
企業資安人才培育的挑戰
駭客社群如何培養 CSIRT 高手
李倫銓 ALAN

OUTLINE

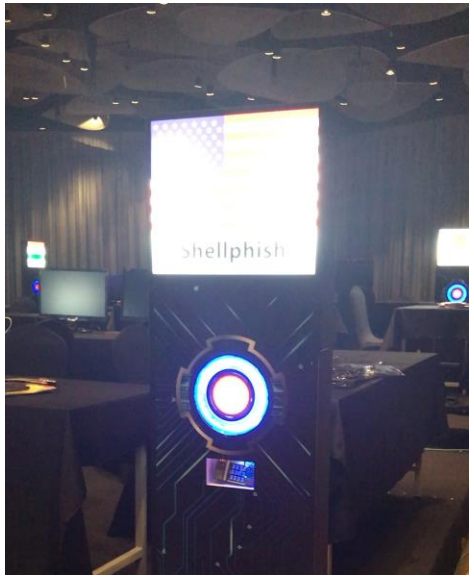
- 快速變化的資安領域，人才面臨的挑戰
- 企業中建立 CSIRT 的挑戰
- 影響企業尋找和留住專業人才的因素

自我介紹

李倫銓

- 現任聯發科資訊本部資安處經理
- 曾任 HITCON CTF 戰隊領隊，取得世界駭客大賽 DEFCON CTF 亞軍 (2014, 2017, 2019)
- 曾協助規劃 HITCON CTF 競賽並推動其成為 DEFCON CTF 種子賽。 (2015 ~ 2019)
- 規劃 HITCON Badge 推動硬體資安人才培育。 (2017 ~ 2019)

舉辦 CTF 駭客比賽培養實戰型資安人才



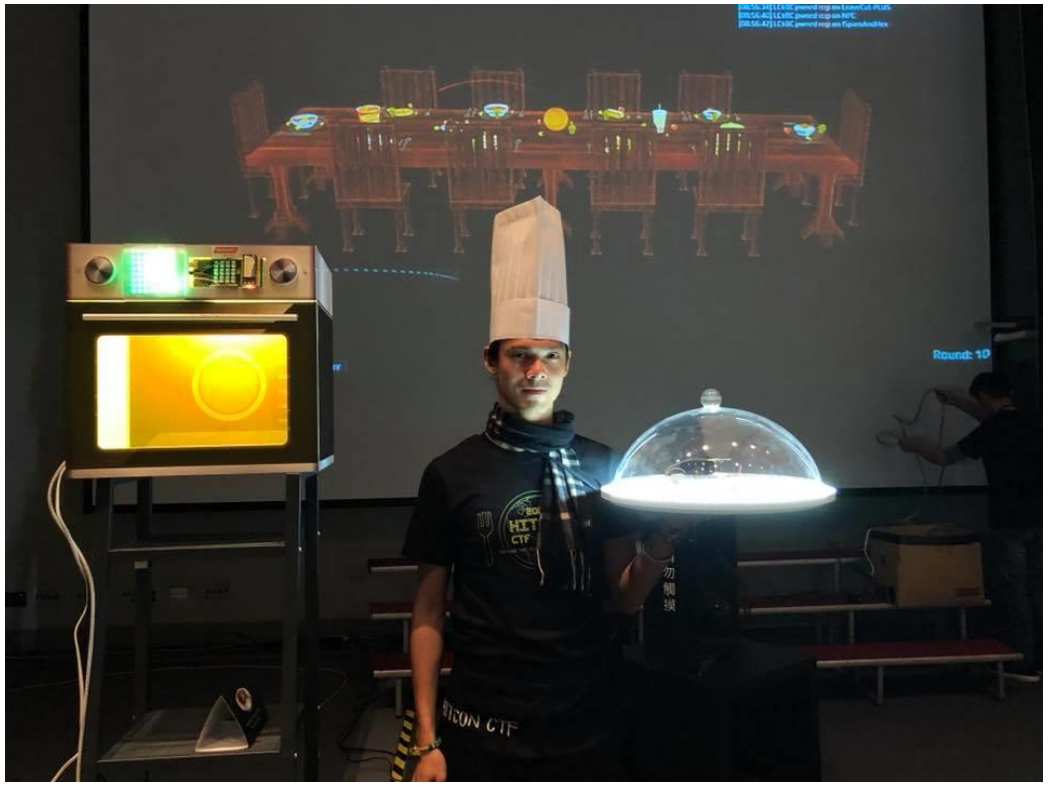
2016 HITCON CTF 決賽戰場特效

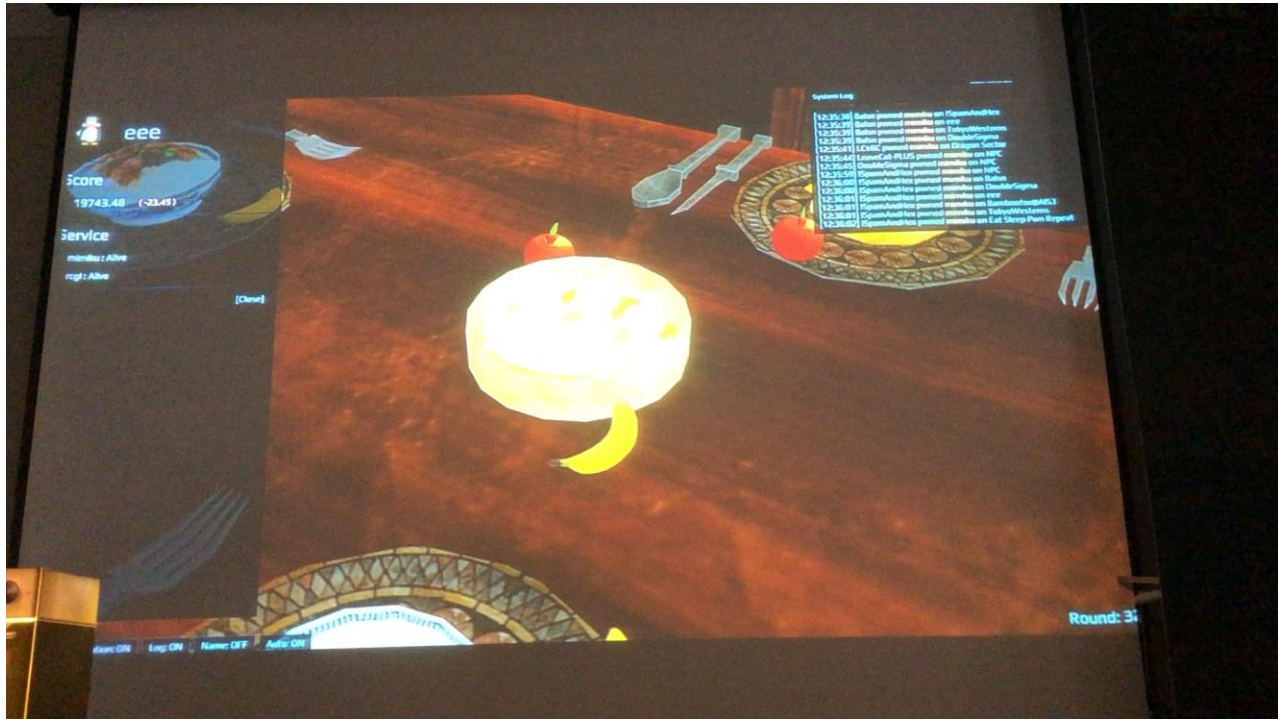
2017 電路板 Badge

2018 電路板 Badge

2019 電路板 Badge

2015 HITCON CTF 決賽戰場特效





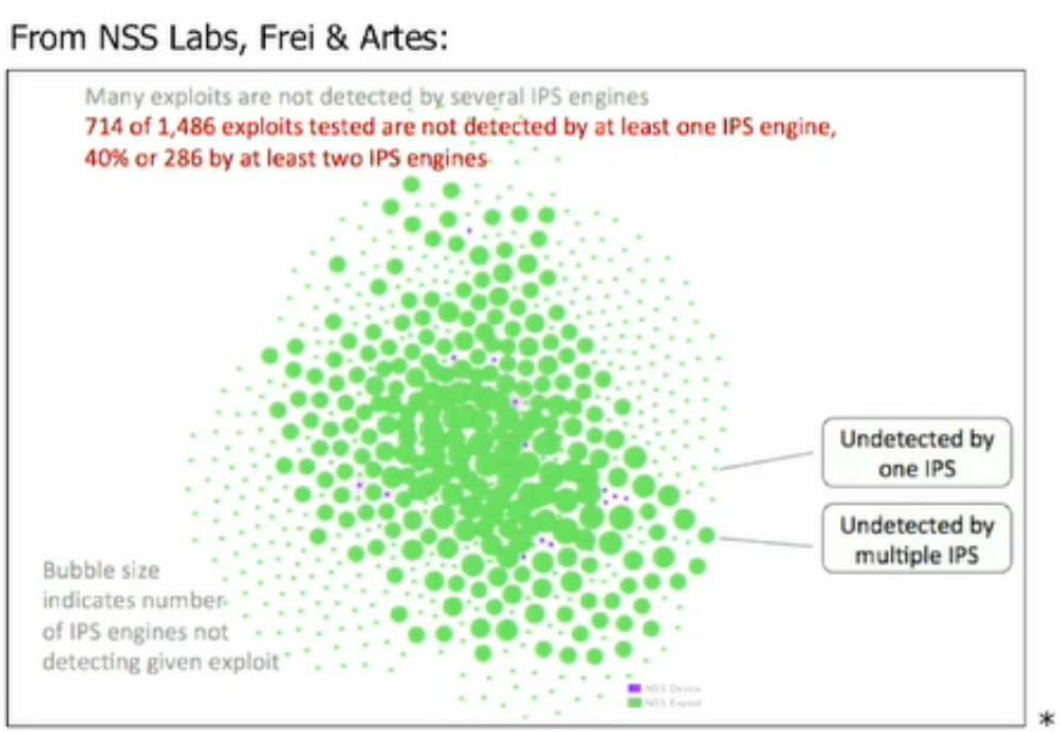
2017 HITCON CTF 決賽戰場特效 – Capture the Food

快速變化的資安領域，人才面臨的挑戰？

- 自動化挖掘漏洞工具的進展，導致人看洞速度是來不及的
- 軟體供應鏈的資安問題，即便是專家也只能疲於奔命被動去解決每一次漏洞災難

1. 隨時得更新技術知識，壓力太大
2. 做不到 100 分 ，當防守方只要被打進一次就輸了

防守方的悲歌 – 聽到駭客開始用 AI



*

NSS 這張圖顯示了當exploit 出現時，
大部分的入侵偵測系統 (IPS) 無法偵測

DARPA 認為光靠人類是不夠的，只有靠電腦的秒級的速度和有系統的判斷，才能控制威脅。

DARPA CGC Cyber Reasoning System (2016)

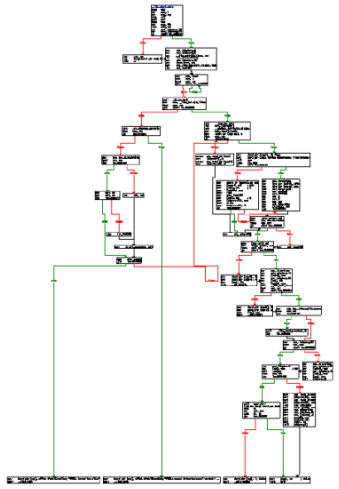
當年的 CGC 比賽，每個隊伍要做出一台 CRS(Cyber reasoning System) 網路推理決策系統，完成下面目的：

- 找出軟體漏洞
- 修補軟體問題 (PCB)
- 分析攻擊
- 設定防火牆
- 製作攻擊(POV)

CGC

DECREE (DARPA Experimental Cyber Research Evaluation Environment) 指令集只有七個

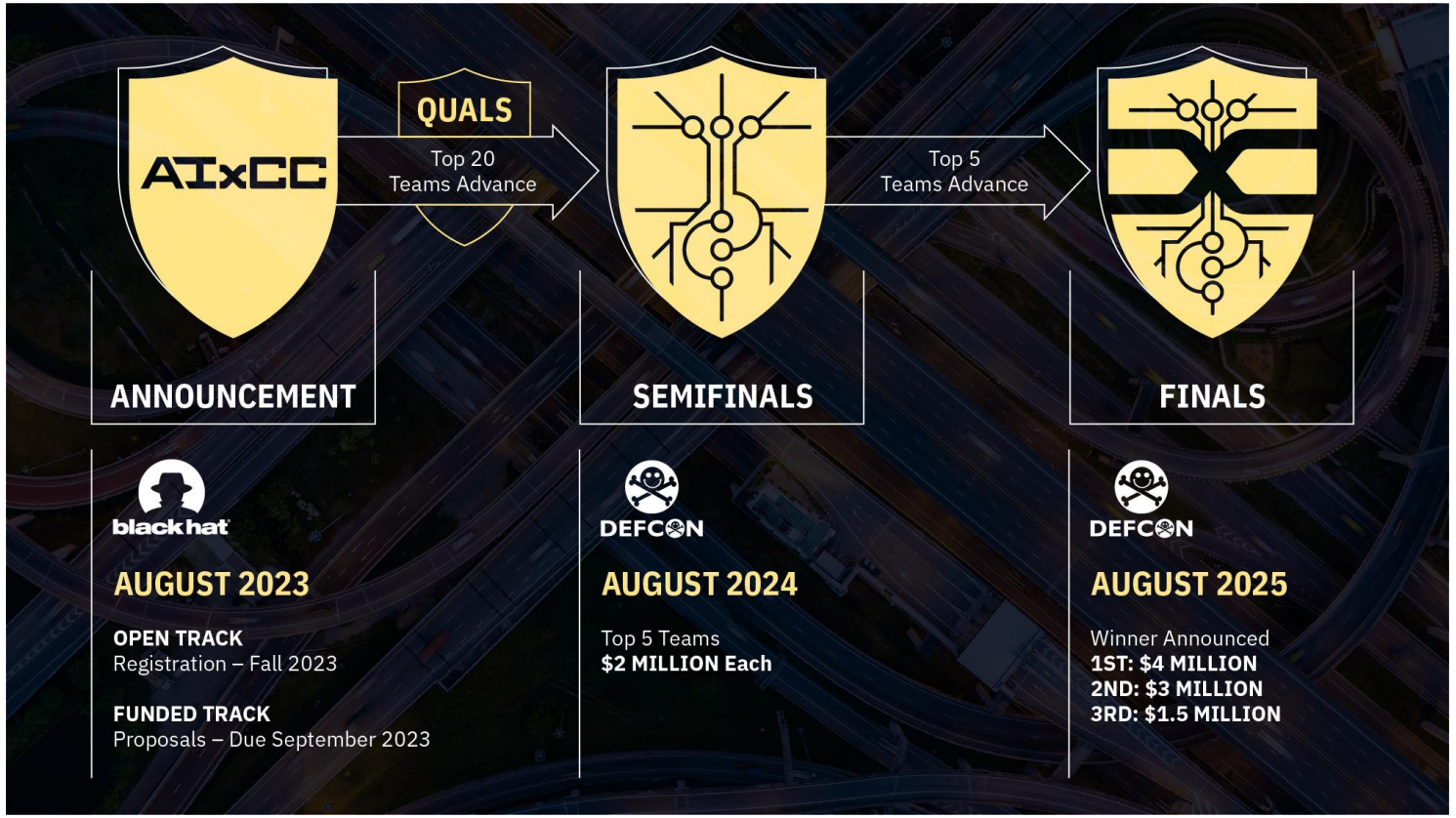
Linux



真實世界的電腦執行路徑非常複雜

2016 年 DARPA CGC 的獎金

AI X CC (2023)



- 初賽獲補助隊伍就可獲得 200萬美金
- 2025 決賽第一名可再獲得 400萬美金

- 拜登政府在 Blackhat 期間宣布一個為期兩年的新計畫，“AI Cyber Challenge”（AIxCC），旨在推動資安技術和AI發展，保護美國的Critical infrastructure。
- 比賽由DARPA主導，並與目前當紅的 AI 公司如 Anthropic、Google、Microsoft和OpenAI合作。總獎金將達到2000萬美元。
- 主辦方會依據真實世界，設計可能存在關鍵開源軟體和關鍵基礎設施的問題，讓參賽隊伍用AI技術解決。
- AIxCC 比賽將分為公開和資助兩個管道，並將在 2024 年和 2025 年的 DEF CON 會議上舉行。

企業中建立 CSIRT 的 10 個挑戰

1. Defining Roles and Responsibilities - 如何建立 **R&R** 與團隊分工？

2. Recruiting Skilled Personnel - 如何招募具有正確技能組合的人才？

3. Training and Development - 持續的培訓對於使團隊瞭解最新的網絡安全趨勢、威脅和回應技術

4. Budget and Resources - 預算與資源的爭取與正確配置

5. Interdepartmental Cooperation - 能不能跨部門合作與溝通？

企業中建立 CSIRT 的 10 個挑戰

6. Incident Response Planning and Testing - 制定全面的事故回應計劃並定期進行測試和更新？

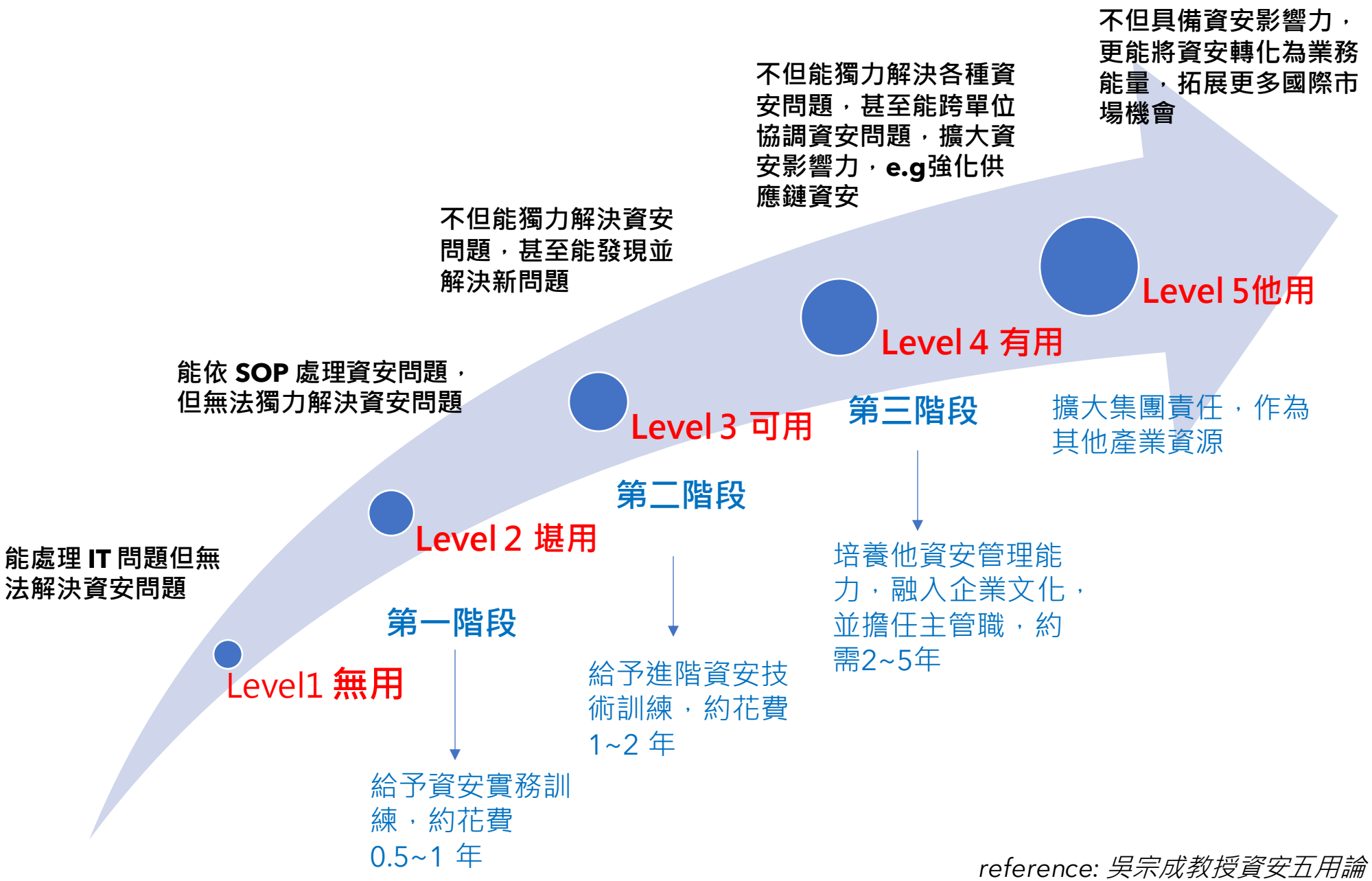
7. Legal and Regulatory Compliance - 理解並遵守法律, 法規要求, 客戶需求

8. Communication and Reporting - 在團隊內部以及與外部利益相關者（如管理機關, 媒體）建立有效的溝通管道

9. Cultural Challenges - 企業文化能接受你的程序嗎？ 也許你需要先在組織裡推廣安全意識

10. Measuring Effectiveness - 建立用於評估 **CSIRT** 效果的指標，並向主管展示效果，這也是一項挑戰。這需要策略性的方法、清晰的領導和來自組織最高層的持續支持。

影響企業尋找和留住專業人才的因素？



reference: 吳宗成教授資安五用論

企業資安人才留用的關鍵

	第一階段 (無用到堪用)	第二階段 (堪用到可用)	第三階段 (可用到有用)
提升目標	**能依 SOP 處理資安問題，但無法獨力解決資安問題**	**不但能獨力解決資安問題，甚至能發現並解決新問題**	**不但能獨力解決各種資安問題，甚至能跨單位協調資安問題，擴大資安影響力，e.g 強化供應鏈資安**
培養能力	給予資安訓練(維運, 檢測..)	培養資安技術學習能力	培養資安管理能力
給予資源	• 給予明確業務發揮空間 • 減少繁瑣業務 (SOC, EDR, AI...)	• 除了給予預算資源，也給予容錯空間 • 增加工作效率 (AI)	共患難，給予願景，讓他認同企業文化
留才方法	**靠教育訓練/考證照綁約**	**靠加薪**	**給予主管職位**
培育週期	0.5~1年	1~2 年	2~5年
效益	約可留用1-3年	約可留用2-5年	約可留用5-10年

參與駭客社群活動有助於掌握駭客思維

- 了解最新的安全威脅
- 學習新技能
- 分享經驗
- 建立人脈
- 參與實戰演練
- 提升問題解決能力
- 道德和法律意識


資安學習道路上的自
我期許及目標設定
企業資安
資安產業
學術研究
專家
新手
參加 PWN2OWN 競賽
HITCON CISO Summit
Bug Bounty Program
Kernel CTF
國際研討會投稿
HITCON
SECCON CTF
DEFCON CTF
DEFCON Village
HITCON CTF 戰隊
Google CTF
Codegate CTF
CTFtime 刷排名 ICC / ACSC CTF
參與實戰演練
國際 CTF 競賽
資安公司實習
Pwnable.tw
HITCON Cyber Range
HITCON Defense
Pwn.College
HITCON Enterprise
CYBERSEC
HITCON Community
神盾盃
金盾獎
持續了解最新的安全威脅
HITCON ZeroDay
AIS3 EOF
CyberDefenders
全國技能競賽
參與攻防演練
HITCON Hackdoor
HITCON Training
台灣好厲駭
AIS3 (Summer School)
My First CTF
HITCON 社群補助
HITCON Girls
HITCON KB
AIS3社團補助
AIS3 Junior


Q/A