CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

CLOUD SECURITY Forum

CLOUD SECURITY FORUM

以雲端方式建構大型醫院防護

Building Large Hospital Protection in a Cloud-Based Way

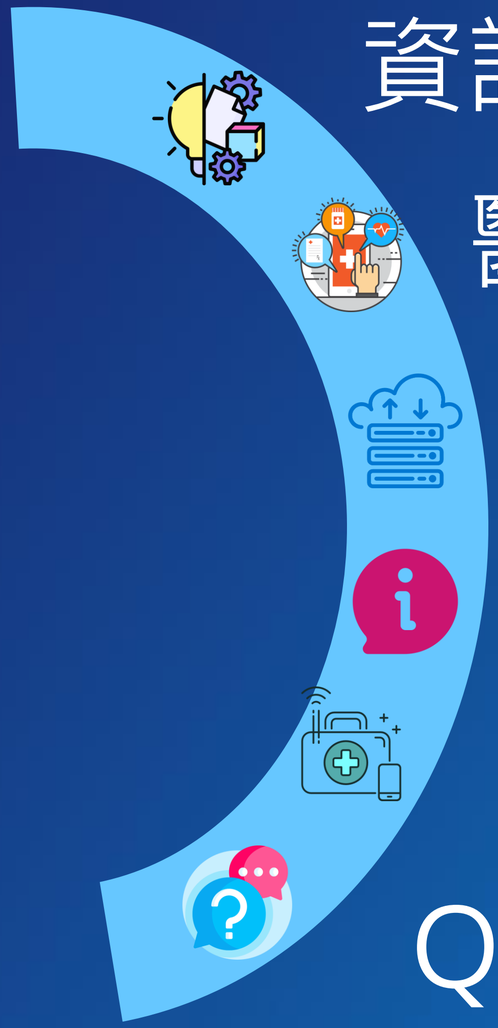
TEAM CYBERSECURITY

郭振宗 Chen-Tsung Kuo

臺北榮民醫院/資訊室

主任

大綱



資訊安全的基本想法

醫院面臨資安的挑戰

雲端平台協防機制

資安防護機制有效性評估

回歸資訊安全核心原則

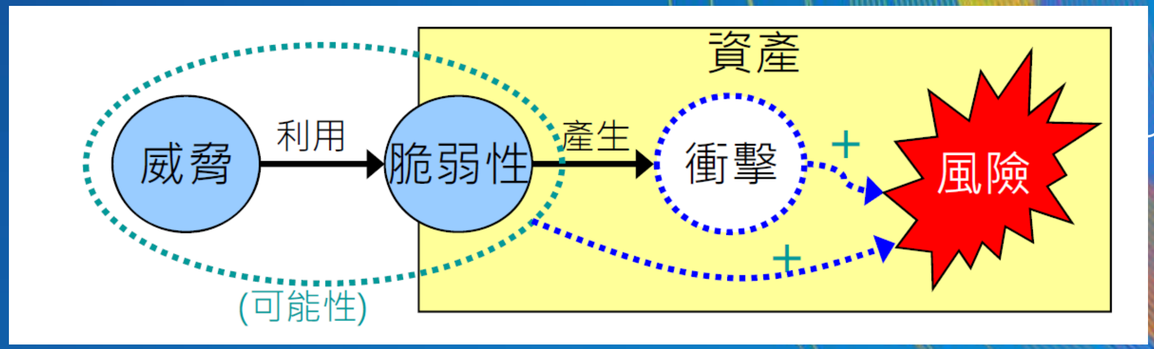
Q&A

CYBERSEC 2025
臺灣資安大會

資訊安全的基本想法

資訊安全是持續性的風險管理
Information security is ongoing risk management

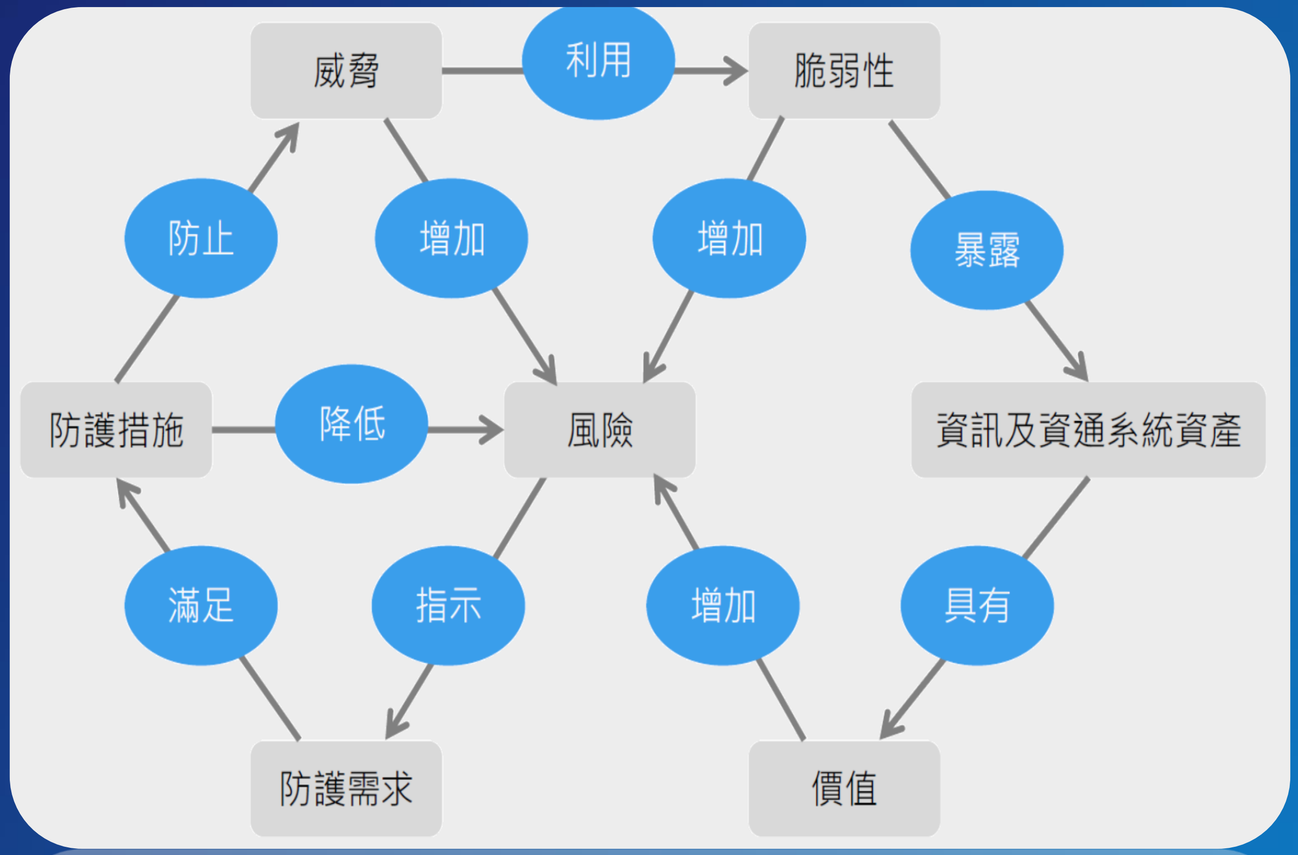
風險的評估模型
風險＝威脅×脆弱性×衝擊



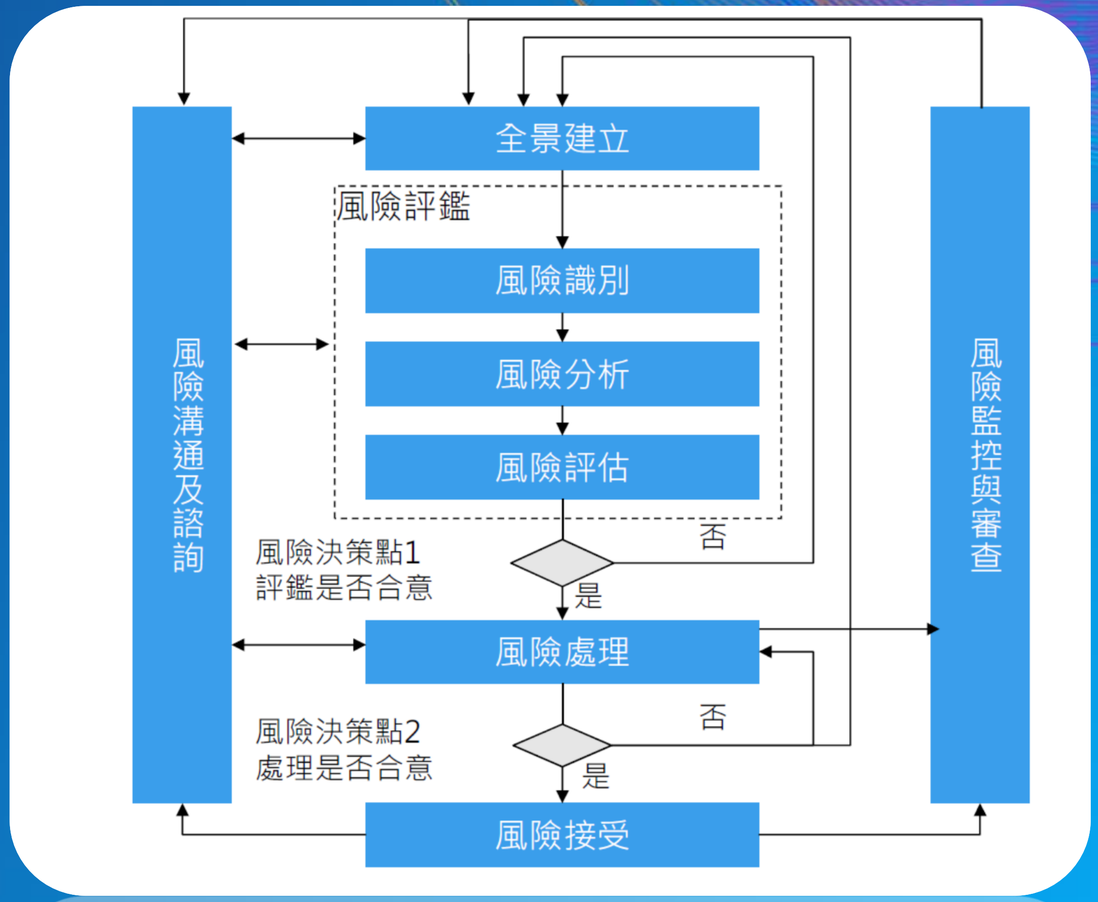
- 威脅(Threat)：任何可能對資產造成損害的事件或行為
  - ✓ 天災(如地震、火災)、駭客入侵、病毒、人員誤操作
- 脆弱性(Vulnerability)：指系統、流程或人員中的弱點，讓威脅有機可乘
  - ✓ 系統漏洞未修補、弱密碼
- 衝擊(Impact)：當威脅成功利用脆弱性後，對組織造成的實際損害或影響
  - ✓ 業務中斷導致損失營收、資料外洩導致客戶信任崩潰、違反法規

風險不是單看威脅有多強，而是威脅是否能利用我們的弱點，造成嚴重後果。

風險管理關係圖



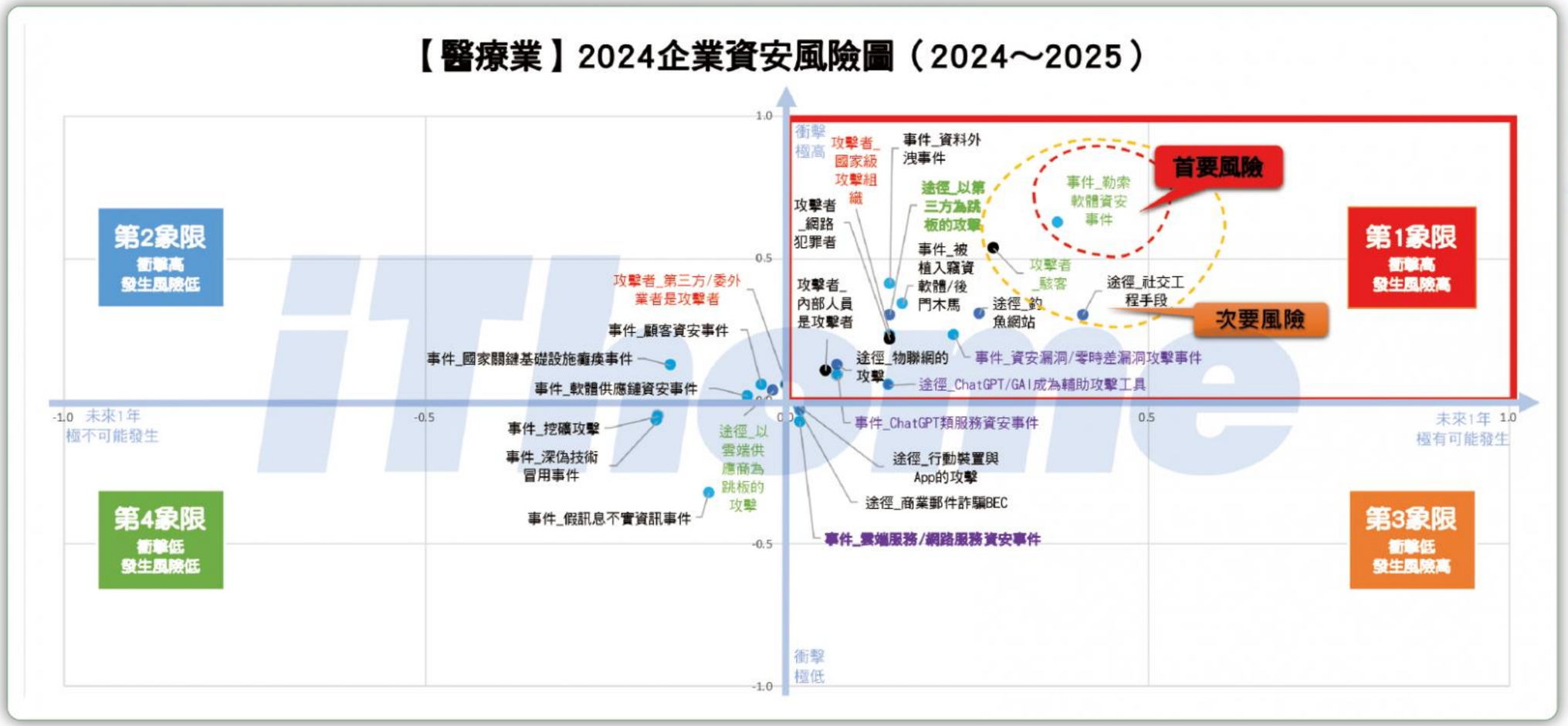
風險管理流程



CYBERSEC 2025
臺灣資安大會

醫院面臨資安的挑戰

醫療業的資安風險圖



https://ithome.com.tw/article/162262

醫院常見的資訊安全威脅類型

- 網路釣魚與社交工程：透過偽造電子郵件 欺騙醫護人員提供登入憑證，進而入侵系統。
- 勒索軟體：駭客加密醫院資料並要求贖金。
- 內部威脅：員工或承包商濫用存取權限，竊取或洩漏病患資料。
- DDoS (Distributed Denial of Service) Service)：透過 大量惡意流量癱瘓醫院網路，導致關鍵系統無法運作。
- 醫療設備駭侵：攻擊者入侵連網醫療設備（如 胰島素幫浦、心律調節器），影響病人安全。

勒索軟體仍是醫院最嚴重的資安威脅

- 財務影響 2024 年對 Change Healthcare 的網路攻擊，導致可能導致 1 億人的資料外洩，造成的財務影響高達 25 億美元，其中包括 17 億美元的直接應對成本和 7.05 億美元的業務中斷損失。[1]
- 營運中斷 94% 的醫院受到 Change Healthcare 網攻影響， 近 60% 的醫院每天營收損失超過 100 萬美元 。
- 病人安全風險 2020 年德國杜塞道夫大學醫院遭勒索軟體攻擊，導致醫療延誤，最終造成 一名患者死亡 。[2]
- 長時間系統停擺成本 ：醫院2018年初至2022年10月期間因勒索軟體攻擊導致的停時間從幾小時到七個月，經濟損失就已超過920億美元，影響時間長達 19.5天(2021)和16天(2022) 。[3]
- 「雙重勒索」越來越常見

1.https://www.cybersecuritydive.com/news/cyberattacks-business-growth-threat/736893/

2.https://www.ithome.com.tw/news/140055

3. https://www.comparitech.com/blog/vpn-privacy/worldwide-healthcare-ransomware-attacks/

國內近期勒索軟體攻擊事件

新聞

馬偕醫院傳出遭CrazyHunter勒索軟體持續攻擊，衛福部與資已成立快速應變小組協助因應

今日（11日）傳出國內馬偕醫院遭受勒索軟體Crazy Hunter勒索軟體的事件，衛生福利部資訊處處長李建璋表示確有此事，這次攻擊已經連續兩日，甚至揚言今日傍晚將持續對醫院發動攻擊。在因應上，衛福部已與資安署合作成立快速反應小組，進駐馬偕醫院協助因應對。馬偕醫院亦表示，這次事件只有影響北淡兩區急診室

文/ 羅正漢 | 2025-02-11 發表

讚 226 分享

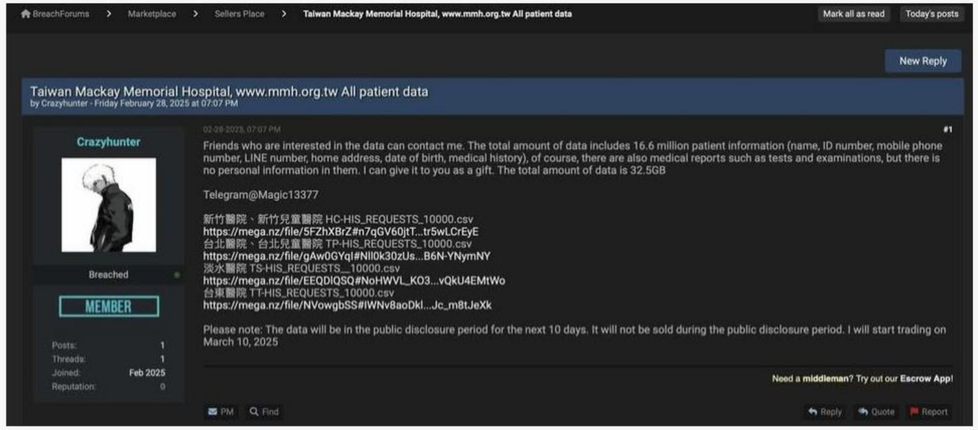
新聞

勒索軟體駭客Crazy Hunter兜售大量馬偕醫院病人資訊

勒索軟體駭客Crazy Hunter在二二八連假攻擊彰化基督教醫院之前，聲稱竊得馬偕醫院所有病人的個資，並開價10萬美元尋求買家，對此，曾經在馬偕看病的民眾應提高警覺，防範歹徒後續利用這些資料從事詐騙

文/ 周峻佑 | 2025-03-05 發表

讚 289 分享



新聞

2025年3月彰化基督教醫院遭勒索軟體攻擊事件歷程總整理（持續更新中）

在2025年3月初的二二八連假期間，彰化基督教醫院也遭遇CrazyHunter這支勒索軟體的攻擊，由於這是繼上個月馬偕紀念醫院遭攻擊後的又一起事件，衛福部資訊處已定調為「系統性攻擊」事件，也發布「醫院面對勒索軟體攻擊的應變指南」，並有業者公布可偵測這次威脅的入侵指標（IOC）。我們在此總結了相關資訊

文/ 羅正漢 | 2025-03-06 發表

讚 60 分享

目前有觀察到2種脈絡，一是教會醫院，二是今年資安演習的另外3家藍隊醫院，不過目前會持續和所有醫院進行演練。他提醒，假日及深夜等資安防護較為鬆散的時段，往往是攻擊者發動行動的高風險期，目前攻擊態勢未完全平息。

https://www.ithome.com.tw/news/167318
https://www.ithome.com.tw/news/167687
https://www.ithome.com.tw/news/167671

捉到了?

CLOUD SECURITY Forum

iThome 新聞 專題 技術 AI Cloud 永續IT 醫療IT 資安 研討會 社群 IT EXPLAINED 搜尋

新聞

接連攻擊臺灣醫院企業的Crazyhunter現形，主嫌身分為20歲中國籍羅姓駭客

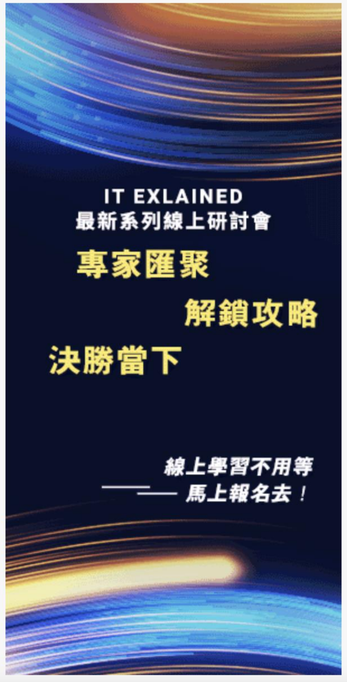
刑事警察局4月2日宣布，首度偵察出勒索軟體攻擊者的真實身分，這兩個月持續鎖定臺灣企業組織攻擊的Crazyhunter，背後是一名中國浙江省籍羅姓男子，警方將依相關協議尋求中國協查，同時提醒國內企業組織當心攻擊再度發生，目前調查案例多是從已知漏洞入侵

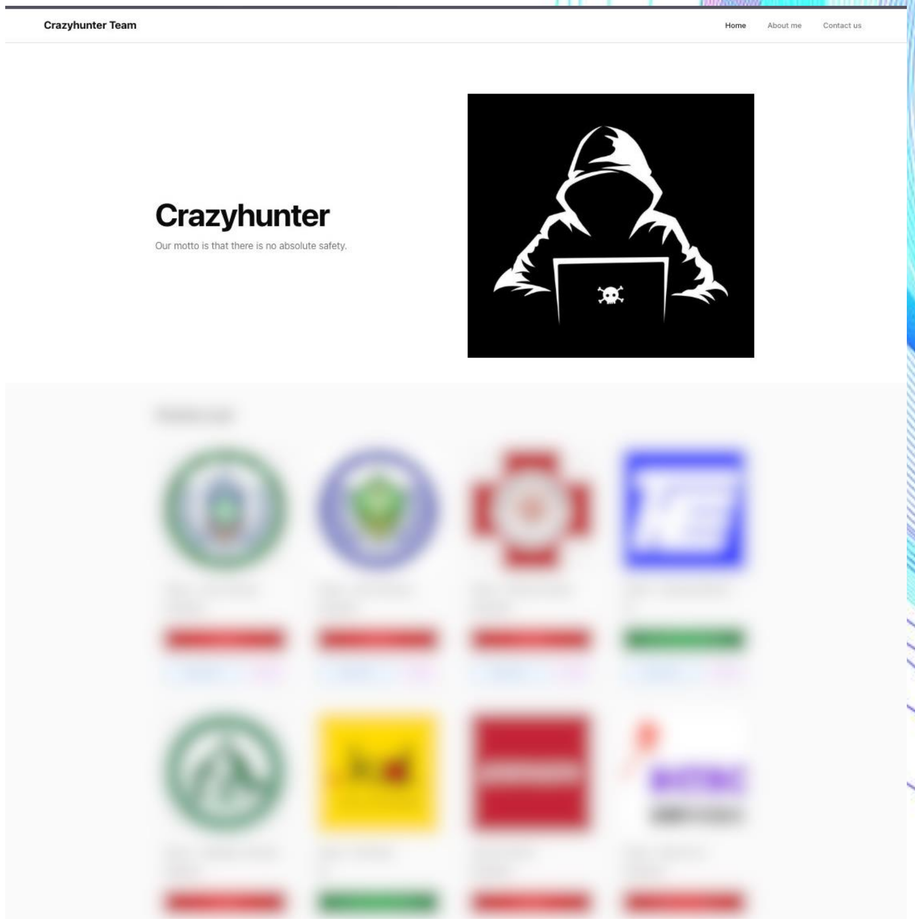
文/ 羅正漢 | 2025-04-02 發表

讚 140 分享

圖片來源: 攝影 / 羅正漢

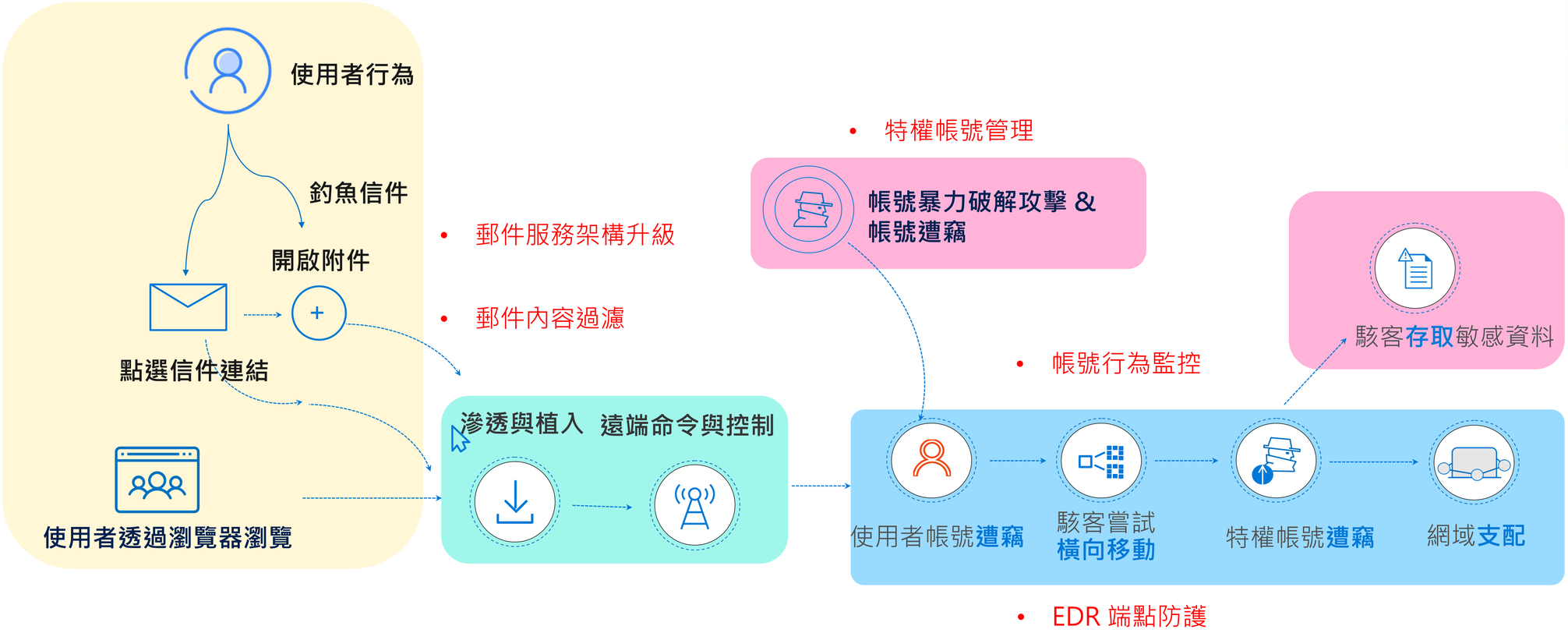
臺灣這兩個月接連發生遭CrazyHunter勒索軟體攻擊的事件，從2月馬偕醫院、3月彰基醫院受害以來，接續又有國內多家上市櫃公司遇害，由於這些攻擊專門鎖定臺灣攻擊，特別是醫院，情況相當嚴峻。今日（4月2



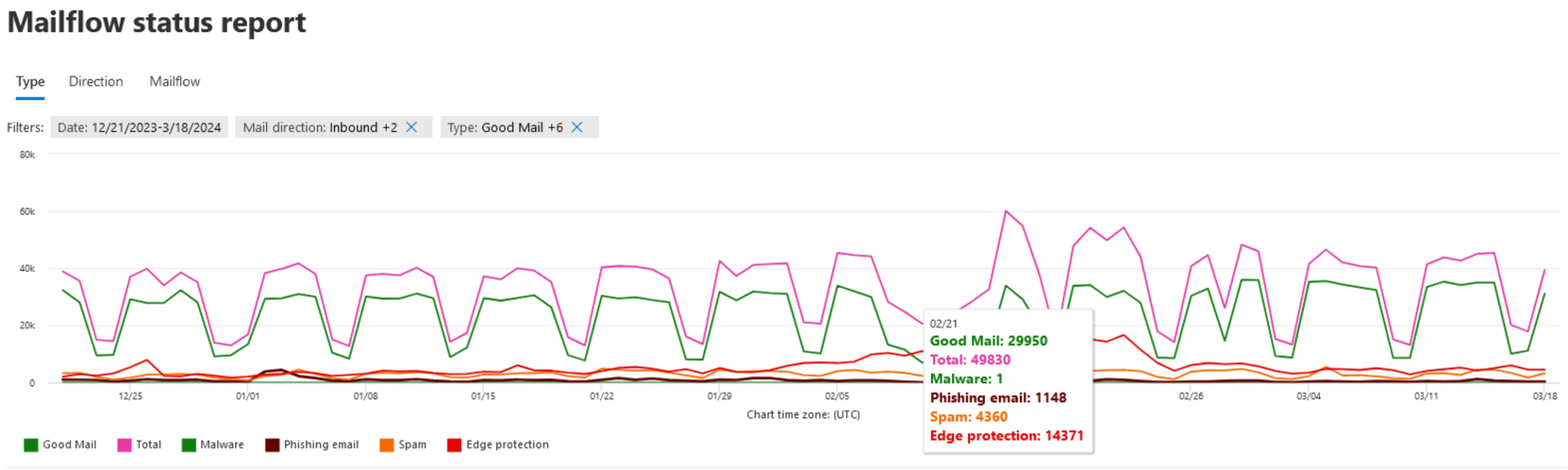


雲端平台協防機制

釣魚郵件的雲端防護架構



釣魚郵件的防護架構



- 平均每天擋下 **1000 封**以上釣魚郵件
- **4000-5000** 封垃圾信件

Mar 20, 2024 9:46:31 AM	78旗國寶級大師🤷帶你穿梭在北印度深邃又具詩意的旗...	service@epaper.ntch.art	Phish
Mar 20, 2024 9:44:00 AM	Повідомлення про відправлення	zbut@novator-tm.com	High Confidence P...
Mar 20, 2024 9:29:19 AM	已傳遞: [redacted] 常小姐 Transcen...	postmaster@fis.com.tw	Phish
Mar 20, 2024 8:43:40 AM	Microsoft Session Expired	nguyen.hoang@digicoms.com.vn	High Confidence P...
Mar 20, 2024 8:43:40 AM	Microsoft Session Expired	nguyen.hoang@digicoms.com.vn	High Confidence P...
Mar 20, 2024 8:43:40 AM	Microsoft Session Expired	nguyen.hoang@digicoms.com.vn	High Confidence P...
Mar 20, 2024 7:40:41 AM	Undeliverable: [系統通知] 計畫 C99-081 之經費已低於底...	postmaster@ad.lotuspharm.com	Phish
Mar 20, 2024 7:29:54 AM	Re: Re: PO#2306060147: 95000K New Order	infoadmin@uppii.com	High Confidence P...
Mar 20, 2024 7:15:06 AM	傳遞和諧、吶喊與關懷的琴聲	par-epaper@par.ntch.art	Phish

您好！

请容我介绍一下自己——我是一名专业黑客，并且已成功黑进您的操作系统。
目前，我已经获得您账户的完整访问权限。
最重要的是，在过去的几个月里，我一直在偷偷地观察并监视您的一举一动。
这都是因为您的电脑被感染了恶意间谍软件，它是在您访问成人视频网站的时候被植入您电脑的。

请给我几分钟解释一下这对您的影响。在木马病毒的帮助下，我现在可以不受限制地访问您的电脑以及您拥有的其他所有电子设备。
也就是说，我可以不受任何限制地看到您屏幕上的所有内容，甚至可以随时在您完全不知情的情况下开启您电子设备上的摄像头和麦克风。
此外，我还可以不受限制地访问您的私密数据，包括电子邮件、聊天记录等。

您肯定想不通，为什么您的杀毒软件就没有检测到我的恶意软件呢？
我完全不介意给您解释一下：我的恶意软件是基于驱动的；因此它每隔4个小时就会刷新一次签名，这确保了它不会被您的杀毒软件检测到。

我制作了一部视频，这部视频的左半边显示的是您激情自慰的样子，而它的右半边显示的则是当时您正在观看的下流视频。^.^

相信我，只需要点击几下鼠标，我就能把这部视频分享给您的个人电脑或其它电子设备上的所有往来邮件地址和聊天软件联系人。
另外，我还可以轻松地公开您所有的电子邮件和聊天记录。

我知道，您肯定不希望发生这样的事情。
我这也确实有一个解决方法——把相当于990美元的比特币汇入我的比特币账户（操作方法很简单，但是如果您对此不甚了解的话，请在网上寻找详细教程）。

我的比特币账户信息如下（比特币钱包）：1M2eLbFgRbmYgQUApuWEyGVc9axPqZXe7q

一旦我的账户收到上面提到的那笔汇款，我就会马上删除那些下流的视频，并从您的生活中永远消失。
请于50个小时（2天）之内完成这笔汇款。
在这封邮件被打开后，我会马上收到一个提示，并同时触发倒计时。

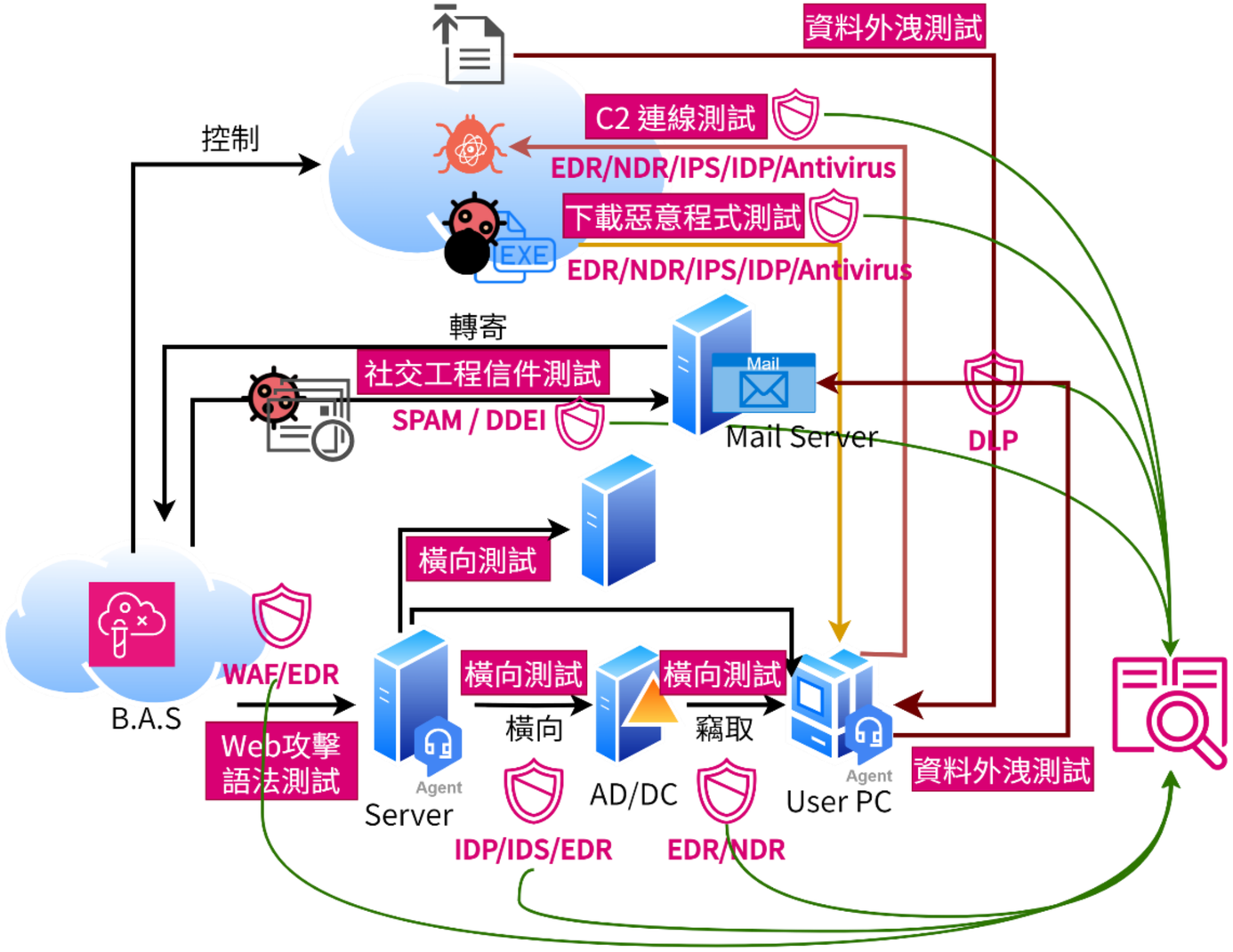
相信我，我是非常谨慎且专业的，从来不会出错。
如果我发现您把这件事情告诉了别人，我就会马上公开您的私人视频。

祝好运！

CYBERSEC 2025
臺灣資安大會

資安防護機制有效性評估

模擬真實攻擊方式，驗證各項機制是否失效



- 驗證設備防護
- 驗證SOC機制

Security Operation Center
Security Information and Event Management

用駭客的思唯來檢視資安架構

- Trust redefined : BAS(Breach and Attack Simulation)為近年來崛起的新興技術應用，它被定義為可以自動模擬駭客進行多面向攻擊的一種即時解決方案。
- 模擬真實世界攻擊者所用的威脅程式、技巧、方法，驗證與測試組織中IT資安設備的成效。
  - ✓測試醫院對這些攻擊的偵測、分析與應對處理的能力
  - ✓通常著重在醫院無法偵測應對到的攻擊方法
- WAF Testing
  - ✓屬 Web Application ，以常見的攻擊為主
  - ✓建議以最近100個較為常見的攻擊威脅進行測試，約 1100 個攻擊方法
  - ✓含SQL Injection 、XSS、OWASP TOP10等E-mail Gateway Testing
- Email Gateway Testing
  - ✓屬 E-mail滲 透，寄入惡意郵件
  - ✓建議以最近100個常見的APT Group惡意程式進行E-mail測試，約250個樣本
- IPS / IDS & Firewall Testing
  - ✓屬 Network滲透，下載惡意程式為主
  - ✓建議以最近100個常見的APT Group惡意程式進行下載測試，約240個樣本

CYBERSEC 2025
臺灣資安大會

回歸資訊安全核心原則

資安事件發生的根本原因

- 人為因素
  - ✓ 錯誤設定系統或防火牆
  - ✓ 員工缺乏危機意識點擊釣魚郵件
- 系統與軟體漏洞
  - ✓ 作業系統或應用程式未及時更新
  - ✓ 使用過時或不再維護的軟體
  - ✓ 未修補的已知漏洞（如Log4j...等）
  - ✓ 同仁的程式寫作習慣
- 脆弱或缺失的資安架構
  - ✓ 沒有適當的監控與偵測機制
- 缺乏資安意識與訓練
  - ✓ 無政策約束（如 BYOD 政策不清晰）
  - ✓ 未定期進行演練或模擬攻擊
- 資安投資不足
- 外部威脅與攻擊者的進化
  - ✓ 勒索軟體攻擊日益複雜
  - ✓ 開放 API、第三方供應商帶來的風險

Windows 系統為何漏洞這麼多?

源頭

- 市佔率高 → 成為駭客首選攻擊目標
  - ✓ Windows 是全球最多人使用的作業系統（特別是企業環境）。
  - ✓ 市佔高 → 攻擊者可以影響更多人、更有價值。
  - ✓ 駭客也是算投報率的，哪裡使用者多，就先攻哪裡。
- 歷史悠久 → 技術債累積
  - ✓ - Windows 支援的程式庫、相容模式極多（向下相容到 Win95、甚至 DOS）
  - ✓ - 這導致很多舊架構無法快速淘汰，藏了許多潛在漏洞。
  - ✓ - 某些 API 太舊但仍被使用，就變成「維護與安全兼顧的難題」
- 功能多、系統複雜
  - ✓ Windows 要支援各種硬體驅動、第三方軟體、網路功能、多用戶登入等等。
  - ✓ 功能多代表潛在漏洞點也多，測試與驗證的難度上升。
- 使用者行為與彈性配置
  - ✓ Windows 使用者常以管理員身分操作（高權限）
  - ✓ 給使用者太多「自由配置空間」→ 容易誤操作或配置錯誤
  - ✓ 很多公司和學校不重視系統更新與安全政策

📌 總結一句話：Windows 並非「不安全」，只是它太普遍、太複雜、太有價值，因此被當作「主要目標」來研究與攻擊。

ISO 27001:2022 改版要點

新增項目 : 8.28 安全程式碼撰寫 (Secure Coding)

開發前

訂定**安全程式碼標準**

遵守組織內期望編碼原則

過往的常見漏洞

配置開發工具

遵循供應商指南

要求開發者安全程式碼能力資格

安全設計及框架(威脅建模)

開發中

使用安全程式開發技術

禁止使用不安全設計

分析記錄常見錯誤

....

開發後

保護原始碼免於遭受竄改

確保部署過程之安全

紀錄錯誤

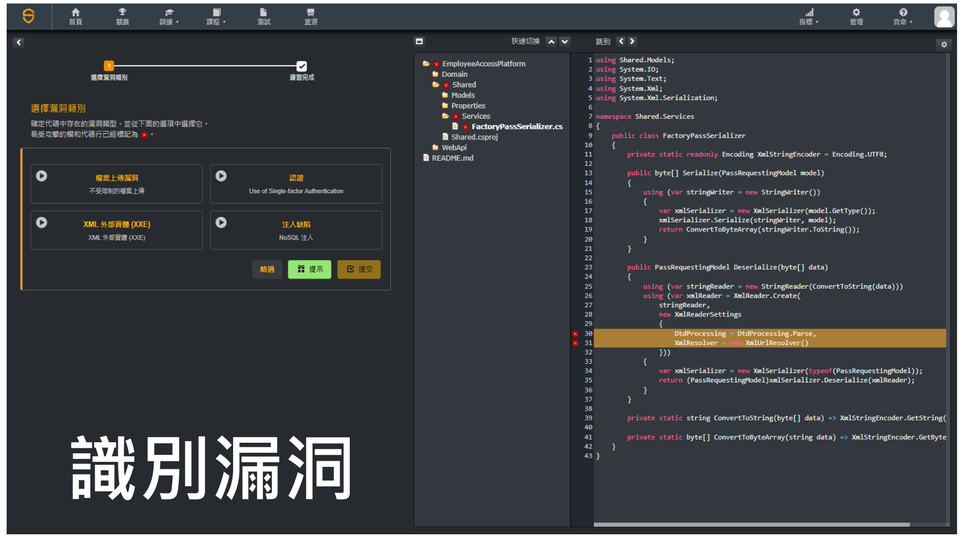
修補已上報/新漏洞

企業應於2025年10月24日完成轉版

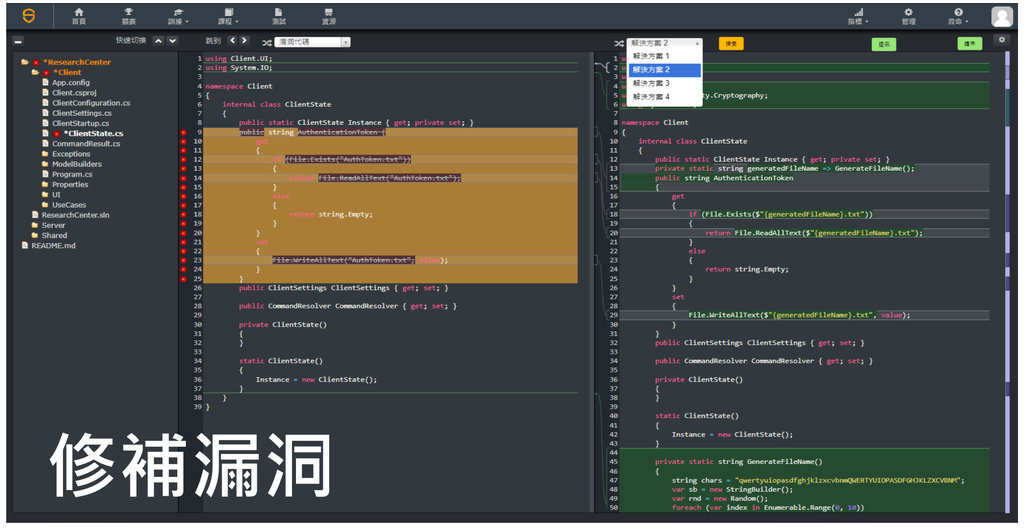
安全開發能力的平台

50+語言/框架，155+漏洞類型，多種應用場景

OWASP、PCI DSS、NIST多種合規課程

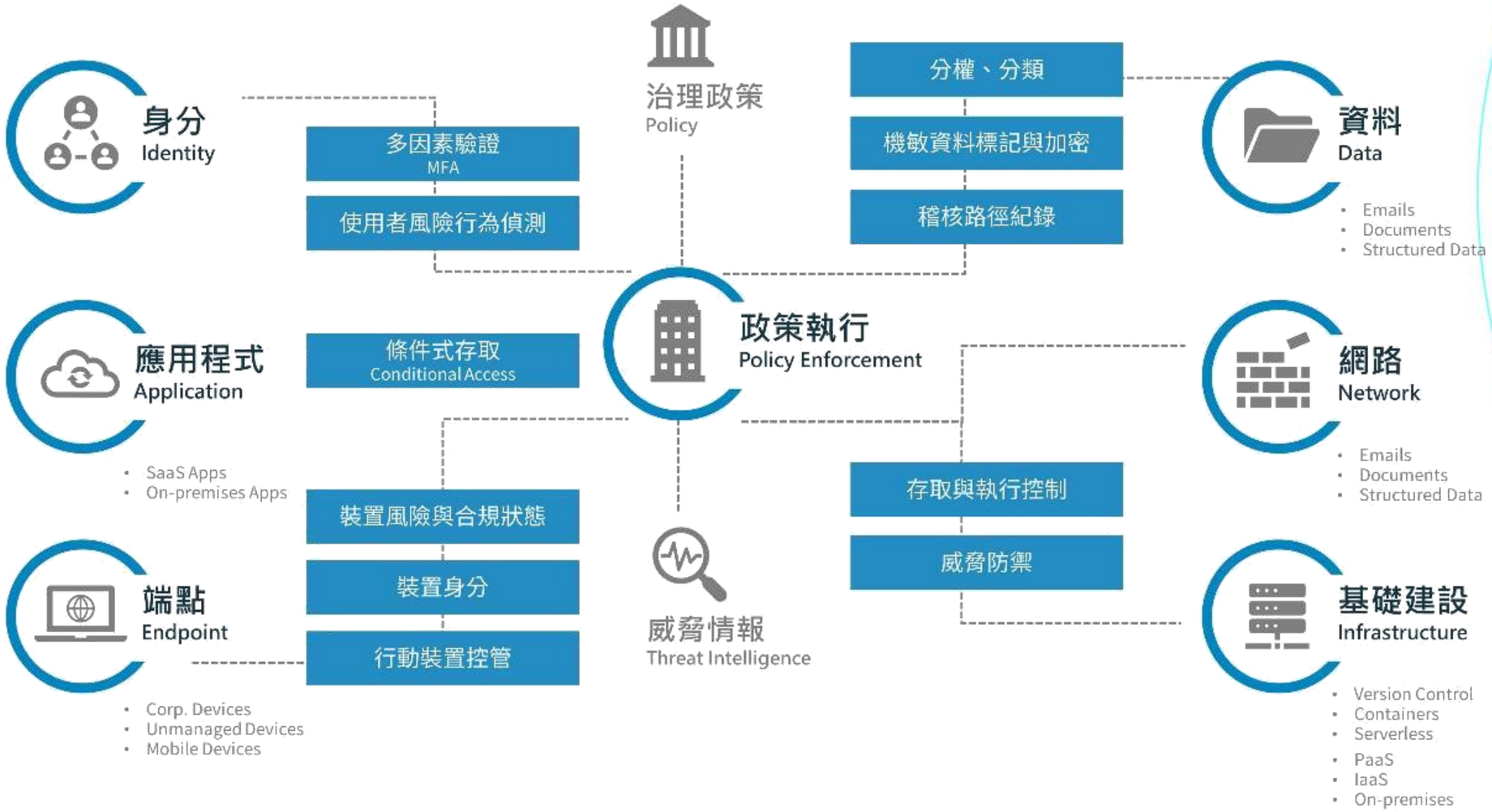


識別漏洞



修補漏洞

Zero-Trust：安全的零信任的規劃



「雖是腹心，猶須驗證；信不及人，防不留情」

敬請指教
Q&A

TEAM
CYBERSECURITY