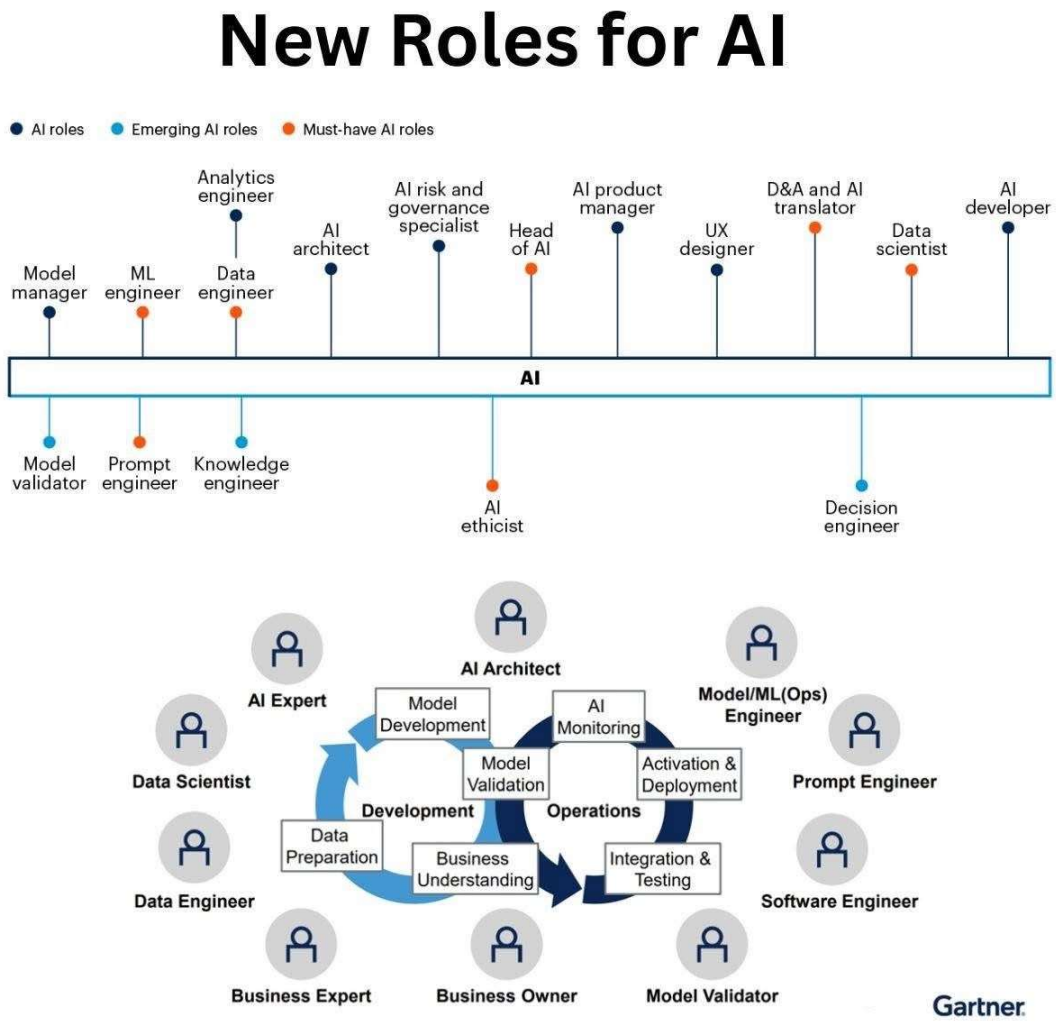
跨域觀點-AI趨勢與資安威脅

- 余俊賢 Jack

大綱

- AI趨勢
- 資安威脅演進 v.s. 零信任架構

誰會被取代？


New Roles for AI
AI roles
Emerging AI roles
Must-have AI roles
Model manager
ML engineer
Analytics engineer
Data engineer
AI architect
AI risk and governance specialist
Head of AI
AI product manager
UX designer
D&A and AI translator
Data scientist
AI developer
AI
Model validator
Prompt engineer
Knowledge engineer
AI ethicist
Decision engineer
AI Architect
AI Expert
Model/ML(Ops) Engineer
Data Scientist
Prompt Engineer
Model Development
AI Monitoring
Model Validation
Activation & Deployment
Development
Operations
Data Preparation
Business Understanding
Integration & Testing
Data Engineer
Software Engineer
Business Expert
Business Owner
Model Validator
Gartner

- 資料分析師
- 資料工程師
- 資料科學家

- 深入了解機器學習技術和程式語言，強大的統計和分析技能，以及熟悉有助於處理大量資料的軟體工具。
- 了解基本的統計原則，清理不同類型的資料，資料視覺化和探索性資料分析。
- 能確保資料庫保持穩定，並維護資料庫的備份，執行資料庫更新和修改。
- 了解資料獲取和儲存的架構和分佈，掌握多種程式語言（包括 Python 和 Java），並了解 SQL 資料庫設計。

- 利用現有工具和問題解決方法來查詢和處理資料，提供報告，總結和將資料視覺化。
- 建立並營運資料管道以收集和整理資料，同時確保資料的可存取性和質量。
- 應用統計、機器學習和分析方法來解釋並交付視覺化的結果，以解決關鍵商業問題。

資料分析師

- 資料分析師負責查詢、處理、提供報告、總結和可視化資料。
- 他們利用現有的工具和方法來解決問題，並幫助像是業務分析師的人員透過即時報告和圖表理解特定的查詢。
- 資料分析師必須了解基本的統計原則、清理不同類型的數據、數據可視化和探索性資料分析。
- 簡而言之，資料分析師透過分析資料幫助企業和其他組織做出明智的決策。

資料工程師

- 資料工程師負責建立和維運資料管道，以收集和整理資料。
- 他們通過整合來自不同來源的資料，並執行資料清理和轉換，確保資料科學家和資料分析師能夠存取並使用高品質的資料。
- 資料工程師需要具備的技能包括了解資料攝取、轉換和儲存的架構、工具和方法；並且精通多種程式語言（包括 Python 和 Scala）。
- 總結來說，資料工程師建立並維運資料基礎設施，為資料分析師和資料科學家進一步分析資料做好準備。

資料科學家

- 資料科學家應用統計學、機器學習和分析方法來解答關鍵的商業問題。
- 資料科學家透過使用視覺化技術、建立資料科學應用程式或講述有趣的故事來詮釋並傳達他們的研究結果，並解決他們的資料（商業）問題。
- 他們處理不同規模的資料集，並對大規模資料集運行演算法。
- 資料科學家必須跟上最新的自動化和機器學習技術。
- 執行這些角色的要求包括統計和分析能力、程式設計知識（如 Python、R、Java）以及熟悉 Hadoop（一套開源軟體工具，便於處理大量資料）。
- 資料科學家是資料管理者，負責組織資料並從中提取價值。

資料分析案例

- **情境 1**：零售公司的行銷部門希望擴大市場佔有率並能更積極地應對市場變化。他們決定聘請一位資料專業人員，負責開發預測模型，以識別公司的新市場並預測外部市場力量對業務的影響。
- **情境 2**：FBN 製造公司的管理層對員工流動率過高表示擔憂。他們決定聘用一名資料專業人員審查公司內部資料庫，收集並分析相關資料，並製作一份有關員工留任的報告，將其呈交給公司領導層。
- **情境 3**：大城市醫院的帳單部門需要改善處理醫療理賠的業務流程。作為流程改善專案的一部分，他們決定引入一個資料專業人員以創建一個新的框架來收集資料並建立必要的工具來實現自動化資料收集。

推薦自學資源

- 高雄亞灣
- 線上課程

https://www.asiabaykh.com/

Copyright Lawsuits v. AI Companies

Canada

CanLII v. Caseway AI
Supreme Ct. of British Columbia

Toronto Star News. v. OpenAI
Ontario Superior Ct. of J.

UK

Getty Images (US) v. Stability AI Ltd.
High Court of Justice in London

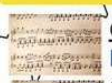
Netherlands

DPG Media v. HowardsHome: TDM exception
Amsterdam Dist. Court

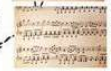
France

National Publishing Union v. Meta
Tribunal Judiciarie de Paris

Germany



GEMA v. OpenAI
Munich Regional Court



GEMA v. Suno
Munich Regional Court

Kneschke v. LAOIN
Hamburg Regional Court

South Korea

Korean Broad. Assn. v. Naver
Seoul Central Dist. Court

China

Shanghai Character License Administrative Co. v. TAB
Guangzhou Internet Court

India

Asian News Int'l. v. OpenAI
New Delhi Court

Copyright + Related Lawsuits v. AI Companies

prepared by ChatGPTiseatingtheworld.com
Mar. 29, 2025

資安Q&A

- 醫療辦公室的員工向患者發送有關其最近就診的電子郵件。如果電子郵件中包含以下哪些訊息，將會危及患者的隱私？
  - 下一次約診
  - 聯絡資訊
  - 姓名和名字
  - 病患記錄

資安Q&A

- 以下哪些安全應用使用了生物辨識技術？請選擇兩個正確答案。
  - 聲音辨識
  - 信用卡
  - 指紋辨識
  - 鑰匙扣
  - 手機

資安Q&A

- 當員工從公司外部連接到企業網路時，公司要求使用安全的加密網路連線。員工旅行並使用筆記型電腦時應該使用哪種技術？
  - 藍牙
  - Siri
  - Wi-Fi 熱點
  - VPN

案例列 慧工 工廠資安全 OT

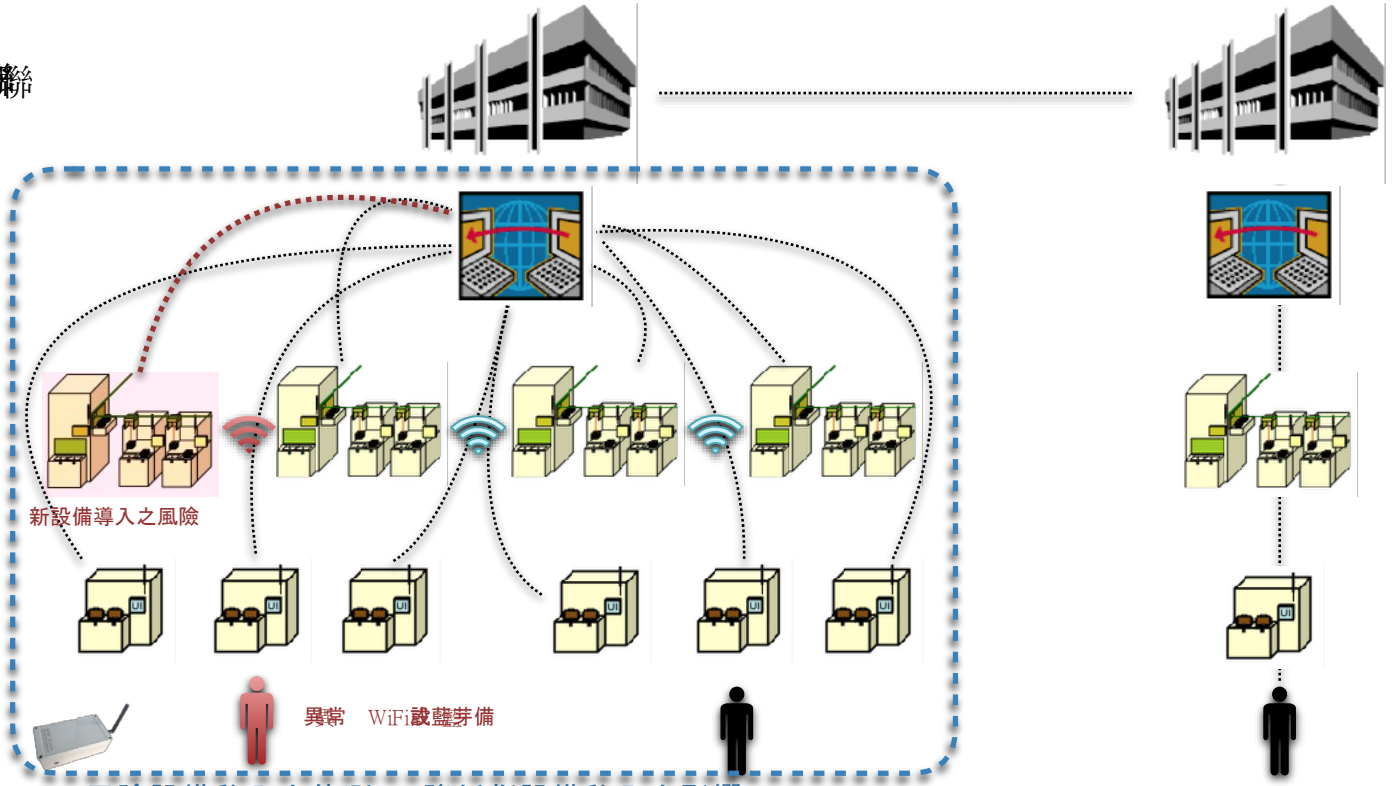
廠區間資訊互聯

工廠製程參參
數資訊串流

系統之資訊串流

生產設備

工廠人員



1. 風險設備移入之偵測 (可降低新設備移入之影響)
2. 異常無線設備偵測 (可偵出惡意擊之)
3. 白名機制 (不影響機常生產設備或系統)
4. 聯防制 (可避免災情擴散)

互聯安睿資通

攻擊者透過賭場魚缸溫度感測器入侵賭場資料庫偷走資料

- 物聯網裝置，如IP Cam、空調、溫控器、冰箱、HVAC系統等，逐漸成為駭客攻擊的目標
- 這些物聯網裝置大大地增加了攻擊面(attack surface)，且往往成為入侵目標網路的跳板

- 賭場資安事件
  - 駭客駭入大廳水族箱的溫度計
  - 以該溫度計作為攻擊內部網路的跳板
  - 駭客接著找到並攻擊賭場核心伺服器，並將其資料上傳雲端
- 英國GCHQ的前任官員表示
  - 被駭客作為攻擊目標的物聯網裝置對企業造成的影響與日俱增
  - 需要法規化要求這些物聯網裝置符合最低安全標準

養雞場

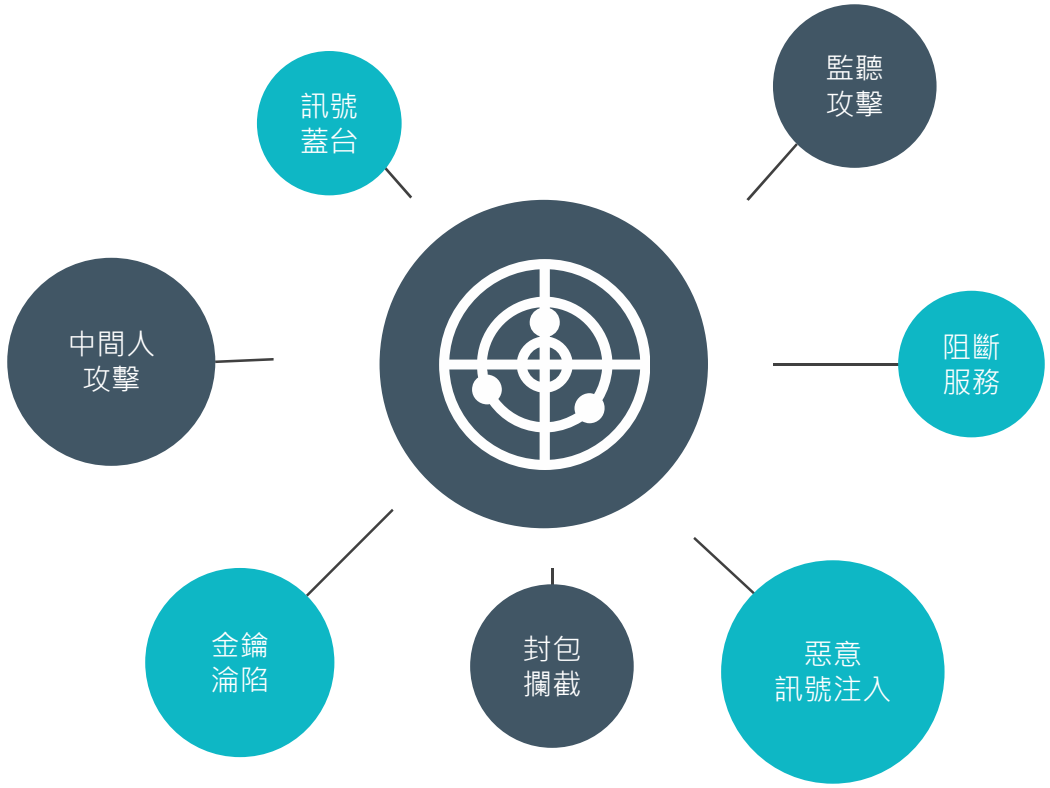
Source: http://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4

手法	衝擊	發現時機
攻擊WiFi AP、物聯網裝置	WiFi 受害及其網路區段成為跳板	攻擊中，攻擊後傳輸異常
WiFi WPA2 KRACK	破解WPA2	大量截收資訊（不會被發現）
中間人攻擊Rough WiFi AP, BLE	中間人攻擊取得資料	出現憑證錯誤
藍芽(Blue Borne)、WiFi Worm	造成感染影響正常營運	被癱瘓時發現
DigiWallet Thief	數位錢包與身分竊取	資料使用時發現
WiFi, BLE DoS	透過攻擊使訊號中斷	服務中斷時發現
供應鏈攜入	故障、內部風險擴散	發生故障、擴散時
App (iPad, Android)	裝置受外來攻擊	資料使用或異常傳輸時發現

供應鏈資安

- 軟體供應鏈：第三方元件安全 NIST / Software Bill of Materials (SBOM)
- 合約、保險
- 委外遠端維護 VPN , Token 多因素認證
- 跳板機記錄（螢幕錄影）
- 新設備入廠驗證機制
- 外部、測試區、上線監控

存在風險



Problems

駭客攻擊

- SCADA/ICS
- 工業4.0
- 無人銷售業
- 數位分行

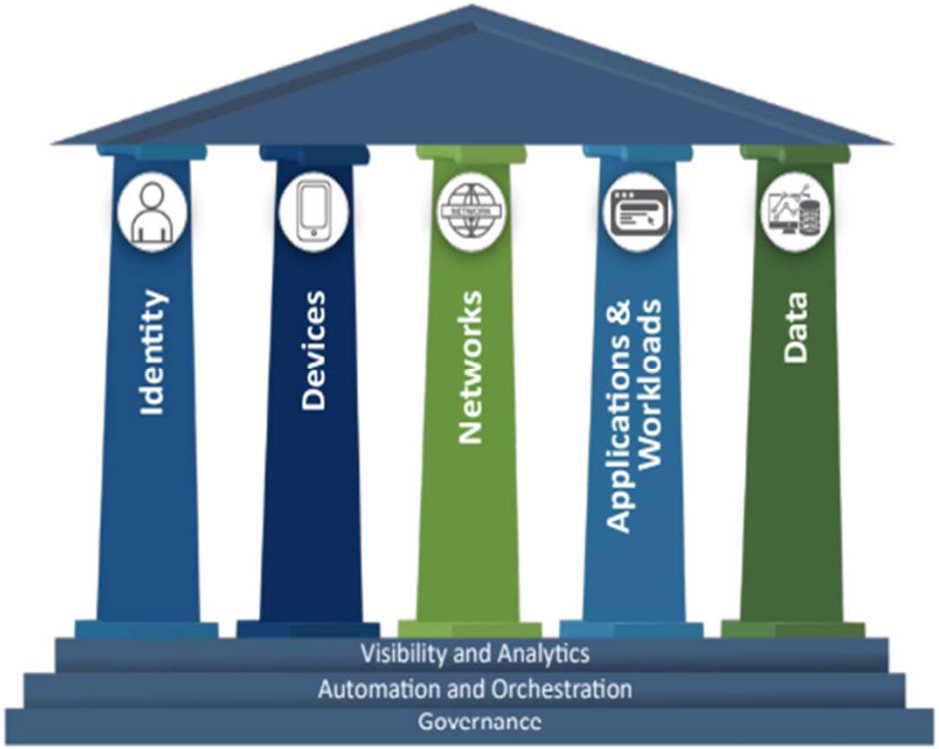
影響

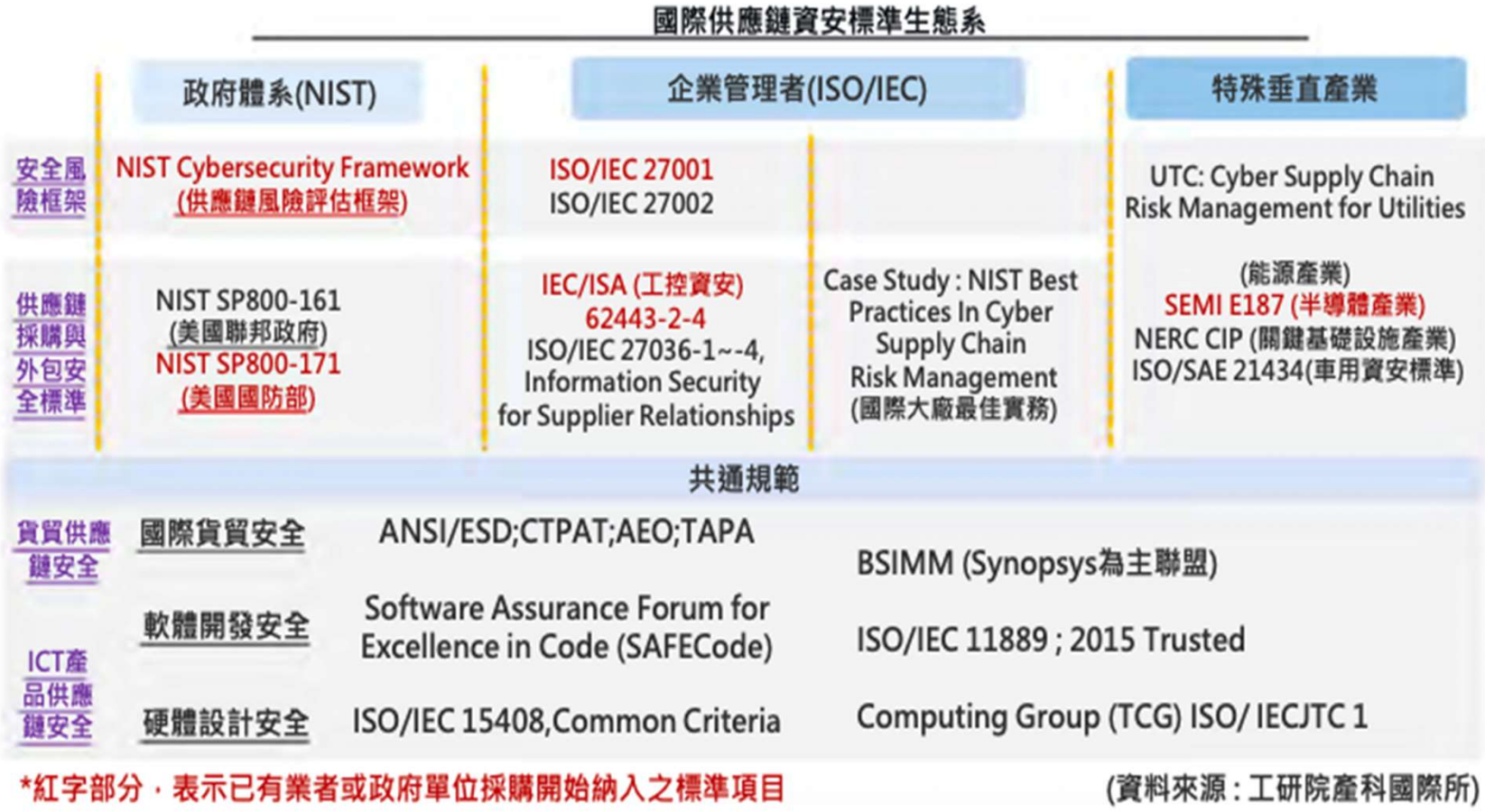
- 重大基礎設施
- 智慧工廠
- 民生銷售商店
- 金融單位

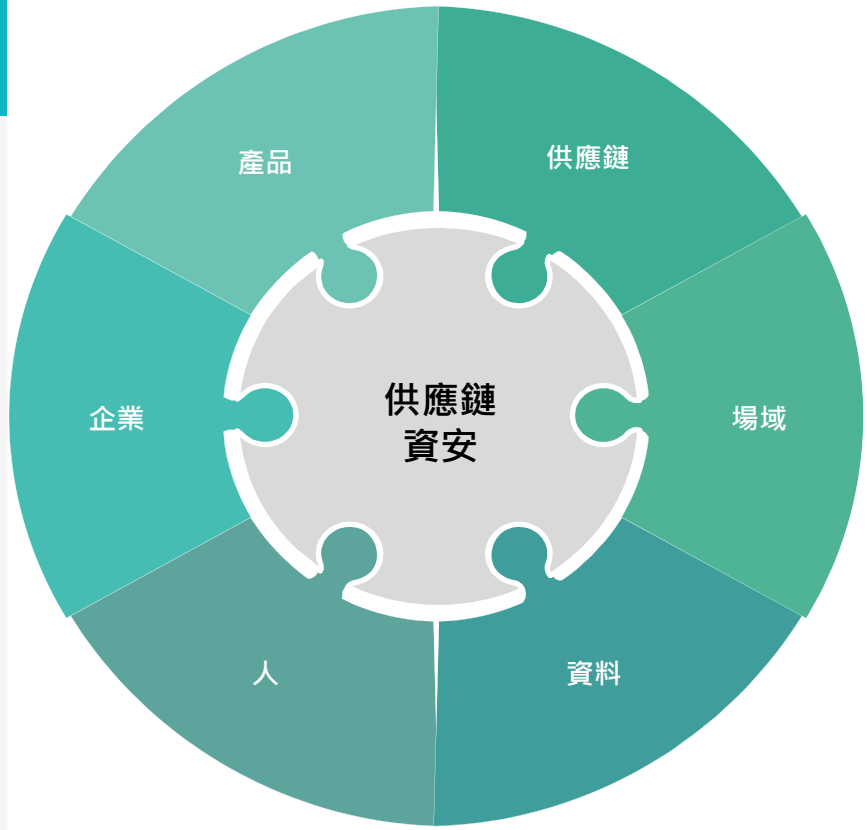
市場

- 侵入系統以控制化學、電力、水源、交通等公領域設施的事件比例，已增加了17倍
- 2018年全球工廠總計將有大約130萬套工業機器人
- 2014~2018 年美國自動販賣機預期複合增長率高於 54.3%

資安新顯學
Zero Trust 架構




國際供應鏈資安標準生態系
政府體系(NIST)
企業管理者(ISO/IEC)
特殊垂直產業
安全風險框架
NIST Cybersecurity Framework
(供應鏈風險評估框架)
ISO/IEC 27001
ISO/IEC 27002
UTC: Cyber Supply Chain Risk Management for Utilities
供應鏈採購與外包安全標準
NIST SP800-161
(美國聯邦政府)
NIST SP800-171
(美國國防部)
IEC/ISA (工控資安)
62443-2-4
ISO/IEC 27036-1~-4, Information Security for Supplier Relationships
Case Study : NIST Best Practices In Cyber Supply Chain Risk Management
(國際大廠最佳實務)
(能源產業)
SEMI E187 (半導體產業)
NERC CIP (關鍵基礎設施產業)
ISO/SAE 21434(車用資安標準)
共通規範
貨貿供應鏈安全
國際貨貿安全
ANSI/ESD;CTPAT;AEO;TAPA
BSIMM (Synopsys為主聯盟)
ICT產品供應鏈安全
軟體開發安全
Software Assurance Forum for Excellence in Code (SAFECode)
ISO/IEC 11889 ; 2015 Trusted
硬體設計安全
ISO/IEC 15408,Common Criteria
Computing Group (TCG) ISO/ IECJTC 1
*紅字部分，表示已有業者或政府單位採購開始納入之標準項目
(資料來源：工研院產科國際所)



- 零信任架構
- 產品、方案
  - 物聯網檢測
  - 黑箱及白箱檢測
- 對輔導對象及供應鏈
  - 網站程式異動監控
  - 源碼檢測
  - 系統弱點掃描
  - 網站弱點掃描
  - 滲透測試
  - 資安健診
  - 電子郵件警覺性測試

防範

惡意RF識別
遠端入侵
監控實體資產
內與外部威脅

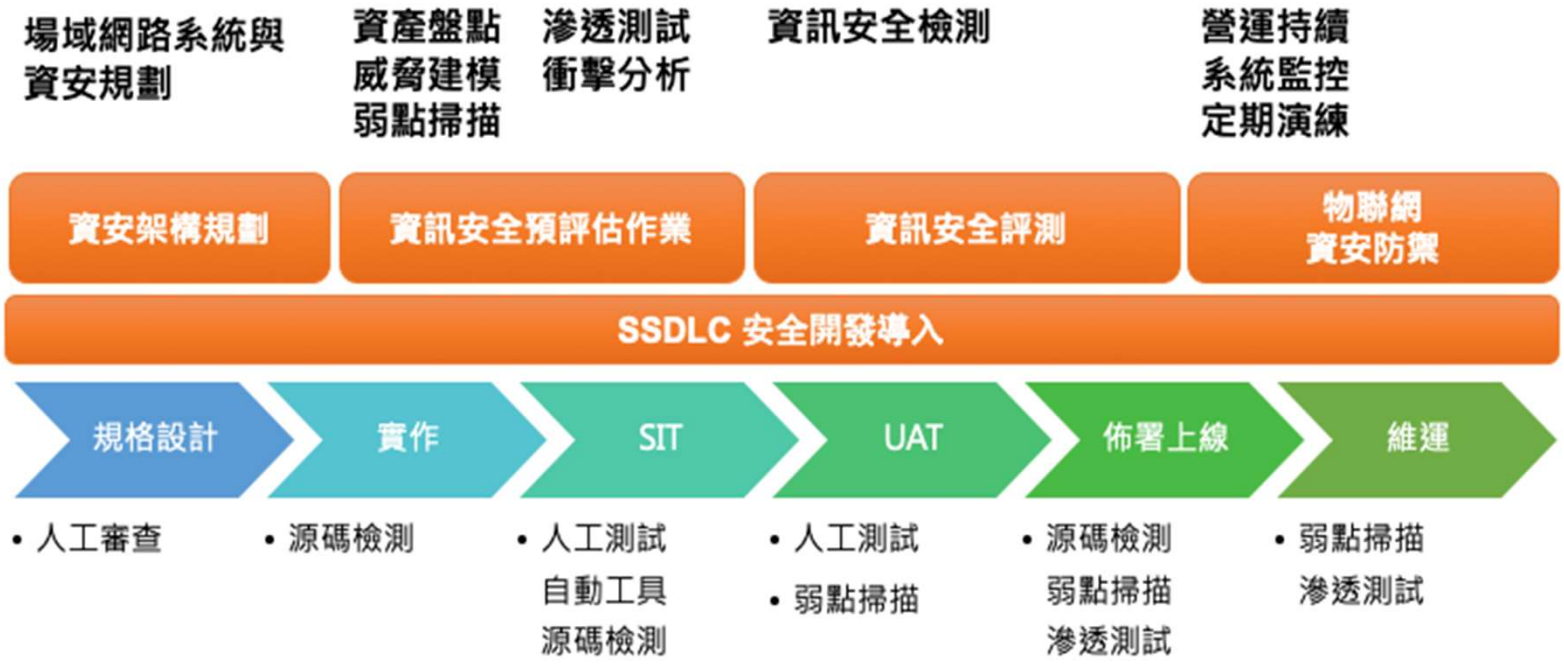
阻擋

風險感染
封包攔截
竊聽攻擊
DDos攻擊
中間人攻擊

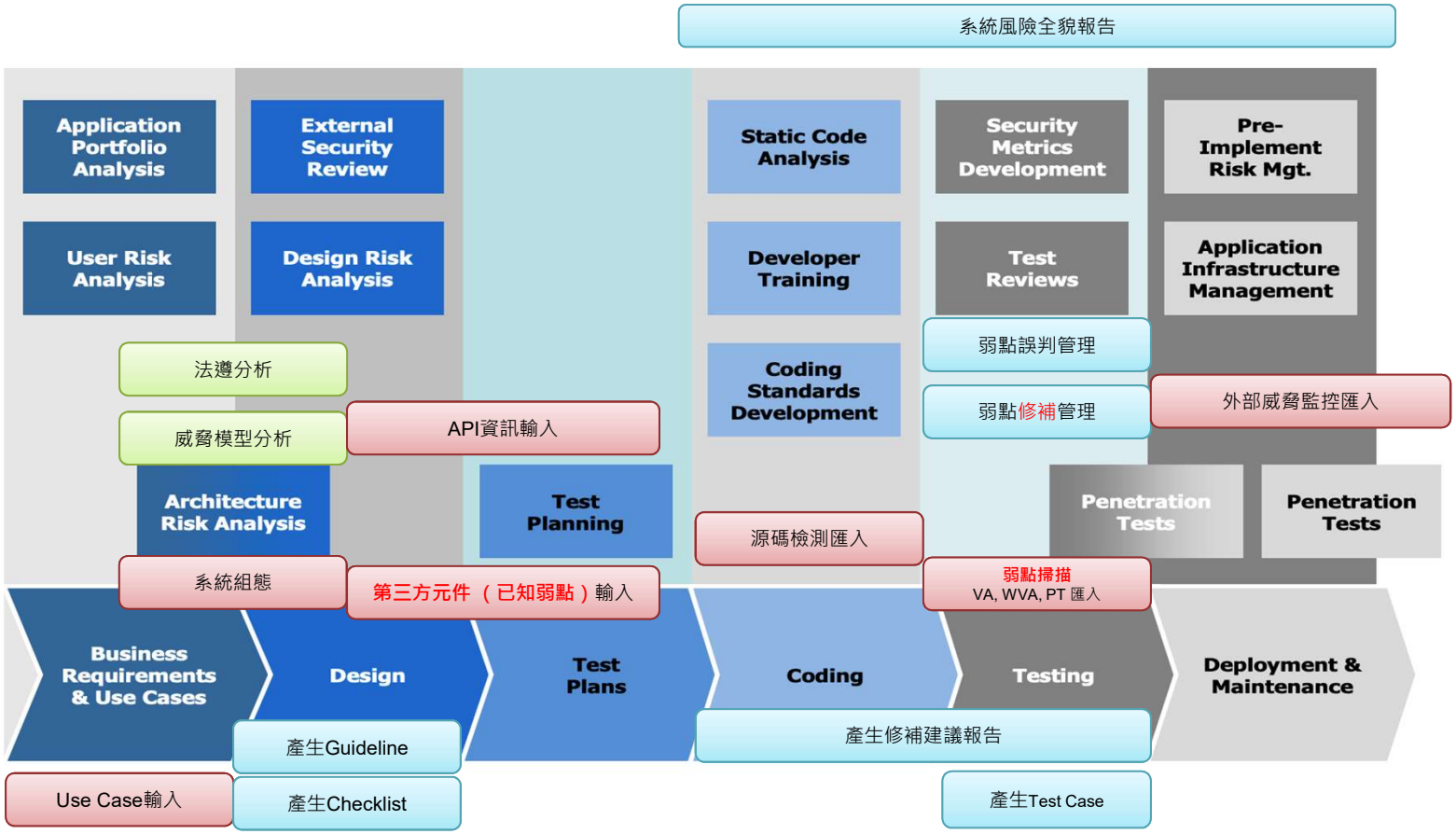
成效

降低風險
威脅分析
網路保護
安全通訊
降低營運損失

資訊系統
安全開發生命週期



SSDLC Map


系統風險全貌報告
Application Portfolio Analysis
External Security Review
Static Code Analysis
Security Metrics Development
Pre-Implement Risk Mgt.
User Risk Analysis
Design Risk Analysis
Developer Training
Test Reviews
Application Infrastructure Management
弱點誤判管理
法遵分析
Coding Standards Development
弱點修補管理
外部威脅監控匯入
威脅模型分析
API資訊輸入
Architecture Risk Analysis
Test Planning
Penetration Tests
Penetration Tests
源碼檢測匯入
系統組態
第三方元件（已知弱點）輸入
弱點掃描
VA, WVA, PT 匯入
Business Requirements & Use Cases
Design
Test Plans
Coding
Testing
Deployment & Maintenance
產生Guideline
產生修補建議報告
Use Case輸入
產生Checklist
產生Test Case