許 芷瑜

網路安全分析師

個人資訊

chiyu.hsu@example.com

0926-514-308

新竹市北區

技能專長

威脅分析

- KQL
- Splunk
- Threat Hunting
- YARA
- MITRE ATT&CK

端點與網路

- Defender for Endpoint
- Nmap
- Wireshark
- DNS
- TCP/IP

分析流程

- Python
- Excel
- Incident Triage
- Jira
- Report Writing

教育背景

國立陽明交通大學

理學碩士

資訊安全研究所

09/2015 - 06/2019

語言能力

中文 母語

英文 威脅情報與技術報告

證書獎項

GIAC Security Essentials

SANS Institute

04/2022

Microsoft Certified: Security Operations Analyst

Microsoft

02/2023

個人總結

網路安全分析師，專注威脅狩獵、SIEM 調查與漏洞優先排序。擅長 KQL、Splunk、Defender for Endpoint、Nmap 與 Python，能把大量遙測資料整理成 SOC 可執行的判斷。

工作經歷

網路安全分析師 11/2021 - 至今

竹安半導體

新竹

- 以 KQL 查詢 9,600 台端點的 Defender 遙測資料，與 8 位 SOC 夥伴建立 42 個 hunting query，疑似入侵確認時間縮短 51%。
- 用 Splunk 分析 3.1 億筆 DNS 與 proxy 事件，和網路團隊新增 18 條偵測規則，惡意網域攔截率提升 27%。
- 以 YARA 與 Python 分析 64 個可疑樣本，協作 5 位 IR 工程師完成 12 次隔離，平均證據整理時間由 2 小時降至 35 分鐘。
- 建立漏洞風險評分模型，結合 CVSS、資產重要性與 2,800 個弱點，和 14 位系統負責人將修補準時率提升至 89%。

資安監控專員 06/2018 - 10/2021

晶瀚電子製造

新竹

- 監看 QRadar 每日 1,200 個告警並依 MITRE 分類，和 6 位輪值分析師將升級事件漏報率降至 1.8%。
- 使用 Wireshark 重建 23 起橫向移動路徑，協作網管與工廠 OT 團隊封鎖 17 個來源，調查週期縮短 44%。
- 以 Nmap 與 Nessus 驗證 640 台產線設備，和 9 位設備工程師安排維護窗口，高風險曝險資產減少 31%。
- 撰寫 26 份事件報告與 11 份管理摘要，協助法遵完成 ISO 27001 證據準備，缺件數由 34 項降至 8 項。

專案經驗

製造網路威脅狩獵

結合端點、DNS 與代理資料建立可重複的 hunting playbook。

KQL Splunk YARA Python

漏洞風險排序模型

將 CVSS、資產關鍵度與可利用性轉成修補優先序。

CVSS Nmap Nessus Excel