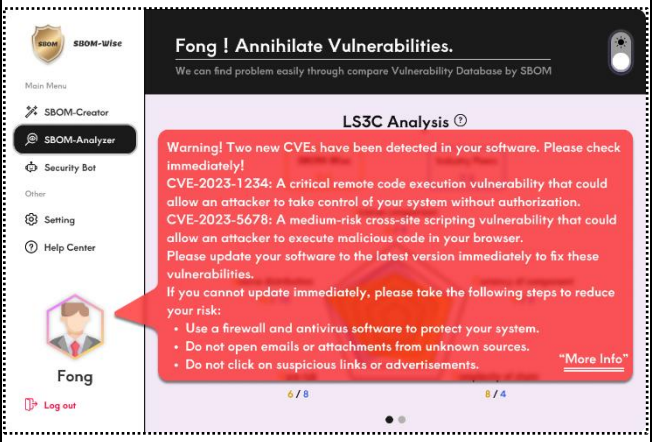


資安五力分數之量化分析，企業可以在同業競品比較，一目瞭然自身優勢與劣勢。

6.LS3C 指標依據詳細解釋



自身開發分析方法詳細介紹，符合使用者友善設計，也幫助新進資安人員快速上軌。

7.具體建議與自我改善方案	8.資安 Gen-AI 模式選擇與自動報告
	
條列整理資安五力的客製化現況改善方法，具體描述需維持與增強的部分。	可以選擇金融、安全和科技三大模式，且對談開始時推送不同面相彙整報告供觀看。
9.資安 Gen-AI 報告呈現與對話情境	10.SBOM 託管與自動漏洞通報
	
提供使用者詳盡報告，對答所有問題，並針對選擇之模式與資訊安全做為回覆基底。	企業選擇將 SBOM 交付託管後，可以在漏洞公布並確定存在時，即時獲得漏洞通報。

（四）商業模式

圖(二) 商業模式九宮格

圖(二)為 SBOM 智慧資安整合與建議平台之商業模式九宮格，我們可以將其分為四大面向探討：

1. 核心價值主張：

採用痛點解決導向的價值主張，圍繞產業與消費者去增進軟體供應鏈安全、企業漏洞管理，提升產業與客戶信心，達成互信互助的雙贏關係。

2. 需求面：

我們順應痛點進入金融業、軟體供應商的資安維護市場，如何在接下來提早佈局厚實的防守，其實重要程度不亞於金控持續推出符合需求的產品。根據 KPMG 之 2021 年調查，金融業向來是所有產業中資訊防護平均分數最高者，但在 DNS 控管[註 3]排名倒數第二、品牌監控與網頁排名最後，顯示金融業對於資安的改善與持續維護仍有高度需求。

[註 3]DNS 控管：網路域名系統控管，常遭駭客進行反射放大、阻斷攻擊。

3. 供給面：

我們扮演多領域協調整合的角色，因應跨域時代所需，我們將與相關機構與組織，進行數據分析的探討和技術實務的佈置，為金融業與軟體供應商提供專業化的資安生態系。

4. 財務面：

為了維護服務的品質與持續更新，掌控成本收益也是必盡之責，我們選擇 B2B 的商業模式，主要收益即平台租用費與服務費用，並且在 SBOM 託管服務收取託管費用，完美解決技術開發上面臨的技術、設備高成本問題。

六、 執行策略

（一）短期策略 - 1 至 6 個月達成

1. 資安專責落實計畫

配合政府目前要求企業設置之資安專責團隊，強化資安責任規劃作業外，針對各軟體服務進行每月漏洞管理評估作業，包括風險控制、漏洞修復、後續策略。

2. 建立資安漏洞管理回饋機制

以減少跨部門資安意識落差為基礎，在企業內舉辦跨部門資訊安全意識和成效交流會議，為總體資安維護、風險控制狀況較佳團隊設立獎勵機制，鼓勵資安落實。

3. 加強 SBOM 形象與意識宣導

SBOM 概念可以簡單理解，但更應加強宣導對企業的優點與應用，並提出使用類似服務之成效以及不使用帶來之威脅，使員工能發自內心感受資安服務重要性。

（二）中期策略 - 6 個月至 2 年達成

1. 完善平台機制

在目前已擁有之 LS3C Analysis 中，尚未完善分析機制，在此階段將結合各主管機關公布之報告、政策，並融合專業統計方法，強調更真實、可信之評估。

2. 強化資安政策、法規遵循管道

加入不同監理機構之政策與法規資料，幫助企業在 SBOM 公開透明化下，融入資安決策快速響應與落實，藉此提高平台影響力，順勢帶動資安落實比率提高。

（三）長期策略 -2 年以上之未來展望

1. 推動技術升級、服務流程創新

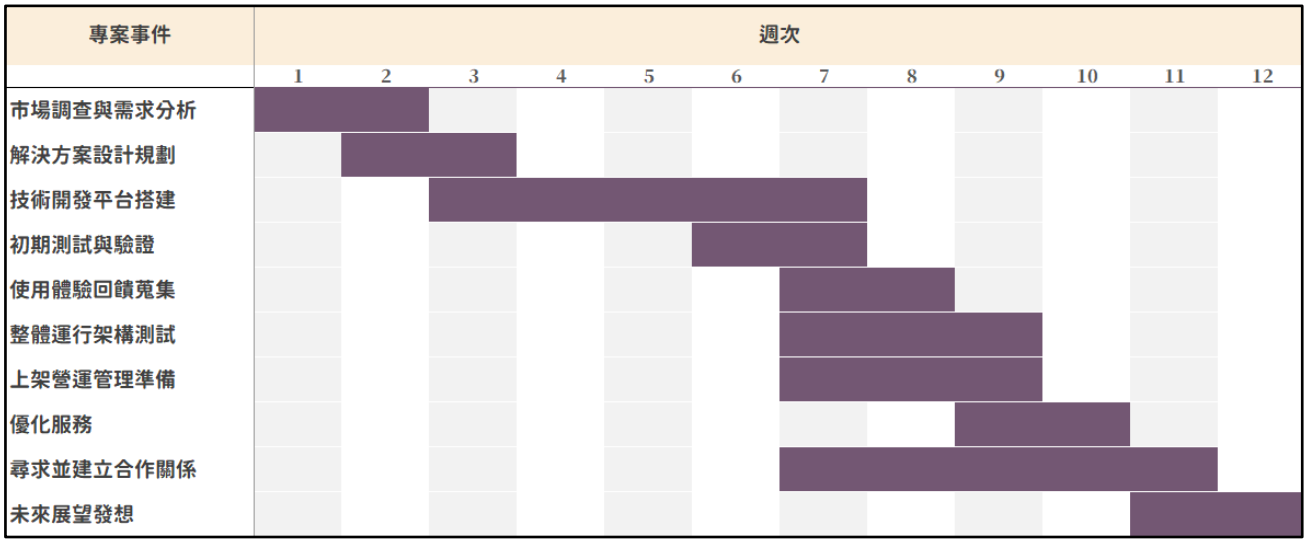
面對技術的爆發成長，科技並不會永遠停在一個時間點等待我們，所以透過不斷的資訊攝取和創新討論會議，增強技術適應力和韌性，我們相信願意面對市場、需求、技術改變而順應，才能在未來發揚光大。

2. 加強品牌實力、展望國際市場

順應服務創新，我們也需跳脫市場思維，將服務國際化，使得供應鏈安全邁向全球，積極尋求國內合作夥伴時，也向國外市場挑戰，深化跨國交流服務。

七、 時程安排

（一）事件與時程規劃



圖(三) 甘特圖

我們的服務開發流程依據 Agile 敏捷開發概念，簡單整理為十個事件，每個事件皆擁有可交付成果，並且將其分配於 12 週次內進行，呈現出一個簡單的規劃方式。此事件分配考慮面向從需求面、技術面、維運面、行銷面、落地流程皆有充分考量，並且提供合理的順序安排，賦予每一份事件充足的可用時間。

八、 成本及效益評估

（一）SBOM 智慧資安整合與建議平台之成本評估

1. 技術開發與維護費用

資安智慧的應用需要導入許多資訊科技及人工智慧相關技術，在後期維護中也必須投資經費於自主資安防護與服務完整性維持。

2. API Token 費用

資安 Gen-AI 目前以 Gemini Pro 擔任主要大型語言模型，雖然目前這個 API 還未向使用者收費，但推測不久的將來會有相關費用方案推出，故需納入規劃。

3. 設備費用

為了能夠負荷高度科技的運算，需要較完善且品質穩定之設備擔任伺服器端，完善工作效率，加強使用者體驗。

4. 教育訓練費用

與企業協商合作，提供平台服務的同時，我們提供教育訓練以使得企業人員能夠快速上手服務，深入理解服務真實帶來的效益，因此需尋找課程設計專家來協助我們，將會是其中一部份的成本。

（二）SBOM 智慧資安整合與建議平台之收益評估

1. SaaS(軟體即服務)租用費

企業在一開始與我們簽訂合作時，將會收取固定的平台租用費，成為較穩定的收益流。

2. 廣告費用

積極尋找資訊安全分數良好的企業合作，幫助推廣其產品至使用我們服務的企業，並且收取廣告費用，順勢鼓勵企業使用較安全之服務，得到雙贏。

3. 託管費用

企業將 SBOM 交付託管時會啟用漏洞自動通報系統，這項服務也會收取簡單的託管費。

（三）SBOM 智慧資安整合與建議平台之效益評估

1. 促進軟體供應鏈健全

此服務以 SBOM 結合 AI 方式，創造公開透明化管道，目的即是希望軟體供應鏈可以透過 SBOM，更機敏快速的估算與應對風險，並提供漏洞解決方案與管理機制，強化企業端點防護，為所有鏈上企業打下厚實基礎。

2. 供應鏈依賴之風險降低

透過我們的服務，金融業依然可以委外尋求供應商服務，不同於過往必須承擔風險，透過 SBOM 的力量，可以快速且徹底了解軟體的資訊，從而解決估算風險時間過久的問題，也降低金融業必須承擔的供應鏈依賴風險。

3. 資安防護壓力減少

以往的漏洞管理方案依然耗時，且無法對漏洞進行有效規劃與修補順序編排，透過我們的”絕對威脅程度評分”和”漏洞自動通報系統”，這兩項問題得以有效解決。

【附件一】團隊成員學生證 (請轉為圖檔依序貼入，請符合下列格距大小)

	正面	背面
1		
2		
3		
4		
5		

【附件二】團隊成員同意書

永豐金控、永豐銀行、永豐金證券與政治大學科研產業化平台(以下合稱主辦單位)共同舉辦永豐金控校園商業競賽活動，根據永豐金控校園商業競賽規範暨報名表，依《所得稅法》等相關規定，獎金將預先扣繳 10%作為填寫者所得計算稅額之用，獲獎人為國內居住的個人，或在國內有固定營業場所的營利事業，其中獎的獎金或給與，若給付金額超過$20,000 元者需扣繳，按給付金額扣取 10%，但應扣稅額未達$2,000 元者免予扣繳。若非本國籍則依相關規定辦理或在國內無固定營業場所的營利事業，一律按給付金額扣取 20%。獲獎隊伍對於獎金領取及分配有任何爭執疑問，概由獲獎隊伍自行處理，與主辦單位無關。

團隊名稱：

本團隊成員皆已詳細閱讀競賽說明與永豐金控校園商業競賽規範，願依相關規定參加決賽。

全部團隊成員簽名: (正楷簽名，同時標記簽名日期)

1	
2	
3	
4	
5	

請入選決賽隊伍於競賽工作坊時，攜帶匯款帳號存摺封面影本或銀行帳號證明與身分證正反影本繳交給主辦單位，以利獎金入帳。