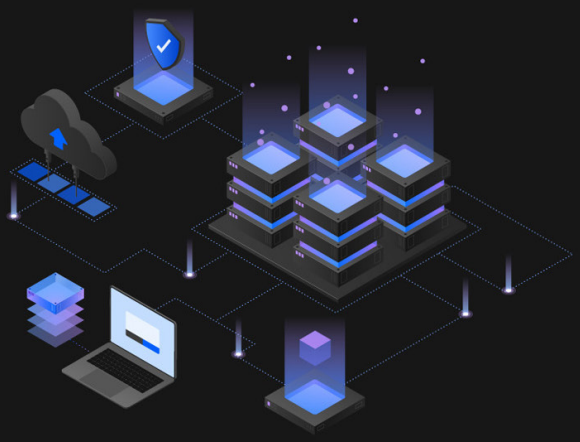


IOT/OT 與資安韌性

近年來資安界最火熱的議題，莫非是 NIST Cybersecurity Framework (2018/4) 改版，與 MITRE ATT & CK (2018/1) 的發布。前者強化了身分驗證識別、風險自評、供應鏈安全，後者透過首次發布的共通描述攻擊手法框架，使資安界各業人士能有一共通語言。而 Resilience（韌性）一詞更是資安界最耳熟能詳的字詞。

資安治理

資安韌性脫離不了企業對於公司治理的思維。OECD 資安治理是目前最被台灣企業界廣泛使用的公司治理原則，也是主管機關宣導公司治理的重要指標之一。公司治理涵蓋六大原則，包含治理的有效性、保障股東權益、證券市場與投資人、利害關係人權益、資訊揭露與透明性、與落實董事會責任。

其中以證券市場與投資人為例，道瓊永續經營指數 (Dow Jones Sustainability Indices, DJSI) 為公司治理的金像獎， 台灣 2020年僅有 26家入選，DJSI 在 2020年最顯著的改變，是加入 Information Security & Cybersecurity 項目，強調企業遭受攻擊時，如何妥適的處理資安事件，此外，隱私權保護亦加入 2020年度評比項目。

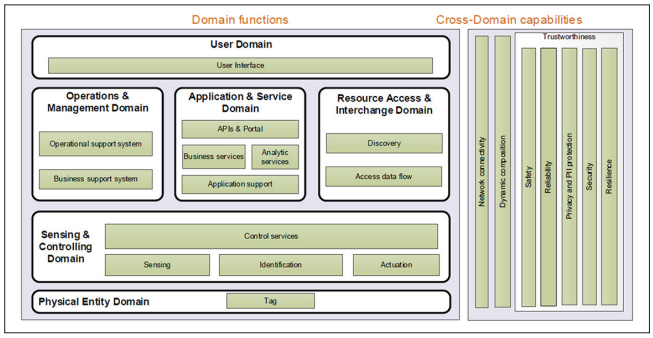
此外，在台灣現行法規體制下，資訊揭露透明性牽涉上市公司年報之資安風險揭露 (風險預防、緊急應變、危機管理、營運持續)，從風管組織架構、資訊安全政策、風險管理系統、資安風險評估、資安管理系統驗證、資安保險的安排，到發生重大資安事件之影響與因應措施，必須呈現於年報上揭露於投資人與社會大眾。

企業做為社會公民所發布的 CSR 企業社會責任報告書，在資訊系統風險項目中，亦有一項資訊安全，闡述企業是否對於資安審查引入外部顧問，完善資訊安全系統，符合資訊安全法規 (如台灣現地個資法、資通安全法，或是外地法規，如 GDPR)。

所以董事會的責任，在於各地法規的遵守與落地執行項目不同，而有所區別，跨國公司為例，除了業務面遵守當地法規之外，不同區域與不同國家另有相關法規與稽核框架，也是必須考慮的。

IOT 的可信賴度 (Trustworthiness)

作為資訊業界標準龍頭，ISO 在 2018年 8月公布 ISO/IEC 30141:2018 IOT Reference Architecture，作為物聯網最頂層的參考架構，包括各種營運、監管、技術等情境考慮在內，亦將 Resilience 一詞定義於跨領域能力的可信賴度 (Trustworthiness) 內，其中包括安全 (Safety)、資安 (Security)、隱私 (Privacy)、可靠性 (Reliability)、韌性 (Resilience)，此處的韌性是以技術面的角度，闡釋 IOT 系統與設備對於在事故後快速回復正常運作狀態的能力。



IOT MITRE ATT&CK ICS

備受矚目的 Mitre ATT&CK 在 2020年 1月發表新版 ICS 版本攻擊矩陣，協助各路資安專家評估資安攻擊防禦強度，增進保護 ICS 系統能力。

以攻擊手法 Initial Access - Internet Accessible Device (T883) 為例，保護 Internet 直連的 ICS 系統視為首要目標。通常這類設備會帶有特定資安控制措施 (如防火牆、加密通道、VLAN、網段隔離或密碼設定)，但不當的或錯誤的設定與政策，無法防止駭客或有心人士的入侵。

如何避免或防止這類情事發生?

1. 設備清單或資產清單 (或資產管理資料庫) 是必要的。清查網路，找出未知或沒有被管理到的黑設備。

2. 監視並控制各種連線。不應該出現的對外連線 (連接到中繼站 ?)，預期中的連線 (設備更新 ?)，或是暫時性的連線 (管理工作或是除錯管理) 應該要了然於胸。然而當設備處於不當連線狀態，是否可監控該連線，告警並進一步阻斷，取決於資訊工具的能力。

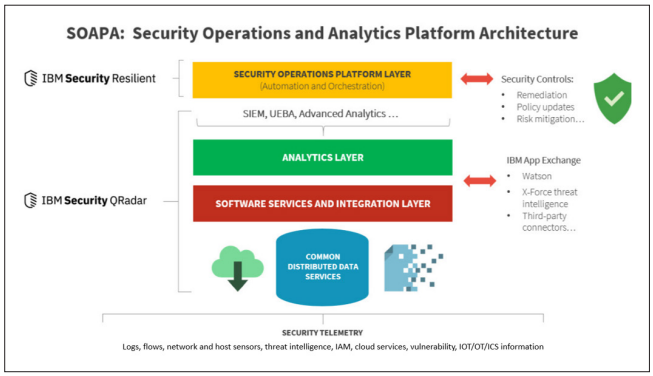
3. 「設後不理」不應該出現在資訊安全系統管理之中。一般在做系統或設備除錯工作時常常會開啟最大權限 (設備最大權限，或網路通過最大權限) 加快除錯腳步。揮汗完成辛苦的工作後，常常忘了最後一步，必須將權限回復至原始設定 (如權限之 Least Privilege 或 Segregation of Duty)，所以導入 IAM 或 PAM 系統有其必要性，此外定期稽核亦有助於管理這類的錯誤產生。

可視度是關鍵

所謂知己知彼，百戰不怠。雷達是軍事戰爭中最重要的偵測工具，現行軍武所謂視距外作戰或視距外作戰，非常仰賴雷達各項偵蒐性能，戰機上所配備的 AESA 電子掃描陣列先進雷達，可協助戰機同時進行對空、對地多目標接戰能力。相對的，在 IOT 資安領域，擁有相對高的設備可視度，是為成功的關鍵條件，設備的辨識度在 IOT 領域中，可視為偵蒐性能指標，在不同產業別上 (如醫療、製造、OA)，能滿足常見或特定的設備，並辨識出該設備之廠牌、型號、作業系統、韌體版本、甚至於弱點，是否有輔助情資能豐富並說明設備的各項資安弱點，並給予後續修補或減緩風險的建議，是作為 IOT/OT 資安平台的重要關鍵能力。

SOAPA 架構與 IBM 作法

一般常聽見的 SOAR (security orchestration, automation, and response) 其實落在所謂 SOAPA (security operations and analytics platform architecture)架構的一部分。簡單而言，SOAR 常見於單一產品或工具進行資安事件處理與自動化，但就 SOAPA 而言，必須將資料收容、處理、分析並與資安維運整合。



企業建構 SOAPA 平台曠日廢時，並且需要各種客製化與分階段進行。若無取得專家顧問協助，對組織或企業而言是一項沉重的負擔。IBM Security 發揮自身產品優勢，整合 IBM Security Resilience、IBM Security QRadar、接入各種 IOT/OT/ICS 平台，輔以 IBM Security 自豪的情資 (IBM Security Intelligence)、IBM WATSON for Cyber Security、IBM X-Force Threat Management 顧問服務，協助企業與客戶管理 IOT/OT/ICS 各種資訊安全難題，簡化 SOAPA 平台的建置。

整合平台框架下，IBM Security 提供給企業或組織的優勢：

1. 整合 IOT/OT/ICS 資訊收容能力，包括：

- 提高設備與未納管設備的可視化程度
- 可疑活動的偵查與監控
- 內部特定設備的偵蒐 (如五眼聯盟規範外設備)
- 設備弱點可視度
- 整合性威情資平台
- 資安作為 (security action) 自動化回應

2. QRadar 與 Resilient 的整合是核心關鍵。QRadar 內建 Resilient plug-in，自動定期更新以支援最新使用案例 (use case)。依據事件的嚴重性或其他條件，甚至或是手動方式，由 QRadar 指定資安事件新增至 Resilient 成為調查案件，並且能自 Resilient 回饋調查的細節至 QRadar，增進偵測能力。

3. QRadar 與 Resilient 整合後，資安團隊可以手動或自動的從 Resilient 案件，在 QRadar 內部資料啟動搜尋，豐富案件資料加速調查進行。

4. QRadar Watson Advisor 與 Resilient 整合後，透過 AI 能力豐富調查資訊，增加案件的可視度，找出攻擊事件與 MITRE ATT&CK 相應程度，了解攻擊手法與深度，也幫助提高資安事件回應的準確性和即時性。

5. QRadar-MITRE content package for Resilient。透過此套件，QRadar 的攻擊事件經 由 QRadar Advisor with Watson 補充 MITRE ATT&CK 攻擊手法與技術資訊，並傳送到 Resilient，提供事件調查、威脅獵捕 (threat hunting)、後續控制措施修正重要參考依據。

關於 IBM

如果需要了解有關 IBM 更多信息，請訪問：
https://www.ibm.com/tw-zh/security

瞭解更多 IBM Security 產品資訊和最新案例

電話咨詢 IBM 專家
0800-016-888 按 1

聯絡 IBM 業務代表
https://ibm.biz/Bdqy8Z

訪問網站
https://ibm.biz/Bdqy8r