



CODE BLUE

**DIGITAL CODE BLUE：當防禦失效，我們負責救活。**

**企業資料的加護病房（ICU）——五匠資料解密救援服務。**

**行動呼籲：尋求全台 MSP、SI 戰略合作夥伴。**

# 病歷報告 (The Diagnosis)

## ⊕ 病危通知單

您的客戶正在「數位瀕死」邊緣。



2024年台灣製造業與醫療業

**66%**  
激增攻擊頻率



**24** 天  
平均停機時間



**273** 萬美元  
平均恢復成本

這不僅僅是 IT 故障，這是企業的心跳停止。  
當防火牆被突破、防毒軟體被繞過、備份被加密，  
誰能接手這場生死攸關的手術？



# 病毒病理學 (The Pathology)



對手已進化：這不是普通的感冒。



**現代勒索病毒**  
(如 LockBit 3.0, Qilin)  
採用軍規級加密演算法  
(AES-256 + RSA-4096)。



**雙重勒索**  
先竊取，後加密。



**針對性獵殺**  
專門攻擊台灣供應鏈、  
醫療系統與虛擬化平台  
(ESXi)。



**備份毀滅**  
攻擊者第一步往往是刪除  
所有的 Shadow Copies  
與備份檔。

**結論：**傳統的「備份還原」策略在面對針對性攻擊時，存活率正大幅下降。

# 市場缺口 (The Gap)

防護廠商



受害企業



五匠



**疫苗無法治療槍傷：防護與救援的斷層。**

大多數資安廠商專注於「預防」 (Prevention) 。  
但當預防失敗時，市場上缺乏專業的「救援」 (Rescue) 服務。



**國際大廠**

限制多，不談判，遠水難救近火。



**硬體救援店**

無法解開邏輯加密鎖。



**五匠定位**

我們填補這個致命缺口。  
我們是數位世界的急診室醫生。



# 五匠解決方案概覽 (The Solution)

## 五匠急救協定



### 檢傷分類區



加密勒索病毒辨識：精準判讀病原體。

感染範圍確認：全身性掃描，確認擴散程度。



談判與支付評估：專業的危機談判專家介入。

駭客談判 (Negotiation)：為客戶爭取生存空間。



解密與數據恢復：獨家技術修復受損資料庫。

### 恢復室



恢復室：數據與系統功能全面復原，確認安全無虞。

我們提供一站式的勒索病毒解決方案：從危機識別到最終復原，我們與您並肩作戰。

# 核心能力 I - 談判專家 (The Negotiator)



## 危機談判：心理戰的藝術。

與駭客溝通需要專業技巧。一句錯誤的回應可能導致贖金翻倍或金鑰被毀。五匠的談判專家團隊：



**知己知彼：**掌握各大勒索家族的底價與信譽評分。



**降低損失：**平均協助客戶降低 30% - 50% 的贖金要求。



**生存證明 (Proof of Life)：**強制駭客先解密樣本檔案，確保交易安全性。

我們是您與深淵之間的防火牆。



## 核心能力 II - 技術解密 (The Surgeon)



### 精密手術：超越解密金鑰。

拿到駭客給的解密器 (Decryptor) 往往只是災難的開始。駭客的工具通常寫得很爛，執行過快會導致大型資料庫 (SQL, Oracle, Exchange) 崩潰。五匠技術優勢：



**資料庫結構修補：**我們能修復解密後仍無法掛載 (Mount) 的資料庫。



**虛擬機救援：**針對 ESXi 被加密的.vmdk 檔有專門的修復技術。



**失敗救援：**即使其他廠商宣告不治，我們仍能透過底層數據雕刻 (Data Carving) 嘗試最後一線生機。

我們是您數位資產的最後一道防線。

# 競爭優勢比較表 (The Comparison)

服務項目 (Service Item)	全球資安大廠 (Global Vendors)	本地硬體救援 (Local Recovery Labs)	五匠有限公司 (Wujiang)
 服務核心 (Service Core)	預防與偵測 (Prevention)	硬體修復 (Hardware)	 解密與救援 (Rescue)
 駭客談判 (Hacker Negotiation)	✗ (政策禁止)	✗ (無能力)	✓ (核心專長)
 資料庫邏輯修復 (Database Logic Repair)	✗	✗	✓
 反應速度 (Response Speed)	需簽約/流程長 (Long Process)	快 (Fast)	⚡ 極速 (24/7 待命) (Ultra-Fast 24/7)
 在地化支援 (Localization Support)	弱 (英語為主) (Weak, English)	強 (Strong)	 強 (台語/中文/英語) (Strong, Multi-lingual)

# 案例研究 A – 製造業



情境 (SITUATION)：遭 LockBit 3.0 鎖定，ERP 系統癱瘓，產線停擺。備份伺服器同步被毀。



T+2小時：確認病毒株，封鎖網路出口。



T+12小時：談判專家介入，將贖金從 50 萬美元談判至 15 萬美元。



T+36小時：取得金鑰，修復 2TB ERP 資料庫。



結果 (RESULT)：48 小時內復工，保住國際大廠訂單。



# 案例研究 B - 醫療業 (Case Study: Healthcare)

## 急救案例：區域教學醫院 PACS 系統救援

情境 (SITUATION)：遭 CrazyHunter 攻擊，醫療影像系統 (PACS) 無法存取，急診手術被迫延期。



識別出該變種病毒的加密漏洞 (無需支付贖金)。



利用五匠自研工具進行逆向解密。



修復受損的 DICOM 影像檔頭。



結果 (RESULT)：24 小時內恢復 95% 影像資料，病患安全無虞。



# 合作夥伴計畫 (The Partner Program)

## 徵召令：加入「數位創傷應變聯盟」。

我們正在尋找 MSP (管理服務供應商)、SI (系統整合商) 與 VAR (加值經銷商)。為什麼您需要五匠？



**風險轉移：**您不需要處理高風險的加密貨幣與談判，這些髒活累活交給我們。



**客戶留存：**當客戶出事時，您能拿出解決方案，而不是只能說「重灌」。救活客戶，才能留住合約。



**利潤共享：**豐厚的推薦獎金與救援分潤機制。

讓我們攜手，共同守護數位世界的生命線。



# 合作模式詳解 (Engagement Models)

## 彈性的合作模式。



### 模式 A：緊急轉診 (Referral)

您只需通報案件，五匠全權處理後續救援。您獲得推薦佣金，零風險。



### 模式 B：白牌服務 (White Label)

五匠作為您的幕後技術團隊，以您的名義出勤。增強您的品牌專業度。



### 模式 C：戰略聯盟 (Strategic Alliance)

將五匠服務打包進您的年度維護合約 (MA)，為客戶提供「資安險」級別的保障。

選擇最適合您的合作模式，共創雙贏局面。

# 給合作夥伴的支援 (Partner Support)

CYBER-MEDICAL

## 您的後勤補給庫。



### 24/7 優先通道

合作夥伴案件享有最高優先級  
(Triage Level 1)。



### 教育訓練



定期舉辦勒索病毒趨勢分析與第一線應變教育訓練。



### 行銷資源



提供聯名行銷素材，協助您教育客戶。

全方位支援，助您成為客戶的資安守護者。

# 常見問題 (FAQ for Partners)

## 關於救援，您需要知道的事。



**Q1：付了贖金真的拿得回資料嗎？**

**A：五匠透過嚴格的「生存證明」驗證與信譽資料庫比對，將成功率提升至 98% 以上。**



**Q2：這合法嗎？**

**A：五匠嚴格遵守當地法律規範，並協助客戶進行合規的支付評估與報案流程。**



**Q3：救援需要多久？**

**A：從進場到解密開始，平均小於 24 小時。**



**專業、透明、高效，是我們的承諾。**

封底與行動呼籲 (Call to Action)

**別讓您的客戶獨自面對黑暗。**



**啟動救援**

**立即加入五匠合作夥伴計畫，成為客戶最信賴的最後一道防線。**

五匠有限公司

[aki@5takumi.com.tw](mailto:aki@5takumi.com.tw)

