未知的風險才是最大的風險

奠定 AI 智慧校園防護基石：

以內網風險可視化驅動零信任架構

曜祥網技:黃士滄

資安事件持續增長

亞太地區勒索軟體事件月增近27%，臺灣事件數排名第三

亞太勒索軟體活動升溫，8月事件數較前月增加近27%，臺灣排名第三。最活躍的勒索軟體組織The Gentlemen也有6起事件涉及臺灣



網路安全業者Group-IB近期回顧2026年8月亞太地區資安威脅，共記錄190起勒索軟體事件，較7月增加26.7%，臺灣當月有20起，在報告列出的國家與地區中排名第三，僅次於印度32起及澳洲24起。

這些勒索軟體事件都利用資料外洩網站公布受害者資訊，向受害組織施壓，也都使用資料加密手法造成影響。Group-IB建議企業持續更新系統、安裝安全修補、部署多因素驗證（MFA），同時定期檢查IT環境中的潛在漏洞。企業也可利用入侵偵測系統（IDS）與端點偵測及回應（EDR）工具發現並處理威脅，另需建立資安事件應變計畫，並定期更新。

資料來源: iThome
https://www.ithome.com.tw/news/179235

駭客攻擊下的智慧校園安全危機

Smart Campus Cyber Security Threats



勒索軟體攻擊持續升級　你我都要提高警覺

數位發展部資通安全署表示，近年駭客手法已從傳統加密檔案勒索，演變為結合竊取機敏資料、威脅公開外洩的雙重勒索模式，加上生成式AI技術助長攻擊自動化與精準化，使全球攻擊事件快速增加。

建立正確資安觀念
落實日常防護
降低攻擊衝擊

勒索軟體攻擊的演變

1 傳統勒索

單純加密檔案，
要求支付贖金解密。



2 雙重勒索

不僅加密檔案，
還竊取機敏資料，
並威脅公開外洩。



3 AI 助攻

生成式AI技術讓攻擊
更自動化、精準化，
全球攻擊事件快速增加。



常見入侵管道

釣魚郵件
假冒機關、企業
誘導點擊或下載附件

惡意網站
透過不安全網站
植入惡意程式

系統漏洞
利用軟體或系統
漏洞入侵

非法軟體
使用未授權或
來路不明的軟體

主要攻擊目標與受駭後果

製造業　服務業　醫療機構

為主要攻擊目標

資料遺失　服務中斷　財務損失　聲譽受損

資安防護 4 大重點

1 落實系統備份



3-2-1 備份原則
- 3 份資料
- 2 種不同型式媒體
- 1 份異地備份

建立定期備份習慣，確保遭遇加密攻擊時，
仍有資料可供重建還原。

2 保持系統軟體更新



- 作業系統更新
- 應用程式更新
- 防毒軟體更新

即時修補漏洞，
關閉可能之入侵通道。

3 強化帳密安全



- 提高密碼複雜度
- 避免跨平台重複密碼
- 啟用兩步驟驗證
- 使用密碼管理工具

保護帳號不被盜用，
降低資料外洩風險。

4 防範社交工程



- 提高警覺心
- 不明簡訊、郵件、連結
- 切勿點擊或下載附件
- 防範AI生成的逼真誘餌

守住人為防線，
避免成為攻擊的突破口。

資安無小事 · 多一分警覺 · 少一分風險 · 讓我們一起打造更安全的數位環境

資安防護關鍵戰略

- 以資安風險管理為基礎
- 落實零信任架構的導入

提升資安治理成熟度



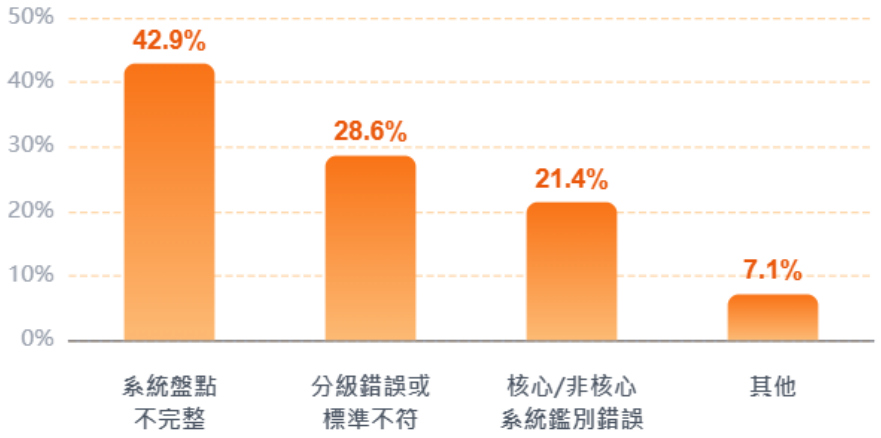
資安風險管理基本功

「資產可視性」

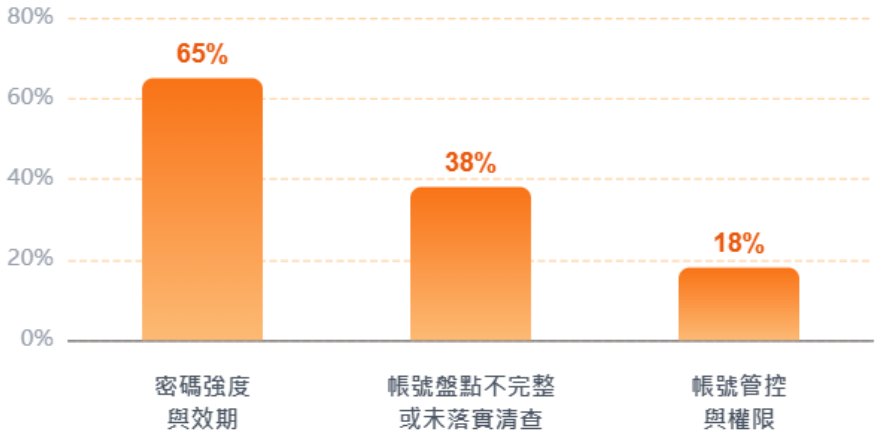
E-SOFT

114-115年度教育體系資通安全查核常見缺失

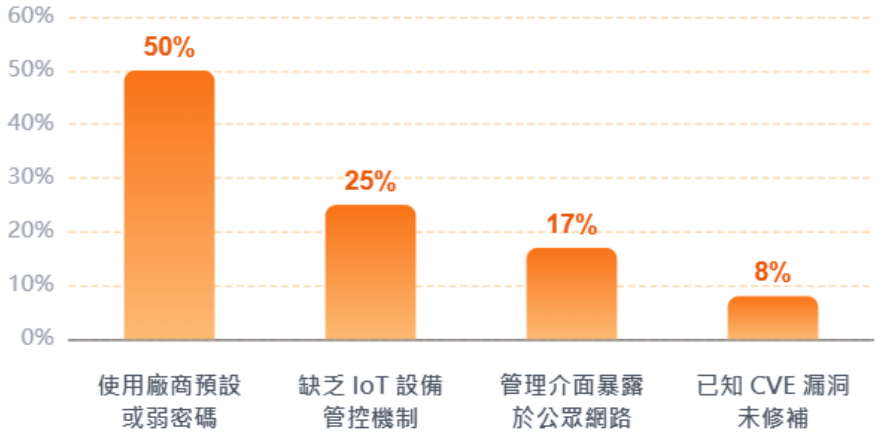
1. 系統盤點與分級缺失 (1.1)



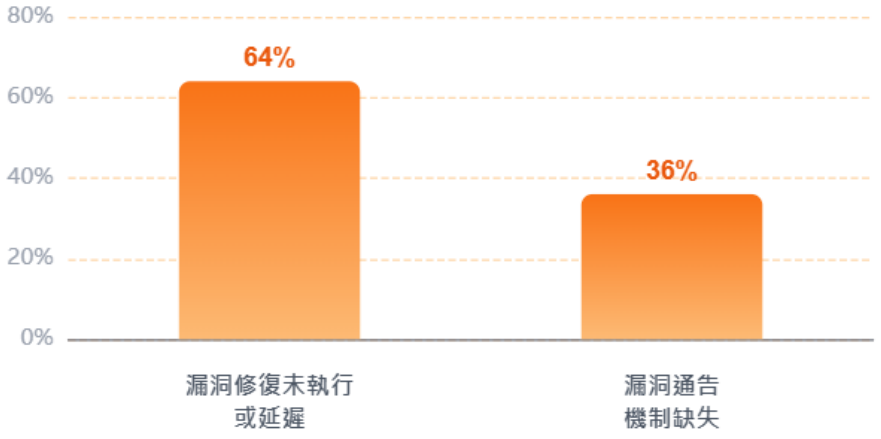
2. 帳號與密碼管理缺失 (7.15)



3. 物聯網 (IoT) 設備管控缺失 (7.15.1)



4. 漏洞修復與通告機制缺失 (8.11)



資料來源: https://iscb.nchu.edu.tw



機關資產可視性的挑戰

策略面			管理面			技術面		
心務其要核業及重性	安策動通政推織資全及組	人經置責及配專力費	及系點險訊通盤風估資資統及評	系服外之措通或委理理施資統務辦管	維畫施之及管制全計實形進效機安護與情精績理	安及措通防制施資全控	系展維全通發維安資統及護	安件情估通事報情評及應資全通及變因
68.24	75.00	70.44	**64.12**	68.24	70.88	69.71	**65.00**	72.88

- 太依賴人工手動紀錄盤點
- 沒有效率的跨部門溝通協調
- 機關網路環境複雜化

  -太多連網的裝置

  -太多安裝的軟體

  -分散式的網路架構

  -不同的網路使用區域

E-SOFT

全機關連網設備資產全面盤點

以網路技術為核心，掌握完整有效IP-Based設備基準

總數不一致？

Excel表
總數2000
沒有活動設備900

資產軟體
總數2200
沒有活動設備1000

網域控制站
總數1800
沒有活動設備800

OA | Server | IOT | VPN | Wireless

整合
關聯分析

Windows設備
1300

1300
完整盤點

1300
完整盤點

1300
完整盤點

500
IoT設備

Printer
IP CAM
刷卡機(卡鐘)
IOT設備

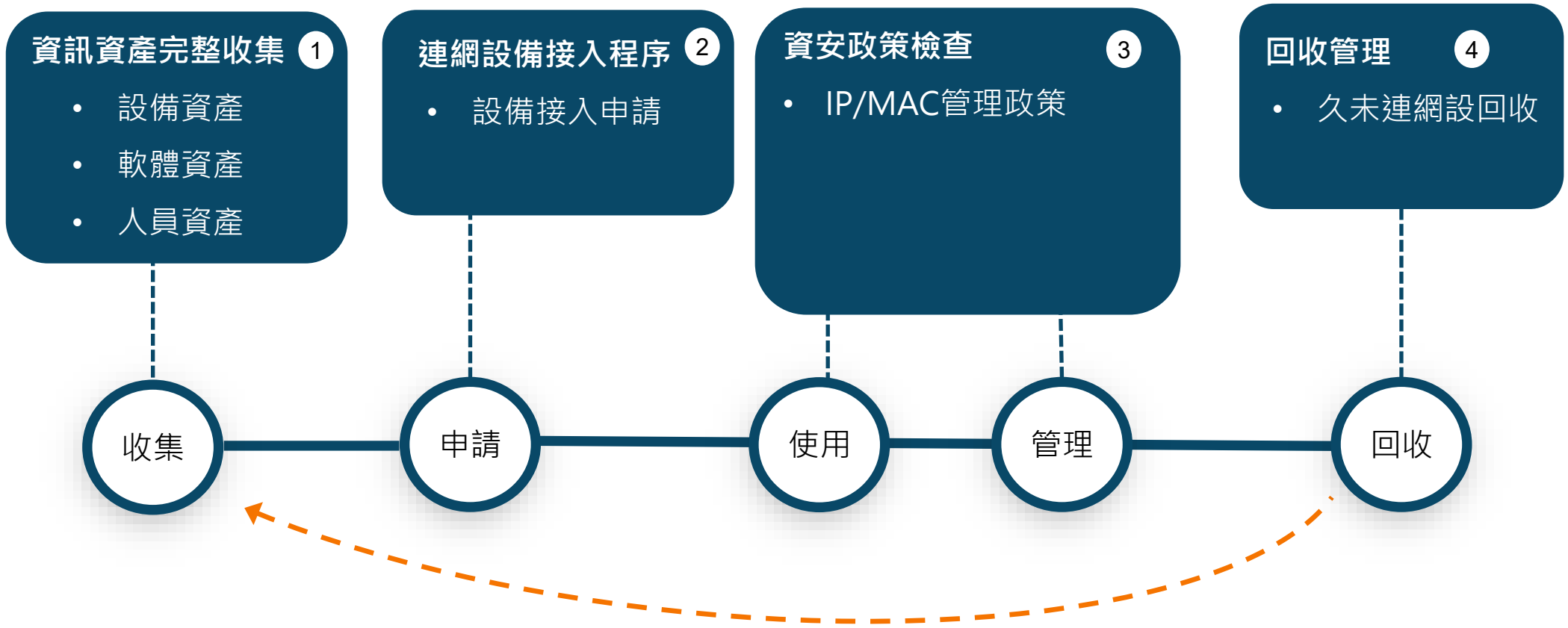
設備資產

軟體資產

人員資產

E-SOFT

建構連網設備生命週期自動化管理



E-SOFT



資安風險管理基本功

「風險評估持續性」

E-SOFT

風險在哪邊?



設備資產
是否受保護?
組態是否一致?

軟體資產
是否更新?

人員資產
帳號是否閒置?

組態設定
是否異常異動?

圖片來源: SEMI

設備防護軟體落實才能發生真正效益

核心觀念：資安不是買保險，而是要落實防禦

總經理，我們每年投入預算購買資安軟體（如防毒軟體），
但最危險的觀念就是以為「有買就好」。



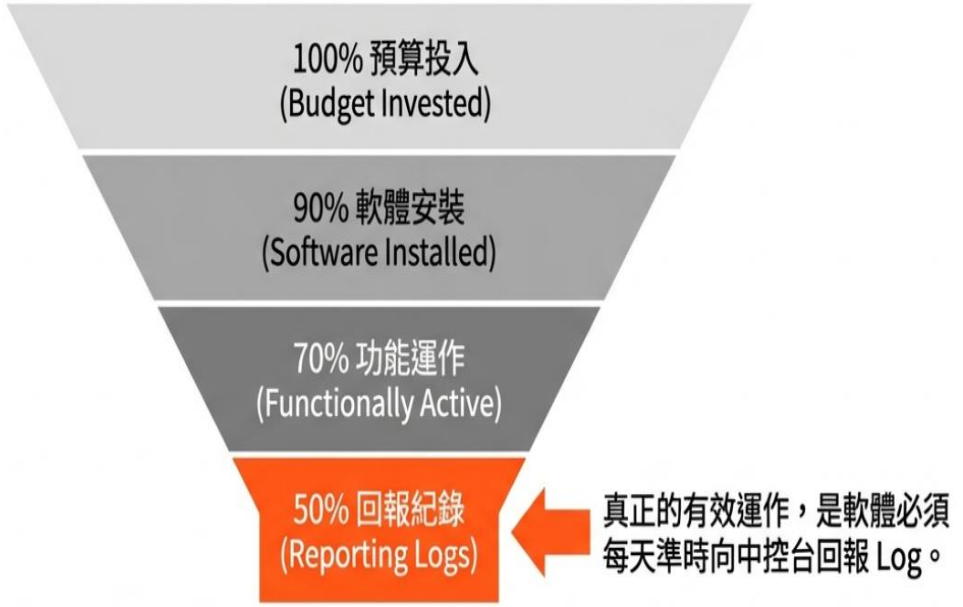
買了 ≠ 裝了

很多設備在網路上跑，但我們根本不知道它有沒有裝防毒。

裝了 ≠ 有用

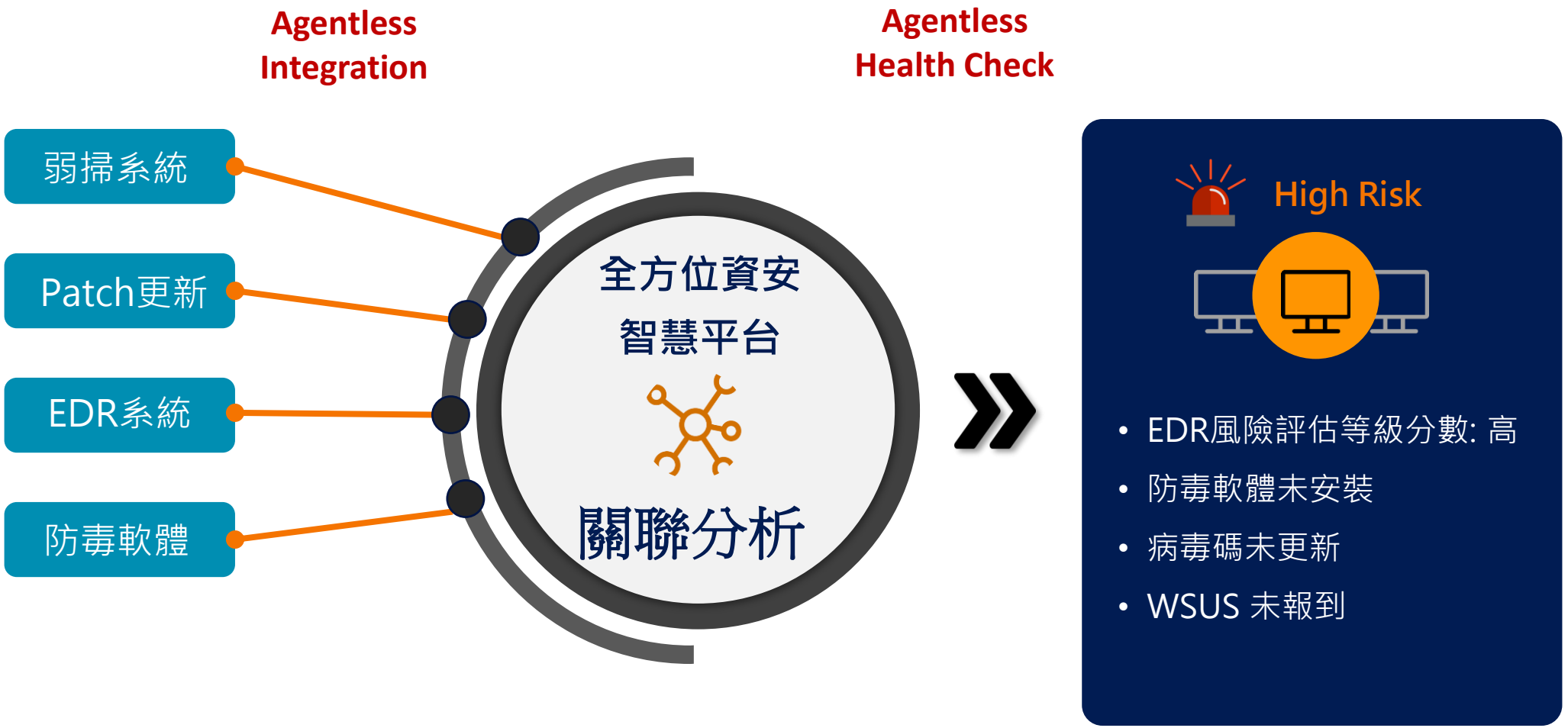
軟體會當掉、會衝突、病毒碼會過期。一旦「脫鉤」，它就是一個擺設。

定義「有效運作」：中控台看不見的，就是風險



影響：如果中控台收不到資料，管理員跟 SIEM 監控系統就會變成瞎子，根本不知道那台電腦已經失控。

建立資安管理政策統一監控平台



設備資產資訊安全查核重點

ISO 27002改版重點

- 將控制措施由舊版14個控制領域整合成4大主題(theme)
  - 組織控制(Organization Controls)37項(34項既有，3項新增)
  - 人員控制(People Controls)8項(皆為既有措施)
  - 實體控制(Physical Controls)14項控制(13項既有，1項新增)
  - 技術控制(Technological Controls)34項控制(27項既有，7項新增)
- 由舊版114項控制措施調整為93項控制措施
  - 全新之控制措施11項
  - 更新之控制措施58項(淘汰過時技術，反映最新的最佳實務)
  - 合併之控制措施24項(將不可分割或密切相關的既有控制措施加以合併)
- 加入5項可供選擇與搜尋的屬性
- 「目的(Purpose)」取代「控制目標(Control Objectives)」

全新控制措施(5/11)

A.8.9 組態管理(Configuration management)

控制措施

應建立、書面記錄、實作、監視並審查硬體、軟體、服務及網路之組態(包括安全組態)

目的

確保硬體、軟體、服務及網絡於所要求安全設定下正常運行，且組態未遭未經授權或不正確變更而更改

實務指引

- 應備妥角色、責任及程序(如資訊資產管理程序書或組態管理程序書)，以確保所有組態建立與變更皆符合要求
- 使用公開可取得之安全組態標準模板(如GCB、廠商及獨立安全組織提供之組態最佳化模板)
- 可藉由自動化或人工方式比對分析組態是否偏差，並採取矯正措施
- 組態設定模板及標的可能係機密資訊，需妥善防護

E-SOFT

風險在哪裡?



設備資產
是否受保護?
組態是否一致?

軟體資產
是否更新?

人員資產
帳號是否閒置?

組態設定
是否異常異動?

圖片來源: SEMI

漏洞層出不窮

第六章 資通安全防護及控制措施

第十八條、依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。

第十九條、具備下列資安防護控制措施：

一、 防毒軟體。

二、 網路防火牆。

三、 如有郵件伺服器者，具備電子郵件過濾機制。

四、 入侵偵測及防禦機制。

五、 如有對外服務之核心資通系統者，具備應用程式防火牆。

六、 進階持續性威脅攻擊防禦措施。

七、 資通安全威脅偵測管理機制(SOC)。

第二十條、針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。

第二十一條、 訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。

第二十二條、 建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。

第二十三條、 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。

第二十四條、 建立資通系統及相關設備適當之監控措施，如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。

第二十五條、 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。

第二十六條、 留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。

漏洞警訊公告

- VMware存在安全漏洞(CVE-2022-31656)，攻擊者可藉此取得管理員權限，請儘速確認並進行更新
  08/08/2022
- 微軟支援診斷工具存在安全漏洞(CVE-2022-30190)，攻擊者可藉此遠端執行任意程式碼，請儘速確認並進行更新
  06/20/2022
- F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2022-1388)，允許攻擊者繞過身分鑑別程序，進而遠端執行任意程式碼，請儘速確認並進行更新
  05/10/2022
- Windows作業系統存在高風險安全漏洞(CVE-2022-26809)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新
  04/20/2022
- Google Chrome、Microsoft Edge、Brave及Vivaldi瀏覽器存在高風險安全漏洞(CVE-2022-1364)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新。
  04/20/2022
- Cisco多款無線網路控制器軟體存在安全漏洞(CVE-2022-20695)，允許攻擊者繞過身分鑑別取得裝置控制權，請儘速確認並進行更新
  04/20/2022
- Trend Micro Apex Central平台存在高風險安全漏洞(CVE-2022-26871)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新
  04/06/2022
- Spring Framework存在Spring4shell高風險安全漏洞(CVE-2022-22965)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新
  04/06/2022
- SonicWall SonicOS存在安全漏洞(CVE-2022-22274)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新
  03/31/2022

設備漏洞

應用程式漏洞

軟體漏洞

E-SOFT

國家資通安全研究院VANS2.0之要求

- 蒐集範圍：資通系統、工業控制系統及使用者電腦之軟體資產



跨平台
軟體資產收集

風險在哪裡?



設備資產
是否受保護?
組態是否一致?

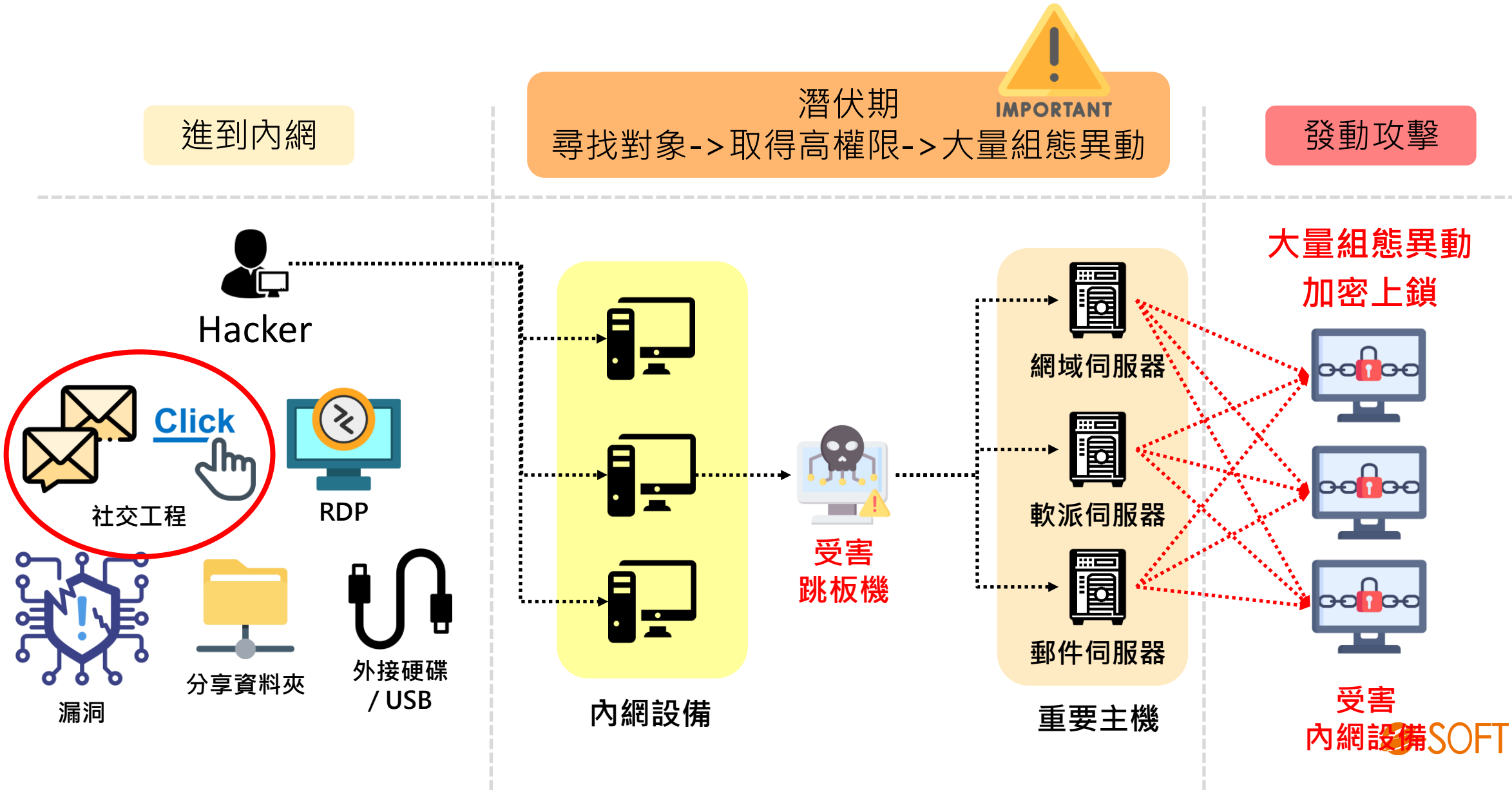
軟體資產
是否更新?

人員資產
帳號是否閒置?

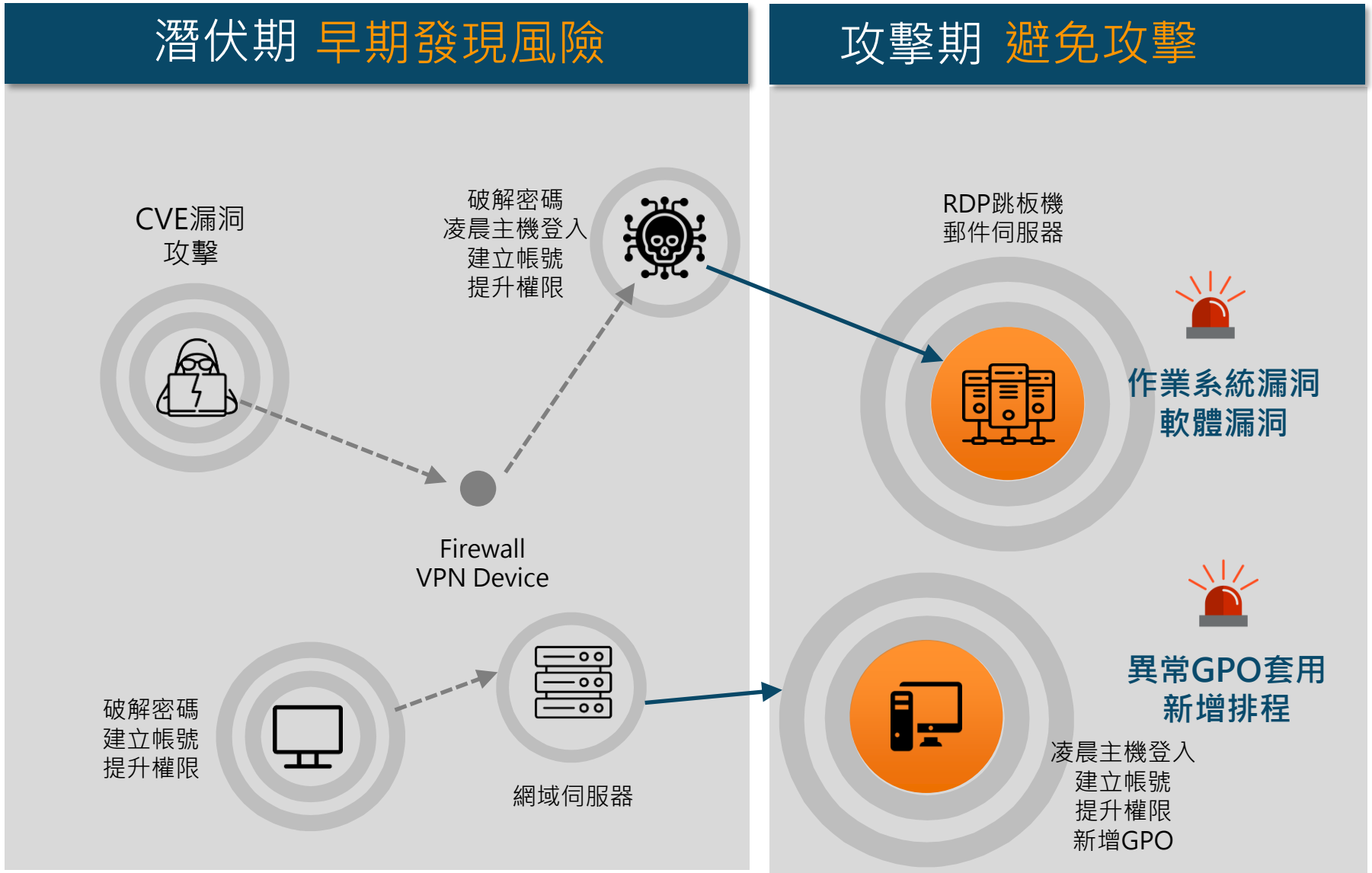
組態設定
是否異常異動?

圖片來源: SEMI

駭客勒索病毒攻擊常見途徑



e-SOFT人員資產風險早期掌握



本機

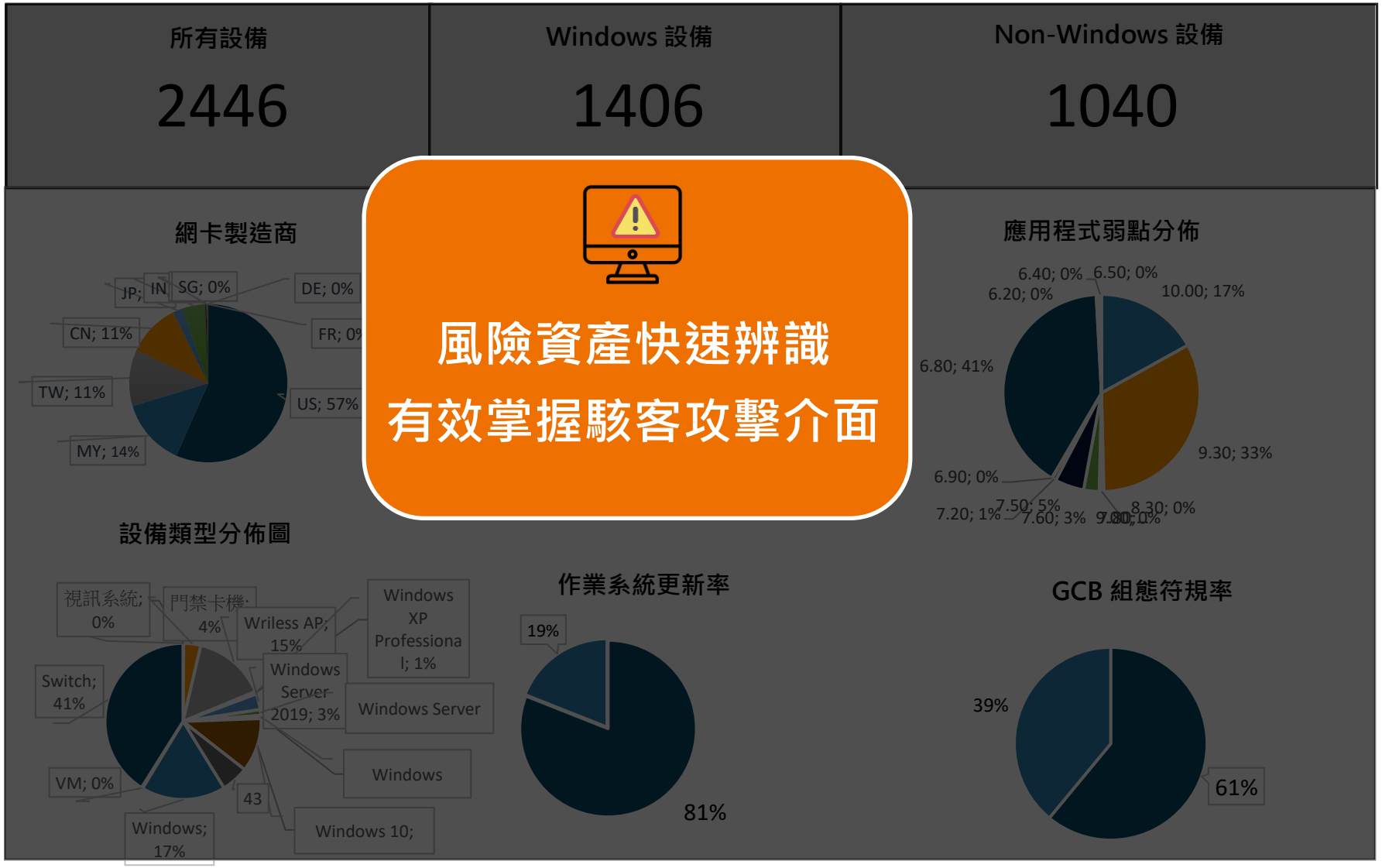
- 非法時間RDP登入主機
- 本機Guest帳號狀態異動
- 本機高權限群組成員異動

網域

- 非法時間RDP登入DC
- 網域帳號狀態鎖定
- 網域帳號新增異動
- 網域高權限群組成員異動

e-SOFT

全面資產風險評估管理



資產完整收集盤點

- 連網設備清單
- 軟體資產清單
- 人員群組清單

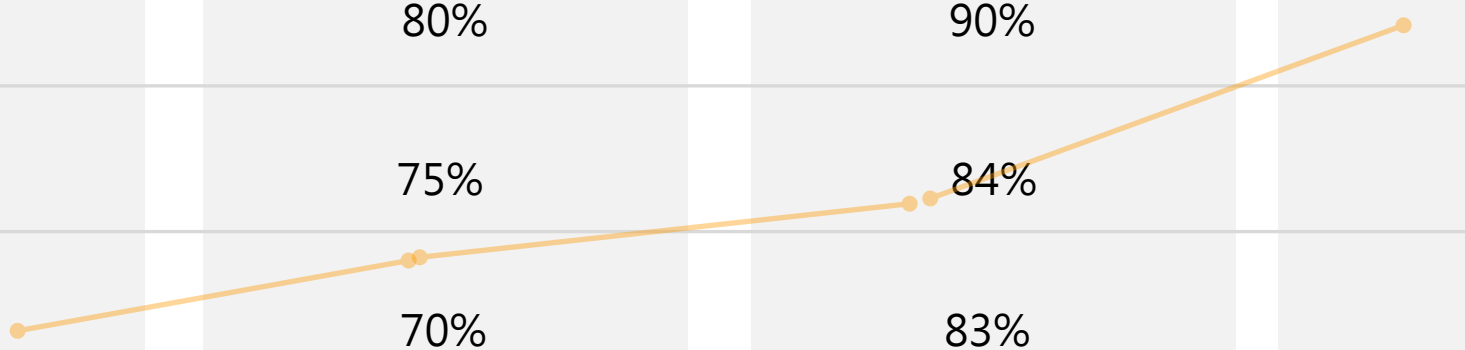
E-SOFT 全方位資安智慧平台

風險全面評估

- 軟體弱點通報
- 特權帳號異動稽核
- Hotfix派送檢視
- 組態合規檢查

資安政策落實度全面提升

	第一季 75%	第二季 80%	第三季 87%	第四季 95%
全公司設備數量	3000	3100	3150	3300
AD網域符規率	75 %	80 %	87 %	95 %
資產軟體符規率 (部署率/有效性)	60%	80%	90%	95%
防毒軟體符規率 (部署率/有效性)	66%	75%	84%	95%
WSUS符規率 (部署率/有效性)	55%	70%	83%	95%



時間成本降低幅可達99%以上

經持續改善作業程序
符規率可達95%資安防護度

E-SOFT

e-SOFT 全方位資安智慧平台

100% MIT

一步一步落實資安管理：AI 智慧戰情與底層平台之整合

【最上層】
AI 智慧戰情分析

- 快速掌握與識別高風險威脅
- 即時資安態勢感知
- 智慧型關聯與預警

AI 數據回饋與決策

Step 01: 設備與資產盤點

- 連網設備與帳號盤點 (IoT, 舊系統)
- 實名化 IP 與數位身份管理
- 異動與閒置帳號查核

»

Step 02: 風險評鑑與盤點

- 資訊資產風險評估
- 軟體黑白名單與 CVE 漏洞查核
- 網域與 GCB 組態檢視

»

Step 03: 智慧防護與部署

- 設備健康檢查與防毒部署
- EDR 與 DLP 部署率提升
- SmartAD 網域組態防護

»

Step 04: 零信任政策納管

- ZTA 零信任管理系統
- 資源安全信任推斷
- 多場域系統安全整合

符合 NIST 零信任管理架構規範

提供統一數據與底層安全基石

【底層】 e-SOFT SIP 全方位資安智慧平台 (Security Intelligence Platform)


「資安就是持續精進的風險管理」
面對無所不在的資安挑戰，要不斷的強化因應的管理機制，打造良好的資安防護力，提升數位免疫力。
E-SOFT

THANK YOU

曜祥網技股份有限公司

E-SOFT