林 昱安

網路安全工程師

yuan.lin@example.com
0912-406-785
台北市內湖區

個人總結

網路安全工程師，專注企業 SOC、雲端防護與事件應變。熟悉 Splunk、Microsoft Sentinel、Python、AWS Security Hub 與 MITRE ATT&CK，能與 IT、開發和法遵團隊把警示轉成可驗證的風險降低。

工作經歷

網路安全工程師

3/2021 - 至今

曜盾雲端服務 • 台北

- 以 Splunk 關聯 2.4 億筆日誌並建立 38 條 MITRE ATT&CK 偵測規則，和 6 位 SOC 分析師將高風險告警誤報率降低 42%。
- 用 Python 自動化 AWS Security Hub 分流與 Jira 建單，協作 4 個平台團隊處理 1,800 個月度事件，平均分派時間由 18 分鐘縮至 4 分鐘。
- 部署 EDR 到 1,420 台端點並以 PowerShell 建立隔離劇本，和 IT 支援及法遵完成 7 次演練，勒索軟體反應時間縮短 63%。
- 依 NIST CSF 盤點 86 項控制措施，協同 12 位系統負責人補齊證據，年度外部稽核重大缺失由 9 項降至 2 項。
- 以 GuardDuty 追蹤 420 個 AWS 帳號的異常行為，與雲端架構師完成 14 個 IAM 修正，未授權存取事件下降 35%。

資安分析師

7/2018 - 2/2021

北極星物流科技 • 新北

- 在 QRadar 建立 24 個物流 API 偵測情境，和 5 位網路工程師分析每日 6,500 萬筆流量，異常發現提前 29%。
- 使用 Wireshark 與 Zeek 調查 31 起可疑連線，協作 3 個資料中心完成封鎖，平均事件關閉時間降低 37%。
- 以 PowerShell 整理 980 台 Windows 端點弱點清單，和桌面工程團隊推動 4 波修補，嚴重弱點逾期率下降 48%。
- 主持 8 場釣魚演練與 420 人訓練，和 HR、法遵追蹤回報率，點擊率由 14% 降至 5%。

系統管理員

8/2016 - 6/2018

森嶼資訊整合 • 台北

- 以 Linux auditd 與 Bash 盤點 230 台伺服器登入紀錄，和 4 位維運同仁建立 12 個高風險門檻，稽核查找時間節省 16 小時 / 月。
- 用 Nessus 掃描 1,100 個資產並以 Jira 分派 76 個修補任務，協作開發與網管將高風險漏洞修復率提升至 91%。
- 部署 OpenVPN 與多因素驗證給 280 位遠端員工，和 HR 及客服完成 3 輪切換，帳號接管事件維持 0 件。
- 整理 19 份備份與復原 runbook，帶領 7 人完成 6 次演練，關鍵服務復原時間由 9 小時縮至 3 小時。

教育背景

資訊工程學士 資訊工程學系

9/2015 - 6/2019

國立臺灣科技大學

技能專長

監控與應變:	Splunk • Microsoft Sentinel • SIEM • EDR • MITRE ATT&CK
雲端與身分:	AWS Security Hub • IAM • GuardDuty • Azure • Zero Trust
自動化與治理:	Python • PowerShell • NIST CSF • Jira • Incident Response

專案經驗

SOC 偵測與應變自動化

把 SIEM、EDR、雲端告警與工單流程串成可追蹤的事件生命週期。

使用技術: Splunk, Python, EDR, Jira

雲端身分風險治理

以 IAM、GuardDuty 與 NIST 控制項降低多帳號環境的未授權風險。

使用技術: AWS Security Hub, IAM, GuardDuty, NIST CSF

證書獎項

- **CompTIA Security+** - CompTIA • 2019
- **AWS Certified Security - Specialty** - Amazon Web Services • 2023

語言能力

- **中文** - 母語
- **英文** - 資安文件與跨國事件會議