



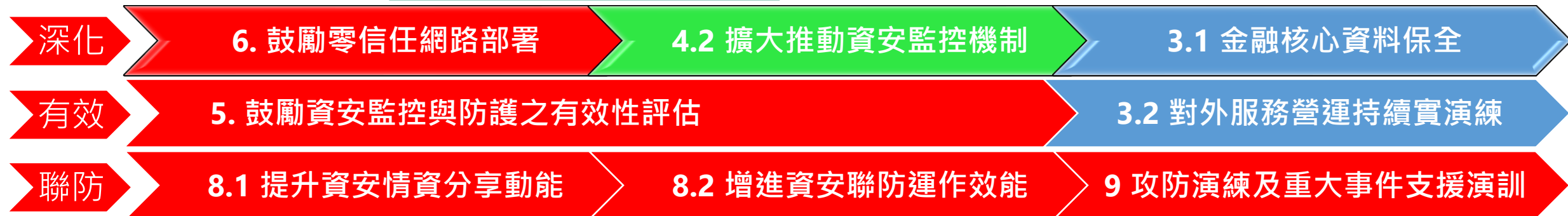
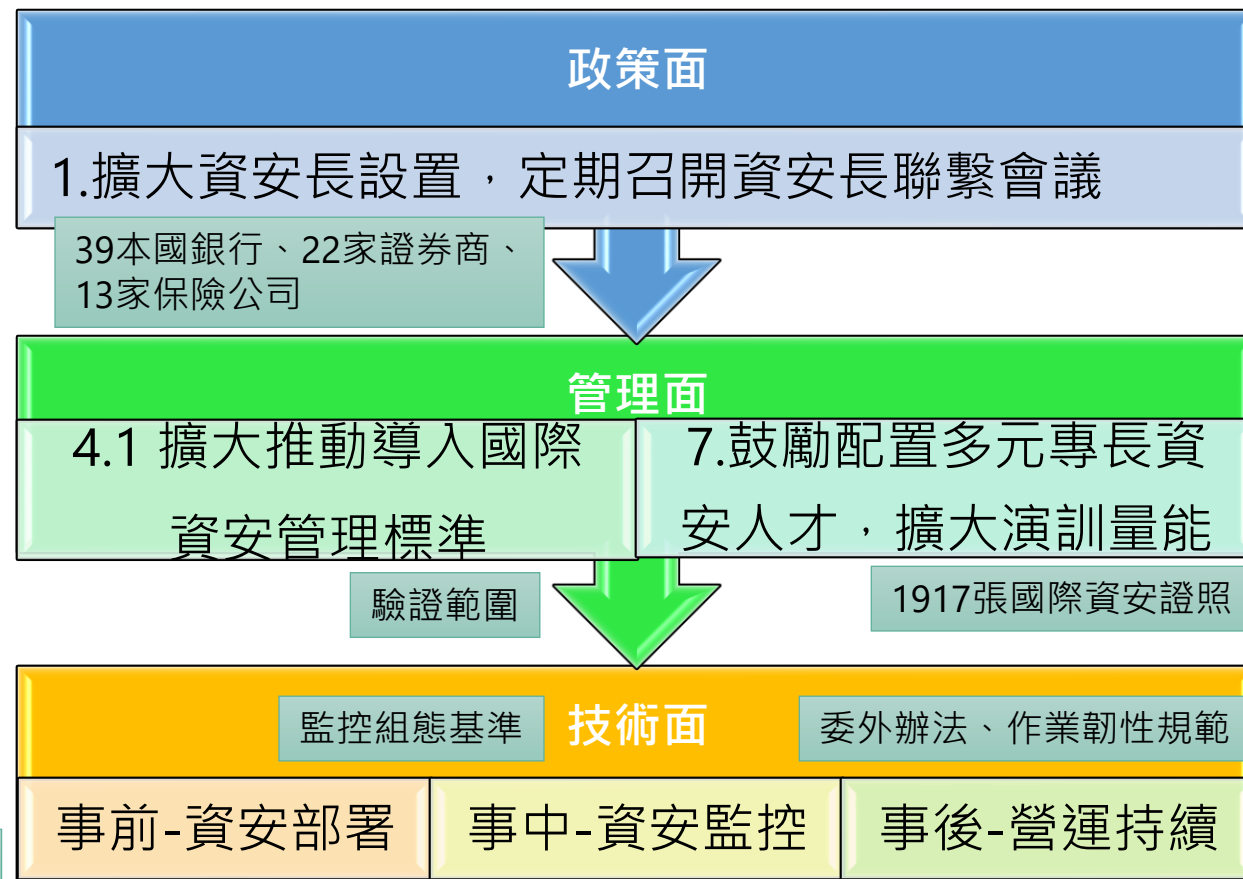
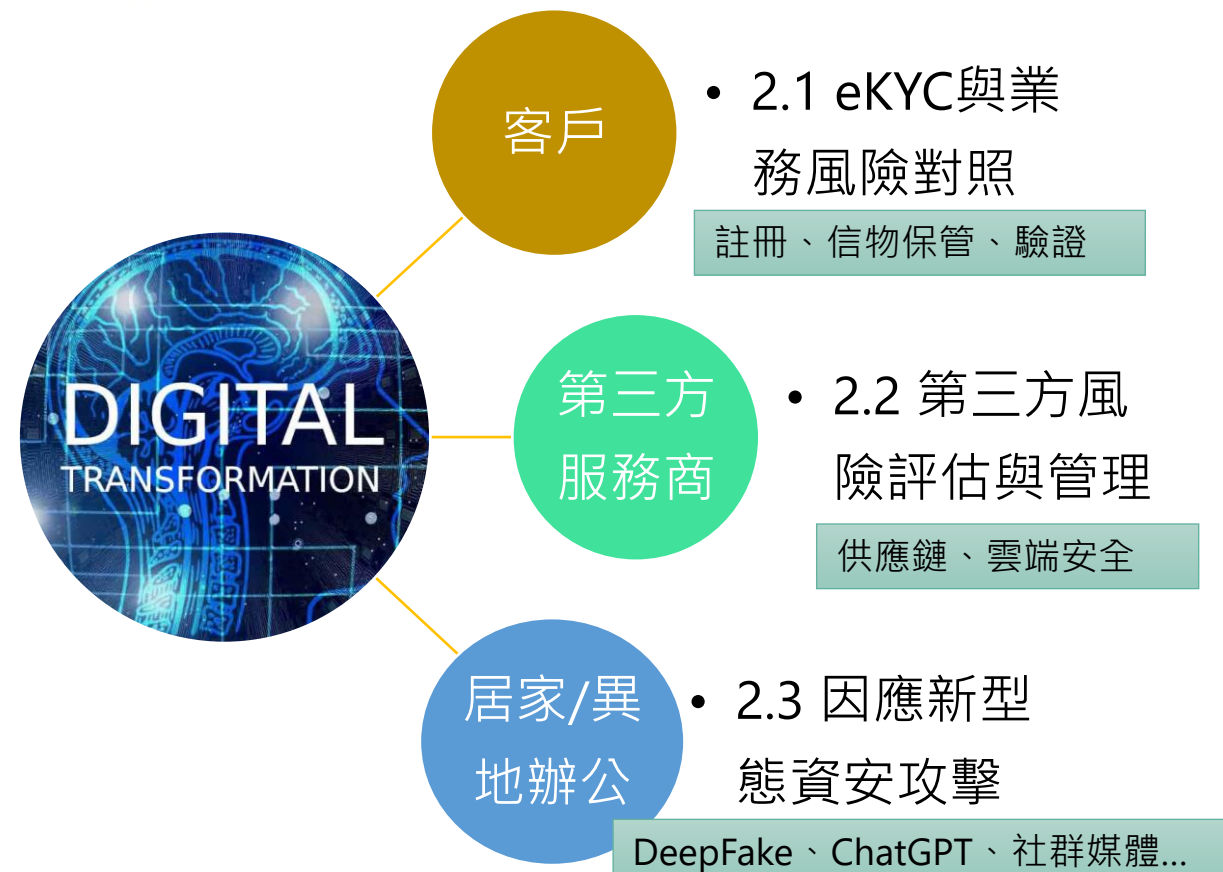
金融資安政策現況與展望



金管會 林裕泰
113年5月16日



金融資安行動方案 2.0 (~2023.12)





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]





零信任

Zero Trust



為什麼需要導入零信任架構？

1

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、設備不可信
- 持續監控內部人員、設備、網路、應用程式、資料
- 每次存取、重新驗證

2

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

零信任思維重新檢視資安政策

- 提高可視性
 - 人員、裝置、應用程式持續監控與驗證
- 縮小攻擊表面
 - 最小授權原則，減少駭客侵入點
- 限縮損害衝擊
 - 網段微分割，避免風險擴散



- 內外網無差別待遇
- 隨處可辦公

1. 盤點資源存取途徑->以零信任思維強化防護縱深

身分

- 採**多(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
 - ⋮

設備

- 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
 - 端點監測

⋮

網路

- 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

應用程式

- 包含源自**內部與外部的安全性檢測**
- 採**最小授權原則**
- 依使用情境(如使用高權限)，**實作動態存取控管機制**

資料

- **資料分類**，依身分別支援最小授權規則
- **機敏性資料加密儲存**

產品？



2. 選定優先保護標的 -> 高風險場域先行



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

- 如重要應用系統之**外部使用者**



3. 資源整合 -> 動態監控支援信任推斷

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

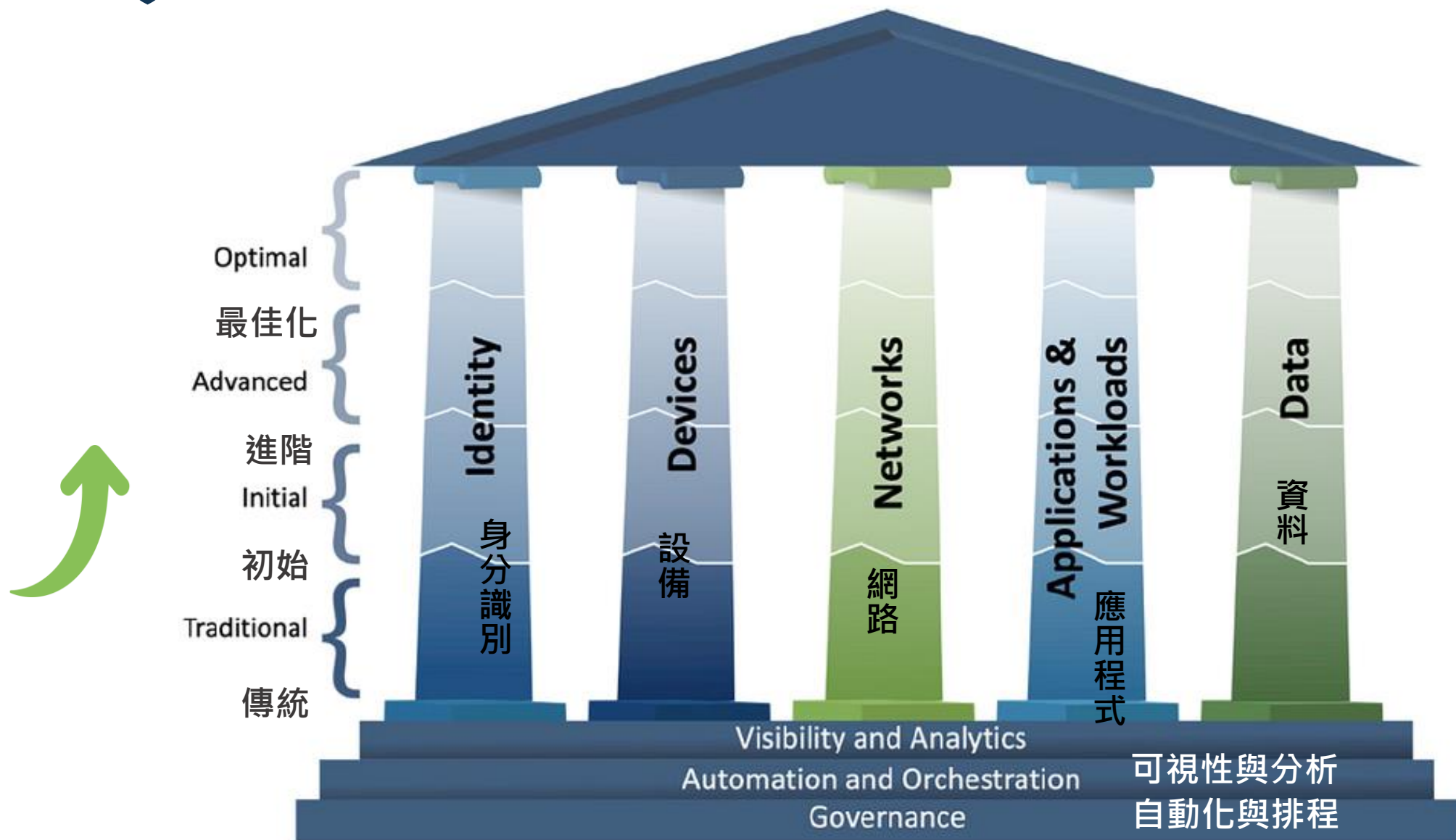
- 存取要求、資源政策要求、威脅情資等
- **結合日誌整合分析**

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



美國網路安全暨基礎設施安全局(CISA)發布零信任成熟度模型2.0 (2023.4發布)

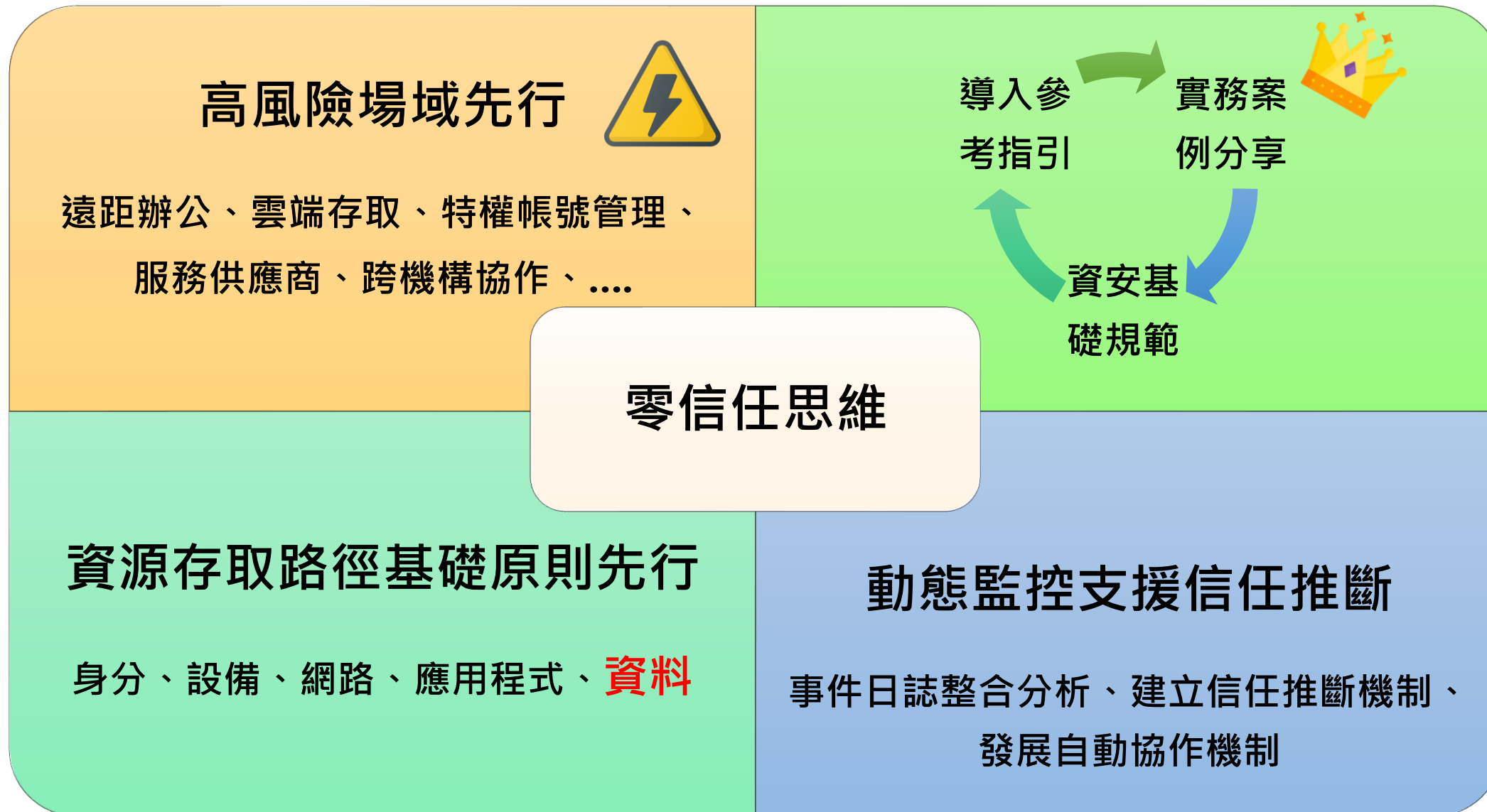




以零信任思維逐步精進資安防護

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.





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

- 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

- 組織內任何人存取任何資訊系統皆須採雙因子認證

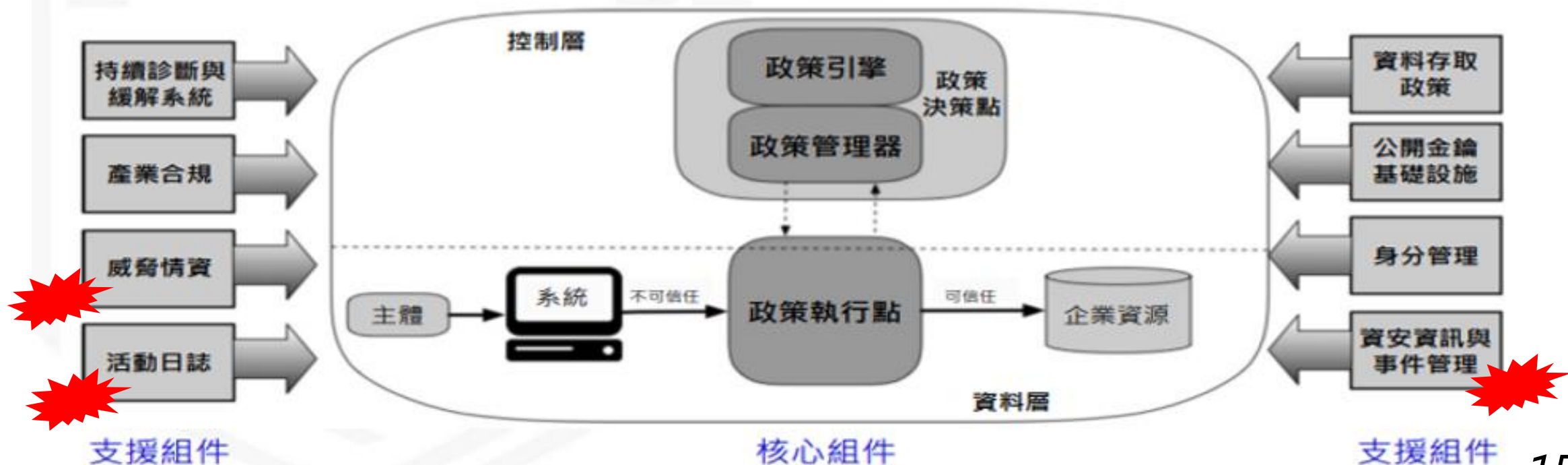
金融資安聯防



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





F-ISAC 112年營運成效

資安威脅預警

國內外資安威脅情資共計蒐整13,692則

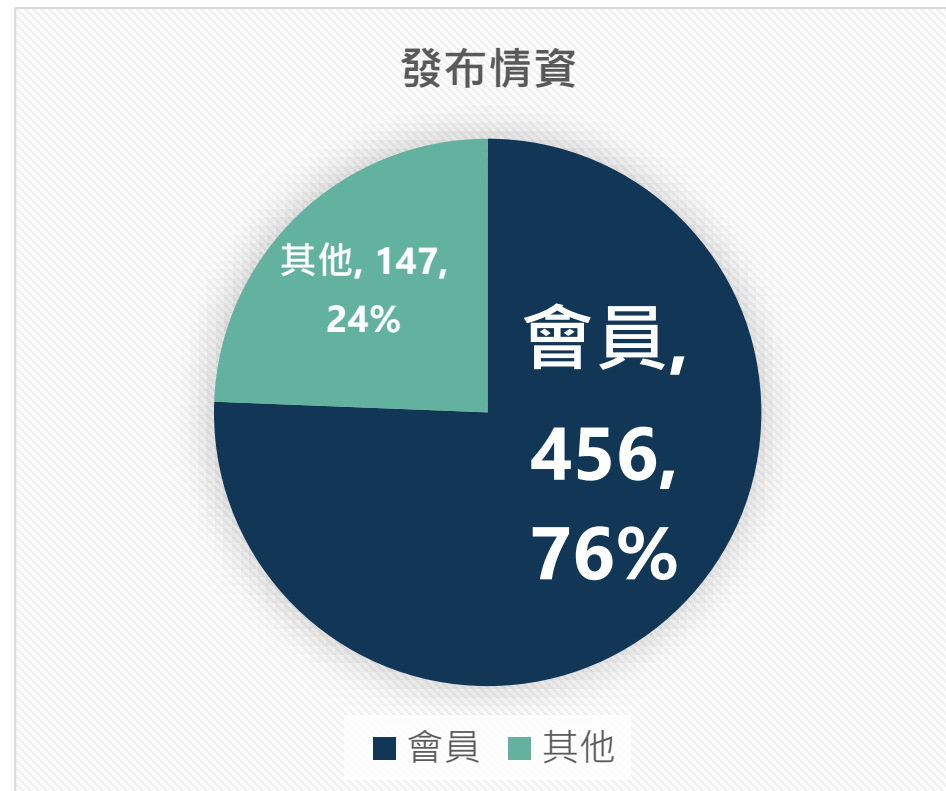
研析後發布資安情資603則

<5%

會員情資分享共計2,497則，

研析後發布資安情資456則

18.2%

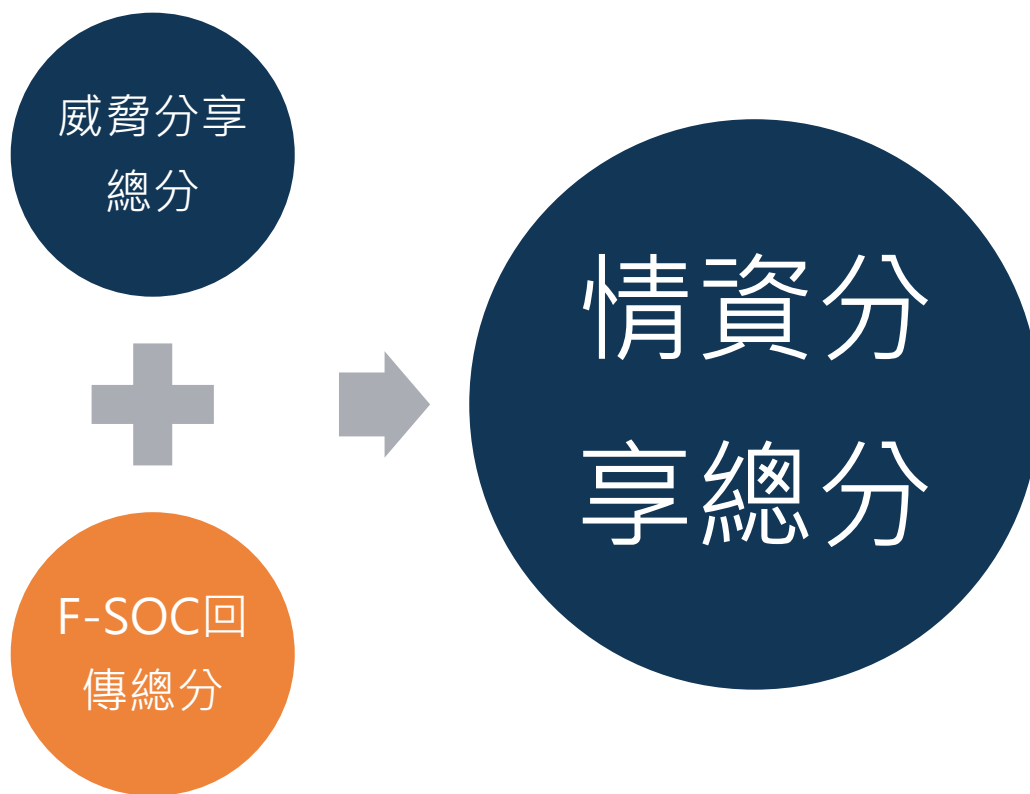


- 透過研析最新國內外資安威脅情資，取得資安態勢、攻擊手法及入侵威脅指標。
- 提供金融機構進行阻擋、監控等，防止金融領域資安事件之發生或降低其損害。



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





金融資安監控協同體系

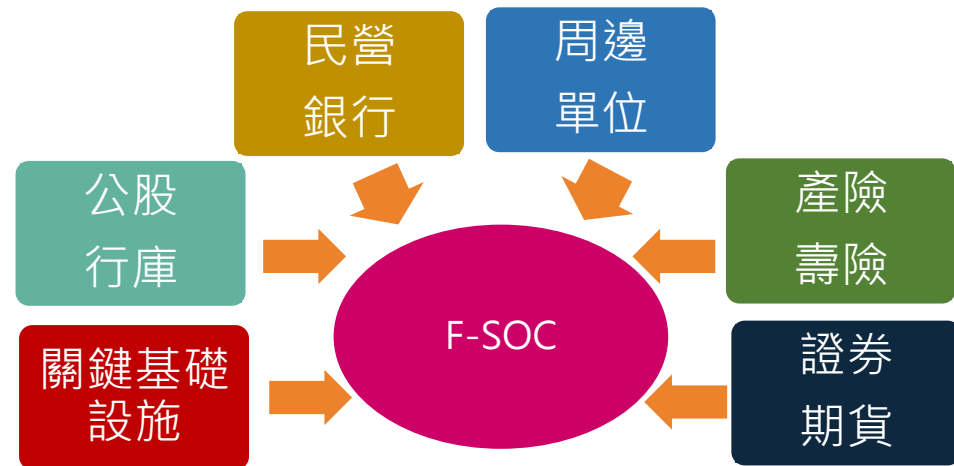
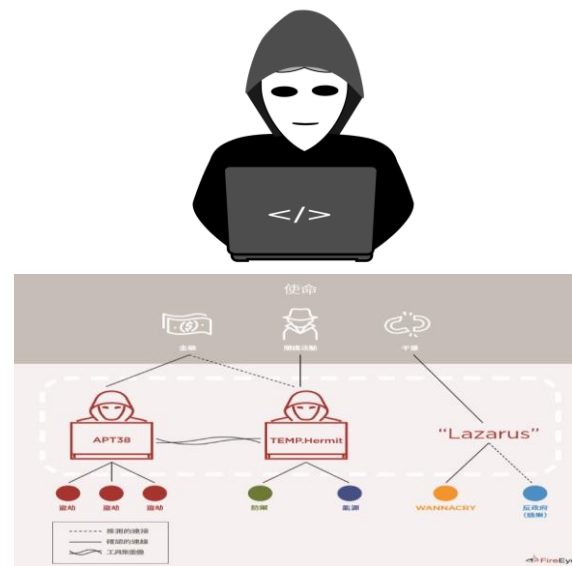
金融機構建置**資安監控**機制(SOC)，及早發現網路異常行為，以扮演資安防護「防微杜漸」的關鍵角色



F-SOC透過研究攻擊手法，並經過系統模擬及驗證，**制定相關監控規則**提供給金融機構SOC運用



F-SOC透過**分析**回傳事件單，**掌握**該組織於我國金融機構之相關**足跡**，**早期預警**，強化金融聯防監控成效



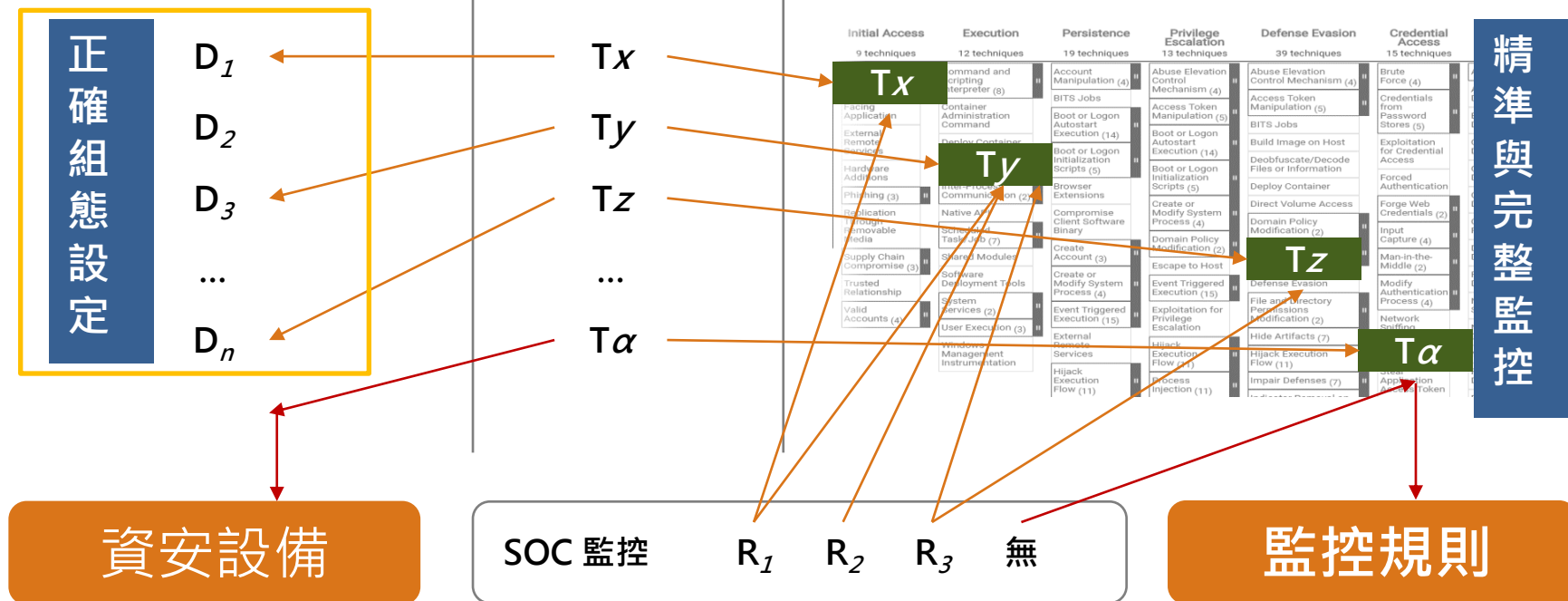
發展資安監控組態基準，鼓勵資安監控與防護之有效性評估

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





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

提升資安情資分享動能，增進資安聯防運作效能



STIX

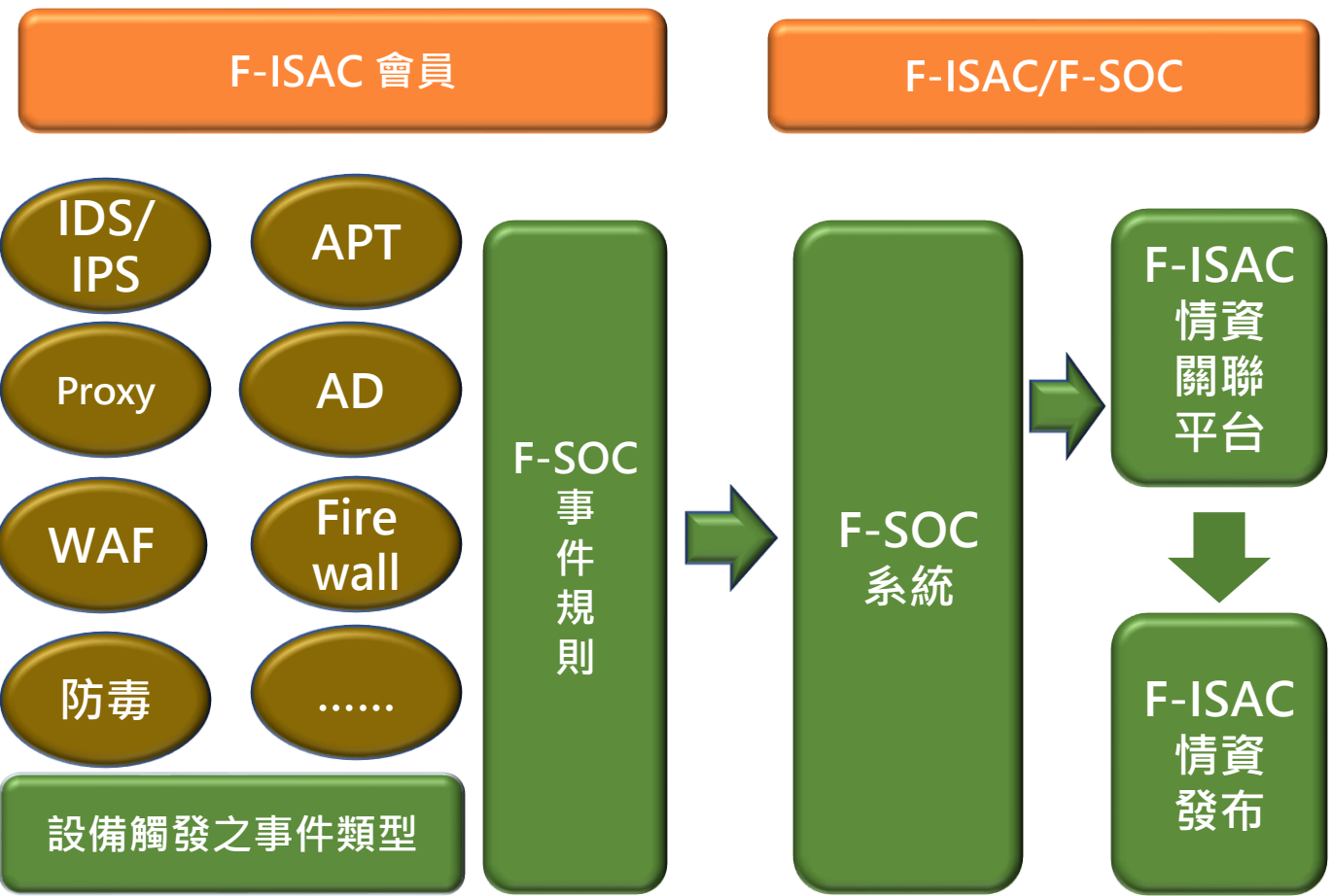


TLP:AMBER
TLP:GREEN
TLP:WHITE

STIX



F-ISAC會員



1. 盤點資源存取途徑->以零信任思維強化防護縱深

身分

- 採**多(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
 - ⋮

設備

- 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
 - 端點監測
 - ⋮

網路

- 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

應用程式

- 包含源自**內部與外部的安全性檢測**
- 採**最小授權原則**
- 依使用情境(如使用高權限)，**實作動態存取控管機制**

資料

- **資料分類**，依身分別支援最小授權規則
- **機敏性資料加密儲存**

產品？

MATRICES

Enterprise

PRE

Windows

macOS

Linux

Cloud

Office 365

Azure AD

Google Workspace

SaaS

IaaS

Network

Containers

Mobile

ICS

Home > Matrices > Cloud

Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: [Azure AD](#), [Office 365](#), [Google Workspace](#), [SaaS](#), [IaaS](#).

[View on the ATT&CK® Navigator](#)
[Version Permalink](#)

layout: flat ▾

show sub-techniques

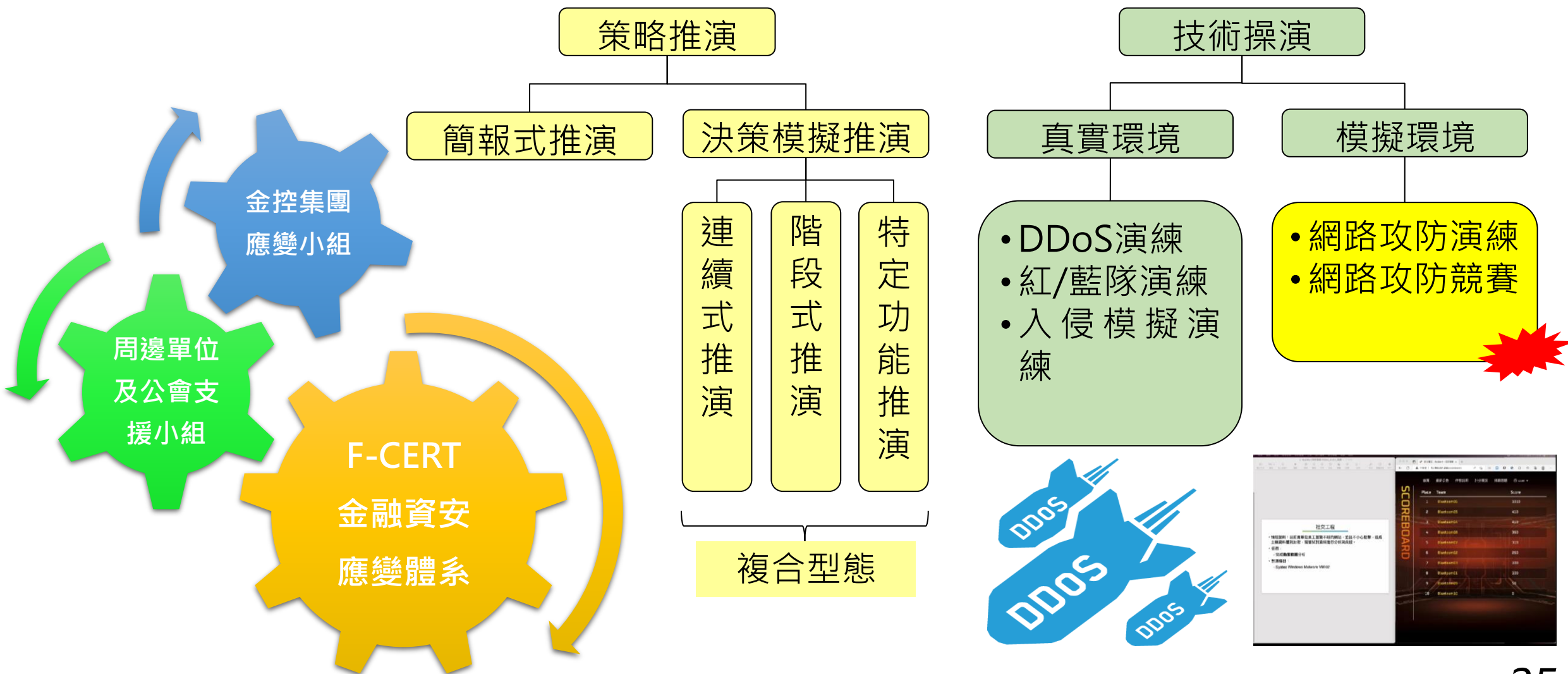
hide sub-techniques

help

Initial Access 5 techniques	Execution 4 techniques	Persistence 7 techniques	Privilege Escalation 5 techniques	Defense Evasion 12 techniques	Credential Access 11 techniques	Discovery 14 techniques	Lateral Movement 4 techniques	Collection 5 techniques	Exfiltration 3 techniques	Impact 9 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)	Create Account (1)	Account Manipulation (5)	Domain 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
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Taint Shared Content	Data from Information Repositories (3)	Transfer Data to Cloud Account	Data Encrypted for Impact
Trusted Relationship	User Execution (1)	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Use Alternate Authentication Material (2)	Data Staged (1)		Defacement (1)
Valid Accounts (2)		Modify Authentication Process (2)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (2)	Cloud Storage Object Discovery		Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration				Financial Theft
		Valid Accounts (2)		Indicator Removal (1)	Network Service Discovery	Network Service Discovery				Inhibit System Recovery
				Modify Authentication Process (2)	Network Sniffing	Network Sniffing				Network Denial of Service (2)
				Modify Cloud Compute Infrastructure (5)	Steal Application Access Token	Password Policy Discovery				Resource Hijacking
				Unused/Unsupported Cloud Regions	Steal or Forge Authentication Certificates	Permission Groups Discovery (1)				
				Use Alternate Authentication Material (2)	Steal Web Session Cookie	Software Discovery (1)				
				Valid Accounts (2)	Unsecured Credentials (3)	System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

資安攻防演練

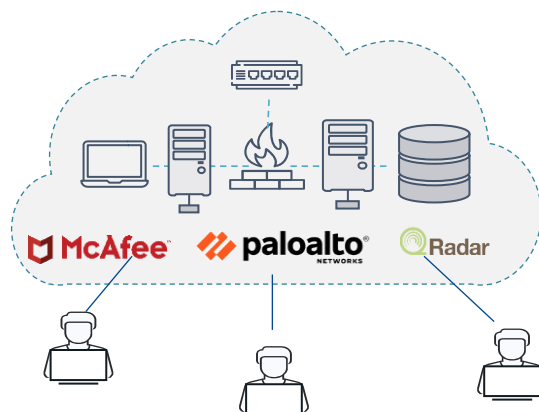
辦理資安攻防演練，規劃重大資安事件支援演訓





網路實兵攻防演練

資安攻防演練平臺



雲端平臺



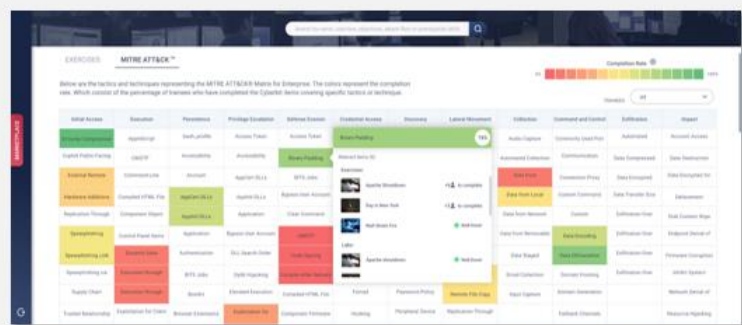
封閉式
虛擬攻防場域



演練情境

MITRE
ATT&CK™

攻擊手法

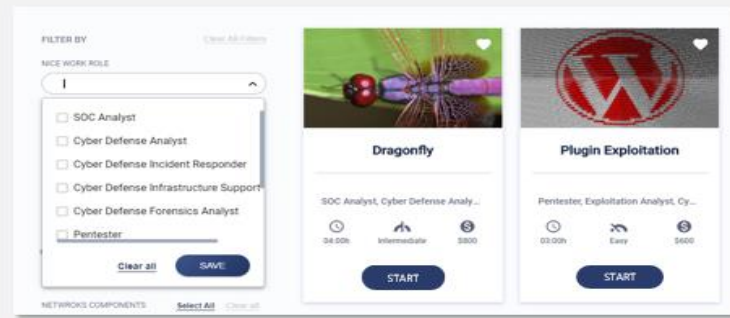


MITRE ATT&CK

Align and track progress according to the MITRE ATT&CK framework

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

防護技術



NICE Cybersecurity Framework

Plan your program and assess trainees according to NICE Work Roles and KSAs



參加人員技術資格



資安技術人員

- 資安設備操作與設定
- 威脅獵捕，SIEM資安事件關聯分析
- 情資蒐集與分享
- 惡意程式分析



系統/網路技術人員

- 系統、網路設備操作與設定
- 系統、網路流量日誌判讀
- 弱點修補、改善



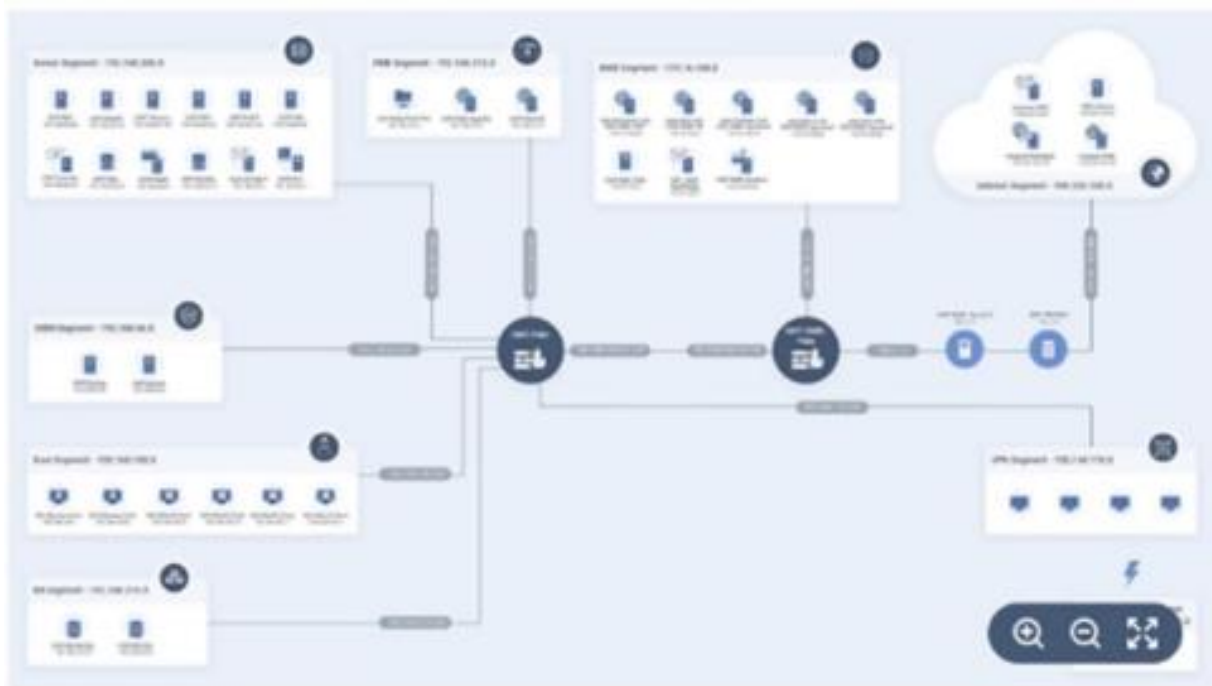
權限管理人員

- AD日誌判讀
- 帳號使用者行為分析
- 權限管理



攻防演練平臺防護設備模組

提供多種類型及廠牌之防護設備套件供參演單位挑選。















MITRE ATT&CK

Align and track progress according to the MITRE ATT&CK framework



網路攻防演練(2023)

WEB Attack Cyber Drill

 <p>Exploit the Plugin (Stockholm)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>3hr (SC) 3 CPE</p>	 <p>Cyberbit's Live-fire Network (Cyberbit's Live-fire Network)</p> <p>Live-fire Exercise</p> <p>Easy</p> <p>40min (SC) 0.75 CPE</p>	 <p>DLL Side Loader with CrowdStrike (Hanoi)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>3hr (SC) 3 CPE</p>	 <p>Ransomware via Log4J (Kyiv)</p> <p>Live-fire Exercise</p> <p>Crisis Simulation</p> <p>Intermediate</p> <p>2hr (SC) 2 CPE</p>
 <p>Coin Miner via Kubernetes (Quito)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>3hr (SC) 3 CPE</p>	 <p>Internal DoS: (Cairo)</p> <p>Live-fire Exercise</p> <p>Crisis Simulation</p> <p>Intermediate</p> <p>3hr 30min (SC) 3.5 CPE</p>	 <p>Data Leakage via SQL Injection (Wellington)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>2hr (SC) 2 CPE</p>	 <p>Epsilon Red (Liverpool)</p> <p>Live-fire Exercise</p> <p>Crisis Simulation</p> <p>Intermediate</p> <p>4hr 30min (SC) 4.5 CPE</p>
 <p>Epsilon Red with CrowdStrike (Monaco)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>4hr 30min (SC) 4.5 CPE</p>	 <p>AWS Cloud - The Enemy within (Barcelona)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>3hr (SC) 3 CPE</p>	 <p>Share-Lock Ransomware Investigation with... (Houston)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>3hr (SC) 3 CPE</p>	 <p>AWS Cloud - Manipulate Data via SSRF (Seattle)</p> <p>Live-fire Exercise</p> <p>Intermediate</p> <p>3hr (SC) 3 CPE</p>

APT Attack Cyber Drill

VPN Attack Cyber Drill

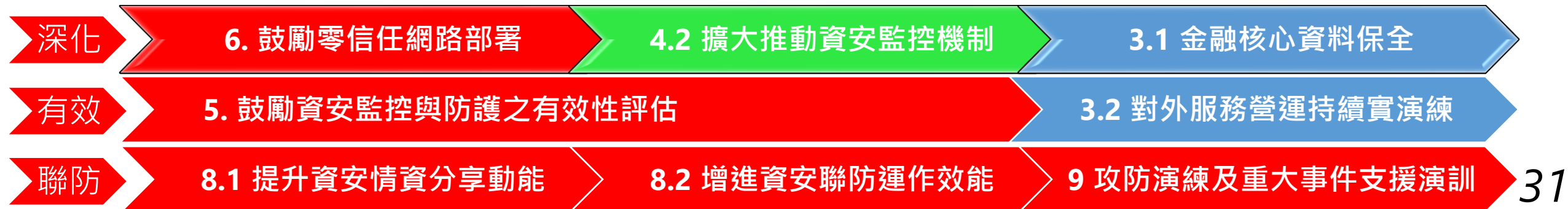
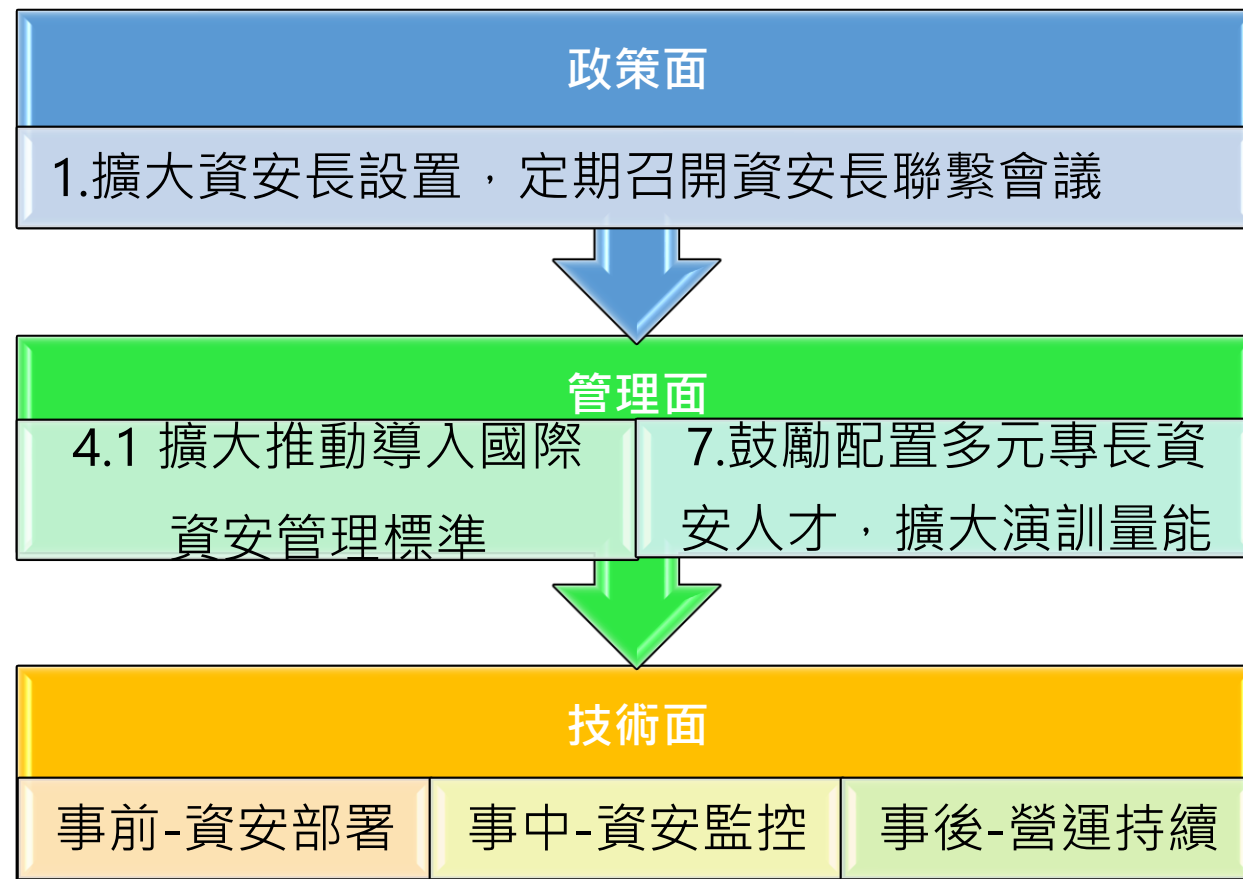


培養網路戰術思維，增進資安防護有效性



- ◆ MITRE ATT&CK (對抗策略、技巧和常見知識) 為美國 MITRE 資安專業組織所開發的架構、資料矩陣和評估工具，旨在協助企業瞭解自身的安全性整備度，並找出其防禦機制的弱點。

金融資安行動方案 2.0 推動藍圖



感謝聆聽