

# CYBERSEC 2025 臺灣資安大會 Day1 4/15 (二) 總議程表

## WE ARE TEAM CYBERSECURITY

最新大會議程請至大會網站，或掃描 QRcode 下載大會超便利 APP 查看：



IOS 下載  
https://t.ittho.me/APP\_IOS



Android 下載  
https://t.ittho.me/APP\_Android

### 7F 會議室

08:00	來賓報到													
09:30 - 09:35	大會開幕致詞													
09:35 - 09:40	貴賓致詞													
09:40 - 09:45	貴賓致詞													
10:00 - 10:30	AI 世代的網路犯罪趨勢與資安防禦革命													
10:30 - 11:00	Scaling Up Your Cybersecurity													
11:00 - 11:30	The Digital Blockade War Game: What we learned at DefCon and Blackhat													
11:30 - 14:00	Lunch & Break													
分堂議程	AI Security & Safety 論壇	Exposure Management 論壇	CISO 論壇	InfraSec 論壇	Data Security 論壇	Cyber Technology & Innovation 論壇				資安品牌日				
時間 / 地點	701B	701D	701G	702	4A 展場會議室	701F	701H	703	1B 展場會議室	智慧資安	Cloudflare	CrowdStrike	Google Cloud	
										701A	701C	701E	1A 展場會議室	
14:00 - 14:30	AI 掀起的猜疑遊戲怎麼玩？中小企業的資安心法與終局攻略 蔡明見 兆勤科技股份有限公司 總經理	以零信任準則全面識別各類設備風險，不遺漏任何資產！ 張恩綾 Forescout 台灣區總經理	導入 NIST CSF 以因應網路安全風險之經驗分享 賴居正 富邦人壽 資訊安全部部長、協理	智慧 XDR 防護   IT 與資安無縫整合 游政卿 黑貓資訊 總經理	解構內部威脅，識別風險與主動回應 陳育徽 精品科技股份有限公司	資料保護解決方案實際案例分享與剖析 陳盈良 Dell Technologies 資深技術顧問	全域視角的威脅預測：AI與資安在數位未來的聯防方案 林佑儒 極風雲創 創新技術研究發展處處長	AI 驅動的風險：機器身份管理與 TLS 證書的挑戰 莊龍源 CyberArk 北亞區技術部 總監	資安風險不可見？如何透視企業的隱藏威脅 李元勳 Tenable Inc. 技術顧問	Passkey與特權帳號管理系統整合—零信任架構下，如何實現組織內使用者安全登入 沈泓智 智慧資安科技 技術服務處 技術經理	Immerse Taipei : Opening & CyberSecurity Survey Report Ben Munroe Cloudflare VP, APJC Field Marketing	Power of The Crowd : Faster Results. Better Security. Lower Cost Chok Chiat Ho CrowdStrike 東南亞及北亞區 業務工程主管	剖析台灣安全性威脅現況：Google Threat Intelligence 洞察 Su Gim Goh Google Cloud Regional Security Architect	
14:45 - 15:15	從資料分類到行為分析：Forcepoint 如何用 AI 守護關鍵資料？ Ray Pai Forcepoint 技術顧問	vRx 從被動檢測到主動解決 AI 與社群的力量 Oren Maguid Vicarius Regional VP	AI 世代下的資安威脅應對策略 王信富 中華資安國際股份有限公司 技術處副總	安全優先！以零信任佈建網路安全網 陳清淵 慧與科技股份有限公司 Aruba 台灣區 技術副總經理	合規的盲點：當資料庫稽核成為一場自欺欺人的投資 Santa Ye 智安數據科技 產品技術部 資深技術顧問	十年信賴：HCLSoftware 以可靠的資安實力推動數位轉型 Terry Leung HCLSoftware 北亞區 總經理	Elastic AI+ML Security：智能分析日誌，快速應對告警，突破傳統 SIEM 限制 Jason Chan Elastic Senior Solutions Architect	解碼 5G 大數據：全網流量分析實務應用與安全防護新視野 姜家齊 威睿科技 技術長	強化企業核心：利用 NetApp 技術鞏固數據防線 吳偉壽 NetApp 技術顧問	DevSecOps中，您可能沒想到的軟體供應安全，從案例中學 林皇興 達友科技股份有限公司 副總經理、CISSP	Modernize Your Applications with AI and Advanced Security Steven Yang Cloudflare Senior Solutions Engineer	Keeping Up with the Ever-Changing Cloud Battlefield 蔡偉良 CrowdStrike 亞太及日本 雲端安全業務總監	次世代雲端原生防火牆：安全也可以很簡單 郭峻嘉 Google Cloud Customer Engineering	
15:30 - 16:00	AI：網路安全自動化的驅動力，融合人類洞察與機器效能 Coco Wang SentinelOne APAC Channels Director, Security Engineering	從效能監控到威脅預警：Flowmon 在網路管理中的應用解析 侯俞帆 零壹科技 資深技術顧問	AI 世代下的資訊安全挑戰 周裕華 OPSWAT North Asia Solution Engineer	Hybrid 無所不在，Citrix 如何應對資安挑戰？ 洪富凱 Citrix Asean GM of Citrix Taiwan	企業機敏文件保護全攻略 羅文聰 以柔資訊股份有限公司 創辦人	後量子密碼論壇 後量子密碼遷移趨勢 陳君明	AI Security & Safety 論壇 迎向AI時代的資安防護新思維 吳啟文 國家資通安全研究院 前副院長	AI in Action - AI 浪潮下 SASE 雲平台的應用與防護 宋建宏 Cato Networks SASE 資深架構師	AI Security & Safety 論壇 AI創新應用與資安治理 王仁甫 元智大學 資管系 專任助理教授	從OT到CPS，工控安全再進化 詹鴻基 Claroty 大中華區 技術顧問	Fireside Chat Zangwill Kwan Cloudflare Senior Sales Manager	用次世代的 SIEM 建構現代化的 SOC 陳建民 CrowdStrike Regional Sales Engineer 技術顧問	最新威脅情報與 AI 主導資安營運技術 Patrick Chiu Google Cloud Security Customer Engineering	
16:15 - 16:45	孤獨的情資分析師：情資自動化搜集及整合 陳憶賢 奧義智慧科技 資安研究員	【16:15 - 17:00】老闆：我全都要。爭什麼，摻在一起做成情資 許宗仁 ASUS Threat Analyst 陳星賢 ASUS Threat Analyst	【16:15 - 17:00】掌握威脅的演變：如何打造前瞻性防守心態，提前擊退新興攻擊 Jesse Ku Bora Pharmaceuticals Global Cybersecurity Manager	【16:15 - 17:00】地緣政治風暴與企業韌性：在變局中駕馭不確定性 曾鈞 安永諮詢股份有限公司 諮詢顧問、執行副總經理	從上市櫃公司到各產業組織，加速達成 ISO27001 資料安全合規性之策略解析 童敬霖 群暉科技 技術客戶經理	【16:15 - 17:00】你以為有 EDR 就安全了？探索攻擊者如何繞過防禦系統 莊友豪 中華資安 監控科資安工程師	【16:15 - 17:00】核級遊戲防護神仙大戰：拆解現代 Hyper-V架構戰勝系統核心外掛威脅 徐念恩 戴夫寇爾股份有限公司 管理部資深副總	【16:15 - 17:00】撥開語言模型偏好迷霧：通往資安評估穩定性的道路 陳樞元 奧義智慧科技 Data Scientist	SecOps 論壇 TXOne Networks Inc. - 蔡耀德 資安威脅研究員 - 馬聖豪 Team Lead	解碼AI網路安全未來戰場 藍博彥 Palo Alto Networks 台灣首席技術顧問	Unlocking Potential Together: The Role of Partners in Cloudflare's Vision Jo Goh Cloudflare ASEAN & GCR Director Partner Sales	透過 Falcon Identity Protection 實現強大的零信任安全性 Richard Lee CrowdStrike 北亞區技術顧問	Google Cloud CNAPP 解決方案：全方位保護您的雲端環境安全 鄭家明 Google Cloud Customer Engineering	

分堂議程	※ Threat Research 論壇
時間 / 地點	4C 展場會議室
12:00 - 12:30	Lunch Learning Session 你的網路設備正在背叛你：從默默運作到成為威脅核心 Lyn Chuang 趨勢科技 技術顧問
14:00 - 14:30	The key ingredient in modern cyber attack - an Infostealer Leonid Rozenberg Hudson Rock Cybercrime and Threat Intelligence Researcher
14:45 - 15:15	黑帽更新技法：濫用過度被信任的系統升級器來降級你電腦的一切防護？ Yi-An Lin TXOne Networks Inc. 資安威脅研究員
15:30 - 16:00	讓 ELF 貓在台灣產業網路中到處鑽洞是正常的嗎？ 夜貓 Fortinet Anti-Virus Analyst
16:15 - 17:00	CoralRaider 瞄準受害者數據和社交媒體帳戶 Cisco Talos - Joey Chen Sr. Threat Researcher Chetan Raghuprasad Threat Researcher

※ 本會議室提供 AI 即時中英文翻譯

### AIoT & Hardware Security Summit

時間 / 地點	4F AIoT & Hardware Security 專區
13:30 - 14:00	CRA 倒數計時：如何補強 ISA/IEC 62443 解鎖資安韌性？ Michael Yao ISA 台灣分會 Program Chair
14:00 - 14:30	安全晶片、藍牙模組、PKI 加速 Matter 合規，部署智慧家庭市場 邱志成 全景軟體股份有限公司 物聯網發展部 資深顧問
14:30 - 15:15	無聲瘟疫來襲：工業物聯網三重防禦劍指行動網路資安漏洞 Alpha Chen 昇頻股份有限公司 執行長 Jason Huang 訊勢科技股份有限公司 執行長
15:20 - 15:50	護國神山保衛戰：從 SECS/GEM 標準來看晶片製造安全 Yenting Lee TXOne Networks Inc. 資深資安威脅研究員
15:50 - 16:20	使用 RISC-V 構建可信執行環境 (TEE) 陳本奇 晶心科技股份有限公司 資深技術經理
16:20 - 16:50	從晶片到系統：原生硬體安全金鑰的定位及其應用 梁淳皓 振生半導體股份有限公司 類比設計經理

### CyberLAB 實機演練

時間 / 地點	4D 展場會議室
12:30 - 14:30	實際案例解析-創造全面防護的AI安全環境 趨勢科技 資深技術顧問 - 任宗偉 - 邱柏翰
15:00 - 17:00	

# CYBERSEC 2025 臺灣資安大會 Day2 4/16 (三) 總議程表

WE ARE TEAM CYBERSECURITY

最新大會議程請至大會網站，或掃描 QRcode 下載大會超便利 APP 查看：



IOS 下載  
https://r.ittho.me/APP\_IOS



Android 下載  
https://r.ittho.me/APP\_Android

## 7F 會議室

08:00 - 09:30	來賓報到	
09:30 - 09:35	大會開幕致詞	吳其勳 / CYBERSEC 2025 臺灣資安大會 主席、iThome 總編輯
09:35 - 10:05	主權 AI 與韌性國家	李育杰 / 國家安全會議 諮詢委員
10:05 - 10:30	Digital Sovereignty: Security of the Information Space in Democracy	Ing. Jan Bartošek, Deputy Speaker, Chamber of Deputies Parliament of the Czech Republic
10:30 - 11:00	Emerging Artificial Intelligence Threats	Christopher B. Porter, Head of International Security Cooperation, Google Cloud
11:00 - 11:30	The Cyber Express: Securing Railways in a Connected World	Dimitri van Zantvliet, Cybersecurity Director, CISO, Dutch Railways
11:30 - 14:00	Lunch & Break	

大會主題演講會場  
701ABCD 會議室

分堂議程	AI Security & Safety 論壇	Cloud Security 論壇	Security Strategy & Case Study	Cyber Technology & Innovation 論壇				資安品牌日										
				卡巴斯基	Fortinet	艾盾資科	HENNGE	卡巴斯基	Fortinet	艾盾資科	HENNGE							
時間 / 地點	701B	701D	4A 展場會議室	701F	703	701A	701C	701E	1A 展場會議室	701A	701C	701E	1A 展場會議室					
14:00   14:30	Nick Cheng Google Cloud Customer Engineering	范茗閣 F5台灣區 技術顧問	Nico Chen NEITHNET 防駭架構部 專案經理	許祐福 精品科技 資安顧問	Allen Lin A10 Networks 台灣區 技術經理	黃茂勳 卡巴斯基 銷售總監	鄭偉基 Fortinet 北亞區市場總監、 首席信息安全官	- Shaul Holtzman Intezer Labs Director of Solutions Engineering	Jon Gaul HENNGE K.K. Cloud Product Development Software Engineer	內部威脅的真相： UAM+AI 掌握員工 不當行為	新一代 Web 應用程 式防護	新一代安全 Kaspersky NEXT	安全納入設計： CISO 需要了解的原則、 承諾與實踐方法	SOC/MDR 資安 分析師如何在從業 中，贏得掌聲與人生	AI 與資安：對企業 帶來的威脅及機會			
14:45   15:15	零信任的回顧與 AI 的整合	新世代 MSSP 資安 威脅防禦：在雲地 混合架構下打造智 慧防線	數位身分識別與零 信任管理策略藍圖	CISO 論壇 資安長與未來資通 安全領導者的六頂 思考帽：全面守護 企業資安的創新思 維	攻擊型安全論壇 滲透測試入門不求 人：老闆我找到洞 了！	資安情資運用案例 分享	AI 驅動的雲原生應 用保護	秘密實體走訪各地 調查，去年底始 的醫療攻擊事件佈 局調查首公開	2025 與密碼在愛與 痛的邊緣	梁耀康 Zscaler 亞洲區 技術總監	李德政 雲力橘子數位股份 有限公司 售前規劃顧問	黃旭鍵 勤業眾信聯合 會計師事務所 科技與轉型服務部 門 協理	小P ISACA總會 外部專家委員	游鎮毓 Appier Senior Software Engineer	謝長軒 卡巴斯基 台灣技術總監	王仁德 Fortinet 雲端領域 資安技術顧問	羅煜賢 艾盾資科股份有 限公司 Technical Consultant Director	Chan Sau Yee HENNGE K.K. Cloud Product Development Division Software Engineer
15:30   16:00	人工智慧系統的安全治理，價值對齊與驗證	雲端數據安全與韌 性：從威脅防禦到 災後復原的全面戰 略	海洋研究機構資安 治理初探與未來展 望	CISO 論壇 不知不覺，你就變 成內鬼	攻擊型安全論壇 我打你應該，不 打你悲哀	技術聯盟、供應鏈 安全	AI 驅動的智能防護 與高效運營	我可能錯了：財富 巨企雲端安全 的第一堂課	雲端檔案安全： 2025 資料洩露風險 與如何防範	萬幼筠 國立政治大學 法律系兼任助理教 授	盧惠光 台灣二版有限公司 高級產品經理	許友貞 財團法人國家實驗 研究院台灣海洋科 技研究中心 正工程師兼組長	許權廣 陽明交通大學竹銘 醫院 資訊長	PD Lee 自由工作者 資安流浪漢	Jeremy Carlson 卡巴斯基 GAM Technology Alliances and OEM	李鵬 Fortinet 技術顧問	陳長志 艾盾資科股份有 限公司 Director of SecOps	徐聖翔 HENNGE K.K. HENNGE One Product Manager
16:15   16:45	AI 外部資產曝險管理與合規	雲端資源與財務管 理：從降低成本到 資源有效運用的管 理方針	SecOps 論壇 漏洞補不完！但更 付不起企業失控的 風險！一起來探討 如何掌握漏洞管理 的關鍵吧！	CISO 論壇 Metrics: Confronting Cybersecurity with data	攻擊型安全論壇 EDR 的魔力探知修 行：從規避手法中 鍛鍊偵測能力	工控安全案例分享	要的不止是合規！ 看 FortiDLP 如何讓 數據安全更智能、 更全面	把重複的事自動 化，一週工作 4 小 時 - 將心力投資於 副業	你的資安意識，決 定公司的命運：社 交工程演練之必要	叢培侃 (PK) 奧義智慧科技 資安長暨共同創辦 人	廖柏命 勤業眾信聯合會計 師事務所 副總經理	Resen Tuan 趨勢科技 Information Service APAC Information Technology IT	李彥民 SHOPLINE CISO	TeamT5 杜浦數位安全 - LiYu Project Manager	謝長軒 卡巴斯基 台灣技術總監	林裕祥 Fortinet 首席工程師	羅煜賢 艾盾資科 股份有限公司 Technical Consultant Director	HENNGE 台灣區頂益 - Kevin Chang 行銷經理 - Karen Chang 銷售經理

分堂議程	※ Threat Research 論壇		※ SecOps 論壇	
	時間 / 地點	4B 展場會議室	時間 / 地點	4C 展場會議室
12:00   12:30	Lunch Learning Session AI Security & Safety 論壇	Lunch Learning Session	Lunch Learning Session	Lunch Learning Session
12:00   12:30	LEARN LLM Security	蔡凱翔 趨勢科技 SPN Architect	18 年了，AD 還在被打：談談微軟安全 編年史	姜尚德 奧義智慧科技 資安研究副處長
14:00   14:30	Kimsuky 持續進化：在新環境中的攻擊 策略演進	Neo Chen TeamT5 杜浦數位安全 威脅情報研究員	藍隊偵測的最後一哩路：融入偵測工程 進行威脅偵測	TXOne Networks Inc. - Mars Cheng 資深威脅研究經理 - Dexter Chen 威脅研究員
14:45   15:15	用 30 分鐘解析八大 C2 工具	Hubert Lin Netskope Principal Threat Researcher	No Hunt, No Insight: 基於代管服務經 驗的威脅狩獵心法	TeamT5 杜浦數位安全 - LiYu Project Manager - Kai Security Engineer
15:30   16:00	SneakyChef Espionage Campaign: Unveiling the Multi-Stage attack on Global Government entities	Chetan Raghuprasad Cisco Talos Threat Reseacher	以藍隊角度出發：企業應如何兼顧雲地 混合安防防護	陳昱崇 伊雲谷數位科技股份有限公司 MSSP Director
16:15   16:45	【16:15 - 17:00】 全球固網商與網路終端設備的安全探討 (與如何研究它們)	Ta-Lun Yen TXOne Networks Inc. Sr. Vulnerability Researcher	Zero to FIRST	許宗仁 ASUS Threat Analyst

※ 本會議室提供 AI 即時中英文翻譯

分堂議程	零信任論壇	
	時間 / 地點	1B 展場會議室
12:00   12:45	Lunch Learning Session AI Security & Safety 論壇	Lunch Learning Session
12:00   12:45	保持絕對專注，以打造次世代 AI 端點語義偵 測	TXOne Networks Inc. - Yi-An Lin 資安威脅研究員 - 馬聖豪 Team Lead
13:00   13:30	通過思想鏈將最先進的大語言模型煉成 7/24 隨時待命的逆向專家	TXOne Networks Inc. - Yi-An Lin 資安威脅研究員 - Jair Chen 資深資安威脅研究員
14:00   14:30	零信任!連帳號管理都沒做好怎麼信任!	黃建笙 (方丈) 登豐數位科技 總經理
14:45   15:15	零信任安全模型：實務導入的挑戰與機遇	孫漢傑博士 中華電信研究院 主任級研究員
15:30   16:00	隨著 AI 的日益普及，如何使用 Zero Trust 網 路來提高網路彈性	Louis Cheung Illumio 亞太地區 高級區域安 全主管
16:15   17:00	Secure by Default: 用 Serverless 實作零 信任的 Port Knocking	林家璋 iFUS System Consultants Ltd. CISO

## 4F 展區 AIoT & Hardware Security Summit

時間 / 地點	4F AIoT & Hardware Security 專區
13:00   13:30	安全快閃記憶體：打造車用電子的安全防線
13:30   14:00	你家的攝影機安全嗎？
14:00   14:30	建構雲端時代的網路安全防護
14:30   15:00	從地端雲端：企業監控資安的全面防護策略
15:20   15:50	集合啦！烏龜洞友會！一揭秘網通設備的漏洞秘辛
15:50   16:20	邊緣運算最新應用與展望
16:20   16:50	探索 AMD SEV-SNP：下一代虛擬化記憶體加密與安全保護

## Cyber Talent 資安人才論壇

時間 / 地點	4F Cyber Talent 專區
14:00   14:30	從工廠到駭客：台積電課長轉生資安工程師的異世界生活
14:30   14:40	動態威脅與人才斷層：企業韌性的資安人才培育方程式
14:55   15:25	OffSec Cert: from 0 to 0.5
15:40   15:50	資安與 AI 的交匯點：人才、技術與未來
15:50   16:20	《哈佛商業評論》資安個案的教學實踐

## CyberLAB 實機演練

時間 / 地點	4D 展場會議室
12:30   14:30	Proofpoint Discovery: 實戰體驗課 - 強化身分安全
15:00   17:00	專為開發團隊設計：常見網頁弱點演習實作課

# CYBERSEC 2025 臺灣資安大會 Day3 4/17 (四) 總議程表

## WE ARE TEAM CYBERSECURITY

最新大會議程請至大會網站，或掃描 QRcode 下載大會超便利 APP 查看：



IOS 下載  
https://t.ittho.me/APP\_IOS



Android 下載  
https://t.ittho.me/APP\_Android

### 7F 會議室

分堂議程	SecOps 論壇	零信任論壇	Secure Software & DevSecOps 論壇	Supply Chain Security 論壇	Cyber-Physical System Security 論壇	Privacy & Data Protection 論壇	AI Security & Safety 論壇	Incident Response 論壇
時間 / 地點	701B	701D	701F	701G	701H	702	703	4A 展場會議室
09:30   10:00	運籌帷幄的危機與防線 - 以 NIST SP 800-223 高效能計算的安全架構窺見資安新戰場攻防 唐雅為 資誠智能風險管理諮詢有限公司 執行董事	探索 0 與 1 的邊界：實踐產品零信任安全機制 台達電子 - 吳東榮 資深研發工程師 - Steven Chen 主任研發工程師	專案執行與資安弱點掃描修正流程整合實踐優化 陳嘉賢 金融相關產業 專案管理師	大談 SBOM - 導入 SBOM 面臨的實際問題與解方 Jason Huang TXOne Networks Inc. 技術經理	關鍵基礎設施場域資安實現：應對工控場域資安挑戰的全面驗證與評估方案 林上智 國際自動化協會 臺灣分會會長	個人資料檔案保護及安全維護趨勢 林逸塵 個人資料保護委員會籌備處 隱私科技組組長	別讓威脅情資只是 Big Data：自動化知識圖譜賦能情資關係推理與檢索 廖冠翰 奧義智慧科技 資料科學家	資安緊急應變 2.0：敏捷的新應用 吳明璋 怡安保險經紀人股份有限公司 副總經理
10:15   10:45	回顧近期資安威脅趨勢與重大案例，應用資安監控應變平台融合 SOC+MDR+SOAR 的最佳實踐 邱永興 中華資安 SOC 服務部協理	「開箱即合規」- 達成零信任的最高境界 Apple 商用團隊 Apple 商用部門	讓修補經驗成為懂你系統的資安顧問 林秉正 震力橋子數位股份有限公司 技術開發二部主任	From SBOM to Zero CVE: 軟體產品開發視角下的供應鏈安全實務分享 鄭馮藏 偉康科技股份有限公司 資深研發經理	Protecting Medical Data: The Risk of DICOM File Attacks on PACS Servers TXOne Networks Inc. - Chizuru Toyama Senior Threat Researcher - Cnanao Kao Threat Research Director	以資料保護設計為預設的系統實踐思維 林逸塵 國立政治大學 資訊管理系 博士	Dark Watchdog：在暗網陰影中潛伏的 AI 利器 洪幸里 奧義智慧科技 資安研究員	如何增強資安事件回應處理能力與提高應變成熟度 DM Wang Team15 杜浦數位安全 產品經理
11:00   11:30	電子郵件安全解析：縮短 RFC 與實作間的差距 鄭翔予 奧義智慧科技 資安威脅研究員	雲端攻防戰：從資安事件看威脅演變 Allen Wang 銓錫國際股份有限公司 資深工程師	從編譯器視角看 App 程式碼安全與防護 陳忠義 ICShell Security Compiler Engineer	建構產品供應鏈永續安全與韌性的關鍵策略 田維誠 台達電子 產品資安處長	IEC 62443-3-3 安全等級在實際應用中的挑戰與解決方案 Moxa - 張凱棠 資安技術經理 - 黃凱偵 軟體技術經理	準備好了嗎？個資行政檢查的攻略與趨勢！ 李怡親 財團法人資訊工業策進會 高級法律研究員	Open Source Security 論壇 Wazuh 打造 XDR 資安防護機制經驗分享 鄭郁霖 節省工具箱有限公司 技術總監	Hello 你的 MFA 被繞過了-從真實 IR 案例反思雲端最佳實踐 Tim Yeh AWS Taiwan Security Architecture
11:45   12:15	潰堤的 PowerShell 防線：逆向拆解 AMSI 防禦架構，如何替藍隊找到偵測防線？ 黃智威 TXOne Networks Inc. 資深資安威脅研究員	後量子密碼論壇 量子電腦對行動通訊身份安全的威脅與量子安全網路的重要性 蔡宜學 財團法人資訊工業策進會 資安科技研究所 資深技術經理	【11:45 - 12:30】 解密 AI 合規：從歐洲白皮書核心原則如何融入 DevSecOps Tommy Tseng ViewSonic Security Architect	歐盟資安韌性法 (CRA) 已倒數計時 - 首當其衝的產品安全團隊該如何應對此戰！ Yenling Lee TXOne Networks Inc. 資深資安威脅研究員	油氣產業的資安全新挑戰：淺談油氣產業常見的資安問題與防禦手法 Linwei Tsao TXOne Networks Inc. 資安威脅研究員	【11:45 - 12:30】 基因檢測後的隱私危機：解構高度連鎖不平衡區風險 林偉盟 先見基因科技 資訊部門經理	Open Source Security 論壇 矛盾大對決：開源後門程式對開源防禦平台剖析 高于凱 勳業眾信聯合會計師事務所 資深經理	以科技打擊詐騙：新興技術在反詐騙中的應用 劉彥伯 台灣數位安全發展協會 理事
分堂議程	SecOps 論壇	CISO 論壇	Secure Software & DevSecOps 論壇	Supply Chain Security 論壇	Cyber-Physical System Security 論壇	Web 3 安全論壇	Product Security 論壇	Security Strategy & Case Study
時間 / 地點	701B	701D	701F	701G	701H	702	703	4A 展場會議室
14:00   14:30	微軟產品與第三方工具的實戰應用與設定：構建企業資安防線 AZ TXOne Networks Inc. Senior Information Security Engineer	探討企業在 GenAI 時代所需的資安策略框架 Brian Shen 趨勢科技 Product Director	你的雲端開發環境值得更好的保護 蔡幸育 華碩電腦股份有限公司 資安架構副師	AI Security & Safety 論壇 AI 如何幫助 O-RAN 專網內的資安 鄭欣明 數位發展部資通安全署 副署長	ICT 風險之 ERM 整合：提升組織韌性與戰略決策 張晉瑞 資誠智能風險管理諮詢有限公司 董事長	Breaking Down Web3 Attack Surfaces: A Dive into Consensus, VMs, Smart Contracts, and Toolchains 王建元 Anatomist Security Co-founder	Pwn2Own 解碼：廠商視角的弱點反思 吳典興 群輝科技 開發研究員	重灌人生太淒涼，來點不一樣的 MDR 廖原甫 宏碁資訊服務股份有限公司 顧問
14:45   15:15	Hide Your Invocation of PowerShell Execution Jie Palo Alto Networks Security Architect	從資安角度看待資安認證 - 資安維運到資安治理之路 楊峻程 友達光電 數位技術發展總部顧問	將 DAST 整合進入 CI/CD 的正確姿勢 高于凱 勳業眾信聯合會計師事務所 資深經理	從零開始面對 EU CRA 賴俊福 台達電子工業股份有限公司 軟體設計副理	車載資安診療室，透過內外科帶你認識威脅與機會 孫沛靖 安華聯網科技 (DEKRA 德凱集團成員) 資安評估處 工程師	AI 驅動的智慧合約漏洞檢測 OneSavie Lab - Alice Hsu Security Research Engineer - Daky Wang Product Development Lead	台灣電子產品安全嗎？從呼叫器爆炸案談產品資安 羅化中 國家資通安全研究院 副院長	Neural-ASR：以 NLP 手段自大型 OT/ICS 攻擊自動提取特徵碼 Mars Cheng TXOne Networks Inc. 資深威脅研究經理
15:30   16:00	紅隊演練強化藍隊戰術指南 ZUSO Generation - Leo Ho 技術長 - Vance Hsieh 技術經理	資通安全風險管理：打造韌性防禦，迎接數位挑戰 游政卿 合勤投資控股股份有限公司 資安長	DevSecOps 和自動化安全檢測的敏捷導入 蔡龍佑 震力橋子數位股份有限公司 技術開發二部副理	臺灣國防供應鏈安全升級戰 - 從 CMMC 合規到自主防衛 黃希儒 財團法人國防安全研究院 委任資深研究員 備役中將	歐盟無線電指令，網路安全法案，EN 18031 標準介紹 薛正 Bureau Veritas 資訊安全服務部 技術協理	重入陷阱：破解智能合約不變性迷思 Helen XREX Security Information Engineer	IEC 62443-4-1：從威脅建模到產品資安認證的挑戰與實務分享 蘇輝博 台達電子工業股份有限公司 資深研發課長	工控協定攻擊案例研究 Yuan Xu 財團法人資訊工業策進會 資安工程師
16:15   16:45	【16:15 - 17:00】 Microsoft Graph API 提高你 (跟駭客) 的生產力 陳彥銘 中華資安 監控科資深資安工程師	【16:15 - 17:00】 從數據到決策與治理 - 簡介 FAIR CRQ 模型 小P ISACA總會 外部專家委員	【16:15 - 17:00】 Regulated Software Threats Modeling; A Practical Walk-Through Renaud Sauvain West Pharmaceutical Inc. R&D Director of Software Engineering	Exposure Management 論壇 Empowering Cyber Defense with Predictive Threat Intelligence and External Attack Surface Management (eASM) Ching Chiao Whois API Inc. Management Head of APAC & Global Partnership	永不軌軌：守護關鍵基礎設施中的軌道安全 TXOne Networks Inc. - Jair Chen 資深資安威脅研究員 - Mars Cheng 威脅研究經理	Security Challenges in Ethereum Layer 2 and Cross-Chain Ecosystems Louis Tsai DeFiHackLabs White Hat	【16:15 - 17:00】 產品資安的未來藍圖：安全產品開發生命週期與國際標準的演進之路 林上智 國際自動化協會 臺灣分會會長	具威脅性工控弱點實例揭密 - The Case Study of the InSecure by Design Daniel Chiu TXOne Networks Inc. Threat Research Manager

分堂議程	資安品牌日	
	CISCO	Microsoft
時間 / 地點	701C	701E
09:30   10:00	簡化維運，極速反應，重鑄資訊安全新防禦 林連貞 Cisco 全球資安產品營運副總裁	重塑資安：AI 時代的挑戰與創新 吳子強 台灣微軟 專家技術群總經理 唐萬容 微軟 資訊安全全球黑帶專家
10:15   10:45	Cisco AI Defense：保障企業 AI 應用的安全轉型 Sean Duca Cisco 亞太區首席技術長	新興威脅下的安全挑戰：全面強化 DDoS 攻擊防禦策略 陳炳中 台灣微軟 雲端解決方案架構師
11:00   11:30	Cisco Splunk & XDR：功能整合 提升 SOC 效益 蔣佳賓 Splunk 北亞區售前部門資深總監	智慧防禦的未來：XDR 解決方案深度剖析 張士龍 台灣微軟 資深資安安全解決方案專家
11:45   12:15	Cisco Zero Trust：全場最強零信任，從使用者到資料中心的全方位防護 朱育民 Cisco 台灣資安事業部總監	以 AI 賦能資安：強化企業單一資安維運平台 陳濠竹 台灣微軟 專家技術群資訊安全專家

分堂議程	金融資安論壇	
	701A	
時間 / 地點		
09:30   09:35	開場致辭 吳其勳 臺灣資安大會 主席、iHome 總編輯	
09:35   09:45	長官致辭 高于凱 勳業眾信聯合會計師事務所 資深經理	
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	「金融資安韌性：實踐與挑戰」經驗分享 座長：林裕泰 金融監督管理委員會資訊處 處長 與談人： 吳佑文 中國信託商業銀行 副總經理兼資安長 康崇原 將來銀行 副總經理兼資安長 林季勳 凱基人壽 副總經理兼資安長 陳明環 國泰金控 資安長	
11:30   12:00	金融機構 API 資安治理及管理機制 蘇清偉 富邦金控 資安長、副總經理	
14:00   14:30	數位鑑識不該是你處理事件應變的重點 陳誌昌 台新金控 資安長	
14:30   14:50	Insider Threats - A Silent Killer in Financial Security Jeff Yeo Trellix ASIA Solution Engineering Senior Manager	
15:05   15:35	資安只出張嘴嗎？淺談資安一、二道防線分工合作 方振維 新光金融控股公司 資深協理	
15:50   16:35	前職金融資安長的省思與蛻變：先相信才會看見 高大宇 永豐銀行 資訊安全處 副總經理	

分堂議程	攻擊型安全論壇	
	701E	
時間 / 地點		
14:00   14:30	紅隊的隱形戰術：Reflective Loader 與 EDR 的對抗藝術 傅柏軒 安華聯網科技 (DEKRA 德凱集團成員) 資深紅隊工程師	
14:45   15:15	Operations Security (OPSEC) - 紅隊不被抓到的秘密！ 游照臨 趨勢科技 Threat Researcher	
15:30   16:00	不定期滲透測試：隱藏的資安炸彈 David Wang Ridge Security Security Software Engineer	
16:15   17:00	以戰代訓 - 透過攻防不斷進化的資安團隊 翁浩正 戴夫寇爾 執行長	

### 上市櫃資安標竿論壇

時間 / 地點	701C
14:00   14:30	上市櫃企業資安治理 - 從合規到競爭優勢 陳志明 安永諮詢服務股份有限公司 副總經理
14:45   15:15	金箍棒與緊箍咒：解密傳產的數位優化與資安治理策略 費而騰 欣陸投資控股股份有限公司 副總經理
15:15   15:35	企業資安挑戰與合規標準：打造穩固營運基礎 沈雅婷 中華電信股份有限公司資訊技術分公司 高級工程師
15:50   16:20	從信任到價值共創——企業如何與利害關係者共建數位未來？ 曾鈞 安永諮詢服務有限公 執行副總經理
16:20   16:50	營業秘密與資安的距離-分類分級思維不同 鄒宗蓋 財團法人資訊工業策進會 科技法律研究所副所長

# CYBERSEC 2025 臺灣資安大會 Day3 4/17 (四) 總議程表

## WE ARE TEAM CYBERSECURITY

最新大會議程請至大會網站，或掃描 QRcode 下載大會超便利 APP 查看：



IOS 下載  
https://t.ittho.me/APP\_IOS



Android 下載  
https://t.ittho.me/APP\_Android

分堂議程	※ Space Cybersecurity 論壇	※ AI Security & Safety 論壇	※ Threat Research 論壇	※ 雲端安全論壇
時間 / 地點	1A 展場會議室	1B 展場會議室	4B 展場會議室	4C 展場會議室
09:30   10:00	流量加密也沒用？以阻斷攻擊拿下整片衛星RCE :) TXOne Networks Inc. 馬聖豪 Team Lead Jair Chen 資深資安威脅研究員	駭客變主人，GenAI 聽指令搞事情 廖凱傑 趨勢科技 資深技術經理	針對台灣產業資安威脅：分析從釣魚郵件入侵的全過程 Rachael Liao Fortinet Anti-Virus Analyst	以雲端方式建構大型醫院防護 郭振宗 臺北榮民總醫院 資訊室主任
10:15   10:45	對抗被拿下的整片衛星：工控場域之衛星網路防護準則 Yenting Lee TXOne Networks Inc. 資深資安威脅研究員	透過 LLM AI 自動分析並提取攻擊資訊達到漏洞預防 TXOne Networks Inc. - Patrick Kuo Senior Threat Researcher - Daniel Chiu Threat Research Manager	永恆之藍的攻擊套路與威脅場域 王湘凱 TXOne Networks Inc. Threat Researcher	Secure by Design 雲端安全管理架構設計 Will Lin 華碩電腦 Director
11:00   11:30	數位星塵中的暗流：從虛擬戰場探尋太空安全的未來 Sol Yang NICS 助理工程師	透過深度神經網路(DNN)攻擊來學習OWASP 徐育正 合作金庫商業銀行 資安部二等專員	從開機到攻擊：分析 UEFI Bootkit 的攻擊技巧 Zeze Team15 杜浦數位安全 Research Engineer	Simplifying Hybrid Cloud Governance - 用簡單的策略駕馭複雜的雲端！ Eric Chien 趨勢科技 資深安全架構師
11:45   12:15	以點破面：從開源衛星通訊協定攻擊看衛星攻擊面向 Vic Huang UCCU Hacker Member	Some things about AI-powered Rule Generation for Network Intrusion Detection System Canaan Kao TXOne Networks Inc. Threat Research Director	【11:45 - 12:30】 DragonRank, a Chinese-speaking SEO manipulator service provider Joey Chen Cisco Talos Sr. Threat Researcher	【11:45 - 12:30】 跨雲分持加密與雲原生安全治理實踐：2024 經驗分享與未來展望 楊世廷 數位發展部 資訊處分析師
分堂議程	※ Car Security 論壇	※ AI Security & Safety 論壇	※ Threat Research 論壇	※ 雲端安全論壇
時間 / 地點	1A 展場會議室	1B 展場會議室	4B 展場會議室	4C 展場會議室
12:40   13:10	Lunch Learning Session 攻擊安全論壇 [12:40 - 13:25] All your base are belong to us, 我要全部 Hans Wang 中華資安國際股份有限公司 檢測部副理	Lunch Learning Session 專精於暗網曝險的資安特工 戴培侃 奧義智慧科技 資安長暨共同創辦人	Lunch Learning Session AI Security & Safety 生成式 AI 合規技術與挑戰 曲華榮 中華電信研究院 高級研究員	Lunch Learning Session 不時默默地以 Admin 操作的雲端管理員 黃星評 ISC2 Taipei Chapter 理事
14:00   14:30	汽車與 IoT 設備找漏洞經驗談 駱一奇 VicOne 資深威脅研究經理	神經級逆向技藝：從人機翻譯到全自動符號語義推理模型，打造仿生逆向聖杯 黃智威 TXOne Networks Inc. 資深資安威脅研究員	小捷徑大威脅，LNK 文件如何成為威脅跳板 Cara Fortinet 資深威脅研究經理	K8s 與容器服務攻擊手法層出不窮，企業如何防禦？ Aspen Yang 敦陽科技 技術經理
14:45   15:15	Blue Archive：揭露於車載系統中的藍色漏洞 陳兆閔 奧義智慧科技 資安研究員	大型語言模型測測革命：LLM-as-a-Judge 的實踐與挑戰 Stanley Chou Coupang Director of Security Engineering	十廠百縫：揭開設備漏洞與攻擊者的連結 Team15 杜浦數位安全 - Jill Liu Project Manager - Jason3e7 資安研究員	洞悉雲端威脅：建構主動式安全監控體系 鄭家明 Google Cloud Customer Engineering
15:30   16:00	Project D：左握方向盤，右打 CarPlay Zef Tien Cymetrics Senior Security Research Engineer	以視覺化AI打造特微碼專家系統一卷積分類惡意程式家族，我們走到了哪？ 馬聖豪 TXOne Networks Inc. Team Lead	VPN 觀落陰——數家 SSL VPN 的防火牆和路由規則穿透漏洞 Ta-Lun Yen TXOne Networks Inc. Sr. Vulnerability Researcher	WHO DO YOU TRUST：多雲架構下的身份安全威脅 李東霖 奧義智慧科技 資安研究員
16:15   17:00	當 GenAI 從雲端降落到車載，深入淺出軟韌體、硬體架構與風險 Shin li VicOne Staff Researcher	大型語言模型裡面五花八門的攻擊與防禦 游家牧 國立陽明交通大學 電機工程學系 副教授	Sneak Skill 100 - 潛在的攻擊面：SCCM 奧義智慧科技 - 蘇俊銘 資安研究員 - 朱興華 資安研究實習生	Boring Cloud Security Ken Lee Independent Security Advisor

※ 本會議室提供 AI 即時中英文翻譯

### 4F 展區 AIoT & Hardware Security Summit

時間 / 地點	4F AIoT & Hardware Security 專區
10:00   10:30	資訊安全認證發展趨勢對智慧聯網市場的影響探討 Joe Wang 是德科技 Senior BDM
10:30   11:00	量子安全時代的晶片安全生命週期規劃之淺見 Jason Lu DataBrushing.ai CEO
11:00   11:30	如何利用動態 PUF 信任來實現後量子 ZTA 應用 Nicolas Fahier 智能資安科技股份有限公司 技術長
11:30   12:00	AIoT 時代的 Edge 安全，RoT 硬體最佳防護策略 JW Yeh, Ph.D. 伊諾瓦科技股份有限公司 產品經理
13:00   13:30	工業物聯網資安「灰犀牛」沉默風暴 Alpha Chen 昇頻股份有限公司 執行長
13:30   14:00	工業 4.0 時代的守護者 - OT 網路安全實戰經驗 王展帆 台灣洛克威爾國際股份有限公司 總監
14:00   14:30	解碼智慧變電站通訊：從架構設計到工業資安防護實踐 余浩宇 四零四科技股份有限公司技術主任

### CyberLAB 實機演練

時間 / 地點	4D 展場會議室
09:30   11:30	透過 Shared VPC 與 VPC Service Controls 實作 Google Cloud Platform 微分割，防止跨專案不當存取與資料外洩 余俊宏 宏庭科技股份有限公司 維運服務處處長
12:30   14:30	隱藏模式 ON：找到隱藏在硬碟深處的祕密 馬洪雲 中華資安國際股份有限公司 高級工程師
15:00   17:00	雲原生 SIEM 威脅偵測實機體驗 鄭宇翔 伊雲谷數位科技股份有限公司 Cybersecurity Security Analyst

### Cyber Talent 資安人才培訓論壇

時間 / 地點	4F CyberTalent 專區
10:00   10:30	紅隊勇者的證照冒險攻略 楊士賢 Cymetrics Security Research Engineer
10:30   10:40	資安人才證照趨勢與需求分析 魏錦志 國立臺北科技大學 副教授
10:40   10:50	數位轉型下的資安挑戰：企業需求與人才機會 蕭詔安 雲力橋子數位股份有限公司 經理
10:50   11:00	專業證照不該只是徽章，更該是資安戰場的通行證與交流工具 唐任威 ISC2 Taipei Chapter President
11:00   11:30	資安人的奇幻旅程：從修漏洞到和資安長修感情 許農育 國泰健康管理顧問股份有限公司 資安專員
11:30   12:15	駭客的鬥法大賽 - 從 HITCON CTF 到 HITCON Cyber Range 台灣駭客協會 陳仲堃 理事 Kyo Chen HITCON Cyber Range 總召
13:45   14:00	以戰代訓新思維：打造資安實戰型人才培育途徑 胡馨元 國家資通安全研究院 人才培力中心研究推廣組 經理
14:00   14:30	資安小白看過來~資安職涯起手式，資安證照與故事 黃景偉 NCU AI與資安研究生
14:30   15:00	從 PDDRO 到 TTQS：結合 ISO 27001 建立企業資安培訓框架，提升訓練投資效益 林毅力 高鼎精密材料股份有限公司 副理
15:00   15:10	保全與科技 沒有距離 KCYao 新堡科技 資深協理
15:15   15:45	藍隊養成記：現實、策略與思維 唐任威 ISC2 Taipei Chapter President
15:45   16:15	從HR的觀點看資安證照的潛力與價值 鄭惠如 Integrated Solutions Technology, Inc. 人資暨財務主管

大會保留議程調整之權利