出國報告（出國類別：開會）

Black Hat 2025及DEF CON 33
資訊安全技術研討會

服務機關：內政部警政署刑事警察局
姓名職稱：劉怡汎偵查正、賴欣妤巡官
派赴國家/地區：美國內華達州拉斯維加斯
出國期間：114年8月1日至8月12日
報告日期：114年10月13日

摘要

本次參加Black Hat 2025與DEF CON 33兩場國際資安盛會，最大收穫是洞悉全球資訊安全領域的最新趨勢，並深入瞭解攻擊與防禦之前瞻技術。這不僅是資安專業人士交流知識與經驗的重要平臺，更透過實地演練與實務挑戰，強化參與者對網路攻防技術的理解與應變能力。在當今資安威脅日益嚴峻的情況下，這樣的學習與實作機會，對我們持續精進資安防護策略具有重大意義。

作為全球資安界的權威指標，Black Hat 聚焦於專業與產業應用，涵蓋從零日漏洞分析、物聯網安全、供應鏈攻擊防禦到最新的 AI 運用科技等多項關鍵議題。會中集結來自世界各地的頂尖研究人員、資安工程師與駭客，共同分享最新的攻擊技術與防禦策略。透過高品質的演講與實作導向的技術課程，我們得以第一時間掌握實戰技巧，並重新思考資安在現代社會中的戰略角色與價值。

相較之下，DEF CON 33呈現出更具開放性與互動性風格，現場設有多樣化的Capture The Flag（CTF）實戰競賽、互動式工作坊及主題 Village，參與者能親身體驗駭客攻防操作，並在實作中培養快速應變與問題解決能力。此活動充分展現駭客社群的創新精神與技術熱情，也讓人深入觀察到全球頂尖駭客團隊如何運用新穎手法進行攻防，對我們的實務操作與資安思維皆有極大啟發。

這兩場盛會幾乎可視為資安領域的兩大代表象徵：Black Hat 側重商業導向與技術前瞻，而 DEF CON 則體現駭客文化與實作精神。在 Black Hat 場內常見正式服裝與企業級主題，如新技術展示與產業應用；而 DEF CON 猶如一場結合

教育與娛樂的嘉年華，甚至以巨蛋演唱會形式作為開場，並設有模擬拆除炸彈、社交工程、破解門鎖及虛擬貨幣等主題展區，在場場精彩的情況下，真的有如進大觀園般感受到處處皆是驚喜。

此次參與不僅加深我們對資訊安全新技術與防護策略的理解，也開啟與國際資安專家的交流大門，建立寶貴的跨境人脈網絡。這些知識與經驗將可直接轉化為本機關在資安政策擬定、技術實施及科技偵查上的核心資源，強化我們因應網路犯罪的能力。同時，我們亦可從實作過程累積實戰經驗，有助於在未來面對複雜多變的資安挑戰時，提升系統韌性與應變效率，將風險與損害降至最低。

展望未來，我們將持續關注此類具國際指標性的資安盛會，不斷吸收新知、掌握技術趨勢，進一步強化本機關在資安人才培育、攻防體系建構及國際合作等方面的整體實力。

目錄

壹、會議介紹

一、會議名稱

(一)Black Hat USA 2025

(二)DEF CON 33

二、會議時間

(一)Black Hat USA 2025：2025年8月2日至8月7日

(二)DEF CON 33：2025年8月8日至8月10日

三、會議地點

(一)Black Hat USA 2025：曼德勒海灣渡假村會議中心（Mandalay Bay Convention Center）

(二)DEF CON 33：拉斯維加斯會議中心（Las Vegas Convention Center）

貳、參加會議目的

在全球數位化快速擴張的當下，資訊安全的戰略地位愈發顯著。無論是政府機構還是民間企業，皆須面對日益精密且不斷演變的網路攻擊手法。參加Black Hat 2025與DEF CON 33這類頂尖資安活動，對我們而言，是提升資安意識與實務能力不可或缺的一環。透過深入接觸最新的攻擊技術、防護工具與應變機制，我們得以強化自身對潛在威脅的辨識與回應能力。

當今的資安風險不再僅止於單一系統漏洞，而是呈現高度複合性，例如勒索病毒程式、零時差攻擊，以及潛伏於供應鏈中的滲透行為，皆使防禦難度大幅提升，面對這類風險，我們必須從源頭理解其原理與發展趨勢，才能有效制定對策。Black Hat 2025提供涵蓋漏洞發掘、攻擊模擬、威脅追蹤與對應措施等全方位技術課程，有助於快速強化我們在實戰場景中的判斷與處置能力；而DEF CON 33所設計的模擬競賽與主題區域，更讓我們得以在情境式的操作中累積實戰經驗，深化對攻防過程的理解。

此外，隨著政府部門與關鍵基礎設施加速數位轉型，網路攻擊所帶來的潛在衝擊亦逐步升高，在這樣的背景下，參與國際性資安交流活動，不僅能掌握全球最前瞻之研究成果與防禦策略，更有助於建立與國際資安社群的合作橋樑。透過實地觀摩與跨域討論，我們得以將最新經驗帶回機關，作為制定內部資安政策與導入技術之依據。

總結來說，此行重點不只係技術層面的學習，更著眼於培養科技偵查的核心能力，為未來面對跨境資安威脅與複雜攻擊模式做好準備。我們期許，透過這樣的參與學習，能進一步強化我方在資安應變、偵查與政策推動上之整體量能。

參、會議行程

一、行程表

Day1：114年8月1日自臺灣桃園國際機場搭機至美國洛杉磯國際機場轉機至美國麥卡倫國際機場

Day2：114年8月2日參加Black Hat USA 2025訓練課程「Tactical Recon for Pentesters-2025 Edition」第一堂

Day3：114年8月3日參加Black Hat USA 2025訓練課程「Tactical Recon for Pentesters-2025 Edition」第二堂

Day4：114年8月4日參加Black Hat USA 2025訓練課程「IntelTechniques 2-Day OSINT Training」第一堂

Day5：114年8月5日參加Black Hat USA 2025訓練課程「IntelTechniques 2-Day OSINT Training」第二堂

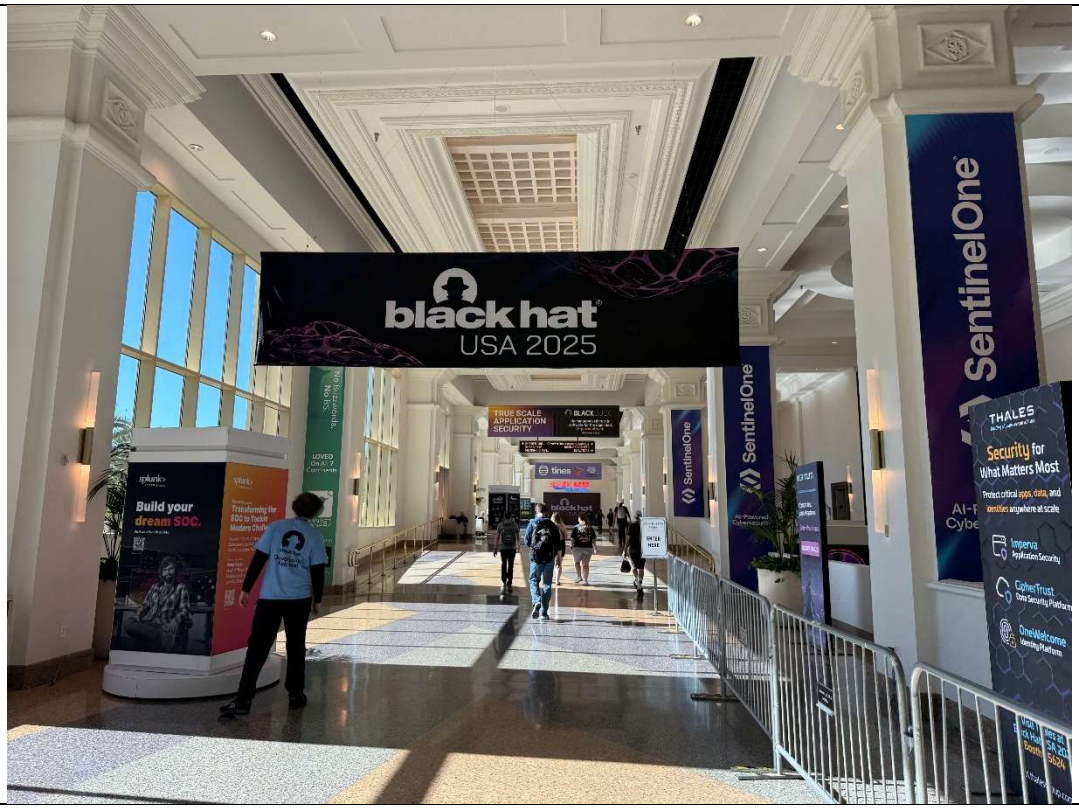
Day6-Day7：114年8月6日至8月7日參加Black Hat USA 2025研究簡報議程

Day8-Day10：114年8月8日至8月10日參加DEF CON 33研討會

Day11：114年8月11日自美國麥卡倫國際機場搭機至美國舊金山國際機場轉機至臺灣桃園國際機場

二、Black Hat USA 2025

Black Hat USA 2025是全球頂尖的資安會議之一，活動前四天提供多場專業訓練課程，主題涵蓋滲透測試、AI、IoT 與應用安全等，適合不同層級參與者。接續兩天上場的是主會議，將舉行百場以上的研究簡報（Briefings），探討最新漏洞、惡意程式、紅隊技術等。參與者也可進入Business Hall，與四百多家資安廠商互動，參加產品展示、現場演示（Arsenal）與講座。整體而言，Black Hat USA 2025是結合技術、實務與產業洞見的資安年度盛會，適合研究人員、業界專才與決策者參加。



前往 Black Hat USA 2025會場通道

- **專業訓練課程（Trainings）：**

Black Hat USA 2025的專業訓練課程為期四天，設計目的是讓資安專業人士透過高強度的實務訓練，強化技術能力與實戰經驗。課程由來自全球的資安專家授課，主打深入實作、即學即用，適合不同資歷與領域背景的學員。

訓練內容涵蓋廣泛，包含滲透測試、漏洞開發、惡意程式分析、逆向工程、藍隊防禦、紅隊技巧、Web 應用安全、行動裝置與物聯網安全、雲端防護與 AI 應用於資安等主題，課程均由 Black Hat 訓練審查委員會嚴格挑選，目的是培養新一代資安專業人才，使其能有效應對日益複雜的網路威脅。有的課程聚焦特定工具與平臺，也有針對特定產業的定制課程，

學員需自備筆電與指定軟體環境，所有訓練課程皆是資安從業者在短時間內強化技能、接觸前瞻技術與實踐經驗的極佳機會。

- **研究簡報（Briefings）：**

Black Hat USA 2025主議程正式從8月6以演唱會形式盛大展開，營造強烈的開場效果。首場Keynote主題為「Three Decades in Cybersecurity: Lessons Learned and What Comes Next」，由資安研究先驅 Mikko Hypponen 擔綱演講，回顧近三十年惡意軟體演化與重大攻擊事件，並展望未來威脅趨勢。緊接 8 月 7 日，Keynote 包括由Nicole Perlroth的「The New Frontline: Cyber on the Precipice」，深入描繪當前惡意工具的演變與 AI 的攻擊影響。

現場除 Keynotes 之外，主會議還包含超過百場的研究簡報（Briefings），由Black Hat黑帽評審委員會挑選，主題涵蓋AI 安全、漏洞開發、逆向工程、雲安全與硬體攻擊等。Black Hat USA 2025 Briefings結合高格調開場 Keynotes、主舞臺主題演講與超過百場創新技術簡報，構建成一場兼具洞察與深度的資安盛會。

Black Hat USA 2025盛大開場

- **商業展場（Business Hall）：**

Black Hat USA 2025的 Business Hall 是這場資安盛會的重要核心，設立旨在打造一處兼具技術展示、業界交流與產品體驗的集中舞臺，讓來自全球的資安專業人士能與領先技術供應商面對面互動，並掌握資安市場最新趨勢。展區匯聚超過四百家資安廠商參展，包括企業巨頭與新創公司，各自透過展位展示解決方案、進行工具演示，強調 AI 防禦、雲安全、供應鏈安全等新興熱門應用領域。

此外，展場特設多個專業區域，如 Arsenal Labs 區提供研究者與開發者示範開源工具、進行實作互動的場域，Community Lounge 區促進社群交流與非正式互動，Drone Zone 區則是今年新增的互動空間，允許參與者挑

戰無人機駭入與實戰 CTF 等活動。Business Hall 不僅是一場產業展示，更串聯技術、創新與人脈網絡，是資安專業人士探索最新工具、洽談合作與擴展視野的重要平臺。

（一）訓練課程—Tactical Recon for Pentesters-2025 Edition

- **課程背景介紹：**

此課程介紹滲透測試之各階段，各種用於執行偵察的工具和技術，以針對現代基礎設施發動攻擊，並深入探討各種從網路中取得資訊的方法，除了解各工具、網路資源等，亦透過講師建立之案例實際操作工具，不僅關注開源情報 (OSINT)，亦介紹如何利用早期階段收集的資訊來制定深入的攻擊策略、如何在攻擊情境中利用取得的資訊，以多種方式在防火牆之外的組織網路中獲取初步立足點，並進一步利用訊息來獲取並維持更高的訪問權限。

- **第一日—理論與駭客思維的導入：**

第一天的課程主要介紹及實作開放來源情報 (OSINT) 之蒐集，各企業目標有不同數位資產，如網域、雲端、IP 等，這些資產有可能暴露於公眾，可透過蒐集情資建構企業相關資料，針對目標了解各攻擊面，再針對各攻擊面進行情資蒐集，而透過 OSINT 可以蒐集到各式資料。蒐集資料之過程會花費許多時間，但從蒐集到之資料可了解目標對象之各漏洞，包含網頁漏洞、第三方工具漏洞、社交工程，當蒐集之資料越全面，實際展開攻擊時便有越多突破口及線索可使用，而蒐集之資料除了以目標對象擁有的漏

洞外亦包含組織架構、人員等，蒐集之資料亦有賴整理成表，將各類情資分門別類，以便於攻擊時快速有效利用。

一開始的建立攻擊面可以使用 whois、Reverse Whois、Nslookup 等工具，這些可透過下指令的方式取得資料，如 dig 指令可以解析網域，進而取得更多 IP 位址等，TLD (Top Level Domains, 如.com/.org 等) 掃描可以取得更多 IP 網址，因企業常購置多個 TLD 以確保其品牌名譽或符合各國法規語言而設立不同 TLD，TLD 掃描可利用指令 tldbrute。當網域蒐集到一定程度，接下來進行子網域的蒐集，子網域通常較容易存取，可使用的工具如搜尋引擎、暴力破解、Shodan 網頁等，搜尋引擎可利用其語法進行進階搜尋，如利用「site：目標.com -help -business」刪減不必要之網頁，當多項工具無結果時可利用暴力破解 DNS 取得資料。取的一定程度之攻擊面後便可開始評估手上的資料是否有 API 端點、機敏文件、可能的弱點、其他子網域等。

- **第二日—進階實作與無線攻擊技術：**

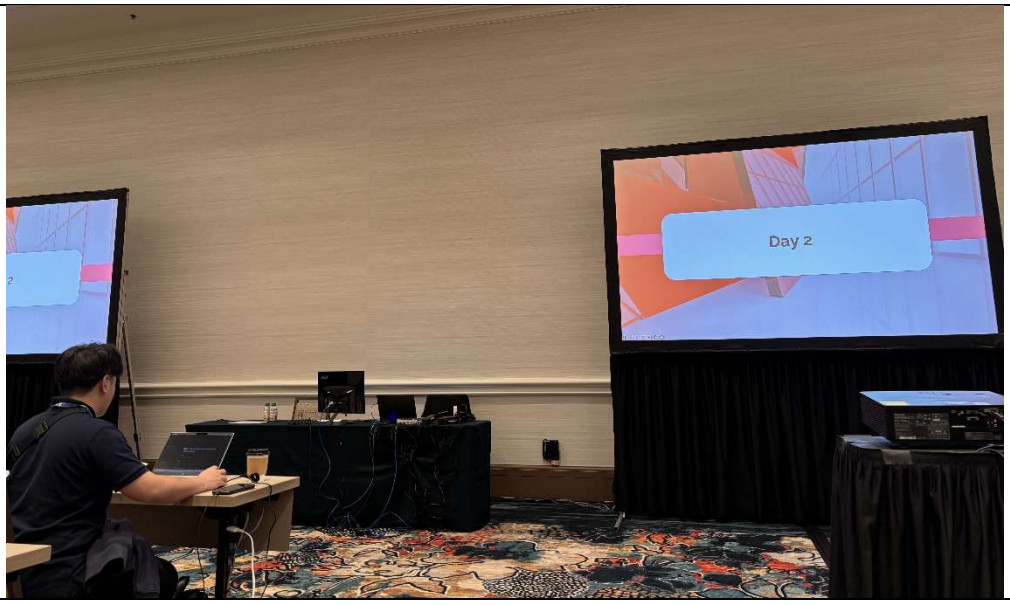
第二天課程開始進行目標滲透，在蒐集完各項資料後，透過這些資料進行各種滲透測試，可使用之工具為 Metasploit，其最常使用之模組有 Auxiliary、Exploit、Payload 等，操作練習使用 Auxiliary 模組進行 SSH 之暴力破解，暴力破解可用前期蒐集之憑證密碼進行暴力破解，在進行各種滲透時以蒐集到之資料進行嘗試，也顯得資料蒐集的廣度及深度極為重要；Source code 常用於各企業，透過如 Github 等平臺可瞭解相關程式之組織架構、是否有漏洞等，有助於增加攻擊面，甚至利用論壇上之程式碼進行攻

擊。

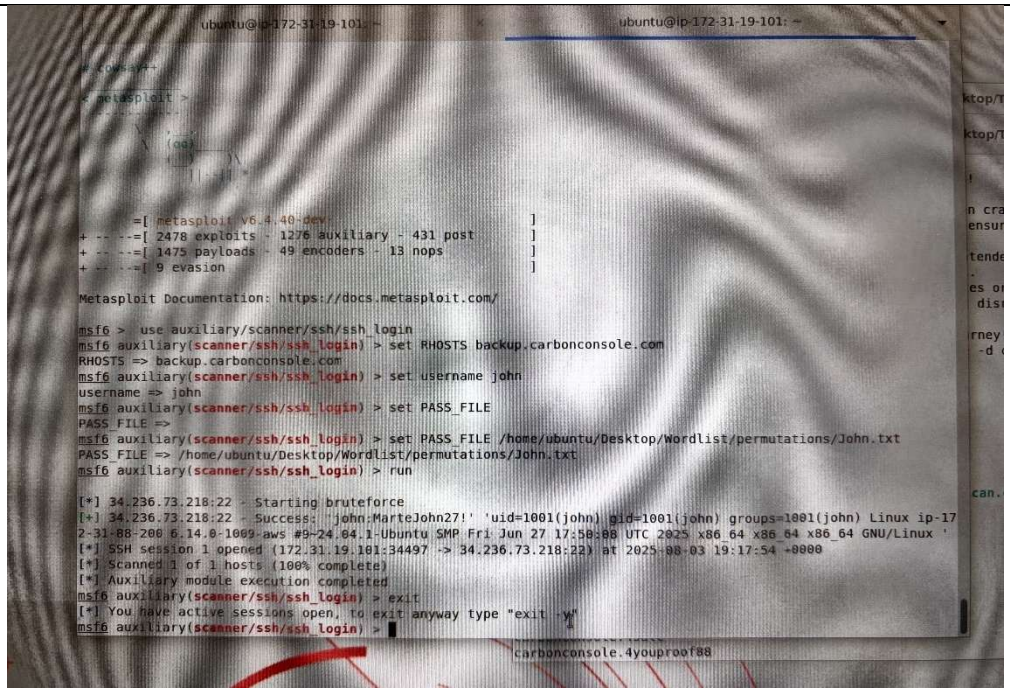
最後也提到社交工程的操作方法， 這部分也很需要前期情資蒐集，藉由各種情資建造適合目標企業之社交工程，最常見的是釣魚連結、釣魚郵件等，如何使目標企業相關人員點擊，內容、標題、連結等皆有其學問，如連結可利用 Typosquatting，將使用者常用或可信連結之字母替換成其他類似字樣，如英文字母 o 換成數字0，或英文字母 l 換成數字1等，更容易讓使用者點擊，再透過工具追蹤目標之後續動作或取得更多資料，另外進行中間人攻擊時可利用工具 Evilginx 3.0，在遇到雙因子驗證時利用蒐集的憑證嘗試繞過驗證。

- **課程特色與學習成效：**

本課程完整教學整套攻擊流程，資安攻防上了解紅隊思維也是很重要的，透過該課程可熟悉攻擊者可能使用之漏洞、工具等，也了解情資蒐集至關重要，也將是企業組織應加強防禦之面相。課程的一個示範令我印象深刻，在針對目標企業組織架構漏洞進行攻擊時，出現一管理者之名字，利用前期蒐集該管理者之資料及憑證密碼，即成功取得管理者權限，在前期蒐集資料時花費大量時間取得各樣資料，在實際操作滲透並運用各種資料才真正了解這些資料是如何運用。



課程實景



實際操作畫面

（二）訓練課程—IntelTechniques 2-Day OSINT Training

- **課程背景介紹：**

「IntelTechniques OSINT 訓練課程」是 Black Hat USA 2025所精選的實務

導向課程，專為想深入瞭解開放來源情報（Open Source Intelligence, OSINT）技術之人士所設計。課程由知名 OSINT 專家-Jason Edison 主講，透過實際操作與案例分析，深入介紹在合法、合規框架下如何從公開網路中有效收集、分析並驗證各類資訊。內容涵蓋進階搜尋技巧、社群媒體調查、網站元資料挖掘、影像與地理定位分析等主題，並搭配專業工具與腳本的實作練習。學員可依自身興趣選擇參與實作或僅觀察課堂示範，課程也提供完整教材供課後練習與延伸學習。無論是資安從業人員、調查記者、執法人員等，或是對數位足跡分析有興趣之專業人士，課程皆能提供實用的 OSINT 能力，協助在快速變動的數位環境中掌握重要情報。

- **第一天課程重點：基礎建構與資料捕獲流程建立**

1. 開場與倫理、法律之考量

   課程一開始，講師會介紹 OSINT 的基本概念與目的，討論調查中該遵守之法律、政策與倫理框架（例如隱私保護、資料來源合法性、使用者同意等），強調學員切勿因為錯誤工具或調查管道而觸犯所在地區之法律規範。

2. 整體課程架構與工作流程概覽

   介紹這兩天課程會涵蓋的25個模組，以及如何從初學者階段逐步進入中高階：從設置工作站、帳戶維護、工具與模板、到最終的文檔與報告撰寫流程。此階段講師會解釋如何管理工作流程（Workflow），保持筆記與紀錄以便後續複查與報告。

3. 環境與工具設置

   學員將學習如何設置操作環境，包括作業系統（Windows 、Mac 或 Linux 虛擬機）與必要工具安裝，建立調查工作用帳戶（電子郵件、社交媒體、虛擬機中的使用者帳戶等），準備筆記模板、案例追蹤、報告格式、來源註釋、OneNote 或其他記錄工具之使用。

4. 資料搜集技術：搜尋引擎與基本工具

使用 Google operators、Yandex、SearXNG、自建搜尋引擎等技巧以學習精準查詢，學習如何利用 ArchiveBox 或相似工具進行網頁封存保存，進而查詢網頁快照及網頁檔案，以回溯方式取得調查情資。

5. 人物識別與網址、使用者名稱、電話及電子郵件追蹤

學習如何從真實姓名搜尋未公開資料，使用公開紀錄、財產登記、公司登記等，以及利用免費郵件、臨時郵件、Header analysis 等介紹電子郵件查找技巧；運用使用者名稱工具與腳本比對同名使用者、相似帳號，並從社群媒體、論壇等追蹤使用者名稱，最後是透過公開電話簿、反向電話查詢網站等追蹤電話號碼使用者。

6. 社群媒體調查基礎

調查社群媒體 Instagram、Facebook、X、TikTok 等平臺的資料與行為模式，從公開貼文、活動、朋友及關係網絡查看使用者之網路行為與時間模式，並進行地理定位提示（如地點標記、照片內部地理資訊）與偽造地理位置之挑戰。

7. 實作練習與案例演練

在第一天學員就會進入實作環節（Individual & Team Exercises），使用模擬目標或真實場景來練習前述資料擷取與搜查技巧，包括從設定調查問題、搜集資料、保存快照、識別潛在重要線索等。講師會在最後回顧整天所學重點與難點，分組分享困難與解決方法，講師也會給出一些練習題或預習內容，例如思考如何查找資料洩露（Data Breach），以及準備照片、影片來源據以驗證等情境。

- **第二天課程：進階分析工具與成果呈現**

1. 影像與影片驗證

課程一開始會深入講解圖像與影片的驗證技術，學員將學習如何使用反向影像搜尋工具（如 Google Images、Yandex、TinEye 等），來確認圖片是否為原創或經過修改。此外，講師說明如何讀取與分析圖片的 EXIF（元資料），從中提取拍攝時間、地點、設備等潛在線索。影片部分則會操作像是 ffmpeg 等開源工具來截取影片片段，分析畫面細節，甚至進行影片來源比對，這些技術在揭露假新聞、詐騙活動或追蹤網路活動來源時，極為實用。

2. 地理與地圖資源、組織文件與企業調查

有關於地理與組織資料分析的模組課程，講師將說明如何運用

Google Maps、OpenStreetMap 等公開地圖情資，判讀照片背景或社群貼文中提到的地理位置，進一步還原真實世界中的活動軌跡。同時，也會帶入企業與組織背景調查的技巧，例如透過公開公司登記資料、域名註冊、營業地址等資訊，建立一個機構的組織架構圖，甚至探索背後的商業關係與利益鏈結，此部分對於企業調查、競業分析與風險評估等尤其重要。

3. 洩露（Break-Ins、Stealer Logs）等資料來源與分析

課程內容來到更具挑戰性的主題：資料洩露與入侵後留下的網路足跡運用。講師介紹常見的資料洩露型態（如 breaches、leaks、stealer-logs），以及如何透過合法管道取得這類資料，方便進行過濾、清理與分析。舉例來說，從某個 stealer-log 中可能發現特定使用者曾登入過可疑平臺，或者是暴露關鍵帳號密碼，講師將會操作範例資料，利用正規表示法（Regex）或指令列工具，進一步篩選出有價值的欄位資訊供後續比對與調查。這部份課程內容有助於支援資訊安全事件調查，也能應用於詐騙帳號識別、身分冒用風險控管等情境。

4. 工具與腳本使用與自訂

工具與腳本模組的實作應用，講師會示範如何自訂或整合開源 OSINT 工具，並建立一個整合型的虛擬調查環境（本次課程使用 Kali Linux），把常用腳本與工具集結安裝於一個乾淨、隔離的系統環境中，提升調查效率與安全性。講師進一步講解如何將某些查詢流程自動化，例如批量查找帳號使用紀錄、驗證電郵與電話號碼的使用歷史，或是比對圖像相似度等，這些內容不但提升調查規模，亦讓我們能更容易與團隊成員複製及共享調查流程。

5. 安全與隱私防護

在進行 OSINT 調查的同時，確保調查者本身與所掌握資料的安全性至關重要。講師於課程中介紹一系列實用的防護措施，包括使用加密容器（如 VeraCrypt）來保護敏感資料，配合良好的密碼管理習慣與工具，確保帳號不易遭破解，同時透過虛擬私人網路（VPN）與分段網路（Segmented Networks）隔離與防止潛在入侵。此外，講師也說明如何管理虛擬電話號碼（VOIP / SMS）及進行匿名域名註冊，並操作路由器韌體的替換與強化，以降低被追蹤或反調查的風險。最後，講師強調如何識別錯誤資訊與假訊息的操縱手法（Disinformation Tactics），並訓練我們在調查過程中保持資訊判讀的敏銳度，避免落入錯誤敘事的陷阱。

6. 報告與簡報製作

課程最後回歸成果整合與報告製作，講師說明如何撰寫標準化的 OSINT 報告，包括註明來源、分析結論與附錄資料，並提供各類報告模板，協助我們依照不同用途（執法簡報、客戶交付、內部紀錄等）產出格式一致、資訊清晰的成果文件檔。此外，講師也有演示簡報技巧，包含如何用視覺化工具呈現複雜資料，如組織架構圖、資料流程圖、時序圖或地理事件分布圖，協助我們如何讓受眾快速理解簡報的情境脈絡。

7. 最終實作練習與回顧

講師總結兩天所學的重點，並提供未來進階學習資源建議，包括 IntelTechniques 的線上課程模組補充、工具更新追蹤管道及常見 OSINT 社群平臺與線上競賽活動網站。講師期許我們在結訓後，能具有獨立進行 OSINT 調查之能力，並具備應用於實際工作或業務場景的完整分析能力。

IntelTechniques OSINT 課程實景與講師 Jason Edison

（三）主題演講

- Behind the Screen: Unmasking North Korean IT Workers' Operations and Infrastructure-SttyK

本場演講揭露北韓（DPRK）遠端 IT 工作者的組織結構、操作工作流程、所使用的工具、通信平臺、身分偽造與隱匿 IP、地理位置的方法等細節。舉例來說，他們可能註冊大量假身分、履歷、作品集（GitHub、LinkedIn 等），也可能使用 AnyDesk、VPN/代理/RMM（Remote-management）工具，或者借助筆電農場（Laptop Farms）作為設備中介，以使操作者身處國外時，仍能使用看似正常的本地網路環境，並將收入匯回北韓以支援該國政府與其軍事或武器計畫。

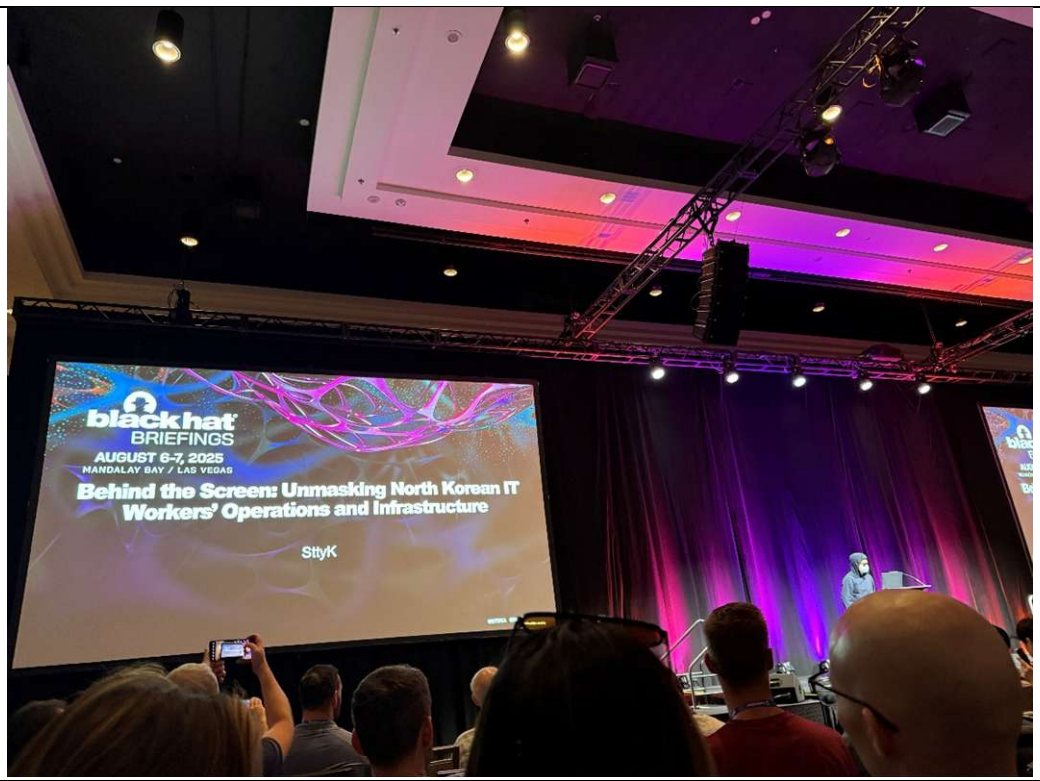
演講中也提到這些「假」工作者如何與企業溝通、面試時語言與書寫風格上的特徵，例如履歷與求職信中的不自然語言、過度使用標點符號、混用語言、偏好 emoji 等），藉此分析可疑徵才案例。

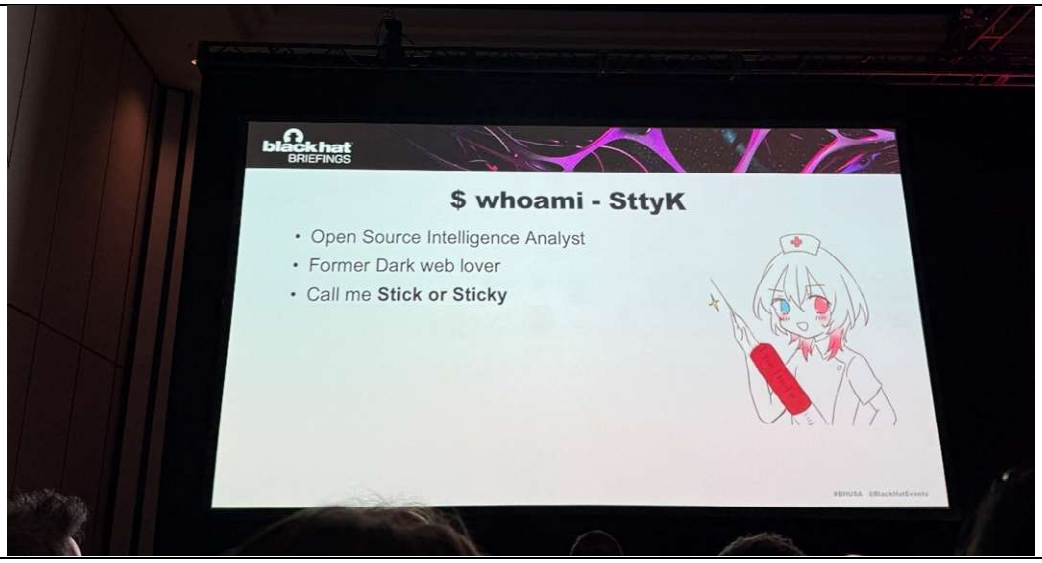
主講者「SttyK」是開源情報 OSINT 研究分析師，其透過收集與分析洩露文件、公開平臺上的資料、招聘/履歷資料與通信紀錄等外部材料，研究北韓 IT 工作者、遠端工作者的運作方式。在演講中 SttyK 展示從洩露來源取得的10+GB 資料，包含上千封郵件、招聘/求職紀錄、聊天紀錄等，並藉此繪製出北韓 IT 工作者，在全球範圍內如何被分組管理、如何利用偽造身份、假文件、中介人及設備農場來運作的組織圖譜，這些發現為首次在此

種細節程度上，讓外界看見這樣隱秘運作機制的內部運作。

這場演講填補了公開知識中一個長期模糊的空白，雖然外界已知道北韓透過駭客、APT、加密貨幣等方式賺取外匯，但關於如何以假 IT 身分形式系統性地滲透西方企業，並獲取收入與敏感資料，細節上很多都是保密或猜測。然而 SttyK 的研究提供具體證據，這對資安社群理解「內部威脅」的風險非常重要。

對企業來說，這種威脅不單是技術安全問題，也牽涉到招聘流程、背景調查與供應鏈安全。從國際政策與制裁的角度，這場演講也凸顯北韓如何在制裁之外創造收入管道，以及如何利用全球化的互聯網工具與平臺運作，這些對於制定政策、執法機構如何追蹤、辨識與打擊偽冒身分等工作是非常有參考價值的。





SttyK 演講實景

- Peril at the Plug: Investigating EV Charger Security and Safety Failures-Trend Micro: Jonathan Andersson / Thanos Kaliyanakis

本場演講主要在分享演講者及其團隊針對電動車充電樁安全性的研究與實驗，他們發現目前是市面上之充電樁存在安全性問題，有心者可利用漏洞取得操控權並進一步進行破壞，且經實驗後成功使多臺充電樁因溫度過高而著火，可見其危險性。

在進行攻擊前應先了解各充電樁之構造、組成，多數充電樁皆有手機 App 可進行操作，藉由解析 App 程式、資料可了解充電樁之各項資料，另外充電樁的充電阜易有漏洞，利用該漏洞可解析充電樁資料，另外其硬體迴路亦存在風險，且其處理器應接收外部訊號而增加攻擊面，在充電樁內部安全未完善的情況下更容易使攻擊者有突破口。在了解充電樁的軟硬體風險後，講者介紹其可能帶來的危害，如竊取電力、個資外洩、濫用充電樁

的運算能力、攻擊雲端等。

演講者現場播放各實驗影片，可清楚看到在破解漏洞並取得權限後可操控充電樁的設定，影片示範隨著電流的提高，充電樁的溫度也升高，當到達一定溫度時便開始著火，即使隨後跳電，火勢也已造成損害，若車子與充電樁連接，其後果不堪設想，且演講者示範多種廠牌之操作攻擊，每支影片皆成功讓充電樁著火，其伴隨的附加風險是電纜的著火，甚至有無法承受其熱度而開始融化支電纜，另可能有有毒物質釋放，然這些損害皆可能發生在日常生活中。

現今電動車愈來愈盛行，公共空間及自宅皆有裝設充電樁，但這些充電樁藏著已知漏洞，並可能造成危害，且透過演講者的影片可知是真正能施行的攻擊，這些漏洞雖已知但也有其緩解方法，講者提到相關作法有：讓充電樁保持離線狀態減少攻擊面、在充電樁上建置零件模組以便於偵測異常時停止供電、升級充電樁硬體使其容忍損害之範圍擴大等，以上緩解方法可減少充電樁遭受攻擊，不過更重要的是供應商從軟硬體面升級安全性防護，讓使用者免於有心人士的攻擊。

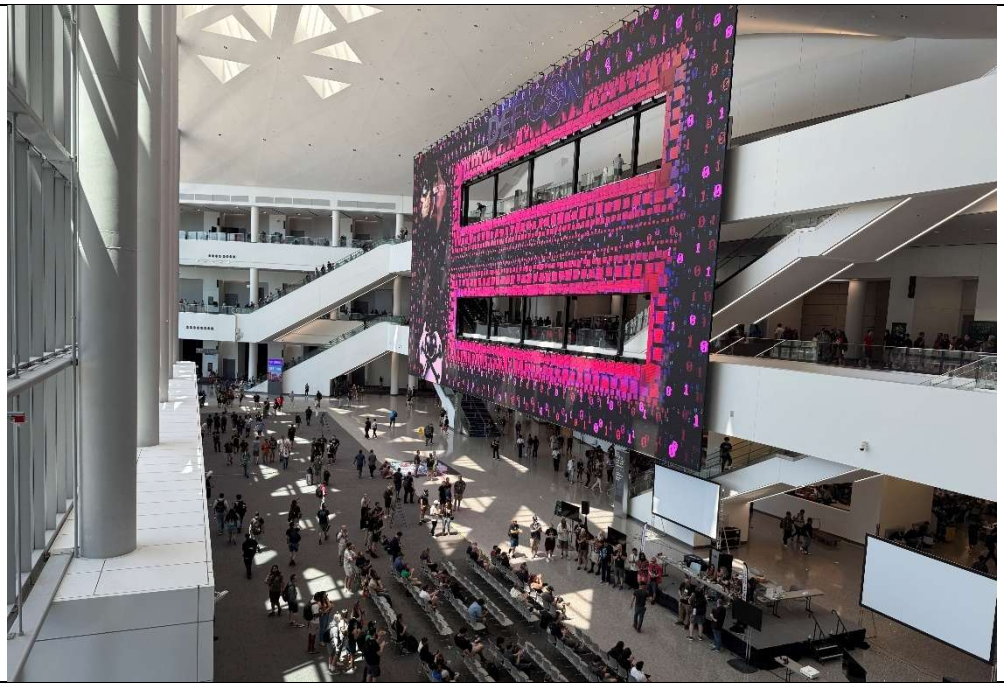
演講實景

三、DEF CON 33資訊安全技術研討會

（一）主題展區簡介

DEF CON 33在Las Vegas Convention Center的各個場域盛大舉行，有超過20個主題展區（Village）安排主題演講、實機操作教學或進行CTF競賽，並讓參與者可從手機下載活動 App，依照每個活動的舉辦時間自行參加感興趣的主題，主題展區的種類多元，幾乎囊括所有與科技、資訊相關的產業及領域，

著名之 Village 包含 Adversary Village、Aerospace Village、AI Village、Car Hacking Village、Cloud Village、Crypto Privacy Village、Crypto Privacy Village、Embedded Systems Village、GameHacking.GG Village、Hardware Hacking Village、ICS Village （Industrial Control Systems Village)、IoT Village、Malware Village、Maritime Hacking Village、Maritime Hacking Village、Maritime Hacking Village、Physical Security Village、Policy Village、Quantum Village、Recon Village、Red Team Village、Voting Village 等主題展區。



DEF CON 33會場外觀及大廳實景

（二）單一主題展區簡介

1. 主題展區—Cloud Village

Cloud Village 是針對雲端安全（Cloud Security）議題的專門空間，適合對攻擊與防禦雲端基礎設施、服務與部署流程有興趣者參加。這個展區包含講座、實作實驗室、工作坊、CTF 競賽與社群討論等形式。參加者可學習如何安全地維護雲端堆疊（Cloud Stack）、查找並管理雲資源中的潛在弱點、探索雲服務角色（IAM Roles）、瞭解服務與政策錯誤配置所帶來之風險等。舉例來說，在 DEF CON 33中，Cloud Village 的議程中有針對 Azure 資源列舉與屬性辨識研究，關於 AWS

「Shadow Resources / Shadow Roles」的議題講座，以及 Kubernetes 安全與容器化系統中之潛在攻擊路徑等。CTF 部分則跨越多個雲服務提供者，挑戰難度從入門到進階不等，既有攻擊也有防禦及調查類型。對於 DevOps / SecOps 工程師、雲安全研究者、紅隊 / 藍隊人員與雲資源管理者而言，Cloud Village 是瞭解雲端安全當前威脅、工具與最佳實踐中最有價值的學習平臺。

2. **主題展區—Adversary Village：**

Adversary Village 是一個聚焦於對手模擬（Adversary Simulation / Emulation）、威脅行為（Threat / APT / Ransomware）、供應鏈安全、Purple Team / Breach & Attack 模擬，以及對對手策略與思維方式研究的社群空間。這個展區提供很多動手操作與互動式體驗，包括技術工作坊、模擬演練、CTF、現場示範與討論面板，參加者能從研究者或實務者的角度，學習如何設計或模擬攻擊路徑、如何評估供應鏈風險、如何推估威脅者可能的策略與目標，以及如何設計防禦或檢測機制因應這些對手。同時，Adversary Village 亦重視思維模式（Mindset）與哲學性議題，探討對手生活方式、戰術（Tactics）、佈局與資源運用，包括如何保持持久性（Persistence）、如何逃避偵測 / 監控、如何在複雜環境中操控權限與橫向移動等議題。這個展區非常適合紅隊或藍隊安全人員、威脅情報分析師與希望深入理解攻擊者如何思考與行動的安

全研究者。

3. 主題展區—Red Team Village

Red Team Village 是 DEFCON 33中專注於進攻安全（Offensive Security）技術與模擬攻擊的展區，這裡包含有挑戰性的 CTF（包括 Web Exploitation、Reverse Engineering、Binary Exploitation 等）、網路攻防演練）及多種技巧工作坊與戰術講座，無論是紅隊老手或是剛入門者，都能在這邊找到適合自己技術層級的活動。在 DEF CON 33的 Red Team Village 內含進階與基礎的各種挑戰與實作，這個展區的特色是「動手」（Hands-on）與「真實情景模擬」（Realistic Scenarios），讓參加者在近似真實的攻擊環境中練習攻擊技巧、滲透測試、漏洞利用等技能，並與其他紅隊/安全研究人員交流心得與技術經驗。

4. 主題展區—Hardware Hacking Village

Hardware Hacking Village 是專門針對硬體層面的駭客/逆向工程/物理裝置操控及破解的展區，這裡有硬體 CTF（例如拆解或反向硬體、固件分析）、Robot Sumo 比賽、各種硬體裝置的實驗與展示，還包括修補與改造電子元件、焊接技術、硬體破解、強化安全設計等。此展區也有提供實體操作設施，例如 Soldering Stations, PCB Teardown 與硬體裝置實作，有關物理層面理解設備漏洞、固件問題、人機介面

安全、IoT/嵌入式裝置安全等範疇，對於這領域感興趣的參加者會非常有吸引力。

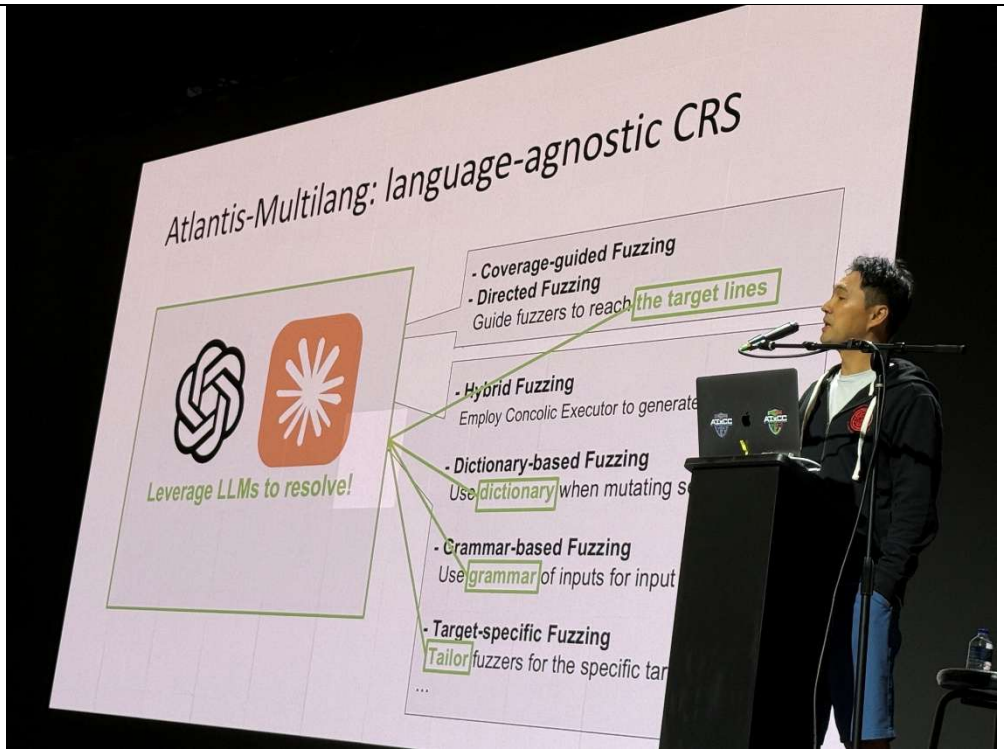
（三）獨立官方競賽簡介—AI Cyber Challenge（AIxCC）

AI Cyber Challenge（AIxCC）是由美國國防高等研究計畫署（DARPA）主導的國家級資安競賽，並非 DEF CON 33所屬的任何 Village。這項競賽的主要目的是推動人工智慧在自動化漏洞偵測與修補上的應用，雖然 AIxCC 的決賽於 DEF CON 33大會期間舉行，但其是以獨立賽事的形式登場，主辦單位、資金、賽制與評審都由 DARPA 與其合作機構（如 ARPA-H、Linux 基金會等）全權負責，針對全球頂尖團隊進行高額獎金競賽，參與門檻高、準備期長，並以技術實力與成果為核心評比，競賽中不僅要發現已知或刻意植入的漏洞，甚至要能處理零日（Zero-day）漏洞及真實世界中未預期的漏洞。

AIxCC 總獎金非常可觀，整個競賽期間獎金池達約2,950萬美元，在淘汰賽階段，各入圍團隊會以自身的系統接受測試，若進入決賽可獲得資金與資源來繼續改進系統。在 DEF CON 33舉辦期間，AIxCC 的最終決賽結果揭曉，Team Atlanta 獲得第一名，贏得4百萬美元獎金。

Team Atlanta 在決賽階段中「故意注入的漏洞」（Injected

Vulnerabilities）及真實軟體中未預期漏洞的偵測與自動修補方面均遙遙領先其他隊伍，決賽中共計有70個故意植入的漏洞供各隊測試，Team Atlanta 找到大部分並修補其中非常高比例的漏洞。比賽評分不僅看漏洞發現率，亦重視補丁的準確性、自動化速度與整體系統的穩定性。Team Atlanta 的系統命名為 Atlantis，是一套結合多種技術（LLMs、大量漏洞分析方法、動態與靜態分析、模糊測試等）的自治系統，能在多種程式語言與應用環境下運作。所有參賽系統將以開源方式釋出，供公共基礎設施設備/開源軟體等採用，讓這些技術可被現實世界採用提高軟體安全性。



AIxCC 國際競賽冠軍隊伍 Team Atlanta

肆、心得與建議

一、心得

今年有幸參加 Black Hat USA 2025與 DEF CON 33，這是一次極具深度與廣度的資安學習體驗。Black Hat 部分偏重於專業技術與產業應用，從 Briefings、工具發表到企業攤位展示，無論是紅隊技術、AI 安全、供應鏈風險或者是資安政策，每場演講都具有高度含金量。今年特別印象深刻的是 AI Cyber Challenge（AIxCC）決賽，讓我看見 AI 結合漏洞分析與修補的實戰潛力，且也是第一次離資安界的世界冠軍那麼近。主題展區部分，則可實地觀察最新的商業資安技術趨勢，包括 XDR、零信任（Zero Trust）、威脅獵捕與 LLM 安全等熱門議題。

而在 DEF CON 33，整體氛圍更自由與社群導向，不僅包含 CTF、Village 議程與現場活動，也有機會與來自各地的駭客/研究員建立難得的交流，且各種 Village 主題豐富，涵蓋範圍超出純技術，更進入社會工程、法規倫理與駭客文化。特別值得一提的是 Red Team Village 的實作環節，從實體入侵模擬到攻防演練都十分逼真且具挑戰性。

整體來說，這趟旅程不只是知識的充實，更是對資安產業脈動的深刻體驗，從實務技術、產業觀察到駭客文化，每一步都令人收穫滿滿。

二、建議

針對未來有意參加 Black Hat USA 與 DEF CON 的同仁，淺略提供一些建議以期提升參與效率與實效。首先，事前規劃行程非常重要，Black Hat USA 的議程較為正式且集中，建議提早瀏覽 Briefings 議程，透過活動專屬 App 選定關注的主題，以準時到達正確的會場。DEF CON 則活動分散，同樣建議下載 DEF CON App，標記有興趣的 Village 或 Workshop，並保留彈性時間排隊入場，畢竟有些場次座位有限，若排不進去可能就必須臨時再去搜尋別的場次。

其次，學習與社交並重，建議攜帶紙本名片或 QRCode 電子名片，主動與其他參與者互動，尤其在 DEF CON 的 Village 或 CTF 場域裡，認識志同道合的技術人脈往往比聽演講更有價值。

最後，體力與裝備準備也不能忽略，建議穿著輕便、準備行動電源、水壺與零食，並攜帶筆電參與 Hands-on Workshop，不過 DEF CON 是白帽駭客與黑帽駭客共存的場所，應避免攜帶工作用手機或電腦，並關閉自動 Wi-Fi 連接功能與藍牙，使用臨時帳號與乾淨設備登入任何系統，以有效

降低潛在資訊安全風險。