

# 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

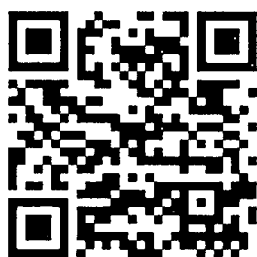
- 指導單位：數位發展部、國家科學及技術委員會
- 主辦單位：iThome 電週文化事業股份有限公司
- 共同主辦單位：趨勢科技股份有限公司

## 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.ihome.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.ihome.com.tw/2026/speaker>



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

| 分堂議程<br>時間/地點 | Data Security 論壇<br>4D 展區會議室                                  | Cyber Technology & Innovation 論壇<br>4E 展區會議室                                                                                                   |
|---------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 12:30 – 13:00 | <b>【Lunch Learning Session】</b><br>精選議程<br>CrowdStrike        | <b>【12:30 – 13:15】</b><br><b>【Lunch Learning Session】【Securing AI 論壇】</b><br>戳破 AI 的防禦幻影：從紅藍隊視角重構 AI 系統安全<br>楊政霖博士<br>奧義智慧科技<br>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<br>許祐福<br>精品科技股份有限公司<br>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？<br>JJ Net                                                                                             |
| 14:45 – 15:15 | 精選議程<br>Zscaler                                               | Agentic AI 實戰應用：重新定義攻擊型資安<br>William Tiew<br>Ridge Security Technology<br>Regional System Engineer Director                                    |
| 15:30 – 16:00 | 精選議程<br>群暉                                                    | 2026 CRA 挑戰倒數！台灣廠商韌性指南<br>陳宗祈<br>Exein<br>Partner & Alliance                                                                                   |
| 16:15 – 16:45 | 精選議程                                                          | <b>【16:15 – 17:00】【Threat Research 論壇】</b><br>SAP as a Cyber Weapon<br>CAIBERP GmbH<br>Researcher, Research<br>- Andreas Wiegstein<br>- Xu Jia |

| 時間/地點         | CyberLAB 實機演練<br>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<br>AIoT & Hardware Security 展區                                                                                                                   |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 13:00 – 13:30 | 精選議程<br>ISA 台灣分會                                                                                                                                                                 |
| 13:30 – 14:00 | 精選議程<br>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<br>Panasonic<br>- Kyo Chen<br>Head, Panasonic Cyber Security Lab<br>- Freddy Ma<br>Senior Threat Intelligence Researcher, Panasonic Cyber Security Lab |
| 14:40 – 15:10 | 精選議程<br>精虞科技                                                                                                                                                                     |
| 15:20 – 15:50 | 如何全方位實踐 IoT 產品資安？以「難打的目標」為例<br>奧義智慧科技<br>- Jimmy Liu<br>資安研究員<br>- Chumy Tsai<br>實習生                                                                                             |
| 15:50 – 16:20 | 精選議程<br>凌華科技                                                                                                                                                                     |
| 16:20 – 16:50 | 精選議程<br>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<br>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 & Government 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<br>時間/地點    | 資安品牌日 –<br>Jamf<br>701A                                                                                                               | AI Security &<br>Safety 論壇<br>701B                                    | 資安品牌日 –<br>Fortinet<br>701C                                         | 資安品牌日 –<br>數位資安<br>701D                                                             | 資安品牌日 –<br>HENNGE<br>701E | 資安品牌日 –<br>艾盾資科<br>701F                                                                                              | 雲端安全論壇<br>701G                                                        | Cyber<br>Technology &<br>Innovation 論壇<br>701H                                              | Cyber<br>Technology &<br>Innovation 論壇<br>703                                       | 醫療資安論壇<br>4A 展區會議室                                                                                             | Secure<br>Software &<br>DevSecOps 論<br>壇<br>4B 展區會議室                                                           | Security<br>Strategy &<br>Case Study<br>4C 展區會議室                                                               |  |
| 14:00 –<br>14:30 | 現代化行動資安新標準：從端點防禦到零信任架構<br>Glee Tsai<br>Jamf<br>亞太區資深技術顧問                                                                              | 精選議程<br>CHT                                                           | 守護現在，預見未來：FortiGate 打造 AI 時代的「全能守護者」<br>余昇瀚<br>Fortinet<br>技術顧問     | 精選議程<br>數位資安                                                                        | 精選議程<br>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<br>陳長志<br>艾盾資科股份有限公司<br>Director of SecOps                                      | 雲端韌性：從供應鏈事件看<br>+C23+C8:G1+C8:G11<br>邱永興<br>中華資安國際股份有限公司<br>SOC 服務部協理 | 精選議程<br>勤晃                                                                                  | 精選議程<br>邁達特                                                                         | 精選議程<br>李建璋<br>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<br>鄭禹誠 (Fiona Cheng)<br>偉康科技股份有限公司<br>產品研發部 資深研發經理                                 | 精選議程<br>AEB                                                                                                    |  |
| 14:45 –<br>15:15 | 打破邊界：建構 iOS 與 Android 跨平台行動防禦陣線<br>Stone Chen<br>Jamf<br>亞太區資深業務代表                                                                    | Prompt Attack：LLM 無法迴避的核心安全破口<br>邱銘彰 (Birdman)<br>奧義智慧科技<br>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。<br>孫嘉陽<br>Fortinet<br>技術顧問         | 精選議程<br>數位資安                                                                        | 精選議程<br>HENNGE            | 序幕：台灣產業的「上雲困境」，Wiz 極小化雲端成本將解憂<br>羅煜賢<br>艾盾資科股份有限公司<br>Technical Consultant<br>Director                               | 精選議程<br>CrowdStrike                                                   | 後量子密碼學 - 守護未來資訊安全的數位盾牌<br>林邦維博士<br>中華電信研究院<br>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？<br>Digicert                                  | 醫療領域之 OT 資訊安全防護特殊性介紹<br>張韶良<br>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 打造通式層級的防護迷宮<br>陳忠義<br>ICEShell 艾斯冰殼 Security Compiler Engineer, R&D Dept.                          | 精選議程<br>Pentera Cyble_ABP                                                                                      |  |
| 15:30 –<br>16:00 | 貓鼠遊戲：解析國家級駭客的行動裝置攻擊策略<br>Elad Shapira<br>Jamf<br>資深資安研究員                                                                              | 精選議程<br>逸盈                                                            | AI 新賽局：在合規與創新中取得平衡<br>李翹<br>Fortinet<br>技術顧問                        | 精選議程<br>數位資安                                                                        | 精選議程<br>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<br>羅煜賢<br>艾盾資科股份有限公司<br>Technical Consultant<br>Director                  | 雲地混合監控的機會與挑戰 - 以及 AI 治理<br>詹曉容<br>雲力橋子<br>資訊安全部                       | 從「自動化」邁向「自主化」Agentic AI NDR 時代<br>林孟忠 (Sam Lin)<br>ExtraHop<br>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<br>盧惠光<br>台灣二版有限公司<br>高級產品經理                    | 精選議程<br>許權廣 (Rock)<br>陽明交大竹銘醫院                                                                                 | LLM 與 DevSecOps 相遇：AI-Powered DevSecOps 的機會與風險<br>Archer Tsai<br>華碩電腦股份有限公司<br>數位安全中心 安全架構部 Security Architect | 【Secure Software & DevSecOps 論壇】<br>不要碰我的 DRIVER!!!<br>Jason Huang<br>TXOne Networks Inc.<br>資安威脅與產品防護中心 主任工程師 |  |
| 16:15 –<br>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<br>- Jimmy Huang<br>Jamf 亞洲區總經理<br>- Stone Chen<br>Jamf 亞太區資深業務代表<br>- 郭杰穎 (Mouse Kuo)<br>可立可 執行長兼共同創辦人 | 精選議程                                                                  | 企業資安安全治理實務：透過 AI 打破傳統 DLP 的盲點，資料外洩保護不再瞎忙<br>呂政穎<br>Fortinet<br>技術顧問 | 精選議程<br>數位資安                                                                        | 精選議程<br>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<br>羅煜賢<br>艾盾資科股份有限公司<br>Technical Consultant<br>Director | 雲端之戰-AI 事變與重啟過遊<br>黃星評 (Kuro Huang)<br>ISC2 Taipei Chapter 理事         | 【Securing AI 論壇】<br>關於 AI 助理凌晨放火燒了公司還順便找 FBI 這檔事<br>游照臨 (Steven Meow)<br>趨勢科技<br>紅隊 資安威脅研究員 | 【Threat Research 論壇】<br>關上 Windows，戰鬥才開始！macOS 在企業安全的崛起與挑戰<br>葉東逸 (Kazma)<br>奧義智慧科技 | AI 軟體器材的資安實戰：從美國 FDA 524B 規範到 Threat Modeling 與 Patch SLA 的完整落地<br>林家聖<br>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？<br>盧建成 (Augustin Lu)<br>靖本行策有限公司<br>CEO、政治大學資訊科學系 兼任助理教授                | 【16:15 – 17:00】<br>【SecOps 論壇】<br>OPNsense×Suricata + SmartNIC 高效能防護實戰<br>鄭明彰<br>南投縣教育網路中心系統組 組長               |  |

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

| 時間/地點         | AIoT & Hardware Security Summit<br>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<br>楊明儒<br>昇頻股份有限公司<br>總經理室                                                                 |
| 13:30 – 14:00 | 精選議程<br>精虞科技                                                                                                         |
| 14:10 – 14:40 | AI 機器人資安攻防實例<br>Aaron Luo<br>VicOne Inc<br>LAB R7 資深威脅研究經理                                                           |
| 14:40 – 15:10 | 精選議程<br>速碼波科技                                                                                                        |
| 15:20 – 15:50 | 精選議程<br>亞力通訊                                                                                                         |
| 15:50 – 16:20 | 精選議程<br>聯發光電                                                                                                         |
| 16:20 – 17:00 | 擊石清障：從韌性到卓越這條路，有夠難<br>ASUS Digital Security Center<br>- 許宗仁 (TJ Hsu)<br>資安威脅分析師<br>-黃鴻碩 (Harold Huang)<br>威脅偵測與應變分析師 |

| 時間/地點         | Cyber Talent 資安人才培訓論壇<br>Cyber Talent 專區                                                          |
|---------------|---------------------------------------------------------------------------------------------------|
| 14:00 – 14:30 | 他們說我是沒有用的年輕人<br>PD Lee<br>自由工作者<br>資安流浪漢                                                          |
| 14:30 – 14:45 | 精選議程<br>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)<br>陳瓊茹<br>MISO<br>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<br>劉孟昌 (Piner Liu)<br>安碁學苑股份有限公司 ACSI Cyber Security Academy<br>營運長 COO |
| 15:40 – 15:50 | 精選議程<br>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<br>謝博尊<br>中華電信<br>資通安全處 資安工程師                                           |

| 時間/地點         | CyberLAB 實機演練<br>702 |
|---------------|----------------------|
| 12:30 – 14:30 | 實機演練課程               |
| 15:00 – 17:00 | 實機演練課程               |

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

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

| 分堂議程<br>時間/地點 | AI Security & Safety 論壇<br>701B                                                                               | 上市櫃資安標竿論壇<br>701C | CISO 論壇<br>701D                                                                                                                                                                                               | 攻擊型安全論壇<br>701E                                                                                         | 後量子密碼論壇<br>701F                                                               | EU CRA 論壇<br>701G                                                                                                   | AI Governance 論壇<br>701H                                                                              | Cyber Marketing & Sales 論壇<br>703                                                                                                                                  | Threat Research 論壇<br>4A 展區會議室                                                                                                                                      | Privacy & Data Protection 論壇<br>4B 展區會議室                                                                               | OT Security 論壇<br>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<br>曹家通<br>Westcon Taiwan<br>首席資安顧問                                   | 見【表一】上市櫃資安標竿論壇    | Security Without Borders: Breaking Language and Cultural Barriers to Harmonize Global Security Operations<br>Jesse Ku<br>Bora Pharmaceuticals<br>Global Cybersecurity Manager                                 | 精選議程<br>張克勤                                                                                             | 精選議程<br>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<br>YU-YU OETTING<br>德國 Lookoon Security GmbH (資安攻防)<br>Strategic Partner | 【Digital Trust 論壇】<br>精選議程<br>謝君豪                                                                     | Solving Security in a World That Changes Faster Than Your Tools<br>Philip Sow<br>Proofpoint<br>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<br>林宜平<br>Fortinet<br>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<br>國家資通安全研究院 - 陳正庭 Chen, Justyn<br>架構設計組 機器學習工程師<br>- 許德丞 Andy Te-Cheng Hsu<br>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<br>Steven Hsu (許育誠)<br>TXOne Networks Inc.<br>Vertical Evangelist 副總                                                                               |
| 14:45 – 15:15 | 精選議程<br>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<br>Hans Wang<br>CHT Security<br>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<br>陳志華 (Abel C. H. Chen)<br>中華電信研究院<br>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?<br>Richard Lin<br>台達電子工業股份有限公司<br>產品資安事業部 資安架構主管                                            | 精選議程<br>黃添澤<br>中華民國電腦稽核協會                                                                             | Cybersecurity Is Far Sexier Than What You Think, and Have Been Saying<br>Annie Quynh Anh - Tech Lady<br>VinCSS<br>Internet Security Services JSC Head of Marketing | Clean Redirects, Dirty SYSTEM: Bug Hunting by Abusing File Operations for Silent Privilege Escalation<br>Sharkkcode<br>TeamT5 杜浦數位安全 Research Engineer, Engine Team | 具身 AI 走進家：隱私攻防新戰場<br>朱益宏<br>VicOne<br>RD 架構師                                                                           | Beyond the Headlines: Protecting Infrastructure from Industrial Cybersecurity Threats<br>Chuck Weissenborn<br>Dragos, Inc.<br>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<br>Deloitte                                                          |                   | 【OT Security 論壇】<br>超越 EPSS：打造更準確的 OT 漏洞利用預測系統<br>TXOne Networks, Threat Signature Research Team - Daniel Chiu<br>Senior Threat Signature Research Team Manager - Queenie Liao<br>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<br>Annie Shih<br>QNAP Systems, Inc.<br>General Counsel, Legal & IP | 淺談 PQC 與實務操作<br>Retro Kuo<br>Google Cloud<br>Customer Engineering             | 歐盟 CRA 倒數啟動：產品資安合規的三大關鍵策略<br>Daniel Liu<br>安華聯網科技 (DEKRA 德凱集團成員)<br>營運中心 技術長                                        | AI 專案管理基本功：來自於 PMBOK 的啟發<br>Bright Wu<br>Aon Taiwan<br>Executive Director, Taiwan Regional Cyber Risk | 【Threat Research 論壇】<br>你的輸入法正在背後偷監視你<br>Nick Dai<br>趨勢科技<br>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<br>黃智威<br>TXOne Networks Inc.<br>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<br>鄧耀東<br>帝淵智慧科技股份有限公司<br>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<br>Mars Cheng<br>TXOne Networks Inc.<br>資安威脅與產品防護中心 資深經理                                                                                       |
| 16:15 – 16:45 | 【16:15-17:00】<br>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<br>馬聖豪<br>TXOne Networks Inc.<br>資安威脅與產品防護中心 Team Lead |                   | 精選議程                                                                                                                                                                                                          | 【16:15-17:00】<br>從 150 場紅隊演練數據看產業安全<br>徐念恩<br>戴夫寇爾股份有限公司<br>管理部 資深副總                                    | 精選議程<br>陳君朋                                                                   | 基於 ISA/IEC 62443 的歐盟網路韌性法案(EU CRA)合規路徑<br>Kenny Lee<br>SGS<br>Head of Cybersecurity Laboratory, CDTL                | 【16:15-17:00】<br>AI 改變企業治理底層邏輯—資安、個資、智財管理的再設計<br>鄒宗萱<br>財團法人資訊工業策進會<br>科技法律研究所 副所長                    | 【Threat Research 論壇】<br>都 6202 年了！Relay Attack 未死，而且還更好用！<br>Wesley Fu<br>趨勢科技<br>Threat Researcher                                                                | 【16:15-17:00】<br>Beyond the SERP：當黑帽 SEO 行動演變為多面向的犯罪威脅<br>Joey chen<br>Cisco Talos<br>Leader, Security Research                                                     | 精選議程<br>陳明皇<br>國立成功大學 計算機與網路中心                                                                                         |                                                                                                                                                                              |

| 分堂議程<br>時間/地點 | SecOps 論壇<br>4D 展區會議室                                                                                                                 | Securing AI 論壇<br>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<br>Gary Sun<br>奧義智慧科技<br>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<br>曲卓榮<br>中華電信研究院<br>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<br>林伯駿<br>友達光電股份有限公司<br>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」<br>廖冠倫 (Steve Liao)<br>奧義智慧科技<br>資料科學家                                                                       |
| 11:00 – 11:30 | 精選議程<br>黑貓                                                                                                                            | 敵人就在本能寺 - 企業應用 AI Agent 風險剖析<br>Will Lin<br>華碩電腦<br>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<br>吳肝語<br>錄恩帕斯科技股份有限公司<br>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<br>黃智威<br>TXOne Networks Inc.<br>資安威脅與產品防護中心 資深資安威脅研究員 |
| 分堂議程<br>時間/地點 | Incident Response 論壇<br>4D 展區會議室                                                                                                      | Web3 安全論壇<br>4E 展區會議室                                                                                                                  |
| 12:40 – 13:10 | 【Lunch Learning Session】【攻擊型安全論壇】<br>同行 20 年：從攻防兩端看見台灣資安的下一步<br>- 翁浩正<br>戴夫寇爾 DEVCORE 執行長<br>- 陳浩維<br>酷澎股份有限公司 臺灣暨日本資安長               | 【Lunch Learning Session】【AI Defense 論壇】<br>用你的魔法對付你！當 Vibe 詐騙遇上 Vibe 駭客！<br>游照臨 (Steven Meow)<br>趨勢科技<br>紅隊 資安威脅研究員                    |
| 14:00 – 14:30 | 【醫療資安論壇】<br>讓醫療產業再次 Level up：淺談 Health Level 7 的資安問題及展望<br>Linwei Tsao<br>TXOne Networks Inc.<br>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<br>朱妍如<br>安永諮詢股份有限公司<br>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<br>陳兆閔<br>奧義智慧科技<br>資安研究員                                                                                     | RWA × 穩定幣 × 金庫落地安全概觀<br>凱特納科技<br>- 曾信田 (Newbug Tseng)<br>創辦入暨執行長<br>- 李尚韋 (Turkey Li)<br>共同創辦人暨策略長                                     |
| 15:30 – 16:00 | 精選議程<br>萬建笙<br>登豐數位科技股份有限公司                                                                                                           | 探討「硬體錢包結合 TSS 門框簽章」的新託管範式<br>CYC<br>AMIS, Maicoi<br>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<br>ASUS, Digital Security Center<br>- 許宗仁 (TJ Hsu)<br>資安威脅分析師<br>- 李東育(Eric Li)<br>威脅偵測與應變分析師 | Drainer-as-a-service: 陰影下的商業模式<br>Vic Huang<br>UCCU Hacker<br>成員                                                                       |

| 時間/地點         | 金融資安論壇<br>701A                                                                                          |
|---------------|---------------------------------------------------------------------------------------------------------|
| 09:30 – 09:35 | 開場致詞<br>吳其勳<br>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<br>林裕泰<br>金融監督管理委員會<br>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？<br>陳詒昌<br>台新新光金控 / 台新銀行<br>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<br>簡經緯 (Fredo Chien)<br>安聯證券投資信託股份有限公司<br>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<br>Sonia Peng<br>美商達信保險經紀人股份有限公司台灣分公司<br>Information Security Manager, CEO Office |
| 16:15 – 17:00 | AI 資安檢測<br>萬幼筠                                                                                          |

| 時間/地點         | 【表一】上市櫃資安標竿論壇<br>701C                                                            |
|---------------|----------------------------------------------------------------------------------|
| 14:00 – 14:30 | 精選議程                                                                             |
| 14:45 – 15:15 | 精選議程<br>易換標<br>遠東新世紀股份有限公司                                                       |
| 15:15 – 15:35 | 精選議程<br>創泓                                                                       |
| 15:50 – 16:20 | 您的資安聯防真的有達到預期的效果嗎？<br>陳昱崇 (Zero Chen)<br>伊雲谷數位科技<br>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<br>Sam Chan<br>自由系統股份有限公司<br>資安服務部 資深資安經理        |

| 時間/地點         | AIoT & Hardware Security Summit<br>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<br>Yenting Lee<br>TXOne Networks Inc.<br>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<br>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<br>陳聖凱 SK Chen<br>SEALSQ<br>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<br>陳志華 (Abel C. H. Chen)<br>中華電信研究院<br>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<br>Robert Wann<br>伊諾瓦科技股份有限公司<br>創辦人兼執行長                               |
| 13:00 – 13:30 | 精選議程<br>晶心科技                                                                                      |
| 13:30 – 14:00 | 精選議程<br>燐碼科技                                                                                      |
| 14:00 – 14:30 | 從晶片卡到遊戲主機，利用旁道與錯誤注入攻擊破解黑產的技術實錄<br>林高裕 (Gary)<br>鑑智實相科技股份有限公司<br>營運長                               |
| 14:30 – 15:00 | 精選議程<br>智能資安                                                                                      |
| 15:10 – 15:40 | 精選議程<br>資拓宏宇                                                                                      |
| 15:40 – 16:10 | 車聯網 C-V2X 結合 V2X_PKI 應用情境<br>劉子正<br>中華電信研究院<br>智慧聯網研究所 分項計畫主持人                                    |
| 16:10 – 16:40 | 精選議程<br>凌羣電腦                                                                                      |

| 時間/地點         | Cyber Talent 資安人才培訓論壇<br>Cyber Talent 專區                                              |
|---------------|---------------------------------------------------------------------------------------|
| 10:00 – 10:30 | 精選議程<br>林子婷 (飛飛 / Phoebe 菲比)<br>七維思股份有限公司                                             |
| 10:30 – 10:40 | 臺灣數位領域就業金卡<br>Kevin Sharma<br>Taiwan DIGI Gold Card Community<br>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<br>唐任威<br>ISC2 Taipei Chapter<br>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<br>林毅力<br>金融業<br>資安治理科 技術副理                                  |
| 11:50 – 12:00 | 精選議程<br>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<br>Jeff Chao<br>TRAPA Security<br>CEO            |

| 時間/地點         | CyberLAB 實機演練<br>702 |
|---------------|----------------------|
| 09:30 – 11:00 | 實機演練課程               |
| 11:30 – 13:00 | 實機演練課程               |