金融監督管理委員會
Financial Supervisory Commission

金融業導入零信任架構推進戰略

資服處 林裕泰
2025.11.18

金融零信任架構-政策回顧

2022.12

- 金融資安行動方案 2.0

2024.07

- 金融業導入零信任架構參考指引

2025.05

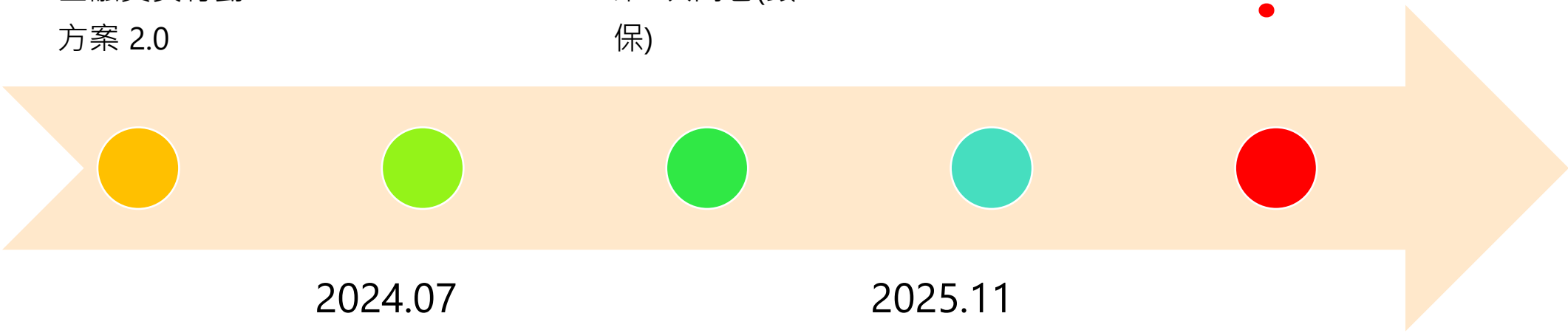
- 評估參考基準
- 第1次問卷(銀、保)

2025.11

- 第2次問卷(銀、保、證)

2026.12

- ?



金融資安行動方案 2.0 (2022.12)

- 客戶
  - 2.1 eKYC與業務風險對照
- 第三方服務商
  - 2.2 第三方風險評估與管理
- 居家/異地辦公
  - 2.3 因應新型態資安攻擊

政策面

1.擴大資安長設置，定期召開資安長聯繫會議

管理面

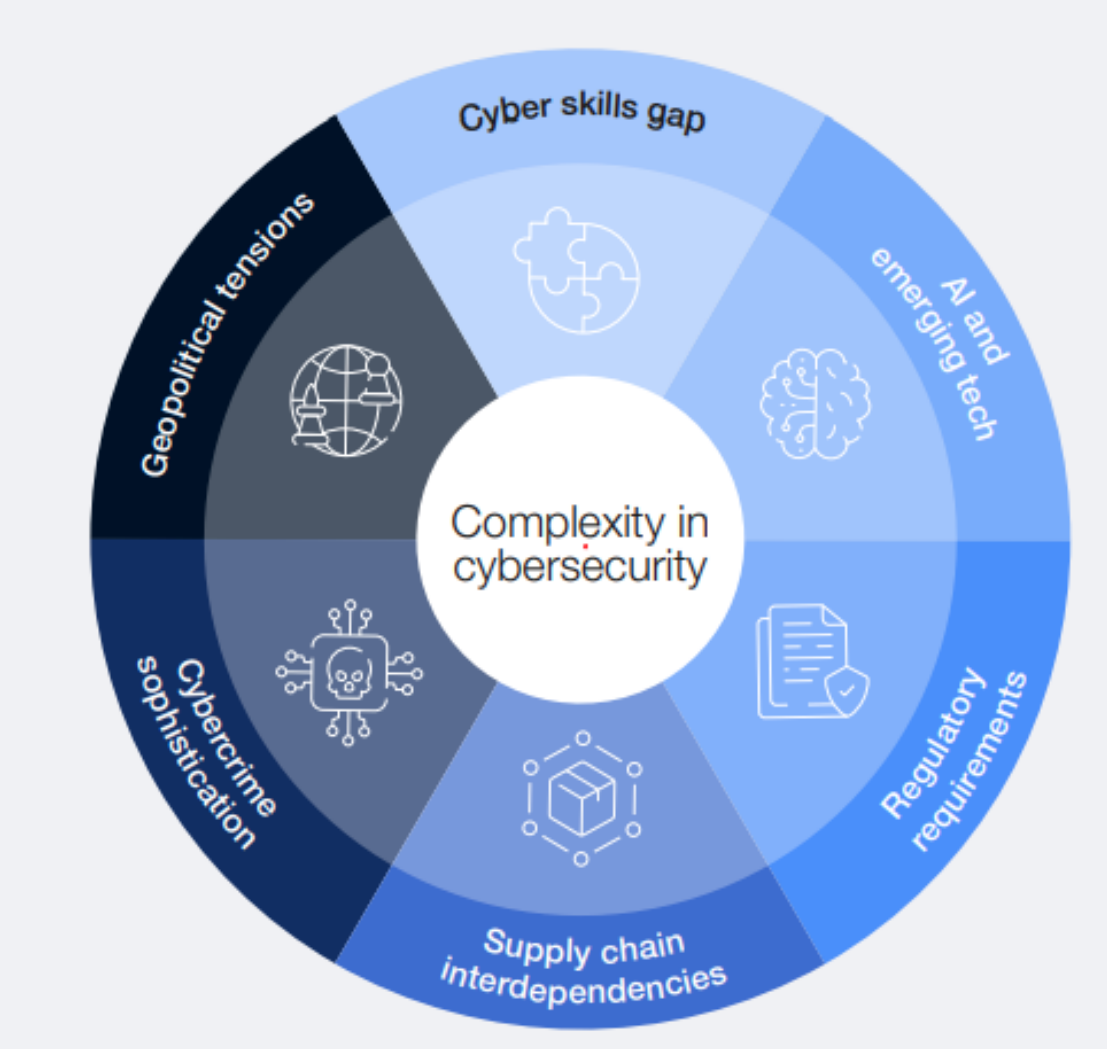
4.1 擴大推動導入國際資安管理標準	7.鼓勵配置多元專長資安人才，擴大演訓量能

技術面

事前-資安部署	事中-資安監控	事後-營運持續

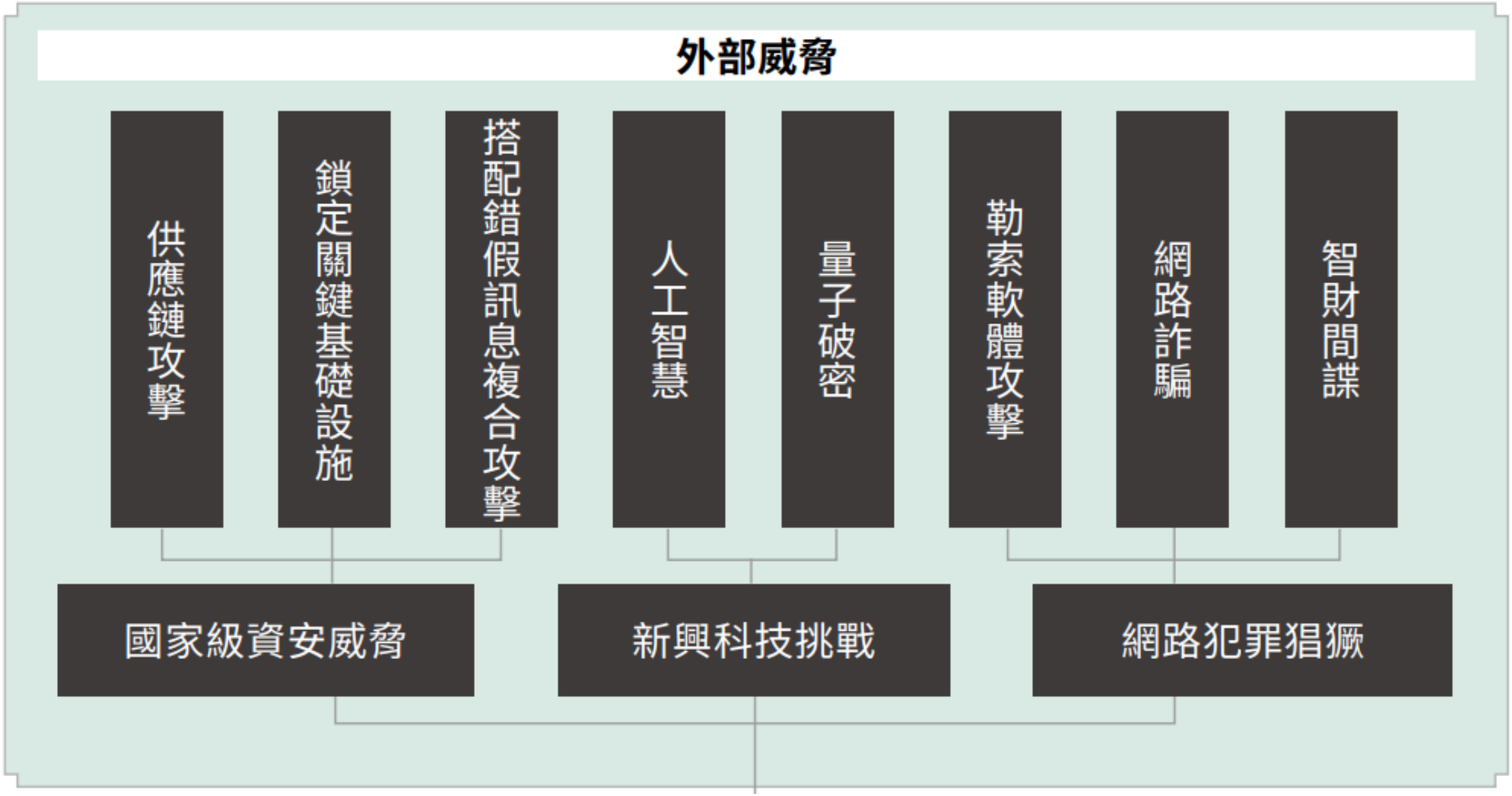
深化	**6. 鼓勵零信任網路部署**	4.2 擴大推動資安監控機制	3.1 金融核心資料保全
有效	5. 鼓勵資安監控與防護之有效性評估		3.2 對外服務營運持續實演練
聯防	8.1 提升資安情資分享動能	8.2 增進資安聯防運作效能	9 攻防演練及重大事件支援演訓

WEF Global Cybersecurity Outlook 2025



- 地緣政治緊張局勢
- 供應鏈相互依賴性
- AI 和新興技術
- 網路犯罪的複雜性
- 網路技能差距
- 監管要求

國家資通安全戰略 2005 – 資安即國安



國家資通安全戰略 2025

一、**跨支柱推行零信任架構**，強化公私部門機構的資通安全 認知和文化。
二、落實資安治理，建立備援並**有效保護公私部門資料**。
三、發展**後量子密碼**之資安防護架構與管理，推動公私部門 加速導入。

在能源、通訊、交通、金融、醫療等領域的關鍵基礎設施分別**制定並執行「資通安全行動方案」，強化其系統網路韌性**。
推動**第三方資安實兵演練及桌上兵推**，以測試及驗證資安防 禦與應變機制。

願景
打造堅韌、安全、可信賴的智慧國家

兩大準則
① 堅實資安治理機制及防護　② 戰略夥伴鏈結

四大支柱

Resilience ①	Infrastructure ②	Supply Chain ③	Emerging Technology ④
全社會防衛韌性	國土防衛與關鍵基礎設施	關鍵產業與供應鏈	人工智慧應用與安全

兩大基石

① 國家資安戰情協同應變中心

六塊基礎聯防體系
國安會｜國安局｜國防部｜調查局｜刑事局｜數發部

跨部會協防體系資源與支援
關鍵基礎設施主責部會｜國科會｜國發會｜相關業務主管部會等

公私協力國際合作｜民間資源與能量｜產學研合作

② 國家資通安全會報及資訊資安預算正規化

為強化供應鏈安全，具體策略做法是與產業公協會及其領導企業合作，**全面盤點關鍵產業、重要企業、供應鏈及其關鍵資源，建立風險管理清單，確保供應鏈的可視性與安全性**。在此基礎上，亦應**研擬符合各關鍵產業需求的「資通安全行動方案」**，並逐步擴大推行範圍，以提升產業資安治理能 力。

一、將 **AI 技術應用**於全社會防衛韌性、國土防衛與關鍵基 礎設施、關鍵產業及供應鏈的資安防護，並打造產業生態系。
二、確保 **AI 技術本身的安全性與可信任性**。

What's Next？資安不只是資安...

金融資安長-企業風險戰略 ???

■ 深化防禦：厚實資安基礎建設
- ➢ **推動零信任架構(ZTA)，提升資安防護基準**
- ➢ 雲地資安接軌，確保資安水準
- ➢ 持續強化備份備援機制，確保關鍵金融服務可用性
- ➢ 深化資安人才交流，協創典範實務(Best Practice)

■ 資安左移：從事後補救邁向早期預防
- ➢ 建構軟體安全流程，安全納入設計(Secure By Design)
- ➢ 強化供應鏈資安，健全金融資安生態系

■ 前瞻部署：因應新興科技挑戰
- ➢ 人工智慧(AI)強化效率，資安守護信任
- ➢ 盤查加密態勢，布局後量子密碼(PQC)遷移

MITRE公布遭駭細節及攻擊指標

2024 / 05 / 08

- MITRE公司公布近期遭網路攻擊的更多詳細資訊。最早的入侵證據可追溯到2023年12月31日。
- 利用Ivanti Connect Secure的兩個零日漏洞CVE-2023-46805及CVE-2024-21887，鎖定MITRE的實驗與研究網路環境NERVE(Networked Experimentation, Research, and Virtualization Environment)，竊取的**管理員帳號**，**最終控制MITRE的VMware基礎架構，並植入一種稱為BRICKSTORM的Golang後門程式，以及一個先前未公開的網路惡意腳本BEEFLUSH**。利用SSH操作與執行可疑指令等手法，維持對受侵系統的控制。
- 在這雙漏洞於2024年1月11日公開揭露的隔日，該威脅團體也部署了另一種稱為WIREFIRE(又名GIFTEDVISITOR)的惡意腳本，以建立隱密通訊並外洩資料。
- **駭客曾嘗試利用MITRE公司的其中一部網域控制站，橫向滲透MITRE的其他系統，但未能成功。**

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11081

BLOCK TEMPO
由社群而生的區塊鏈媒體

巴西央行1.4億鎂儲備金被駭！贓款換成比特幣、駭客成本僅2,760美元，服務供應商成破口

by Editor Jr. — 2025-07-05 in 犯罪

AA

據加密貨幣鏈上偵探 ZachXBT 7 月 4 日披露，2025 年 6 月 30 日，巴西央行服務供應商 C&M Software 慘遭駭客攻擊，六家銀行的央行準備金帳戶瞬間被轉走約 1.4 億美元。

然而，駭客只付出約 2,760 美元，便從一名員工手中買到登入憑證，輕取金融中樞大門鑰匙。ZachXBT 強調，這是今年「最令人震驚的案件之一」，卻在巴西以外鮮少獲得關注。

低成本滲透，高額失血

據了解，C&M Software 負責串接銀行與巴西央行支付基礎設施，包括即時支付系統 Pix。員工帳密外流後，駭客直接操控了平台介面，把資金自六家銀行的央行帳戶轉出，合計 8 億雷亞爾。具體細節包括：

- 目標帳戶：攻擊鎖定約五至六家小型金融機構在巴西央行的儲備帳戶，這些帳戶專用於銀行間結算，直接由央行託管，涉及巨額資金。
- 攻擊執行：駭客通過未經授權的訪問，操縱 C&M Software 的系統，執行非法轉帳。攻擊利用了C&M Software 作為第三方服務商的關鍵角色，直接連通巴西央行與金融機構的資金流。
- 損失金額：部分報導估計損失高達 10 億雷亞尔（約 1.8 億美元），但路透社援引匿名官員表示，實際損失可能低於此數額，且未涉及客戶直接資金損失。

https://www.blocktempo.com/cm-software-hit-by-cyberattack/

金融監督管理委員會
Financial Supervisory Commission

金融業導入零信任架構參考指引

2024.7.15

金融零信任架構推動路徑

導入參考指引

行政指導：金融機構於導入實務仍得考量既有資訊與資安環境、資安防護水準、資源及人力、業務風險、相關解決方案成熟度等因素調適；或另為適切之規劃，不以本參考指引為限。

實務案例分享

鼓勵金融機構分享實務案例，供金融同業交流研討最佳實務，帶動持續深化及擴散。

資安基礎規範

定期調查導入規劃及進程，與各同業公會、周邊單位共同依據對各金融業別屬性、規模及業務風險等，衡量實際資安防護需求及執行可達性，適時納入資安規範，提升整體資安防禦水準。

美國政府- 2024零信任安全目標 (2022.1.26發布)

沒有任何參與者、系統、網路或服務是可靠的，因而必須驗證任何試圖建立存取權限的事物

- **身分**：員工應該擁有**大型企業等級的受管帳號**，以讓他們得以存取工作上所需資料，同時提供可靠的資安保護，避免遭到針對性且複雜的網釣攻擊
- **設備**：員工的工作設備也將持續受到追蹤與監控，並在賦予造訪權限時考量這些**設備的安全狀態**
- **網路**：各個聯邦機構的系統是相互**隔離**的，彼此間互動的流量則是**加密**的
- **應用**：需經**內部與外部的測試**，並可安全地藉由網路提供給員工
- **資料**：各個資安及資料團隊必須合作建立**資料類別及安全規則**，以偵測及封鎖未經授權的資訊存取

美國國防部 2022年11月 發布零信任框架與藍圖，預計於 2027年 完成零信任部署

November 29, 2023

NYDFS Finalizes Significant Amendment to Part 500 Cybersecurity Regulation

更明確資安長權責並賦予執行彈性

- 授權資安長可就規範中滯礙難行部分，核定另採相當之控制或補償措施

擴及第三方服務供應商

- 於資安事件通報、營運持續及災難復原計畫等範圍，擴及第三方服務供應商，要求明確識別及相關影響評估

資訊系統自防護邊界內部及外部執行滲透測試

V

- 強調亦從資訊系統邊界內部執行滲透測試以防範內部攻擊事件發動攻擊

全面實施多因子身分驗證

V

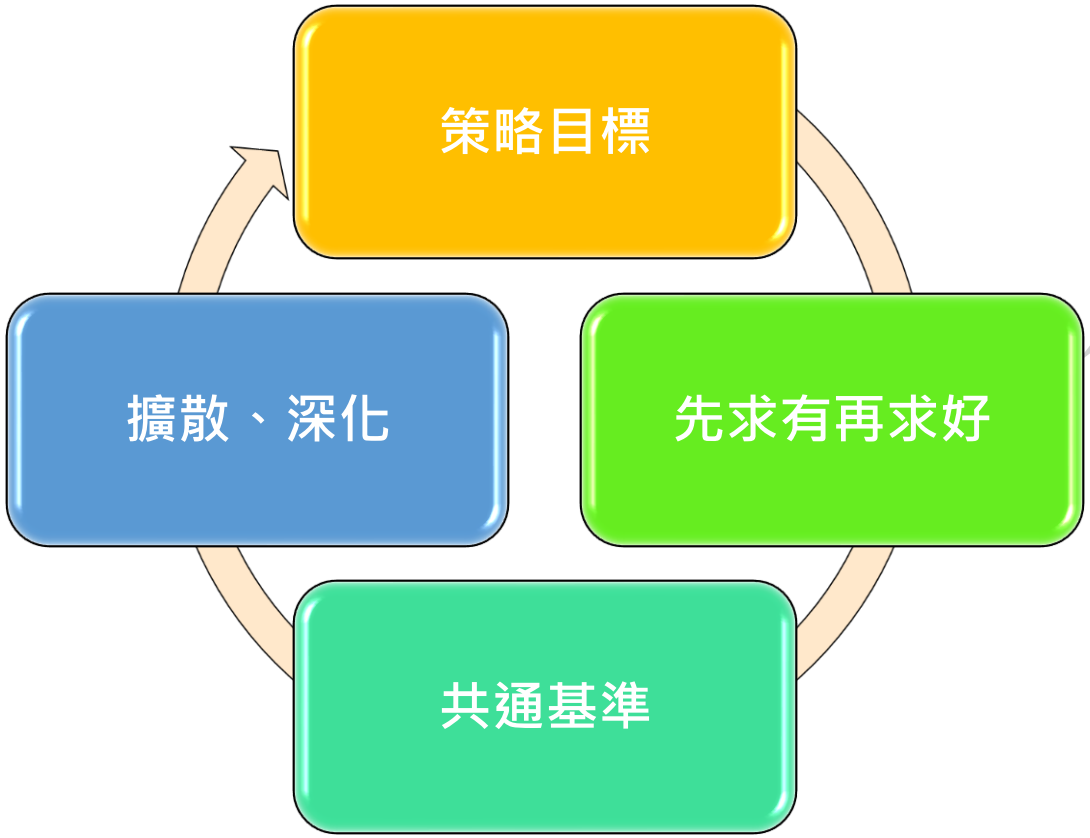
- 組織內任何人存取任何資訊系統皆須採雙因子認證

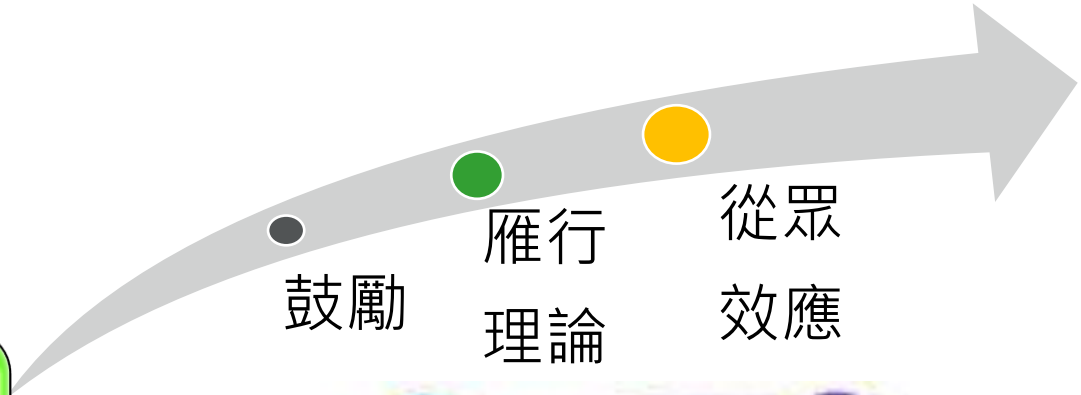
NYDFS Part 500 最終要求將於 2025年11月1日生效

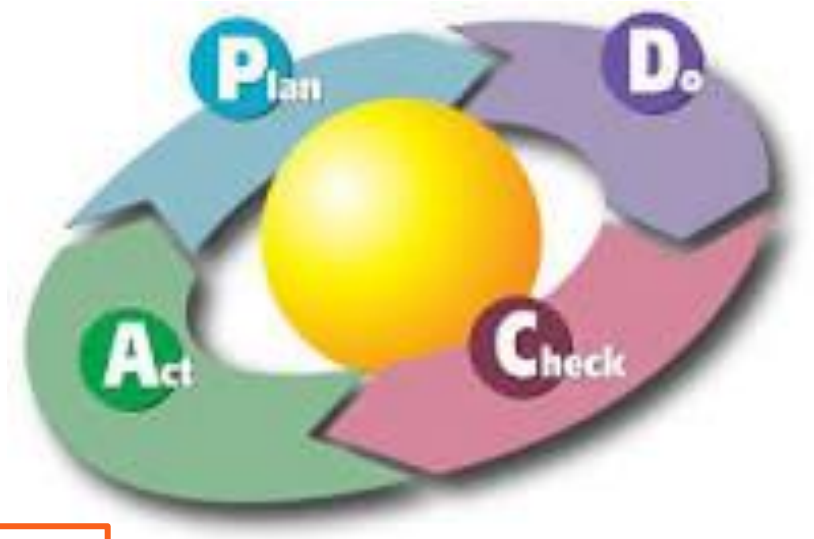
- 所有受規範金融機構，必須對組織內任何可存取資訊系統人員實施加強版MFA (Part 500.12)
- **[例外]**：依Part 500.19(a)符合有限豁免之小型企業，必須對以下情境採用MFA：
  - 遠端存取其資訊系統
  - 遠端存取第三方應用程式
  - 所有具特權帳號(不包括禁止互動登入之服務帳號)
- IT服務台人員遭受社會工程攻擊的事件日益增多：NYDFS觀察到，近期**駭客者透過非法遠端存取資訊系統來操縱服務台人員的事件增加。他們誘騙服務台人員重置多因素身份驗證（MFA）令牌或更改密碼**。當威脅行為者偽裝成內部IT專業人員和/或使用來電顯示欺騙技術時，這些攻擊更難被發現。各組織應提醒所有相關人員注意這些威脅，審查並加強身分驗證協議，**監控異常行為**，並進行模擬社交工程攻擊演練以培訓員工。

https://www.leadingageny.org/providers/ccrc/ccrc-policy-and-legislative/dfs-cybersecurity-regulation-updates/

推動、檢討與精進 - 從共通基準邁向策略目標





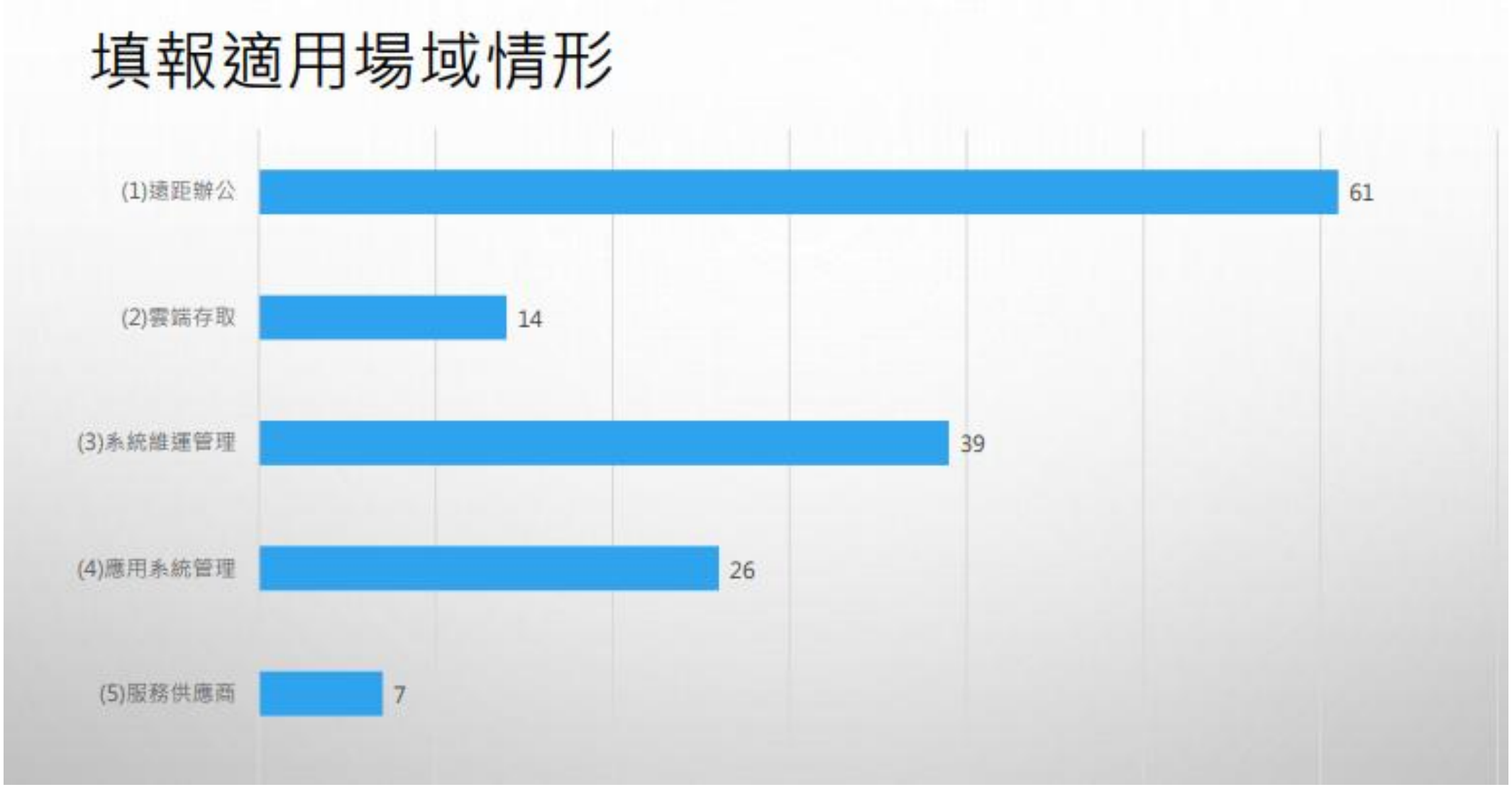


- 遠端存取其資訊系統
- 遠端存取第三方應用程式
- 所有具特權帳號(不包括禁止互動登入之服務帳號)

風險導向->擇高風險場域先行[例舉]

遠距辦公	• 使用者及設備位於**傳統資安防護邊境外**
雲端存取	• 雲端資源位於**傳統資安防護邊境外**
系統維運管理	• 含重要**主機設備及系統軟體**(作業系統、資料庫等)之**特權帳號**管理
應用系統管理	• 重要**應用系統之管理者**(如帳號管理員)或**高權限使用者帳號**(如可接觸大量個資或機敏資料使用者)
服務供應商	• 如委外廠商之**遠端維運**管理
跨機構協作	• 如重要應用系統開放予**外部使用者**從外部存取，其人員到離或使用設備非屬本機構管控範圍者。

114年-上半年問卷調查



循序漸進->依分級指標分階段導入

Ⅰ 傳統

靜態指標

- **RBAC 基於角色存取控制**
- 優先盤點既有資安防護機制之完整性，規劃**防禦深度之優化及整合**。

Ⅱ 起始

動態指標

- **ABAC 基於屬性存取控制**
- 將**動態屬性(如時間、地點, 設備合規性等)**納為授權審核條件，動態撤銷、限縮存取授權或發出告警。

Ⅲ 進階

即時指標

- **SIEM/SOC**
- 整合或收容事件日誌，建立定期審查及異常行為**(IOC、Mitre ATT&CK TTP)**之偵測、告警及回應機制。
- **UEBA** 使用者和實體行為分析。

Ⅳ最佳

整合指標

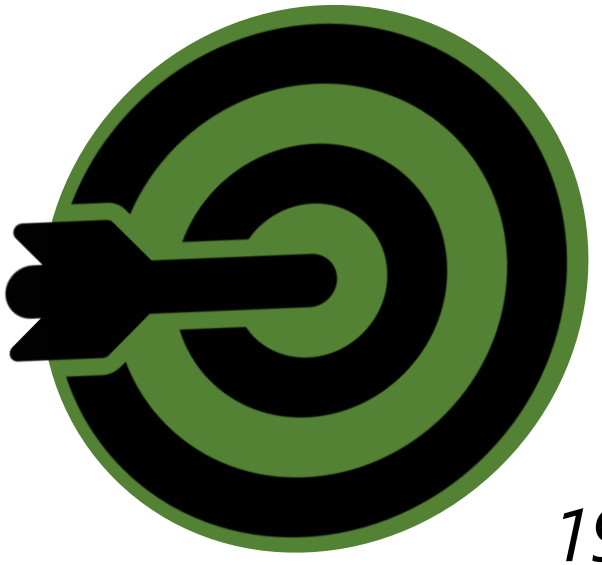
- 建立可依資安政策快速調適之一致性且自動化之管理機制，確保安全性及合規性。
- **點►線►面**

永不信任、持續驗證

問題討論：金融零信任架構-推進戰略

成熟度	場域(A)	標的	推進
I	遠距辦公	Pilot	深化
II	系統維護	關鍵核心	擴散
III	服務供應商		

場域(B)	影響
雲端服務	高風險、低衝擊
應用系統管理	高風險、高衝擊
跨機構協昨	

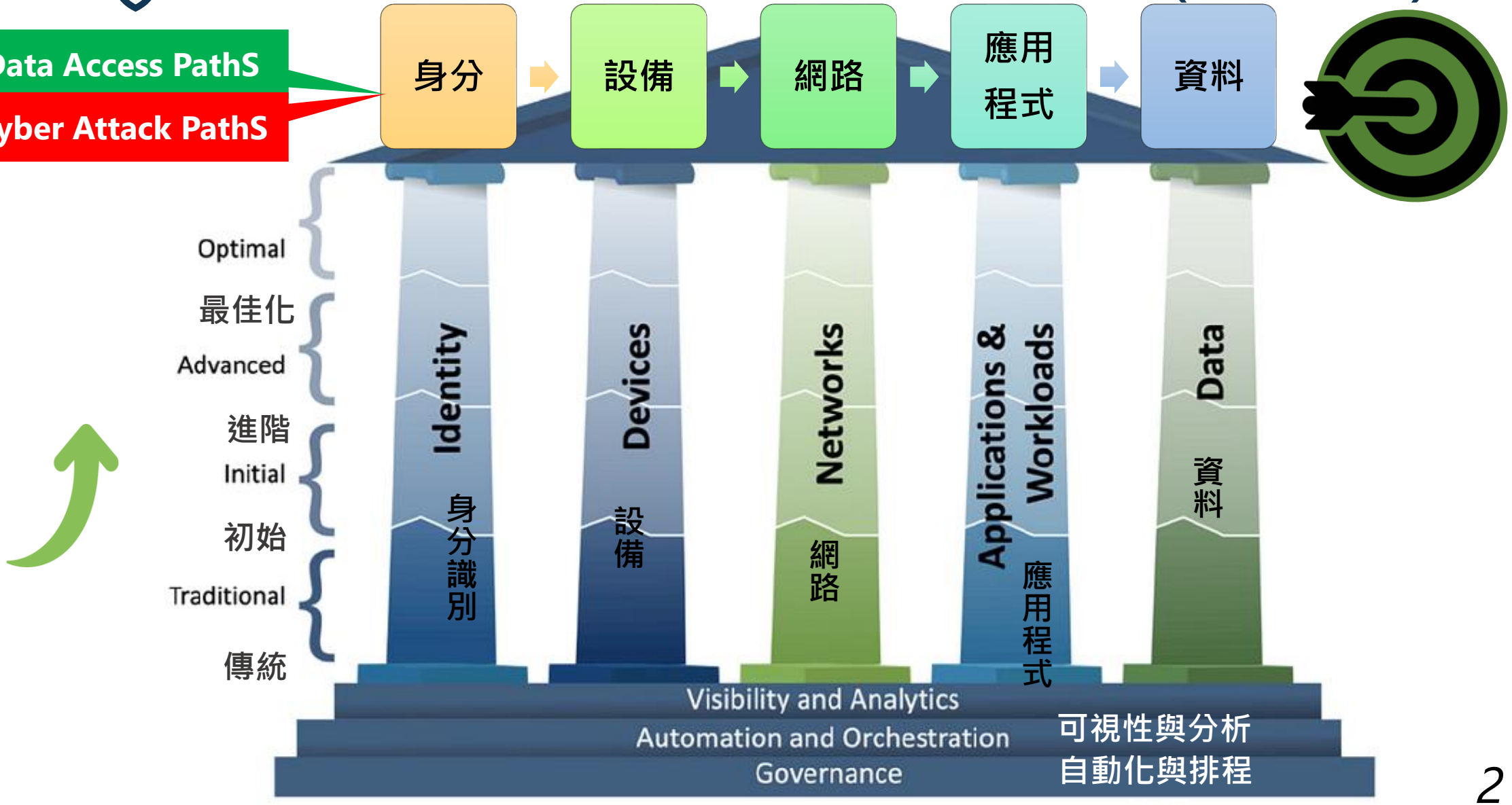


實作案例分享

美國網路安全暨基礎設施安全局(CISA)
零信任成熟度模型2.0 (2023.4發布)

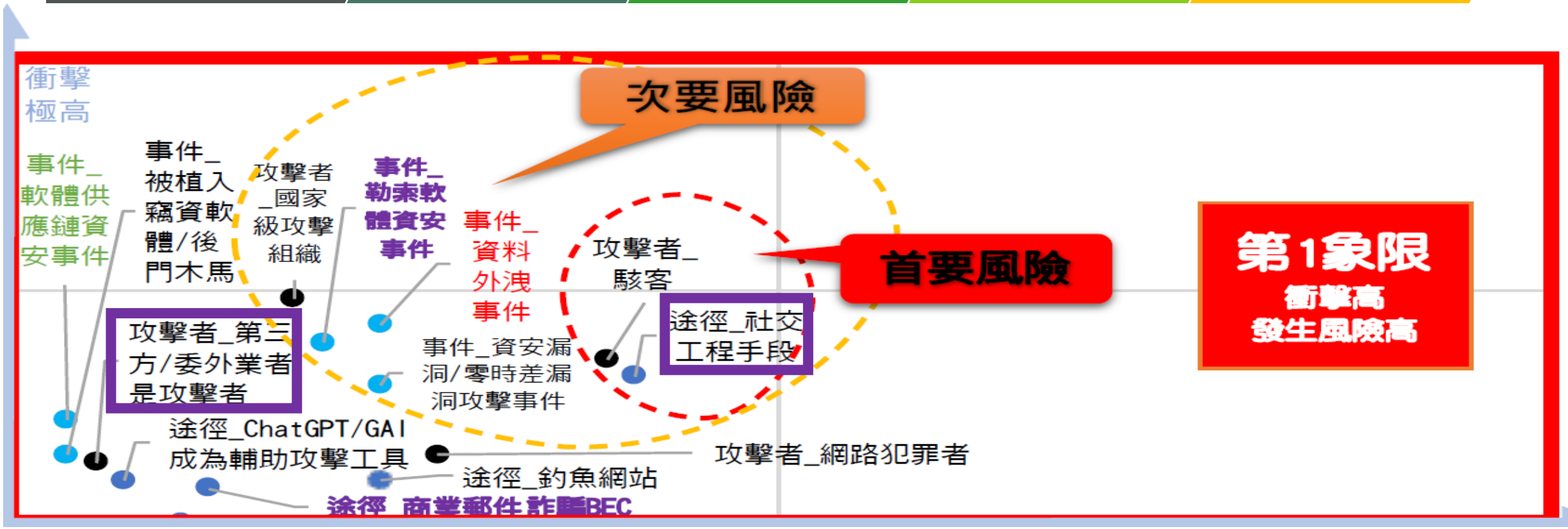
Data Access PathS

Cyber Attack PathS



零信任核心->從核心資料盤點存取路徑及防護邊界

身分	設備	網路	應用程式	資料
• 帳密外洩 • 社交工程	• 木馬程式 • 零時差	• 封包竊聽 • 橫向擴散	• 漏洞攻擊 • 帳號提權	• 加密勒索 • 資料外洩



盤點資源存取途徑->以零信任思維深化資安防護

產品？

身分	設備	網路	應用程式	資料
●**雙因子**身分驗證 ●優先選擇**安全強度較高、可抗網路釣魚者** ➢具數字配對APP ➢FidO ➢晶片卡 ●**動態屬性存取授權** ●**身分活動即時偵測及回應** ⋮	●可識別為**已納管**之設備 ●具設備**健康合規性**管理 ➢作業系統更新 ➢防毒軟體病毒碼更新 ●**動態屬性存取授權** ●**設備活動即時偵測及回應** ⋮	●全程**加密傳輸** ●具適當**網段分割**，採最小需求原則的網路連線 ➢建議採各系統獨立之網段區隔 ●**網路活動即時偵測及回應** ⋮	●包含源自**內部與外部的安全性檢測** ●採**最小授權原則** ●**動態屬性存取授權** ●**應用程式活動即時偵測及回應** ⋮	• 機敏性**資料加密儲存** • 支援最小授權規則 • **資料外洩防護** • **動態屬性存取授權** • **資料存取活動即時偵測及回應** ⋮

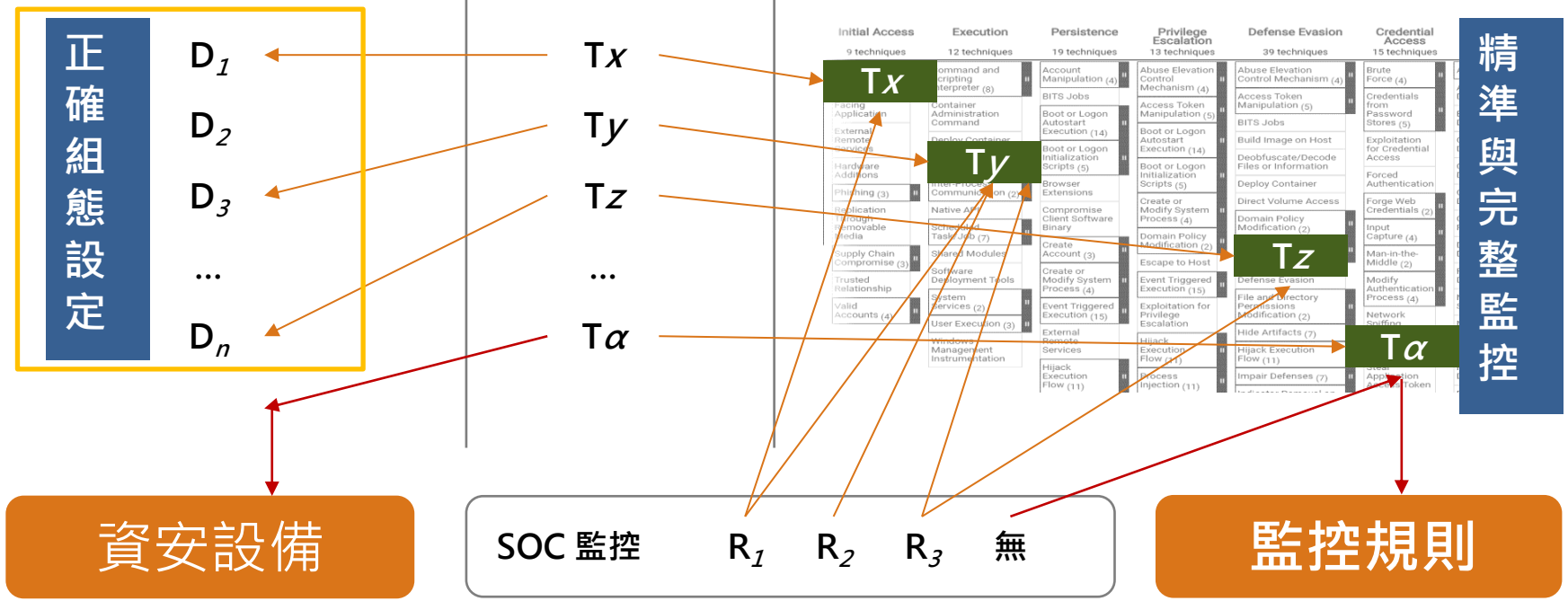
日誌收集　日誌與事件管理　資安監控/事件應處

資安監控與防護之有效性

偵測與防禦視角
（偵測、阻擋覆蓋率）

金融
APT Group

攻擊視角
(SOC可見度覆蓋率)
MITRE ATT&CK Matrix



- 運用 DeTT&CT 防禦方法論，將金融機構常用之資安、網路、應用系統等設備，映射至MITRE ATT&CK蒐整的網路攻擊手法，針對所對應到的攻擊技術，研析其特徵與手法，產出相對應之監控平台(SIEM)的金融機構資安監控規則

駭客組織攻擊手法 → 資安設備組態設定 → 異常樣態偵測告警 → 監控規則關聯分析 → 事件單作業指引

攻擊手法與可監控設備對應（節錄）

項次	ID	攻擊手法	Windows	Linux	AV	FW	IPS	WAF	Router	Switch	網域控制台	DNS	網站應用系統	資料庫系統
1	T1001	Data Obfuscation				V	V							
2	T1003	OS Credential Dumping	V	V		V		V						
3	T1005	Data from Local System	V					V						
4	T1008	Fallback Channels			V	V	V							
16	T1040	Network Sniffing				V	V		V	V				
24	T1056	Input Capture			V	V	V	V					V	
44	T1110	Brute Force	V	V		V	V	V	V	V				V
80	T1491	Defacement				V		V					V	
82	T1498	Network Denial of Service				V	V	V						
83	T1505	Server Software Component				V		V					V	

與各設備原廠合作，
核對、增修可監控設備與方式

支援金融資安監控組態設備(~2024.12.31)

項次	種類	系統設備類別	廠牌
1	電腦作業系統	Windows 伺服器作業系統	Windows server 2012 R2
			Windows server 2016
			Windows server 2019
			Windows server 2022
		Red Hat Linux	Red Hat 7
			Red Hat 8
			Red Hat 9
2	網路設備	路由器	Cisco
			Vanguard Network
		交換器	Cisco
			HP
		負載平衡設備	F5
3	應用系統	網域控制台	Windows
		網域名稱系統	Windows DNS
			F5
		網站應用系統	IIS
			Apache
		資料庫系統	Microsoft SQL Server
			IBM DB2
			Oracle

項次	種類	系統設備類別	廠牌
4	資安防護設備		Symantec
		防火牆	Fortinet
			Check Point
		入侵偵測防禦系統	Cisco
			McAfee
			TippingPoint(113新增)
		Web應用程式防火牆	F5
			Citrix
			Imperva
			Arkamai AAP
		端點防護	TeamT5
			Cycraft
			SentinelOne (113新增)
		網路偵測與回應	ExtraHop
			DarkTrace (113新增)
		郵件閘道防護	SPAM SQR (113新增)
		服務阻斷防護	Arbor (113新增)
5	日誌收集	安全性資訊與事件管理SIEM系統	ArcSight
			IBM QRadar
			Splunk

場域-雲端服務資安接軌

責任共治模型 - 雲地整合的破口？

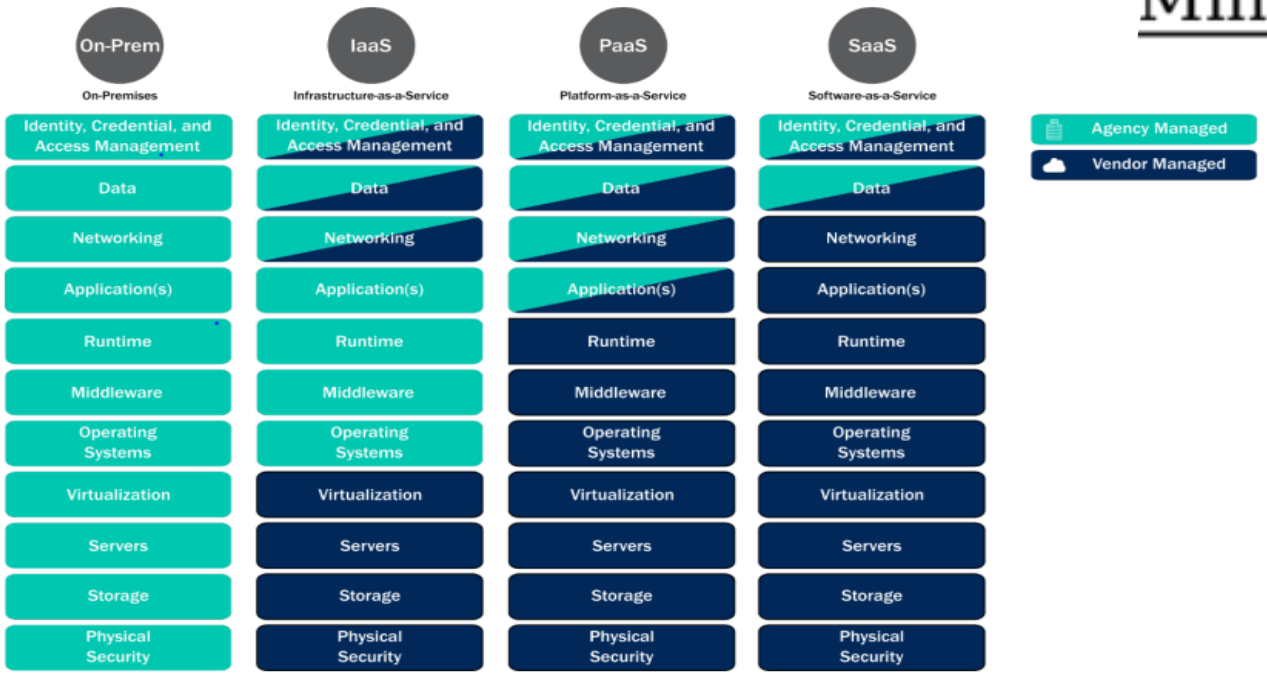
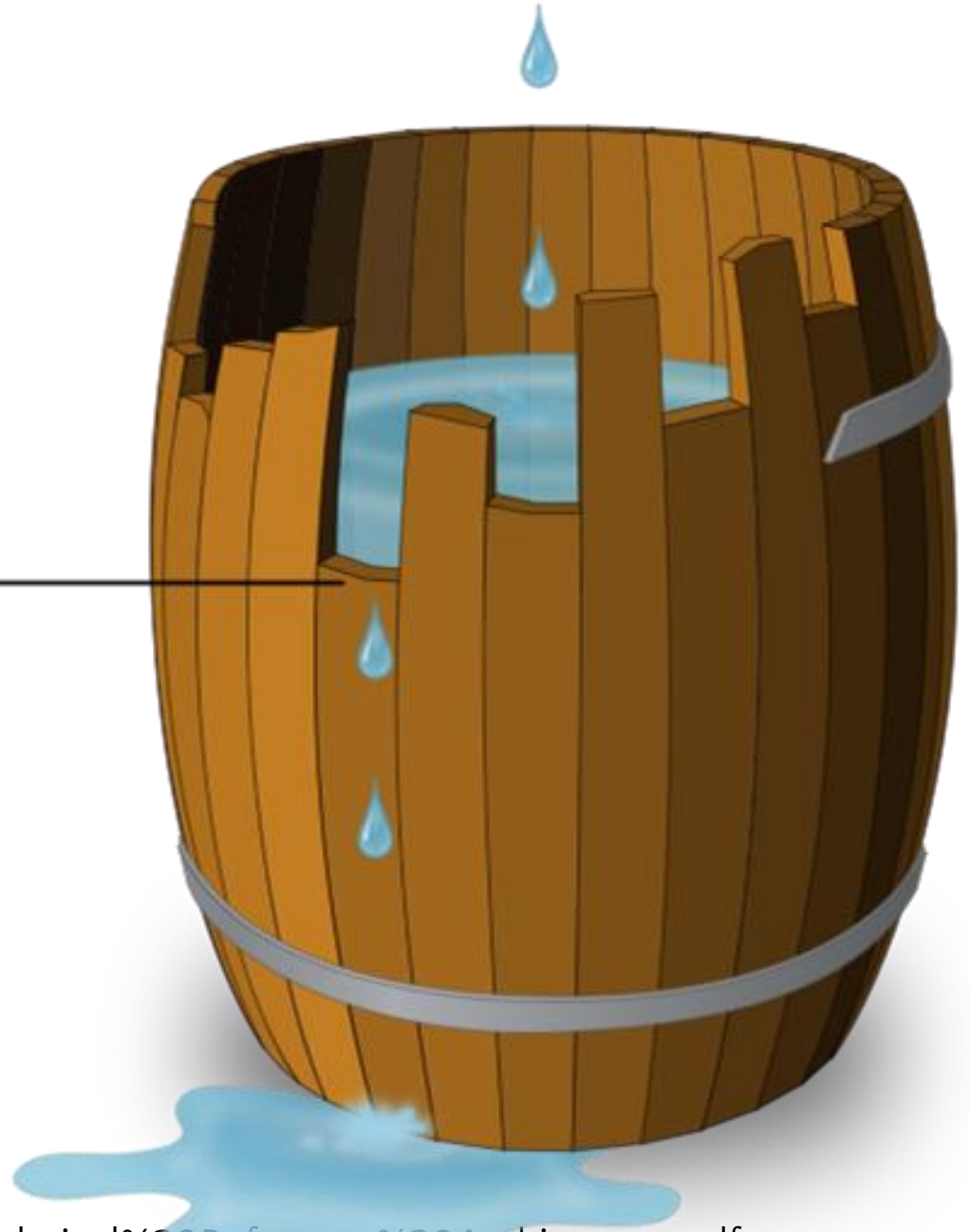


Figure 2: Responsibilities for Different Service Models



https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architec

MATRICES

- Enterprise
  - PRE
  - Windows
  - macOS
  - Linux
  - Cloud
    - Office Suite
    - Identity Provider
    - SaaS
    - IaaS
  - Network Devices
  - Containers
  - ESXi
- Mobile
- ICS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	5 techniques	8 techniques	5 techniques	14 techniques	11 techniques	14 techniques	5 techniques	5 techniques	3 techniques	10 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protocol	Account Access Removal
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Cloud Application Integration	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)	Data from Cloud Storage	Exfiltration Over Web Service (1)	Data Destruction (1)
Phishing (2)	Serverless Execution	Create Account (1)	Domain or Tenant Policy Modification (1)	Email Spoofing	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools	Data from Information Repositories (5)	Transfer Data to Cloud Account	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Event Triggered Execution	Event Triggered Execution	Exploitation for Defense Evasion	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data Staged (1)		Defacement (1)
Valid Accounts (2)	User Execution (1)	Implant Internal Image	Valid Accounts (2)	Hide Artifacts (1)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)	Email Collection (2)		Email Bombing
		Modify Authentication Process (3)		Impair Defenses (3)	Multi-Factor Authentication Request Generation	Log Enumeration				Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Network Sniffing	Network Service Discovery				Financial Theft
		Valid Accounts (2)		Indicator Removal (1)	Steal Application Access Token	Network Sniffing				Inhibit System Recovery
				Modify Authentication Process (3)	Steal or Forge Authentication Certificates	Password Policy Discovery				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal Web Session Cookie	Permission Groups Discovery (1)				Resource Hijacking (4)
				Modify Cloud Resource Hierarchy	Unsecured Credentials (3)	Software Discovery (1)				
				Unused/Unsupported Cloud Regions		System Information Discovery				
				Use Alternate Authentication Material (2)		System Location Discovery				
				Valid Accounts (2)		System Network Connections Discovery				

TREND | 企業 解決方案

最常導致資安事件的雲端組態設定錯誤

https://www.trendmicro.com/zh_tw/research/22/c/the-most-common-cloud-misconfigurations-that-could-lead-to-secur.html

組態設定錯誤看似單純且可避免，但卻是目前雲端環境最常見的一項風險。事實上，有 65% 至 70% 的雲端資安挑戰都是因為組態設定錯誤而引起。雲端包含了各式各樣的設定、政策、資產，以及環環相扣的服務和資源，這使得雲端變成一個非常複雜的環境，不但難以理解透徹，也不容易正確設定。一些因為遠距上班需求而被迫迅速移轉至雲端的企業更是如此。不幸的是，當企業太快導入新的技術卻沒有完全掌握其複雜性時，組態設定錯誤就在所難免。

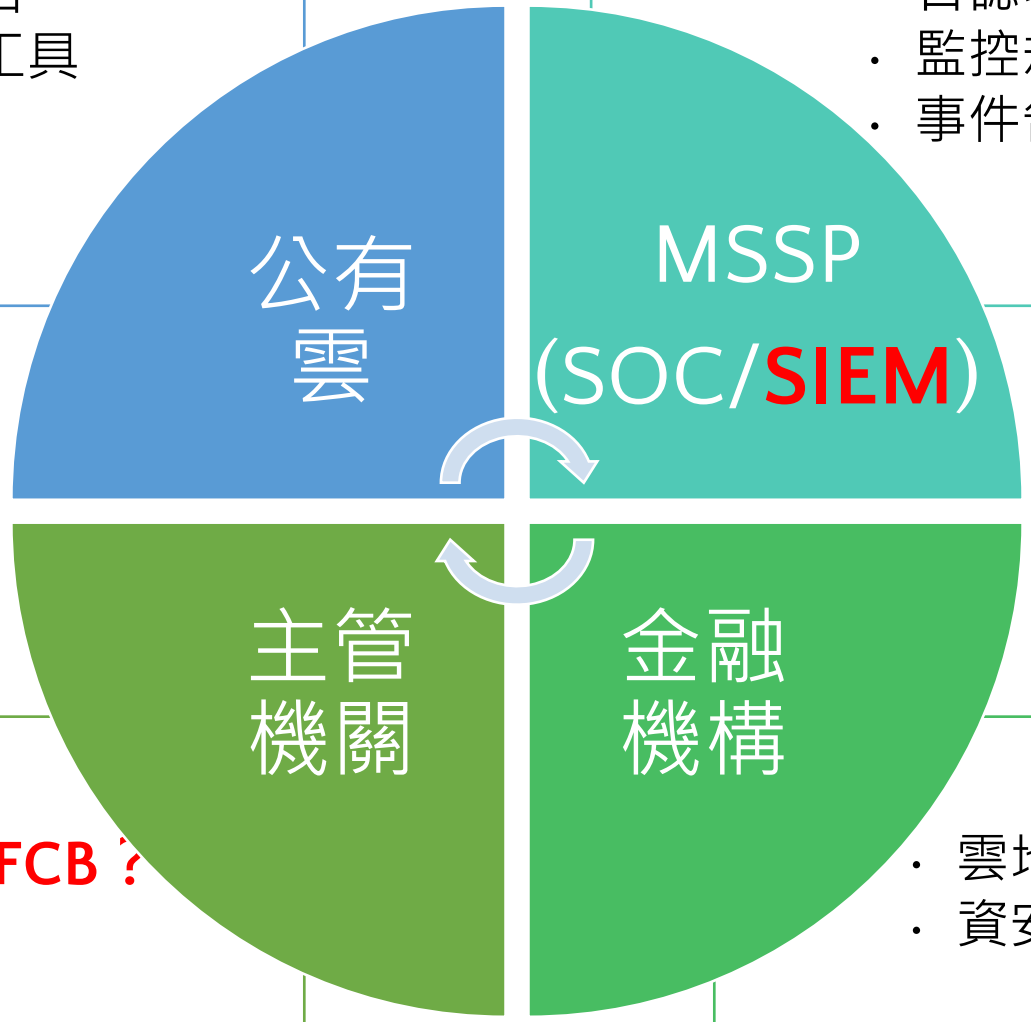
由於組態設定錯誤有可能成為駭客攻擊利用的途徑，因此很可能導致嚴重後果，這也是近年許多大型資安事件背後的元凶。2018 和 2019 年間，因雲端組態設定錯誤而引起的資安事件造成了將近 5 兆美元的企業損失。2020 年，全球化妝品品牌 Estee Lauder (雅詩蘭黛) 外洩了 4.4 億筆資料，其中包含了使用者電子郵件地址，以及稽核、錯誤、CMS、中介軟體、生產線等記錄檔，全都只因為某個資料庫未正確設定密碼所致。2020 年，成人網站 CAM4 意外洩漏了108.8 億筆資料，其中包含了使用者的個人身分識別資訊 (PII)、付款記錄以及密碼雜湊碼，同樣也是因為某個 Elastic Search 資料庫未設定安全防護所引起。

TREND MICRO

從地端到雲端

- 共通平台
- 雲原生工具
  - ➢SIEM
  - ➢**CSPM**
  - ➢**CWPP**

- 日誌收集
- 監控規則
- 事件告警



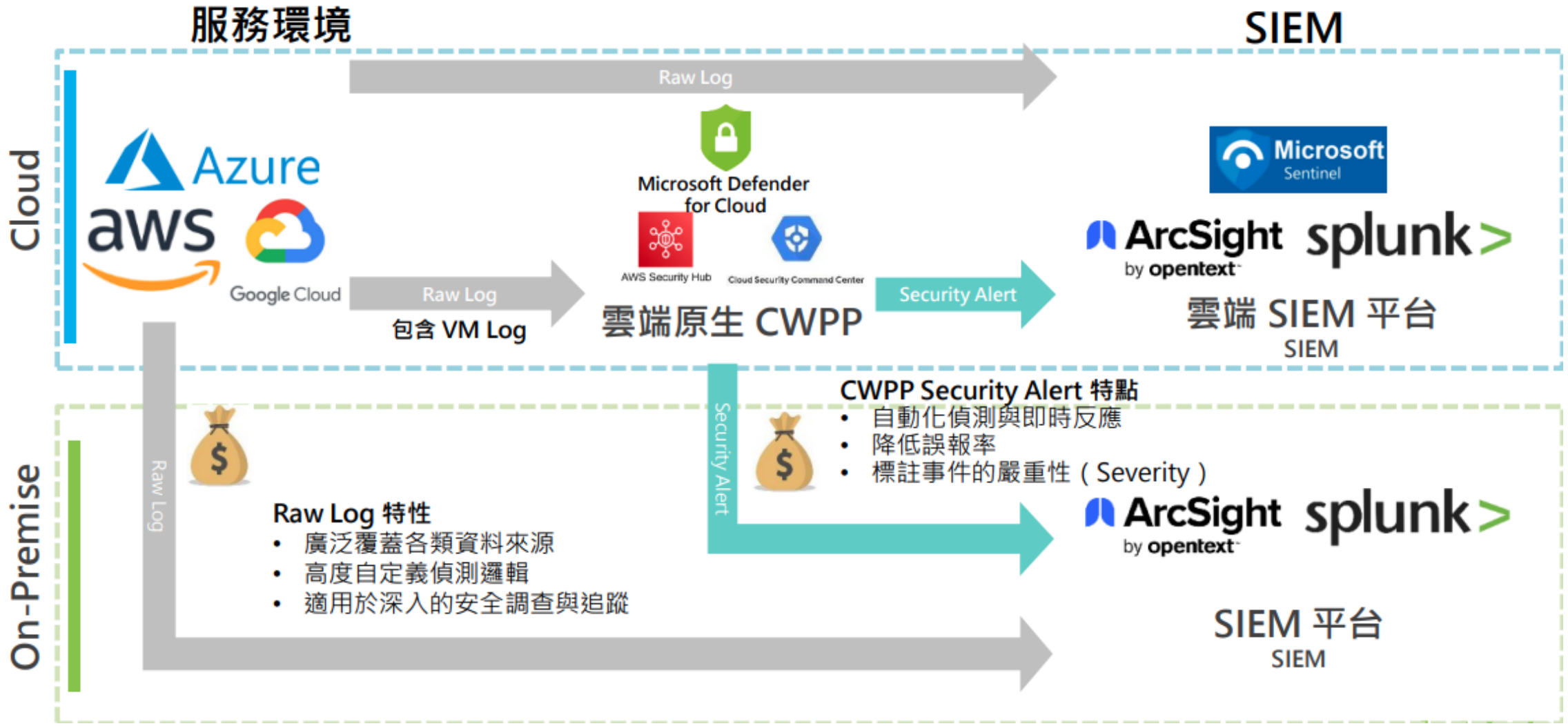
CIS Center for Internet Security

MITRE | ATT&CK

- **Cloud FCB ?**
- **Cloud MCB ?**

- 雲地整合
- 資安基準

雲端監控日誌蒐集/雲地監控架構整合



金融雲端資安監控基準 – 成果驗證

界定研究範圍

雲端安全組態基準
CIS Cloud Security Foundations 基準與 CSP 最佳實作

駭客攻擊手法
MITRE ATT&CK Cloud Matrix 共計 69 種攻擊手法

資通/資安設備
4 個 OS、12 個雲服務
13 個網路安全設備
3 個 SIEM 平台

雲端安全監控標準
AWS、GCP、Azure 三大公有雲 CIS Foundations 基準

制定金融雲端資安監控基準

研析駭客攻擊手法 → 比對安全組態基準 → 關聯對照 CSPM

雲端服務資安組態基準

研析駭客攻擊手法 → 制定監控規則與設定 ← 雲端安全監控標準補充

SOC 監控規則

SOC 監控設定

驗證雲端 MCB 有效性

環境部署
測試環境部署
BAS 系統部署

雲端監控基準部署
SOC 監控規則部署
SOC 監控設定部署

BAS 攻擊驗證
Security BAS
涵蓋 42 種攻擊手法

人工攻擊驗證
專業攻擊團隊
涵蓋 69 種攻擊手法

金融雲端資安監控基準—雲端基礎服務

帳號管理

- Microsoft Entra ID
- AWS IAM
- GCP IAM

靜態資料儲存

- Azure Blob Storage
- Amazon S3
- Cloud Storage

託管虛擬機

- Virtual Machines
- Amazon EC2
- Compute Engine

稽核紀錄

- Azure Monitor Activity Logs
- AWS CloudTrail
- Cloud Audit Logs

Serverless

- Azure Functions
- AWS Lambda
- Google Cloud Function

機密與金鑰管理

- Azure Key Vault
- AWS Secrets Manager/ Parameter Store / AWS KMS
- GCP Secret Manager

金融雲端資安監控基準—資通/資安設備

電腦作業系統

項目	平台	名稱
Windows 作業系統	Azure	Windows server 2016 Windows server 2019
	AWS	
	GCP	
Linux 作業系統	Azure	Redhat Enterprise Linux 7 Redhat Enterprise Linux 8
	AWS	
	GCP	

SaaS

項目	平台	名稱
SaaS	Microsoft	Office365 (IAM 為主)
	Google	Workspace (IAM 為主)

網路安全設備

項目	平台	名稱
Firewall	Azure	Azure Firewall
	AWS	AWS Network Firewall
	GCP	Cloud Firewall
WAF	Azure	Azure Web Application Firewall
	AWS	AWS WAF
	GCP	Cloud Armor
IPS	Azure	Azure Firewall
	AWS	AWS Network Firewall
	GCP	Cloud Next Generation Firewall
AV	Azure	Trend Micro Apex One (IaaS 為主)
	AWS	
	GCP	

CSPM/CWPP

項目	平台	名稱
雲端資安態勢管理(CSPM) / 雲端工作負載保護平台 (CWPP)	Azure	Microsoft Defender for Cloud
	AWS	Security Hub
	GCP	Security Command Center

SIEM

項目	平台	名稱
日誌收集 (安全性資訊與事件管理 SIEM)	地端	ArcSight
		Splunk
	Azure	Sentinel

金融雲端資安監控基準

114 推廣試行

監控基準報告書（監控規則）

攻擊手法	Technique$_1$	Technique$_2$	…	Technique$_{69}$
可監控設備與邏輯	T$_1$對應 Windows	T$_2$對應 Windows	…	T$_{69}$對應 Windows
	T$_1$ 對應 WAF	T$_2$ 對應 WAF	…	T$_{69}$對應 WAF
	…	…	…	…
	T$_1$ 對應 FW	T$_2$ 對應 FW	…	T$_{69}$ 對應 FW
監控規則	ArcSight Rules	ArcSight Rules	…	ArcSight Rules
	Splunk Rules	Splunk Rules	…	Splunk Rules
	Sentinel Rules	Sentinel Rules	…	Sentinel Rules
組態	T$_1$ 對應組態基準	T$_2$ 對應組態基準	…	T$_{69}$ 對應組態基準

駭客雲端攻擊手法

監控設定手冊

監控設備設定方式

Windows Server 2016
Microsoft Azure WAF
…
AWS Network Firewall

- 監控設備應啟用哪些功能？
- 啟用哪些偵測規則？
- 是否需撰寫客製偵測規則？(人/事/時/地/物)

雲服務組態基準

人工智慧 in 資訊安全 - 傳統 初始 進階 最佳

威脅偵測與入侵預警（Threat Detection & Prediction）

應用：AI 模型分析網路封包、系統日誌、終端行為，找出異常行為或潛藏威脅。

技術：機器學習 + 行為分析（UEBA、NBAD）

AI 驅動的電子郵件與社交工程防護

應用：AI 分析郵件內容、結構、發件行為，辨識釣魚信、BEC 攻擊（商業電郵詐騙）。

技術：自然語言處理（NLP）、語意相似度分析、圖神經網路

自動化事件處理與威脅回應（SOAR）

應用：AI 協助自動化處理資安事件，包括隔離設備、阻擋流量、通報分析。

技術：強化學習 + 事件決策模型

惡意程式與異常行為分析（Malware & Insider Threats）

應用：AI 分析二進位檔案、程式執行行為、記憶體特徵，辨識新型態惡意程式或內部濫用。

技術：深度學習（CNN/RNN）、特徵萃取與行為建模

資安風險預測與脆弱性管理（Predictive Risk Scoring）

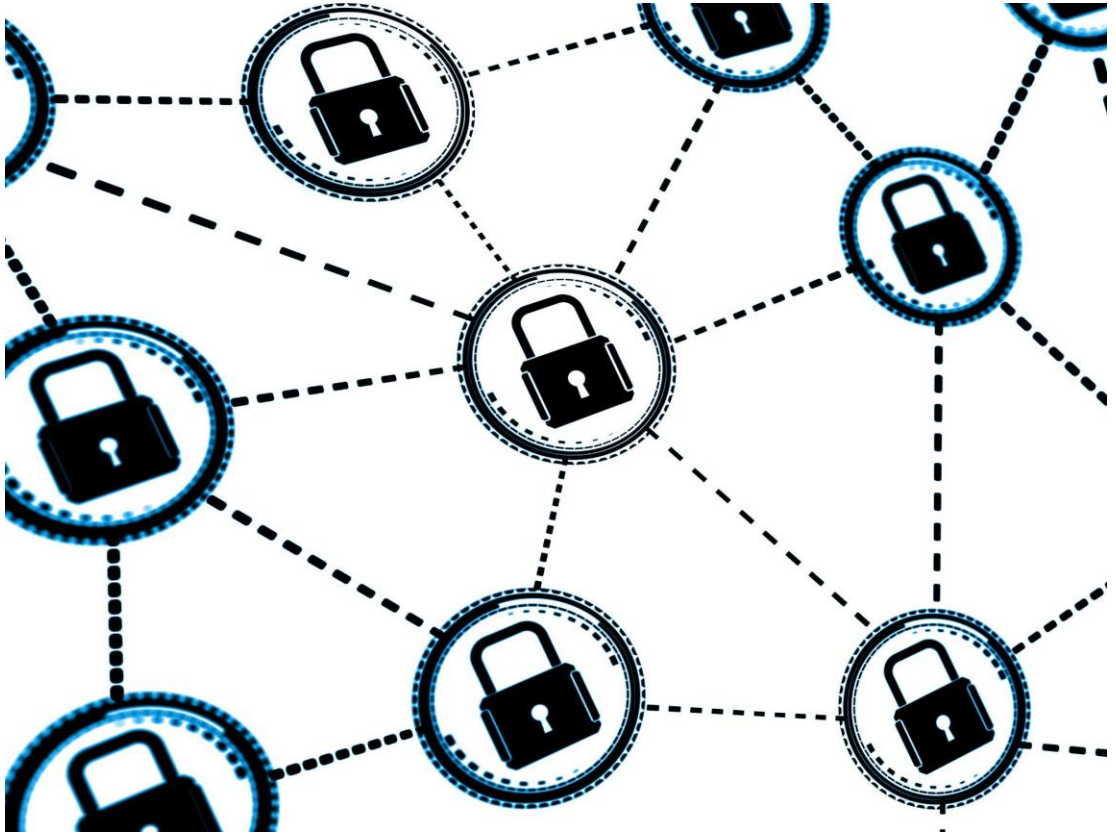
應用：AI 預測哪些系統或資產最容易被攻擊，提供優先修補建議。

技術：機器學習 + 攻擊路徑模擬（Attack Graph）

生成安全規則與補丁（AI for DevSecOps）

應用：AI 協助自動撰寫安全防火牆規則、YARA 規則、修補程式建議等。

技術：大語言模型（LLM）、程式碼分析模型



零信任心法

NIST 800–27 Operative Definition:
Zero trust (ZT) provides **a collection of concepts and ideas** designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised.

感謝聆聽

附表

零信任架構實作參考原則
分級表

身分

項次	功能	原則	等級
1.1	身分認證	採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險。	I
1.2	身分認證	採用包含綁定實體載具(如FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對APP等，排除簡訊、語音及電子郵件OTP)的多因子驗證機制，可抗網路釣魚風險	II
1.3	身分互通	對外部使用者(如服務供應商或跨機構協作)提供或採用不低於內部使用者信賴等級之身分鑑別機制。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I
1.4	身分互通	如具多元身分鑑別機制且有互通之必要，其信賴等級應具一致性之標準。(參照 ISO 29115 評估身分登錄、信物管理與身分驗證三階段)	I
1.5	權限存取	完成身分鑑別後，除依角色屬性存取控制(RBAC)落實最小授權原則外，並具基於屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點等)納為授權審核條件，**動態撤銷、限縮存取授權或即時告警**。	II
1.6	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單或SOAR Playbook等)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III
1.7	自動化治理	建立可依資安政策快速調適之一致性且自動化之管理機制，確保於帳號生命週期之安全性及合規性。	IV

設備

項次	功能	原則	等級
2.1	設備合規	具有效盤點且可唯一識別(如TPM等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制。	I
2.2	設備合規	具納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。	II
2.3	供應鏈風險	對外部設備(如BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之合規中繼閘道(如VDI等)存取。	I
2.4	資源存取	可將設備之動態屬性(如是否納管及合規、設備位址、或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，**動態撤銷、限縮存取授權或即時告警**；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼閘道(如VDI等)存取。	II
2.5	威脅防護	對設備活動紀錄具有即時偵測及回應機制(EDR)，在偵測到威脅指標(IOC)時，可自動隔離或即時應處(如發出事件單即時追蹤處置)。	III
2.6	可視化分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與應處(如事件單、SOAR Playbook)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III
2.7	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於設備生命週期之安全性及合規性。	IV

網路

項次	功能	原則	等級
3.1	網路區隔	具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。	I
3.2	網路區隔	具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表面。	II
3.3	流量管理	呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。	II
3.4	流量加密	於資源存取路徑之資料傳輸加密(如採https等加密協定)。	I
3.5	網路韌性	對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，**動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警**，以維持網路服務，將對業務影響最小化	III
3.6	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook等)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III
3.7	自動化治理	具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。	IV

應用程式

項次	功能	原則	等級
4.1	存取授權	以作業屬性及風險區隔角色，並依角色風險等級定義授權條件(如身分及設備鑑別之等級)，採最小授權原則定義授權範圍；並針對特權作業採獨立角色授權(不混用於非特權作業)，減少特權帳號之濫用及風險。	I
4.2	存取授權	可將帳號動態屬性(如MFA強度、設備合規、連線時間及地點等)納為每個工作階段(Session)之授權審核條件；並針對特權作業採即時存取(Just-in-Time Access)機制，可動態撤銷、限縮存取授權或即時告警。	II
4.3	威脅防護	對應用程式活動紀錄具有即時偵測及回應機制，並可**依據使用者行為或使用模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，動態撤銷、限縮存取授權或即時告警**。	III
4.4	程式安全	從網際網路及防護邊界內部對應用程式執行資安檢測(如源碼檢測、弱點掃描、滲透測試等)，確保應用程式本身安全性，具直接開放經Internet存取之防護能力。	II
4.5	程式部署	為應用程式開發、測試及部署建立持續整合及部署(CI/CD) 通道，分階段採最小授權原則，並評估採自動化機制減少人員介入誤失，或由不同團隊執行落實**權責分離**。	II
4.6	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III
4.7	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於應用程式生命週期之安全性及合規性。	IV

資料

項次	功能	原則	等級
5.1	外洩防護	針對機敏資料部署防止資料外洩防護機制，如依據資料特徵之DLP、資料不落地等	I
5.2	外洩防護	具監控資料存取和使用情況機制，可依據資料存取行為或資料處理模式等因素評估風險(如雖屬授權範圍但不符作業常規等)，**動態撤銷、限縮存取授權或即時告警**偵測及阻止疑似資料外洩之行為。	III
5.3	資料分類	建立資料盤點、分類及標籤機制，確保依資料分類分級落實資料保護政策，並支援最小授權規則。	I
5.4	資料可用性	建立本地端高可用性、異地端備份，並確保備份資料可被有效保護(如離線備份、儲存於隔離環境、防止寫入等)及有效還原。	I
5.5	資料存取	可將資料存取的動態屬性(如MFA強度、設備合規、時間、地點等)納為每個工作階段(Session)之授權審核條件，並具啟動重新驗證之機制，可**動態撤銷、限縮存取授權或即時告警**。	II
5.6	資料加密	依資料分級對機敏性資料加密儲存，並確保加密金鑰的安全管理。	I
5.7	可視性分析	整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CK TTP)進行即時的判斷與回應(如事件單、SOAR Playbook)。(參照F-ISAC威脅情資及金融資安監控組態基準)	III
5.8	自動化治理	可依資安政策快速調適之一致性且自動化管理機制，確保於應用程式生命週期之安全性及合規性。	IV