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發布)

資訊服務處
2024.11.19

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

六、鼓勵零信任網路部署，強化連線驗證與授權管控

世界重要國家政府推動規劃

- 零信任已從概念探討階段進入實務部署規劃，世界重要國家之政府紛紛建立國家零信任網路安全戰略

美國

具體規劃2024年前聯邦網路完成初步遷移。

歐盟

2020年建立歐盟網安戰略，提出標準框架，協助成員國轉型。

- 行政院「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任網路資安防護環境，**推動政府機關導入零信任網路**，完善政府網際服務網防禦深廣度

身分及設備兩相驗證，授予相應權限，並循環監控

iThome 2024資安大調查

【金融業】2024企業資安風險圖（2024～2025）

iThome 2024資安大調查[金融業]

為什麼需要導入零信任架構？

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.

1 企業邊界模糊，場域外人員及設備安全控管不易

- 居家辦公、遠端工作
- 供應商、合作商
- 雲端平台

2 假設資安有缺口，攻擊者一定會進入內網

- 內網是資安防禦最脆弱的一環，已獲授權人員、設備等不可信
- 內網探測、滲透、橫向擴散

身分 → 設備 → 網路 → 應用程式 → 資料

零信任思維重新檢視資安政策

- ☐ 整體資安防護框架
- ☐ 既有資安防護基礎

- 由外而內
  - ➢ 縮小攻擊表面、增加防禦深度
- 由內而外
  - ➢ 擴大防護表面、限縮損害衝擊
- 提高可視性
  - ➢ 持續監控與驗證

導入零信任架構實施原則

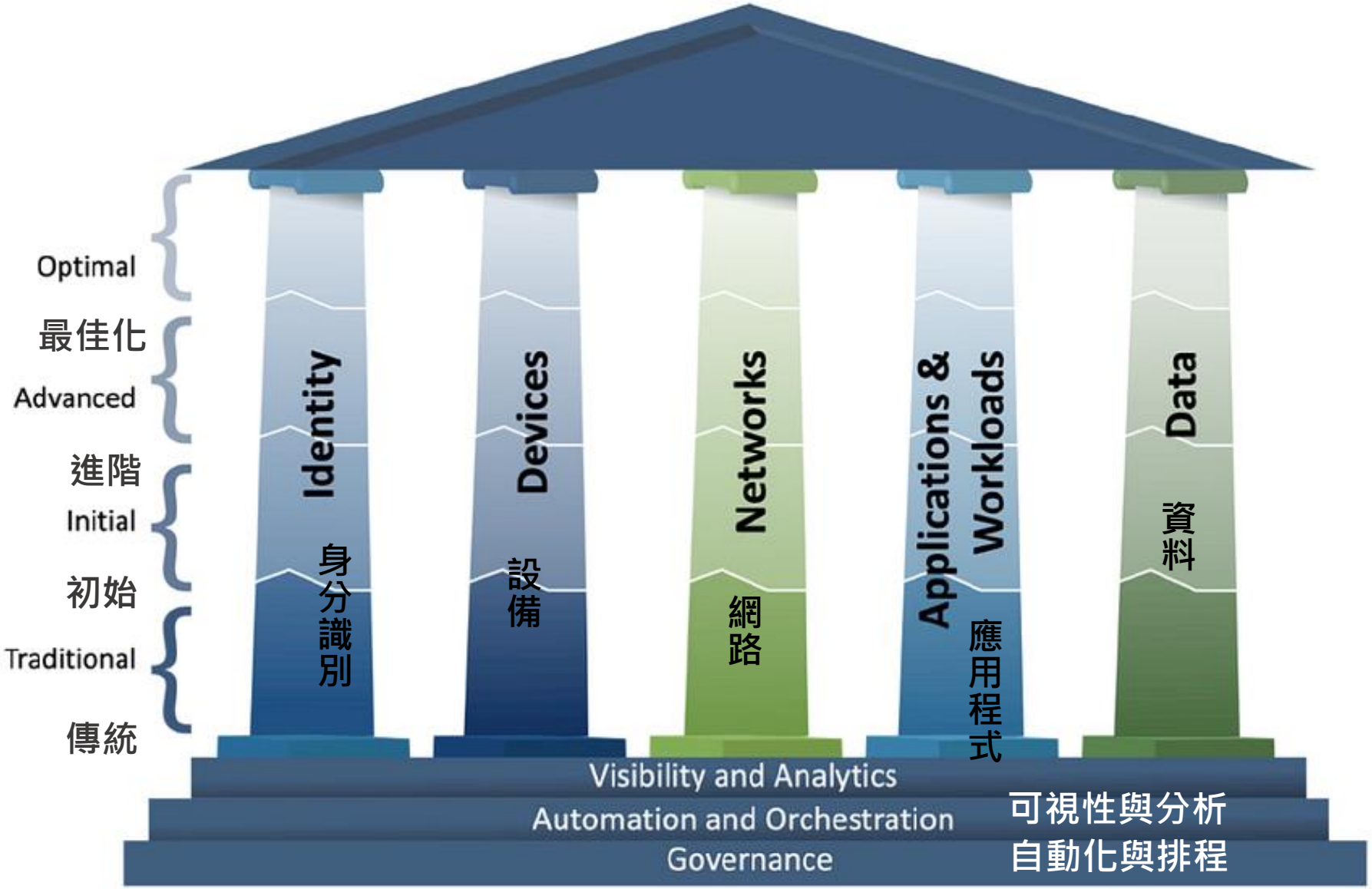
- 風險導向
- 循序漸進
- 目標導向
- 技術中立

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.

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。

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)



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

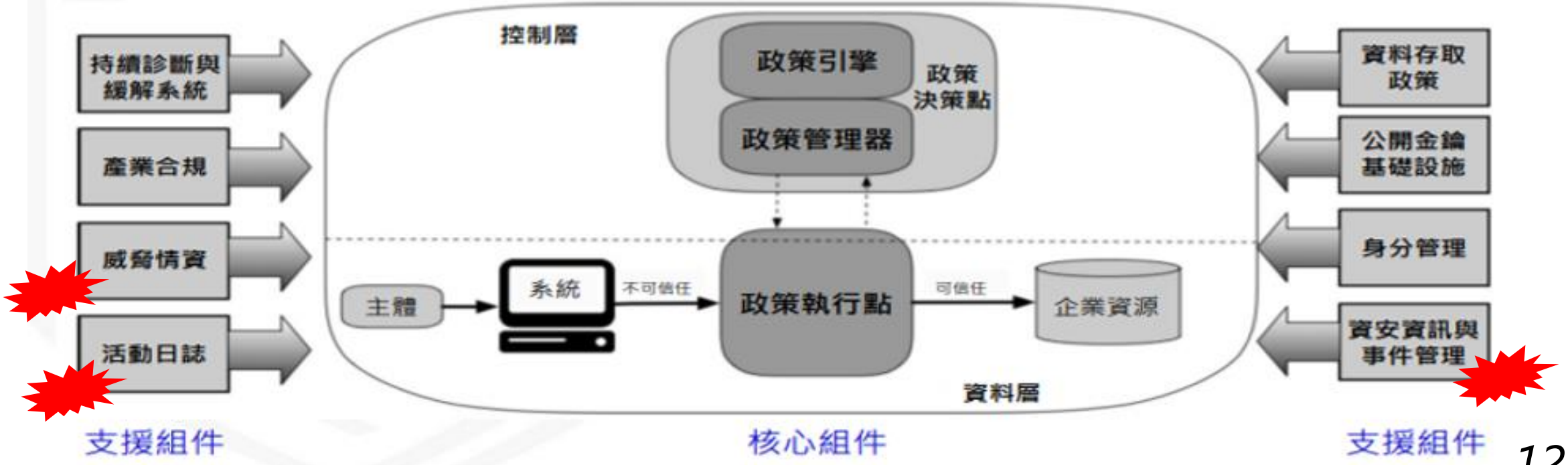
盤點資源存取途徑->以零信任思維 增進防護縱深

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** ⋮	●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** ⋮

NIST 零信任導入建議 (2020.08)

- NIST SP 800-207將零信任架構分成核心組件與支援組件
  - 核心組件：執行鑑別、決定授權及管理連線
  - 支援組件：支援存取決策的資訊與系統

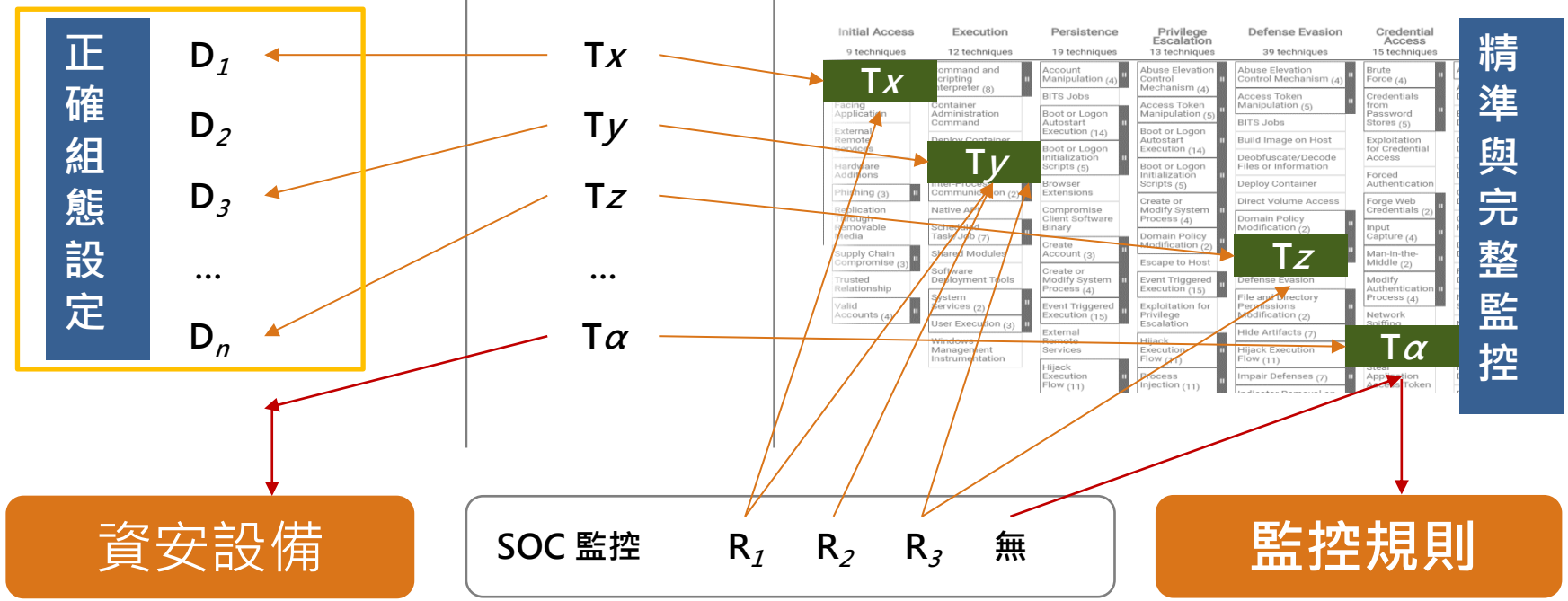


資安監控與防護之有效性

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

盤點資源存取途徑->以零信任思維深化資安防護

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** ⋮	●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

資源整合 -> 動態監控支援自動化治理

1.事件日誌整合分析

- 建立自動**蒐集及分析**各面向**事件日誌機制**
- 包含高風險及異常行為偵測等，逐步增進可視性及關聯分析能力

2. 建立信任推斷機制

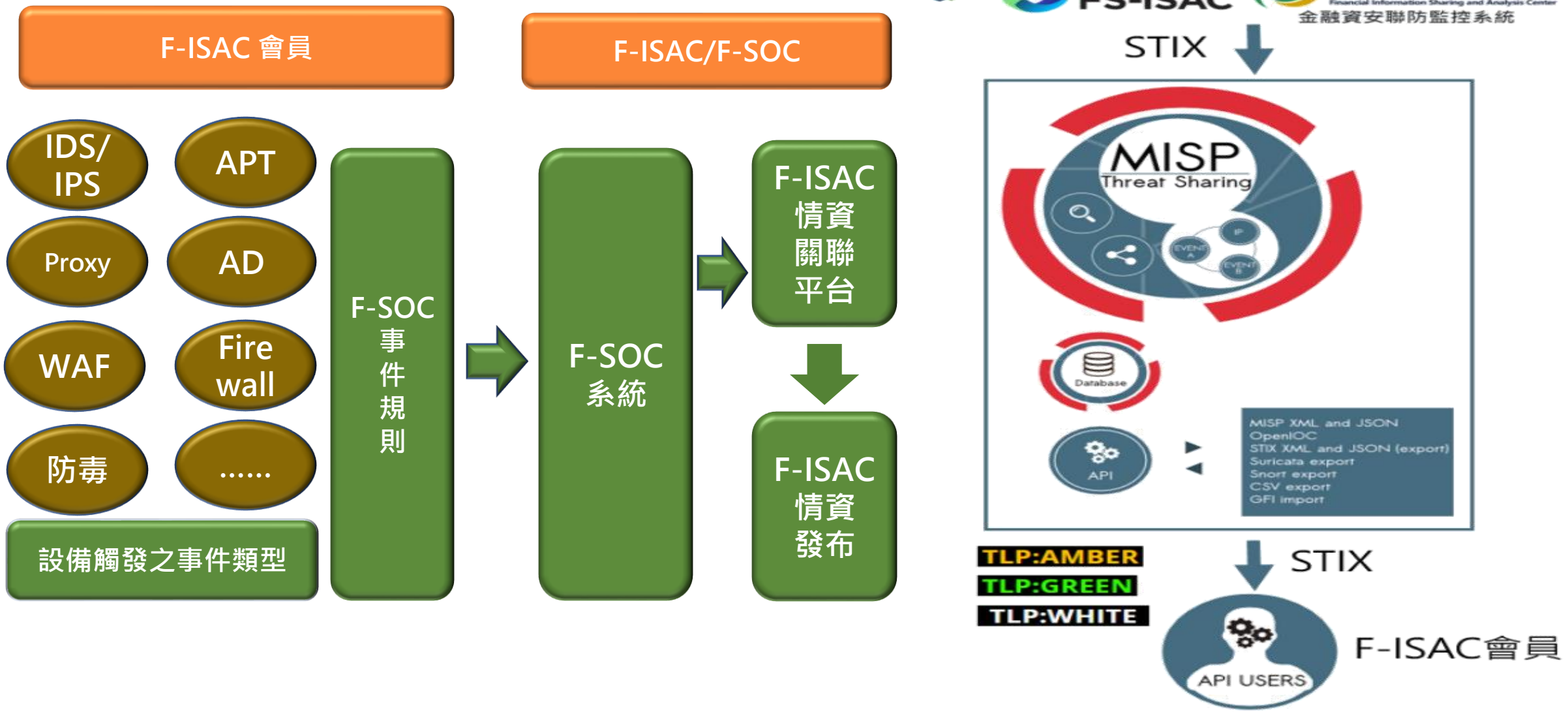
- **結合日誌整合分析**
- 入侵指標(IOC)
- 攻擊行為樣態(Mitre ATT&CK TTP)

3. 發展自動協作機制

- **動態調整存取**控制
  - 允許存取
  - 限制高權限存取
  - 阻斷存取等
- **應處**機制
  - 事件追蹤
  - 脆弱點修補等

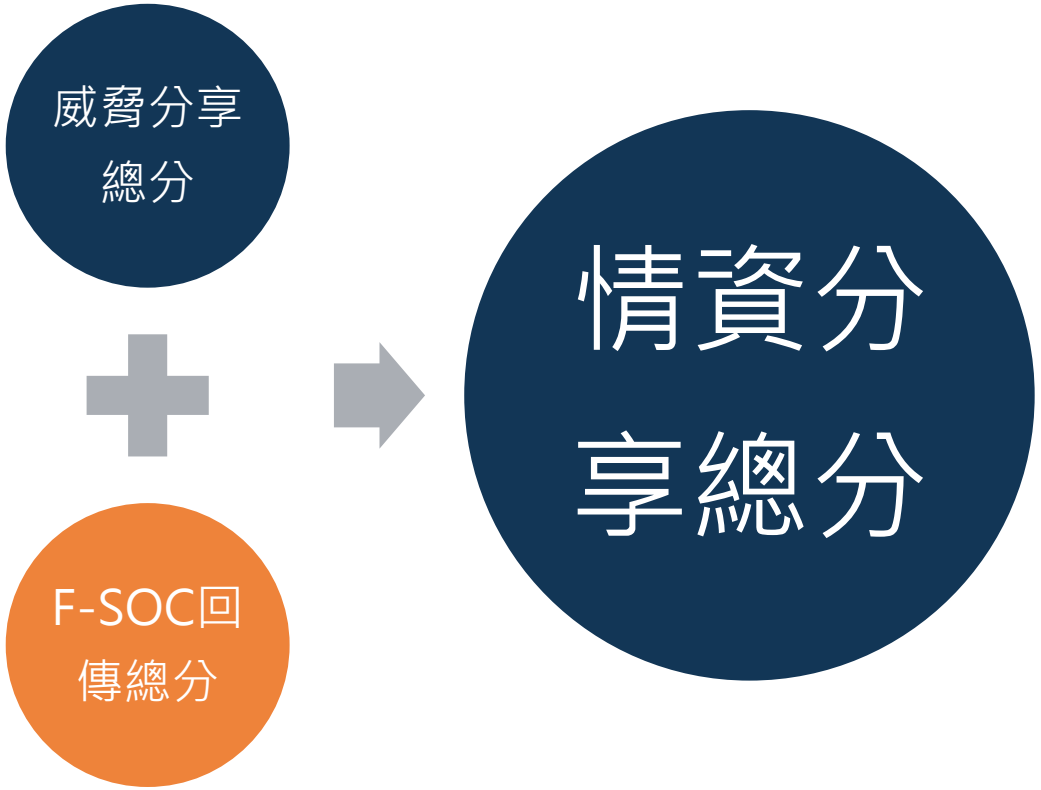
Log Collection → SIEM → SOC/SOAR

提升資安情資分享動能，增進資安聯防運作效能



情資分享計分標準

- 為鼓勵會員分享高重要性情資，及依情資屬性使用不同管道進行情資分享，調整現行會員分享資安情資獎勵作業要點評分方式。
- 113年1月起依112年執行之實務狀況，修訂評分方式



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

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