本課程歡迎企業包班~請來電洽詢 承辦人劉小姐 03-5743729

# AI 資安攻略：強化生成式 AI 資安防護力 以 ChatGPT 為例

## 課程簡介

生成式 AI 正在迅速改變我們的工作方式與生活環境，但它同時也帶來了新的資安威脅和挑戰。隨著生成式 AI 在企業運營、個人生活及公共領域的廣泛應用，理解其原理、應用場景與潛在風險已成為每人的必要技能，特別是從事資安相關工作者。

本課程將幫助學員**掌握生成式 AI 潛在的資安風險及應對策略**。透過模型範例**學習 LM Studio 操作，達到實踐提升對生成式 AI 資安的敏感度與防護能力**，確保在使用這項技術時，既能充分發揮其潛力，又能有效應對其風險。

## 課程目標

1. 瞭解生成式 AI 在資料隱私、偏見處理及使用者保護方面的做法，並學會如何評估其在實際使用中的安全性與可靠度。
2. 瞭解如何解決使用生成式 AI 工具時，可能造成之資料外洩、駭客攻擊與系統漏洞等資安問題，確保系統的安全性。
3. 學習在使用生成式 AI 過程中，如何遵守資料隱私、網路安全及智慧財產相關的法律法規，避免侵犯他人權益。

## 課程特色

1. 系統化的生成式 AI 資安風險概論。
2. LM Studio 操作及社交工程情境 ChatGPT 實際演練。

## 適合對象

1. 資訊安全人員
2. 內部稽核與電腦稽核人員
3. ISO/CNS 27001 輔導及建置相關人員
4. IT 和 MIS 部門有意強化資訊安全管理系統與稽核技能的從業人士

## 課程內容

| 時間 | 單元 | 內容 | 時數 |
|---|---|---|---|
| 114 年<br>6 月 11 日<br>(三) | 生成式 AI<br>簡介 | • 生成式 AI 簡介<br>• 生成式 AI 的運作原理與應用場景 | 2 |
| | 生成式 AI<br>教學及演練 | • 生成式 AI ( ChatGPT ) 使用教學<br>• 生成式 AI ( ChatGPT ) 演練 | 3 |
| | 生成式 AI<br>資安風險概述 | • 資安威脅全景圖 : 資料外洩、社交工程與攻擊向量<br>• 常見誤區與過度依賴的風險<br>• 隱私權(個人資料)保護<br>• 似是而非的生成內容 | 1 |
| 114 年<br>6 月 12 日<br>(四) | 建置<br>LLM 模型 | • 建置可在個人電腦上使用下載的 LLM 模型<br>• LM Studio 使用教學<br>• 選擇及安裝模型 | 3 |

本課程歡迎企業包班~請來電洽詢 承辦人劉小姐 03-5743729

| 時間 | 單元 | 內容 | 時數 |
|---|---|---|---|
| 114 年<br>6 月 12 日<br>(四) | 生成式 AI 的防護策略 | • 聊天記錄與資料的保護措施<br>• 資料加密與匿名化技術的應用<br>• 偏見處理、隱私權保護及使用者保護<br>• 智慧財產、知識產權與版權保護 | 1 |
| | 實戰演練與案例分析 | • 模擬演練：社交工程攻擊中的 ChatGPT 應用<br>• 資安事件處理流程演練<br>• 最新案例分析與專家解讀 | 1.5 |
| | 未來展望與行動計畫 | • 全球生成式 AI 資安趨勢分析 | 0.5 |

**註：因應天候或不可抗力因素，主辦單位有調整議程之權利。**

## 價格收費(含稅、午餐、講義)

| 課程原價 | 早鳥優惠價 | 團報優惠價 |
|---|---|---|
| 12,000 元/人 | 10,800 元/人 | 10,200 元/人 |

## 開課資訊

【主辦單位】: 工業技術研究院 產業學院

【上課日期】: 2025/6/11~6/12，9:30~16:30，共 2 天、計 12 小時

【上課地點】: 工研院 產業學院 新竹光復院區 1 館**(實際上課教室請依據上課通知函為準!)**

【招生人數】: 本班預計 20 人為原則，依報名及繳費完成之順序額滿為止。

【課程費用】: 課程學費、午餐、講義

【培訓證書】: 參加本課程之學員，出席率超過 80%(含)以上，即可獲得工研院頒發的培訓證書。

【報名方式】: 線上報名

【課程洽詢】: 03-5743729　劉小姐

【繳費方式】: 確定開班再付款，恕不受理現場報名和繳費。

**(一) 信用卡：**

繳費方式選「信用卡」，直到顯示「您已完成報名手續」為止，才確實完成繳費。

**(二) ATM 轉帳：**

繳費方式選擇「ATM 轉帳」者，系統將給您一組虛擬帳號「銀行代號、轉帳帳號」，此帳號只提供本課程報名者一人轉帳使用，若多人報名，且費用是由公司統一轉帳處理，請電洽本院，將提供專屬帳號！

【退費標準】: 學員於開訓前退訓者，將依其申請退還所繳上課費用 90%，另於培訓期間若因個人因素無法繼續參與課程，將依上課未逾總時數 1/3，退還所繳上課費用之 50%，上課逾總時數 1/3，則不退費。

## 貼心提醒

1. 參訓學員**需自備筆記型電腦**。
2. 為確保您的上課權益，報名後若未收到任何回覆，敬請來電洽詢方完成報名。
3. 為配合講師時間或臨時突發事件，主辦單位有調整日期或更換講師之權利。
4. 講義將於課程當天提供紙本，請尊重講師智財權勿外流。
5. 報名時請註明欲開立發票完整抬頭，以利開立收據；**未註明者，一律開立個人抬頭，恕不接受更換發票之要求，課程開始當天不得要求退費**。