林彥廷 | 資深資安工程師 | 紅隊演練與事件回應

中國臺灣,台北市,台北市,台北市大安區復興南路一段 123 號 8 樓,106
+886 2 2712 3456 • yenting.lin@cybersec.tw • https://www.yen-ting-lin.dev
@yentinglin-cyber • @yentinglin-cyber • @yenting-lin

簡介

- 具備超過 8 年資訊安全經驗,專注於滲透測試、紅隊演練、事件回應與資安維運。
- 熟悉 MITRE ATT&CK、OWASP Top 10、NIST CSF 與 ISO 27001 等框架,能將攻擊手法轉化為可執行的防禦策略。
- 擅長使用 Python、Go 與 Shell 開發自動化工具,提升弱點管理與威脅偵測效率。
- 具備跨部門溝通與專案管理能力,曾帶領 4 人小組完成金融業零信任架構導入。

教育背景

國立臺灣大學 **https://www.ntu.edu.tw/**

碩士,資訊工程學系,成績:4.1/4.3 2014 年 9 月–2016 年 6 月

- 研究主題聚焦於入侵偵測與惡意流量分析
- 參與實驗室與企業合作之資安專案,建立威脅情報分析流程
- 擔任課程助教,協助教授計算機安全與密碼學課程

課程:計算機安全、密碼學、網路安全、作業系統、資料庫系統、分散式系統

國立交通大學 **https://www.nctu.edu.tw/**

學士,資訊工程學系,成績:3.9/4.3 2010 年 9 月–2014 年 6 月

- 建立程式設計與計算機網路基礎
- 參加校內資安社團,開始接觸 CTF 競賽

課程:資料結構、演算法、計算機組織、作業系統、網路程式設計

工作經歷

藍盾資訊安全股份有限公司 **https://www.blueshield-sec.tw/**

資深資安工程師 2021 年 3 月至今

- 主導滲透測試與紅隊演練專案,涵蓋金融、電商與政府單位,年均完成 20 餘件專案
- 建立以 MITRE ATT&CK 為基礎的攻擊模擬與偵測規則,提升 SIEM 告警準確率 35%
- 規劃與執行事件回應流程,協調跨部門進行入侵調查、橫向移動分析與復原
- 帶領 4 人資安小組,負責專案排程、技術指導與客戶溝通
- 推動 ISO 27001 與 NIST CSF 控制措施落地,協助客戶通過第三方稽核

關鍵字:滲透測試、紅隊演練、事件回應、MITRE ATT&CK、SIEM、弱點管理、ISO 27001

雲峰科技股份有限公司 **https://www.cloudpeak-tech.tw/**

資安工程師 2018 年 4 月–2021 年 2 月

- 負責企業客戶資安健診、弱點掃描與滲透測試,提供修補建議與風險排序
- 建置與維運 ELK 日誌分析平台,設計威脅偵測規則與儀表板
- 協助客戶處理資安事件,進行惡意程式初步分析與數位鑑識
- 撰寫資安報告與 SOP,並對客戶進行資安意識教育訓練

關鍵字:弱點掃描、滲透測試、ELK、數位鑑識、資安健診、教育訓練

台灣數位金融股份有限公司 **https://www.twdigitalfinance.tw/**

網路安全分析師 2016 年 7 月–2018 年 3 月

- 監控網路與端點安全事件,進行告警分流、調查與升級處理
- 維運防火牆、WAF 與 IDS/IPS,定期檢視規則與調整政策
- 參與行動銀行 App 安全檢測,協助修補 OWASP Top 10 相關弱點
- 建立資安事件通報流程與每月營運報表

關鍵字:事件監控、WAF、IDS/IPS、OWASP Top 10、行動安全、通報流程

語言

中文：母語或雙語水平 — **關鍵字**：母語

英語：完全專業水平 — **關鍵字**：TOEIC 950、IELTS 7.5

日語：初級水平 — **關鍵字**：JLPT N4

專業技能

滲透測試與紅隊：專家 — **關鍵字**：OWASP Top 10、Burp Suite、Metasploit、Nmap、Kali Linux、社交工程

事件回應與鑑識：高級 — **關鍵字**：SIEM、Splunk、ELK、數位鑑識、惡意程式分析、MITRE ATT&CK

程式與自動化：高級 — **關鍵字**：Python、Go、Bash、PowerShell、SQL、REST API

雲端與容器安全：中級 — **關鍵字**：AWS、Azure、GCP、IAM、Kubernetes、容器安全

資安治理與合規：高級 — **關鍵字**：ISO 27001、NIST CSF、風險管理、合規稽核、資安政策

榮譽

年度最佳資安專案獎

藍盾資訊安全股份有限公司 — 2023 年 12 月

- 表揚於金融業紅隊演練專案中發現重大風險並提出有效改善方案
- 專案協助客戶降低橫向移動風險並強化偵測能力

台灣資安 CTF 競賽第一名

台灣資安社群聯盟 — 2019 年 8 月

- 帶領 4 人團隊於 Web、Pwn 與 Reverse 題型中取得佳績
- 負責解題策略規劃與弱點利用腳本開發

證書

CISSP 國際資訊系統安全認證 — **https://www.isc2.org/certifications/cissp**

ISC2 — 2022 年 6 月

OSCP 滲透測試認證 — **https://www.offsec.com/courses/pen-200/**

Offensive Security — 2020 年 11 月

AWS Certified Security - Specialty — **https://aws.amazon.com/certification/certified-security-specialty/**

Amazon Web Services — 2021 年 9 月

CEH 道德駭客認證 — **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/**

EC-Council — 2019 年 5 月

出版刊物

台灣資訊安全期刊 — **https://www.taiwan-infosec-journal.tw/articles/attck-supply-chain**

以 MITRE ATT&CK 為基礎的供應鏈攻擊偵測方法 — 2022 年 11 月

- 提出結合 ATT&CK 技術與 SIEM 規則的偵測框架
- 以實際事件案例驗證偵測覆蓋率與誤報率改善

項目

紅隊演練自動化平台 — **https://github.com/yentinglin-cyber/redteam-automa**

以 Python 與 Go 開發的紅隊演練輔助平台，整合偵察、弱點驗證與報告產出。 — 2022 年 1 月–2023 年

- 整合 Nmap、Burp Suite 與自製腳本，自動化執行偵察與弱點驗證
- 建立 ATT&CK 技術對應標籤，協助團隊快速彙整攻擊路徑與防禦建議
- 將報告產出時間由 2 天縮短至 4 小時

關鍵字：自動化、紅隊演練、Python、Go、ATT&CK

金融業零信任架構導入

協助金融客戶規劃與導入零信任架構，涵蓋身分驗證、裝置信任與微隔離。 — 2021 年 8 月–2022 年 12 月

- 盤點關鍵資產與高風險存取路徑，制定分階段導入計畫
- 導入多因子驗證、條件式存取與網路微隔離控制
- 建立監控指標與異常行為告警，提升橫向移動偵測能力

關鍵字：零信任、身分驗證、微隔離、條件式存取、金融安全

興趣愛好

CTF 競賽：Web、Pwn、Reverse、Crypto

戶外活動：登山、馬拉松、攝影

志願服務

台灣資安教育推廣協會 **https://www.taiwan-cyber-edu.org/**

資安志工講師 2019 年 1 月–2023 年 12 月

- 至大專院校與高中分享資安職涯與基礎防護觀念
- 協助辦理資安工作坊與 CTF 新手教學
- 參與偏鄉資訊教育營隊，教授網路安全與密碼學入門