吳 欣怡

初級網路安全分析師

hsinyi.wu@example.com 0986-741-235 桃園市中壢區

個人總結

初級網路安全分析師，具備 SOC 告警分流、端點盤點與資安報告經驗。熟悉 Microsoft Sentinel、Defender、Excel 與 PowerShell，能在輪值團隊中維持清楚的證據與升級紀錄。

工作經歷

初級網路安全分析師
橙線電商集團
4/2023 - 至今

- 以 Sentinel 分流每日 680 個告警，和 5 位 SOC 輪值夥伴依 KQL 建立 14 個篩選條件，升級準確率提升 23%。
- 用 Defender 盤點 1,060 台端點並以 PowerShell 推送修正，協作 IT 團隊將未安裝安全更新比例由 17% 降至 6%。
- 以 Excel 整理 420 個弱點與資產重要性，和 8 位系統負責人追蹤 3 波修補，高風險逾期件減少 39%。
- 撰寫 96 份事件摘要與 12 份週報，協作主管、客服及法遵完成 4 次檢討，重複追問工單下降 18%。

IT 安全助理
禾日會員服務
7/2021 - 3/2023

- 用 Nessus 掃描 350 個伺服器與網路資產，和 3 位維運工程師確認修補影響，嚴重漏洞關閉率達 88%。
- 以 PowerShell 查核 2,400 個本機管理員帳號，協作 IAM 團隊回收 620 個過度權限，權限例外減少 46%。
- 參與 5 次釣魚郵件調查，整理 1,800 個郵件標頭並交給 SOC，平均初步回覆時間縮短至 25 分鐘。
- 建立 11 份 Confluence 操作指南，與客服培訓 34 位同仁，資安工單一次解決率提升 21%。

教育背景

資訊管理學士
元智大學
9/2015 - 6/2019

技能專長

SOC 分析

Microsoft Sentinel, KQL, Alert Triage, Defender, Incident Notes

端點與弱點

PowerShell, Nessus, Asset Inventory, Patch Tracking, Windows

協作工具

Excel, Jira, Confluence, Ticketing, Presentation

專案經驗

零售 SOC 告警分流
以 Sentinel、KQL 與端點資訊改善初級告警判斷與升級品質。

Microsoft Sentinel | KQL | Defender | PowerShell

權限盤點與修補追蹤
把帳號、資產與弱點狀態整理成可供團隊協作的清單。

Nessus | Excel | Jira | Confluence

語言能力

中文 母語

英文 SOC 文件閱讀

證書獎項

Microsoft SC-900
Microsoft
2023

CompTIA Security+
CompTIA
2024