星球永續健康線上直播

星球健康週新知 &

專題: 智慧數位資安 (3)

醫療智慧資安

2026-04-15

CHE團隊：
陳秀熙教授、許辰陽醫師、陳立昇教授、嚴明芳教授、林庭瑀博士、
劉秋燕、羅崧瑋、林家妤、陳虹彣

資訊連結:
https://www.realscience.top/7

星球永續健康線上直播

https://www.realscience.top/4

Youtube影片連結: https://reurl.cc/gWjyOp

漢聲廣播星球永續健康:
https://audio.voh.com.tw/TW/Playback/ugC_Playback.aspx?PID=323&D=20240615

新聞稿連結: https://reurl.cc/no93dn

本週大綱

- 健康科學新知 (2026 / W15)
- 醫療數位資安生命週期
- 醫療智慧數位資安防禦實例

健康科學新知

2026 / W15

美國-伊朗停火談判破局:「危機循環」

以色列持續空襲德黑蘭軍事設施摧毀軍機
與飛彈發射設施 報復反擊加劇中東戰爭局勢

以色列對黎巴嫩發動持續空襲與轟炸
造成數百平民傷亡 引起國際關注

川普威脅轟炸伊朗電廠要求重啟海峽
中東戰事升溫引發全球油價劇烈波動

教宗李奧十四世主持復活節彌撒
對美伊衝突發出呼籲 期盼領袖們選擇和平

美國副總統范斯代表美方上週於巴基斯坦
與伊朗進行停火談判目前尚未能達成協議

美國-伊朗停火談判破局:「危機循環」

以色列持續空襲德黑蘭軍事設施摧毀軍機
與飛彈發射設施 報復反擊加劇中東戰爭局勢

以色列對黎巴嫩發動持續空襲與轟炸
造成數百平民傷亡 引起國際關注

川普威脅轟炸伊朗電廠要求重啟海峽
中東戰事升溫引發全球油價劇烈波動

教宗李奧十四世主持復活節彌撒
對美伊衝突發出呼籲 期盼領袖們選擇和平

美國-伊朗停火談判未能達成協議
美方宣布封鎖荷姆茲海翔禁止所有船艦出入

中東衝突加深歐美分歧:「內外交迫」

美伊達成兩週停火並重啟海峽 歐洲領袖視為關鍵契機 共同呼籲以外交手段推動持久和平


法國總統馬克宏

美國副統統范斯

川普抨擊北約拒援伊戰 威脅撤軍並重提格陵蘭主權歸屬 令安全同盟面臨瓦解


北約秘書長馬克·呂特

美國國務卿盧比奧

lemonde.fr


rfi.fr

英國首相斯塔默

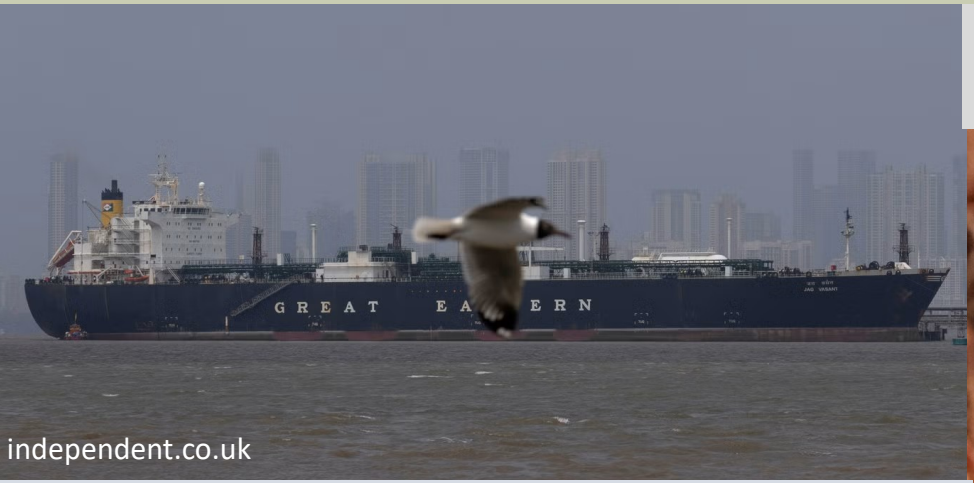
德國總理默茨

北約秘書長呂特赴美嘗試與川普協調 盡力打消美國退出北約意向


Getty Images

北約秘書長呂特

英國及亞洲國家爭取航道安全:「權力重構」



荷莫茲海峽從共享航道轉為戰時協商籌碼
亞洲多國為確保能源運輸已直接與伊朗交涉

英國將召集荷姆茲海峽安全協調會議
推動航道運輸安全與能源供應穩定

日本為確保能源通道積極與伊朗高層
保持對話試圖在危機尋求斡旋空間

日本除關注荷莫茲航道安全也積極與伊朗交
涉建立管道爭取被拘留於伊朗日本人獲釋

AI算力擴建與地緣風險交織:「算力為王」

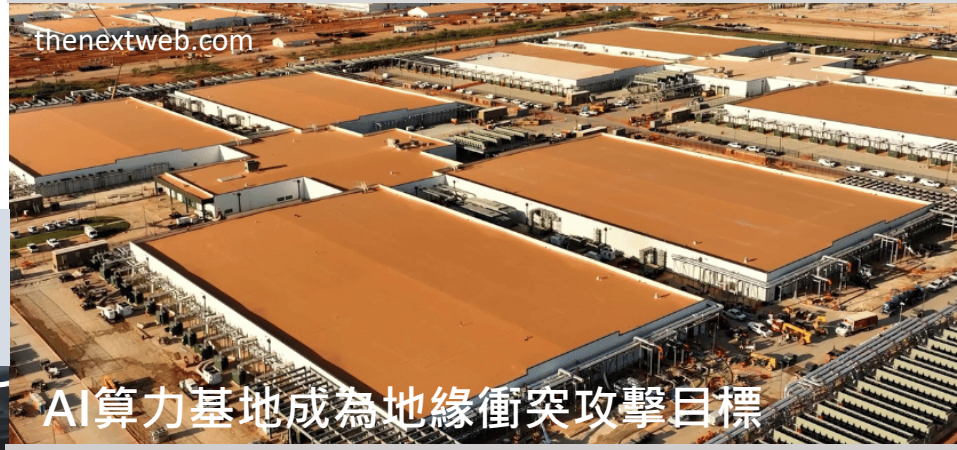
ANTHROP\C

Google | BROADCOM

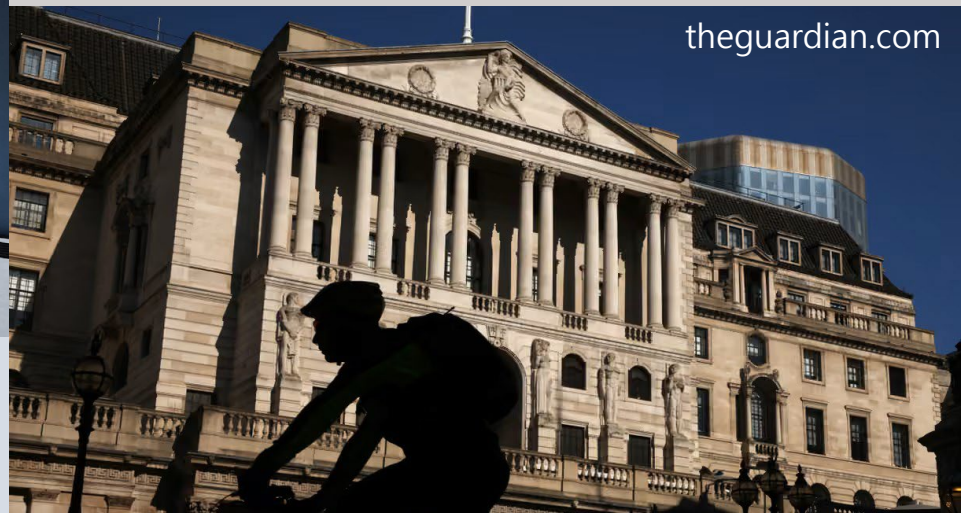
Anthropic攜手Google與博通擴大算力布局，鎖定數吉瓦TPU與雲端資源

高階算力如同石油成為關鍵資源，硬體、雲端與AI產業結盟形成緊密垂直整合

伊朗對OpenAI設置於阿布達比星際之門計畫資料中心基礎設施發出攻擊威脅



英國央行警告若電力與供應鏈壓力持續將影響AI資料中心投資報酬
衝擊數位產業企業估值與金融市場穩定



英國量子與核融合科技投資:「國力競技」

- 英國政府宣布投入共 45 億英鎊發展量子與核融合技術 David Adam, *Nature, 2026*
- 相關資源並將運用於培育英國科學人才確保能源技術獨立性
- 此計畫被視為應對脫歐後獨立於歐洲大型科研項目關鍵

核心戰略規劃

- 量子運算整體規劃：投入 20 億英鎊於硬體、軟體研發與初創企業商業化
- 核融合原型：投入 25 億英鎊打造 STEP 原型電廠與 AI 超級電腦

全球競爭分析

- 技術障礙：大規模量子運算與核融合能源輸出仍未成熟
- 資金缺口：專家認為維持競爭力需更長期的投入，非單次撥款能解決

英國先進能源獨立研發計畫隱憂

- 具備高度不確定性與風險波動性
- 資源過度集中於經濟目標，恐削弱基礎科學研究持續性
- 削減大學科研經費可能導致早期科學人才流失性

AI研究助理重塑科學研究模式:「機智共生」

Nature, 2026

AI研究協作與輔助

- 自動化科研流程：文獻回顧 → 假設生成 → 實驗 → 論文撰寫
- 提升研究效率：加速程式編寫、數據分析與文獻搜尋整理
- AI能產出接近學術期刊水準研究

- 科技公司如 Google、OpenAI 等積極發展自動化研究工具，推動科學研究模式轉變
- 智慧科學研究工具存有幻覺、虛構引用與可信度判斷不足等限制，可能造成大量低品質研究與自動化 P-hacking(只追求統計顯著結果不追求科學真相)，增加審查系統負擔
- 學術界需建立新規範(如揭露AI使用、強化透明性)以因應其影響

健康數位資料治理模式:「數據共治」

現狀痛點

Melissa A. Haendel et al., Science, 2026

- ◆ 數據割裂：健康數據分散於個別醫院、研究機構及相關廠商，缺乏互通性
- ◆ 機制失效：現行共享多屬自發性，缺乏法律約束與經濟誘因
- ◆ 監管過時：現行資料法規如HIPAA難以應對基因、穿戴裝置等新型數據

核心理念

- 基礎設施化：將數據視為公共利益，而非單一機構的私產
- 聯邦式架構：採取去中心化模型，兼顧機構自主與資安及研發統整需求
- 透明化補償：建立定價與公平回報機制，確保參與者獲得合理補償

關鍵治理權衡

- 效益平衡：在「個人隱私」與「公共利益」間尋求動態平衡
- 架構選擇：利用FHIR(Fast Healthcare Interoperability Resources) API等標準落實技術互通
- 多方監督：納入患者、研究者與政府，成立效用委員會監督運作

未來行動建議

- 立法改革：擴大隱私法覆蓋範圍，消除「數據屏蔽」行為
- 經濟補償：提供數據紅利或醫療費用抵減等財務誘因
- 人才發展：培育具備技術與倫理素養的專業治理團隊

醫療數位資安生命週期

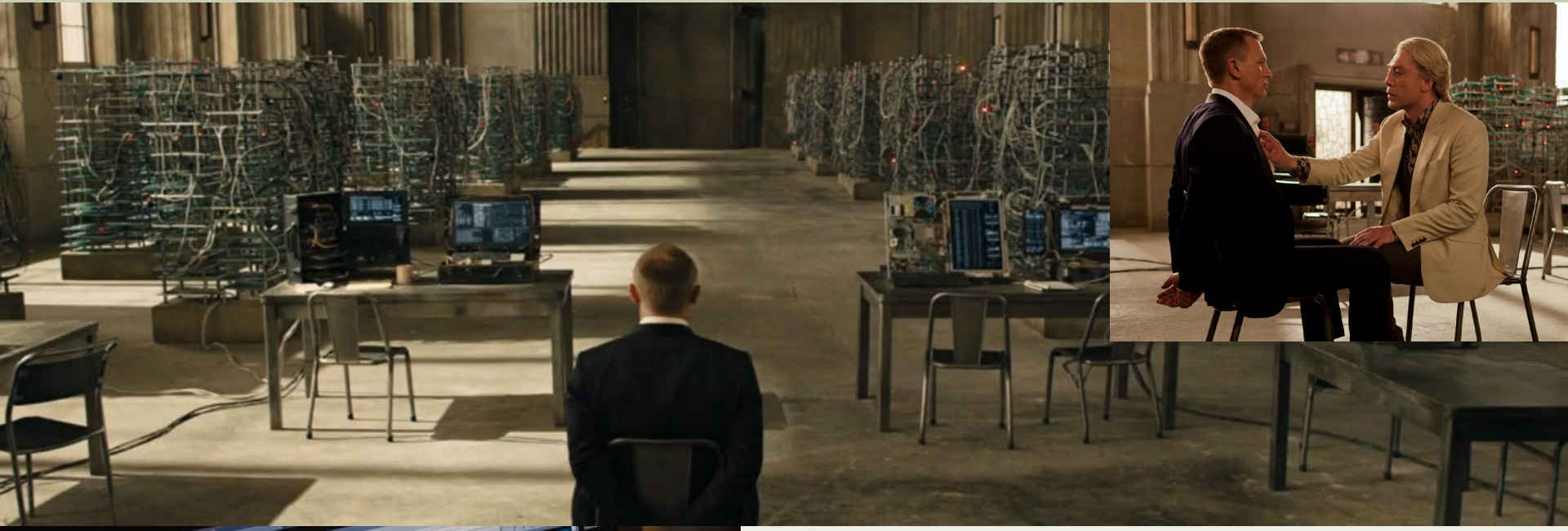
資安情報戰: 空降危機 Skyfall

- 龐德在伊斯坦堡追捕傭兵派翠斯竊走儲存北約所有臥底身分極機密硬碟
- 一旦名單外洩潛伏全球特務將面臨致命風險成為英國情報史空前資安危機
- 此事件為前MI6特工席爾瓦精心策動攻擊起點，逐步摧毀 MI6的情報運作

數位資安威脅連動實體災難

- MI6通報失竊硬碟正遭破解，攻擊者已突破防線入侵 MI6 內部系統
- 席爾瓦駭入M電腦顯示”想想你的罪行”施加心理威嚇
- 此資安入侵事件結合遠端控制大樓瓦斯引爆攻擊造成傷亡

孤島情報攻擊中心



- 席爾瓦每週在YouTube公開五名臥底特務身分，藉此持續打擊 MI6，並導致多名特務遇害
- 龐德追查至設於廢棄孤島操控情報行動技術中樞大型機房
- 席爾瓦稱自己遭 M出賣而策劃復仇

特洛伊木馬入侵情報指揮中心

- 資訊官Q解析席爾瓦筆電發現其中以拓樸密碼藏有倫敦地鐵路線圖程式具自動變形能力難以追蹤
- Q嘗試連接解密網絡取出資料即偵測筆電預藏病毒，觸發異常行動警示使情報中心誤報火警解除所有門禁

AI資安生命週期治理

Kaur et al., 2023

週期	AI for Cybersecurity	Cybersecurity for AI
Identify	找出系統風險	找出AI本身風險
Protect	用AI防禦攻擊	保護AI模型
Detect	偵測威脅	偵測AI被攻擊
Respond	自動回應	AI安全事件處理
Recover	系統復原	AI模型復原

智慧時代數位資安威脅

攻防速度
自動化與高速攻擊對抗

攻擊規模
突破傳統安全邊界
大規模探索

邊際成本
攻擊工具與技術門檻
急遽降低

自動化協作程度
攻防雙方無人化與共演化 (Co-evolution)

AI 時代資安核心風險超越

單純系統被駭

轉變為系統被操控

(Manipulated)、

被誤導 (Misled)、

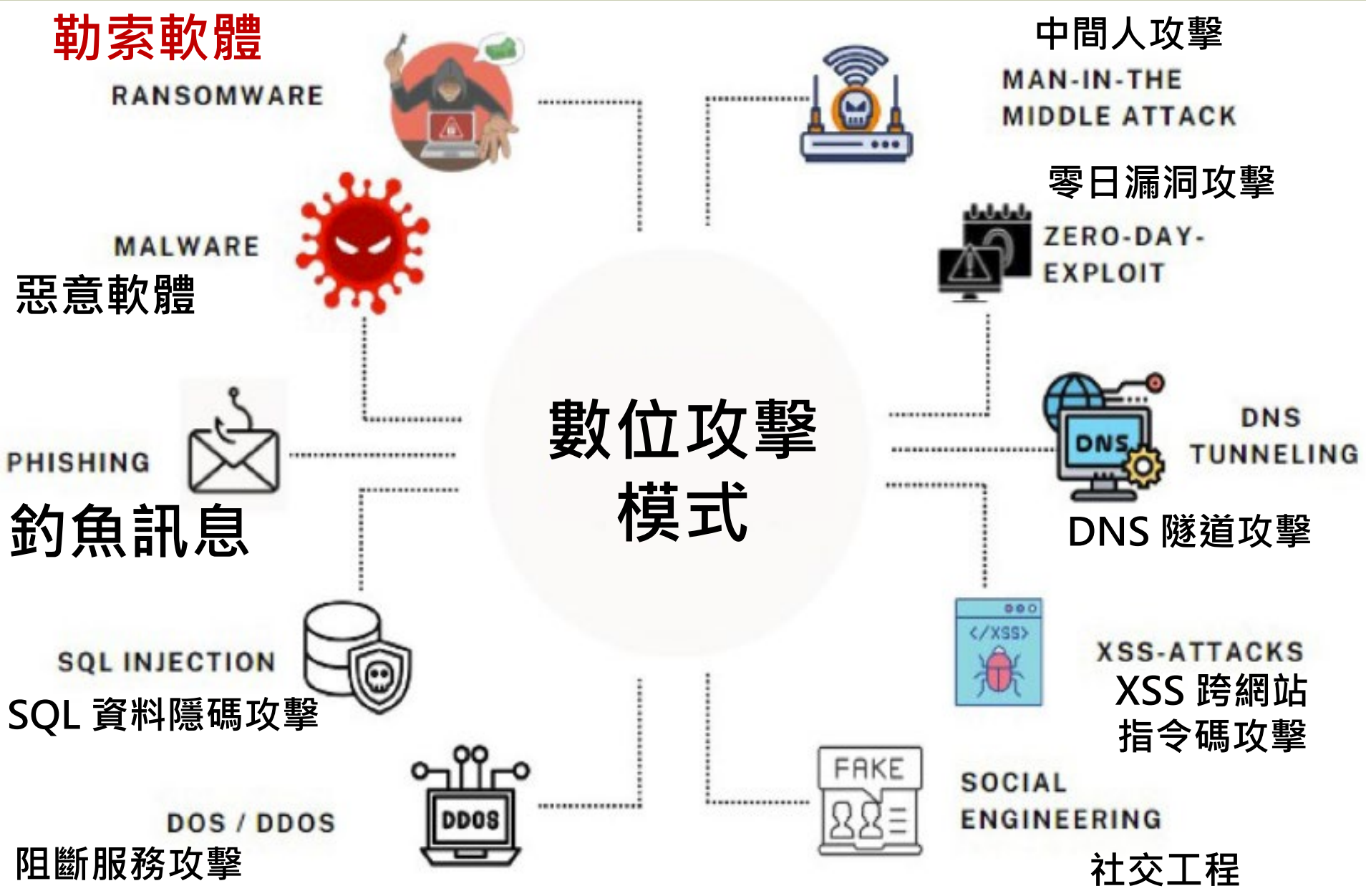
被竊取 (Stolen)、

被濫用 (Abused)，產生

看似可信卻錯誤決策

數位資安常見攻擊型態

Swetha et al., 2025



醫療院所資安治理階段實例

某醫學中心遭遇勒索病毒(Ransomware)攻擊
攻擊目標:
電子病歷（EMR）、健保申報資料 、PACS影像系統

資安治理階段	實務情境	AI 應用技術	案例說明
辨識風險 Identify 找出哪裡可能被攻擊	醫院導入 AI 進行： • 資產盤點 (Asset inventory) - 哪些系統最重要？ - 哪些含敏感資料(病歷、基因資料) • 使用者風險評估 - 哪些帳號權限過高？ - 哪些員工有異常登入行為？	AI 技術應用 • 機器學習(ML) 風險分群 • 關聯網路 (Graph-based risk mapping)	實務案例 發現「放射科某台舊 Windows 機器」未更新 → 高風險節點

醫療院所資安治理階段實例

資安治理階段	實務情境	AI 應用技術	案例說明
防護 Protect 預防攻擊發生	動態權限 (AI-driven access control) 敏感資料標記自動分類 網路釣魚(Email phishing)過濾	AI 技術應用 • NLP 偵測釣魚信件 • BiLSTM 分析敏感資料	實務案例 AI 偵測一封「偽裝成健保署通知」的 phishing mail → 自動攔截
偵測 Detect 即時發現攻擊	某天凌晨，某帳號突然： • 大量下載病歷 • 非正常時間登入 • 從國外 IP 連線	AI 技術應用 • 異常偵測 (Anomaly detection) • 深度學習(DL) + 時序模型	實務案例 AI 判斷：行為偏離正常模式（baseline）→ 判定為可能 APT 攻擊

醫療院所資安治理階段實例

資安治理階段	實務情境	AI 應用技術	案例說明
回應 Respond 攻擊發生時即時處理	當 AI 判定攻擊，系統自動執行： • 封鎖帳號 • 切斷網路連線 • 隔離感染主機 (network segmentation)	AI 技術應用 • 強化回饋學習(RL)最佳決策 • 自動 SOC (Security Operation Center)	實務案例 RL 模型決定：「是否立刻斷網 vs 觀察」→ 平衡醫療不中斷 vs 安全
復原 Recover 讓系統恢復正常	攻擊後： • 還原備份 • 恢復電子病歷系統 • 評估資料是否外洩	AI 技術應用 • 數位孿生模擬復原策略 • 貝氏模式損害評估	實務案例 模擬：若先恢復急診系統 vs 住院系統 → 哪個對病患影響最小？

醫療智慧數位資安

防禦實例

愛爾蘭衛生管理機構勒索軟體攻擊事件

2021年5月，愛爾蘭衛生體系(HSE)遭 Conti 勒索軟體攻擊，全國醫療 IT 系統大規模斷線

病患資料遭非法存取，預約、檢查與行政流程嚴重中斷

此為全球首宗針對國家醫療體系發動資安入侵造成嚴重影響案例

事件核心

事件時間：
2021年3月（潛伏）→ 5月14日（引爆）
攻擊者：Conti（俄語系犯罪組織）
目標：愛爾蘭全國醫療資訊系統

影響規模

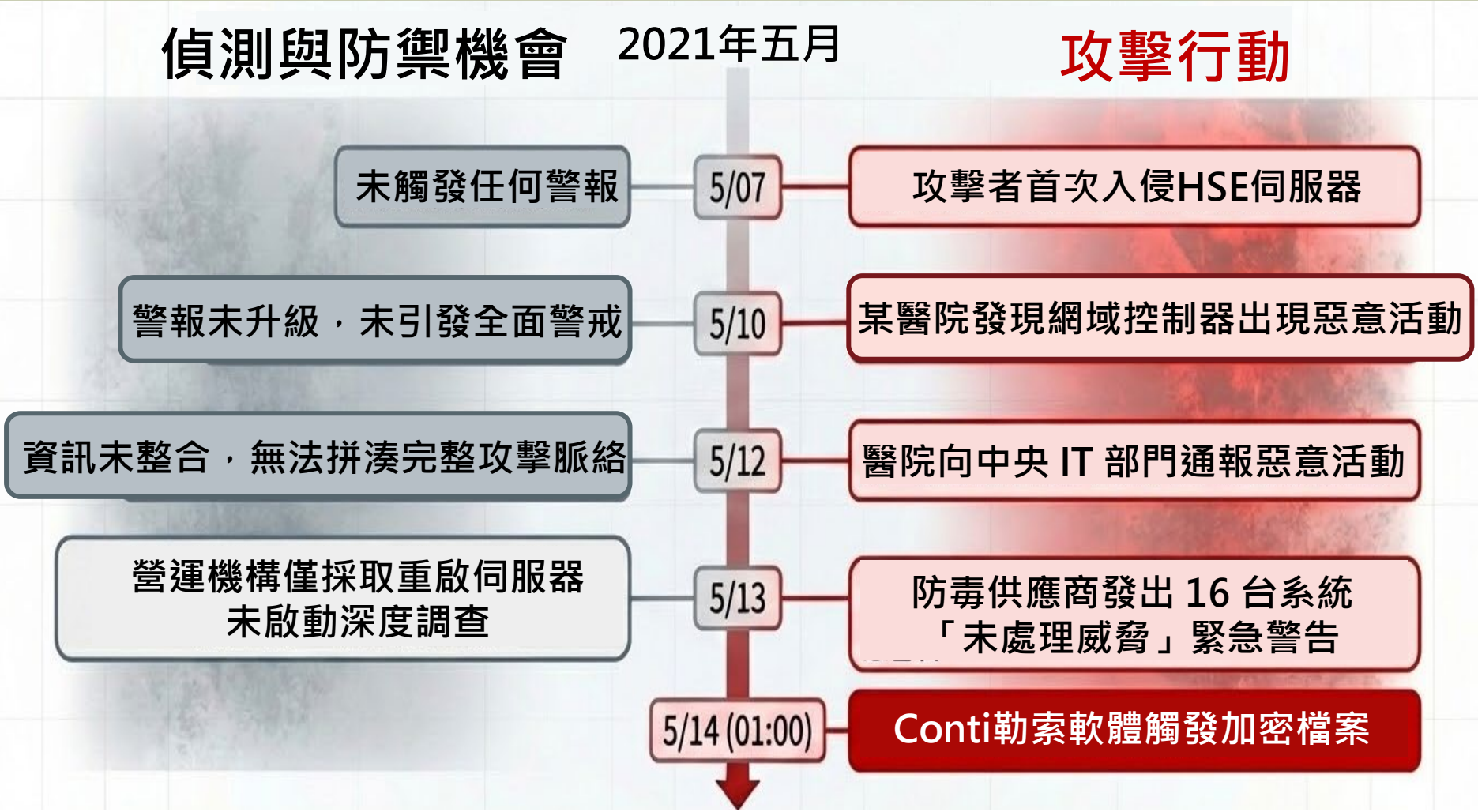
> 80,000 台裝置 受影響
資料外洩：**700GB** 敏感與病患資料
醫療降級：放射科、化療、急診被迫紙本手工作業

財務損失

贖金要求：**2,000 萬美元**(拒絕支付)
直接復原成本：**> 6,000 萬歐元**
間接損失：
全國醫療服務中斷成本難以估算

單一釣魚郵件即可引發全國性醫療危機
攻擊者潛伏長達八周未被偵測

關鍵警訊失聯導致勒索攻擊全面爆發



多起異常警訊未整合觸發調查與防禦部屬，導致攻擊逐步擴散

勒索軟體藉由網路橫向移動感染終端機癱瘓醫療系統

資安攻擊下醫療工作流程變化

常態數位工作流程

開單與傳遞：

電子系統開單，即時傳輸

影像調閱與診斷：

螢幕隨時調閱過往影像比對腫瘤進展，20台報告工作站

報告產出：

系統打字，電子病歷整合

攻擊後
應變工作流程

開單與傳遞：

紙本手寫開單人工親自遞送

影像調閱與診斷：

無法調閱歷史數位影像

全院僅餘非專用螢幕可使用

報告產出：

醫師手寫病歷與報告

數位影像無法存取 歷史檢查無法調閱影響臨床工作
病患需重複接受影像檢查 腫瘤分期與臨床治療被迫延宕

影像檢閱工作站失效 臨床檢查須仰賴傳統調閱實體片
第一線醫療工作以傳統方式取得所需資訊維持基礎運作

Dordogne醫療組織資安事件挑戰

規模

11 間附屬醫院

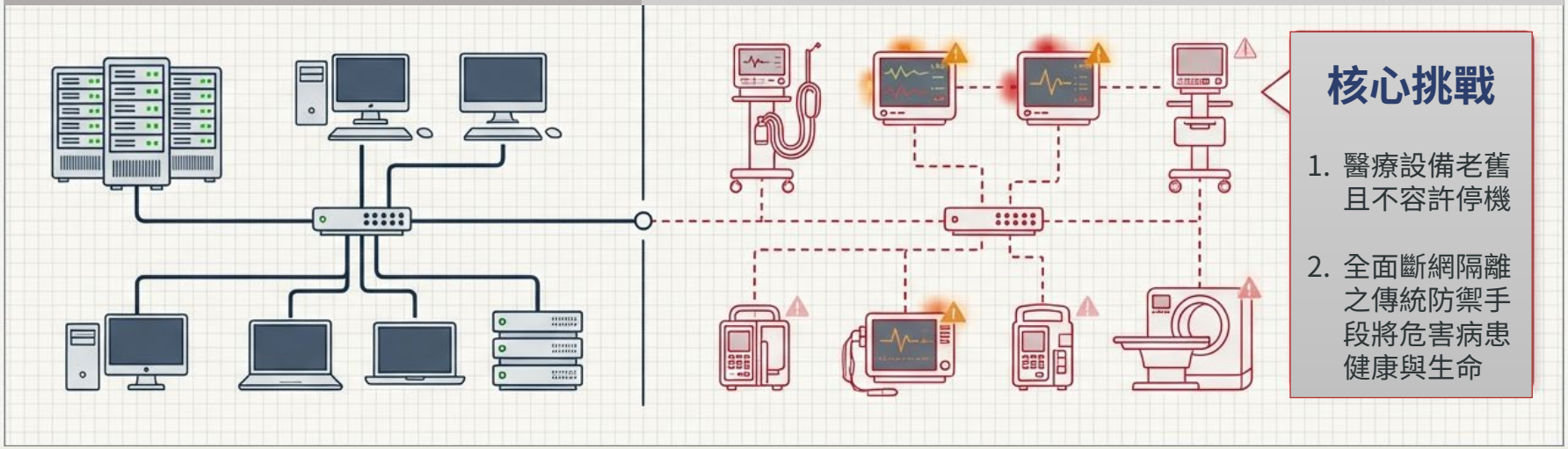
人力

近 5,000 名員工

範圍

企業設備 +
關鍵醫療與急診維生設備

企業資訊技術(Enterprise IT)	Medical OT/ER Devices(醫療營運技術與急診設備)



核心挑戰

1. 醫療設備老舊且不容許停機
2. 全面斷網隔離之傳統防禦手段將危害病患健康與生命

法國Dordogne聯盟：涵蓋 11 間醫院、近 5,000 名員工

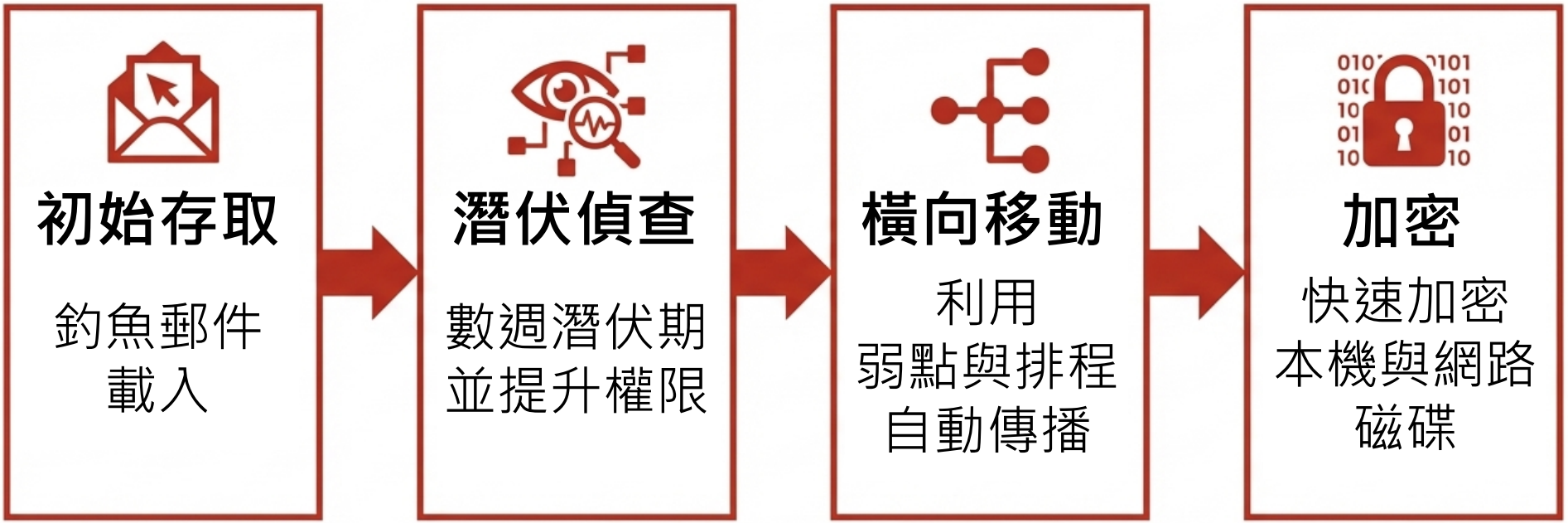
防禦範圍包括企業資訊技術,關鍵醫療營運技術與急診設備

Ryuk勒索軟體攻擊鏈流程與擴散機制

前導攻擊	潛伏偵查	橫向移動	加密
釣魚郵件或 載入器潛伏	長期隱匿傳統 特徵碼難以察覺	利用 RDP/SMB (Port 445)擴散	RSA-4096+AES-256 混合加密與磁碟擴展

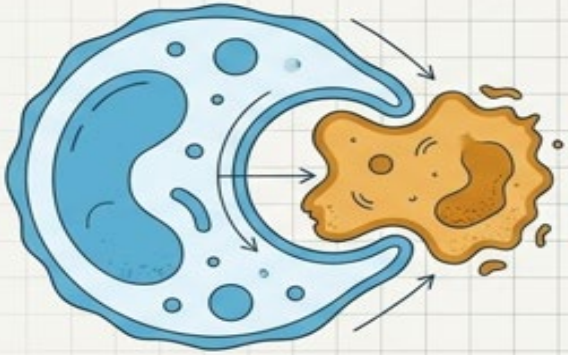
1. 具備高度變異且無固定特徵碼 (Signature-less) 特性
2. 為傳統防毒軟體無法辨識的防禦盲區

歷史事件：2021 年曾癱瘓美國逾 200 間醫院，具高度毀滅性

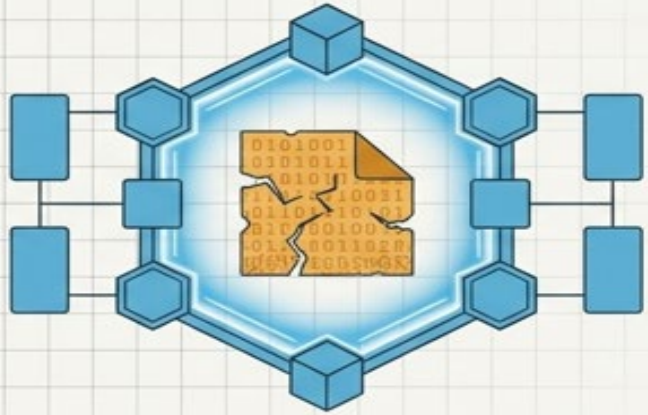


企業免疫系統與多維度行為模型

人體免疫邏輯



數位免疫邏輯



不依賴曾經生病的歷史經驗
透過全面認識自我細胞
精準排斥入侵病原與異常細胞

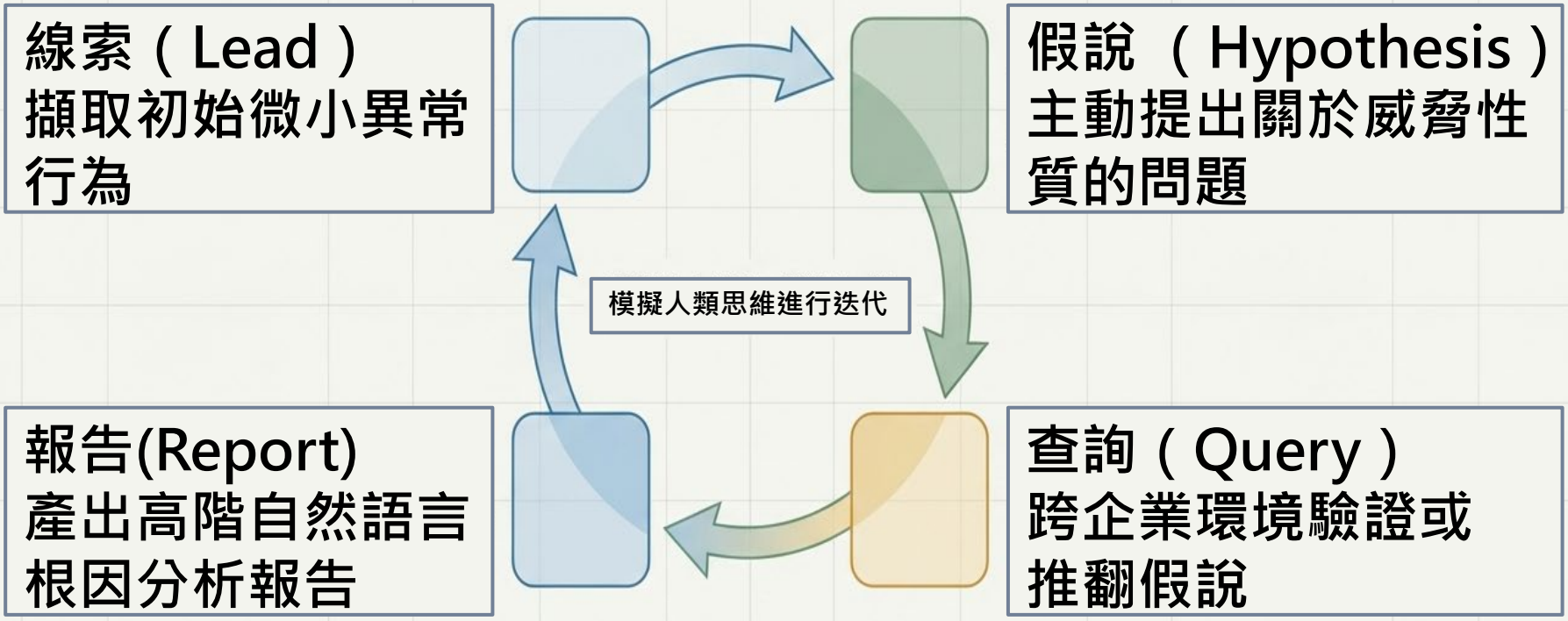
非監督式機器學習
不依賴已知威脅特徵碼，從零學習組織正常狀態攔截未知的攻擊

生活模式 (Pattern of Life) 多維度行為模型

- 透過時序行為、連線模式、資料流量、同儕比較及情境因素進行行為建模
- 防禦會自動調整確保在環境變遷下維持零時差防禦

Darktrace 虛擬資安分析師

自動化調查流程: 模擬人類思維，自動執行尋找微小異物線索、提出假說、跨環境查詢驗證、產出自然語言報告分析完整循環



減少92%調查時間

少於4%事件需人工介入

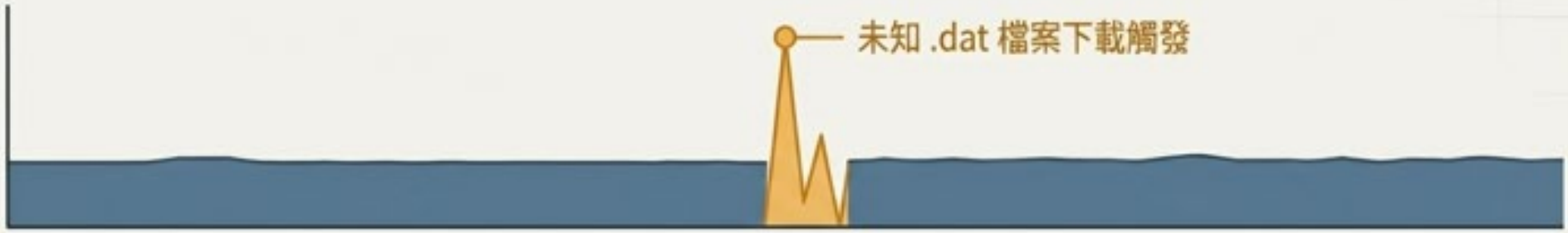
攻擊初始信號偵測

傳統 IDS / 防毒視角

未符合系統已知特徵碼，因而未觸發警報，系統判定為正常活動。

Darktrace AI 視角（行為偏移）

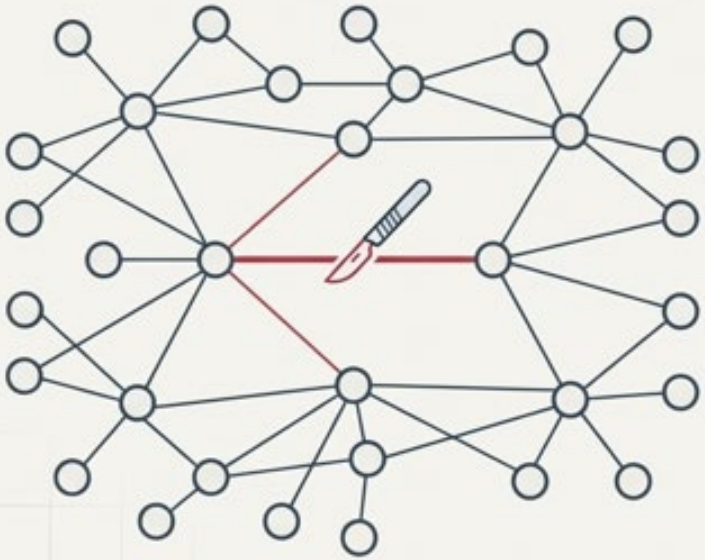
- [!] 100% 連線罕見度 (系統部署以來從未見過此 IP)
- [!] 檔案類型偏差 (.dat 不符合該醫療設備日常行為)
- [!] 同儕與時序偏差 (時間點異常，同部門無此行為)



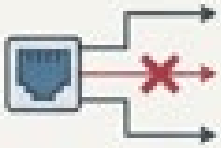
- AI異常偵測不依賴 Ryuk 之已知特徵碼，攻擊之 .dat 檔案
- 傳統之防毒軟體或入侵偵測系統（IDS）中極可能被歸類為正常活動而未觸發警報

Antigena 自主回應技術之運作機制

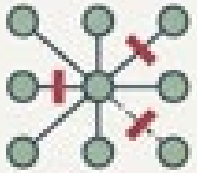
以最小影響原則精準阻斷威脅，
不讓防禦本身變成醫療中斷風險



即時連線阻斷
只切斷可疑連線
不影響其他正常通訊

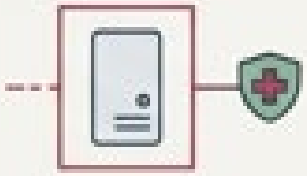


生活模式強制執行
只允許設備維持平常正常的通訊行為



保護醫療設備
必要時全面中斷設備對外與對內連線

持續監控與調整
降低可疑設備傳輸速度，減少資料外洩風險



- Antigena 精準阻斷惡意連線，使醫療設備在維持核心功能下仍能有效防禦攻擊
- 其決策引擎計算在最短時間內有效阻止攻擊擴散之最佳行動方案

星球永續健康
線上直播


林庭瑀
博士


陳秀熙
教授

國立台灣大學


梅少文 主持人


侯信恩主持人


楊心怡製作人


林家妤


許辰陽
醫師


陳虹彣


劉秋燕


羅崧瑋


嚴明芳
教授


陳立昇
教授

台北醫學大學