鄭 柏翰

高級網路安全分析師

pohan.cheng@example.com

0928-517-460

新北市板橋區

技能專長

進階調查

Digital Forensics · Velociraptor · Volatility · Threat Hunting · Chain of Custody

情報與 SIEM

MISP · Splunk · MITRE ATT&CK · YARA · STIX/TAXII

事件領導

Incident Command · Root Cause · Python · Executive Briefing · Mentoring

教育背景

理學碩士 – 資訊工程學系
國立臺灣大學
2015-09 – 2019-06

語言能力

中文 母語

英文 威脅情報與跨國事件指揮

證書獎項

GIAC Certified Incident Handler
SANS Institute · 2018-12

GIAC Certified Forensic Examiner
SANS Institute · 2020-05

個人總結

高級網路安全分析師，專注威脅情報、數位鑑識與複雜事件指揮。熟悉 MISP、Velociraptor、Splunk、Python 與 MITRE ATT&CK，能帶領分析師從證據、根因到管理層復原決策。

工作經歷

高級網路安全分析師

遠洋航運集團 · 新北 — **2019-08 – 至今**

- 以 MISP 與 STIX/TAXII 整合 27 個威脅情報來源，帶領 9 位分析師更新 63 條 Splunk 偵測，命中率提升 34%。
- 使用 Velociraptor 與 Volatility 調查 18 起跨區域入侵，協作 IT、船舶系統與法務共 31 人，證據交付時間縮短 47%。
- 以 Python 自動化 1,900 台端點的 IOC 搜尋與隔離，和 6 個國家服務台建立流程，初步遏制時間由 52 分鐘降至 11 分鐘。
- 主持 14 次紫隊演練並依 ATT&CK 建立 38 個缺口，協作工程與 SOC 團隊完成 82% 修正，重大重複事件下降 29%。
- 培訓 12 位中階分析師建立鑑識筆記與 chain of custody，年度重大事件報告準時率達 100%。

資安事件分析師

星河電信服務 · 台北 — **2016-03 – 2019-07**

- 以 Splunk 分析每日 4.6 億筆電信流量，和 7 位情報研究員建立 21 個異常通聯模型，帳號濫用事件下降 26%。
- 使用 YARA 與 sandbox 分析 140 個惡意樣本，協作 5 位端點工程師封鎖 320 個 IOC，誤封率維持低於 1.5%。
- 以 Volatility 重建 11 台受感染主機的記憶體證據，與法務完成 8 次報告，平均鑑識週期縮短 41%。
- 建立 17 份事件 playbook 並主持 10 場演練，和客服及公關對齊通報流程，重大事件升級時間減少 38%。

資安分析師

啟明資安實驗室 · 台北 — **2013-07 – 2016-02**

- 用 Wireshark 與 Zeek 分析 8,400 萬筆封包，協助團隊建立 16 個偵測案例，異常連線確認時間縮短 22%。
- 以 Nessus 驗證 760 台伺服器弱點，和 4 位系統管理員規劃修補窗口，嚴重漏洞數量降低 33%。
- 撰寫 46 份調查摘要與 9 份高階報告，與 3 個客戶團隊對焦根因，報告採用率達 92%。
- 協助建立 24 小時輪值表與升級矩陣，協作 8 位分析師，週末事件交接遺漏下降 61%。

專案經驗

跨國威脅情報融合

把外部情報、端點 IOC 與 SIEM 偵測轉為可衡量的防禦覆蓋。

MISP　STIX/TAXII　Splunk　MITRE ATT&CK

鑑識證據自動搜尋

以 Velociraptor、Volatility 與 Python 縮短大規模端點調查。

Velociraptor　Volatility　Python　YARA