出國報告（出國類別：其他）

「新加坡(SICW)資安週參展計畫」
出 國 報 告

服務機關：經濟部工業局
姓名職稱：林青嶔科長
派赴國家：新加坡
出國期間：107 年 9 月 17 日至 9 月 20 日
報告日期：107 年 11 月

摘要

為加速國內資安廠商交流與國際合作，本局率團參加新加坡 SICW 資安週活動，透過臺灣資安館之整體品牌形象設計，形塑臺灣資安產品形象，並推廣我國資安政策至海外，以呈現我國資安自主研發與服務之創新能量。

新加坡國際資安週 (SICW, Singapore International Cyber Week) 是由新加坡國家網路安全局 (CSA) 以國家力量支持之資安活動，今年主題為「 Forging a Trusted and Open Cyberspace 」，以邁向一個可信賴並開放的網路環境作為年度推動重點，今年開幕致詞為新加坡副總理張志賢。

新加坡為自由貿易的外銷導向國家，加上其市場穩定、語言多元、投資環境佳、且地理位置與東南亞各國相近等因素。因此，藉由參與本次活動，亦可做為連結新南向市場之最佳跳板。在本次率團參展與參訪過程中，除了累積國內業者國際市場拓展及溝通經驗，也從新加坡面對東協資安產業的政策與經驗中，討論臺灣資安產業國際市場推動方向。

目 錄

圖目錄

表目錄

壹、出國目的

一、前言：

第三屆新加坡國際網路安全週（Singapore International Cyber Week, SICW）是由新加坡政府舉辦，也是新加坡政府及國家網路安全局(CSA)全年唯一支持之資安活動，每年以國家資安作為主題，SICW 邀請各國資安政策決策者及相關業者與會，透過多項展覽、論壇等交流活動促進網路安全技術與解決方案之交流，吸引超過 8 千名參觀者。

今年 SICW 開幕儀式，由新加坡副總理兼國家安全協調部長張至賢代表致詞，說明東南亞整體資安產業發展環境、新加坡對資安產業政策方向，在 SICW 會議同期還舉辦資安相關會議及展覽：

(一) 東協網路安全部長級會議（ASEAN Ministerial Conference on Cybersecurity, AMCC）

(二) 政府軟體（GovWare）展覽和會議：全球超過 250 家資安業者參與

(三) 2018 年全球網路專業論壇年會

(四) 全球穩定委員會聽證會網路空間

(五) 第六屆國際刑警組織與歐洲刑警組織網路犯罪會議

(六) 東協網路犯罪檢察官圓桌會議

新加坡面積、人口、資源與臺灣相對少，在二十多年前與臺灣同屬於亞洲四小龍，歷經幾次數位與資訊化轉型，帶動國家整體競爭力的提升。如今，新加坡可看到未來 10 年資安發展在東南亞區域之重要性，其資安產業發展戰略係以東協地區為目標市場，從產業國際化策略、人才及新創育成、到新興技術交流。面對全球化的網路威脅，新加坡從 2016 年起，將資安重要性從國家層級提升到東協區域跨國政府、產業與學界的合作。新加坡政府對資

安產業的扶植，無論是人才培育、關鍵技術研發、新創企業栽培，逐漸使新加坡資安產業擁有在全球市場競爭實力。臺灣正值資通安全產業推動發展之際，尤其是推動產業國際輸出，新加坡在資安產業、政府部門都是臺灣學習的標竿，各項務實措施得以作為後續我國資安技術深化與產業推動的參考依據。

本次出國透過帶領國內資安廠商參加「新加坡 SICW 資安週」之論壇及展會活動，除了瞭解新加坡資安產業發展情形、最新資安技術與趨勢資訊；同時，輔導國內業者參加國際展覽活動與安排國際商談媒合，協助國內資安廠商拓展海外市場契機。

二、目的：

(一)聚集臺灣資安業者，形塑整體品牌形象：

SICW 年度吸引全球超過八千名資安領域重要決策人士參與，是國際上資安產業重要舞台，本次出國整合國內 12 家資安業者解決方案，聚焦國內業者自主研發的解決方案，系統性地在國際間展出臺灣資安產業與環境的形象，呈現與展示臺灣產業在資訊安全領域的自主研發及服務解決方案之能量。

(二)推動業者國際合作，加速海外市場拓銷：

配合新加坡國內年度最大資安盛事，與法人共同帶領國內資安業者藉由國際會展機會，拜訪國際大廠，積極地參與各項商談會、展覽、跨國交流活動，將臺灣業者的資安廣宣型錄、宣傳影片、介紹資料傳遞給國外潛在客戶，並協助本土業者對國外買家進行拓銷。

(三)借鏡國外經驗，發展新興資安關鍵技術：

關鍵基礎設施之資安防護逐年受到重視，雖然大多系統都宣稱封閉，

然而隨著數位化與物聯網的時代來臨，當這些系統被入侵時，可能會造成國家某種程度的影響，爰如何發展 OT 資安防護逐漸成為發展新興資安技術被探討之重要議題。

三、參與團員：

本次出訪人員共 35 名，包含本局 1 位、國安會代表 1 位、資策會 10 人、及 12 家國內資安參展業者 23 人。

表 1：國內資安廠商代表列表

公司名稱	產品/服務屬性	姓名	職稱
大宏數創意	Endpoint & Messaging Security	黃重道	營運長
中華資安國際	Security Operation	陳振楠	董事長
		洪進福	總經理
		陳怡如	協理
杜浦數位安全	Threat Intelligence	蔡松廷	執行長
神盾	PKI	張心玲	副總經理
捷而思	Endpoint & Messaging Security	吳建東	董事長
		林雅雯	董事長特助
竣盟科技	Security Operation	鄭加海	總經理
		鄧翠盈	客戶經理
奧義智慧	AI Security Analytics	邱銘彰	創辦人兼執行長
		吳明蔚	創辦人
		蘇鈺婷	品牌經理
		林明緯	產品經理
新思鹿	Endpoint & Messaging Security	李庚	營運長
		李民偉	資深經理
瑞擎數位	Network Security	王騰嶽	技術長
精品科技	Encryption & DLP	劉新玫	PM
		劉孝葳	PM
		陳育徽	PM

公司名稱	產品/服務屬性	姓名	職稱
歐生全科技	Authentication	黃啟峰	副總經理
戴夫寇爾	Security Assessment	翁浩正	執行長
		岑志豪	全端工程師

表 2：政府、媒體及執行團隊代表列表

單位名稱	姓名	職稱
工業局	林青嶔	科長
國安會	王仁甫	專委
資策會	于孝斌	執行長
資安所	毛敬豪	資安所所長
國際處	謝京蓓	國際處處長
國際處	連立琦	國際處組長
資安所	邱之崧	資安所組長
資安所	黃惇慧	資安所資深工程師
資安所	石美琪	資安所正規劃師
資安所	葉建綸	資安所副規劃師
資安所	李美玲	資安所工程師
資安所	蔣天儀	資安所管理師

貳、過程

一、行程表：

本次行程自 2018 年 9 月 17 日至 20 日，全程安排共 4 天 3 夜，行程內容以參加新加坡 SICW 活動(9 月 18 日至 20 日)為主，今年 SICW 活動及展覽館地點位於 Suntec Singapore Convention & Exhibition Centre。本次於展覽期間，同時安排國內業者於會場之 B2B 商機洽談會，安排國內業者共 9 家與東南亞第一大電信業者新加坡電信(SingTel)交流。另活動中，CSA (Cloud Security Alliance) 國際資安重要組織，知悉台灣政府積極力推資安產業標準，特邀臺灣相關業者，共同探討與發起全球物聯網資安標準。

另為了解新加坡關鍵基礎設施之工控資安推動情形，亦安排參訪新加坡科技設計大學(Singapore University of Technology and Design，簡稱 SUTD)，瞭解自來水廠資安控制系統研究、IoT 資安控制系統研究、電力能源控制系統研究之實驗室等。

表 3：行程表

日期	行程內容
9/17(一)	上午：07:40 臺北桃園 搭長榮 BR225 12:00 抵達新加坡
9 /18 (二)	全天：參加新加坡資安週 Cyber Week 2018 論壇及展覽
9 /19 (三)	全天：參加新加坡資安週 Cyber Week 2018 論壇及展覽 上午：接待梁國新大使蒞館參觀、拜會新加坡科技設計大學 下午：與新加坡電信舉辦 B2B 商談會
9 /20 (四)	上午：參加新加坡資安週 Cyber Week 2018 論壇及展覽 下午：15:10 新加坡搭乘長榮航空 BR216 20:00 抵達臺北

二、參訪活動及拜會情形：

(一) SICW 大會論壇整理：

1. 副總理**張志賢**主席致詞：**新加坡**推動**資安產業**重點**策略**

今年 SICW 年度主題為「Forging a Trusted and Open Cyberspace」，以邁向一個可信賴、開放的網路環境作為年度推動重點。並強調**如何連結民間資安業者技術以強化政府資安體質、新加坡對資安產業政策與其在東協產業的角色定位**，其致詞內容重點包括：

(1) 結合民間技術以強化政府資安能力(**Government Bug Bounty Program**)：藉由**舉辦國際競賽**、提供優厚**獎勵誘因**，吸引新加坡與國際間的白帽駭客參與，針對特定及政府網路系統進行**測試攻擊**，透過頂尖駭客的偵測，同時評估測試相關的防禦技術，找出**政府**部門網站的**漏洞**，並作為後續政府改善的基礎，以達到 Smart Nation 的願景。

(2) 東協國家高速成長力道將帶動資安強烈需求：東協十國的人口有 **6.3 億**，雖然不如整個歐盟地區或中國大陸，但卻是全球經濟成長速度最快的地區之一。更重要的是，東協人口平均年齡比歐盟年輕 10 歲以上，人口紅利所帶動的快速經濟成長，為東協地區每年新增加百萬的中產階級。在全球分工下，東協整體產業在物聯網、工業 4.0 的發展速度尤其重要，當製造業邁向物聯網、工業 4.0 發展，製造生產機台、生產數據可以連網帶來即時分析、決策便利，但也潛藏資料曝光風險，對於資安需求等級也相對提昇，需求也更高。在2016年新加坡政府就已經投入1千萬美金推出東協網路安全能力提升計畫（**ASEAN Cyber Capacity Program, ACCP**），結合**政府**、**產業**、**學界**力量，深化**區域網路能力**及因應網路安全威脅的能力。新加坡未來會將

計畫層級提升到「東協與新加坡網路安全卓越中心」（**ASEAN-Singapore Cybersecurity Centre of Excellence, ASCCE**），加速成員國間資安訊息交流及分享的能力。

(3) **輔導資安新創**企業以強化產業價值鏈：隨著駭客攻擊手法創新，防禦方式也必須不斷創新，以產生創新解決方案和新創公司成長機會，這些創新解決方案與新創公司是帶動產業成長的動力。在2018年3月**新加坡電信**所投資的創投公司 **Singtel Innov8**、**新加坡大學**、**英國倫敦資安加速器**業者 **CyLon** 合作設立第一個以推動「**網路安全新創公司**」的資安創業育成中心-「**資安創新生態 71 區**」（Innovation Cybersecurity Ecosystem Block 71, ICE 71），以輔導資安新創業者透過該平台發展創新解決方案。

2. SICW 大會論壇整理：

2018 SICW 大會論壇活動主軸為 GovernmentWare (GovWare)，邀請全球各國之產官學研等高層、資安專家與會，參加包括今年資安年會、研討會及廠商展覽。2018 GovWare 主題共有 13 個：

(1) BIG DATA ANALYTICS & DEEP MACHINE LEARNING
(2) CYBER OPERATIONS & RESPONSE
(3) CYBER THREAT LANDSCAPE & INTELLIGENCE
(4) CYBERSECURITY IN THE CLOUD
(5) CYBERSECURITY OPS CENTRE: METHODOLOGIES & OPERATIONS
(6) DARKWEB, CYBERCRIME, CYBERWARFARE
(7) EMERGING SECURITY TECHNOLOGY
(8) ENTERPRISE SECURITY & DATA PROTECTION: TRENDS & TECHNOLOGY
(9) INTERNET OF THINGS (IOT) SECURITY
(10) PROACTIVE CYBER DEFENCE

(11) PRACTICAL PERSPECTIVES AND INSIGHTS FROM REAL WORLD IMPLEMENTATION IN AN END USER ENVIRONMENT

(12) SMART NATION

(13) STRENGTHENING THE RESILIENCY OF THE CYBERSPACE

表 4：SICW – GovWare 2018 Agenda –重要場次盤點

項次	日期	時間	議程名稱	主講人	主題	議題類型
1	9/18	1300 – 1340	Securing the Digital Nation to Combat Cybercrime	Christopher PETERSEN Co-Founder, Chief Product & Technology Officer Log Rhythm	Smart Nation	政策面：數位國家打擊網路犯罪議題
2	9/18	1420 – 1500	Securing the Connected Citizen & Public Sector Digital Transformation	Jonathan NGUYEN-DUY Vice President, Strategy & Analytics Fortinet	Cybersecurity Ops Centre: Methodologies & Operations	政策面：公部門數位轉型之安全議題
3	9/18	1530 - 1610	Let's Talk about Accelerating DevOps with SECURITY	Jeff WILLIAMS Co-Founder & Chief Technology Officer Contrast Security, Inc.	Enterprise Security & Data Protection: Trends & Technology	維運面：系統開發維運之安全議題掌握
4	9/18	1650 - 1730	Applying AI to Practical Cyber Security	Sean PEA Head of Threat Analysis, Asia Pacific Dark trace	Enterprise Security & Data Protection: Trends & Technology	技術面：人工智慧資安新興技術
5	9/18	1650 - 1730	Collaborating with the Attackers: An Approach to Upgrade and Validate your	Vivek CHUDGAR Managing Director FireEye	Cybersecurity Ops Centre: Methodologies & Operations	維運面：資安監控升級模式

項次	日期	時間	議程名稱	主講人	主題	議題類型
			SOC			
6	9/19	0900 - 0930	The Cancer Within: Insider-Based Cyber Attacks	Mike McCONNELL Former Director, NSA & National Intelligence Strategic Advisory Board Member Securonix	Keynote	技術面：內網攻擊議題
7	9/19	1100 - 1140	Conquering Threat Actors with Automated Incident Response and Threat Intelligence	Richard SOROSINA Director of Solutions Architecture and Sales Engineering Log Rhythm	Cyber Threat Landscape & Intelligence	情資面：自動化事件處理與威脅情資議題
8	9/19	1600 - 1640	Best Practices in Public/Private Sector Collaboration to Fight Global Cybercrime	Jon CLAY Director, Global Threat Communications Trend Micro Inc.	Darkweb, Cybercrime, Cyberwarfare	政策面：公/私部門打擊國際網路犯罪議題
9	9/19	1600 - 1640	Levelling the Cyber Playing Field with Proactive Cyber Defense	Siang-tse FOO Chief Executive Officer Quinn Singapore	Proactive Cyber Defence	技術面：積極網路防護(新加坡本土資安公司)
10	9/20	0900 - 0930	A System Approach in Securing Critical Infrastructures	Ravinder SINGH President, Electronics ST Engineering	Keynote	人培面：安全守護關鍵基礎設施議題、資安人培合作
11	9/20	1150 - 1230	Know Your Enemy: How to Build a Proactive Cyber Threat Intelligence and Threat	Sidney PEARL Global i2 Cyber Leader IBM Security	Big Data Analytics & Deep Machine Learning	情資面：威脅情資與狩獵

項次	日期	時間	議程名稱	主講人	主題	議題類型
			Hunting Program			
12	9/20	1330 - 1410	AI Techniques for Cyber Intelligence Analytics	Prof Kwok Yan LAM Professor Nanyang Technological University	Internet of Things (IoT) Security	技術面：人工智慧資安新興技術、產學研合作推動

(二) 參加新加坡 SICW 展覽：

1. 以臺灣資安館形象整體參展：

本次參展攤位總面積 54 平方公尺(6 個標準攤位大小)，臺灣組團參展由資策會主辦，軟協、TCA 協辦，臺灣參展廠商包含，捷而思、奧義智慧、杜浦數位安全、戴夫寇爾、歐生全科技、精品科技、竣盟科技、新思鹿、泓格、大宏數創意、中華資安、瑞擎等 12 家業者參與展示。另在臺灣攤位準備了臺灣整體資安業者暨產品型錄，提供中英文內容介紹臺灣資安業者的產品/服務特色、連絡資訊。透過會展期間發放給國際潛在客戶或有興趣的業者、機構，俾利參觀者事後連繫。另於參展期間，透過商談媒合活動，以一對一商機洽談會形式，安排 9 家國內業者與新加坡電信(SingTel)交流，並洽談合作機會與主題。

圖 1：SICW 臺灣館正面與參展業者合影

2. 形塑臺灣資安品牌形象：

國內個別資安廠商規模小、國際品牌辨識度低，所以在本次帶團參展規劃中，特別在臺灣館主題牆介紹臺灣在資安法規政策、檢測標準等議題,由我國政府對資安產業政策的努力、到需求端實證、資安業者技術創新，及新興資安產品實證及能量累積，塑造臺灣資安業者具備成為全球資安監控委外服務商的能力形象，連結到業者技術發展、產業價值鏈及解決方案，主題牆說明如下：

(1) 臺灣資安法規與檢測標準：說明臺灣已制訂明確的相關資安法規與規範，並積極將產業經驗與參著國際標準轉化為各項檢測標準，並讓各國瞭解臺灣政府如何引領政策法規來帶動產業發展，如：物聯網資安標準認證驗證制度。

(2) 資安監控委外服務商(Managed Security Service Provider, MSSP)解決方案：整合我國資安廠商的解決方案，輔導公私機關行號之資安防護以符合法規標準，資安業者可透過技術服務、顧問服務，或產品銷售等形式，提供各種資安產品服務，以協助客戶應對新興資安威脅，其中，MSSP 包括了即時監控、事件反應、威脅防禦及維護等四個面項。

(3) ICS 資安解決方案：在工業 4.0 議題發酵下，企業不僅在製造層面積極轉型與升級，對於資訊安全考量上,也同步提升防護等級，以因應工廠、設備因連網後，可能受到攻擊或其他危險事件。在 ICS 資安解決方案說明中，強調臺灣資安業者有能力成為全球企業轉型升級進入工業 4.0 業者的最佳資安合作夥伴。

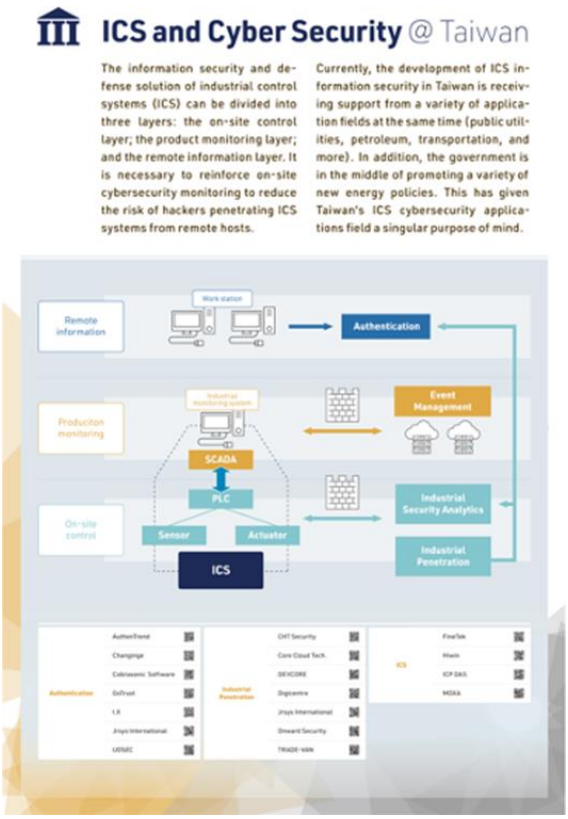

圖 2：臺灣法規、檢測標準、MSSP 解決方案說明主題牆

3. 廠商展示區：

本次共同參展的 12 家廠商於臺灣資安館分別依公司技術能量參展，由於展會前一天 9 月 17 日抵達新加坡時，獲駐星梁國新大使邀請，並向其說明臺灣資安產業發展現況、目前國家政策推動策略、國際合作的發展方向、以及選擇來新加坡參展的目的等交換意見。駐星梁大使並於 9 月 19 日公忙之餘蒞臨館臺灣資安館參觀，實際了解臺灣資安廠商的技術能量，並給予代表我國參展的資安公司予以加油打氣，並表示駐星代表處將會盡力協助臺灣資安廠商拓展商機。

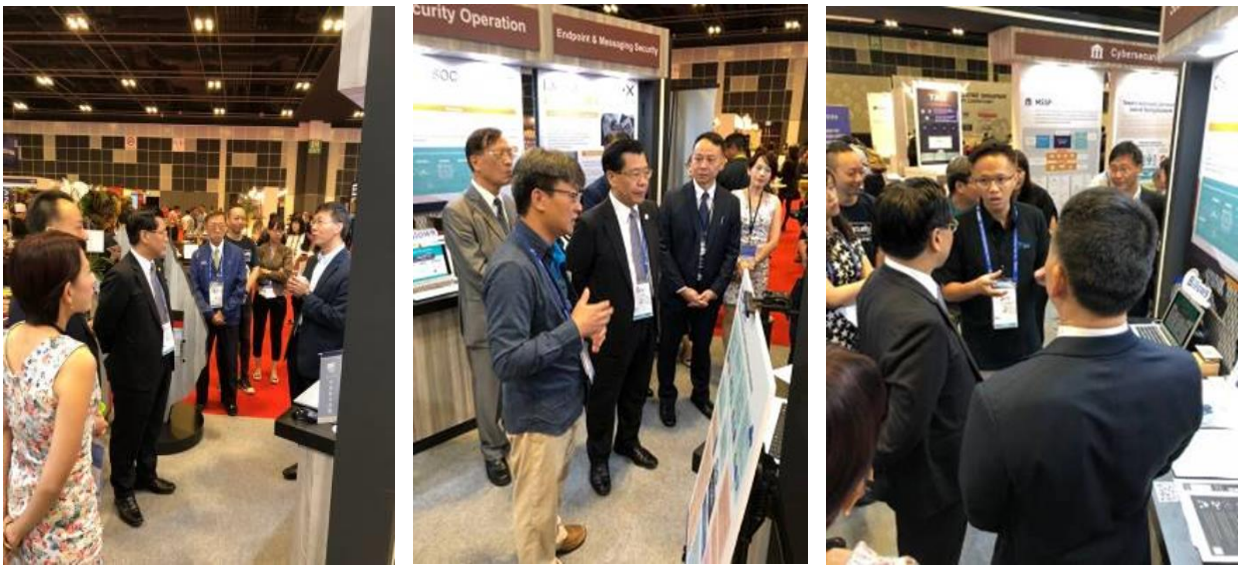

圖 3：駐星梁國新大使蒞臨 SICW 臺灣資安館

表 5：臺灣資安廠商參與展出主題

編號	廠商名稱	展出主題
1	泓格科技	ICS Security
2	歐生全	Authentication
3	新思鹿	Endpoint & Messaging Security
4	瑞擎數位	Network Security
5	中華資安國際	Security Operation
6	捷而思	Endpoint & Messaging Security
7	竣盟科技	Security Operation
8	大宏數創意	Endpoint & Messaging Security
9	精品科技	Encryption & DLP
10	奧義智慧科技	AI Security Analytics
11	戴夫寇爾	Security Assessment
12	杜浦數位	Threat Intelligence

(三) 拜會新加坡科技設計大學工控系統研究中心：

新加坡科技設計大學是世界上第一所集設計與創新於研究與工程中的大學，在 2012 年正式開學，設有工藝與永續設計、工程產品開發、工程系統與設計以及資訊系統技術與設計四個系。在專業領域上，以土木與環境工程、生產線管理以及製造工程等三個領域著名。

本次參訪新加坡設計大學的工控系統研究中心是由新加坡**國防部**及**國科會**投資成立，在工控系統研究中心下又設立測試平台(Testbed)進行技術研究及工控系統人才培訓，涵蓋領域範圍包括：**水處理廠**、**配水廠**、**電力控制系統**、**物聯網無線通訊**等。本次參訪團及主要參訪資訊說明如下：

1. **水處理廠 Secure Water Treatment(SWaT)**：自來水處理平台(Testbed)於 2015 年 3 月啟動，於此系統上建立防禦機制，針對各式模擬測試攻擊再重新做設計，藉此強化防護能力，網路部份包括分層通信網路(layered communications network)，可編程邏輯控制器(Programmable Logic Controllers，PLC)，人機界面(Human Machine Interfaces，HMI)，監控和數據採集系統 Supervisory Control and Data Acquisition (SCADA)，工作站(Workstation)以及 Historian，並由 Allen-Bradley 的 PLC 控制整個流程，水處理程序包含六個程序：Raw water supply & storage(採取原水)、Chemical dosing(添加必要的化學品)、Ultra Filtration (以超過濾系統進行過濾動作)、Dechlorinating(使用紫外燈對其進行脫氯程序)、RO(將程序 4 的水送至逆滲透系統)、RO permeate transfer，UF

backwash(使用前一項程序所產生的水清潔 UF 的膜)。

2. **配水系統 Water Distribution (WADI)**：配水系統於 2016 年 7 月啟動，由水處理平台延伸的系統，採用部份 SWaT 的反滲透液和原水（osmosis permeate and raw water）建構成一個完整的處理、儲存、分配架構。由於配水系統於實際場域中屬於跨越大面積的應用，WADI 也模擬物理攻擊的影響，例如漏水和惡意化學品注入（malicious chemical injections）。WADI 採用了與 SWaT 不同的 PLC 品牌，以便建立並驗證防禦偵測模組，有助於強化此模組的可用性及穩健性。
3. **Electric Power Intelligent Control (EPIC)**：電力和智慧控制（EPIC）屬於電網測試平台，其中涵蓋發電，傳輸，微電網與智慧家居四個階段，屬於基礎設施，主要可讓網路安全人員進行實驗，驗證評估防禦機制的有效性。
4. **Internet of Things Automatic Security Testbed (IoT)**：物聯網自動安全測試平台包括屏蔽室（shielded room）與三個不同的獨立機器執行測試，收集數據，用於進行安全取證分析。這個平台主要功能在於測試裝置的安全性和隱私性，透過模擬不同類型的測試環境與傳感器活動，並支援各種市面上常見的通信協議，如 Wi-Fi，ZigBee 和藍牙等。在這個平台所產出的成果包含物聯網設備的類型、連接能力、支援的通信協議及狀態。

5. **Training Skid**：Training Skid 提供一系列的培訓課程，讓相關人士學習並擁有基礎實作技能，其中涵蓋四大項技能課程，包括：Rockwell、National Instruments、Schneider、Siemens。

圖 4：Secure Water Treatment(SWaT) Testbed

圖 5：Electric Power Intelligent Control (EPIC)Testbed

圖 6：Internet of Things Automatic Security Testbed (IoT)

圖 1：Training Skid-Rockwell & Skid-National Instruments

(四) 與新加坡電信舉辦 B2B 商談會紀錄

新加坡電信有限公司(Singapore Telecommunications Limited, Singtel)成立於 1879 年，是一家由新加坡政府全資擁有的公司，也新加坡最大的電信公司。新加坡電信由新加坡前第一任總理李光耀的次子，現任新加坡總理李顯龍的弟弟李顯揚是 SingTel 的總裁暨首席執行官。

新加坡電信有主力產品包括無線以及互聯網平臺，包括聲訊、通訊服務，涵蓋商用以及家用兩個領域，共於 22 個國家皆設有營運機構，擁有 4 億用戶，是全世界第二十至三十大的行動電話服務商，其附屬公司包括：SingNet（網絡部門）、SingTel Digital Media、NCS 有限公司（通信工程部門）。聯營公司有新加坡郵政，在臺灣也有其投資的公司，包括：臺灣新世紀資通（sparq*速博，新電信持有 sparq*速博 24.5%股份）、天空傳媒（yam 天空）。旗下同時持有一家新創投資公司，新電投資公司(Innov8) ，其第一期基金規模已達到 2 億新幣，所投資金額，根據投資標目的不同的發展階段，投資額度以 10 萬～3,000 萬新幣(約 230 萬新

臺幣)不等。

本次參展期間同時臺灣資安業者與新加坡舉辦商談媒合活動，安排場內的一對一商機洽談會，安排國內業者共 9 家與東南亞第一大電信業者新加坡電信(SingTel)交流與合作，現場由各家廠商準備自有產品之 DM 介紹或利用投影片解說等。本次商談會洽談地點安排於展場內所租用之會議室，並選擇下午 3 點人員較少的時段，參展人潮較少之時段，並根據廠商屬性、需求分為 3 個時段與場次，以爭取更多機會與新加坡業者洽談。

- 日期：2018 年 9 月 19 日(三)下午 3:00~4:30。
- 地點：Suntec Singapore Convention & Exhibition Centre，第二洽談室。
- 對方接待人：Sintel 資安部門莊添善總監、Innov8 總監 Florence Tay。
- 議程安排：
  - 時段一(15:00-15:30)：國內媒合資安業者：捷而思、杜浦數位安全、戴夫寇爾。
  - 時段二(15:30-16:00)：國內媒合資安業者：精品科技、大宏數創意、竣盟科技。
  - 時段三(16:00-16:30)：國內媒合資安業者：歐生全科技、中華資安國際位、瑞擎數位。

參、心得與建議

一、心得：

本次參訪從參加 SICW 會議到拜訪新加坡大學、與新加坡電信業者進行 B2B 商談會，從在臺灣組團、整體形象設計、再到國際會議及商談會過程，協助臺灣資安廠商進入國際市場並爭取國外客戶訂單。從整體研討會參加、國際業者交流心得可歸納如下：

(一) **國家資訊應用能力越強、對資訊安全投資需求也越高：**網路科技越發達、攻擊事件也越來越多，在 SICW 開幕主席致詞中提到，2018 年 7 月新加坡最大的醫療保健集團 SingHealth，該集團旗下擁有 2 家三級醫院、5 家國家級專科醫院和 8 家綜合診所，SingHealth 的資訊系統就遭到駭客攻擊，駭客盜取了超過 150 萬筆患者資料與記錄，並竊取約 16 萬名患者的「門診配藥」資訊，包括新加坡總理李顯龍和少數部長。即使是新加坡過去在聯合國國際電信聯盟(U.N. International Telecommunication Union, ITU)全球網路安全指數(Global Cybersecurity Index, GCI)經常排名在前三名，也會遇到重大資安攻擊事件，這些重大事件往往一發生就是產生重大損失。各國對於資訊安全的需求伴隨著該國資訊應用能力及水準，資訊應用能力越好的國家，也潛藏較高的風險與問題。鑑於此，新加坡政策制訂單位很早就體認到「如果要彰顯發展資訊通訊科技（ICT）和數位科技的力量，就必須讓人民對網際網路信任，而落實網路安全就是讓人民信任的關鍵，網路安全問題就是國家安全層面的重要議題。」並且在 2016 年底起宣示，提撥 8%的政府 IT 預算作為資安防護預算，對於新加坡而言，已將資訊安全視為落實智慧國家政策的基礎。

(二) **新加坡的資安產業發展與推動經驗**：從這次新加坡 SICW 會議及參

訪中，發現新加坡在資安產業整體政策就是「國際化」，吸引國際人才進入新加坡、將新加坡國內資安企業帶出去。新加坡政府對內結合民間資安業者技術，力強化政府資訊安全保護；對外結合國際機構設立資安新創企業的育成中心，並且善用新加坡於東協地區的優勢地位，投入預算及資源在建立與東協國家之間的資訊安全建設。就新加坡內部而言，新加坡政府舉辦網路漏洞懸賞計畫，吸引全球「白帽駭客」入侵國防部、國民服役及中央人力局等8個網路系統，如果發現網路漏洞，白帽駭客將獲新幣150元（約新臺幣3,300元）到2萬元（約新臺幣44萬4,200元）不等的獎金，透過這項政策新加坡可以吸引到全球頂尖白帽駭客幫助新加坡政府檢視網站的安全性。從新加坡在設立資安新創育成中心或與東協之間的合作關係，核心精神在於引進國際經驗及連結國際市場及關係，透過國際連結強化新加坡境內資安業者的能量。

(三) **為國內資安產業國際化發展奠立良好基礎**：SICW大會過去並不開放臺灣組團參展，今年度在臺灣積極爭取下，首次取得組團參展之先例，不僅讓臺灣業者有機會透過SICW平台與國際業者交流，在會展中更以打造臺灣資安品牌形象，對國際資安領域重要人士進行宣傳與擴散。對於本次與會的國內資安業者來說，透過這次活動與交流，使得臺灣業者與國際業者、大會建立對口關係，以利於未來技術交流、商業合作或經貿往來，對國內資安產業的國際化與發展奠定良好的基礎。

二、建議：

新加坡為自由貿易的外銷導向國家，加上其市場穩定，語言多元，且地理位置與東南亞各國相近等因素，因此，藉由參與本次活動，亦可做為連結南向市場的最佳跳板。

(一) **規劃資安新南向國際推動政策**：在本次參訪過程，接觸到新加坡及來自各國的與會人士，在會議中共同論及東協是近年來全球經濟成長速度最快的地區之一，東協地區人口族群具備年輕化、高成長等特質，對於資通訊科技應用需求及接受度高，對於網路安全防護、資安防護韌性的需求也隨之提升，再加上近年來大量製造代工的價值活動轉移到東協地區，東協市場不僅在民眾端對於資安需求提升，企業端也因為智慧製造、工業 4.0 等議題推波助瀾，產業對於資安的需求日益提升。新加坡早在 2016 年就投入約 3 億臺幣推動東協網路安全能力提升計畫，2019 年起的五年內將投入 6.6 億元臺幣設立「東協－新加坡網路安全卓越中心」，新加坡政府積極地投入資源在培訓及研究上，提升東協成員國網路安全能力，新加坡有系統、有策略及作法地想要扮演東協國家中的資安主導者與促進者。無論從相關次級資料統計數據，或本次參訪國際業者經驗，新南向國家臺灣資安業者未來不可忽視的市場之一，臺灣資安業者技術能力並不遜於國外廠商，下階段在資安產業政策推動過程，新南向無疑是一個重要的國際出口，宜對臺灣資安產業國際輸出進行(Master Plan)，尤其是因應新南向國家產業及市場需求。

(二) **推動臺灣資安產業與國際生連結**：臺灣在資安產業鏈的上中下游已經具備良好基礎，但對應到 SICW 參展國際大廠，仍有努力空間。從本次參訪新加坡學校經驗、與國際資安大廠經驗交流過程，對臺灣資安產業能量提升未來可以朝向二個方向：

1. **推廣臺灣資安國家隊**：與國際大廠相較之下，現有臺灣資安廠商規模普遍不大，個別業者在國際化或國際市場拓展的過程面臨第一個問題就是資源不足、跨國溝通困難等問題。在本次參展經驗，集結臺灣廠商在國際聯合曝光與行銷，以「臺灣隊」的

品牌對外聯合宣傳，不僅可以減輕個別業者對外溝通的負擔，透過政府部門整合，也可提升國外買家對國內廠商的信心。未來無論透過實體展覽、網路平台、國外當地通路或技術支援，可朝向透過同一模式進行複製與擴散，以降低國內業者進入國際市場的門檻。

2. **完善資安新創國際生態系**：從新加坡推動資安新創育成政策經驗中，資安創新生態 71 區集結了新加坡內部及國際資源與資金共同推動新加坡資安新創生態系。在臺灣，近年來有許多資安業者獲得國際大廠併購，顯示國內資安新創團隊技術能量、創業主題價值以及國際化潛力高，未來可強化資安新創的育成政策，讓更多國內潛在具備潛力的資安新創團隊能夠更快速發展、獲得更多國際關係與連結。