2024 RSA Conference

國際資安大會出國報告

資訊部 張鈺峻

RSA Conference（RSA 大會）是全球領先的網路資訊安全盛會，聚集了來自世界各地的資訊安全專家、企業領袖、技術創新者和政府官員。自 1991 年創辦以來，RSA 大會已成為全球網路安全領域最具影響力和規模最大的年度盛會之一，每年在美國舊金山 Moscone 中心舉行，並且在亞太地區和歐洲設有分會。大會的宗旨是：

- 促進全球網路安全專業人士的交流與合作。
- 分享最新的技術創新和最佳實踐。
- 探討未來網路安全的趨勢和挑戰。
- 提升整個行業的安全意識和防護能力。

本屆會議主題

2024 年本屆的主題是「The Art of Possible」，旨在強調科技創新的無限可能性與潛力。這一主題反映了當前技術快速發展的現狀，尤其是人工智慧（AI）、雲計算、區塊鏈和量子計算等新興技術在網路安全中的應用及挑戰。議程為期四天，計有來自 130 個不同的國家，超過 4 萬多名網絡安全專業人士參與盛會。

會議日期與場地

- **日期**：2024 年 5 月 6 日至 5 月 9 日
- **場地**：美國加州舊金山 Moscone Center

(位在舊金山市中心的 Moscone Center, South Stage)

本屆大會統計資料

- 超過 41,000 名與會者，召開 425 個會議，共 650 名演講者、400 多名媒體

成員以及展示會場的 600 家參展廠商。

- 共進行 33 場主題演講(Keynote)。 West Stage 主題演講包括贊助商主題演講、小組討論和備受尊崇的嘉賓演講，而 South Stage 則帶來了行業專家就一系列主題進行的令人高度關注的深入探討會議。
- RSAC 大學日 迎來了超過 750 名大學生、安全學者和教職員工，他們與頂尖的公司建立了聯繫，探索就業機會，參加專門的教育活動，並體驗 RSA 會議和展覽場地。
- 與 RSA Conference 2024 相關的 550 多條媒體內容，帶來了 6.55 億以上的社群互動和 28 億以上的潛在讀者群。

(議程電子看板，主題、時間、會議室一目了然)

本屆的亮點包括

- 資安新創公司 Reality Defender 被擁有技術、創投和安全產業相關的專家組成的

Innovation Sandbox 評審團評為 「RSA Conference 2024 最具創新性新創公司」 。

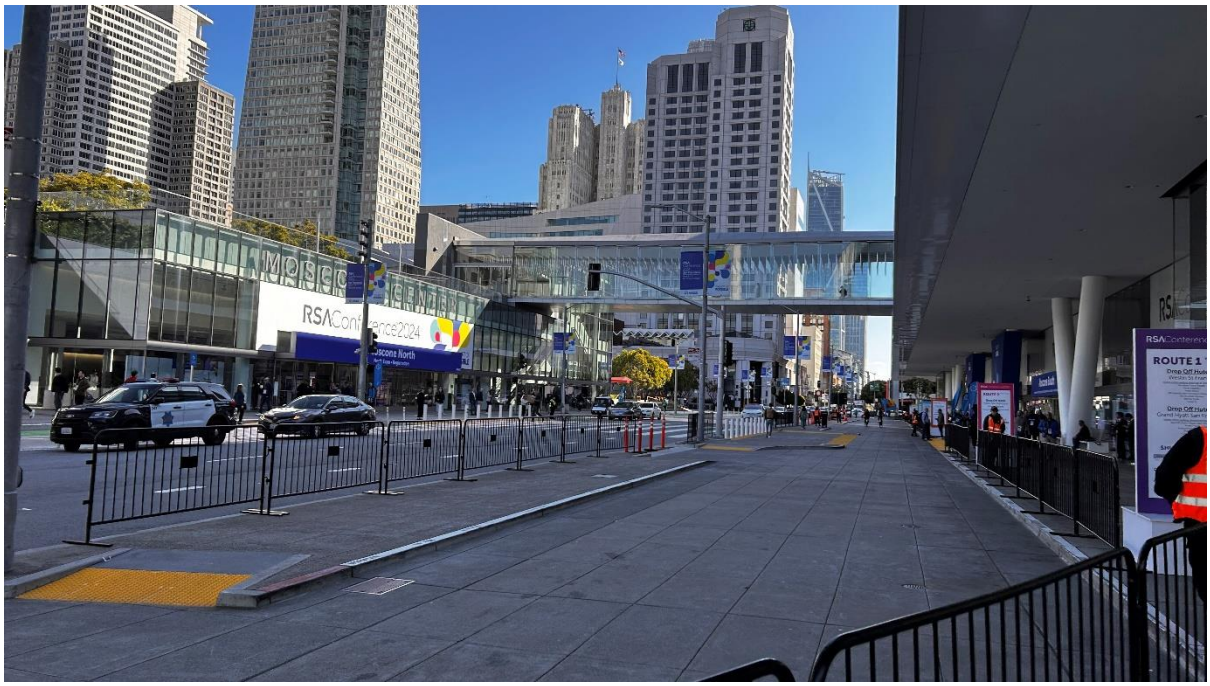
(Reality Defender 獲大會評審選為 2024 最佳資安新創公司)

- Culminate、Knostic 和 Tamnoon 被評為 RSAC Launch Pad 2024 決賽入圍者。
- 終身成就獎 授予美國海軍退休少將 Michael Brown，數學領域卓越獎授予 TripleBlind CTO Craig Gentry 和 Courant 研究所教授 Oded Regev 紐約大學數學科學博士。
- 主要會議和研討會的亮點包括：
    - *AI Safety: Where's the Puck Headed?* (*人工智慧安全：小精靈走向何方？*) – 由微軟的數據牛仔 Ram Shankar Siva Kumar 主持的爐邊座談，邀請 Google 安全工程副總裁 Heather Adkins，人工智慧安全中

心創辦人 Dan Hendrycks， NVIDIA 軟體產品安全副總裁 Daniel Rohrer，以及哈佛大學甘迺迪學院安全技術專家 Bruce Schneier 共同討論。

- *Technology and the Transformation of U.S. Foreign Policy* (*科技與美國外交政策的轉變)* – 美國國務卿 U.S. Secretary of State Antony J. Blinken (布林肯)
- *The Five Most Dangerous New Attack Techniques You Need to Know* (你*需要了解的五種最危險的新攻擊技術*) – Ed Skoudis，SANS 技術學院院長主持的座談會，邀請多位來自 SANS 研究所的專業人士探討最新攻擊技術。
- *Artificial Intelligence: The Ultimate Double-Edged Sword* (*人工智慧：終極雙面刃)* – 由史丹佛大學人類中心人工智慧研究所所長 Dr. Fei-Fei Li，美國司法部副總檢察長 Lisa Monaco；以及國家人工智慧諮詢委員會 (NAIAC)主席兼 EqualAI 總裁兼執行長 Miriam Vogel 一起探討主題。
- *Homeland Security in the Age of Artificial Intelligence* (*人工智慧時代的國土安全)* – 有多重身分的美國人工智慧科學特使，Humane Intelligence 執行長兼聯合創始人 Rumman Chowdhury，以及國土安全部長 Alejandro N. Mayorkas 一起對談。

- 高階主管計畫 – RSA 會議為特定主管和政府受眾舉辦了五個閉門計畫包含 CISO 新手訓練營 (CBC)、網路領袖論壇 (CLF)、 國際網路安全論壇(ICSF)、高階主管安全行動論壇(ESAF) 和 eFraud 全球論壇 (eFG)。



(位在舊金山市中心的 Moscone Center, North Stage)

各場地所舉辦的議程與活動

除上述的幾個大會亮點外，大會在 Moscone Center 的三個展場，各別舉辦了多場不同形式的專題演講、沙盒工作坊和技術展示等，與會者得依照三種通行證級別自行參加符合資格之活動。以下為各展場主辦項目：

1. **Moscone North**：
    - **專題討論**：圍繞 AI、機器學習、區塊鏈和量子計算的應用和挑戰，進行

深入探討。

- **數據隱私與合規**：探討全球隱私法規的影響、數據洩露應對策略以及隱私增強技術的應用。
- **未來趨勢與戰略規劃**：展望未來的網路威脅與防禦策略，討論物聯網和邊緣計算的安全挑戰，並探討安全運營中心的未來發展。
- **B1 展場 (與 South 相通)**：各家廠商的技術展示場地。

2. **Moscone South**：
   - **專題討論**：圍繞 AI、機器學習、區塊鏈和量子計算的應用和挑戰，進行深入探討。
   - **技術工作坊**：提供實踐導向的沙盒演練，涵蓋基礎到高級的防禦技術。
   - **創新實驗室**：展示最新的安全技術和解決方案。
   - **B1 展場 (與 North 相通)**：各家廠商的技術展示場地。
3. **Moscone West**：
   - **主題演講**：由全球頂尖的技術領袖和思想家分享未來網路安全的見解和願景。為最大演講廳，至少可容納 3000 人以上的會議廳。
   - **技術交流中心**：最高級別通行證人士的交流中心。

(各大廠商積極投入行銷廣告, Moscone Center)

議程探討主軸

四天的會議議程涵蓋了多個重要的資安領域：

1. **創新與技術前沿**：
    - 人工智慧和機器學習在威脅檢測、自動化響應和預測分析中的應用。
    - 區塊鏈技術在數據安全和身份驗證中的應用。
    - 量子計算對現有加密演算法的影響及新型量子加密技術。
2. **雲計算與安全架構**：
    - 雲安全的最佳實踐、多雲環境的安全管理。
    - 零信任架構的設計和實施方法。
    - 容器和微服務架構中的安全挑戰和管理。

3. **數據隱私與合規**：
    - 各國隱私法規（如 GDPR、CCPA）對企業的影響。
    - 數據洩露的預防、檢測和響應策略。
    - 隱私增強技術（如同態加密、差分隱私）的發展和應用。
4. **未來趨勢與戰略規劃**：
    - 網路威脅情報的收集、分析和應用。
    - 高級持續威脅（APT）的檢測和防禦。
    - 物聯網設備和邊緣計算環境的安全挑戰。
    - 安全運營中心（SOC）的自動化和智能化發展趨勢。

(位在舊金山市中心的 Moscone Center, West Stage)

參與的議程重點整理

The Power of Community 社區的力量

2024 RSA 大會的主題演講由大會執行主席 Hugh Thompson 開場。

今年大會的主題是「可能的藝術」。 Hugh Thompson 談到了社區在網路安全中的重要性。他分享了一個關於他的祖先是燈塔看守人的故事。他們的工作是保持燈塔亮著，以便船隻能在夜間安全航行。同樣，網路安全專業人員就像燈塔看守人一樣，照亮黑暗的地方，保護人們免受網路威脅，指引方向。

2024 年倦怠情緒再次飆升。今年，網路安全專業人員面臨著新的挑戰，例如勒索軟體攻擊，這導致他們優先記錄事件而不是響應事件。

人工智慧在網路安全無所不在，人們正在尋找利用人工智慧（例如 LLM 大型語言模型）來提高防禦網路攻擊能力的方法。然而，人們也開始擔心人工智慧演變出的新型威脅與攻擊風險。

風險管理是一個持續的過程，當發現新的威脅時，會經歷一段學習和討論的時期，然後製定框架來管理威脅。新的挑戰將不斷湧現，需要持續的警覺。

Hugh Thompson 也鼓勵與會者走出舒適圈，結識新朋友，並對新想法持開放態度。他提醒我們，我們是網路安全專業人員的強大社群的一份子，我們都致力於讓世界變得更安全。

(大會執行主席 Hugh Thompson 的開場演說)

Technology and the Transformation of U.S. Foreign Policy

美國國務卿布林肯的演講主題為《科技與美國外交政策的轉變》，強調了新興技術在全球外交和國家安全領域中的戰略必要性和挑戰，並提出數位創新對國際關係的變革性影響。

1. **技術進步與國家安全**：布林肯強調了人工智慧、量子計算和網絡安全等技術進步對國家安全的深遠影響。他指出這些技術正在重塑地緣政治格局，改變國家之間的互動和競爭方式。
2. **網絡安全作為外交重點**：網絡安全被提出作為美國國務院的首要任務。布林肯闡述了強大的網絡防禦系統對保護關鍵基礎設施和敏感信息免受惡意行為者攻

擊的必要性。他強調國際合作和建立規範與協議以減少網絡威脅的重要性。

3. **美國國際網際空間和數位政策戰略**：演說中，布林肯介紹了美國國際網際空間和數位政策戰略。這一綜合戰略旨在加強數位團結，促進開放、安全和可靠的網際空間。其重點是加強聯盟、推進民主價值觀以及對抗技術的威權主義使用。
4. **應對敵對國家的挑戰**：布林肯直言不諱地談到了中國和俄羅斯等敵對國家帶來的威脅。他討論了這些國家利用技術破壞民主機構和影響全球政治的行為。為應對這些挑戰，他呼籲增加對技術創新的投資並加強國際聯盟。
5. **創新和技術發展中的倫理考量**：演講並強調了技術發展中的倫理考量。布林肯倡導尊重人權和民主原則的技術，確保創新對社會和全球穩定做出積極貢獻。
6. **與私營部門的合作**：他體認到私營部門在技術進步中的關鍵作用，布林肯呼籲加強公共-私營合作夥伴關係。他敦促科技公司與政府合作，創建安全和有彈性的數字基礎設施，並在設立技術使用的倫理標準方面發揮領導作用。

(美國國務卿布林肯蒞臨大會演講)

The Five Most Dangerous New Attack Techniques

SANS 研究所主持的備受期待的主題演講《你需要了解的五種最危險的新型攻擊技術》。網絡安全專家在此強調了新興威脅以及應對這些威脅所需的措施。演講重點介紹了五種對全球組織構成重大風險的關鍵攻擊技術：

1. **高級釣魚攻擊**：現代釣魚攻擊變得更加複雜，利用人工智慧來製作高度可信的電子郵件，甚至可以欺騙最謹慎的收件人。這些攻擊越來越多地針對供應鏈和第三方供應商。
2. **勒索軟體的演變**：勒索軟體攻擊正在演變，採用雙重勒索等新策略，攻擊者不僅加密數據，還威脅要公開敏感信息，除非支付贖金。這些攻擊變得更加針對

性，通常由組織精良的網絡犯罪集團主導。

3. **雲安全漏洞**：隨著更多組織遷移到雲端，攻擊者正在尋找新的方式來利用雲基礎設施。這包括對雲的組態配置、容器漏洞和 API 安全漏洞的攻擊。
4. **人工智慧（AI）和機器學習（ML）攻擊**：網絡犯罪分子使用 AI 和 ML 來增強其攻擊策略，創建更加自適應和有彈性的惡意軟體。這些技術也被用來自動化攻擊，使其更快、更難檢測。
5. **物聯網（IoT）和工控（OT）系統的漏洞**：將物聯網設備和工控系統整合到業務環境中，開闢了新的攻擊面。這些系統通常保護不足，使其成為攻擊者的主要目標，旨在破壞操作或竊取數據。

會議提供了如何加強防禦這些新興威脅的實用見解。建議包括採用多層次的安全方法、投資於威脅情報以及確保持續監控和評估安全狀態。

整體而言，主題演講強調了保持對最新攻擊技術的了解以及採取積極的網絡安全措施以保護免受這些不斷演變的威脅的重要性。

(AI 是本屆的熱門話題)

Artificial Intelligence: The Ultimate Double-Edged Sword

這場主題名為「人工智慧：終極的雙面刃」，深入探討了 AI 技術對社會各方面的深遠影響，探討其巨大的潛力與顯著的風險。演講者強調了 AI 在多個行業中的變革力量，包括醫療保健、金融和交通運輸，同時也談到了隨著 AI 快速發展而來的倫理和安全挑戰。

AI 的變革力量

AI 在革新各行各業方面具有巨大的潛力。在醫療保健方面，AI 驅動的診斷和個性化治療計劃可以顯著改善病人的治療效果。金融機構利用 AI 進行詐欺檢測和演算法交易，提高了效率和安全性。自駕車和智慧交通系統有望減少事故並優化交通流量，展示了

AI 在提升公共安全和便利性方面的能力。

倫理和安全的挑戰

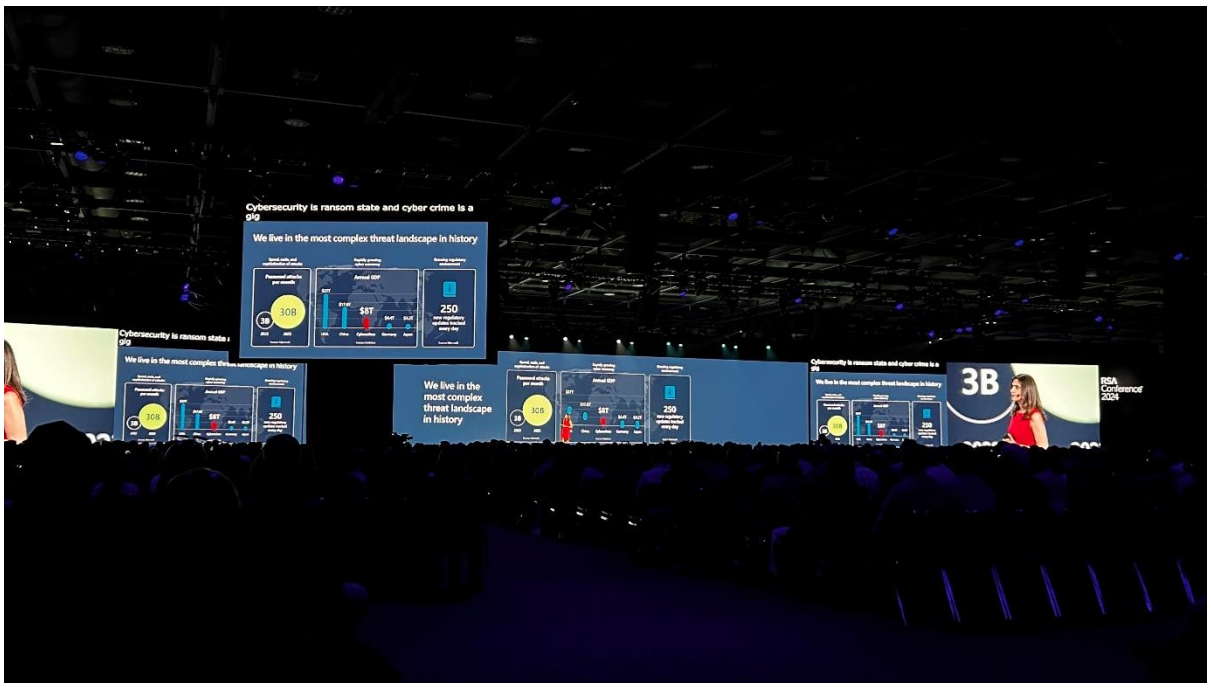
巨大的力量伴隨著巨大的責任。演講者強調了 AI 帶來的倫理困境，如演算法中的偏見、隱私問題以及潛在的工作替代。確保 AI 系統的透明、公平和負責至關重要，以減少這些問題。此外，與 AI 相關的安全風險，包括在網絡攻擊和虛假訊息活動中的惡意使用，則被強調為需要強有力的防範措施和規範。

法規與合作

為了在最大限度發揮 AI 的好處同時最小化其風險，演講者呼籲建立全面的法規框架和國際合作。制定清晰的 AI 開發和部署指南和標準對於確保安全和公平至關重要。跨國合作可以促進最佳實踐的分享和全球規範的建立，從而促進更安全和更公平的 AI 環境。

未來展望

展望未來，演講者設想了一個 AI 無縫融入日常生活並帶來利益的未來。然而，要實現這一願景，需要政府、企業領袖和公眾的共同努力，來應對 AI 的倫理、法律和社會影響。通過積極應對這些挑戰，社會可以釋放 AI 的全部潛力，同時保護人類的價值觀和利益。



(面對 AI 浪潮, 網路犯罪也在精益求精中)

AI Governance & Ethics: A Discussion with the Big Players

主題為「AI 治理與倫理：大玩家的討論」的座談會，聚焦於人工智慧（AI）的快速發展及其帶來的潛在風險和挑戰。這場討論由數位頂尖專家參與，包括來自 Microsoft、Google、NVIDIA 等公司的代表，他們共同探討了 AI 技術的安全性、信任以及合規性等問題。

會議首先強調了 AI 技術在全球市場中的迅速採用，同時也帶來了相應的風險和擔憂。討論中指出，AI 技術的發展不僅需要考慮到技術上的進步，還需在設計、部署和治理方面進行風險評估和緩解。專家們分享了各自企業在建立 AI 系統安全和信任方面的措施，以及他們對於新興標準的回應。

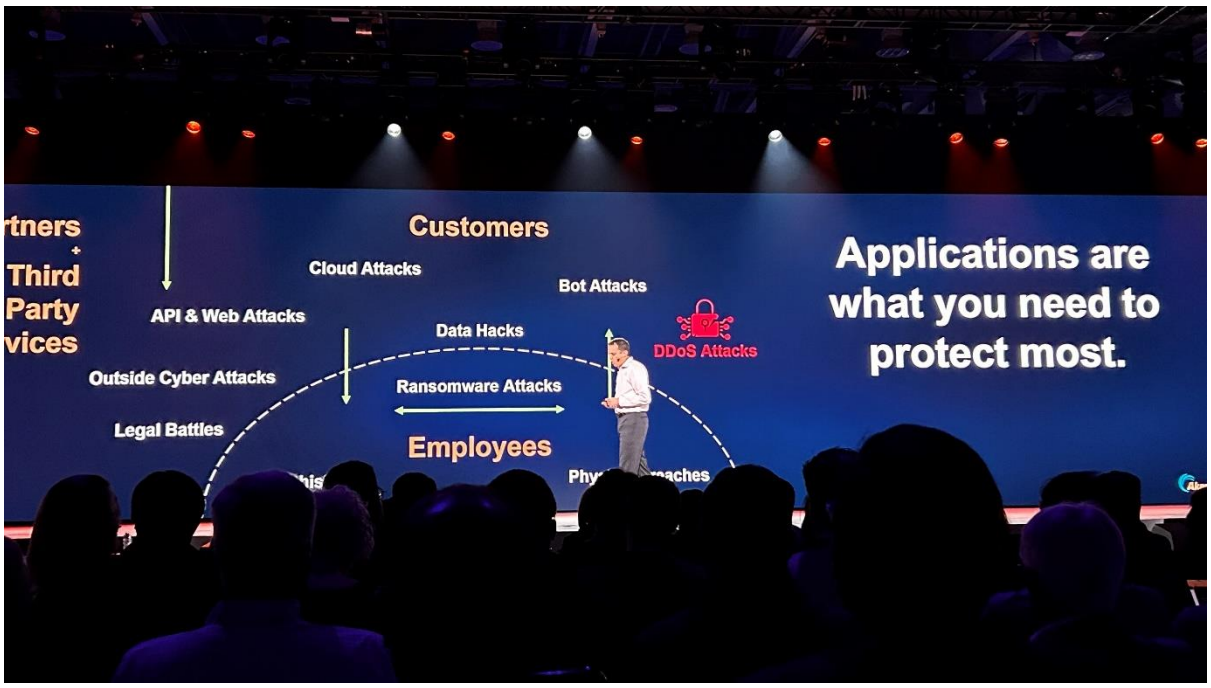
在討論 AI 治理時，專家們強調了合規性和網絡安全的關鍵角色。AI 的快速發展已經

引發了監管機構的高度關注，特別是在美國和歐洲。討論中提到的例子包括歐洲的 NIS2 指令和 DORA 規範，這些新規定擴大了對企業的網絡安全要求，並對 AI 技術的合規性提出了更高的標準。

此外，會議還探討了 AI 技術在網絡安全中的應用。例如，Snyk 收購了 DeepCode，利用 AI 進行代碼安全分析，這一舉動被認為是應對全球安全挑戰的重要步驟之一。專家們指出，這些收購和聯盟正在改變網絡安全的格局，推動了技術的融合和創新。

討論還涵蓋了國際合作在 AI 治理中的重要性。特別是在當前的地緣政治背景下，國家間的技術合作和標準制定變得尤為重要。專家們呼籲全球各國共同努力，建立健全的 AI 治理框架，確保技術的安全和可靠性。

總結來說，這場討論強調了 AI 技術發展的兩面，即在推動創新和進步的同時，也必須謹慎應對潛在的風險。與會專家一致認為，建立一個安全、可信和合規的 AI 系統，需要全球各方的共同努力和合作。



(專家學者、企業領袖輪番分享對資訊安全保護的見解)

Next-Gen SIEM: Converging Data, Security, IT, Workflow Automation & AI

CrowdStrike 的 CEO George Kurtz 發表的主題演講「Next-Gen SIEM: Converging Data, Security, IT, Workflow Automation & AI」強調了由 AI 和自動化驅動的下一代安全訊息和事件管理（SIEM）系統的變革潛力。Kurtz 指出，隨著網絡威脅的迅速發展和日益複雜，網絡安全創新變得至關重要。

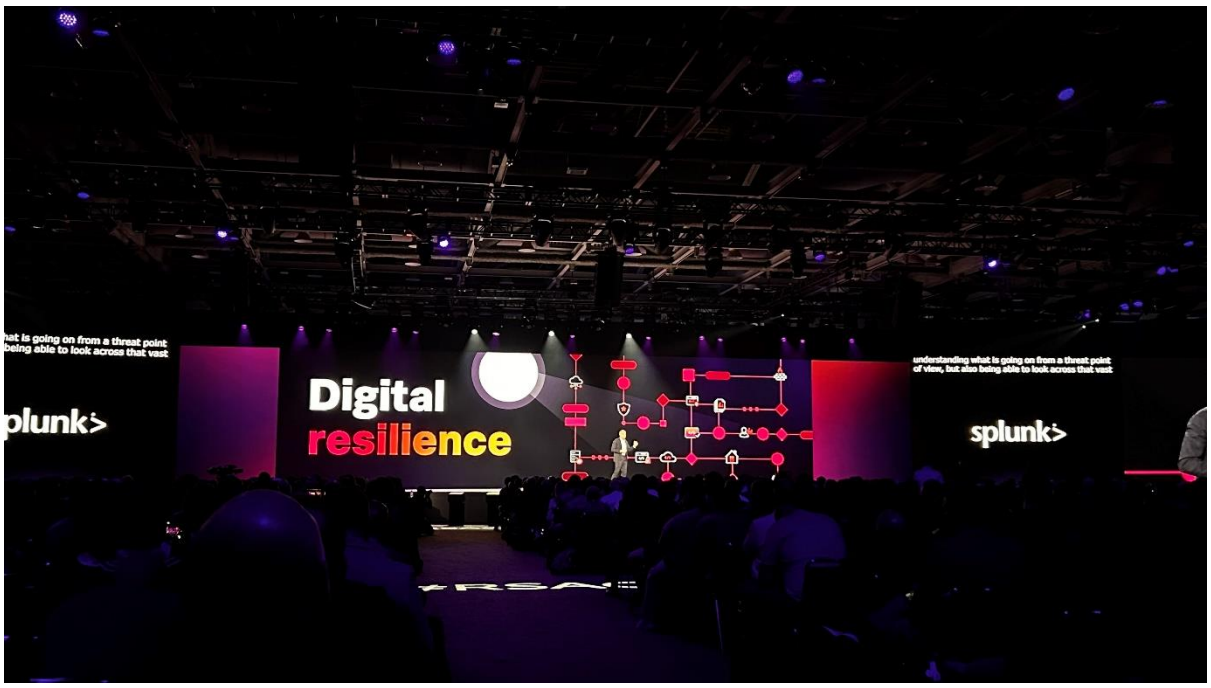
Kurtz 首先談到了傳統 SIEM 系統的不足之處，這些系統往往未能實現其實時威脅檢測和響應。相反地，這些系統只是成為數據囤積地，缺乏必要的速度和效率來有效對抗現代網絡威脅。他指出，攻擊者變得越來越快和高效，有些攻擊者能夠在幾分鐘內突破被入侵的系統並進行橫向移動。例如，CrowdStrike 觀察到一個攻擊者僅用了 31 秒

就下載了其工具包並開始進行偵察。

為了應對這些挑戰，他提倡採用一種現代化的 SIEM 方法，這種方法整合來自各種來源的數據，利用 AI 進行增強的威脅檢測，並使用工作流程自動化來快速響應。這種下一代 SIEM 系統旨在為安全運營中心（SOC）提供必要的工具，以利用 AI 和機器學習的能力超越對手。他強調了下一代 SIEM 系統的幾個關鍵特性和優勢：

1. **AI 集成**：通過整合 AI，這些系統可以快速且準確地分析大量數據，識別可能表明安全威脅的模式和異常情況。這使得更具前瞻性和預測性的安全措施成為可能。
2. **自動化**：工作流程自動化減少了威脅檢測和響應所需的手動工作，使安全團隊能夠專注於更具戰略性的任務。自動化響應可以顯著縮短威脅緩解時間，從而將潛在損害降到最低。
3. **數據融合**：整合來自各種 IT 和安全來源的數據提供對威脅的全面檢視，從而做出更明智的決策並制定更有效的安全策略。
4. **提高效率**：下一代 SIEM 系統設計得更加高效，減少了傳統 SIEM 解決方案的複雜性和開銷。這種效率有助於降低總擁有成本，同時提高安全成果。

Kurtz 在演講的最後敦促組織採用這些先進的 SIEM 系統，以保持對不斷發展的網絡犯罪分子的領先地位。他強調了網絡安全創新的重要性以及在快速變化的威脅格局中採取主動防禦措施的必要性。



(網路犯罪技術的精進, 資安產品也必須不斷推陳出新)

Tech Diplomacy: Building Cyber Resilience Together

座談會「技術外交：共同建立網絡韌性」，參與討論的有來自波蘭、烏克蘭、美國、德國和愛沙尼亞的網絡特使。包括：

- **Tadeusz Chomicki**，波蘭外交部
- **Anton Demokhin**，烏克蘭外交部
- **Nathaniel Fick**，美國國務院
- **Regine Grienberger**，德國外交部
- **Tanel Sepp**，愛沙尼亞外交部

討論要點

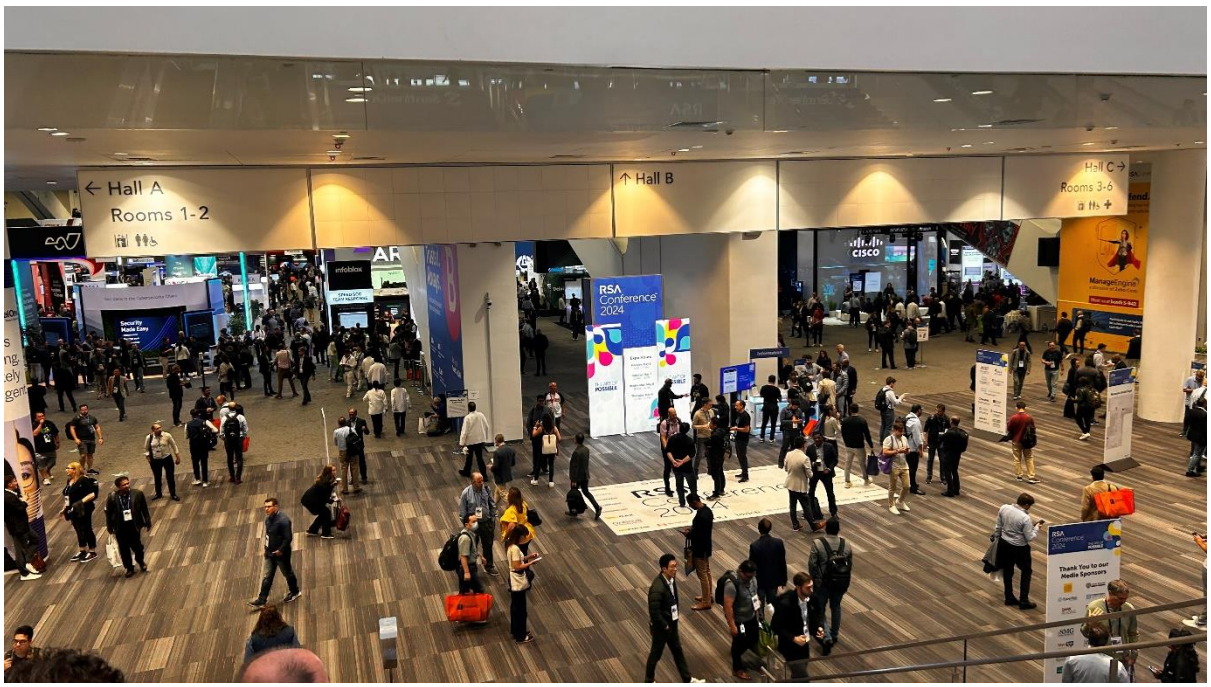
1. **國際合作在網絡安全中的作用**：強調面對敵對勢力利用技術破壞全球秩序時，國際合作的必要性。參與者強調通過合作努力建設網絡能力和韌性的重要性。
2. **烏克蘭在衝突中的網絡安全**：討論內容集中在俄羅斯入侵背景下烏克蘭的網絡安全環境。參與者分享了應對挑戰和保護烏克蘭數位基礎設施的策略，包括實時威脅響應和加強防禦措施。
3. **網絡特使的角色**：討論了網絡特使的角色，特別是他們在促進國際對話和合作方面的作用。各國特使分享了他們的經驗及其外交努力對建立安全數位環境的影響。
4. **塑造國際技術環境**：參與者探討了如何通過外交渠道和國際協議來塑造更具韌性和安全的技術環境。他們強調需要統一的政策和共享標準以有效緩解網絡威脅。
5. **挑戰與機遇**：討論涉及建立強大網絡防禦的挑戰與機遇。議題包括不同國家的政策差異、技術進步的速度和網絡威脅的複雜性。機遇方面，強調了通過國際合作在網絡安全實踐中創新的潛力。

各國特使見解

- **Tadeusz Chomicki** 討論了波蘭增強網絡能力的方法，重點在於培訓計劃和基礎設施改進。他強調需要持續投資於網絡安全，以適應不斷演變的威脅。

- **Anton Demokhin** 來自烏克蘭，詳細介紹了該國在持續衝突中加強網絡防禦的努力。他分享了一些成功的網絡操作案例，這些操作緩和了威脅並保護了關鍵基礎設施。Demokhin 強調了國際支持和共享情報的重要性。
- **Nathaniel Fick** 代表美國國務院，他強調網絡外交在建立促進全球網絡穩定的規範和協議中的作用。他指出美國領導的透明度和合作舉措，促進了國際夥伴間的信任。
- **Regine Grienberger** 來自德國，討論了歐洲在網絡外交方面的視角。她強調了歐盟的努力，創建一個統一的網絡安全政策框架，使成員國可以採用，確保協調應對網絡威脅。
- **Tanel Sepp** 來自愛沙尼亞，分享了愛沙尼亞先進的網絡基礎設施及其經驗如何塑造其網絡韌性方法。他強調了公私合作在制定有效網絡安全策略中的重要性。
- 參與者共同討論了各自國家所採取的各種技術進步和戰略舉措，包括開發先進的威脅檢測系統、網絡安全演習和模擬，以及實施嚴格的數據保護法規。
- 他們還強調了教育和意識計劃在培養網絡安全意識方面的重要性。討論中不斷提及需要擁有技能的網絡安全人才，並討論了吸引和培養這一關鍵領域人才的舉措。

  本次座談總結了國際合作和外交在應對網絡安全複雜性中的關鍵作用，並呼籲各國繼續對話和合作，共同建立一個具有韌性的全球網絡環境。



(South Stage 與 North Stage 相通的 B1 大展場為廠商產品展示交流區)

參展廠商攤位巡禮

位於 Sourth Stage 與 North Stage 共通的 B1 會場是百家爭鳴的廠商展示會場，此屆大小廠加總大約 600 家以上參展廠商，規模實在難得一見。各家廠商也使出渾身解數，努力吸引參訪者的目光，不只為了提升品牌知名度，也鼓勵各地專業人士上前討論與了解他們的產品與技術。提供以下幾間與我有互動的商家:

1. **CrowdStrike:** 提供基於雲端的端點保護平台，專注於威脅情報和端點偵測及回應（EDR），能夠快速識別和應對複雜的攻擊，並強調 AI 新世代 SIEM。
2. **FireEye:** 專注於網絡安全威脅情報和事件回應，提供先進的威脅偵測和分析平台，幫助企業預防和回應網絡攻擊。
3. **Fortinet:** 提供全面的網絡安全解決方案，包括防火牆、入侵防護系統（IPS）

和安全 SD-WAN，確保網絡的高效運行和安全性。

4. **Palo Alto Networks:** 提供下一代防火牆和雲安全解決方案，專注於威脅防護和零信任網絡架構，保障企業數據和應用的安全。
5. **Check Point:** 專注於網絡安全解決方案，提供防火牆、移動安全和雲安全產品，幫助企業保護其數據和基礎設施。
6. **Cisco Systems:** 提供全面的網絡安全解決方案，包括防火牆、入侵防護系統和安全網關，確保企業網絡的安全運行，並在會場建立新世代 SOC 情報中心。
7. **McAfee:**專注於端點安全和威脅防護，提供全面的反病毒和防間諜軟體，保護個人和企業免受網絡攻擊。
8. **Symantec (Broadcom):** 提供全面的網絡安全解決方案，包括端點保護、數據保護和雲安全，幫助企業保護其數字資產。
9. **Tenable:** 專注於漏洞管理和合規性，提供先進的漏洞掃描和風險管理解決方案，幫助企業識別和修復安全漏洞。
10. **Splunk:** 提供數據分析和安全信息及事件管理（SIEM）解決方案，幫助企業收集、分析和可視化其網絡數據，從而實現安全監控和威脅偵測。
11. **Proofpoint:** 專注於電子郵件安全和防護，提供反釣魚、反垃圾郵件和數據洩露防護（DLP）解決方案，確保企業的電子郵件通信安全。
12. **Aqua Security:** 專注於雲原生安全，提供容器和 Kubernetes 安全解決方案，幫助企業保護其雲原生應用程序和基礎設施。

13. **Armis:** 提供物聯網（IoT）和運營技術（OT）安全解決方案，專注於可見性、風險管理和威脅偵測，確保連接設備的安全。
14. **Okta:** 專注於身份和訪問管理（IAM），提供單點登錄（SSO）和多因素認證（MFA）解決方案，幫助企業確保用戶身份的安全。
15. **CyberArk:** 提供特權訪問管理解決方案，專注於保護關鍵數據和系統免受內部和外部威脅，確保企業的數字資產安全。

這些參展廠商代表了當今網絡安全領域的最先進技術和解決方案，涵蓋了從端點保護、威脅偵測到雲安全和身分辨識管理等多個方面，其中也不乏採用 AI 技術來完備更全面的防禦。這些公司在 2024 RSA 大會上展示其最新的創新技術和資安產品，目的在幫助企業應對不斷變化的網絡威脅和挑戰。

(沙盒實驗室, 分為多個攤位提供情境式實作演練)

心得與建議

參加 2024 RSA Conference 是一次令人振奮且深受啟發的經歷。這次會議的主題"可能的藝術"，字面上就帶給我們很大想像空間，畢竟在科技發展日新月異的今天，很多事都不無可能，加上這兩年 AI 技術蓬勃發展，應用場景隨處可見，相同的，對應在網路犯罪攻擊也不無可能，運用 AI 進行各式的駭客行為已成為不可避免的趨勢；今年的議程中多數的話題皆圍繞在 AI，脫離不了相關的總總面向，水能載舟亦能覆舟正好說明了 AI 在當今的重要性，它是雙面刃，能拿來做防守的工具，當然也能作為攻擊的利器，這一攻一防，端看正邪兩方如何做好最全面的措施與各方的通力合作。

RSA 大會不僅是一個技術交流的社區平台，更是一個促進合作與創新的場域。通過參與 RSA 大會，與會者除能夠了解最新的行業趨勢、獲取尖端的技術分享，並可建立寶

貴的同業聯繫。這些都將幫助企業和組織在日益複雜的網路環境中維持穩定安全並保有競爭優勢。

總之，RSA 大會是網路安全領域的年度盛事，對推動全球網路安全的發展、促進技術創新和合作具有重要意義。台灣是先進半導體製造國家，不論軍事位置或科技發展在國際均有一定的重要地位，身處台灣，我鼓勵同仁有機會多參與此類型具有國際性、前瞻性代表的大型會議，打開視野，接收最新最優秀的技術分享。

建議未來參加此類型會議的同仁：

1. **積極參與專題講座**：這些講座提供了寶貴的學習機會，可以直接從業內領袖和專家那裡獲得最新的知識和洞見。
2. **廣泛交流與體驗沙盒演練**：利用大會的網絡平台與沙盒演練，與來自不同背景和領域的專業人士交流，建立人脈並分享經驗。
3. **關注新興技術**：了解最新的安全技術和趨勢，特別是人工智慧、雲端安全和零信任架構，這些技術將在未來的網絡安全領域中扮演重要角色。