教育背景

工學碩士
國立臺北科技大學
電機工程學系
2015-09 - 2019-06

技能專長

OT 與工控

- Claroty
- Nozomi
- IEC 62443
- SCADA
- Asset Discovery

偵測與分析

- Splunk
- Python
- YARA
- Threat Modeling
- Network Forensics

治理與應變

- NIST 800-82
- Risk Workshop
- Incident Command
- Vendor Review
- Training

證書獎項

GIAC Global Industrial Cyber Security Professional
SANS Institute
2019-10

ISA/IEC 62443 Cybersecurity Certificate
ISA

個人總結

網路安全專家，專注 OT 安全、威脅建模與高風險環境防禦。熟悉 Claroty、Nozomi、Splunk、Python 與 IEC 62443，能協調工程、營運與監管需求保護關鍵設備。

工作經歷

網路安全專家
重岳能源系統
台北
2018-11 - 至今

• 以 Claroty 與 Nozomi 建立 14 座工廠的 OT 資產可視性，和 22 位控制工程師分類 6,800 台設備，未知資產下降 72%。
• 依 IEC 62443 與 NIST 800-82 帶領 19 場風險工作坊，協作營運與供應商識別 205 個風險，關鍵控制覆蓋率提升 41%。
• 用 Splunk 與 Python 建立 27 條工控異常偵測規則，和 SOC、維運團隊完成 8 次演練，告警確認時間縮短 58%。
• 審查 63 家設備供應商的遠端存取與更新流程，協同採購完成 31 份改善計畫，高風險例外下降 46%。
• 主持跨部門事故指揮與復原測試，動員 37 位工程、法遵及公關成員，年度重大中斷時間縮短 34%。

OT 安全工程師
磐石工業網路
台中
2015-06 - 2018-10

• 以 Nozomi 監控 9 個製造網段與 2,100 台設備，和 8 位網路工程師建立 17 個基線，異常流量告警準確率提升 36%。
• 用 Python 整理 480 個韌體與設備版本，協作維護團隊排出 4 波更新，過期版本數量下降 29%。
• 依 NIST 800-82 重整 12 份 OT 事件 playbook，帶領 6 場桌上演練，初步分工時間由 48 分鐘縮至 16 分鐘。
• 以 YARA 與網路鑑識檢視 28 起 USB 與遠端連線事件，和廠務及資安團隊完成封鎖，重複事件下降 40%。

2021-06

語言能力

中文 母語

英文 工控標準與供應商會議

網路安全工程師 新竹
東嶺自動化 2013-07 - 2015-05

• 用 Wireshark 分析 190 個 PLC 通訊情境，和 5 位控制工程師建立白名單，未授權協定使用降低 31%。
• 以 Nmap 掃描 620 個設備服務，協作維運關閉 84 個不必要埠號，外部暴露面下降 27%。
• 整理 15 份安全架構與連線圖，支援 4 個客戶稽核，補件往返次數減少 45%。
• 協助規劃 3 套隔離環境並驗證復原，與 9 位現場工程師完成 5 次演練，關鍵設備恢復時間縮短 25%。

專案經驗

跨工廠 OT 資產可視性
以被動監測、資產分級與控制規則掌握工控環境風險。

Claroty Nozomi IEC 62443 SCADA

工控事件指揮演練
把技術遏制、營運持續與供應商通報納入同一套 playbook。

NIST 800-82 Splunk Python Incident Command