資通安全政策與新思維

數位發展部
資通安全署署長蔡福隆

中華民國114年9月

臺積電資安的經驗

- **封鎖所有對外連線**，上網透過 RBI(代理瀏覽器)
- **運用雲端 CDN**, 有效應對 DDOS攻擊
- **全面安裝 EDR**, 有效應付勒索軟體
- **每個監控到的事件**，都會仔細分析事件根因及強化防禦機制
- **台積電供應鏈管理**, 十項管控措施, 稽核 2人1組出去查核

臺積電資安的經驗

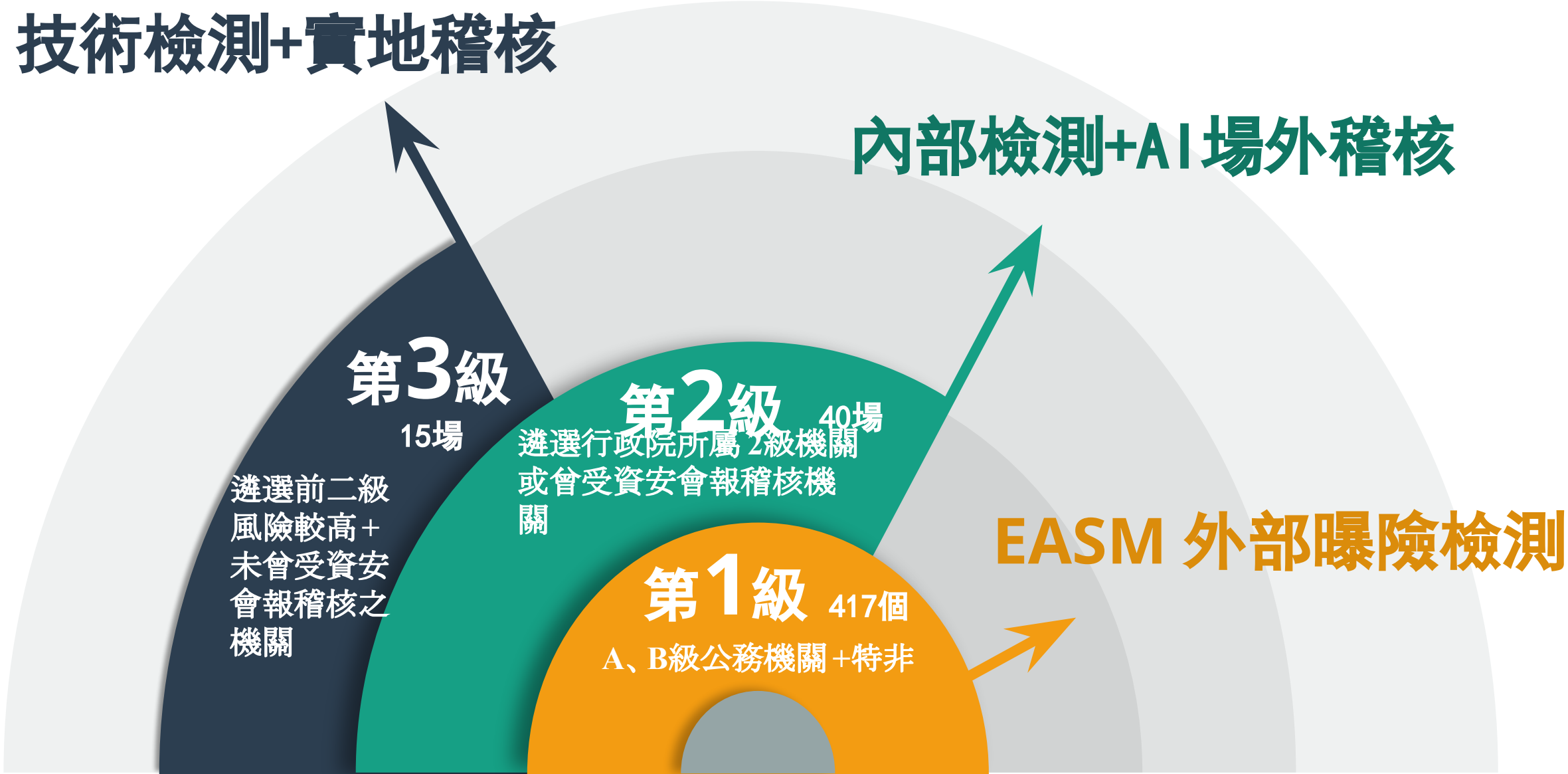
- **封鎖所有對外連線**，上網透過 RBI(代理瀏覽器)
- **運用雲端CDN**，有效應對 DDOS攻擊
- **全面安裝EDR**，有效應付勒索軟體
- **每個監控到的事件**，都會仔細分析事件根因及強化防禦機制
- **台積電供應鏈管理**，十項管控措施，稽核 2人1組出去查核

管控措施
電腦設備安全管控
惡意程式防護
可攜式儲存媒體管控
安全性更新與管理
帳號密碼管理
遠端連線管理
高權限帳號管理
對外網路防護
電子郵件防護
網路網路存取管控

資安政策新思維

- 整個政府的資安政策，要從 mindset 、architecture 改起
- 防禦於大外網：資源向上集中，封鎖所有對外連線，遵守紀律，落實稽核
- 減法法則：各機關資安應辦事項要減少。增加技術面處理　，減事減人
- 稽核重成效：務實、有效、重技術

技術檢測+實地稽核



內部檢測+AI場外稽核

EASM 外部曝險檢測

第1級–EASM 外部曝險檢測

檢測風險類別

委託廠商提供技術諮詢服務

以**外部**角度

非侵入式檢測

資產**曝險**評估

稽核平臺發信**追蹤**處置情形

第2級-內部檢測

1天3人

1 檢測軟體

運用檢測工具

機關派送

- Theatsonar(惡意威脅鑑識分析)
- RapixEngine(GCB)

現場執行

- Nessus Pro(弱掃)
- Acunetix (網站弱掃)
- IASM(帳號安全管理)

提前2週由委託廠商協助佈署軟體/確認網路開通情形

2 檢測報告

檢測團隊彙整報告

- 資安院/廠商技術諮詢
- 蒐整檢測資料
- 確認報告內容

3 檢測結果

提供機關檢測結果

- 透過稽核平臺發信通知
- 逾風險值者請機關修補
- 未逾風險值者供機關自行參考

委託廠商提供技術諮詢服務

4 修補追蹤

機關修補弱點

- 機關進行修補
- 本署於稽核平臺持續追蹤管考

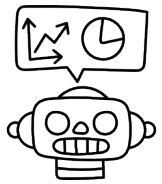
第2級-AI場外稽核

1

機關提供文件

- 資通安全維護計畫
- ISMS四階文件
- 機關自評表及其紀錄文件

提升機關上傳率



2

AI自動化分析

- 透過稽核平臺AI分析
- 文件自動分析比對
- 跨系統整合(實施情形、VANS、前一次稽核改善情形等)

3

人工審核結果

- 稽核組同仁/稽核委員人工複審確認AI分析結果
- 符合行政院及所屬機關(構)使用生成式AI參考指引

4

機關進行修正

- 機關依據文件審核結果進行相關修正
- 持續追蹤管考機制

第3級–技術檢測

3天12人

使用者電腦安全檢測

物聯網設備檢測

網域主機安全防護檢測

資料庫安全檢測

核心資通系統安全檢測

網路架構檢測

組態設定安全檢測

網路惡意活動檢視

第3級-實地稽核

- 稽核領隊 1人
- 稽核委員 8~10人
- 技檢團隊 至多12人
- 觀察員 至多6人
- 觀摩人員 視需求
- 工作人員 3~6人

- 核心業務
- 資安政策
- 資安推動組織
- 資安專責人力
- 資安經費配置

- 系統盤點
- 風險評估
- 委外管理
- 持續精進/績效管理

- 事件日誌
- 營運持續計畫
- 系統服務獲得
- OT網路架構
- 存取控制
- 識別/鑑別
- 防護
- 系統資訊完整性
- 組態管理

- 資安防護控制
- 系統發展安全
- 資安事件通報應變
- 情資評估因應

執行效益

減人減事

務實有效重技術

優稽核 顧資安

115年

稽核範圍更廣

稽核機關 40個

EASM檢測機關 417個

技術面檢測場次增加

技術面

15個（技術檢測） → 15 +40個（技術檢測 / 內部檢測）

以AI輔助程序面稽核

程序面

40個（實地稽核） → 30 +40個（實地稽核 / AI場外稽核）

116年～

第1級

EASM檢測擴大至7000多個資安法納管機關

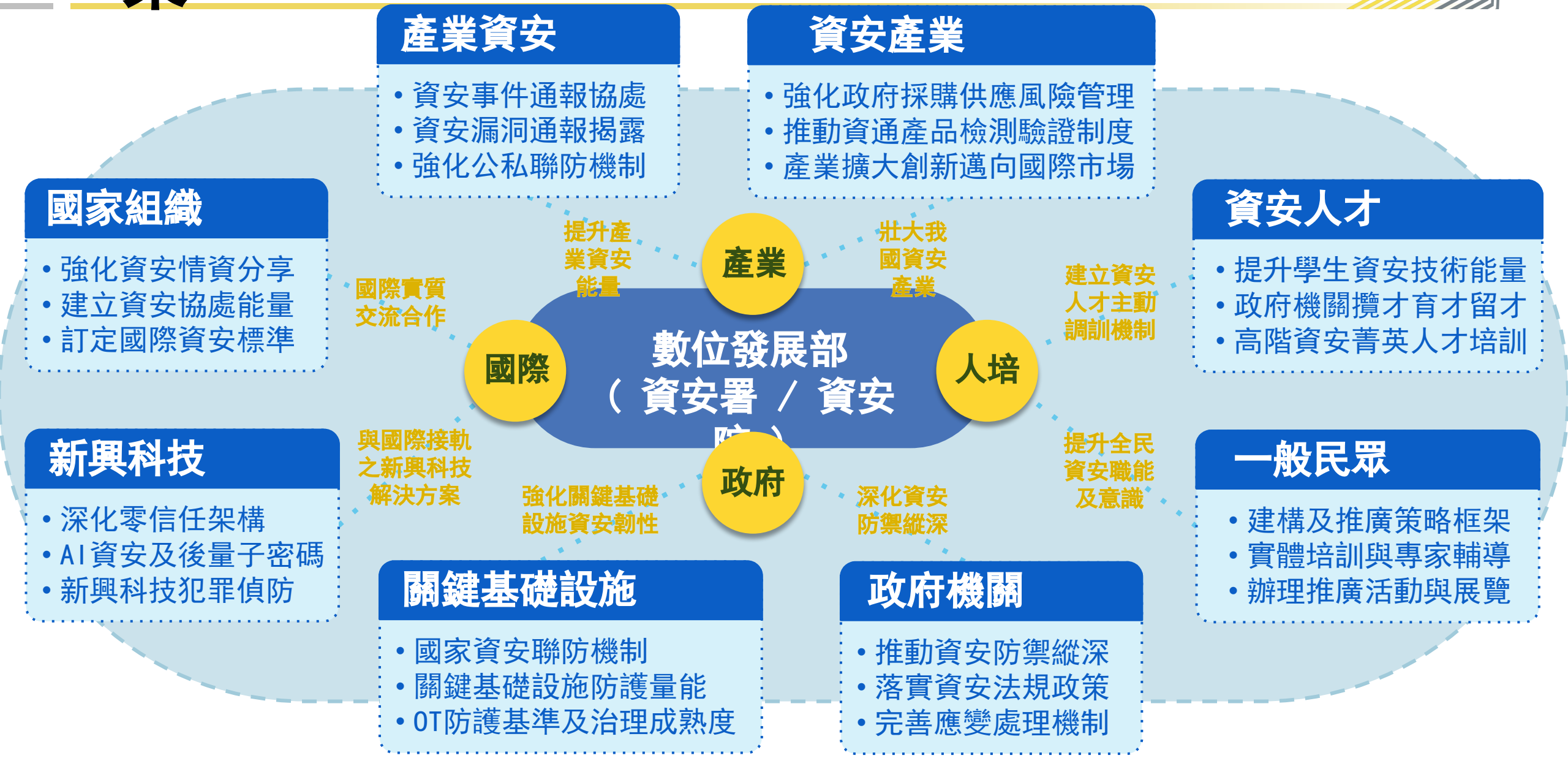
第2級

內部檢測+AI場外稽核擴大至100場

實際執行場次視 114年試辦結果滾動調 整

第七期
國家資通安全發展方案
（114年–117年）

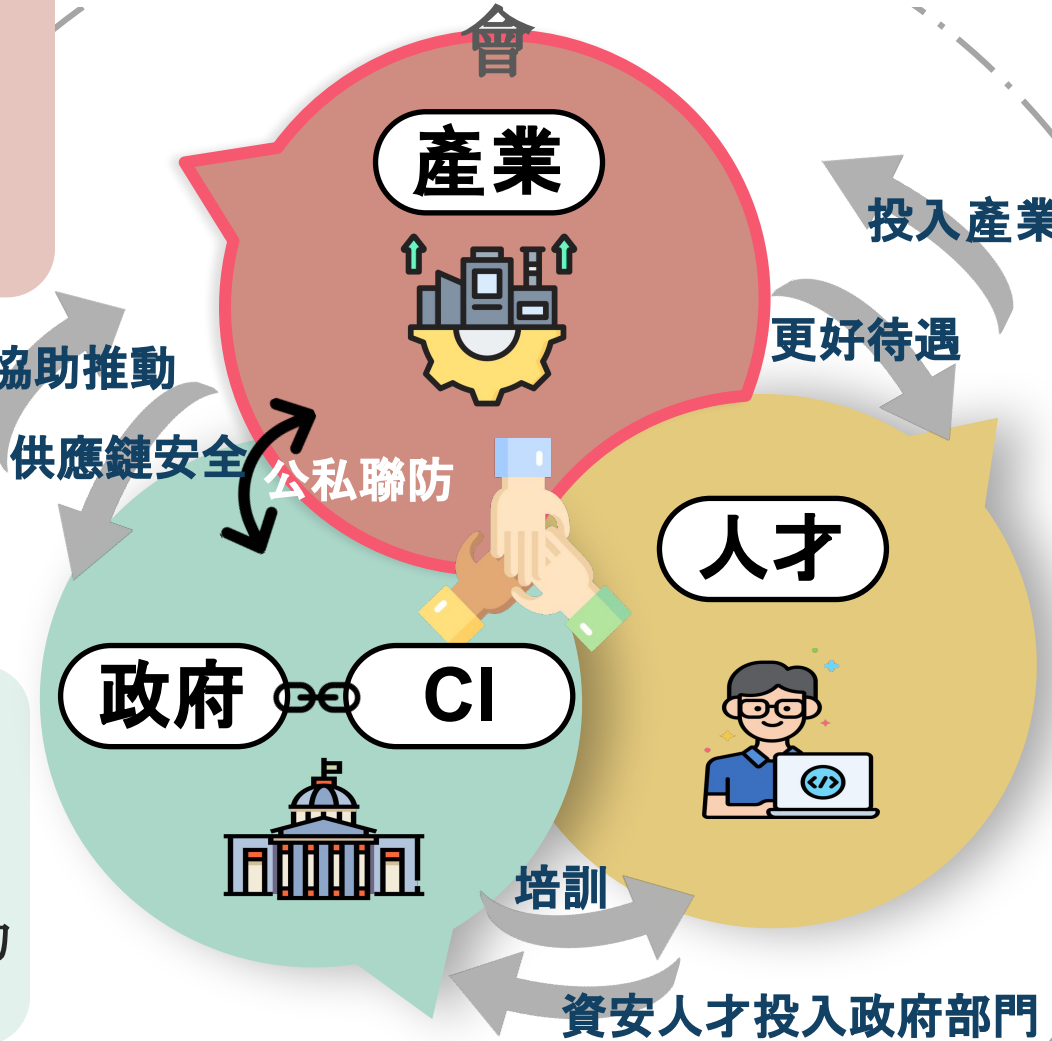
國家資安推動整體框架


產業資安
• 資安事件通報協處
• 資安漏洞通報揭露
• 強化公私聯防機制
資安產業
• 強化政府採購供應風險管理
• 推動資通產品檢測驗證制度
• 產業擴大創新邁向國際市場
國家組織
• 強化資安情資分享
• 建立資安協處能量
• 訂定國際資安標準
資安人才
• 提升學生資安技術能量
• 政府機關攬才育才留才
• 高階資安菁英人才培訓
提升產業資安能量
壯大我國資安產業
國際實質交流合作
建立資安人才主動調訓機制
產業
國際
人培
數位發展部
（資安署 / 資安院）
政府
與國際接軌之新興科技解決方案
提升全民資安職能及意識
強化關鍵基礎設施資安韌性
深化資安防禦縱深
新興科技
• 深化零信任架構
• AI資安及後量子密碼
• 新興科技犯罪偵防
一般民眾
• 建構及推廣策略框架
• 實體培訓與專家輔導
• 辦理推廣活動與展覽
關鍵基礎設施
• 國家資安聯防機制
• 關鍵基礎設施防護量能
• OT防護基準及治理成熟度
政府機關
• 推動資安防禦縱深
• 落實資安法規政策
• 完善應變處理機制

第七期方案核心價值

- 提升數位產品信賴
- 擴大資安產業規模
- 促進資安市場國際化

建構信賴安全之數位社會



整合資源與力量

正向的循環成長

強化鏈結與協作

- 培育高階、政府、產業、學研資安人才
- 提升全民資安職能意識
- 促進國際交流合作

- 完善國家應變機制
- 建立CI防禦體系
- 強化整體資安治理能力

第七期國家資通安全發展方案框架

扣合戰略2025

推動策略與具體措施

策略一

全社會資安防禦

1-1 完善國家資安應變機制
1-2 提升全民資安職能及意識
1-3 建構全社會資安防護網

策略二

提升關鍵基礎設施資安韌性

2-1 建立關鍵基礎設施資安防禦體系
2-2 提升關鍵基礎設施資安聯防能量
2-3 精進關鍵基礎設施資安治理能力

願景

建構信賴安全之數位社會

目標

✔ 強化全社會資安防禦韌性
✔ 豐富資安產業生態系
✔ 構築新興科技防禦技術

策略三

壯大我國資安產業

3-1 推動資通產品檢測制度
3-2 強化政府採購供應鏈風險管理
3-3 擴大資安產業規模並向國際輸出

策略四

AI新興資安科技應用與合作

4-1 拓展AI技術應用以提升資安防護能量
4-2 強化新興資安科技前瞻研究
4-3 促進國際資安交流合作

策略一　全社會資安防禦

全社會資安防禦

完善國家資安應變機制

- 完善應變處理機制
- 支援重大資安事件
- 強化資安會報統籌

提升全民資安職能及意識

- 提升社會資安意識
- 培育高階資安人才
- 推動資安人才框架

建構全社會資安防護網

- 強化科技偵查犯罪
- 精進資安鑑識能量
- 強化數據隱私保護

充實資安人力

穩定資安預算

資安全民資安意識推廣

推廣研析

- 研析資安先進國家之推廣模式與實務經驗
- 建構符合我國實務情境、社會文化與資源條件之資安推廣策略框架

實作參與

- 提供實體培訓與專家輔導服務，協助企業建立基本資安治理能力
- 依據民眾年齡層與使用情境，開發對應之資安意識課程、教材教具與數位學習資源

認知導

- 辦理旗艦型推廣活動與展覽
- 依據不同受眾特性運用多元傳播管道宣傳

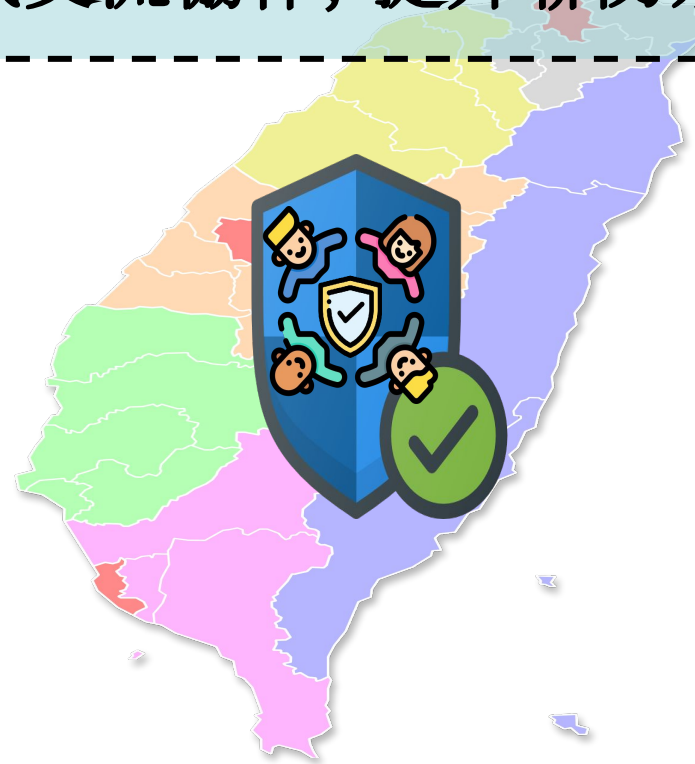
資安體系人才培育理念

資安專職訓練

培訓資安人才
打造資安團隊，強化資安聯防

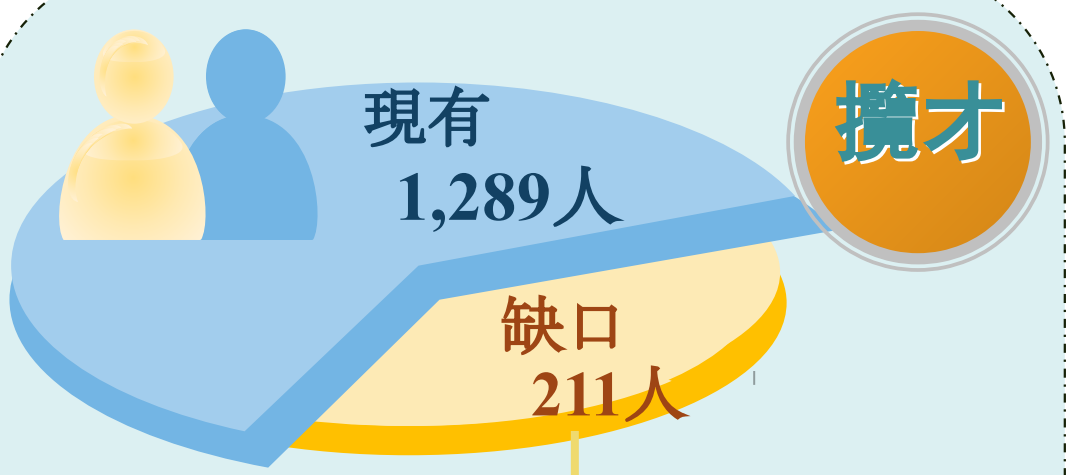
活動交流

促進團隊凝聚力
跨域交流協作，提升聯防效益



資安人才培育

攬才



民間攬才 -增設高等三級考試「資通安全」類科
機關招才 -政府資安人力職能轉換訓練

115年起資安儲備人力＞缺口

育才

資安長/高階政府資安菁英

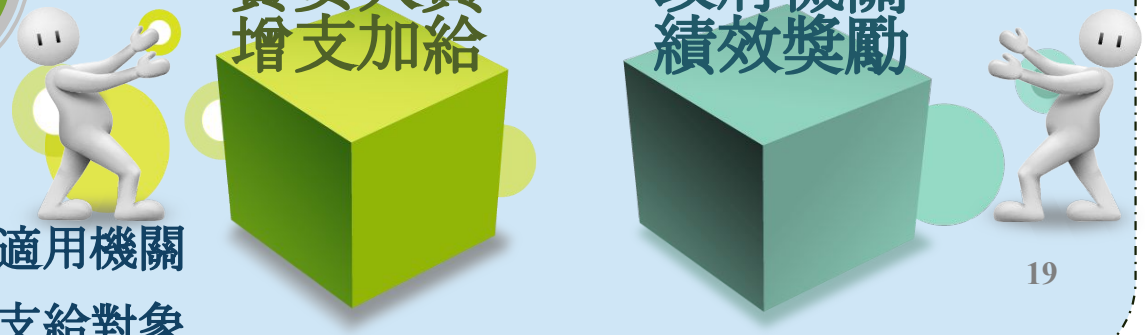
每年培訓逾600人

資安專職(責)人員

累計培訓逾8,000人取得證書、開辦資安實戰訓練、資安菁英人才班、職能及增能訓練、AI資安課程等

114年	115年	116年	117年
培訓逾 2,000人	累計逾 4,000人	累計逾 6,000人	累計逾 8,000人

留才



√擴大適用機關
√增加支給對象

策略二　提升關鍵基礎設施資安韌性

強化我國
關鍵基礎設施資通安全

01
工控系統
深入檢測

02
長期持續監控

03
建立本土自有之網路威脅資料庫

04
擇共通性環境
經驗快速擴散

05
整合現有防護
鏈結本土廠商

06
強化資安
聯防綜效

策略三 壯大我國資安產業

強化政府採購
供應風險管理

- 強化採購契約
- 提升產品安全
- 優質資安服務

推動資通產品
檢測驗證制度

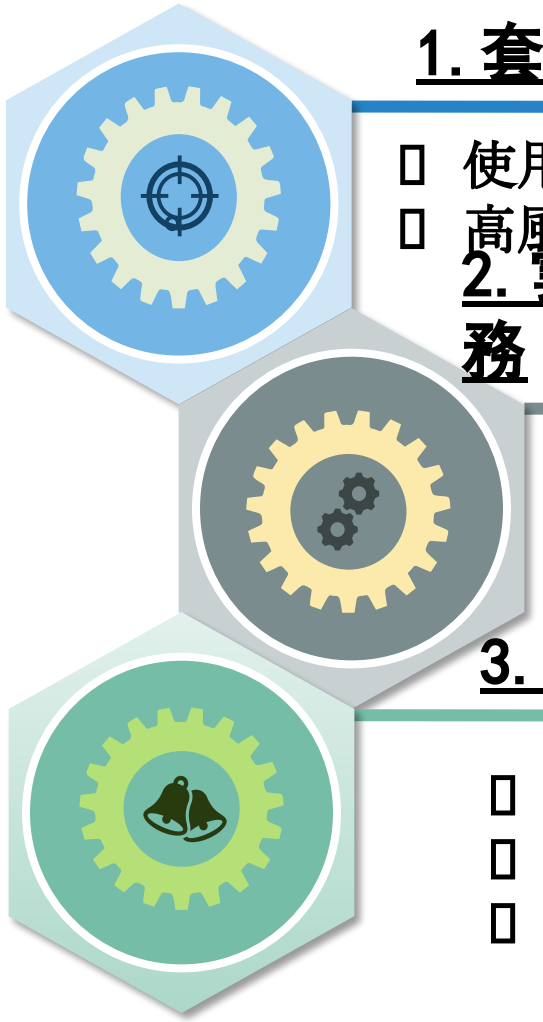
- 國際接軌驗證標準
- 檢測驗證標準
- 公私協力信賴驗證

產業擴大創新
邁向國際市場

- 研發自主資安技術
- 擴大國際輸出
- 資安產業創新
- 參與民主供應鏈
- 資安科技園區

強化政府採購供應風險管理

推動策略



1. 套裝軟體 強化產品安全

- 使用機關數、金額、訂購數量
- 高風險產品(例如資產管理、GCB、防毒等)

2. 雲端/資訊服務 落實資安管理

- 國內雲端服務產商
- 國內資通系統開發及維運廠商

3. 資安服務 精進資安技術

- SOC服務
- 資安健診
- 弱點掃描
- 滲透測試
- 社交工程
- 紅隊演練

1. 推動產品**漏洞獵捕計畫**
2. 增訂上架共契**資安規範**(須通過資安檢測、漏洞更新機制等)

1. 推動導入**PSIRT**機制
2. 透過**資安訪視**輔導廠商落實管理

1. 精進**廠商評鑑**機制
2. **強化**產官合作(資安攻防演練、資安自主 產品)

策略四 AI新興資安科技應用與合作

拓展AI技術 提升資安防護

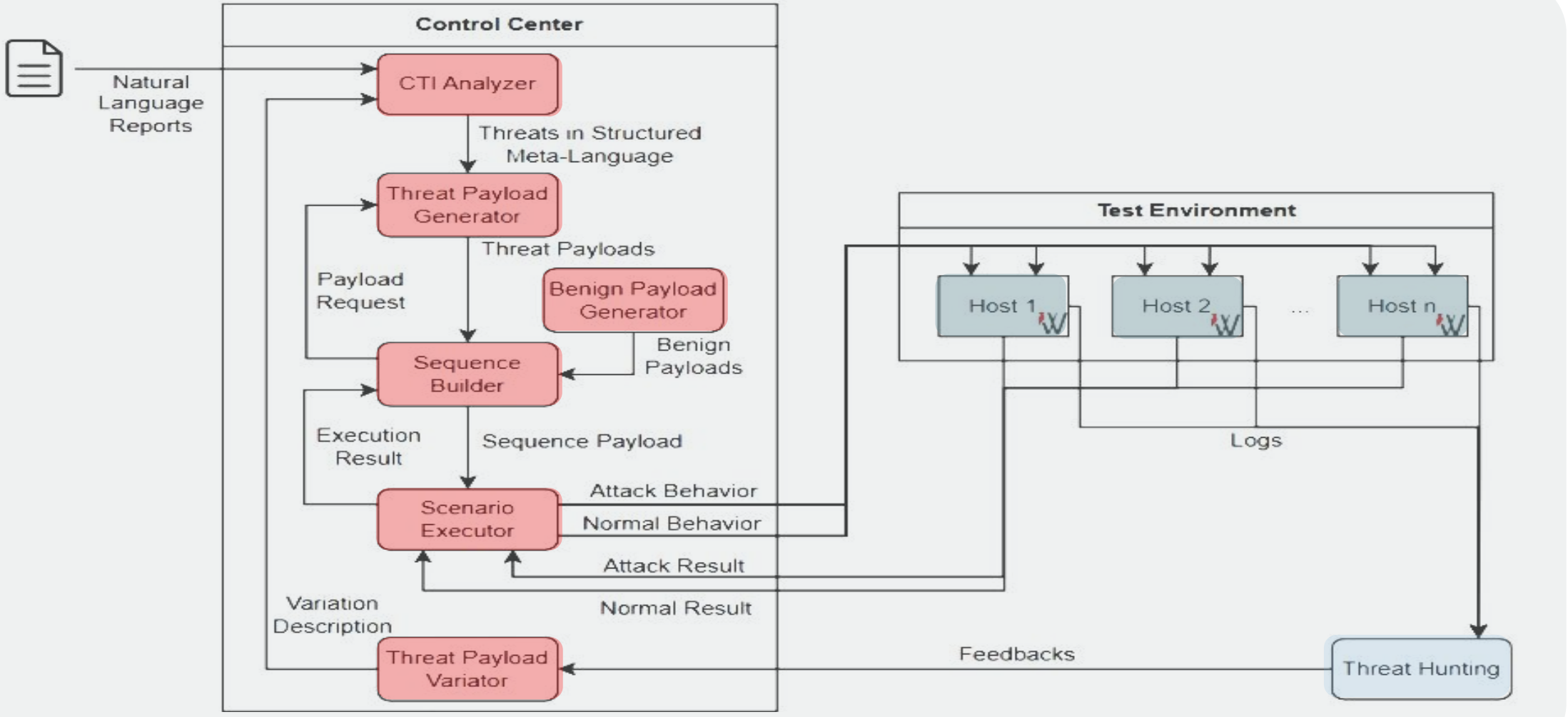
1. 加速情資整合與關聯性分析
2. 自動化產製防護建議
3. 自動化產製具適應性及靈活性之防護規則
4. 威脅模式預警，協助前線資安人員及早應變
5. 升級監控、管理及通報等應變能力

公私協力強化資安聯防

推動後量子加密技術 深化零信任架構

1. 因應量子破密，盤點依賴傳統公鑰密碼演算法之關鍵數位基礎建設
2. 制訂國內後量子密碼遷移策略，進行適切資源分配
3. 建立後量子加密試辦環境並進行概念性驗證。深化零信任機制，逐步導入與整合現有系統

AI模擬資安攻防訓練機制



AI 網路主動式防禦關鍵技術研究

目標

打造下一代AI資安防護系統

運用深度學習技術辨識異常攻擊行為	分析歷史資料預測攻擊模式即時告警	發現威脅主動隔離提升資安防護效率	蒐集全球資安事件即時風險評估因應
AI自動偵測異常行為	智慧預測即時告警	自動化應變防禦機制	整合多來源威脅情報

規劃後量子密碼遷移程序

規劃後量子密碼遷移程序

- 擬定我國政策並對齊國際趨勢
- 盤點現行密碼現況與風險
- 推動政府與CI建立遷移計畫

評估後量子產品評測制度

- 建立一致性的測試流程
- 提供機關透明決策依據
- 發展標準化測試項目及自動化測試流程

預期達成效果

- 提升密碼安全意識
- 政策與制度接軌
- 政府整體遷移規劃


千江有水千江月
資安有如千手觀音守護著我們