CYCRAFT
奧義智慧科技

產業客戶案例－政府 A 級機關：經濟部

臺灣政府機關的資安挑戰

網路犯罪活動頻繁，臺灣遭受的攻擊次數全球居冠，負責處理國家安全機敏數位資料的中央一、二級機關，以及外交、情報、國境安全、財稅、經濟、金融、醫療及重要民生基礎設施等單位，皆是國家級網軍攻擊的重點目標。跨部會施政平台、公文交換、稅務電子閘門、自然人憑證管理、刑案資訊整合等重要機敏系統，更是首當其衝。

近年來，公部門與關鍵基礎機構在遭遇網路攻擊後，主要蒙受兩大後果：個資外洩和系統癱瘓，例如 2022 年上千萬筆內政部戶政資料疑似在暗網公開兜售、2020 年中油與台塑內部系統遭植入勒索軟體而影響營運等重大資安事件。針對公部門的網路攻擊行動不僅降低了行政效率、增加額外的維護成本，也將動搖社會大眾對於政府單位的信任感，甚至像 2023 年臺北故宮逾十萬件文物圖檔外流，在中國網購平台上被低價出售一案，還可能觸動到敏感的國際地緣政治。

如何在攻擊發生前掌握資安防禦與事件應變的能力？如何在沒有攻擊事件、且不影響日常營運的前提下測試與評估保護措施的有效性？奧義智慧最新推出的 XCockpit 自動化威脅曝險管理平台，是我國經濟部選擇的解決方案之一。

經濟部業務範圍橫跨多元領域，除了促進工商企業發展、推動與他國經貿往來之外，還掌管多家國營基礎設施單位，包括台灣電力股份有限公司、台灣中油股份有限公司以及台灣自來水股份有限公司等。該部與所轄機構的投資招商、能源發展、創新研發計畫等機敏資訊，對於駭客而言都是極具攻擊價值的目標。因此，經濟部資訊處林聰仁處長極為重視該部與所轄單位面對攻擊行為的應變與處理，務求建立「高效率」、「全面性」的資安事件調查及鑑識流程。

奧義智慧 XCockpit Endpoint 三大特色，落實全場域自動監控

經濟部於 2023 年與奧義智慧合作，進行了為期 17 天的紅隊演練，奧義智慧 XCockpit 自動化威脅曝險管理平台於此期間有效監控了 1,371 台電腦，成功偵測到 8 台紅隊活動，並發出 97 封無誤報的告警通知，在平台上自動建立 53 件工單。

紅藍隊演練是目前臺灣 A 級政府機關檢驗資安韌性的常見作法之一，紅隊使用社交工程、組織流程漏洞等多元的攻擊手法，在限定時間內嘗試入侵組織，有助於補足其他檢測方式可能忽略的防禦邊界或因人為疏失而產生的防禦盲點。透過紅隊模擬真實攻擊，不僅能測試藍隊的防禦和回應能力、評估資安產品投資的適切性，還能讓演練結果更具參考價值，有助於單位每年檢視整體的資安架構。

經濟部此次演練展現了奧義智慧 XCockpit Endpoint 三大特色，最重要的是導入 AI 自動化鑑識技術，大幅降低監控所需的人力、時間與費用成本。XCockpit Endpoint 的儀錶板 (Dashboard) 會即時更新事件處理時間，在此次演練結束後，顯示其平均建單時間 (MTTD) 為1分鐘、平均分析時間 (MTTI) 為 23 分鐘。相較於未偵測出任何紅隊攻擊的其他事件管理廠商，偵測與分析速度明顯更為卓越。

在快速偵測和精準告警之後，XCockpit Endpoint 第二特色是監控完成後、會自動整併端點告警至工單系統，協助 IT 與SOC 團隊建立事件應變分工與管理流程。每一張工單皆有視覺化根因分析，方便第一線管理人員迅速掌握攻擊脈絡，也能快速排查相關事件與對應的 MITRE ATT&CK® 攻擊手法。

在操作上，XCockpit Endpoint 固然鉅細靡遺，介面設計非常清楚、容易上手。林聰仁處長在演練後讚譽：「XCockpit Endpoint 的 UI 設計邏輯清晰，讓沒有資安背景的主管或同仁都能理解呈現的資訊，滿足跨部門協作需求、降低一來一往的溝通成本。」

在地資安產品，連結國際脈動

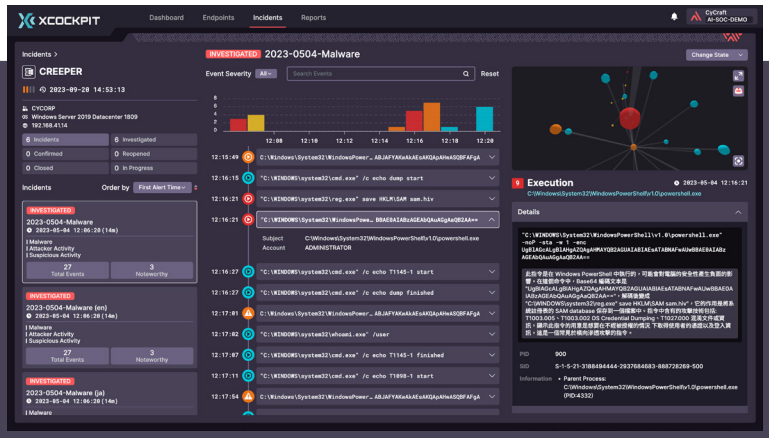
一直以來，臺灣政府機關和關鍵基礎設施承受的網路攻擊方興未艾，烏克蘭公部門在烏俄戰爭中的處境可謂前車之鑑。因此，政府單位採用的資安產品能與攻擊並行已是必然、超前防禦才是未來的重要目標之一。

本次演練，奧義智慧成功拆解並分析了紅隊使用的攻擊手法，也比對出部分手法與近期美國網際安全暨基礎設施安全局 (CISA) 示警的攻擊手法相同。該手法以美國國內的關鍵基礎建設設施為主要目標，並藉由身分識別攻擊方式入侵企業內部環境。奧義智慧在對接國際第一手情資後，XCockpit Endpoint 可自動產出分析報告與防禦建議，有助受駭單位應對潛在威脅，強化整體資安防禦。

對此，林聰仁處長深有感觸地表示：「對政府組織來說，我們需要的不只是能夠按照規格書提供服務的廠商，更需要的是能夠與我們共同成長、面對不斷變化的攻擊手法的夥伴。」奧義智慧的紅隊演練和 XCockpit Endpoint 不僅提供了自動化、快速且全面的資安防禦，更能和組織與時俱進，一同處理未來的資安挑戰。

經濟部與奧義智慧資安防護三大要點：

1. 紅隊演練在不影響日常運作下，有效盤點並發掘單位尚未偵測到的潛在漏洞。
2. 奧義智慧 XCockpit 自動化威脅曝險管理平台引入 AI 鑑識技術，自動化、可視化、量化各設備與用戶的風險，快速提升單位內部的資安防禦有效性。
3. 對接國際情資與 MITRE ATT&CK® 攻擊手法，提供簡明易懂的摘要報告與可立即執行的處置建議，提高跨部門溝通效率、持續賦能單位以面對多變的資安挑戰。



XCockpit 導入 AI 大型語言模型，自動化產出鑑識摘要，輔助企業資安團隊快速了解案情。
*示意圖內容僅為產品展示，所有數據及資料均與客戶無關。

關於奧義智慧科技

奧義智慧科技 (CyCraft Technology) 是一間專注於 AI 自動化技術的資安科技公司，研發出自動化的威脅曝險管理平台「XCockpit」，整合端點偵測與回應、特權帳號衝擊分析、外部攻擊面管理等防禦構面，提供一站式的全方位自動化資安防護。

奧義智慧科技長期為亞太地區的政府機關、警政國防、銀行和高科技製造產業提供專業資安服務，並獲得淡馬錫控股旗下蘭亭投資 (Pavilion Capital) 的強力支持、國際頂尖研究機構 Gartner、IDC、Frost & Sullivan 的多項認可，以及海內外大獎的多次肯定。

CYCRAFT 奧義智慧科技
聯絡奧義：cycraft-tw@cycraft.com +886-7739-0077