出國報告（出國類別：開會）

參加「2022年以色列國土安全暨資安大會」及參訪當地提供政府資安及AI服務之研究機構

服務機關：財政部財政資訊中心
姓名職稱：周子元組長
陳成威助理程式設計師
曾柏勳助理程式設計師
林冠伯助理程式設計師
派赴國家/地區：以色列／特拉維夫
出國期間：111年11月25日至12月3日
報告日期：112年2月22日

摘要

「資安就是國安」於現今環境已是不容置疑之事實，隨著各類新興技術快速發展，網路系統及資訊安全受到的威脅越來越多，攻擊也越來越頻繁。不論是資訊系統的攻擊或假訊息的散布，都有可能對社會、經濟造成重大危害。政府除了持續強化國家層級的資訊安全外，期待與大家共同努力提升資安防禦及應變能力，進一步強化臺灣整體韌性。面對鋪天蓋地沒有煙硝的資訊戰，沒有人可以置身事外。政府2018年通過<資通安全管理法>，2022年8月數位發展部正式成立，政府持續與更多國際盟友一起打造更具韌性、安全的供應鏈，強化國家資通安全能力。

財政部財政資訊中心(下稱本中心)肩負財政部與所屬機關(構)資訊系統及資訊安全規劃、宣導及評核之重責，對資訊安全之重視更是要求，考量安全程式碼、設計階段即納入安全考量(Security by design、Security by default)為資訊安全的基礎，時值本中心使用逾十年之既有國稅應用系統、地方稅應用系統、電子發票應用系統等資訊作業平台重新規劃建置之際，相關先進資訊安全防護機制實有瞭解之必要；又隨著少子化、實質勞動人口之減少，有效應用新興技術(如：人工智慧(AI)工具)來協助同仁更有效率與效果的執行工作，亦是刻不容緩的待辦事項。為求有更完善之規畫與選擇方案評估，參與相關國際研討會，快速吸收新知與他國經驗不失為一良好方法。

經查，以色列位處中亞，人口雖僅900多萬人，卻是數千家新創公司的創辦地和總部，首都台拉維夫為創投聚集地，科技活耀度極高。其在資訊領域強大的創新力與引資能力，每年產生近千家的新創公司，在數位技術及AI等各種應用逐年上升。以色列與台灣同處政治角力的中心，強制兵役，大量年輕公民普遍受過面臨生死的訓練和考驗，以色列軍隊也有科技職位，專門替作戰和情報人員開發尖端通訊情報科技，退役後將經驗和心態帶入就職公司，畢業生進入科技業後互相提攜，提供各種幫助。

2022年11月27日至29日於以色列台拉維夫舉行之「2022年以色列國土安全暨資安大會」以實體國土安全及網路資安為主軸，探討國家安全、網路資安保護、物聯網科技及AI等議題，正符合本中心之需要，另為更了解應用軟體端之安全與AI模式於稅務應用上之發展，於11月30日及12月1日規劃參訪當地提供政府資安及AI服務之科技廠商，期盼能多了解以國資安產業發展情形，及可供我國參考之應用。

目錄

壹、前言

一、動機

「資安就是國安」於現今環境已是不容置疑之事實，隨著各類新興技術快速發展，網路系統及資訊安全受到的威脅越來越多，攻擊也越來越頻繁。不論是資訊系統的攻擊或假訊息的散布，都有可能對社會、經濟造成重大危害。政府除了持續強化國家層級的資訊安全外，期待與大家共同努力提升資安防禦及應變能力，進一步強化台灣整體韌性。面對鋪天蓋地沒有煙硝的資訊戰，沒有人可以置身事外。

行政院國家資通安全會報更是自90年迄今，陸續推動6個階段、各為期4年之重大資通安全計畫或方案。鑒於資通訊服務應用廣泛，以及我國重大科技創新政策，為能因應國際趨勢與新型態資安攻擊與威脅，除持續落實第五期國家資通安全發展方案(106年至109年)，於107年通過<資通安全管理法>，行政院國家資通安全會報為逐步提升我國資通安全防護能量，更於110年2月23日提出國家資通安全發展第六期方案(110年-113年)，作為我國推動資安防護策略與計畫之依循目標。

第六期發展方案以「打造堅韌安全之智慧國家」為願景。搭配「成為亞太資安研訓樞紐」、「建構主動防禦基礎網路」、「公私協力共創網安環境」3大政策目標，並從「吸納全球高階人才、培植自主創研能量」、「推動公私協同治理、提升關鍵設施韌性」、「善用智慧前瞻科技、主動抵禦潛在威脅」及「建構安全智慧聯網、提升民間防護能量」等四個面向著手，搭配六大核心戰略產業之資安卓越產業發展方案，規劃持續推動資安產業，期以打造安全堅韌之智慧國家。111年8月數位發展部正式成立後，可以預期政府將持續與更多國際盟友一起打造更具韌性、安全的供應鏈，強化國家資通安全能力。

考量財政部財政資訊中心(下稱本中心)肩負財政部與所屬機關(構)資訊系統及資訊安全規劃、宣導及評核之重責，對資訊安全之重視更是要求，認知安全程式碼、設計階段即納入安全考量(Security by design、Security by default)為資訊安全的基礎，時值本中心使用逾十年之既有國稅應用系統、地方稅應用系統、電子發票應用系統等資訊作業平台重新規劃建置之際，相關先進資訊安全防護機制實有瞭解之必要；又隨著少子化、實質勞動人口之減少，有效應用新興技術(如：人工智慧(AI)工具)來協助同仁更有效率與效果的執行工作，亦是刻不容緩的待辦事項。為求有更完善之規畫與選擇方案評估，參與相關國際研討會，快速吸收新知與他國經驗不失為一良好方法。

以色列每年產生近千家的新創公司，是數千家新創公司的創辦地和總部，首都台拉維夫為創投聚集地，科技活耀度極高。其在資訊領域強大的創新力與引資能力，在數位技術

及AI等各種應用逐年上升。111年11月27日至29日將於以色列台拉維夫舉行「2022年以色列國土安全暨資安大會（Israel HLS & Cyber 2022)」，以實體國土安全及網路資安為主軸，探討國家安全、網路資安保護、物聯網科技及AI等議題，會議期間將集結60多家專業公司以及20多位國際講者為大眾演繹以色列備受肯定的新一代防衛科技；另為更加了解以色列資訊及資安產業之合作交流，主辦單位於會議期間亦安排實地參訪資訊/資安科技工具應用於警務界之實境模擬演練及該國相關產業之攤位展示說明，期盼讓與會者能多了解該國資安產業發展情形。蒐集完上開資訊，該大型資訊安全國際會議，正符合本中心現階段之需要，有必要派員前往取經；另考量該大會之講者與分享案例較著重於實體資訊安全防護之經驗分享，對於應用軟體端之安全與AI模式於稅務上之應用較無著墨，為讓派員出席之取經團更有收穫，更了解應用軟體端之安全與AI模式於稅務應用上之發展，於111年11月30日及12月1日規劃參訪當地提供政府資安及AI服務之科技廠商，期盼能多了解以國資安產業發展情形，及可供我國參考之應用。

二、參訪國(以色列)背景介紹

以色列位處中亞，人口雖僅900多萬人，卻是數千家新創公司的創辦地和總部，首都台拉維夫為創投聚集地，科技活耀度極高。惟其在資安領域強大的創新力與引資能力，每年產生近千家的新創公司，在數位技術及AI等各種應用逐年上升。以色列與台灣同處政治角力的中心，強制兵役，大量年輕公民普遍受過面臨生死的訓練和考驗，以色列軍隊也有科技職位，專門為作戰和情報人員開發尖端通訊情報科技，退役後將經驗和心態帶入就職公司，畢業生進入科技業後互相提攜，提供各種幫助。

以色列是一個移民國家。自1948年建國至今，以色利的人口超過10倍。2019年10月人口已經超過9百萬，是不同民族背景、生活方式、宗教、文化和傳統的大融合，其中猶太人人口占75.4%，非猶太居民占24.6%，這其中大多數為阿拉伯人（20.5%)。以色列90%的人口居住在城市。大約有200多個城市，其中一些城市建造在古蹟上。5%的人口居住在農村，他們具有獨特的生活方式，一起合作，共同分享，這樣的生活方式被稱為基布茲和莫沙夫。

主要城市耶路撒冷為以色列首都（2019年人口超過90萬），自3000年前大衛王將其定為首都之後，一直是猶太人民國家和精神生活中心。今天的耶路撒冷是一個繁榮充滿活力的大都市，是以色列政府所在地，也是以色列最大的城市；特拉維夫-雅法(人口43萬)，建於1909年，是第一座猶太新城，今天是以色列的工業、商業、金融和文化中

心。

以色列的研究與開發主要是在7所大學、數十個政府和公共研究機構和數百個軍用、民用企業裡進行。醫學中心和許多公用事業企業，諸如電信、電力和動力生產以及水資源管理等領域，從事大量的研究工作。政府和公共機構是研究與開發經費的主要來源，為以色列半數以上的研究與開發活動提供了財政支助。這些用於民用研究與開發目的經費大部分用於經濟發展，主要是用於工業和農業領域，與其他國家相比，占整個研究與開發活動費用的比例很大；40%以上的經費是通過國家、國家之間和政府的研究基金以及通過高等教育委員會管理的綜合大學基金對各大學的撥款用於增進科技知識項目。其餘的則專門用於各種衛生保健與社會福利領域。

以色列在自然科學、工程、農業和醫學領域裡出版著作的人數，在其勞動大軍中的比例大大高於其他國家；以色列科學家與其他國家科學家合著的出版物在該國的出版物中佔據著相當高的份額。為了使以色列科學界與國際科學界融為一體，以色列鼓勵人們參加國際上的科學會議，同時也鼓勵去國外進行博士後研究，以及利用假期去國外工作。以色列在研究機構、大學和政府級別上還與海外的相應組織保持著廣泛的交流計劃和合作項目。以色列也是舉辦國際科學會議的重要中心，每年都主辦許多場類似此次規模之國際會議。

貳、行程

一、行程表

日期	時間	行程
11/25-11/26 (星期五-六)		搭機前往以色列特拉維夫市
11/27(星期日)	19:00-22:00	研討會
11/28(星期一)	9:00-15:00	研討會
	15:00-17:00	訪問IVIX公司
11/29(星期二)	11:00-18:30	研討會： 前往Beit Shemesh(車程1.5hr)， 參訪以色列警察大學(Show Case)
11/30(星期三)	6:30-13:30	參觀首都耶路薩冷
	15:00-17:00	訪問Digital.ai公司
12/1(星期四)	9:00-11:00	拜會Radware公司
	11:00-12:30	拜會Checkmarx公司
	12:30-14:00	拜會駐以色列台灣辦事處
12/2-3(星期五-六)		搭機返臺

二、研討會會議議程與展場各區安排

圖1、研討會會議議程

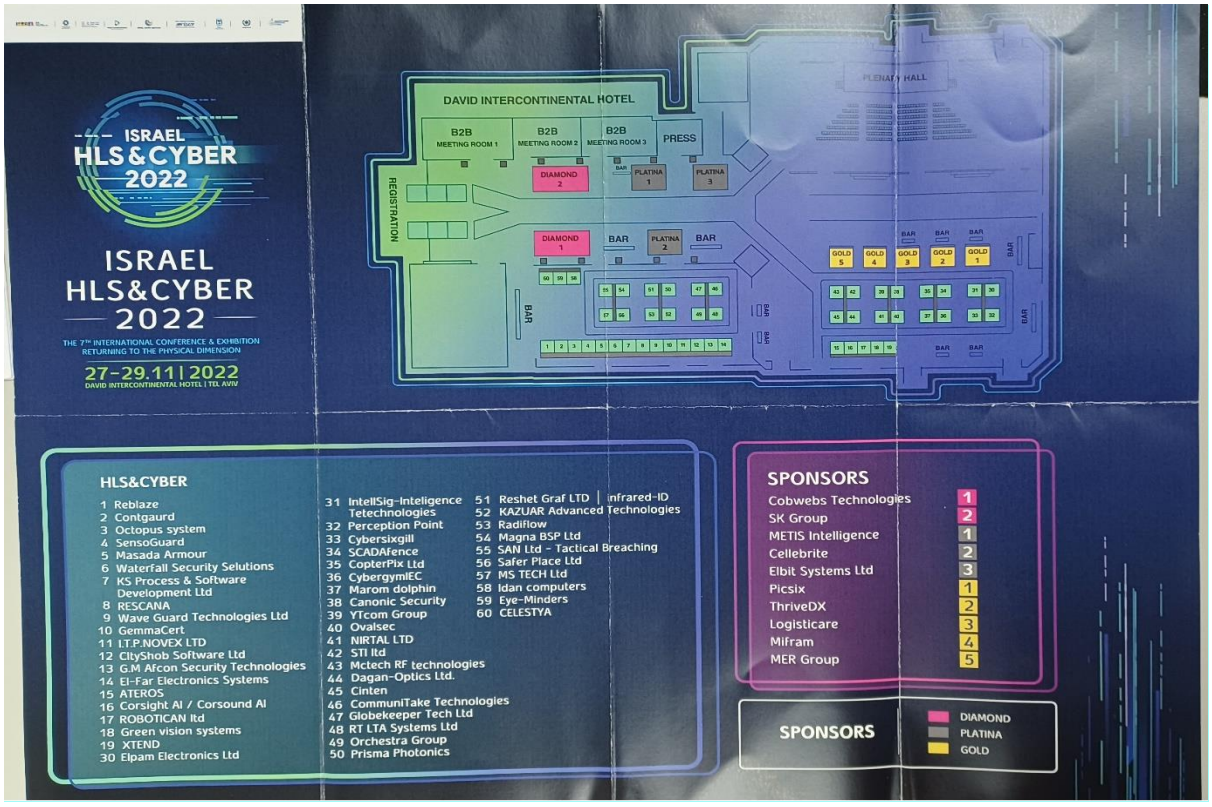


圖2、展場各區安排

三、會議講者照片與行程花絮留影

圖3、主辦方opening

圖4、以國總統致詞

圖5、以國公共安全部長致詞

圖6、以國經濟和工業部對外貿易管理局局長致詞

圖7、以國外交部副司長、經濟事務司司長致詞

圖8、以國官員致詞

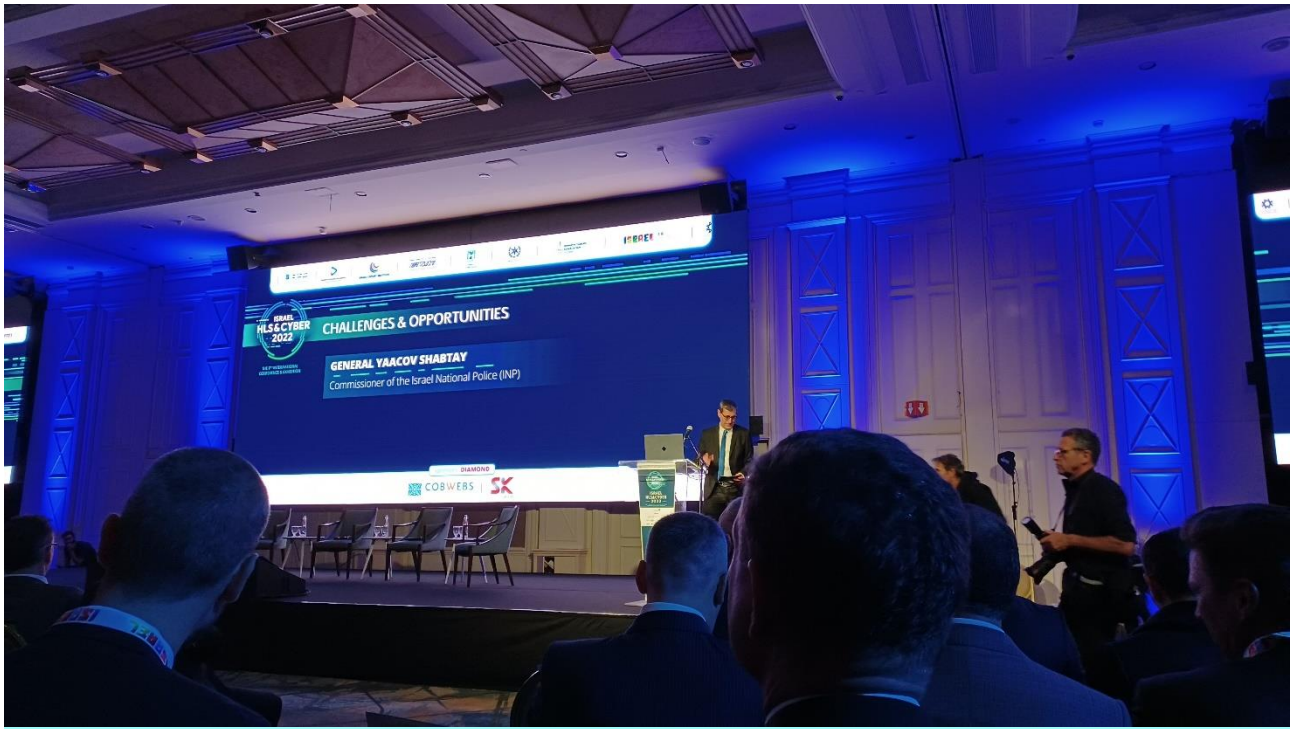


圖9、以國出口協會主席(主持人)致詞

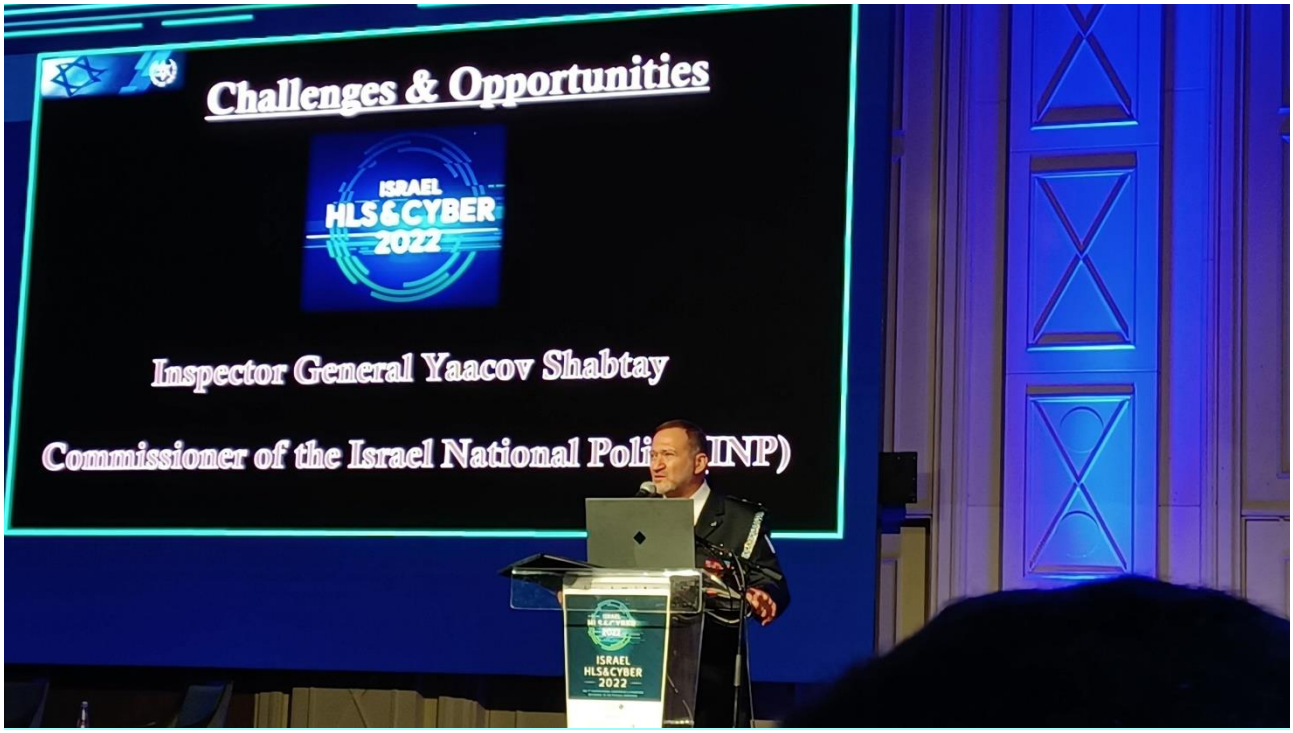


圖10、以國國家警察署署長致詞

圖11、「我們如何防止下一個威脅？來自世界各地的警察專員分享他們的見解」對談

圖12、「關鍵基礎設施不斷擴大的領域：預測、保護和預防」對談

圖13、「人群管理：“網絡穹頂”與公共安全」對談

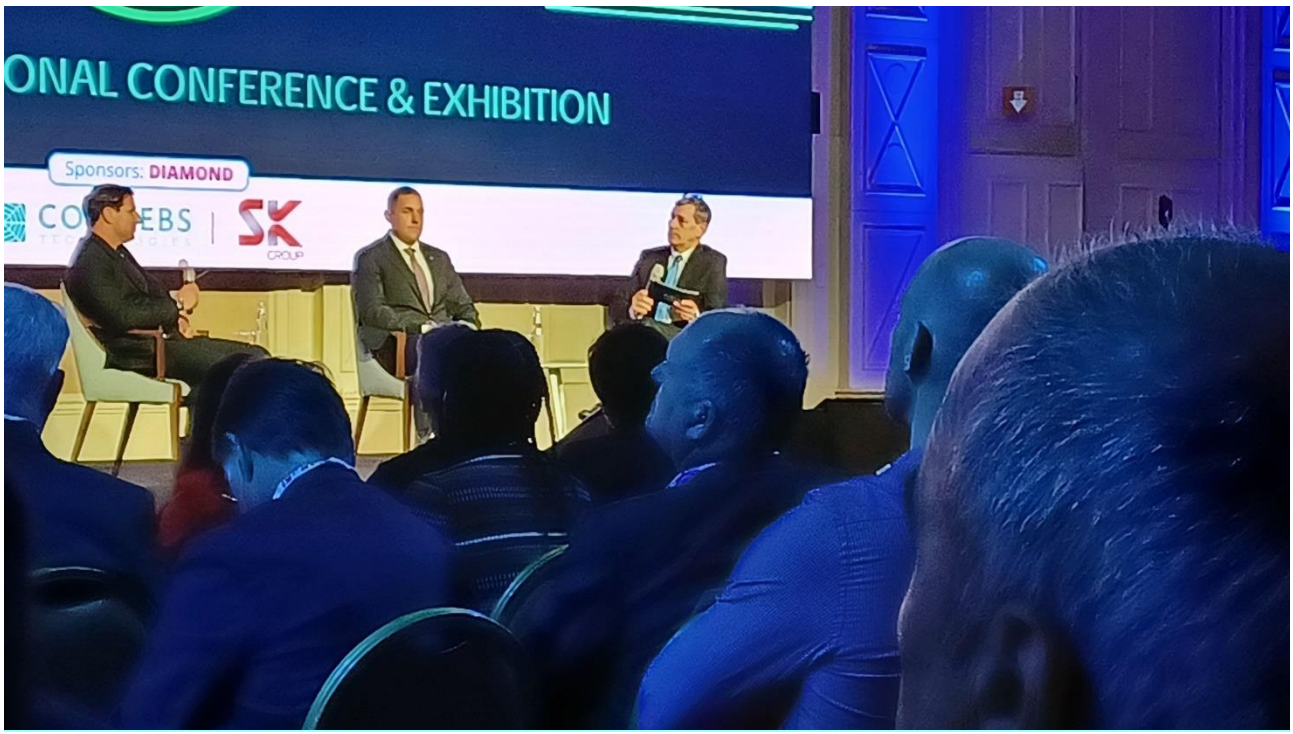


圖14、「人群管理：“網絡穹頂”與公共安全」對談

圖15、Maya——救援單位的綜合情報

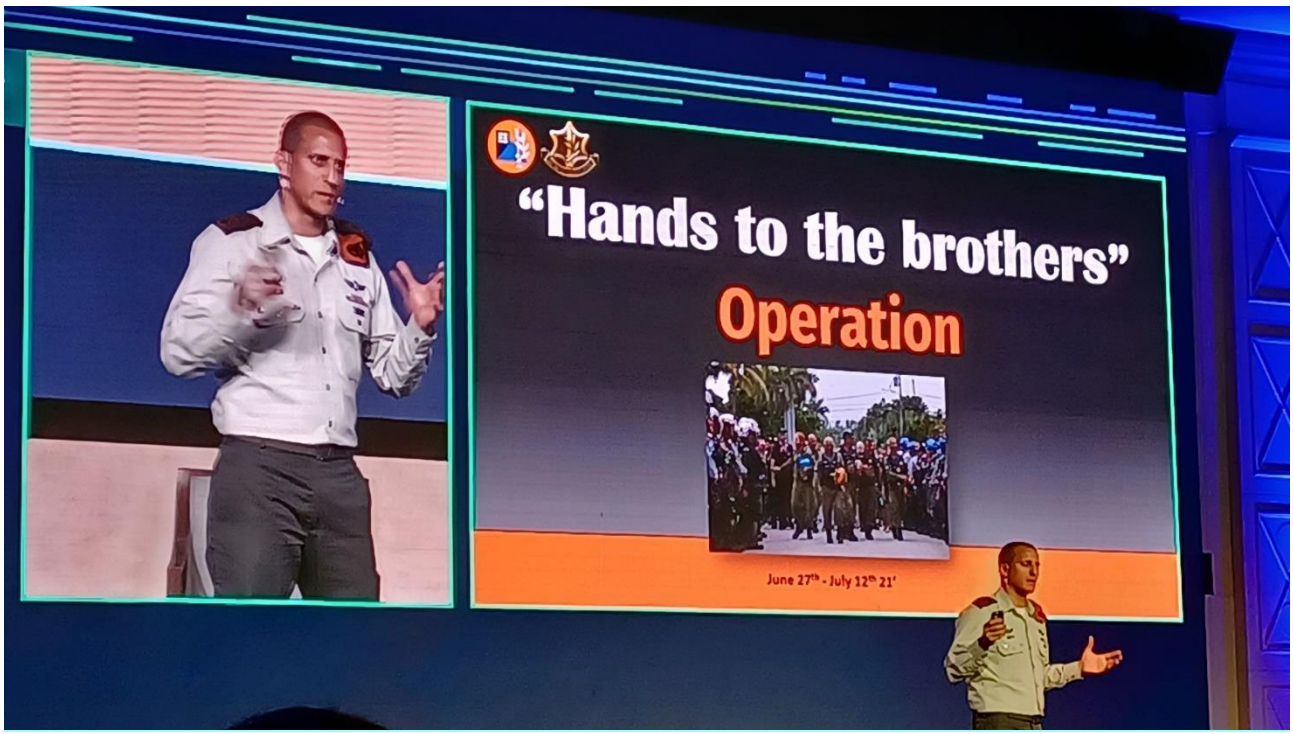


圖16、Maya——救援單位的綜合情報

圖17、「塑造未來：執法中的人工智能和機器人技術」對談

圖18、與會代表：陳成威

圖19、與會代表：曾柏勳

圖20、與會代表：林冠伯

圖21、與會代表：周子元

圖22、代表團合影

圖23、參訪國家警察學院代表團合影

圖24、參訪國家警察學院展示攤位

參、會議內容重點摘述

本次於11月28日參加「2022以色列國土安全暨資安大會（Israel HLS & Cyber 2022)」中，了解該國資安產業發展情形，並於11月29日參訪以色列警察在國家警察學院的科技展示，會議期間亦參訪該國相關產業之展示攤位。

一、 參訪以色列國土安全研討會

1. 挑戰與機遇

講者表示，現階段我們面對的議題包括網路上的意識形態、匿名化、網路犯罪以及加密貨幣。近年來，由於加密貨幣的使用一直在增加，它常常被連結到一些非法活動，例如網路犯罪和洗錢；另外，網路上的意識形態可能導致錯誤的訊息或是極端主義的傳播，造成極端化和分裂的加劇；而匿名化會被使用於多種的目的，像是網路犯罪、騷擾和欺詐等非法活動；網路犯罪的範圍很大，舉凡駭客攻擊、網路詐騙、販賣非法物品以及前面提到的加密貨幣洗錢等。每個議題都是我們面對的極力挑戰，但也是未來努力方向的機會點，這些機會點有賴跨部門、跨機關、跨國之合作，才可創造共贏之世界。

2. 我們如何防止下一個威脅？來自世界各地的警察專員分享他們的見解

以德國的數據為例，近10年來，以互聯網為犯罪工具的犯罪數量增長了67%，無論是數量或是質量都在持續上升；自2015年以來，有關網路犯罪防治領域的新創企業已經增長了100%；另外，越來越多的關鍵基礎設施、公共管理機構及供應鏈遭受攻擊。罪犯的結構也在發生變化，他們越來越國際化、進行任務分工，並轉化成一連串有紀律的網路行為，我們稱它為CaaS(Crime as a Service)。

美國的國土安全部(Department of Homeland Security，DHS)有7千名特工、超過10萬名員工專注於威脅美國公共安全和國家安全的跨國犯罪組織。而他們發現加密貨幣已成為暗網市場的主要支付方式，另外，DHS的報告中現在的網路可疑活動幾乎是2010年的3倍，特別2021年整年的報告中勒索軟體(ransomware)占了一大部分。這對DHS及執法部門來說，這可能是最重大的挑戰。

總體而言，各個國家都必須要持續發展並接納網路化的勞動力，世界需要這些技術

人才，並投資於這些勞動力。在美國，DHS為了防止技術人才跳槽到私人企業，提供了許多激勵措施並大量投資識別網路加密貨幣交易及網路犯罪的認證技術，還有聘請大量資料科學家、擁抱最新技術等。

羅馬尼亞官員表示為了打擊網路金融犯罪，他們選擇與私人企業合作，並在2022年11月初創建了跨境金融犯罪融合中心(Cross Border Financial Crimes Fusion Center)，與私人企業一起參與打擊網路金融犯罪，私人企業可以在犯罪發生的早期階段就識別出這些威脅並訓練同仁進步，儘管有相關隱私及法律議題，但這也是一個擴大合作範圍的絕佳機會。

德國官員認為面對數位轉型，必須要加快數位適應能力，德國發展了數位部隊，用於合作調查、情報共享、犯罪打擊等，另外，這些合作也避免了不同單位間的重複工作。

總歸而言，不同國家雖然做法不盡相同，但大致上都是選擇和不同單位、私人企業間的合作，擴大打擊範圍，並且增加投資於執法部門和國土安全部門的經費，延攬相關專業人才等。

3. **關鍵基礎設施不斷擴大的領域：預測、保護和預防**

隨著世界繼續擴大對機場、海港和電力基礎設施等關鍵基礎設施的保護，能源、交通、醫院、銀行等領域出現了新的挑戰，保護關鍵基礎設施對於確保特定國家持續運行基本服務（包括政府和民用服務）的能力至關重要，並提高了考慮控制論和動力學問題的重要性。

實體基礎設施如機場、國土，有實體安全的議題。隨著科技的進步，關鍵基礎設施引入科技資源，而這些科技由人來操作控制，人們必須了解不同的操控資訊。

人雖然控制著科技，卻也同時控制危機。不同國家因文化背景不同，在關鍵基礎設施上各有獨特性，並有些許差異，但仍有部分相同處，有關維持鍵基礎設施的安全，這些經驗必須共享，可參考其他國家成功的經驗，並將本身的經驗分享出去。

這些議題衍伸出隱私權(攝影機)、零信任、數位解決方式等，為了不失去資訊，必

須做好前置作業，以降低資安事件的發生。

4. 人群管理：“網絡穹頂”與公共安全

講者提及，在本次會議中，我們將與執法和公共機構管理領域的專業人士會面，討論我們如何在預測和預防危險的同時繼續保護關鍵基礎設施。在當今時代，保護人群既發生在現實世界中，也發生在虛擬世界中。這些空間中的人群在有影響力的國家中既是敏感又重要的目標。

在本次會議中，我們將討論尋找正確的安全措施來管理各種空間中由人為或自然引起的緊急事件所面臨的挑戰。在我們的討論中，我們將重點關注民用空間作為支持各國應對緊急情況的一個因素。

好的關係非常重要，包含國家間的合作與密切關係，部分關係與軍事有關，公司間的關係來自金錢利益，如果一些事情發生，可以快速恢復，不同的費用。因為科技產生網路上虛擬的關係，如社交平台，所產生的個資也需要維護。實體環境人群管理，及虛擬環境的人群管理，所衍伸出個資、資安議題，需適當處理，並避免影響公共安全。

5. Maya——救援單位的綜合情報

過往消防安全往往只能依靠相對低科技產品(如煙霧偵測器)被動進行偵測，但隨著現代社會人口增多，使用產品越來越多也越來越易燃(如電動車電池)，但現今仍有許多範圍能藉由導入新科技讓災害可以提前預警，並減少災害的發生，如森林大火原為自然生態循環的一部分，但隨著人類開發、居住範圍逐漸擴大，若大火、濃煙接近人生活的社區則極有可能造成大災難。美國消防局平時依靠架設攝影機及空拍機取得大量圖資，並導入AI分析每一場森林大火的數據，當森林大火發生時，消防單位可以根據實時的監控畫面加上AI來預測可能受影響的區域，以達到預警功能，提前疏散民眾及將火勢控制在一定範圍內。

2021年，美國佛羅里達州邁阿密一棟蓋在海邊的大樓於半夜突然倒塌，早成多人失聯的情形，由於事件發生時間為半夜，造成等待救援的人非常多，且大樓為垂直崩塌，造成搜救難度升高，若單純靠搜救人員大範圍搜索及怪手逐步開挖可能會造成搜救時間的浪費，導致民眾錯失黃金72小時的救援時間，搜救人員至現場後運用軟體重建倒塌現場，分析大樓倒塌方式及倒塌後每個樓層的相對位置，對比原先建築圖，描繪出倒塌現場每一戶的位置在哪。另外，透過住戶家屬的社群帳號，分析出事故發生時，住戶是否在家，藉由上述兩點資訊交互對照，搜救人員變無須逐層逐

戶搜索，可以針對推測有人的地方先進行搜救，大幅減少受難者等待救援時間。

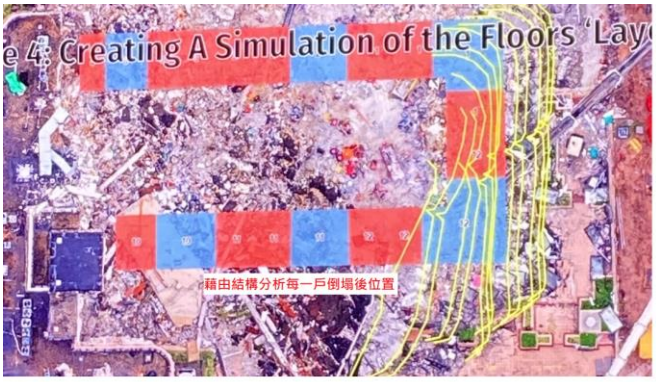


圖25、演示示意圖

圖26、演示示意圖

過往人類在面對大型災害時往往會陷入被動情況，由於資訊片面，現場指揮官往往也只能依照當下所獲得的片面資訊加上過往的經驗，做出相對比較妥當的決策，但隨著科技產品的進步，我們開始可以運用新技術進行資訊蒐集，進一步輔助決策，甚至達成24小時監控及預警，除了減少受災程度外，更開始可以達成避免災害發生的好處。

6. 塑造未來：執法中的人工智能和機器人技術

當新技術進入人類生活的開始，人類往往都會容易有排斥心理，並把新科技想像的跟魔鬼終結者一樣的恐怖，但後續在順利導入人類生活後，都可以帶給人類生活方便，且大大的改變人類原本生活。雖然新科技的發明立意都是為了創造更好的生活，但仍然應該要有相關規定去規範(如更方便的工具往往會根據得到的個人資訊

去輔助，但該工具可以獲取到哪種程度的個人資訊則需要加以規定，否則會造成個人資訊的洩漏)，然而過於保守也容易造成社會進步緩慢(因更新更方便的技術及工具無法進入社會)，因此如何平衡兩者變成是未來會持續發生、會更需要溝通的課題。講者表示身為新科技的發明者，更有義務去消除社會對於未知的恐懼，藉由提供充足的資訊，跟社會大眾解釋新科技的應用，並與立法者溝通，建立一個可以帶給人類方便，但又不侵害人權的雙贏畫面。

7. **會議中設攤廠商簡報：**

(1)Reblaze：

Reblaze是一家網路資安公司，提供Web應用程式和API保護等的解決方案，以保護企業免受威脅。他們的解決方案在於防範一系列威脅，包括SQL注入攻擊(SQL injection)、XSS攻擊，以及針對 Web 應用程式和API的其他類型的網路攻擊，並提供一個整合性的網路安全平臺(an all-in-one web security platform)。

以下是 Reblaze 的 Web 應用程式和 API 安全解決方案的一些關鍵特性和功能概述：

・即時保護(real time protection)：Reblaze的解決方案使用先進的機器學習演算法來分析傳入的流量並即時檢測和阻止威脅。

・自定義的安全規則(Customized security rules)：Reblaze的解決方案允許使用者創建自定義的安全規則以滿足使用者特定需求。

・API安全(API security)：Reblaze 的 API 安全解決方案可防止特定的API威脅，例如 API濫用和未經授權的存取。

・次世代Web應用程式防火牆(next-gen WAF)：Reblaze的WAF可防禦範圍廣泛的Web應用程式攻擊，包括 SQL 注入攻擊、XSS攻擊等。

・即時流量監控管理(real-time traffic monitoring&control)。

・與公有雲服務供應商(AWS、Azure、GCP)全面整合，可依據使用者所選擇的雲端平台彈性部署。

圖27、廠商資料

(2)Cobwebs：

Cobwebs Technologies 是AI驅動(AI-Powered)的公開來源情報(Open-Source Intelligence,OSINT)領域的全球領先者，Cobwebs致力於透過對公開可用資料的無縫式存取，產生威脅報告和即時告警，保護全球的社群和組織免於犯罪、威脅和網路攻擊。

以下是Cobwebs產品的核心特色：

- 監測並分析開放資料、暗網
- 將單一的線索轉化為全面、深入、清晰的威脅報告
- 即時分析結構化和非結構化資料，提供自動的即時告警
- 利用大數據和精簡的人工智慧提供自動化洞察

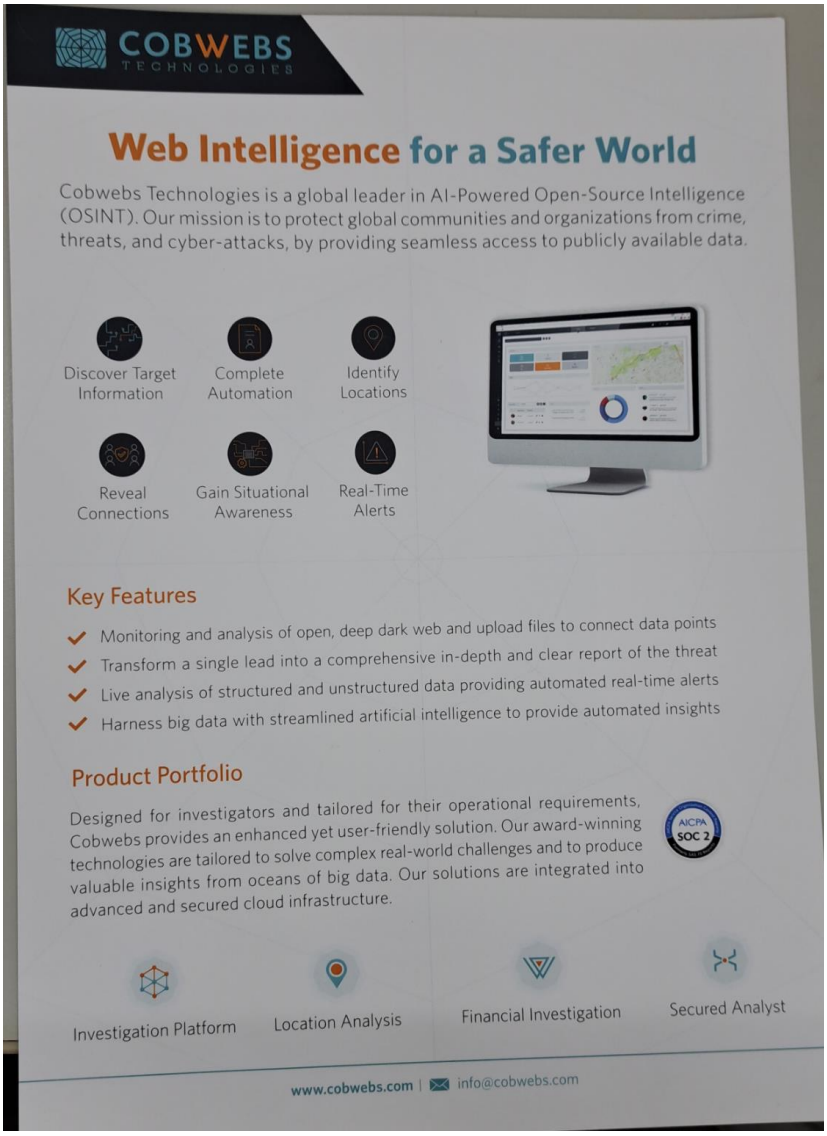


圖28、廠商資料

二、參訪警察大學

第三天的行程，主辦單位帶與會者到以色列國立警察學院(National Police Academy)進行參訪。國立警察學院是以色列警察的專業培訓機構。它位於耶路撒冷(Jerusalem)附近的貝特謝梅什(Beit Shemesh)，負責培訓以色列警察的所有新人，並為經驗豐富的警官提供高級培訓。該學院成立於2015年，將全國所有以前的警察培訓中心合併為一個，並提供所有類型的警察培訓。該學院提供範圍廣泛的培訓項目，包括新兵基礎培訓、防暴警察和邊防警察等專業單位的高級課程，以及高級軍官的領導力發展項目，該學院還通過其國際培訓部為來自其他國家的警官提供培訓課程。

該學院擁有占地23公頃的廣闊校園，且由一系列獨特且最先進的培訓設施組成，包括射擊場、射擊模擬器、動物訓練設施、健身房和舉重室、教室、遺產中心等，該

學院甚至還有一個研發部門，致力於改進警務技術。

學院裡的訓練人員引導我們進入射擊模擬的設施中，在其中學員可以在射擊模擬的各種情境中學習到經驗，印象最深刻的是訓練人員跟我們展示了酒醉的丈夫持槍威脅妻兒的情境，並且為了增加互動，讓兩位參觀者擔任警察的角色，透過與丈夫的對話不同也會導致不同的結果，警察手中的槍支在對著投影布幕射擊後若順利射中丈夫，那麼他手中的槍也不會擊發射死妻子，但若是射不中丈夫反而會刺激他直接開槍射死妻子，另外如果學員透過對話與丈夫交涉順利，也會有讓他棄槍投降的場景，可以了解這種結合模擬實境的射擊訓練模式，藉由模擬實境的場景，讓學員學習現場突發狀況中的臨場反應。

另外在其他展區，訓練人員向我們展示了以色列警方會使用的各種機動車輛，像是鎮暴水車、通訊指揮車、押解犯人的警車、國道專用警車、重型機車等，最後主辦單位讓我們參觀者集中於一個廣場中，並展示了各種情境，讓參觀者了解以色列警方如何透過現代科技與警察結合，處理各種緊急狀況：

- 首先第一個情境是一群抗議群眾與警方對峙的場景，在對峙的過程中，警方一直透過空中的四軸飛行器掌握整體狀況，並透過騎乘馬匹的警察以及鎮暴水車去沖散、壓制人群。

圖29、情境示意圖

• 第二個情境的演示是警察帶著警犬在市場中尋找可疑的嫌疑犯，鎖定特定人士後，警犬就會先衝上前攻擊，隨後警察跟上壓制嫌疑犯。

圖30、情境示意圖

• 第三個情境演示了一群嫌犯挾持了一輛巴士，警方很快地就讓巴士停下，並進入巴士將所有嫌犯控制並帶出，警方持續透過儀器檢查巴士中是否存在有爆裂物。

圖31、情境示意圖

• 第四個情境演示了警察接獲通報，據稱在超市的角落有一個疑似爆裂物的物品，警方進入超市並緊急疏散群眾並確保這個區域已經被清空後，警方隨即派出一台配備有槍枝的履帶機器人，這個機器人也有移除爆裂物的能力，接著警方將一隻警犬與履帶機器人連接起來，履帶機器人就在後面跟著警犬的方向移動，警犬會配合尋找爆裂物的位置，警犬和機器人的身上配有攝影機，全程都可以清楚看到他們的移動方向，當靠近爆裂物時，綁在機器人上的警犬繩子會被自動解開，警犬會繼

續更精確地尋找爆裂物，要是找到了它就會在原地坐下，接著離開讓機器人去進行拆除。

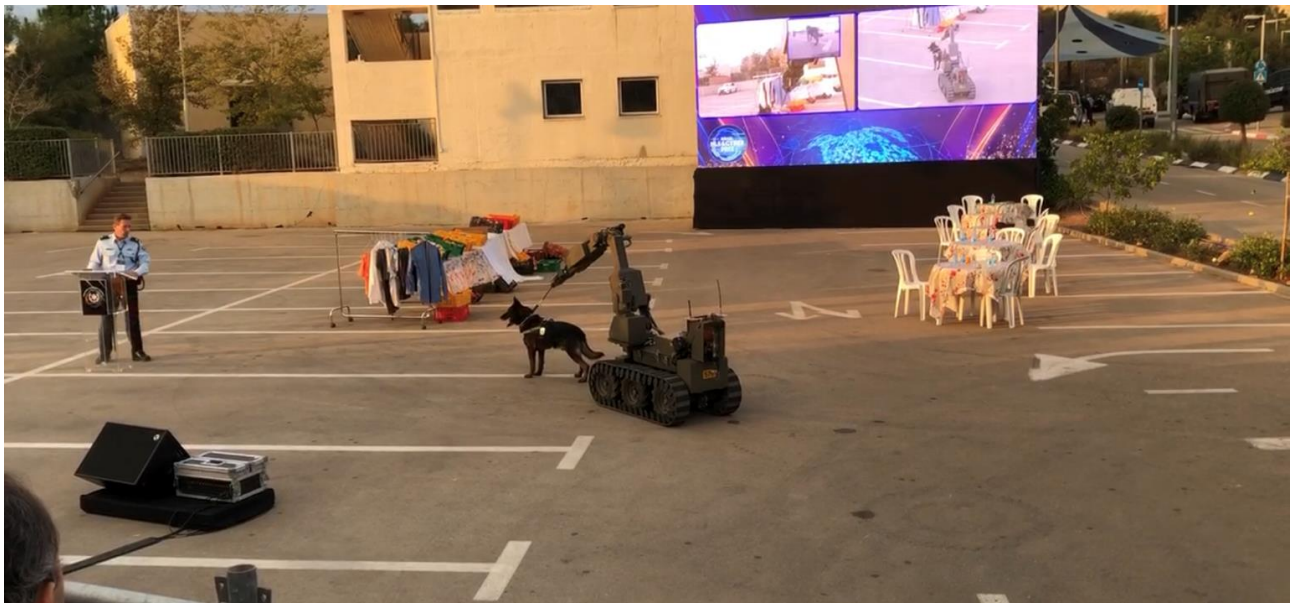


圖32、情境示意圖

• 第五個情境演示了警方透過直昇機，直接派遣警察進入恐怖份子控制的建築物中，直昇機上配備了一個狙擊手，同時地面及頂樓上也各有一組警察準備進入建築物，建築物的360度都已經被警察包圍了，接著當信號響起，所有警察就一口氣衝進建築物，並在盾牌和頭盔上配備了閃光的手電筒以及使用煙霧彈，讓建築物中的恐怖分子在還沒來的及搞清楚狀況的情況下就被制伏。

圖33、情境示意圖

圖34、情境示意圖

肆、 參訪內容摘述

拜會企業

一、11月28日下午：拜會以色列IVIX

現階段本中心實作之AI主題仍以內部資料為主要分析範圍，而現今網路時代，許多線上經濟並無法單純以內部資料進行分析並查核，而外部資料資料量極度龐大，若需由查核人員逐筆進行查核將會大量花費時間，因此可找尋明確目標，並大量且快速蒐集資訊的工具在未來會愈發重要。IVIX為一家AI公司，該公司平台提供強大的公開平台資料蒐集功能，並可以根據客戶需求客製化平台功能。在功能展示部分，IVIX展示了該平台幾項重要功能:

功能一:找出誰該繳稅:藉由網路上公開資訊交互比較，找出真正需繳稅之自然人(此次展示以airbnb為例，將網站上的房東姓名、房東照片與社交網站上個人專業資訊進行交叉比對，並於最後找出該房東真實姓名)

功能二:推估收入:藉由網站上提供之資訊，推估營業人可以有多少收入(此次展示同樣以airbnb為例，該平台將自動去搜尋該房源何時已出租，並藉由試點擊訂房按鈕得知該房源每晚租金，並藉由上述兩點資訊(已出租日期、每晚租金)推估營業人收入)

該平台除提供公開資訊蒐集外，也將所蒐集資訊整理成對查審人員更有幫助、更簡潔的資訊，也能同時解決不知道該查核誰的困境，在未來線上電商平台必定會蓬勃發展的情況下，此類型的輔助工具可以幫查核人員更有效的掌握稅基。

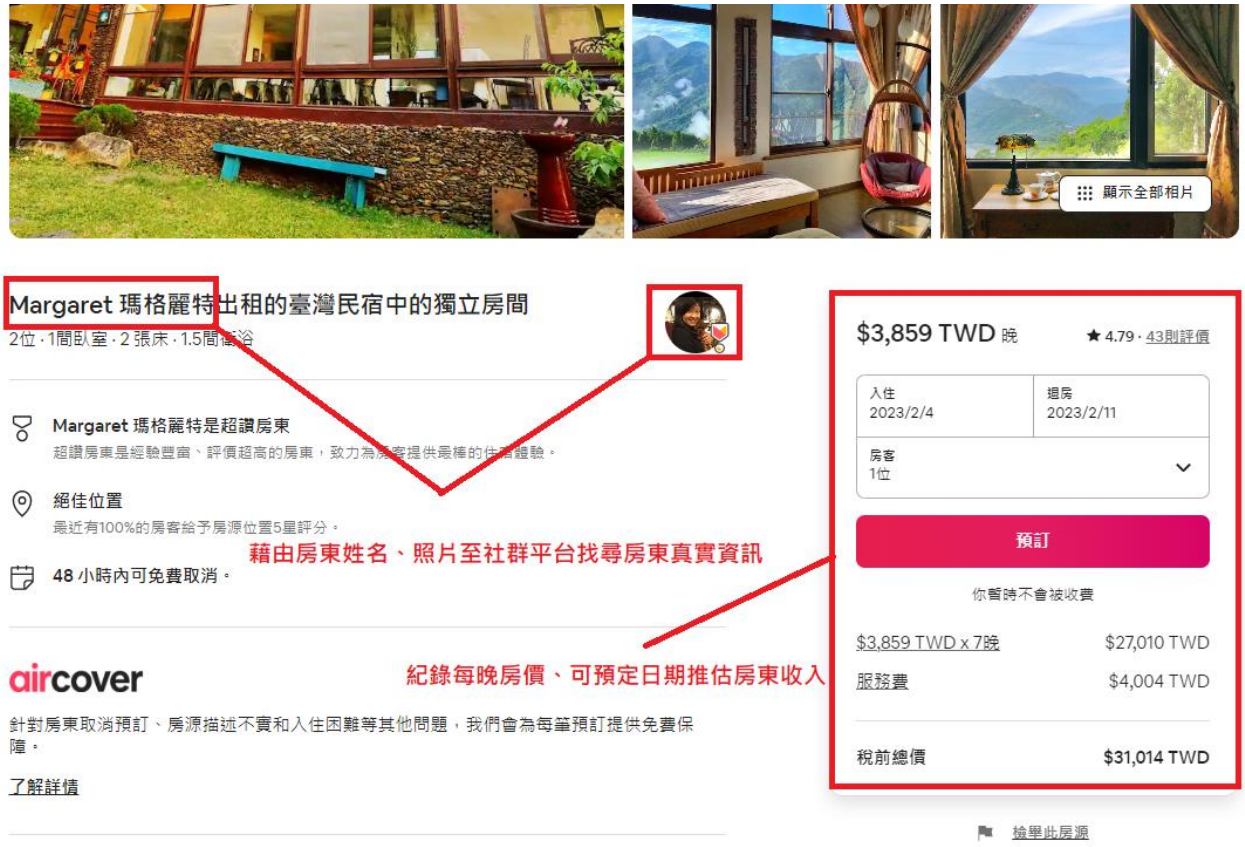


圖35、示意圖

由上述之展示結果，我們可以發現現階段網路上的交易並不容易被量化的紀錄，也因為資料到處分散，不易藉由人工比對等特性導致稅基流失，而網路上的資訊可以依靠越來越智慧化的工具及平台幫助查審人員蒐集、彙整、比對資料，並將已經具有相當資訊量的資訊提供查審人員進行後續查審作業。

圖36、與IVIX人員合影

二、11月30日下午：拜會以色列Digital.ai

圖37、與Digital.ai人員合影

Digital.ai是一家行業領先的科技公司，致力於幫助全球5000強企業實現數字化轉型目標。公司通過在整個軟件交付和開發生命週期中統一、保護和生成預測性見解，使技術驅動型企業能夠加速數字化轉型。

Digital.ai平台讓您建置安全軟體，並透過全面監控與即時反應，維護軟體安全性：

1. 防護：在程式編譯慣階段使用模組進行程式碼加密與混淆，可使應用程式更加安全。藉由簡單的設定模組「安全防護藍圖」，可提供應用程式客製化不同的防禦與使用情境。而透過模組防禦後的應用程式，每次防禦後的內容皆為獨一無二的可執行程式碼。

2. 監控：受到模組安全防護的應用程式，將內建自動通報與告警機制，這些安全機制使你瞭解應用程式是否正在遭受攻擊或處於不安全的環境，以及這些事件發生的時間與內容，且每當應用程式碼遭到逆向工程或程式變更時，都會收到通知。

3. 即時反應：透過模組即時反應措施可進行主動防禦與告警，並藉此阻撓駭客攻擊事件並停止其惡意行為，這些反應措施包括在應用程式運作之前強制執行身份驗證或客製化反應動作。

4. 保護在手機、網站、桌面和伺服器上的應用程式：無論將應用程式部署在手機、網站、桌面與主機，Digital.ai皆能夠幫助您建置更安全的軟體，讓應用程式持續受到保護。

本次見面詢問產品相關問題，得到回覆如下：

1. 產品在程式編譯階段進行程式碼加密與混淆，所需額外花費的時間多在此階段，使用者執行階段較無感，不影響程式執行時的效率。

2. 雖然執行時的監控需額外的成本，但遠低於程式被破解的損失。產品若在無網路的環境遭到逆向工程或變更，當程式執行時仍可透過監控而發現。

3. 駭客攻擊攻擊的手法日新月異，該公司有研發部門，每年投入大量資源，不斷精進產品，提升安全防護。

三、12月1日上午：參訪以色列Radware

圖38、與Radware人員合影

Radware(NASDAQ：RDWR)成立於1996年5月，公司總部設立於以色列台拉維夫，在全球40多個國家設立辦事處與分公司，為雲端和軟體定義的資料中心提供網路安全和雲端應用交付的供應商。

面對未知的網路攻擊行為時，Radware的DefensePro提供了自動化的解決方案，可

以自動分析攻擊的特性並產生相對應的防護措施，這是一般傳統IPS所無法提供的功能，透過行為模式分析引擎(Behavioral APSolute Immunity Engine)自動針對未知的攻擊即時產生防禦特徵碼(Signature)，完全不需要人為的介入，就可以在造成危害前阻擋零時差攻擊，最快能於18秒內自動產生特徵碼，達到防禦零時差攻擊的目的。DefensePro可以迅速且精確地辨識以下3種使用者行為，以大幅地降低誤判率：

1.合法的使用者流量。

2.攻擊流量。

3. 合法行為的不正常流量。

另外DefensePro也可以防護分散式阻絕服務攻擊(DDoS Attack)，因為不是單純以限制流量瓶頸(bottleneck)的方式，阻斷攻擊的同時並不會影響合法使用者的流量，所以在遭受攻擊的情況下，重要的網路服務依舊可以維持運作，提高應用程式的可用性。

另外，DefensePro亦可配置在各種網路拓撲中，與其他安全解決方案集成，例如負載平衡器和內容交付網路，以提供針對網路威脅的分層防禦。

除了零時差攻擊，常見的分散式阻絕服務攻擊(DDoS Attack)、應用層攻擊、VoIP服務濫用、SSL攻擊等也都可以即時進行防護。

另外，Radware的APSolute Vision是Radware應用程式交付和應用安全解決方案系列的網路管理和監控工具，APSolute Vision可以提供一個管理平台介面，可以集中監控和管理單位整個網路，它從一個中央統一的控制台（即使有多個資料中心）提供對單位整體範圍應用程式交付以及網路和應用程式安全基礎設施的健康狀況、即時狀態、性能和安全性的即時可見性。Vision Analytics模組也提供了一個直觀、可客製化的GUI對應用程式的效能、DoS和Web應用程式攻擊有精細的取證洞察力。

Radware的產品主要是快速減輕傷害的方式，在處理新型態攻擊，產生阻擋防禦特徵碼時，並不是完全地解決問題，而是儘可能地在短時間內最大化減少新型態攻擊對企業所造成的損失，讓服務使用者感受到最小的限制及不便。

四、12月1日上午：參訪以色列Checkmarx

圖39、與Checkmarx人員合影

Checkmarx是一家以色列源碼安全檢測廠商，總部位在以色列特拉維夫。隨著全球企業機構往現代軟體開發方法改進，將包含現代軟體功能的Checkmarx軟體資安平台應用於軟體開發環境，是保障應用程式符合安全的第一步。此外，Checkmarx平台亦能確保應用程式不會出現其他資安與品質問題，避免嚴重資料外洩或不當應用敏感資料等災難。

Checkmarx奠定軟體資安的根本基礎：與軟體開發整合且完美嵌入部門的整體持續整合與持續部署，包辦從未編譯的程式碼到執行期間錯誤的所有檢測。Checkmarx完整性平台堅持對速度與靈敏的要求，將資安導入現代軟體開發的每一步，重新定義開發商的專業水準。

產品特點如下：

1. 從源頭降低弱點：安全程式開發教育訓練，建立安全程式開發習慣。
2. 簡易好上手：安全程式開發教育訓練，建立安全程式開發習慣。
3. 快速修復時程：圖形化顯示弱點路徑及「最佳修復點」，可迅速修復弱點。
4. 支援範圍廣：支援常見程式語言包含手機APP。

5.整合性高：可與版控整合，提升開發人員工作效率。

6.方便管理：清楚呈現各系統安全狀況。

伍、心得與建議

經過這幾天密集會議內容及參訪拜會之洗禮，覺得收穫頗豐，僅將所獲得來自講者分享或受訪廠商簡報所提內容之外顯經驗知識，內化為我們的心得與知識，以下將所獲心得與知識結合本中心實務業務作業環境，摘要略述或可供本中心參考採行之建議如下：

一、 培育專業人才刻不容緩

最令我們印象深刻的是，不管是於會上講者或甚至是所參訪之資安科技大廠處長都提及，現在資訊/資安專業人才嚴重短缺，進行規劃設計資訊安全防護機制的人員自身的資訊安全素養不足，規劃或所提建議之解決方案本身就存在相關資訊安全漏洞，在這樣的條件下會讓整個組織，甚至國家面臨嚴重的資安威脅及危機，畢竟「資安即國安」是現在不容否認的事實，因此，本中心在資訊/資安人才的養成上(不管是實務操作演練或理論基礎的了解)，更應投入相當資源，如，ISO27001於2022年10月改版，本中心應該籌設開立相關課程教育訓練中心同仁，這些課程資源的分配也要稍微注重均平，特別是資訊安全的水桶理論隨時警示著我們：資訊安全人人有責，且本中心有輪調機制，應該每位同仁都要有這些國際標準與制度的認識，預算經費許可下，或可開放予全體同仁參與。

研討會講者亦提及美國為了防止技術人才跳槽到私人企業，提供許多激勵措施並大量投資識別網路加密貨幣交易及網路犯罪的認證技術，還聘請大量資料科學家、擁抱最新技術等，我們要同仁有競爭力又能留得住人才，就必須要捨得投資教育資源於同仁身上，畢竟要馬兒好就不要讓馬兒餓到。

二、 跨單位、跨機關合作

他山之石可以攻錯，於研討會講者的分享中亦多次提及，不同國家因文化背景不同，在關鍵基礎設施上各有獨特性，並有些許差異，但仍有部分相同處，有關維持鍵基礎設施的安全，這些經驗必須共享，可參考其他國家成功的經驗，並將本身的經驗分享出去。在研討會期間本中心的與會代表於會場中巧遇法務部調查局的出席代表，言談間了解，大家對資訊安全的重視程度相當，且均希望藉由學習他國之長來增進自身功力，讓機關的資訊安全防禦能力更強化，能萬事防範於未然讓災害損失降至最低，相信2022年度成立之數位發展部應該也有相同期許，或許可以藉由不同機關間相互交流，如：定期舉辦跨機關研討會議，來切磋了解新技術可以如何應用於實務防禦上，或許更能發揮一加一大於二的效果與效用。

三、 新系統推出之前，預先考量使用者抗拒或影響配套

研討會講者曾提及當新技術進入人類生活的開始，會因為決策者之「樂觀」與「保守」態度而決定是否採行該等新技術，如何平衡這兩種態度變成是未來會持續發生、會更需要溝通的課題。講者亦提及身為新科技的發明者，更有義務去消除社會對於未知的恐懼，藉由提供充足的資訊，跟社會大眾解釋新科技的應用，並與立法者溝通，建立一個可以帶給人類方便，但又不侵害人權的雙贏局面。

考量本中心執掌所面對的利害關係者，包括稅務同仁與民眾兩大群體，當我們在推出新的資訊系統供其使用前，即應預為想像並規劃配套之因應措施，如面對民眾部分：推出手機報稅便民措施前，即先對行動報稅所涉之資訊安全議題，進行防護強化、製作廣宣品/說明文件讓民眾安心使用該措施，不用擔心因為使用該措施而遭致資安風險或威脅。這部分本中心在110年首次推出時，已予考慮並實作，成效亦不斐。

未來在面對稅務同仁部分，本中心亦將面臨許多挑戰，時值國稅資訊作業平台、地方稅資訊作業平台之重新再造之際，在稅務同仁已習慣所使用之系統操作畫面、功能、流程之條件下，如何降低其面對新平台作業環境之抗拒，是我們所需先予規劃考量的，如：於規劃之初即邀集相關利害關係者的投入、事前辦理相關的教育訓練、提供友善易懂的操作手冊等等，均是可考量的措施之一。

另外，對於像引進AI模式協助稅務查審、機器人自動化工具(RPA)的導入開發應用等，亦都需要事前對稅務同仁進行教育訓練，讓他們體會到這些工具或作業流程的導入，確實未來能協助其工作效率的提升，而非額外增加其工作量，此部分本中心在近2年與五地區國稅局的跨機關合作試辦分階段導入RPA應用時，已予考慮並實作，成效不斐，將來稅務查審AI模式工具的導入，或亦可按此模式進行，讓五地區國稅局同仁隨著本中心同仁一同成長。

四、 引進能增進同仁工作效率工具的必要

本中心近年受到人才流失與所使用之既有工具無法滿足實務需求之困擾，在本次會議中講者曾提及，過去只能依照當下所獲得的片面資訊加上過往的經驗，做出相對比較妥當的決策，但隨著科技產品的進步，我們開始可以運用新技術進行資訊蒐集，進一步輔助決策，甚至達成24小時監控及預警，除了減少受災程度外，更開始可以達成避免災害發生的好處，這讓我們想到是否可以藉由這樣的過往數據比對，來協助我們資訊操作人力的解省，如：引進相關AI即時自動比對過往數據與當下資

訊，若發現數據模式不同以往，即發送預警告知機房操作人員或網路管理人員，這樣當這些年長之機房操作人員退休後，在遇缺不補的情況下，我們可以藉由此類新工具讓日常監控作業不致因人力減少而造成威脅。

又，現行電子發票平台為防護分散式阻絕服務攻擊(DDoS Attack)，係採行以限制流量瓶頸(bottleneck)的方式阻斷攻擊，此方式在遭受攻擊的情況下，會影響合法使用者的流量，未來或許可以再多方蒐集不同廠商之解決方案，考量引進新工具或方法，看是否能在遭受攻擊或流量大於原先系統規劃之容量情況下，重要的網路服務依舊可以維持運作，合法使用者的流量不至受到過多影響，提高應用程式的可用性。

另，現行本中心隨著行動化、智慧化的要求，所使用之開發軟體環境多樣，後端配套的管理工具與所需管理人力亦呈倍數成長，因此，似有必要重新檢視我們所採用的開發工具、軟體品質檢測工具等，看是否足以因應目前環境所需，若不足，或可藉由資訊作業平台再造之際，蒐集不同廠商之解決方案，採購相關的輔助工具供使用，如：能協助同仁在進行程式編撰過程中能邊做邊學以製作安全程式碼的輔助工具等。

五、 讀萬卷書亦得搭配行萬里路

本次公務出差為相當難得的經驗，除了參加研討會學習到資訊及資安新知識，並參訪當地資訊公司，在工程師的介紹下了解到各種資訊產品的實際操作與資訊，最難得的是體驗了不同國家的文化差異。該國因宗教信仰，當地餐飲幾乎無豬肉，另每周五傍晚至周六為安息日，除大部分餐廳皆休息，連大眾運輸也停駛。另因特殊的國家環境全民皆兵，兵役期間不僅做體能及軍事上的訓練，部分士兵也能學習到專業知識，對於出社會後有相當幫助，造就非常多的新創公司，兵役期間未與社會脫節。由本次的文化洗禮，讓我們體會到我們除了要注重專業知識外，多到世界各地走走，除能增廣見聞學著融入當地文化外，也能觸發更多身、心、靈之成長，另外平時亦要多運動培養良好體能，才能對國家做出更大的貢獻。

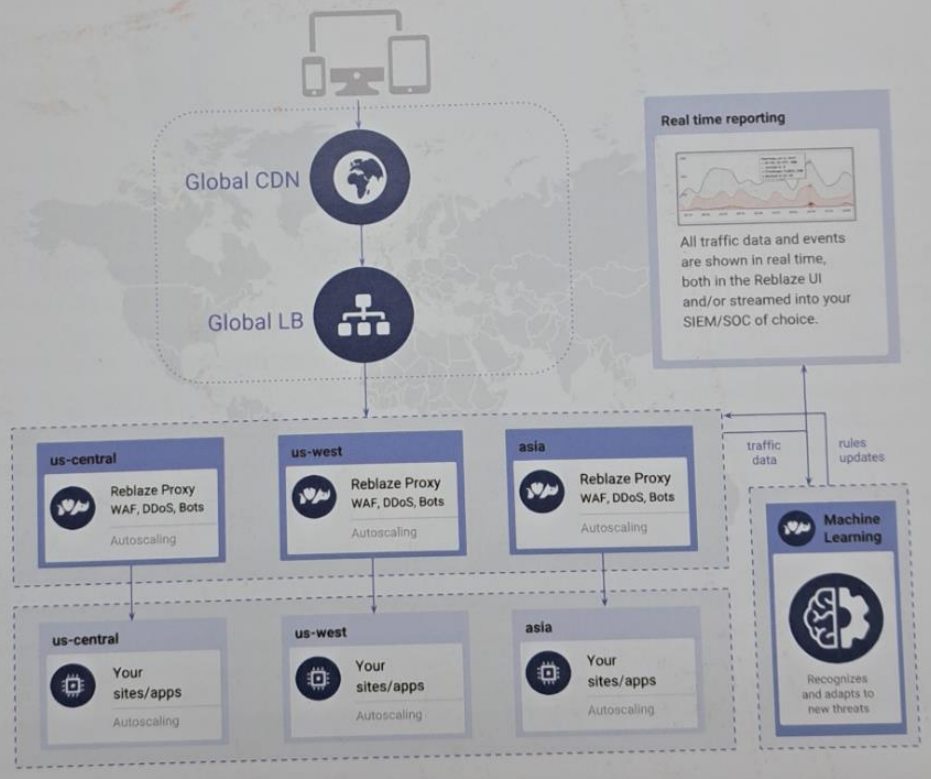
陸、參考資料

Reblaze | Web Application & API Security

COMPREHENSIVE CLOUD-BASED SECURITY

Reblaze Technologies offers an all-in-one web security platform. It includes a next-gen WAF, full-scope autoscaling DoS/DDoS protection, advanced bot management, real-time traffic monitoring & control, and more. Reblaze is fully integrated with the top-tier public cloud providers (AWS, Azure, and GCP), and runs on the customer's clouds of choice.

The platform is designed around a no-compromise approach to web security. All customers enjoy comprehensive protection, without having to purchase premium tiers or subscribe to additional services. Each customer receives a dedicated Virtual Private Cloud, eliminating multi-tenancy vulnerabilities. For maximum privacy, all traffic data is processed exclusively inside the customers' clouds (many competing solutions decrypt customer data on their own servers). Multivariate threat detection, behavioral analysis, and machine learning ensure accurate, adaptive protection.



PCI DSS Certified

Reblaze's clouds are fully compliant with GDPR, SOC 2/ SSAE 16/ ISAE 3402, FISMA Moderate, ISO 27001, FIPS 140-2, HIPAA, and CSA. Reblaze Technologies is a PCI DSS Certified Level 1 Service Provider.

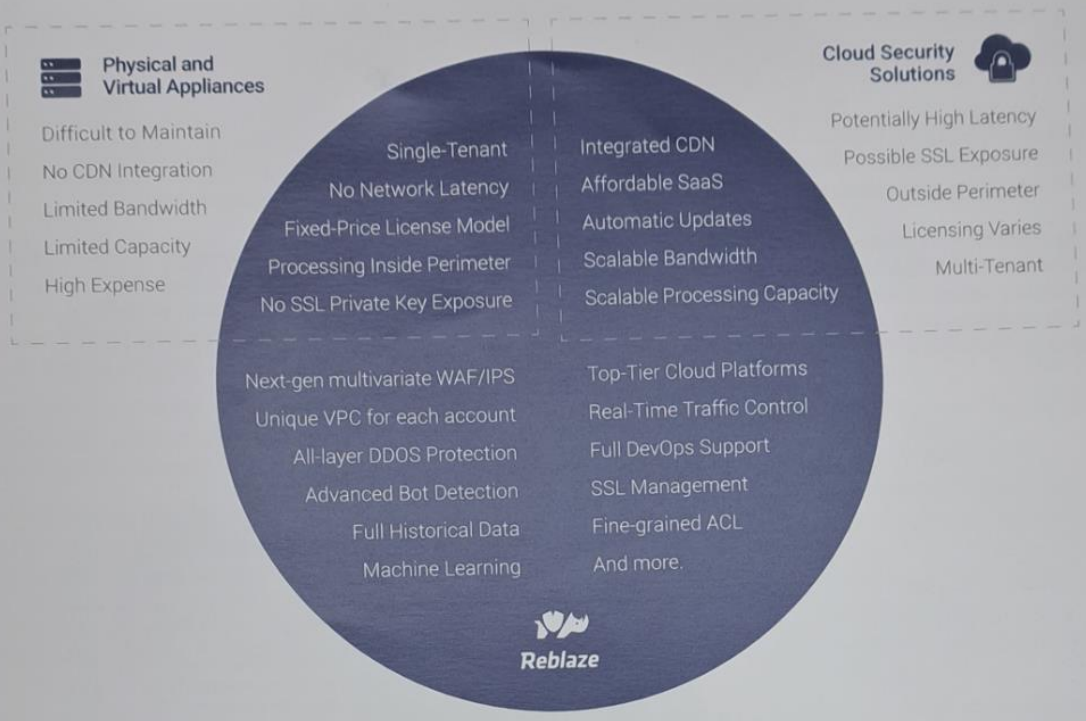
AICPA SOC | ISO 27001

reblaze.com | hello@reblaze.com | +1 (408) 907-7712

Google Cloud Partner | aws partner network | Microsoft Partner

ADVANTAGES

Reblaze provides the advantages of appliances and cloud solutions, without their drawbacks.



NEXT-GENERATION WAF/IPS

Reblaze defeats breach attempts, code and SQL injection, XSS, form manipulation, protocol exploits, session poisoning, malicious payloads, data theft, and other forms of attack.

DOS/DDOS PROTECTION

Reblaze is effective against DoS/DDoS across all layers and scales, from malformed-packet DoS attempts to massive DDoS assaults.

BOT MANAGEMENT

Industry-leading bot management prevents data theft, scraping, credential stuffing, dictionary attacks, vulnerability scans, & more.

REAL TIME TRAFFIC CONTROL

Real-time traffic sniffing (including Layer 7) provides full statistics and visibility of **all** requests, even during large-scale attacks.

MACHINE INTELLIGENCE

Reblaze continually analyzes global traffic data, using machine learning for accurate, dynamic threat detection. Even as new attack vectors arise, Reblaze adapts & hardens itself against them.

FULLY MANAGED SAAS

The platform is maintained remotely 24/7 by Reblaze personnel. Your web security is always up-to-date, and always effective.

CDN, LOAD BALANCING, AND AUTOSCALING

These accelerate your web apps' responsiveness to your users. Resources scale automatically, with no pre-warming required.

DEEP TRAFFIC ANALYSIS

Full traffic logs and statistics enable understanding of security events, user behavioral patterns, application anomalies, and more.

reblaze.com | hello@reblaze.com | +1 (408) 907-7712

Google Cloud Partner aws partner network Microsoft Partner

COBWEBS
TECHNOLOGIES

Web Intelligence for a Safer World

Cobwebs Technologies is a global leader in AI-Powered Open-Source Intelligence (OSINT). Our mission is to protect global communities and organizations from crime, threats, and cyber-attacks, by providing seamless access to publicly available data.

Discover Target Information

Complete Automation

Identify Locations

Reveal Connections

Gain Situational Awareness

Real-Time Alerts

Key Features

- Monitoring and analysis of open, deep dark web and upload files to connect data points
- Transform a single lead into a comprehensive in-depth and clear report of the threat
- Live analysis of structured and unstructured data providing automated real-time alerts
- Harness big data with streamlined artificial intelligence to provide automated insights

Product Portfolio

Designed for investigators and tailored for their operational requirements, Cobwebs provides an enhanced yet user-friendly solution. Our award-winning technologies are tailored to solve complex real-world challenges and to produce valuable insights from oceans of big data. Our solutions are integrated into advanced and secured cloud infrastructure.

AICPA SOC 2

Investigation Platform

Location Analysis

Financial Investigation

Secured Analyst

www.cobwebs.com | info@cobwebs.com