工業技術研究院
Industrial Technology Research Institute

生成式 AI 在資安防禦應用實戰

一、課程緣起：

隨著資安威脅的型態快速演化，攻擊者已大量運用 AI 技術加速弱點探勘、社交工程與攻擊流程，自動化駭侵已成為新常態。面對攻防落差日益擴大、資安監控人力不足、資安事件量暴增的挑戰，組織必須建立能有效整合生成式 AI 與資安分析的全新防禦架構。本課程旨在協助學員理解生成式 AI 在資安防護上的核心運作模式，並掌握 AI 可能帶來的新型風險與治理議題。同時透過 SIEM/Log 數據分析、ML 威脅偵測、AI 協助事件處理與防護建議生成等實務操作，協助學員真正將 AI 轉化為資安工作的效率槓桿，提升組織的事件處理速度、威脅偵測能力與防禦決策品質。

~本課程歡迎企業包班，請來電洽詢 課程承辦人 黃小姐 02-23701111#306 ~

二、課程目標：

本課程旨在培養學員以資安場景為核心，整合 AI 創新模式、資安防護、ML 異常偵測、SIEM 日誌分析、生成式 AI 工具應用。

三、適合對象：

資安工程師、SOC 分析人員、IT 基礎架構與系統管理人員、資安主管、風險管理與內控人員等

四、課程注意事項

請學員自備筆電。

五、課程日期：

115 年 8 月 12 日-8 月 13 日，週三四白天 9:30 ~12:30,13:30~16:30 ，共 2 天、計 12 小時。

五、課程大綱：

大綱
● 理解生成式 AI 與資安防護結合的核心模式與運作流程。 ● 掌握使用 AI 工具時的資通安全風險、隱私保護與企業內控要點。 ● 熟悉 SIEM / Log 的結構、資料型式與巨量處理挑戰。 ● 使用 ML 方法（異常偵測、分類）分析資安日誌與威脅行為。 ● 使用生成式 AI 協助進行威脅分析、事件調查與初步防禦建議。

*本課程歡迎企業包班~請來電洽詢 課程承辦人 黃小姐 02-23701111#306

- **熟悉 AI 防禦框架（MITRE ATLAS / MITRE ATT&CK for AI）與應用情境。**
- **實作 AI 工具於資安工作流程：**
  - **日誌摘要**
  - **威脅初步分類**
  - **生成事件報告**
  - **自動生成防護建議**
- **能評估 AI 導入資安作業時的風險與治理需求。**

* 課程執行單位保留調整課程內容、日程與講師之權利

七、課程費用與繳費：

1. 本課程費用含課程、講義、餐點。

報名方案	費用
課程原價 (每人)	$12,000 元
14 天前報名 優惠價(每人)	$10,800 元
14 天前報名+3 人(含)以上揪團同行 優惠價(每人)	$10,200 元

2. 課程若未如期開班，費用將全額退還。
3. 繳費方式
   - ATM 轉帳（線上報名）：繳費方式選擇「ATM 轉帳」者，系統將給您一組轉帳帳號「銀行代號、轉帳帳號」，但此帳號只提供本課程轉帳使用，各別學員轉帳請使用不同轉帳帳號！！轉帳後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」傳真至 02-2381-1000 林小姐 收。
   - 信用卡（線上報名）：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。
   - 銀行匯款(公司逕行電匯付款)：土地銀行 工研院分行，帳號 156-005-00002-5（土銀代碼：005）。戶名「財團法人工業技術研究院」，請填具「報名表」與「收據」回傳 itri462692@itri.org.tw 林小姐 收。
   - 計畫代號扣款(工研院同仁) :請從產業學院學習網直接登入工研人報名；俾利計畫代號扣款。

八、報名確認與取消：

1. 已完成報名與繳費之學員，課程主辦單位將於開課三天前以 E-mail 方式寄發上課通知函；若課程因故取消或延期，亦將以 E-mail 方式通知，如未收到任何通知，敬請來電確認。

2. 已完成繳費之學員如欲取消報名，請於實際上課日前以書面通知業務承辦人，主辦單位將退還 80% 課程費用。

3. 學員於培訓期間如因個人因素無法繼續參與課程，將依課程退費規定辦理之：上課未逾總時數三分之一，欲辦理退費，退還所有上課費用之二分之一，上課逾總時數三分之一，則不退費。

4. 本單位保留是否接受報名之權利。

5. 如遇不可抗拒之因素，課程主辦單位保留修訂課程日期及取消課程的權利。