第一銀行 First Bank

www.firstbank.com.tw

第一銀行
金融資安精進措施經驗分享

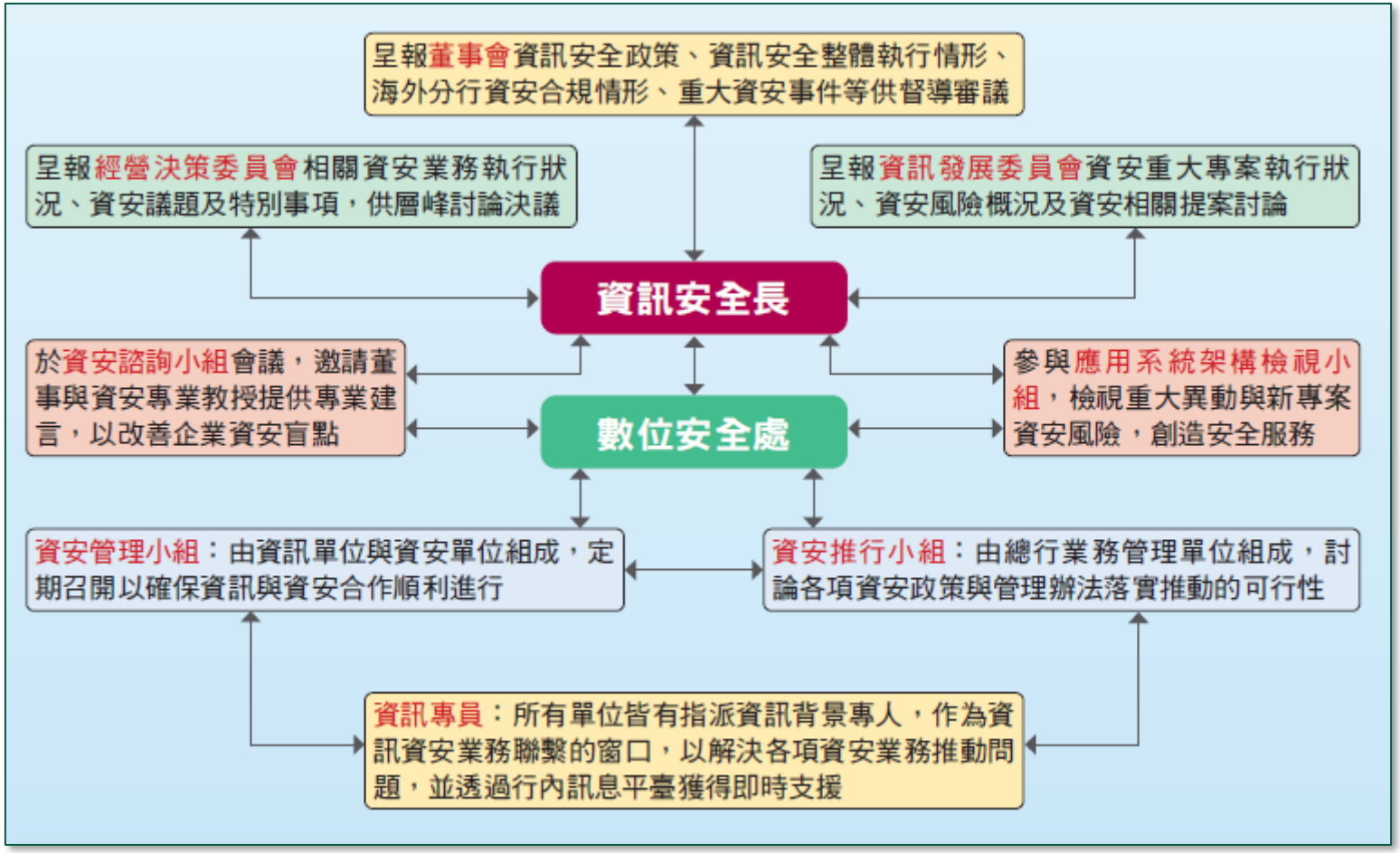
報告人：劉培文副總經理

資安長核心能力

- 資安的核心價值是讓企業在資安風險可控的狀況下全速前進
- 資安長核心能力

- 透過定期資安長聯繫會議，提升資安聯防量能

完備的資安組織

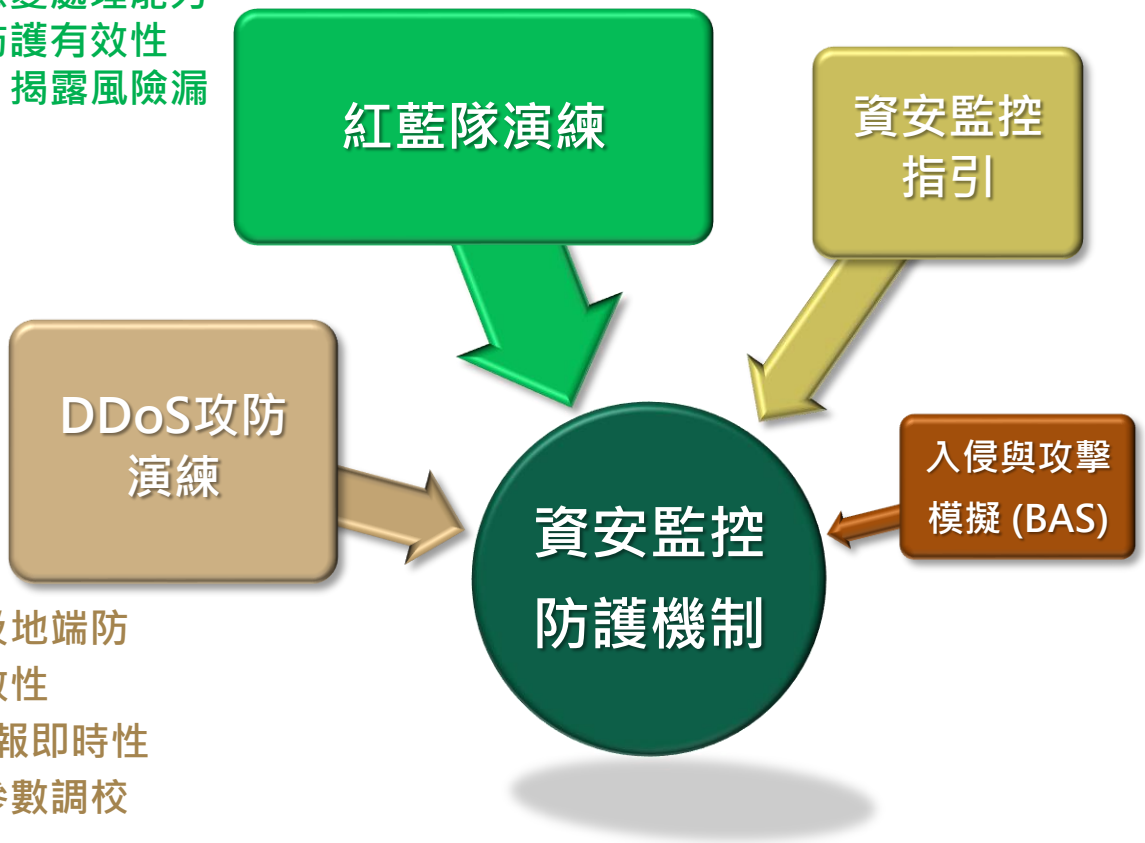

呈報董事會資訊安全政策、資訊安全整體執行情形、海外分行資安合規情形、重大資安事件等供督導審議
呈報經營決策委員會相關資安業務執行狀況、資安議題及特別事項，供層峰討論決議
呈報資訊發展委員會資安重大專案執行狀況、資安風險概況及資安相關提案討論
資訊安全長
於資安諮詢小組會議，邀請董事與資安專業教授提供專業建言，以改善企業資安盲點
數位安全處
參與應用系統架構檢視小組，檢視重大異動與新專案資安風險，創造安全服務
資安管理小組：由資訊單位與資安單位組成，定期召開以確保資訊與資安合作順利進行
資安推行小組：由總行業務管理單位組成，討論各項資安政策與管理辦法落實推動的可行性
資訊專員：所有單位皆有指派資訊背景專人，作為資訊資安業務聯繫的窗口，以解決各項資安業務推動問題，並透過行內訊息平臺獲得即時支援

核心資料保全與營運持續

- 導入軟體定義網路(SDN)架構
- 建構主/備雙活中心提升持續營運
- 使用雲端備份確保核心資料保全
- 取得ISO 22301持續營運認證

資安監控防護之有效性評估

- ✓ 選擇最佳專業廠商執行
- ✓ 反映人員及委外廠商即時通報及應變處理能力
- ✓ 確認監控防護有效性
- ✓ 深度滲透，揭露風險漏洞



- ✓ 參與監控及組態指引訂定
- ✓ 參照MITRE ATT&CK共制定300條以上監控規則
- ✓ 定期檢討監控狀況及調整規則

- ✓ 驗證雲端及地端防護機制有效性
- ✓ 驗證ISP通報即時性
- ✓ 優化設備參數調校

- ✓ 持續性且自動化驗證防護機制有效性
- ✓ 資安人力有限之單位有所幫助

零信任架構部署

選定目標及方法
- ✓ 採用CISA Maturity Model結合27001管理制度，訂定成熟度目標並每年評估本行零信任成熟度現況
- ✓ 建立單一場域/系統零信任成熟度評分表

建立零信任基礎架構
依資通安全研究院建議，規劃資源入口架構，導入身分鑑別、設備鑑別及信任推斷系統，同時搭配微分段系統進行存取最小化限制，降低橫向移動之風險

策略執行與分析
- ✓ 依成熟度評分表找出各面向不足之處進行補強(身分、設備、網路、應用程式及資料)
- ✓ 部署提供各面向成熟度所需之零信任工具，逐漸滿足滿零信任架構原則

挑選先導試行場域
- ✓ 挑選一個風險與衝擊小的場域/系統優先導入
- ✓ 使用成熟度評分表評估所需納入的零信任元件(如MFA)

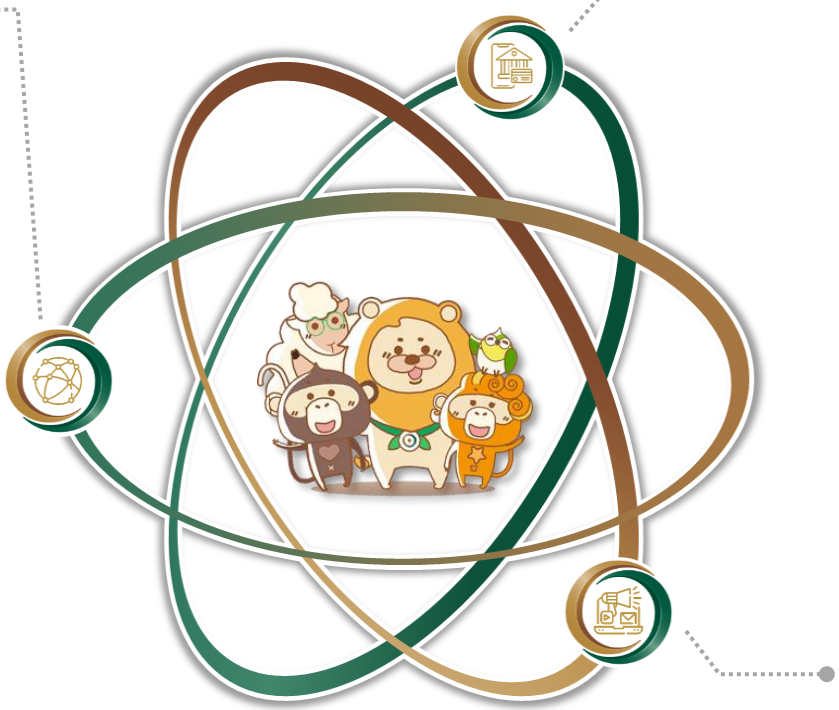
持續優化與改善
- ✓ 持續收集資料並優化信任推斷原則
- ✓ 基於條件(Criteria-versus)動態授予存取權限
- ✓ 根據風險評分(score-based)決定是否允許存取

持續導入與精進
- ✓ 於新系統建立/舊系統提升前執行成熟度評分表
- ✓ 評分表強度不足之相面納入零信任元件補強
- ✓ 依各系統特性持續評估導入不同的零信任工具/元件
- ✓ 持續將所有系統均納入零信任架構

多元專長資安人才

持續培訓

- ✓ 透過各類專案舉辦專業技術課程
- ✓ 補助同仁取得高階國際資安證照及參加外部專業課程
- ✓ 鼓勵參與外部技術討論會、各類演練、競賽等以獲得實作經驗
- ✓ 推派資安主管參與金融資安高階主管儲訓計劃(CISE)
- ✓ 參與國際資安研討會(如Black Hat、RSA、Gartner)



專業多元化

- ✓ 招募及配置多元資安人才，包含資安管理、遵法、防禦、檢測、監控及鑑識等，強化整體資安防護量能

知識分享

- ✓ 定期技術月會、法規宣導與讀書心得分享，藉由知識分享，促進經驗交流與傳承
- ✓ 建立主責業務輪調機制，藉此使同仁不侷限單一技術經驗

發揮資安聯防

攻防演訓量能

培養本行資安防護團隊，透過參與攻防演練，提升本行防禦量能

防駭壓力測試 金融業10月大演練

2023.09.25 / 03:00 / 工商時報 孫彬訓

史上最大規模，金融業防駭演練10月將進入第二階段。 圖／摘自unsplash網站

史上最大規模金融業防駭演練時程

演練名稱	首屆「金融資安攻防演練及評比活動」
辦理單位	金融資安資訊分享與分析中心(F-ISAC)
第一階段時間／地點	7月3日至9月29日／金融研訓院芬恩特創新聚落
第二階段時間／地點	10月11日至10月31日／聯徵中心

資料來源：綜合整理　　製表：孫彬訓

史上最大規模金融業防駭演練時程

金融業史上最大規模防駭演練下半年啟動，10月將進入第二階段，各金融業無不積極組隊參與報名，以擬真的架構分組演練，希望強化應變處理的實際能力。

據悉，這次是金管會為推動「金融資安行動方案2.0」，希望透過實際演練提升資安人員技術及應變能力，今年委由金融資安資訊分享與分析中心（F-ISAC）辦理首屆「金融資安攻防演練及評比活動」。參與銀行主管指出，這次活動是以

第一銀行 First Bank

www.firstbank.com.tw

John Kindervag 的零信任是一種策略

1. 首先必須認知不論我們在網際空間的哪裡，我們永遠身處在一個已被入侵的環境(*Assumed Breach*)
2. 其次，策略上最優先的是要定義出網際空間中，我們皇冠上的寶石(*Crown Jewel*)是什麼。寶石就是最重要最關鍵系統上的資料，例如身份、應用資料、系統設定等等，你得自己定義。
3. 圍繞著這個寶石定義出保護表面(*Protect Surface*)
   - 定義出誰、在什麼時候、從什麼管道位置、因為什麼原因、可以如何存取這個寶石，不屬於這樣的行為，就是不被信任的行為。
4. 把前述行為相關的紀錄及背後代表的行為進行持續的監控。
5. 針對二級重要、三級重要的寶石重複*2~4*的作法進行辨識、定義存取行為、收集行為記錄進行監控

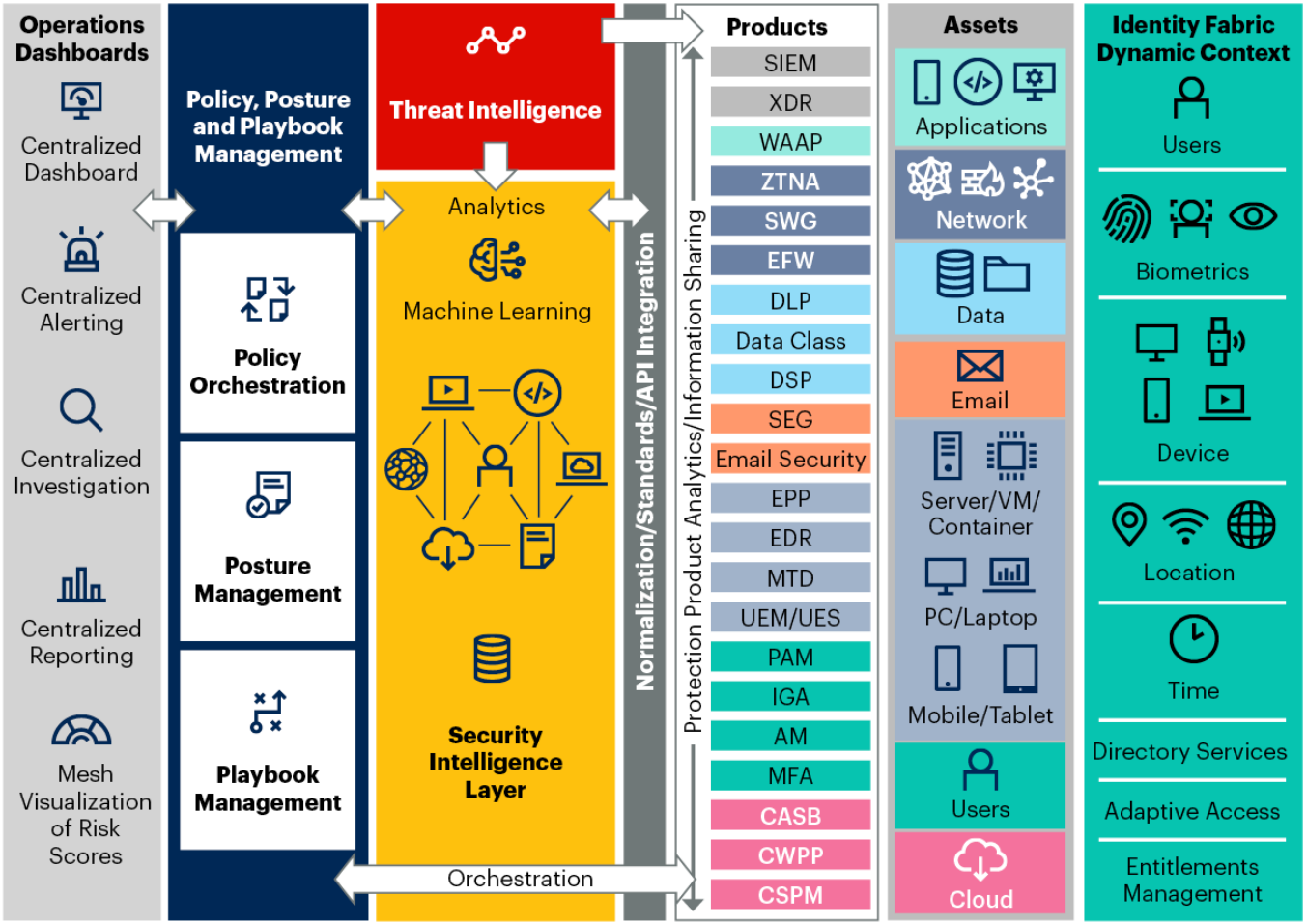
John Kindervag 的零信任重點

1.是一種*inside-out*的策略：先從最重要、最核心、最小的保護表面開始

2.要落實這個策略，未必需要投資新的資安設備

3.要將資安監控高階化、智慧化，也就是資安監控不是只看資安設備的*log*，而是要往第七層走，對真正重要的應用資料存取行為進行監控

Gartner Cyber Security Mesh Architecture



Source: Gartner

Note: Products included in the diagram are not all of the products that can be included but an example list of possible tools that protect assets

754315_C

JK Zero Trust vs. Gartner CSMA

- *JK*的零信任是見樹的資安策略(*Strategy*)

  *CSMA*是見林的資安參考架構(*Reference Architecture*)。
- *JK*的零信任是*Inside-out*的策略

  *CSMA*則是*Outside-in*的架構
- 目前業界很多零信任解決方案可以嵌入到*CSMA*的架構中(例如*ZTNA*)，其主要目的比較偏向縮小被攻擊的表面(*Attacked Surface*)。