

課程名稱：17695_企業數位韌性的 AI 新視野資訊與資安 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- **適合族群：**初學者與資安實務人員。內容聚焦於深層式 AI 在實務上的應用概念，適合想瞭解 AI 自動化資安維護與科技創新的學員。
- **能力門檻：**入門。無需複雜的前置專家背景，講師強調善用 AI 將技術轉化為一般人看得懂的語言。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：**生成式 AI 與資安自動化趨勢 — 介紹奧義智慧導入生成式 AI 的背景與面對駭客變種的解決思維。
 - **章節二：**AI 應用的核心四要素 (PET) — 闡述將 AI 視為「聰明的寵物」之概念，包含智慧 (Smart)、產能 (Productivity)、科技賦能 (Enabled technology) 與以人為本 (Human-centric)。
 - **章節三：**新型態身分安全與路徑模擬 — 解析面對 Identity Related compromise 的新式威脅，如何透過 Graph 與 AI 找出潛在特權問題。
 - **章節四：**資料收集與持續性聯訪網絡 — 探討鑑識等級原始資料 (Raw data) 的重要性，以及建構 Collective Intelligence (集體情報) 防護網。

3. 必備前置知識清單

- **基本資安觀念：**建議具備基礎資訊安全及常見網路威脅的概念，以便更好理解案例。
- **無特定工具軟體限制：**課程主要為經驗分享與概念解析，無須事先安裝特有軟體。

4. 專有名詞與概念辭典

- **聰明的寵物 (PET)：**講者對 AI 的比喻，強調 AI 必須具備 Productivity

（產能激增）、Enabled Technology（科技突破）與以人為本（T，對人類社會有所貢獻）的特性。

- **鑑識等級資料 (Artifacts / Raw data)**：指如同警方在犯罪現場拉封鎖線所採集的原始證物資料，未經二次處理，用以供 AI 學習與還原事實。
- **Identity Related Compromise**：新型態攻擊方式，指駭客不透過惡意程式，而是取得合法或信任帳號進行入侵。

5. 課程學習職能對照

- **對應職能名稱**：資安分析師 / 資訊安全規劃人員
- **主要工作任務/能力指標**：
 - [分析與決策能力]：能夠理解生成式 AI 於資安防衛中的應用邏輯，評估新舊資安架構的威脅路徑。
 - [工具操作與執行能力]：掌握鑑識等級原始資料收集原則，並評估如何透過自動化工具節省調查時間。