數聯資安

鏈結多層資安防護網，抵禦目標式勒索攻擊

Jim Huang | 黃繼民

資安管理平台發展處-副處長

數聯資安股份有限公司

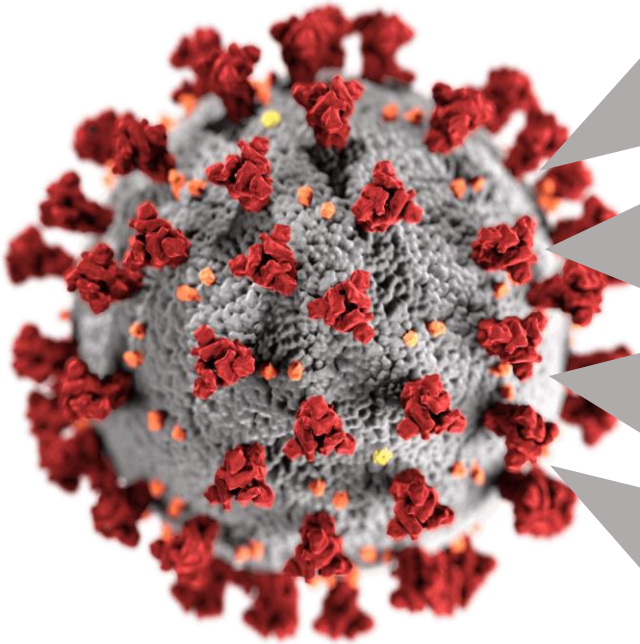
2021/5/10

遠傳電信 關係企業

數聯資安
Information Security Service Digital United

令人無奈的「新常態」

COVID-19



隱形攻擊

目標不限

災害不斷

尚無良方

Ransomware

資安事件頻傳，勒索攻擊持續增溫

2016 ~ 2019

2020 ~ NOW

新一代勒索攻擊

Targeted Ransomware Attacks

目標式勒索攻擊

為何成為目標:

有機可趁、有利可圖、你很在乎

勒索為何有用:

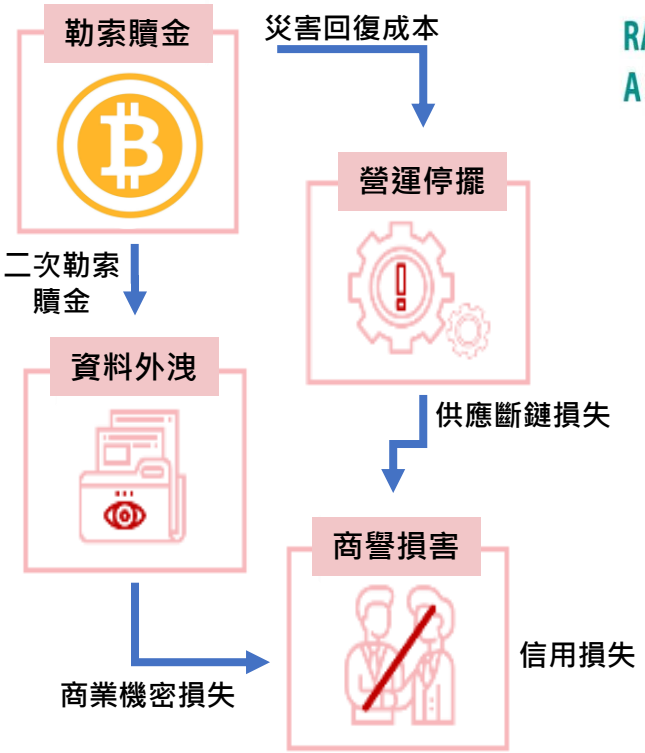
害怕失去、擔心影響、恐懼傷害

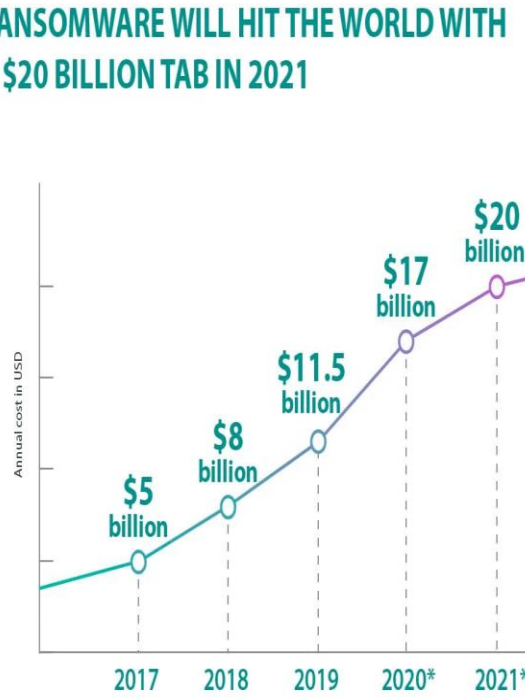
哪些攻擊有效:

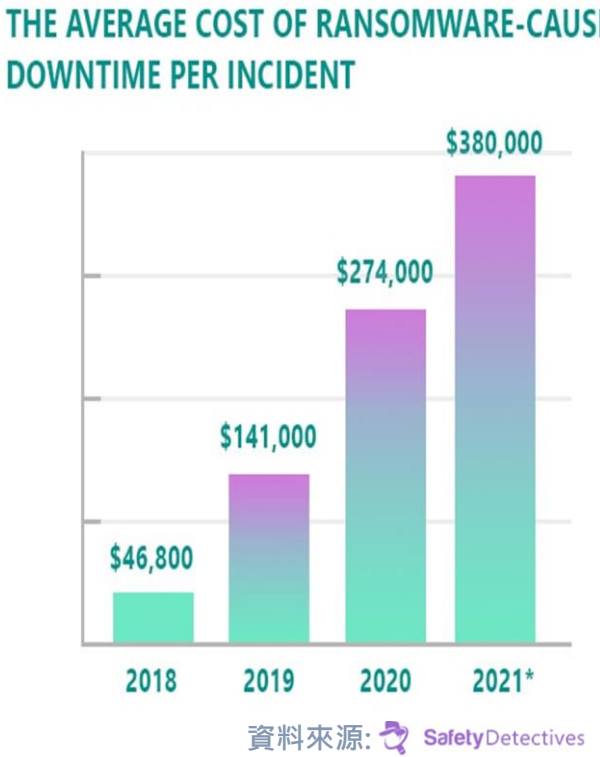
加密、洩漏、破壞

不是新的病毒

勒索金錢只是勒索攻擊總成本的一小部分







目標式攻擊破口 可利用的弱點及漏洞

94%
94%的惡意軟體透過電子郵件傳送

80%
超過 80% 的資安事件來自社交郵件

45%
45%的漏洞與黑客有關

27%
勒索病毒佔惡意程式攻擊27%

漏洞揭露率增加，資安脆弱度提升

微軟 | NSA | CVE-2020-0601 | 漏洞 | PoC | CryptoAPI | 簽章憑證 | 資安

鎖定微軟CVE-2020-0601漏洞的PoC攻擊程式在24小時內就出爐了

CVE-2020-0796 | Windows 10 | Server Message Block | SMB | 修補 | 重大漏洞

美政府警告駭客開始針對Windows 10 SMBGhost漏洞發動攻擊

微軟 | CVE-2020-1206 | CVE-2020-0796 | SMBGhost | SMBleed | 漏洞 | 修補

Windows 10再傳可串聯SMBGhost的SMBleed漏洞

Windows Server | DNS | 漏洞 | CVE-2020-1350

美國土安全部發布史上第三次緊急指令，要各聯邦機構限時修補Windows DNS Server的安全漏洞

微軟Patch Tuesday | Netlogon | Zerologon漏洞

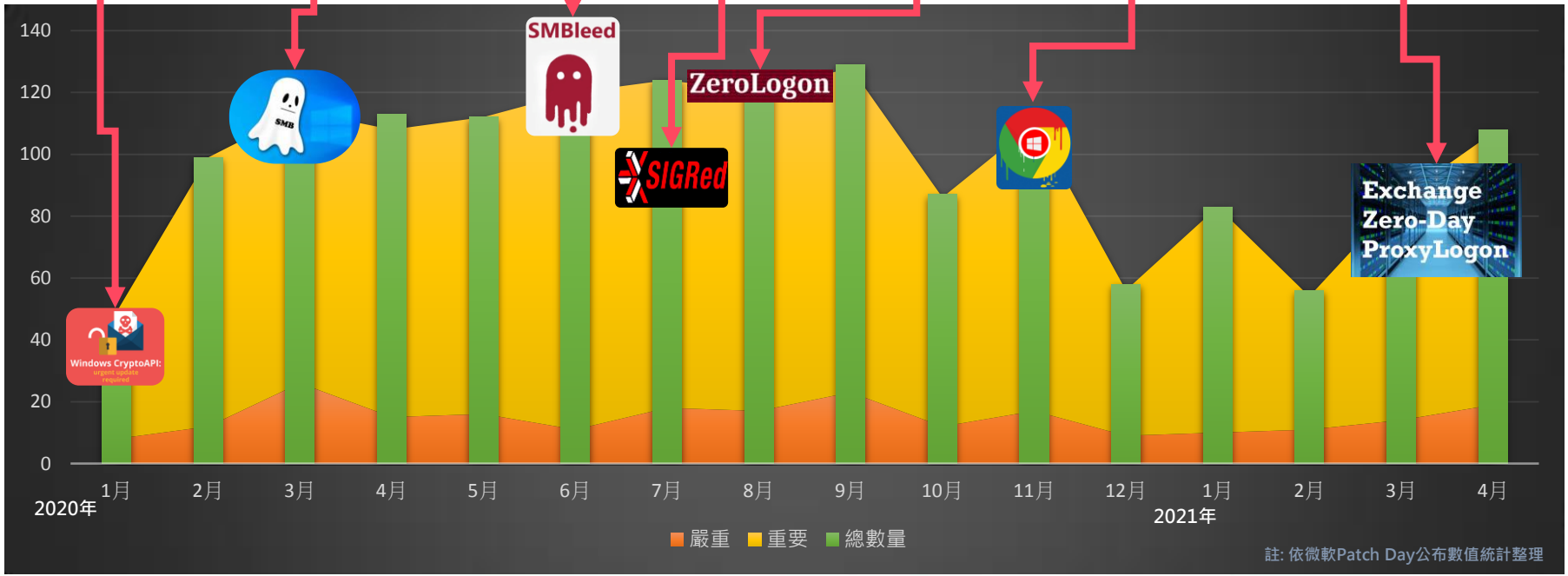
Windows重大漏洞Zerologon可讓駭客輕易掌控AD網域

Chrome漏洞 | CVE-2020-15999 | Windows核心漏洞 | CVE-2020-17087

Windows核心和Chrome瀏覽器的零時差漏洞已被駭客串聯發動攻擊，現在先更新Chrome，Windows修補還在路上

微軟 | Exchange | 勒索軟體 | DearCry | Win32/DoejoCrypt.A | ProxyLogon | 漏洞 | 資安

駭客用Exchange Server漏洞植入勒索軟體

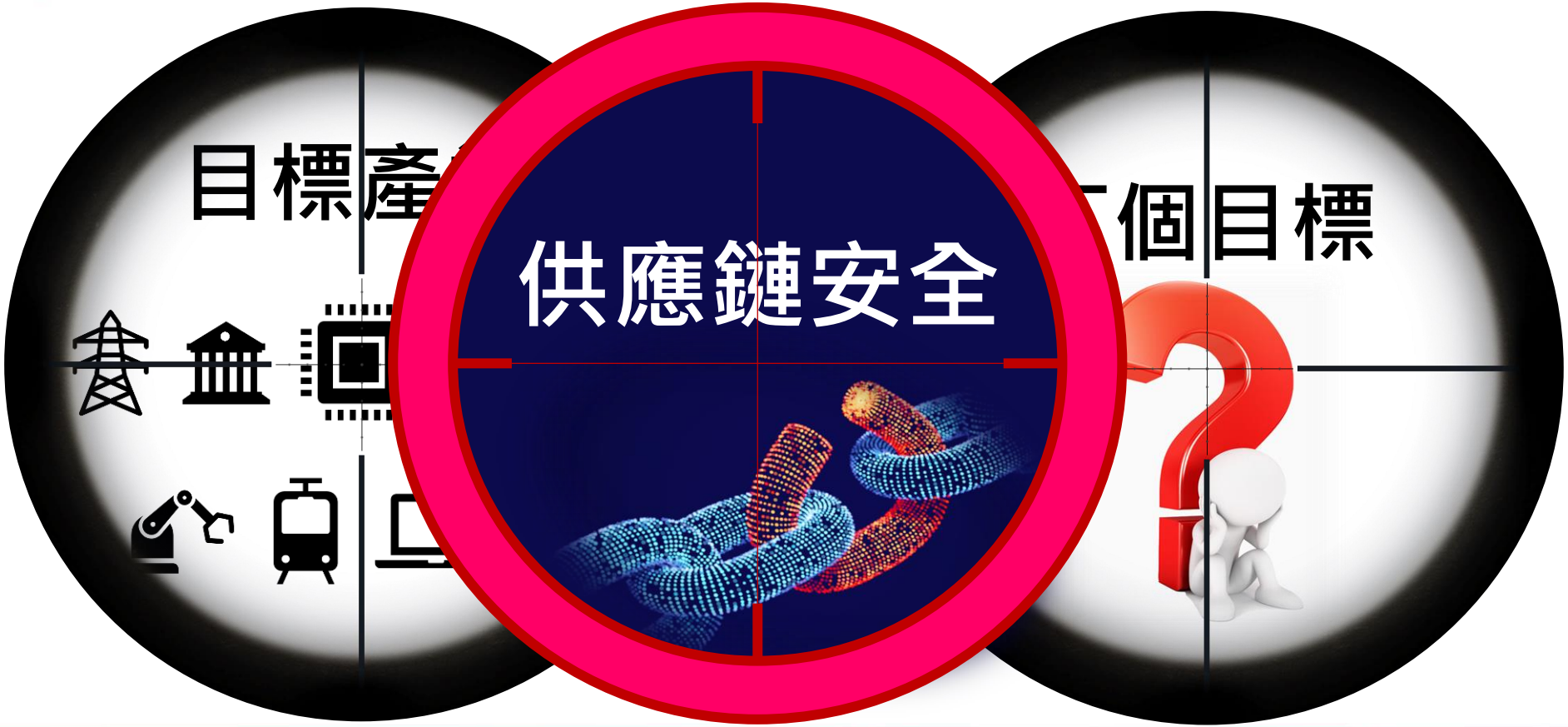


註: 依微軟Patch Day公布數值統計整理

勒索攻擊猖獗的因素解析

- 藤原效應
- 可利用弱點
- 漏洞武器化
- 勒索即服務

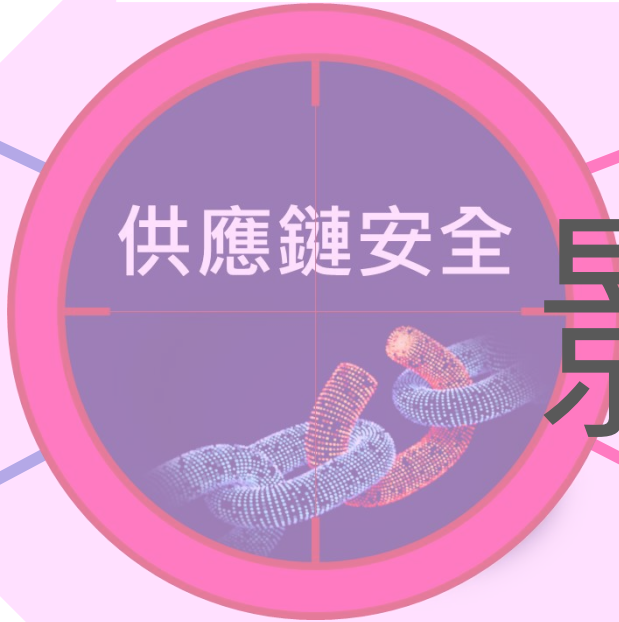
更針對性的勒索目標式攻擊



重新定義「供應鏈安全」

產業
供應鏈

生產
供應鏈



影響

軟體
供應鏈

- Active Directory
- Exchange
- Remote Desktop
- SharePoint
- WSUS

服務
供應鏈
(委外/契約)

系統
供應鏈

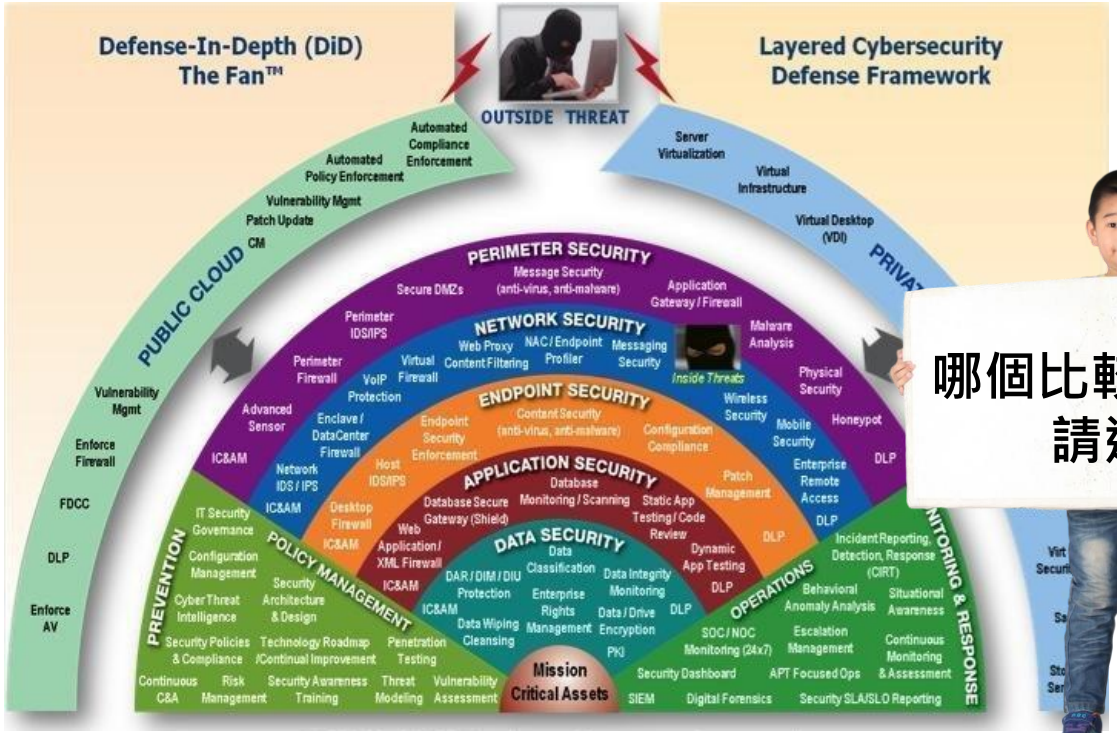
- 帳號認證系統
- 電子郵件系統
- 遠端操作系統
- 企業資源分享系統
- 軟體派送系統

供應鏈威脅: 脆弱環節多、傳導效果佳！

勒索攻擊防禦戰略方針

- 目標式防護
- 多維度防禦
- 零信任安全
- 持續性自適應風險管理

資安沒有完美、防護沒有永恆！



哪個比較有保佑?
請選擇

目標式防護: 重點 x 敏捷 x 效率

(例:)

獲知訊息

前期	中期	後期
機動偵查	目標式防禦	快速反應

- 資產盤點
- 弱點盤查
- 風險評估
- 修補狀態

- 異常偵測
- 外部控制
- 虛擬修補
- 目標防護
- 修補處理

- 事件通報
- 關聯比對
- 情資蒐集
- 應變處理

多維度防禦目標式攻擊


NGFW
弱點掃描
(防禦補強)
偵察掃描
駭客清查企業在網際網路上可建立的通訊連線。
觸發系統弱點
試圖入侵暴露在網際網路上的作業系統或服務的弱點。
IPS
安裝後門程式
下載駭客佈放在網際網路上的惡意程式。
建立駭客通道
企業內部已感染的電腦主機試圖與網際網路上的駭客中繼站建立通訊管道。
內部攻擊擴散
下載駭客佈放在網際網路上的惡意程式。
(縱向防護)
(異常偵測)
NGAV & EDR

零信任安全: 逆向思考、反證方法

Jericho Forum	ZT	BeyondCorp	ZTX	ZTA
2004	2010	2014	2017	Today

去邊界化

- 2004年Cisco召開一場國際CISO論壇討論【解決網路邊界崩壞問題】
- 結論：網路存取需要【信任; Trust】

零信任安全

- 2010… …究報告中首… …概念
- 20… …將開始… …出B… …端服…
- 201… …年小組，提出軟… …)架構，2019年精進推出 SDP 2.0

持續自適應

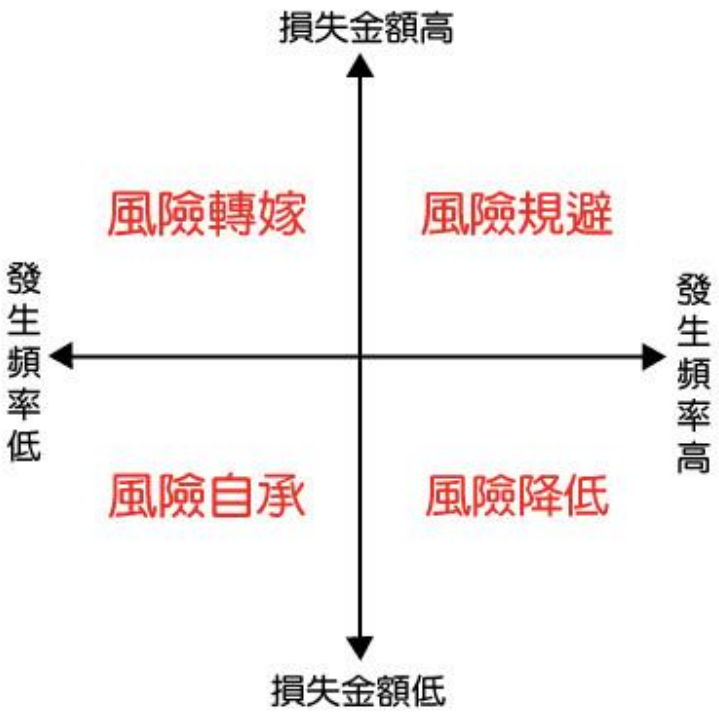
- 2017年Gartner發佈自適應安全 CARTA 3.0
- NIST於2019、2020年連續發表SP800-207 ZTA草案Draft2, 強調信任必須持續評估認證，而非默認

資料來源：工研院產科國際所ITIS研究團隊(2020/09)

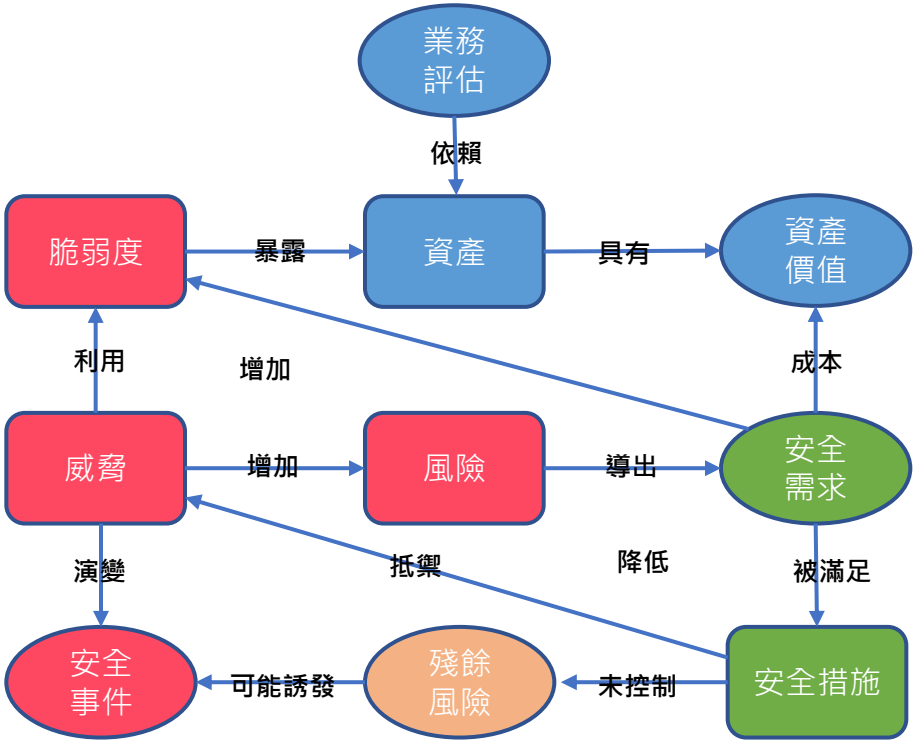
持續性自適應風險管理 (CARTA)

Continuous Adaptive Risk and Trust Assessment
2017年Gartner安全與風險管理高峰會議

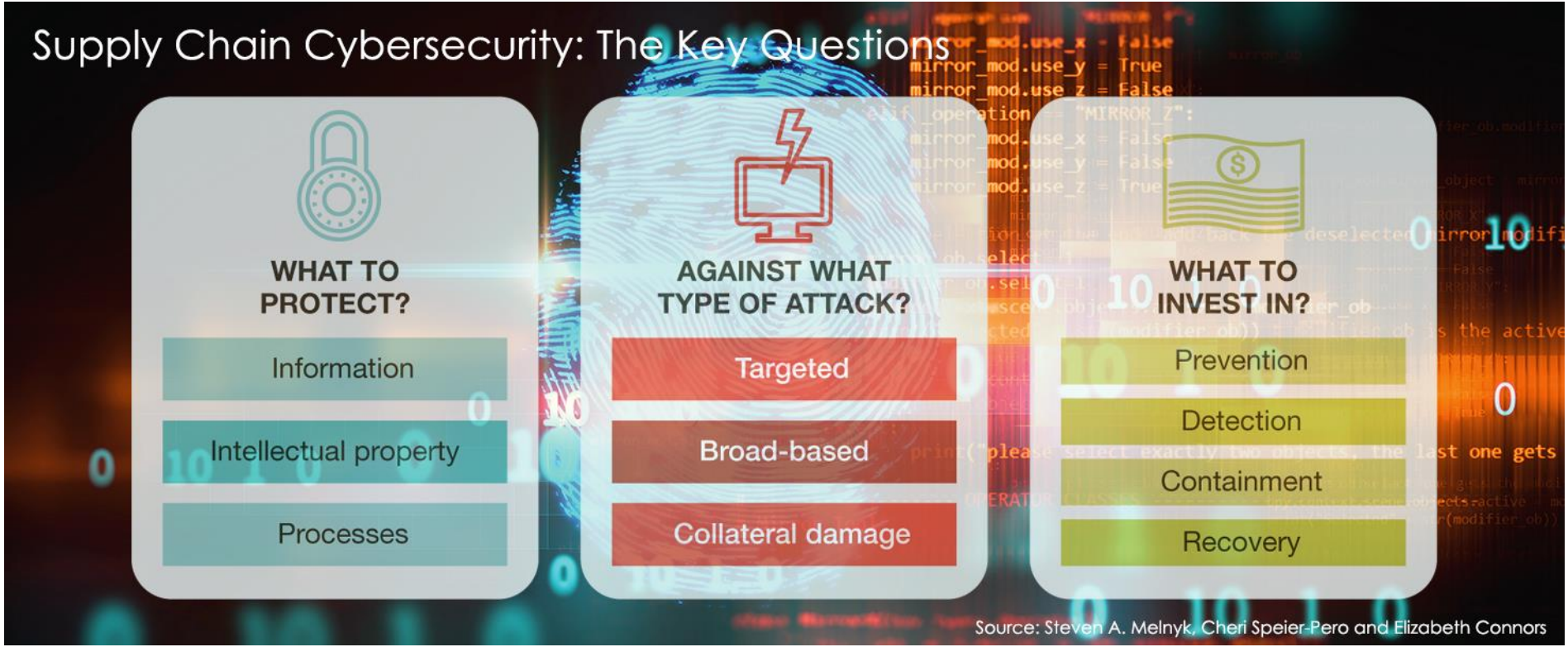
[保險業: 風險地圖]



[風險評估要素關係圖]

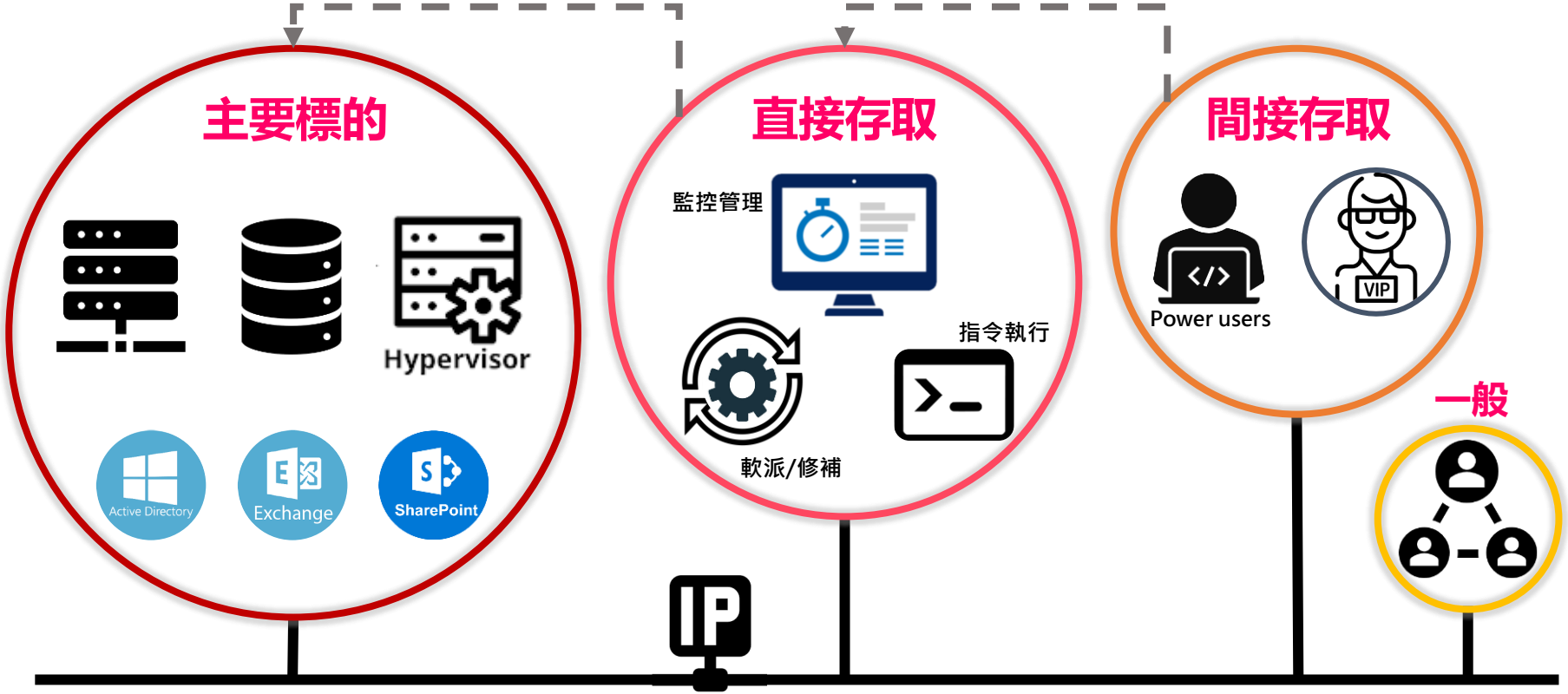


資安防護的思考邏輯

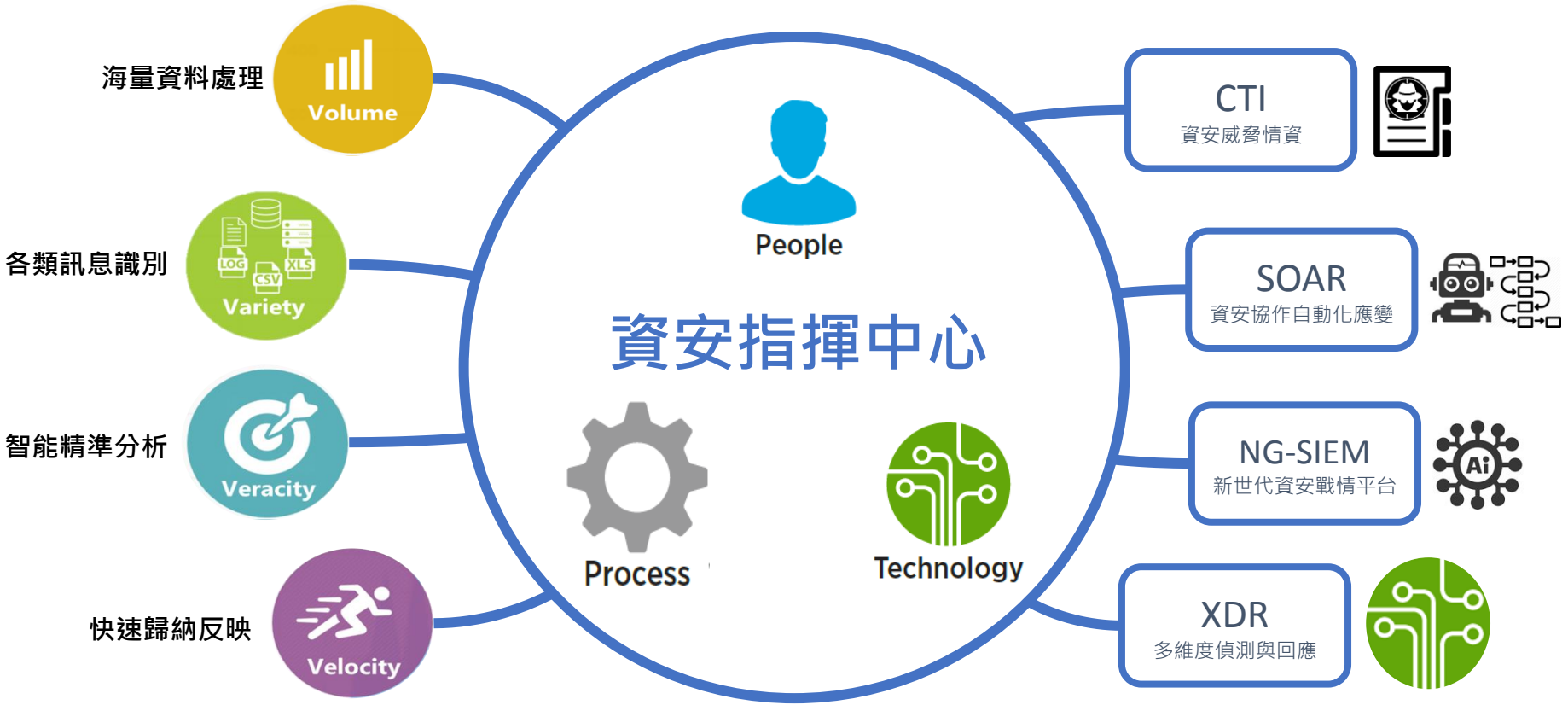

Supply Chain Cybersecurity: The Key Questions
WHAT TO PROTECT?
Information
Intellectual property
Processes
AGAINST WHAT TYPE OF ATTACK?
Targeted
Broad-based
Collateral damage
WHAT TO INVEST IN?
Prevention
Detection
Containment
Recovery
Source: Steven A. Melnyk, Cheri Speier-Pero and Elizabeth Connors

數聯資安
Information Security Service Digital United

資安防護標的評估建議



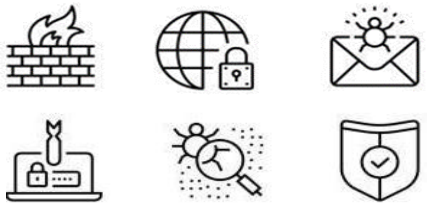
鏈結資安: NG-SOC 資安指揮中心概念



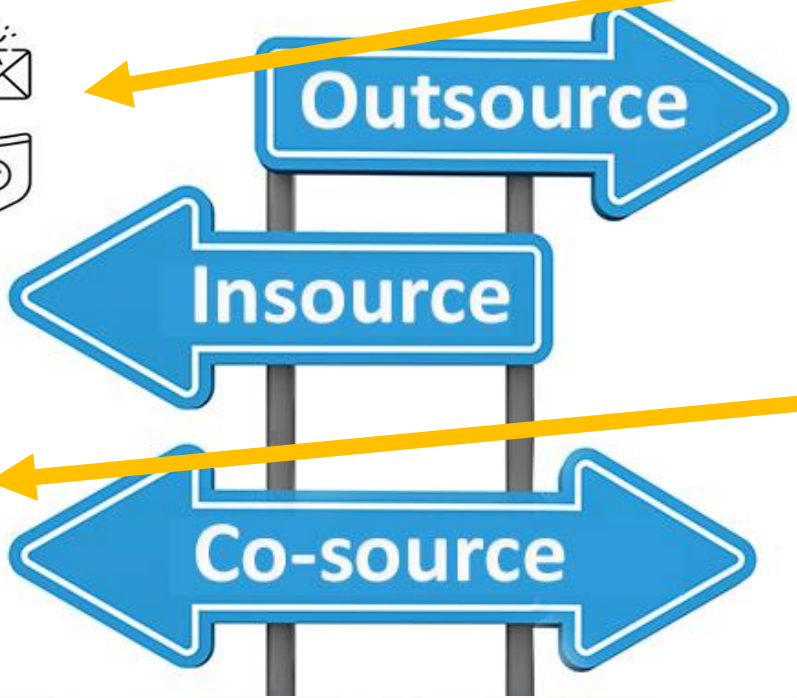
數聯資安
Information Security Service Digital United

資安維運模式

COMPANY



自建自維模式



委外服務模式

協同維運模式
訂閱服務模式

結語

- *駭客從來不講武德規矩.*
- *資安防護沒有完美一招.*
- *天下武功惟快不破，資安也是.*
- *跨域思考，借鏡學習.*
- *千萬不要挑戰「莫非定律」.*

The End

公司簡介

遠傳FET *100% 子公司*

成立時間: 2004年

專業服務能量

超過15年以上
資安服務實務經驗

智能資安監控平台

全台首座SOC
企業級資安監控中心

全方位資安服務

資安專業顧問
資安產品規劃
技術教育訓練

預防
強化威脅應對
威脅防護及驗證
法規遵循與導入
強化資安意識

監控及補強
縮減威脅潛伏
事件及軌跡分析
情資整合與判讀
漏洞識別與持續修補

應變及調查
消彌威脅入侵
資安事件鑑識舉證
威脅行為獵捕與消弭

專業資安服務整合 面面俱到

資安監控服務
- USOC® 監控服務
- 資安設備代管
- 緊急應變處理(ERS)
- 網站惡意連結監控服務
- 端點偵測回應服務(MDR)

資安解決方案
- 防火牆
- 端點偵測及回應
- 入侵防禦系統
- 進階持續威脅防務
- 網頁應用程式防火牆
- 智能資安戰情平台
- DDoS防護

資安檢測服務
- 滲透測試
- 系統弱點評估
- 網站弱點評估
- 資安健診
- APP檢測
- 社交工程演練
- 原始碼檢測
- DDoS演練

資安治理顧問
- ISO 27001資訊安全管理制度
- PIMS個資保護管理制度
- 金融機構電腦系統資安評估
- 物聯網及智慧城鄉查驗評估
- 企業資安稽核
- 員工資安教育訓練

3S資安訂閱服務
- 網路安全
- 端點安全
- 資安檢測服務

數聯資安

Thank You

數聯資安官網

3S資安訂閱服務