CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

CYBER TALENT

藍隊養成記：現實、策略與思維

TEAM CYBERSECURITY

唐任威 Vincent
ISC2 Taipei Chapter
President

ISC2 Taipei Chapter President / 台灣國際認證資安專家協會 理事長
精誠資訊恆逸教育訓練中心 資深講師

唐任威
Vincent

✓認證

講師證照	ISC2、OffSec 認證講師、CEI、MCT
資安管理	CISSP、CCISO
駭客攻防	OSEP、OSCP、LPT Master、CPENT、ECSA (Practical)、ECSA、CEH Master、CEH (Practical)、CEH
安全防護	SSCP、CND、ICS/SCADA Cybersecurity、ENSA、RESILIA Foundation、TCSE
應變情資	CHFI、ECIH、CTIA、CSA
雲端資安	CCSP、CCSE、CCSK
安全開發	CSSLP、ECDE、CASE .NET、CASE Java、ECSP.NET、ECSP
系統管理	MCSE、MCSA、MCITP、MCTS、MCSE on Security、MCP+Internet、MCP、Compaq ASE

✓獎項 2024、2013、2019-2016 EC-Council Instructor Circle of Excellence Award
2023-2020 EC-Council Instructor (CEI) of the Year Award

✓專長 資訊安全管理、資訊安全風險評鑑、滲透測試、駭客手法分析、網路環境安全性評估、惡意程式防護與分析、安全系統開發、電腦鑑識、資安事件調查、微軟網路環境規劃、整合與建置(含目錄服務、訊息系統、網路安全性架構)

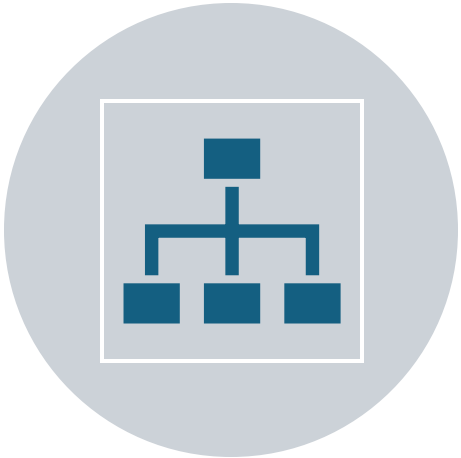
✓著作 《Windows Server 2008網路服務與安全》、《網路概論》、《網路概論與實務》

藍隊

維持企業資安狀態；
保護資訊系統正常使用；
防禦真實攻擊；
對抗來自紅隊的演練

source: CNSSI 4009-2015

企業資安三面向



管理

技術

法規遵循

Security

功能	單位	活動
Prevention	ITSec ISAC	IT 防禦 情資預警
Detection	SOC	資安監控
Correction	CERT	事故應變

藍隊五大現實

日常作業

藍隊人力不足	• 缺乏足夠具備資安技能的專業人才 導致輪班壓力大、監控疲乏
工具分散、系統破碎	• 資安工具多但整合性差，資訊無法匯流 增加誤判與遺漏風險
事件通報與應變緩慢	• SOP 缺乏演練，流程不成熟，導致處置效率不佳

環境

攻擊手法日新月異	• 面對 APT、零時差、勒索等多樣攻擊 藍隊反應不夠及時
供應鏈風險轉嫁	• 外部廠商或合作夥伴的資安事件，卻由內部藍隊 承擔責任
資安要求愈加嚴格	• 面臨客戶、主管機關與產業標準的合規壓力與 查核頻率上升

人才

招不來、留不住	• 優秀藍隊人才競爭激烈，企業待遇與學習機會無法吸引或留任
學用落差	• 新進人員對實戰缺乏認識，培訓成本高但成效慢
內部缺乏資安意識	• 非資安部門對藍隊不了解、不合作 導致工作推動困難

治理

資安非決策核心	• 藍隊建議經常被忽視，資安被視為成本而非價值
缺乏跨部門協作機制	• 事故應變無法快速聯動 IT、HR、法務等單位
報告無法說服高層	• 資安風險難以用財務語言呈現，導致資源預算難爭取

風險

持續暴露在高風險	• 弱點未修補、威脅未偵測，形成攻擊者的長期據點
攻防落差擴大	• 紅隊與攻擊者的創新快速，而藍隊缺乏應變空間與創新資源
缺乏事後學習	• 事件發生後無系統性復盤與知識轉化，無法成長進步

內外加劇的挑戰

內部治理與 外部風險落差	沒有內部治理強度，就無 法抵禦外部攻擊壓力
內部人才不足及 外部攻擊壓力大	藍隊疲於奔命 難有餘力預防與預警
內部預算有限且 外部法遵要求增加	導致資源無法支持合規與 實務並重，陷入兩難

人力不足、系統破碎、應變緩慢

優化流程自動化	• 導入 SOAR 平台，加速事件偵測與回應
標準化通報流程	• 建立清楚明確的 IR Playbook，並定期演練 如 Tabletop Exercise。
工具整合與視覺化	• 統整 SIEM、EDR、NDR 等系統資料，提升 可觀察性（observability）。

攻擊手法變化快速
外部風險內部承擔、合規壓力上升

定期威脅情資更新與行動化	• 引入情資平台並與偵測規則連結
建立供應鏈資安評估機制	• 要求供應商資安自評或第三方審核
主動合規導向轉型	• 將法遵轉化為營運優勢，例如 ISO 27001 或 NIST CSF 導入專案化

招不來、留不住、跨部門不支持

發展資安職涯路徑與內部輪調制度	• 明確晉升機制、鼓勵 IT 人才轉職藍隊
建立學習型團隊文化	• 設立學習日制度、鼓勵參加實戰演練平台
跨部門資安意識教育	• 定期對非技術部門進行資安演練與社交工程模擬測試

資安無法進入決策層
跨部門配合不順、難以說服高層

資安治理納入董事會與高階決策	• 設立資安長（CISO）直屬 CEO 或董事會
導入資安 KPI 與財務語言轉譯	• 以風險影響分析（RA/BA）與 ROI 模型提升報告說服力
建立跨部門資安治理委員會	• 形成共同承擔與治理共識

高風險持續暴露
攻防差距擴大、缺乏學習機制

建立紅藍對抗常態化	• 將紅隊導入為內部壓力測試工具，提升防禦真實性。
事件檢討機制化	• 每一次事件皆需執行事後點討，並轉化為修正與訓練材料
持續風險評估與優先排序	• 導入 CVSS 與企業影響評估模型，優先處理高風險弱點

重新定義資訊安全：
價值導向的資安觀

藍隊可以是...

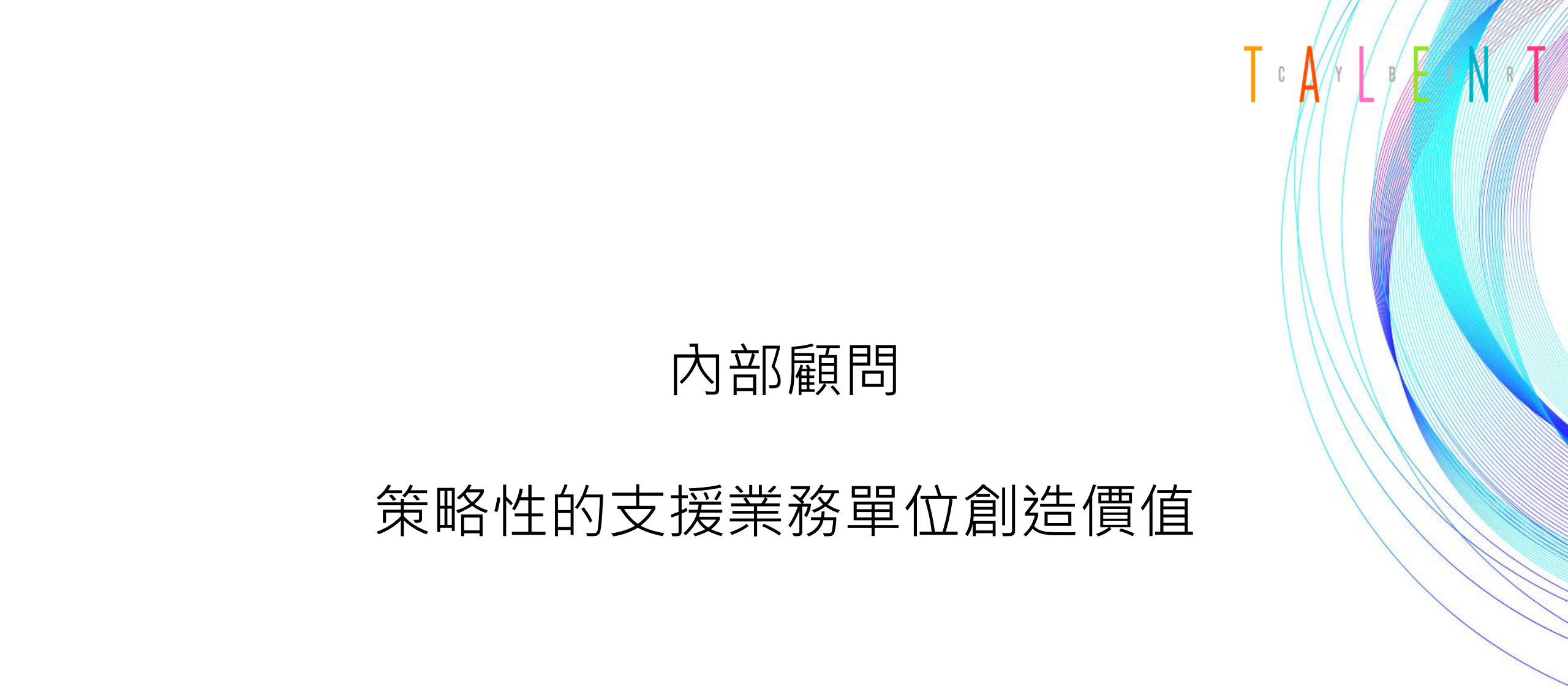
價值守門人與風險對沖中心
是創造價值的策略性單位

價值守護

「避免損失」、「維持營運」、「保護品牌」

風險減損

透過損害控制與減災避免「負利潤」



內部顧問

策略性的支援業務單位創造價值

風險預測與應變已成為企業競爭力的關鍵

危機處理能力=存續能力=投資價值提升

資安工作特性

高度風險環境	• 高度壓力、高度不確定、高即時反應的需求情境
需雙模作業	• 平時維運監控，攻擊即時反應
需高度管控	• 需處理敏感資訊與高風險決策
需高度專業	• 需持續訓練與專業證照

給企業的建議

高度風險環境	• 建立標準作業程序（SOP）與 緊急應變流程（Incident Response）
需雙模作業	• 建立韌性（resilience）與持續演練機制（drill/exercise）
需高度管控	• 需建構權限控管、資訊通報、風險分級與保密機制
需高度專業	• 明確分工與強化跨域整合

ISC2 CHAPTER | TAIPEI

【關於我們】

ISC2 Taipei Chapter 是 ISC2 在台灣的分會組織，致力於推廣資安專業知識、交流與社群互助。成員包括經 ISC2 認證的資安專家，及各領域資安專業人士。

【成立宗旨】

提升台灣資安專業社群的能見度與凝聚力。

【使命與活動】

- 推廣資安認證與專業發展
- 舉辦技術講座、各種資安研討活動
- 促進會員交流與跨界合作
- 參與國際資安社群互動

https://www.isc2chapter.tw

contact@isc2chapter.tw

加入 ISC2 Taipei Chapter 讓您的資安之旅，有專家同行！