

2025年企業的 資安策略或佈局

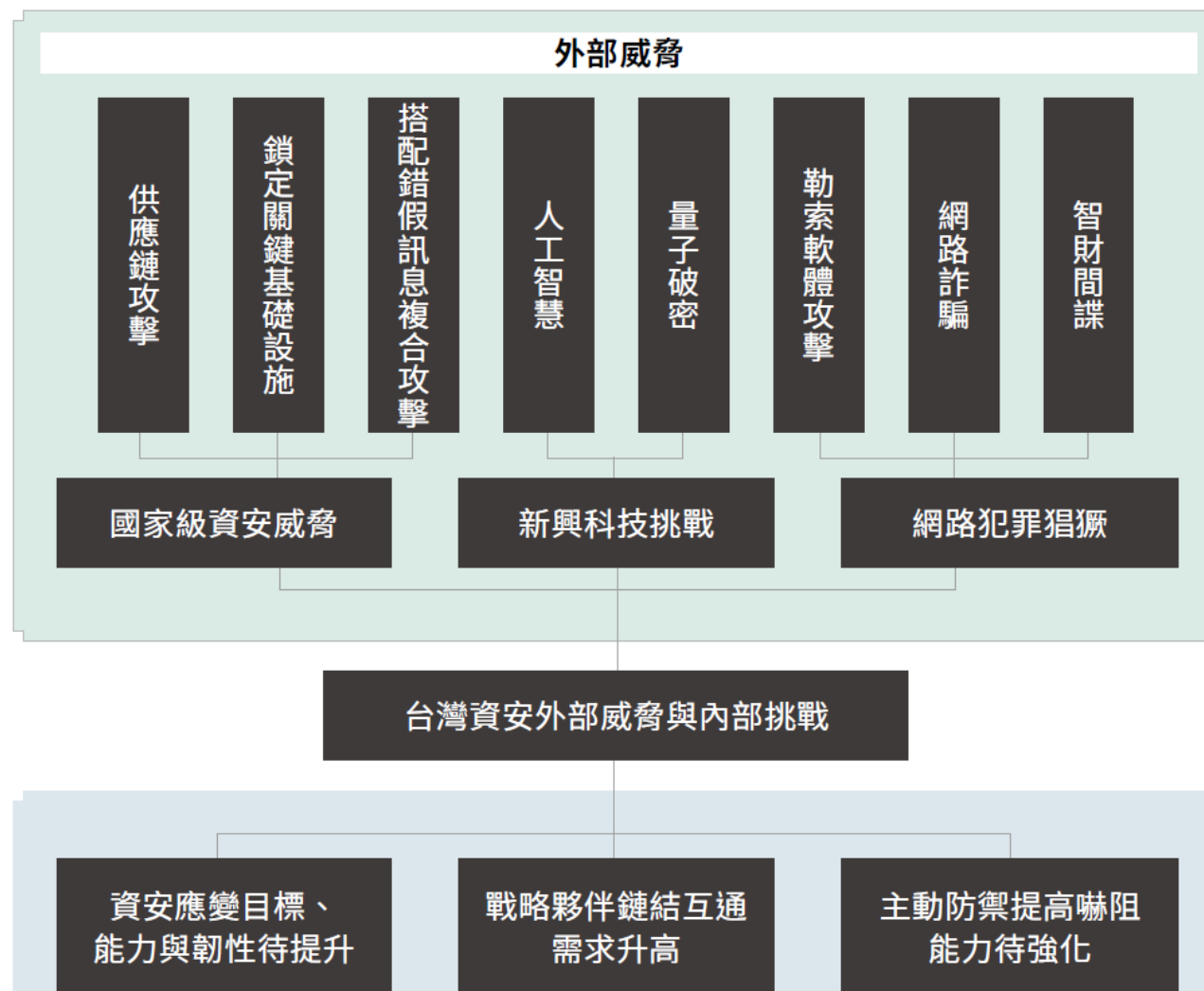
林家瑋 (Ray Lin)
2025/04





- 全球首批 GCR首位 AWS Security Hero
- iFUS System Consultants Ltd. – 資安長(CISO)
- DataBrushing.ai (QSP) – 數位長(CDO)
- 長宏專案(PM-ABC) – PMI授權培訓講師 (PMP/PMI-ACP)
- 全智網科技(AI Network) – ISC2授權講師 / AWS授權講師
- 巨匠電腦 – 資安課程合作講師
- ISC2 Taipei Chapter – 理事 / 媒體公關委員會 主委 | PMI Taiwan獎項辦公室(PTGA) – 執行長
- DevSecOps Taiwan – 社長
- 登豐數位、鑑智實相、捷虹資訊、德慎精算、睿峯管顧 – 顧問 / 講師
- 曾服務於美商、日商、台商、新創、上市櫃、跨國集團等不同型態的公司
- 擔任過CEO、COO、CISO、CDO、產品主管、IT主管、業務主管、資深SI工程師與資深PG
- 曾獲台灣發明家創意獎、PMI-TW優良志工獎與績優執行理監事、翻譯出版7本知名敏捷書籍，並取得超過40張國際證照

2025/4/8公布國家資通安全戰略2025



量子安全

常見密碼破解方式

- **暴力破解(Brute-Force Attack)**: 使用自動化工具試錯法來破解密碼
 - 嚴謹定義: 嘗試每一個數字、字母以及特殊符號的所有可能組合, 保證可以破解成功, 時間早晚問題
 - 寬鬆定義: 使用字典或彩虹表等方式來破解
- **字典攻擊(Dictionary Attack)**: 使用常用密碼攻擊
- **彩虹表攻擊(Rainbow Attack)**: 常用密碼轉Hash存成表, 再使用此表攻擊
- **密碼噴灑攻擊>Password Spraying)**: 在同個系統針對大量帳號嘗試同個常見密碼登錄, 避免帳號鎖定機制
- **憑證填充攻擊(Credential Stuffing)**: 又稱為**撞庫攻擊**, 使用從其他系統洩露的帳號密碼組合, 嘗試在目標系統進行登錄



八字元密碼 37 秒內可破解

- Hive Systems使用12張RTX 4090評估
 - 1秒能暴力破解簡單12字元密碼(MD5)
 - 37秒能暴力破解簡單8字元密碼(bcrypt)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

> Learn how we made this table at hivesystems.io/password

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024					
How did we make this? Learn at hivesystems.com/password					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

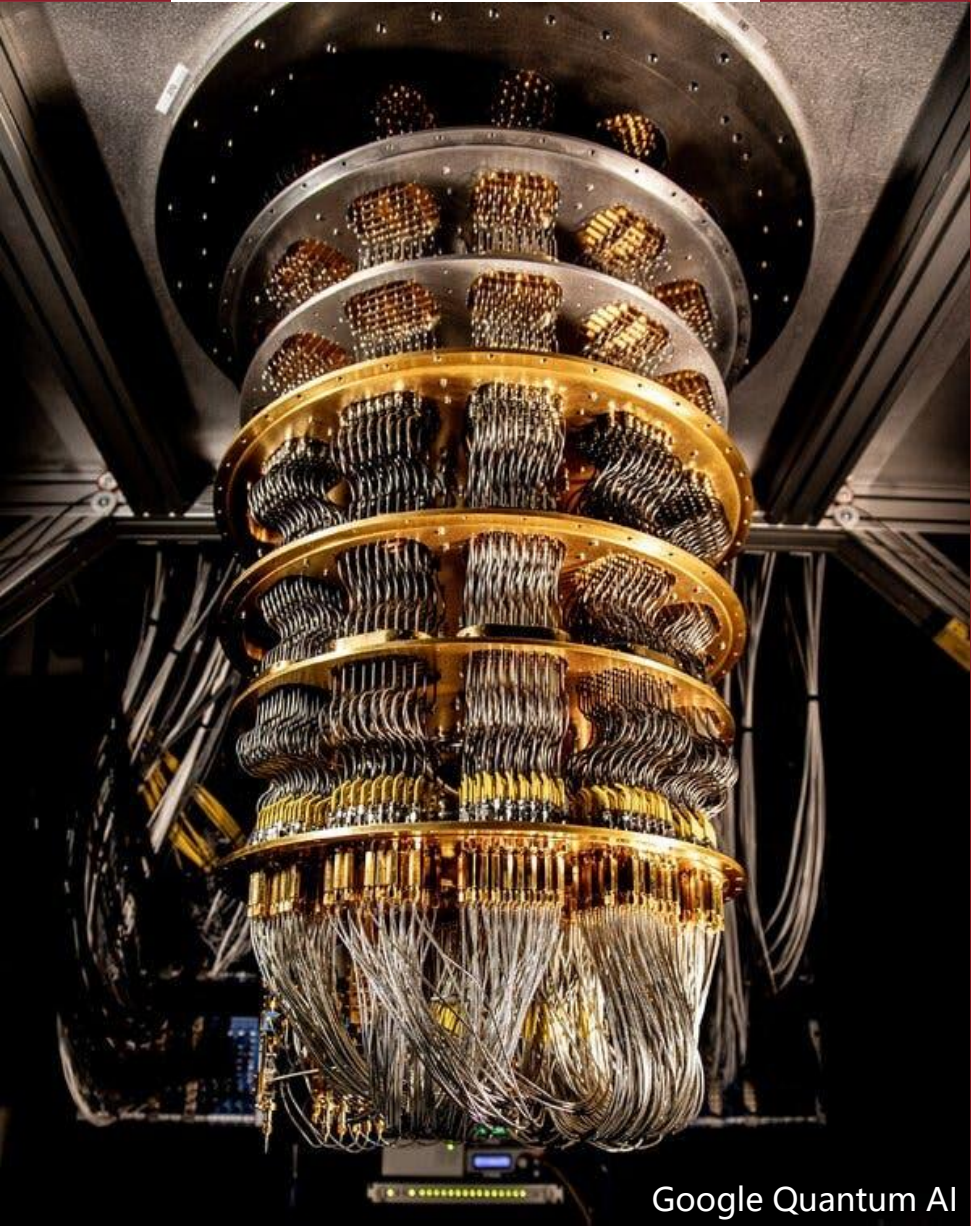
> Hardware: 12 x RTX 4090 | Password hash: bcrypt

量子電腦威脅

- 量子電腦只需要數小時即可破解RSA等非對稱加密， AES-256對稱式加密保護效果折半

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

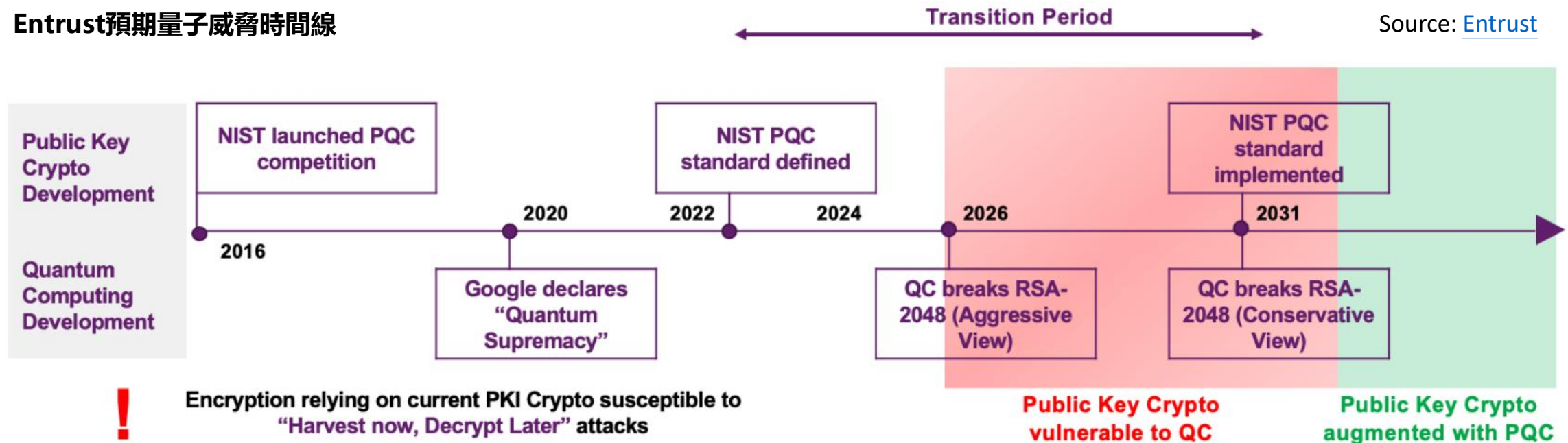
[NIST IR 8105 - Report on Post-Quantum Cryptography, April 2016](#)



Harvest now, decrypt later

- 現在收集，未來解密(Harvest now, decrypt later)：先蒐集無法解密的資料並長期儲存，等未來解密技術突破再解密，這種時間點稱為Y2Q或Q-Day
- 加密敏捷性(Crypto Agility)：在不影響系統運行下快速更換脆弱加密算法

Entrust預期量子威脅時間線



IBM Quantum Safe Roadmap



DataBrushing.AI



IBM Quantum Safe Roadmap

Source: [IBM](#)

🟢 First generation available 🟡 On target ⬜ Planned

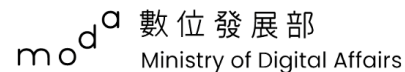
	2022	2023	2024	2025	2026+
Regulatory milestones	NIST selects algorithms for standardization	Federal agencies plan for PQC adoption	NIST publishes PQC standards	CNSA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC
Consortia	🟢 Open Quantum Safe (OQS) 🟢 Post-Quantum Telco Network	🟢 NCCoE 🟢 PQC Coalition (MITRE)	🟡 Payments (EPAA, NACHA) 🟡 PQC Alliance (Linux Foundation)	⬜ Critical Infrastructure Protection Coalition	⬜ Healthcare Coalition
IBM services		🟢 Quantum-safe preparation & advisory	🟢 Quantum-safe transformation services	🟡 Application modernization 🟡 Security Platform modernization	⬜ Quantum-safe talent transformation
IBM Quantum Safe technology		🟢 IBM Quantum Safe Remediator 🟢 Adaptive Proxy 🟢 Performance benchmarking		🟡 TLS, VPN, SSH 🟡 Encryption/key/certificate mgmt. 🟡 Crypto-agility framework	⬜ Automated remediation ⬜ LLM-based recommendation
		🟢 IBM Guardium Quantum Safe 🟢 Dynamic Inventory 🟢 Cryptography Posture Management 🟢 Cryptography Policy Management		🟡 Risk-based prioritization 🟡 Enriched metadata	⬜ AI-driven risk analysis
		🟢 IBM Quantum Safe Explorer 🟢 Static scan 🟢 CBOM generation 🟢 CI/CD integration		🟡 Custom library support 🟡 Remediation recommendation	⬜ LLM-assisted scanning
Algorithms, protocols, standards, libraries	🟢 Key encryption: CRYSTALS - Kyber 🟢 Digital signature: CRYSTALS - Dilithium, FALCON	🟢 Cryptography Bill of Materials (CBOM)	🟡 MAYO, UOV, SQISign 🟡 OpenSSL		
IBM infrastructure		🟢 IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	🟡 IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power : Strategy & Planning	⬜ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power : Phase-1	⬜ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power : Phase-2

Google也在戰場上

- Google Chrome已在TLS中啟用[抗量子破解金鑰交換機制](#)，可防止使用者流量日後遭到量子電腦解密
- 2024/12/9 Google量子AI創始人兼負責人Hartmut Neven公布最新的量子晶片[Willow](#)，Willow在不到5分鐘的時間內完成了超級難題計算，這需要最快的超級電腦10澗年(Septillion, 10的25次方)才能完成



PQC後量子加密演算法



2022/07
NIST
公布首批入選PQC
標準的4款演算法

2023/12
台灣數發部
PQC被列為國家核
心關鍵技術

2025~
FIPS, ISO, IETF, ANSI
量子安全遷移標準



2022/11
美國白宮
發布MOU, 宣布全美
進入量子安全遷移時代



2024/08
NIST
正式公布PQC標準

金鑰建立FIPS203: Kyber (ML-KEM)
數位簽章FIPS204: Dilithium (ML-DSA)
數位簽章FIPS205: SPHINCS (SLH-DSA)

2030~
Year to Quantum

AI安全

程式設計師職缺大衰退



Anthropic研究發現 AI最多被用來解決程式問題



電腦與數學37.2%	藝術與媒體10.3%	教育與圖書館9.3%
職業	職業	職業
程式設計師6.1%	技術寫作人員1.8%	教師1.6%
系統軟體開發人員5.3%	文案寫手1.6%	檔案管理員1.5%
應用程式開發人員3.4%	編輯1.0%	教學設計師0.8%
主要任務	主要任務	主要任務
開發與維護應用程式和網站16.8%	為電影、電視、戲劇和音樂製作內容1.8%	設計與開發全面的教育課程和教材1.9%
編寫程式、為電腦系統與機器除錯6.9%	管理組織的公共關係與戰略溝通1.3%	在各種教育環境中教授和指導不同的科目1.7%
設計與維護用於資料管理和分析的資料庫系統2.3%	制定和執行跨行業的行銷與促銷策略1.2%	管理書籍和文件的出版流程1.4%
辦公室與行政7.9%	生命、物理與社會科學6.4%	商業與金融5.9%
職業	職業	職業
生物資訊技術員2.9%	臨床心理師0.5%	安全管理專家0.5%
統計助理0.4%	歷史學家0.4%	信貸顧問0.4%
文書處理員0.4%	人類學家0.4%	財務分析師0.4%
主要任務	主要任務	主要任務
執行例行的IT系統管理與維護1.8%	進行學術研究並傳播研究成果1.2%	分析財務資料並制定投資與預算策略0.8%
編寫程式、為電腦系統與機器除錯0.7%	記錄、分析並報告營運與研究數據0.5%	提供個人理財建議與教育0.8%
設計與維護用於資料管理和分析的資料庫系統0.6%	對各種物質進行化學分析與實驗0.3%	記錄、分析並報告營運與研究數據0.4%

應用案例-建立服飾電商網站

- ChatGPT指令

- 我想要做一個服飾電商網站，請幫我製作To Do List
- 我想要自己建設一個電商平台，請幫我產出規格書
- 針對第2點和第3點，請提供我更多細節讓我可以繪製wireframe
- 針對用戶註冊和登錄功能，提供我頁面規格

- 其他服務應用

- 將規格提供到其他應用軟體中產出
- [Figma成果](#)

- [ChatGPT參考](#)



ChatGPT-ECommers.png

< 用戶註冊

姓名

電子郵件

請輸入電子郵件

密碼

請輸入密碼

確認密碼

請確認密碼

註冊

已有帳號連結

已經有帳號？登錄 >

社交媒體登錄選項

選擇社交媒體帳號

Google

Facebook

如果輸入信息有誤或密碼不匹配，請確認輸入信息是否正確。

AI...馬A撿土豆(便便)...?



Source: ITmedia

AI...馬A撿土豆(便便)...?

便の形状 Bristol stool form scale



Lacy B, et al. Gastroenterol. 2016; 150: 1393-1407

日本消化器病学会. 機能性消化管疾患診療ガイドライン2014-過敏性腸症候群(IBS), 南江堂, 東京, 2014

便の大きさ



高齢者施設様の 排便記録の一例

介護スタッフ様が 排便状況を 記録用紙に手書きで記録



高齢者施設では、便秘傾向による腸閉塞、下痢傾向による脱水症状を懸念しており、入居者のQOL向上のためにも、日々の排便状況を記録・管理しています。

Source: ITmedia

Google相片辨識誤將黑人標成大猩猩



AI需要大量圖片訓練辨識精準度

- 案例：臉部辨識廣泛應用在安全監控系統、手機解鎖、支付驗證與社交媒體
- 資安威脅：臉部辨識系統可能遭受偽裝攻擊或欺騙，如使用照片、影片或3D模型來模仿合法使用者。臉部辨識資料庫如果被駭客入侵，可能會導致大規模的個人隱私洩露。此外，臉部資料的蒐集和處理也會有隱私和資料保護的問題 ([人民幣 3 元就可以買到 80000 張人臉照片](#))

AI大師意外爆大陸人臉交易內幕

- 李開復在HICOOL全球創業者峰高會演講說道：「曠視科技是我們8年前投資的企業...我們早期幫助他們找尋合作夥伴，包括美圖、螞蟻金服，讓他們拿到大量臉部資料，幫助他們分析怎麼切入各產業。」

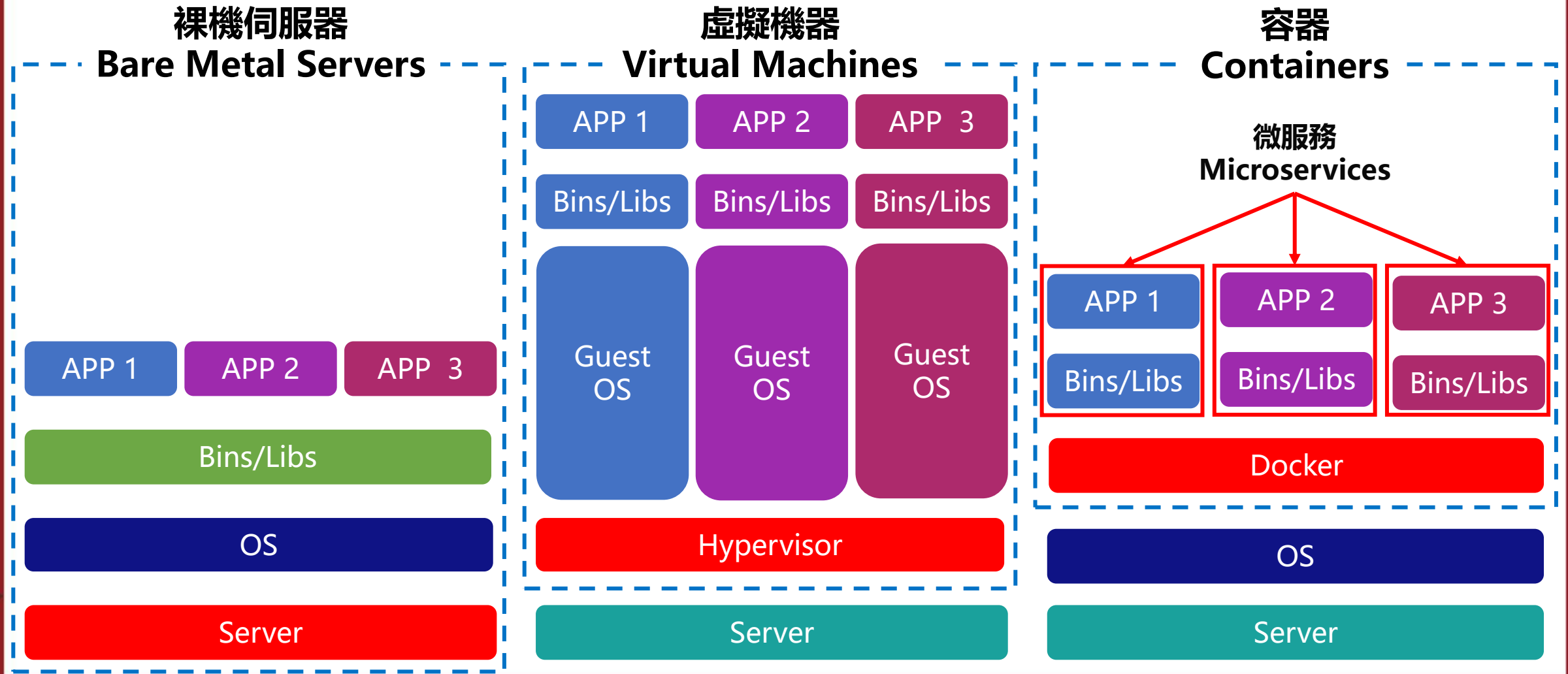
影子AI風險

- 「影子AI」是指**公司員工在管理階層毫不知情的情況下，將AI工具整合到工作流程中。**
 - 根據Forrester Research預測，2024年約有**60%**員工在工作中使用自己的AI工具
 - Salesforce針對全球14個國家、14,000名員工的調查顯示，有**28%**員工在工作中使用生成式AI，超過**50%**沒有經過批准
- 資料安全服務商Cyberhaven統計旗下企業用戶共**160萬**名員工的使用行為
 - **8.2%**員工在職場使ChatGPT
 - **3.1%**將機敏資料上傳ChatGPT
 - 外洩資料類型以**機密文件最多，其次是顧客資料**

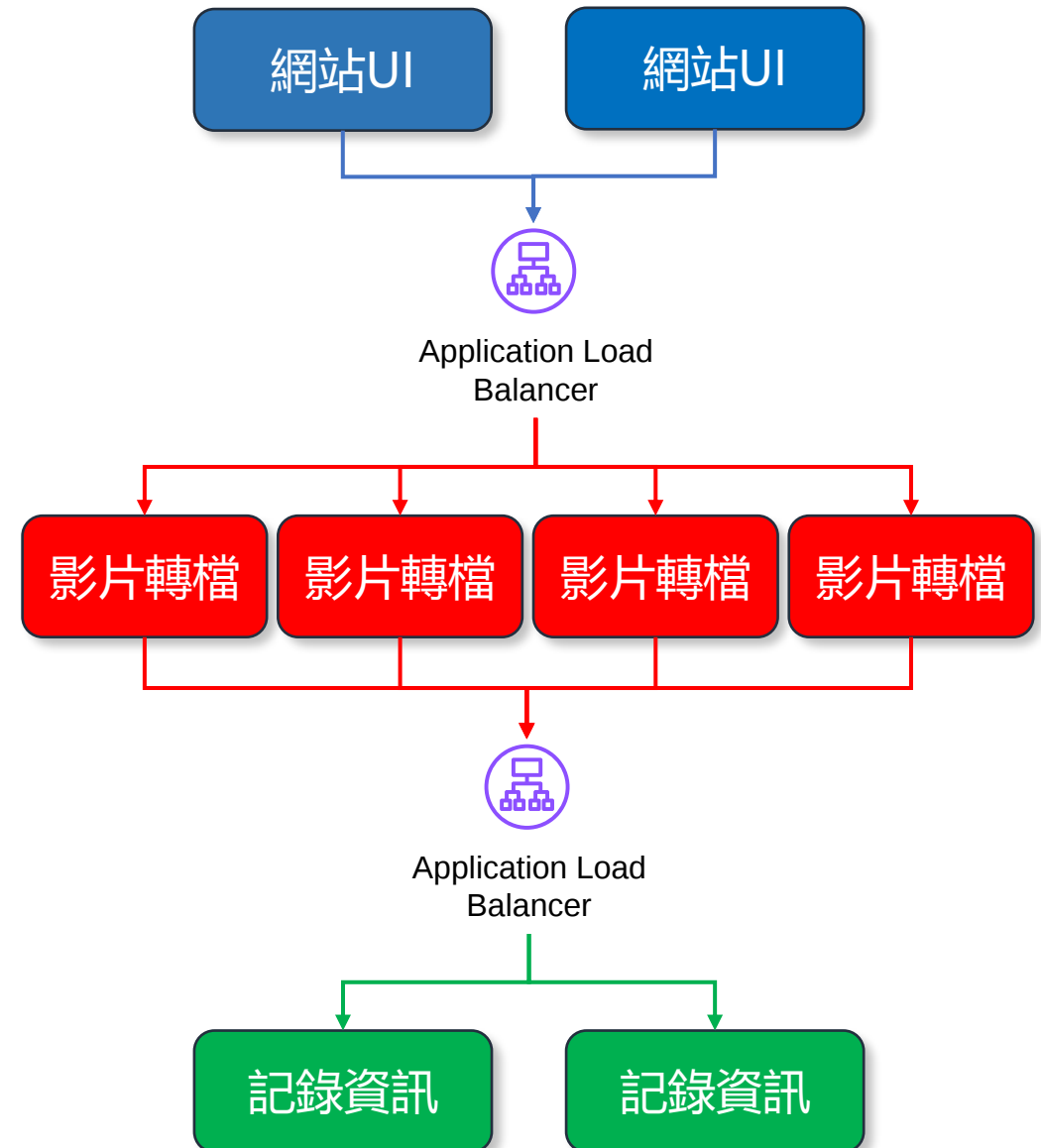
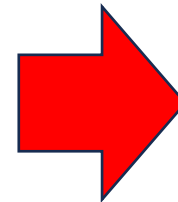
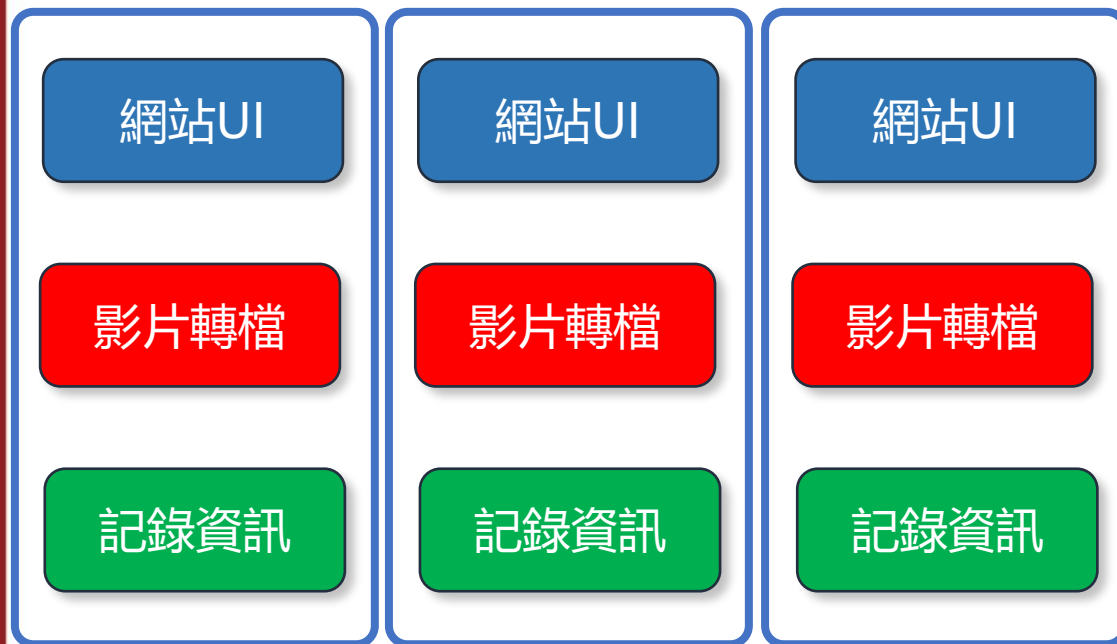


雲端安全

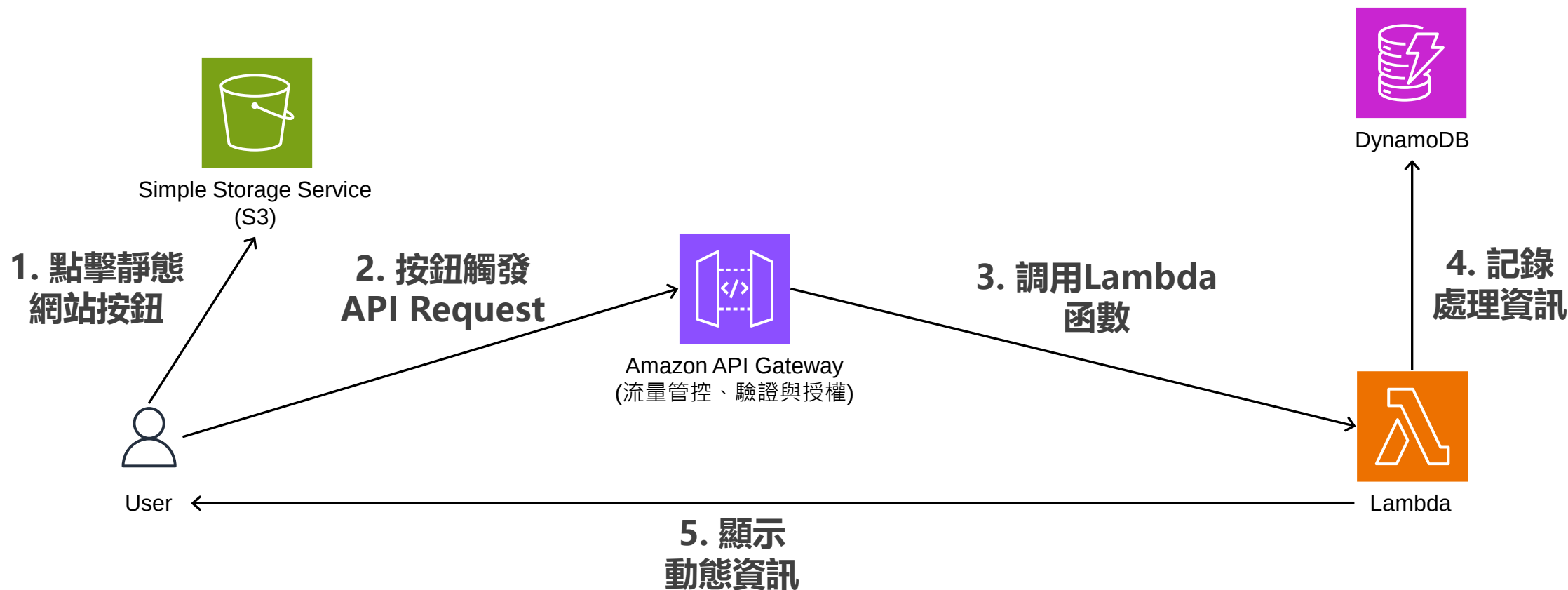
虛擬機器(VM) vs. 容器(Container)



解耦(Decoupling)



AWS無伺服器(Serverless)案例



使用雲端服務的考量

上雲的主要理由	
成本效益	異地備援
敏捷彈性	安全合規
更新部署	碳排能耗
溝通協作	風險管理
競爭力 \$\$\$	

雲端安全事件劇增154%

- AI驅動與雲端交付網路安全平台領導廠商Check Point公布《2024年雲端安全報告》指出：
 - 雲端安全事件數量較去年遽增154%，有61%組織通報重大攻擊事件
 - 高達96%受訪者擔心無法有效管理雲端風險
 - 91%組織優先以AI增強安全態勢，將焦點轉由AI進行主動威脅防禦
 - 雖然威脅態勢日益嚴峻，卻僅有25%組織全面部署雲端原生應用程式保護平台(CNAPP)
 - 54%受訪者在跨多雲環境中保持一致監管標準面臨挑戰。49%受訪者表示很難將雲端服務整合到傳統系統，且有限的IT資源往往讓問題更複雜

雲端潛在的威脅與影響

- 根據雲端安全聯盟(CSA)2024/8/5的報告指出, Top 11雲端威脅如下

Rank	2022	2024	Change
1	身分與存取管理(IAM)	錯誤配置與不充分的變更控制	+2
2	不安全的介面與API	身分與存取管理(IAM)	-1
3	錯誤配置與不充分的變更控制	不安全的介面與API	-1
4	雲端安全策略的選擇/實施不充分	雲端安全策略的選擇/實施不充分	=
5	不安全的軟體開發	不安全的第三方資源	+1
6	不安全的第三方資源	不安全的軟體開發	-1
7	系統漏洞	雲端運算資料意外洩露	+1
8	雲端運算資料意外洩露	系統漏洞	-1
9	無伺服器與容器工作負載的錯誤配置與利用	雲端可見性/可觀察性有限	▲
10	進階持續威脅(APT)	未經驗證的資源共享	▲
11	雲端儲存資料竊取	進階持續威脅(APT)	-1

Source: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024>

勒索軟體安全

勒索軟體的發展和演變



2000年初期 簡單加密與鎖住螢幕

鎖定受害者的電腦螢幕或加密文件，
要求支付一小筆贖金來解鎖

2015年~ 蠕蟲功能的整合

整合蠕蟲功能，使其能自
動在網路中傳播

近年來 勒索軟體即服務(RaaS) (Ransomware as a Service)

勒索軟體開發者提供服務，允許其他犯罪分子
使用這些工具進行攻擊，並分享贖金收益



2010年初期 加密勒索軟體的興起

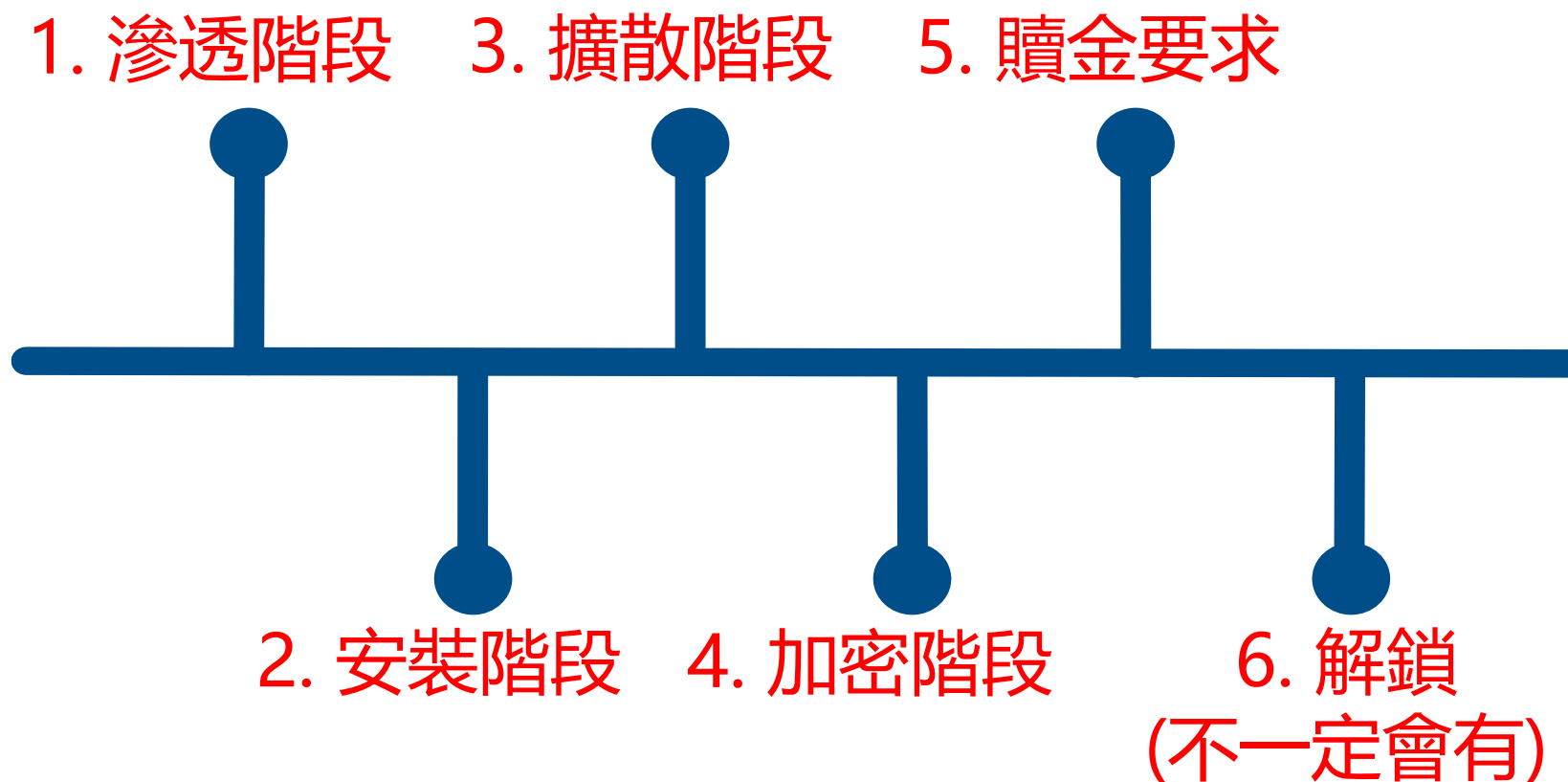
開始使用更複雜的加密算法來鎖
定文件，並提高贖金金額

2019年~ 雙重敲詐 (Double Extortion)

不僅加密受害者的資料，還威脅公開或
銷售這些資料，除非支付更高的贖金

勒索軟體攻擊步驟

- 勒索軟體攻擊通常包括以下幾個主要步驟：



為何許多受害者選擇支付贖金

- 資料復原的迫切性
- 缺乏備份或備份失效
- 財務考量
- 法律和規範壓力
- 心理壓力和威脅



為何許多受害者選擇支付贖金

- 然而，**支付贖金並不能保證資料會被成功解密**，也可能鼓勵犯罪分子繼續從事勒索活動。因此，專家通常不建議依照指示支付贖金，支付後會被鎖定為可再度勒索的肥羊，**平均也只有65%的文件可被救回**



台灣敏捷部落(TAT) - DevSecOps Taiwan



林家瑋|大Ray@DevSecOps社長

DevSecOps Taiwan (2000+)



https://bit.ly/AG3_DevSecOps



- 每個月免費線上分享
 - 每月固定一場 👉 1~2小時分享
 - 不定期快閃 👉 0.5~1小時分享
- 每季一次系列講座(3月/6月/9月/12月)
 - 從零開始的跨雲生活系列
- 社群分享主題與交流方向
 1. Agile / Waterfall / Hybrid
 2. DevSecOps (DevOps + Security)
 3. AI + Security
 4. Cybersecurity
 5. Cloud (AWS / Azure / GCP / SaaS)



歡迎加我好友



Email: ray.lin@ifus.tw