115 年第 1 期資安防護實戰產業資安菁英班課程（臺北場）

課程計畫

一、 目的

為因應現代化網路環境中高度複雜與多變之資安威脅，協助各產業領域資安人員提升其防護應變能力，爰規劃辦理「資安防護實戰產業資安菁英班課程」，聚焦於資安防禦技術之實務應用與演練。

115 年第 1 期課程（臺北場）**聚焦於雲端安全與應用防護，以攻防對照思維為核心**，從紅隊攻擊視角理解威脅態勢，再導入藍隊防禦實務強化組織雲端體質，協助學員建立完整防禦策略。課程涵蓋雲端環境之滲透攻擊技術演練、IAM 稽核監控及事件調查機制建置，以及常見網頁應用程式弱點之防禦實作，並邀請資深資安專業講師授課。

二、 主辦/執行單位

- 主辦單位：數位發展部資通安全署
- 執行單位：社團法人台灣駭客協會

三、 課程日期與時間

本期課程共 4 天，日期分別為 115/05/30（六）－05/31（日）、115/06/06（六）－06/07（日）。

- 第一天：115 年 5 月 30 日（六）

課程主題	雲端安全實戰：紅隊攻擊與滲透
報到時間	08:50-09:20
開幕式(含參訓須知等)	09:20-09:30
課程時間(上午)	09:30-12:30
午休時間	12:30-14:00
課程時間(下午)	14:00-17:00

• 第二天：115 年 5 月 31 日（日）

課程主題	雲端安全實戰：藍隊防禦與建構
報到時間	09:00-09:30
課程時間(上午)	09:30-12:30
午休時間	12:30-14:00
課程時間(下午)	14:00-17:00

• 第三天：115 年 6 月 6 日（六）

課程主題	2026 年還在講網頁安全？
報到時間	09:00-09:30
課程時間(上午)	09:30-12:30
午休時間	12:30-14:00
課程時間(下午)	14:00-17:00

• 第四天：115 年 6 月 7 日（日）

課程主題	分組競賽
報到時間	09:00-09:30
分組與開賽說明	09:30-10:00
競賽時間(上午)	10:00-12:30
午休時間	12:30-14:00
競賽時間(下午)	14:00-16:00
計算分數、貴賓報到	16:00-16:30
頒獎典禮	16:30-17:00

四、 課程地點

臺北市進出口商業同業公會 IEAT 會議中心 1101 會議室（臺北市中山區松江路 350 號 11 樓）(實際地點仍以開課通知為準)。

五、 課程及講師資訊

➢ 課程一

課程名稱	〈雲端安全實戰：紅隊攻擊與滲透〉
課程講師	林殿智（Dange Lin）
講師簡介	林殿智（Dange Lin）現為奧義智慧科技的資深資安主任研究員，專精於機器學習、紅隊演練、車輛安全與雲端安全。除了在攻擊性安全領域的技術專長外，他也在資安管理方面擁有豐富經驗，並持有 CACSP 證照。 作為 DEFCON Malware Village 的共同創辦人，他積極為全球資安社群做出貢獻。他的研究與成果曾發表於 Black Hat USA/Europe、HITCON CMT/ENT、USENIX Security、CYBERSEC、MOPCON 及 ECCWS 等多場國際會議。 在研究之外，他也曾於 AIS3、HITCON Training 和 NICS 等活動中擔任講師。他同時也是資安教育桌遊「Cybercans」與「Cybercrete」的開發者之一。
課程摘要	雲端環境的普及帶來了新的安全挑戰，其中多數源於使用者對服務的錯誤配置。本課程旨在從攻擊者視角，深入解析雲端安全的核心問題。課程將從雲端安全概述與常見漏洞案例出發，結合 Cloud Security Alliance Top 11 等業界報告，剖析最新的雲端攻擊趨勢。 在實戰環節，本課程將聚焦於紅隊的攻擊技術與入侵步驟。學員將學習如何運用專業工具對雲端環境進行偵察（Recon）、竊取服務憑證（Credential Dumping），並利用 IAM 的配置弱點進行提權

	(Privilege Escalation)。此外，課程還將涵蓋如何在目標環境中建立持續性的潛伏(Persistence)手法。透過一系列的動手實驗，學員能掌握駭客滲透雲端的核心技術，學會主動發掘系統風險。
課程介紹	● 雲端安全概述 ■ 雲端計算的基本概念 ■ 雲端安全的重要性和挑戰 ■ 實戰演練：熟悉雲端環境 ● 雲端安全常見問題 ■ 使用者錯誤配置的影響 ■ 典型的安全漏洞案例分析 ■ Cloud Security Alliance - Top 11 ■ 雲端攻擊概念與最新攻擊趨勢 ● 紅隊攻擊技術 ■ 紅隊入侵步驟和工具介紹 ■ 紅隊如何滲透雲端環境 ■ Lab：雲端資源 Recon ■ Lab：雲端服務 Credential dumping ■ Lab：IAM 提權手法 ■ Lab：雲端環境 Persistence
學員先修技能	具備 Linux、網頁、雲端基本基礎知識即可
學員自備工具	VMware Workstation、VMware Fusion(Mac User 請使用非 M1/2 晶片之 Mac)，硬碟空間需求 30G 以上，記憶體 8G 以上

➢ 課程二

課程名稱	〈雲端安全實戰：藍隊防禦與建構〉
課程講師	林殿智（Dange Lin）
講師簡介	同課程一
課程摘要	了解如何正確配置與監控雲端服務，是防禦資安威脅的根本。本課程旨在建立學員全面性的雲端防禦能力，從基礎概念、常見問題分析，到完整的藍隊防禦策略。課程內容將結合雲端安全防禦框架與成熟度模型，幫助學員系統化地建構防護體系。 在實戰環節，本課程將聚焦於藍隊的日常維運與稽核任務。學員將學習如何盤點與審核 IAM 權限及可能外洩的憑證，並對不安全的組態設定進行稽核。更進一步，課程將指導學員如何建立有效的安全監控機制、設計應變措施，並在真實的雲端環境中進行事件調查（Incident Investigation）。透過這些實作練習，學員能掌握保護雲端資產的關鍵技能，為企業打造穩固的雲端防線。
課程介紹	● 雲端安全基礎與風險認知 ■ 從防禦者角度看使用者錯誤配置的影響 ■ 從真實案例學習防禦失敗的教訓 ● 藍隊防禦策略 ■ 雲端安全防禦框架與成熟度框架 ■ 藍隊工具整理與資源介紹 ■ Lab：IAM 盤點 ■ Lab：外洩憑證盤點 ■ Lab：不安全組態設定稽核 ■ Lab：安全監控和應變措施

	■ Lab：雲端事件調查 ● 雲端體質強化流程
學員先修技能	具備 Linux、網頁、雲端基本基礎知識即可
學員自備工具	VMware Workstation、VMware Fusion（Mac User 請使用非 M1/2 晶片之 Mac），硬碟空間需求 30G 以上，記憶體 8G 以上

➢ 課程三

課程名稱	**〈2026 年還在講網頁安全？〉**
課程講師	蘇學翔（Boik Su）
講師簡介	蘇學翔（Boik Su）現為奧義智慧科技的資安研究經理，同時也是知名資安社群 CHROOT 成員之一。 他專精於 Web 滲透測試、雲端安全及區塊鏈安全，且曾於 Virus Bulletin/HITB/OWASP AppSec/FIRSTCTI/HackerOne/HITCON 等國際知名資安研討會發表研究成果，也在 HITCON、NICS 等場合擔任 Training 講師。
課程摘要	課程中以最新版本的 OWASP Top 10 2025 切入，探討為何到今日，網頁安全仍舊是企業不可避免的課題。課程輔以大量練習題，因此學員將深刻體會到網頁安全在這幾年之間攻擊型態的轉變，以及如何提升防禦思維、防患於未然。

課程介紹	● 上午課程： ■ OWASP Top 10 2025 簡介及常用攻擊手法 ■ 案例演練 1（SQLi、Command Injection、XSS） ■ 進階防禦技巧、前沿漏洞利用（上） ■ 案例演練 2（1-day Vulnerabilities/LFI/XXE/SSRF/反序列化） ● 下午課程： ■ 進階防禦技巧、前沿漏洞利用（下） ■ 案例演練 3（Electron-based Apps/WebLogic/ASP.NET） ■ 案例檢討
學員先修技能	網頁安全基本概念
學員自備工具	無特殊需求

六、參訓資格

(一)授課對象為各產業領域之在職資安人員，包含金融、軟體、智慧製造、資安、法人/學校/醫院、特定政府機關及其他綜合產業，屬高階技術實戰培訓。

(二)具中華民國國籍，並擁有資安領域2年以上實務經驗。

(三)以企業資安技術人員、資安公司研發人員及其他單位資安技術人員為主要對象，但不限於此範圍。

(四)每一企業(公司)限兩名人員報名。

七、報名方式

(一)報名期限自即日起至115年5月17日（日）23時59分，請至課程活動報名網站填寫資訊（https://hitcon.kktix.cc/events/elite-industry-course ）。

(二)完成報名後將進行學員遴選，獲正取通知後始得參與課程。主辦單位保有是否錄取學員之權利，錄取結果另以電子郵件通知。

八、注意事項

(一)課程期間提供午餐。

(二)本課程學員須全程參訓，禁止由他人冒名頂替參與課程。課程上下課時間以講師實際授課情形為準。

(三)如報名錄訓後因故無法參訓，請於開課日前3天通知主辦單位，以利安排遞補。

(四)為保障智慧財產與著作權，課程中禁止拍照、錄影及錄音。學員自本課程所取得之課程相關教材，未經主辦單位授權同意，不得任意重製、傳輸、散布等受著作權法規範之行為。

(五)為課程結案需要，課程中將進行拍照紀錄。

(六)課程期間如遇不可抗力因素（如：颱風、水災、地震、疫情等，依行政院人事行政總處或中央疫情指揮中心公告）導致課程停辦或延期，異動資訊以主辦單位公告為準。

(七)為確保參與者之學習品質及達到培訓目的，並避免浪費訓練資源，若出席總時數未達 20 小時，該名學員將於一年內喪失參與數位發展部資通安全署及國家資通安全研究院所有活動之權利。

九、 課程聯絡窗口

(一)數位發展部資通安全署 黃繼民專案分析師

電話：02-2380-8743

E-mail：jiminhuang@acs.gov.tw

(二)社團法人台灣駭客協會秘書處

電話：02-2700-0073

E-mail：info.elite@hitcon.org