出國報告（出國類別：定期會議）

出席 2023 美國舊金山 RSA 大會
暨美商資安交流活動
出國報告

單位名稱：數位發展部 闕河鳴 政務次長
數位發展部 陳睿臻 專案規劃師
數位發展部 吳銘仁 副司長
數位發展部 鄭欣明 副署長
數位發展部 黃哲上 簡任視察
數位發展部 邱俊霖 科長
數位發展部 杜欣怡 科長
財團法人電信技術中心 王秉豐 經理
財團法人電信技術中心 謝昀羲 副工程師
財團法人電信技術中心 曾尹宣 副管理師

派赴國家：美國 舊金山
出國期間：112 年 4 月 22 日~112 年 4 月 30 日
報告日期：

摘要

RSA Conference(國際資訊安全會議，簡稱 RSAC)為全球最大且最具權威的資訊安全業界標竿會議及展覽。本次會議於 2023 年 4 月 24 至 27 日於美國舊金山莫斯康展覽中心(Moscone Center)辦理，會議主題為 Stronger Together，超過 500 家資安廠商參展，匯集超過 650 名專家、學者和政府人員擔任講座，提供 33 場主題演講和超過 350 場小組討論會議及研討課程，吸引來自世界各地 140 多個國家超過 4 萬名資安領域人士與會，熱門議題包含資安地緣政治、供應鏈安全、最新資安攻擊技術及解決方案、政府單位間與公私部門合作、國際資安聯防合作倡議、雲端安全、零信任架構等。訪團除蒐集各相關意見，瞭解美國政府及各大企業最亟待解決的資安議題外，也藉機於場邊與美國政府官員及廠商進行交流，就雙方合作各項議題進行討論。

目錄

壹、 目的

我國由於政經情勢特殊，所受各項資安威脅未曾消退，總統亦多次宣示「資安即國安」的核心理念，使資安相關議題成為政府與民間各界共同關注的焦點；俄烏戰爭爆發前後資安攻擊事件頻傳，更使全世界愈發重視資安防護的重要性。

緣此，本次應美國在台協會(AIT)邀請，由數位發展部闕河鳴次長率團參訪 RSA Conference 2023(國際資訊安全會議，下簡稱 RSAC)，除瞭解最新資安威脅議題及各國政府與企業因應做法、掌握資安業界最新技術發展趨勢、蒐集潛在攻擊樣態及解決方案資訊，並發展未來資安政策布局方向建議外，亦借此機會與美國官員會晤，就雙方關切議題及合作方向進行交流，協助我國與國際資安趨勢接軌，同時與友好國家建立並強化領域內國際合作關係。

本次參訪期能達到三大目的：

1. 知識交流與學習： RSAC 匯集世界各地的資安專家，藉由這個平台，團員得以分享、交流資安領域的知識和專業，並從其他國家和組織的經驗中學習，以提升我國於資安領域的能力和洞察力，並更好地應對日益複雜的安全挑戰。
2. 發展政策制定方針：RSAC 的講者之一 NIST 為制定美國資訊安全政策和制度的一個重要角色，藉由參與 NIST 的相關會議，能夠吸取有關政策和制度的討論，並對其發展提出建議和貢獻；此外，亦能藉由瞭解國際資安趨勢，調整及擬定相關政策發展方向，強化我國資安韌性。
3. 促進國際合作： RSAC 作為一個國際性的安全大會，吸引了來自全球各地的政府官員、安全專家、學者和業界代表，供了寶貴的交流平台，透過參加 RSAC，團員得以從政府及學術等不同面像與來自各國的資安專家建立關係，藉由分享經驗、見解和資源，共同應對全球安全挑戰；此外，本次亦安排與美方人員交流，期能建立更加穩定的合作關係，共同強化安全的國際秩序。

貳、 行程

日期	行程
4 月 22 日 (六)	啟程，前往美國舊金山
4 月 23 日 (日)	RSCA 報到、領取相關會議手冊及資料袋、開幕前交流會
4 月 24 日 (一)	RSAC 會議- (一)假訊息是新的惡意軟體(Misinformation Is the New Malware) (二)網路營運整合：CISA 與 CyberCom-CNMF 夥伴關係 (Integrating Cyber Operations: CISA & CyberCom-CNMF Partnership) (三)反思諸神的黃昏：烏克蘭入侵後的網路威脅情勢 (Reconsidering Ragnarok: The Cyber Threat Terrain After the Ukraine Invasion) (四)嗡嗡作響：監視俄羅斯在烏克蘭戰爭中的噪音 (Droned Out: Surveilling the Noise in the Russian War in Ukraine) (五)如何在大型企業衡量軟體供應鏈的來源安全 (Scaling Software Supply Chain Source Security in Large Enterprises) (六)揭露事實 – 消費者零信任架構的個案研究 (Unveiling the Truth – A Case Study on Zero Trust for Consumers) (七)地緣政治韌性：為何營運韌性不再足夠 (Geopolitical Resilience: Why Operational Resilience Is No Longer Enough) (八)危險的貼文：社交媒體中暴露的生物識別風險 (Perilous Posts: The Risks of Biometric Patterns Exposed in Social Media) (九)RSAC 創新沙盒競賽 (RSAC Innovation Sandbox Contest) 美商資安交流活動 (一)Mandiant at RSAC for APJ Delegation Program & Google Campus 參訪
4 月 25 日 (二)	RSAC 會議- (一) 建立國際聯合部隊以擴大防禦規模(Building International Coalitions to Scale Defense) (二)密碼學家對談(The Cryptographers' Panel)

	(三)誰說資安不能具有創造性?(Who Says Cybersecurity Can’t Be Creative?) (四) Emotet 曝光：網路犯罪分子供應鏈的內幕 (Emotet Exposed: Insider the Cybercriminal's Supply Chain) (五)軟體材料表上的世界(The World on SBOMs) (六)網路釣魚：NIST 網路釣魚規模與網路安全意識 (Phishing With a Net: The NIST Phish Scale and Cybersecurity Awareness) (七)攜手更強大：美國-烏克蘭網路合作關係(Stronger Together: The US-Ukrainian Cyber Partnership) (八)駭客的雲端治理指南(The Hacker's Guide to Cloud Governance) (九)NIST 800-207 指南：零信任議題的概念到提案(A NIST 800-207 Playbook: Zero Trust from the Whiteboard to the Boardroom) 美商資安交流活動- (一)Striderintel (二)Fidelis Cybersecurity
4 月 26 日 (三)	RSAC 會議- (一)2023 年及其後的安全：自動化、分析和架構 (Security in 2023 and Beyond: Automation, Analytics and Architecture) (二)五種最危險的新型攻擊技術(The Five Most Dangerous New Attack Techniques) (三)沒有更多的時間：縮小與攻擊者的差距(No More Time: Closing the Gap with Attackers) 美商資安交流活動- (一)Mandiant (二)SailPoint 資安新創公司拜訪與交流- (一)Skydio, Inc.
4 月 27 日 (四)	參加 RSA- (一)從公司部門夥伴關係到營運合作(From Public-Private Partnerships to Operational Collaboration)

	(二)在 OT/ICS 環境中保持對抗性 AI 的領先地位——緩解 CWE-1039 (Stay Ahead of Adversarial AI in OT/ICS Environments – Mitigating CWE-1039) (三)NIST 網路安全框架 v2.0：改變何在？(NIST Cybersecurity Framework v2.0: What's changing?) (四)40 位 CEO 告訴我們的關於建立網絡彈性的事 (What 40 CEOs Told Us About Building Cyber Resilience) (五)這是一段旅程……NIST 將以網路安全框架為首 (It's a Journey…Where is NIST Headed with the Cybersecurity Framework) (六)保衛電動汽車充電網路的攻擊面和數據孤島 (Protecting the Attack Surface and Data silos of an EV Charging Network) 美商資安交流活動- (一)Varonis
4 月 28 日 (五)	美商資安交流活動- (一)Palo Alto Networks
4 月 29 日 (六)	返回臺灣
4 月 30 日 (日)	抵台

參、 團員名單

姓名	單位	職稱
闕河鳴	數位發展部	次長
陳睿臻	數位發展部政務次長室	專案規劃師
吳銘仁	數位發展部韌性建設司	副司長
鄭欣明	數位發展部資通安全署	副署長
黃哲上	數位發展部資通安全署	簡任視察
邱俊霖	數位發展部資通安全署	科長
杜欣怡	數位發展部產業發展署	科長
王秉豐	財團法人電信技術中心	經理
謝昀羲	財團法人電信技術中心	副工程師
曾尹宣	財團法人電信技術中心	副管理師
林盈達	資通安全研究院	副院長
彭敏君	資通安全研究院	經理
彭妍之	資通安全研究院	規劃師
鄧惟中	亞洲·矽谷計畫執行中心	人資長
簡志穎	亞洲·矽谷計畫執行中心	經理
王邦傑	財團法人工業技術研究院	經理
古涵詩	財團法人工業技術研究院	研究員
林岳	財團法人資訊工業策進會	業務總監
吳東杰	財團法人資訊工業策進會	副主任

肆、　會議過程及內容

一、　RSAC 2023 概述

RSAC 2023 主題為“Stronger Together”（攜手更強大），強調合作的重要性，席間各項議題討論，經出國人員觀察、分析與綜整，可大致分為策略面、技術面與國際合作面等 3 大部分，討論層面含括資安地緣政治、供應鏈安全、最新資安攻擊技術分享、政府單位間與公私部門合作、國際資安聯防合作倡議等都是各界迫切關注的議題。

RSAC 包含會議及展覽，規模摘要如下[1]：

- 超過 500 家供應商
- 超過 650 位演講者
- 超過 40,000 名與會者
- 33 場主題演講(Keynotes)
- 超過 350 場小組討論會議及研討課程(Sessions)

[1] Businesswire(2023), RSA Conference Concludes 32nd Annual Event by Convening Strong Cyber Community and Experts Together 檢自 https://www.businesswire.com/news/home/20230428005105/en/RSA-Conference-Concludes-32nd-Annual-Event-by-Convening-Strong-Cyber-Community-and-Experts-Together (2023,Jun 12)

二、 講座及研討會

(一) 假訊息是新的惡意軟體(Misinformation Is the New Malware)

本議題由 Catherine Gellis 律師、Alethea 協會 Lisa Kaplan 及 UC Berkeley 大學的 Yoei Roth 擔任講座。

講座認為，目前各國都有假訊息氾濫的問題，因此對於遏止假訊息也發展出許多作法。由於假訊息有簡單、低成本、快速傳遞且難以評估衝擊的特性，與一般資安攻擊並不相同。假訊息為何有效，是因為根本無從知悉假訊息從何而來、難以從源頭追溯假訊息由何處產生，也因此無法預先防範與事先防堵，因此，各國雖積極發展相關作法因應，但都未能發展出成熟有效的作法。

由於美國憲法第一修正案 (First Amendment to the United States Constitution)內容係保障人民言論自由，因此在言論自由保障與防範假訊息兩者之間，有其難以達到平衡之處。為了避免寒蟬效應(chilling effect)，並遵守憲法第一修正案，禁止假訊息傳播為政府最後手段(last resort)。

與會講座分析，假訊息具有多面向威脅的特性，如果只就單一方式或管道進行防範，難收全面圍堵之效，並可能從其他管道滲透而衍生問題，因此不能以單位孤立的方式(no isolation)處理假訊息的威脅。目前美國政府單位各行其是(silo agency)，是造成無法有效打擊假訊息之主因。

從法規面而言，目前美國相關法令並未統整對於防範假訊息的一致性與連貫性，因此在法規層面的禁止上，無法形成法規範與法遵循的緊密連結，這也是造成人民無法落實法律的另外一個主要原因。

此外，許多社群媒體被高度使用，以 TikTok 為例，美國有許多人高度使用該 app，尤其是年輕人特別喜愛觀看 TikTok 並透過 TikTok 分享影片，但他們並不瞭解個人資料有被盜取的風險、以及中國政府有意透過 TikTok 傳遞假訊息，以攻擊美國等國家之民主制度與國家安全的背後意圖。

講座認為，未來如欲有效遏制假訊息氾濫與傳播，應該從以下方面進行推動：

1. 法制面：應有效釐清寒蟬效應與美國憲法第一修正案間之界線，並藉此統整美國國內各法令禁止假訊息散布的相關內容，建立法規範之一致性。

2. 制度面：政府應建立更完善的訊息分享機制，協助各機關爭取時間釐清假訊息謬誤之處，並建立假訊息統一回應窗口；一方面可有效降低假訊息傳遞速度、另方面設立澄清機制，則可有效降低假訊息的負面衝擊。

3. 國際合作面：各國間也應強化相互合作，以面對假訊息傳播的議題與訊息共同分享，共同打擊假訊息氾濫的問題。

(二) 網路營運整合：CISA 與 CyberCom-CNMF 夥伴關係(Integrating Cyber Operations: CISA & CyberCom-CNMF Partnership)

本議題由 CISA 的助理執行局長(Executive Assistant Director)Eric Goldstein 及美國國防部網戰司令部（Cyber Command, CyberCom）網路國家任務小組(Cyber National Mission Force, CNMF)William Hartman 將軍共同分享組織合作現況。

本場分享美國政府針對網路一項新興的反網路攻擊策略，及如何運用此策略來更好地保護組織的資訊安全。會議重點包括：

1. Hunt Forward 行動的核心原理和目標：深入探討了此行動的基本原理，旨在提高組織對網路攻擊的預防和應對能力。

2. 實施方法和案例：分享了 Hunt Forward 行動的具體實施方法，並介紹了一些實際應用案例，以顯示該策略在保護組織資訊安全方面的效果。

3. solarwinds 事件分析：以 solarwinds 事件作為一個具有代表性的資訊安全事件，並以該事件中的攻擊行為和反制行為的時間序為例，展示了如何應用 Hunt Forward 行動的執行方式來應對類似的攻擊。

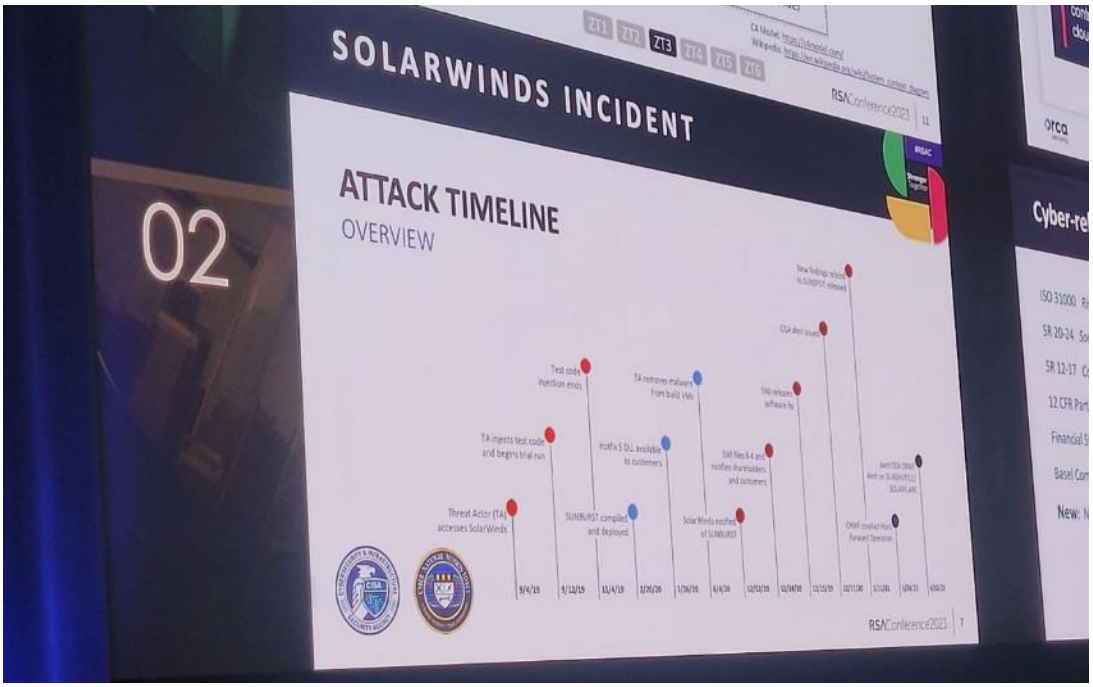


圖 1、資安事件 solarwinds 事件時間線

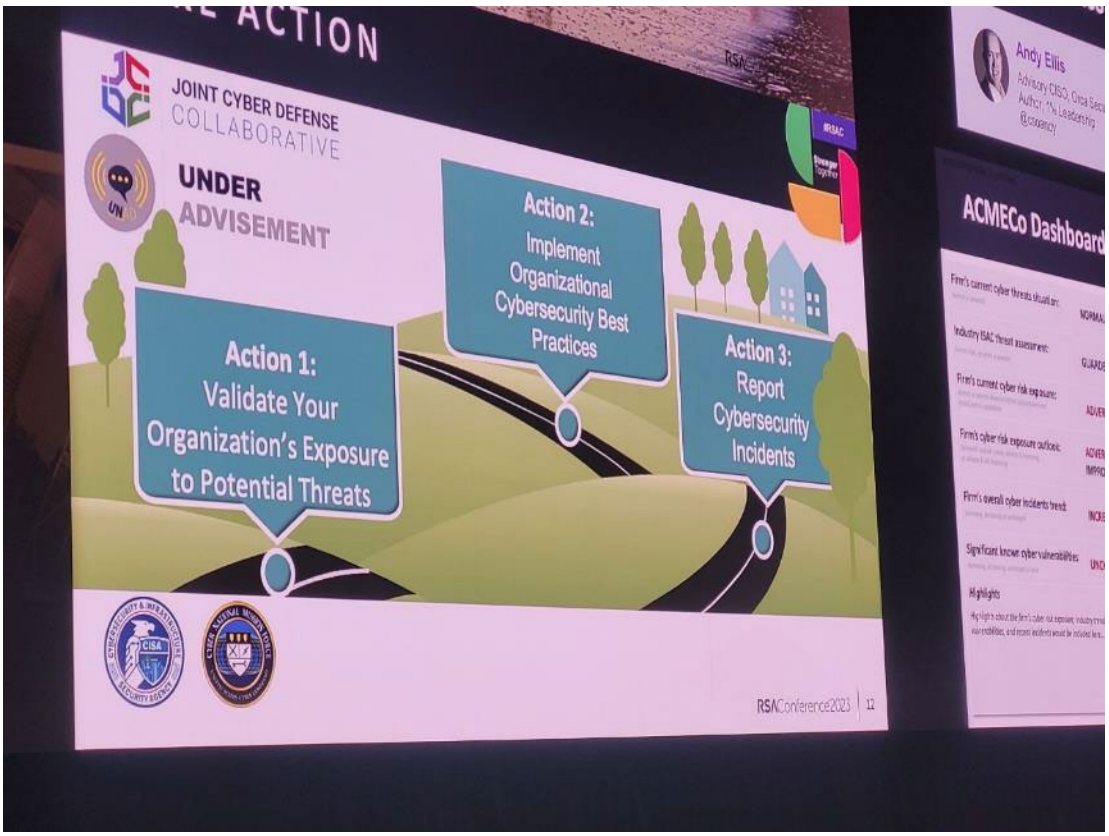


圖 2、Hunt Forward 行動步驟

Eric Goldstein 助理執行局長及 William Hartman 將軍說明兩單位強化美國網路安全作法，包括：

1. 增加敵人進行網路攻擊的成本：Eric Goldstein 及 William Hartman 皆認為，現今網路攻擊氾濫、勒索軟體犯罪組織愈發猖獗，再加上目前全球政經局勢的變化，要完全杜絕網路攻擊無異緣木求魚。因此目前美國策略在於進行適當佈署，增加敵人網路攻擊成本，進而嚇阻敵人的攻擊意圖。
2. 迫使改變敵人的模式：透過掌握威脅模式、評估潛在風險、掌握網路攻擊模式等，預先瞭解己方的各項資安風險，並做好相關防範措施，迫使敵人放棄以往攻擊模式，進而放棄攻擊目標。
3. 快速回應敵人的網路攻擊：一旦發現網路攻擊或可疑的網路行為，就應以最迅速方式進行回應，讓敵人知悉被攻擊目標已做好相關準備，進而促使敵人放棄攻擊。
4. 相互合作並建立深入夥伴關係：無論是 CISA 或 CNMF 都認為，單位之間建立相互信任合作關係、共享資安情資、共同打擊資安威脅與攻擊，有助於建構完善安全的資安環境。

CNMF 表示有超過 2,000 名經過長期訓練且對於保障國家網路安全具高度熱誠的服務人員，有效執行國家所賦予的網路安全維護相關任務。CNMF 雖也與其他政府部門合作，但最重要的還是跟國土安全部(Department of Homeland Security)的合作最為密切。為了有效及精準執行網路安全任務，CNMF 必須與 CISA 快速分享情資、共同打擊目標網路威脅。此外，CNMF 不僅與 CISA 高階人員以安全網路通話方式快速交流訊息，也與一般工作階層的網路分析師及工程師就技術面深入合作。

當遇到可疑的網路活動，CISA 與 CNMF 會標註該可疑活動，並適度擴大該可疑活動的影響範圍，以做好更有效的防範工作。CNMF 也會迅速找到攻擊來源、讓敵方知道 CNMF 已做好相當準備，藉此嚇阻敵方的進一步攻勢。因此對 CNMF 來說，如何部署(deploy)相關資源、中斷(disrupt)敵方攻擊、嚇阻(deter)敵方攻擊意圖，以及探查(detect)對方攻擊來源及手法，也是其重要工作項目。

最後對於 2020 年美國總統大選期間所遭受的網路攻擊威脅，CISA 與 CNMF 都表示，敵方惡意攻擊並未有效影響美國選舉之投票與計票系統(voting and tallying system)，美方相關單位也都阻敵於先(get ahead of these malicious activities)，並與負責選舉的權責機關相互合作(work with election

jurisdiction)，中斷與破壞敵方持續性的威脅(disrupt the persistent and ongoing threats)。對於 2024 年總統大選，如何確保美國選舉系統免於網路攻擊、保障美國民主制度，更是 CISA 與 CNMF 的首要任務。

CISA 另外也說明，為了結合國際勢力對抗資安危脅，CISA 也與全球公、私部門組織成立聯合網路防務合作小組(Joint Cyber Defense Collaborative, JCDC)：

1. 建立網路安全策略性與實務性的聯盟(Strong strategic and operational alliances within the cybersecurity community)。
2. 提高對網路威脅態勢的可見性和洞察力(Increased visibility and insight into the cyber threat landscape)。
3. 透過多樣化資源與專業知識，以推動具有創造性的網路安全解決方案(Diverse resources and expertise to fuel creative cybersecurity solutions)。
4. 大量強化蒐集、分析、分享資安情資以防範資安威脅的能力(Vastly amplified capacity to gather, analyze, and share information to defend against cyber threats)。

(三) 反思諸神的黃昏：烏克蘭入侵後的網路威脅情勢(Reconsidering Ragnarok: The Cyber Threat Terrain After the Ukraine Invasion)

本議題由 Loeb & Loeb 的合夥人 Chris Ott 擔任主持人、舊金山 FBI 的助理特工主管(Assistant Special Agent in Charge) Elvis Chan 及 Unit 42 的 CTO & 工程 VP 暨 Palo Alto Networks 的威脅情報員(Threat Intelligence) Michael Sikorski 擔任與談人。

本會議聚焦於美烏網路夥伴關係(US-Ukraine cyber partnership)議題，介紹烏克蘭與俄國戰爭中俄國如何透過網路攻擊影響烏克蘭的政權及攻擊重要節點，以達到戰略目的，這些攻擊包括常規的漏洞入侵、服務阻斷攻擊以及破壞組織的不實訊息攻擊等。

詳細的網路攻擊包含：

1. 漏洞入侵：攻擊者利用已知或未知的軟體漏洞，進入目標系統並獲取控制權。這可能涉及操縱操作系統、應用程序或網路協議的弱點。

2. 服務阻斷攻擊（DDoS）：攻擊者通過向目標系統發送大量流量或請求，癱瘓其處理能力，從而使其無法正常運作，這導致網路服務失能，對烏克蘭的政權和關鍵基礎設施造成嚴重影響。

3. 不實訊息攻擊：攻擊者散佈虛假、誤導性的訊息，旨在操縱民眾的觀點、調動情緒或破壞組織聲譽。這種攻擊通常利用社交媒體平台和網路傳播，可以對烏克蘭的政治和社會氛圍產生重大影響。

4. 深偽技術(Deepfake)攻擊：在會中也說明了 ChatGPT 等強 AI 的出現，讓不實訊息(社交攻擊)這類的攻擊，更為氾濫且難以識別，因為這些 AI 服務降低了攻擊成本，並提升不實訊息的內容品質及數量，加劇混淆人員對攻擊手段的識別，這些攻擊手法在烏克蘭與俄國之間的衝突中可能受到廣泛應用，並對烏克蘭的政權和關鍵基礎設施造成實質威脅。

圖 3、Reconsidering Ragnarok: The Cyber Threat Terrian After the Ukraine Invasion 會議

(四)　嗡嗡作響：監視俄羅斯在烏克蘭戰爭中的噪音(Droned Out: Surveilling the Noise in the Russian War in Ukraine)

本議題由 Recorded Future 的副威脅情報分析師 Alexander Leslie 擔任講座。

本場議程主要聚焦於烏俄戰爭對網路生態與網路攻擊變化的影響，包含以下議題與討論內容。

1. 戰爭中攻擊參與的組織與團體有哪些，主要的攻擊方式與特徵為何？

由圖 4 可見俄方的攻擊力量與陣營相對較多，包含中國、伊朗等國家的攻擊力量，烏克蘭方除烏克蘭自己的軍事力量外，還有部分是反俄或西方的志願力量。

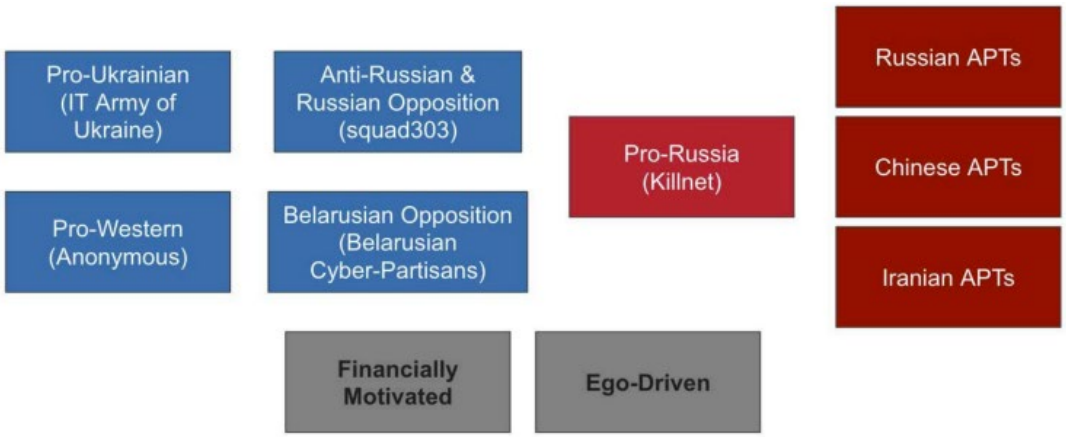


圖 4 、俄烏戰爭網路攻防陣營

而俄羅斯佔據了約 60%的所有聲稱的網路攻擊，這表明俄羅斯在網路攻擊活動中扮演了重要角色，涉及了大量的個人和組織。

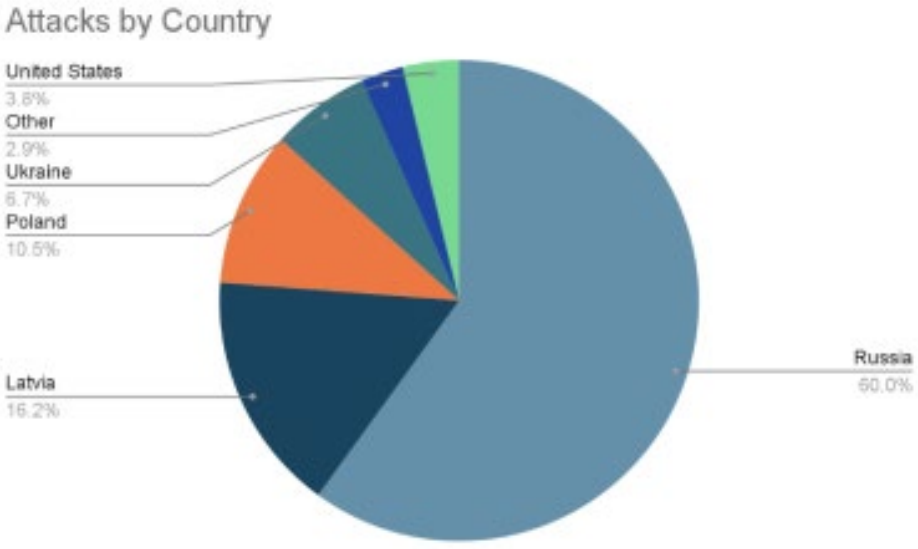


圖 5 、網路攻擊類型分布圖

在攻擊類型中，分散式阻斷服務攻擊(DDoS)佔據了所有攻擊的 94%。網站篡改佔據了 3%，這顯示了 DDoS 攻擊是最常見的攻擊類型，被廣泛用於干擾目標的網路服務可用性。

而烏克蘭軍隊聲稱其發起了大多數針對俄羅斯的攻擊，數量約為 750 個。但其中只有約 150 個可以得到證實，這可能顯示了烏克蘭的技術軍隊與力量參與了大量的網路攻擊，但對其聲稱發起的目標進行驗證真實性存在一定的難度。

這些關鍵發現顯示了網路攻擊的一些趨勢和參與者的分佈情況，俄羅斯在網路攻擊中的存在佔據主導地位，而 DDoS 攻擊是最常見的方式。烏克蘭聲稱發起大量攻擊目標，但驗證這些攻擊的真實性存在挑戰，並不一定全部為真實的，可能有戰略與宣傳考量。但這些發現能夠為進一步研究於戰爭發生時，不同陣營的網路安全攻擊與防禦提供了有價值的參考訊息與研究方向。

在攻擊目標方面，俄羅斯金融部門佔 26%、俄羅斯政府服務佔 12%、俄羅斯關鍵基礎設施佔 7%，然而受到匿名者攻擊，能有效查證的受攻擊目標中，約 30 個裡目前只有 4 個聲稱的網路攻擊有確實的證據。

2. TTPs、IOCs 是什麼？

TTPs 代表技術、戰術和程序(Tactics, Techniques, and Procedures)。它是一種描述攻擊者在進行網路攻擊或滲透時使用的方法、技術和行為的框架。TTPs 可以包括攻擊者使用的惡意軟體、漏洞利用技術、社交工程手段、網路偵察方法等。瞭解和分析攻擊者的 TTPs 可以幫助網路安全專業人員識別和應對潛在的威脅。

IOCs 代表攻擊識別指示器(Indicators of Compromise)。它是一種用於識別可能遭受到威脅或已經受到攻擊的系統或網路的特定指示器。 IOCs 可以是特定的 IP 地址、域名、文件雜湊(Hash)、惡意軟體的特徵、異常行為模式等。通過監測和分析 IOCs，網路安全團隊可以識別出已知的威脅和攻擊，採取相應的防禦和響應措施。

TTPs 和 IOCs 通常在威脅情報和安全運籌時使用。通過收集、分析和共享關於攻擊者的 TTPs 和已知的 IOCs，安全專業人員可以更好地瞭解和預防潛在的威脅，並加強網路防禦和響應能力。

3. 俄羅斯在烏克蘭的戰爭如何改變了網路犯罪威脅格局與趨勢？從戰爭

的第一年可以吸取哪些教訓，如何將這些教訓應用到未來的地緣政治危機中？

暗網論壇公告因開發相關軟體人力缺乏，暫時無法繼續進行開發，可能跟俄烏戰爭開始影響部分駭客的主要攻擊方向，以及俄羅斯部分動員令有關。

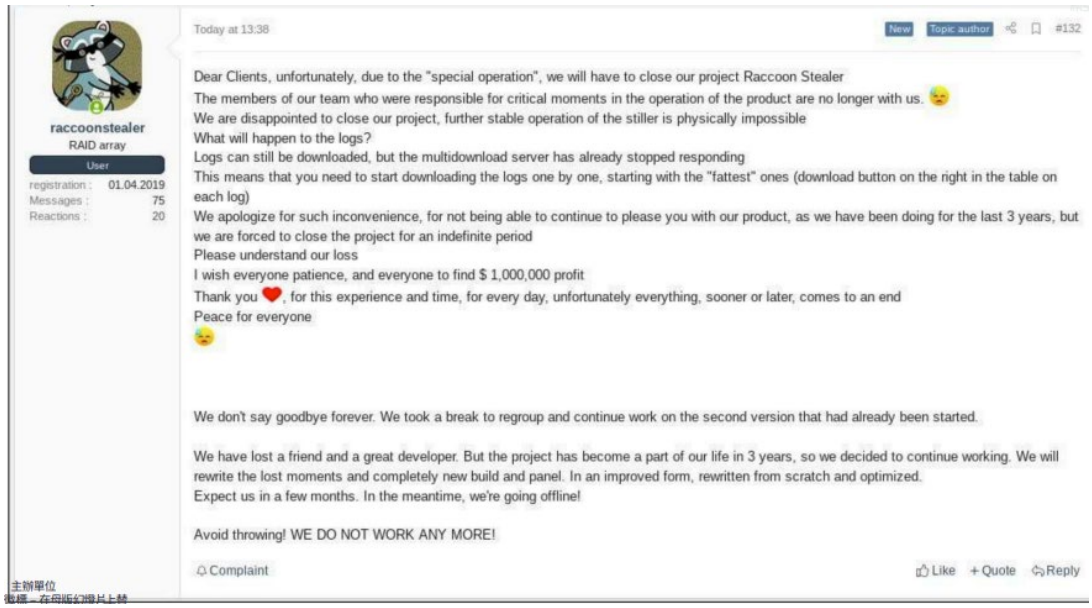


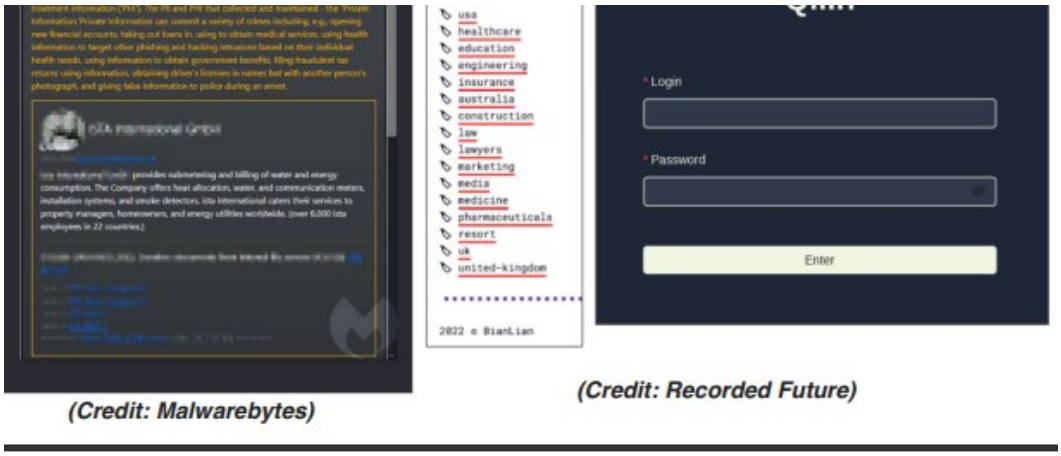
圖 6 、駭客論壇公告

我們無法確定惡意軟體的需求與相關詢問度提高的確切原因，但可能與戰爭的需求、或是相關駭客因戰爭而被徵召或是改變其開發、攻擊行為模式有關。

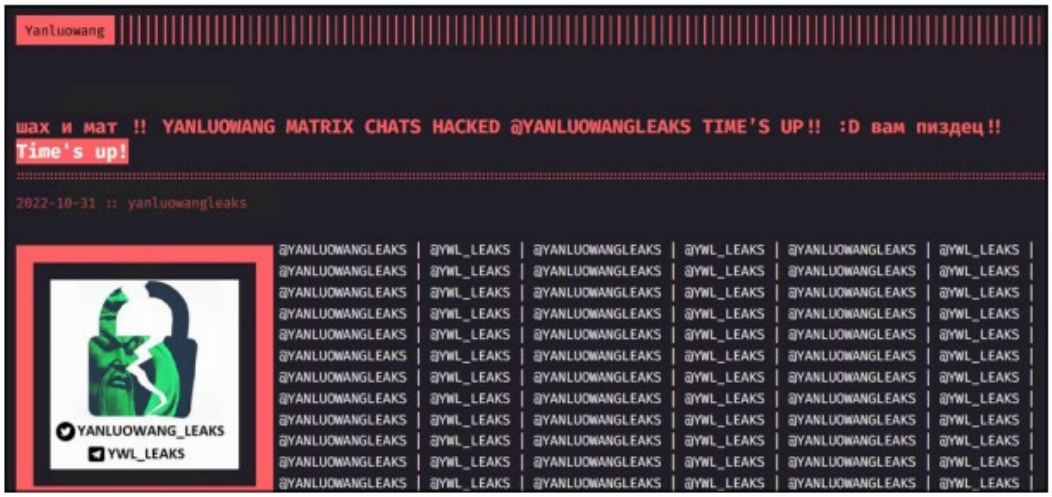
圖 7 、惡意軟體的詢問度提高

而在這段期間，勒索軟體也再次出現(如圖 8)，被勒索軟體攻擊的產業分布如圖 9 所示，可以發現除難以分類的其他產業外，醫療、生產、通訊等關鍵基礎建設也是主要被攻擊的目標，顯示在當前的戰爭趨勢下，透過網路力量打擊或破

壞基礎建設以達到快速結束戰爭的目標是可用戰略之一。目前我國數位發展部業已進行相關的研究與標準制定，以期能應對未來若發生戰爭時，確保基礎建設與相關設備與架構的安全性。



(Credit: Malwarebytes)　　(Credit: Recorded Future)



(Credit: Recorded Future)

圖 8 、勒索軟體再次出現

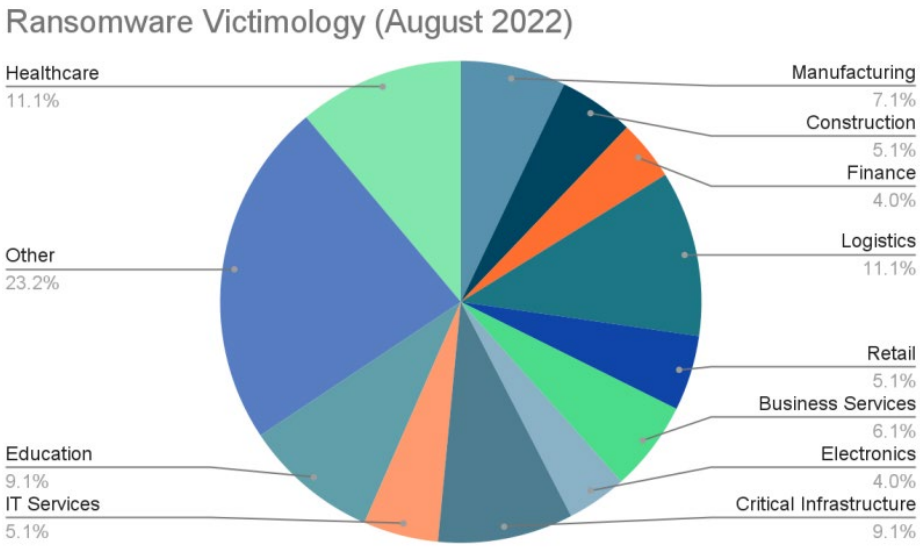


圖 9 、被勒索軟體攻擊的產業

自烏俄戰爭開始，暗網論壇的活動相對穩定，但在 2022 年 11 月有明顯的下降，講者相信與俄羅斯的部分動員令有關係；而論壇的相關貼文與討論度也有下降，講者也認為一些攻擊者被俄羅斯網路軍隊或 IT 部門招募，以及相關網路安全人才外流至愛沙尼亞、喬治亞、芬蘭、哈薩克等相關部門。

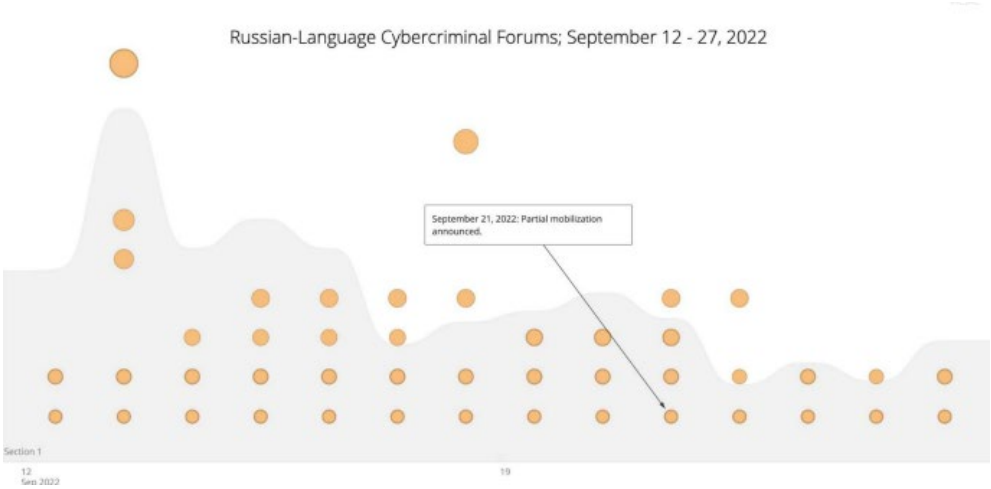


圖 10 、俄羅斯語系的網路犯罪論壇熱度趨勢

(五) 如何在大型企業衡量軟體供應鏈的來源安全(Scaling Software Supply Chain Source Security in Large Enterprises)

本議題由 JPMorgan Chase 的產品安全主管 Rao Lakkakula 擔任講座。

講座說明，過去 3 年有關軟體供應鏈(Software Supply Chain)被攻擊的情形增加 742%，並提到 Gartner 預測至 2025 年，全球 45%的組織會受到軟體供

應鏈的攻擊，該數字將會是 2021 年供應鏈受到攻擊數量的 3 倍以上。

Rao Lakkakula 指出，比起有形體產品供應鏈(Physical Supply Chain)而言，軟體供應鏈的保護更為複雜。包括軟體來源(source)、軟體衛生(software hygiene)、軟體配置情形(software deployment)等，都必須一一釐清其安全性。

Rao Lakkakula 提出保障軟體供應鏈方法如下：

1. 瞭解軟體流程(Understand Software Processes)：確認企業中軟體整合情形(Identify entry points into the enterprises where Software if integrated.)。
2. 監控攝取流程(Monitor Ingestion Processes)：驗證供應商、開源軟體與非開源軟體的安全性(Validate security of providers and dependencies of opensource and closed-source components.)。
3. 建立完整的物料清單(Build Comprehensive Bill of Materials)：就相關使用軟體的供應商與開源軟體等部分建立清單，並標註配置情形(Build Asset Inventory of both vendor and open source software and where they deployed to.)。
4. 保障內部持續整合/持續佈署流程(Secure Internal CI/CD Pipelines)：保障內部基礎設施的來源整合性、發展整合性與佈署整合性(Secure Source Integrity, Build Integrity, and Deployment Integrity of internal infrastructure.)。
5. 建立自動化弱點監控(Automate Vulnerability Monitoring)：利用資產地圖與物料清單，持續監控款體弱點並隨時修補(Continuously monitor for new vulnerabilities to patch deployed software. Leverage Asset map and Bill of Materials.)。

最後，Rao Lakkakula 並建議各組織應採取以下步驟，以建立自身的軟體供應鏈安全性：

1. 協助組織繪製不同的供應鏈地圖(Map Various Supply Chains in Your Firm)：瞭解各項軟體涉入來源點以及為何使用該軟體之各項政策考量等，並依此繪製屬於自己組織的供應鏈地圖。

2. 建立組織的財產清單、物料清單與軟體配置清單(Build Inventory of Assets, BOM, Deployed Software)：掌握開源軟體與非開源軟體的內容以及在組織內的佈署情形。

3. 建立內部發展基礎設施的安全(Secure Internal Development Infrastructures)：落實軟體來源、發展與部屬的整合性檢視。

4. 參與公私部門的相關計畫方案(Join Public and private sector Initiatives)：如CISA的物料清單工作小組(https://ntia.gov/SBOM)或OpenSSF(https://openssf.org/getinvolved/)。

5. 建立屬於自己軟體的物料清單(Ask for SBOMs. Produce SBOMs for your software)。

(六) 揭露事實 - 消費者零信任架構的個案研究(Unveiling the Truth - A Case Study on Zero Trust for Consumers)

本議題由Microsoft的首席產品經理Shinesa Cambric擔任講座。

Shinesa Cambric首先表示由於網路詐騙(fraud)行為日新月異，許多個人與企業也因此受到程度不一的損害，故此議題相當受到各國廣泛重視。

網路詐騙與網路濫用(abuse)有其差異，她將網路詐騙定義為「個人或組織透過網路服務有意詐稱，以獲取利益」(When an individual or entity is deliberately misrepresenting in order to benefit from a service or use it for profit)；而濫用則定義為「以違反網路相關規範之方式使用網路服務，並涉及犯罪行為」(Any use of the service that violates terms of service or for gain on the part of the perpetrator)，其中可能涉及網路犯罪(cybercrime)、對網路服務造成傷害(cause harm to the service)、對於消費者及網路本身造成傷害(cause harm to customers or the Internet at large)，講座並表示，最大的差異在於後者沒有涉及金錢詐取。

講座認為，網路防護(cyber protection)的五大支柱，包括防範(prevention)、控制(containment)、偵查(detection)、調查(investigation)以及減少災損(mitigation)。

1. 防範：在閘道上利用機器學習模型(ML models)及其規則以防止不當使用(Leveraging ML models and rules at the gate or before usage

beings to prevent consumption.)，涉及身分驗證要求。

2. 控制：針對特定身分予以終止或取消使用權(Suspension or disabling of an identity.)。
3. 偵查：發展行為模式以偵測、調查或阻止未經授權的帳號(Developing behavioral models to detect, investigate, or block post provisioned accounts.)。
4. 調查：利用業者調查工具，識別詐騙或已被入侵之帳號與資源(Utilize proprietary investigation toolkit to identify fraudulent or compromised accounts or resources.)。
5. 調查：運用合作夥伴對於帳戶狀態的瞭解，提醒服務團隊有關詐騙或被入侵帳號，或直接停止資源濫用(Leverage partner team insights for account status, notify service teams of fraudulent or compromised accounts, or directly stop/terminate resource abuse.)。

Shinesa Cambric 認為，建立使用者信心與確認身分驗證是建構零信任架構的重要工作，對抗網路詐騙與網路濫用需要相互合作，並應注意以下面向：

1. 找出攻擊者及其攻擊目標(Adversary and Objective)：攻擊者有可能包括不知名的個人駭客、惡意國家或犯罪組織；而攻擊目標可能包括金錢獲取、政治目的、諜報活動(espionage)等。
2. 如何獲得存取權(Acquisition)：包括帳號接管(account takeover)、支付詐騙(Payment Fraud)、免費試用註冊(Free trial signup)等。
3. 瞭解線上平台及其功能(Platform and Features)：瞭解哪些線上服務遭到濫用(What Online Services are being abused?)。
4. 釐清受害者(Victomology)：需考量受害對象(包括組織、個人或網路)、受攻擊模式(包括垃圾郵件攻擊、釣魚信件、DDOS、Crypto Mining 等)、受害類型(金錢損失、關閉營運、信譽受損、造成他人損害等)。

零信任架構的建立，是一場與網路攻擊者之間無止境的相互競爭，應確保以下步驟：

1. 防範手法多樣化(diversifying tool kit)。
2. 運用可迅速調整的方法(adjustable levers)。

3. 評估風險容忍度(assessing risk tolerance)。

4. 守住防線(holding the line)。

有關建立零信任架構的時程表，她從一週、一個月、三個月等時程進行短、中、長期相關建議如下：

1. 一週時程：建立資安工作識別基準線，以釐清對資安保護有利與不利的行為；規劃資安門檻(thresholds)與資安容忍度。

2. 一個月時程：面對新型態網路攻擊，採取詐騙預防、偵測與控制等作法時，應發展相關權衡的準則(develop agreement on tradeoffs)；對於顧客帳戶生命週期(consumer account lifecycle)的潛在資安風險予以稽核。

3. 三個月時程：建立諮詢委員會，以確保相關資安措施符合企業或組織的資安要求；建立並採取相關策略機制以即時反應多樣化的詐騙行為。

(七) 地緣政治韌性：為何營運韌性不再足夠(Geopolitical Resilience: Why Operational Resilience Is No Longer Enough)

本議題由 Microsoft 安全營運發展部門(Security Business Development)的 Ann Johnson 及 Team 8 公司的 Nadav Zafrir 共同解說。

講座認為，全球從去年開始發生以下的巨大變化，包括：

1. 去全球化(deglobalization)重新塑造了我們所處的世界與社會。

2. 世界陣營兩極化(deep polarization)成為網路威脅與破壞的溫床。

3. 極權國家更明目張膽並直接與網路駭客合作(working with cyber attackers)。

4. 對於企業運作維持與預算合理使用顯得更加困難(difficult decisions with operational and fiscal impact)。

為此，私人企業在面對這種世界局勢轉變的情況下，也必須採取相關措施及選定立場。

由於政治地緣的巨變，而觸發經濟發展趨緩，也造成以下情形：

1. 全球經濟成長幅度預期將達到歷史新低。

2. 更多解僱情形(layoffs loom)發生在各產業及世界上各角落。
3. 企業擔心即將浮現的經濟大蕭條(fears of an impending recession)。
4. 網路威脅持續氾濫，因此促使高效能自動化生產模式需求大增。

因此具有領導地位的國家與企業必須一起合作，克服目前的問題。

AI 與量子學發展有助於推動全球進步，但與此同時，領域內的創新也將顛覆既有的安全規範(security norms)。這些深植於 AI 與量子學的經濟與國家安全利益，將會進一步觸發 AI 與量子學的全球競爭，而使得地緣政治的關係更為惡化，因此，這將是一個繁盛或消亡的生存之戰(thriving or surviving)，各國必須確保政治地緣的韌性(ensure geopolitical resilience)。

講座表示，資安長(CISO)與資安領導者對於因地緣政治變化而造成組織或國家資安風險提升的情形，應肩負起相當的責任。他們並指出，發展更先進的 AI，需要關注以下面向：

1. 以可信且負責任的態度與方式發展 AI。
2. 主動與公共場域的論述及對話進行連結。
3. 隨著 AI 更普及地發展，各國應分享相關學習經驗與最佳實踐。

各國必須重新思考供應鏈，以強化供應鏈韌性，步驟包括：

1. 持續不斷重新整體評估企業的供應鏈。
2. 必須將地緣位置所產生的各項風險一併考量(take into account embedded location-based security risks)。
3. 跨部門的相互合作，以強化任何對於供應鏈資安攻擊的各項準備、偵測與調查工作。

講座建議各國及各企業體認以下事實並加強合作，包括：

1. 共同承認網路也是基礎建設之一。
2. 先進國家與企業應思考，共同致力提升資安貧窮線(raise the cyber poverty line)。
3. 我們必須審慎評估成立世界資安組織(potential of a World Cyber

Organization)的可能性。

4. 我們必須推動具有合作潛力的創新研發技術以提升相互合作的動能(drive innovation that supports cooperation)。

最後，講座說明，有關公私部門資訊相互分享與建立更深入的夥伴關係實為必要，若我們不想辦法把所有人都提升到更高的資安水準，終將發現我們掉入更不具保護能力的資安水準中。

(八) 危險的貼文：社交媒體中暴露的生物識別風險(Perilous Posts: The Risks of Biometric Patterns Exposed in Social Media)

本議題由趨勢科技的首席架構師 Craig Gibson 解說。

講座說明敏感的生物特徵數據，包括各式聲音、臉型、耳朵、指(掌)紋、虹膜、影片及其元數據(metadata)、描述、評論及主題標籤(hashtags)等，每天都在數十億則社交貼文中無意間暴露在網路上，如 Facebook、Instagram、YouTube 和 TikTok 等地方；生物特徵是一種密碼，我們可以重置任何密碼，但無法有效地重置生物特徵密碼，它的使用可以將網路攻擊的複雜性提升到新的層級。講座透過一連串展示此類濫用和誤用所暴露的生物特徵數據的規模、主要風險和場景，包括各式繞過身份驗證、數位身份盜竊、名譽攻擊及深偽技術(Deepfake)等，如獲取政治人物的相關生物識別訊息及個人資料，駭客即可嘗試使用它們註冊生物識別系統。

講座說明，冒用各類個人資料在各式網站註冊服務結果所衍生經濟犯罪態樣包括：訊息詐騙(Messenger scams)、商業電子郵件詐騙(BEC)、 創立帳戶(Creation of Accounts)、帳戶劫持(Accounts Hijacking)、勒索(Blackmail)、虛假宣傳活動(Disinformation campaigns)、技術支援詐騙(Tech support scams)、社交工程攻擊(Social engineering attacks)及劫持物聯網設備(Hijacking of IoT devices)等。

以 SIM 卡劫持(SIM swap attack)為例，冒用者可以從 Facebook 或其他方面獲得他人聲音副本及個人資料後，打電話到電信公司的呼叫中心，於通話過程中核對身分資料後，就能夠透過語音、身份驗證系統來冒領 SIM 卡，將被害者的電話號碼從對方的 SIM 卡轉移至攻擊者，之後再透過簡訊來存取包括被害者的 Email、社群帳號甚至電子錢包、加密貨幣帳號等，或透過視訊會議繞過驗證，以解鎖加密錢包、在金融機構確認賬戶等。

講座歸納現今我們身處數位環境，相關技術門檻及犯罪模式分析如下：

1. 低技術壁壘：所有技術支柱(technological pillars)都已到位。
2. 進入門檻低：普通人的身份都可以從公開曝光的媒體中被盜用或重新創建。
3. 低技術門檻：有心人士已經可以冒充和竊取政客、公司高層主管和名人的身份。
4. 大規模首次註冊詐欺：深偽技術(deepfake)模型可能導致大量出現從未存在過的人的身份。

為此，講座對於處理生物識別技術的企業組織建議如下：

1. 對於生物識別導入零信任。
2. 對於受信任和不受信任分別使用單獨的驗證流程。
3. 依賴生物識別技術的業務流程，確保其相關存儲、處理和整個生命週期的安全。
4. 以最小化的方式保護生物識別模式潛在的個人資料外洩。
5. 提高對深偽技術(deepfake)存在的認識，特別是專注於可以被採用實時實現(Real-time Implementation)的電話會議。

(九) RSAC 創新沙盒競賽 (RSAC Innovation Sandbox Contest)

RSAC 的創新沙盒競賽(Innovation Sandbox)持續為資安新創公司提供創新技術思維的展示平臺，迄今已舉辦第 18 年，本次 4 月 24 日在 Moscone Center South 2 樓舉辦的 RSAC 創新沙盒競賽，讓這些資安新創公司有機會向來自世界各地的大型資安廠商和創投業者，盡其所能針對各式新興資安威脅議題提出全新獨創的技術和解決方案，以獲得創投資金挹注。每一年進入最後決賽的 10 家資安新創公司，無不把握機會抓住鎂光燈，透過 3 分鐘的產品解說和問答環節，向與會者展示自家獨特的創新產品和服務的優越性，以爭奪年度最具創新力的初創企業(Most Innovative Startup)稱號。

本年奪下后冠的 HiddenLayer 產品主要功能為 AI 攻擊對抗，以非入侵式平臺的方式保障 AI 模型安全，以因應許多使用開源代碼開發的 AI 模型部署容易受到惡意軟體、數據中毒和推斷攻擊(inference attack)的問題。更重要的是 ，GitHub 上現在至少有 30 種自動化攻擊工具，使得對機器學習(Machine

Learning)或基於 AI 模型的攻擊比以往任何時候都要容易，故 HiddenLayer 產品提供機器學習威脅檢測與反應(Machine Learning Detection & Response，MLDR)服務，重點在解決現今 AI 人工智慧可能加劇的資安問題。統計自競賽創辦以來，RSAC 創新沙盒大賽的前 10 名決賽入圍者總共進行了超過 75 次收購，籌集了超過 125 億美元的投資，幾位獲獎者也成為了上市公司，由此可見 RSAC 創新沙盒競賽的新創公司推廣媒合模式，對新創公司的成長茁壯至關重要。

圖 11、本年奪下后冠的 HiddenLayer

(十) 建立國際聯合部隊以擴大防禦規模(Building International Coalitions to Scale Defense)

本議題由美國 National Security Agency(NSA)的 Rob Joyce、澳洲 Australian Cyber Security Centre (ACSC)的 Rita Erfurt、加拿大 Canadian Centre for Cyber Security(CCCS)的 Sami Khoury 及英國 National Cyber Security Centre(NCSC)的 Felicity Oswald 共同分享。

各國講座都對於勒索軟體(ransomware)日增的資安威脅表示關切，並認為勒索軟體會對各國政府及組織造成災難性的後果，但仍有相關步驟可以因應防範。為了協助各國政府及組織瞭解勒索軟體所造成的威脅以及如何提升資安防護，美國、英國、澳洲等國家積極合作，組成「資安聯合諮詢委員會」(Joint Cybersecurity Advisory)，共同勾勒出最新的資安威脅圖像並提供關鍵建議。他們並強烈建議各國領袖及組織領導人，瞭解資安威脅情形以及資安警示的意義，確保組織內資安團隊採取正確的行動以強化組織韌性。

勒索軟體對於不論組織或個人而言，依舊是最具破壞性的資安威脅(most disruptive cyber threats)，講座表示，這個全球性的資安問題需要全球性的方案來解決，這也是為何英、美、澳共同發起成立資安聯合諮詢委員會，為各國在面對資安威脅時提供建議的因應措施。對於無論是個人、組織、企業乃至於政府機關，遵循資安聯合諮詢委員會的策略與建議，強化自身網路防禦以免於資安威脅，都是至關重要的。

我們身處於一個每個政府部門、企業組織、個人都必須留意自己是否成為勒索軟體受害者的時代，雖然近幾年各國政府都致力提升資安意識，讓大眾瞭解新型態的資安威脅，但對於提升整體的資安韌性，仍待許多努力。透過英國 NCSC、澳洲 ACSC、美國 FBI 與 NSA 等相互合作，分享資安情資、分析資安威脅與趨勢等，能有效協助各國政府及組織採取相關行動以強化資安保障，並向各國政府回報可疑的網路行為及資安事件。

講座們分享，在建立跨國資安聯合諮詢委員會時應在技術、人員、教育等部分都予以側重，另外在產業、學術與政府間更應強化橫向聯繫。至於各國間，則著重於資訊分享之即時性、精確性與完整性等，才能有助於資安情資的掌握與分析。另外，由於各國時區不同，因此有必要增加各國間的信任連結，並就高層人員間建立資安資訊分享的共通機制。在收到資訊後，也必須第一時間分享給不同產業及專家學者。這些都必須建立在深厚的相互合作與信任關係上。

(十一) 密碼學家對談(The Cryptographers' Panel)

本議題由劍橋大學 Gonville and Caius College 的榮譽院士 Whitfield Diffie 擔任主持人，並由獨立顧問 Clifford Cocks、IBM Infrastructure 的傑出工程師 Anne Dames、Dell Technologies 的 Radia Perlman 及以色列魏茲曼科學研究所的 Adi Shamir 擔任與談人。

本座談分享三十年前的九零年代，地平線上出現了三種有前途的新技術：第一個是人工智慧、第二個是密碼學、第三個是量子電腦。由於人工智慧領域的發展與實踐，如 Chat GPT 等技術超出了我們的預期，未來將會邁入蓬勃發展的階段；在密碼學中，因為有很好的傳輸層安全性協定(Transport Layer Security,TLS)實現密碼學的加密協議，讓資訊分享知識的傳播更加快速。但在量子電腦的發展上，目前幾乎還沒有任何可交付事物，也就是說還沒有一個問題被證明用量子電腦可以比傳統電腦更快地解決的實際問題，但是發展的潛力無限。

評估現有系統有可能會因潛在的量子電腦而受到威脅，公鑰系統是最容易受到量子電腦攻擊的系統，由於格羅弗演算法(Grover's algorithm)，必須考慮對稱密鑰(symmetric key)和雜湊函式(hashing functions)，但可能只需增加密鑰或資訊摘要的大小，因此，只有像 AES 這樣的對稱系統會受到量子電腦的影響，而在物理學家的思維上，RSA 加密演算法、迪菲-赫爾曼密鑰交換(Diffie-Hellman)、橢圓曲線迪菲-赫爾曼金鑰交換(elliptic curve Diffie-Hellman)都是會受到量子電腦的攻擊威脅。

即使目前量子電腦尚無法以任何可用的形式存在，但未來三十或四十年內，等待科技進步到足以發展量子電腦，現階段使用的加密演算法系統會有密碼被破解的危險。雖然，量子電腦的威脅目前不會直接發生，但今日所使用的 RSA 加密演算法或橢圓曲線等舊密碼學演算法，在未來將可能變得可被破解。

目前研究單位於量子電腦研究中經常被談論的議題是系統中的量子位元（qubits）數量。專家們在這方面做了大量的研究，考慮因素包括量子體積（the quantum volume）或品質、量子位元（qubits）、規模、性能等議題，來進行量子電腦研究的突破。

講座亦提到近期有篇中國論文闡述使用 300 個左右的量子電腦進行攻擊，論文基本上建立在 Claus Schnorr 因式分解方法(factoring method)之上，該方法使用格中最接近的向量來創建需要找到平滑關係以進行因式分解。這篇論文本質上是使用量子超位置(quantum super position)來查看圍繞可能是改進它的最小向量的值雲(cloud of values)。論文表明它非常適用於小型模組化，中型模組化，並可以看雲點(cloud point)數量呈現指數級的增長，但實際上沒有任何證據表示這對大型密碼的模組化會產生任何影響。

在幾個月前，耶魯大學（Yale University）的一組研究人員展示如何將存儲中的量子位元（qubits）壽命從 1 毫秒延長到 1.8 毫秒。因此，為了分解 2,048 位的 RSA 加密演算法，可能需要持續數天的計算。如果要運行格羅弗演算法，可能需要運行很多年。所以，量子電腦離解決問題的時間還需要很久。

NIST 於 2016 年啟動了一個專案，研究識別能夠抵抗量子電腦攻擊的演算法。計畫中選擇了四種算法進行標準化，期中三種都使用相同的基礎知識和數學原理來保證它們的安全性，從某種意義上說，這些都是一個弱點的威脅。雖然，量子電腦距離實用程度還需要一段時間，但，如果擔心 50 年或 100 年的系統安全性，建議不要使用公鑰密碼方法進行系統安全的保護。傳統的密碼系統雖因需要

手動交換密鑰而較為麻煩，但公鑰密碼演算法卻有其固有的風險，故若期望在未來百年內持續維持的最高安全級別的系統，公鑰密碼系統並無法提供任何強而有力的保證。

(十二) 誰說資安不能具有創造性?(Who Says Cybersecurity Can’t Be Creative?)

本議題由 Axios 的 Sam Sabin、Hacker Valley Media 的 Chris Cochran、Sustaining Creativity 的 Mari Reisberg、TikTok 的 Caitlin Sarian、Axonius 的 Danial Trauner 共同分享相關經驗。

講座認為，創造性由奉獻精神、熱情及動力等所組成，然而如何取得創造性並無標準答案，必須依據不同情境，並取決於多元因素，才能找到獨特的創造性。

講座指出，進行資安工作就像說故事一樣，不能一再講述同一套內容，否則將失去故事的生動性與活潑性。資安工作也是如此，如果一再以同一方式及流程進行資安維護，就難以創造出更佳的資安保障方法。講座認為，在真實世界中，直接面對資安事件進行訓練，而非以模擬方式訓練，將更有助於啟發受訓者的創造性。

如果碰到真實資安事件，不能眼不見為淨，而必須從解決問題的角度，以類似遊戲的方式來思考，才更能創發出新的思維。另外，處理資安事件，建議可以彈性的方式，並且將其應用於每日的工作中，以創造性的視野理解資安任務。他們也建議可以用模擬的方式，提供同仁最差的情境案例，並觀察同仁如何進行改善。

有關如何培養創造性，講座也建議在工作的過程中帶入適當的歡樂元素，讓更多人參與，藉此納入更多不同想法。另外，在同儕間盡可能分享想法，也有助於發展出最佳的解決方案。如果有時候無法找出問題解決方案，可以適度休息及抽離，以唱歌、跳舞的方式放鬆，更容易激發不同的工作想像。

他們指出，創造性有時候是很細微的部分，但透過細小部分的不斷累積，能讓整體創造力發揮最大功效。而有時候也需要以內省的方式，不斷詢問自己、抱持好奇心，才能激發創造力，並使工作產出發揮到極致。

最後，講座分享，有時候組織必須要有容錯空間，才能讓組織工作文化優質

提升，如果員工一直擔心是否因犯錯而被責備，則不可能發揮創新想法，如果一直要求員工自行負擔出錯的成本，則他們會一直墨守成規。在面對 AI 不斷發展的趨勢下，講座一致認為，無論科技如何發展、無論組織如何導入新科技與技術的運用，人作為創造力來源的元素，是永遠能被抹滅的。

(十三) Emotet 曝光：網路犯罪分子供應鏈的內幕(Emotet Exposed: Insider the Cybercriminal's Supply Chain)

本議題由 VMware 公司的安全服務副總裁 Christopher Kruegel 及威脅情報高級總監 Giovanni Vigna 擔任講座。

會議藉由 VMware 的新分析深入研究了 Emotet 僵屍網路的最新浪潮，深入瞭解該惡意軟體交付機制的惡意組件和模組、執行鏈及其軟體發展生命週期，並展示了 VMware 研究人員繞過反向分析技術映射 Emotet 動態基礎架構的主要發現和收穫。

講座說明 Emotet 是一種惡名昭彰且影響久遠的僵屍網路，由 Mummy Spider 和 MealyBug 組織控制，是迄今為止部署最具規避性和破壞性的惡意軟體傳送系統之一。Emotet 常通過包含惡意軟體標記的檔案或嵌入惡意網址的垃圾郵件等方式進行傳播。研究並提到 2022 年 1 月觀察到的 3 組不同攻擊，其中 Emotet 通過 Excel 4.0 (XL4)巨集、帶有 PowerShell 的 XL4 巨集和帶有 PowerShell 的 Visual Basic Application (VBA)巨集交付，並詳細分析了 Emotet 的更新和附加模組，包括它們提供的功能、來源以及隨著時間的演變，其功能模組亦不斷翻新。研究展示 Emotet 攻擊範圍相當廣泛，例如 VMware 威脅分析部門最近攔截到了 2 個更新的模組：一個為專門針對 Google Chrome 瀏覽器，目的在竊取信用卡資訊，另一個是利用網路芳鄰(SMB)協定，目的為進行橫向傳播。

因應 Emotet 的基礎架構不斷變化，VMware 威脅分析部門為此開發了技術和工具來提取 Emotet 惡意程式樣本使用的設定檔，以更好地瞭解 Emotet 僵屍網路用於命令和控制(Command and Control,C2)基礎架構，通過分析相關涉及的網路端點，VMware 威脅分析部門能夠追蹤和記錄 Emotet 僵屍網路的演變。

從歷史上看，Emotet 有幾個基礎設施，稱為 Epochs。在 2021 年 1 月遭執法部門打擊之前，Epochs 1、2 和 3 是攻擊者最常使用的基礎設施，而 Epochs 4 和 5 則是在打擊後復甦時出現。

Emotet 最早從地理範圍德國地區稍微擴大到更廣泛的美國及拉丁美洲，並開始刪除過往不同的版本，使其更難檢測，並使其具更高效率和傳播。VMware 威脅分析部門分析了 329 個 IP 地址的地理分佈，顯示超過 18%的 IP 地址位於美國，其次是德國和法國，其他受歡迎的地區包括南亞、巴西、加拿大和英國，研究團隊並在 329 IP 地址中找到 4 個常用通訊埠，其中 port 8080 佔 54.1% (178)、port 443 佔 33.7% (111)、port 7080 佔 8.5% (28)及 port 80 佔 3.6% (12)。

講座分享 Emotet 研究結論如下：

1. 感染過程中涉及的執行鏈不斷演進。
2. 這個威脅背後的行為者竭盡全力使得有關惡意軟體樣本的命令和控制(C2)基礎設施的訊息難以被提取。
3. 此份報告提供對 Emotet 殭屍網路的命令和控制基礎設施(C2)涉及的網路端點進行全面分析的資訊。
4. VMware 威脅分析部門已開發出一個工具，可以繞過 Emotet 作者使用的反分析技術，並獲取 Emotet 推送給受感染主機的更新檔案。
5. 從新的 Emotet 攻擊中，研究團隊攔截到兩個具有不同功能的新模組：一個專門針對 Google Chrome 瀏覽器的信用卡資訊竊取模組，以及一個利用 SMB 協議進行傳播的模組。
6. 通過 VMware 的調查，可以推斷 Emotet 的行為者可能正在實施某種形式的反分析技術。近年來機器學習(Machine Learning)在資安攻防雙方都得到了應用。

VMWARE 建議組織實施以下技術、程序和流程，以建置強大的資安基礎，從而更好地抵禦 Emotet 和其他惡意軟體：

1. 次世代防火牆(Next generation firewalls)：在網路關鍵控制點(Critical Control Point, CCP)啟用流量檢查，並利用威脅情報來阻止已知惡意和 C2 IP 位址的網路流量進(Inbound)或出(Outbound)。
2. 端點偵測及回應(EDR)：結合了即時的持續監控、端點資料蒐集，以及進階交叉關聯，來偵測並回應主機和端點連線的可疑活動，提供基於特徵值或啟發式（異常）分析和檢測攻擊的惡意軟體保護，然後對端點上的威脅發出警報和分類。

3. 入侵偵測或防護系統(IDS/IPS)：使用已知惡意網路活動的特徵值來檢測和阻止攻擊。

4. 網路偵測及回應(NDR)：提供基於特徵值的檢測和偵測能力，並在沒有特徵值的情況下運用行為分析、機器學習和人工智慧對抗網路威脅。

5. 分段/微分段(Segmentation/Micro-segmentation)：對網路進行微分段，組織或企業應將網路分成多個圍繞業務需求和技術要求設計的子網段，以遏止可能已經進入網路的威脅並防止其進行橫向傳播。

橫向安全-檢查東西向流量(Lateral Security - Inspect east-west traffic)：企業或組織可利用東西向網路流量分析來識別可能是危害指標的模式和異常行為。

1. 掃描網路工件(Scan network artifacts)：企業或組織可通過使用人工智慧(AI)和機器學習(ML)來檢測各式惡意代碼，動態分析文件行為是否存在威脅。

2. 實施強大的密碼策略(Implement robust password policies)：企業或組織應刪除所有預設的、共享的和寫死的(hard-coding)身份驗證過程，以取代更強大的身份驗證機制。鼓勵在可行的情況下使用多因素身份認證。

3. 修補管理(Patch management)：企業或組織應定期、及時地對各式作業系統、軟體、硬體和應用程式安全進行安全性更新。

4. 滲透與弱點測試(Penetration and vulnerability testing)：企業或組織應定期進行滲透測試和弱點掃描，以瞭解並減少組織潛在的攻擊面，並避免受攻擊面暴露在外。

5. 主動威脅搜尋(Active threat hunting)：企業或組織應監控網路中的日常活動和流量，並調查可能的異常情況以發現任何尚未發現可能導致安全漏洞的資安威脅。

6. 電子郵件安全(E-Mail Security)：企業或組織應提供用於保護電子郵件帳戶、內容和通信的預防、檢測和回應框架。攻擊者常使用電子郵件來傳播惡意軟體、垃圾郵件和網路釣魚攻擊，因此保護電子郵件的隱私和完整性至關重要。

(十四) 軟體材料表上的世界(The World on SBOMs)

本議題由 Cybeats 首席佈道師 Chris Blask 和 Linux 基金會可靠嵌入式系統副總裁 Kate Stewart 共同解說。

本場強調了軟體材料表（software bill of material，SBOMs）和供應鏈智慧模型在改變軟體開發的各個面向，如風險管理、維運、許可和透明度方面的重要性。並提到了關鍵基礎設施部門日益依賴網路和電腦化，強調需要解決這些領域的網路安全風險。講者強調 SBOM 內部的可追溯性和明確跟踪資訊的重要性。與其將所有資訊合併到一個單一的 SBOM 中，關鍵在於擁有模塊化且相互連接的 SBOM，以便更容易理解和分析。

使用 SBOM 的目的在於增強軟體供應鏈中的透明度、可追蹤性和安全性，有助於組織更加瞭解所使用的軟體元件，追蹤其來源，評估可能與這些元件相關的漏洞或授權等問題，已被世界各國公認為更好地保護軟體供應鏈的關鍵工具之一。它是一份清單，列舉各式軟體應用程式或系統建構中使用的元件和相依性，包括開放原始碼和第三方函式庫、框架、模組及其對應的版本等資訊，這些元件使用在軟體產品的開發和部署過程中。企業組織通過維護準確的 SBOM，軟體開發人員、供應商和使用者將能夠更有效管理資安風險，確保軟體產品的完整性和安全性。

在本次專題演講中，講座概述代表軟體生命週期各個部分的高品質 SBOM 是如何改進風險管理活動，降低運營成本、改善知識產權控制及軟體供應鏈安全等，如 2021 年底著名的 Log4j 開放原始碼漏洞，即仰賴開源社群釋出修補程式，如若組織未主動下載修補套件，漏洞威脅將持續延燒。而當愈來越多關鍵基礎設施電腦化及網路化後，供應鏈安全問題也隨之提高，如美國燃油管道營運業者 Colonial Pipeline 遭勒索軟體攻擊事件，影響美國東岸多達 45%的燃料供應，迫使美國政府一度宣布緊急狀態，讓燃油能透過陸路來運輸。

現今我們擁有的關鍵基礎設施也同樣混合了開源及專有資源，據 Synopsys 等多家公司調查，在軟體開發中，有多達 90%至 98%代碼庫(code base)含有開放原始碼，目前在 GitHub 上亦有多項免費的開源軟體盤點工具，可協助組織自動產出符合 SPDX 規範的 SBOM，企業組織可搭配 CVE 弱點及美國國家弱點資料庫(NVD)，瞭解其內部使用開源軟體究竟有多少弱點，以及後續的修補方式，因此組織可利用適當的工具和建立有效的流程，隨時做好安裝修補程式的工作，保護其代碼免受可能的資安漏洞影響。

講座說明可以在軟體生命週期的不同階段收集相關軟體組件資訊，包括從軟

體來源、建構時或建構後通過二進制分析工具收集，最小 SBOM 元素包含如下：

1. 供應商名稱：創建、定義和標識組件的實體名稱。
2. 組件名稱：分配給原始供應商定義的軟體單元名稱。
3. 組件版本：供應商使用的標識，用於指定軟體相較於先前的版本更改。
4. 其他唯一標識：用於識別組件的其他標識符號，或作為相關資料庫的查找鍵(Foreign Key)。
5. 依賴關係：描述與上游軟體組件之間關係。
6. SBOM 數據作者：創建 SBOM 數據的實體名稱。
7. 時間戳：記錄 SBOM 數據組裝的日期和時間。

SBOM 還有助於提升整個軟體供應鏈合規性，可以更好地管理供應鏈中的風險，確保使用的軟體符合相關法規和標準要求。這對於在一些受監管或對安全性要求較高的領域，如醫療、金融和能源等，尤為重要。

最後，講座建議有關應用 SBOM 的時程表，組織可從接下來的 1 週、3 個月到 6 個月期程，分別從供應商、集成商(Integrator)及操作員去進行實做，並透過與組織上下游夥伴間交換資料，清楚瞭解使用了哪些開源軟體及這些軟體與產品之間的對應關係；接收者也可以根據 SBOM 資訊，檢視對應的授權要求及判斷是否受到已知安全漏洞的影響，減少軟體供應鏈攻擊影響，進而提升組織的資安防護能力。

(十五) 網路釣魚：NIST 網路釣魚規模與網路安全意識(Phishing With a Net: The NIST Phish Scale and Cybersecurity Awareness)

本議題由美國國家標準與技術研究所的 Shanée Dawkins 博士和 Jody Jacobs 共同擔任講座。

本講座主題為釣魚的防治措施。在會議中，講者提供有關釣魚信件防禦的統計結果，表明透過設備和資安相關技術，我們能夠抵擋大約 90%的釣魚攻擊。然而，仍有約 10%的釣魚信件會成功讓終端使用者看見。

圖 12、釣魚郵件攻擊訓練

為了解決這最後 10%信件對組織內部系統的造成的影響，我們通常會透過資安教育的方式來強化使用者的安全意識。然而，目前評估釣魚信件的方式僅限於釣魚郵件的點擊率，但是現有的點擊率的分析無法提供釣魚郵件欺騙使用者的詳細的訊息，包括使用者點擊的模式和原因。

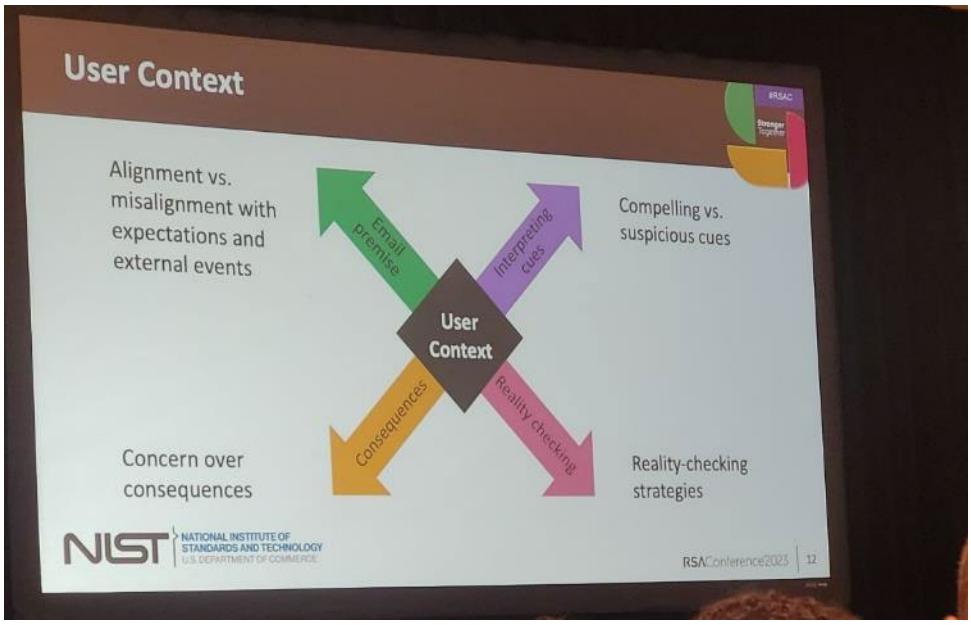


圖 13、使用者分析

因此，NIST 在內部網路進行了釣魚信件的研究，並進一步訪談受測者，這些

研究結果都指出，點擊釣魚郵件的人過於信任系統的安全性和過於信任人性。這類研究結果可以協助降低釣魚郵件的點擊率，並加強針對這一弱點辦理相關的教育訓練。

這次會議為我們提供了寶貴的洞察，瞭解到在釣魚防禦方面的挑戰和解決方案。釣魚攻擊的防治需要綜合考慮技術措施、資訊安全教育和內部研究的成果。通過加強使用者的安全意識和提供更具針對性的教育訓練，我們可以減少組織內部人員對釣魚郵件的點擊率。這些措施將有助於提高組織的資訊安全水平，減少釣魚攻擊所造成的損害。

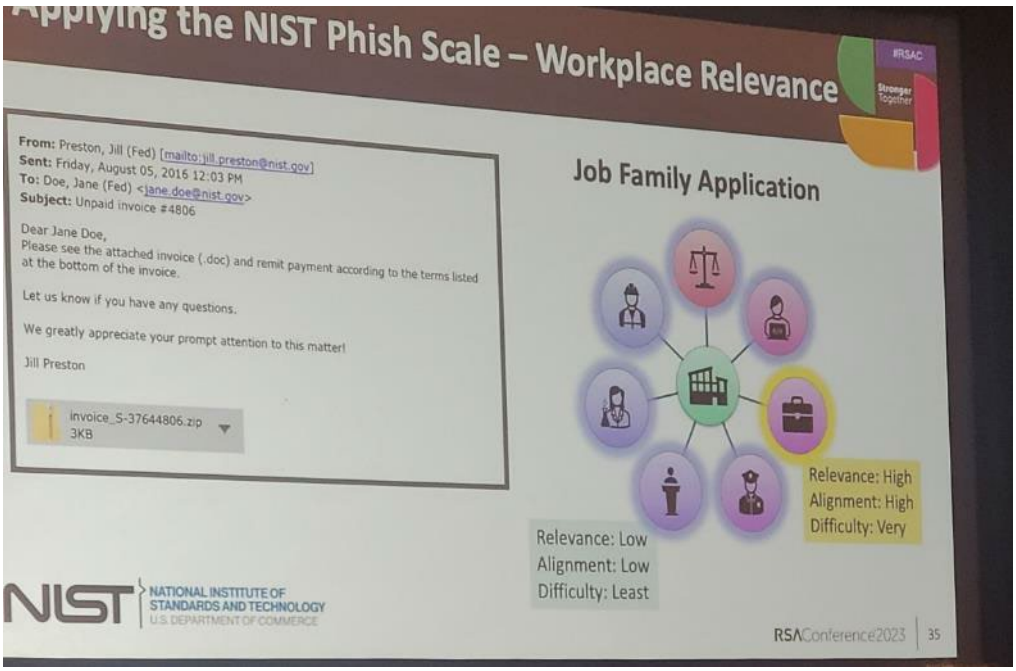


圖 14、釣魚信件樣態研究與分析

(十六) 攜手更強大：美國-烏克蘭網路合作關係(Stronger Together: The US-Ukrainian Cyber Partnership)

本議題由 FBI 的 Bryan Vorndran 擔任主持人、Cyber Threat Intelligence Integration Center 的 Laura Galante、FBI 的 Alex Kobzanets 及烏克蘭國家安全局的 Illia Vitiuk 擔任與談人。

烏克蘭國安局網路和訊息安全部門負責人 Illia 詳細描述了自 2014 年以來，烏克蘭持續遭受來自俄羅斯的攻擊。這些攻擊包括中間人攻擊、DDoS 等多種常見攻擊手法。例如在 2015 年，俄羅斯透過攻擊烏克蘭電網，造成超過 25 萬人民沒有電力供應，引發了恐慌。在這段時間內，烏克蘭成為俄羅斯進行網路攻擊和相

關實驗的測試場所。

從 2020 年開始，隨著烏俄戰爭的醞釀與爆發，網路攻擊關鍵設施的次數逐年增加，在 2021 年達到了 1400 次，2022 年更上升到 4500 次。這些攻擊涵蓋了 70 個州，包括資料竊取等行為。儘管這些攻擊對國家的運作沒有造成太大影響，但隨著時間推移，對民眾的影響逐漸加深；在 2023 年，攻擊開始針對衛星訊號進行攻擊和散播虛假訊息。俄羅斯選擇攻擊衛星主要是因為衛星系統在軍方使用中具有重要性，而散播虛假訊息則是為了達到戰略目的，降低人民的抵抗意志。

講座提到在戰爭中最重要的是，各項服務應該在國外的雲端進行異地備援，以防止開戰時國家本土遭受砲擊而導致資料和機器的毀損無法恢復服務。此外，講座亦強調與美國及其他國家的合作應為持續性的、不容中斷的合作。參與者們也強調，在戰爭來臨時，需要持續進行多面向思考，並不間斷地與合作夥伴國家分享情報，並提到臺灣與中國之間的關係與烏克蘭與俄羅斯之間的關係相似，需要時刻關注動態發展。

這次會議提供了一個寶貴的平台，讓與會者們深入瞭解烏克蘭所面臨的網路安全挑戰和威脅，以及如何應對這些威脅。這些洞察將有助於其他國家和組織更好地理解並應對類似的情況，加強彼此之間的合作與訊息共享

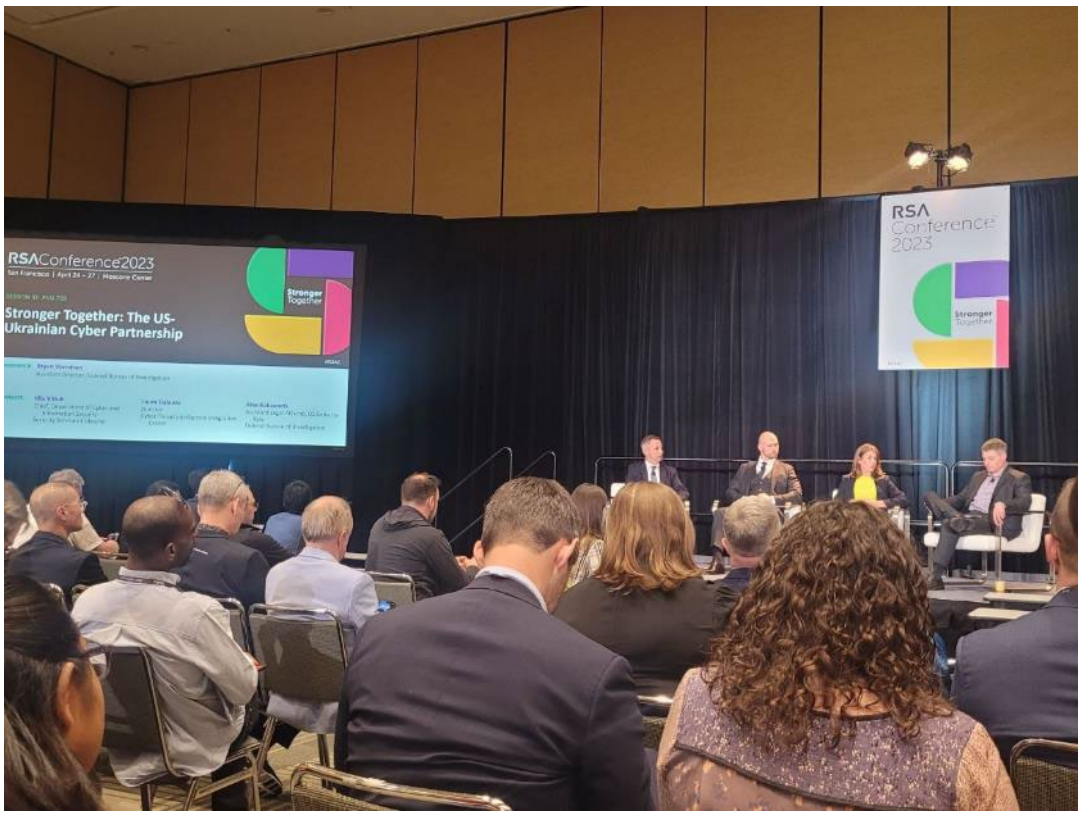


圖 15、Stronger Together 講者與主持人

(十七) 駭客的雲端治理指南(The Hacker's Guide to Cloud Governance)

本議題由 FireMon 的 Rich Mogull 擔任講座。

本講座主要探討雲端運算如何破壞企業的治理，以及如何透過反制措施來保護企業資訊安全。在雲端運算中，企業將數據和應用程式儲存在第三方伺服器上，這使得企業失去了對其數據和系統的直接控制權。同時，雲端運算也帶來了新的安全風險和挑戰，例如資料洩露、身份驗證問題、供應鏈攻擊等。

管理雲端環境的理論主要有以下特性：

1. 雲端運算是分散的，與傳統的集中式資訊技術系統不同。企業安全和治理策略通常是為集中式架構設計的，它們假定所有數據和系統都位於同一地點或數據中心。
2. 雲端管理是統一的，企業可以通過單一控制台、通道或 API 來管理其整個雲端環境。這使得管理更加方便和高效。
3. 雲端環境中，大多數安全措施僅依賴用戶名稱和密碼這樣簡單的身份驗證方式。這種身份驗證方式容易受到惡意攻擊者的攻擊，因此企業需要實施其他安全措施來保護其數據和系統。

在傳統的資訊安全中，邊界通常是指防火牆、入侵偵測系統等技術控制點，但隨著雲端運算和移動裝置的普及，這些傳統的邊界已經變得不再有效。現在，身份認證成為了新的邊界，因為它可以確保只有授權的使用者才能夠存取敏感資料和應用程式。

而導入的可能原因與會有衝突包含以下幾點：

1. 管理階層們分心且過於抽象，無法關注實際的技術問題，且被文章和趨勢所誤導，無法判斷實際導入的問題與障礙。
2. 從業人員負荷過重，不一定都想學習新事物，即使他們想學習，也不一定有時間。
3. 管理層不想放棄對系統的控制權，或者因預算的問題而無法轉換環境。

而若能夠模擬對雲端服務的攻擊，以測試其安全性和弱點。透過這種方式，組織可以發現並修復可能存在的漏洞和安全問題，以提高其雲端服務的安全性。

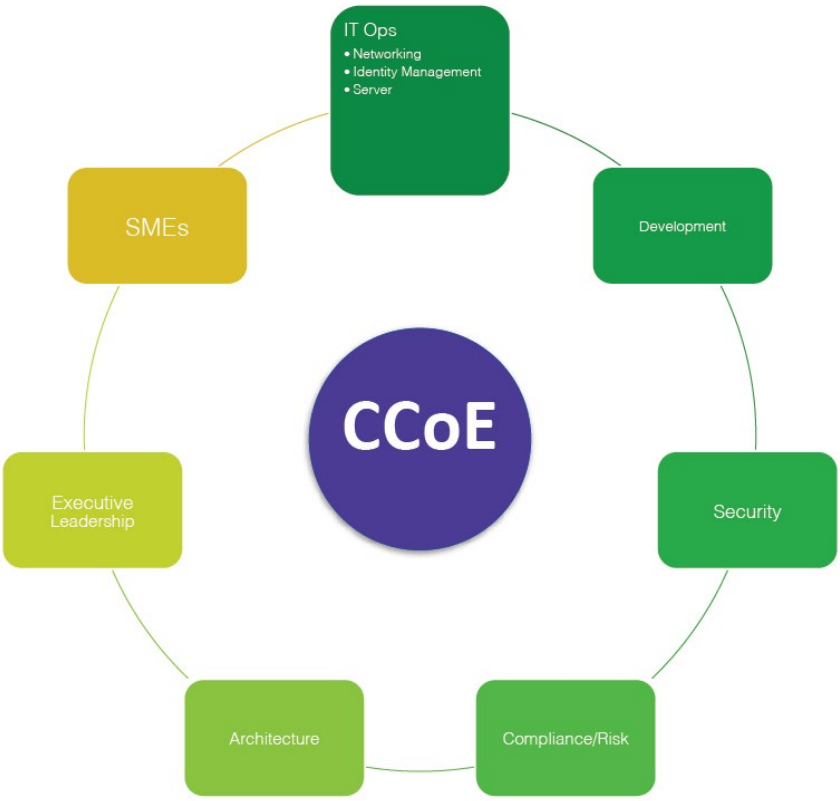


圖 16、雲端卓越中心（CCoE）的功能架構

1. 雲端註冊表

建立適當的雲端註冊表(Clou Registry)對於雲端的治理也十分重要，包含但不限於以下幾個項目，對於釐清責任歸屬、合規、管理、除錯都具有一定的幫助。

(1) 提供者(Provider)

(2) 環境身分/帳號(Environment ID, e.g. account ID)

(3) 描述性名稱(Descriptive name)

(4) 合規性分類(Compliance classification)

(5) 風險分類(Risk classification)

(6) 環境分類(Environment classification (dev/prod))

(7) 擁有者(Owner)

(8) 技術聯絡人(Technical contact)

(9) CSP 聯絡人(CSP contacts)

2. 雲端安全控制目標

本項目應包含：

(1) 一份期望或要求控制的清單，列出所需或期望的安全控制措施，以及在雲端環境中需要實施的控制項目。

(2) 撰寫時以結果為導向：控制目標的描述通常著重於結果，而不指定如何實施。它們描述了期望實現的目標，而不涉及具體的實施細節，除此之外，這些目標應該是可衡量的。

(3) S.M.A.R.T.原則：目標應該符合 S.M.A.R.T.原則，即具體、可衡量、可實現、切實可行，並可以根據需要設定時間框架。

(4) 與特定平台分離：這些目標應該與特定的雲端平台無關，以確保其適用於不同的雲端提供商或平台。

(5) 避免使用像「需要制定政策和程序」等的語言：應該避免使用這樣的描述，以免指定具體的實施方式，且應該專注於描述目標本身。

(6) 根據需要進行細分：控制目標可以根據組織的需求進行細分，以確保涵蓋到必要的細節。

(7) 所有控制措施都將映射到一個控制目標：所有實施的控制措施都應該與一個明確的控制目標相關聯，以確保整個安全控制體系的完整性。

3. 隔離生產

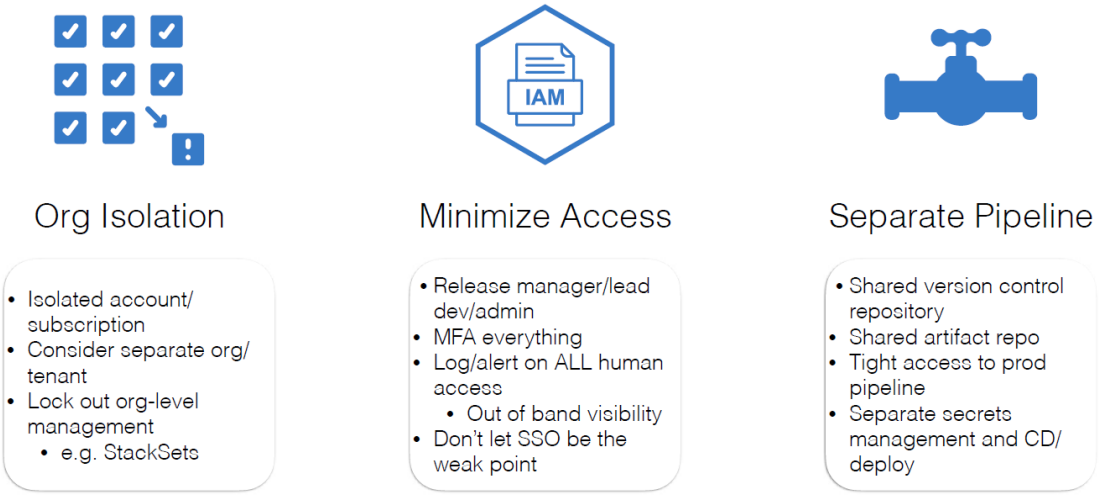


圖 17、管理目標：隔離生產

隔離生產 (Isolate Production) 包含組織隔離、最小化訪問及分離流程，指的是將生產環境與其他環境分隔開來，以維護其穩定性、安全性和可靠性的做法。這包括實施特定措施，將生產環境與開發、測試或暫存環境區分開來。這種隔離有助於減少中斷、未經授權訪問和意外後果對生產環境中的關鍵系統造成的風險，實際上在開發階段也會將成程式碼與部署區域分成生產、測試、開發等區域，避免直接在生產區域除錯或開發的意外影響。

組織隔離 (Org Isolation) 是指將組織的不同部門、業務單位或團隊相互分隔或隔離。這包括建立明確的邊界或區隔，確保每個實體獨立運作，並且不能無限制地訪問或控制組織內其他實體的資源或活動。組織隔離有助於維護數據的保密性，防止利益衝突，並限制未經授權的數據訪問或濫用的可能性。

最小化訪問 (Minimize Access) 是指限制和控制對資源、系統或數據的訪問，僅允許具有特定角色或職責的人員或實體進行訪問。通過最小化訪問權限，可以降低未經授權的訪問風險，確保只有需要的人員可以訪問相應的資源，從而提高安全性和保護數據的機密性，講者也提到許多新進人員在未實施最小化訪問的公司裡，剛入職就可以存取許多公司機密資訊，對於需要防止商業機密外洩或重視資安的企業是非常大的漏洞與挑戰。

分離流程 (Separate Pipeline) 意味著將不同的工作流程或流水線分隔開來，以避免相互干擾和影響。這通常用於軟體開發或持續整合/持續交付(CI/CD)環境中，不同的開發、測試和部署流程被隔離，以確保每個流程的獨立性和穩定性。分離流程有助於減少衝突、錯誤傳播和不必要的干擾，提高開發和部署的效率和可靠性。

4. 建立一個安全的版本控制系統和工作元件儲存庫

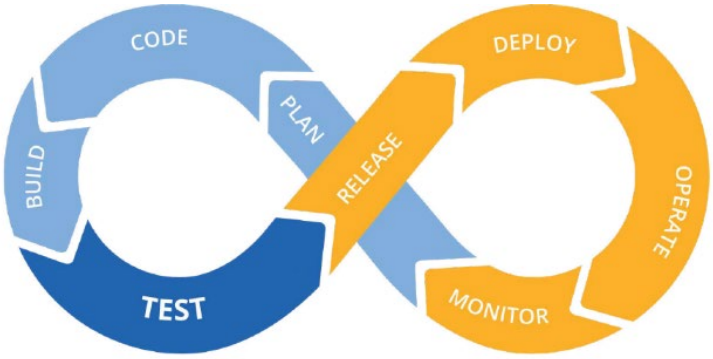


圖 18、建立安全版本控制和工作元存儲庫

而在軟體開發過程中，建立一個安全的版本控制系統和工作元件儲存庫，以

確保程式碼和其他相關資源的安全性。這些儲存庫可以包括基礎架構即程式碼(IaC) 模板、預先批准的模式、必要的基準線模板、控制目標、控制規格、策略、CI/CD 工具整合、容器映像和虛擬機/實例映像等，還包含內置安全工具，以及供開發人員和研發人員使用的「開放」映像。

5. 全面採用(Go Full DevOps)

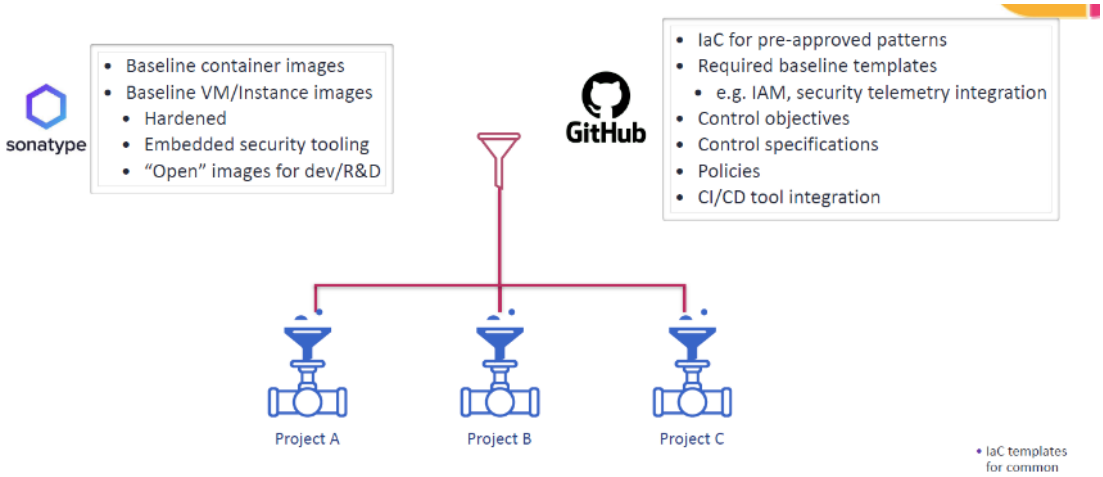


圖 19 、Full DevOps 流程

全面採用旨在打破傳統的隔閡，改善協作，提高軟體品質，加速交付週期，實現在軟體開發和運營中更高的效率和靈活性。它促進一種協作、自動化和持續改進的文化，以應對數字時代不斷變化的需求。

其包含以下這些部分：

(1) 安全製品流程(Pipelines for security artifacts)：建立用於處理安全製品，例如安全測試、漏洞掃描等的自動化流程，以確保安全性納入軟體開發和部署的整個過程中。

(2) 自動化(Automation)：使用自動化工具和實踐來簡化和自動化重複性任務，例如程式碼構建、測試、部署和基礎架構配置。自動化有助於減少錯誤，節省時間，提高一致性。

(3) 程式碼治理(Governance as code)：將治理原則和規範以程式碼的形式納入到開發和部署過程中，實現自動化、可版本控制和可重現的治理措施。

(4) 使用 ChatOps 工具和平台，將團隊成員的協作和交流整合到聊天室或即時通訊工具中，提高溝通和協作效率。

6. 如何實現這一目標

分散式操作需要分散式治理，並建議建立一個 CCoE 來實現這一點。如果必要，可以採取非傳統的方法來實現目標。此外，它還提到了將安全策略轉換為程式碼的重要性，以及使用 IaC、ChatOps 等工具來實作安全措施，同時仍然具有可見性和可控制性。

(十八) NIST 800-207 指南：零信任議題的概念到提案(A NIST 800-207 Playbook: Zero Trust from the Whiteboard to the Boardroom)

本議題由 Zscaler 的 Bryan Green 擔任講座。

本場旨在介紹和探討「NIST 800-207 指南」中的 Zero Trust 架構，並強調其重要性和優勢。報告首先回顧了過去 1990 至 2020 的信任模型演變，指出以網路安全為基礎的信任模型已經無法應對當前的威脅環境，並導致安全政策執行的無效性，降低了靈活性、性能和增加了成本、複雜性和技術負債。接著，報告介紹了 Zero Trust 架構的概念和原則，並強調其以資源為中心、基於驗證和授權的訪問控制，以及動態策略決定訪問的特點。重點摘述如下：

1. 零信任架構基礎

本報告總結了基於 NIST 800-207 指南的演講內容，重點介紹 Zero Trust 架構的重要性以及其與傳統網路安全架構之間的區別，並強調 Zero Trust 架構在保護和簡化混合和多雲環境中的優勢，及探討「Extend the Corporate WAN」和「Secure Communications Over Any Network」之間的對比，分別是複雜性和風險增加與保護與簡化。

2. 推動零信任的宏觀趨勢

這部分進一步探討 Zero Trust 架構發展的宏觀趨勢，包括應用程序轉型、網路轉型和安全轉型。舉例來說，應用程序的轉型從傳統的資料中心工作負載轉向多雲環境和服務化導向模式。網路轉型則將企業網路直接連接到互聯網上，與傳統的企業網路模型有所不同，而安全轉型則由傳統的網路安全架構轉向零信任架構。而此議程的報告中，引用了 NIST 800-207 指南中的 零信任架構，該架構強調了建立在 NIST 800-207 指南基礎上的零信任架構的重要性。並總結了 NIST 800-207 零信任指南的相關內容。這項指南旨在將傳統的網路安全模型轉變為更為靈活、安全且符合現代威脅環境的零信任架構。此章

節介紹了兩種對立的架構、宏觀趨勢以及零信任觀點對於網路的看法。同時闡述了零信任架構的六項原則，並強調資料和計算資源的重要性、安全通信的必要性、訪問控制的原則、動態策略的重要性以及監控和執行安全策略等。

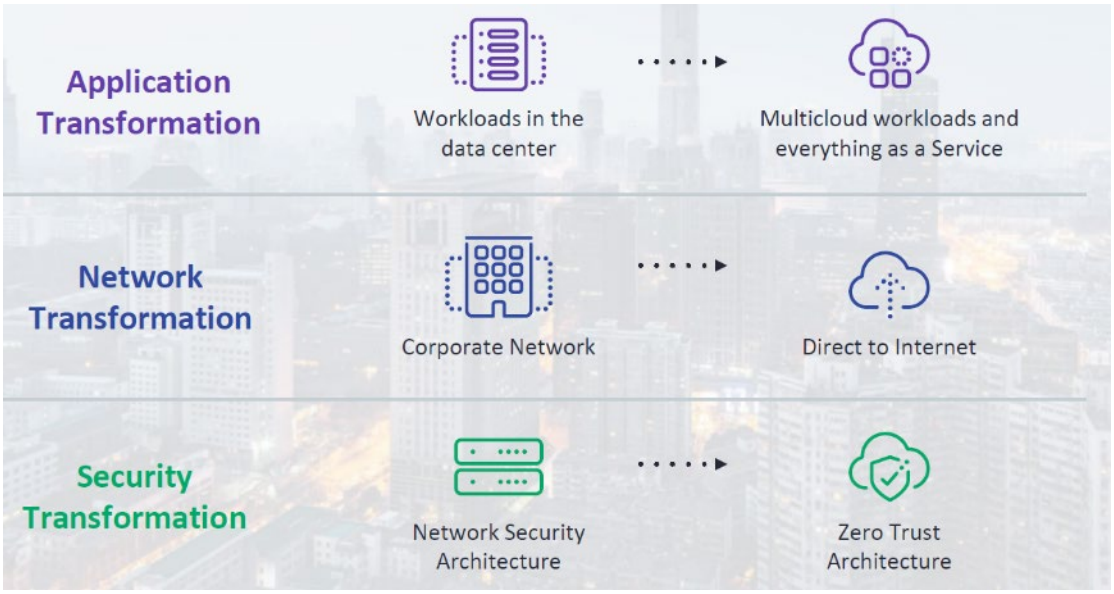


圖 20、零信任的宏觀趨勢

基於網路的零信任架構的六項原則說明如下：

(1) 攻擊者總是存在於所有網路上，企業不能假設自己的網路是安全的，必須始終保持警惕。

(2) 企業資源存在於非企業擁有的基礎設施上，例如雲端服務提供商、合作夥伴等。這意味著企業需要對這些基礎設施進行嚴格的監控和管理。

(3) 本地網路不能被信任，必須假定已被入侵。因此，企業需要實現嚴格的訪問控制和安全監控。

(4) 沒有任何資源是一定可被信任的，所有資源都需要通過身份驗證和授權才能被訪問。這可以防止未經授權的用戶或系統訪問敏感資源。

(5) 安全姿態和策略必須始終得到執行，包括身份驗證、訪問控制、安全監控等。這可以確保企業網路的安全性。

(6) 假設已經被入侵，企業需要實施應急計劃和嚴格的安全監控，以及進行後續調查和修復工作。這可以幫助企業更快地發現和應對安全事件，減少損失。

3. 打造你的零信任策略

圖 21、Building your Zero Trust strategy

本章主要說明如何建構 Zero Trust Strategy 的基礎，包含理論、方法和架構，主要分為安全導向與業務導向，分述如下：

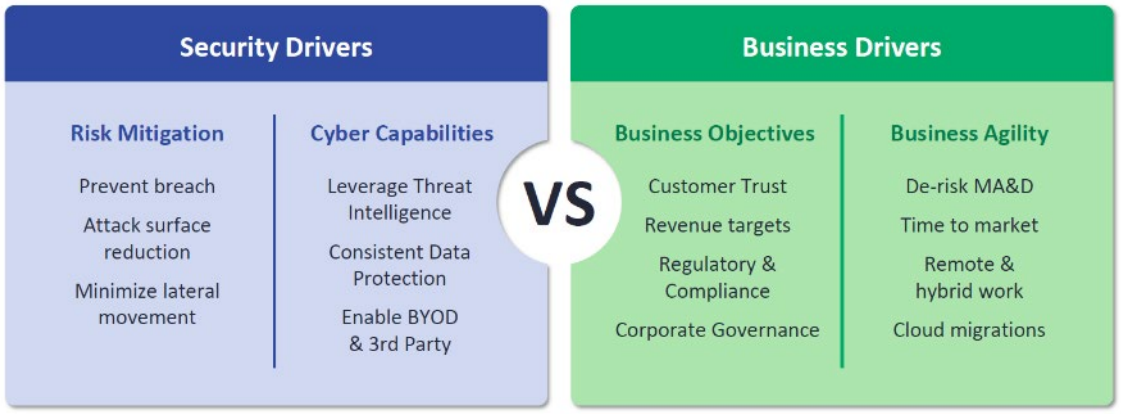


圖 22、安全導向與業務導向

(1) Risk Mitigation

I. Prevent breach：企業需要防止未經授權的訪問和數據洩露。

II. Attack surface reduction：企業需要減少攻擊面，以降低受到攻擊的風險。

III. Minimize lateral movement：企業需要限制攻擊者在系統內部移動的能力，以減少受到攻擊的影響範圍。

(2) Cyber Capabilities

I. Leverage Threat Intelligence：企業需要利用威脅情報來瞭解最新的威脅和攻擊，以制定更有效的安全策略。

II. Consistent Data Protection：企業需要確保其數據在整個組織中得到一致的保護。

III. Enable BYOD & 3rd Party：企業需要支持員工使用自己的設備和第三方供應商，同時確保其安全性。

(3) Business Objectives

I. Customer Trust：指客戶對企業產品和服務的信任程度。安全策略需要保護客戶數據和隱私，從而贏得客戶的信任。

II.Revenue Targets：收入目標是指企業為實現其財務目標而設定的具體收入目標。安全策略需要支持收入目標，以確保企業能夠實現其財務目標。

III. Regulatory & Compliance：監管和合規要求是指企業需要遵守的法律法規和行業標準。安全策略需要確保企業能夠遵守監管和合規要求，以減少法律風險。

IV.Corporate Governance：企業治理是指企業管理層對企業運營的監督和管理。安全策略需要支持企業治理，以確保企業能夠有效地管理風險和確保企業的長期穩定發展。

(4) Business Agility

I. De-risk MA & D：降低併購和拆分風險指企業在進行併購或拆分時需要降低風險。安全策略需要支持降低併購和拆分風險，以確保企業能夠成功實現併購或拆分。

II.Time to market：上市時間指企業將產品或服務推向市場所需的時間。安全策略需要縮短上市時間，以確保企業能夠更快地推出產品或服務，滿足客戶需求。

III. Remote & hybrid work：遠程和混合工作是指員工可以在不同的地點工作，包括在家中、咖啡廳等地方。安全策略需要支持遠程和混合工作，以確保員工能夠安全地訪問企業系統和數據。

IV.Cloud migrations：雲遷移是指將應用和數據從本地基礎設施轉移到雲端基礎設施。安全策略需要支持雲遷移，以確保企業能夠安全地將應用和數據轉移到雲端基礎設施。

4. 定義指引(Defining the North Star)

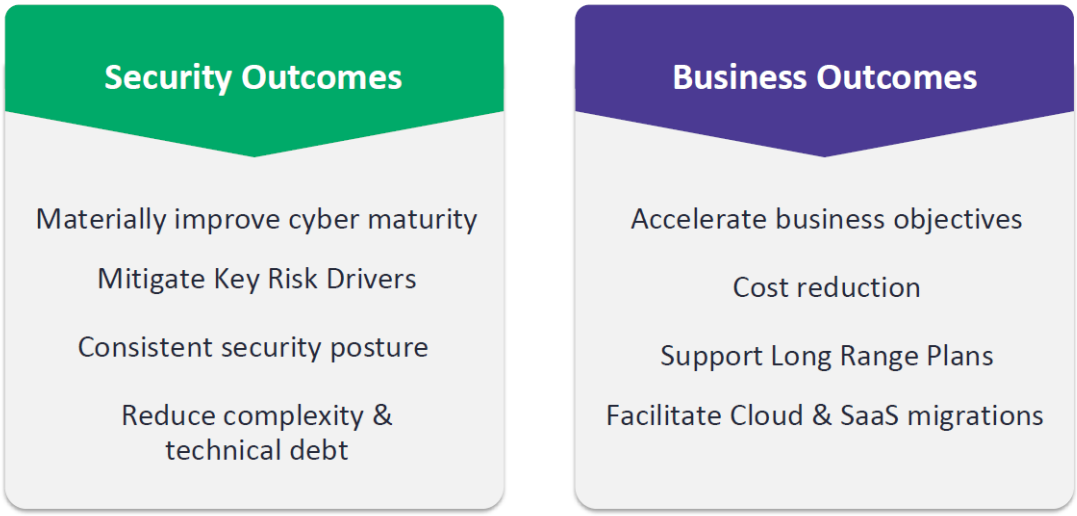


圖 23、Defining the North Star

組織需要平衡安全驅動因素和業務驅動因素。它提醒組織要全面考慮網路安全的成熟度、風險管理、安全態勢的一致性、成本效益、長期計劃和業務需求。這種綜合性的方法可以幫助組織建立一個具有零信任架構的安全環境，同時支持業務的持續發展和創新。

5. Migrating to a Zero Trust Architecture

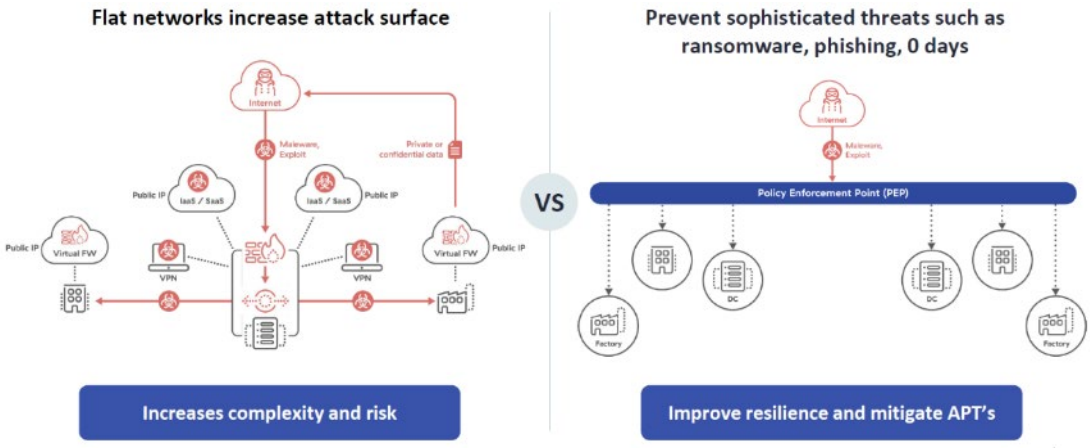


圖 24、Migrating to a Zero Trust

Flat Network 只透過較少數量的交換器與路由器來切分各個子網路與邊界，且存取點與連接方式十分多樣，因此攻擊面相對較高，可能遭受攻擊的漏洞也相對增加。

而應用 PEP(Policy Enforcement Point)後，可對應提升對於目前常見的勒索軟體、釣魚攻擊和 Zero-day 漏洞的應變與預防機制，透過實施適當的安全措施和防禦機制，且不限於軟體或硬體的應用，可以減少這些高級威脅對系統的影響，提高安全性。

6. 數據保護：防止敏感數據丟失和洩露

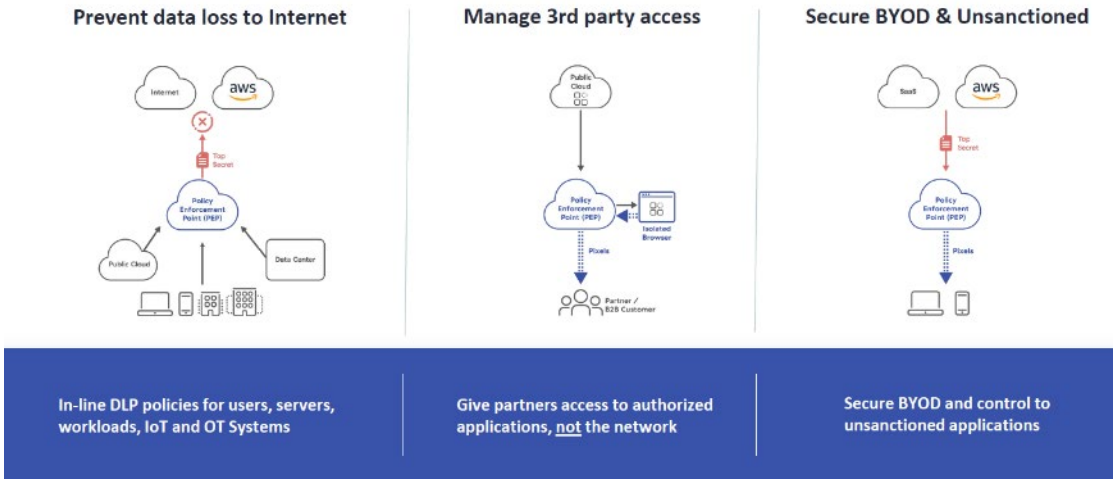


圖 25、數據保護：防止敏感數據丟失和洩露

在網路環境下防止數據損失的重要性較高，意味著需要實施相應的控制措施，如加密、防火牆、入侵檢測系統等，以保護數據免受未經授權的訪問、外部攻擊或數據洩露的風險。

另外，也需要管理和監控第三方或其他合作廠商對系統和數據的訪問。組織可能與供應商、合作廠商或外包服務提供商等第三方進行業務往來，這些第三方可能需要訪問組織的數據和系統，而組織需要實施適當的控制措施，如授權和驗證機制、訪問監控和審計、合同和協議管理等，以確保第三方的訪問是受控和安全的，並防止敏感數據的損失或濫用。

而在當前的工作與開發環境下，需要保護由員工自己攜帶的設備和未經授權的設備對組織的數據和資源的訪問。隨著越來越多的組織允許員工使用個人設備進行工作，以及非授權的設備可能存在於組織的網路中，需要實施適當的控制措施，如設備註冊和驗證、遠程訪問策略、數據加密、容器化或遠程抹除等措施，以確保 BYOD 和非授權設備的安全性。此外，還需要制定政策和執行

相應的培訓，以提高員工對設備使用的安全意識，並確保敏感數據不被未經授權的設備訪問或洩露。

7. 零信任下的分割(Segmentation with Zero Trust)

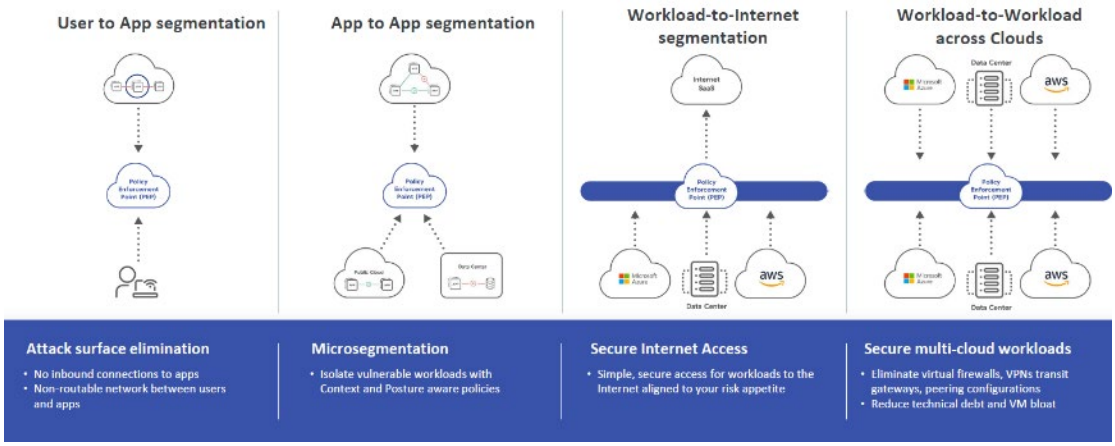


圖 26、零信任下的分割

除了採用最小化訪問權限分配外，分割應用、工作負載、系統並應用合適的 PEP 十分重要，限制使用者只存取必要的應用，以及對不同的應用、工作負載、系統等通訊與交互進行驗證與限制，可以降低對應的安全風險。

8. 零信任網路流量的交通流(Zero Trust Network Access (ZTNA) traffic)flow

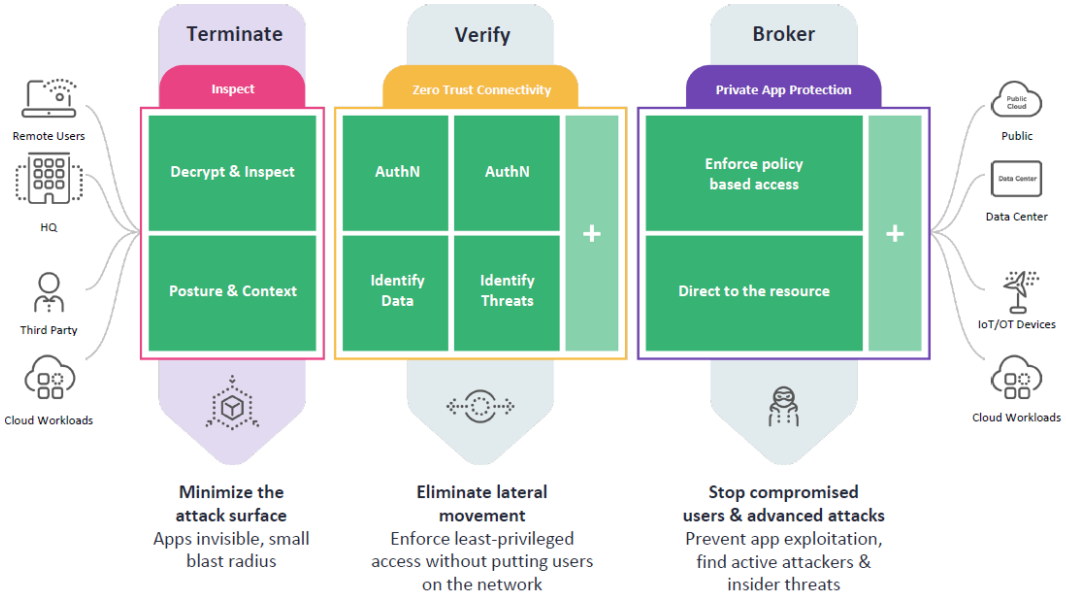


圖 27、零信任網路流量的交通流

ZTNA(Zero Trust Network Access)是一種網路安全架構和方法論。它強

調不信任任何內部或外部的網路流量，並要求對每個用戶和設備進行身份驗證和授權，並在需要時僅提供最小的訪問權限。ZTNA 旨在提高網路的安全性，並提供更精確的訪問控制。

傳統的網路安全模型通常基於城堡與護城河(castle-and-moat)的思維，即內部網路被視為安全的，而外部網路則被視為不可信任的。相反，ZTNA 假設內部網路和外部網路都是不可信任的，並採用更加嚴格的安全措施來保護資源和數據。

ZTNA 的主要原則包括

(1) 零信任原則：不信任任何用戶、設備或流量，並要求對每個用戶和設備進行驗證和授權，以確定其訪問權限。

(2) 最小化訪問權限原則：僅提供用戶和設備所需的最小化訪問權限訪問資源，以減少潛在的攻擊面和風險。

(3) 精確訪問控制：根據用戶的身份、設備狀態和上下文信息，實現精確的訪問控制，包括基於應用程式、資源和數據的控制。

(4) 認證和身份驗證：要求每個用戶和設備進行身份驗證，以確保其合法性和合規性。

ZTNA 的實現方式可以包括使用虛擬私有網路(VPN)、多因素身份驗證(MFA)、密碼管理、訪問控制列表(ACL)和行為分析等技術。它的目標是為組織提供更強大、更靈活和更安全的網路訪問控制，使得無論用戶和資源的位置如何，都能實現安全的連接和訪問。

最後，講者提供了對於實際導入零信任架構與應用的建議，包括避免過度分析，導致想的比做的多，導致計畫拖延等等不利因素，且重點應該在進步而非一次達成使用完美的方式，需能夠考量並根據組織當前能負荷的預算、公司

文化、時間點、應用範圍、風險等因素，逐步導入並達成可實現的目標。

圖 28、零信任架構與應用導入建議

(十九) 2023 年及其後的安全：自動化、分析和架構(Security in 2023 and Beyond: Automation, Analytics and Architecture)

本議題由 Akamai 高級副總裁兼首席安全官 Boaz Gelbord 擔任講座。

本場聚焦於網路安全行業面臨的挑戰和趨勢。講座談到對關鍵基礎設施的威脅增加、雲端化的過程會帶來新的風險，以及安全社群需要跟上快速移動的攻擊者腳步。講座還提到了在網路安全中使用自動化、分析和架構的重要性，以及如何利用人工智慧(AI)和機器學習(ML)來製定更有效的網路安全策略。

講座並以實體犯罪與網路犯罪的消長討論不斷變化的威脅格局。加密貨幣的匿名性以及跨境司法管轄的合作成本皆助長網路犯罪的提升，攻擊面亦是一個重大問題，每年都有數以千計的漏洞被發布。在日益複雜的供應鏈中，組織的關鍵供應商也遭到破壞。

講座引用了 Akamai 網路狀況報告的統計數據，顯示 Web 應用程式攻擊同比增長 137%，且針對某些行業攻擊有所增加，例如在製造業中有 30%為 DNS 攻擊；分散式阻斷服務(DDoS)攻擊也不斷增長，金融機構同比增長 22%，歐洲增長超過 70%。

講座接續討論了自動化、分析和架構在防範各種網路攻擊（例如 CEO 冒充、帳戶接管、API 攻擊和 Log4j 等組件中的漏洞）的重要性。攻擊者正在快速移動，甚至在相關 CVE 發布後的 24 小時內即開始掃描攻擊含有該 CVE 漏洞的系統。因此，講座強調自動化的重要，需要將保護過程自動化，避免完全依賴手動過程無法即時處理資安問題。講座還強調瞭解決住宅物聯網(IoT)漏洞

的重要性，因為自過往以來，駭客一直在使用這些物聯網設備來建立殭屍網路軍隊。

講座強調了自動化、分析和架構在確保未來安全性方面的重要性。網路中不斷增加的數據量使得區分各式連線行為的好壞變得更加困難，而自動化是唯一的解決方案。講座還強調了彈性架構的重要性，用以防止一個系統的漏洞導致整個組織的漏洞。講座另強調自動化、分析和架構對於保護組織免受不斷變化的威脅至關重要，並且需要長期投資才能實現此一目標。最後，講座並鼓勵安全社群中的人員協作和交換情資，以因應未來不斷發展的資安威脅。

(二十) 五種最危險的新型攻擊技術(The Five Most Dangerous New Attack Techniques)

本議題由 SANS 安全專家 Ed Skoudis、Heather Mahalik、Katie Nickels、Stephen Sims 及 Johannes Ullrich 擔任講座。

SANS(System Administration, Networking and Security)係以網路社群型式經營，為國際間重要的資安研究及學術教育組織，本次發表最新研究成果，對於 2023 年最值得關注的 5 種新興網路攻擊技術及其特點如下：

1. 搜索引擎優化攻擊(SEO)

如同普通公司利用搜索引擎優化(SEO)來提高某些關鍵字的排名以促銷他們的產品並將網路流量吸引到目標網站一樣，網路攻擊者也會求助於 SEO，使得非法網站的訪問量大幅提高，從而提升攻擊活動的成功率。Katie Nickels 講座表示，SEO 優化攻擊是一種危險的新興攻擊方法。攻擊者們開始大量利用常用的網路推廣策略，實現其非法攻擊目標。

在這種攻擊情況下，攻擊者利用 SEO 關鍵字誘騙受害者訪問詐欺網站、引導使用者下載惡意程式，或通過漏洞實現遠端用戶訪問，攻擊者還會使用一些技巧來保護惡意樣本以進行長期潛伏。SEO 優化攻擊表明網路攻擊者開始變得更加積極且主動，攻擊者逐漸拋棄那些容易被防禦的傳統攻擊技術。為了應對 SEO 優化攻擊，企業組織需要實施更有針對性的內部資安意識培訓計畫。

2. 惡意廣告利用攻擊

類似於營銷人員如何利用通過搜索引擎優化(SEO)的自然搜索技術和利用廣告

付費搜索技術，網路犯罪分子也在做同樣的事情。偷渡式攻擊也同樣受到惡意廣告(malvertising)活動的推動，這些活動人為地提高某些關鍵字的網站排名。講座並以一款名為 Blender 的免費 3D 圖形軟體的模仿廣告為例。當使用者搜索這個關鍵字時，排在最上面的 3 個網站連結都指向了惡意的詐欺網站，直到第 4 個搜尋結果，用戶才能進到真正合法的軟體網站。而那些非法的惡意網站看起來和真正的 Blender 官網幾乎完全相同，一般用戶很難分別其真偽。

3．軟體供應鏈攻擊

研究顯示，現代軟體系統的底層程式碼中有超過 90%都是開源的，這意味著幾乎所有軟體的研發與應用都存在著一條供應鏈，包括各種元件的引用，以及在軟體設計、開發、測試、部署和維護期間所涉及的各種環節，各式資安漏洞隨時可能出現，因此在企業軟體供應鏈中可能導致安全風險的因素也愈發複雜。

SANS 研究表示，軟體供應鏈攻擊已經成為現代企業或組織必須高度重視的最危險攻擊方式之一。講座並以 2022 年的 LastPass 漏洞事件就是最好的證明，攻擊者會利用協力廠商軟體漏洞繞過現有資安控制措施並訪問特權環境。對於各大行業的企業組織而言，LastPass 漏洞攻擊再次強調了要與各家協力廠商軟體供應商保持緊密合作的重要性，以便實現企業組織整體的安全架構、相互分享威脅情報，並熟悉不斷發展的資安攻擊技術。企業組織在解決軟體供應鏈的安全問題時，需要基於軟體應用的完整生命週期來考慮，監控和保護其中的每個環節，避免成為資安破口。

4．AI 人工智慧的進攻性使用

隨著像 ChatGPT 這樣的大型語言模型(LLM)的爆炸式增長，防守者應該有所預期，攻擊者、甚至是非常不具技術的攻擊者，利用這些 AI 工具加速他們的漏洞利用和零時差(zero-day)發現。

5．將 AI 武器化用於社交工程

Heather Mahalik 講座並表示，除了 AI 的技術攻擊用途外，預計攻擊者今年將大幅增加對於 AI 的使用，以使他們的社交工程和模仿嘗試變得高度可信。ChatGPT 可以非常真實流暢地模仿人類寫作，這個特點使其有可能成為一種強大的網路釣魚和社交工程工具，特別是當威脅分子需要進行跨語言的詐欺攻擊時，ChatGPT 可被用來更有效地傳遞惡意軟體。

在 ChatGPT 技術加持下的社交工程攻擊會更具欺騙性和危害性，這也意味著企業組織將比以往任何時候都更容易受到攻擊，內部人員只需誤點擊一個惡意檔案，就可能使整個公司面臨資安風險。在這種更嚴峻的攻擊面管理挑戰下，需要組織自上而下宣導網路謹慎文化，以確保員工能夠提前認識到與 ChatGPT 相關攻擊導致的資安事件。

(二十一)　沒有更多的時間：縮小與攻擊者的差距(No More Time: Closing the Gap with Attackers)

本議題由卡達國家網路安全局(NCSA) 國家網路融合事務主管 Ahmed Al Hammadi 及 IBM 全球安全服務部總經理兼副總裁 Chris McCurdy 擔任講座。

講座說明網路安全團隊從未有過更多的數據來尋找模式和阻止攻擊，然而檢測和回應攻擊者的時間仍然以數週、有時甚至以數月來衡量。與此同時，攻擊者已將部署勒索軟體所需的時間從 2 個月大幅縮短至不到 4 天。講座說明時間在網路安全中的重要性，以及如何優化它以領先於攻擊者。他們強調需要採取更主動的網路安全策略，即利用人工智慧和自動化方式處理最新的攻擊手法，並瞭解組織的受攻擊面和資安威脅。

Al Hammadi 講座討論了為確保 FIFA 世界杯足球賽等重大賽事安全的挑戰，強調公部門和私部門之間合作，以及各國之間共享知識和情資以領先於攻擊者的重要性。

IBM Security 全球副總裁兼總經理 Chris McCurdy 談到時間是我們生活中的一個關鍵因素，以及它如何影響網路安全。講座解釋，人類已經適應了通過預測未來、確定任務優先層級以及根據重要性、緊迫性和復雜性做出決策來優化反應時間。然而，控制網路安全時間非常具有挑戰性，因為攻擊者也會不斷創新來減少部署勒索軟體和其他攻擊所需的時間。隨著勒索軟體將部署時間從兩個月大幅縮短到四天以內，AI 人工智慧等自動化解決方案對於幫助資安團隊快速檢測和回應攻擊是必不可少的。

講座另強調了關注準備、利用人工智慧和自動化，以及瞭解組織的攻擊面和資安威脅以優化網路安全時間的重要性。人工智慧的實施必須建立在信任的基礎上，因為誤報和盲點將會導致重大缺陷。準備工作至關重要，組織必須準備好應對違規行為，因為絕大多數組織都沒有為網路威脅做好充分準備；講座並提倡積極主動的網路安全策略，而不僅僅是對威脅做出反應。

講座 Ahmed Al Hammadi 探討了卡達及其國家網路安全機構在確保 FIFA 世界杯足球賽安全方面所面臨的挑戰規模和範圍。該活動有超過 300 萬觀眾和數十億全球觀眾，由於網路安全是營運安全的一部分，因此不僅要確保實體區域的嚴密安全，更要確保營運技術的嚴密安全。

講座 Ahmed Al Hammadi 並討論了 Hayya 應用程式的開發和測試，Hayya 應用程式是在 IBM 公司的幫助下為 FIFA 世界杯足球賽創建的移動應用程式 APP。該團隊創建了大約 150 個場景來測試應用程式免受惡意軟體、帳戶接管、內部威脅和分散式分析服務等威脅。隨後，Ahmed Al Hammadi 講座更深入探討以網路安全的運營視角，強調預防、檢測和應對網路安全威脅的重要性。

Ahmed Al Hamadi 講座向負責 2026 年世界杯足球賽安全的人員提供建議，該世界杯將在美國、墨西哥和加拿大舉行。講座強調了公部門和私部門之間合作與協作的重要性，因為在網路威脅和攻擊方面並沒有邊界。講座並強調，世界杯需要一個框架，該框架採用非常合作的方法來開拓工作，並鼓勵各國之間共享資安情報和知識，以此來保持領先於攻擊者。

(二十二)　從公司部門夥伴關係到營運合作(From Public-Private Partnerships to Operational Collaboration)

本議題由 National Security Agency(NSA)的 Morgan Adamski、美國財政部(Department of the Treasury, DoT)的 Todd Conklin、FBI 的 Cynthia Kaiser、美國能源部(Department of Energy, DoE)的 Kyle Pfeiffer 及 Joint Cyber Defense Collaborative(JCDC)的 Clayton Romans 共同擔任講座。

講座從擔任政府機關部門資安人員的角度進行分享，認為分析性的資安情資必須盡可能與私部門分享，才能有效達到資安資訊共享與資安聯防體系發揮最大綜效的功能。有關分析機制，則必須在設計之初就考量其安全性問題，才能達到更頻繁、更安全的深度性與分析性資安情資分享。目前美國 FBI、CISA、NSA 等，已建立資訊分享平台，也都透過這些方式分享重要情資。

講座說明，自從 2019 年後，俄國大量以網路方式攻擊美國，也促使美國行政部門積極與利害關係人就技術支援與情資進行交流，以求更深入瞭解各資安事件現況，以及尋找適當的解決方案。

講座也分享，由於資安資訊分享平台積極運作，使得美國政府部門在 2023 年

到目前為止，已經向 100 多所學校、醫院等單位示警，成功嚇阻資安事件發生。當然仍有許多民間部門由於資安預算與經費比較不足，所以無法獨立分析可疑的資安情資，但建議可以立即傳送給政府部門，透過進一步分析與放大資安情資，找出資安威脅，並加以防範，藉此提高資安防護，而這一切都仰賴公私部門建立互信關係，才有辦法達成。

(二十三)　在 OT/ICS 環境中保持對抗性 AI 的領先地位——緩解 CWE-1039 (Stay Ahead of Adversarial AI in OT/ICS Environments – Mitigating CWE-1039)

本議題由 ObjectSecurity LLC 的研究軟體工程師 Jason Kramer 及創辦人 Ulrich Lang 共同擔任講座。

本場會議主要討論運營技術和工業控制系統、網路安全以及現在和將來如何被 AI 影響，並探討如何採取主動和被動的緩解策略方式以保護相關 AI 模型。

Handling of Adversarial Input Perturbations 是指 AI 產品使用機器學習等自動化機制模型將複雜的數據（如圖像或音頻）輸入以識別為特定概念或類別，但它無法正確檢測或處理，導致該機制進行修改或構建模型後，輸入執行檢測時，產生不同或不正確的概念。

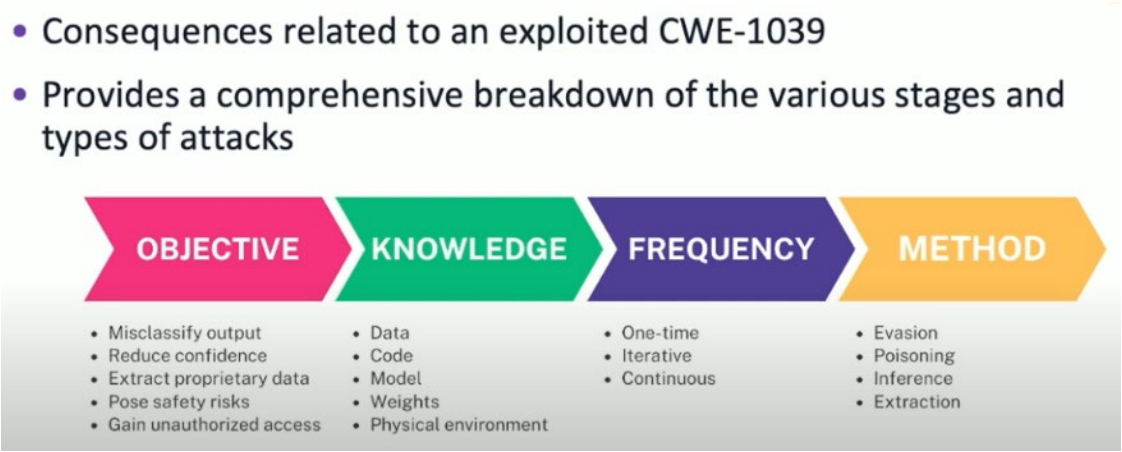


圖 29、CWE-1039 : Automated Recognition Mechanism with Inadequate Detection or

於 OT/ICS 背景下的 AI 模型威脅，本質上是一種基於電腦視覺系統做出錯誤轉彎或錯誤決定，導致自動駕駛汽車不正確，探討各種攻擊和緩解措施。其中一個關鍵部分是可能發生的物理和網路物理損壞。所以特別是傳感器網路，自動駕駛汽車、智慧城市、智慧電源等領域所使用的電腦視覺或其他機器學習的東西，

由於網路實體特很容易受到攻擊而造成惡意的資料入侵的破口。

AI 模型被惡意的資料入侵的緩解措施基本上分為兩類：一種是檢測，另一種則是保護緩解。需要以某種方式確保模型保持安全， MITRE ATLAS 被稱為威脅矩陣的地圖集，提供基於威脅、戰術等攻擊框架的分類，可以用來進行威脅行為的檢測。

舉例說明，送貨無人機或自動駕駛車輛的實際入侵或攻擊而造成損壞，都將會造成服務提供者的名譽損失，也可能會造成破壞或盜竊，如：一架送貨無人機偷包裹是可能發生的情況之一。而在自動化工廠上也有很多針對這類物聯網系統的攻擊，可能造成分析傳感器數據被攻擊，影響物理環境和消費者的安全。威脅行為者引入惡意數據，進入 AI 機器學習的訓練模型中或形成商業間諜活動，本質上就像是營業機密和經營效率的數據洩漏一樣，通常是會造成有財務、產品、商譽、人身、品牌等損失。

圖 30、可能的威脅情境-送貨無人機

現階段資安人員尚不認為人工智慧和機器學習是一種威脅，所以不會真正監控 AI 運作，也沒有考慮攻擊面。此外，攻擊可能不會留下痕跡或簽名以供追蹤檢測。因此，即使知道模型可能受到了攻擊，也可能很難弄清楚在哪裡受到攻擊的。例如，在電腦視覺中，很難瞭解哪些圖像受到攻擊。

AI 模型的保護可以分為主動保護模型與被動保護模型兩種類型，使用形式驗證模型檢測邊界違規條件，建立可解釋性和理解模型的基本決策方法，並獲得對

於決定判定的解釋功能，並包括持續監控和機器學習操作管道。兩種模型分述如下：

1. 主動保護 AI/機器學習(Proactively Securing AI/ML)可以採取下面防禦措施或方式分類如下：

(1) 穩健優化(Robust optimization)

(2) 最大限度地減少模型對攻擊者的暴露(Minimizing model’s exposure to attackers)

(3) 對抗訓練(Adversarial training)

(4) 防禦淨化(Defensive distillation)

(5) 檢測後門和中毒的輸入(Detecting backdoors and poisoned inputs)

(6) 驗證和認證(Verification and certification)

(7) 水印數據(Watermarking data)

(8) 模型壓縮(Model compression)

就主動保護模型而言，模型在訓練之前是穩健的，並最大限度地減少模型對攻擊者的暴露，包括限制誰有權訪問模型或其 API 、限制其他方式進行推理，或可以訪問哪些數據，包括對抗性訓練的數據，可以針對特定類型的攻擊進行提供訓練樣本，使其能更強大地抵禦這些攻擊。而防禦性淨化則是在模型再訓練中，針對驗證原始模型然後檢測是否有任何違規或差異，也可給數據加浮水印或使用區塊鏈來確保數據不會隨時間而改變。最後，有一些特定的方法可以壓縮模型，使模型更健壯並進行優化以抵抗對抗性攻擊。

2. 被動保護 AI/ML(Reactively Securing AI/ML)可以採取下面保護措施或方式：

(1)對抗檢測(Adversarial detection)
(2)去噪(Noise removal)
(3)預處理數據(Preprocessing data)
(4)模型微調(Model fine-tuning)
(5)檢測分佈數據(Detect out of distribution data)
(6)禁止訪問並強化系統(Disable access and fortify system)等等。

就被動保護模型而言，其針對需要監控的數據區域可進行對抗性檢測，並在

推理之前或之後檢測攻擊，然後確定是否擬定對抗性攻擊。去噪、預處理數據可對數據進行清理，針對數據進行子採樣，並確保它不會在模型訓練完成後受到攻擊。因此，可以微調模型並隨著時間的推移對其進行改進，藉由檢測出數據分佈資料，可視化給出用於推理的一組特定樣本，並檢視該集群是否有漏洞。最後，可禁止訪問並強化系統，以阻止可能引入對抗性攻擊的訪問。

(二十四)　NIST 網路安全框架 v2.0：改變何在？(NIST Cybersecurity Framework v2.0: What’s changing?)

本議題由 Optic Cyber Solutions 的網路安全工程師 Kelly Hood 及 Paladin, LLC 的網路安全工程師 Greg Witte 共同解說。

網路安全框架 1.1 版最初於 2014 年發布，而網路安全框架 2.0 版則剛剛發佈。如何衡量一個組織的改進有其困難，因此審視層級代表一個新思考的機會，如：「有建立正式的風險管理流程嗎？是否將風險管理其融入日常工作中，成為所做的每一部分？有多大程度共享資訊？」這些是層次就是 NIST 將在本此網路安全框架更新時，期望構建內容的一部分。

網路安全框架 2.0 版的其中一個關鍵點圍繞在供應鏈風險管理上，包括供應商管理、瞭解風險、可以從供應商那裡得到什麼、以及供應商從我們這裡得到什麼、如何保護我們的數據和我們的系統等等。因此，網路安全框架 1.1 版的有些類別和子類別被移動了，相關如下圖所示。

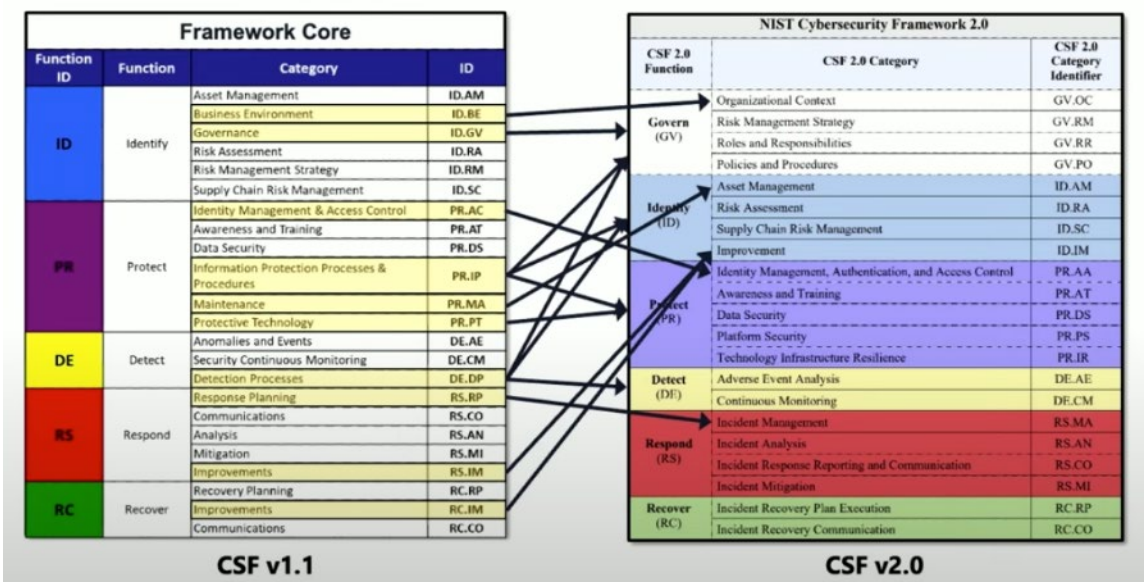


圖 31、網路安全框架異動對照

NIST 網絡安全框架 1.1 版類別分為：識別(ID)、保護(PR)、檢測(DE)、回覆

(RS)、恢復(RC)。1.1 版的一項重要成果是明述靜態數據受到保護，作為一個團隊的資安專責成員需要弄清楚哪些數據需要保護，並定義什麼是足夠的保護。1.1 版可有效的解決網路安全風險，但為了使組織更容易更有效地應付當前及未來的網路安全挑戰 ，NIST 在 2.0 版最調整了資安事物的治理，有機會將資安議題觸及到領導層級的內容，並仍然會識別、檢測、保護、回覆的所有事物，並從中恢復。故網路安全框架 2.0 版類別是：治理(GV)、識別(ID)、保護(PR)、檢測(DE)、回覆(RS)、恢復(RC)，藉由治理、識別和保護功能為關鍵的資產預防網絡安全事件，並通過檢測、回覆和恢復功能來檢測和反應事件，並通過包含組織環境、風險管理戰略、政策和程序以及角色和責任的新治理職能進行網路安全治理。

(二十五)　40 位 CEO 告訴我們的關於建立網絡彈性的事(What 40 CEOs Told Us About Building Cyber Resilience)

本議題由 ISTARI 的 CEO Rashmy Chatterjee 及 ISTARI 與牛津大學的 Manuel Hepfer 共同解說。

此演講為 ISTARI 與牛津大學展開為期一年的研究成果，報告名稱為《The CEO Reort on Cyber Resilience》，主要與全球大型企業 37 位 CEO 進行訪談，u 瞭解 CEO 們協助企業建立網路韌性時所扮演的角色、觀點和所發揮的作用。

ISTARI 是淡馬錫創立的一家全球資安公司，致力於協助客戶建立網路韌性。該公司與牛津大學賽德商學院(Said Business School)公佈 CEO 報告調查結果。該報告以高階管理人員的視角切入，強調 CEO 在建立網路韌性所發揮的關鍵作用。

演講者為 ISTAR 知識與洞察力負責人暨牛津大學賽德商學院 Manuel Hepfer 博士，他與美、歐和亞洲 CEO 進行長達一小時面對面訪談，這些公司的平均營收超過 120 億美元，平均僱用 40,000 名員工。三分之一的受訪者來自亞洲，接受採訪的 9 位 CEO 表示，他們的公司度曾遭到嚴峻的網路攻擊事件。

圖 32、演講者 ISTARI Rashmy Chatterjee 執行長及 Manuel Hepfer 博士

當網路攻擊事件發生時，身為企業 CEO 不可避免地處在事件中心。網路攻擊成為業主擔心何時會發生的議題。企業 CEO 自然在資安事件發生時承擔相關責任。不過根據演講者調查，企業 CEO 對資安風險的真實看法，乃是充滿隱藏地恐懼、不確定性和不適應性。這揭示了企業 CEO 們在管理資安風險方面的情緒和掙扎，特別是在匿名調查過程中，CEO 們較為誠實地論述他們對資安的感受、沮喪和遺憾。

企業 CEO 們承認，他們對監管機關、股東及董事會負責及報告。然而，大多數 CEO(72%)表示，他們對資安決策感到沒有把握，這會導致 CEO 將資安責任和對資安的理解委託給技術團隊，但這可能會危及組織和企業的韌性。演講者表示，在訪談過程中許多 CEO 強調，在資訊不對稱的情況下，必須做出痛苦的決定。特別是在缺乏瞭解的資安領域中承受著無形的壓力。

研究者建議企業 CEO 可採用的四種思維建立企業網路韌性：

1. 負起共同責任，而不僅是問責。所有接受訪談的企業 CEO 表示，對資安負有重要責任。然而，一項針對首席資訊安全官(CISO)的調查發現，有二分之一的歐洲企業 CISO 和三分之一美國企業中 CISO 認為，他們的 CEO 沒有責任感。根據研究，此種認知上的差距，在於問責制，也就是 CEO 不認為自己負有資安責任，CEO 應與 CISO 一起共同承擔建立網路和資安韌性的責任。
2. 從盲目信任轉變為知情信任。企業 CEO 不應盲目信任技術團隊的建議，更應保持不斷學習和嘗試理解問題的本質，進而掌握企業的網路韌性成熟度。

3. 持續準備應對網路攻擊。企業 CEO 應接受所謂的「準備悖論」，就是準備永遠不會有結束的一天，企業應對網路攻擊的準備不應自滿，否會會危及企業組織的網路和資安韌性，企業必須隨時保持警惕和警覺。

最後，調整溝通方式，調節來自外部利害關係人的壓力。利害關係人可能因為立場不同，甚至是有著相互衝突的需求。CEO 應針對董事會、股東、監管機關、客戶及供應商調整溝通方式，CEO 可能是壓力的傳遞者、過濾器、吸收者或放大者，須建立彈性的溝通方式。

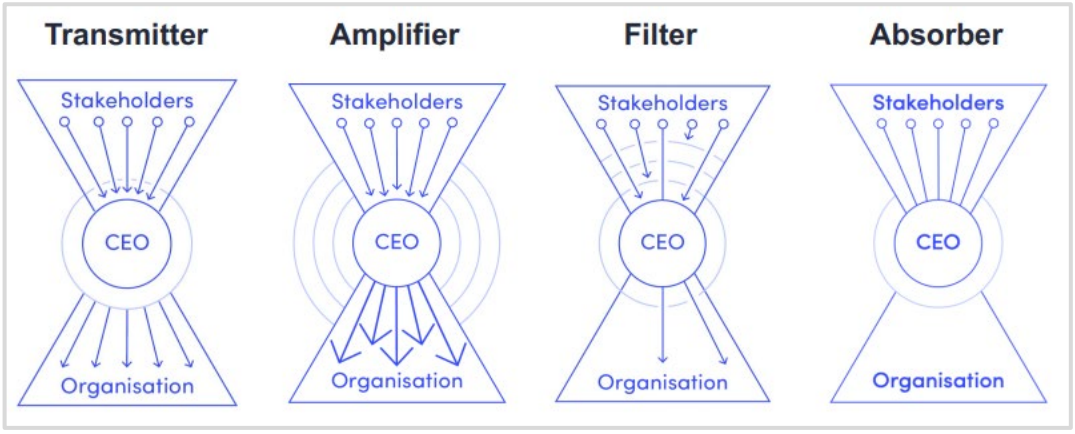


圖 33、企業 CEO 針對不同利害關係人溝通時所扮演的角色

ISTARI 的 CEO Rashmy Chatterjee 表示，網路攻擊的影響超出了對 IT 的認知，CEO 難以領導當企業發生資安事件時如何進行響應。從這些坦率的訪談和調查中，可以更好地回答 CEO 所應扮演的角色，並填補 CEO 需要做什麼來建立企業組織的網路韌性。

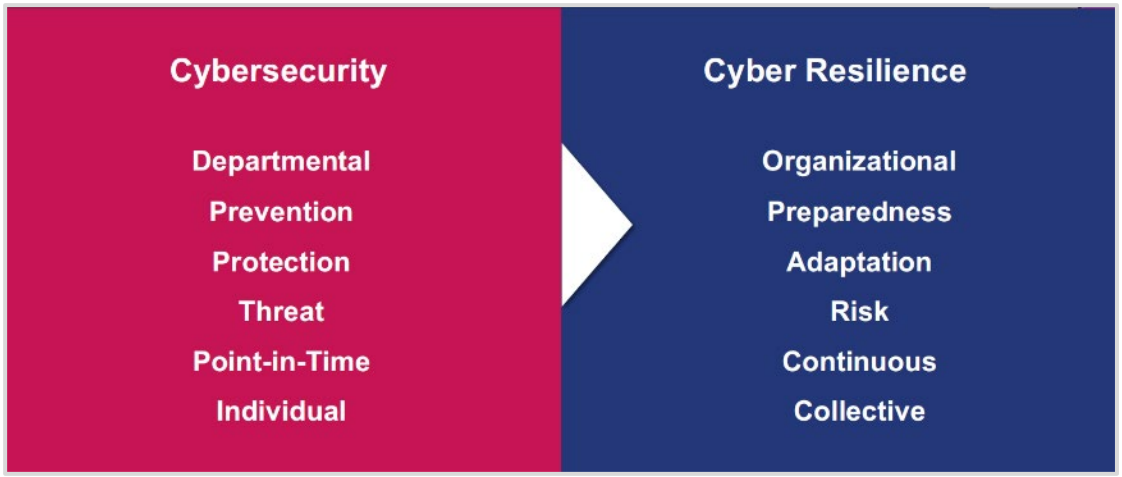


圖 34、CEO 從關注網路安全到轉而關注建立企業網路韌性

此報告希望能為企業的 CEO 建立網路韌性的 SOP 和腳本，列出 CEO 可以採取的具體步驟，預測、防禦、響應和應對網路攻擊。包括重新審視風險管理、衝新

審視現有資安做法、重新審視資安預算分配、重新審視董事會的參與、並重新審視企業對資安的意義。

(二十六)　這是一段旅程……NIST 將以網路安全框架為首(It’s a Journey…Where is NIST Headed with the Cybersecurity Framework)

本議題由美國商務部國家標準與技術研究院 (NIST) 國際政策專家 Amy Mahn 及高級技術政策顧問 Cherilyn Pascoe 共同解說。

NIST 前身為美國國家標準局(NBS)，屬於美國商務部的非監管機構，其使命為推展測量科學、標準和技術，合作對象包括政府機關、工業界及學術界，並和國際合作夥伴一同制定指南，如同本次演講主題「網路安全框架(Cybersecurity Framework, CSF)」，這個框架目的是為組織提供有關如何預防、偵測和回應網路攻擊的指引，包含管理網路安全相關風險的標準、指南和最佳實踐，NIST 自 2014 年推出 CSF 1.0 版框架至今，經 2018 年 CSF 1.1 改版，已成為世界各國都在使用的網路安全評估框架。

講座說明目前 NIST 正進行 CSF 2.0 改版作業，並在去(2022)年 2 月進行意見徵集(Request for Information, RFI)，作為改版依據，徵集結果總共獲得超過 130 多則來自國際網路安全標準組織與各國政府回覆，超過半數為來自產業意見，尤其以 IT 科技產業為大宗，包括 Microsoft、IBM 及 Cisco 等，其他則來自通訊、能源、金融及醫療等產業。多數建議認為 CSF 2.0 版應維持簡單、彈性且能適用於各產業，並確保新舊版本之相容性。另一方面希望強化 NIST 與聯邦法制、國際安全標準等非 NIST 體系之研究資源的一致性，強化框架與其他實施指引間的對應關係。

NIST 的 CSF 2.0 版意見徵集反映了對雲端服務、開源軟體使用、供應鏈風險管理等新興議題關注，重點徵集意見如下：

IT/OT 匯流的技術趨勢：CSF 2.0 版需反應現階段資訊科技/營運科技(IT/OT)匯流的技術趨勢，在網路風險管理層面，應考量橫跨 IT、OT、物聯網(IoT)、容器(container)與雲端環境之資訊資產，或將工業控制系統(ICS)安全指引與新版框架之間做對應。

1. 雲端運算與共享服務的商業模式：CSF 2.0 版需關注雲端運算和共享服務的商業模式，因為這是未來必需考慮的重要議題。

2. 評量工具的差異性：CSF 2.0 版應強調評量工具會因不同評估對象的不同(例如自評、供應商、產品或服務)而有所差異，並提供額外指引。

3. 供應鏈安全管理：供應鏈安全管理是近年來全球普遍關注的問題，對於供應鏈風險管理(Supply Chain Risk Management, S-CRM)框架，一般意見認為應將其納入現有的 CSF 框架中，以避免混淆和重複建立新框架。

4. 軟體物料清單(SBOM)：建議在資產管理方面加強對物料清單的指引，尤其是對軟體物料清單(SBOM)的安全指引，SBOM 在雲端服務供應鏈屬於重要環節。

目前 NIST 已在今(2023)年 1 月發布 CSF 2.0 版概念文件，並陸續舉辦網路論壇、工作坊等形式蒐集利害關係人對於 CSF 2.0 版草案的回饋，講座說明 NIST 預計在 2024 年初正式公告 CSF 2.0 版，預料將對各國政府組織、民間企業的網路安全防禦策略產生重要影響，其 CSF 2.0 改版時序如下圖所示。

圖 35：CSF 2.0 改版時序

CSF 2.0 版草案框架定義六大核心功能，分別為治理(Govern)、識別(Identify)、防護(Protect)、偵測(Detect)、回應(Response)及復原(Recover)，較 1.1 版定義的 5 大核心功能，多增加了「治理(Govern)」功能，此外，原 1.1 版的 23 個類別與 108 個子類別，在新版中也調整為 21 個類別與 112 個子類別，改版重點如下：

1. 明確界定用途和適用範圍

CSF 1.1 版文件名稱為「提升關鍵基礎設施網路安全框架（Framework for Improving Critical Infrastructure Cybersecurity)」，易造成外界誤解僅適用於關鍵基礎設施，NIST 將更改 CSF 2.0 版的標題與文件敘述，明確界定其用途和

適用範圍。

2. CSF 2.0 保持框架形式，提供現有標準與資源的全景與其他框架連接

CSF 2.0 版將透過利用與連接全球公認的標準和指南(如風險管理框架、隱私框架和 MITRE ATT&CK 威脅模型框架)的方式，產生組織所期望的資安價值。例如許多組織會將 CSF 框架結合 MITRE ATT&CK 框架，以實現組織滿足合規性要求和目標。

3. 全新的治理（Governance）功能

CSF 2.0 版本將擴大對治理主題的廣度和深度，以便將未來其他正在發展中的標準或框架的治理功能納入其中，如 NIST 的「人工智慧風險管理框架（Artificial Intelligence Risk Management Framework，AI RMF)」，將有助於組織更全面地回應網路安全挑戰，實現網路安全目標。

表 1：CSF 2.0 核心功能和類別名稱

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

講座說明 NIST 鼓勵更多國家採用 CSF 框架，框架的核心精神，即是一個為組織建立能夠持續運作的成熟度評估框架，而我國政府為落實資安，自 2014 年起開始推動資安治理制度，首先建立政府資安治理架構，包含 4 大面向與 18 個流程構面，以及政府機關資安治理成熟度評估機制與自動化評估工具，近期國內已有政策欲將此一概念推動到國內各產業，尤其是製造業與金融業。數位部與工研院打造的 SECPAAS 資安整合服務平臺，推出「資安成熟度評級服務」，許多資安業者也紛紛提出資安成熟度評估機制，提供企業客戶或供應商作為評估自己資安成熟度的參考，持續精進資安。

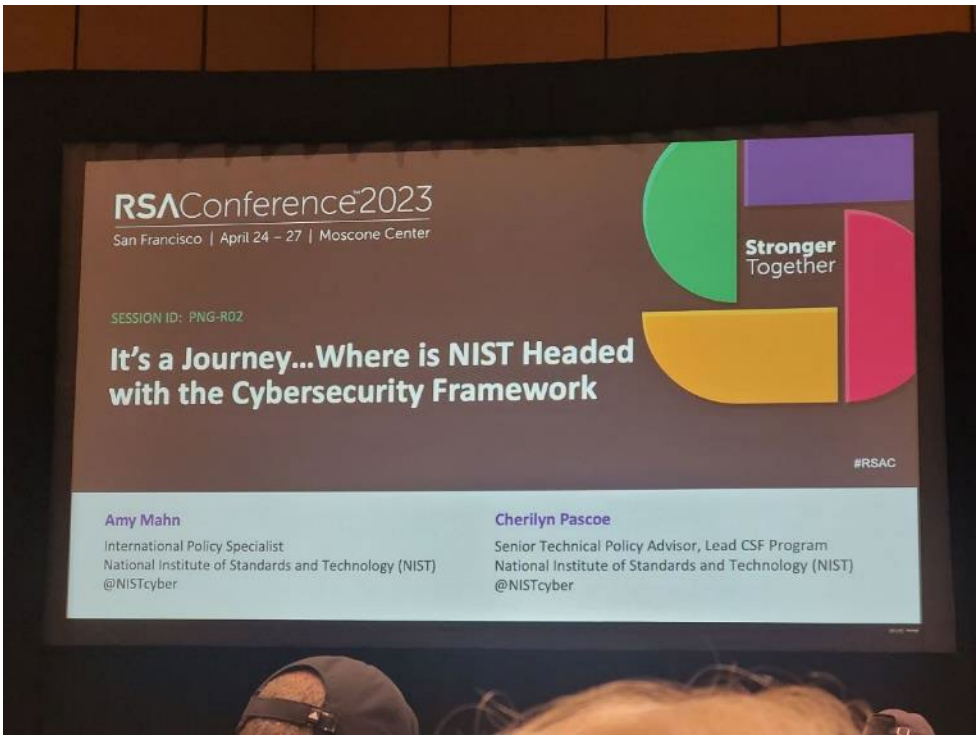


圖 36、It's a Journery…Where is NIST Headed with the Cybersecurity Framework

圖 37、NIST 講者

(二十七) 保衛電動汽車充電網路的攻擊面和數據孤島(Protecting the Attack Surface and Data silos of an EV Charging Network)

本議題由 Techniche 的 Thomas Caldwell 擔任講座。

本議程彙整了現代與電動充電裝置及網路的安全相關問題，在日益蓬勃發展的電動載具，包含電動車、無人機等裝置有任何網路或通訊協定的情況下，其安全也被視為重要的議題。本議程討論目前研究發展，以及如何防護資訊洩漏或可能攻擊面的防護，與如何制定或研析對應的措施。

目前之 EV 充電裝置可能有的風險包含：

1. 製造商為中國
2. 樹莓派嵌入家庭充電器中
3. 可能會存在火災風險
4. 家庭充電器可能存在的與家庭網路相關的安全漏洞。這些漏洞可能會被駭客利用，從而對家庭網路和相關設備造成損害或風險。

卡巴斯基在 EV 充電裝置發現，目前市面上家用充電裝置有以下特點：

1. 支援 Wi-Fi 和藍牙協定
2. 使用 J1772 相關標準

3. 簡化的硬體和軟體設計，不必處理費用支付和先進電力管理

而卡巴斯基的報告中提到可能安全漏洞與攻擊方式如下：

1. 充電裝置存在開放的 Telnet 端口，雖需要密碼驗證才能訪問，但若存在暴力破解或弱密碼相關問題，攻擊者可以利用這個漏洞來入侵充電裝置並控制其功能。
2. 充電裝置存在漏洞，攻擊者可以利用這個漏洞來調整最大電流，從而導致線路過熱，引起火災。
3. 攻擊者可以暫時禁用用戶家庭電氣系統架構的某些部分，如果設備連接不當，線路可能會因過熱而引起火災。
4. 藍牙堆疊中發現了一些漏洞，但對系統影響較小。
5. 攻擊者可以成功入侵充電站並遠端控制，從而阻止汽車充電。這可能會導致用戶無法使用他們的汽車，或者在需要時無法及時充電。

講座進一步探討 EV 充電裝置的殭屍網路，表示 EO 公司生產了近 4000 個充電裝置，其中大約四分之三安裝在英國，而攻擊者可以通過將自己的程式碼推送到這些充電器上來實現入侵。

攻擊者可以在 10 分鐘內獲得充電器的完整源碼、編碼字符串中的網路拓撲概述、FTP 和 SMTP 認證訊息以及加解密密鑰等敏感訊息。這些訊息可以讓攻擊者更容易地控制和管理僵屍網路。

而講者認為只有通過合作才能實現更強大的安全防護。這需要整個社區的參與，包括企業、政府和個人等。同時，自動化和整合是減少人為因素的關鍵，可以通過建立合作夥伴關係和透過使用 API 來實現。此外，還存在許多後端數據庫，需要採取相應的安全措施來保護數據。者主張通過合作、自動化和整合等方式來實現更強大的安全防護。

EV 充電裝置的攻擊面十分廣泛，其原因和特徵可統整如下：

1. 為何 EV 充電裝置要連接網路？

(1) POS 系統：一些 EV 充電器與 POS 系統相連接，使用戶可以支付充電服務費用。

(2) OCPP 遠程監控和控制：開放式充電點協議 (OCPP) 是一種標準協議，用於 EV 充電器和中央管理系統之間的通信。讓使用者可以遠程監控和控制充電過程。

(3) 智慧電子看板：一些 EV 充電器配備了智慧電子看板，顯示有關充電過程的訊息，例如充電狀態和預計剩餘時間。

2. EV 充電站如何連接網路？

(1) 蜂窩 LTE 4G/5G 連接：一些 EV 充電裝置可以使用蜂窩網路連接到網路。

(2) Wi-Fi：許多 EV 充電裝置支援 Wi-Fi 連接，這使得用戶可以通過手機或平板控制充電過程。

(3) 乙太網路(LAN)：一些 EV 充電裝置可以通過有線以太網連接到網路。

(4) 其他類型的連接：例如 FTP、Telnet、RFID 和車輛充電裝置等。

這些不同的連接方式提供了不同的優點和風險。例如，使用 Wi-Fi 連接可能會增加系統的攻擊面，而使用有線乙太網路可能會更加安全但不夠靈活。因此，在實施這些連接時需要考慮安全性和便利性之間的平衡。

而 EV 充電裝置容易接收來自網路的韌體更新，這可能會被駭客利用注入惡意程式碼或漏洞。同時，EV 充電裝置還可以將日誌數據傳輸到遠端伺服器，這可能會導致用戶數據洩露或其他安全問題。

除此之外，攻擊者可能會利用漏洞或弱點來入侵充電裝置，從而獲取敏感訊息、控制充電裝置或對其進行破壞性攻擊。圖 38 為風險可能會導致個人和企業的財務損失，以及對公共安全和基礎設施造成威脅。

Risk	Est. Impact
Loss of personal and financial information	> $100 per person per year for credit monitoring + exploit management cost (if any)
Damage to EV battery and other EV systems	> $3,000 per event per vehicle
EV charging station malfunction	> $100 per diagnostics + repair/replacement cost per station
Grid outage	~ $40,000 per hour
Building network breach	• Hotel: up to $0.5M per incident per property • Restaurant: up to $0.4.M per incident per location • Supermarket: up to $1.9M per incident per location • School: up to $1.1M per incident per school location • Residential: up to $5,000 per incident per tenant • Manufacturing: up to $0.8M per incident per location

圖 38、攻擊可能損失預估

講座亦分享 EV 充電裝置對電力網路的影響。現代 EV 充電裝置需要從電力網路中存取大量的能量，而快速充電裝置的功率水平已經超過了 350 kW。研究人員討論了使用正確的攻擊方法可能對電力網路造成重大干擾的能力，讓大量充電裝置同時停止工作可能會威脅到電力網路的頻率和電壓穩定性。

Vehicle-to-Grid Chargers 是指一種充電裝置，可以將電動車的電池中儲存的能量反向輸出到電力網路中。這種充電裝置的出現可能會帶來風險，因為攻擊者可以利用它們進行攻擊。例如若 EV Charger Botnet 突然改變控制和供應電力的能量，可能會導致停電並使某些基礎設施停止運作。

而對於 Charge Point Management Platform (CPMS) 中，對於 CPMS 管理平台之發現包含以下幾點：

1. 以色列的 Saiflow 在使用 Open Charge Point Protocol (OCPP) 通過 Web 服務連接的中發現了兩個漏洞。

(1) 處理多個充電器連接的不當：代表充電裝置發起假連接到 CPMS

(2) 弱身份驗證策略：偽造連接的身份驗證可以輕易被駭客攻擊

2. 風險包含阻斷服務(DoS)攻擊、數據和能源竊取。
3. 可能會變成用於對 EV 充電裝置網路進行 DDoS 攻擊的僵屍網路。

4. 有著最佳實踐密碼管理。

5. 這些漏洞是在廣泛部署的 OCPP 1.6J 中發現的，然而它們仍然存在於 OCPP 版本 2.0.1 版本中。

在政府管理方面，Federal Highway Administration: National Electric Vehicle Infrastructure Standards and Requirements 是一份由美國運輸部聯邦公路管理局發布的新法規，是國家電動汽車基礎設施（NEVI）計劃資助的項目，用於建立 EV 充電裝置的最低標準。這些法規包括早期的安全標準，涵蓋各種主題，其中包括了針對 Plug & Charge 等多個主題的早期網路安全標準，以進一步保護消費者。這些法規用於確保公共充電站的安全性和可靠性，以促進電力交通工具的普及。

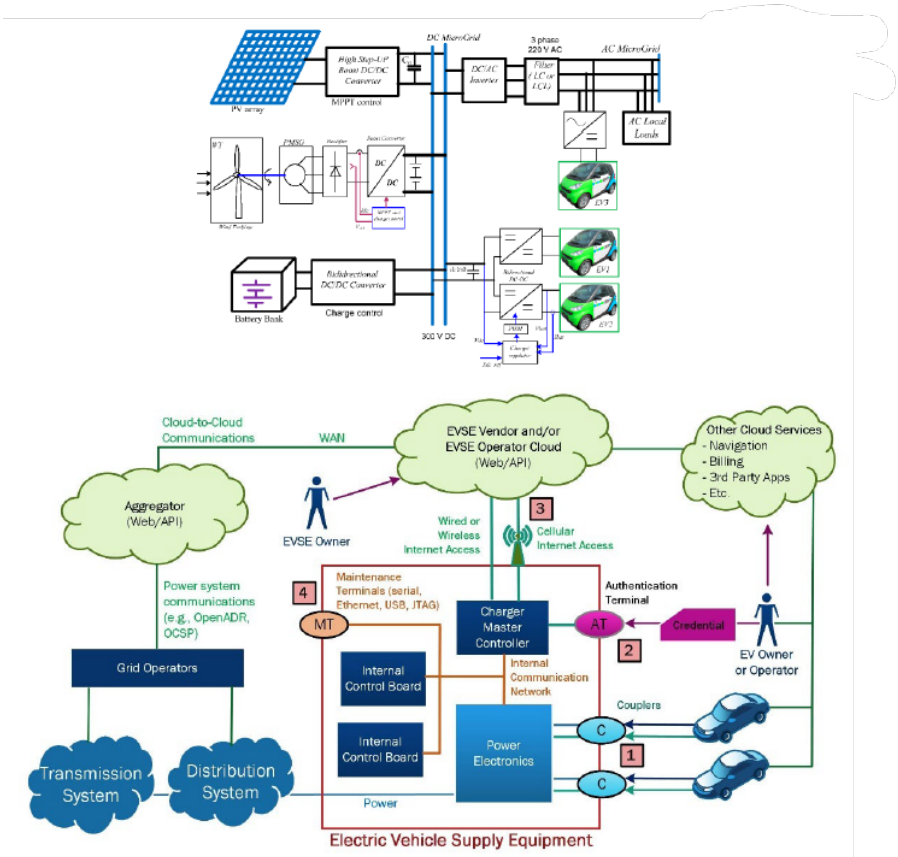


圖 39、EV 充電裝置架構圖

EV 充電裝置亦為一種物聯網設備類型，因此建議採取一些措施來保護它們免受網路攻擊。需立即實施的作業包含網路安全評估或滲透測試，並閱讀 Sandia National Labs 的最佳實踐文件以瞭解如何保護 EV 充電裝置及相關基礎設施。而在三個月及以後，建議檢查物理訪問、安裝防篡改傳感器、檢查系統強化措施等。以及建議升級到 OCPP 2.0.1 以保障網路安全。最後，建議將 EV 充電器視為

未開發完整的智慧 IoT 設備，像駭客一樣思考，以更好地保護它們免受攻擊。可參考的規範與標準包含 ISO 15118 中提到了 OCPP 2.0.1 與 Vehicle-to-Grid 的通訊。

三、 展場觀察

(一) RSA SOC 戰情室(RSA SOC Room)

在 RSA 會議期間，團員有機會參觀 1. RSA SOC 戰情室，由 netwitness、cisco 和 IBM 共同組成，專門用於監控和保護 RSA 會議期間的網路環境，以確保會議期間的網路安全，並迅速應對任何潛在的安全威脅。

整個 RSA SOC 戰情室的運作流程非常複雜而高效。首先，所有的網路流量都通過底層的 Cisco 網路設備（Cisco Catalyst 9200）進行控制和管理。這些設備使用 SPAN 技術（port mirror）將流量鏡像到其他關鍵設備進行進一步的分析和處理。

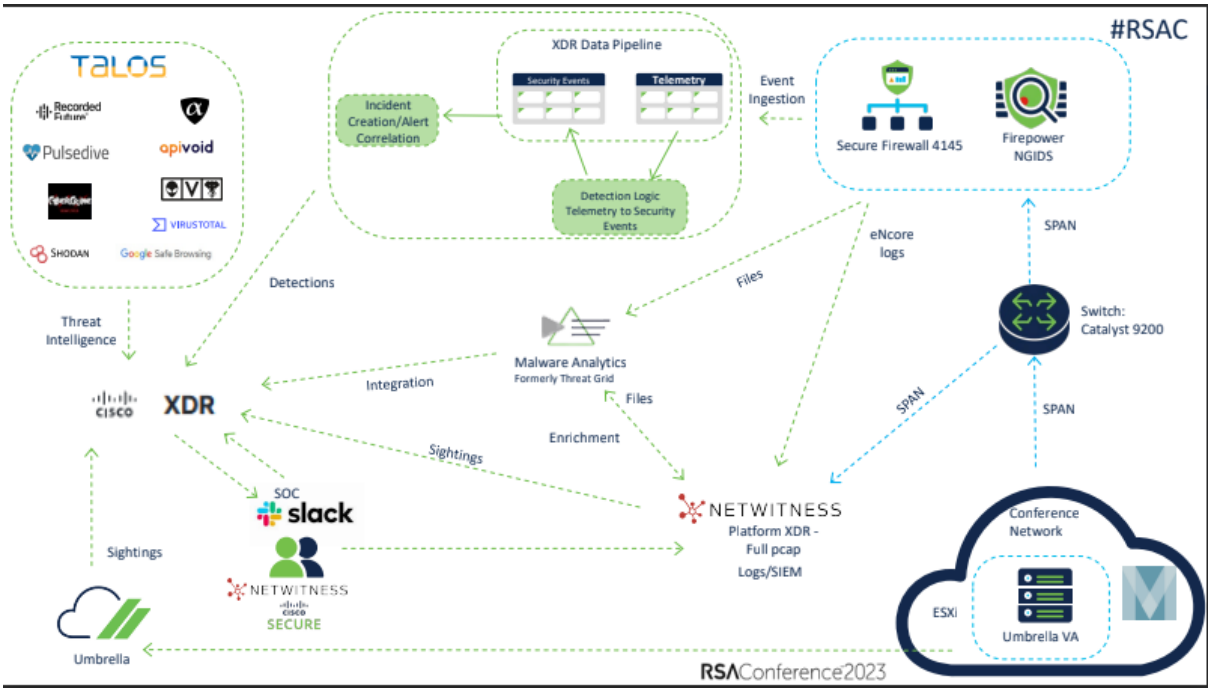


圖 40、RSA conference SOC 網路架構

Cisco Firepower 系列的 Next-Generation Intrusion Detection System（NGIDS）和 Secure Firewall 負責分析和阻擋潛在的入侵和威脅。這些設備利用先進的安全演算法和資料庫，對網路流量進行即時監控和檢測，以確保會議期間的網路環境的安全性。

同時，NetWitness 被用作事件分析和安全資訊和事件管理（SIEM）平台。它接收和分析從 Cisco 設備和其他來源收集的事件和日誌資料，以提供綜合的安全狀態和威脅情報。

除了內部監控和分析，RSA SOC 戰情室還整合了外部威脅情報平台資源。這包括 VirusTotal、MIPS 和 SHODAN 等知名平台，它們提供了關於已知威脅和漏洞的資訊，以便迅速識別和應對潛在的威脅。

RSA SOC 戰情室的建置時間非常短，只需要大約 3 天的時間。在這段時間內，需要進行軟硬體的建置、軟體設備的部署和測試。這顯示了 RSA SOC 戰情室團隊的高效能和專業水準。

此外，會議還提到，在 RSA 會議結束後，RSA SOC 戰情室將對會場內的網路流量進行進一步的分析和資料揭露。這項評估將有助於瞭解該次會議期間網路的流量分佈和可能的安全威脅。會後公布的資料中提到，發現了一些流量來源，如利用會場內的網路進行針對中國境內 IP 的現場直播以及未加密的 SIP 通話連線等。

RSA SOC 戰情室在保護 RSA 會議期間的網路安全方面發揮了重要作用。通過整合不同的安全設備、分析工具和威脅情報平台，它能夠全面監控、分析和應對潛在的安全威脅。同時，該會議還強調了對會場內流量的分析和資料揭露，以加強對網路威脅的識別和解決能力。這些措施顯示了 RSA 對維護會議網路安全的重視和努力。

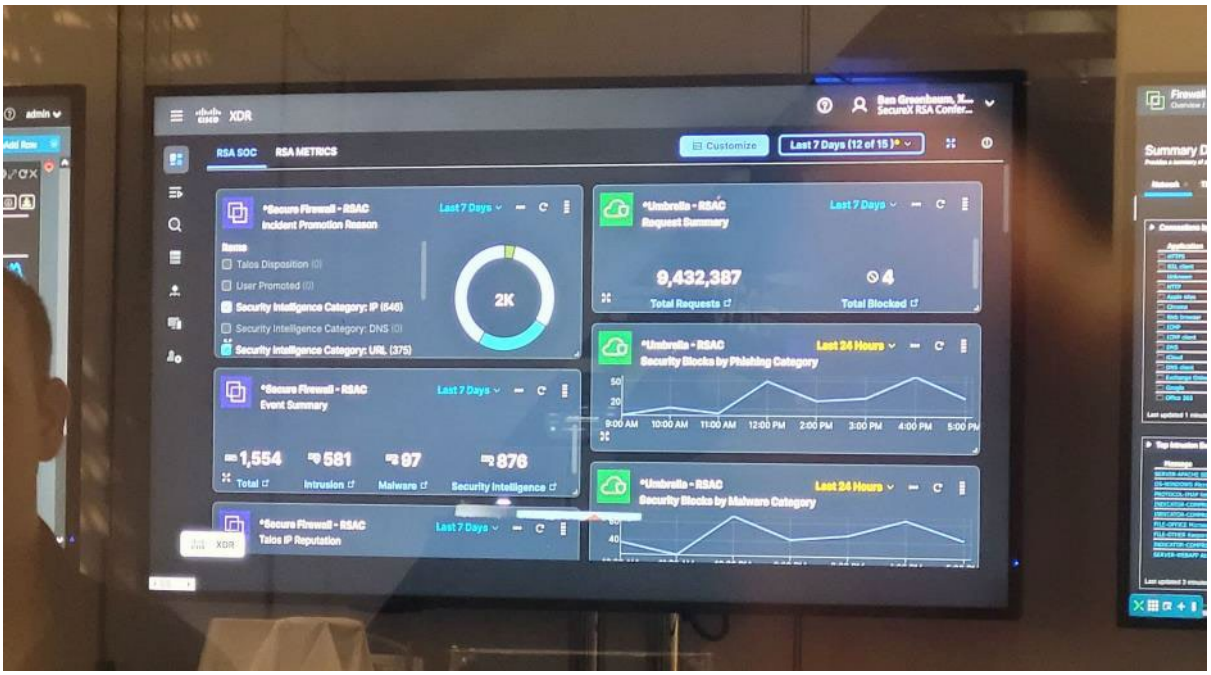


圖 41、RSA conference SOC 使用 cisco XDR 畫面

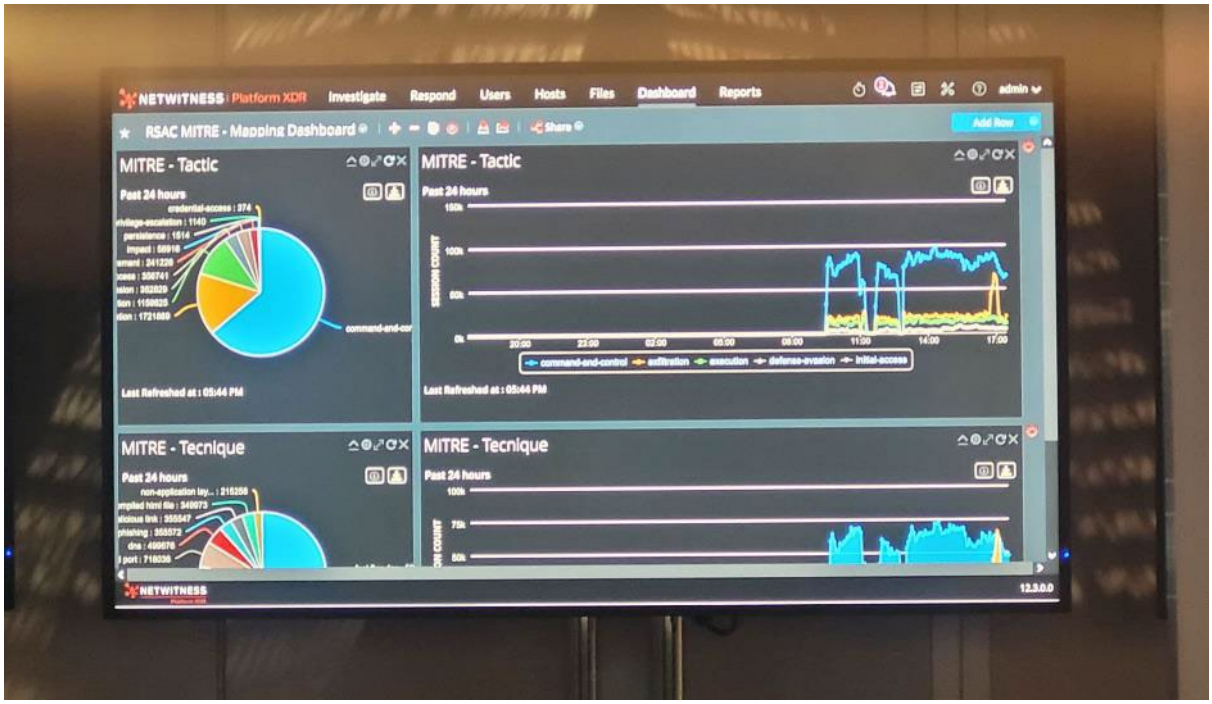


圖 42、RSA conference SOC 使用 NETWITNESS 畫面

(二) Fortanix

Fortanix 是一家數據安全公司，專注於保護在雲端、邊緣運算和混合環境中的數據安全。該公司成立於 2016 年，總部位於美國加州。2022 年 9 月宣布完成 9,000 萬美元 C 輪募資，由高盛資產管理公司(Goldman Sachs)旗下的成長股權業務領投。新投資者 GianLeap Capital 及現有投資者 Foundation Capital、Intel Capital、Neotribe Ventures 也參與了該輪募資。

儘管過去十年網路和基礎設施安全取得長足進步，但數據安全仍未得到解決。隨著企業加速數位轉型並將大規模數據遷移至雲端，企業面臨的挑戰變得更加複雜。而雲端數據按照數據所處狀態被分為三大類，分別是(1)數據傳輸狀態(Data in Transit)，即網路傳輸過程中的數據、(2)數據儲存狀態(Data at Rest)，即數據在磁碟和存儲過程中、(3)數據使用狀態(Data in use)，即處於內存、運算中的數據。即使對靜態數據和通過網路傳輸的數據進行加密，數據仍然容易在運行時受到未經授權的訪問和篡改。因此，保護正在使用的數據對於在數據生命週期中提供完整的安全性至關重要。

Fortanix 認為，傳統的數據安全模型無法跟上雲端優先的世界。機密運算(Confidential Computing)解決方案是一種保護數據隱私和安全的技術，該技術可確保數據在使用期間始終處於加密狀態，即使在雲端、邊緣運算和混合環境中

也是如此，這種方法透過在運算過程中使用可信執行環境(Trusted Execution Environment, TEE)來實現。可信執行環境(TEE)是一種硬體和軟體組合，可以提供安全和隔離的執行環境，以保護應用程式和數據免受惡意攻擊和威脅。在 TEE 中運行的應用程式和數據可以受到硬體級的保護，以防止未經授權的訪問和數據洩漏。

以下是 Fortanix 機密運算解決方案的主要特點：

1. 安全執行環境：Fortanix 利用硬體安全模組(HSM)和 TEE 來建立安全的執行環境，確保應用程式和數據在運行時受到保護。
2. 數據加密：數據在使用期間始終處於加密狀態，只有經過授權的應用程式可以解密和處理數據，從而保護數據的隱私性。
3. 隱私保護：機密運算解決方案透過在運算過程中保護數據隱私，確保數據在運算過程中不會被未經授權的訪問者或惡意攻擊者所窺視。
4. 應用程式保護：利用機密運算技術，Fortanix 可以保護應用程式的代碼和運行時環境，防止未經授權的訪問和攻擊。

機密運算解決方案可在各種場景中應用，包括敏感數據處理、機器學習模型的訓練和推理、保護智能合約等。它可以幫助組織在雲端和邊緣運算環境中實現數據安全和隱私保護，並確保機密數據得到有效的保護。其中，ARM 和 Intel 皆在機密運算領域進行相應的發展，包括 ARM TrustZone 技術及 IntelSGX (Software Guard Extensions)硬體擴展技術。2021 年 9 月 Intel 與 Fortanix 合作，在機密運算領域進行技術合作與產品整合，提供更強大的機密運算解決方案。

(三) Orca Security

Orca Security 是一家總部位於以色列的雲端安全公司，成立於 2019 年。Orca Security 提供的雲端安全解決方案，能讓受保護的系統在毋需進行任何安裝下，快速和簡便地進行資安部署。

該公司對於雲端安全有革命性願景，希冀能大幅簡化並自動化雲端安全防護與合規性，使開發團隊能快速構建和部署，並使安全團隊能配合雲端發展速度擴展安全性。Orca Security 的核心產品是其雲端安全平台(Orca Security Platform)，可辨識、確認優先等級並引導修復跨 AWS、Azure、GCP、阿里雲、

Oracle Cloud 等雲端平台、容器和 Kubernetes 的資產安全風險和合規問題。

2019 年，隨著 Orca Security 實現打造無代理(Agentless)、雲端原生安全平台一願景後，Orca 不斷獲得業界認證，包括成為 2022 年度 AWS 全球資安合作夥伴，以及 Databricks、Lemonade、Gannett 和 Robinhood 等全球創新者的信賴。

以下是 Orca Security 解決方案的特點和功能：

1. 雲端安全狀態管理(CSPM)

傳統的 CSPM 解決方案可協助組織保持合規性並解決雲端風險，例如錯誤配置和過於寬鬆的身份驗證。但是，這僅是涵蓋攻擊面的一部分風險，且將雲端工作負載、事件監控和機敏資料發現排除在外。

Orca 將雲端工作負載、配置、身份和權限安全、容器安全、機敏資料發現、檢測和回應等整合到單一平台中，並橫跨整個生命開發周期(SDLC)。這讓 Orca Security Platform 能瞭解風險脈絡，並識別看似無關的問題何時會產生危險的攻擊路徑。運用這些洞察，Orca 能確認風險的優先順序，確保資安團隊可以優先處理最關鍵的告警。

2. 雲端工作負載保護平台(CWPP)

與其他 CWPP 不同，Orca 不需安裝代理程式，可在幾分鐘內覆蓋對雲端工作負載及雲端資產風險的可見性，並能橫跨雲端 VM、容器、無伺服器應用程式、Kubernetes 及雲端基礎設施。此外，Orca 可以掃描雲端配置和用戶身份，提供完整的上下文分析和告警優先排序。

3. 雲端基礎設施授權管理(CIEM)

Orca 將身份風險與其他風險數據(漏洞、錯誤配置、惡意軟體、機敏資料的儲存位置和橫向移動風險)結合起來，以幫助組織優先考慮環境中的風險。若發現過於寬鬆的身份認證時會發出告警，並能根據潛在的業務影響進行風險優先排序。

圖 43、Orca Security 之雲端原生應用程式防護平台(CNAPP)得以自動防護雲端資產

(四) CrowdStrike

CrowdStrike 成立於 2011 年，公司總部位於美國德州奧斯丁。同時於英國、愛爾蘭、印度、日本，及新加坡等地設有辦公室。該公司為透過雲端提供服務的次世代端點保護領導者。期下擁有 Falcon 品牌系列產品，應用於雲端管理、端點安全防護、IT 部門防護及身份與登入存取管理等作業流程。該公司同時提供網路攻擊偵測、輔助防禦與應變，和資安意識員工訓練等服務。

該公司競爭對象為其他主要資安廠商，如 McAfee、火眼公司、Palo Alto Networks，以及旗下供有資安防護服務的 Broadcom 和微軟等公司。截至 2021 年統計，共有九千八百個客戶訂閱戶，其中包含六十間財星前百大企業。另外，截至 2022 年 4 月，CrowdStrike 總市值為 513.4 億美元，該公司於 2019 年 6 月那斯達克上市。其中，訂閱費用佔總營收的 92%，專業服務營收則佔 7%。美國本土佔總營收 72%，其次為佔 14%的歐洲、中東與非洲地區市場，亞太地區佔 9%。

以下是 CrowdStrike 公司的一些產品和優勢：

1. Falcon 平臺：CrowdStrike 的核心產品是 Falcon 平台，這是一個基於雲的端點保護平臺，提供了端到端的威脅檢測、回應和預防功能。該平臺所使用的入侵防護技術，採用非特徵比對的人工智慧、機器學習、攻擊

指標(Indicator of Attack, IOA)所組成，為企業提供跨系統單一平台的管理機制，阻擋已知與未知的入侵威脅，防禦各種新興網路攻擊。運用的創新技術核心為 CrowdStrike Threat Graph™，每天針對部署在 170 多個國家的感應器，針對 900 多億個事件進行關聯分析，即時預防和檢測威脅，持續精進次世代端點防護系統的能力，為企業組織提供獨特的雲端防護。

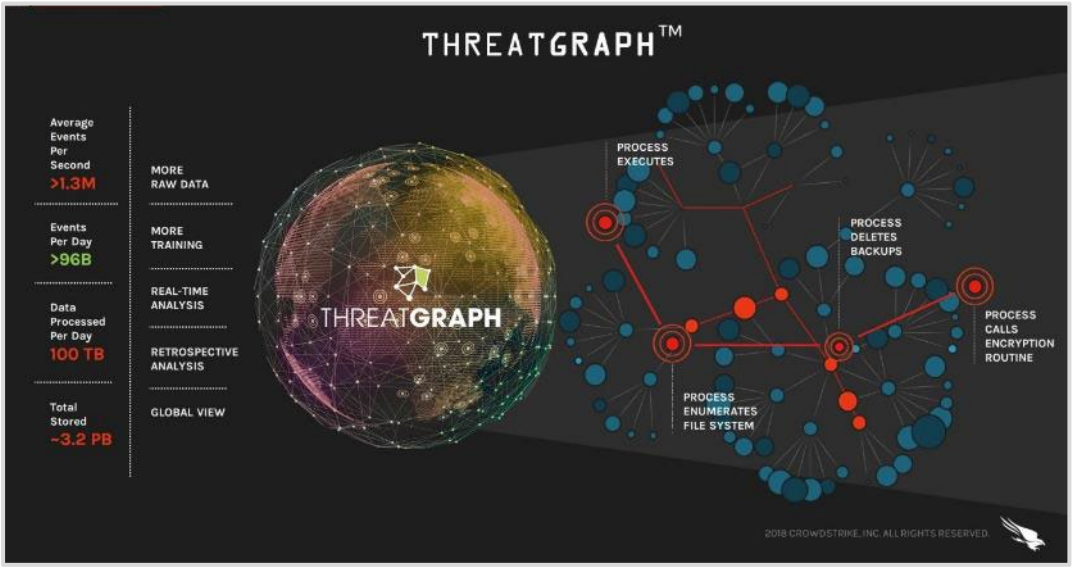


圖 44、CrowdStrike 端點防護之創新核心技術 Threat Graph™

2. 威脅情報：CrowdStrike 提供即時的全球威脅情報，說明企業瞭解當前的網路威脅趨勢和攻擊技術。利用情資驅動，精準地偵測與獵捕威脅，並使用 MITRE ATT&CK®為攻擊手法描述，提供通用且完整的攻擊資訊，並自動攔阻攻擊及非法程式行為。這些情報可以幫助企業預測和預防新型的威脅，加強網路防禦和應對能力。

3. 回應服務：CrowdStrike 提供專業的威脅回應服務，說明企業迅速應對和處置安全事件。他們的安全專家團隊可以快速調查和回應潛在的安全威脅，並提供修復建議和持續的監控支援。

4. 雲原生架構：CrowdStrike 的解決方案採用雲原生架構，充分利用雲計算和彈性資源的優勢。這使得他們能夠實現高度可擴展性、靈活性和性能，適應不斷變化的威脅環境和企業需求。

(五) Akamai Technologies

Akamai(阿卡邁)於 1998 年成立，該公司總部位於美國麻薩諸塞州劍橋，同時加拿大、英國、德國、新加坡、中國、日本、韓國、臺灣等地設有辦公室。作為

全球最大的分散式運算(Distributed computing)平台，Akamai 宣稱，他們在全球 134 個國家皆有伺服器部署其服務，每日處理的網站流量更達每秒 100TB 以上。2022 年營收達 36 億美元，同比增長 8%。該公司競爭對手為其他網路服務商，如 AWS、CloudFlare、Google Cloud，以及 Fortinet 等公司。

旗下業務分成兩大部門運作，分別為：邊緣運算科技部及資訊安全科技部。邊緣運算科技部佔總營收 61%，提供客戶企業數位化轉型與邊緣運算技術等解決方案。該部門協助客戶於網路平台，上傳、傳播自家媒體，增進終端客戶的使用體驗，同時針對服務供應商領域客戶，提供網路流量，及服務訂閱者管理方案，協助處理數位資料。另針對開發商領域客戶，提供邊緣運算技術，協助他們進行程式碼開發與發佈作業；另外，資訊安全科技部則佔總營收 38%，提供客戶維護網際網路基礎建設、網站、應用程式與使用者資安的解決方案與產品。此部門採用自動化流程等技術，制定滿足客戶需求的客製化風險防範、管理專案，供應客戶身分辨識與存取管理、DDoS(分散式阻斷服務攻擊)緩解、零信任模式架設及資訊盜用防範等服務項目。

該公司的主要客戶有資安防護與網路服務需求的各領域客戶，業務範圍涵蓋科技業、零售業、運輸業、媒體與娛樂業，及政府部門等領域族群。其中，Adobe、可口可樂、FedEx、IKEA、Sony，及 NBC 環球等大牌公司，皆為該公司客戶。

以下是 Akamai Technologies 的主要產品和服務：

1. 內容遞送網路(CDN)：Akamai 的 CDN 服務(Content Delivery Network)是其核心產品之一。它通過全球分散式的伺服器網路，將客戶的內容和應用程式緩存到靠近使用者的邊緣節點上，從而實現快速的內容交付和優化使用者體驗。CDN 服務可以減少網頁載入時間、提供流暢的視訊和音訊廣播，並承受大量訪問流量的壓力。
2. 資安應用解決方案：Akamai 提供全面的網路安全解決方案，包括分散式拒絕服務攻擊(DDoS)防禦、Web 應用程式防火牆(WAF)、Bot 管理和身份認證等。這些安全服務說明企業保護網路和應用程式免受惡意攻擊和資料洩露。
3. 雲端性能優化：Akamai 的雲端性能優化解決方案說明客戶優化其雲基礎架構和雲應用程式的性能。它通過加速資料傳輸、優化網路連接和提供即時性能監控，提高雲端服務的可靠性、回應速度和使用者體驗。

4. 媒體交付解決方案：Akamai 的媒體交付解決方案用於提供高品質的線上視頻和音訊流媒體服務。它支援流暢的直播和點播體驗，並提供高度可擴展的媒體傳輸、內容加密和數位版權管理功能。

(六) 荷蘭館

荷蘭為連續第五年參加 RSA 大會。荷蘭被公認為適合資安產業發展的重要國家，在「海牙資安三角洲」(The Hague Security Delta, HSD)的推動下，荷蘭擁有蓬勃發展的資安新創和國際企業。而在今年 3 月，北約創新基金(NATO Innovation Fund, NIF)則宣布將總部設在荷蘭，將聚焦在人工智慧、量子科技、生物科技、創新材料、太空和能源等領域之軍民兩用新創早期投資。

荷蘭創新中心(Innovation Quarter)在 Topsector ICT 的支持下，荷蘭外交部和荷蘭企業署(Netherlands Enterprise Agency)共同於 RSA 大會成立荷蘭館，八家荷蘭資安業者展示創新的資安解決方案，包括威脅情資、安全營運和事件響應、資料安全、資安風險管理和零信任架構等。

以下為參加 RSAC 2023 八家荷蘭資安廠商及解決方案。

1. Attic Security 提供加強和監控 SaaS (如 Microsoft 365)之資安解決方案，協助中小企業建立網路彈性。
2. Awareways 是一家資安培育和提高資安意識解決方案公司。他們專注於提高員工對安全風險的認識，提供相應的培訓和教育資源。Awareways 的目標是為組織建立強大的資安文化，使員工能夠識別和應對各種資安威脅。
3. BreachLock 專注於提供全面的網路和應用安全測試服務。他們的目標是為組織發現和修復潛在的安全漏洞和弱點，以加強網路和應用程式的安全性。
4. DTACT 提供簡單和自動化數據分析解決方案，能為雲端數據管理和儲存上節省大量時間與成本。
5. ON2IT 專注於提供先進的威脅檢測、防禦和回應解決方案。他們的目標是為組織建立強大的安全防護能力，以應對不斷演變的網路威脅和攻擊。
6. PRODAFT 成立於 2012 年，提供網路威脅情資服務，主要以 U.S.T.A.網路

威脅情資平台為主，將最新的威脅情資和安全性漏洞資訊傳遞給組織，協助企業瞭解和預防潛在的資安威脅。

7. Reporter 提供一站式滲透測試平台服務，該平台具有改進協作、工作流程、報告和提高效率之功能。

8. Ubiqu 的遠程安全元件是第一個符合歐盟電子簽章法(eIDAS)之解決方案，可以安裝到任何現有的應用程序和設備中。

圖 45、RSA 2023 荷蘭館由荷蘭王子 Prince Constantijn Van Oranje-Nassau、RSAC 副主席 Linda Gray Martin 及荷蘭外交部副部長 Peter Potman 主持開幕

圖 46、NL 荷蘭館展示荷蘭網路安全創新

(七)　西班牙館

西班牙的資安產業正逐漸發展壯大，成為國家數位化轉型的重要支柱之一。西班牙擁有大約 1,800 家資安公司，包括資安服務提供者、威脅情資公司、資料安全解決方案供應商等。這些企業在資安技術和解決方案的研發、創新和提供方面發揮著重要作用。此外，西班牙也孕育了一些資安新創和創新生態系，為資安領域的新興公司提供支援和發展機會，西班牙目前約有 15 萬名資安工作者。

西班牙有一些重要的資安研究單位和大專院校，為培養資安專業人才和推動技術創新做出重要貢獻，西班牙共有 58 個資安研究團隊，25 個國家工業網路實驗室。其中，西班牙國家網路安全研究所(Incibe)以歐洲網路安全技能框架(European Cybersecurity Skills Framework, ECSF)，作為西班牙網路安全人才培育的基本框架，亦加深與歐盟其他國家的合作，共同抵禦網路攻擊。

另外，西班牙政府高度重視資安，並採取了一系列政策和倡議來支持和促進該領域的發展，其中包括資助創新項目、鼓勵公私合作、加強法規和監管框架等方面的舉措。有以下三項計畫促進西班牙資安產業的發展：

1. Incibe Emprende 計畫：該計畫約有 3 千萬歐元預算，開發、孵化和加速發展資安新創。
2. Talento Hacker 計畫：旨在招聘、培訓和僱用資安領域的專業人員，該項目將投資約 4,000 萬歐元，目標培養資安人才以滿足產業對資安人才的需求。
3. Ciberinnova 計畫：為提升國家資安技術之研發能力及創新解決方案之競爭力，該計畫預算投入約 2.35 億歐元，以開發高附加價值的解決方案和資安服務。

圖、西班牙政府至 2026 年之資安投資與支出

以下為參加 RSAC 2023 西班牙國家館之資安廠商及解決方案：

1. A2SECURE：A2SECURE 為組織提供各種資安營運及合規服務，提高企業資安成熟度與業務彈性。主要解決方案包括：資安託管服務及資安營運託管服務等。
2. A3SEC：提供廣泛的資安解決方案和服務，是一家擁有專利和創新資安解決方案的跨國企業，包括網路攻擊面管理(動態應用程式分析、SecDevOps、安全態勢管理、網路演習等)及智慧擴展檢測和響應(藍隊、EDR、Threat Hunting 等)。
3. AIUKEN CYBERSECURITY：為一家國際 IT 安全公司，提供託管安全服務(MDRS)，提供整合式資安解決方案和雲端服務。
4. AREXDATA：成立於 2020 年 11 月，主要開發數據保護 Arexdata 平台，協

助企業進行資料安全防護。

5. BEYGOO：為數位風險防護平台，專注於早期資安事件檢測和預防詐欺，使用人工智慧和自動化流程監控組織的數位資產。

6. GMV：成立於 1984 年，為一家全球性技術和業務諮詢公司，提供資安風險評估、漏洞管理、安全架構設計和滲透測試服務等。

7. INETUM：為全球性 IT 集團，在 27 個國家和地區擁有約 2 萬 7 千名員工。提供資安營運中心(事件響應和 IAM、端點保護和數據保護等)和數位身分解決方案(生物識別、身分驗證、預防詐欺)等。

8. INSSIDE CYBERSECURITY：提供紅藍隊資安服務、治理、風險與合規等。

9. INTERNET SECURITY AUDITORS：成立於 2001 年，提供技術審查、資安標準和法規實施及合規性等專業服務。

10. IRONCHIP：提供 Ironchip Identity Platform 整合身分無密碼平台及 Ironchip 詐欺檢測等服務。

11. LEX PROGRAM：為開發隱私和合規技術之新創企業。

12. MALTIVERSE：為企業組織提供 SIEM、SOAR、EDR、防火牆等可操作威脅情資，協助企業組織檢測、分析和響應網路威脅。

13. QUSIDE：以量子技術實現更安全的連接和高速運算，是創新型的量子安全通訊公司。該公司亦是歐盟量子旗艦聯盟成員，提供量子安全通訊、量子密鑰分發(QKD)系統及量子隨機數生成器等。

14. REDBORDER：專注於 IT、OT 資安，利用即時採集技術和人工智慧來保護和預防網路攻擊。

15. SOFISTIC CYBERSECURITY：成立於 2009 年，提供威脅情資和 SOC 資安服務等解決方案，目標協助關鍵基礎設施保護關鍵資訊資產，產品與服務包括：MSSP Exabeam、MSSP Darktrace、MSSP CrowdStrike、區塊鏈及智能合約審計及移動威脅防護等。

16. SSHTEAM CYBERSECURITY：以技術為基礎之資安新創，提供軟體開發服務、資安培訓、諮詢、合規性和滲透測試等專業服務。

17. BLOOCK：專注於跨行業應用之區塊鏈解決方案公司，解決來源和身分問題，如數據安全可追溯性、零售產品來源、數位簽名、去中心化數位身分、文件防偽等。

18. S2 GRUPO：提供威脅檢測和風險管理服務、資安事件管理、資安意識培訓等，確保企業在安全和系統營運方面的合規性。

圖 47、RSAC 2023 西班牙國家館參展之資安廠商

四、 美商資安交流活動

本次訪團除參加 RSAC，並與各資安新創公司進行交流外，亦參與 AIT 安排之資安廠商交流活動，以強化與美方連結，瞭解資安防護趨勢及解決方案並建立互動，尋求潛在合作機會。

(一) Mandiant at RSAC for APJ Delegation Program & Google Campus 參訪、臺灣網路彈性探討(Cyber Resilience In Taiwan)

Mandiant 是一家全球領先的網路安全公司，成立於 2004 年，總部位於美國加利福尼亞州。Mandiant 有著一群專業的資安團隊，擁有豐富的網路安全經驗和技術知識。公司的技術重點在於 APT 攻擊的檢測和處理，以及進階威脅情資的收集和分析。Mandiant 的團隊使用自己研發的威脅情資平台，可以實時收集和分析全球的威脅情資，提供客戶即時的威脅情資和分析報告。此外，Mandiant 團隊還擅長利用大數據和機器學習技術，分析和識別網路攻擊行為，幫助客戶及時發現 APT 攻擊。Google 於 2022 年 9 月完成收購 Mandiant，期能透過整併 Mandiant 的深度威脅情報資源至自家的 Google Cloud，尤其是近期俄烏戰爭爆發，資訊戰與網路安全更顯重要。

本次由 Mandiant 安排了兩場講座，包含 RSAC for APJ Delegation Program 講座暨 Google Campus 園區導覽及臺灣網路彈性探討，分述如後。

1. Mandiant at RSAC for APJ Delegation Program & Google Campus 參訪

講座部分說明了目前 Google Cloud 的發展，及 Google Cloud 現在所提供的服務，如何整合 AI 判斷資安事件警報、情資來源、相關異常事件分析等提高準確度與效率，並且具體呈現量化的數據佐證其服務能降低的成本與帶來的效益，同時比起其他競業如 AWS、Azure 等，目前的定價優勢與使用彈性，以及所採用的軟硬體等介紹。主要分為四大主題，分述如下。

第一個主題是由谷歌雲 Vertex 和 Cloud AI 解決方案的產品管理總監 Nenshad Bardoliwalla 以 AI outcomes Delivered by Google Colud 說明目前在其雲端技術使用了 TENSORFLOW 等的創新技術以及經由自行設計的 TPU 晶片和 CPU 及 GPU 的整合提供更強大的人 AI 及 ML 能力。

第二個主題是由谷歌雲安全副總裁兼總經理 Sunil Potti 就目前 Google

Security: Strategy & Priorities 為題說明 GOOGLE 在安全合規上的策略及重點，並且如何建立公私有並行的混合雲環境，符合全球各政府不同的法規及要求以及在網路威脅下如何確保維運一個高可信賴的合規平台。Sunil Potti 提及兩大資安的推動力，數位主權(Digital Sovereignty) 與 The Nation State "Pivot"，數位主權是指國家或政府對其網路、數位資源及數位領域的自主權利與掌控權，確保其網路安全、資訊安全及資料安全，由於數位資源的重要醒與價值日益提升，數位主權已成為許多國家和政府的重要戰略和目標。而 The Nation State "Pivot" 則說明網路威脅態勢從過往的數位犯罪到國家層級的網路戰，其攻擊規模較以往更大、更複雜且持續，特別是針對政府單位與關鍵基礎設施。然而，面對這樣的威脅，世界上較具規模的超過 25 萬家企業，如何能自我保護，亦或是他們可具備像 Google 一樣的資安防護等級，在此方面，Google Cloud 打造一個 AI-Powered 資安平台，Cloud Security、CISO/GCAT、Mandiant、DeepMind (AI)、Core Privacy, Safety & Security 等各面向的資源以應對嚴峻的資安威脅。

第三個主題則是以 Frontline Threat Intelligence Meets Cloud Innovation 並且由 GOOGLE COULD 總裁 Thomas Kurian、Mandiant 總裁 Kevin Mandia 等人進行多方對談，討論了許多在雲端創新上所面對的各種威脅。

第四個主題由 PHIL Venables 谷歌雲副總裁兼資安長以 Security Outcomes Delivered by Cloud 的主題說明谷歌雲的 Cybersecurity Action Team 如何為政府機關、重要基礎架構、企業和小型公司提供安全性與數位轉型策略的方法論及程序，包括了在 Mandiant 加入 Google 補充 Google Cloud 既有的安全優勢，涵蓋 Beyond Corp Enterprise 、Virus Total、Chronicle、安全指揮中心及網路安全行動團隊等，讓 Google Cloud 得以強化端對端的安全操作，並有更多的能力來支援雲端及就地部署環境並且具備從安全顧問服務、威脅偵測與情資、自動化與回應工具、測試及驗證，以及受控防禦等強大能力。

在完成 Seminar 議程後，接著進行 Google Bayview 園區導覽參觀，其導覽人員提及，Google 非常重視永續發展與環保，其園區大量採用太陽能板，且少有中央空調冷氣。印象較深刻的是，其辦公環境中包含許多裝置藝術，例如植物、海洋、飛鳥、腳踏車等，裝置藝術的組成亦不乏廢物重新再利用，充分感受到 Google 重視環保與永續的理念。

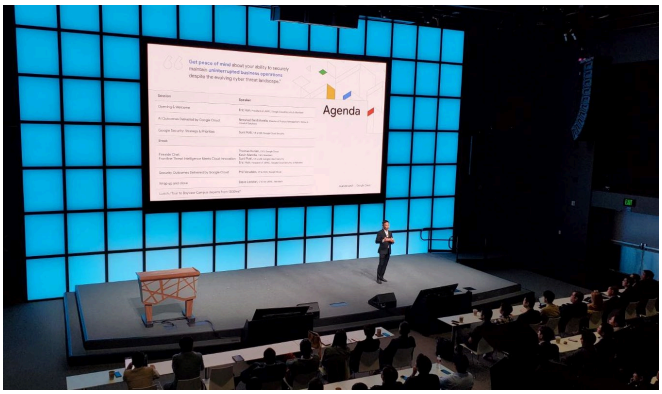
2. 臺灣網路彈性探討

本次演講提到了下列幾個重點：

(1) 網路韌性：講者強調，當預防、檢測、調查和應變相結合時，可以實現網路韌性。藉由威脅情資以瞭解網路威脅和攻擊者資訊，對於做出應變判斷並追蹤入侵者至關重要。

(2) 資安事件應變處置演練：講者強調資安事件應變計畫的演練與危機溝通的重要性。這些演練有助於組織內部的餐與，建立團隊合作，以利在發生資安事件時，能有效地及時做出適當的處置。

人工智慧在網路安全中的應用：講者提到人工智慧正在被應用於網路安全技術，特別是威脅情資領域。其可幫助彙總大量資訊，制訂惡意軟體或攻擊的偵防規則，並增強整體資安防護能力。



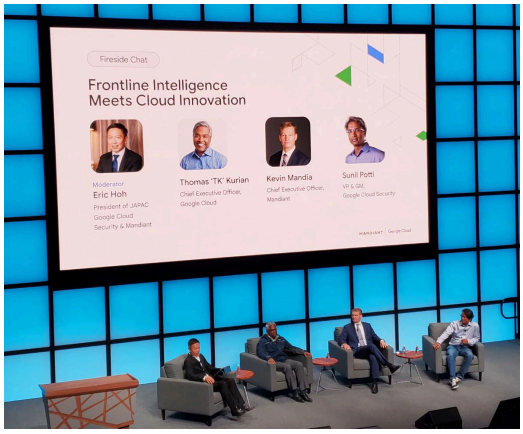


圖 48、RSAC for APJ Delegation Program

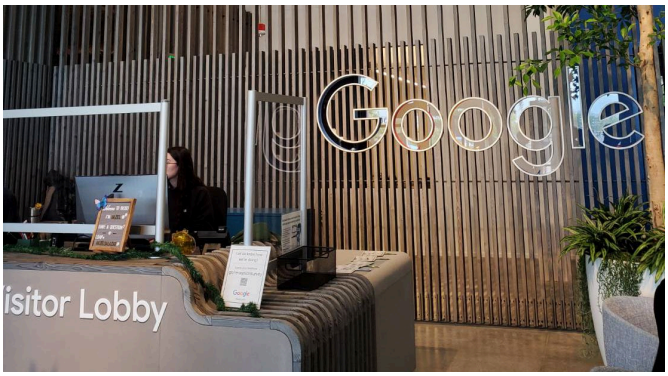


圖 49、Google Campus 參訪

圖 50、臺灣網路彈性探討講座

(二) Striderintel

Strider 以強化臺灣國家經濟安全為主題來說明該公司的產品及服務特色，其產品方向聚焦於保護自由世界創意和創新，所以 Strider Intelligence 平台透過專利數據收集和處理引擎，收集從世界各地數以萬計的獨特數據點來源，通過專有

方法分析這些數據，以識別、評估和跟踪在特定科技領域中的對手行動，為企業和政府客戶提供可擴展的能力。

Striderintel 可歸類為新創公司，成立於 2019 年 5 月，主要辦公室目前分別在猶他州鹽湖城、維吉尼亞州麥克萊恩和英國倫敦，目前已經募集了 5700 萬美元資金，超過 125 名員工，6 名以上的董事會成員具有情資和政府經驗，公司沒有美國以外的所有權，具備的 10 種以上的語音能力，客戶群涵蓋產業的財富 500 強企業包括：石油和天然氣、半導體、製造業、科技產業、航空和國防工業、生物技術和製藥業等以及美國和友好政府和國際產業與研究機構。

首席策略長於席間指出，在 2019 年 11 月，中國國務院臺灣事務辦公室發言人朱鳳蓮表示，至少有 72 名臺灣的專家學者加入千人計畫。所以根據 Strider 初步數據評估從 2004 年以來至少有 88 名居住在臺灣受教育或因職業關係被選入中國國家或地方人才計畫，有 706 家中國大陸組織擁有臺灣股東，這些組織至少在一份中國大陸政府、軍事或國防工業採購記錄中出現。緣此，Strider 推薦其產品 RISK 和 Shield，此兩項產品便是針對此類風險所提供的解決方案，能夠識別風險和威脅並保護他們的創新技術及競爭力。目前 Strider 的產品尚未有臺灣的使用者。

圖 51、關次長代表訪團致贈禮物

(三) Fidelis Cybersecurity

Fidelis Cybersecurity 認為網路強韌性為環境在受攻擊時維持業務關鍵操作的能力，企業與組織應能快速檢測、評估和響應持續的攻擊，並能夠及時恢復正常業務運作。

而講者也認為，目前的網路攻擊與資安威脅的程度與數量尚未到達頂峰，因此

許多企業雖未建立更進一步的主動防禦或身分驗證解決方案，受到的攻擊可能還不明顯或僅是尚未被發現，但直至 2031 年，Fidelis Cybersecurity 預估每年關於勒索攻擊所帶來的損失、防禦成本、攻擊頻率都將到達一個新高度，因此，提前準備應對措施及導入解決方案不僅可以解決現在的問題，亦可以為未來的攻擊做準備。

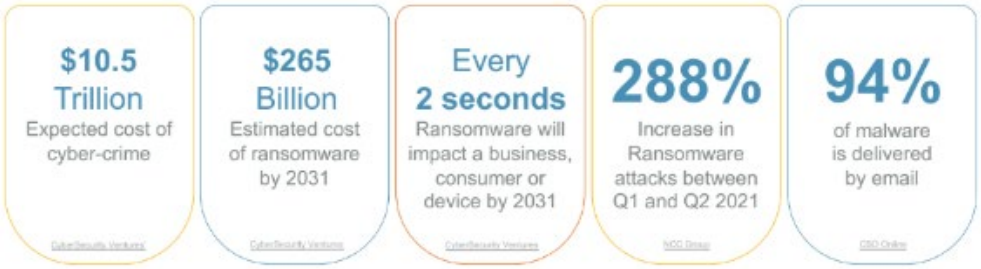


圖 52、預測 2031 年攻擊趨勢與相對成本

而 Fidelis Cybersecurity 提供網路強韌系統自動識別漏洞和設置錯誤的服務，提供攻擊者不斷變化互動的環境，快速檢測威脅，在系統內建立冗餘和彈性，以承受和應對網路攻擊和事件。其認為網路安全策略不僅僅在於合規，還應該採取積極的防禦解決方案如設置誘餌、主動偵測與識別攻擊特徵與來源，讓防禦者能夠積極參與威脅獵捕和事件調查。

除此之外，Fidelis Cybersecurity 也提供了一些佐證數據來指出當前的企業情況，包含人為造成的數據洩漏占大多數，企業的資訊安全與網路人才不足，面對新型態與複雜的網路攻擊，傳統的安全防禦措施已經不再適用等，指出需考量除被動防禦外，Fidelis Cybersecurity 也提供了主動偵測的解決方案，提供企業與組織加強網路強韌性。

圖 53、Fidelis 代表分享資安解決方案

(四) SailPoint

SailPoint 從 2005 年成立總部位於美國德克薩斯州 Austin，是一家數位身份管理公司，為企業提供身分識別管理解決方案的供應商。其開放式身份平臺，讓用戶能夠在複雜的混合 IT 環境中訪問應用程式和資料。至今已經幫助全球超過 2500 家公司建立了先進的身分管理方法，為他們提供一個有效的解決方案並滿足他們不同的身分管理需求。

本次 SailPoint 以「身份安全不妥協(Identity Security Uncompromised)」為主題進行交流，就 SailPoint 的說明，根據美國 Identity Defined Security Alliance 所做的年度調查中顯示，參與調查的公司有 84%在過去一年中曾經歷過與身分相關數據洩漏事件，其實我們大家也可以回想一下在去年媒體也曾報導許多重大個人資訊外洩事件。在報告中這些發生數據資料外洩的公司中，有 96%的公司承認如果他們實施更好的身分管理及更好的控制事實上是可以避免的。這也正顯示許多公司對於身分安全規劃仍未有完整的規劃，而且依賴於舊的技術和流程，而這些都無法因應現今複雜的需求。

企業身分安全認證是 SailPoint 的核心，運用先進的技術人工智慧和機器學習讓機構保持高度的資訊安全滿足合規要求，維持高效能運作又能易用取得使用者存取權限。

SailPoint 在其身分安全解決方案有三個核心：

1. 具有智慧性，可以幫助全方位觀察、瞭解並監督所有身分及其存取的需求。
2. 主動協助，以加快重要身分決策的速度，從而促使機關的相關人員可以將精力專注於更有意義的任務上。
3. 與基礎 IT 架構完美連接，便於將身分資訊坎入整個數位系統中，以發揮巨大的作用。

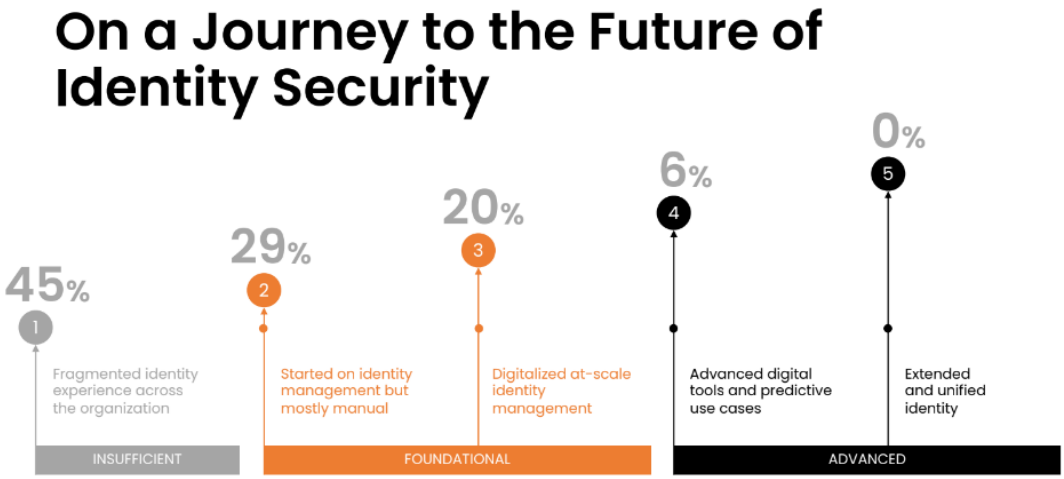


圖 54、身分安全管理機制層級

圖 55、Sail Point 講座

圖 56、鄭副署長代表致詞

(五) Varonis

這場演講的主題是關於資料外洩和資料保護的重要性。講者提到近年來發生的各種資料外洩事件，並探討了這些事件的共同點和原因。他指出資料是攻擊者的目標，因為資料是知識產權、創造力和價值的核心。

當發生資料外洩事件時，組織往往對受到影響的範圍一無所知。他們可能無法確定哪些資料被竊取，也不清楚損害的程度。這可能會對股東、組織的聲譽產生重大影響，並可能引起監管機構的關切與調查。講者提到這個問題不限於特定行業，而是普遍存在，無論企業的規模大小，政府機構還是製造業、高科技等領域，都受到同樣的影響，因為資料驅動著他們的業務。

演講中提出了一系列資料保護的議題，包括：組織不知道自己有哪些資料、不知道哪些人擁有存取權限、不知道資料是否被正確使用，以及不知道什麼是適當的資料使用方式。這些問題都使得保護資料變得非常困難。對此，Varonis 提出了相關解決方案：Varonis 資料安全平台 (Varonis Data Security Platform)，以自動化方式減低資料暴露。該解決方案整合現有的許多工具與平台，包含 SaaS、雲端、資料庫、身分驗證方案等，能夠快速分析存有的資安風險，偵測與監看如資源存取請求、身分驗證請求、檔案存取請求、公開共享連結等行為，並且支援合規流程追蹤、自動化攻擊應對、威脅模型建立等功能，包含但不限於地端、雲端、資料庫、資料流等各種形式目標的防禦機制與解決方案。

Varonis 也透過修正設定風險、帳號風險、第三方 App 風險，讓駭客或者內部威脅就算能成功進入內部網路，都不容易接觸或者偷走重要資料，進一步強化保安姿態，具體做法包含監測設定、帳號、檔案存取的權限並視覺化，提供直接修改設定與自動修正的功能，也可以與現有的服務如 Microsoft 365、Google Drive、Salesforce 整合，快速修補未正確設定的存取權限或內容。

圖 57、Varonis 監控平台

(六) Palo Alto Networks

Palo Alto Networks 是全球網路安全領域的領導者，提供一系列創新的產品和服務，應對不斷演變的網路安全威脅，為組織提供堅韌、整合和有效的資安解決方案，保護其重要資產和資料，免受各種威脅和攻擊。著重於預防網路威脅，Palo Alto Networks 提供先進的資安解決方案，幫助組織保護其網路、端點和雲環境。

講者提到現代化的資安維運方法、自動化及強化韌性的重要性，需要利用自動化和聯防協作以應對攻擊。其提到資訊的價值以及它如何被網路犯罪分子利用。當中提及網路攻擊對關鍵基礎設施和行業可能產生的潛在影響，並說明對網路安全採取不同方法的必要性。接著，進一步討論在聯邦生態系統中實施零信任的情況，並重申零信任不是產品，而是涉及人員、流程和技術，零信任的核心原則之一是「假設網路不安全」(Assume Breach)，這意味著不論是內部還是外部的網路都應被視為不可信任的。

Palo Alto Network 並介紹了 Cortex XDR、XSOAR、Xpanse 等新推出資安協調自動化以及反應機制平台，提高企業與組織的威脅反應與分析能力。其中功能包含網路釣魚回應、惡意軟體調查與回應、零時差威脅回應、遠端使用者存取佈建、威脅情報管理、雲端安全事件回應、弱點管理、攻擊範圍管理、MITRE ATT&CK 對應、網路作業自動化等功能。

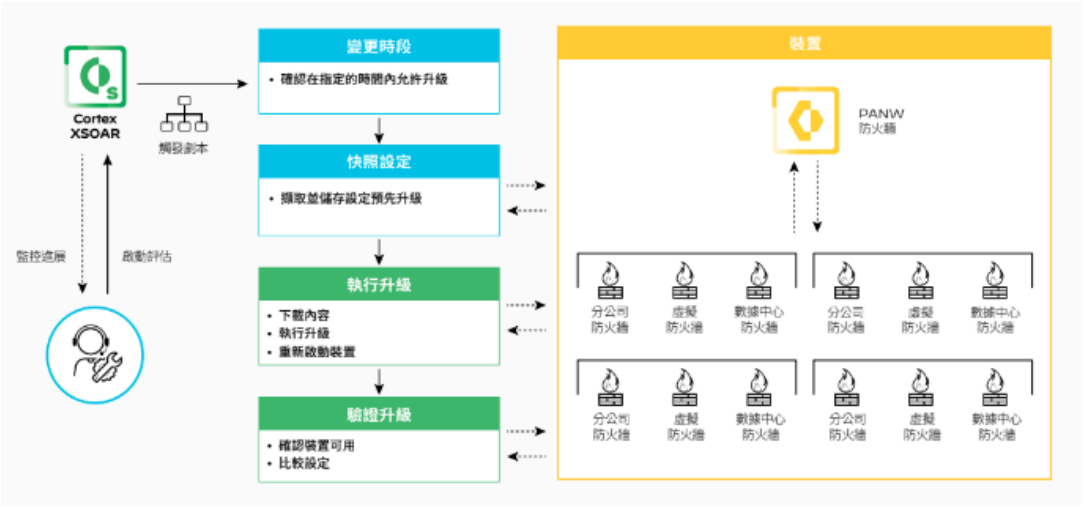


圖 58、自動化防火牆升級工作流程

Cortex XSOAR 是一個多功能且強大的整合解決方案，提供如強制執行多因素驗證、監控 VPN 通道安全狀況、封鎖威脅、產生 OSINT 與其他威脅報告等功能，對於使用許多網路裝置包含防火牆、IDS/IPS、路由器等的企業組織，管理與防禦所有的網路裝置、更新、升級等例行性作業佔去了許多時間，Cortex XSOAR 也提供了自動升級所有裝置與自動驗證的功能，並且建立升級前的快照以防有任何問題可快速回復原本狀態。

而採用自動化服務與設置的優點包含加速事件回應、整合安全基礎結構、標準化和擴充程序、提高分析人員生產力、簡化事件處理、合理運用現有資源等，除了可以降低人力消耗外，亦減少人為錯誤與判斷錯誤的可能性，僅將人力用在關鍵政策決斷與規則制定，同時能提升檢測與防禦效率。

圖 59、Palo Alto Networks 講座

五、 資安新創公司拜訪與交流

RSAC 為世界級資安盛會，今次有超過 500 家供應商與會，故訪團亦把握機會與預約拜訪多家資安新創公司，以瞭解趨勢並發展潛在合作機會。

(一)來毅數位科技(LYDSEC)

來毅數位科技此次在 RSAC 2023 主要展示的產品為 KEYPASCO，此產品著重於以多因素身分認證(MFA)為中心的零信任架構解決方案，運用雲端方式提供身分安全認證服務，以純軟體設計為主，安裝於用戶的終端設備，如電腦、手機、平板、或筆電中，經由綁定自己的設備，同時收集設備特徵值以及地理位置作為認證依據，以確保只有經過認證授權的人及設備，結合獨特 PKI 分散專利和雙通道的驗證機制，並搭配智慧風險管理引擎來強化網路使用者的身分安全，也可以和現有環境整合無需改變用者習慣，除此之外客戶也可以依其需求選擇使用地端方式在自有的主機中心佈署相關方案。

林政毅董事長在現場進行展示及簡介說明中也強調其產品的特色可以依據使用者的地理位置而更新授權方式，同時來毅科技的 KEYPASCO 也已經獲得全球 16 國專利，目前朝向全球銷售方向佈局，仍然期望能夠在政府的協助下，結合更多的臺灣業者共同擴展國際市場。

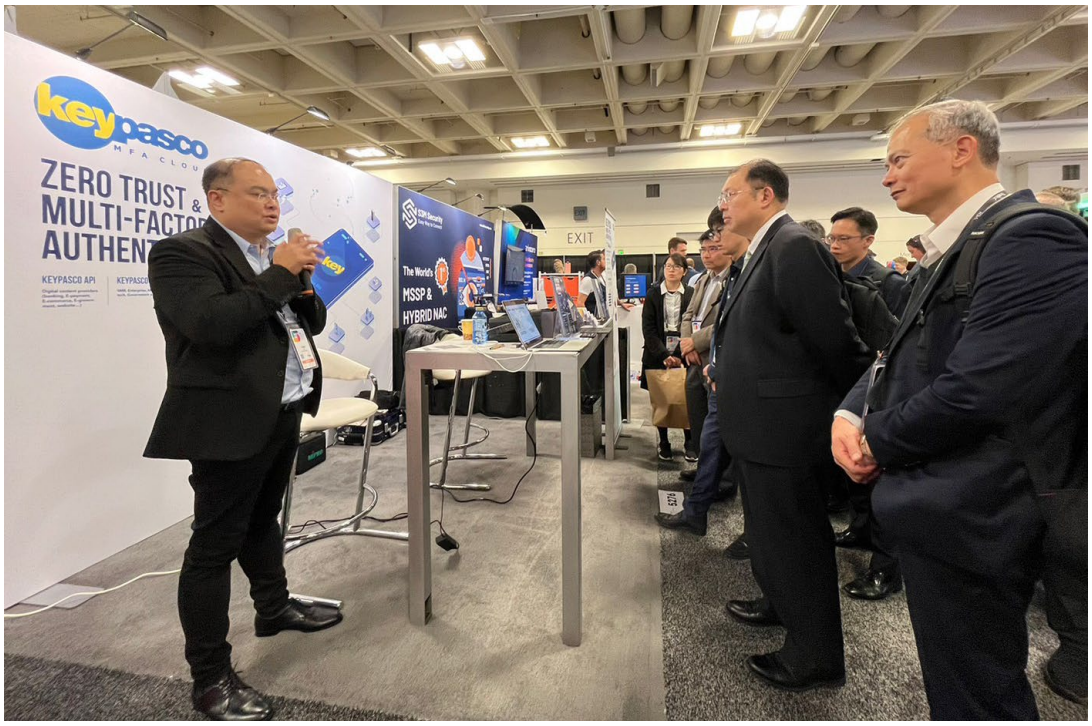


圖 60、參訪來毅數位科技攤位

(二)睿控網安

睿控網安(TXOne) 為趨勢科技投資成立之公司，主要致力於工控資安的臺灣廠商，專注於工業環境場域以及關鍵基礎設施提供零信任的網路架構解決方案，此次在 RSAC 2023 主要展示其專為 OT 場域風險評估及資產管理，解決供應鏈資安問題，所推出最新、無需安裝代理程式(Angetless)及惡意程式的產品-- Portable Inspector solution，並且由睿控網安執行長劉榮太親自說明這項產品的特點在不需安裝程式，使用 USB 隨身碟中的檢查工具，就可以產出無病毒報告以符合法規，並且可以掃描系統漏洞，並利用 TXOne Networks 的 Element One 管理控制台為企業組織提供相關產業控制系統 (ICS) 和 OT 環境進行風險評估。

劉執行長特別表示此行展出的這套工具 Portable Inspector solution 可以簡化稽核工作，同時在 SEMI E187 合規要求下，有效管理過去不易管理的資產，整合組織現有的流程，並不會引入額外的複雜度或負擔。這款 TXOne Networks 解決方案可以在不需要重新啟動系統並且不留下系統足跡的情況下進行惡意軟體的檢測和清除，這符合設備製造商的銷售條款中禁止安裝或更改設定的規定。對於產業

OT 環境解決方案滿足各種垂直行業在設備檢測、端點保護和網路防禦方面的獨特需求，是一個相當重要功能。

圖 61、TXOne 解決方案

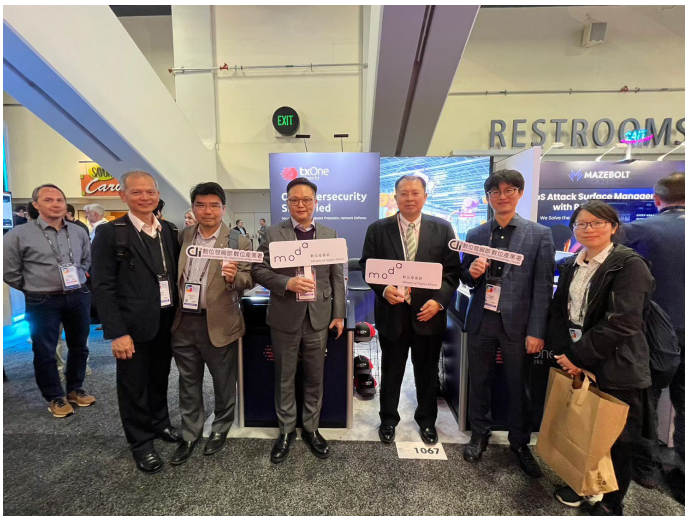


圖 62、參訪 TXOne 攤位

(三) Skydio, Inc.

Skydio 於 2014 年 1 月成立，總部位於美國加利福尼亞州的聖馬特奧市(San Mateo)，製造工廠位於加利福尼亞州的海沃德(Hayward)。2023 年 2 月完成了 2.3 億美元的 E 輪融資，累計融資達到 5.62 億美元，融資後估值高達 22 億美元。Linse Capital 為 E 輪融資的領頭者，其他投資方包含 Andreessen Horowitz、IVP、DoCoMo、NVIDIA 和 Axon 等，其中 Axon 是全球公共安全領域的技術領導者，也是 Skydio 重要的技術合作夥伴。該公司宣稱 Skydio 無人機已被美國國防部的每個分支機構、超過一半的美國交通運輸部、47 個州的 200 多個公共安全機構和 60 多個能源公用事業公司使用，憑藉其自主技術，Skydio 是現在美國最大的無人機製造商，並獲 2022 年 Deloitte Technology Fast 500™ 獎項中被公認為北美增長最快的公司之一。

Skydio 主要藉由人工智慧技術，創建智慧無人機，其智慧自主飛行技術，在自動避障和自動追蹤使用者方面，都有亮眼的表現。該公司於 2022 年 12 月宣布新一代 Dock 系列(Dock and Dock Lite)，擁有最迷你、最輕薄和擁有 AI 技術的無人機「雲端連接基站」。該系列內建 Skydio 最新的 Remote Ops 軟體技術，讓客戶能夠隨時隨地在世界任何地方，進行遠端監控、態勢感知任務和測繪，可應用於倉庫監控、檢查安全邊界和檢查自然災害後的基礎設施評估等，Skydio Dock 僅佔地面積僅為 4 平方英尺，重量 62 磅，可自由部署在狹窄複雜的空間中。此外，Skydio 也

推出突破超視距(BVLOS)障礙的監管服務，協助客戶在超視距範圍內操作無人機，包括完全遠程操作等，實現了無人機帶來的高效率和可擴增的遠端操作功能。

圖 63、Skydio 展示無人機技術

圖 64、參訪 Skydio

(四) Rubrik

Rubrik 於 2014 年 1 月成立，總部位於美國加利福尼亞州的帕羅奧圖市(Palo

Alto)。2019 年完成 E 輪融資，累計融資達到 5.53 億美元，融資後估值高達 33 億美元。Rubrik 在全球設有 16 個分公司，客戶包含民間與政府單位等累計超過 4500 家，威實康科技(Westcon Taiwan)為其台灣區代理商，協助 Rubrik 向東南亞和大中華地區的客戶提供產品和解決方案。

Rubrik 的雲端數據管理解決方案(Rubrik Security Cloud)，可進行跨數據中心和雲端資料管理，具數據彈性(Data Resilience)、數據可觀察性(Data Observability)以及數據恢復(Data Remediation)三大功能，幫助企業在任何地方安全地恢復、移動和管理數據，並提供抵禦勒索病毒攻擊事件的資料損失以及減輕數據隱私洩露的營運風險。

Rubrik 的技術合作夥伴包含 Google、AWS、NetApp、VMware、IBM、Cisco 等；其中微軟在 2021 年對該公司進行股權投資，雙方共同提供 Microsoft 365 與混合雲的資料保護服務，並整合 Microsoft Azure 上的各式雲端服務，將 Rubrik 的勒索軟體攻擊資料復原、自動化資料處理及資料遷移至雲端的能力，應用在 Microsoft 365 在內的資料中心、邊緣及雲端環境上。

圖 65、關次長代表訪團致贈禮物

(五) Mammoth Cyber

美商安佩科技(Appaegis Inc.)成立於 2019 年，並於 2023 年 2 月正式更名為 Mammoth Cyber，總部位在美國加利福尼亞州的帕羅奧圖市(Palo Alto)。2021 年底曾獲得台杉投資(水牛五號科技基金)領投，包含 TSVC、Alumni Ventures、Silicon

Valley Future Capital 等共同投資合計獲 770 萬美金種子資金。2022 年獲選為該年度 Red Herring Top 100 Global Winner。

該公司致力於研發雲端資訊安全技術，推出在企業雲端架構層搭載零信任的資安防護系統(Mammoth Enterprise Access Browser)，功能包含身份管理、遠端瀏覽器隔離、資料檢測與外洩防護等，支援不同應用程式或協定如 Web、SSH、RDP、Bitbucket®等，可整合企業現有不同雲端服務的安全防護。其知名企業夥伴包含 AWS Marketplace、Microsoft 等。

(六) Traceable

Traceable 成立於 2018 年，總部位於美國加州舊金山市區。於 2022 年 5 月完成 B 輪融資，由 Institutional Venture Partners(IVP)領投，其他投資者包括 Tiger Global Management 以及原 A 輪投資者 Unusual Ventures 和 BIG Labs，總獲 6000 萬美元，融資後估值達 4.5 億美元。

Traceable 利用機器學習技術與 API Data Lake 儲存功能來擷取、存放及分析用戶上下文數據，以了解正常應用程式行為並檢測偏離規範之活動，並透過點到點分散式追蹤及雲端原生集應用，為客戶提供 API 評估風險以及可識別、可追蹤之安全監測服務，讓企業能夠輕鬆分析攻擊企圖與原因，阻止 API 受攻擊，並進行安全操作。

圖 66、Traceable 說明會

(七) SafeLiShare

SafeLiShare 成立於 2021 年 8 月，總部位於美國東岸大紐約區，種子輪投資者為台杉投資(水牛五號科技基金)及大亞創投，總獲得 500 萬美元投資金額。SafeLiShare 是一間提供零信任資料保護的安全數據共享框架，利用安全隔離區技術創建零信任計算環境，達到真正的資產級別保護及數據隱私。

SafeLiSahre 使用最新進程的機密運算技術，於工作流中提供程式與數據策略性驅動存取權，並透過該技術將用戶所定義的敏感代碼與數據與執行環境進行隔離，以避免惡意攻擊或干擾，讓所有運行數據、各階段工作流程都能被控制在安全機制上，讓用戶即使於公有雲上進行遠端操作，也能保障安全。

伍、 心得及建議

本次出席會議，包括相關議程討論以及與國外政府官員交流等部分，經出國人員彙整、觀察及研析，爰整理以下建議供參：

一、 策略面：

本次會議討論，由於國際情勢極化、對抗氛圍升高，因此各國政府皆強調跨國、跨部會、公私合作的重要性，以及整合每個夥伴成員不同知識和經驗以聯合對抗網路威脅之必要性。至於有關資安工作的思考邏輯，也從以往強調資安防護、阻絕敵人於資安體系以外的思考邏輯，逐漸轉變為資安攻擊無可避免，以及如何強化資安系統韌性、減少資安攻擊災損、在最短時間恢復系統運作等角度，整體建構強化資安防護體系。另外也強調可以從資安攻擊者的角度思考，透過提高攻擊者的負擔成本，讓攻擊者審慎考量目標選擇，藉此嚇阻資安攻擊發生。其次，有關中國、俄國與勒索軟體組織合作，為全世界帶來更多且更強的資安威脅，美國政府部門包括CISA、NSA、 CyberCOM 等如何合作及因應等，也都值得我國思考與借鏡。

資安框架 NIST CSF 2.0 的更新內容和相關時程，及其在組織的資訊安全和風險管理中之應用亦深具啟發性，我國或可參考應用該框架來增強組織的資訊安全防禦能力，提升組織的資訊安全水平。此外，應持續協助提升國人資訊安全意識，加強培訓和教育，確保每個人都能夠認識到資安的重要性，並且能夠遵守相關的安全措施和政策。

二、 技術面：

本次會議主題 Stronger Together，期以多方合作來面對不斷變化的資安威脅，討論議題從資源和人才的發掘到零信任架構的營運，再到生成式人工智慧(AI)和大型語言模型(LLM)，本次會議有多達 10 幾場的 AI 應用講座最為熱門，AI 工具除可用來檢測威脅、保護系統和數據外，如對抗網路釣魚及勒索病毒攻擊等，另自去年 11 月公開發布 ChatGPT(AI 聊天機器人)以及 Midjourney(AI 自動生成圖片)等技術大放異彩，免不了還有攻擊者如何利用 ChatGPT 來查找零日漏洞、編寫惡意軟體及網路釣魚電子郵件，或利用 AI 換臉詐騙等行為，與任何工具一樣，電腦工具同樣可用來造福我們或造成傷害。

如同本次 RSAC 創新沙盒競賽前 10 名的比賽過程中，各家參賽選手的產品基本圍繞 2 個問題：AI 本身的安全和如何利用 AI 技術做到資安，廠商若能提供優異的

人工智慧(AI)/機器學習(ML)輔助及使用者導向優先次序判斷機制與自動化，來彌補人才短缺問題的產品將備受市場青睞，就像今年競賽冠軍 HiddenLayer 主打用於 AI 對抗性攻擊的非侵入式平台服務即是。另呼應本次 SANS 研究所報告「The Five Most Dangerous New Attack Techniques」，主講人之一 Heather Mahalik 的建議，人們不要害怕生成式 AI 的力量，而是要花時間去理解它並進行多層次防禦，而我國國科會目前亦召集各部會研議「公務機關使用生成式 AI 參考指引」，將可作為政府部門使用生成式 AI 時確保個資安全與資安防護的參考依據。

此外，透過單一操作介面、平台式方法以及託管式服務來簡化資安營運，同樣也是大會的主要話題，尤其在本次會議期間資安廠商博覽會(Expo)有不少託管式服務供應商(Managed Service Provider,MSP)及威脅偵測與應變服務(MDR)廠商產品展出，不少資安從業人員的共同心聲都希望將技術工具整合、簡化工作流程及程序、減少情境切換與資安警報疲勞問題，同時也希望藉由平台式技術與 7*24 小時的威脅監控、資安風險管理以及事件回應支援來解決全球共通資安人才短缺的問題。

零信任部分亦為今年熱門議題之一，其核心「絕不信任、持續驗證」目標是解決現今網路環境中的資安問題，特別是信任邊界不明確的情況，透過對任何資料存取都持保留懷疑的態度，並要求持續進行驗證，以便更快跟上駭客的攻擊速度。而我國最近一期的行政院國家資通安全發展方案(110 年至 113 年)，也已逐步推動政府機關採用零信任網路，數位部政府資料傳輸平臺(T-Road）更預計在今(2023)年底全面實踐零信任驗證管理制度，取用任何資料都須通過身分、設備、行為模式的檢驗，以防範資料外洩，強化公部門的資安韌性。

今年大小廠商無不積極展示受攻擊面管理、曝險管理及受攻擊面分析產品，說明盤點資訊資產對於防範資安風險、不讓駭客趁機利用這些暴露的受攻擊面至為重要，在「5 Open Source Security Tools All Developers Should Know About」講座提到開發者在開發代碼的過程中，常會擔心專案打包的映像檔是否存資安疑慮，並推薦 5 個開源的安全工具，分別為 Semgrep(檢測代碼中存在的脆弱性問題)、OSV-Scanner(檢測代碼所依賴具有漏洞的元件)、KICS(檢測提交到雲端前的安全配置)、Trivy(檢測容器鏡像中的漏洞和配置問題，及 ZAP(檢測應用程式或 API 的漏洞)，協助開發人員提前修補漏洞；另在「The World on SBOMs」講座說明透過維護準確的 SBOM，能有效管理風險，確保軟體產品的完整性和安全性，降低資安事件發生機率，再再說明檢測及修補的重要性，降低組織暴露在外的風險。而我國在 110 年 8 月 23 日修正發布之資通安全責任等級分級辦法，已明訂資通安全責任等級 C 級以上之公務機關與關鍵基礎設施提供者，應完成資通安全弱點通報機制(VANS)導

入，期藉由逐步推動方式強化資訊資產管理與弱點管理，提升我國整體資安防護能力。

三、 國際合作面：

美國資訊安全(RSA)大會每年召開，吸引來自全球各地的資安專業人士、政府代表和企業領袖，這種多方參與和交流的環境有助於我國建立國際合作夥伴關係，就各國與企業最關切議題進行討論，各資安產業也無不全力以赴展現自家產品的優勢，的確對於出席人員掌握最新資安趨勢、以產業角度重新思考資安防護整體架構、與其他各國出席人員交流意見以強化國際關係與合作可能等，都有相當重要幫助，也是本次各出席人員最重要的參與收穫。

烏俄戰爭及美烏合作經驗議題通我們相關的防禦工作參考，幫助瞭解各國之間的合作和訊息分享的重要性，包括建立國際間的合作機制和交流平台，以促進資安領域的合作與共識。資安攻擊是一個全球議題，唯有合作，才能有效應對挑戰與威脅。