STEM 與永續發展人才培育

【資安攻防與 AI 應用實戰班】

第 3 梯次

招生簡章

主辦單位 ｜ 國立陽明交通大學、陽明交大雷射系統研究中心

訓練領域 ｜ 數位資訊

訓練職類 ｜ 其他資訊專業人員

課程時數 ｜ 108 小時

課程時間 ｜ **115/3/31 (二)~115/7/30(四)**

上課時間 ｜ 每週二、四 晚上 18:30-21:30

上課地點 ｜ 遠距教學

訓練費用 ｜ **請加官方 line@ 諮詢。※本班為自費課程，無補助。**

報名期間 ｜ 即日起 至 115/3/26 (四) 23:59

課程諮詢 ｜ 陽明交大雷射系統研究中心 鄭小姐 0933-906-833 或
Email 至 nycuitstem@gmail.com
line@ 諮詢 ，或 Line ID 搜尋 @nycustem

招生網站 ｜ https://it.stem.lasercenter.nycu.edu.tw/

※本班最低開班人數：20 人

■ 課程簡介

在現今數位化的社會中，資訊安全已成為所有組織與個人不可忽視的關鍵課題。隨著網路犯罪、資料外洩及系統攻擊事件頻頻發生，如何保護資料隱私、維護系統穩定等，成為企業和個人的重大挑戰。而全球雲端市場的迅速擴張，企業將業務轉移至雲端已成為趨勢，同時開發並部署更多雲端應用雖帶來靈活性與效率，但也大幅提升了攻擊面，讓雲端安全防護變得更加複雜且具挑戰性。根據網路資安廠商 Fortinet 最新發布的《2025 年資安技能落差報告》指出，「資安技能落差」是資安事件增加的關鍵因素，超過一半以上的企業認為，包含員工缺乏資安意識、缺乏具備資安技能的人員，或缺少必要的資安產品或工具等，都是造成資安事件頻傳的主要因素。

工研院產科國際所預估，臺灣資安產值在 2025 年達 912.4 億元，年成長率 11.5%，預期 2026 年將有望挑戰 1,000 億元。根據 iThome 2025 年 CIO&CISO 大調查發現，每三家企業就有一家要招募資安人才，金融業徵才需求增加 3 成，服務業更高達 5 成（圖 1），顯現企業對於資訊安全愈加重視，也代表著全面提升員工資安意識、技術能力、事件應變能力與升級系統，是所有產業共同要努力的資安挑戰。

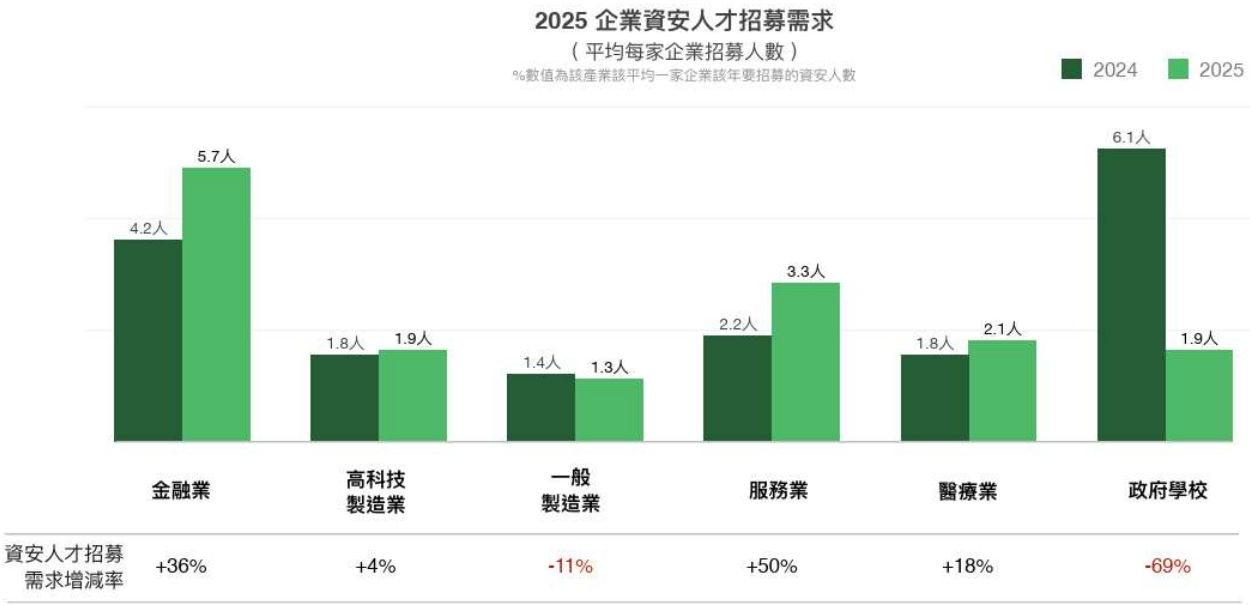

圖 1. 2025 企業資安人才招募需求

(資料來源：iThome 2025 CIO&CISO 大調查)

而為了因應 AI 所驅動的網路攻擊，愈來愈多企業採用 AI 技術來強化資安防禦。AI 的強大運算與分析能力，讓駭客能更快、更精準地尋找系統漏洞，同時也讓資安防護具備了前所未有的智能化與主動性。本課程將帶領學員探索資訊安全的基礎與實務，並學習如何運用 AI 工具提升防護能力與實現高效攻防對抗。透過全方位的知識講授與實機操作，本課程旨在讓您在 AI 與資安交織的時代下，掌握核心技能，應對未來挑戰。

課程規劃專為資安初學者設計，包含五大主要部分，涵蓋「基礎網路與系統概論」、「網站與網頁安全基礎」、「資料庫安全基礎」、「基礎網路安全」以及「資安防護基礎」。課程貫穿資訊安全知識與內容，每個主題主要以投影片講授基礎概念，並以實機操作示範；除講授理論也穿插實作練習，強調學員親自動手實作，搭配實驗環境的建立，如虛擬機、網路模擬、靶機系統等理論與實作並重的課程。

1. 學習基本資安攻防：透過本課程，將會教導學員如何將基礎資安防護應用在專業領域。
2. 練習與試錯：課程中會提供範例資料給學員演練，並搭配 AI 工具實作。

■ 適合對象

1. 不限職務，對作業系統、網站資訊安全、企業資安防禦領域有興趣者。
2. 想了解如何運用 AI 工具解決資安問題者。
3. 目前在職中或待業中 55 歲以下皆可報名。

■ 課程目標

1. 了解資訊安全的基本概念與核心知識。
2. 掌握基礎網路、網站、資料庫與系統的安全防護技巧。
3. 學習如何運用 AI 工具進行資安問題的分析與解決。
4. 能建立並操作虛擬機、網路模擬與靶機系統，進行攻防實作。
5. 為進階資安學習及相關職涯發展打下堅實基礎。

■ 課程特色及優勢

1. **專為初學者設計**：無需專業背景，從基本知識開始系統學習。
2. **理論與實作結合**：課堂講授基礎概念，並搭配實機操作與實驗環境。

3. **AI 工具輔助學習**：透過 AI 工具進行資安問題模擬與解決，提升學習效率。
4. **全方位資安基礎**：涵蓋網路、網站、資料庫與系統安全，紮實建立多面向基礎。
5. **動手實作強化**：設置虛擬機、網路模擬及靶機系統，模擬真實攻防場景。
6. 上課方式：概念引導與範例應用學習，部分課程搭配電子白板授課，提供課後講師筆記電子檔，課程皆會進行錄影，提供課後複習與練習。
7. 直播錄影課程可重複觀看至最後一堂直播結束後 2 個月。

★ 上課證明：課程依**班級評量方式達 70 分以上**，並**完成結訓意見調查表**，將由陽明交通大學雷射系統研究中心核發上課證明。

■ 就業展望

本班為初階課程，學員結訓後如有以下就業規劃，可修習進階課程或考取相關證照。

- 網路資安工程師、資訊安全工程師、資安測試工程師、資安管理(維護)工程師、滲透測試工程師、軟體測試工程師
- 資安分析師、資安顧問師、資安架構師、資安專案經理

■ 課前準備

電腦規格：

桌上型電腦或者筆電，RAM 至少 8GB（16GB 為佳），處理器至少 i5。

※講師課堂皆以 Windows 系統操作演練， Mac 電腦使用者請勿報名。

■ 報名方式

1. 成為 STEM 與永續發展人才培訓會員：報名參加訓練課程前，請先於網站會員註冊。
   （網站會員註冊：https://it.stem.lasercenter.nycu.edu.tw/register ）
   ※註冊之信箱請務必以常用信箱為主，避免重要通知信件無法正常收件。
2. 會員登入後，選擇要報名之課程：選擇課程進入課程介紹頁面，點選課程介紹頁面上方之「我要報名」。
3. 購買課程步驟：
   (1.) 確認訂單資訊：請確認選擇報名之課程名稱、價格及開訓日期。
   (2.) 選擇付款方式：可選擇 ATM 虛擬帳號付款或信用卡線上刷卡，依指示步驟完成付款。
   (3.) 完成報名：成功付款後，將會出現訂單完成頁面，訂單狀態及繳費狀態將會顯示「成功」，並會寄發繳費成功通知信，請務必留意。

4. 查看課程：會員登入後，點選會員中心之「班級總覽」，可以查看已報名的課程資訊，包含開課後之課程連結及學習平台連結等。
5. 開訓前通知：開課前三天內將會寄發課前通知信，包含課程相關社群資訊、課程連結、課表及課程規定等重要資訊，請務必留意信箱。

※如未收到通知信，請務必來電或以 Line@進行確認，以免錯失重要資訊。

■ 課程條款

學員報名後表示同意並遵守以下課程條款

1. 學員同意以下事項，若有違反任一條款，開課單位有權立即終止契約，並依退費條款退還款項，並保留追究法律責任的權利。
   - 學員應遵守課堂的基本秩序，包括但不限於：不打擾其他學員、不使用不當語言或行為、尊重授課教師及助教， 若有違反上開規定且經制止而再犯者。
   - 學員應對所有授課教師、助教、工作人員與其他學員保持尊重。任何形式的不當言語，如咒罵、咆哮、威脅、騷擾或人身攻擊均屬於不可接受的行為。
   - 學員以任何形式針對課程與開課單位進行惡意中傷或不實宣傳者。
2. 契約終止後，學員不得再參加開課單位所提供的任何課程或服務。
3. 學員同意開課單位，因課程執行或其他考量，可保留學員參加課程之權利，開課單位可將已經報名繳費的學員進行全額退費。
4. 開課單位保留隨時修改或更新本條款的權利，且毋須事先通知。學員若不同意修改後的條款，有權選擇終止契約，並依照退費條款進行退費。

■ 注意事項

1. 請各位學員自行準備筆電，並確保網路環境，以利上課所需。
2. 課程為直播授課，每堂課皆會錄影並上傳至學習平台供課後複習，為保護智財權，課程影片都有加密，建議使用 windows+chrome 或 Mac+chrome 上課。(手機或 ipad 平板無法看錄影課程)
3. 退費說明：

   (1.) 會員自報名課程至實際開課上課日前申請退費者，可全額退款。

   (2.) 自實際開課上課日算起未逾全期三分之一者，退還已繳學費之半數。

   (3.) 自實際開課上課日算起已逾全期三分之一者，不予退還。

   (4.) 退費方式：請於退費期限內提出申請退費，ATM 虛擬帳號繳費者需上傳本人身份證

照片以及在台金融單位存摺照片。

4. 為尊重講師之智慧財產權益，授課教師提供之上課教材請勿翻印或再製。
5. 如需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。

■ 課程大綱

課程名稱	課程內容/大綱	時數
網路基礎入門	1.網路基本概念 - 什麼是網路 - 網路類型介紹 - 基本網路術語 2.OSI 模型與 TCP/IP 協議 - OSI 七層模型基礎 - TCP/IP 協議簡介 - 常見通訊埠號 ▲實作：使用 Wireshark 觀察基本封包 3.IP 網路基礎 - IP 位址基本概念 - 子網路概念入門 - 基本的「IP 定址練習 - 實作：使用指令確認網路設定 4.基礎網路服務 - DNS 基本概念 - HTTP/HTTPS 基礎 - FTP 與 SSH 入門 ▲實作：基本網路連線測試	15
系統基礎入門	1.作業系統基礎 - Windows 與 Linux 系統介紹 - 檔案系統基本概念 - 使用者帳號概念	15

	2.Linux 基礎操作 - 基本 Linux 指令 - 檔案權限概念 - 基本的 Shell 操作 ▲實作：基本 Linux 操作練習 3.Windows 系統操作 - Windows 系統設定 - 基本安全設定 - 系統維護概念 ▲實作：Windows 安全性設定	
網站開發基礎	1.網頁技術基礎 - HTML 基本語法 - CSS 基本樣式 - JavaScript 入門 ▲實作：使用 AI 輔助撰寫基礎網頁 2.基礎網站安全 - 網站安全概念 - XSS 基礎防護 - CSRF 基礎防護 ▲實作：AI 程式碼檢測實作與基本安全防護	15
Web 應用程式安全入門	1.OWASP Top 10 基礎概念 2.基本的漏洞掃描 3.網站防火牆基礎 ▲實作：AI 輔助漏洞掃描	12
資料庫基礎	1.資料庫基本概念 2.SQL 基礎語法 3.基本的資料庫管理 ▲實作：基礎 SQL 操作	9

資料庫安全入門	1.SQL 注入基礎防護 2.基本的資料庫備份 3.簡單的權限管理 ▲實作：AI 輔助資料庫安全檢測與基本安全設定	9
網路安全基礎	1.基本網路攻擊類型 2.防火牆基礎設定 3.基本的 IDS/IPS 概念 ▲實作：AI 輔助威脅偵測基本防護設定	12
安全監控基礎	1.基本的日誌分析 2.簡單的網路監控 3.基礎事件處理 ▲實作：AI 輔助日誌分析與基本監控設定	9
基礎防護技術	1.基本的資安威脅 2.簡單的防護措施 3.基礎社交工程防範 ▲實作：基本防護演練	6
資安管理基礎	1.基本資安政策 2.簡單的事件應變 3.基礎資安意識 ▲實作：基本應變演練	6
總時數		108

※主辦單位保留調整課程內容與講師等之權利。

■ 課程規劃表

- 週二晚上 18:30-21:30；週四晚上 18:30-21:30
- 實際上課時間及課程連結，以開課前通知信為準

上 課 日 期	課 程 名 稱	時 數
115 / 3 /31 (二)	網路基礎入門(1)	3
115 / 4 / 2 （四）	網路基礎入門(2)	3
115 / 4 / 7 （二）	網路基礎入門(3)	3
115 / 4 / 9 （四）	網路基礎入門(4)	3
115 / 4 /14 (二)	網路基礎入門(5)	3
115 / 4 /16 (四)	系統基礎入門(1)	3
115 / 4 /21 (二)	系統基礎入門(2)	3
115 / 4 /23 (四)	系統基礎入門(3)	3
115 / 4 /28 (二)	系統基礎入門(4)	3
115 / 4 /30 (四)	系統基礎入門(5)	3
115 / 5 / 5 （二）	網站開發基礎(1)	3
115 / 5 / 7 （四）	網站開發基礎(2)	3
115 / 5 /12 (二)	網站開發基礎(3)	3
115 / 5 /14 (四)	網站開發基礎(4)	3
115 / 5 /19 (二)	網站開發基礎(5)	3
115 / 5 /21 (四)	Web 應用程式安全入門(1)	3
115 / 5 /26 (二)	Web 應用程式安全入門(2)	3
115 / 5 /28 (四)	Web 應用程式安全入門(3)	3
115 / 6 / 2 （二）	Web 應用程式安全入門(4)	3
115 / 6 / 4 （四）	資料庫基礎(1)	3
115 / 6 / 9 （二）	資料庫基礎(2)	3
115 / 6 /11 (四)	資料庫基礎(3)	3
115 / 6 /16 (二)	資料庫安全入門(1)	3
115 / 6 /18 (四)	資料庫安全入門(2)	3
115 / 6 /23 (二)	資料庫安全入門(3)	3
115 / 6 /25 (四)	網路安全基礎(1)	3
115 / 6 /30 (二)	網路安全基礎(2)	3

115 / 7 / 2 （四）	網路安全基礎(3)	3
115 / 7 / 7 （二）	網路安全基礎(4)	3
115 / 7 / 9 （四）	安全監控基礎(1)	3
115 / 7 /14（二）	安全監控基礎(2)	3
115 / 7 /16（四）	安全監控基礎(3)	3
115 / 7 /21（二）	基礎防護技術(1)	3
115 / 7 /23（四）	基礎防護技術(2)	3
115 / 7 /28（二）	資安管理基礎(1)	3
115 / 7 /30（四）	資安管理基礎(2)	3
	合計正課時數	108