出國報告（出國類別：開會）

2025 RSA Conference 資安展及參訪美國資安公司

服務機關：台灣中油公司
姓名職稱：蔡凱翔組長
派赴國家/地區：美國舊金山
出國期間：114年04月27日 至 114年05月04日
報告日期：114年05月29日

摘要

今年 RSA Conference 2025（RSAC 2025）資安大會主要聚焦零信任架構和 AI 在網路安全領域的影響，凸顯企業須採取更全面的策略，以應對日益複雜的攻擊與防禦挑戰。隨著 AI 技術的快速發展，駭客已利用 AI 來快速精進網路釣魚與勒索軟體攻擊，使企業面臨更嚴峻的安全考驗。在零信任架構的進一步發展，企業開始採用 AI 驅動的安全模型，確保所有訪問請求皆經過嚴格驗證，降低未經授權存取的風險。身分驗證技術（如 PassKey）則成為防禦網路釣魚攻擊的重要工具，提升企業防禦能力。隨著供應鏈風險上升，企業必須加強監控與風險管理，以應對第三方供應鏈的安全挑戰。開源漏洞管理工具在企業安全策略中的應用日益增加，幫助企業更有效地管理潛在風險。面對 AI 驅動的攻擊與防禦變革，企業開始整合 AI 於安全營運中心（SOC），提升威脅偵測與應變能力。AIT 美國在臺協會安排的美國資安公司參訪行程，邀請的資安大廠涵蓋威脅情資、端點 MDR、網路安全設備、代管安全服務、CDN 服務等範疇，透過與美國原廠團隊面對面方式瞭解最新資安趨勢與進展，也透過此機會與國內指標企業代表們交流彼此的需求與想法。

目次

一、目的

RSA Conference 是安全業界的標竿會議，為全球最知名的資安大會，展示最先進的資安技術，進行最新的資安趨勢探討。今年的主題包括：資安分析與情資、雲端安全、零信任與身分安全、第三方與供應鏈安全、零信任與身分安全、駭客與進階威脅等，皆為目前推動資安工作的重要議題。

該會議涵蓋 IT 及 OT 領域相關最新資安議題，如混合式工作環境安全挑戰、IT/OT 整合的複雜性、AI 與自動化威脅偵測等，有助於提升各關鍵基礎設施單位防護檢視，並規劃後續資安管理精進作為。

AIT 美國在臺協會安排的資安公司參訪，直接與資安領導廠商面對面探討資安需求與想法，可從資安行業領導者和演講嘉賓汲取最新趨勢，並從經驗豐富的業界先進瞭解實際經驗的第一手資料。

二、過程

日期	地點	行程
114.04.28	舊金山	參加 RSA 2025資安展、參訪 Trellix 公司
114.04.29	舊金山	參加 RSA 2025資安展、參訪 SailPoint 公司
114.04.30	舊金山	參加 RSA 2025資安展、參訪 Google 公司
114.05.01	舊金山	參加 RSA 2025資安展、參訪 PaloAlto 公司
114.05.02	舊金山	參訪 Cloudflare 公司

RSA Conference 2025（RSAC 2025）於4月28日至5月1日在美國舊金山舉行，本次會議含括450多場專題演講及設有650家企業展位。今年的主題為「Many Voices. One Community.」（多元聲音，一個社群），強調全球網路安全產業的多樣性和合作共識，鼓勵不同背景的專業人士共同應對資安挑戰。

RSAC 2025也關注一些當前的全球重要趨勢，如 AI 在網路安全的雙重角色、身分安全的重要性、Agentic AI（代理 AI）的崛起等。AI 在網路安全中具有雙重角色：既是防禦工具，也是潛在威脅；企業需採取更全面的安全策略，包括提升身分驗證技術、強化供應鏈監管，以及推動零信任架構；代理 AI 在網路安全領域的應用已愈趨廣泛，不僅能執行預設任務，還能自主學習依環境變化來調整政策。

今年 AIT 美國在臺協會安排與美商資安公司參訪，透由資安公司各方視角來瞭解最新的資安議題，並直接面對面與資安業界先進學習交流，探討議題有威脅情資與即時回應、統一整合平台、AI 帶來的安全威脅與挑戰、零信任安全架構等。

茲依RSAC 2025會議參與之演講主題：雲端安全與AI安全、身分安全與PassKey、國家資助的網路威脅與 FBI InfraGard 組織，以及美商資安公司參訪行程，摘錄內容如下：

（一）雲端安全與 AI 安全

1. 技術顛覆與企業敏捷性：每隔10年，技術演進皆帶來一些顛覆性的變革，從移動裝置、雲端、物聯網、AI，已經對企業及工作模式產生了深遠的影響，也面臨著更嚴峻的安全挑戰。駭客專注且不斷地調整技術，企業卻常因網路架構慣性（如邊界防火牆、VPN、內部受信任網路）而缺乏快速應變能力，需要轉向更細緻的安全設計，如點對點的應用程式連接。
2. 雲端應用程式與資料安全：預估2025年底全球地端和雲端資料量將達到181ZB，資料安全管理的複雜度急劇上升，企業雖持有網路日誌、伺服器日誌、資料庫日誌與端點日誌，但真正的挑戰在於存取權限與擴展管理。AI 使資料存取與分析更快速有效，但若無強大的資料安全架構，則可能放大風險，企業需要更高的可見性、身分管理與自動化技術，即時偵測與監控雲端應用程式中的異常活動和錯誤配置，以確保企業能夠應對不斷演變的網絡威脅。
3. 減少公共 IP 數量與零信任架構（Zero Trust Architecture）設計：減少企業的公共 IP 暴露面，能降低遭受直接攻擊的可能性；但完全無對外 IP 並不符合實際現況，員工仍需存取雲端服務、VPN 或 API，因此須確保重要服務受到防火牆保護。企業可採用零信任架構，將員工設備與企業網路隔離，比擬為每個節點都是一家咖啡廳，它不是企業網路的一部分，皆視為員工在咖啡廳上網一樣。當員工連接內部資源時，每次請求都經過身分驗證，員工設備連網只能使用訪客網路，即使他們的位置在內部網路，零信任架構設計將有助於企業減輕遭受各類型攻擊的損害，包括 AI 驅動的攻擊。
4. 非人類識別（NHI）和代理 AI（Agentic AI）安全挑戰與治理：企業內部有許多非人類識別（NHI），他們可以是應用程式、服務或裝置的數位身分，如 API 金鑰、服務帳戶、代理 AI 等，未經適當管理的 NHI（如暴露的 API 金鑰）可能導致資料洩露或業務中斷。因此，企業必須建立有效的身分治理機制，限縮 NHI 的訪問權

限，並利用監測工具來警示異常行為。代理 AI 除了執行單一任務，還會形成記憶並透過上下文理解來執行更複雜的業務，例如：模擬人類入職過程，觀看培訓影片、閱讀文件等。隨著代理 AI 自主性逐漸增加，對安全與可視性要求也將提升，企業需要考慮如何監控 AI 的行為，確保在長期運行中不偏離預期，且須利用加密硬體來保護 AI 模型權重與客戶資料，確保 AI 部署時不洩露敏感資訊。

5. AI 改變雲地混合 SOC 的挑戰：傳統 SOC 主要處理企業地端和邊境安全事件，但如今生成式 AI 和代理 AI 的興起正在改變企業的安全防護架構，SOC 必須快速適應 AI 驅動的雲端環境和惡意威脅，例如：攻擊者已在利用 AI 機器人攻擊企業系統，快速滲透漏洞（據統計最短220秒），防禦者則需利用 AI 進行即時威脅偵測與回應。企業應重新設計安全架構來應對 AI 風險，必須假設雲端服務和雲地應用程式（包含資料）可能遭遇攻擊，積極採取新的身分驗證與行為監控技術，包括使用沙箱技術（如 Google gVisor 容器）和提升 AI 執行階段可視性。

（二）身分安全與 FIDO PassKey

1. FIDO、PassKey 和數位身分未來：FIDO（Fast IDentity Online）聯盟成立於2012年，致力於解決數位身分驗證，減少對傳統密碼的依賴，朝向更安全且便捷的使用者體驗。PassKey 技術已被全球許多大型科技公司採用，如蘋果、Google、Microsoft、Amazon、VISA 等，並廣泛應用於金融、醫療和物聯網領域，許多科技公司回報 PassKey 可大幅減少密碼重置需求、降低 IT 服務中心成本，並提升員工生產力。主要特色包括：使用指紋、臉部辨識或硬體安全密鑰進行驗證，可跨平台兼容在不同裝置和作業系統上運行，認證過程不需將使用者的生物辨識資料或私鑰傳輸到伺服器，防止敏感資訊遭盜用。
2. 因應與日俱增的網路釣魚攻擊：生成式 AI 讓網路釣魚攻擊更加複雜，攻擊者可透過精心設計語法的詐騙網站，繞過 MFA 機制並竊取憑證。PassKey 因為沒有密碼可供竊取，攻擊者無法藉由釣魚網站獲得帳號憑證。再者，本質上透過教育訓練員工防範釣魚郵件仍不足以防範社交工程攻擊，企業應採用 AI 驅動的防禦工具來自動偵測並攔截釣魚郵件，透過機器學習和行為分析技術，即時辨識可疑郵件並降低人工判讀的風險。
3. 企業強化登入憑證策略：

(1) 強化應用程式白名單：各主機透過組態白名單設定方式，阻擋 PowerShell 和命

令列連接外部網路；限制未經授權應用程式軟體的執行；防止存取特定資料夾的惡意文件寫入。

(2) 正確設置 EDR 並提升 EDR 監控：攻擊者不再依賴惡意軟體，而是利用合法帳號進行攻擊。企業應正確設置 EDR 為阻止並隔離，而非僅偵測，且必須及時更新 EDR 版本，防止攻擊者繞過端點防禦；設置看門狗（Watchdog）背景處理程序，監看 EDR 的健康狀況或回應能力，如果 EDR 無回應或發生異常，便自動重新恢復或發出警報，來防止 EDR 遭惡意關閉。

(3) 部署防網路釣魚 MFA：任何可讀的共用密鑰（如 OTP）皆有被攔截竊取的風險，企業應設計一套導入 PassKey 或基於 FIDO2標準的身分驗證框架。PassKey 可綁定特定網站讓使用者登入，攻擊者無法將憑證轉移至其他惡意網站。企業應著手評估現有資通訊設備的支援性，確保現行系統能夠兼容 FIDO2、PassKey 或 Windows Hello，強化身分驗證安全性。

（三）國家資助的網路威脅與 FBI InfraGard 組織

InfraGard 是 FBI 與民間企業建立的網路安全與關鍵基礎設施保護計畫，目標是建立一個信任關係，促進私人企業和政府間的情報共享，讓政府機構、民間企業和安全專家能夠共同應對網路威脅、恐怖主義及間諜活動，達成保護美國的關鍵基礎設施和人民。

全球網路攻擊的加劇，持續對美國的安全、創新和關鍵基礎設施構成了最大的威脅。網路犯罪集團透過跨國合作，使用 AI、自動化及勒索加密技術擴大攻擊範圍，擴展至關鍵基礎設施，如電信、醫院、學校、執法機構，甚至金融機構。InfraGard 最新觀察到中國 APT 族群使用零日漏洞攻擊邊界 IoT 設備以躲避防火牆與端點檢測，然後利用 Cisco 路由器和代理伺服器建立殭屍網路（Botnet）隱藏來源或操控受感染設備。攻擊者甚至入侵或干擾合法攔截系統（Lawful Interception），比方美國政府機構或執法機關依法監控電信網路通訊，藉此影響執法單位情報收集和資料安全的風險。

FBI 長期監控北韓網路活動，並發現其針對金融、區塊鏈等產業滲透。FBI 和 InfraGard 近日也偵獲北韓 IT 工作者偽裝成自由職業者，透過人頭帳戶申請北美、歐洲、韓國等地的 IT 職位，他們使用假 ID 身分、AI 工作履歷、深度偽造面試來提高職缺錄取率。北韓 IT 團隊的滲透行為持續進化，企業和政府必須加強內部審查與網路安全防護，不定時透過指紋辨識、背景調查、現場面試、VPN 流量監控等措施來識別異常行

為，防範滲透者竊取機密資訊或部署惡意軟體。

（四）資安公司參訪

今年 AIT 美國在臺協會安排的參訪行程，邀請的資安公司類型涵蓋範圍包括有資安威脅情資、端點 MDR、網路安全設備、代管安全服務、CDN 服務等，透過與美國原廠團隊面對面方式瞭解資安產業最新趨勢與進展，並與隨團的指標企業代表們有機會交流彼此的需求與想法。摘錄部分議題研討內容如下：

1. 雲地混合架構防護

企業在雲地混合使用資料和服務的環境下，面臨更為複雜的資安挑戰，駭客可以利用混合架構的漏洞發動攻擊，造成資料洩露、系統入侵或業務中斷。為能有效防護，企業必須採取多層次安全策略，確保資料存取安全、網路與服務穩定，以及應用程式免遭受攻擊。

(1) 零信任架構是目前最重要的資安模型之一，透過不斷驗證每個存取要求，確保未經授權的行為無法獲得資源存取權限。

(2) 企業應部署跨平台資安監控，利用 SIEM 與 SOAR 技術來即時監測異常行為，並快速應對潛在威脅。

(3) 強化 API 安全管控，API 未經適當保護很容易成為駭客攻擊目標，確保 API 存取皆受控並經過加密，以防止未經授權的資料竊取。

2. 因應 AI 驅動的攻擊威脅

駭客已開始利用 AI 技術來提升攻擊的效率，企業面臨極遽增長的資安挑戰。勒索軟體集團正在運用 AI 來自動化攻擊行為，包括編寫加密程式、掃描網站漏洞、生成欺騙性訊息，甚至規避偵測機制，來加快攻擊速度並擴大影響範圍。駭客也透過 AI 更精確地過濾與驗證被盜的憑證，使攻擊成功率提高，導致企業的敏感資料更容易遭到竊取。

面對 AI 驅動的威脅，駭客攻擊手法已更為精密，企業不能只依賴傳統的防禦方式，而必須利用 AI 來強化防禦，並採取主動防禦策略，確保網路安全與業務持續運行。

(1) 帳號登入憑證與身分驗證仍然是防範網路攻擊的基本要素，透過多因素驗證、生物識別技術或零信任架構來降低被竊取風險。

(2) 企業應採用 AI 技術來提高資安防護能力，例如透過 AI 來分析攻擊模式、監測

異常行為，並自動調整防禦規則，以提升回應速度。

(3) 企業應定期測試與演練自身的安全設置，利用 AI 來識別潛在威脅，確保防禦機制能及時適應最新攻擊技術。

(4) 除了內部防禦措施，企業需與資安專家、供應鏈夥伴、政府機構合作，建立威脅情報共享機制，快速應對新型攻擊模式，確保整體防禦能力不斷提升。

3. 保護 AI 安全議題

隨著 AI 在企業中的應用日益普及，AI 安全管理成為企業不可忽視的核心議題。企業在雲端運行 AI 應用時，需面對模型操控、資料洩露、惡意攻擊及 API 不當存取風險等挑戰，確保 AI 在運行過程中的安全性，避免潛在威脅影響業務運作。

(1) AI 模型可能受到資料污染（Data Poisoning）或惡意輸入（Prompt Injection）攻擊，導致被操控來產生錯誤決策，因此必須強化防護機制，如加密存取控制與模型審核流程，以確保 AI 的運行可信度。

(2) AI 驅動的即時威脅防護能夠監測代理 AI 與應用程式的異常行為，迅速阻止攻擊，提高系統的穩定性。

(3) AI 服務的 API 安全性也是一大關鍵，企業需透過授權機制與存取管理，防止未經授權的存取或惡意利用。

4. 建置現代化 SOC 平台

在亞太地區企業的 SOC 運作效率面臨嚴峻挑戰，三分之二的安全事件是由外部通知（如執法機構）發現，而非內部監測。既有 SOC 效率不佳的原因包括速度與規模問題、威脅情資不足和警報疲勞等。

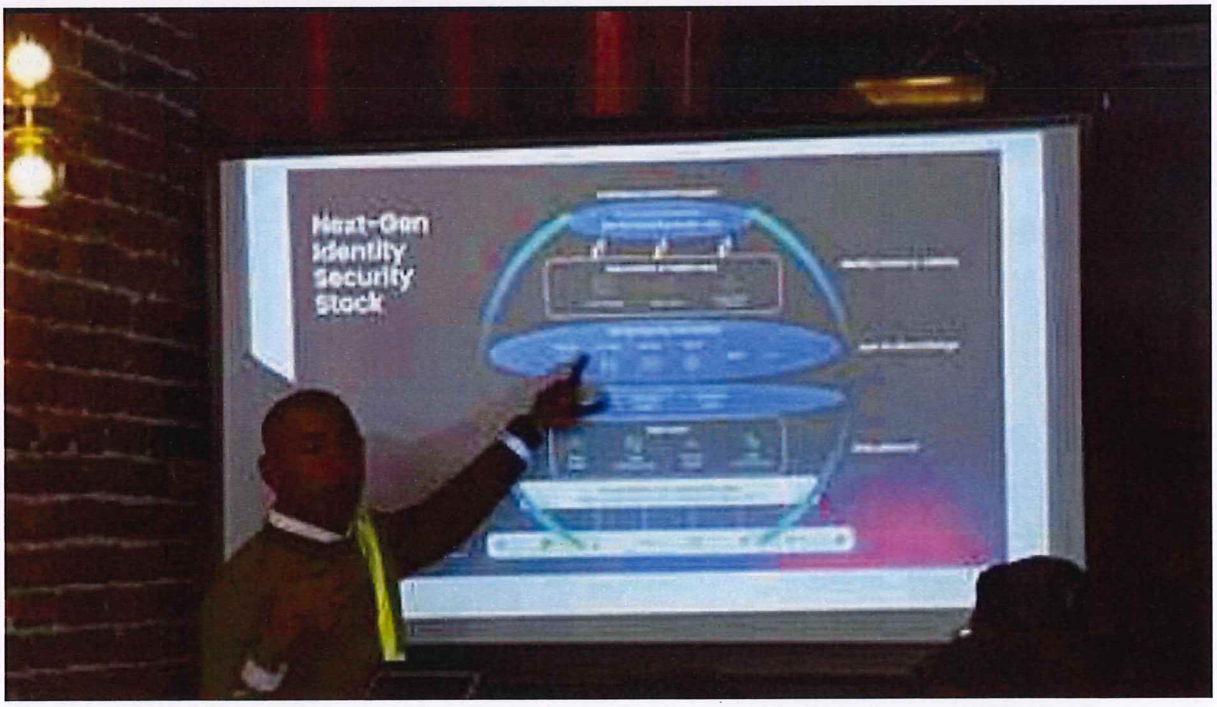
(1) 速度與規模受限導致無法有效處理日誌資料，缺乏 AI 驅動的自動化分析，讓過多的手動處理影響整體效率。

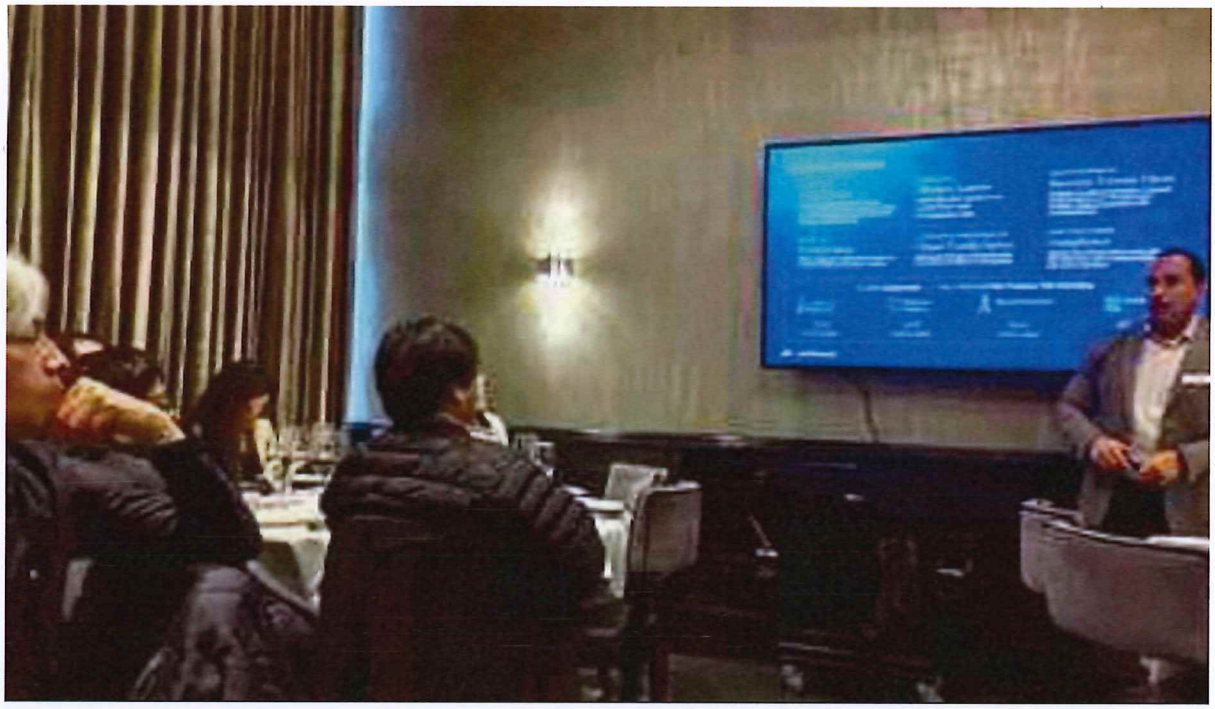
(2) 威脅情資不足使得誤報過多，造成分析師負載過重，影響回應品質，使得安全事件可能被延遲處理或忽視。

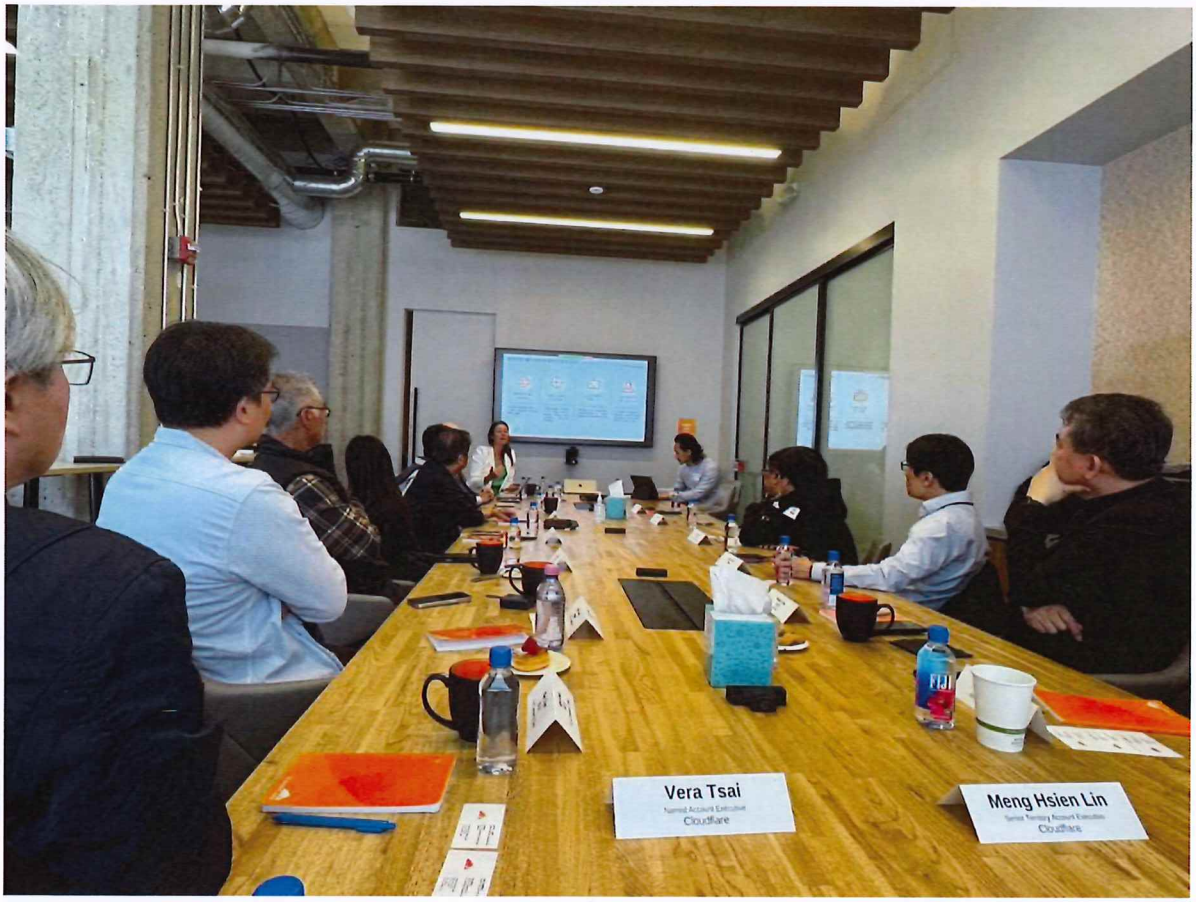
(3) 過度仰賴靜態告警規則，透過分析師手動編寫關聯規則來偵測威脅，這種方法已無法負荷現代 AI 驅動的網路攻擊技術。

為解決 SOC 效率問題，企業應採用統一整合平台，使 AI 技術成為資安防禦的重要工具，幫助企業透過 AI 技術強化即時監測與防禦能力，從「被動防禦」轉向「主動預防」。整合式 SOC 平台提供自動化威脅分析與警報處理，減少人力負擔並提升回應速度，讓資安團隊能夠快速識別與應對攻擊。

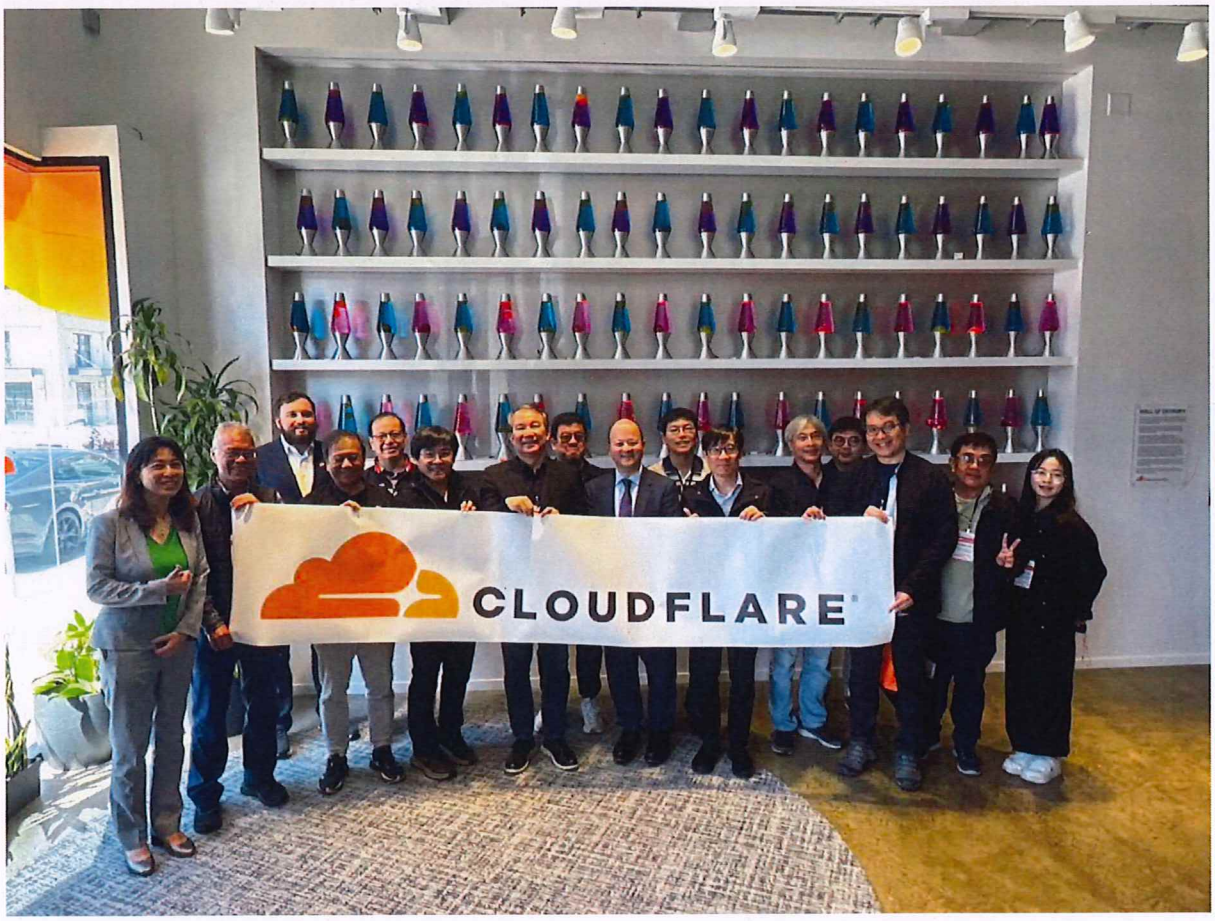

The Dark Side of
Innovation:
Generative AI in
Cybercrime


Next-Gen
Identity
Security
Stack




Vera Tsai
Named Account Executive
Cloudflare
Meng Hsien Lin
Cloudflare


paloalto
REAT
CTOR


CLOUDFLARE

三、具體成效

（一）今年到場參加 RSA Conference 2025資安會議，研討最新的網路安全趨勢與技術創新，最主要除了汲取資安領域的最新應用，也包括企業應對安全威脅的策略。

1. AI 攻防技術：AI 不僅被用於資安防禦，也被駭客用來發動更精密的攻擊，例如 AI 生成擬真的釣魚郵件與假網站，誘騙企業員工洩露憑證，進而滲透關鍵系統。企業開始導入主動式威脅獵捕（Threat Hunting）平台，以 AI 行為模型提前發現潛在的網路攻擊，而不是等到事件發生後才進行應對。
2. 身分管理與零信任架構：隨著非人類識別（NHI）存取行為遽增，企業須開始強化身分與存取管理（IAM），導入零信任架構，並加強非人類識別監控與審核流程。
3. 全球資安聯防：美國政府官員在會議中強調，資安已不再是單一企業的責任，企業應主動參與資安聯盟，如 MITRE ATT&CK、ISAC、FIRST 等全球性社群，並與政府建立情資共享機制。

（二）瞭解到 IT 及 OT 工控系統面臨之全球性資安威脅與議題，由於近兩年全球衝突加劇，包括俄羅斯、伊朗與中國政府支持的網路攻擊活動，影響能源、電信與製造業等領域。其中，伏特颱風（Volt Typhoon）被視為對美國關鍵基礎設施的重大威脅，駭客組織利用無文件（Fileless）和不落地（Living off the Land）技術現成系統內建工具滲透系統。鹽颱風（Salt Typhoon）鎖定美國電信業，影響至少8家美國電信公司，是歷史上最嚴重的電信駭客事件，目標是竊聽政府高層與企業通訊機密。勒索軟體組織如 RansomHub 利用跨平台惡意程式與選擇加密技術攻擊各行業，UAT-5918針對台灣電信、醫療及科技業發動攻擊，利用零日漏洞取得初始存取權限，再透過開源工具與 Web Shell 竊取使用者憑證並建立後門，進行長期監控與資料竊取。

（三）美國政府機構提出關鍵基礎設施的防禦策略，強調應優先保護對軍事或經濟至關重要的實體設施，避免資源過度分散，降低防禦能力。此外，也強調關鍵基礎設施評估供應鏈風險的重要性，攻擊者透過滲透 ERP 系統或遠端桌面軟體，植入惡意程式，影響能源、交通、醫療等工控設施，企業須進一步導入 AI 與 ML，以加強威脅檢測能力。也需深化與國際間的互助合作，如 CISA 和美國國家安全局等機構的協助，可提供更全面的防禦支援。

（四）本次與美國資安原廠專家面對面，著眼台灣目前遇到的資安問題，提出建議有助於台灣應對日益嚴峻的資安挑戰。國外資安專家對台灣的建議主要聚焦於強化關鍵基礎設施防禦、推動 AI 資安技術及提升供應鏈安全。

1. 台灣近期遭受多起勒索軟體攻擊，駭客組織利用 AI 技術提升攻擊精準度，並透過社交工程與惡意廣告滲透企業網路。為應對這些挑戰，企業應強化 AI 偵測異常行為，導入 AI 驅動的威脅獵捕技術，並積極參與國際資安聯盟，以提升整體防禦能力。
2. 專家建議台灣應加強對電信、能源及金融業的防禦，導入零信任架構，確保所有存取請求都經過嚴格驗證。
3. 在供應鏈安全方面，專家強調台灣應建立主動式供應鏈風險評估，確保第三方供應商符合資安標準，避免供應鏈成為攻擊者的突破點。

四、心得及建議

（一）考量訪客網路（Guest Network）和個人自攜裝置（BYOD）通常設定有條件式的例外開放存取，包括身分驗證和設備驗證，相較於公司員工內部使用的企業網路，容易忽略造成最脆弱的資安破口。公司可加速建置零信任架構，將員工設備與企業網路隔離，將每個連入節點視為外部網路的一家咖啡廳存取點。當員工連接內部資源時，每次請求都經過身分驗證，員工設備連網只能使用訪客網路，即使他們的位置在內部網路。長遠來看，導入 PassKey 強化身分驗證安全，駭客已經使用 AI 快速生成客製化的釣魚郵件，員工密碼容易被仿真的釣魚網站誘騙輸入，PassKey 因為需仰賴設備本地驗證，駭客無法偽造登入請求來竊取密碼和 SMS OTP。

（二）駭客已在利用 AI 工具高效率且自動化漏洞掃描和攻擊企業系統，也利用 AI 工具快速過濾與驗證從暗網取得的帳號憑證，提高暴力破解成功率，公司應假設雲端服務和雲地應用程式（包含資料）可能遭遇攻擊，採取新的身分驗證與帳號行為監控技術，包括使用雲端沙箱技術和提升員工使用 AI 工作階段的可視性。企業可引進 AI 驅動的防禦工具來自動偵測並攔截釣魚郵件，透過機器學習和行為分析技術，即時辨識可疑郵件並降低人工判讀的風險。

（三）由於資安專家觀察到勒索軟體攻擊模式不斷演變，滲透時間縮短至平均5～26天，但49%由攻擊者發動後發出通知，而非企業偵測。公司可規劃擴展多方即時情資來源與主動威脅狩獵，提升對後門惡意軟體的內部偵測能力。現代化 SOC 已經須具備快速適應 AI 驅動的雲端環境和惡意威脅，整合端點、網路、公司雲端資料，並提供即時威脅情資，SOC 安全機制架構應重新設計來應對 AI 驅動威脅帶來的風險。

（四）近期頻傳中國 APT 族群使用零日漏洞攻擊邊界 IoT 設備以躲避防火牆與端點檢測，甚至駭入美國政府機構或執法機關的監控電信網路通訊，來竊取國家情報資料。關鍵基礎設施的 OT 環境安全監管凸顯了至關重要，OT 環境過去多倚賴封閉式系統，但隨著網路連接增加導致攻擊面擴大，企業應確保所有存取行為都須經過驗證。強化工業控制系統 ICS 與 SCADA 防禦，加強流量分析技術來即時偵測異常，並導入威脅獵捕機制主動辨識攻擊。監管 OT 供應鏈安全，進行第三方供應商資安風險評估，確保所有 OT 設備供應商符合安全標準，避免供應鏈成為駭客利用的突破口。

（五）美國關鍵基礎設施遭受駭客攻擊以電信網路業、公用設施為多，台灣則是科技業、公共服務與醫療業。為提高網路和資訊韌性，企業需採取持續威脅偵測、集中安全事件管理與主動防禦機制。

1. 單一整合平台監測、分析網路與雲地日誌資料，透過 AI 自動化防禦，迅速處置安全事件。
2. 整合 CDN 的安全過濾功能，透過分散式架構降低 DDoS 攻擊風險，並過濾惡意流量加以阻擋。
3. 定期進行模擬網路攻擊、伺服器故障或數據中心異常，與持續營運計畫演練，驗證系統的穩定性與復原能力。
4. 設立長期韌性計畫，保護企業在遭受攻擊後72小時內恢復運作，並提升資通訊彈性，利用 CDN 降低單點故障風險，確保業務穩定運作。