出國報告（出國類別：開會）

2023 RSA Conference 資安展及參訪美國資安公司

服務機關：台灣中油股份有限公司
姓名職稱：李東波　主任
派赴國家/地區：美國 舊金山
出國期間：112 年 4 月 23 日至 4 月 30 日
報告日期：中華民國 112 年 5 月 29 日

◆ 摘要（200-300 字）

RSA Conference 2023 是 2023 年全美國最主要也是世界上盛大的資安研討會之一，走過新冠疫情的挑戰，於今年 4 月 24 日至 4 月 27 日在美國舊金山舉辦，共計 4 天，共吸引全球超過 4. 5 萬名與會者參加。本次大會的主題為 Stronger Together，強調在新興的網路攻擊模式變化下，應該要協同合作抵抗網路駭客的攻擊，遏止犯罪以降低風險。 本次研討會內容涵蓋如何評估 AI 和機器學習在網宇安全中的適用性、分析、情報和回應、反詐欺、駭客威脅、身份驗證、行動裝置和物聯網資安、應用程式安全、隱私保護、資料保護和密碼學應用、風險管理等重要議題。本次參訪活動行程為參加 AIT 所安排的相關主題研討、資安公司參訪以及 RSA Conference 展點廠商所展示的資安防護技術運用；藉此次外部參訪，汲取經驗，提升及強化本身專業能力外，並適時運用在本公司的資安防護。

◆ 、目次

壹、目的

RSA Conference 2023 資安展係全球最大規模之資訊安全展，本次資安大會的主題為 Stronger Together，強調在新興的網路攻擊模式變化下，各方應該要協同合作，抵抗網路駭客的攻擊，遏止犯罪以降低風險。

本次活動係應美國在臺協會 (American Institute in Taiwan，簡稱 AIT)之邀，由數位發展部闕次長河鳴帶團，國家安全局、國防部、國防安全研究院、數位發展部資通安全署、數位發展部產業發展署、數位發展部韌性建設司署、國家資通安全研究院、電信技術中心、工業技術研究院、資策會、亞洲矽谷計劃執行中心、國泰金控、第一銀行、鴻海精密工業、鴻海研究院、動力安全公司、中華資安國際公司、台灣中油公司與美國在台協會共同出席與會。

本次參加 RSA Conference 2020 會議的目的為掌握美國資安公司最新資安防護技術發展的方向，以及如何在目前嚴峻的攻擊環境中導入解決方案，降低發生資安事件的風險，及有如何保障使用者安全。

貳、過程

本次參訪團先於 4 月 13 日於美國在台協會舉行行前說明會，4 月 23 日晚上搭乘長榮 BR18 班由桃園機場出發，並於 4 月 29 日凌晨由舊金山搭乘長榮 BR17 班機返回，於 4 月 30 日清晨 4:40 抵達桃園機場。

一、RSA Conference 會展紀要

大會活動與展場地點主要在 Moscone Center 區域，共分為三個主場地：Moscone South、North 及 West 館，舉辦 Keynotes、 Sessions & Events、Tutorials & Trainings、Learning Labs、Sandbox 以及廠商產品攤位展示等(Booths)等各類活動主題，包括如何評估 AI 和機器學習在網宇安全中的適用性、分析、情報和回應、反欺詐、應用安全和 DevOps、駭客和威脅、身份驗證、行動裝置和物聯網資安、政策和政府、隱私、專業發展和人員管理、資料保護和應用密碼學、風險管理等重要議題，圍繞當前資訊安全領域的熱門話題展開深入探討，並呈現出最新的行業趨勢和技術創新。

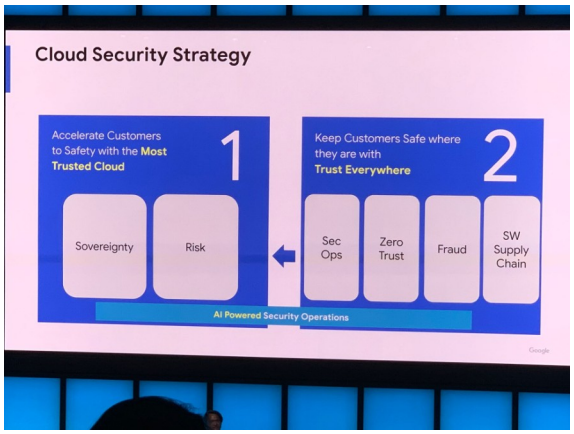
RSA 首席執行官 Rohit Ghai 在開幕主題演講“迫在眉睫的身份危機 The Looming Identity Crisis”中將 AI 置於中心位置，以此作為開端。Ghai 在演講開始指出“AI 會讓我們人類對我們在這個世界上的角色完全困惑”。他提出了為何 AI 將成為保護身份的關鍵，“沒有好的 AI，零信任就沒有機會。” 他並指出 AI 能成為網路安全的基礎。我們需要 AI 來阻止利用 AI 發起的攻擊。但他也表示，安全領域的 AI 並非意味著要取代人類。目前資安公司推出的大多數 AI 解決方案都是“輔助駕駛”類型的解決方案。在網路安全方面，AI 將會使得決策變得更容易。

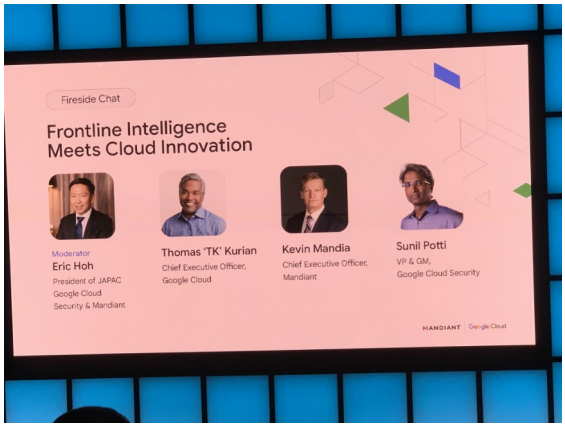
由 SANS 技術研究所所長 Ed Skoudis 主持的“The Five Most Dangerous New Attack Techniques 五種最危險的新攻擊技術”會議，詳細介紹了五種對組織構成嚴重安全風險的新攻擊技術。包括：SEO 攻擊、惡意廣告、針對開發人員的攻擊、惡意軟體（勒索軟體）。

Kelly Hood 及 Greg Witte 在展會中以"NIST Cybersecurity Framework v2.0: What’s changing?"為題，介紹NIST CSF 2.0預期會發生哪些更改，以及如何在整個更新過程中回饋意見，並預估今年冬季發佈版本 2.0 。

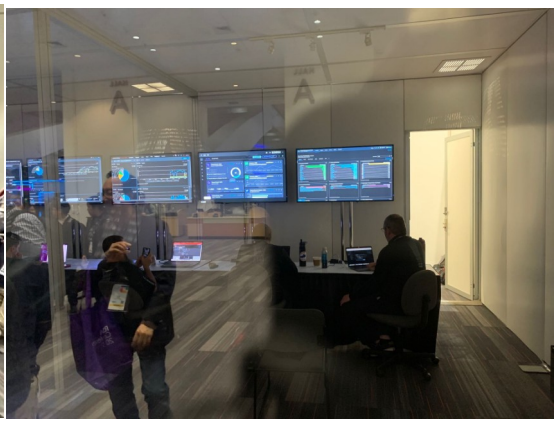
二、AIT 安排活動

(一) Google 公司參訪：由 Google Cloud Security VP & GM Sunil Potti 介紹了"GoogleSecurity: Strategy and Priorities"。接著由 Google Cloud CEO Thomas Kurian、 Mandiant CEO Kevin Mandia、Google Cloud Security VP & GM Sunil Potti、Google Cloud Security and Mandiant President of JAPAC Eric Hoh 就 "Frontline Threat Intelligence Meets Cloud Innovation 一線威脅情報與雲創新相遇"展開座談，最後由 Google Cloud 資安長（Chief Information Security Officer，CISO）Phil Venables 簡報"Security Outcomes Deliverd by Google Cloud"。





(二)「RSA Conference 展會與資安監控防護中心」：本次 AIT 安排，由 NetWitness 美洲 SE 總監 Dave Glover 及 Cisco 戰略聯盟總監 Jessica Bair 人員進行了 導覽，介紹了展場的 SOC 監控機制。



(三) Striderintel ：Strider 公司成立於 2019 年屬性為美國戰略情報公司，專注於如何防範外國政府瞄準私人組織，以獲得專有技術和資訊，以推進其國家目標(如我們地緣政治關係的林國)。該公司提供了一個獨特且不斷增長的高風險、國家支援的情報資料庫，可以使用該資料庫來豐富現有的內部安全系統。本次 AIT 安排，參加由該公司曾駐中華人民共和國，專注於安全和經濟問題，在危機談判和解決方面經驗豐富的戰略主管 Corey Johnston，以及出生於高雄的情報高級總監 Sabrina Jennings，以"Strengthening National Economic Security in Taiwan"為提之進行研討，會中以美國公司某半導體竊密案為例，展示了該公司如何對潛在內部威脅所提供的重要資訊。

(四) Fidelis 公司 ：Fidelis Cybersecurity 是一家網路安全公司，專注於威脅檢測，搜尋和響應高級威脅以及數據洩露。此次應 AIT 之安排，參加 Fidelis 之研討會，由該公司亞太區銷售總監 Terence Heah 進行"Cyber Resilience"簡報，簡報中以美國奧克蘭市於今年 3 月遭勒索病毒攻擊事件為例，說明了安全與韌性的差異，強調網路安全策略不應僅僅關注違規防範，還應該採取積極的防禦解決方案，讓防禦者積極參與威脅獵捕和事件調查，策略越積極主動，網路事件的成本就越低。

(五) Mandiant 公司：Mandiant 是一家總部位於美國，為威脅情報和網路安全前線專業知識的市場領導者，於 2022 年 8 月正式被 Goole 併購。為了讓組織為網路威脅做好準備，Mandiant 通過 Mandiant Advantage SaaS 平台擴展其情報和專業知識，以提供最新情報、警報調查自動化以及來自各種供應商的安全控

制產品的優先級排序和驗證。本次應 AIT 之邀，參加研討會"Cyber Resilience In Taiwan - For Public & Private Sector Organizations"，由該公司亞太區包括日本副總裁及首席技術總監 Steve Ledzian 進行簡報，簡報中指出 Mandiant 發現了一組影響公眾和公眾網路間諜活動，持續情報收集。該活動至少自 2013 年初開始活躍，其特點是使用 Capgeld 和 TSCookie 惡意軟體，並專注於損害臺灣政府的利益。此外，也監測到正在尋求訪問關鍵基礎設施網路和資源。可疑目標包括臺灣國防、政府和民間組織： 海軍、 立法院、內政部、經濟部水資源局、中央氣象局、媒體、學術界和智庫、政黨、負責向政府部門提供安全服務的組織等，在該公司的 M-Trends 2023 報告中，指出亞太地區的網路攻擊停留時間中位數從(2021)年的 21 天增加至(2022 年)的 33 天時，需保持時刻警剔。 此外，儘管涉及勒索軟件的入侵百分比在全球範圍內有所下降，但 Mandiant 觀察到與(2021)年相比，美洲涉及勒索軟件的調查百分比一致。 亞太地區的勒索軟件 2022 年為 32%，而 2021 年為 38%，調查雖減少了 6 個百分點，但這個數字仍然幾乎是 2020 年（12.5%）和 2019 年（18%）的調查百分比的兩倍。Mandiant 在 2022 年進行的調查中，漏洞利用仍然是駭客使用的最有效的入侵途徑。在識別出初始入侵中，32% 的入侵屬於漏洞利用。

(六)Sail Point 公司：Sail Point 是一家總部位於美國，擁有超過 17 年經驗和實施經驗的身份治理領導者。本次應 AIT 之邀，參加研討會 "Identity Security – Uncompromised" 由該公司產品執行副總裁 Grady Summers (前 GE 公司 CISO) 進行簡報。

(七)Varonis 公司：Varonis 是一家總部位於美國紐約的資安公司，是數據安全和分析領域的先驅，專注於數據保護、威脅檢測和響應以及合規性軟體。Varonis 通過分析數據活動、邊界遙測和用戶行為來保護企業數據；通過鎖定敏感數據來防止災難；並通過自動化有效地維持安全狀態。本次應 AIT 之邀參加研討會 "　What if Security started with looking at Data first"，由該公司擔任 Director of Field Engagement 的 Kilian Englert 進行簡報，研討如何防範資料外洩。

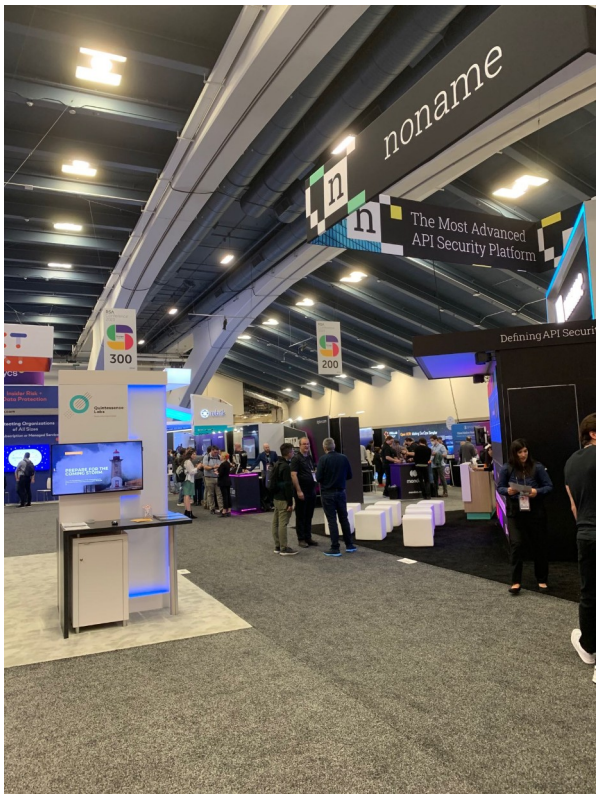
(八) Palo Alto Networks 公司參訪：Palo Alto Networks 是一家總部位於 Santa Clara 的網路科技公司，是企業防火牆的早期推動者和市場領導者，其核心產品為「次世代防火牆」（Next-Generation Firewall）平台，提供全面覆蓋雲端、網路和行動裝置，為高效、創新的網路安全解決方案。本次安排到 PA 的總公司參訪，針對"CYBERSECURITY 2023 and BEYOND CONNECTING TAIWAN IN THE FIGHT AGAINST CYBER ATTACK"討論，由副總裁暨亞太區與日本首席資訊安全長 Sean Duca 進行 "Cybersecurity Transformation and Trends "簡報，提出「從預防為主到採用零信任戰略與架構，當務之急是在防禦中採用廣泛和最深入的網路技能與威脅情資，更重要的是，企業組織與企業領導者必需具有彈性思維與應用，來應對許多不可避免的攻擊。」、產品管理高級總監 Ashwath Murthy 簡報"Applying Zero Trust To Real Scenarios "。


SESSION
CYBERSECURITY
2023 and BEYOND
CONNECTING TAIWAN
IN THE FIGHT AGAINST CYBER ATTACK

參、具體成效

資安展：

今年 RSA 展聚焦於 AI 的應用，如微軟的 Security Copilot、Google 基於安全的 LLM(large language models)、IBM 基於 AI 的安全服務，還是 Veracode 利用機器學習工具查找代碼漏洞，皆為網路安全推出最新的 AI 服務。這些產品都宣稱具有 AI 功能，但對於全新網路 AI 產品，或許需要供應商提供具體的例子和指標，以便評估工具性能。



參訪及研討會：

在 Mandiant 的研討中提及觀察到俄羅斯與駭客協同實施涉及俄烏戰爭的網絡攻擊，Mandiant 公司持續對烏克蘭政府和網路防禦援助協作組織下的關鍵基礎設施實體提供直接援助，包括妥協評估、事件回應服務、共用網路威脅情報和安全轉型服務， 以幫助烏克蘭政府檢測、緩解和防禦網路攻擊。Mandiant 也確定了影響臺灣公共和私營行業的網路間諜活動，損害臺灣的利益。此外，該公司也偵測到正尋求訪問關鍵基礎設施網路和資源的網路間諜活動。本公司在去年美國眾議院議長裴諾西訪台期間，也因地緣政治關係，遭到駭客攻擊次數暴增，未來可考慮引進相關服務，提昇防護能力。

在 Fidelis Cybersecurity 的 研討中強調了網路韌性的重要性，以下是幾個主要重點：

1. 傳統的網路安全措施已不足以阻擋日益複雜和頻繁的網路攻擊。
2. 網路安全策略需要重新思考並致力於網路強韌性。
3. 網路安全強韌性與網路安全防護不同，前者聚焦於威脅預防。
4. 網路強韌安全需要自動化、漏洞管理、符合法規標準、事件響應和災難恢復的組合以適應不斷發展的環境。
5. 落實網路強韌性需要採用零信任架構、投資於持續培訓、測試事件響應計劃。
6. 網路強韌性的核心包括新法規、可見性、控制、檢測和響應。

在 Sail Point 的研討中，提到身分安全解決方案有三個核心部分：

1.需要具有智慧性，全方位觀察並監督所有身分及其存取的需求。

2.需具主動性，以加快身分決策的速度。

3.需與現有 IT 基礎架構介接，便於將身分資訊嵌入數位系統中，以發揮作用。

建議透過融合 AI 技術的自動化工具來進行身分管理，進而逐步落實零信任架構的資安策略。

在 Palo Alto 參訪的研討過程結論：企業正面臨不斷轉型，從而加劇了不斷

擴大的網路攻擊面。這種網路威脅也挑戰我們的回應能力，必須採取積極的網路安全戰略， 以便：

- 具有凝聚力和全面性，以應對現有和未來的威脅媒介。
- 做好預防、檢測和有效回應每個媒介（網路、雲端點和軟體供應鏈）中所有威脅的能力。
- 最大限度地提高安全效率，同時優化總擁有成本。
- 推薦採用 零信任 + 平臺 = 面向未來。
- 消除隱式信任並建立在持續驗證之上的策略。
- 在需要的地方連接同類最佳的功能，以實現最大的可見性、控制和效率。
- 讓您能夠快速、安全地運營和創新，從而簡化安全轉型。
- 提供領先於威脅的網路安全，而不僅僅是對威脅做出反應。

肆、心得及建議事項

本次資安展聚焦的重點為身分驗證、雲端、資料偵測及回應以及機器學習在身分、使用者、個體行為與數資料分析方面在資安領域應用情境。未來採用 XDR 產品，必須要能提供涵蓋這些領域以及其他資安管道的原生監測資料，以便能與端點偵測及回應的活動資料進行進階交叉關聯分析。

隨著近日 ChatGPT 造成資料外洩的議題登上媒體版面，AI 模型很可能遭駭客濫用，技術廠商在針對最重要的資安情境打造解決方案時，應該將 AI 治理列為優先要務，以避免因輕忽 ChatGPT 淺藏的資安風險以及潛在影響，成為駭客攻擊的新弱點。

RSA 首席執行官 Rohit Ghai 在開幕主題演講強調了 AI 的重要性，他甚至宣稱如果沒有 AI 的支持，零信任就沒有機會被採用，我們在研擬導入零信任架構時，也必須將 AI 治理考量進去。

網路釣魚攻擊仍然是最常見的網路安全威脅之一，應強化員工資安意識教育訓練並讓他們努力防止違規，**以參與式教育和培訓來提升員工識別威脅的能力**，讓員工從風險轉變為優勢。

我們無法阻止所有網路威脅，但可以將回應時間最小化，面對日新月異的威脅情勢，以及未來雲地混合式環境，我們面臨日益複雜的安全性挑戰。XDR 安全性能因應這些情況，帶來更有效、更主動的解決方案。目前公司已採用端點偵測及回應 (EDR) 系統，為更廣泛的針對端點、伺服器、雲端應用程式和電子郵件等提供整合保護措施，並結合防護措施、調查和回應以及提供可視性、分析、互相關聯的事件警示和自動化回應，**可以考慮引進統一的安全平台，來降低網路韌性的複雜性，以改善資料及系統的安全性並打擊威脅**。

企業高階管理者需具備資安治理思維，此次 RSAC 中揭露 NIST CSF 2.0 已納入「治理功能」，將被新增為第 6 項功能，資安治理就是資安韌性的基礎；同時預計也將「網路安全供應鏈風險管理」，我們**應持續關注網路安全框架 CSF 2.0 版的相關議題，建立與有效實施網路安全框架**，以**強化零信任架構與網路安全風險管理，進而提高資安的韌性與成熟度，確保資通安全**。