CYBERSEC 2026 臺灣資安大會

一、活動時間

2026 年 5 月 5 日（二）至 5 月 7 日（四）

二、活動地點

臺北南港展覽館 2 館 1 樓、4 樓、7 樓（臺北市南港區經貿二路 2 號）

三、活動目的

數位威脅如同永不平息的風暴，安全的定義持續演變，防禦的核心不再只是阻擋風險，更在於承受衝擊、迅速恢復，並維持運作的韌性。iThome 自 2015 年起辦理 CYBERSEC 臺灣資安大會，旨在提升臺灣資訊安全意識、強化整體資安防護成熟度，促進產官學研跨界交流，並推動臺灣資安產業發展，每年吸引上萬名資安從業人員到場參與。

CYBERSEC 臺灣資安大會於 2026 年迎來 12 週年，三天會期逾 400 家國內外標竿資安品牌參展，匯聚 300 場前瞻趨勢演講盛況，不僅是臺灣規模最大，更成為亞洲資安備受矚目的年度盛會。大會每年邀請眾多國內外資安專家，帶來最新全球資安趨勢與貼近企業實務的資安防禦經驗；並透過資安主題論壇，探討各產業獨特資安議題，共同建構數位環境的守護韌性，促成跨界對談與經驗交流。

四、展會主軸

CYBERSEC 2026 臺灣資安大會以「RESILIENT FUTURE」為主題，邀請各界共同凝聚觀點、交流實踐並累積經驗。大會匯聚展現在地自主研發成果的「臺灣資安館」、深化培育動能的「Cyber Talent 資安人才培訓專區」，以及探索智慧聯網與硬體安全的「AIoT & Hardware Security Zone」。同時，大會持續將影響力擴及亞洲各國，透過辦理「Asia Cyber Channel Summit」東南亞資安通路媒合活動，並邀請各國駐臺代表與全球重量級專家來臺分享，打造跨國交流、公私協力的聯防平台，創造更安全、安心及安穩的數位未來。

五、合作單位

- 指導單位：數位發展部、國家科學及技術委員會
- 主辦單位：iThome 電週文化事業股份有限公司
- 共同主辦單位：趨勢科技股份有限公司

六、與會對象

- 技術專家：匯聚國內外知名資安技術領袖與趨勢專家、白帽駭客高手、及各領域資安專家
- 資安政策制定者：中央及地方資安領域相關官員、各縣市政府及機關資安首長、資安業務相關承辦人員
- 第一線資安從業人士：來自各產業的資訊人員、資安從業人員，涵跨資訊長、資安長、中階主管，到第一線企業專責人員皆熱情參與
- 推動資安發展團體：各界組織社群、產業發展協會等從業人士
- 媒體及有興趣之社會大眾

七、活動官網

詳細議程與講者介紹請見官網：https://cybersec.ithome.com.tw/

八、展會介紹（註：完整活動及議程資訊將持續更新於官網中）

- 資安會議
  - ✓ 盛大的會議規模：會期三天，現場提供 14 軌同步議程、超過 300 場專業技術議程，涵蓋最新且熱門資安議題與技術面向。並透過資安技術範疇 Tag 標示指引，以及課程等級建議，包含：通識、中階、進階，幫助來賓快速選擇。

✓ 完整的主題議程： 匯聚多位海內外知名資安專家進行「大會主題演講」，並涵蓋多元且前瞻的資安議題，包括：

AI 應用與安全治理：
聚焦人工智慧時代的安全防禦與治理框架，涵蓋「AI Security & Safety 論壇」、「AI Defense 論壇」、「AI Governance 論壇」、「AI Offense 論壇」、「Securing AI 論壇」與「Attacking AI 論壇」等深度論壇，並設有「AIoT & Hardware Security Summit」探討軟硬體整合安全。

前瞻新興技術與應用趨勢：
引領技術發展先機，包含「零信任論壇」、「後量子密碼論壇」、「Web3 安全論壇」、「EU CRA 論壇」、「Digital Trust 論壇」、「Cyber Physical System Security 論壇」、「Secure Software & DevSecOps 論壇」、「Cyber Technology & Innovation 論壇」及「Cyber Talent Forum」。

跨領域產業資安導入與策略：
針對垂直產業提供實務路徑，涵蓋「金融資安論壇」、「醫療資安論壇」、「OT Security 論壇」、「上市櫃資安標竿論壇」、「Supply Chain Security 論壇」、「InfraSec 論壇」、「Privacy & Data Protection 論壇」及「Security Strategy & Case Study 論壇」等專題論壇。

資安實戰攻防與技術研究：
深耕技術核心，包含「Threat Research 論壇」、「Incident Response 論壇」、「攻擊型安全論壇」、「雲端安全論壇」、「CISO 論壇」及「CYBERSEC GLOBAL」；並透過「CyberLAB」實機操作環境，提供最擬真的資安攻防演練。

✓ 堅強的講師陣容：邀請國內外資安領域重量級專家齊聚一堂，以前瞻資安思維、深厚實務經驗及多元洞察，提供策略性視野，啟發企業應對未來資安挑戰的新思路。

■ 資安展覽

✓ 會期三天預計集結超過 400 家國際大廠與臺灣知名資安品牌，現場匯聚逾 1,300 個攤位規模，網羅上千種最新資安產品與實務應用。作為亞洲成長最快、臺灣唯一超規格的資安專業盛會，我們展示最全面且前瞻的技術解方，並透過豐富的互動解說與專家深度交流，助您全方位掌握年度市場脈動與技術趨勢。

- ✓ 臺灣資安館：匯聚臺灣頂尖自主研發能量與品牌，聚焦「硬體根源信任、AI 安全治理、零信任韌性架構」等戰略支柱，展現臺灣如何將深厚的供應鏈優勢，轉化為接軌國際標準的資安韌性實力，為全球夥伴構築堅實的信任基礎。透過「臺灣自主研發特展」、「臺灣資安品牌導覽」與「資安論壇活動」，臺灣資安館致力於打造貼近實務的多元交流場域，串聯政策方向、產業需求與國際趨勢。全面呈現臺灣在半導體供應鏈、關鍵基礎設施與智慧應用中的實戰應用，協助企業因應技術演進與數位轉型帶來的挑戰。

- ✓ AIoT & Hardware Security Zone:在技術革新和裝置升級的新時代，不僅帶來無限可能，也使企業面臨前所未有的資安挑戰。從生產線到供應鏈，攻擊面持續擴大，企業須強化資安韌性。臺灣作為全球製造業重要樞紐，需透過跨領域整合與技術創新，降低風險並提升國際競爭力。館內設有 AIoT & Hardware Security Summit 論壇專區，透過產學研各家專家分享，深度洞察產業動脈，多方探查未來趨勢，保持競爭優勢。

- ✓ CYBERSEC ARENA：今年特別邀請 ISC2 Taipei Chapter 與國家資通安全研究院專家親臨現場指導，推出攻防桌遊與醫療情境推演，模擬現代常見資安威脅與應變決策，帶領您貼近真實的資安防禦體驗，強化風險辨識及應變處置能力，全面提升組織因應數位威脅之資安韌性。

- ✓ Asia Cyber Channel Summit：CYBERSEC 臺灣資安大會當中，專為臺灣資安業者橋接國際技術及市場夥伴所規畫的活動。以「帶進國際資安買家，串連亞洲資安通路」為號召，並以臺灣資安大會－全臺最大資安盛會所集結的資源，規劃相關活動，多元化呈現臺灣廠商實力，加速臺灣資安品牌走向國際。

- ✓ Cyber Talent：隨著數位科技迅速演進，世界正式進入一個由創新與演算共同驅動的時代，物聯網、自駕載具、衛星通信、AI 等新興科技全面加速推動產業發展，相互依存的世界伴隨衍生資安威脅，資安人員不再只是維護網路與設備安全，Cyber Talent 資安人才培訓專區，持續深化培育動能，致力讓學界、在學或在職的資安人才與產業接軌，透過人才 Talent x 職涯 Path x 培訓 Training 等多元面向，打造最完整、有效的資安人才供需交流平台，為臺灣厚植各行各業資安防護能量，連結產業動脈，打造更完整的資安體系。

九、報名方式

- 即日起開放報名（額滿為止），請上大會官網 https://signupcybersec.ithome.com.tw/signup/2026

1. 提前完成線上報名者免報名費，食宿及交通自理；若未提前完成線上報名者，需於活動現場辦理，並酌收現場報名作業費新台幣 500 元。

2. 因座位有限，主辦單位保留報名資格審核之權利。

3. 活動好禮：(註：詳細兌獎辦法請以官網公告內容為準，每人限領乙份，贈完為止)

➢ 來賓於 5 月 5 日至 5 月 7 日展會期間，至 1F 大會服務台完成報到即有機會獲得「CYBERSEC 2026 專屬提袋」、「CYBERSEC 資安市場地圖」乙份。

➢ 來賓於 5 月 6 日出席者即有機會獲得【CYBERSEC 2026 臺灣資安年鑑】乙份，內含最新資安議題發展關注焦點、資安趨勢預測。

➢ 來賓於 5 月 7 日出席者即有機會獲得【CYBERSEC 2026 紀念襪】乙雙。

➢ 展攤集點禮：參與「超級品牌」與「旗艦型」展攤互動，任一展攤皆視為 1 點，來賓集滿 30 點，即有機會獲得【CYBERSEC 2026 旅行盥洗包】乙個。

➢ 深度參會集點禮：任一堂議程 / 展攤皆視為 1 點，來賓集滿 40 點，即有機會獲得【大會主題紀念款 T-shirt】乙件。

4. 收到報名資料後，系統將寄發確認信函通知已收件；經資料審核通過後，將於活動前二週內以電子郵件寄發會前通知及報到 QR Code。

5. 報名及活動聯絡人

姓名：開小姐

電話：(02) 2562-2880 #3622

大會議程暨講者陣容：

大會議程表：https://cybersec.ithome.com.tw/2026/agenda

（大會議程表籌備中，預計於3月下旬正式上線）

詳細講者陣容：https://cybersec.ithome.com.tw/2026/speaker

更多展覽資訊：https://cyber.ithome.com.tw/2026/cybersecExpo

CYBERSEC 2026 臺灣資安大會 議程表 5/05 (TUE.) Day 1

08:00 – 09:30	來賓報到		大會主題演講會場 701 ABCD 會議室
09:30 – 09:35	大會開場致詞	吳其勳 / CYBERSEC 2026 臺灣資安大會 主席、iThome 總編輯	
09:35 – 10:00	貴賓致詞		
10:00 – 10:30	精選議程	陳立白 / 法務部調查局 局長	
10:30 – 11:00	當信任徹底失效：AI 時代的網路犯罪新商業模式	Ryan Flores / Director of Technology Research, TrendAI Inc	
11:00 – 11:30	精選議程	Mastercard	
11:30 – 12:00	Ambient and Autonomous Security: Building Trust in the Agentic AI Era	Vasu Jakkal / CVP Security Business, Microsoft	
12:00 – 14:00	Lunch & Break		

分堂議程 時間/地點	資安品牌日 – 智慧資安 701A	AI Security & Safety 論壇 701B	資安品牌日 – Microsoft 701C	資安品牌日 – Google Cloud 701D	資安品牌日 – Cloudflare 701E	SecOps 論壇 701F	CISO 論壇 701G	Secure Software & DevSecOps 論 壇 701H	InfraSec 論壇 703	Threat Research 論壇 4A 展區會議室	Attacking AI 論壇 4B 展區會議室
14:00 – 14:30	精選議程 智慧資安	當 AI 成為攻擊入口：企業如何防禦 Agentic AI Threats？ 詹凱富 (Mika Chan) Radware Cloud Architect, APAC 亞太區雲端架構師	攻擊來得快，你擋得更快 - AI Agents × XDR × Security Copilot 幫 SOC 火力瞬間升級 沈志明 (Alex Shen) 台灣微軟 資深資安顧問	資安營運的新浪潮：代理化防禦 (Agentic Defense) 的崛起 Patrick Chiu Google Cloud Security Customer Engineering	精選議程 Cloudflare	防火牆 AI 異常檢測系統：泛用性設計與部署實踐 威剛科技股份有限公司 資通安全部 - 梁秀如 資深工程師 - 馬健騰 技術副理	AI 安全該怎麼管? 陳詰昌 台新新光金控 / 台新銀行 資安部 資安長	API 安全防護—數位時代的基石 蔡宜瑾 (APril Tsai) ASUS	精選議程 聯達	內網中的幽靈：Earth Kurma 的隱身手法與長期的攻擊策略 Nick Dai 趨勢科技 資深威脅研究員	精選議程 陳仲竉 奧義智慧科技
14:45 – 15:15	精選議程 智慧資安	企業導入 AI 的第一個安全問題：如何在創新與資料保護之間取得平衡 白瑞祥 (Ray Pai) Forcepoint 資安技術顧問	當攻擊開始鎖定 AI：如何防禦生成式 AI 應用程式、保護模型、資料與代理，化風險為可控事件 陳雋中 (George Chen) 台灣微軟 雲端安全資深架構師	AI 驅動的跨雲新紀元：建構具備數位韌性的安全網路架構 Retro Kuo Google Cloud Customer Engineering	精選議程 Cloudflare	精選議程 Ta-Lun Yen TXOne Networks Inc.	建構堅不可摧的資料堡壘：NetApp 網路韌性解決方案 謝進霖 (Eric Hsieh) 零壹科技 資深技術顧問	精選議程 曾國韋 安華聯網科技股份有限公司	精選議程 Dell	The Cybercrime Factory: Infostealers. Annual Intelligence Brief. Leonid Rozenberg Hudson Rock Cybercrime and Threat Intelligence Researcher, Research	AttackGPT: It Can Talk the Kill Chain — But Can It Afford To Walk It? Jan Michael Alcantara Netskope Senior Threat Research Engineer, Netskope Threat Labs
15:30 – 16:00	精選議程 智慧資安	精選議程 逸盈	不只零信任，還要零失控：讓 AI Agent 有邏輯、也有紀律，零信任驅動的行為治理 林堅樂 (Jaron Lin) 台灣微軟 專家技術群資安技術專家	安全守護，創新加速：Google Cloud Security 全方位資安轉型 William Tam Google Cloud Global Security Solutions Architect	精選議程 Cloudflare	全方位資安治理的"六脈神劍" —— 整合架構與永續實踐 陳琬茹 MISO Sr. Information Security Risk and control Analyst	AI 領航 SOC 轉型實戰：打造自動化與智慧化的資安監控中心 Elena Lee Elastic 台港區域資深方案架構師主管	解構 Python 程式碼保護機制：Pyconcrete 的逆向工程與金鑰提取 lokJin Sih 中華電信股份有限公司 資訊技術分公司 資訊安全應用處 滲透測試與紅隊演練工程師	精選議程 威睿	以太藏刀: 鏈上不死 C2 - Sol Yang NICS 鑑識處理組 助理工程師	惡 PromptWare：LLM 惡意程式前線戰術指南 陳頡 TXOne Networks Inc. 資安威脅與產品防護中心 Staff Engineer
16:15 – 16:45	精選議程 智慧資安	保障人工智慧安全、抵禦人工智慧攻擊、安全使用人工智慧 Billy Chuang Illumio 高級安全技術總監	讓 AI 更聰明、資料更放心： 帶你把合規變簡單 李佳芸 (Jojo Lee) 台灣微軟 資深雲端解決方案架構師	安全建構及使用 AI 應用程式與服務 (Security for AI) Nick Cheng Google Cloud Customer Engineering	精選議程 Cloudflare	【16:15 – 17:00】 Original Sin of Active Directory - Long Live with NTLM Relay Jimmy Su 奧義智慧科技 資安研究員	精選議程 HENNGE	搭乘 Vibe Coding 這艘船，安全航向新世界 翁心慈 華碩電腦股份有限公司 數位安全中心 安全架構部 安全架構工程師	精選議程 邵楚珩 (Alex Chih) 七維思股份有限公司	【16:15 – 17:00】 Masks, Monsters, and Drivers: Unpacking the Deception of Chaos, Kraken, and DeadLock Chetan Raghuprasad Cisco Talos Threat Research Engineering Technical Leader, Threat Intelligence	【16:15 – 17:00】 Standardizing Gen AI Vulnerability & Categorization 胡辰溍 (Henry Hu) OWASP Taiwan Chapter Chapter Leader、安創資訊股份有限公司 執行長暨創辦人

分堂議程 時間/地點	Data Security 論壇 4D 展區會議室	Cyber Technology & Innovation 論壇 4E 展區會議室
12:30 – 13:00	【Lunch Learning Session】 精選議程 CrowdStrike	【12:30 – 13:15】 【Lunch Learning Session】【Securing AI 論壇】 戳破 AI 的防禦幻影：從紅藍隊視角重構 AI 系統安全 楊政霖博士 奧義智慧科技 資料科學處 處長
14:00 – 14:30	直擊「Shadow AI」失控現場，全面防止資料外洩 許祐福 精品科技股份有限公司 技術服務部 技術經理	以 AI 制 AI：CyberArk 如何利用「智慧身分防禦」重構企業安全基因？ JJ Net
14:45 – 15:15	精選議程 Zscaler	Agentic AI 實戰應用：重新定義攻擊型資安 William Tiew Ridge Security Technology Regional System Engineer Director
15:30 – 16:00	精選議程 群暉	2026 CRA 挑戰倒數！台灣廠商韌性指南 陳宗祈 Exein Partner & Alliance
16:15 – 16:45	精選議程	【16:15 – 17:00】【Threat Research 論壇】 SAP as a Cyber Weapon CAIBERP GmbH Researcher, Research - Andreas Wiegenstein - Xu Jia

時間/地點	CyberLAB 實機演練 702
12:30 – 14:30	實機演練課程
15:00 – 17:00	實機演練課程

時間/地點	AIoT & Hardware Security Summit AIoT & Hardware Security 展區
13:00 – 13:30	精選議程 ISA 台灣分會
13:30 – 14:00	精選議程 全景軟體
14:10 – 14:40	建構從產品製造到供應鏈的全方位 AI 網路安全防禦 Panasonic - Kyo Chen Head, Panasonic Cyber Security Lab - Freddy Ma Senior Threat Intelligence Researcher, Panasonic Cyber Security Lab
14:40 – 15:10	精選議程 精盧科技
15:20 – 15:50	如何全方位實踐 IoT 產品資安？以「難打的目標」為例 奧義智慧科技 - Jimmy Liu 資安研究員 - Chumy Tsai 實習生
15:50 – 16:20	精選議程 凌華科技
16:20 – 16:50	精選議程 東擎科技

CYBERSEC 2026 臺灣資安大會 議程表 5/06 (WED.) Day 2

08:00 – 09:30	來賓報到		大會主題演講會場 701 ABCD 會議室
09:30 – 09:35	**大會開場致詞**	吳其勳 / CYBERSEC 2026 臺灣資安大會 主席、iThome 總編輯	
09:35 – 10:05	**精選議程**	陳浩維 / 酷澎股份有限公司 臺灣暨日本資安長	
10:05 – 10:30	**精選議程**		
10:30 – 11:00	**精選議程**	Jason Lish / VP & CISO, Cisco	
11:00 – 11:30	**精選議程**	Sam Kaplan / Public Policy & Governement Affairs Senior Director, Palo Alto Networks	
11:30 – 12:00	**精選議程**	Shane Huntley / Sr. Director, Google	
12:00 – 14:00	Lunch & Break		

分堂議程 時間/地點	資安品牌日 – Jamf 701A	AI Security & Safety 論壇 701B	資安品牌日 – Fortinet 701C	資安品牌日 – 數位資安 701D	資安品牌日 – HENNGE 701E	資安品牌日 – 艾盾資料 701F	雲端安全論壇 701G	Cyber Technology & Innovation 論壇 701H	Cyber Technology & Innovation 論壇 703	醫療資安論壇 4A 展區會議室	Secure Software & DevSecOps 論 壇 4B 展區會議室	Security Strategy & Case Study 4C 展區會議室
14:00 – 14:30	**現代化行動資安新標準：從端點防禦到零信任架構** Glee Tsai Jamf 亞太區資深技術顧問	**精選議程** CHT	**守護現在，預見未來：FortiGate 打造 AI 時代的「全能守護者」** 余昇瀚 Fortinet 技術顧問	**精選議程** 數位資安	**精選議程** HENNGE	**供應鏈間互不信任的危機：解構《以色列在台灣》背後的數位信任危機與鑑識挑戰** 陳長志 艾盾資料股份有限公司 Director of SecOps	**雲端韌性：從供應鏈事件看 +C23+C8:G1+C8:G11** 邱永興 中華資安國際股份有限公司 SOC 服務部協理	**精選議程** 勤昱	**精選議程** 邁達特	**精選議程** 李建璋 衛福部資訊處 處長	**當 AI 能轉生成任何角色：面對產品與供應鏈安全新挑戰** 鄭禹葳 (Fiona Cheng) 偉康科技股份有限公司 產品研發部 資深研發經理	**精選議程** AEB
14:45 – 15:15	**打破邊界：建構 iOS 與 Android 跨平台行動防禦陣線** Stone Chen Jamf 亞太區資深業務代表	**Prompt Attack：LLM 無法迴避的核心安全破口** 邱銘彰 (Birdman) 奧義智慧科技 技術長暨共同創辦人	**Unified SASE 平台戰略：從整合到智能，創造無限價值** 孫嘉陽 Fortinet 技術顧問	**精選議程** 數位資安	**精選議程** HENNGE	**序幕：台灣產業的「上雲困境」，Wiz 極小化雲端成本將解憂** 羅煜賢 艾盾資料股份有限公司 Technical Consultant Director	**精選議程** CrowdStrike	**後量子密碼學 – 守護未來資訊安全的數位盾牌** 林邦暉博士 中華電信研究院 資安通安全研究所 分項計畫主持人	**從憑證管理到數位信任：DigiCert 如何建構 AI 時代的全球信任架構？** Digicert	**醫療領域之 OT 資訊安全防護特殊性介紹** 張韶良 亞東紀念醫院、秀傳、羅東博愛 醫學工程部門 醫學工程顧問、中華民國生物醫學工程學會 醫療器材資通訊安全委員會 主任委員	**從編譯器視角為 App 打造函式層級的防護迷宮** 陳忠義 ICEshell 艾斯冰殼 Security Compiler Engineer, R&D Dept.	**精選議程** Pentera Cyble_ABP
15:30 – 16:00	**貓鼠遊戲：解析國家級駭客的行動裝置攻擊策略** Elad Shapira Jamf 資深資安研究員	**精選議程** 逸盈	**AI 新賽局：在合規與創新中取得平衡** 李鵬 Fortinet 技術顧問	**精選議程** 數位資安	**精選議程** HENNGE	**SIEM 已歿：「去中心化」的 Log 管理將解決訂閱制的年年漲價痛點，拒當數據人質** 羅煜賢 艾盾資料股份有限公司 Technical Consultant Director	**雲地混合監控的機會與挑戰 – 以及 AI 治理** 詹曉容 雲力橘子 資訊安全部	**從「自動化」邁向「自主化」Agentic AI NDR 時代** 林孟忠 (Sam Lin) ExtraHop 資深銷售工程師	**AI 驅動的資安聯防：如何透過 MDR 與自動化打造企業『自癒級』防線** 盧惠光 台灣二版有限公司 高級產品經理	**精選議程** 許權廣 (Rock) 陽明交大竹銘醫院	**LLM 與 DevSecOps 相遇：AI-Powered DevSecOps 的機會與風險** Archer Tsai 華碩電腦股份有限公司 數位安全中心 安全架構部 Security Architect	**【Secure Software & DevSecOps 論壇】** **不要碰我的 DRIVER!!!** Jason Huang TXOne Networks Inc. 資安威脅與產品防護中心 主任工程師
16:15 – 16:45	**【專家座談】守護企業核心：高階主管與關鍵目標的進階防禦實務** - Jimmy Huang Jamf 亞洲區總經理 - Stone Chen Jamf 亞太區資深業務代表 - 郭杰穎 (Mouse Kuo) 可立可 執行長兼共同創辦人	**精選議程**	**企業資料安全治理實務：透過 AI 打破傳統 DLP 的盲點，資料外洩保護不再瞎忙** 呂政穎 Fortinet 技術顧問	**精選議程** 數位資安	**精選議程** HENNGE	**依賴是脆弱的開始，韌性來自於選擇權：如果企業資安團隊能重新選擇，他們會選擇 AI-SOC 服務，而您現在擁有這個選擇權** 羅煜賢 艾盾資料股份有限公司 Technical Consultant Director	**雲端之戰- AI 事變與重啟迴游** 黃星評 (Kuro Huang) ISC2 Taipei Chapter 理事	**【Securing AI 論壇】** **關於 AI 助理凌晨放火燒了公司還順便找 FBI 這檔事** 游照臨 (Steven Meow) 趨勢科技 紅隊 資安威脅研究員	**【Threat Research 論壇】** **關上 Windows，戰鬥才開始！macOS 在企業安全的崛起與挑戰** 葉東逸 (Kazma) 奧義智慧科技	**AI 軟體醫材的資安實戰：從美國 FDA 524B 規範到 Threat Modeling 與 Patch SLA 的完整落地** 林家聖 國立陽明交通大學 醫工學院 醫學影像 / 訊號人工智慧分析實驗室 博士生	**DevSecOps 的五大反模式：為什麼工具跑了，流程建了，韌性卻沒有提升？** 盧建成 (Augustin Lu) 鎮本行策有限公司 CEO，政治大學資訊科學系 兼任助理教授	**【16:15 – 17:00】** **【SecOps 論壇】** **OPNsense×Suricata + SmartNIC 高效能防護實戰** 鄭明彰 南投縣教育網路中心 系統組 組長

分堂議程 時間/地點	零信任論壇 4D 展區會議室	CISO 論壇 4E 展區會議室
12:30 – 13:00	【12:30 – 13:15】 【Lunch Learning Session】【Securing AI 論壇】 **Mental Jailbreak: Scaling Law ≠ Human Reasoning** **開源從頭打造越獄防護** 馬聖豪 TXOne Networks Inc. 資安威脅與產品防護中心 Team Lead	【Lunch Learning Session】【AI Offense 論壇】 **Vibe Pentesting 入門不求人** 游鎮毓 (Cheng-Yu Yu) Appier Senior Software Engineer, Information Security
14:00 – 14:30	**精選議程** CrowdStrike	**資安單位預算≠資安預算好嗎?** 方振維 台新新光金融控股公司 資安部 資深協理
14:45 – 15:15	**AI-Driven Zero Trust Security Transformation for SMB and Mid-Market with SonicWall** Chandrodaya Prasad SonicWall Inc Chief Product Officer (CPO)	**如何有效地降低企業資訊安全風險** Jerry Chen 宸鴻科技 資訊安全部 資深經理
15:30 – 16:00	**Zero Trust That Works in the Real World: Containment and Antifragile Cyber Resilience** John Kindervag Illumio Chief Evangelist	**CISO 和高階主管的風險對話：從風險胃納和風險承受的角度出發** 李彥民 Anthony SHOPLINE CISO
16:15 – 16:45	**重塑數位邊界：勒索眾信如何透過零信任架構，驅動企業資安的韌性與敏捷** Deloitte	**合規即戰力：CRA 強制執行倒數，如何將「產品安全」轉化為全球信任競爭力** 游政卿 合勤投資控股 董事長室 資安長

時間/地點	CyberLAB 實機演練 702
12:30 – 14:30	實機演練課程
15:00 – 17:00	實機演練課程

時間/地點	AIoT & Hardware Security Summit AIoT & Hardware Security 專區
13:00 – 13:30	**萬物連網，萬物破口：物聯網資安的殘酷真相與防線重建** 楊明儒 昇貿股份有限公司 總經理室
13:30 – 14:00	**精選議程** 精虜科技
14:10 – 14:40	**AI 機器人資安攻防實例** Aaron Luo VicOne Inc LAB R7 資深威脅研究經理
14:40 – 15:10	**精選議程** 速碼波科技
15:20 – 15:50	**精選議程** 亞力通訊
15:50 – 16:20	**精選議程** 聯發光電
16:20 – 17:00	**擊石清障：從韌性到卓越這條路，有夠難** ASUS Digital Security Center - 許宗仁 (TJ Hsu) 資安威脅分析師 -黃鴻碩 (Harold Huang) 威脅偵測與應變分析師

時間/地點	Cyber Talent 資安人才培訓論壇 Cyber Talent 專區
14:00 – 14:30	**他們說我是沒有用的年輕人** PD Lee 自由工作者 資安流浪漢
14:30 – 14:45	**精選議程** 國家資通安全研究院
15:00 – 15:30	**資安人該如何自我定位與未來職涯展望（實際案例分享）** 陳瑰茹 MISO Sr. Information Security Risk and control Analyst
15:30 – 15:40	**AI 時代的資安勝戰：從技術防禦轉型為組織匯聚戰力** 劉孟昌 (Piner Liu) 安碁學苑股份有限公司 ACSI Cyber Security Academy 營運長 COO
15:40 – 15:50	**精選議程** 七維思
15:50 – 16:20	**如何成為不被討厭的資安人員-打工人要好好保護自己篇** 謝博尊 中華電信 資通安全處 資安工程師

CYBERSEC 2026 臺灣資安大會 議程表 5/07 (THU.) Day 3

分堂議程 時間/地點	零信任論壇 701B	資安品牌日 – Cisco 701C	CISO 論壇 701D	資安品牌日 – HP 701E	AI Defense 論壇 701F	Supply Chain Security 論壇 701G	Cyber Technology & Innovation 論壇 701H	Cyber Physical System Security 論壇 703	Threat Research 論壇 4A 展區會議室	AI Security & Safety 論壇 4B 展區會議室	OT Security 論壇 4C 展區會議室
09:30 – 10:00	從 Device Posture 到 ZTNA：打造完整端點零信任架構 陳育徹 (Alden Chen) FineArt Technology 精品科技 資安顧問	精選議程 Cisco	台灣高科技產業資安評比 CSF 2.0 洞察報告 Bright Wu Aon Taiwan Executive Diretor, Taiwan Regional Cyber Risk	精選議程 HP	AI: 我家 SOC 的超級實習生 - 從 SOCCMM 看次世代 SOC 唐雍為 資誠智能風險管理諮詢有限公司 風險與控制服務 執行董事	精選議程	精選議程	具身 AI 覺醒：當人工智慧開始掌控現實世界（從雲端到機器狗，物理攻防戰正在展開） 鄭奕立 VicOne Inc. CEO	蔓延的惡意:看銀狐的擴張與演進 Rachael Liao Fortinet FortiGuard Labs Anti-Virus Analyst	雙生共競：生成式 AI 驅動的自動化防禦演進與信任架構實踐 中華資安國際股份有限公司 - 李宗霖 研發工程師 - 陳昕孚 研發工程師	精選議程
10:15 – 10:45	醫院資安從小到大 建立零信任架構 黃冠凱 中山醫學大學附設醫院 醫療資訊中心 副主任	精選議程 Cisco	臺灣人體生物資料庫的資安文化養成經驗 張中科 中央研究院 臺灣人體生物資料庫 策略長（資安長）	精選議程 HP	與 AI 並肩作戰，企業藍隊邁向智慧防禦與背後的故事 楊庭瑋 緯創資通 資訊安全系統監控部 技術經理	精選議程 台達電子工業	Cyber Innovation：重塑網路與端點的威脅獵捕防線 劉叡 中華資安國際 經理	虛實融合下的挑戰：汽車產業數位分身安全防護 TXOne Networks Inc. - Chizuru Toyama 威脅研究部 資深資安威脅研究員 - Linwei Tsao 資安威脅與產品防護中心 資安威脅研究員	Operation TradeBait：假案真駭的釣魚詐騙行動 TeamT5 杜浦數位安全 - Tay Cheng CTI Researcher, ThreatVision - Jessica Fang CTI Analyst, ThreatVision	【AI Offense 論壇】 Modern AI Real-Time Voice Cloning and Voice Phishing Adin Drabkin Google Cloud Offensive Security Consultant	精選議程
11:00 – 11:30	用主觀邏輯打造動態信任分數：零信任架構的實戰演算法則 Jason Chuang NEXCOM 新漢 AI Technical Baily Lo NEXCOM OT Security 椰蜜科技 技術副理	精選議程 Cisco	從管理到治理，資安部門價值呈現新思維 蔡秉諺 (Stanley Tsai) 群創光電 資通安全部 資深副理	精選議程 HP	智能代理 AI 在資安監控的應用情境 (Agentic AI for SOC) Nick Cheng Google Cloud Customer Engineering	SEMI E187/E188 標準落地實踐：半導體供應鏈安全的一致性檢測與應用 王德銘 TeamT5 杜浦數位安全 產品經理	【Digital Trust 論壇】 超越資安：DTEF 從防護思維走向信任治理 陳政龍 ISACA Taiwan Chapter 台灣分會 副會長	精選議程 Bureau Veritas	化被動為主動：守株待想要鑽洞的 Meow 夜貓 Fortinet Anti-Virus Analyst, FortiGuard Labs	當 AI 成為應用核心：企業安全治理的下一個戰場 范茗閎 (Joshan Fan) F5 Sr Solutions Engineer 台灣區技術顧問	精選議程
11:45 – 12:15	AI 從小兵變指揮官，擊殺鏈如何從工具箱進化為核彈 - 陳齊修 (Harry Chen) 網路中文資訊股份有限公司 資安部 紅隊主管 - 邱楚珩 (Alex Chih) 七維思股份有限公司 技術部 資安暨雲端顧問	精選議程 Cisco	【11:45 – 12:30】 資安是一種企業能力，不是專案 胡修武 東元電機 數位發展處 處長	精選議程 HP	學資安的 AI 不會變壞，但會搶飯碗? 中華資安國際股份有限公司 - 陳彥銘 監控科 資深資安工程師 - 陳昕孚 研發工程師	我的供應商檢核了 500 題，然後上新聞了 許農育 叡揚資訊股份有限公司 資安事業發展部 技術顧問	【11:45 – 12:30】 【Digital Trust 論壇】 AI 時代司法聯盟鏈：區塊鏈資安治理與智慧監控實踐 魯志遠 法務部調查局 資通安全處 科長	鎖定海事資安戰力 — 為 AI 時代的全球港埠打造數位韌性 陳頡 TXOne Networks Inc. 資安威脅與產品防護中心 Staff Engineer	別怕黑，開 Tor 就對了！— 暗網入門與合法生存指南 Yuki Hung 奧義智慧科技 資安研究員	【AI Offense 論壇】 From Prompt to Shell - Weaponizing AI Agents with the Model Context Protocol Jie Cybersecurity Enthusiast	精選議程

分堂議程 時間/地點	AI Security & Safety 論壇 701B	上市櫃資安標竿論壇 701C	CISO 論壇 701D	攻擊型安全論壇 701E	後量子密碼論壇 701F	EU CRA 論壇 701G	AI Governance 論壇 701H	Cyber Marketing & Sales 論壇 703	Threat Research 論壇 4A 展區會議室	Privacy & Data Protection 論壇 4B 展區會議室	OT Security 論壇 4C 展區會議室
14:00 – 14:30	預見 2026：如何利用 AI 領航的情資網路，建構「端點到雲端」的企業安全韌性 曹家通 Westcon Taiwan 首席資安顧問		Security Without Borders: Breaking Language and Cultural Barriers to Harmonize Global Security Operations Jesse Ku Bora Pharmaceuticals Global Cybersecurity Manager	精選議程 張克勤	精選議程 陳君明	從德國 OT 滲透測試團隊攻擊鏈洞察：製造業迎接歐盟《網路韌性法 CRA》的備戰策略 YU-YU OETTING 德國 Laokoon Security GmbH (資安攻防) Strategic Partner	【Digital Trust 論壇】 精選議程 謝君豪	Solving Security in a World That Changes Faster Than Your Tools Philip Sow Proofpoint Head of System Engineering - South Asia, System Engineering	攻擊鏈解構：從在地化誘餌到真實威脅的研究案例剖析 林宜平 Fortinet FortiGuard Labs 資安威脅研究經理	上吧！資料百變怪！讓合成資料成為你 AI 安全可信的夥伴 國家資通安全研究院 - 陳正庭 Chen, Justyn 架構設計組 機器學習工程師 - 許德丞 Andy Te-Cheng Hsu 資料保護組 副研究員	從框架到現場：132 項 OT 資安控制的落地實踐 Steven Hsu (許齊誠) TXOne Networks Inc. Vertical Evangelist 副總
14:45 – 15:15	精選議程 極風雲創		精選議程	是不是我的 18 歲 注定讓藍隊掉眼淚 - MITRE ATT&CK V18 Hans Wang CHT Security 檢測部 副理	後量子密碼學憑證方案和車聯網憑證方案的標準化進程 陳志華 (Abel C. H. Chen) 中華電信研究院 資通安全研究所 高級研究員	面對未來資安法規需求，如何強化提升資安成熟度? Richard Lin 台達電子工業股份有限公司 產品資安事業部 資安架構主管	精選議程 黃淙澤 中華民國電腦稽核協會	Cybersecurity Is Far Sexier Than What You Think, and Have Been Saying Annie Quynh Anh - Tech Lady VinCSS Internet Security Services JSC Head of Marketing	Clean Redirects, Dirty SYSTEM: Bug Hunting by Abusing File Operations for Silent Privilege Escalation Sharkkcode TeamT5 杜浦數位安全 Research Engineer, Engine Team	具身 AI 走進家：隱私攻防新戰場 朱益宏 VicOne RD 架構師	Beyond the Headlines: Protecting Infrastructure from Industrial Cybersecurity Threats Chuck Weissenborn Dragos, Inc. Chief Technology Officer, Dragos Public Sector
15:30 – 16:00	駕馭生成式 AI 的雙面性：勤業眾信如何建構「安全與效能並行」的 AI 防禦體系 Deloitte	見【表一】上市櫃資安標竿論壇	【OT Security 論壇】 超越 EPSS：打造更準確的 OT 漏洞利用預測系統 TXOne Networks, Threat Signature Research Team - Daniel Chiu Senior Threat Signature Research Team Manager - Queenie Liao Threat Signature Researcher	委外滲透測試的治理全生命週期：預算、法規、流程、與企業安全成熟度的下一步 Annie Shih QNAP Systems, Inc. General Counsel, Legal & IP	淺談 PQC 與實務操作 Retro Kuo Google Cloud Customer Engineering	歐盟 CRA 倒數啟動：產品資安合規的三大關鍵策略 Daniel Liu 安華聯網科技（DEKRA 德凱集團成員） 營運中心 技術長	AI 專案管理基本功：來自於 PMBOK 的啟發 Bright Wu Aon Taiwan Executive Diretor, Taiwan Regional Cyber Risk	【Threat Research 論壇】 你的輸入法正在背後偷偷監視你 Nick Dai 趨勢科技 資深威脅研究員	PS C:\> Live Off the .NET Gadgets - 從指令解析缺陷到符號引擎的新視野 黃智威 TXOne Networks Inc. 資安威脅與產品防護中心 資深資安威脅研究員	AI 發展下的隱私法遵與安全落實 鄒耀東 帝寬智慧科技股份有限公司 研發部 總經理	關鍵基礎設施防護的優先序：深度剖析跨部門依賴關係與級聯效應 Mars Cheng TXOne Networks Inc. 資安威脅與產品防護中心 資深經理
16:15 – 16:45	【16:15 – 17:00】 異常≠威脅：從時序到時頻，打造具解釋性 AI/ML 異常威脅感知的專利實務 馬聖豪 TXOne Networks Inc. 資安威脅與產品防護中心 Team Lead		精選議程	【16:15 – 17:00】 從 150 場紅隊演練數據看產業安全 徐念恩 戴夫寇爾股份有限公司 管理部 資深副總	精選議程 陳君朋	基於 ISA/IEC 62443 的歐盟網路韌性法案(EU CRA)合規路徑 Kenny Lee SGS Head of Cybersecurity Laboratory, CDTL	【16:15 – 17:00】 AI 改變企業治理底層邏輯—資安、個資、智財管理的再設計 鄒宗萱 財團法人資訊工業策進會 科技法律研究所 副所長	【Threat Research 論壇】 都 6202 年了！Relay Attack 未死，而且還更好用！ Wesley Fu 趨勢科技 Threat Researcher	【16:15 – 17:00】 Beyond the SERP ：當黑帽 SEO 行動演變為多面向的犯罪威脅 Joey chen Cisco Talos Leader, Security Research	精選議程	精選議程 陳明皇 國立成功大學 計算機與網路中心

分堂議程 時間/地點	SecOps 論壇 4D 展區會議室	Securing AI 論壇 4E 展區會議室
09:30 – 10:00	AD 安全報告：深度分析超過 100 家台灣企業的 Active Directory 安全現狀 Gary Sun 奧義智慧科技 資深軟體工程師	Beyond Prompt Attacks：用開放技術打造可落地的 LLM 合規防護鏈 曲華燊 中華電信研究院 雲端運算研究所 高級研究員
10:15 – 10:45	矛盾協作：紫隊打造製造業資安韌性 林伯駿 友達光電股份有限公司 資安處技術部 工程副理	打破 AI 合規假象：拒絕靜態測試的「虛假安全感」 廖冠綸 (Steve Liao) 奧義智慧科技 資料科學家
11:00 – 11:30	精選議程 黑貓	敵人就在本能寺 - 企業應用 AI Agent 風險剖析 Will Lin 華碩電腦 數位安全中心 安全架構部 Sr. Director
11:45 – 12:15	當老闆覺得防毒軟體＝資安成熟度 100 分時 吳阡語 錸恩帕斯科技股份有限公司 資訊經理	打造 OT/ICS 的地端偵測模型: 以 Learning On the Land (LOTL) 對抗 Live Off the Land (LOTL) 攻擊 黃智威 TXOne Networks Inc. 資安威脅與產品防護中心 資深資安威脅研究員
分堂議程 時間/地點	**Incident Response 論壇 4D 展區會議室**	**Web3 安全論壇 4E 展區會議室**
12:40 – 13:10	【Lunch Learning Session】【攻擊型安全論壇】 同行 20 年：從攻防兩端看見台灣資安的下一步 - 翁浩正 戴夫寇爾 DEVCORE 執行長 - 陳浩維 酷澎股份有限公司 臺灣暨日本資安長	【Lunch Learning Session】【AI Defense 論壇】 用你的魔法對付你！當 Vibe 詐騙遇上 Vibe 駭客！ 游熙臨 (Steven Meow) 趨勢科技 紅隊 資安威脅研究員
14:00 – 14:30	【醫療資安論壇】 讓醫療產業再次 Level up：淺談 Health Level 7 的資安問題及展望 Linwei Tsao TXOne Networks Inc. 資安威脅與產品防護中心 資安威脅研究員	穩定幣與虛擬資產的金融應用設計、合規趨勢與資訊安全 朱妍如 安永諮詢股份有限公司 諮詢顧問 協理
14:45 – 15:15	0.5 個人的藍隊：與 AI 共舞的孤獨調查家 陳兆閎 奧義智慧科技 資安研究員	RWA × 穩定幣 × 金庫落地安全概觀 凱特納科技 - 曾信田 (Newbug Tseng) 創辦人暨執行長 - 李尚韋 (Turkey Li) 共同創辦人暨策略長
15:30 – 16:00	精選議程 黃建笙 登豐數位科技股份有限公司	探討「硬體錢包結合 TSS 門檻簽章」的新託管範式 CYC AMIS, Maicoin Research team 首席科學家
16:15 – 16:45	Intelligence FAST & FIRST！真的有這麼神？從誕生到退休 ASUS, Digital Security Center - 許宗仁 (TJ Hsu) 資安威脅分析師 - 李東育(Eric Li) 威脅偵測與應變分析師	Drainer-as-a-service: 陰影下的商業模式 Vic Huang UCCU Hacker 成員

時間/地點	金融資安論壇 701A
09:30 – 09:35	開場致詞 吳其勳 CYBERSEC 2026 臺灣資安大會 主席、iThome 總編輯
09:35 – 09:45	長官致詞
09:45 – 10:15	金融政策現況與展望 林裕泰 金融監督管理委員會 資訊處 處長
10:15 – 11:15	座談分享
11:30 – 12:00	金融業弱點管理怎麼管？ 陳詰昌 台新新光金控 / 台新銀行 資安部 資安長
14:00 – 14:30	精選議程
14:45 – 15:15	金融業物聯網資訊安全治理與導入經驗分享 簡經緯 (Fredo Chien) 安聯證券投資信託股份有限公司 資訊安全 /台灣資安長與資訊安全專家
15:30 – 16:00	浪潮下的資安治理：跨國企業合規與跨部門實戰 Sonia Peng 美商達信保險經紀人股份有限公司台灣分公司 Information Security Manager, CEO Office
16:15 – 17:00	AI 資安檢測 萬幼筠

時間/地點	【表一】上市櫃資安標竿論壇 701C
14:00 – 14:30	精選議程
14:45 – 15:15	精選議程 易換棣 遠東新世紀股份有限公司
15:15 – 15:35	精選議程 創泓
15:50 – 16:20	您的資安聯防真的有達到預期的效果嗎？ 陳昱崇 (Zero Chen) 伊雲谷數位科技 Director, Cybersecurity MSSP
16:20 – 17:00	有關資安事件的那些事：資安事件教會我的操作及如何使得組織更健壯 Sam Chan 自由系統股份有限公司 資安服務部 資深資安經理

時間/地點	AIoT & Hardware Security Summit AIoT & Hardware Security 專區
09:30 – 10:00	**從 Nano-GPT 建模技術打造數位分身，保護虛實整合系統持續運營** Yenting Lee TXOne Networks Inc. 資安威脅與產品防護中心 資深資安威脅研究員
10:00 – 10:30	**精選議程** 漢芝電子
10:40 – 11:10	**量子時代 AI、IoT 與加密貨幣的危機：由 SEALSQ 保護信任重建** 陳聖凱 SK Chen SEALSQ 大中華區業務協理
11:10 – 11:40	**基於 Ascon 確定性隨機位元產生器應用於嵌入式系統** 陳志華 (Abel C. H. Chen) 中華電信研究院 資通安全研究所 高級研究員
11:40 – 12:10	**當無人載具落入敵手：現有資安防線缺失與全面性防禦策略** Robert Wann 伊諾瓦科技股份有限公司 創辦人兼執行長
13:00 – 13:30	**精選議程** 晶心科技
13:30 – 14:00	**精選議程** 熵碼科技
14:00 – 14:30	**從晶片卡到遊戲主機，利用旁通道與錯誤注入攻擊破解黑產的技術實錄** 林高裕 (Gary) 鑑智實相科技股份有限公司 營運長
14:30 – 15:00	**精選議程** 智能資安
15:10 – 15:40	**精選議程** 資拓宏宇
15:40 – 16:10	**車聯網 C-V2X 結合 V2X_PKI 應用情境** 劉子正 中華電信研究院 智慧聯網研究所 分項計畫主持人
16:10 – 16:40	**精選議程** 凌羣電腦

時間/地點	Cyber Talent 資安人才培訓論壇 Cyber Talent 專區
10:00 – 10:30	**精選議程** 林子婷 (飛飛 / Phoebe 菲比) 七維思股份有限公司
10:30 – 10:40	**臺灣數位領域就業金卡** Kevin Sharma Taiwan DIGI Gold Card Community Business Development
10:40 – 10:50	**工作沒有不見，只怕變成你認不得的樣子：AI 時代下的資安人才生存法則** 唐任威 ISC2 Taipei Chapter President
10:50 – 11:20	**精選議程**
11:20 – 11:50	**從化工業環安主管考取 CCSP 到金融業資安治理** 林毅力 金融業 資安治理科 技術副理
11:50 – 12:00	**精選議程** 電腦技能基金會
14:00 – 14:30	**從競技場到戰場：CTF 與 Cyber Range 如何強化資安防禦韌性** Jeff Chao TRAPA Security CEO

時間/地點	CyberLAB 實機演練 702
09:30 – 11:00	實機演練課程
11:30 – 13:00	實機演練課程