國家資通安全研究院
National Institute of Cyber Security

臺灣資安大會 CYBERSEC 2025 | TRACK: Cyber Talent 資安人才培訓論壇

以戰代訓新思維：打造資安實戰型人才培育途徑

國家資通安全研究院 人才培力中心
胡馨元 經理

胡馨元 | Megan Hu

學經歷

國家資通安全研究院 人才培力中心 研究推廣組 經理（現職）

財團法人國家實驗研究院 資安卓越中心規劃建置計畫 佐理研究員

Kantar Taiwan 凱度洞察 質化研究員

國立臺灣大學圖書資訊學系暨研究所

研究興趣

資安人才培育發展研析、資安意識推廣研析

消費者行為研究、資訊架構與設計、使用者需求研究

獲獎紀錄

斐陶斐榮譽學會會員

Kantar Taiwan凱度洞察 亞太地區最具潛力質化研究員

三大願景 資安院 2.0

具體戰略與作為

願景一 **國家數位安全防禦基礎**

- 建立全社會資安防禦能力
- 保護國家關鍵基礎設施
- 推動打詐情資分析分享平台

願景二 **Team Taiwan資安生態系**

- 公私協力建立資安防護與服務量能
- **厚植資安人才培育系統**
- **提升全社會資安動能**

願景三 **國家資安治理政策智庫**

- 建立資安政策研究團隊
- 打造國家資安治理情資平台
- 推動國際資安合作與交流

進階資安人/CI資安人

- 在各企業組織中具備一定的資安技術，豐富的相關知識與經驗，已準備好接受更進階訓練
- 任職於關鍵基礎設施擔任技術、策略型人才者

在職資安人

有志擔任或甫就任資安相關職務者，已擁有特定領域的專業知識（如：資訊科學、法律學、會計學）

潛在資安人（大眾、IT人）

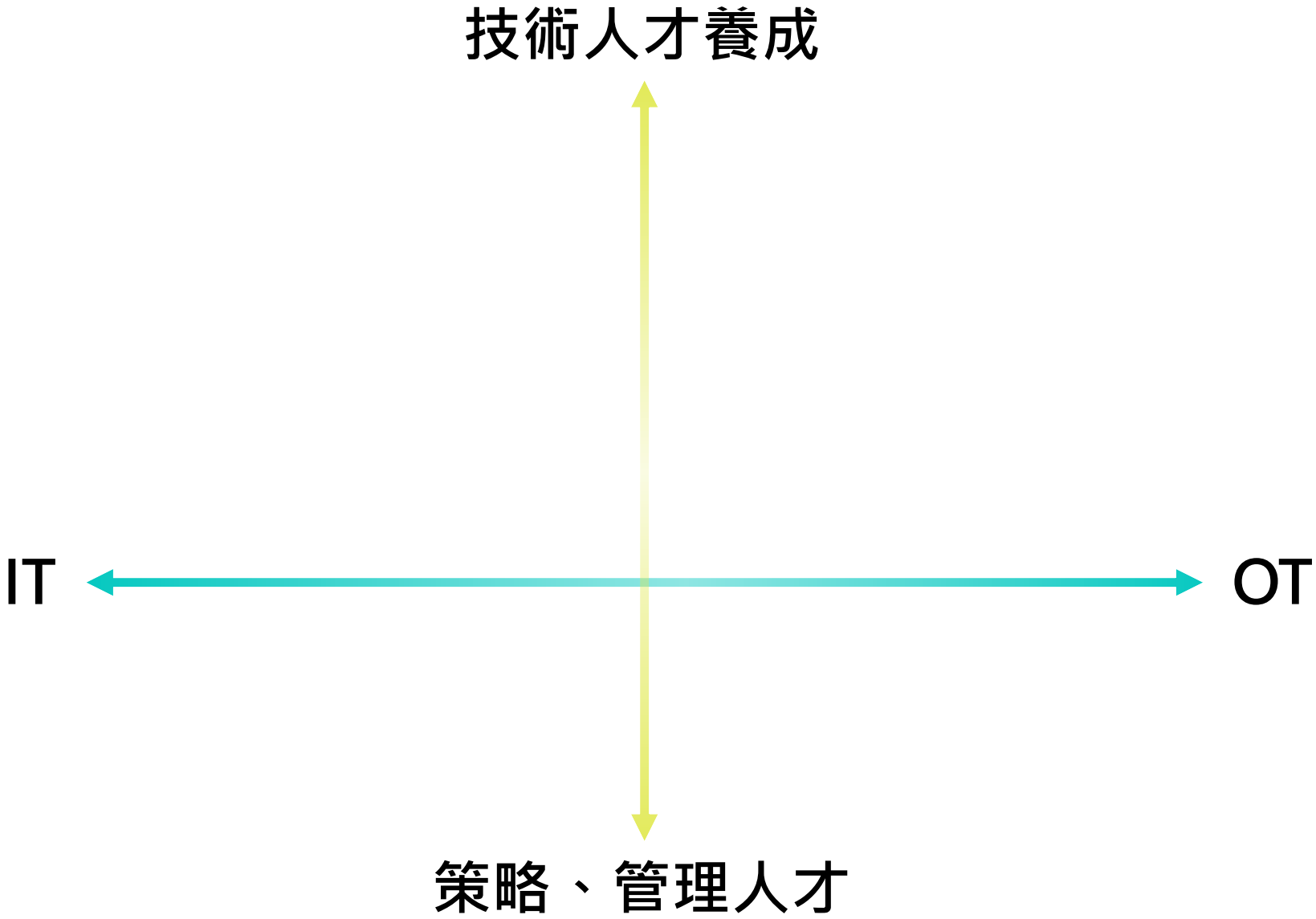
透過科學溝通，提升大眾資安意識；也透過多樣活動，讓對資安領域有些了解的人員、有機會加入資安領域

進階資安人/CI 資安人

- 在各企業組織中具備一定的資安技術，豐富的相關知識與經驗，已準備好接受更進階訓練
- 任職於關鍵基礎設施擔任技術、策略型人才者

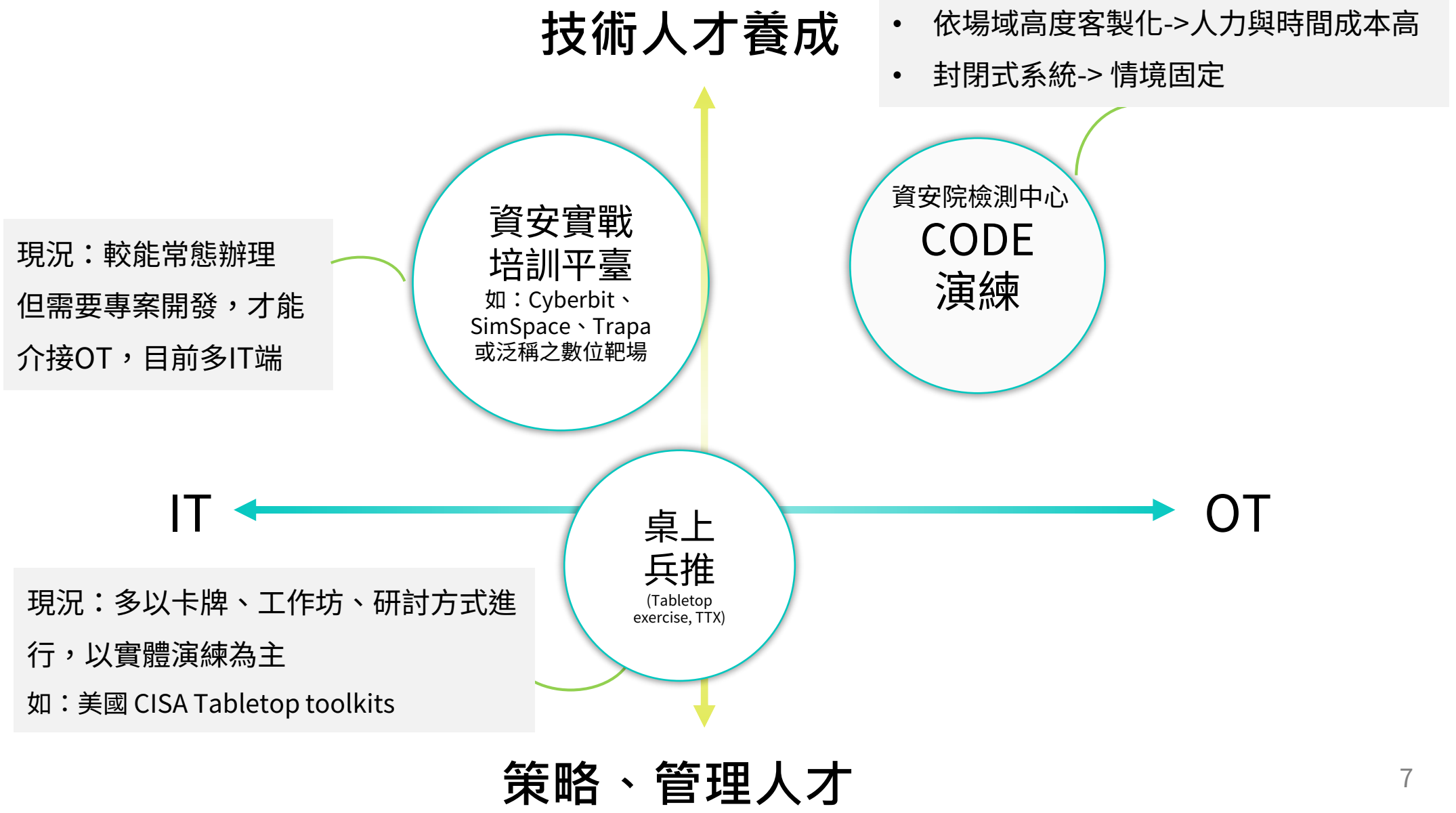
目前培育挑戰：缺乏實戰環境與進階練習工具

資安實戰演訓工具



Source: 本院林盈達副院長2023年11月神盾盃引言

資安實戰演訓工具


技術人才養成
現況：
• 依場域高度客製化->人力與時間成本高
• 封閉式系統-> 情境固定
現況：較能常態辦理
但需要專案開發，才能
介接OT，目前多IT端
資安實戰
培訓平臺
如：Cyberbit、
SimSpace、Trapa
或泛稱之數位靶場
資安院檢測中心
CODE
演練
IT
OT
桌上
兵推
(Tabletop
exercise, TTX)
現況：多以卡牌、工作坊、研討方式進
行，以實體演練為主
如：美國 CISA Tabletop toolkits
策略、管理人才

跨國網路攻防演練
Cyber Offensive and Defensive Exercise (CODE)

- 2025年11月中旬將以醫療機構作為演練場域，提升關鍵基礎設施的防護能力
- 由國內醫院組成藍隊、國內外學研政府專家組成紅隊進行演練


聯合新聞網

聯合報 經濟日報 陽光行動 有設計 有行旅 願景 我的新聞

即時 要聞 娛樂 運動 全球 社會 地方 產經 股市 房市 生活 寵物 健康 橘世代 文教 評論 兩岸 科技

快訊 中秋節後為何是牙科急診高峰期？專家告訴你如何自救及預防 10:50

udn / 產經 / 財經焦點

18國資安專家匯聚展開資安攻防演練 台灣奪下冠軍

2023-10-23 14:43 經濟日報／記者余弦妙／即時報導

+ 資安

資安署表示，10月18至20日在我國舉辦2023年跨國網路攻防演練，此次活動選定與民生相關的水資源領域建置仿真的場域，由台灣自來水公司擔任藍軍，紅軍則由國內外攻擊隊伍分別扮演，包含美國、捷克等國際菁英好手、國內政府機關聯隊以及我國參與國際駭客競賽的獲獎選手組團，共有八隊進行實戰的演練及切磋，充分地模擬多方駭客針對關鍵基礎設施進行攻擊，而防禦組演練面對多方攻擊的高壓下，如何快速應變及處置，場邊並有其他國際資安專家參與觀摩及觀察攻擊演練活動。我國參與團隊表現優秀，在比賽甚至獲得第1名的佳績，顯示國內資安人才培育成果。

https://udn.com/news/story/7238/7524050 https://www.ithome.com.tw/news/16748

目前培育挑戰：缺乏實戰環境與進階練習工具

資安院解方 | **以戰代訓** 發展人才實戰演訓與開發工具

實戰平台開發與培訓
#進階技術型人才

桌上推演研發與推動
#策略型人才

目前培育挑戰：缺乏實戰環境與進階練習工具

資安院解方 | **以戰代訓** 發展人才實戰演訓與開發工具

實戰平台開發與培訓
#進階技術型人才

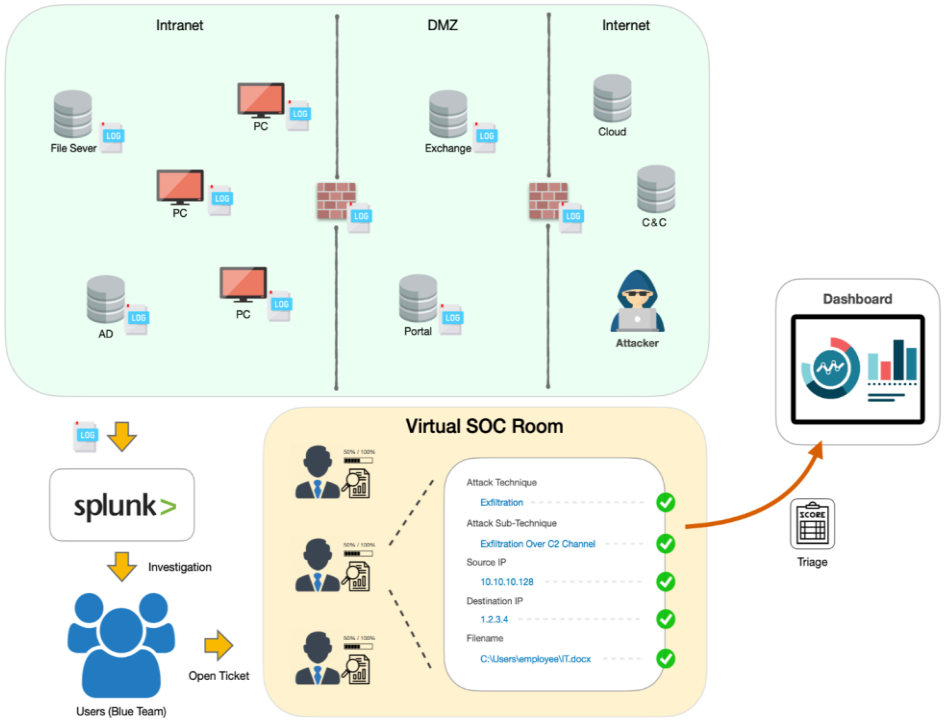
桌上推演研發與推動
#策略型人才

實戰平台開發與培訓

以實戰訓練強化組織資安技術面防護能力

開發APT防禦演練平台

以虛擬網路環境、SIEM、APT攻擊劇本、相關攻擊概念程式及提供整體資訊的儀表板，在虛擬網路環境中模擬真實的APT攻擊



培訓目標

參與者扮演SOC成員，熟悉搜索、鑑識攻擊手法，第一時間處理警報、判斷嚴重程度、做簡易調查並訂立處理方針，培育企業與政府單位最需要的防禦性資安人才

網路威脅防禦平台訓練

- 自2021年起，資安院每年辦理資安菁英人才培訓課程，使用APT防禦演練平台進行「網路威脅防禦競賽」，讓學員體驗訓練組織內防禦方角色之調查事件反應能力
- 2022年、2023年與日本SecHack 透過線上與線下活動與實作的結合，在一流的技術與培訓師的支持下，培養 25 歲以下的新興資安技術人員
- 未來規劃開放對外課程，讓更多產業資安、政府資安人員可以體驗學習、透過擬真環境訓練，提升臺灣整體資安能力

SecHack365
SECURITY+HACKATHON 365 DAYS

目前培育挑戰：缺乏實戰環境與進階練習工具

資安院解方 | **以戰代訓** 發展人才實戰演訓與開發工具

實戰平台開發與培訓
#進階技術型人才

桌上推演研發與推動
#策略型人才

資通安全桌上推演 Tabletop Exercise (TTX)

以實戰訓練強化組織資安策略面防護能力

為什麼發展桌上推演？

以往實戰訓練是多是針對資安技術人才，但**策略型人才**也需要學習在發生資安事件時該怎麼應對和臨場處理

桌上推演是什麼？

TTX 是一個討論型的演練，參與者在演練中討論【日常業務過程中高機率發生的資安威脅案例】，並設想遇到這些狀況時，要如何運用手邊的資源、人力、工具來應對

資通安全桌上推演 Tabletop Exercise (TTX)

基於日常業務的
高風險情境

兩難的討論題項

腦力激盪決策過程

建立與增強產業與
CI人才之資安意識
與事件應變能力

（想像中）TTX情境撰寫

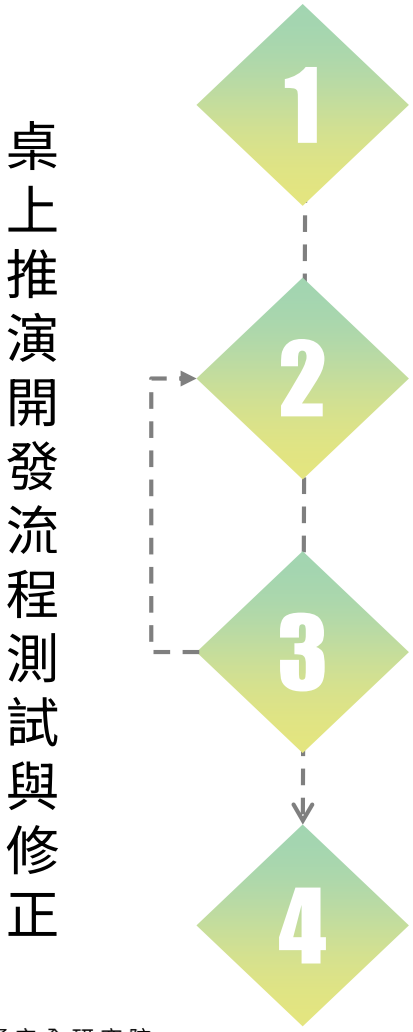
在購物節前夕，某大型購物中心的顧客數量突然激增。客服部門的新進員工小元接到一位顧客的緊急求助，立即趕到現場處理。在成功解決顧客的問題後，小元想要在系統中記錄這次的服務細節，但發現無法登入客戶關係管理系統(CRM)。

她試圖查看銷售系統來確認顧客的購買歷史，卻發現該系統也無法使用。隨後，連監控商場安全的閉路電視系統也出現異常。小元意識到情況不對勁，立即聯繫IT部門尋求協助，希望能盡快恢復系統運作。IT人員開始檢查公司網路流量和系統log，發現有大量未經授權的IP嘗試存取系統資料，並且網路流量也顯示目前有不合理的檔案傳輸狀況…

情境撰寫…看似很容易

僅憑「想像」，專業真實度與深度恐不足，也無法面對領域中時常改變的新的威脅，發展自己的「桌上推演方法論」，隨著技術發展和實踐經驗進行調整，是資安院採取的策略

桌上推演情境設計研發流程



成立桌上推演開發工作小組、設計訪綱、試訪、修正

訪談利益相關者探詢關鍵業務可能的風險，例如：
業務營運第一線人員、主管、IT人員、委外廠商

與學者專家、業界代表、兵推顧問合作撰寫風險情境、
修改、檢討、獲取專家反饋

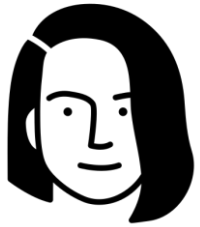
設計教案、完成桌上推演活動流程設計、
製作演練執行素材

桌上推演研發團隊角色

情境研發團隊

訪談研究員

- 執行訪談
- 發想討論題項
- 撰寫參考指引



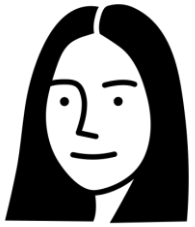
資安專家

設計攻擊手法

演練辦理團隊

引導員

- 引導討論切合學習目標
- 以中立的方式提問



場域資安專家

作為權威角色，確保討論合乎專業知識

行政人員

協助工作坊場地、餐飲與流程進行順暢

培育引導員擴充演練量能

桌上推演執行方法論

以討論和情境模擬為主的資安演練方式，不需要實際的系統操作，專注於反應流程、角色協作和決策過程

研發演練工具

- 釐清產業/CI 之重大風險與影響：訪談第一線業務執行者，釐清業務中的關鍵風險(key risks)
- 設計多元且合理的攻擊情境：訪談產業/CI 的 IT 人員，了解組織資訊基礎架構

設計演練討論題項

- 設定演練目標
- 擬定開放且清晰之討論題項：基於學習目標設計討論題目，須確保題項的敘述具體且具討論空間。

辦理演練活動

引導學員討論題項：由專業引導員偕同場域專家引領學員深入理解攻擊情境，並確保討論具交學習目標

評估演練效益

紀錄演練討論內容：由引導員紀錄學員討論內容，並於演練尾聲偕同場域專家給予建議與回饋

CISA Tabletop Exercise Packages

Cybersecurity Scenarios

These CTEPs include cybersecurity-based scenarios that incorporate various cyber threat vectors including ransomware, insider threats, phishing, and Industrial Control System (ICS) compromise. There are also sector-specific cybersecurity scenarios for elections infrastructure, local governments, maritime ports, water, and healthcare.

Physical Security Scenarios

Active shooters, vehicle ramming, improvised explosive devices (IEDs), unmanned aircraft systems (UASs), and many more. There are also CTEPs that are geared towards specific industries or facilities to allow for discussion of their unique needs.

Cyber-Physical Convergence Scenarios

Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector. While CTEPs within the cyber and physical sections may touch on these subjects, convergence CTEPs are designed to further explore the impacts of convergence and how to enhance one's resiliency.

CTEP Documents

Leverage pre-built templates to develop a full understanding of roles and responsibilities for exercise planners, facilitators / evaluators, and participants. Additionally, the documentation includes templates for the initial invitation to participants, a slide deck to use for both planning meetings and conduct, a feedback form to distribute to participants post-exercise, and an After Action Report. In conjunction with selecting one of the above situation manuals, your exercise planning team will be able to fully develop your own tabletop exercise and update information sharing processes; emergency response protocols; and recovery plans, policies, and procedures.

- 美國網路安全與基礎設施安全局(CISA)發展了一系列的資源與手冊來輔助資安或IT主管進行資通安全桌上演練
- 資源包含執行手冊、回饋表等，涵蓋了從前期規劃到後續檢討的全流程。藉由這些範例，各單位可依自身需求，在桌上推演專家的協助下，客製化演練內容，用以檢視並強化內部的資安事件應變與調度資源能力

資料來源：https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

資通安全桌上推演未來發展

Now

首先以醫療場域
為例設計演練

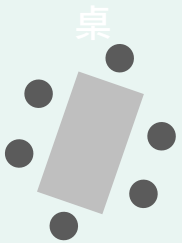
編寫資通安全桌上推演指引

文件化桌上推演方法論與指引，以提供各機關利用於資安策略型人才培訓

演練形式一：資安長班

相同產業的資安長共同討論情境並交流經驗，將課程所學帶回組織檢視現況。

演練形式二：企業專屬情境演練

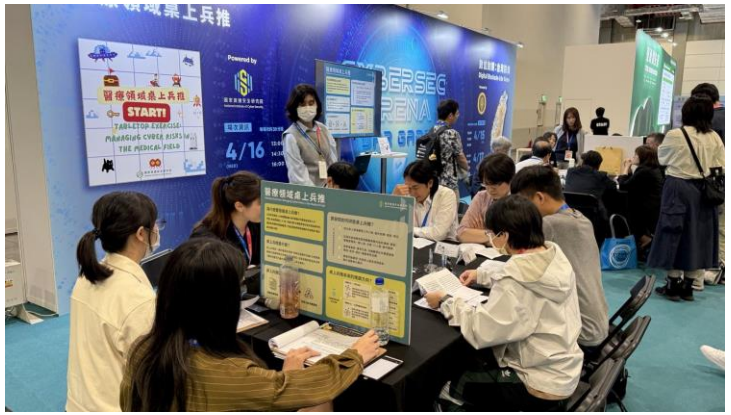


組織決策層共同討論情境，檢視目前的資安應變措施與跨部門協調是否合適。

逐步推廣至關鍵基礎設施與產業

- 通訊傳播
- 交通
- 緊急救援與醫療
- 銀行與金融
- 高科技園區
- 能源
- 水資源
- 中央與地方政府

感謝大家的參與！Cybersec Arena - 桌上推演活動



醫療資安長高階領導班

<資安長職能培訓系列課程>

報名招生中！
5月23日(五)截止

依資安院資安人才職能框架，設計專為醫療及健康領域機構資安主管之職能訓練計畫，以專家實戰分享、五大職能主題、團隊策略激盪、以及桌上推演演練等四大核心訓練，全面提升醫療領域資安主管資安領導力與應變能力，強化醫療體系資安防護力！

詳細課程與報名資訊

資安院徵才中！

威脅狩獵專家
Threat Hunting Specialist

請洽資安院
CT01攤位

工作內容

配合檢測時程派駐國內關鍵基礎設施執行檢測(Assess)、威脅狩獵(Threat Hunting)及事件處理(Incident Response)等服務，協助辨識OT場域的潛在風險與攻擊行為，以保護關鍵基礎設施安全。

工作福利

- 每年定期派員前往國外國家實驗室接受培訓
- 每年補助員工參與國內資安相關教育訓練，以取得資安認證
- 派駐於國內關鍵基礎設施時，給與額外25%駐點加給

技能需求

- 具備資訊安全基礎概念
- 具資安相關經歷(如CTF實績、網頁攻防、資安競賽、資安研究成果等)尤佳
- 熟悉網路基礎知識、熟稔網路產品與設定尤佳
- 熟悉流量檢測、威脅狩獵及主機鑑識基礎知識尤佳
- 熟悉資安檢測相關工具(Wireshark、Security Onion、FTK Imager、IDA Pro、x64dbg等)尤佳
- 熟悉工控通訊協定(Modbus、DNP3等)尤佳
- 具CTIA、OSTH、GNFA等資安相關證照尤佳

學歷

學士以上 (碩士以上優先考慮)

資安院人培中心整體推動策略		持續目標
進階	**以戰代訓：** 發展人才實戰演訓與開發工具	持續強化與深化進階資安人才 之專業與競爭力
中階	**以職能標準推動精準培訓：** 發展我國資安職能基準研究	建構完整資安人才發展體系 滿足職能，逐步提升人才的資安專業
基礎	**系統化方法推動民眾培養意識：** 以社會科學實徵研究洞察推動	深化國民資安意識，展現數位韌性 找尋潛在資安人才加入資安專業

國家資通安全研究院
National Institute of Cyber Security

Thank you & see you at 4F Cyber Talent “CT01”

FB/IG 請搜尋 「資安人蔘」