讓修補經驗成為懂你系統的資安顧問

符合你系統的資安建議，不是購買來的，而是用經驗養成的

雲力橘子
技術開發二部 副理 蔡龍佑 Tygrus
技術開發二部 主任 林秉正 Beck

About Me

Experience

- 雲力橘子 - 技術開發二部 主任
- 果核數位 - 軟體開發安全部 主任
- 一宇數位 - 專案工程師

Skills

- 原碼檢測服務
- 原碼顧問諮詢
- 安全檢測工具導入
- DevSecOps 平台導入

Agenda

- 為什麼需要懂你系統的資安顧問
- 怎麼訓練一個 Security Champion
- 案例分享
- 未來展望

為什麼需要懂你系統的資安顧問

gamania CloudForce 雲力橘子

CVSS 4.0與環境因素的重要性

同一個評分為7.5的高風險漏洞：

- 在一個與外網隔離的測試環境中，實際風險可能下降
- 在處理敏感客戶數據的生產系統中，實際風險可能上升

資安專業知識必須結合系統知識

不了解您系統的資安顧問面臨以下限制：

- 無法準確識別系統特有的漏洞和風險點
- 難以評估漏洞在您特定環境中的實際影響
- 提供的修復建議可能與您的系統架構不相容

為什麼需要懂你系統的資安顧問

gamania CloudForce 雲力橘子

安全建議必須具備環境資訊&弱點上下文才有實際價值！

懂得您系統的AI資安顧問不僅能識別潛在的安全漏洞，還能準確評估這些漏洞在您特定環境中的真實風險，專注於真正重要的威脅。

開發團隊對一般安全建議的實際困擾

難以理解的安全建議

安全建議與開發人員的鴻溝

無法直接套用的修補方案

需要轉換才能套用

與現有架構衝突的安全措施

安全建議與系統設計相衝突

案例: 直接到客戶端，現場看程式碼，理解架構，給予合適建議，客 戶表示，之前收到的建議太攏統或是不合乎他們的架構

弱點修補的挑戰與理想

挑戰	一般安全建議	理想狀態
上下文理解	❌無	✅ 多元
系統架構理解	❌表面	✅ 深入
業務影響評估	❌不足	✅ 全面
建議實用性	❌低	✅ 高
傳統資安掃描報告與理想之間存在巨大鴻溝。		

為什麼你需要懂你系統的資安顧問

gamania CloudForce 雲力橘子

了解你的技術

了解你的語言與框架

熟悉你的系統架構

了解微服務之間的調用關係

理解你的業務邏輯

了解你的資料流程

知道你的開發流程與環境

了解你的CI/CD管道與部署環境

唯有深入理解您的系統，才能提供真正有價值的資安建議

怎麼訓練一個
Security Champion

怎麼訓練一個 Security Champion

培訓理念

原本怎麼訓練新人 - SOP

遵循系統化流程，從基礎知識到實戰案例逐步提昇

AI 就是怎麼訓練

將經驗轉化為結構化知識

知識與實踐結合

確保理論知識能夠在實際環境中得到有效應用

持續反饋與改進

建立持續反饋機制，不斷改善培訓方法和內容

培養 Security Champion - 新人訓練流程

2W

基礎評估與準備階段

評估學員當前技能水準

系統性整理現有修補資料

4W

基礎知識培訓階段

安全基礎課程 (OWASP Top 10、安全編碼原則等)

掃描工具使用培訓

8W

指導式實踐階段

在Security Champion指導下修復實際弱點

定期案例分析弱點

4W

半獨立實踐階段

在實際項目中應用

學習平衡安全修復與程式功能

2W

認證與後續支持階段

全面能力評估

目標

可以獨立處理 8 成原碼弱點且不影響程式

人員背景

開發2~3年，資安經歷1年以下的人員

背景資訊

有富含開發經驗與資安經驗的 secure champion 擔任指導者

學習資料

已有修補資料，可以供學習人員參考，並由secure champion 訓練

培訓時間的疊加因素

gamania CloudForce 雲力橘子

總培訓時間: 28週 (+8)

基礎 20 週	+8週

程式語言與框架切換

切換到不同的程式語言、框架會面臨不同的語法錯誤和安全模式

8週

架構切換

不同架構(如微服務、前後端分離)有不同的安全考量

非全力培訓

仍有其他工作項目，分散注意力

培訓時間的疊加因素

gamania CloudForce 雲力橘子

總培訓時間: 34週 (+8+6)

基礎 20 週	+8週	+6週

程式語言與框架切換

切換到不同的程式語言、框架會面臨不同的語法錯誤和安全模式

8週

架構切換

不同架構(如微服務、前後端分離)有不同的安全考量

6週

非全力培訓

仍有其他工作項目，分散注意力

培訓時間的疊加因素

gamania CloudForce 雲力橘子

總培訓時間: 44週 (+8+6+10)

基礎 20 週	+8週	+6週	+10 週

程式語言與框架切換

切換到不同的程式語言、框架會面臨不同的語法錯誤和安全模式

8週

架構切換

不同架構(如微服務、前後端分離)有不同的安全考量

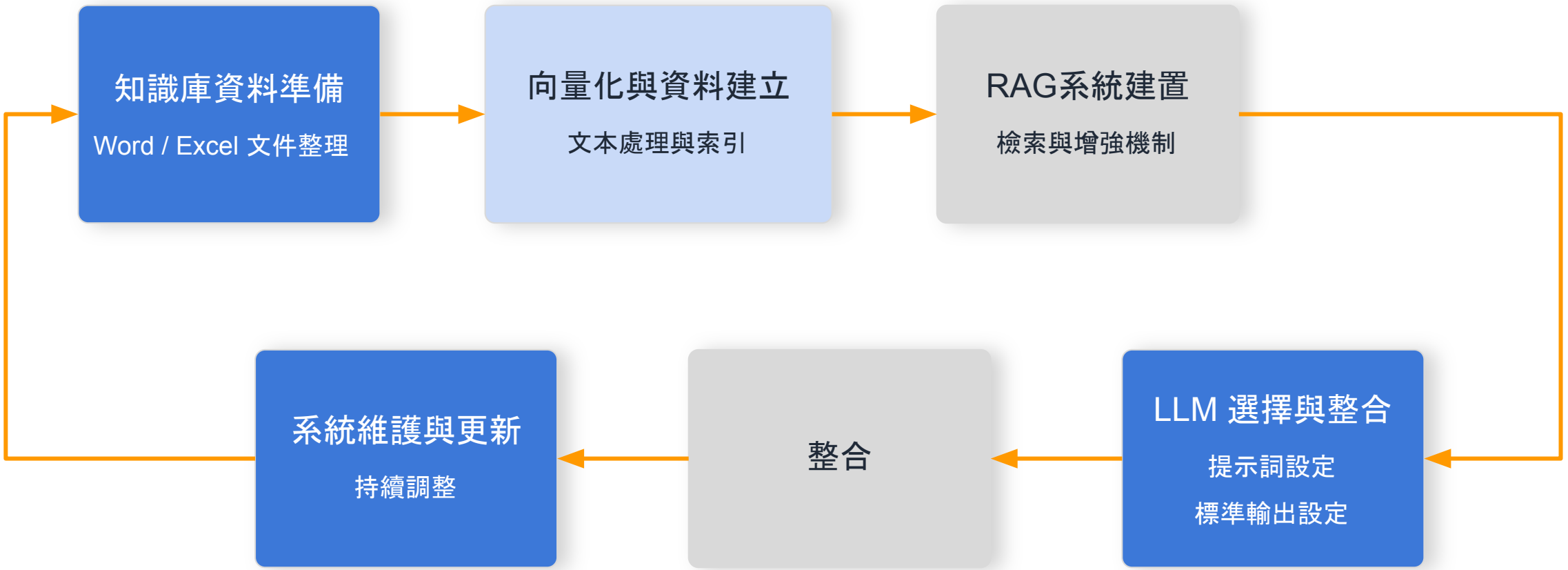
6週

非全力培訓

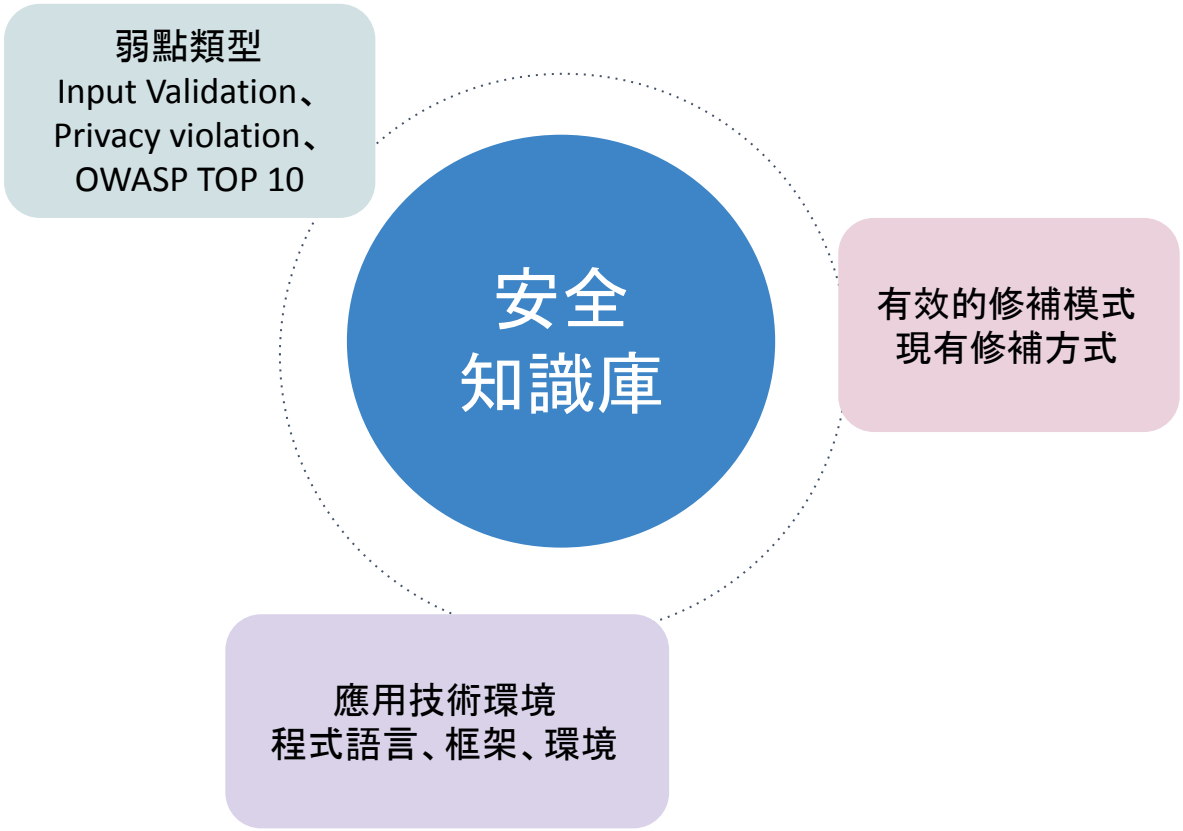
仍有其他工作項目，分散注意力

10週

培養 Security Champion - AI 版流程



弱點修補範例與資料庫



Path Manipulation

摘要

允許使用者輸入來控制檔案系統操作中使用的路徑，可讓攻擊者存取或修改受保護的資源。

說明

當發生以下情況的時候，會 產生 path manipulation 錯誤：

1.攻擊者可以指定在檔案系統操作中所使用的路徑。

2. 攻擊者可藉由指定資源來取得一般情況下不被允許的權限。

修補方式

避免最佳方法是使用間接方法：建立白名單，而使用者只能從白名單中選取。使用此方法，使用者所提供的輸入就不會直接用來指定資源名稱。

業務情境相關的修補建議

技術上的準確性

- 符合當前使用技術特性
- 考慮現有程式碼

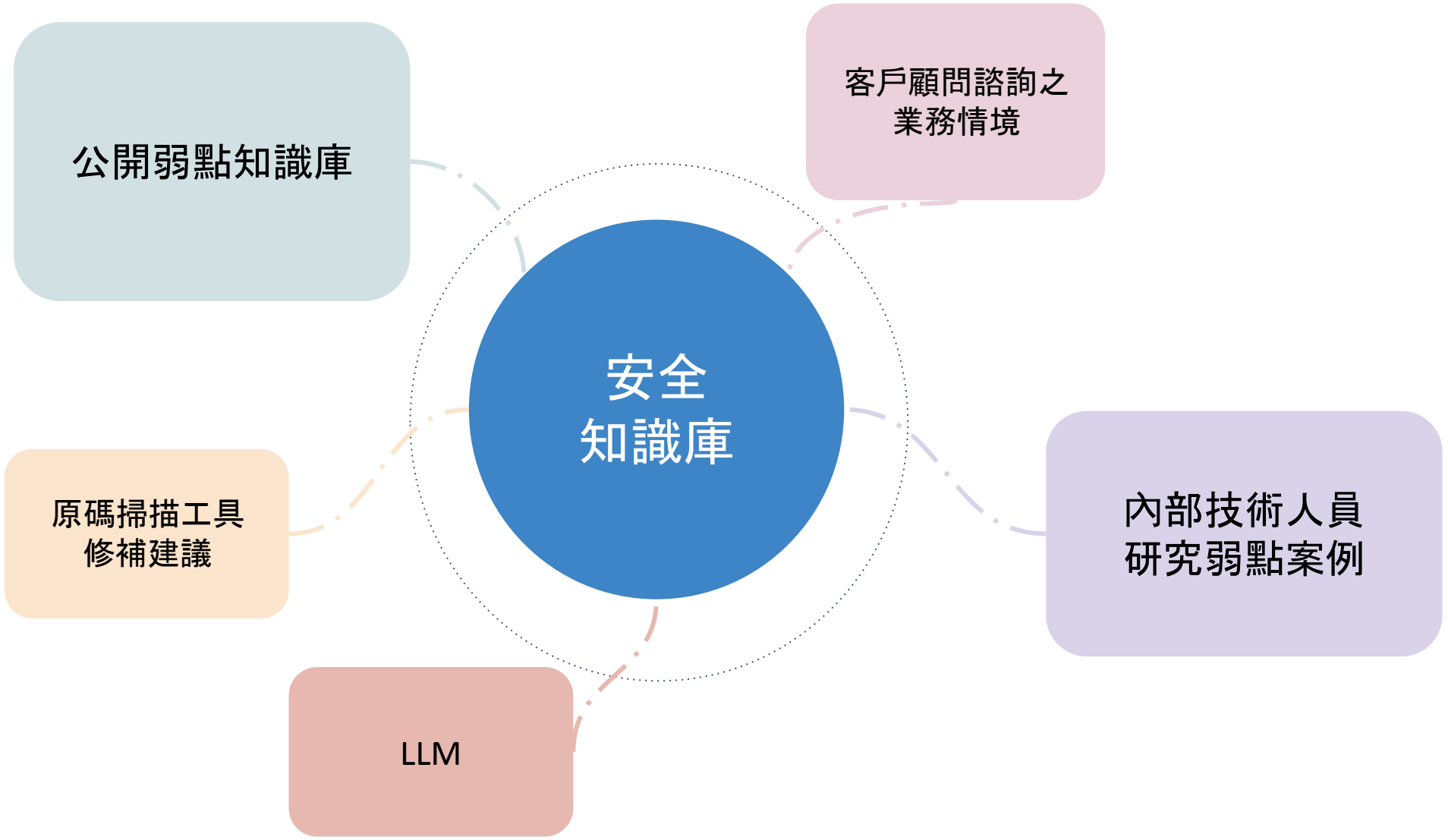
業務上的適用性

- 維持業務邏輯完整性
- 符合業務安全需求

實施上的可行性

- 分階段實施計劃
- 明確的執行步驟

整合性修補建議



RAG 技術應用

gamania CloudForce 雲力橘子

檢索 (Retrieval)

從知識庫中找出相關參考資料

- 語義檢索
- 相似度匹配
- 背景知識取得

增強 (Augmentation)

整合多來源補充知識

- 知識整合
- 上下文整合
- 關聯性增強

不同LLM 的差異

Claude	GPT-mini	GPT-4o
針對csrfToken，若確認為CSRF-Token之驗證用途，則得以排除此問題。 確保有適當的伺服器端驗證機制，不單純依賴前端傳來的 值。	請確認該隱藏欄位的 內容未包含任何個人識別資訊或敏感資料，以符合《個人資料保護法》的要求。建議您提供該隱藏欄位的具體使用情境與 內容確認，以利進一步評估。	需特別留意確認隱藏欄位中的資料不會被用於關鍵的邏輯判斷或安全性驗證，以避免潛在的風險。如變數“carfToken”為CSRF-Token之驗證用途，則應進行更嚴格的安全性檢 查。請確認後再行排除。
清晰指出問題 並且此問題後端更重要被提出	有點模糊焦點	清晰指出問題

AI 資安顧問回覆原則

gamania CloudForce 雲力橘子

客觀評判原則

以客觀方式進行評判，以信任提問者說明與佐證為原則

法規遵循原則

若資訊足夠判斷情況下違反外部法規，則不應放寬標準

資安風險評估原則

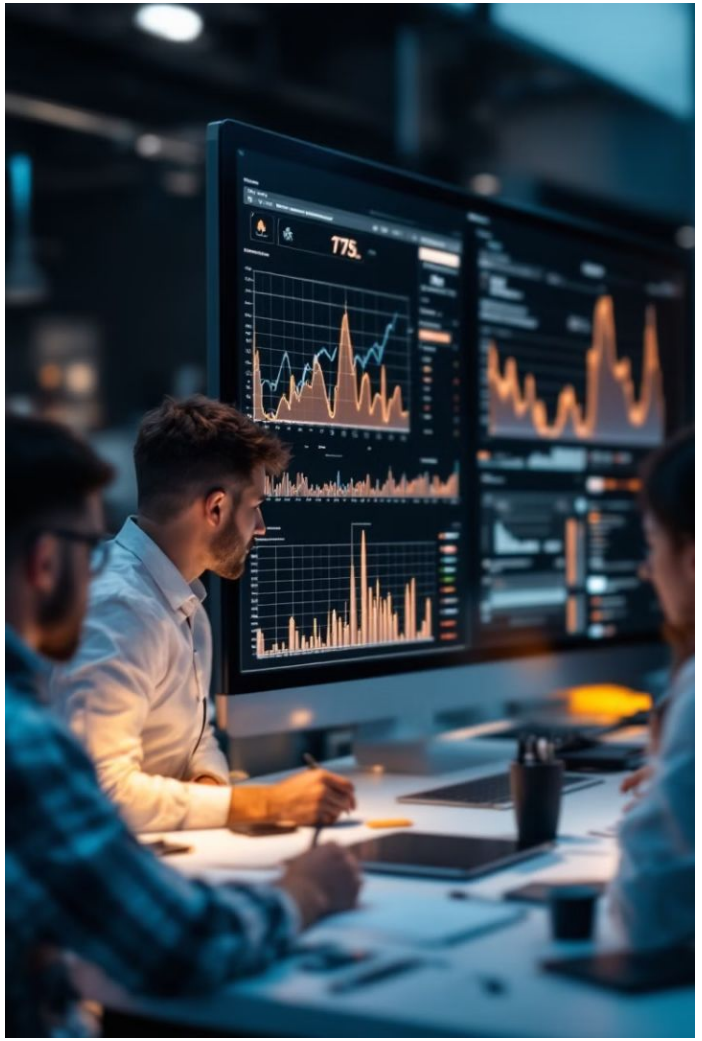
對於密碼、PII等敏感資訊，即使提問者說明非敏感資訊，仍應謹慎處理

程式管理彈性原則

若未直接造成資安風險，僅屬於程式管理疑慮，則可視情況放寬要求

回應原則

應明確說明與複誦可排除的根據與原因，並說明可能的威脅情境



AI 資安顧問標準回覆格式

弱點類別	Input Validation and Representation
弱點名稱	Path Manipulation
程式碼(請檢	File attach = new File(fileString); if
說明	該路徑由系統自動產生，使用者無法直接輸入或影響。
回覆	若確認並無使用者直接輸入之資料，則建議排除此問題。

根據您提供的資訊，由於路徑是由系統產生且使用者無法輸入或影響，因此建議可以排除此問題。請確保系統產生的路徑符合業務邏輯需求即可。

索引	關鍵字	說明
1	排除	當允許提問者使用 Suppress功能時。
2	屬於工具誤判	當某問題屬於工具誤判，非提問者問題時。
3	以利進一步評估	佐證或說明不夠完善無法進行判別時。
…	…	…

案例分享

案例研究 1：CSRF 跨站請求偽造

gamania CloudForce 雲力橘子

系統背景

前後端分離網站架構

前端 React

後端 C#

弱點描述

跨站請求偽造（CSRF）是一種攻擊，利用用戶已登入的身份，誘使其在不知情情況下執行未授權的操作。攻擊者透過構造特定網站請求，讓受害者的瀏覽器自動提交惡意請求。

一般建議

在控制器中添加[ValidateAntiForgeryToken]屬性來驗證來自客戶端的防偽標記
在View 中，使用@Html.AntiForgeryToken()

案例研究 1：CSRF - AI修補建議

gamania CloudForce 雲力橘子

AI 資安顧問深入分析

架構理解

考量並非前後端皆使用.NET 框架，無法使用框架提供防範手段

在前後端分離的架構中，例如使用React作為前端框架，處理CSRF攻擊的方式會有所不同。下面是一個常見的處理流程，如何在React前端和ASP.NET後端應用中實現CSRF防護：

後端 (ASP.NET) 設置

1. **在伺服器端生成CSRF令牌：**
   後端會在用戶登錄或載入時生成一個CSRF令牌，然後將這個令牌作為Cookie或者HTTP頭返回給用戶。
2. **驗證CSRF令牌：**
   對於需要保護的API請求，後端會驗證從前端發送過來的CSRF令牌。

前端 (React) 設置

1. **從Cookie中獲取CSRF令牌：**
   前端在發送API請求時，從Cookie中獲取CSRF令牌，並在HTTP頭中將其發送出去。

案例研究 2:弱加密

gamania CloudForce 雲力橘子

系統背景

系統與外部系統對接，外部系統會傳來加密資料，系統會解密後進行處理，使用加密為DES

弱點描述

弱加密是指因算法強度不足、密鑰長度過短或設計缺陷而無法提供足夠安全保障的加密技術。使用此類加密會使敏感資訊容易被未授權第三方破解，導致資料洩露風險。

一般建議

建議使用AES-256位元長度或更高，更快更安全性，是目前的建議選擇。

案例研究 2:弱加密 - AI修補建議

gamania CloudForce 雲力橘子

AI 資安顧問深入分析

架構理解　業務理解

考量系統與外部系統對接，加解密之演算法需要共同修改

4. **實施計劃與時間表:**

1. **清晰界定時間表**：明確界定過渡完成的時間範疇，並根據實施進程制定合理的時間表。
2. **監控與反饋**：在過渡期間，密切監控系統整合狀況，並確保有適當的反饋和異常處理機制。

5. **過渡完成與系統升級:**

當需要更改為更安全的加密算法，而該更改需受到外部系統的協同配合時，可以考慮以下建議步驟，以確保遷移過程的順利進行並最大化地降低風險:

1. **風險評估與需求確認:**

1. **風險評估**：評估現行使用的加密算法的風險程度，並界定因維持弱加密算法而可能暴露的安全性風險。
2. **需求確認**：確認新的加密算法所需的具體要求和外部系統需要配合的部分，確保皆有明確的規範條款。

2. **與外部系統協商:**

1. **協作溝通**：與外部系統的技術團隊進行溝通，具體說明更換算法的必要性以及新算法的優勢。
2. **共同制定計畫**：共同制定一個中短期的計畫，以確保雙方系統能夠順利過渡到新的加密算法。

3. **建立過渡方案與測試環境:**

1. **過渡階段設計**：設計一個過渡方案。通常可考慮雙線模式運行，即同時支援舊有與新的加密算法，在一定時間內支持雙向運行以便逐步遷移。

人機對決: Security Champion養成比較

真人Security Champion	AI Security Champion
目標 : 可以獨立處理8 成原碼弱點且不影響程式	
基準 : 開發經驗 2~3 年+ 資安經驗 1年	基準 : 現有常見 LLM 與 RAG 串接工具
學習方式: 富含開發經驗與資安經驗的security champion擔任指導者，以及修補資料自行學習	學習方式: 藉由修補資料與安全知識庫與LLM 選擇
參考資料: 現有修補資料	

人機對決:資安顧問養成比較

真人Security Champion

❌

- 培訓時間因人而異
- 人力成本較高

✅

- 訓練者看人成長成就感
- 根據情境靈活應變

訓練時間 9個月~1年

AI Security Champion

❌

-初期需要整理資料

-對非典型案例理解有限

✅

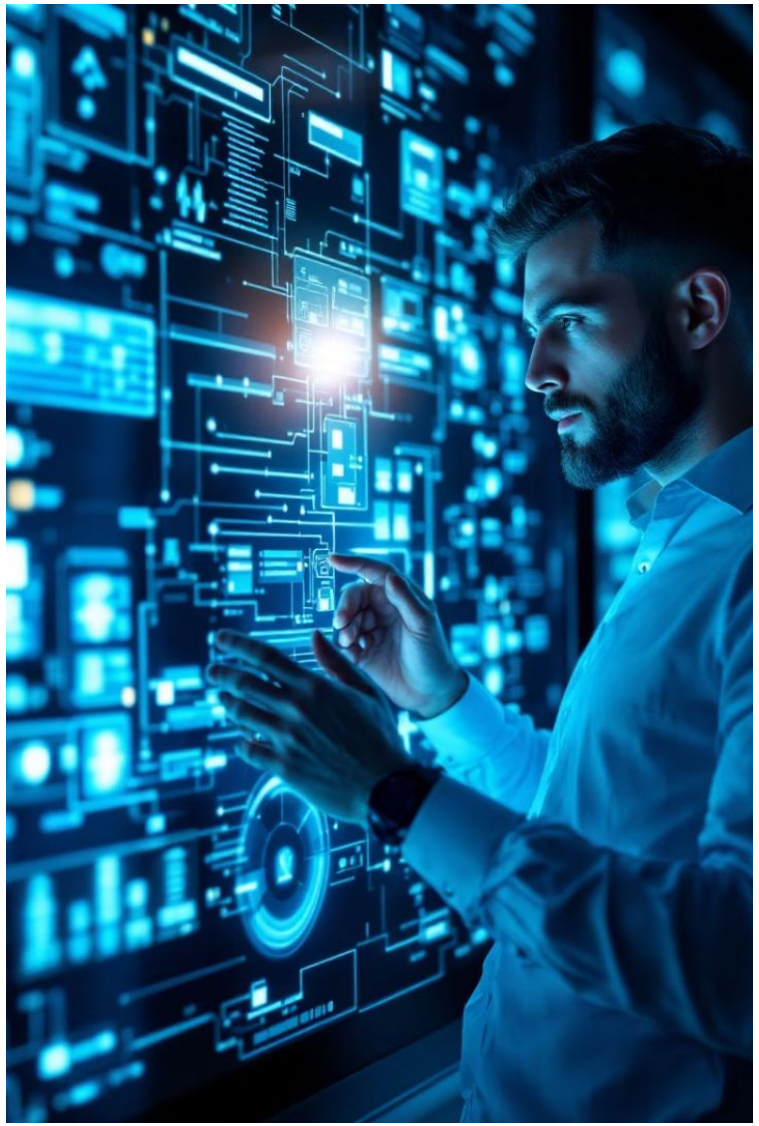
- 不同程式語言學習成本低
- 迭代速度快
- 7x24

訓練時間 2週

REF: https://www.tvtime.com/ja/show/185041

未來發展

願景：打造真正懂你的資安顧問



預測性

在漏洞形成前給出預警，主動識別設計缺陷。

適應性

隨系統演進持續學習，適應新技術和架構變化。

協作性

成為開發團隊的一員，與業務目標協同改善。

可解釋性

提供透明的建議理由，安全知識的傳遞與培養。

未來展望

gamania CloudForce 雲力橘子

讓 AI Review AI

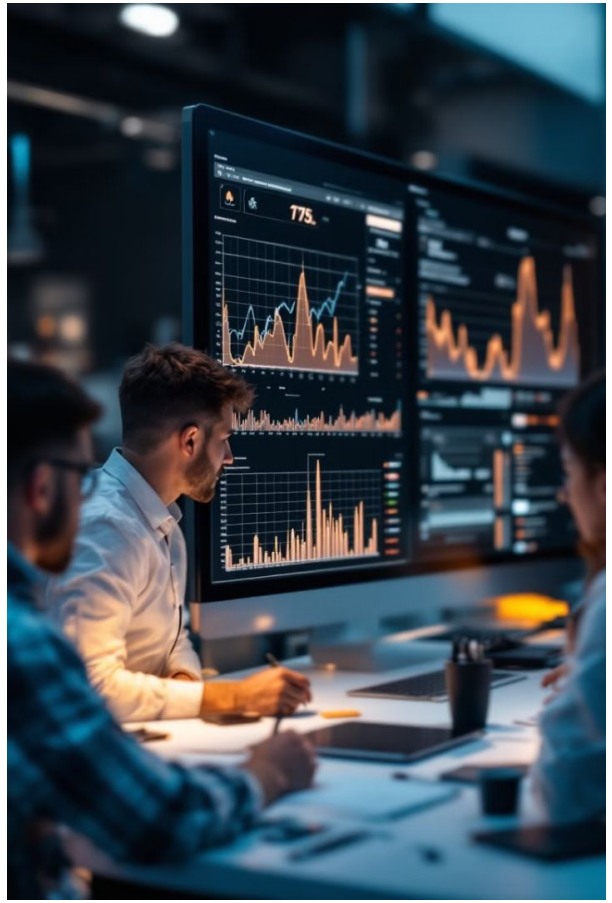
透過不同 LLM 來互相驗證回覆內容正確性

整合 CI Pipeline

進行程式碼進行Code review

整合 AI Agent

整合prompt 進開發Agent，給的建議就是沒有弱點的寫法



DevSecOps 和自動化安全檢測的敏捷導入

4/17 (四) 15:30 - 16:00 7F 701F

此議程將探討 DevSecOps 和自動化安全檢測的實施經驗，介紹如何在敏捷開發中整合安全檢測，並展示安全和效率可以並行不悖。聽眾將學到實際操作方法，並理解如何改變團隊對於資安檢測的傳統觀點。

講者

蔡龍佑 (Tygrus)

雲力橘子

技術開發二部 副理

Thank you for listening.